RSA Ready Implementation Guide for RSA Security Analytics

ixia Phantom 3.7.0.4-1vmw.500.0.0.472560

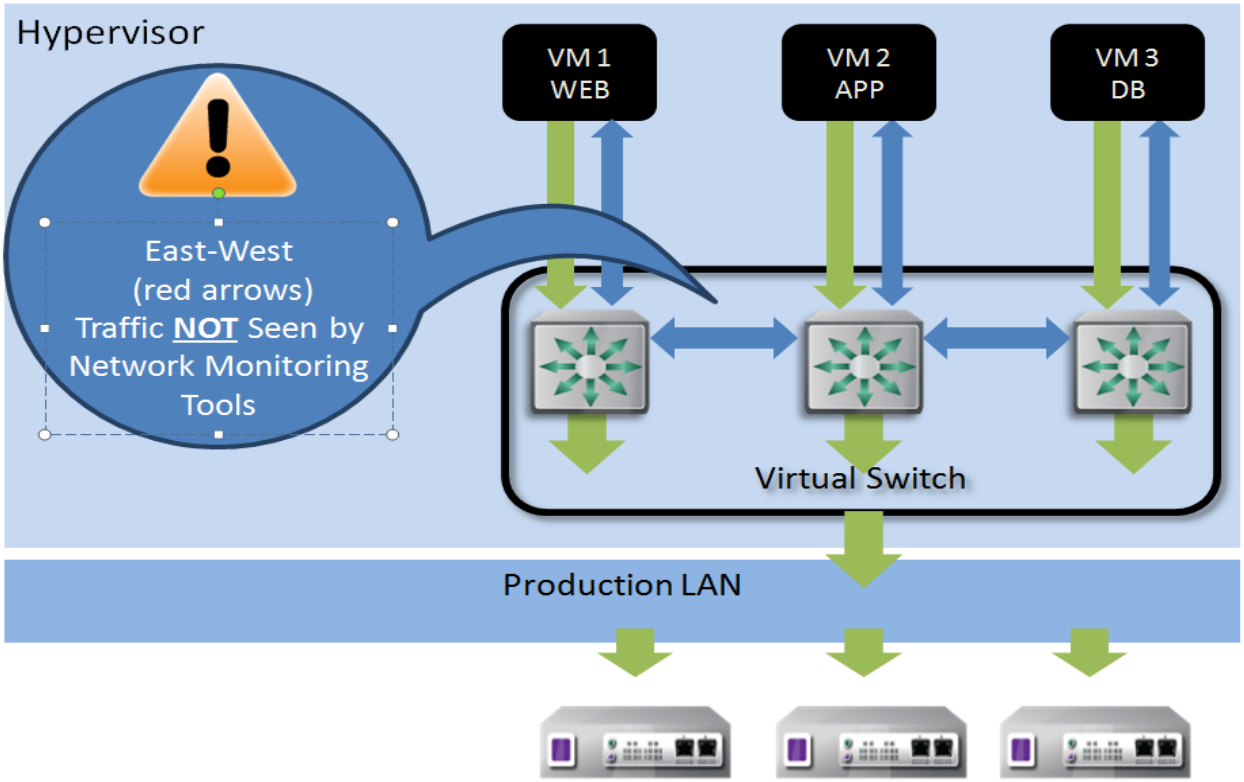
FAL, RSA Partner Engineering
Last Modified: 3/11/16

RSA READY

Solution Summary

The Ixia Phantom Virtualization Tap™ (vTap) solution is an "all-in-one" virtual traffic Monitoring tool—providing centralized management with an easy-to-use web UI for total access and control of your security and performance monitoring needs. The Phantom vTap captures east-west network packets passing between internal virtual Machines (VMs) and sends that traffic of interest to any existing virtual and physical Monitoring tools. In addition, it provides unprecedented visibility of packet-level data that allows users to manage virtual network security, compliance and performance using a variety of instrumentation layer tools (physical or virtual). Since the Phantom vTap can bridge virtual-to-physical in converged environments, users can maintain Current policies without having to buy new expensive monitoring tools for virtualized deployments. It can be used in conjunction with Ixia 5288 TAP with the GRE module for more control and de-duplication.

RSA Security Analytics Tested Features <Partner Product Name and version>	
Flow / Traffic Mapping	Yes
De-duplication	No



Partner Product Configuration

Before You Begin

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

ixia Phantom Configuration

The Phantom Manager will install the vTap module appropriate to the host environment. The vTap Module is installed as a low-level component in ESXi 5.0, ESXi 5.1 and KVM hosts environments. For ESXi 5.5 and ESXi 6.0 with Virtual Distributed Switch (vDS) environments, the Phantom vTap module is installed on a host as a tap VM, one VM for each vDS connection. The purpose of this module is that it performs the tapping function. This module enables you to configure complex network packet mirroring, filtering and forwarding. Install the VM as outlined in the Ixia documentation for the appropriate Virtual environment.After successfully installing the Management Server and assigning it an IP address, you can log in to the Management Server through a browser.

