



## RSA Ready Implementation Guide for RSA Security Analytics

Last Modified: March 2 2015

### Partner Information

---

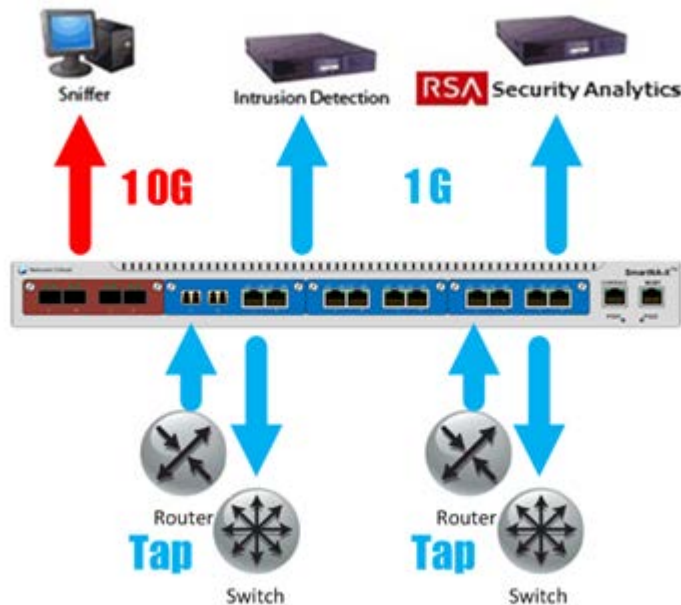
Product Information	
Partner Name	Network Critical
Web Site	<a href="http://www.networkcritical.com">www.networkcritical.com</a>
Product Name	SmartNAx Series
Version & Platform	6.102
Product Description	Network Critical offers modular-based intelligent traffic visibility nodes. These hybrid TAP/Packet Broker devices extend traffic visibility to more remote portions of network running critical applications that require monitoring.



## Solution Summary

The SmartNA-X Series delivers performance, ease of use, and intelligence as a hybrid TAP and Packet Broker for predominantly 1G networks and 1 and 10G tools. With an extremely easy to use web-based interface (Drag-n-Vu) and a powerful filtering and mapping algorithms, the SmartNA-X is able to replicate, filter, and selectively forward network traffic to monitoring, management, and security tools such as RSA Security Analytics. Optional SmartNA-X functions including , By-pass VLine™ taps for inline applications; Advanced Packet Filtering; Packet Slicing and Masking; Header Stripping; create a robust distributed monitoring solution. By combining SmartNA-X 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.

RSA Security Analytics Tested Features	
Network Critical SmartNAx	
Flow / Traffic Mapping	Yes
De-duplication	No



## Partner Product Configuration

---

### ***Before You Begin***

This section provides instructions for configuring the SmartNAX 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 Network Critical 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 SmartNAX is properly configured and secured before deploying to a production environment. For more information, please refer to the SmartNAX documentation or website.**

---

### ***SmartNAX Configuration***

#### **Launching the Web Management Interface**

*DRAG-N-VU™* provides you with an intuitive, drag-and-drop interface for your nodes. Although the familiar command-line interface will always be available for all configuration tasks, DRAG-N-VU™ 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 DRAG-N-VU™ web interface.

1. Browse to the login page of the SmartNA-X Series device (e.g. [https:// 192.168.100.254](https://192.168.100.254))
2. Enter the administrator's username and password that was created during the initial setup of the device (admin) (admin).
3. Click **Login**.



Welcome to SmartNA-X™

User ID

Password

## Configuring Flow / Traffic Mapping

Flow Mapping is at the heart of the power of the SmartNA-X where you decide how traffic arriving on a network port is distribution to other network ports, and ends with tool ports. Network ports are where you connect data sources to the SmartNA-X systems. They can then be configured to send packets to a tool port. Tool ports are where you connect destination devices for the data arriving to tools such as SA. You decide which traffic should be forwarded, where it should be sent, and how it should be handled once it arrives. In this case we used port 2a for the network and 2c for the tool/SA.

