RSA Ready Implementation Guide for RSA Security Analytics

Ixia Vision ONE Network Packet Broker v4.7.4

FAL, RSA Partner Engineering

Last Modified: 4/30/2018

RSA READY

Solution Summary

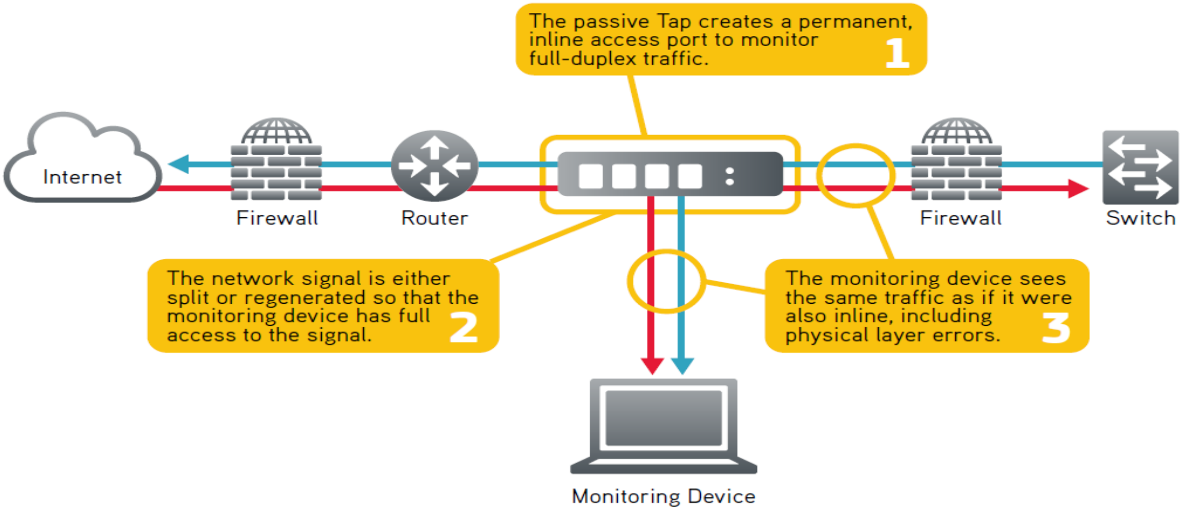
The Ixia Vision ONE delivers performance and intelligence as a Network Packet Broker (NPB), with port density and speeds that scale to your needs from 1Gb to 100Gb. With an intuitive web-based interface, and a powerful API, the NPB Visibility Fabric is able to replicate, filter, and selectively forward network traffic to monitoring, management, and security tools such as RSA Security Analytics.

RSA Security Analytics Tested Features	
Vision ONE NPB v4.7.4	
Flow / Traffic Mapping	yes
De-duplication	yes

HOW IT WORKS

Network Tap Deployment

Network Taps use passive splitting or regeneration technology to transmit inline traffic to an attached management or security device without datastream interference.



The passive Tap creates a permanent, inline access port to monitor full-duplex traffic. 1

The network signal is either split or regenerated so that the monitoring device has full access to the signal. 2

The monitoring device sees the same traffic as if it were also inline, including physical layer errors. 3

RSA Security Analytics

Before You Begin

This section provides instructions for configuring the Ixia Vision ONE NPB 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 Ixia 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 Ixia Vision ONE is properly configured and secured before deploying to a production environment. For more information, please refer to the Ixia Vision ONE documentation or website.

