

Cisco FirePOWER with Gigamon Inline Deployment Guide

COPYRIGHT

Copyright © 2016 Gigamon. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without Gigamon's written permission.

TRADEMARK ATTRIBUTIONS

Copyright © 2016 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal- trademarks. All other trademarks are the trademarks of their respective owners.

Contents

Use Cases
Use Case 1: Load Balancing (Parallel) mode
Use Case 2: Serial Mode
Deployment Prereguisites
Architecture Overview
Access Credentials
2 Configurations
Cisco FirePOWER Configuration: Inline Tools11
Step 1: Create default access control policies for each sensor
Step 2: Register Devices
Step 3: Configure Inline Set
Step 4: Configure Cisco FirePOWER Settings14
Step 5: Create Sensor policies
Step 6: Apply the device level policy to global access policy and assign to target sensors
Step7: Deploy Policies
GigaVUE-HC2 Configuration
Configuring the GigaVUE-HC2 Inline Network and Inline Tools
Step 1: Configure Network and Tool Ports
Step 2: Configure the Inline Networks
Step 3: Configure the Inline Tools
Step 4: Configure the Inline Tool Group
Step 5: Configure the Inline Serial Tools
Configuring the Inline Traffic Flow Maps
Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule
Step 2: Configure the Inline Traffic Collector Map
Step 3: Change Inline Network Traffic Path to Inline Tool
Testing the Functionality of the FirePOWER Inline Tool
IPS Test Results
DLP test results
Load Balancing between Malware Sensors:
3 Summary and Conclusions43

1 Overview

Gigamon's GigaSECURE Security Delivery Platform and Cisco FirePOWER offer a combined solution that meets today's active inline security needs. This solution can scale as the protected network infrastructure grows with the addition of network links. With Gigamon's bypass functionality in place, quick addition and removal of inline security devices for maintenance, software/firmware upgrades, or simply to move the device to another area of the network is seamless, eliminating the need to schedule downtime during off-peak hours. The inline tool group with Cisco FirePOWER ensures that the inline security *service* remains available regardless of appliance maintenance or failure. Additionally, Gigamon's bypass protection capability provides continuous network availability in the event of failure of any GigaSECURE nodes used for bypass protection.

The Cisco FirePOWER System is an integrated suite of network security and traffic management products, deployed either on purpose-built platforms or as a software solution. The use cases in this guide were validated with virtual FirePOWER sensors (also called NGIPSv) and virtual FirePOWER Management Center deployed on an ESXi host using the VMware vSphere Hypervisor. The Cisco virtual FirePOWER appliance was validated in conjunction with a GigaVUE-HC2 node. The GigaVUE-HC2 is a 4-slot visibility appliance that is part of the GigaSECURE Security Delivery Platform. The steps outlined in this guide are also applicable for inline deployment of a physical FirePOWER appliance with a Gigamon GigaVUE-HC2.

The solution described in this guide is based on a standard active inline network and tool deployment where virtual NGIPSv sensors configured to act as Intrusion Prevention System (IPS), File Download Detection, and Malware appliances are directly cabled in series to one GigaVUE-HC2 chassis. Upon full deployment, the GigaVUE-HC2 sends only the traffic of interest to these inline tool groups for traffic analysis, file and malware inspection.

This chapter covers the following:

- · Use Cases
- · Deployment Prerequisites
- Architecture Overview
- Access Credentials

Use Cases

This section describes the following use cases:

- Load balancing (parallel mode)
- Serial Mode

Use Case 1: Load Balancing (Parallel) mode

There are multiple network links of varied speeds and media in an infrastructure that need to be protected by Cisco security solutions. When the aggregate traffic exceeds the capacity of any single Cisco sensor, multiple sensors must be deployed with the ability to distribute traffic among the group of sensors. The Gigamon GigaSECURE Security Delivery Platform provides the ability to select traffic of interest, while bypassing the rest, then distributing the selected traffic of interest amongst two or more sensors.

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 traffic will be distributed amongst the remaining members, thereby ensuring availability of the security functions provided by Cisco FirePOWER.

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 a setting in the inline network link, eliminating the need for physical change control procedures.

Use Case 2: Serial Mode

This use case is similar to the above except there are several different types of Cisco inline security tools that network traffic will pass through sequentially. Traffic can be filtered in the Gigamon GigaVUE-HC2 for each inline tool so only relevant traffic will flow through that tool.

The above two use cases are validated together by configuring IPS and DLP sensors in series going to two Malware sensors in parallel for load balancing. Refer Figure 1-1. However, if only serial or parallel mode is desired for other specific use cases then the relevant subset from this user guide can be leveraged.

Deployment Prerequisites

The Gigamon and Cisco FirePOWER combined solution consists of the following:

- GigaVUE-HC2 chassis running GigaVUE-OS 4.5 with:
 - 1 TAP-HC0-G100C0 Copper bypass module
 - o 1 TAP-HC0-D25AC0 Fiber bypass module
- · GigaVUE-FM version 3.2 Fabric Manager
- Cisco Virtual FirePOWER Management Center appliance version 6.0.0 (Snort version 2.9.8 GRE)
- · Cisco Virtual Next-Generation IPS (NGIPSv) for VMWare version 6.0.0
- Two Windows virtual machines used to simulate as server and a client. The server VM runs Webserver uploaded with files types such as .exe, pdf, RIFF and malware files. When the user from a client VM attempts to access these files, the FirePOWER appliance inspects the files and depending on the configured policy in FirePOWER, the content would be blocked or allowed and the action logged.

Note: The GigaVUE-HC2 offers inline bypass modules for both 1Gb Copper and 10Gb Fiber interfaces. Both types of modules have the same bypass functionality. The 10Gb Fiber bypass module additionally offers tool ports on the same module. For this deployment guide the Copper interface module was used on the GigaVUE-HC2 as the Cisco NGIPSv was set up with 1Gb copper interfaces. In this deployment guide, only the tool ports on the GigaVUE-HC2 Fiber bypass module are used.

This guide assumes that all appliances (both physical and virtual) are fully licensed for the features used, management network interfaces have been configured, and an account with sufficient admin privileges is used.

This document is intended to provide the information of integrated solution for evaluation purpose and should be modified appropriately for production deployments.

Architecture Overview

This section presents the combined solution using a GigaVUE-HC2 inline bypass node with Cisco FirePOWER System. The reference architecture in Figure 1-1 shows the position of each component in the overall infrastructure, where all network components and inline security tools are connected directly to the GigaVUE-HC2. The proposed monitoring configuration uses eight ports on module 1 for inline tools, and four ports on module 3 as protected inline bypass ports. Figure 1-2 shows the logical layout of the setup where traffic flow traverses the IPS, DLP, and Malware engines in the Cisco FirePOWER suite sequentially. The two malware engines are connected in parallel for load-balancing purposes. Figure 1-3 shows the traffic flow diagram. All inline bypass links are inherently bidirectional. The traffic flow diagram below shows only one direction of traffic flow to simplify the illustration. Ports 1,6,7,12 represent inline network ports while ports 2,3,4,5 represent inline tool serial and ports 8,9,10 and 11 represent inline tool group ports.



Figure 1-1: Gigamon Inline Bypass with Cisco FirePOWER System



Figure 1-2: Logical Layout for Inline tools



Figure 1-3: Traffic Flow Diagram

Note: For any inline configuration, it is critical to align tools so that the trusted (or inside or client side) connection is on the correct port of the tool or tools. With out-of-band monitoring, port ordering is less important because only a copy of the original packet is delivered to the out-of-band tool with the original packet in the network unaffected. For inline monitoring, failure to ensure that the trusted and untrusted sides are connected properly will cause the inline tool to improperly apply protections. For example, attaching the Internet connection to the inside port would cause a firewall to permit almost any traffic to enter the protected network. Inside client-originated traffic incorrectly connected to the outside port of a firewall would likewise have virtually all communications blocked.

The setup in this guide has FirePOWER virtual sensors deployed and configured with two network port groups – Inside and Outside. Data flows from inside (trusted) side where the clients reside to outside (unprotected) side for Internet access and vice versa. The network adapter (vmnic) assigned to Inside and Outside port group of FirePOWER sensors should match Port A and Port B, respectively, of inline network and inline tool configuration in a GigaVUE-HC2.

Access Credentials

The following are the Gigamon GigaVUE-FM default access credentials:

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

The following are the Cisco virtual sensor/management center access defaults:

- · Username: admin
- Password: Admin123

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-HC2 with Gigamon's centralized management application GigaVUE-FM. For the equivalent H-VUE and CLI configuration commands, refer to the *Gigamon-OS H-VUE User's Guide and GigaVUE-OS CLI User's Guide*, respectively, for the 4.5 release.

2 Configurations

This chapter describes the configuration procedures for GigaVUE-HC2 through GigaVUE-FM and procedures for NGIPSv sensors policies through Cisco FirePOWER Management Center. The procedures are organized as follows:

- Cisco NGIPSv Configuration: Inline Tools
- · Gigamon GigaVUE-HC2 Configuration: Inline Network and Inline Tool, Series Groups

The Cisco FirePOWER Management Center provides a centralized management console with a Web interface that you can use to perform administrative, management, analysis, and reporting tasks. For this deployment guide, the procedures focus on setting up the NGIPSv sensors with policies. This chapter assumes that all four FirePOWER virtual sensor nodes are deployed and setup with initial jumpstart configuration. Note that all NGIPSv sensors are deployed virtually with the same ovf image. Based on the licenses applied and policies configured, these sensors can be tuned to perform different roles. In this guide, four sensors are used – one sensor configured with IPS policy, a second sensor configured with file download detection policy and third and fourth sensors, connected in parallel for load balancing, configured with malware detection policy.

All the sensors are directly connected to the GigaVUE-HC2 as shown in Figure 1-1. All GigaVUE-HC2 ports that connect to virtual NGIPSv sensors should be configured as port type *Inline Tool*. Furthermore, all GigaVUE-HC2 inline bypass ports that connect to the inline network should be configured as port type *Inline Network*. For specific instructions on how to complete these tasks, refer to the Help Topics links in GigaVUE-FM.

Cisco FirePOWER Configuration: Inline Tools

This section explains the steps to configure various elements of Cisco FirePOWER inline sets, access control policies, and related settings.

Step 1: Create default access control policies for each sensor

Access control is a hierarchical policy-based feature that allows you to specify, inspect, and log (non-fast-pathed) network traffic. Especially useful in multi-domain deployments, you can nest access control policies, where each policy inherits the rules and settings from an ancestor (or *base*) policy. You can enforce this inheritance or allow lower-level policies to override their ancestors. Each managed device can be targeted by one access control policy.

In the Cisco FirePOWER Management Center, do the following:

- 1. Select to Policies > Access Control > Access Control.
- 2. Click **New Policy**, and then create a default policy from any source zone to any destination zone keeping all the default parameters intact.
- 3. Repeat this step 2 for each sensor.

Overview Analysis Policies	Devices Objects	АМР	Deploy 🧕 System Help 💌 admin 💌
Access Control + Access Control	Network Discovery	Application Detectors Correlation Actions •	
			Object Management Intrusion Network Analysis Policy DNS Import/Export
			O New Policy
Access Centrol Policy		Status	Last Modified
File Download Detection - DLP		Targeting 0 devices	2016-02-01 13:20:17 Modified by "admin"
IPS		Targeting 0 devices	2016-02-09 16:30:45 Modified by 'admin'
Malware-Detection		Targeting 0 devices	2016-02-01 13:20:18 Modified by "admin"

Step 2: Register Devices

For a sensor to be managed by Cisco FirePOWER Management Center, it needs to be registered.

