RSA Ready Implementation Guide for RSA Security Analytics

Gigamon GigaSECURE Visibility for OpenStack Clouds

Jeffrey Carlson, RSA Partner Engineering

Last Modified: 04/20/2016

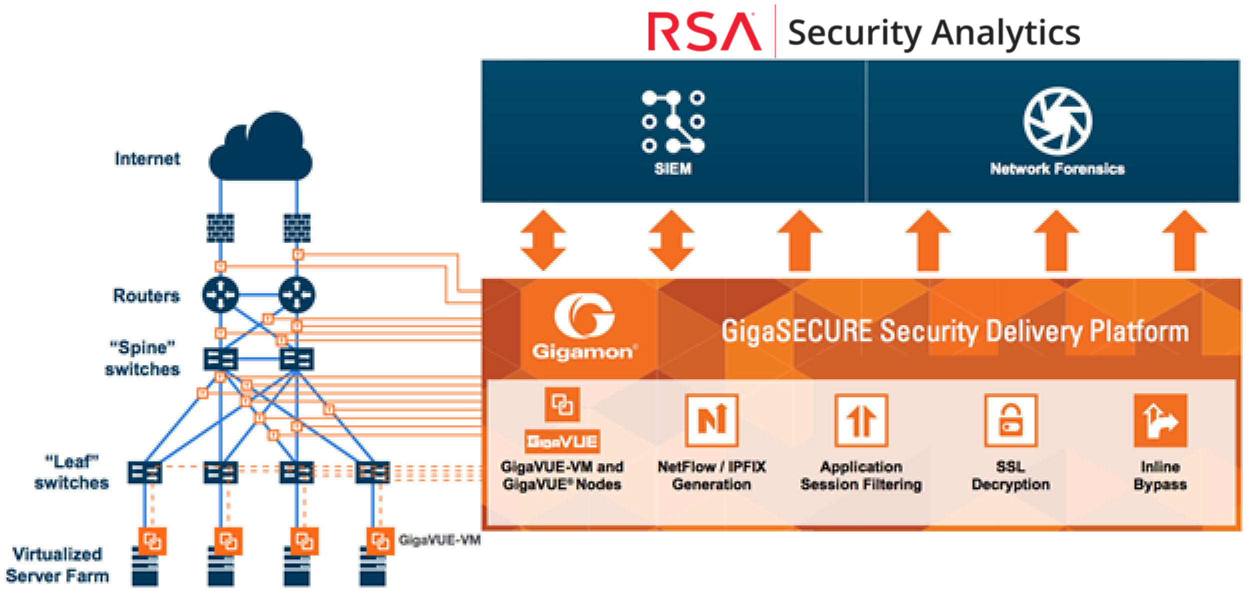
Solution Summary

The GigaSECURE security delivery platform is comprised of scalable hardware and software elements that give security administrators unparalleled visibility and capability for bolstering security effectiveness. By delivering targeted traffic to RSA Security Analytics, organizations will have enhanced visibility of both virtual and physical network traffic and are better able to manage this traffic through a single console, correlated to one security tool.

Additional key benefits of the GigaSECURE platform include:

- Infrastructure-wide reach via Gigamon's GigaVUE-VM and GigaVUE® nodes to feed RSA Security Analytics with pervasive traffic visibility.
- NetFlow record generation that is unsampled.
- Application Session Filtering, which eliminates unwanted traffic such as streaming video from the examined traffic flows.
- SSL decryption for faster threat analysis.

RSA Security Analytics Tested Features	
Gigamon GigaSECURE Visibility for OpenStack Clouds	
Flow / Traffic Mapping	Yes
De-duplication	Yes



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Gigamon GigaSECURE platform with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Gigamon GigaSECURE components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure the Gigamon GigaSECURE platform is properly configured and secured before deploying to a production environment. For more information, please refer to the Gigamon GigaSECURE documentation or website.

Gigamon GigaSECURE Configuration

RSA Security Analytics gives organizations the necessary context to help detect and respond to today's advanced attacks before they can inflict widespread damage. By delivering virtual traffic to RSA Security Analytics, GigaSECURE is designed to provide security operations teams with active visibility to detect, investigate and take timely and targeted action against advanced threats.

In order to manage the various components of the Gigamon framework, you must first install the GigaVUE Fabric Manager. GigaVUE-FM is a web-based fabric management software that provides high-level visibility and management of both the physical and virtual traffic visibility nodes that form the Gigamon Traffic Visibility Fabric^{TM}. GigaVUE-FM can manage both physical GigaVUE nodes (GigaVUE G Series, GigaVUE TA Series, GigaVUE H Series, and virtual GigaVUE nodes.

GigaVUE-FM also extends visibility into the virtual environments by allowing for the discovery, configuration, and management of the GigaVUE-VM virtual traffic visibility node. GigaVUE-VM provides powerful Flow Mapping technology for the traffic flowing between virtual machines, allowing distribution of cloud-based traffic to physical tool ports in the visibility fabric.