Ixia Vision ONE Configuration

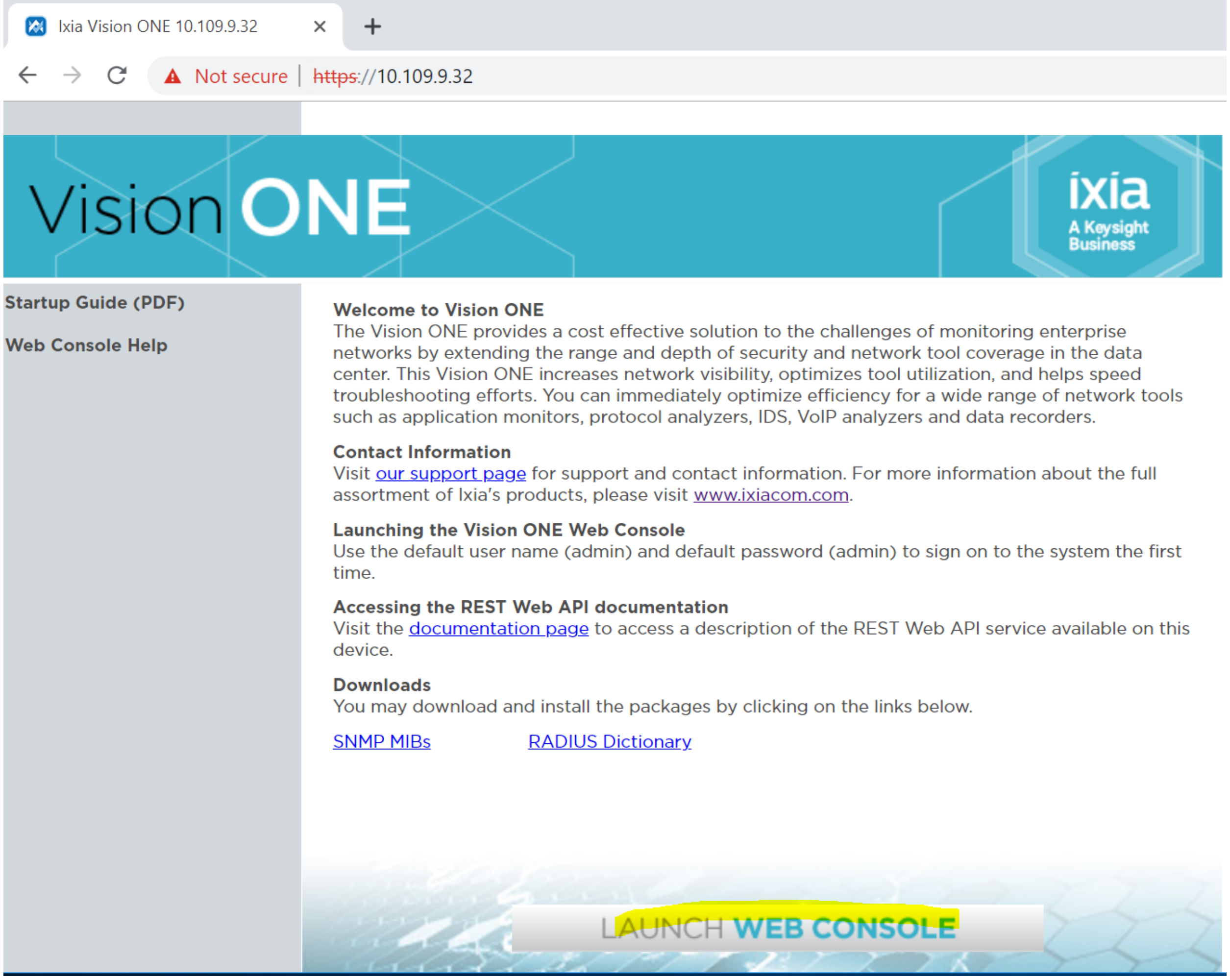
Launching the Ixia Vision ONE Web Management Interface

Ixia Vision ONE provides you with an intuitive, drag-and-drop interface for your nodes. Although a familiar command-line interface could be used for similar configuration tasks, Vision ONE 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 Vision ONE web interface.

Configuring Flow / Traffic Mapping

Flow Mapping is the power at the heart of the Ixia Vision ONE where you decide how traffic arriving on network port is handled. Ixia Vision ONE packet distribution starts with network ports and ends with tool ports. Network ports are where you connect data sources to the Ixia Vision ONE systems. 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. Point to the Vision ONE and launch the Web Console l and log in



Welcome to Vision ONE
The Vision ONE provides a cost effective solution to the challenges of monitoring enterprise networks by extending the range and depth of security and network tool coverage in the data center. This Vision ONE increases network visibility, optimizes tool utilization, and helps speed troubleshooting efforts. You can immediately optimize efficiency for a wide range of network tools such as application monitors, protocol analyzers, IDS, VoIP analyzers and data recorders.

Contact Information
Visit our support page for support and contact information. For more information about the full assortment of Ixia's products, please visit www.ixiacom.com.

