Gigamon
GigaVUE H Series

RSA Security Analytics Ready Implementation Guide

Last Modified: June 17th, 2014

Partner Information

Product Information	
Partner Name	Gigamon
Web Site	www.gigamon.com
Product Name	GigaVUE H Series
Version & Platform	4.0
Product Description	Gigamon GigaVUE® offers modular-based intelligent traffic visibility fabric nodes. This extends traffic visibility to more remote portions of the network running critical applications that require monitoring.

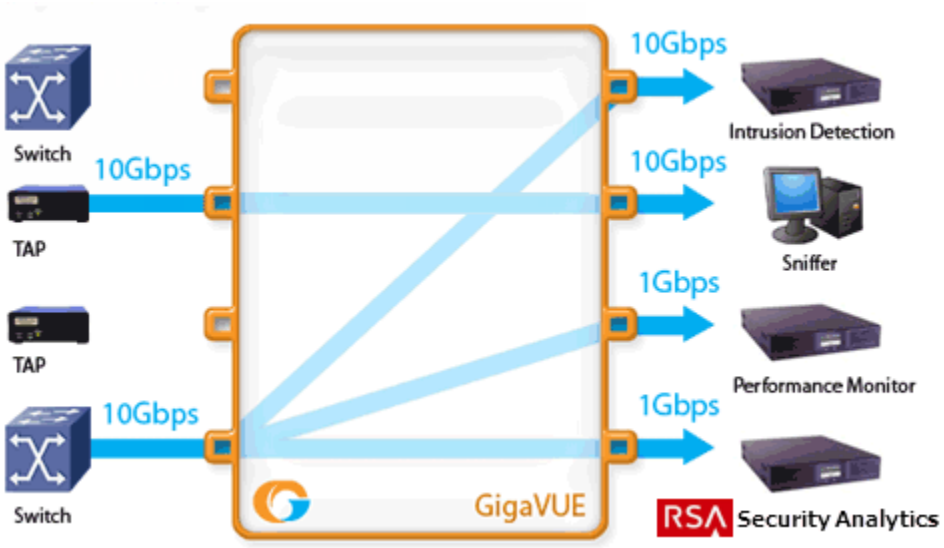
Solution Summary

The GigaVUE H Series delivers performance and intelligence as a Traffic Visibility Fabric™ node, with port density and speeds that scale to your needs from 1Gb to 100Gb. With an intuitive web-based interface (H-VUE) and a powerful CLI, the Visibility Fabric is able to replicate, filter, and selectively forward network traffic to monitoring, management, and security tools such as RSA Security Analytics.

Optional GigaSMART® functions including Adaptive Packet Filtering, NetFlow Generation, Tunneling, Packet Slicing and Masking, Source Port Labeling, Header Stripping, Flow Mapping™, GTP Correlation and De-duplication, create a robust distributed monitoring solution.

By combining Gigamon® with RSA Security Analytics, you empower network forensic and packet capture devices by providing customized data streams aggregated from multiple points on the production network. Advantages of such a solution include preventing data loss, collecting more relevant data per packet capture device, de-duplication for tool optimization and masking to address compliance concerns.

RSA Security Analytics Tested Features	
Gigamon GigaVUE H Series	
Flow / Traffic Mapping	Yes
De-duplication	Yes



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Gigamon GigaVUE® 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.

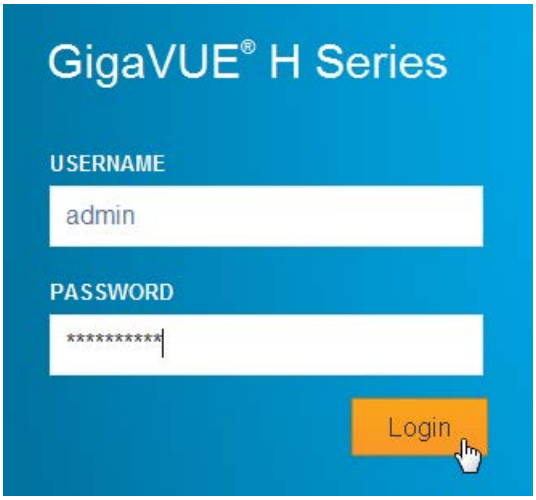
! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure the Gigamon GigaVUE is properly configured and secured before deploying to a production environment.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

Gigamon GigaVUE Configuration

Launching the GigaVUE Web Management Interface

H-VUE provides you with an intuitive, drag-and-drop interface for your H Series Visibility Fabric nodes. Although the familiar command-line interface will always be available for all configuration tasks, H-VUE simplifies many common tasks, allowing you to configure packet distribution visually instead of entering text in the CLI. All the administration tasks of this guide will be performed through the H-VUE web interface.

