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



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.





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.

ixia		
Username		
Password		
	Log In	



--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

		Host Status						
/Time Setting	gs	Host	\$	Driver			\$	Actic
nagement	Configu	iration				x		
anagement				10 8 2	8 - 2		¢	Actic
	No virt	ualization platfor	m configured. You will not be rtualization platform at this po	able to use the fu	Il functionality unti	l you configure one.		
	20 100	mane to add a m	tualization platform at this p					
						Add Cancel		

- 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.

Platform Type*(1)	<please select=""></please>	-
1	<please select=""></please>	
Hostname / IP Address*	KVM-OVS	
	VMware-vSwitch (ESXi 5.0.0/5.1.0)	
Username*	VMware-vDS (ESXi 5.5.0/6.0.0)	
Password*		

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.

TUSL SUGLUS									
Host	٠	Platform Type	٠	Version	٠	Тар		Action	•
10.215.185.27		VMware-vDS (ESXI 5.5.0/6.0.0)		ESXI 6.0.0		bia_vtap_3.7.0.102		🖙 Uninstall Tap	
10.215.185.28		VMware-vDS (ESXi 5.5.0/6	.0.0)	ESXI 6.0.0		Not installed		≓ Install Tap	
10.215.185.14		KVM-OVS		OVS 2.0.2		1.0.0.0		🖙 Uninstall Tap	
10.215.185.6		VMware-vSwitch (ESXi 5.0.	0/5.1.0)	ESX 5.1.0		Not installed		🕬 Install Tap	
						1100.0100000			
lost Licensing Status		٥	Status				٠	Action	
lost Licensing Status Host 10.215.185.6		٠	Status connected				•	Action Assign License	
lost Licensing Status Host 10.215.185.6 10.215.185.14		•	Status connected connected				٠	Action Assign License Assign License	
Host Licensing Status Host 10.215.185.6 10.215.185.14 10.215.185.28		¢	Status connected connected connected				٠	Action Assign License Assign License Release License	

- 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.

Enter username ar	nd password of host.	
ESXi Host	10.215.185.6	
User Name*		
Password*		
Version to install	vtap_vmkern_esx5_3.7.0.3	\$

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

Host Setup		
Datastore *	datastore1 (1) (411.3GB available)	\$
Free space needed	8GB free space needed on datastore.	
Forwarding vmnic *	None	\$
Tap Setup		
GRE Source IP		
GRE Subnet Mask		
GRE Gateway		
Version to Install *	ixia_vtap_3.7.0.102	\$

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.

ixia								My 210	nie Network	I LOOIS EXPORT	connguration	Expor	t Logs	Hep Lo	ng Uut
	**		alisian Co	- P		11							w	elcome, f	frank
Dashboard	Inventory	,	rolicies Co	nngurabon		Donses									
Policies		For	warding Policies	5											
		1 Forv	varding Port								🕒 New	0	Edit	Dele	lete
			Forwarding Port	٥	Туре Ф	IP Address / VLAN ID	٥	Forwarding-Port Name	¢	Fragmentati	on	• 5	ession	Id	•
			1		GRE	10.100.51.170		SA		true					

Add Formerding V VLAN ERSPAN Type GRE	Forwarding Port 2	×
GRE		
Name*	SA-2	
IP address*	10.100.51.170	
Fragmentation	OTrue False	
	Save	el



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.

💋 Add Network Wizard				
Virtual Machines - Netwo Virtual machines reach n	rk Access networks through uplink adapters attached to vSphe	re standard si	witches.	
Connection Type Network Access	Select which vSphere standard switch will handle vSphere standard switch using the unclaimed net	the network twork adapter	raffic for this connection. You may also create s listed below.	a new
Connection Settings Summary	• Create a vSphere standard switch	Speed	Networks	
	O Use vSwitch0	Speed	Networks	
		1000 Full	10.100.48.1-10.100.55.254	
	Preview: Virtual Machine Port Group visibility Switch	Physical Adapter No adapters	5	
Help			< Back Next	:> Cancel



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.