In the Cisco FirePOWER Management Center, do the following:

- 1. Select Devices > Device Management > Add Device.
- 2. Fill out the information as shown in the following figure, and then click Register.

Host:	10.115.154.11	
Display Name:	IPS_sensor	
Registration Key:	Gigam0n123	1
Group:	None	~
Access Control Policy:	IPS	~
Licensing		
Protection:	Ч.	
Control:	v	
Malware:	A	
URL Filtering:		
VPN:	π.	
 Advanced 		
To add Firepower T with the Smart Licensir	hreat Defense devices, register this console na Server.	

Notes:

- In the Registration Key field, enter the same registration key used while configuring sensor jumpstart settings.
- Choose an Access Control Policy to be used by the device.
- · Choose licenses to apply to the device.
- 3. Repeat step 2 for each sensor.

The finished Device Management page should look similar to what is shown in the following figure.

Overview Analysis Policies Devices Objects	AMP		Deploy 🤗 Syste	m Help * admin *
Device Management NAT VPN Platform Settin	ngs			
			By Group	• 🔕 Add •
				🔾 Add •
Name	Model	License Type	Access Control Policy	
4 🧔 Ungrouped (4)				
FileDownloadDetection_Sensor 10.115.154.12 - NGIPSv for VMware - v6.0.0	NGIPSv for VMware	Protection, Control, Ma	File Download Detection - DLP	28
IP5_Sensor 10.115.154.11 - NGIPSv for VMware - v6.0.0	NGIPSv for VMware	Protection, Control, Ma_	IPS	/ 8
MalwareDetection1_Sensor 10.115.154.13 - NGIPSv for VMware - v6.0.0	NGIPSv for VMware	Protection, Control, Ma	Malware-Detection	28
MalwareDetection2_Sensor 10.115.154.14 - NGIPSv for VMware - v6.0.0	NGIPSv for VMware	Protection, Control, Ma_	Malware-Detection	2.8

Step 3: Configure Inline Set

Before you can use inline interfaces in an inline deployment, you must configure inline sets and assign inline interface pairs to them. An inline set is a grouping of one or more inline interface pairs on a device; an inline interface pair can belong to only one inline set at a time. This is a way to bridge together the incoming and outgoing interface for the traffic.

In the Cisco FirePOWER Management Center, do the following:

- 1. Select **Devices > Device Management > Inline Sets**
- 2. Click Add Inline Set.

Overview Analysis Policies	Devices Objects AMP		Deploy 🔩 System	Help v edmin				
Device Management NAT	VPN Platform Settings							
FileDownloadDetectio	on_Sensor		You have unapplied					
Device Interfaces Inlin	e Sota							
				Add Inline Set				
Name -		Interface Pairs						
InineDLP		eth1 eth2		29				
5 **46C 0F 2								
Overview Analysis Policies	Devices Objects AMP		Deploy 🤷 System H	ep v admin v				
Overview Analysis Policies Device Management NAT FileDownloadDetectic	Devices Objects AMP VPN Platform Settings		Deploy 🔒 System H You have	ielp + admin + unapplies changes				
Overview Analysis Policies Device Management NAT FileDownloadDetectic NGPSv for VMware Device Interfaces Inline	Devices Objects AMP VIN Platform Settings on_Sensor		Deploy 🔍 System H	ielp * edmin * unapplied changes				
Overview Analysis Policies Device Management NAT FileDownloadDetectic GBPSv for VMware Device Interfaces Inline Name	Devices Objects AMP VPN Platform Settings on_Sensor sets security Zone	Used By	Deploy 9 System H You have MAC Address	elp + admin + wappled changes				
Overview Analysis Policies Device Hanagement NAT FileDownloadDetectio IGPSv for VMware Device Interfaces Infine Name Rame Z eth1	Devices Objects AMP VPN Platform Settings on_Sensor	Used By InlincDLP	Deploy 🍕 System H You have MAC Address 00:30:16:42:40:13	elp + admin + unapplies changes				

Step 4: Configure Cisco FirePOWER Settings

a) Time Synchronization Setting

In the Cisco FirePOWER Management Center, do the following:

- 1. Select **System > Configuration**.
- 2. Select **Time Synchronization** from the navigation panel on the left. Change the NTP server if needed.

Overview Analysis Policies D	evices Objects AMP						Deploy	9 Syster	Help *	admin +
		Configuration	Users	Domains	Integration	Updates	Licenses *	Health * P	Ionitoring •	Tools *
										10020000
										- save
Information										
HTTPS Certificate	Serve Time via NTP	Enabled								
External Database Acoms		Manually in Local Co	nôguration							
Detabase	Set My Clock	O Via NTP from								
Management Interfaces		0.sourcefire.pool.ntp.or	g, 1.sourcefin	5						
Process										
Remote Storage Device										
Change Reconciliation										
Acoms Control Preferences										
Access List										
Audit Log										
Deshboard										
DNS Cache										
Email Notification										
Intrusion Policy Preferences										
Language										
Login Banner										
Network Analysis Policy Preferences										
SNMP										
571G Compliance										
Time										
Time Synchronization										
Shell Timeout										
Vulnerability Mapping										
VMware Tools										

b) Default Settings Policy

A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. This is done by configuring "platform settings". Any changes to a "platform settings" policy affects all managed devices where the policy is applied.

In the FirePOWER Management Center, do the following:

- 1. Select **Devices > Platform Settings**.
- 2. Name the policy Default Settings Policy. Add all devices. Refer to the following figure.

liting Policy: Default (Last M	odified: Mon 08 Feb 2015 02:32:26 PM PST) Devices			Save Cerc
tukey Name Default hildy Description Default System	Select devices to which you would like to apply the policy. Available Devices , Search by name or value		Selected Devices	
Access Lat Audit Log Exernal Automotication Linguispe Lingui Benuer Soliti Tremeli Soliti Tremeli Stilli Completion These Synchronization	an PS, Sereer an Meleo e Ontaria S, Sen., an Pitche-manDetector, an PathereDetector, Sen.	Add the Policy	MolvereOrection FileDownloadDetection MalvereOrection1_San.	

c) Time Synchronization for Sensors

Select **Time Synchronization** from the navigation panel on the left. Confirm that the **Via NTP from Management Center** radio button is selected. You can also use a Cisco FirePOWER Management Center as a Network Time Protocol (NTP) server for its managed devices.

Overview Analy	vsis Policies Devices	Objects AMP	Deploy 🌒 System Help + admin +
Sevice Management	t NAT VPN Platfo	rm Settings	
Editing Policy: D	Default (Last Modified: M	on 08 Feb 2016 02:32:26 PM PST)	Same Cancel
Policy Name	Default		
Policy Description	Default System Policy		
Access List Audit Log External Authentics Language	Set My Clock	Via NTP from Management Center Via NTP from	
Login Banner			
Shell Timeout			
STIG Compliance			
Time Synchronia	ation		

Step 5: Create Sensor policies

a) Intrusion Policy

To add Intrusion policy through Cisco FirePOWER Management Center, select **Policies > Access Control > Intrusion**.

The first example below adds a rule to replace and allow a string with "ProjectQ" text string with "ProjectR" in a traffic flow. The second example detects and blocks a flow when "ProjectZ" text string is detected. These policies are created with following rules,

alert tcp any any -> any any (msg:"ProjectQ replaced"; content:"ProjectQ"; replace:"ProjectR"; sid: 1001001; rev:1;)

alert tcp any any -> any any (msg:"ProjectZ detected"; content:"ProjectZ"; sid: 1001002; rev:1;)

Note: These simple string match detection rules are created for testing purpose only. Refer to Cisco's documentation to learn how to create policies manually.



Overview Analysis Polici Access Control + Intrusion	Les Devices Objects	AMP Deplo	y 🤒 System Help 🔹	admin +
Edit Policy: Tech-Da	ay-IPS			
Policy Information	Rules			< Bock
Policy Information Rules	Rule Configuration Rule Content Category epp-detect biockies browser-firefox browser-firefox browser-other browser-other browser-other	Filter: Cetegory: "local" I selected rule of 2 I selected rule of 3 I selected rule of 4 I selected rule of 3 I selected rule of 4 I selected rule of 4 I selected rule of 5 I selected rule of 6 I selected rule of 7	Policy → 3 ▼ C Q → ×	× *
	browser-webict content-replace decoder exploit-kit file-fash file-fash file-fash file-identify file-identify file-identify	Hide details Suppressions (0) Dynamic State (0) Averts (0)	K (L d 1)	N Add O Add O Add
	Ne-multimedia Ne-office Ne-other	Comments (0) Documentation		O Add
	19-03 Classifications Microsoft Vulnerabilities Microsoft Womma Platform Specific Preprocessors Priority Rule Update	rule alert top any any -> any any (mag:"Project2 detected"; content:"Project2"; sid:100 Summary This rule does not have documentation Palse Positives None known at this time False Negatives None known at this time SRU	1001) rev;1) classtype:unknown;	3

Overview Analysis Polic	ies Devices Objects Af	P		Deploy 🔒 System	Help + admin +
Access Control + Intrusion	Network Discovery Applicat	ion Detectors Correlation	Actions •		
				Import/Expert Intrusien Bules Access Control N	etwork Analysis Policy
				Compare Policie	s O Create Policy
Intrusion Policy	Drug when Inline	Status		Last Hodified	
IDS-1	Yes	Used by 1 eccess control ; Policy up-to-date on all 1	zolicy devices	2016-02-01 14:57:50 Modified by "admin"	1560 / 8
Tech-Day-IPS	Yes.	Used by 1 sccess control (Policy up-to-date on all 1	zolicy devices	2016-02-01 14:58:01 Nodified by "admin"	EQ/a

b) Malware Policy

To add Malware policy through Cisco FirePOWER Management Center, select **Policies > Access Control > Malware and File**

In the following example, certain file formats such as PDF, graphics, and executables are checked for malware content. If any malware is detected, file access is blocked.

Malware-Detection							(B Sen) (C
Rules Advanced	View File Rule	ny	v	Action	Block Malware	¥	T X
File Types Category: Dynamic Analysis Cate Category: Stratem Res Category: Stratem Category: Strated () more)	File Type Categories	riy.	File Ty	pes	Dynamic Analysis Coccil Malware Analysis & Reset Connection		Unknown Open Custom Selected File Categories and Types
	Office Documenta Archive Mutomedia Executables Por Res Encoded Graphics System Ries Dynamic Analysis Cape Local Maiware Analysis	16 17 3 7 1 0 0 2 2 4 0 2 2 4 0 2 2 3 5	4 Se 72 40 80 80 80 80 80 80 97 97 97	(7-20 cm (7-20 cm (208 (Hicto 3 (Compres NARY_DATA NHEX (Mac) (3202 cm (3202 cm (3202 cm (3202 cm (3202 cm) (3202 cm	and description present file) with Access 2007 free) pod andhive file) (Universal Binary/Davis Bytes most Binaries & Compressed A greated anthree) Unive presided with the core all Active presided with the core all Active created with the core all	Add	Category: Dynamic Analysis Capable S Category: System files S Category: Graphics S Category: Proceed S Category: Executables S Category: Multimedia S Category: Multimedia S Category: Office Documents S

c) File Inspection Policy

To add File Inspection policy through Cisco FirePOWER Management Center, select **Policies > Access Control > Malware and File**.

In the first example below, certain file formats such as PDFs, graphics, and executables would be reported as detected and event logged for the user.

In the second example, RIFF files such as audio/video would be blocked and event logged for the user.