1. Browse to the login page of the GigaVUE H Series device (e.g. **https://192.168.1.1*)***
2. Login with the administrator's username and password that was created during the initial setup of the device.
3. Click **Login**.

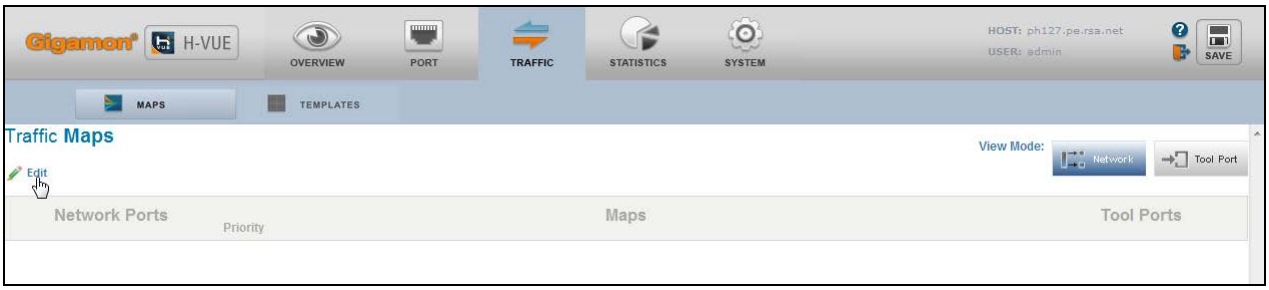


Configuring Flow / Traffic Mapping

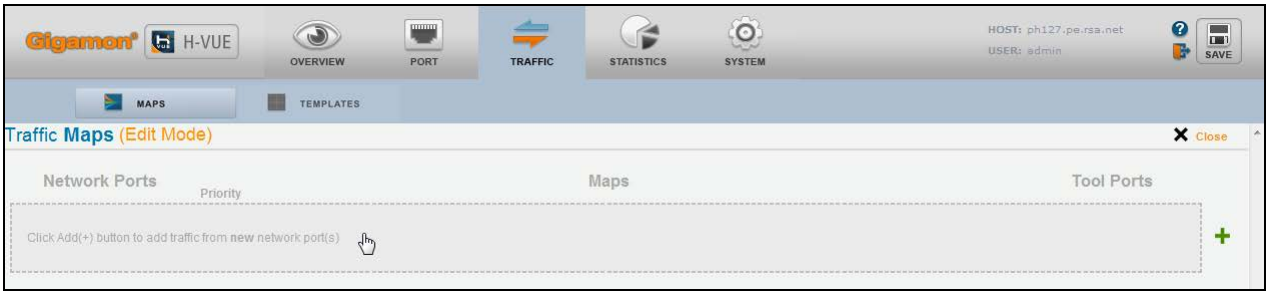
Flow Mapping is the power at the heart of the Gigamon Visibility Fabric where you decide how traffic arriving on network port GigaVUE packet distribution starts with network ports and ends with tool ports. Network ports are where you connect data sources to the GigaVUE systems should be sent to tool port GigaVUE packet distribution starts with network ports and ends with tool ports. Tool ports are where you connect destinations for the data arriving on network ports. You decide which traffic should be forwarded, where it should be sent, and how it should be handled once it arrives.