Component Overview

OpenStack is an open source cloud operation system that controls large pools of compute, storage, and networking resources throughout a data center. Integrating GigaVUE-FM with an OpenStack environment makes it possible to extend network traffic visibility into public, private, and hybrid OpenStack clouds. The following sections provide an overview of the components used in the integration

GigaVUE-vTAP Agents

G-vTAP agents enable monitoring of a vNIC. The agents are a software package (debian or rpm) installed inside a VM. After installation, the vNICs are registered with the agent for monitorability. The vNICS can be registered to monitor in either the ingress direction or egress, or both.

G-vTAP Controller

The G-vTAP controller is a single point for communicating with all monitored G-vTAP agents on the monitored VMs in the OpenStack cloud. The controller is responsible for discovering the vNICs permissions as well as configuring mirrors and maps on the monitored VMs by talking to the G-vTAP agent on them. G-vTAP agents are installed inside the VMs to be monitored.

GigaVUE-VM

GigaVUE-VM in an OpenStack cloud is connected to the tenant's networks and provides additional filtering and slicing of traffic to Visibility Fabric. The GigaVUE-FM page under OpenStack > Visibility Fabric displays information about the GigaVUE-VM instances in the OpenStack cloud launched by GigaVUE-FM. To view the information about the GigaVUE-VM instances, select **OpenStack > Visibility Fabric > GigaVUE-VM**

Installation and Integration Overview

This section provides the steps for integrating OpenStack and GigaVUE-FM. Installing and setting up Gigamon components for the OpenStack cloud consists of the following general steps:

- **Step 1:** Network Configuration
- **Step 2:** Install the G-vTAP Agents
- **Step 3:** Upload Images to Glance
- **Step 4:** Install the GigaVUE-FM Server
- **Step 5:** Configure GigaVUE-FM to Monitor OpenStack Traffic

For the purposes of this document, only **Step 5** will be covered in detail.

! Important: The installation and Integration Steps outlined here are being covered at a high level. For in-depth detailed instructions, please consult the *Configuring Visibility for OpenStack Clouds* section of the *GigaVUE-FM User's Guide*

Configuring GigaVUE-FM to Monitor OpenStack Traffic

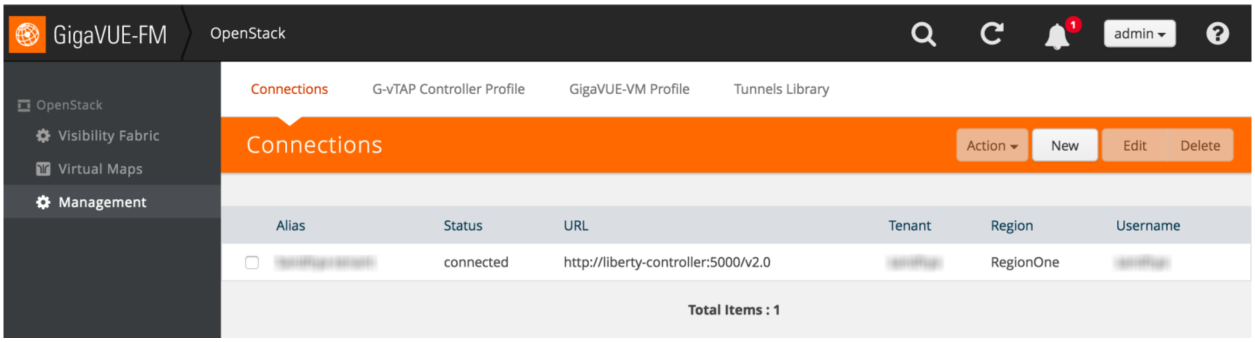
The **Management** link in the OpenStack navigation pane provides access to the pages for configuring the connections to the OpenStack cloud and the profiles for the G-vTAP controllers and GigaVUE-VM instances.

Configuring GigaVUE-FM to monitor OpenStack traffic involves several tasks.

1. **Creating a Connection**
2. **Create a G-vTAP Controller Configuration Profile**
3. **Create a GigaVUE-VM Configuration Profile**
4. **Create a Tunnel to the GigaSMART Device**
5. **Create Virtual Maps**

Creating a Connection

The connection defines the parameters of the connection to the OpenStack cloud. To see the currently defined connections and their status, select **Management >Connections**.



Alias	Status	URL	Tenant	Region	Username
[redacted]	connected	http://liberty-controller:5000/v2.0	[redacted]	RegionOne	[redacted]

Total Items : 1

This task adds the OpenStack cloud controller to GigaVUE-FM.

