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
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.

<table>
<thead>
<tr>
<th>RSA Security Analytics Tested Features</th>
<th>Vision ONE NPB v4.7.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow / Traffic Mapping</td>
<td>yes</td>
</tr>
<tr>
<td>De-duplication</td>
<td>yes</td>
</tr>
</tbody>
</table>

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.

1. The passive Tap creates a permanent, inline access port to monitor full-duplex traffic.
2. The network signal is either split or regenerated so that the monitoring device has full access to the signal.
3. The monitoring device sees the same traffic as if it were also inline, including physical layer errors.

Monitoring Device
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.

重要：配置显示在本实施指南中的配置仅用于示例和测试目的。它不是计划设备的最优设置。强烈建议客户确保 Ixia Vision ONE 正确配置并安全后，再部署到生产环境中。有关更多信息，请参阅 Ixia Vision ONE 文档或网站。

Ixia Vision ONE Configuration

Launching the Ixia Vision ONE Web Management Interface

Ixia Vision ONE 提供了一个直观的、拖放界面，为您的节点使用。虽然熟悉命令行界面可用于相似的配置任务，Vision ONE 可以简化许多常见任务，允许你以可视化方式配置分发包，而不是通过 CLI 输入文本。所有此指南的管理任务将在 Vision ONE 网页界面中完成。
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 I and log in

[Web Console URL]

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.

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.
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 they 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
Traffic De-Duplication

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

10. Right click the Dynamic Filter and select Packet Processing, then check the De-Duplication box
# Certification Checklist for RSA Security Analytics

Date Tested: March 30 2018

<table>
<thead>
<tr>
<th>Certification Environment</th>
<th>Product Name</th>
<th>Version Information</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RSA Security Analytics</td>
<td>10.5.0.1</td>
<td>Virtual Appliance</td>
</tr>
<tr>
<td></td>
<td>Ixia Vision ONE</td>
<td>Server software 4.7.4</td>
<td>Linux</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Analytics Test Cases</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Packet Loss</strong></td>
<td></td>
</tr>
<tr>
<td>Syslog TCP data consumed by the SA Log Decoder</td>
<td>✔️</td>
</tr>
<tr>
<td>Syslog UDP data consumed by the SA Log Decoder</td>
<td>✔️</td>
</tr>
<tr>
<td>Various packet data consumed by the SA Packet Decoder</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>De-duplication</strong></td>
<td></td>
</tr>
<tr>
<td>Replaying data files to the SA Packet Decoder</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Traffic Mapping</strong></td>
<td></td>
</tr>
<tr>
<td>Mapping network service ports to dedicated ports</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td></td>
</tr>
<tr>
<td>SA Log Decoder minimal EPS performance</td>
<td>✔️</td>
</tr>
<tr>
<td>SA Packet Decoder minimal EPS performance</td>
<td>✔️</td>
</tr>
</tbody>
</table>

✔️ = Pass  ❌ = Fail  N/A = Non-Available Function