Interface Masters
4272

RSA Ready Implementation Guide
for RSA Security Analytics

Last Modified: October 2th 2015

Partner Information

Product Information	
Partner Name	Interface Masters
Web Site	www. Interface Masters.com
Product Name	4272
Version & Platform	25f58c0-6
Product Description	Bypass and TAP switch

Solution Summary

The Interface Masters 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 and a powerful CLI, the Visibility Fabric is able to replicate, selectively forward network traffic to monitoring, management, and security tools such as RSA Security Analytics.

By combining Interface Masters 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

Note: The 4272 only supports 1 gig or higher speed.

RSA Security Analytics Tested Features	
Interface Masters 4272	
Flow / Traffic Mapping	Yes
Failover (bypass fail open or fail close)	Yes
Health check via hart beat packet	Yes
Dual power supplies	Yes
AC and DC support	Yes
Ability to be in TAP (passively look at the traffic)	Yes
High availability (support active passive)	Yes
Management capabilities: GUI, CLI, TACACS, SSH, SNMP, Syslog, e-mail notification, NTP	Yes
Filtering	Yes
De-duplication	No[2]

[2] De-duplication can be performed by using the a5002

Interface Masters

TECHNOLOGIES

Innovative Network Solutions

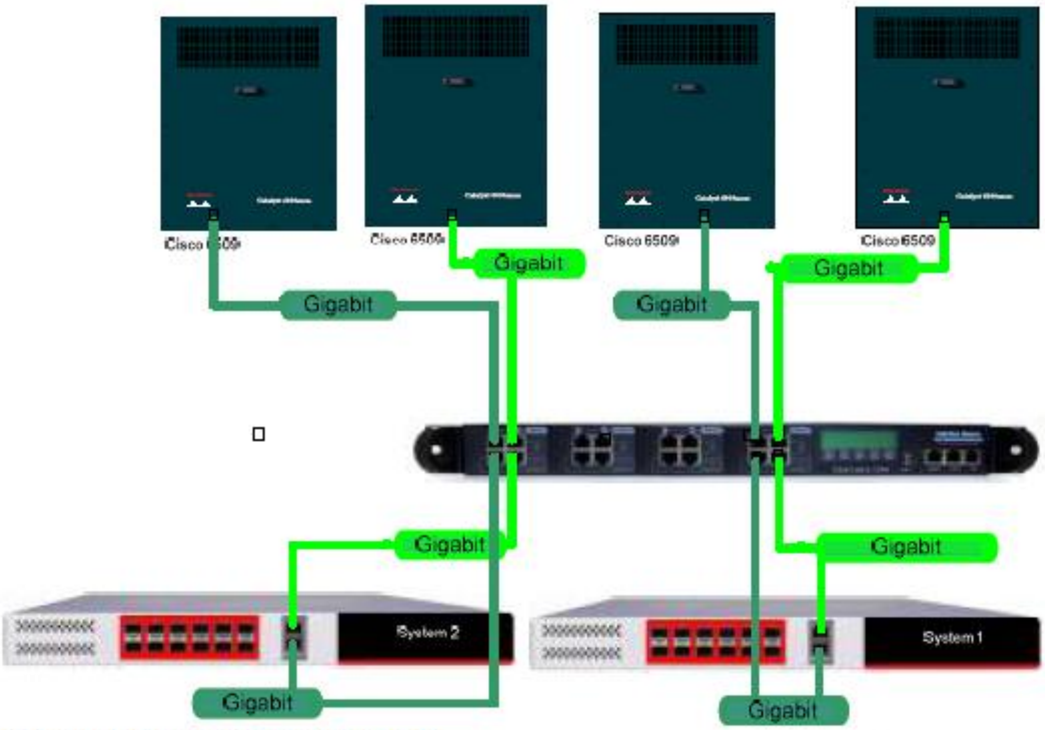


Figure 1 Connectivity example,

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the 4272 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.