1. From the web management interface, click the **TRAFFIC** icon from the top menu.

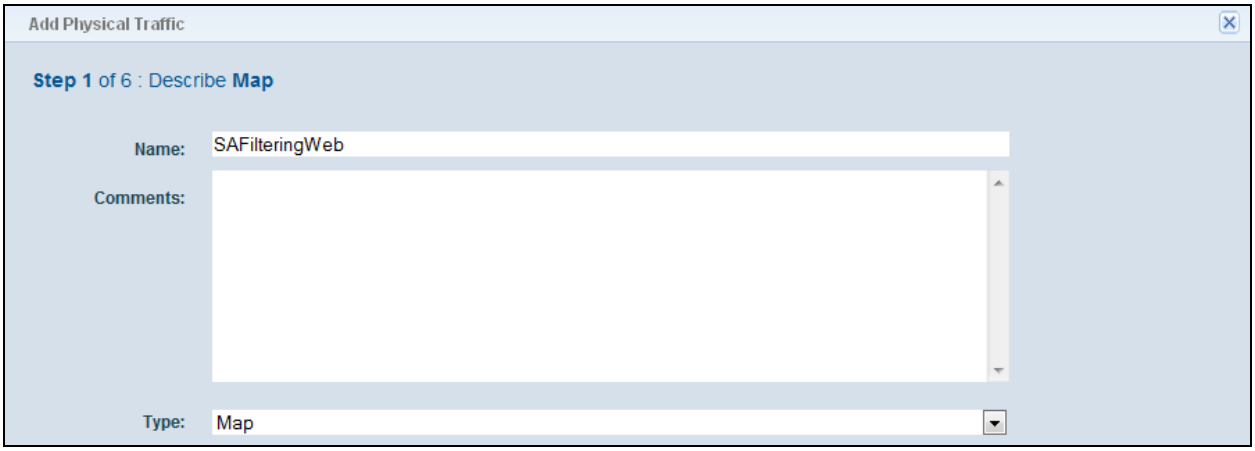
> **Note: When you first open the Traffic > Flow Mapping page, it is in view only mode, summarizing existing maps. To create a new map, edit an existing map, or adjust map priority, you must enter Edit mode, as shown below.**



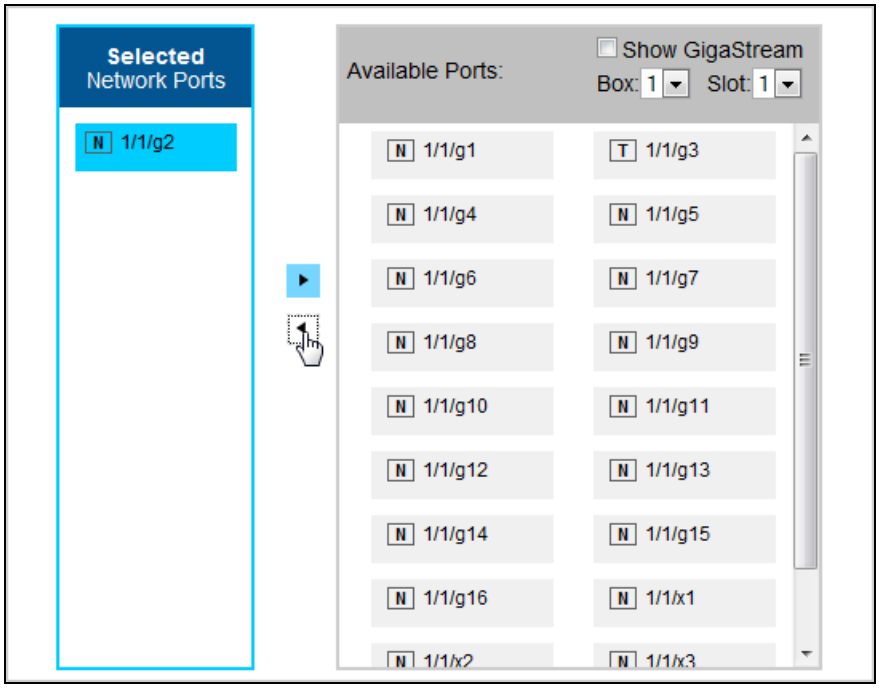
2. Click the **Edit** button.
3. Next click the open box or Add(**+**) button to add traffic from the new network port.