1. Enter the IP address of the Management Server in the URL of a browser.

--After logging into the Management Server, a dialog appears asking you to connect a Virtualization Platform you want to monitor. A Virtualization Platform can be:

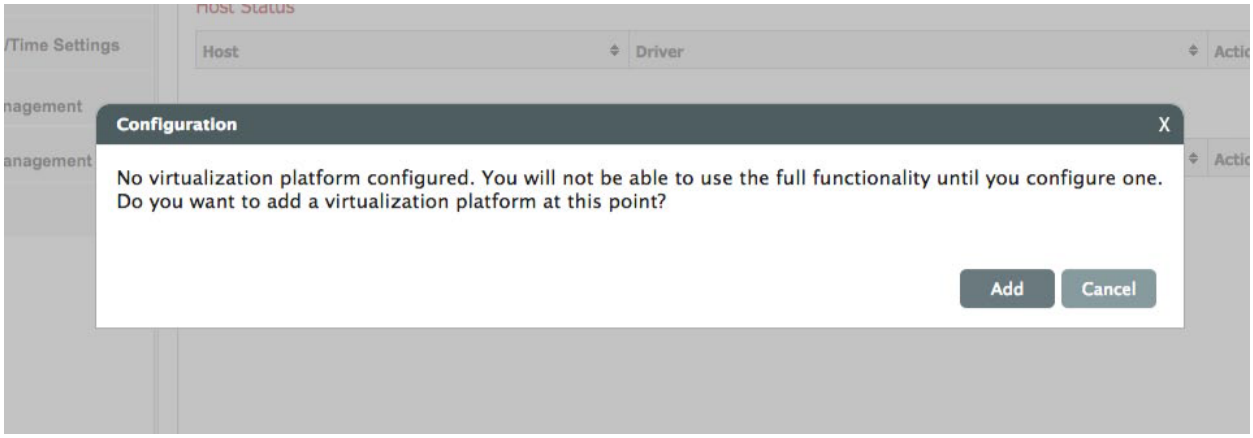
- a standalone ESXi host
- a vCenter containing 5.0 or 5.1 ESXi hosts for tapping vSwitches

> **Note: Even if the vCenter contains 5.5 and 6.0 hosts, they will not be displayed in Inventory as they cannot be monitored**

- a vCenter containing 5.5 or 6.0 ESXi hosts for tapping Virtual Distributed Switches (vDS)

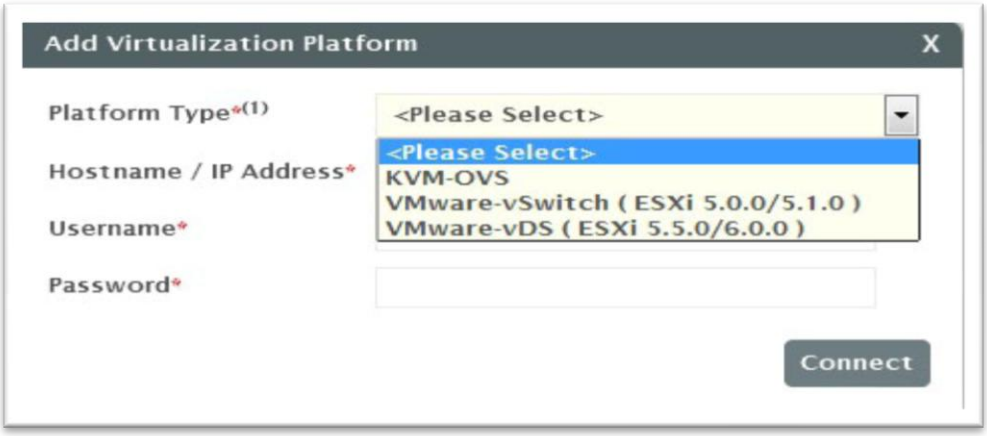
> **Note: even if the vCenter contains 5.0 and 5.1 hosts, they will not be displayed in Inventory as they cannot be monitored**

- a KVM host
- a KVM host in Open Stack



2. Click the **Add** button (if necessary, navigate to **Configuration** tab > **Virtualization Platforms** page).

3. Click **Add Virtualization Platform** (right side of the page) to add a vCenter, vCenter using vDS, standalone ESXi host or KVM host.