1. In GigaVUE-FM, select OpenStack > Management > Connections.
2. Click New.
3. Enter values in the following fields:

You can use the following controls on the Connections page to make changes:

If GigaVUE-FM connects to OpenStack successfully, the connection status will be displayed on the Connections page as connected in the Status column. Otherwise, one of the following errors will be reported:

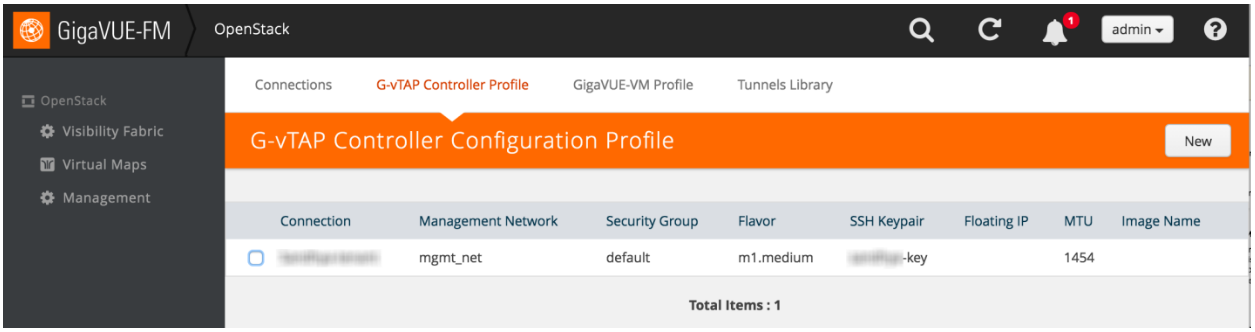
- authFailed—the authentication did not go through.
- invalidUrl—the URL provided is not valid
- connFailed—the connect failed for another reason, such as incorrect regionName, the OpenStack controller was not reachable, or its name is not DNS resolvable from GigaVUE-FM.

Once a connection is created, GigaVUE-FM discovers the inventory of the cloud in the

Create a G-vTAP Controller Configuration Profile

The G-vTAP Controller profile defines the parameters of a G-vTAP Controller. To display the parameters of currently configured profiles, select Management > G-vTAP Controller Profile.

Creating the configuration profile automatically deploys the G-vTAP Controller.

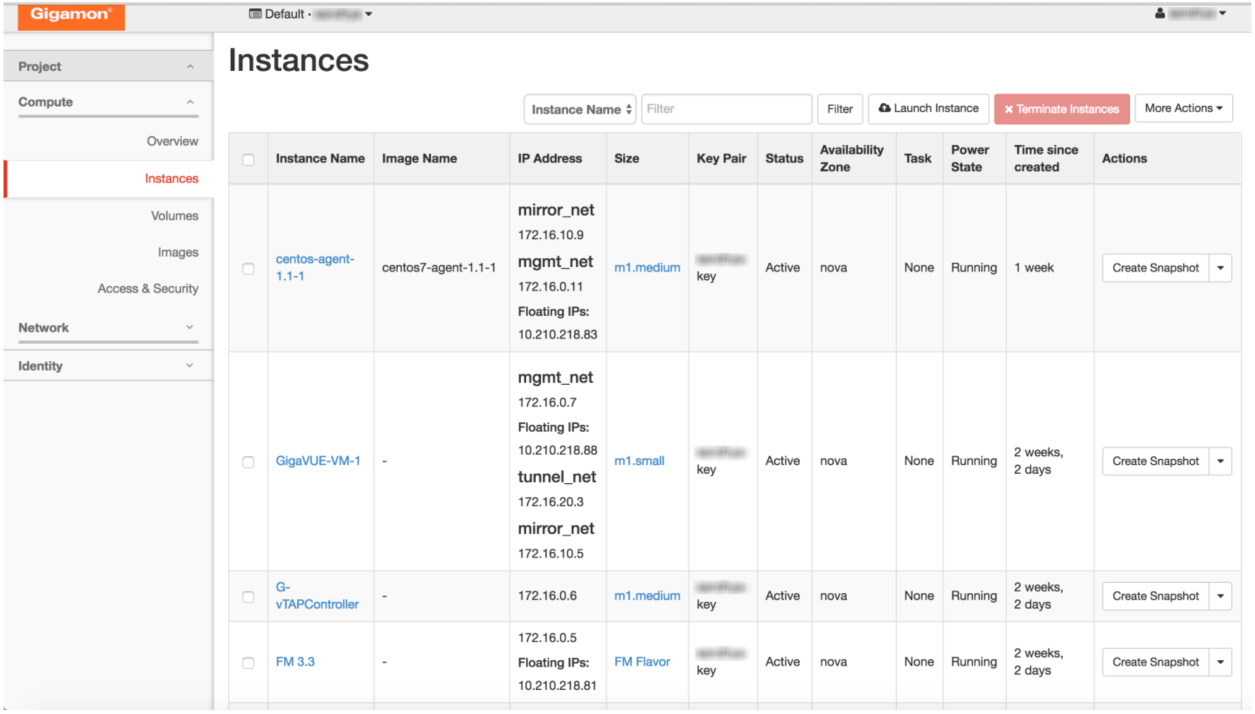


Connection	Management Network	Security Group	Flavor	SSH Keypair	Floating IP	MTU	Image Name
[redacted]	mgmt_net	default	m1.medium	[redacted]-key		1454	

Total Items : 1

1. In GigaVUE-FM, select **OpenStack > Management > G-vTAP Controller Profile**.

2. Click **New**.
3. Enter values for all of the appropriate fields. Consult the *GigaVUE-FM User's Guide* for more details.
4. Verify that the G-vTAP Controller instance is created and running by doing the following:
    a. Verify in the OpenStack Horizon UI. Select **OpenStack Horizon UI > Compute > Instances**:



Instances

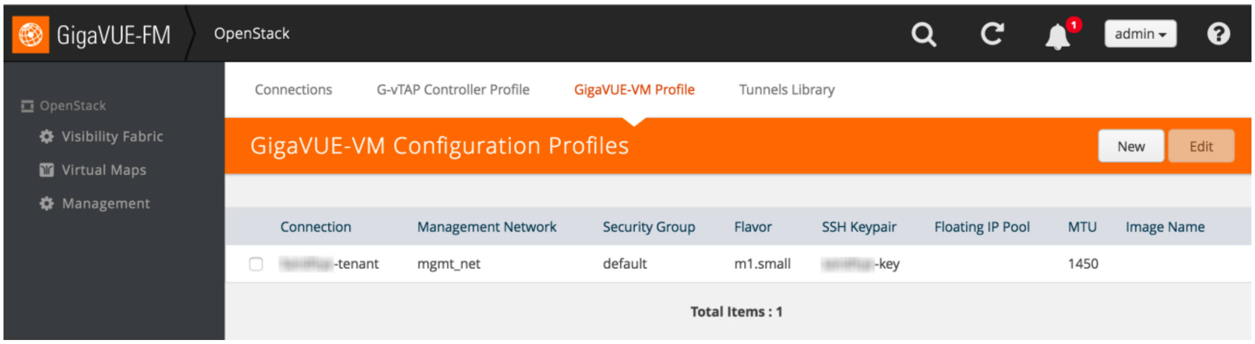
☐	Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
☐	centos-agent-1.1-1	centos7-agent-1.1-1	mirror_net 172.16.10.9 mgmt_net 172.16.0.11 Floating IPs: 10.210.218.83	m1.medium	[redacted] key	Active	nova	None	Running	1 week	Create Snapshot ▾
☐	GigaVUE-VM-1	-	mgmt_net 172.16.0.7 Floating IPs: 10.210.218.88 tunnel_net 172.16.20.3 mirror_net 172.16.10.5	m1.small	[redacted] key	Active	nova	None	Running	2 weeks, 2 days	Create Snapshot ▾
☐	G-vTAPController	-	172.16.0.6	m1.medium	[redacted] key	Active	nova	None	Running	2 weeks, 2 days	Create Snapshot ▾
☐	FM 3.3	-	172.16.0.5 Floating IPs: 10.210.218.81	FM Flavor	[redacted] key	Active	nova	None	Running	2 weeks, 2 days	Create Snapshot ▾

    b. Verify in GigaVUE-FM. **Select OpenStack > Virtual Visibility Fabric > G-vTAP Controllers**

    Wait for the **Version** field to be populated. Click on the "Refresh" icon on the top right corner to refresh this page. If it does not get populated within a short interval, something either went wrong in the process of launching, or the parameters provided are improper. The status will go to **Unreachable** for a while before the management IP field gets populated.

Create a GigaVUE-VM Configuration Profile

The GigaVUE-VM configuration profile defines the parameters of the GigaVUE-VM deployed in the OpenStack cloud. To see the currently defined GigaVUE-VM profiles, select, OpenStack > Management > GigaVUE-VM Profile.



GigaVUE-VM Configuration Profiles

	Connection	Management Network	Security Group	Flavor	SSH Keypair	Floating IP Pool	MTU	Image Name
□	[redacted]-tenant	mgmt_net	default	m1.small	[redacted]-key		1450	

Total Items : 1

To create a GigaVUE-FM profile, do the following:

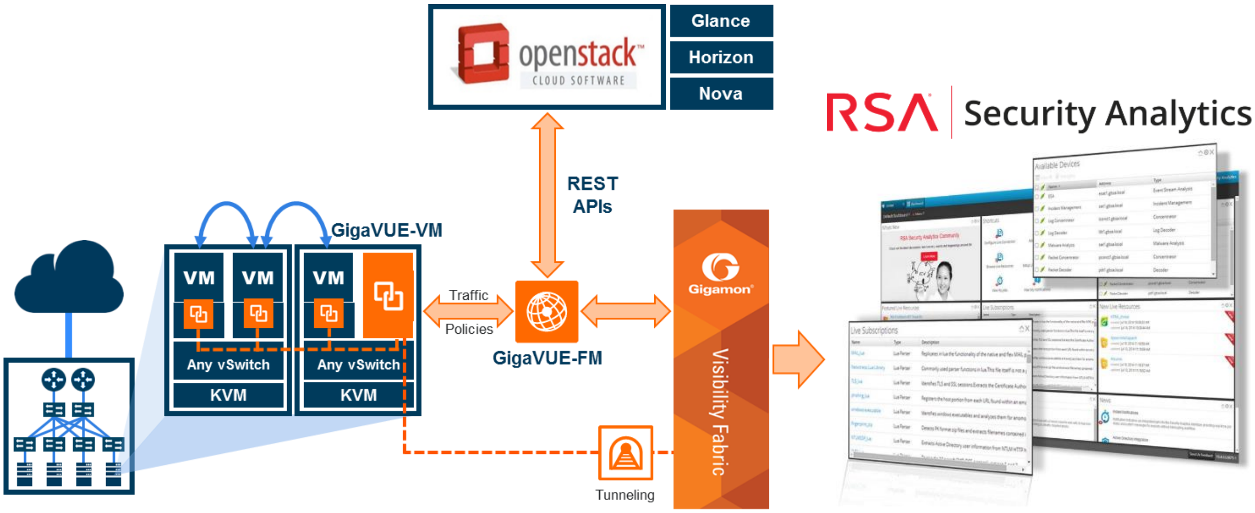
1. In GigaVUE-FM, select **OpenStack > Management > GigaVUE-VM Profile**.
2. Click **New**.
3. Enter values for all of the appropriate fields. Consult the *GigaVUE-FM User's Guide* for more details.
4. Click **Save**. The GigaVUE-VM deployment process starts.
5. Confirm that the minimum number of GigaVUE-VMs instances are launched and running.
    a. Verify in OpenStack Horizon UI. Select **OpenStack Horizon UI > Compute > Instances**.
    b. Verify in FM. Select **OpenStack > Virtual Visibility Fabric > GigaVUE-VM**

