Gigamon
GigaSECURE®

RSA Ready Implementation Guide for RSA Security Analytics

Last Modified: November 11th, 2015

Partner Information

Product Information	
Partner Name	Gigamon
Web Site	www.gigamon.com
Product Name	GigaSECURE
Version & Platform	GigaVUE-FM 3.1.00
Product Description	The GigaSECURE® Security Delivery Platform connects into the network, both physical and virtual, and can be configured to deliver traffic to all of the applications that require it. Security appliances such as RSA Security Analytics simply connect into the GigaSECURE platform—at whatever interface speeds they are capable of—to receive a high-fidelity stream of relevant traffic from across the network infrastructure. The GigaSECURE platform also extracts flow-based meta-data from network traffic, which can be routed to various security tools for analysis.

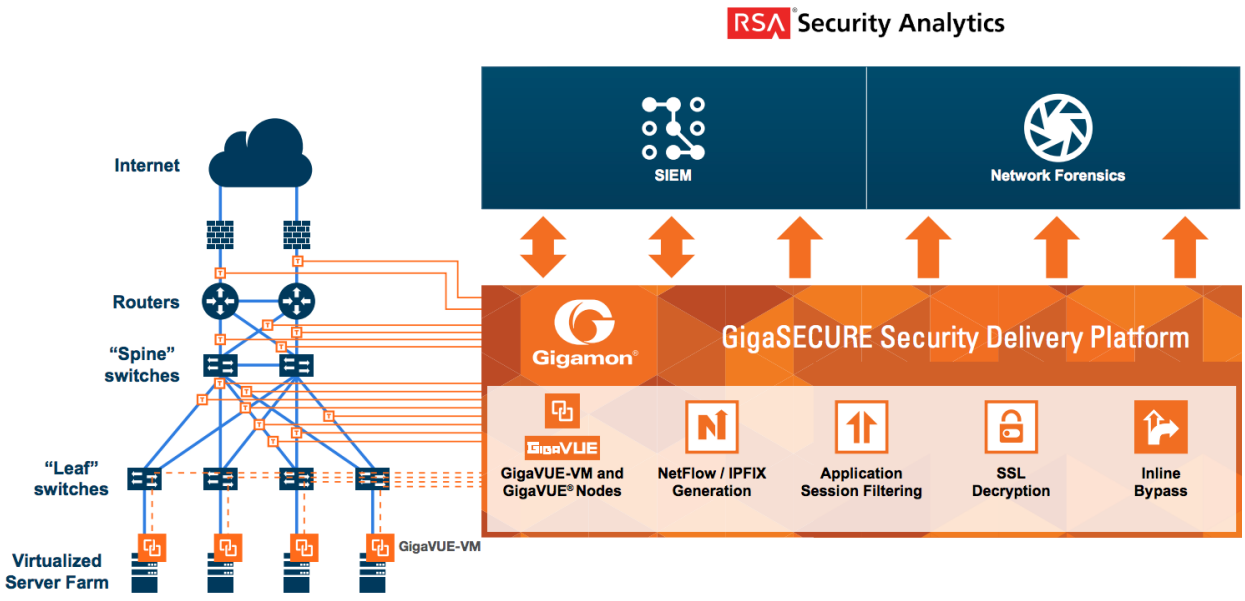
Solution Summary

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 security delivery platform	
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 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™. 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.

Deploying GigaVUE-VM

The GigaVUE-VM software package is distributed as an OVA file. The following section describes how to deploy GigaVUE-VM nodes on an ESXi host.