Overview Analysis Policies	Devices Objects	АМР				Deploy 🤷 System	Help + admin +
Access Control + Malware & File	Network Discovery	Application Detectors	s Correlation	Actions *			
File-inspection						B	ave Cancel
Rules Advanced							
						Used Its 1 access control polyc	Add File Rule
Pile Types	Applicatio	in Protocal	Direction	Action			
Category: Executables Category: Archive Category: Ortho Documents Category: Dynamic Analysis Capable (5 more)	Any		Алу	Interest	Files		10
Raff POP	Any		Any	X Block	Files with Reset		20

Overview Analysis Polic Access Control - Halware & F	ies Devices Objects file Network Discovery	AMP Application D	etectors Correlation Actions •	_	Deploy 🐴 System	Help + admin +
File-inspection					18	Seve Grant
Rules Advanced	Edit File Rule	law.	N Advant of Database Street		Store files	1 ×
File Types	Direction of Transfer	Any	v Veter veter		1 Sec. 1 Sec. 1	
Category: Executatives Category: Archive Category: Office Documents Category: Dynamic Analysis Cape (5 more)						za
Ager Por	Office Documents Office Documents Arthve Multimodia Executables POF files Encoded Graphics System Nies Dynamic Analysis C Local Melware Analysis	20 18 20 11 2 2 0 12 4pable e yos Capable 5	Proc Types Search name and description Z2 (7-20 compresent file) S35644 S45644 S55644 S55644 S55644 S55644 S55644 S55644 S55644 S5564 S5564 S5564 S556 S556 S556 S556 S556 S556 S55 S5 S5	Add	Category: Executations Category: Antive Category: Office Documents Category: Office Documents Category: Dynemic Analysis Capacie Category: System Ries Category: System Ries Category: Forded Category: PDF Ries Category: Multimedia	8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8
					Save Can	ori

Access Control + Mal	ware & File Networ	* Discovery	Application	Detector	Correlation Actio	na •		Seve Creat
Hules Advanced	View File Rule						7.X	O MI IN LIN S M
Pile Types	Application Protocol	Any	*	Action	X Block Files	*	Store files	
Category Executables Category Ardive Category Office Discor Category Office Aru (5 more)	Direction of Transfer	Arry	T		Reset Connection			20
BUTT PDF	File Type Categories		File Ty	pes :			Selected File Categories and Types	18
	Coffice Documents Arthive Multimedia Decostables POF files Decostables Graphica System files Oynamic Analysis Lucel Malware Anal)) Capable Hyels Capable	0 4 500 8 72 0 900 1 AO 2 AM 2 AM 2 AM 3 AM 4 AM 5 AM	ICh clame (2-31) cor (IVE (Wor CDB (Hich F (Advanc R (Advanc) R (A	and description typessed file) taxes for registry have (ABCI) such Access 2007 file) and Hocks Files to destail in Michi-Late Code: File) and anthree file) th Windows Media Audorition Indows Audorum attact file) All researce Anthree Testas (Ine). Au	Add	RIFF (Assured Interchange File Parmat) ()	

Overview Analysis Policies	Devices Objects	AMP			(De	ploy 🥞 System	Help * admin *
Access Control + Malware & File	Network Discovery	Application Detectors	Correlation	Actions •			
							Appens Control
						Compare Policies	O New File Policy
Flie Policy					Last Hodified		
Malware-Detection					2016-02-14 23:30:38 Modified by "admin"		100
File-inspection					2016-02-11 23:20:26 Modified by "admin"		2Da

Step 6: Apply the device level policy to global access policy and assign to target sensors

This section describes how to apply the device level policy to the global access policy, and then assign it to the target sensors.

a) IPS Access Control Policy

To assign IPS sensor level policy to global access control policy through Cisco FirePOWER Management Center, do the following:

- 1. Select Policies > Access Control > Access Control > IPS > Edit > Inspection.
- 2. Select the **Intrusion Policy** of interest. In the following example, the **Intrusion Policy** selected is **Tech-Day-IPS**.

IPS			Editing R	ule - Monit	or Only						7 ×	0. cm
dentity Policy: 16	111	SSL Policy:	Action v	onitor Only Allow			V IPS: Tech	Ony-SPS	Variables	Have a default Files: no respectiv	Logging:	
Autor Securit	ty Intelligence	HTTP Response	Zones	Networks	VLAN Tags	4 Users	Applications	Ports	URLE	ISE Attributes	Comments Logging	Publicy etailityments (
-	Several /	Dest Zoner	Tech-Day	sicy UPS					(*) 🖉	Variable Set Default Set		
· admin_sates	045 (2-1) MY (1)	4410 10	Haiware Po None	άξγ							(w)	
* standard_cat	epory (1-1)							_		ок	Cancel	
1 Mansar Drift	()	-	75		100	- 10	199	**	-	9. D#	V Alter	0
· mot, categor	r (+) 6 Int Little contragramy.	Add Rule										J.
Default Action			_	_		_	_	_	Netwo	rk Discovery Only		-

3. Now assign it to targeted devices using the **Policy Assignments** link in the right hand side corner.

Overview Analysis	Policies Devices Objects AMP			Dephy 🇌 Syr	stern Help + admin +
Access Control + Acces	a Control Network Discovery Application Detectors	Correlation Ac	ctions •		
IPS					Const.
Identity Policy: Note	SSI, Policy: front				
4 10	Policy Assignments			7 × 7	Percy Assignments (1)
Rules Security Intelli	Targeted Devices				
A Filter by Deven	Select devices to which you want to apply this policy. Available Devices		Selected Devices		
· Handstory - 195 (1-5	Search by name or value		#IPS_Sensor	0	
admin_sategory (-) There are an ourse in this o	FieldownicadDetection If 5_server MalwareDetection1_Sen MalwareDetection2_Sen				20
standard_category () Mandar Only	- 3 c. 40 20 c and 5 2 5 6 4 1	Add to Pulsy	Impacted Devices		1 - 11 + 24
Pool, Category (-) There are no more at the s					+
Default Action					112 F
				OK Cancel	
1 Sov Selected				Deploying 1 - 1 of 1 rules (1), (1)	Rope 1 of 5 $> > 6$

b) File Inspection Access Control policy

To assign File Inspection sensor level policy to global access control policy through Cisco FirePOWER Management Center, do the following:

- Select Policies > Access Control > Access Control > File Download Detection-DLP > Edit > Inspection.
- 2. Select Malware Policy as File-inspection.

Overview Analysis Polic	es Devices Objects AM		Onstoy 🔥 System Help + admin +
Access Control + Access Cont	rol Network Discovery App	ication Detectors Correlation Actions •	
File Download Deter	ction - DLP	Editing Rule - File Inspection	7 X
Listentity Palicy: 1004	SS. Polevi Simi	Name File Inspection	Hove
		Action of Allow PS: no policies Variable	es: 0/2 Piles: File-Inspection Logging:
Ruine Security Intelligence	HTTP Responses Advanced	Zones Networks VLAN Tags Users Applications Ports URG	a ISE Attributes Comments
R Filler by Device		Entrustes Belles/	Uniohis Cat
e Name Zones	Dest Source Dest Zanes Networks Nation	None V	Default for
· Handstory - File Download C	Henertium - OLP (3-1)	Maiware Policy	
w. admin_category (-)		File-inspection	* <i>2</i>
There are no rules of the pategory	Add Aule		
* standard_category (1-1)			OK Canal
1. Ne Inspection and			- VAIN 0 10 1 10
· Outsult - File Download Dete	ethin - DLP (+)		
• rest_category (•)	And Aute		
Default Action		Network Discovery Only	

3. Now assign it to targeted devices using the **Policy Assignments** link in the right hand side corner.

The second s	Dallas Ascissorante				P.
TOWNERA SHIERS, 19506	Policy Assignments			1.4	2013. 11
Bulles Security Intellig	Select devices to which you want to apply this policy.		Selected Devices		CT verso verstoverse (1)
	0, Search by same or value	1	FieDownloadDetection	0	for any a
Annual Annu	MaleareDetection1_Sen.	Add to Palloy	Ingetted Devices		20 20 20
Default Action			OK	Cancel	

c) Malware Detection Access Control Policy

To assign Malware-Detection sensor level policy to global access control policy through Cisco FirePOWER Management Center, do the following:

- 1. Select Policies > Access Control > Access Control > Malware-Detection > Edit > Inspection.
- 2. Select Malware Policy as Malware-Detection.

Overview Analysis Policies	Devices Objects	AMP				Deptoy (System Help + admin +
Access Control + Access Control	Network Discovery	Application Detectors	Correlation	Actions *			
Malware-Detection	Editing Rule - Alk	w Rule				†.×	El ITAL Q Greet
	Name Alow Rule			C Enabled	Move		
Identity Policy: Mana Si	Action 🖋 Allow		· IPS: no p	olicite Variables:	U/F Files: Nalware Detection	Logging:	
	Zones Network	IS VLAN Tage User	a Applications	Ports UIILS	ISE Attributes	Comments	torge I 📉 Pullcy Assignments (2)
Rater Security Intelligence HT			A Second Concession		Inspection	Logging	
B fitter by Dervice	Intrusion Policy				Variable Set		er - 36
Barris Des	None			×	Charles for		-
- Hendeling & Helmann Detection (1)	Melware Policy						
· admini_safegory (-)	Malware-Detection					(H) 🖉	20
These are no none in the congress, Add I					DK	Cancel	
· standard_compory (1-1)	6					-	×
1 Alter Auto and Anto							No
w Default - Halvere Detection (-)							
• root_category (-) There are no color in this company: Add A	64						#4
Default Action					Network Dissivery Only	8	
1 Now Selected					Disclaring	3 - 1 of 1 mins	(/ Page 1) #1 2 7 6

3. Now assign it to targeted devices using the **Policy Assignments** link in the right hand side corner.

Overview Analysis	Pulicies Devices Objects AMP			Darry 🔥 Syst	em Helg v admin v
Malware-Detecti	Control Network Discovery Approxition Detactors	Correlation Ac	oons *		Certai
Edentity Palicy: Sone	Policy Assignments Targeteit Devices Select devices to which you want to apply this policy. Available Devices		Selected Devices	* *	🕂 Policy Assignments (2)
Kanss Same Kansser Mandetopy - Mathematic Admini, category (1) There are necessary in the first administration of the first admin	Bearth by name or value FieldownikaeOntection, FieldownikaeOntection, FieldownikaeOntection, FieldownikaeOntection, TelewardOntection,	Add to Policy	MawwanDetection1_Sen MawanVDetection2_Sen	3	8 7 * 2 0 8 0 4 2 0 8 0 4 2 0
There are no nairs in the or Default Action			Desires	K Carool	

The completed Access control policy page should look similar to what is shown in the following figure.

Overview Analysis Policies	Devices Objects	АМР	Deploy 🍳 System Help = admin =
Access Control + Access Control	Network Discovery	Application Detectors Correlation Actions •	
			Object Management Indusion Network Analysis Policy DNS Import/Export
			New Policy
Access Control Policy		Status	Last Hodified
File Download Detection - DLP		Targeting 1 devices Lip-to-date on all targeted devices	2016-02-01 13 20:17 Modified by "admin"
195		Targeting 1 devices Up-to-date on all targeted devices	2016-02-09 16:30:45 Modified by "admin"
Mahware-Detection		Targeting 2 devices Up-to-date on all targeted devices	2016-02-01 13 20 18 Modified by "admin"

Step7: Deploy Policies

Click **Deploy** in the upper right hand corner of the Cisco FirePOWER Management Center UI. Check the checkboxes for all devices, and expand the list to see the details.

