IXIA PHANTOM VTAP™ WITH TAPFLOW™ FILTERING

DATA SHEET

OVERVIEW

The Ixia Phantom vTap™ with TapFlow filtering is a software solution providing visibility into virtual data center network traffic. The product supports VMware ESXi, Microsoft Hyper-V, KVM virtualization solution for Linux, as well as OpenStack. The Phantom solution supports VLAN, ERSPAN, and GRE tunneling encapsulation for traffic forwarding.

PHANTOM VTAP MONITORING SOLUTION – TAPPING, FILTERING, AND FORWARDING

Security and performance monitoring tools require a complete view of traffic traversing virtual switches. This is typically a challenge as these tools do not have access above the internal virtual switch layer within the hypervisor. The Ixia Phantom vTap monitors all inter-VM traffic and captures only traffic of interest. This capability enables the customer to forward packets to any end-point tool of choice, whether physical or virtual; local or remote, to achieve full visibility and verification across their networks. The Phantom solution does not require any services or agents to be installed in the virtual machine. The Phantom vTap is vSwitch agnostic, supporting VMware vSS, vDS, and third-party virtual switches.

HIGHLIGHTS

- Enables security, availability, and performance through proactive monitoring of virtual data centers
- Provides complete visibility of inter-VM traffic
- Includes a single management interface for the entire virtual visibility system
- TapFlow filtering enables the grooming of virtual traffic to isolate interesting data and prevent network congestion
- Supports multiple hypervisors including VMware ESXi, Microsoft Hyper-V, KVM and OpenStack KVM
- Improves troubleshooting to optimize user experience
- Meets SLAs and compliance requirements (SOX, PCI, HIPAA)
- Helps root cause analysis and reduces mean time to resolution (MTTR)
- Increases ROI and lowers TCO of existing tools

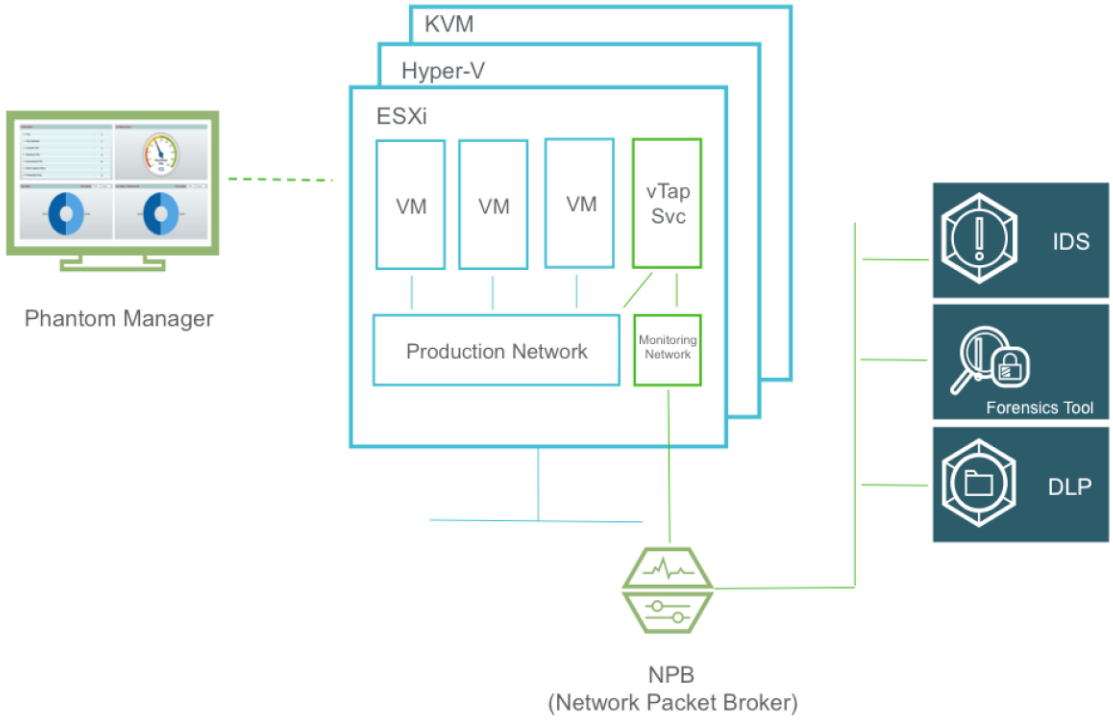
The Ixia Phantom vTap can mirror all traffic within the virtual switch, apply smart TapFlow™ filtering, and send only traffic of interest to any monitoring tools of choice. Virtual traffic is bridged to the physical wire in a GRE- or VLAN-encapsulated tunnel that can be terminated by an Ixia NTO, or any other capable end-point termination tool (physical or virtual) of your choosing. The Phantom solution is an all-in-one solution providing unified, centralized management via a “single pane of glass.” That means you gain total access and control of your security and performance monitoring needs with the product’s easy-to-use web UI.