> **Note: The following instructions have been tested on VMware vSphere 5.0 and later.**

Deploying GigaVUE-VM nodes consists of the following major steps:

1. Configure port-groups and port-profiles within vSphere. Refer to the Configuring Port Groups/Port-Profiles section of the ***GigaVUE-FM and GigaVUE-VM User's Guide*** for more information on how to do this.
2. Set up the connection between the Fabric Manager and the Virtual Center. Refer to the **Setting**

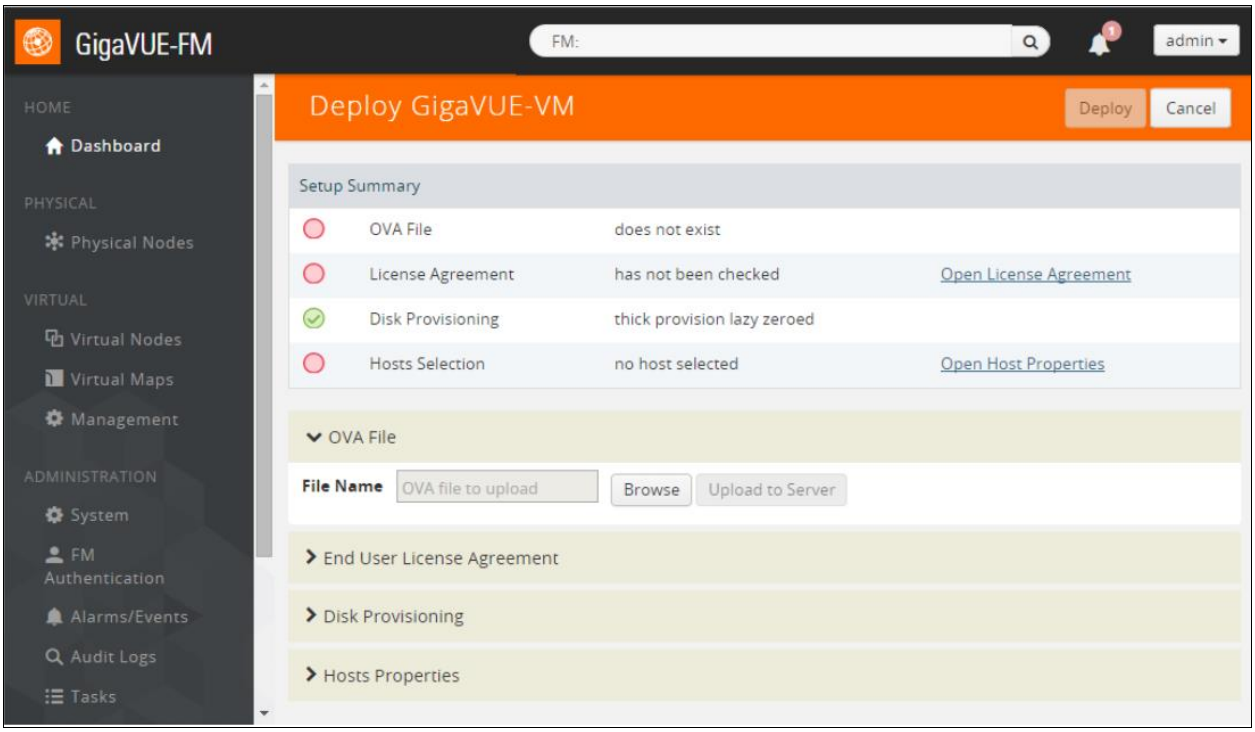
up the Connection between GigaVUE-FM and Virtual Center section of the ***GigaVUE-FM and GigaVUE-VM User's Guide*** for the necessary steps to configure the connection.

3. Deploy GigaVUE-VM nodes using the Bulk Deploy feature in GigaVUE-FM. Bulk-deployed nodes are automatically added to GigaVUE-FM's list for management. Refer to the **Bulk Deploying GigaVUE-VM Nodes** section of the ***GigaVUE-FM and GigaVUE-VM User's Guide***.

The following procedure explains how to use the Bulk Deploy feature:

1. Navigate to the **Virtual > Management > Virtual Nodes** tab.
2. Select the OVA image file to be used for the Bulk Deploy. Browse and upload an image file from your local client computer to GigaVUE-FM or use an existing file that has already been uploaded to GigaVUE-FM.

   Note that the **Use Existing File** option does not appear until after an image file has been uploaded to GigaVUE-FM.