Depl	oy Policies Version: 2016-02-09 04:30 PM		? ×
	Device	Group	Current Version
V 3	MalwareDetection2_Sensor		2016-02-09 04:30 PM
	Access Control Policy: Malware-Detection		
	Intrusion Policy: Balanced Security and Connectivity		
	🛇 – Intrusion Policy: No Rules Active		
	File Policy: Malware-Detection		
	ONS Policy: Default DNS Policy		
	Platform Settings: Default		
	Network Discovery		
	Device Configuration		
	FileDownloadDetection_Sensor		2016-02-09 04:30 PM
	Access Control Policy: File Download Detection - DLP		
	Intrusion Policy: Balanced Security and Connectivity		
	ONS Policy: Default DNS Policy		
	S - File Policy: File-inspection		
	Platform Settings: Default		
	Network Discovery		
	Device Configuration		
V ±	IPS_Sensor		2016-02-09 04:30 PM
V 🗉	MalwareDetection1_Sensor		2016-02-09 04:30 PM
s	elected devices: 4		Deploy Cancel

GigaVUE-HC2 Configuration

This section explains the steps to configure the GigaVUE-HC2 for all inline network and inline tool elements that you will use to create traffic flow maps. This configuration consists of the following procedures:

- · Configuring the GigaVUE-HC2 Inline Network and Inline Tools
- Configuring the Inline Traffic Flow Maps
- Testing the Functionality of Cisco FirePOWER Inline Tool

Configuring the GigaVUE-HC2 Inline Network and Inline Tools

This section walks you through the steps needed to configure inline network bypass pairs and an inline network group for those pairs. As the infrastructure grows, additional inline network pairs can be added to the inline network group. The basic steps are as follows:

- Step 1: Configure Network and Tool Ports
- Step 2: Configure the Inline Networks
- Step 3: Configure the Inline Tools
- Step 4: Configure the Inline Tool Group
- Step 5: Configure the Inline Serial Tool

The steps described in this section assume that you are logged in to GigaVUE-FM. To configure the GigaVUE-HC2 of interest, select **Physical Nodes** in the left pane and then select GigaVUE-HC2 on the Physical Nodes page.

NOTE: This section assumes all GigaVUE-HC2 ports connected to network devices are set as Inline Network port type. For specific instructions on completing these tasks, refer to Help Topics links in the GigaVUE-FM or the *Gigamon-FM/VM User's Guide*.

Step 1: Configure Network and Tool Ports

To configure the Network and Tool Ports, do the following:

- 1. Log into GigaVUE-FM, select Physical Nodes.
- 2. Select the GigaVUE-HC2 from the list of physical nodes managed by GigaVUE-FM.
- 3. Select Ports.
- 4. Edit the ports of interest. Enable the port and select port type as "inline Tool" or "inline Network".

- C 2 2 2 2	10.115.152.58 - H	Series			This	Node:			c		admin •
	Ports P	urt Groups Turtvel Ports P	ort Pairs	. Tani	Mirrura Sac	k Linka					
	All Ports	Pure Discours									
Cherview		- Concentration of the concent						-	and the stars		-
	Ports							ton P	Ref Quick	PortEditor	Export
His .											
Ports	Fitered By : No	14									
E Mayo	Port Id	Alas	Type	Speed	Acmin Enabled	Link Status	Transceiver Type	Utilization (TeRs)	Port Filter	Discovery	Protocol
S Infine Burner	2 3/1/x1	ESX9-vmmic2	m	10G	4	ίφ	s'p+sr	0/0	074	017	
SWIEWS GREAT	3/1/12	ESX9-vmmic3	8	196	1	site.	sip+ sr	070		07	
	O 3/1//3	RE-5_Port-1	8	10G	-	dawn		0/0	$(-\pi)^{-1}$	011	
Charcelle	3/1/94	FE-1_port-2	8	106	4	diser.		0/0	17.1	011	
Roles and Livers	3/165	FE 2_port.1	8	105	*	disen		0/0	070	011	
	0 3/106	182.port2		136	*	down		0/0	171	07	
	S \$107		8	126	×	dawn		0/0	17.1	orr	
	3 0 10			194	20.	cown.		470	170	61	
	0 3169	ESX10_VNIC2_FirePower1_Inside	8	15	4	10	staci	0/0		0ff	
	3/t/x10	ESX10_VNIC3_FirePower2_Outside		15	1	10	speci	0/0		or	
	2/10/11	ESX14_VNC2_FirePower2_Inside	8	16	*	100	sip cu	010		017	
	0 3/1/x12	ESK14_VNIC2_FirePower2_Outside		10	1	10	elp cu	0/0	100	011	
	D 3/1/x13	ESX16_VNIC4_FirePower3_Inside		16	*	10	sip cu	010		01	
	3/1/x14	ESX16_VNC5_FirePower3_Outside		15	8	10	ຮ່ອເບ	010		or	
	0 3/1/x15	ESX15_VNC4_FireFower4_inside		15	×	10	sib ci	0/0	-	Off	
	3/1/x15	ESX15.VVIC5.FirePower4.Outside		1G	×	10	ร่อณ	0/0	-	01	
	3/1//17			105	1	down	bps sols?	010	1.7.1	on	
Gigavoc-rivi	10.113.132.30				78.0	Aladar			0.0	. 👥	admin
	Sec. 1				The	i Node	_	_	<u>ه</u> و	· /	admin
w:	Ports	Port Groups - Tunnel Ports	Port Pairs	15	of Mirrora Sta	i Nođe ick Links			a) c	*	admin
us A Overview	Ports Al Ports	Port Groups Tunivel Ports	Port Pains	10	al Mimora Sta	i Node: Ick Links			 c 	*	admin
tiş ♠ Oservinu 7: Werkfons	Ports Al Ports Ports	Port Groups Tunnel Ports Port Discovery	Port Pains	15	al Mimora — Sta	i Node: ick Links		idi	Q C	k Port Editor	admin
tus A Overview 7: Wortflows stife:	Ports Al Ports Ports	Port Groups Tunnel Ports :	Port Pairs	. 15	al Mimora Sta	i Node		(d)	Q C	k Port Editor	admin
tus A Overview T: Workflows Milite: A Ports	Ports Al Ports Ports	Port Groups Turnet Ports Port Discovery	Port Pairs	3 796	al Mirrons - Sta	(Node IckLinks		idt	Q C	k Port Editor	admin Export
tos A Overview Tr Workflows NTR Ports W Mago	Poits Al Ports Ports Filtered By 1 No	Port Groups Turnet Ports Ports Olicowey	Port Pairs	10	Thy al Mirron Sta	i Node ick Linis		(dr	Q C	k Port Editor	admin Export
tij ∰ Overview T: Wortfows stre: ➡ Ports ¥: Maps \$ orgaSMAITTB	Ports Al Ports Ports Filtered By 1N	Port Groups Junnel Ports Ports Olicowey	Port Pars Type	loi Speed	Admin Enabled	Link Status	Transceiver Type	Edit	Q C	k PortEditor	admin Export
NIC A Controllow To Workflows NIC Ports Y Mages GragadMAITTE S Index Synders	Ports Al Peres Ports Filtered By : No Dent Id Dot 2266	Port Groups Junnel Ports Ports Discovery	Port Pairs Type	Speed 10G	Admin Enabled	Link Status down	Transceiver Type	Edit Utilization (TwThd) 6/0	a) C Fiter Quid PortFiter -	k Port Editor Discover Off	admin Export
NI A Construint T Workflows NITC Ports GagaSMAITTR GagaSMAITTR (Intel Sypans 1131	Ports Al Pers Ports Filtered By IN Per Id 3/2x6 3/2/x7	Port Groups Juniel Ports Ports Discovery Ports Alles Team6-BC-A	Port Pains	Speed 10G	Admin Enabled	Link Serius down	Transceiver Type sTp+sr	Edit Lockastion (Twitig 0/0 0/0	a) C Fiter Quid PortFiter -	k Port Editor Discover Off	admin Export
LUE A Controllous T Workflows Affre: Ports CogesMAITE Coges CogesMAITE Coges C	Parts Al Ports Ports Filtered By 1 No Port d 302x6 302x7 202x8	Port Groups Junnel Forts Ports Discovery	Port Pairs Type C	100 Speed 10G 10G	Admin Enabled	Link Status doan up	Transceiver Type sfp+ sr sfp+ sr	Edit Utilization (TwThd 0/0 0/0 0/0	a) C Fiter Quid Post Fiter - -	k Port Editor Discover Off Off	admin Expon
	Parts Al Ports Ports Filtered By IN Port II 302x6 302x7 322x8 322x8	Port Groups Junnel Forts Ports Discovery Ports Discovery Alias Team6-8C-A Team6-8C-B Tea	Port Pars	Speed 10G 10G 10G 10G	Admin Enabled	Link Statuy Goven up up	Transceiver Type sfp+ sr sfp+ sr sfp : sr	Edit Utilization (TwThd 6/0 0/0 0/0 0/0	a) C Fiter Quid Port Fiter - -	Discover Off Off Off Off	admin Deport
	Parts Al Ports Ports Filtered By 1N Port Id 302x6 302x6 302x6 302x6 302x6	Port Groups Junnel Forts Ports Diversively Ports Diversively Alias Alias Team6-8C-0 Team6-8C-0 Team6-FE1-0 Team6-FE1-0	Port Pairs	100 Speed 10G 10G 10G 10G 10G 10G	Admin Enabled	Link Satur Govn up up up	Transceiver Type sTp+ sr sTp- sr sTp cu stp cu	Edit Utilization (TwThd C/O C/O C/O C/O C/O C/O C/O C/O	 Quict Fitter Quict Fort Fitter - 	Discover Off Off Off Off Off Off	admin Export
	Parts Al Pers Ports Filtered By IN Port Id D 3/2Ad	Port Groups Junnel Forts Port Olicowey Alas Team6-8C-A Team6-8C-B Iteam6-8C-B Iteam6-FE1-B Team6-FE1-B	Fort Pairs	100 Speed 10G 10G 10G 10G 10G 10G 10G	Admin Enabled	Link Statur Gorn up up up up	Transceiver Type sTp+ sr sTp- sr sTp cu sTp cu efp cu efp cu	Edit Utilization (huffid) 0/0 0/0 0/0 0/0 0/0 0/0 0/0	 Quict Fitter Quict Port Fitter - -	Discover Off Off Off Off Off Off Off Off Off	admin Export
 A Overview A Overview A Vertrilows A Ports A Ports A Ports G GassMAITTR A Intere Bypacs Holles Bypacs Holes And Listers Chesisis Roles and Listers Settings 	Parts Al Pers Ports Filtered By IN Port M D 3/2/49 D 3/2/49 D 3/2/49 D 3/2/41 D 3/2/	Port Groups Junnel Forts Port Discovery Ports Discovery Alas Team6-8C-A Team6-8C-A Team6-8C-B Team6-8C-B Team6-8C-B Team6-8C-B Team6-8C-B Team6-8C-B Team6-8C-B Team6-8C-B Team6-8C-B Team6-8C-B	Post Pairs Type C C C C C C C C C C C C C C C C C C C	100 Speed 10G 10G 10G 10G 10G 10G 10G 10G 10G	Admin Enabled	Link Setur Link Setur doen up up up	Transaceiver Type afp+ar afp-ar afp cu afp cu afp cu afp cu afp cu	Con. Contraction (Purified C/O C/O C/O C/O C/O C/O C/O C/O C/O C/O	Q) C	Discover Off Off Off Off Off Off Off Off	Suport
45 A Overview T Workflows ITC. Ports G GyssMAITTR G GysSMAITTR Million Bypacs Ital Chesols Chesols Chesols Settings	Parts Al Perts Ports Ports Ports Port Id Document Al 2006 Port Id Document Al 2006 Document D	Port Groups Juniel Forts Port Groups Juniel Forts Ports Discovery Alses Team6-8C-A Te	Port Pain Type C C C C C C C C C C C C C C C C C C C	100 Speed 10G 10G 10G 10G 10G 10G	Admin Enabled	Link Server Geen up up up up up up	Transceiver Type efp+sr sfp+sr sfp cu sfp cu sfp cu sfp cu sfp cu sfp cu sfp cu	Edit Utilization ("utility) 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/	a) C	Discover Off Off Off Off Off Off Off Off Off Of	admin Diport
 A Overview Workflows Workflows Ports Ports G OgasMAITTE Alline Bypass Holley Bypass CharsSis CharsSis B CharsSis B CharsSis Settings 	Parts Al Perts Ports Filtered By 1No Port S	Port Groups Juniel Ports Port Discovery Port Discovery Ales Ales Facri6-8C-A Facri6-8C-A Facri6-8C-A Facri6-8C-B Tarti6-8C-A Facri6-8C-B Tarti6-8C-A Facri6-8C-B Facri6-8C-B Facri6-8C-B Facri6-8C-Care Facri6-8C-Care Facri6-8C-Care Facri6-8C-Care	Port Pain Type C C C C C C C C C C C C C C C C C C C	599990 1005 1005 106 106 106 106 1006	Admin Enabled	Link Seruar den up up up up up up up up up up up up up	Transaceher Type eTp+sr sfp+sr sfp cu sfp cu sfp cu sfp cu sfp cu sfp cu sfp cu sfp cu sfp cu	Edit Utilization (TwThid C/O C/O C/O C/O C/O C/O C/O C/O C/O C/O	Quict Fitter Quict Fitter -	Discover Off Off Off Off Off Off Off Off Off Of	admin
45 A Overview T Workflows TC Ports C Overview Ports C Overview C Overv	Parts Al Perts Ports Filtered By 1 No Port d 202x8 302x9 302x9 302x9 302x9 302x9 302x1 302	Port Groups Junnel Ports Port Discovery Port Discov	Port Pain Type C C C C C C C C C C C C C C C C C C C	599990 100 100 100 100 100 100 100 100 10	Admin Enabled	k Link Setur duk Setur duk Setur du du du du du du du du du du du du du	Transceiver Type efb+ sr sfb+ sr sfb tu sfb tu sfb tu sfb tu sfb tu sfb tu sfb tu sfb tu sfb tu sfb tu	Edit Utilization (PurRed C/O C/O C/O C/O C/O C/O C/O C/O C/O C/O	 q) C Fiter Quict Port Fiter - -<	Discover Off Off Off Off Off Off Off Off Off Of	admin
4 Overview 7 Workflows 10 10 10 10 10 10 10 10 10 10	Parts Al Ports Ports Ports Filtered By 1 N Port Id Por	Port Groups Junnel Forts Port Groups Junnel Forts Port Discovery P	Port Pains	599990 509990 100 100 100 100 100 100 100 100 10	Admin Enabled	K Linis K Linis Unk Statup Statu 19 19 19 19 10 10 10 10 10 10 10 10 10 10 10 10 10	Transceiver Type efp+sr sfp-sr sfp cu sfp cu sfp cu sfp cu sfp cu sfp cu sfp cu	Edit Utilization ("witho) 6/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0	a) C	Discover Off Off Off Off Off Off Off Off Off Of	admin
 Derrivies Pors Pors GagaSMATTE GagaSMATTE Inline Bypass Tell ChansS Arbes and Users Settings 	Parts Al Ports Ports Filtered By IN Port II 302x6 302x7 302x6 302x7 302x6 302x	Port Groups Junnel Forts Port Groups Junnel Forts Ports Discovery Alas Team6-8C-A Team6-8C-B Team6-8C-B Team6-8C-B Team6-8C-B Team6-FE2-B	Port Pains	5000 5000 500 500 500 500 500 500 500 5	Admin Enabled	Node Christer Christer Storn Stor	Transceiver Type sflp+ sr sflp- sr sflp cu sflp cu sflp cu sflp cu sflp cu sflp cu sflp sr sflp sr	Corr UKRisetion (%/%) C/O C/O C/O C/O C/O C/O C/O C/O C/O C/O		Discovery Off Off Off Off Off Off Off Off Off Of	admon
LU A Overview Werkfore F Workfore Ports G GgaSMATTB G GgaSMATTB I Inles Spass Tabl Chens5 A Roles and Users Settings	Parts Al Ports Ports Filtered By 1N Port Id Al 2006 Port Id Po	Port Groups Junnel Forts Port Groups Junnel Forts Port Discovery Alas Team6-8C-A Team6-8C-A Team6-8C-B Team6-8C-B Team6-8C-B Team6-8C-B Team6-8C-B Team6-8C-B Team6-8C-Cere T	Part Pains Type C C C C C C C C C C C C C C C C C C C	59444 59444 10G 10G 10G 10G 10G 10G 10G 10G 10G	Admin Enabled	Node ick Linis Linis Satur dom ig ig ig ig ig ig ig ig ig ig	Transceiver Type sfp+ sr sfp+ sr sfp cu sfp cu sfp cu sfp cu sfp cu sfp cu sfp sr sfp+ sr	Edit Utilization (huffie) 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/		Discover Off Off Off Off Off Off Off Off Off Of	admin Export y Pretacal
uti A Crenview T Workfore T Workfore A Ports Y Mage G GgaSMART® ↓ Intere System Creases L Roles and Users ◆ Sectorys	Parts Al Ports Filtered By 1 N Filtered By 1 N Filtered J 2006 J 2006 J 200	Port Groups Junnel Forts Port Groups Junnel Forts Port Groups Junnel Forts Port Groups Junnel Forts Akies Akies Fearr6-8C-A Fearr6-8C-A Fearr6-8C-B Fearr6-8C-B Fearr6-8C-B Fearr6-8C-B Fearr6-8C-B Fearr6-8C-Cere Fearr	Type C C C C C C C C C C C C C	104 5peed 105 105 105 105 105 105 105 105 105 105	Admin Enabled V V V V V V V V V V V V V	Node ick Linis Link Satur down ig ig ig ig ig ig ig ig ig ig	Танжениет Туре 15р+17 15р си 15р си 15р си 15р си 15р си 15р си 15р си	Edit Utilization (%/%) 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/		Discover Off Off Off Off Off Off Off Off Off Of	admin Export
uli A Overview T Workfores IT:: Ports G GyaSMAITE G GyaSMAITE G Intele System Total Cheese A Roles and Users G Settings	Parts Al Perts Ports Filtered By IN Port Id 3/2/46 3/2/47 3/2/4 3/2/47 3/2/4 3/2/47 3/	Port Groups Junnel Forts Port Groups Junnel Forts Port Diveowry Alas Alas Team6-8C-A Team6-8C-0 Team6-10 T	Port Pain Type C C C C C C C C C C C C C C C C C C C	599990 599990 100 100 100 100 100 100 100 100 10	Admin Enabled	Node ick Linis ick Statuy doen ig ig ig ig ig ig ig ig ig ig	Transaceiver Type aflp+ ar aflp- yr aflp cu aflp cu aflp cu aflp cu aflp cu aflp a u aflp a r	Contraction (%x%) C/C C/C C/C C/C C/C C/C C/C C/C C/C C/		e Port Editor Off Off Off Off Off Off Off Off Off Of	admin Deport