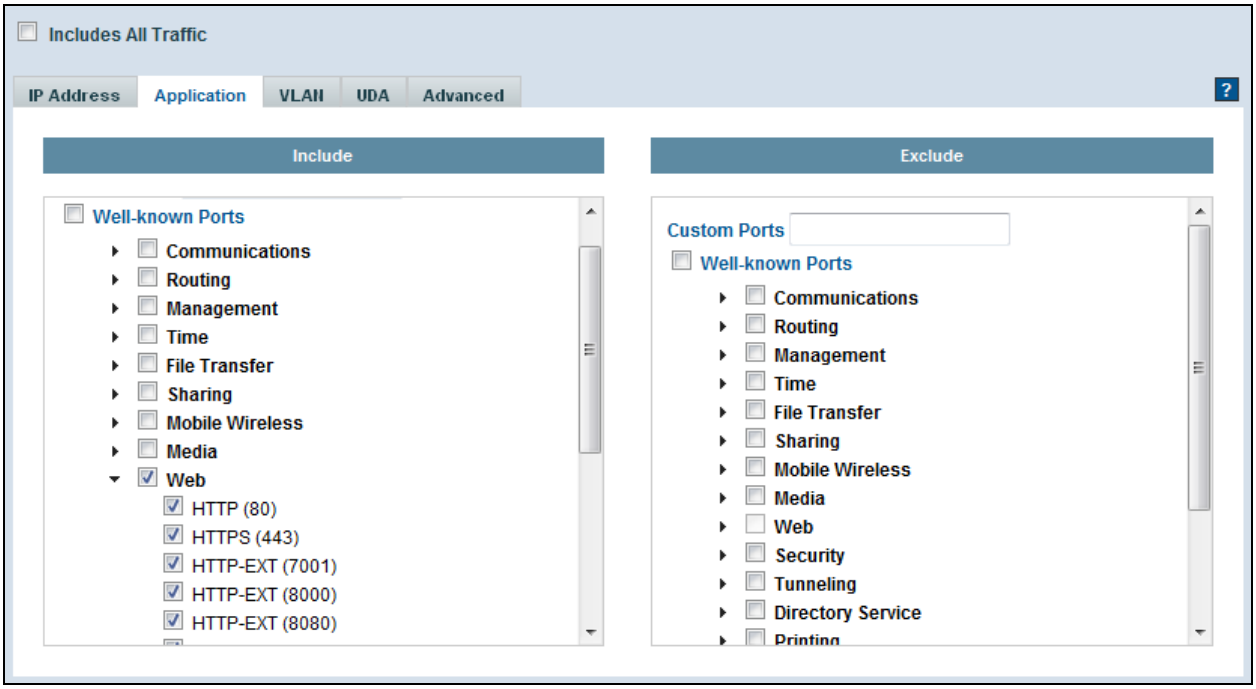
4. Add a name of name for the new Map, click **Next**.



5. Select the available network port and click the left arrow, click **Next**.

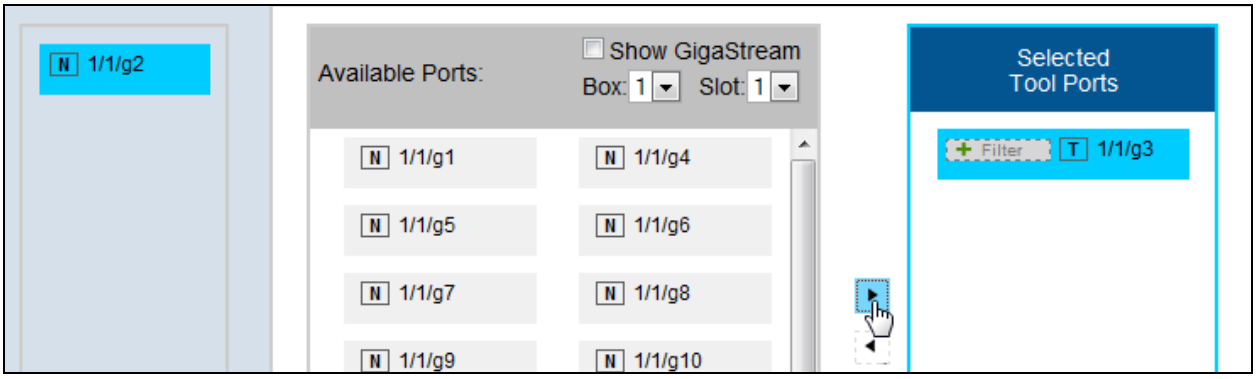


6. Depending on the flow of traffic you are creating, you may want to use the **IP Address**, **Application**, **VLAN**, **UDA** or **Advanced** tab. In this example, we'll use **Application** tab and filter on **Web** ports.