4. From the web management interface, click anywhere within the appliance box to see the current configuration.
5. Click on port 2a and configure it with the pull downs to the values shown then apply changes at top

The screenshot displays the SmartNA-X web management interface. At the top, there is a navigation bar with the Drag-n-Vu logo, a 'Help' button, a 'View manual' button, a 'Review/apply changes' button, and a 'Log out' button. The main content area shows a network diagram with two racks of ports. Rack 1 has ports A, B, C, and D. Rack 2 has ports A, B, C, and D. A 'V-Line' is indicated between ports A and B in rack 1. Below the diagram, there is a 'Port configuration' section with tabs for 'Traffic', 'Errors', and 'Health'. The 'Port 2A' configuration is shown with the following settings:

Parameter	Value
Description	[Edit icon]
Usage	Network
Type	RJ
Auto-Negotiation	Off (fixed)
Speed	100M
MDI	Auto
Duplex	Full
Mastery	Master?
TAP	Off
Autolock	<input type="checkbox"/>
Lock	<input type="checkbox"/>

- Click on port 2b and choose the same settings except use slave? For mastery then apply changes at top.

The screenshot displays the SmartNA-X web interface. At the top, there is a navigation bar with the Drag-n-Vu logo, a 'Help' button, 'View manual' and 'Review/apply changes' buttons, and a 'Log out' button. Below this is a network diagram showing two switches, labeled 1 and 2. Switch 1 has four ports (A, B, C, D) with various colored lines connecting them. Switch 2 has four ports (A, B, C, D) with yellow and blue lines. To the right of the diagram is a 'REAR PORTS' section with two ports labeled A and B. Below the diagram is a configuration panel for 'Port 2B'. The panel has tabs for 'Port configuration', 'Traffic', 'Errors', and 'Health'. The 'Port configuration' tab is active. The configuration options are: Description (with an edit icon), Usage (Network), Type (RJ), Auto-Negotiation (Off (fixed)), Speed (100M), MDI (Auto), Duplex (Full), Mastery (Slave?), TAP (Off), Autolock (checkbox), and Lock (checkbox).

- Repeat for port 2c with usage labeled as tool

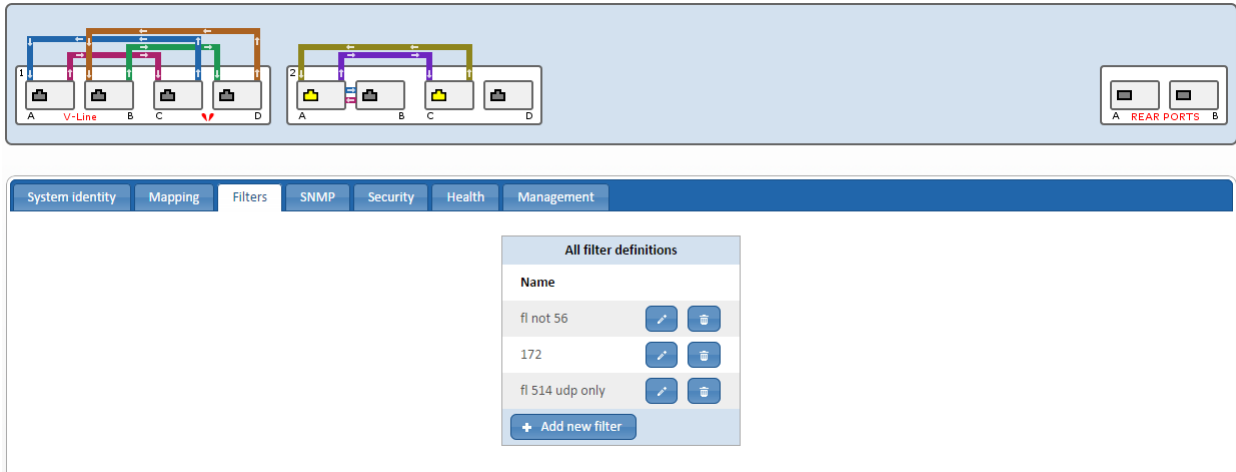
8. Click on port 2a and drag to 2B and release, repeat from 2c to 2a. Apply changes at top.