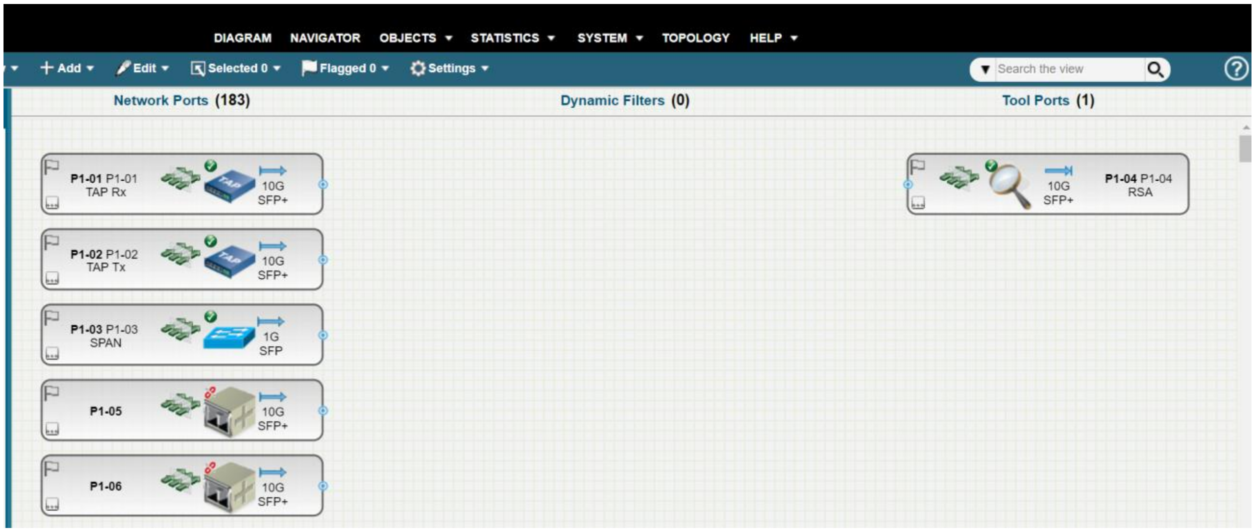
Launching the Vision ONE Web Console
Use the default user name (admin) and default password (admin) to sign on to the system the first time.

Accessing the REST Web API documentation
Visit the documentation page to access a description of the REST Web API service available on this device.

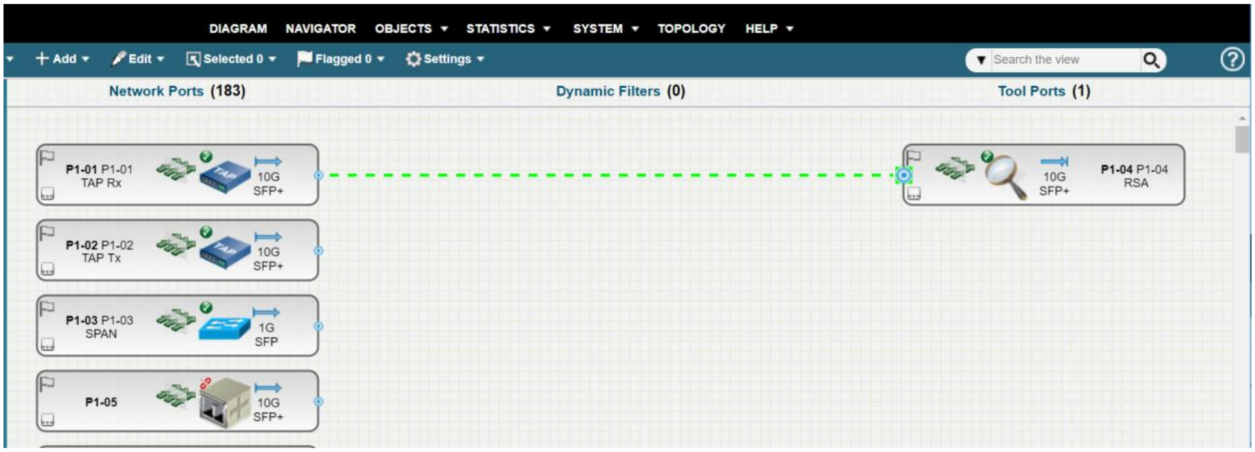
Downloads
You may download and install the packages by clicking on the links below.