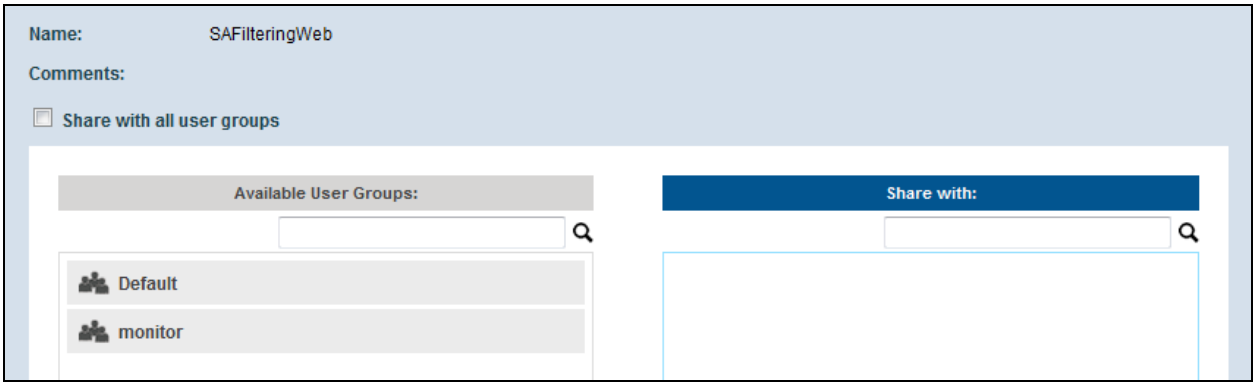


7. Next, select any GigaSMART operations you would like to add. For this example, will not select any of the GigaSMART Operations. Click **Next**.

8. Select the appropriate tool port for your environment, click **Next**.



9. If you wish to share this map with other users in the group, check the **Share with all user groups** and then make the appropriate changes. Click **Next** when finished.



10. Click **Finish** to save the Map.

Note: For further information configuring the GigaVUE device, please refer to the H-VUE User Guide or Online Help.

Configuring De-duplication

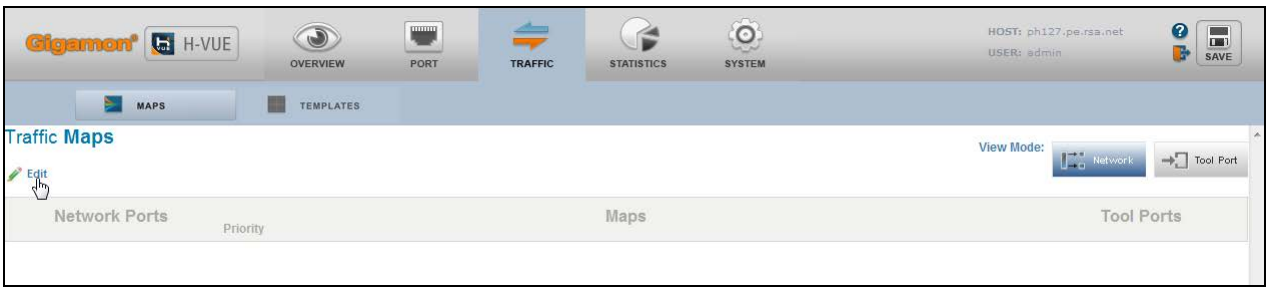
GigaSMART Operation Groups with a de-duplication component can tally or remove any duplicate IPv4 and IPv6 packets detected within a configurable interval of the original packet (10-50,000 microseconds).

Duplicate packets are common in network analysis environments where both the ingress and egress data paths are sent to a single output (for example, as a result of a SPAN operation on a switch). They can also occur in asynchronously routed environments. The de-duplication component lets you eliminate these packets, reducing unnecessary processing load on your tools.

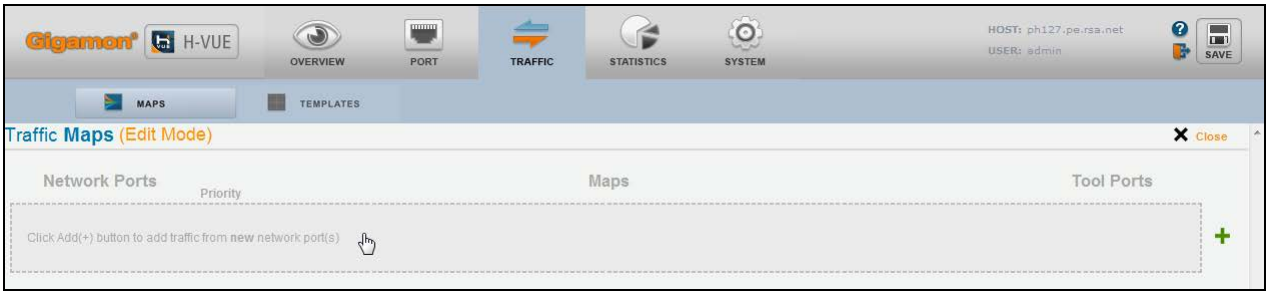
The de-duplication feature examines IPv4 and IPv6 packets for duplicates. A packet is considered to be a duplicate if its bits are identical to the original packet from Layer 3 (Network layer) onwards, including the payload. Keep in mind the following when configuring GigaSMART Operation Groups with a de-duplication component.