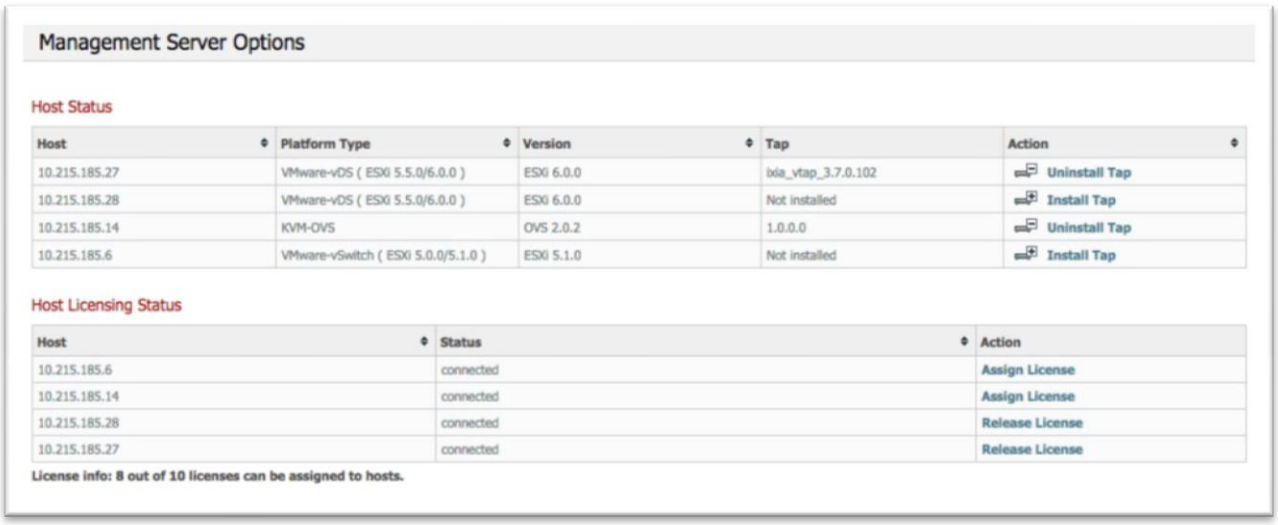


4. Select the Platform type from the drop down.: Enter the IP address or hostname of the Virtualization Platform you are adding. the username and password of a user on that system and connect.

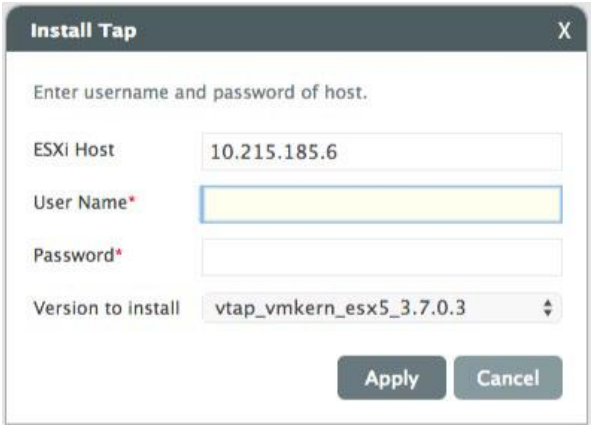
Platform Type Select
ESXi vCenter v5.0 or v5.1 w/vSwitch **VMware-vSwitch**
ESXi vCenter v5.5 or v6.0 w/vDS **VMware-vDS**
KVM or KVM w/Open Stack **KVM-OVS**

For KVM hosts, you can also define the VLAN interface which will be used to forward mirrored traffic, if a VLAN forwarding policy is defined.

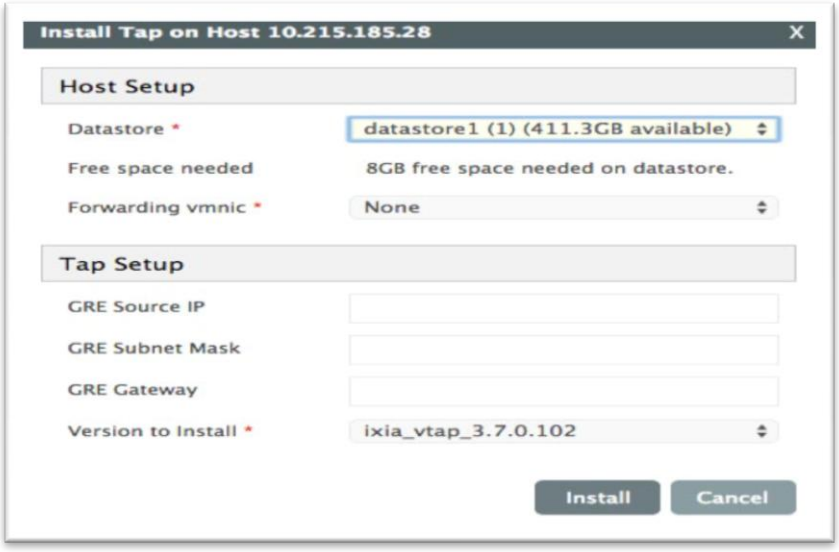
After the platform is connected, the platform appears on the Management Server Options and Virtualization Platforms lists.



5. Under the Host Status section, click **Install Tap** on the host where you want to install the vTap Module.
6. If the host platform type is non-vDS, this Install Tap box appears.
7. a. Enter the username and password of a user that has access to the host.
8. b. Select the version of the Phantom vTap Module Tap to install.
9. c. Click **Apply**.