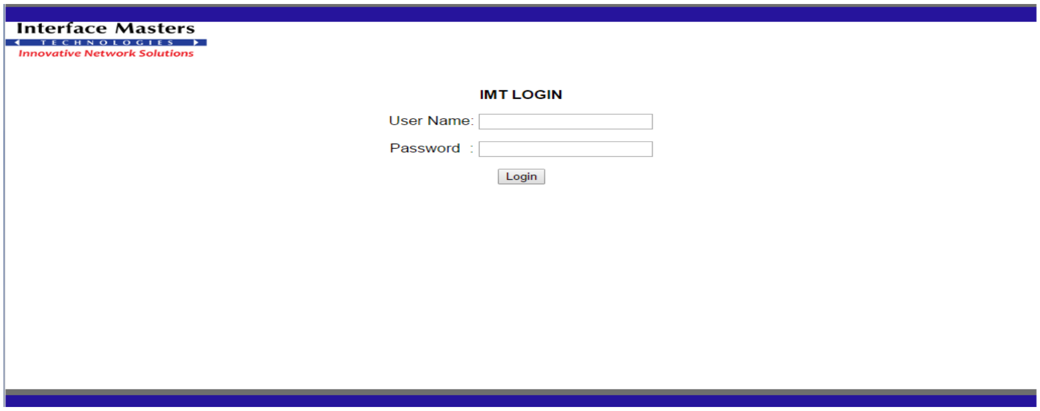
All Interface Master components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! 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 Product is properly configured and secured before deploying to a production environment. For more information, please refer to the Product documentation or website.