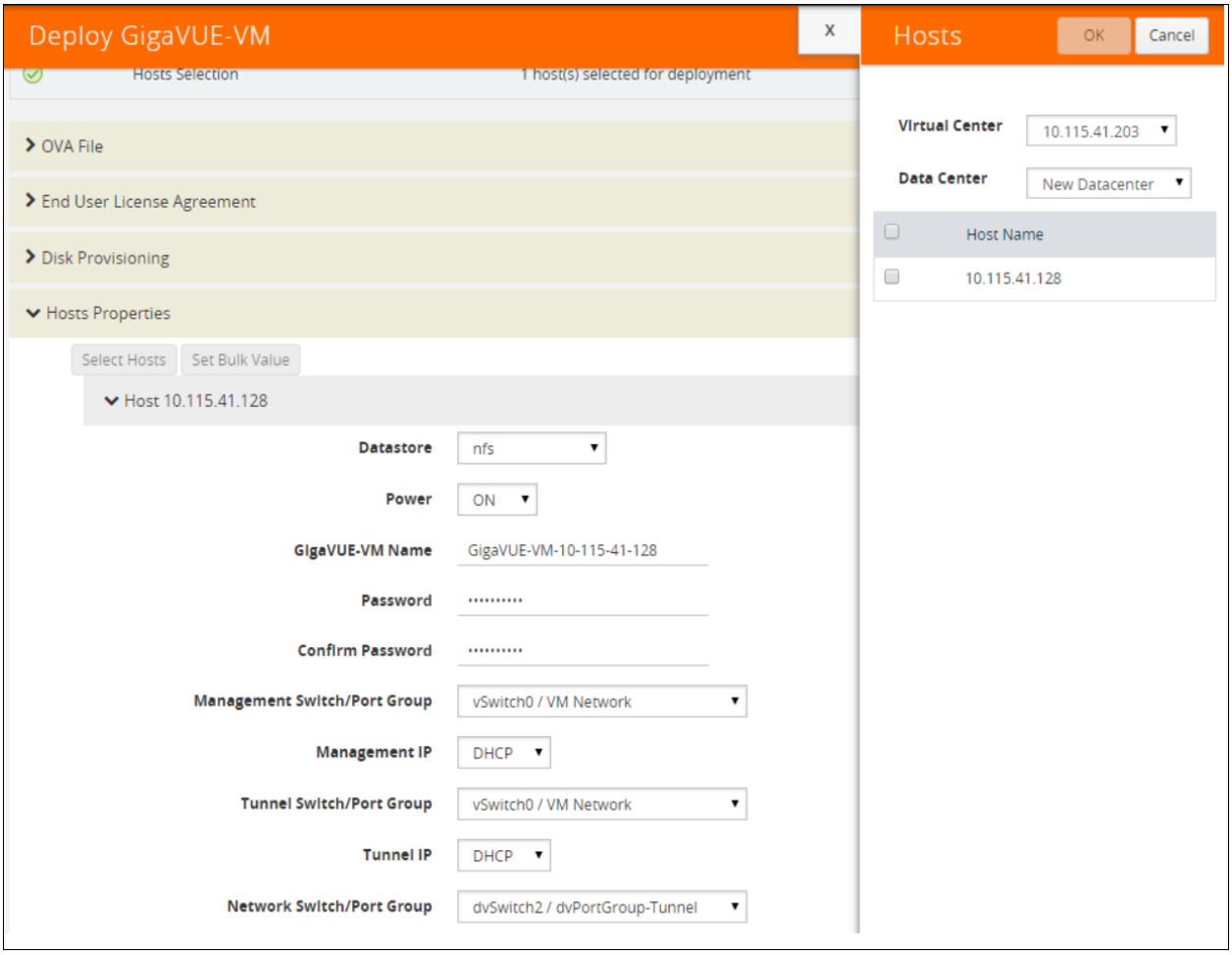


3. License Agreement - After careful review of the EULA, click Accept to continue.
4. Disk Provisioning – Select the provisioning policy to be used by the virtual disk for GigaVUE-VM nodes.
5. Next select the host where you want to deploy GigaVUE-VM nodes.
   - **Select Hosts** – The wizard automatically displays all available ESXi hosts associated with the selected datacenter (ESXi hosts with existing GigaVUE-VM nodes installed are not listed).
   - Check the box for each host where you would like to deploy a GigaVUE-VM node. You can quickly select all hosts by checking the box.
   - Select the Virtual Center and Datacenter with the ESXi hosts to be provisioned with GigaVUE-VM nodes. The drop-down lists all datacenters available on the Virtual Center

Server specified in the **Virtual > Management > Virtual Centers** tab.