1. From the web management interface, click the **TRAFFIC** icon from the top menu.

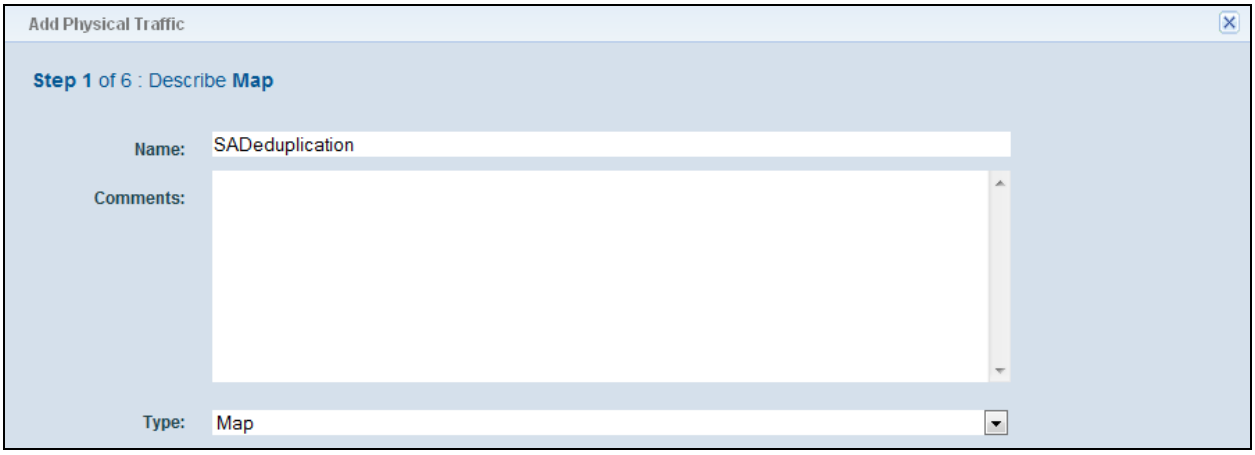
> **Note: When you first open the Traffic > Flow Mapping page, it is in view only mode, summarizing existing maps. To create a new map, edit an existing map, or adjust map priority, you must enter Edit mode, as shown below.**



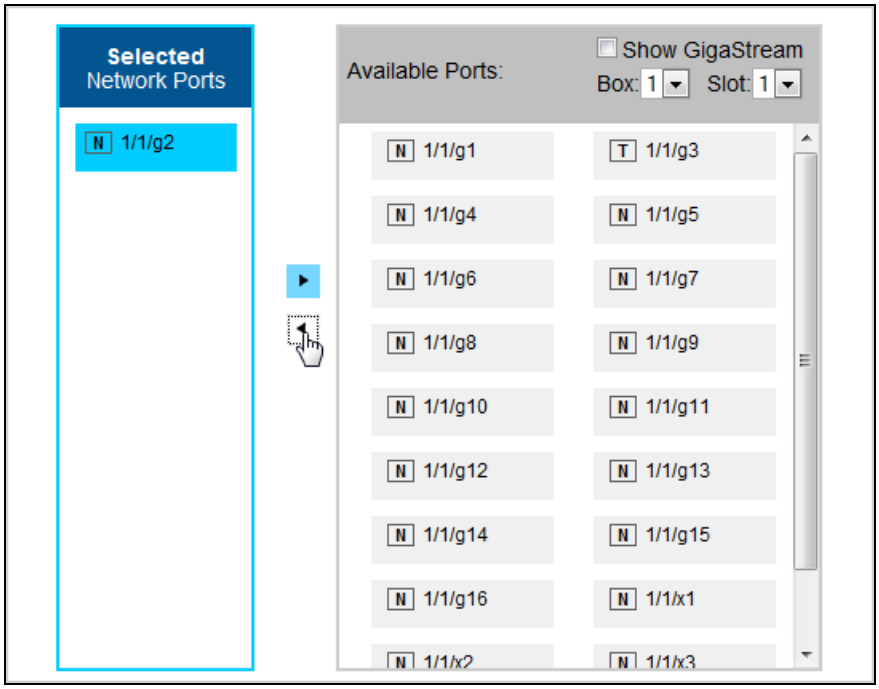
2. Click the **Edit** button.
3. Next click the open box or Add(**+**) button to add traffic from the new network port.