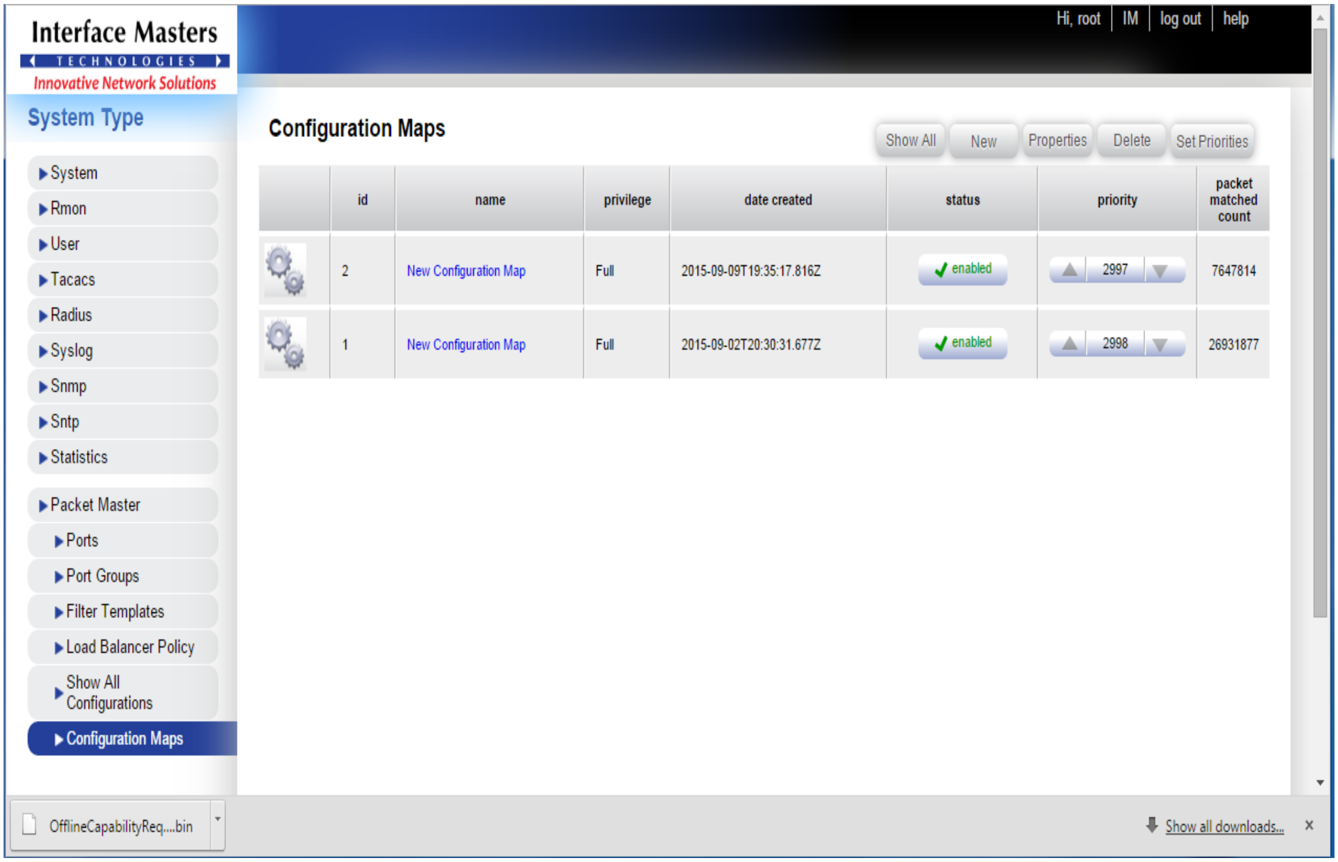
4272 Configuration

The 4272 possesses active bypass functionality for seamless failover, TAP functionality for traffic monitoring, and extensive management capabilities. It is available with independent segments with various media combinations including copper, single-mode fiber, multi-mode fiber, multi-mode fiber to single-mode fiber conversion and copper to fiber conversion options. The intelligent bypass also enables plug-and-play connectivity, includes an auto heartbeat and requires no additional drivers to be installed on connected appliances. Below is a sample use case setup for the 4272.

1. Log into the 4272 GUI user root, Password admin123



2. Click on a Configure Maps on the left and New Configuration Map to the right

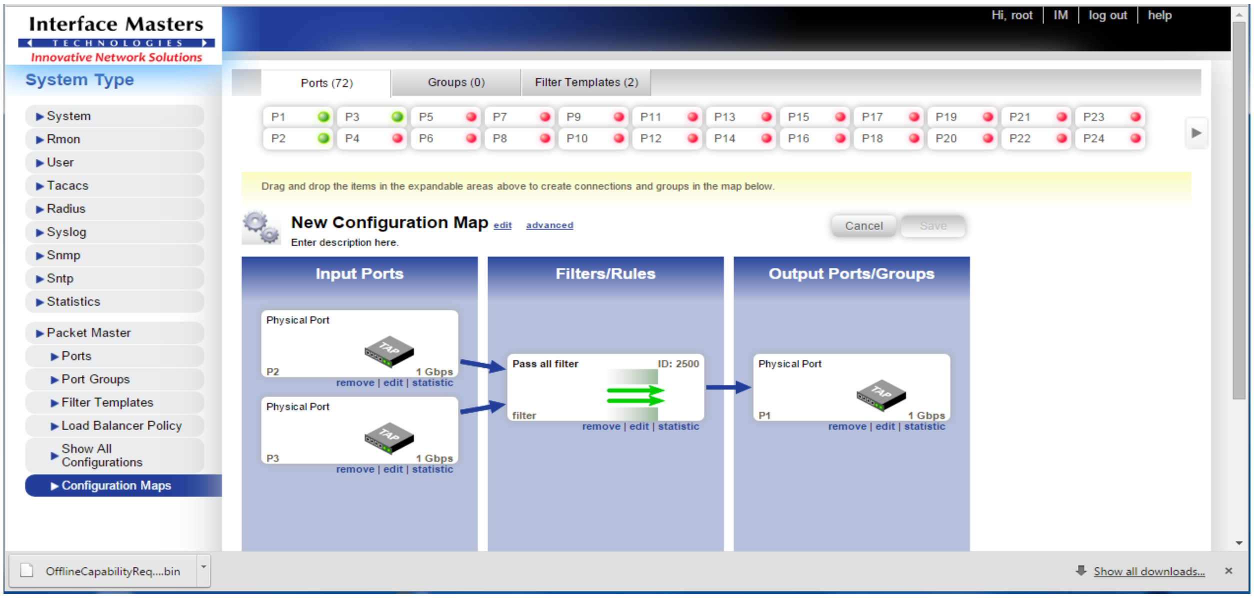


Configuration Maps

	id	name	privilege	date created	status	priority	packet matched count
	2	New Configuration Map	Full	2015-09-09T19:35:17.816Z	✓ enabled	2997	7647814
	1	New Configuration Map	Full	2015-09-02T20:30:31.677Z	✓ enabled	2998	26931877