10. If the host platform type is vDS, this Install Tap box appears.

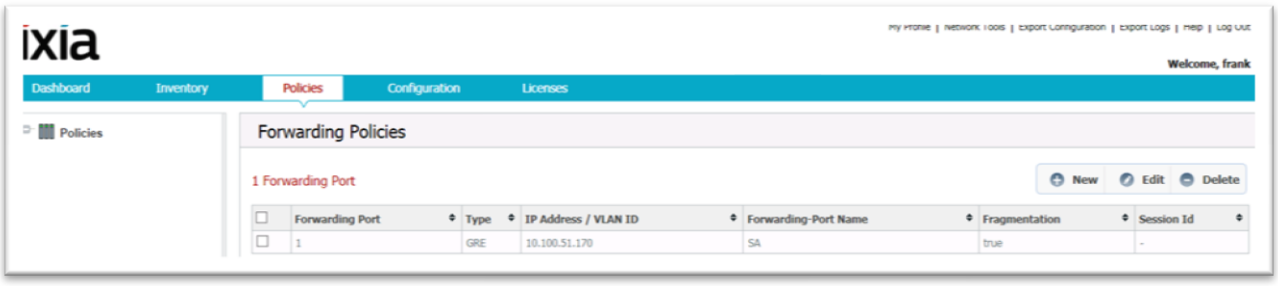


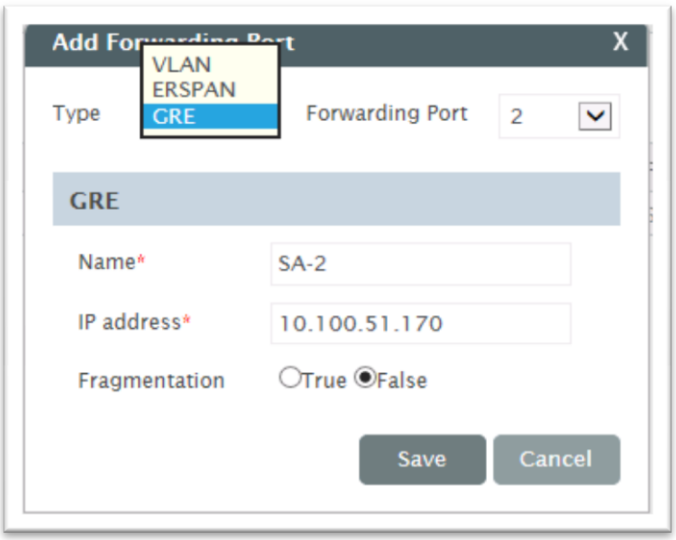
Note: The GRE source is the IP assigned to the Ixia 5288 containing the GRE card and the VMnic would be a nic on the vDS.

Policies

Phantom vTap enables you to more narrowly define the types of traffic to monitor. The vTap enables you to define the traffic you want to monitor by configuring policies. There are two types of policies - Capture Policies and Forwarding Policies. At the initial installation, there are no policies defined. Therefore it will be up to the, the user, to create and assign these policies to the virtual machines you want to monitor. By default, a Universal Capture Policy is defined, which has assigned to it all VMs from all hosts added in the Management Server. However, no rules are defined in this policy. If you want to use the Universal Policy, you must first define a Forwarding Policy and then add a Capture Rule within the Universal Policy.