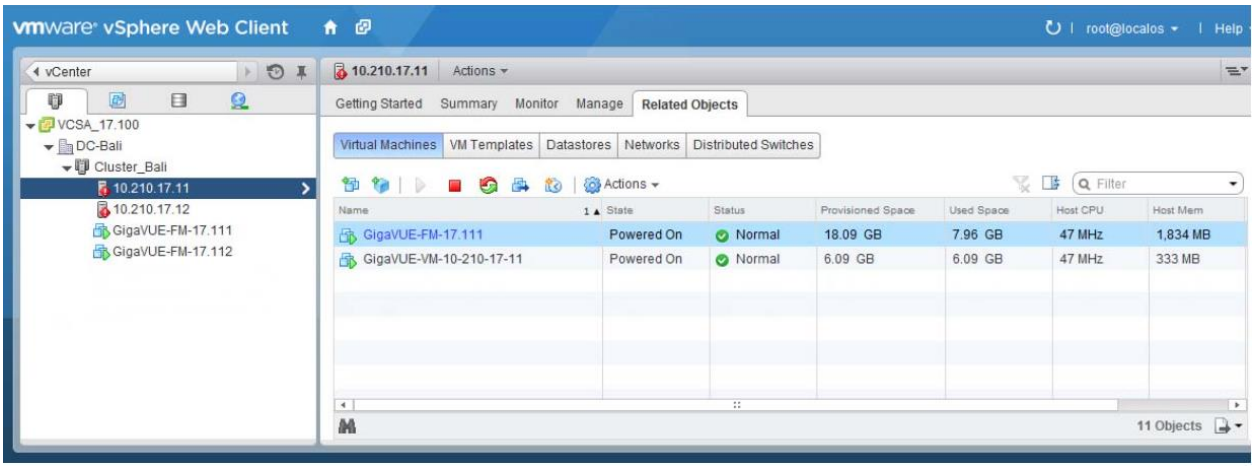
- Once you have selected the hosts where you want to deploy GigaVUE-VM nodes, click **OK** to continue.

6. Next configure settings for the GigaVUE-VM nodes to be deployed, supplying a name and password and selecting the Port Groups for management, tunnel, and network ports.



7. Click **Deploy** when you have finished configuring settings for GigaVUE-VM nodes.
8. Click **Finish** to launch the Bulk Deploy. You can monitor the progress of the Bulk Deploy in the **Administration > Alarms/Events** page. For example:

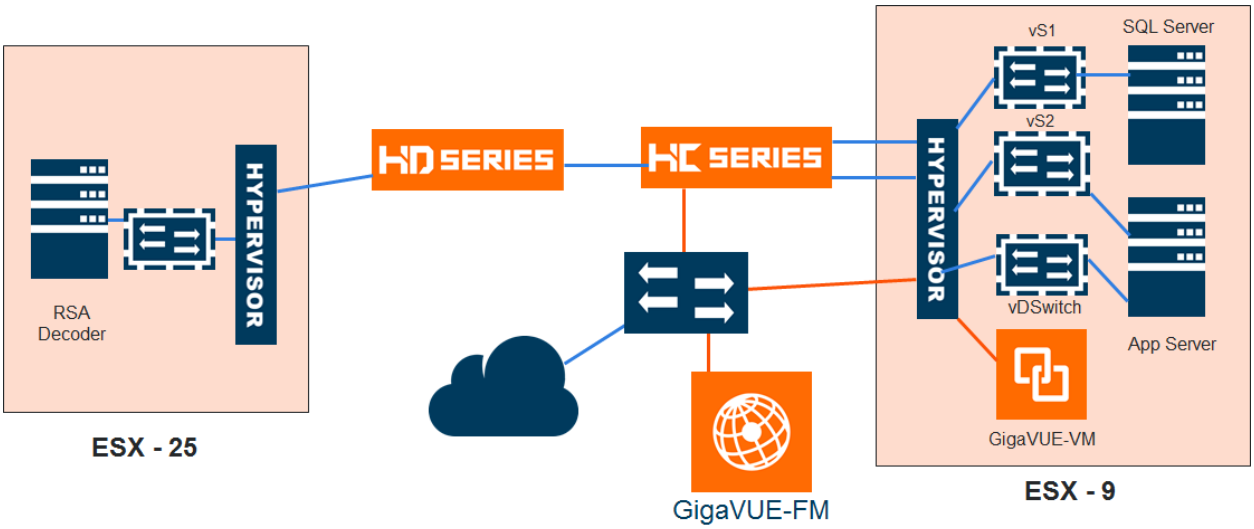
   Bulk Deploy takes place by deploying an initial OVF template to the first requested host. Once the initial OVF file is deployed, vSphere clones that template to all other requested hosts. Cloning takes place in waves of four GigaVUE-VM nodes at a time – if you request a Bulk Deploy of 21 GigaVUE-VM nodes, the OVF file is deployed to the first node in the list, followed by two successive waves of four cloned nodes.



Configuring the GigaSMART Tunnel

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 GigaVUE-VM delivers the same traffic identification, selection, and direction capabilities as exist on Gigamon's physical nodes. This enables RSA Security Analytics to establish visibility to virtual network traffic within the hypervisor or across multiple hypervisors. The GigaSECURE platform is able to detect vMotion events, and when a VM is moved from one hypervisor to another, the GigaSECURE Security

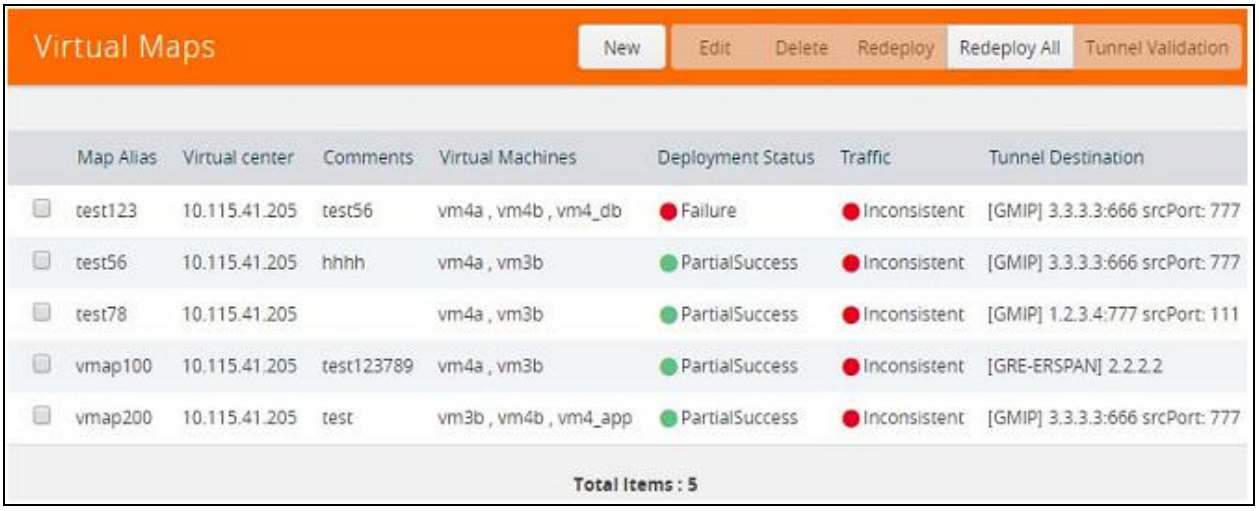
Delivery Platform will track the VM and dynamically configure the fabric to maintain continuous visibility.

This combination is an ideal solution for organizations interested in enabling their IT organization to investigate what was targeted, how the exploit occurred, how the attacker moved laterally, and the magnitude of the attack – across physical and virtual infrastructures.