SNMP MIBs RADIUS Dictionary

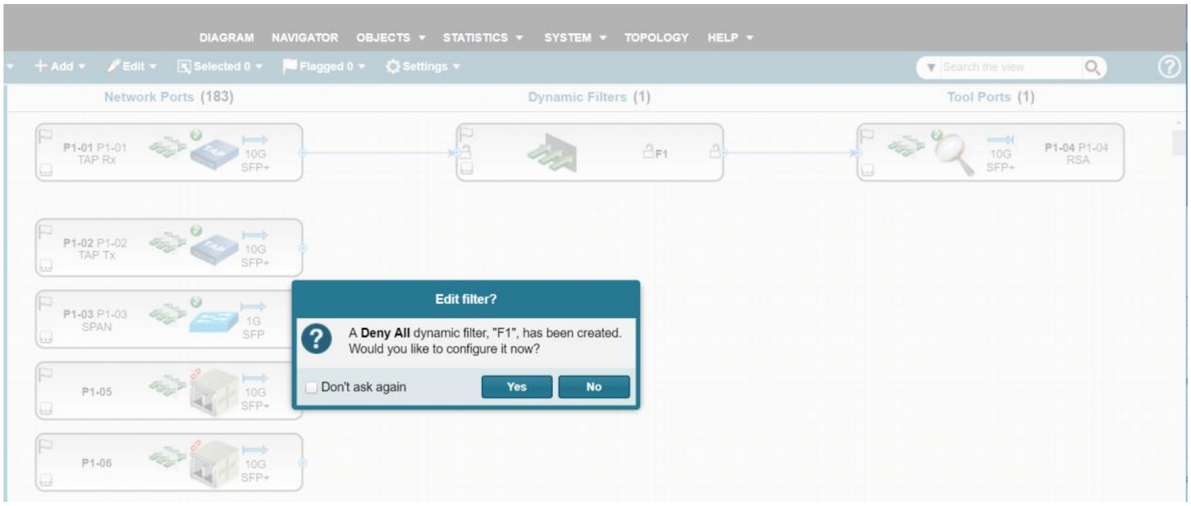
2. Click on the Diagram icon on the left.
3. Right click the ports you want to configure for traffic.
   - Set the mode to Network for TAP/SPAN Connections and Tool mode for RSA Security Analytics
   - Enable the port
   - Under properties rename the port for convenience



4. Select a Tap Rx port and from the small blue square click and drag to tool Port that you want to connect to



5. Click Yes in the pop up.



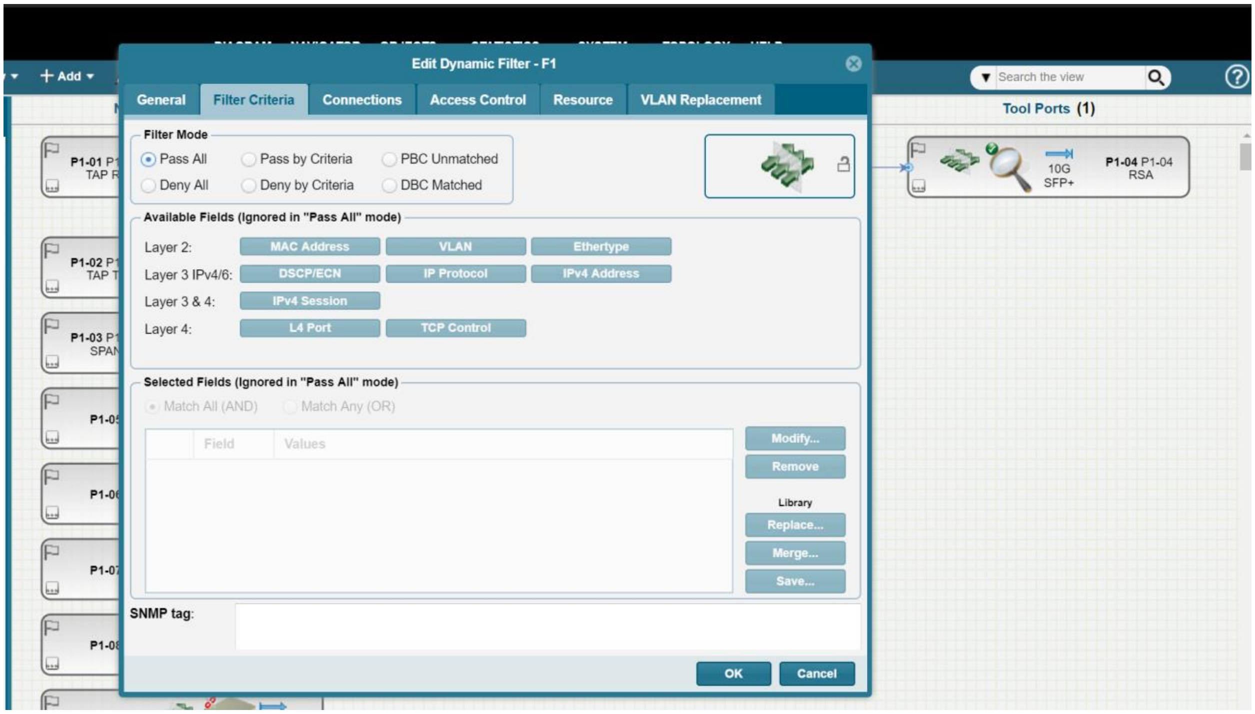
Edit filter?