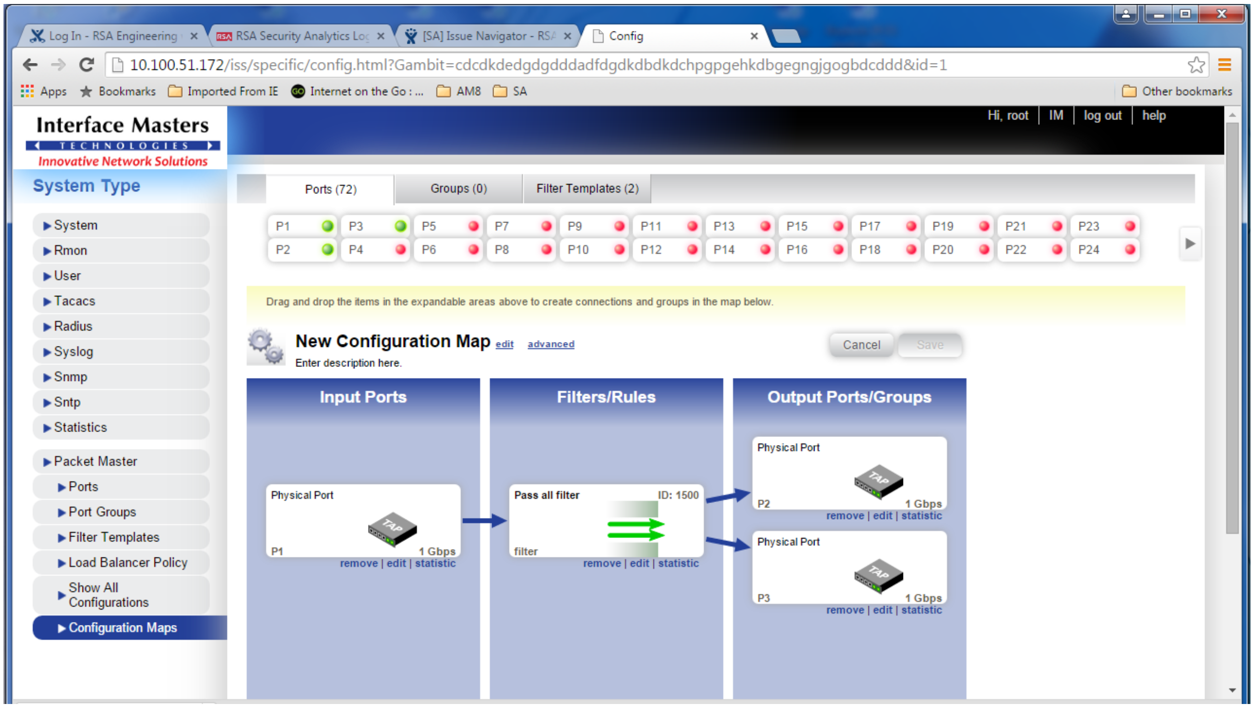
3. Click and drag the ports you want to configure for input, with filter and destination.

Note: This is one directional so a second configuration needs to made for the other direction.



Drag and drop the items in the expandable areas above to create connections and groups in the map below.

Enter description here.

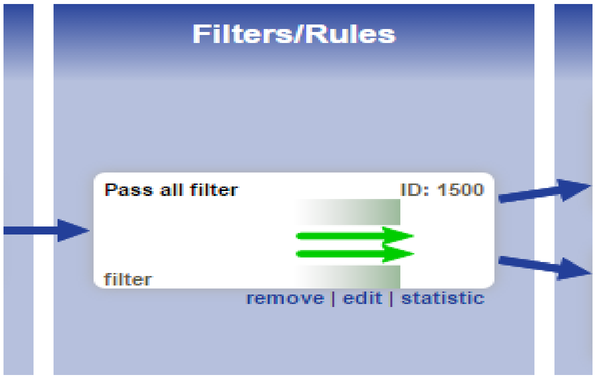


Drag and drop the items in the expandable areas above to create connections and groups in the map below.