Note: The ports referred to as "intermediate1" and "intermediate2" are connected back-toback. This is needed to support serial and parallel mode setting of tool in the same configuration. The goal is to have traffic from server side first sent to serial sensors (IPS and DLP) and then sent to the port "intermediate1". From "intermediate1", traffic would be looped back to port "intermediate2", where it is sent to the parallel malware sensors and then to the client connected on the tool side. Refer Figure 1-1 and Figure 1-3. To configure the inline networks, do the following:

1. In GigaVUE-FM, select Inline Bypass > Inline Networks.

NOTE: If there is a bypass combo module in the GigaVUE-HC2, there will be four preconfigured Inline Network port pairs as shown below. If you are using the physical bypass interfaces, the step will be similar to those covered but limited. Notably you will not be able to change the alias and port A and B are preselected. If your network is 1G or 10G fiber, use one of these preconfigured inline bypass pairs. In this deployment guide, NGIPSv is used with 1 Gb Copper interfaces hence we would be using 1Gb Copper bypass modules for inline bypass testing.

A Overview	1	Inline M	aturirk T	Inline Ner	work Genunk	Infine Tools	Inine Tool Genun	Infine Serial Tools	Heartheam	Redundations
rissing	l	Inline	Netw	orks	rees to sope	THE LOUI	some nur comp		New Cone	Edit Delete
¥ Maps S GigaSMART		•	Allas		Comment	Туре	Forwarding State	Link Propagation	Physical Bypass	Traffic Path
Therefore a	Ŀ	dei dei	fault_inline, fault_inline_	net_3_1_1 not_3_1_2		protected protected	physicalBypass physicalBypass	crue crue	enabled enabled	Bypass Bypass
Roles and Users	L		fault_inline_	net 3,1,3		protected	physicalBypass	chue .	enabled	Bypass
C Settings	P.	L. UE	autorine.	INCC. 1.4		produce	Total Items : 4	u ve	ermoleu	oypess

- 2. Click New. The Inline Network configuration page is displayed.
- 3. On the Inline Network page, do the following, and then click **Save** when you are done:
 - In the Alias field, enter an alias for the network link this Inline Network bypass pair represents. For example, FirePower_Server_inlineNetwork and FirePower_Client_inlineNetwork
 - b. Select the port for **Port A** by using the drop-down list or by typing the port label. The value in the **Port B** field is automatically populated once you select **Port A**.
 - c. Retain default values for Traffic Path and Link Failure Propagation.
 - d. Select Physical Bypass. This minimizes packet loss during traffic map changes.

The configuration page should look similar to the example shown in the figure below.

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

🕘 GigaVUE-FM	10.115.152.58 - In Series			This Node:	٩	c		admin.+
	Inline Network Fire	Power_Server_inline*	Network				Save	Cancel
 Derivise Workfines 	Inline Network Info							
A fam	Alian Communit	Feature Sever Heatlebook						
S Cysteratu In Infee System	Ports							
 A traine Appension A trained and Unions 	Port A	Part Editor						
O Settings	Configuration							
	Traffic Path	Dypess	•					
	Link Fallure Propagation	8						
	Physical Bypans	0						
	Redundancy Profile		•)					

📀 GigaVUE-FM	10.115.152.58 -H Serve			This Nuclei	a) C 📌 atrice
	Inline Network Fire	Power_Client_Inline	Network		Sive Cancel
A Greensteen N with allows	inline Network info				
Same -	Alles	frePosel,ChenQitine/tebook			
W Maps	Comment	Convert			
G Cassimation	Ports				
C DITTEM		Port Editor			
II Crim	Part A	araigs (contermediated)	•		
A Rear and Users	Pert B	(cofas) hg/k 🛅			
	Configuration				
	Traffic Path	Novi	*		
de la	Link Failure Propagation				
	Physical Bypass				
	Redundancy Profile	The second secon	-		

The completed Inline Networks page should look similar to what is shown in the following figure.

🙆 GigaVUE-FM	10.115.152.58 - H Serves			This Not	ŧ	٩	c 🤰	admin •
-club A Destroise N Workflowe	Infine Networks	Hidne Tools Infe	e Tud Griups	Volue Serial Tools He	rtbeats Redunsiansies	New	Cane 18	I Delete
Franke A Ports V Maps S GastMATH Printe Opposi Disting Disting S International Distings	Alas Profileer, client, clienterweck Profileer, sterer, interfetierweck default, mine, ant (, 1, 1, 2) default, joine, ant (, 1, 1, 2) default, joine, ant (, 1, 1, 2) default, joine, ant (, 1, 1, 4)	Comment	Type protected protected protected protected protected protected	Forwarding State physicalByparts physicalByparts physicalByparts physicalByparts physicalByparts physicalByparts physicalByparts physicalByparts	Link Proagetien Stee Stee Stee Stee Stee Stee	Physical Bypers matched enabled enabled enabled enabled	Traffic I Bygans Bygans Bygans Dygans Oygans	reth

Step 3: Configure the Inline Tools

Steps 3 through 5 walk you through the configuration necessary to define the inline tools, inline tool groups and serial tools that will be used in the traffic flow map defined in subsequent steps.