       Wait for the **Version** field to get populated. Click on the Refresh icon on top right corner to refresh this page. If it does not get populated within a reasonable time (this may take a few minutes or longer, depending on resources), something either went wrong in the process of launching or the parameters provided are improper. The status goes to **Unreachable** for a while before the management IP field gets populated.

Create a Tunnel to the GigaSMART Device

The GigaSECURE platform ensures that RSA Security Analytics has access to the right virtual traffic and network metadata from all across the network. The platform consists of distributed physical (GigaVUE H Series platforms) and virtual (GigaVUE-VM) nodes that provide an advanced level of filtering intelligence, managed as a single fabric. At its heart is Gigamon's patented Flow Mapping® technology that identifies and directs incoming traffic to single or multiple tools based on user-defined rules.

Packets from virtual workloads find their way to physical tool ports on Gigamon physical devices through a GigaSMART tunnel. The tunnel starts at the GigaVUE-VM node and ends at a network port on a GigaSMART-enabled GigaVUE G Series or GigaVUE H Series node. In both cases, the receiving end of the tunnel must have a tunnel decapsulation GigaSMART Operation bound. Consult the **Configuring the GigaSMART Tunnel** portion of the ***GigaVUE-FM and GigaVUE-VM User's Guide*** for more information on how to do this.

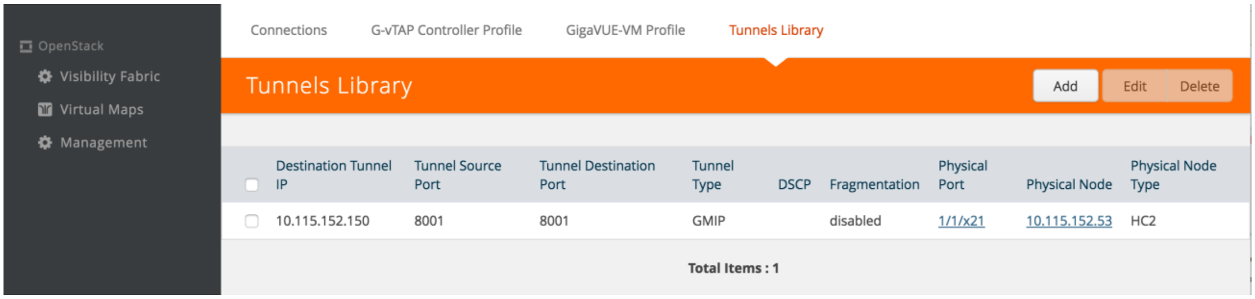


The Tunnels Library page is where you define the destination tunnel IP of the GigaVUE node that the GigaVUE-VM instance uses to communicate with the node.

NOTE: In the current release, OpenStack integration only supports GMIP tunnels.

To create a tunnel to the GigaSMART device, do the following:

1. In GigaVUE-FM, select **OpenStack > Management > Tunnels Library**.



Tunnels Library

	Destination Tunnel IP	Tunnel Source Port	Tunnel Destination Port	Tunnel Type	DSCP	Fragmentation	Physical Port	Physical Node	Physical Node Type
□	10.115.152.150	8001	8001	GMIP		disabled	1/1/x21	10.115.152.53	HC2

Total Items : 1

2. Click **Add**.
3. The GigaVUE tunnels discovered should be displayed on Tunnels Library page. If it is displayed, do the following:
   a. Select the tunnel that is configured to receive traffic from the GigaVUE-VMs in the OpenStack cloud.
   b. Enter the **Tunnel Source Port**. This value can be used on the H Series GigaSMART device to associate which source port the mirrored traffic is originating from. Enter 1 if this is not expected to be used.
   c. Click **OK**.
4. If the desired GigaVUE tunnel was not discovered, you must enter the tunnel information manually:
   a. Select **Other**.
   b. For **Type**, select **GMIP**
   c. For the **Destination Tunnel IP**, enter the destination tunnel IP address. This is the IP address of the tunnel port on the H Series device with GigaSMART.

d. For **Tunnel Destination Port**, enter the destination port. This should be the port that is configured to receive traffic from the GigaVUE-VMs in the OpenStack cloud.

e. For **Tunnel Source Port**, enter the source port. This value can be used on the H Series GigaSMART device to associate which source port the mirrored traffic is originating from. Enter 1 if this is not expected to be used.

f. Click **OK**.