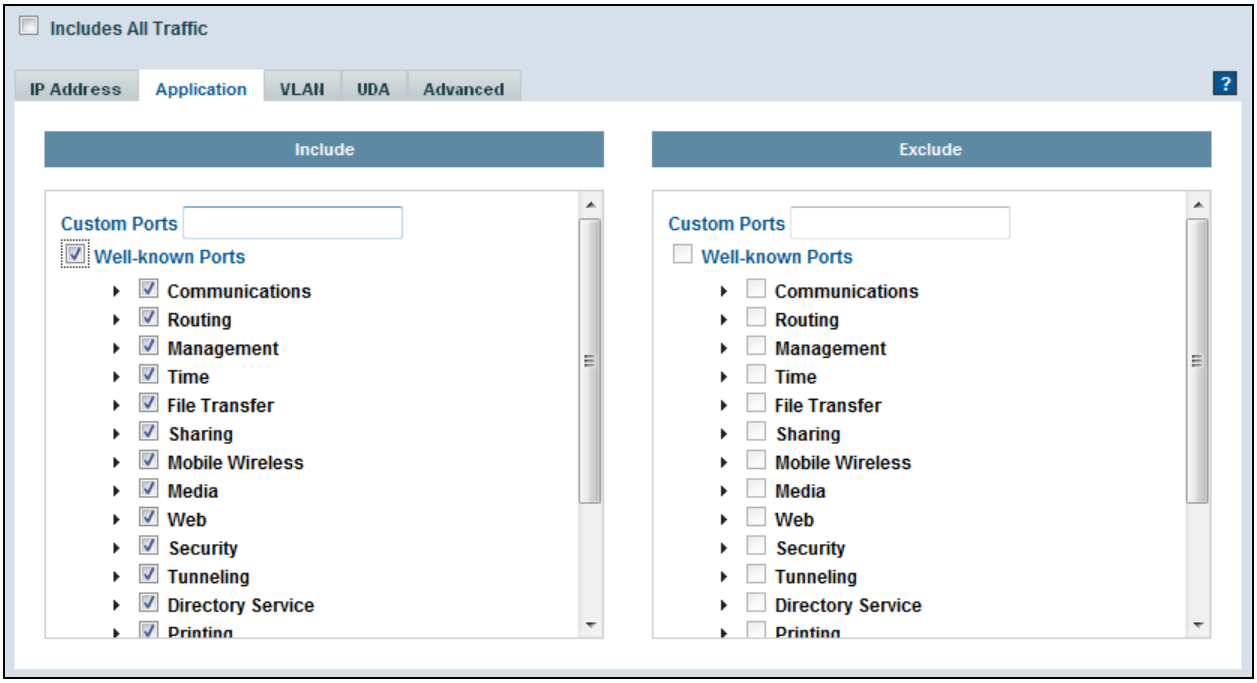
4. Add a name of name for the new Map, click **Next**.



5. Select the available network port and click the left arrow, click **Next**.

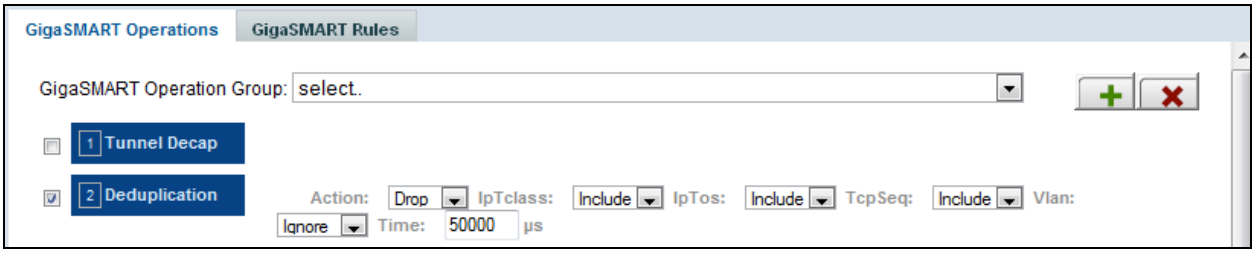


6. Depending on the rule you are creating, use the **IP Address**, **Application**, **VLAN**, **UDA** or **Advanced** tab. In this example, we'll use the **Well-known Ports** checkbox.