Configuring the Virtual Traffic Map

To configure vMaps on the virtual nodes, select **Virtual > Virtual Maps**

> **Note: It is imperative that you create a tunnel (as described above) prior to creating the maps.**

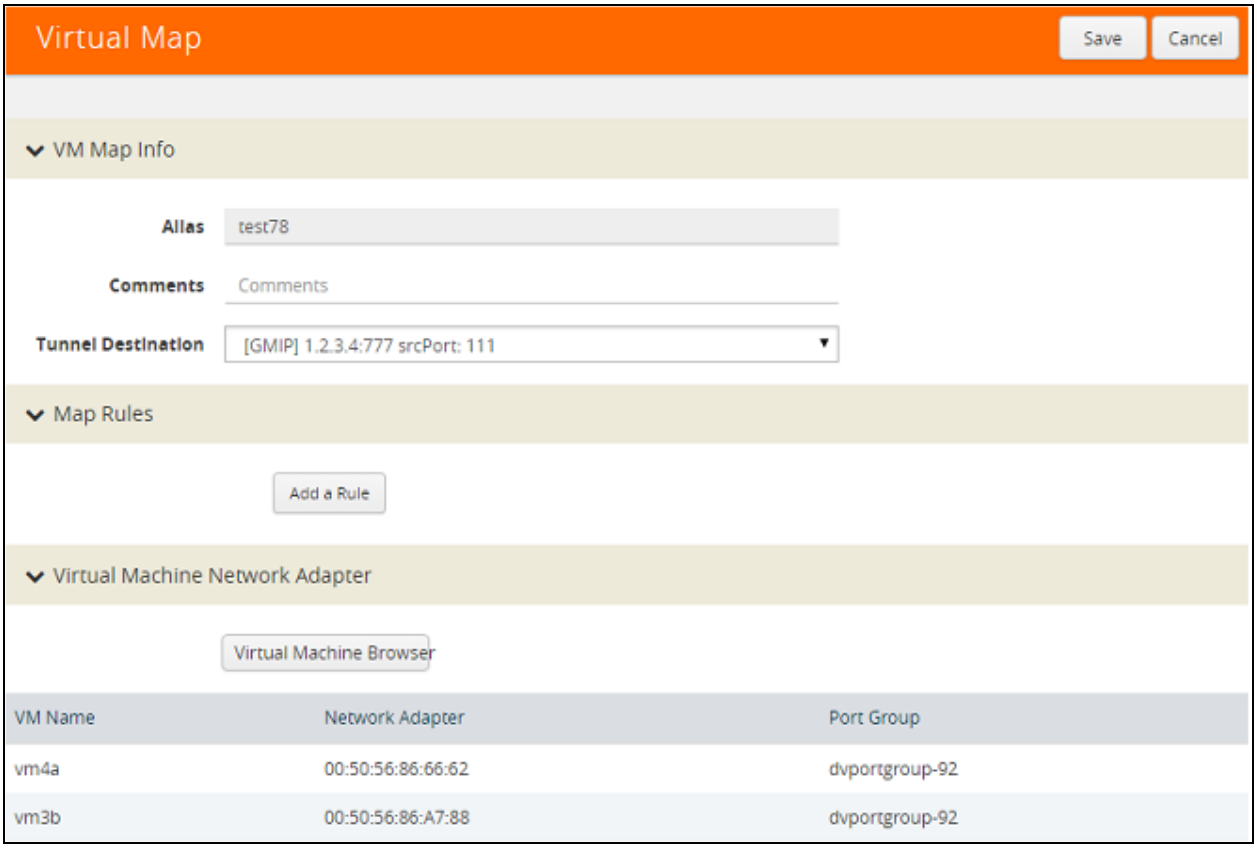


This page allows you to configure maps that define the traffic to be monitored between two virtual machines in the same port group. Before configuring maps, you first need to set up the connection between the Fabric Manager and the Virtual Center.