1. In GigaVUE-FM, select Inline Bypass > Inline Tools.

	^	Ports	Port Groups	Tunnel Ports	Port Parts	Tool Mirrors	inline Bypass	Stack L	nks				~
A Overview		Initive Netwo	orks Inline	Network Groups	inline Tools	Inline Topi Gro	sups Intin	e Serial Tools	Heit	rtbeats	Redund	ancies	
TRAFFIC	-1	Inline T	ools					New	Cone	Recover	Edit	Detete	ŀ
W Maps GigaSMABT		A5a	5	Comment (Operational State	Inline Too	vi Status	FattoverAct	son	Heartbea	at Profile		-

- 2. Click New to open the configuration page for inline tools.
- 3. In the **Alias** field, enter an alias for the inline tool this inline tool pair represents. For example, FP_DLP_InlineTool.
- 4. In the Ports section, specify the ports as follows:
 - For **Port A**, specify the port that corresponds to the inside network of the sensors.
 - For **Port B**, specify the port that corresponds to the outside network of the sensors.
- 5. Leave the default setting for the remaining configuration options.

Your configuration should be similar to the example shown below.

😳 GigaVUE-FM	10.115.152.58 - H Series			Tims Node:	9	C		adeta •
adda (Inline Tool FP_DLP.	iniineTool					See	Cancel
Coursian To monthous	Inline Tool Info							
Parts	Alles	PF_DUF_inite/bel						
W Maps	Commant	-isomerand						
p- mine System	Ports							
Tractal Theorem	1	Port Editor						
1 Roles and Users	PartA	SHUNT (\$5014, VIEC2, Re)	•					
	Part 8	MUV12(EST14,VMC3,FP)	+1					
	Configuration							
100	Enabled	•						
l and	Failower action	ToolbyRass	•					
	Becavery Mode	automatic	•					
	Enabled Peartheat							
	Profile	delaut.	•					

- 6. Click Save.
- 7. Repeat steps 2 through 6 for all additional inline tools.

NOTE: The failure action for this inline tool is **ToolBypass**. This means that the GigaVUE-HC2 will not send traffic to this inline tool if it is considered to be in a failure mode. There are other options for inline tool failure that are fully described in the online help and GigaVUE-OS Configuration Guide. The other options have very different effects on the overall traffic flow. Because the heartbeat feature is not enabled, the failover action will only take place if one of the tool port interfaces fails.

The completed Inline Tools page should look similar to what is shown below.

🞯 GigaVUE-FM	10.115.152.58 H Series			This Node:		a) C 🌹 admin-
weeks	Infra Networks Infra Network Groups	Inline Spok	Inline Tool Groups	Inive Setal Tools Heartbeats	Redundancies	
 Oversides Workflowd 	Inline Tools				New	Date Tarmer 192 Dette
THE .	· Alm	Comment	Operational State	Inline Tool Status	FalloverAction	Heartbest Profile
A Perty	 IP_DUP_InterVal 		up	enabled	Tool Bypans	orfault
W Masi	(D PP_PS_strikeTool		up	enabled	Toti Bypass	stela-It
S Infin Brown	Interfactor		sep.	enabled	Soci-Bypates	Rules
	7P,Maware2,minefool		vp	enabled	Tool Bypass	aviaus
Dienn Chenn Anies and there G Serbigs				Total Items : 4		

Step 4: Configure the Inline Tool Group

To configure the inline tool group, do the following:

- 1. In GigaVUE-FM, select Inline Bypass > Inline Tool Groups.
- 2. Click **New** to open the Inline Tool Groups configuration page.
- 3. In the **Alias** field, type an alias that describes the inline tool groups. For example, FP_Malware1_2_InlineToolGroup.
- 4. In the Ports section, click the **Inline tools** field and select all the inline tools for this group from the I
- 5. ist of available inline tools.
- 6. In the Configuration section, do the following, and then click **Save** when you are done:
 - · Select Enable.
 - Select Release Spare If Possible if applicable.
 - Keep the defaults for Failover action, Failover Mode, and Minimum Healthy Group Size.
 - Select a-srcip-b-dstip for **Hash**.

The configuration should look similar to the example shown below:

🞯 GigaVUE-FM	10.115.152.58 - H Series			This Node:	Q)	c		atrin •
- Alar	Inline Tool Group F	P_Malware1_2_Inlin	neToolGroup				Save	Cancel
* Oversien * worklows	Inline Tool Group Info							
THEFT.	Alles	FF_Malware1_1_initia/Too/Group	÷.					
W Maple	Comment	Garonere						
S GystMartin In Infine Sypani	Ports							
TATAM ED Chieses	Inline Tools	Honory, Honor -						
A Roles and Users	Inline Spare Youl							
O Settings	Configuration							
	Frabled Release Spare if Possible	•						
	Fallover Action	TooleyPass	•					
	Failover Mode	Spreet						
	Minimum Healthy Group Size	1	•					
	Hash	a wdp-b-dstp						

Step 5: Configure the Inline Serial Tools

To configure the inline serial tool group, do the following:

- 1. In GigaVUE-FM, select Inline Bypass > Inline Serial Tools.
- 2. Click **New** to open the Inline Serial Tool Groups configuration page.
- 3. In the Alias field, type an alias that describes the inline tool groups. For example:

FP_IPS_DLP_InlineSerialToolGroup.

- 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 serial tools.
- 5. In the Configuration section, do the following, and then click **Save** when you are done:
 - · Select Enable.
 - · Select Failover action as Per Tool

The configuration should look similar to the example shown below:

💿 GigaVUE-FM	10.115.152.58 (Hilerin:		This Node	a) C 📌 admi	n+
	Inline Serial Tool G	roup FP_IPS_DLP_InlineSerialTor	alGroup	Save Cance	8
To workflows	Inline Serial Tool Group Info				
TARING A Funts W Maps	Allas	PP_IPS_DLP_INVederIa/ToolGroup			
S GigaDWATTE	Inline Port				
	Inline Tools	(Construction) - (Const			
 Roles and Usery G. Sentrugs 	Configuration				
	Enabled. Failover action:	Der Tosi +			



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 FirePOWER tool group allowing you to test the deployment functionality of the FirePOWER virtual sensors within the group. This will be done in three steps as follows:

- Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule
- Step 2: Configure the Inline Traffic Collector Map
- Step 3: Change Inline Network Traffic Path to Inline Tool

After completing these steps, you will be ready to test the deployment of the FirePOWER sensors. The test procedure is described in *Testing the Functionality of the FirePOWER Inline Tool*.

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

This section walks through the configuration of traffic flow map between the Inline Network Group and the Inline Tool Group.

- 1. In GigaVUE-FM, go to the **Maps** page.
- 2. Click New. The New Map page displays.
- 3. In the Map Info section, do the following:
 - In the **Alias** field, enter a map alias that represents the network source and tool destination.
 - Set **Type** to Inline.
 - Set **Sub Type** to By Rule.
 - Set Traffic Path to Normal.
- 4. In Map Source and Destination, set the **Source** and **Destination** as follows:
 - Set Source to the inline network group that you created in Step 2: Configure the Inline Network Group of the previous section.
 - Set Destination to the inline tool group and inline serial groups that you created in Step 4: Configure the Inline Tool Group and Step 5: Configure the Inline Serial Tools Group, respectively, in the previous section.
- 5. In Map Rules, click Add a Rule.
- 6. Specify the following for the rule:
 - Click in the Condition search field for the Rule and select IP Version v4 from the drop-down list.
 - Select **Pass**. (This is the default.)
 - · Select **Bi Directional**.

• Add a rule to pass all IPv4 traffic.

The map rule should look like the rule shown in the following figures:

Inline flow map for Server to IPS_DLP inline tool group:

GigaVUE-FM	10.115.152.58 - H Sarles		This Node:	۵)	c	2	admin •
	Edit Map: FP_IPS_D	LP_MapRule				Seve	Cancel
A Overview Nº Westellows	Map Alles Commenta	(P_PS_SLP_WaphJe					
Taline Parts Y Maps	Type Sub Type Trutte Parts	intre d					
A come phirms	✓ Map Source and Destination	a 					
 Denni ▲ Roles and thers ♦ Sensign 	Source Destinution	Part Editor					
	v Map Rules	800F					
	K Role 1 Rule Comment	Could Sollier Import Add a finite Execution reserve. OPA Construent IP Version Version 14 1	es Drog 🖬 B Decclouel				

Inline flow map for Malware inline tool group to Client:

🙆 GigaVUE-FM	10.115.152.58 -H Series				This Node:	Q	c		admin.+
	Edit Map: FP_Maiwa	are1_2_MapRul						Save	Carcel
A Deresee Tr Workflam	Map Alias	IP, Malwaret, X, Mapliple							
Aurec Pons 'g: Noos	Type Sub Type	Intere By Rule	-						
G. Gigissukens 20 Soline Report	Traffic Path	Normal	1						
Clickens 21 chesses 2 chesses totare	✓ Map Source and Destination	n Part lidher							
O (Horizon)	Source	Failwer Det Finder	insk 1						
	6509	Nore	Э						
11. K.	✓ Map Rules								
r Ş	n Rule 1 Rule Converse	Querk faltur Import As Constituer poerts Economics IP Version Wenter va	C Parts O D	top 🚦 III Directional					

Note: Additional traffic can be bypassed by adding rules to the map.

7. Click Save.

Step 2: Configure the Inline Traffic Collector Map

This section walks you through the steps to create another traffic map, which is a collector. This map sends all the traffic not matched in the first traffic flow map to the inline tool group. This Collector pass rule must be created because there is no implicit pass for traffic, meaning all inline traffic from any given inline network not matched by a pass rule is discarded.

To configure the collector map, do the following:

- 1. In GigaVUE-FM, navigate to **Maps** page, and then click **New.** The New Map page displays.
- 2. In the Map Info section, do the following:
 - In the Alias field, type a map alias that identifies that this collector map is for the same inline network as the traffic map you created in Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule.
 - · Set Type to Inline.
 - Set **Sub Type** to Collector.
 - Set **Traffic Path** to ByPass.
- 3. In Map Source and Destination, set the **Source** to the same source as the first rule map configured in *Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule*.

🞯 GigaVUE-FM	10.115.152.58 - H Series		This Node:	a) c	admin +
HOME	Edit Map: FP_IPS	_DLP_Collector		Sa	ve Cancel
A Description	✓ Map Info				
TEATRIC Ports W Maps GigaSMART® () Inline Bypass	Map Alias Comments Type Sub Type Traffic Path	PP_IPS_DLP_Collector Intine Collector ByPass			
Changes	✓ Map Source and Destin	nation			
 Holes and Users Settings 	Source Destination GSOP	Port Editor PrePower, Server, InterNetwork Select Lents	ork. *		
	✓ Map Rules				
LL A.		Quick Eistor Import Add a	(Refer		

🙆 GigaVUE-FM	10 1 15 152 58 - H Serves		This Node:	a)	c		admin •
LOVE	New Map					Szee	Cancel
Overview Workflows	✓ Map Info						
TRAFFIC A Ports W Maps GigastMARTIN P Intere Typpage	Map Allas Comments Type Sub Type Traffic Pach	FP_Mabaare1_2_Collector Indine • Collector • ByPass •					
Cheese	✓ Map Source and Destin	ation					
 Ansatz and lotters Settings 	Source Destination GSOP	Port Editor Fertiver, Direct, Hitrefectorick + Select ports None					
	🛩 Map Rules						
		Quick Editor Import Athl a Bule					

The finished screen for maps should look as shown in the following figure.