A **Deny All** dynamic filter, "F1", has been created.
Would you like to configure it now?

☐ Don't ask again

Yes No

6. Right click the filter criteria and select properties at the bottom and in the filter tab select the Pass all Button and click ok until done.



Edit Dynamic Filter - F1

General | Filter Criteria | Connections | Access Control | Resource | VLAN Replacement

Filter Mode

● Pass All ○ Pass by Criteria ○ PBC Unmatched
○ Deny All ○ Deny by Criteria ○ DBC Matched

Available Fields (Ignored in "Pass All" mode)

Layer 2:	MAC Address	VLAN	Ethertype
Layer 3 IPv4/6:	DSCP/ECN	IP Protocol	IPv4 Address
Layer 3 & 4:	IPv4 Session		
Layer 4:	L4 Port	TCP Control	

Selected Fields (Ignored in "Pass All" mode)

● Match All (AND) ○ Match Any (OR)

Field	Values

Modify... Remove

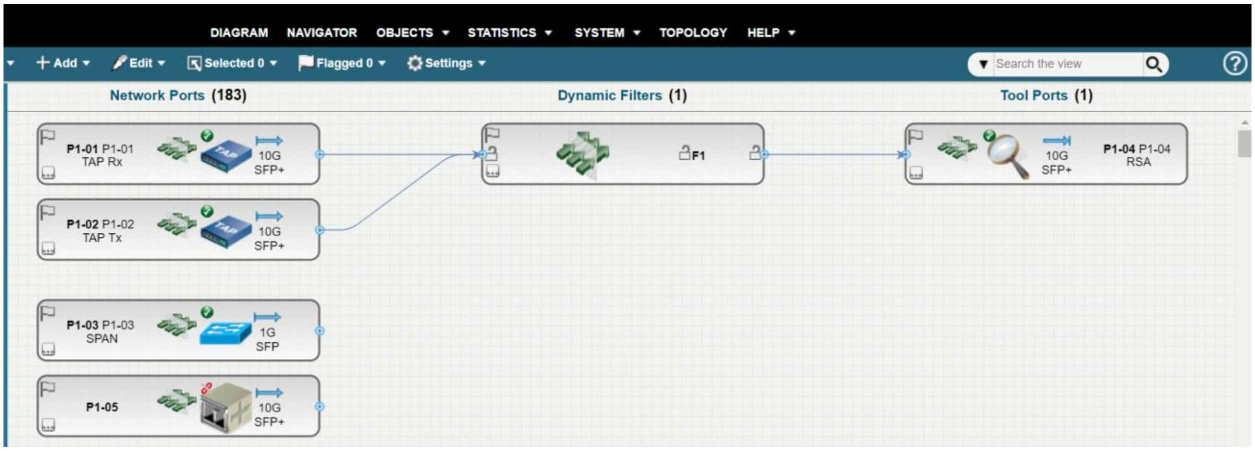
Library

Replace... Merge... Save...