11. Click New to add a new policy, we chose GRE.

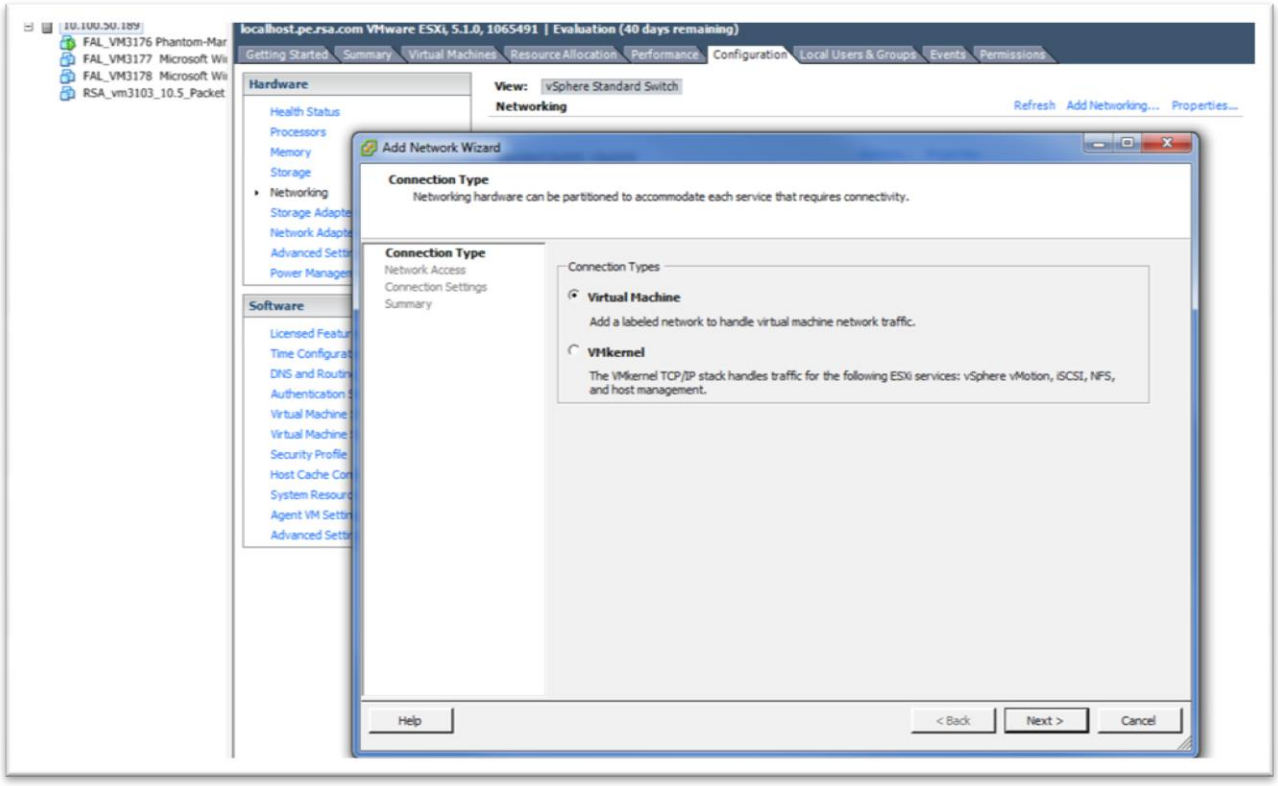




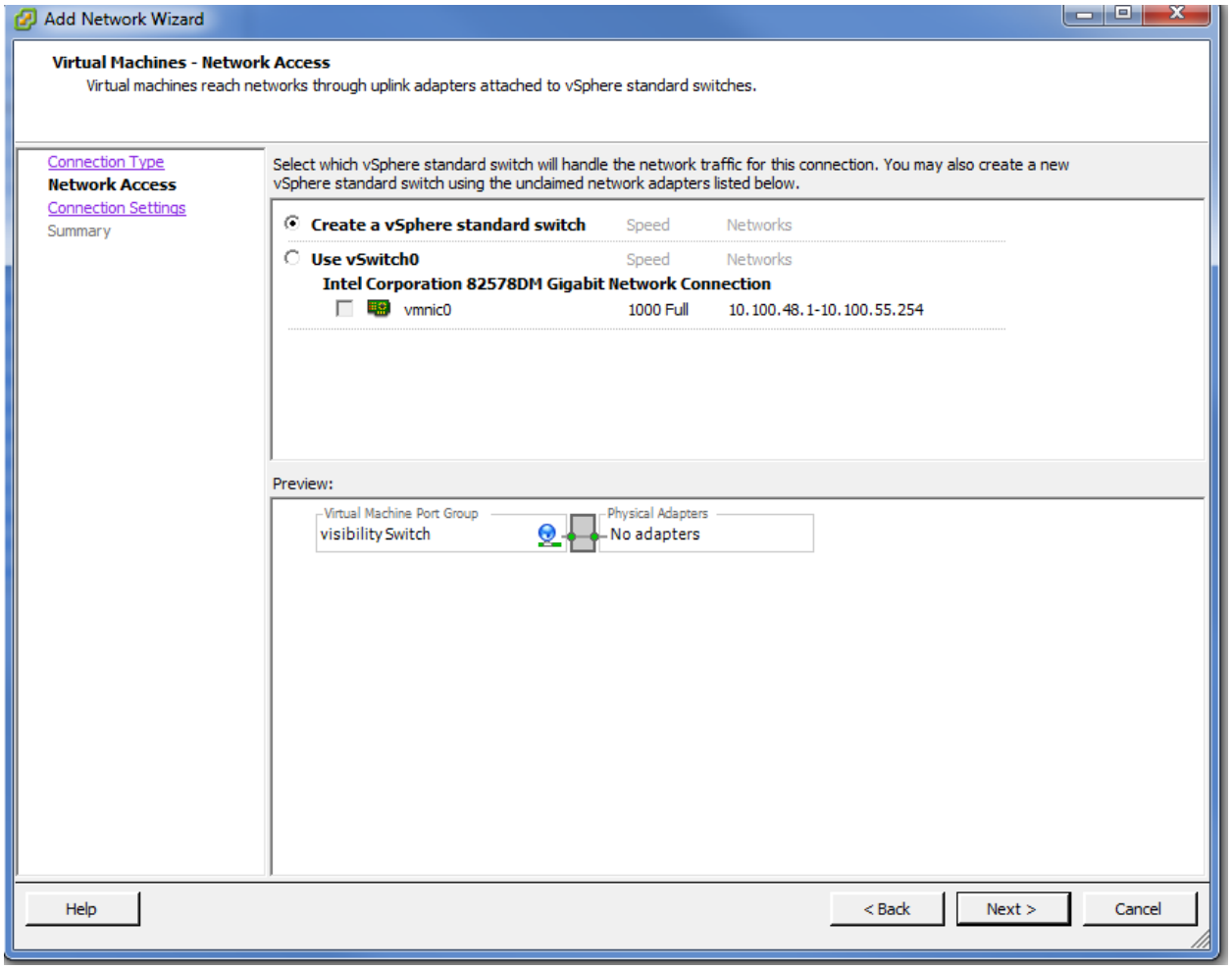