THE VIRTUAL MONITORING CHALLENGE

Enterprises have been utilizing tap solutions for network traffic access for many years. Traffic capture, analysis, replay, and logging are now part of every well-managed network environment. In recent years, the significant shift to virtualization is yielding great efficiency benefits. However, today’s virtualization-based deployments create challenges for network security, compliance, and performance monitoring. This is because Inter-VM traffic is optimized to speed up connections and minimize network use on the physical core network switches. Such optimization can make traffic invisible to physical tools unable to extend easily into the virtual environments. Costly new virtualization-specific tools plus training can affect the economic benefits and cost-savings of virtualizing. Currently, many tools suffer from limited throughput, hypervisor incompatibility, and excessive resource utilization.

Next-generation data centers use virtualization technology to deploy private/public cloud environments on a single physical server or across a clustered group of servers, local and remote. Traditional taps cannot see the traffic between VMs that reside on the same hypervisor (east-west traffic), nor can they “follow” VMs as they are migrated from one host to another.

Visibility is further reduced by the complexity of blade servers that have each blade running multiple VMs on a hypervisor. Traffic running on blade servers shares a common backplane and creates a network blind spot, since the physical network and its attached tools are unable to see traffic above the virtual switch layer or the blade chassis network modules.



Phantom vTap virtual solution deployment scenario

KEY FEATURES

- Enables complete visibility of east-west, inter-VM, and blade server mid-plane traffic through virtual tapping, filtering and traffic forwarding
- Offers a solution with full access to network packets passing between VMs on hypervisor stack
- Provides TapFlow, multi-layer L2-L4 filtering engine
- Supports multiple hypervisors, including VMware ESXi, Microsoft Hyper-V, KVM, and OpenStack KVM
- Integrates with OpenStack orchestration and management to offer multi-tenancy and Tap-as-a-Service (TaaS) support.
- Supports vSS (virtual standard switch), vDS (virtual distributed switch), and third-party virtual switches for a switch-agnostic solution
- Sends traffic to any existing end-point appliance, physical or virtual (tool agnostic)
- Follows VMs for continuous visibility throughout migration (VM-level monitoring)

- Supports vMotion and DRS
- Enables proactive monitoring and security of virtual data centers
- Optimizes user experience by increasing troubleshooting capabilities
- Meets SLAs and compliance requirements (SOX, PCI, HIPAA)
- Helps resolve root causes to reduce MTTR through visibility and verification
- Allows retention of system resources by eliminating any need to install agents or services on the VM or application layer
- Increases ROI and lowers TCO of existing security and performance monitoring tools
- Allows control of multiple Phantom instances (included software component) for centralized management

SPECIFICATIONS

SUPPORTED HYPERVISORS			
VMware	ESXi 5.0 & 5.1	ESXi 5.5	ESXi 6.0
ESXi - vSwitch (Kernel Module)	Yes	Yes[i]	No
ESXi - vDS	Yes	Yes[ii]	Yes[ii]
ESXi - vSS	No	Yes[ii]	Yes[ii]
Microsoft Hyper-V	Windows 2012 and 2012 R2[iii]		
KVM	v.2.01 and above with Open vSwitch (OVS) 2.0 and above		
OpenStack KVM	Liberty with KVM OVS (see above)		
OpenStack Tap-as-a-Service (TaaS)	Liberty, Mitaka with v2 authentication (Keystone)		

SPECIFICATIONS	
Network Connectivity	Phantom Management Server VM must be accessible via HTTP to access Web UI TCP port 22, 80, 443, and 5989 must be open between Phantom Management Server VM and VMware vCenter server
Disk Storage	Phantom Manager: 4 GB - vTap Service (SVM): 2-4GB – TaaS SVM: 5GB

SPECIFICATIONS	
CPU	Phantom Manager: 2 vCPU - vTap Service (SVM): 1-2 vCPU
Memory	Phantom Manager: 8GB (recommended) – vTap Service (SVM): 512MB to 3GB (Hyper-V), 3GB (ESXi) – Taas: 1GB - KVM (integrated with OVS, no additional resource)
Web Browser	Google Chrome, Internet Explorer, and Firefox

[i] For upgrading existing customer or special cases
[ii] vCenter required (No standalone ESXi)
[iii] Standalone Hyper-V Hosts (No SCVMM)