SNMP tag:

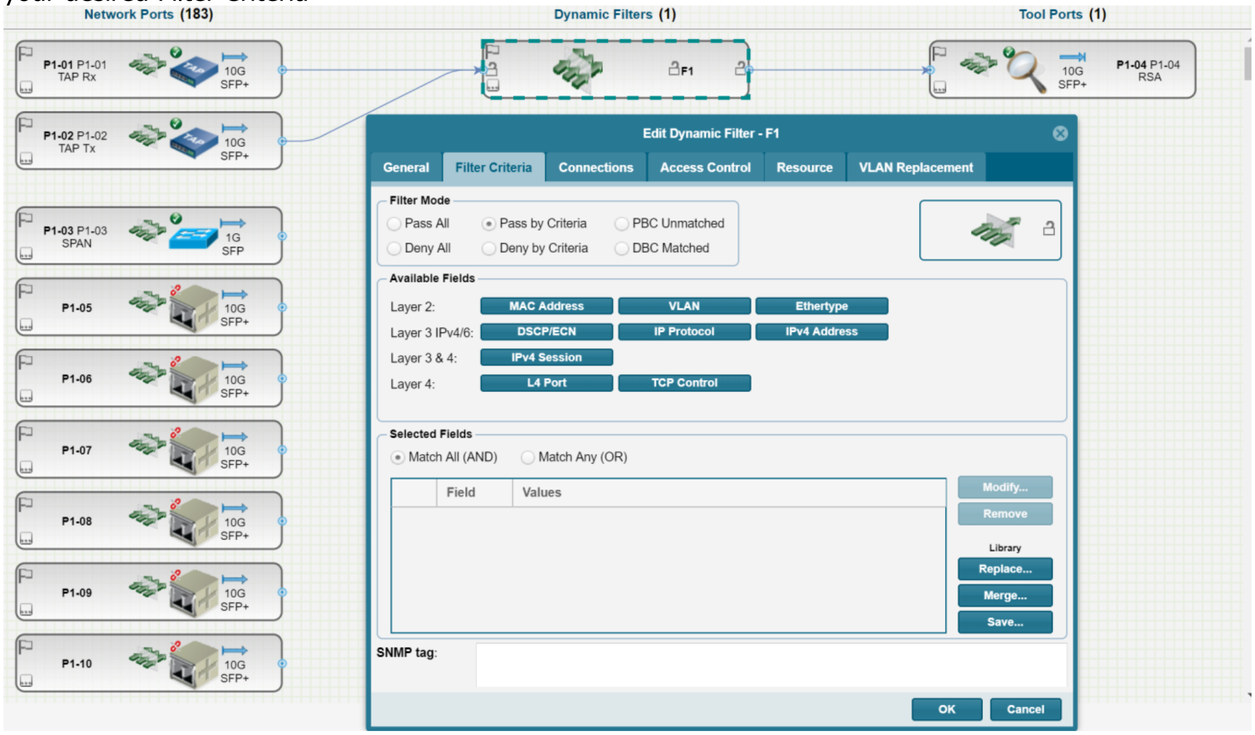
OK Cancel

7. Connect Tap Rx to RSA Tool via the Dynamic filter created in previous step (and repeat again for any needed network SPANs or TAPs) Note: Taps are preferred because the do not drop packets.



Traffic Filtering

8. Right click Dynamic Filter and select properties at the bottom and in the Filter criteria tab choose your desired Filter Criteria



Edit Dynamic Filter - F1

General | Filter Criteria | Connections | Access Control | Resource | VLAN Replacement

Filter Mode

○ Pass All ● Pass by Criteria ○ PBC Unmatched

○ Deny All ○ Deny by Criteria ○ DBC Matched

Available Fields

Layer 2:	MAC Address	VLAN	Ethertype
Layer 3 IPv4/6:	DSCP/ECN	IP Protocol	IPv4 Address
Layer 3 & 4:	IPv4 Session		
Layer 4:	L4 Port	TCP Control	

Selected Fields

● Match All (AND) ○ Match Any (OR)