Configure virtual maps table has buttons that allow you to create virtual maps and manage the information that appears in the table: New, Edit, Delete, Redeploy, Redeploy All, and Tunnel Validation.

> **Note: Consult the Configuring the Virtual Traffic Map section of the *GigaVUE-FM and GigaVUE-VM User's Guide* for detailed information on these controls and their options.**

When you select a map in the table, quick view window is displayed. By clicking on **Edit** on the top of the quick view, you can review or update these parameters.

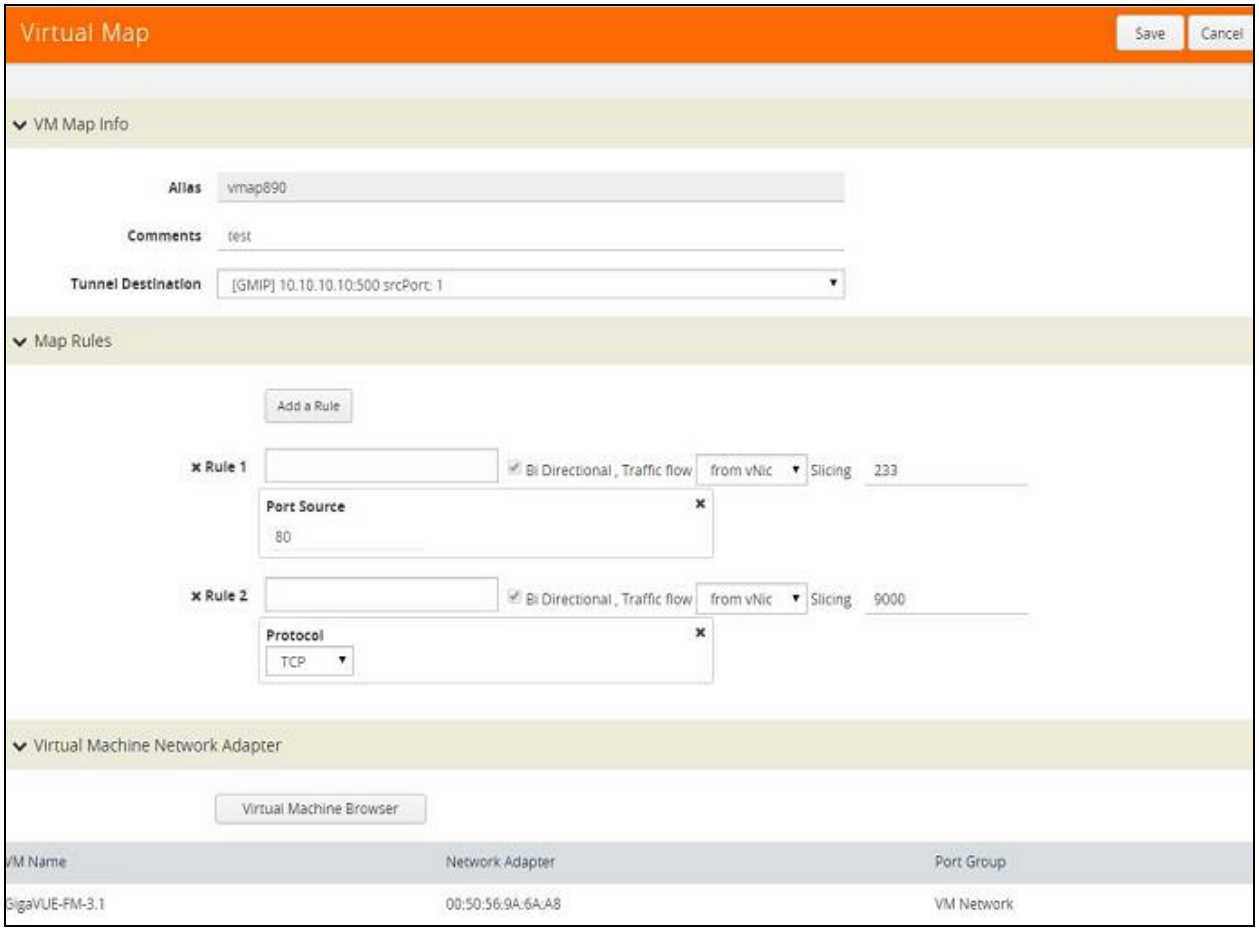


Create Map Dialog

To configure the vMap, select New to see the following window.