Create Virtual Maps

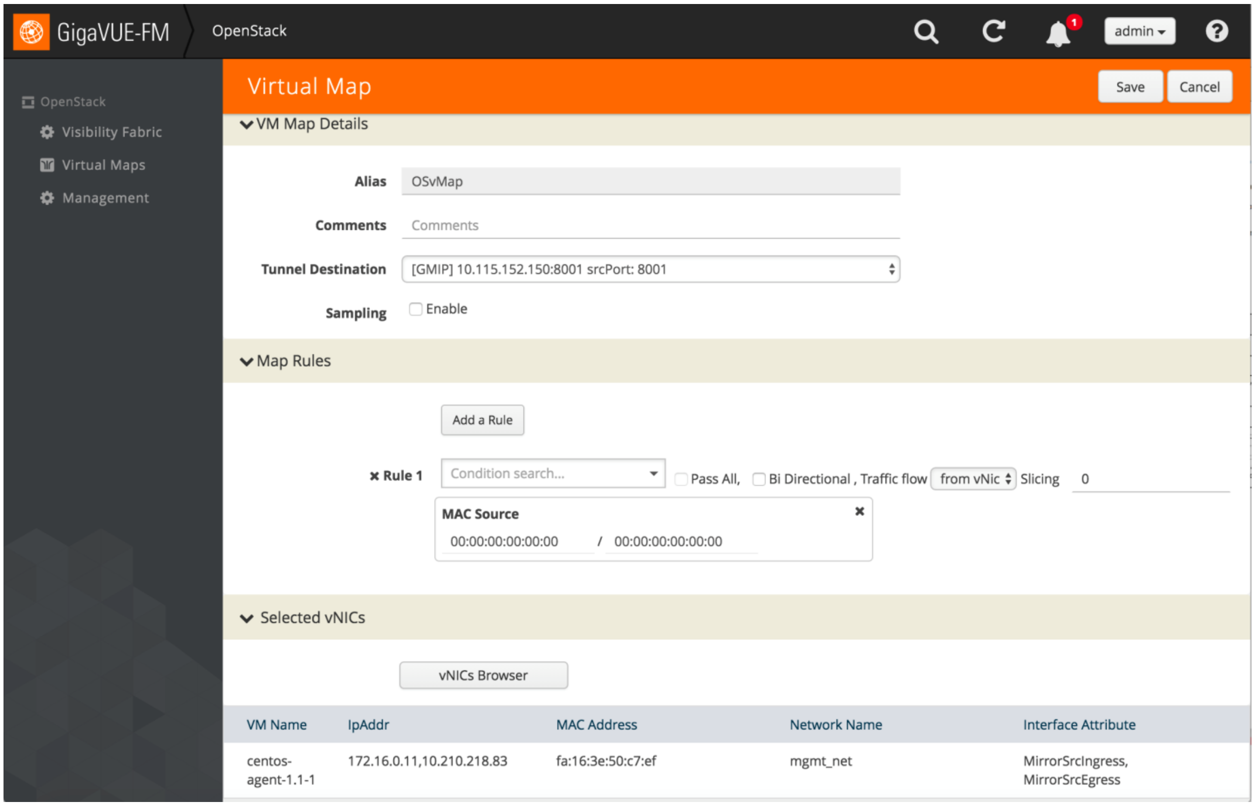
The virtual maps for OpenStack integration are used to specify which vNIC to monitor and how to filter the traffic, and whether the traffic is to or from the vNIC.

Virtual maps for OpenStack differ from VMware maps. Bi Directional is selectable for OpenStack but not for VMware. There is also a Pass All check box to indicate whether the rule should pass the traffic without filtering. VMware maps do not have this option. You can also specify whether the traffic to be monitored flows out from the vNIC or into the vNIC.

Once the Virtual maps are deployed, any existing maps created manually or by another application will be destroyed on the GigaVUE-VMs and G-vTAP agents

To create virtual maps, do the following:

1. In GigaVUE-FM, select OpenStack > Virtual Maps.
2. Click **New**.



Alias: OSvMap

Comments: Comments

Tunnel Destination: [GMIP] 10.115.152.150:8001 srcPort: 8001

Sampling: □ Enable

× Rule 1: Condition search... □ Pass All, □ Bi Directional , Traffic flow from vNic Slicing 0

MAC Source: 00:00:00:00:00:00 / 00:00:00:00:00:00

VM Name	IpAddr	MAC Address	Network Name	Interface Attribute
centos-agent-1.1-1	172.16.0.11,10.210.218.83	fa:16:3e:50:c7:ef	mgmt_net	MirrorSrcIngress, MirrorSrcEgress

3. In the Virtual Maps page, specify the following:

Field	Description
Alias	An alias that helps identify the map.
Comments	Optional detailed description of the map.
Tunnel Description	Select a tunnel destination. This is the tunnel to the H Series GigaSMART device created in the *Create a Tunnel to the GigaSMART Device*.
Add a Rule	Construct rules for the map by selecting from the available choices.
vNICS Browser	Select the virtual network interfaces to be monitored from the Quick view that displays. Some of the items in the list will be grayed out and will not be selectable. These are the vNICs that are either not registered with the G-vTAP agent for ingress or egress direction monitoring, or those that do not have a G-vTAP agent at all, or those that are registered for mirrorDst.