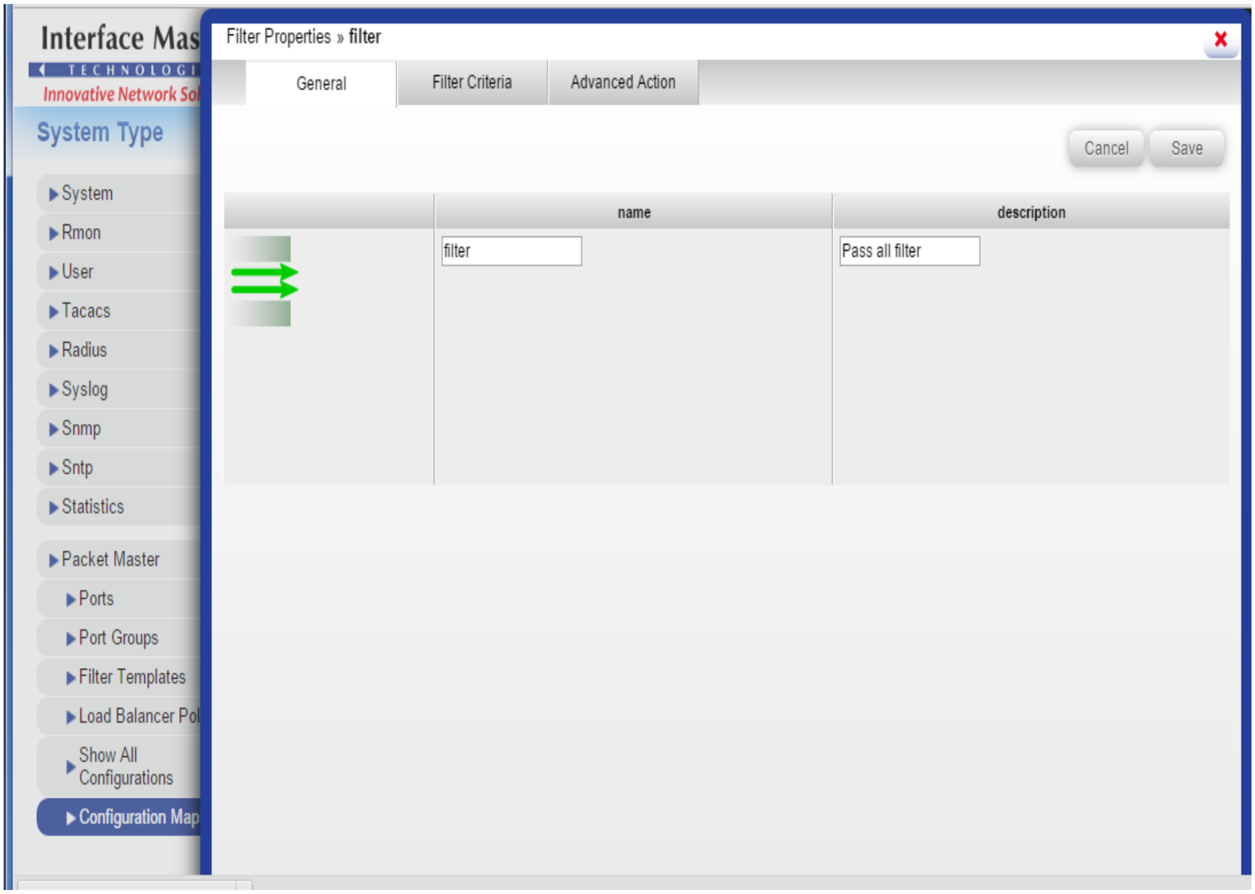
Enter description here.