🞯 GigaVUE-FM	10,115	152.58 - H Series			This	Node:					Q	c	. 🧖	admin +
HOME	м	aps Map Templat	asi .											
n Overslew	M	laps				New	Clone	Eğt	Delete	4	G		4	÷
Thaine A Ports	6	♠ Alias	Comments	Туре	Sub Type	Soun		No of Rules	GSOP	Priority	Access L	evel	Destination	
W Maps	.0	FP_JPS_DLP_Collect	ctor	inine	collector(ByPass)	0. FireF	lower_Serve Network	4 <u>0</u>			admin			
 Grand Dypana 	9	FP_IPS_DLP_MapR	lule	inline	byRule	Firef	ower_Serve	r. 1		1	admin		FP_IPS_DLP erialToolGro	_Inline5 rup
	.0	FP_Malware1_2_C	ollector	inine	collector(ByPass) Firef nline	Power_Clien Network	ti o			admin			
El Chassis	0	FP_Malware1_2_N	lapRule	inine	byRule	firef	ower_Clien Network	0.10		10	admin		FP_Malwa	re1,2,jni ip
O Settings					Total	Items : 4								

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 Ports > Inline Bypass > Inline Networks.
- 2. Select one of the inline networks that you defined previously (refer to *Step 2: Configure the Inline Network Group*), and then click **Edit**.
- 3. In the Configuration section, make the following changes:
 - Set **Traffic Path** to Inline Tool.
 - Uncheck Physical Bypass.

🞯 GigaVUE-FM	10.115.152.58 - H Series			This Node	q	c		admin •
HOHI	Inline Network Fire	Power_Server_InlineN	(etwork			1	Save	Carcel
 Decision Transferme 	Inline Network Info							
TRAFIC	Alles	FireProver_Server_Intinetverwork						
W Mage	Comment	Continent						
💋 Digutawarter 🌫 Indre Bypass	Ports							
sister.		Pert Editor						
E Owin	Port A	3/3/g1 (taServer)	•					
A failes and Dears	Fort B	3/3/g2 (tointerredute1)	•					
1000000000	Configuration							
	Traffic Path	To mine Tool	-					
	Link Failure Propagation	0						
10.00	Phylical Bypass	a.						
	Redundancy Profile		•					

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

Testing the Functionality of the FirePOWER Inline Tool

The configuration procedure described in the previous section configures the GigaVUE-HC2 to send live traffic to all FirePOWER NGIPSv sensors. While testing the functionality of the sensors, it may be helpful to monitor the port statistics on the GigaVUE-HC2. To access the port statistics for the inline network and inline tool ports, do the following:

- 1. Get the statistics for the inline network and the inline tool ports from the GigaVUE-HC2.
- 2. Launch a serial console or SSH session to the GigaVUE-HC2.
- 3. Log in as admin and enter the following commands at the command prompt (HC2>), where the port lists in the command are the inline network and inline tool ports:

```
HC2 > en
HC2 # config t
HC2 (config) # clear port stats port-list 3/1/x9..x16,3/3/g1..g4
HC2 (config) # show port stats port-list 3/1/x9..x16,3/3/g1..g4
```

After entering the show port command, you should see the port statistics for the specified port list.

Inline Network and Inline Tool Port Statistics:

Counter Name	Port: 3/1/x9	Port: 3/1/x10	Port: 3/1/x11	Port: 3/1/x12
IfIn0ctets:	38370	446877	38370	443841
IfInicastPkts:	216	365	216	364
TfTnNIIcastPkts:	46	370	46	378
IfInPktDrons:	40	5/5		5/6
IfInDiscards:	a	ă	å	ě
IfInErrors	0	â	ő	6
TfTnOctetsPerSec:	83	472	83	472
If InDecketsPerSec:	1	4/2	1	4/2
If InfacketsFeldet.	446041	20270	446912	29626
TfOutlleastPkts:	365	216	365	30020
TfoutNilcastPkts:	303	210	303	220
IfOutDiscords:	300	40	3/0	40
IfoutEcores	0		0	0
IfoutOctote PerSect	473	02	472	83
TfoutBacketsBerSec:	4/2	0.5	*/2	63
ITOULPACKELSPEISEC:	,	1	,	1
Counter Name	Port: 3/1/x13	Port: 3/1/x14	Port: 3/3/g1	Port: 3/3/g2
IfInOctets:	13362	416360	445575	38056
IfInUcastPkts:	140	291	363	218
IfInNUcastPkts:	1	238	367	45
IfInPktDrops:	9	0	0	0
IfInDiscards:	9	0	0	0
IfInErrors:	9	0	Ø	0
IfInOctetsPerSec:	9	229	472	83
IfInPacketsPerSec:	9	4	7	1
IfOutOctets:	416360	13362	37800	442539
IfOutUcastPkts:	291	140	214	362
IfOutNUcastPkts:	238	1	45	366
IfOutDiscards:	9	0	0	0
IfOutErrors:	9	0	0	0
IfOutOctetsPerSec:	229	0	83	472
IfOutPacketsPerSec:	4	0	1	7
Counter Name	Port: 3/3/q3	Port: 3/3/q4		
IfInOctets:	442539	38056		
IfInUcastPkts:	362	218		
IfInNUcastPkts:	366	45		
IfInPktDrops:	0	0		
IfInDiscards:	0	0		
IfInErrors:	0	0		
IfInOctetsPerSec:	472	83		
IfInPacketsPerSec:	7	1		
IfOutOctets:	38056	442475		
IfOutUcastPkts:	218	362		
IfOutNUcastPkts:	45	365		
IfOutDiscards:	0	0		
IfOutErrors:	0	0		
IfOutOctetsPerSec:	83	472		
IfOutPacketsPerSec:	1	7		
HC2-C04-31 (config) #	¢			

HC2-C04-31 (config) # show port stats port-list 3/1/x9..x14,3/3/g1..g4

IPS Test Results

Overv	iew An	lysis Policies	Devices Objects	MP			Deploy	0, System	Help +	admin 1
Contes	t Explorer	Connections •	Intrusions + Events	Files • Hosts •	Users • Vulnerabi	ities Correlation	Custom •	Search		
						Bookmark This Page Report	t Deligter Di	ashboard View B	ociumarka	Search ¥
EVel Onilido No Sea	nts By wn of Even	Priority and t. Priority, and Clas ts (Edit Search)	Classification (m adjustion + Table View of Ex-	dahiwarkhami mta > Becketa			II 2016-02	-18 21:37:23 - 2	016-02-19	00:44:11 Expanding
	Heis	set .			* Princity	Classificat	lien		Cosot	
\$	Etgied	Q replaced (1:10010	(2:1)		bim	Unknown T)	otts		5	
4	- Project	Z detected (1:10010	(4:42		law	Unknown T	offs		4	
4 (EROTO	COL-1CHP Echo Reph	v (1:408:8)		lani	Misc Active	r .		3	
	Page 1 of	1 >>> Displaying	rows 1-3 of 3 rows							
	Vite		Copy	Delate	Review	Download	Packeta	1		

DLP test results

Fil	e Si	ummary sessions of the local	1		Doctmark The Page Report 1	esigner Dahlbaard view bookmarks Saach • III 2016 02 18 21:37:23 - 2016 02 18 23:36:11 ⁽²⁾ Expanding
No 3	earch	Constraints (Edd Search)				
1	0	Gategory	lus	- Duposition	Action	Count
4	0	COLUMN .	EDE	O Vinkesent	Halware Could Lookup	1
4		ESP. fina	525	O MANAR	Balwarn Stock	1
4		Executables	MORNE	O Clean	Malware Cloud Lookup	*
4	0	Bultimedia	HILT		Box	5
4		EQLina	EDE.		fflock	¥.
4		Executables	MISENE		Detect	*
\$		Aston	728		Detest	1
R	· Page	e 1 of 17) Dapaying in	in 1-7 of 7 rows			

Malware test results

ontext Exp	larer Connections • Intrusions •	Files • Natware Events	Hosts + Users	Vulnerabilities +	Correlation +	Custom •	Search		
					Dookmark The	Page Tapart S	Insigner Dealls	oard. Yes B	ickments Search
alwar	e Summary (setth workfast)						II 2010-02-10	211/27/22 - 2	116-02-18 23-37.3 Expande
Search Co	NUCLEARED (LOC MELLE)								
Search Co	The local sectors of the local		File Name	File SHATTS			File Tons	_	• Count
Search Co	Obtection Name	1	Els.Name	Dis SHA256	65168M		Dis.Lust		• Cosett
Search Co	Oktochen Neme Distantion Neme Distantion Neme Distantion Neme Distantion Neme Distantion Neme Distantion		Elsc.Name	Dis SHA256 O 225e02166 O 25464dee	sizititi Secolari		Elis.Type: Elism 20		• Count 7
Search Co	Outpection Name Detection Name DOM_DIGM_Text file nut: a since tod 002.000%_bits1 002.2embes.NetMicros		Kilk Name Kisk John Kisk John Ala Zambes Jah	0 22562356 0 22562356 0 25663616x	sauthof Dendad Official		Elin Juen Elian Zit Elia		- Count 7 4 1

The hashing done with *a-srcip-b-dstip* configured as part of Step 4 under *"Configuring the GigaVUE-HC2 Inline Network and Inline Tools"* ensures all packets in a given TCP/UDP session go to the same malware group member. It also ensures that if any member of the group goes offline for any reason, the traffic will be distributed amongst the remaining members, thereby ensuring availability of the security functions provided by Cisco FirePOWER. For this test, ten unique IP streams are sent through Inline network port using Spirent test center.