Creating a New Visibility vSwitch

From

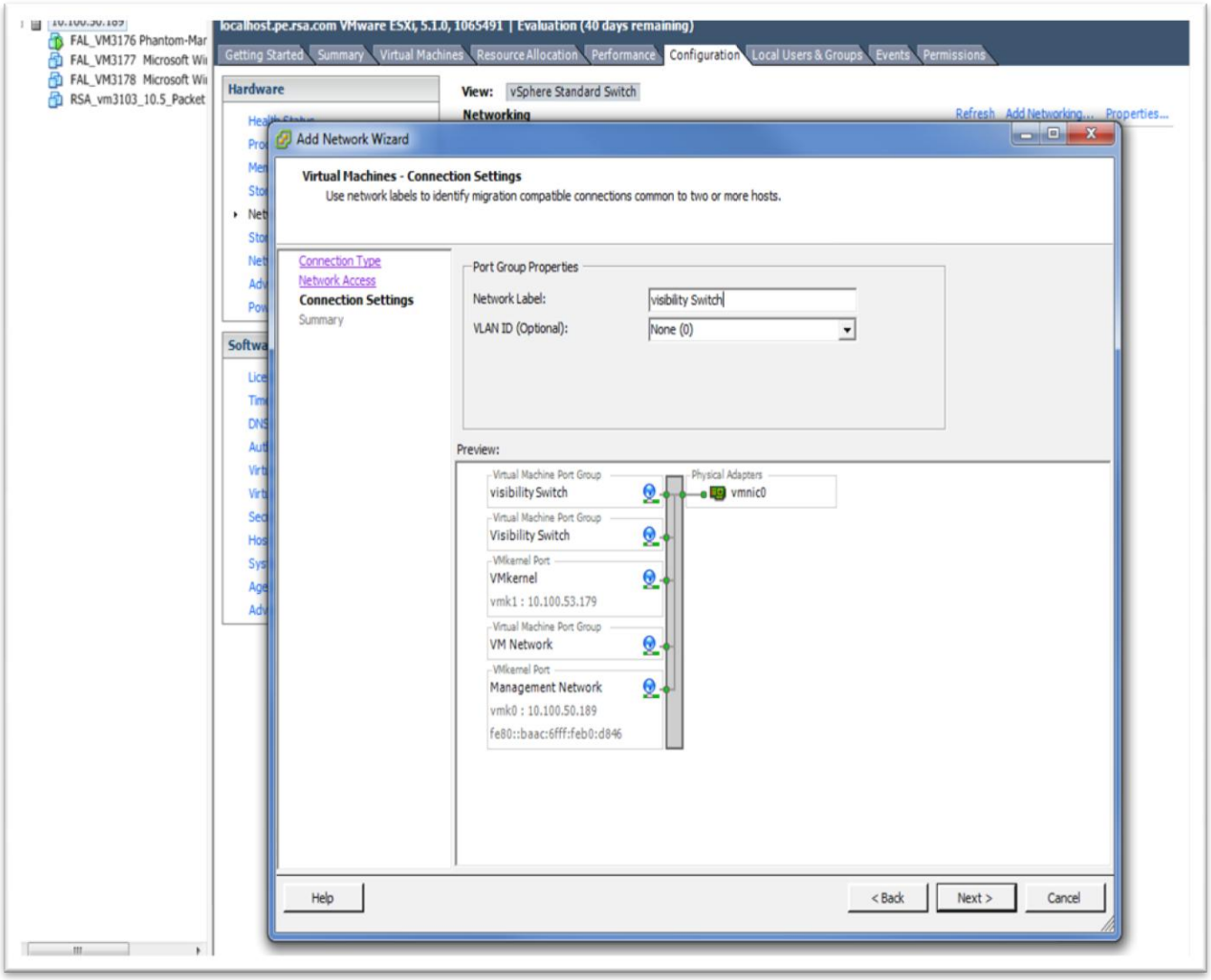
12. the vSphere Client, select "Add Networking."