The screenshot shows the Drag-n-Vu SmartNA-X interface. At the top, there are navigation buttons: Help, View manual, Review/apply changes, and Log out. The interface displays two network diagrams. The left diagram shows a switch with four ports (A, B, C, D) and a V-Line connection. The right diagram shows a switch with four ports (A, B, C, D) and a REAR PORTS connection. Below the diagrams is a port configuration panel for Port 2B. The configuration includes: Description (edit icon), Usage (Undefined), Type (RJ), Auto-Negotiation (Off (fixed)), Speed (100M), MDI (Auto), Duplex (Full), and Mastery (Slave?).

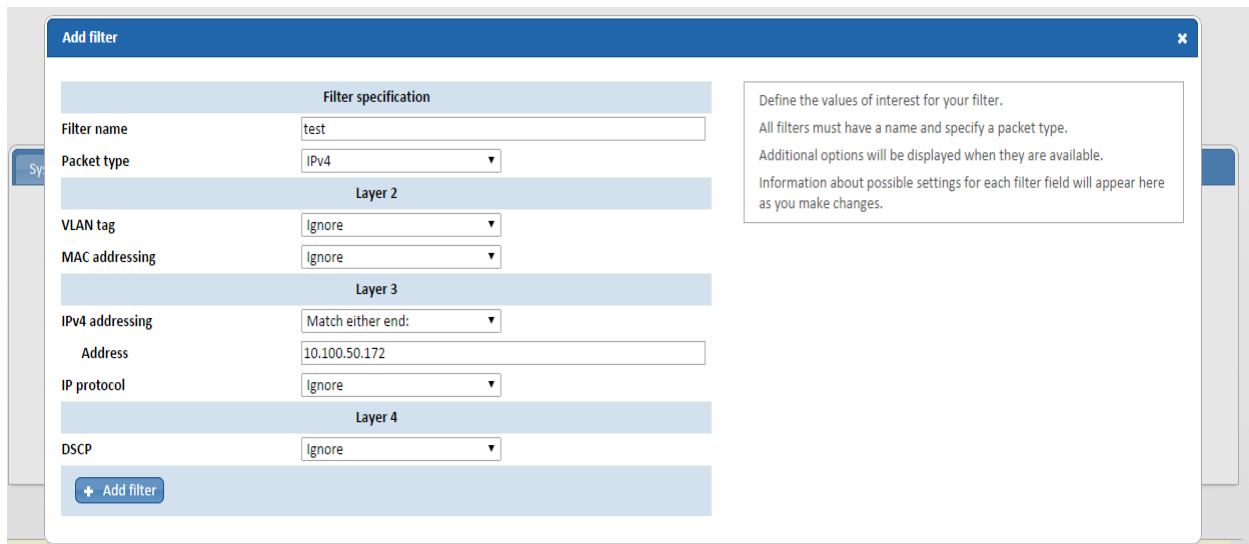
9. Repeat click and drag for 2a to 2b and 2b to 2a review and apply changes

The screenshot shows the Drag-n-Vu SmartNA-X interface. At the top, there are navigation buttons: Help, View manual, Review/apply changes, and Log out. The interface displays two network diagrams. The left diagram shows a switch with four ports (A, B, C, D) and a V-Line connection. The right diagram shows a switch with four ports (A, B, C, D) and a REAR PORTS connection. Below the diagrams is a port configuration panel for Port 2B. The configuration includes: Description (edit icon), Usage (Undefined), Type (RJ), Auto-Negotiation (Off (fixed)), Speed (100M), MDI (Auto), Duplex (Full), and Mastery (Slave?).