VMkernel - IP Connection Specify VMkernel IP se	n Settings ttings			
Connection Type Connection Settings IP Settings Summary	C Obtain IP settings automatically C Use the following IP settings: IP Address: Subnet Mask: VMkernel Default Gateway:	· · · · · · · · · · · · · · · · · · ·	Edit	
	Vikemel Port Visability Switch -Virtual Machine Port Group Visibility Switch -VMkernel Port VMkernel vmk1 : 10.100.53.179 Virtual Machine Port Group VMkernel vmk1 : 10.100.53.179 Virtual Machine Port Group VM Network VMkernel Port vmk1 : 10.100.50.189	Physical Adapters		

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.

Hardware Options Resources Virtual Machine Version: 7 Show All Devices Add Remove Device Status Connected Hardware Summary Connected Connected Connected CPUs 2 Video card Video card Adapter Type Current adapter: E1000 E1000 MAC Address Color:29:05:bf:f5 Manual DirectPath I/O Status: Not supported I Network adapter 1 (edite Visibility Switch Network Connection Network Connection Network label: Visibility Switch Visibility Switch Network Connection	FAL_VM3176 Phantom-Management-Server - Virtual Ma	chine Properties
Show All Devices Add Hardware Summary Memory 8192 MB CPUs 2 Video card Video card VMCI device Restricted SS SCI controller 0 LSI Logic Parallel Hard disk 1 Vitual Disk Network adapter 1 (edite Visibility Switch DirectPath I/O Status: Not supported 1 Network Connection Network label: Visibility Switch Visibility Switch Network Connection Network Connection Network Connection Network Connection Network label: Visibility Switch Visibility Switch Network Connection Network label: Visibility Switch Network label: Visibility Switch Network label: Network l	Hardware Options Resources	Virtual Machine Version: 7
Hardware Summary Memory & 192 MB CPUs 2 Video card Video card VIdeo tortoller 0 LSI Logic Parallel Hard disk1 Virtual Disk Image: Network adapter 1 (edite Visibility Switch DirectPath 1/0 Status: Network label: Visibility Switch	Show All Devices Add Remov	e Device Status
Memory 8192 MB CPUs 2 Video card Video card VMCI device Restricted SCSI controller 0 LSI Logic Parallel Hard disk 1 Virtual Disk Network adapter 1 (edite Visibility Switch DirectPath I/O Status: Not supported Network label: Visibility Switch	Hardware Summary	Connect at power on
	Hardware Summary Memory 8192 MB CPUs 2 Video card Video card VMCI device Restricted SCSI controller 0 LSI Logic Parallel Hard disk 1 Virtual Disk Network adapter 1 (edite Visibility Switch	Adapter Type Current adapter: E1000 MAC Address 00:0c:29:05:bf:f5 Automatic C Manual DirectPath I/O Status: Not supported Network Connection Network label: Visibility Switch
Help OK Cancel	Help	OK Cancel

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.

íxia							My Profile	e Network Tools Export Configuration Export Logs Help Log Out
								Welcome, frank
Dashboard	Inventory	Policies	Configuration	Licenses				
vTap Management	Server	Dashboard	d					
WWware Host v S	witch - 10.100.50.189	Overall Status					Compliance Status	
□	□ ⊕ 10.100.50.189	 Host 				1		
⊖ FAL_VM317	7 Microsoft Windows	 vTap D 	eployed			1	20	40 50 60
⊖ RSA_vm310	3_10.5_Packet D	License	d Host			1	-20 80-	80-
		Monitor	red VMs			4	10	Monitora 90
		- Active (Canture Delinu			0	0	VMs 10
		 Active C 	Lapture Policy			1		100%
		 Forward 	uing Port			1		
		Top Talkers			Time Interval 5 Min	🖌 Bytes 🔽	Top Talkers - Monitored VMs	Time Interval 5 Min 🔽 Bytes 💌



Certification Checklist for RSA Security Analytics

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	

Date Tested: March 16 2016

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	V
Various packet data consumed by the SA Packet Decoder	\checkmark
De-duplication	
Replaying data files to the SA Packet Decoder	N/A
Traffic Mapping	
Mapping network service ports to dedicated ports	\checkmark
Performance	
SA Log Decoder minimal EPS performance	
SA Packet Decoder minimal EPS performance	\checkmark

 \checkmark = Pass \times = 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

Install Status	s: 2 out of 2 tapped distributed switches	
vDS	Tap Status	
DSwitch1	Tapped with warnings: • tap is not powered on	