13. Select the Create a VSphere standard switch and VMnic if more than one available and click next.

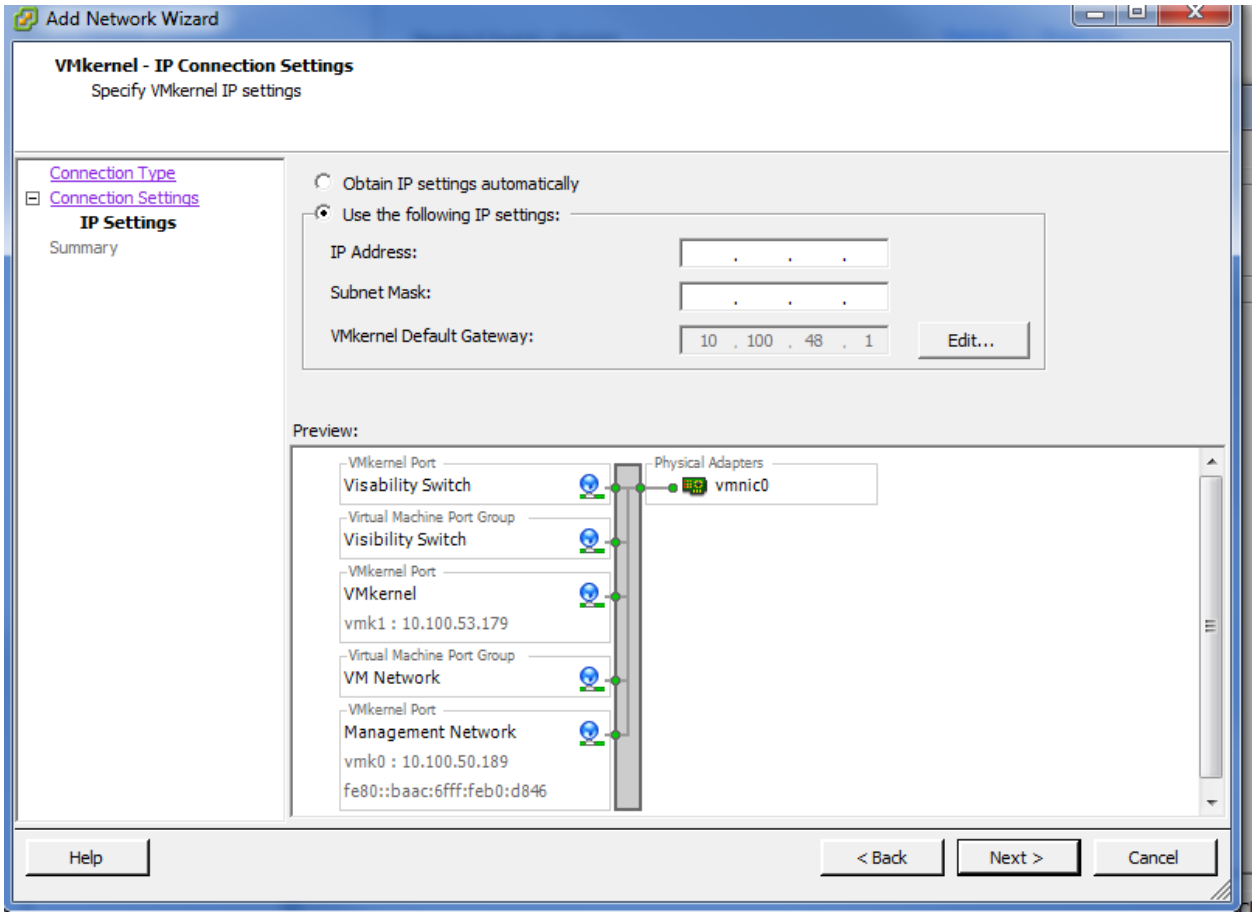


14. Type the Network Label name (visibility vSwitch) and optional Vlan ID click next and finish.

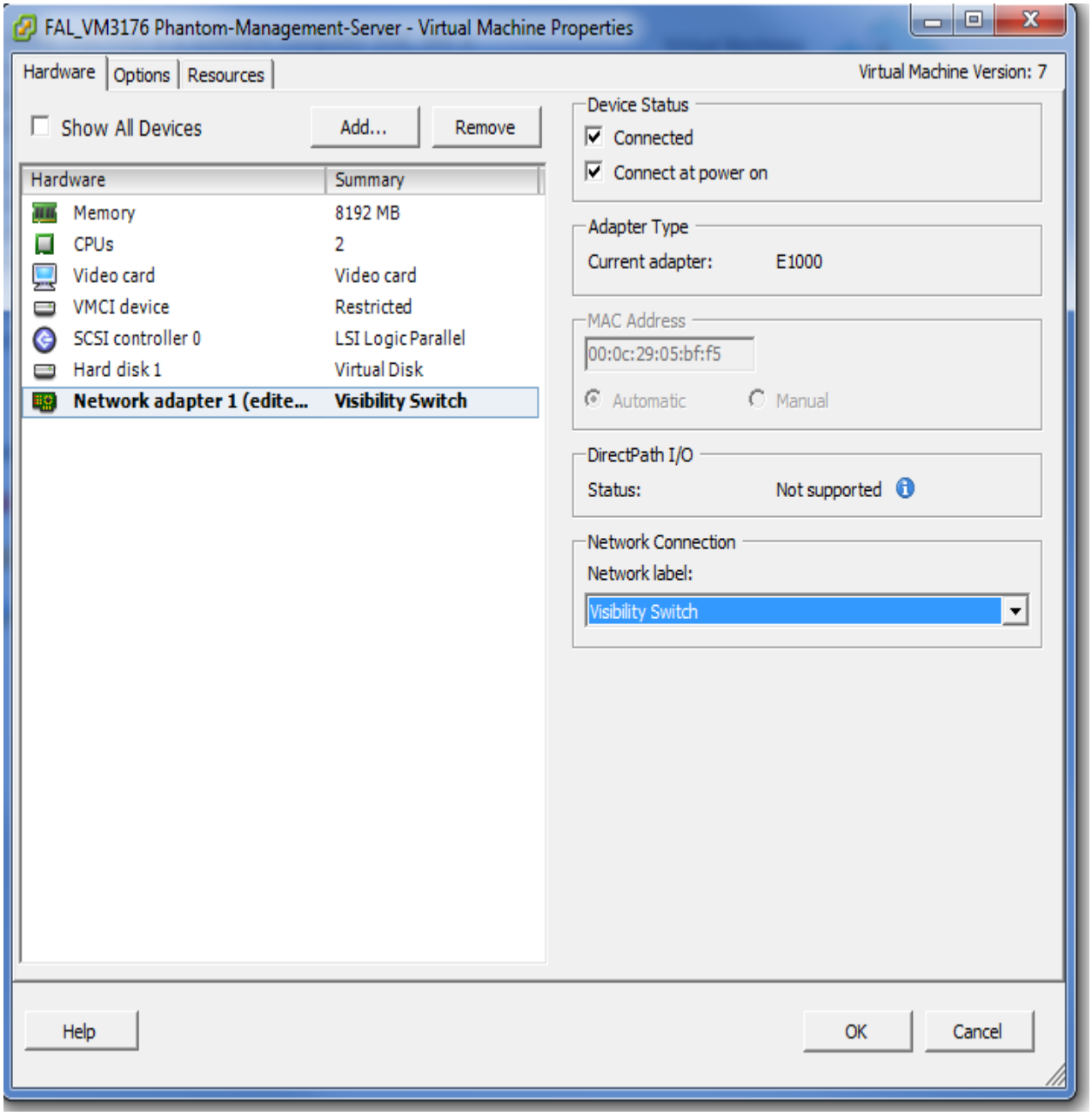


If the environment is based on ESXi v5.0 and/or v5.1, when using GRE to forward mirrored traffic, a VMkernel port needs to be attached to the Visibility vSwitch, with an IP address of the Ixia 5288 switch that allows connectivity to the GRE destination. This address will be used as the GRE source IP address.