10. Click anywhere on the appliance box to get back to the main screen and click the filters tab.

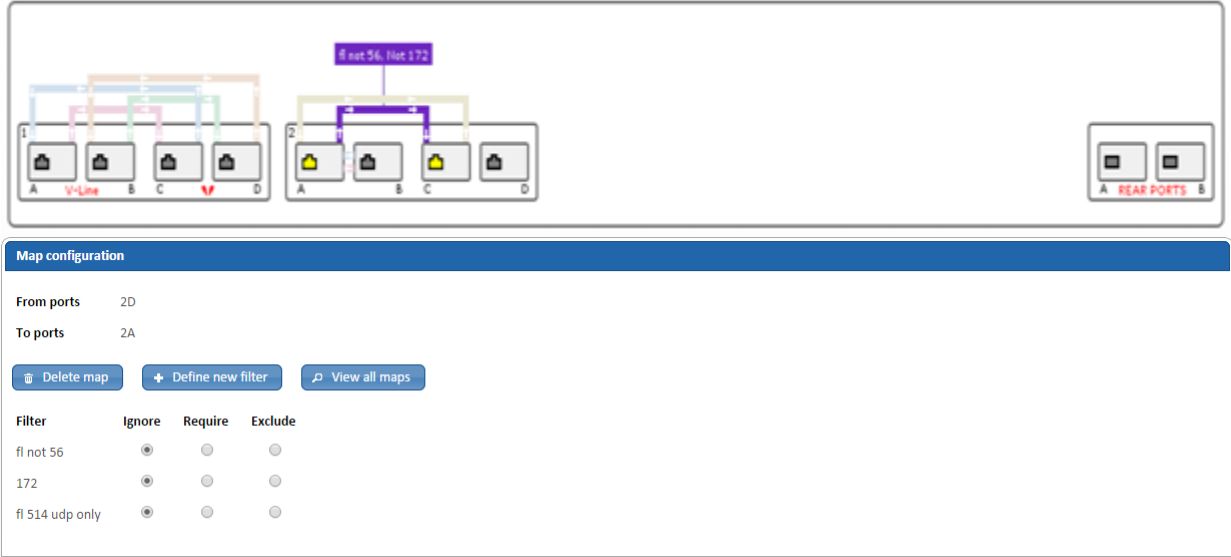


11. Fill out the filter menu for the desired filters and click add filter



12. Apply filter to tool port by clicking the path you wish to apply the filter on and picking the appropriate radio button.

 **Note: Require will only pass through whatever the filter is configure for and Exclude will pass everything except what the filter is configured for.**



The diagram shows two server racks, labeled 1 and 2. Rack 1 has four ports labeled A, B, C, and D. Rack 2 has four ports labeled A, B, C, and D. A filter configuration panel is shown below the racks. The panel has a blue header "Map configuration" and the following fields:

From ports 2D  
To ports 2A

Buttons: Delete map, Define new filter, View all maps

Filter	Ignore	Require	Exclude
fl not 56	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
172	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
fl 514 udp only	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>



## Certification Checklist for RSA Security Analytics

Date Tested: February 11, 2015

Certification Environment		
Product Name	Version Information	Operating System
RSA Security Analytics	10.4	Virtual Appliance
SmartNAX	6.102	Appliance

Security Analytics Test Cases	Result
<b>Packet Loss</b>	
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	✓
<b>De-duplication</b>	
Replaying data files to the SA Packet Decoder	N/A
<b>Traffic Mapping</b>	
Mapping network service ports to dedicated ports	✓
<b>Performance</b>	
SA Log Decoder minimal EPS performance	✓
SA Packet Decoder minimal EPS performance	✓

FAL

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