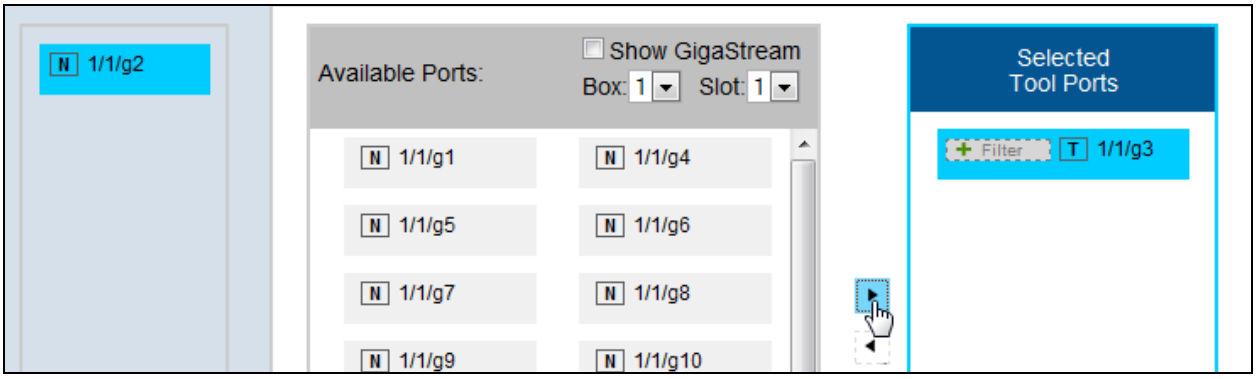


7. Next, select the **Deduplication** box. For this operation, you must also select a *GigaSMART Operation Group* or *GigaSMART Engine Group*, click **Next**.

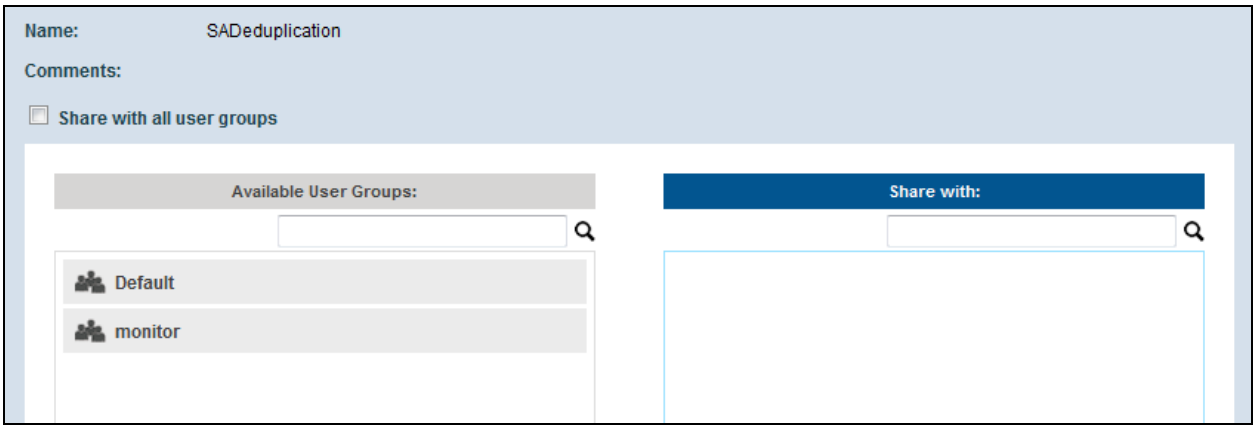
Note: Select which fields to include or exclude when determining whether or not a packet is considered a duplicate. The TCP sequence number and/or VLAN tag are common fields to consider. Also, set the time window; lower windows result in better performance, but duplicates that fall outside the window will not be considered duplicates.



8. Next, select the appropriate tool port for your environment, click **Next**.



9. If you wish to share this map with other users in the group, check the **Share with all user groups** and then make the appropriate changes. Click **Next** when finished.



10. Click **Finish** to save the Map.

Note: For further information configuring the GigaVUE device, please refer to the H-VUE User Guide or Online Help.

Certification Checklist for RSA Security Analytics

Date Tested: June 17th, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.3.3	Virtual Appliance
Gigamon GigaVUE-HB1	4.0	Appliance

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	✓

JJO

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