1. Enter values for each of the controls in the dialog.

Controls	Description
Alias	The name of your vMap.
Comments	An informational comment about this rule.

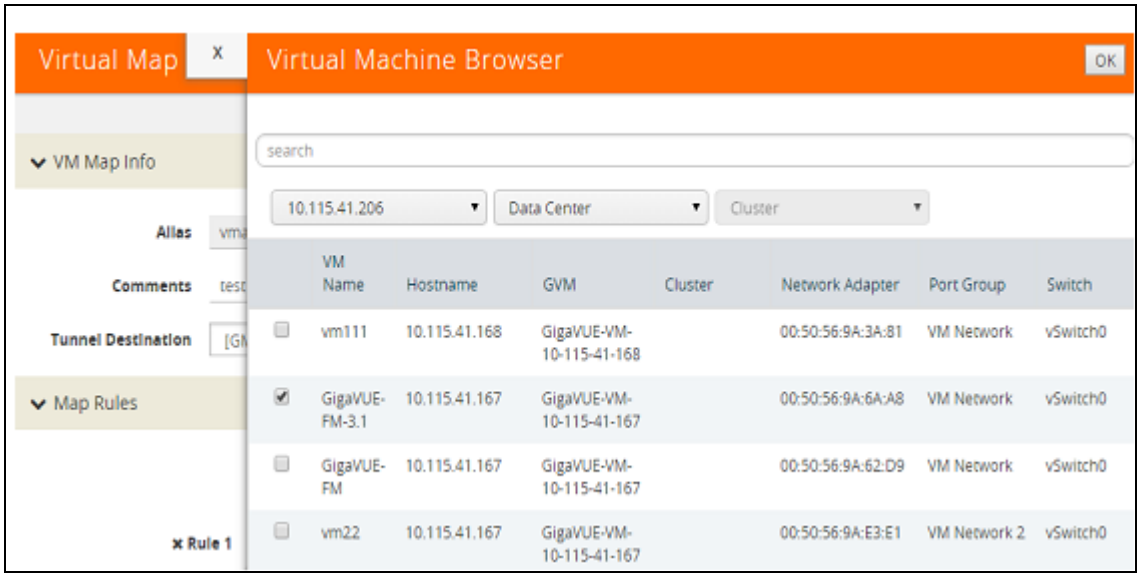


Controls	Description
Tunnel	This is the tunnel definition used for your tunnel.

2. Select a VM (Network Adapter) to associate with your vMap.

Field	Description
VM Name	Name of an VM instance.
Network Adapter	This is the virtual network adapter with the associated MAC address of the VM being monitored.
Port Group	The Port Group that is used by that vNIC to connect to the virtual switch

3. Select a VM (Network Adapter) to associate with your vMap. Select the button labeled, **Virtual Machine Browser**. This will pull the quick view window to set the VM Network Adapter. Select the virtual center by selecting the bubble to the left of the VM name.



vMap Rules

Keep in mind the following rules when working with vMaps:

- A single vMap supports a combined maximum of ten application ports.
- Slicing can only be used together with other vMap port filter criteria. It cannot be used as the only criteria in a vMap.

Creating a vMap using a vNIC on vSS

When creating a vMap using a vNIC on vSS to monitor traffic, there are no additional actions to perform. The following occurs:

- GigaVUE-VM automatically creates a port group called, **GigaPG_<vswitch name>** in order to monitor traffic.
- The port group is configured as **Promiscuous mod**e with VLAN 4095.
- The port group is automatically deleted when deleting the vMap.

Certification Checklist for RSA Security Analytics

Date Tested: October 4th, 2015

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
Fabric Manager (FM)	3.1.00	GigaVUE-FM
Virtual Agent	3.1.00	GigaVUE-FM
GigaVUE-HC2	4.4.01	GigaVUE-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	✓

JEC / PAR

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