

VIRTUAL Total Network Visibility

The migration to virtual computing architectures has created a new blind spot in the enterprise: the traffic between virtual servers in the same physical chassis. This “invisible traffic” never crosses any network segment where it can be easily captured. Invisible traffic is a problem for any data center team trying to troubleshoot, optimize, or secure its virtual server operations. You can’t tune what you can’t see. And with enterprises virtualizing more and more of their data center operations, the size of this blind spot is destined only to grow. As a result, network engineers have little or no visibility into the traffic among virtual servers. Until now...

With the combination of Net Optics Phantom Virtual Tap and WildPackets OmniPeek® network analyzer, network engineers have unfettered access to the network and application traffic traversing virtual servers. The Phantom Virtual Tap eliminates the blind spot created by invisible traffic and enables network engineers to use the powerful root-cause analysis capabilities of OmniPeek to troubleshoot, optimize, benchmark, and secure virtual servers and virtual applications.

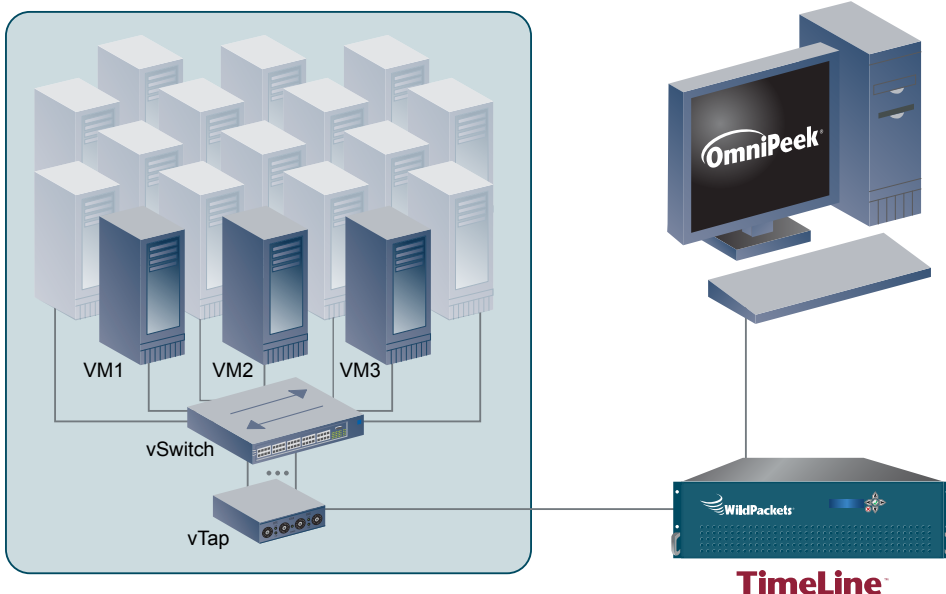
Together WildPackets and Net Optics offer unprecedented network visibility.

Phantom Virtual Tap:

- 100 percent visibility of TCP/IP traffic between Virtual Machines (VMs)
- Follows VMs as they move (vMotion) between physical servers
- Installs in hypervisor kernel for full TCP/IP traffic visibility
- Sends replicated VM network traffic out physical NICs in encapsulated tunnels

OmniPeek network analyzer:

- Gain unprecedented visibility into network and application traffic
- Accelerate find-to-fix times
- Discover and close network security gaps
- Increase end user productivity



The Phantom Virtual Tap can replicate all traffic within the virtual switch, apply smart TapFlow™ filtering, and send traffic directly to OmniPeek for real-time analysis or to distributed Omnipliance® and TimeLine™ network recorders for post-mortem digital forensics.

Phantom Virtual Tap – Innovative, Fault-Tolerant Architecture

Requiring no changes and creating no single point of failure, the versatile Phantom Tap is VMware ESX and ESXi-certified, supporting VMware version 4.x at the kernel level. It aggregates traffic from multiple VMs and performs smart filtering, while offering the high capacity needed to match port density and traffic volumes. The Phantom Virtual Tap integrates kernel-level monitoring into the heart of the hypervisor switching system and enables monitoring and access control in dynamic and distributed virtual environments, as well as supporting “bare-metal” installations whatever the virtual switch vendor.

About Net Optics

Net Optics is the leading provider of Intelligent Access and Monitoring Architecture solutions that deliver real-time IT visibility, monitoring and control. As a result, businesses achieve peak performance in network analytics and security. More than 7,000 enterprises, service providers and government organizations—including 85 percent of the Fortune 100—trust Net Optics’ comprehensive smart access hardware and software solutions to plan, scale and future-proof their networks through an easy-to-use interface. Launched in 1996, Net Optics maintains a global presence through leading OEM partner and reseller networks. For further information about Net Optics’ market-leading solutions visit www.netoptics.com.

OmniPeek – What’s in your network?

Serving a dual role as both a portable network analysis solution and as a software console for OmniEngine™ software probes and Omnipliance and TimeLine network recorders, OmniPeek® offers an intuitive, easy-to-use graphical interface that engineers can use to rapidly analyze and troubleshoot enterprise networks. OmniPeek provides centralized Expert Analysis for all networks under management. Using OmniPeek’s intuitive user interface and “top-down” approach to visualizing network conditions, network engineers can quickly analyze faults from multiple network segments, drill down through multiple layers of analysis, and pinpoint problems that need correction.

WildPackets Distributed Network Analysis

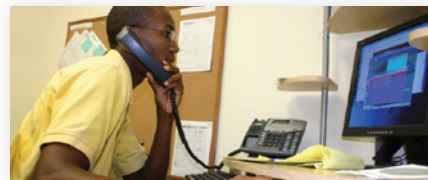
WildPackets gives network engineers real-time visibility into every part of the network—simultaneously from a single interface—including 10/100, Gigabit, 10G Ethernet, 802.11 wireless, and VoIP. Using OmniPeek’s local capture capabilities, centralized console, distributed OmniEngine intelligent software probes, Omnipliance and TimeLine network recorders, and Expert Analysis, engineers can monitor their entire network, rapidly troubleshoot faults, and fix problems to maximize network uptime and user satisfaction.

About WildPackets, Inc.

WildPackets develops hardware and software solutions that drive network performance, enabling organizations of all sizes to analyze, troubleshoot, optimize, and secure their wired and wireless networks. WildPackets products are sold in over 60 countries and deployed in all industrial sectors. Customers include Boeing, Chrysler, Motorola, Nationwide, and over 80 percent of the Fortune 1000. WildPackets is a Cisco Technical Development Partner (CTDP). For more information, visit www.wildpackets.com.



Total Network Visibility



Edge to Core Network Analysis

WildPackets’ solutions enable businesses to

- Gain unprecedented visibility into networks and applications
- Accelerate find-to-fix times
- Discover and close network security gaps
- Maximize ROI on existing networks and applications
- Increase IT efficiency and responsiveness
- Reduce costs associated with network downtime and service degradation
- Reduce IT labor costs
- Increase end user productivity



1340 Treat Blvd, Suite 500
Walnut Creek, CA 94597
(925)937-3200 | fax (925)937-3211
www.wildpackets.com



5303 Betsy Ross Drive
Santa Clara, CA 95054
(408)737-7777 | fax (408)745-7719
www.netoptics.com