Field	Values

Modify... Remove

Library

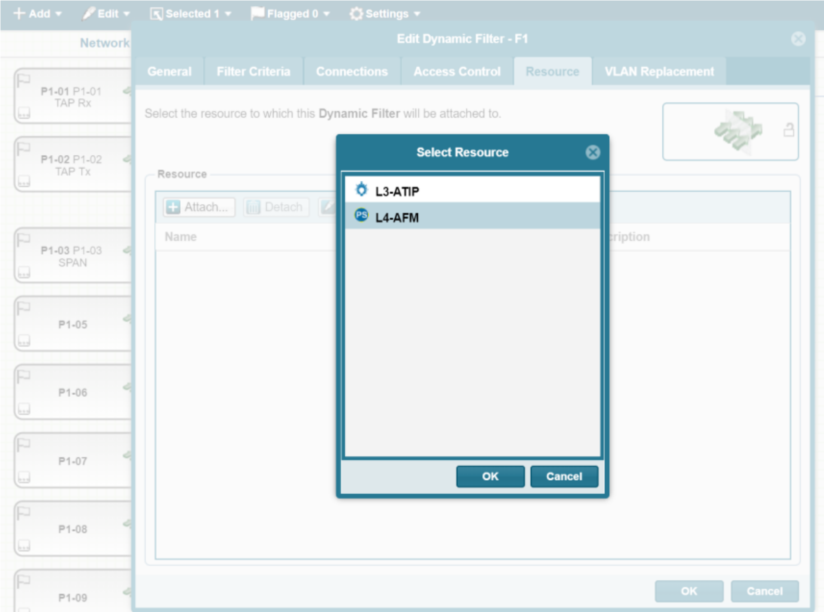
Replace... Merge... Save...

SNMP tag:

OK Cancel

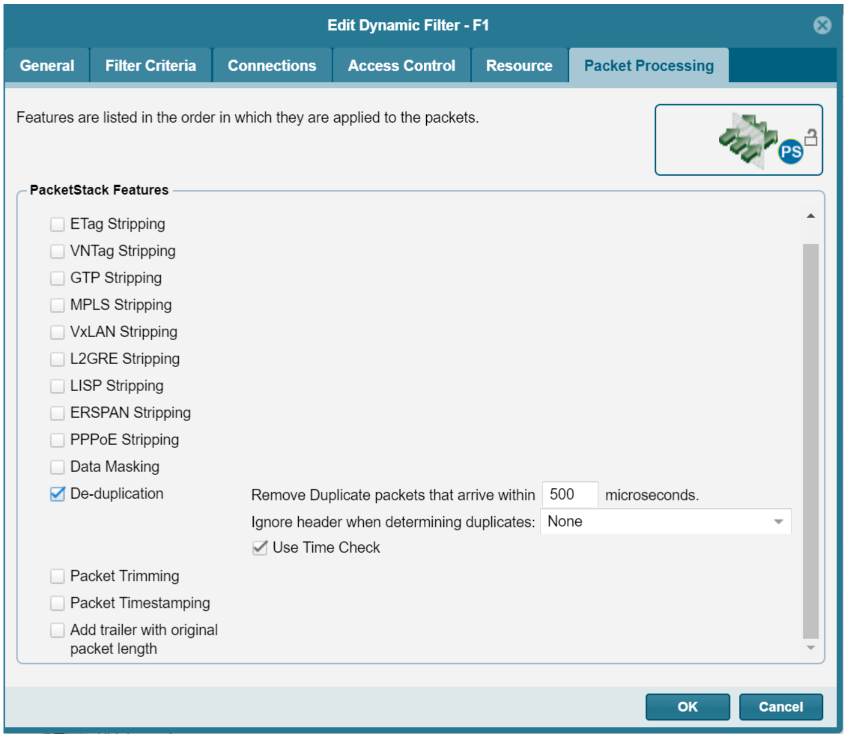
Traffic De-Duplication

9. Right click the Dynamic Filter and select Resources and assign an AFM resource



Select the resource to which this Dynamic Filter will be attached to.

10. Right click the Dynamic Filter and select Packet Processing, then check the De-Duplication box



Features are listed in the order in which they are applied to the packets.

PacketStack Features

☐ ETag Stripping
☐ VNTag Stripping
☐ GTP Stripping
☐ MPLS Stripping
☐ VxLAN Stripping
☐ L2GRE Stripping
☐ LISP Stripping
☐ ERSPAN Stripping
☐ PPPoE Stripping
☐ Data Masking
☑ De-duplication

Remove Duplicate packets that arrive within 500 microseconds.

Ignore header when determining duplicates: None

☑ Use Time Check

☐ Packet Trimming
☐ Packet Timestamping
☐ Add trailer with original packet length

Certification Checklist for RSA Security Analytics

Date Tested: March 30 2018

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5.0.1	Virtual Appliance
Ixia Vision ONE	Server software 4.7.4	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	✓
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