4. Click **Save**.
5. Click the refresh icon on top right corner of the UI to refresh the map status.

RSA Security Analytics Configuration

Overview

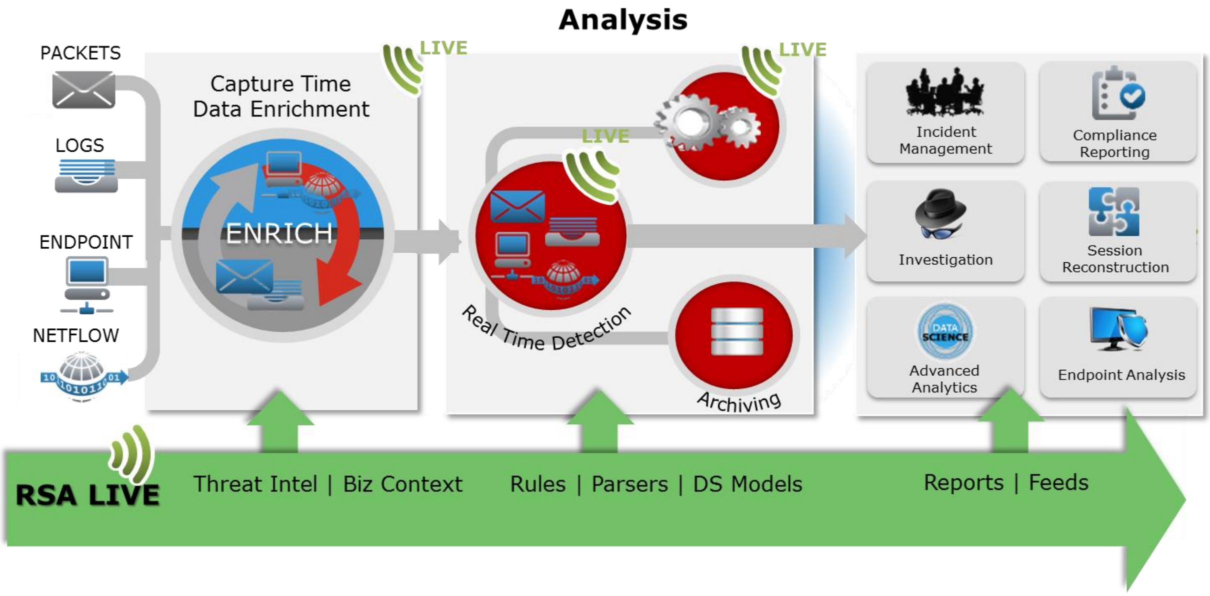
Security teams need to evolve to stay in front of attackers and the latest threats, but in recent years this has become much more difficult. Attackers continue to advance and use sophisticated techniques to infiltrate organizations. Attackers spend significant resources performing reconnaissance to learn about organizations and develop techniques specifically designed to bypass the security tools being used.

Tools, Tactics and Procedures (TTPs) are the ways the attackers work to target, exploit and compromise organizations. In recent years, attacker TTPs have become more sophisticated, mimicking normal user enterprise behavior, and undetectable by preventative, perimeter based security controls.

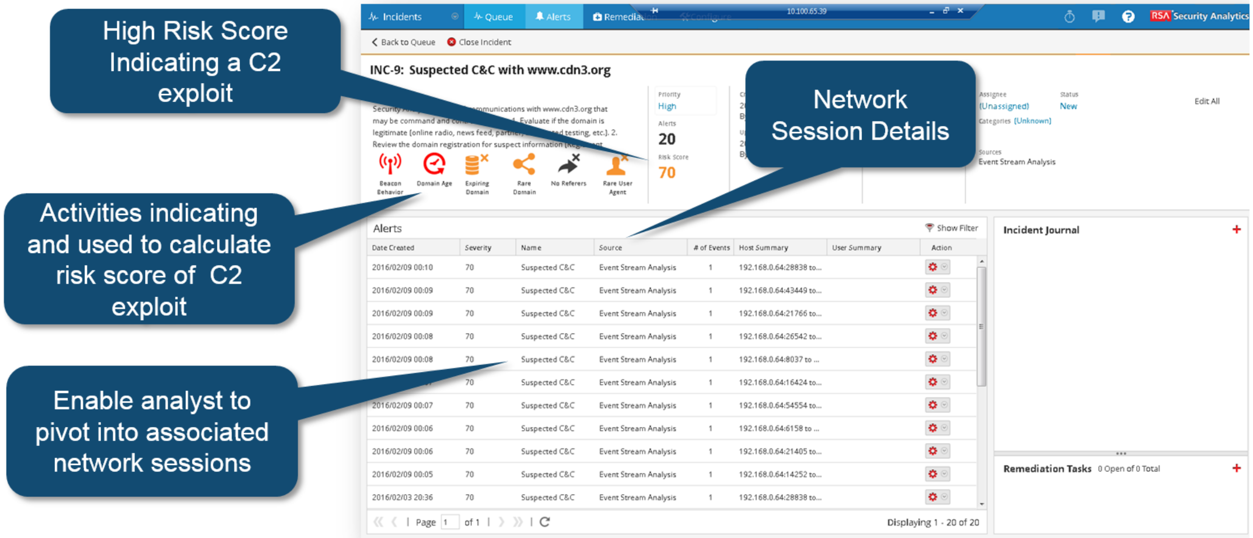
RSA Security Analytics provides pervasive visibility with real-time behavior analytics to detect and investigate the sophisticated attacker TTPs. Visibility is provided across:

- Data Sources – Full Packet Capture, NetFlow and Logs
- Threat Vectors – Endpoint, Network and Cloud

RSA Security Analytics' unique architecture captures and enriches data sources with security context in realtime. Additionally, threat intelligence is applied to the enriched data to identify high risk indicators as APT domains, suspicious proxies or malicious networks. This method of processing large data sources in realtime provides analysts with security insight into their entire environment from on-premise to cloud.



Analysts can detect and investigate sophisticated attacks and truly understand the attacker TTPs. RSA Security Analytics captures full network packets, which means an attack can be reconstructed to fully understand the attacker TTPs and in turn implement an effective remediation plan to stop the attacker from achieving their objective.



High Risk Score Indicating a C2 exploit

Network Session Details

Activities indicating and used to calculate risk score of C2 exploit

Enable analyst to pivot into associated network sessions

INC-9: Suspected C&C with www.cdn3.org

Security [illegible] communications with www.cdn3.org that may be command and con[illegible] 1. Evaluate if the domain is legitimate (online radio, news feed, partner, [illegible]ed testing, etc.). 2. Review the domain registration for suspect information [illegible]

Priority High

Alerts 20

Risk Score 70

Assignee (Unassigned)

Status New

Categories (Unknown)

Sources Event Stream Analysis

Alerts

Date Created	Severity	Name	Source	# of Events	Host Summary	User Summary	Action
2016/02/09 00:10	70	Suspected C&C	Event Stream Analysis	1	192.168.0.64:28838 to...		
2016/02/09 00:09	70	Suspected C&C	Event Stream Analysis	1	192.168.0.64:43449 to...		
2016/02/09 00:09	70	Suspected C&C	Event Stream Analysis	1	192.168.0.64:21766 to...		
2016/02/09 00:08	70	Suspected C&C	Event Stream Analysis	1	192.168.0.64:26542 to...		
2016/02/09 00:08	70	Suspected C&C	Event Stream Analysis	1	192.168.0.64:8037 to ...		
[illegible]	70	Suspected C&C	Event Stream Analysis	1	192.168.0.64:16424 to...		
2016/02/09 00:07	70	Suspected C&C	Event Stream Analysis	1	192.168.0.64:54554 to...		
2016/02/09 00:06	70	Suspected C&C	Event Stream Analysis	1	192.168.0.64:6158 to ...		
2016/02/09 00:06	70	Suspected C&C	Event Stream Analysis	1	192.168.0.64:21405 to...		
2016/02/09 00:05	70	Suspected C&C	Event Stream Analysis	1	192.168.0.64:14252 to...		
2016/02/03 20:36	70	Suspected C&C	Event Stream Analysis	1	192.168.0.64:28838 to...		

Page 1 of 1

Displaying 1 - 20 of 20

Incident Journal

Remediation Tasks 0 Open of 0 Total

As a platform, Gigamon GigaSECURE is comprised of scalable hardware and software elements that give security administrators unparalleled visibility and capability for bolstering security effectiveness. By delivering targeted traffic to RSA Security Analytics, organizations will have enhanced visibility of both virtual and physical network traffic and are better able to manage this traffic through a single console, correlated to one security tool.

Certification Checklist for RSA Security Analytics

Date Tested: April 14th, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
GigaVUE FM	3.3	OS
GigaSMART	4.6	OS
OpenStack	Liberty	OS

Security Analytics Test Cases	**Result**
Packet Loss	
Syslog TCP data consumed by the SA Log Decoder	✓
Syslog UDP data consumed by the SA Log Decoder	✓
Various packet data consumed by the SA Packet Decoder	✓
De-duplication	
Replaying data files to the SA Packet Decoder	✓
Traffic Mapping	
Mapping network service ports to dedicated ports	✓
Performance	
SA Log Decoder minimal EPS performance	✓
SA Packet Decoder minimal EPS performance	✓

✓ = Pass ✗ Fail N/A = Non-Available Function