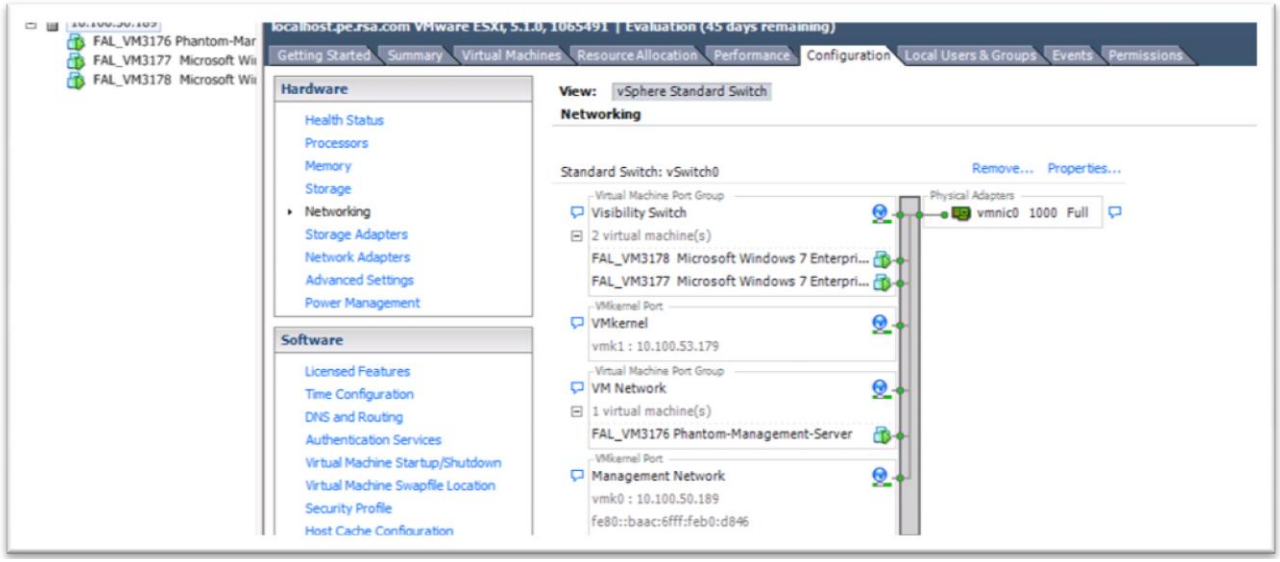
15. Enter the IP and subnet mask of the Ixia 5288 switch hit next and finish.



16. Go to the VM host you want to monitor and edit the hardware to add to the visibility switch by highlighting network adaptor, and set the network connection to the Visibility switch.

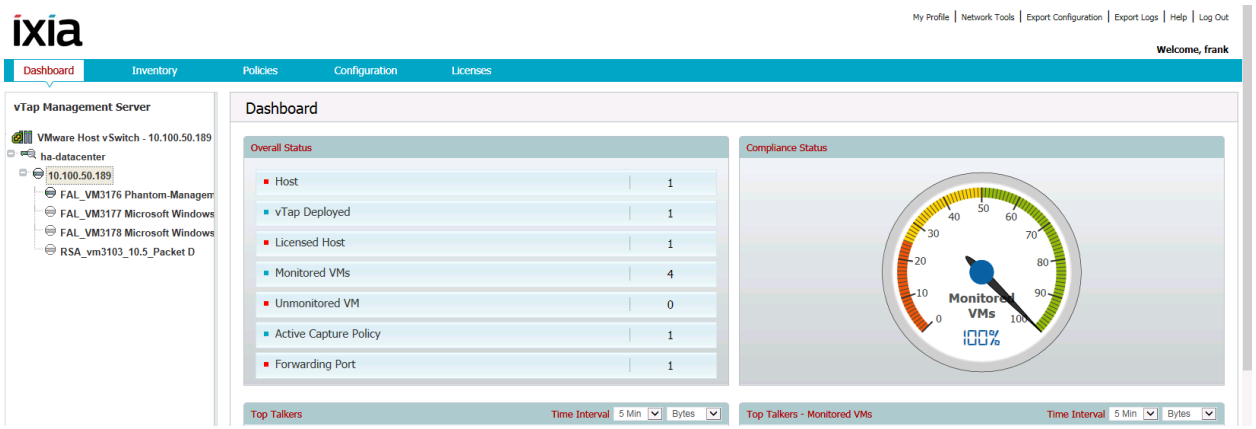


17. Check network configuration and make sure the VM hosts you want to monitor are under the visability switch.



Dashboard Introduction

The Dashboard displays overall status for Phantom vTaps and monitored/unmonitored virtual machines. In addition, it also displays compliance status of all monitored virtual machines and pie charts for both top talkers of machines and top talkers of monitored virtual machines.



Certification Checklist for RSA Security Analytics

Date Tested: March 16 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5.01	Virtual Appliance
Ixia Phantom	3.7.0.4-1vmw.500.0.0.472560	Virtual 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	N/A
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

Known Issues

Partial Install

For VMware-vDS virtualization platforms, when installing the Tap on a host, it is possible that the tapping will only succeed for a subset of the Virtual Distributed Switches connected to that host due to external factors. This partial Install is shown in the UI with a warning sign in the Tap column. On mouse-over a status is offered for the overall host and some details for each failure. Most of these failures can be corrected by user actions.

Example:Adding Notes to the Document Outline