Filter setup

4. Click on edit to set filter names and settings

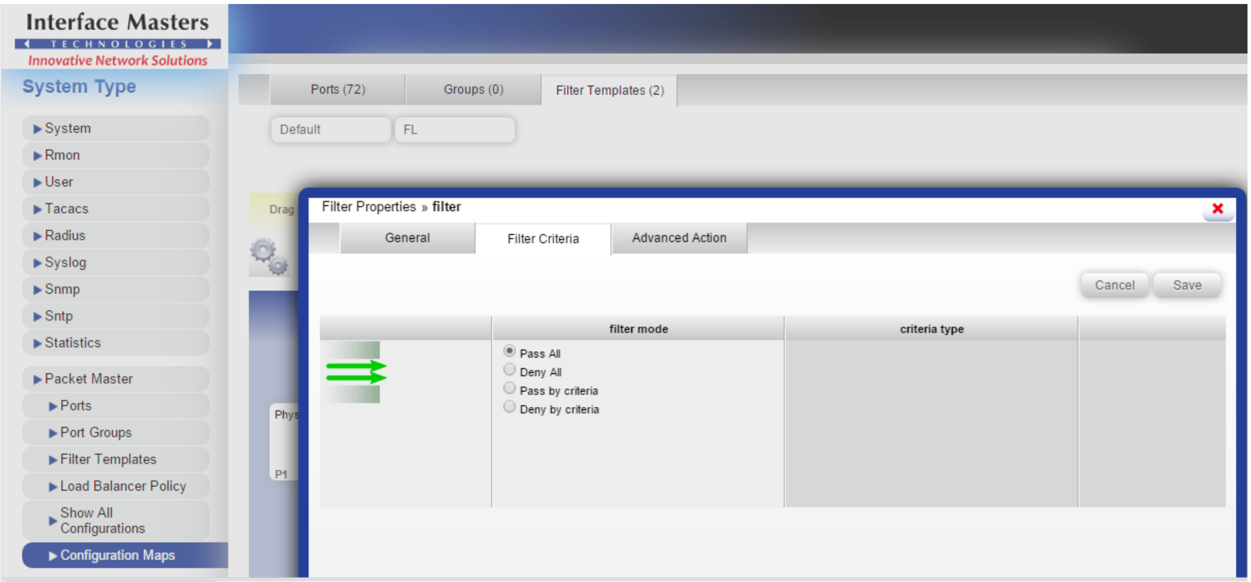


5. Go to general tab and choose a filter name



name	description
filter	Pass all filter

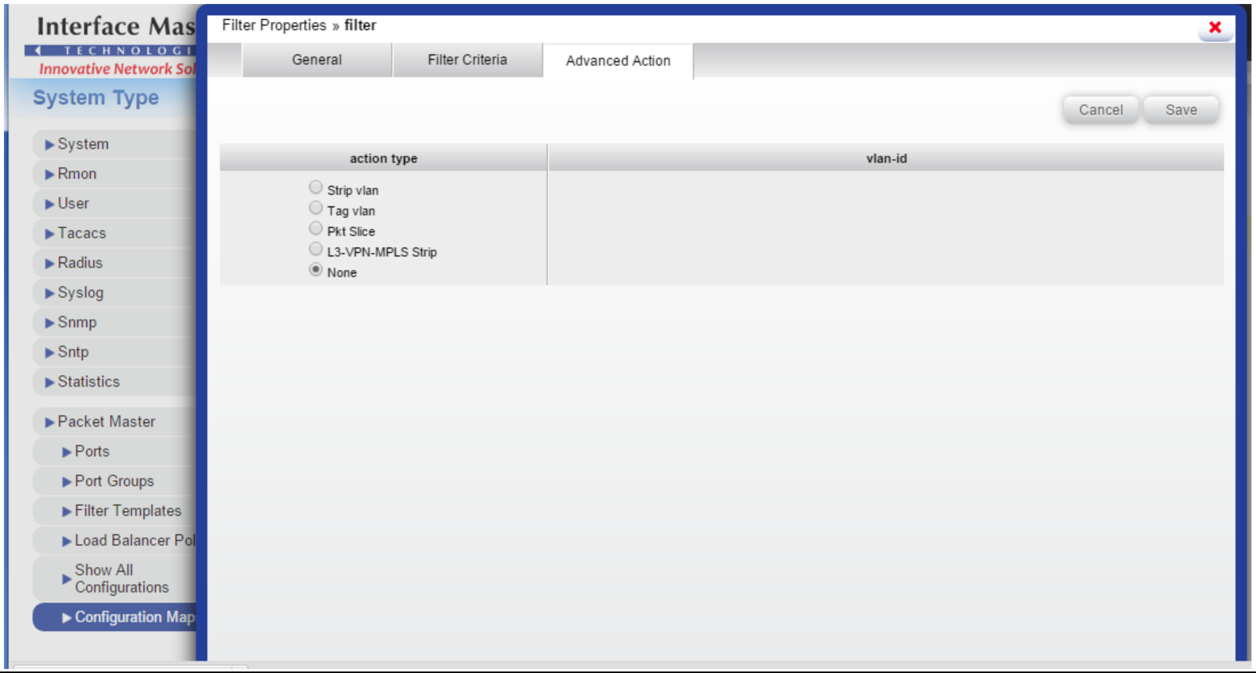
6. Click on filter tab and pick the desired functions



Filter Properties » filter

filter mode	criteria type
● Pass All ○ Deny All ○ Pass by criteria ○ Deny by criteria	

7. Click on Advanced Actions tab and pick the desired functions



Filter Properties » filter

action type	vlan-id
○ Strip vlan ○ Tag vlan ○ Pkt Slice ○ L3-VPN-MPLS Strip ● None	

Certification Checklist for RSA Security Analytics

Date Tested: October 2th 2015

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
4272	25f58c0-6	Linux

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	N/A
Traffic Mapping	
Mapping network service ports to dedicated ports	✓
Performance	
SA Log Decoder minimal EPS performance	✓
SA Packet Decoder minimal EPS performance	✓

INIT / FAL

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