Traffic across Malware sensor 1:

	☆ sgupta — ssh — 119×56
Last login: Tue Mar 15 <u>14:44:18 on ttys000</u> lt-sgupta-mac:~ sguptas ssh admin@10.115.154.13 Password: Last login: Tue Mar 15 21:19:00 2016 from 10.55	.21.122
Copyright 2004-2015, Cisco and/or its affiliate Cisco is a registered trademark of Cisco System All other trademarks are property of their resp	s. All rights reserved. s, Inc. ective owners.
Cisco Fire Linux OS v6.0.0 (build 258) Cisco NGIPSv for VMware v6.0.0 (build 1005)	
> system support capture-traffic	
Please choose domain to capture traffic from: 0 - eth0 1 - InlineMalware (Interfaces eth1, eth2)	
Selection? 1	
NOTE: These changes will be lost the next time	detection is reconfigured!
Please specify tcpdump options desired. (or enter '?' for a list of supported options) Options: -n HS_PACKET_BUFFER_SIZE is set to 4. Opening SFPacket device 'fp1:fp2'	
tcpdump: verbase output suppressed, use -v or listening on fp1:fp2, link-type EN10MB (Etherne 21:45:37.629156 IP 10.10.1.7.1006 > 10.20.1.7.2 21:45:37.629156 IP 10.10.1.9.1008 > 10.20.1.9.2 21:45:37.629200 IP 10.10.1.1.1000 > 10.20.1.1.2	vv for full protocol decode t), capture size 96 bytes 306: Flags [.], ack 234567, win 4096, length 70 308: Flags [.], ack 234567, win 4096, length 70 300: Flags [.], ack 234567, win 4096, length 70
21:45:37.629200 IP 10.10.1.3.1002 > 10.20.1.3.2 21:45:37.629251 IP 10.10.1.5.1004 > 10.20.1.5.2 21:45:37.629251 IP 10.10.1.7.1006 > 10.20.1.7.2 21:45:37.629251 IP 10.10.1.7.1006 > 10.20.1.7.2	2021 Flags [.], ack 234567, win 4096, length 70 2004: Flags [.], ack 234567, win 4096, length 70 2006: Flags [.], ack 1, win 4096, length 70 2021 Flags [.], ack 1, win 4096, length 70
21:45:37.629301 IF 10.10.1.1000 > 10.20.1.1.2 21:45:37.629301 IF 10.10.1.11000 > 10.20.1.1.2 21:45:37.629304 IF 10.10.1.11000 > 10.20.1.1.2	2003; Flags [.], ack 1, win 4096, length 70 300: Flags [.], ack 1, win 4096, length 70 302: Flags [], ack 1, win 4096, length 70
21:45:37.629590 IP 10.10.1.5.1004 > 10.20.1.5.20	002: Flags [.], ack 1, win 4096, length 70
21:45:37.629590 IP 10:10:1.9.1008 > 10:20.1.9.20	008: Flags [.], ack 1, win 4096, length 70
21:45:37.629590 IP 10.10.1.3.1002 > 10.20.1.3.2	002: Flags [.], ack 1, win 4096, length 70
21:45:37.629590 IP 10.10.1.5.1004 > 10.20.1.5.2 21:45:37.629590 IP 10.10.1.7.1006 > 10.20.1.7.2	204: Flags [.], ack 1, win 4096, length 70 206: Flags [.], ack 1, win 4096, length 70
21:45:37.629590 IP 10.10.1.9.1008 > 10.20.1.9.2 21:45:37.629590 IP 10.10.1.1.1000 > 10.20.1.1.2	008: Flags [.], ack 1, win 4096, length 70 000: Flags [.], ack 1, win 4096, length 70
21:45:37.629590 IP 10.10.1.3.1002 > 10.20.1.3.20 21:45:37.629590 IP 10.10.1.5.1004 > 10.20.1.5.20	002: Flags [.], ack 1, win 4096, length 70 004: Flags [.], ack 1, win 4096, length 70
21:45:37.629646 IP 10.10.1.7.1006 > 10.20.1.7.2 21:45:37.629646 IP 10.10.1.9.1008 > 10.20.1.9.2	006: Flags [.], ack 1, win 4096, length 70 008: Flags [.], ack 1, win 4096, length 70
21:45:37.629837 IP 10.10.1.1.1000 > 10.20.1.1.2	000: Flags [.], ack 1, win 4096, length 70 002: Flags [.], ack 1, win 4096, length 70
21:45:37.629837 IP 10.10.1.5.1004 > 10.20.1.5.2	004: Flags [.], ack 1, win 4096, length 70
21:45:37.629837 IP 10.10.1.9.1000 > 10.20.1.7.2 21:45:37.629837 IP 10.10.1.9.1008 > 10.20.1.9.2	000: Flags [.], ack 1, win 4090, length /0 008: Flags [.], ack 1, win 4096, length 70

Traffic across Malware sensor 2:

🔹 😑 🔵 🏠 👔	sh — 125×56
Last login: Tue Mar 15 <u>14:45:12 on ttys000</u> lt-sgupta-mac:~ sgupta <mark>\$</mark> ssh admin@10.115.154.14 Password: Last login: Tue Mar 15 21:44:34 2016 from 10.55.21.122	
Copyright 2004–2015, Cisco and/or its affiliates. All rights res Cisco is a registered trademark of Cisco Systems, Inc. All other trademarks are property of their respective owners.	served.
Cisco Fire Linux OS v6.0.0 (build 258) Cisco NGIPSv for VMware v6.0.0 (build 1005)	
> system support capture-traffic	
<pre>Please choose domain to capture traffic from: 0 - eth0 1 - InlineMalware1 (Interfaces eth1, eth2)</pre>	
Selection? 1	
NOTE: These changes will be lost the next time detection is reco	onfigured!
<pre>Please specify tcpdump options desired. (or enter '?' for a list of supported options) Options: -n MS_PACKET_BUFFER_SIZE is set to 4. Opening SFPacket device 'fpl:fp2' tcpdump: verbose output suppressed, use -v or -vv for full proto listening on fp1:fp2, link-type EN10MB (Ethernet), capture size 21:47:02.168580 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], a 21:47:02.168580 IP 10.10.1.6.1005 > 10.20.1.4.2005: Flags [.], a 21:47:02.168580 IP 10.10.1.8.1007 > 10.20.1.8.2007: Flags [.], a 21:47:02.168580 IP 10.10.1.2.1001 > 10.20.1.4.2003: Flags [.], a 21:47:02.168580 IP 10.10.1.4.1003 > 10.20.1.4.2009: Flags [.], a 21:47:02.168580 IP 10.10.1.6.1005 > 10.20.1.6.2009: Flags [.], a 21:47:02.168580 IP 10.10.1.10.1009 > 10.20.1.10.2009: Flags [.], a 21:47:02.168580 IP 10.10.1.4.1003 > 10.20.1.4.2009: Flags [.], a 21:47:02.168580 IP 10.10.1.4.1003 > 10.20.1.4.2009: Flags [.], a 21:47:02.168638 IP 10.10.1.4.1003 > 10.20.1.4.2009: Flags [.], a 21:47:02.168638 IP 10.10.1.4.1003 > 10.20.1.4.2009: Flags [.], a 21:47:02.168692 IP 10.10.1.2.1001 > 10.20.1.2.2001: Flags [.], a 21:47:02.168892 IP 10.10.1.2.1001 > 10.20.1.2.2001: Flags [.], a 21:47:02.168892 IP 10.10.1.4.1003 > 10.20.1.2.2001: Flags [.], a 21:47:02.168892 IP 10.10.1.4.1003 > 10.20.1.4.2009: Flags [.], a 21:47:02.168892 IP 10.10.1.8.1007 > 10.20.1.8.2007: Flags [.], a 21:47:02.168892 IP 10.10.1.8.1007 > 10.20.1.8.2007: Flags [.], a 21:47:02.168892 IP 10.10.1.8.1007 > 10.20.1.8.2007: Flags [.], a 21:47:02.168892 IP 10.10.1.8.1007 > 10.20.1.8.2007:</pre>	bool decode 96 bytes 96 bytes 16ck 234567, win 4096, length 70 16ck 1, win 4096, length 70 17ck 1, win 4006, length 70 17ck 1, win 4006, len
<pre>21:47:02.169143 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], a 21:47:02.169143 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], a 21:47:02.169143 IP 10.10.1.6.1005 > 10.20.1.6.2005: Flags [.], a</pre>	sck 1, win 4096, length 70 sck 1, win 4096, length 70 sck 1, win 4096, length 70
21:47:02.168892 IP 10.10.1.10.1009 > 10.20.1.10.2009: Flags [.], 21:47:02.168892 IP 10.10.1.2.1001 > 10.20.1.2.2001: Flags [.], a 21:47:02.168892 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], a 21:47:02.168892 IP 10.10.1.6.1005 > 10.20.1.6.2005: Flags [.], a 21:47:02.168892 IP 10.10.1.8.1007 > 10.20.1.6.2007: Flags [.], a 21:47:02.168892 IP 10.10.1.20.009 > 10.20.1.10.2009: Flags [.], 21:47:02.168892 IP 10.10.1.4.1003 > 10.20.1.2009: Flags [.], 21:47:02.168892 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], 21:47:02.168892 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], 21:47:02.168892 IP 10.10.1.8.1007 > 10.20.1.4.2003: Flags [.], 21:47:02.168894 IP 10.10.1.8.1007 > 10.20.1.8.2007: Flags [.], 21:47:02.168944 IP 10.10.1.8.1007 > 10.20.1.8.2007: Flags [.], 21:47:02.168944 IP 10.10.1.2.1001 > 10.20.1.2.2001: Flags [.], 21:47:02.168944 IP 10.10.1.2.1001 > 10.20.1.2.2001: Flags [.], 21:47:02.169143 IP 10.10.1.4.1003 > 10.20.1.4.2003: F	, ack 1, win 4096, length 70 ack 1, win 4096, length 70

Device Management NAT VPN Platform Settings							
			By Group	*	0	A35	
Name	Model	License Type	Access Centrol Peller				
• G Ungrouped (4)							
PReDownloadDetection_Sensor 10.115.154.12 - NOJPSir for VMware - v6.0.0	MGIPSv for VMware	Protection, Control, Malware, URL -	File Download Detection - DLP	3	2.8		
C IPS_Sensor 10.115.154.11 - NGIPSr for VIIIware - v6.0.0	NGIPSv for VMware	Protection, Control, Malware, URL	15		1 8		
HalwareDetection1_Sensor 10.115.154.13 - NGIPSr for VMware - v6.0.0	NGIPSv for VMware	Protection, Control, Malware, URL	Patware Detection		ø i		
MalwareDetection2_Sensor 10.115.154.14 - NGIPSr for VMware - v6.0.0	NGIPSv for VMware	Protection, Control, Malware, URL	Palware-Detectory	70	/ 8		

Malware sensor 1 goes down:

Traffic re-distributed to Malware sensor 2:

• • •	
Last login: Tue Mar 15 14:27:14 on ttys000 lt-squpta-mac:	
Copyright 2004-2015, Cisco and/or its affiliates. All rights r Cisco is a registered trademark of Cisco Systems, Inc. All other trademarks are property of their respective owners.	eserved.
Cisco Fire Linux 05 v6.0.0 (build 258) Cisco NGIPSv for VMware v6.0.0 (build 1005)	
> system support capture-traffic	
Please choose domain to capture traffic from: 0 - eth0 1 - InlineMalware1 (Interfaces eth1, eth2)	
Selection? 1	
NOTE: These changes will be lost the next time detection is re	configured!
NOTE: These changes will be lost the next time detection is re Please specify tcpdump options desired. (or enter '?' for a list of supported options) Options:	tocol decode e 96 bytes ack 234567, win 4096, length 70 ack 1, win 4096, length 70
21:4217.050637 IP 10:10:1.5.1000 > 10:20.1.9.2000; Flags [, 21:4217.050637 IP 10:10:1.1009 > 10:20.1.12.2009; Flags [, 21:42:17.056637 IP 10:10:1.1.1000 > 10:20.1.2.2001; Flags [,] 21:4217.056946 IP 10:10:1.2.1001 > 10:20.1.2.2001; Flags [,]	ack 1, win 4096, length 70 ack 1, win 4096, length 70
21:42:17.056946 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], 21:42:17.056946 IP 10.10.1.5.1004 > 10.20.1.5.2004: Flags [.], 21:42:17.056946 IP 10.10.1.6.1005 > 10.20.1.5.2004: Flags [.], 21:42:17.056946 IP 10.10.1.6.1005 > 10.20.1.5.2004: Flags [.],	ack 1, win 4096, length 70 ack 1, win 4096, length 70 ack 1, win 4096, length 70 ack 1, win 4096, length 70
21:42:17.030340 1P 10.10.1.7.1000 > 10.20.1.7.2000; Plags [.],	ack 1, win 4090, tength /0

3 Summary and Conclusions

The previous chapters showed how to deploy Gigamon GgiaVUE-HC2 bypass protection with Cisco FirePOWER network security sensor. This combined solution using the Gigamon-GigaVUE-HC2 chassis for inline tool high availability and traffic distribution achieves the following objectives:

- High availability of FirePOWER NGIPSv Platform 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.
- 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 <u>www.gigamon.com</u>.

How to get Help

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

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

See Inside Your Network $^{\rm TM}$

4061-01 04/16