NetOptics®

Addressing Monitoring, Access, and Control Challenges in a Virtualized Environment

White Paper

Today, network traffic between Virtual Machines (VMs) is skyrocketing past predictions, while network administrators continue to lag in terms of visibility and control of that inter-VM communication. As this traffic soars to more than 50 percent of all traffic on the network, the security and compliance challenges raised by lack of visibility into the virtualized environment have become acute.

The financial and legal consequences of this visibility deficit are severe and of long duration, with an enormous impact on the business. Data passing between VMs cannot be monitored against intrusion and disruption or captured for auditing; the sources of issues cannot be pinpointed in a timely manner. Headlines blare the shocking statistics of security breaches: huge losses and millions of accounts compromised. Lack of compliance risks heavy fines, costly legal complexities and bad publicity. The inability to fulfill SLAs brings loss of goodwill and customer flight.

For years, traditional Tap solutions were sufficient to help IT professionals effectively manage and protect their complex networks—meeting compliance needs, facilitating traffic capture, analysis, replay, and logging. But no longer. Today and from now on, neither traditional Taps, nor any other conventional solution can capture all the traffic that flows between VMs. IT professionals urgently need a solution that can provide comprehensive visibility of all data passing between VMs and on dedicated backplanes.

NetOptics®

Addressing Monitoring, Access, and Control Challenges in a Virtualized Environment

White Paper

The Challenge of the Virtual Environment

Virtualization consists of deploying several computing environments onto a single server managed by a hypervisor. Hypervisor software manages multiple operating systems (OSs) or multiple instances of the same OS. This allows consolidation of physical servers onto a virtual stack on a single server.

Among the benefits of virtualization are nearly limitless elasticity and expandability that demand fewer resources. In addition, new services can be deployed without procuring new hardware (servers) or installing an OS with all of its associated ongoing costs and management responsibilities.

Traffic between virtual servers residing on the same hypervisor (VM to VM or inter-VM traffic) is managed by virtual switching internal to the hypervisor. In a traditional, non-virtual (physical) network, traffic is "seen" on the wire. In a virtualized environment, however, inter-VM traffic is switched locally on the virtual switch and never gets out to a network wire connected to monitoring tools. Therefore, this traffic is unseen—it is a "black hole" from a monitoring perspective. Inter-VM traffic is invisible to physical security and monitoring devices on blade servers as well, where every blade can host multiple VMs. The connectivity between the blades is a hardware backplane (which is also, in essence, a "black hole"). In a blade server with 10 blades running 20 VMs on each blade, the reality is that 200 VMs are interconnecting essentially unmonitored.

Monitoring tools on the market today are, unfortunately, incapable of providing a comprehensive, raw view of all this traffic because they cannot see that vital internal communications layer within the hypervisor. Solutions such as installing agents on every VM or using spanning virtual switch ports do exist. However, they place a sizeable burden on the hypervisor and still do not provide the full visibility required. Such lack of visibility also creates operational challenge "black holes" in tightly managed and regulated, business-critical, high-speed and high-frequency environments such as trading systems, where latency (delay) is unacceptable. To add an inspection VM on the ESX would be costly, intrusive, and difficult to manage.

Virtual Visibility: "Tried This. Tried That."

Organizations have attempted various solutions to this virtual visibility problem. One of the more common alternatives has been to install clients on virtual machines. These range from sniffers, which capture traffic and direct it elsewhere, to smart clients that capture traffic using smart filters and deliver the monitored streams to another destination. The problem with this solution is that these clients must be installed and images built on every VM. This often results in loss of performance.

Competition has grown white-hot among players in the hypervisor arena. VMware has been the dominant leader in the market, but the entry of Microsoft Hyper-V, among others, makes a hypervisor-agnostic approach the most sensible long-term strategy. In fact, such a strategy can be the key to success and flexibility. An ideal solution:

- Provides complete visibility to virtual network traffic
- Operates without negatively affecting the performance of the virtual environment
- Enables the enforcement of the same stringent compliance regulations across the converged, virtualized, and physical infrastructures
- Integrates with virtualization technologies without requiring architectural changes or a large footprint
- Supports the elasticity of the infrastructure and is able to "follow" machines as they are moved around for optimized performance.

White Paper

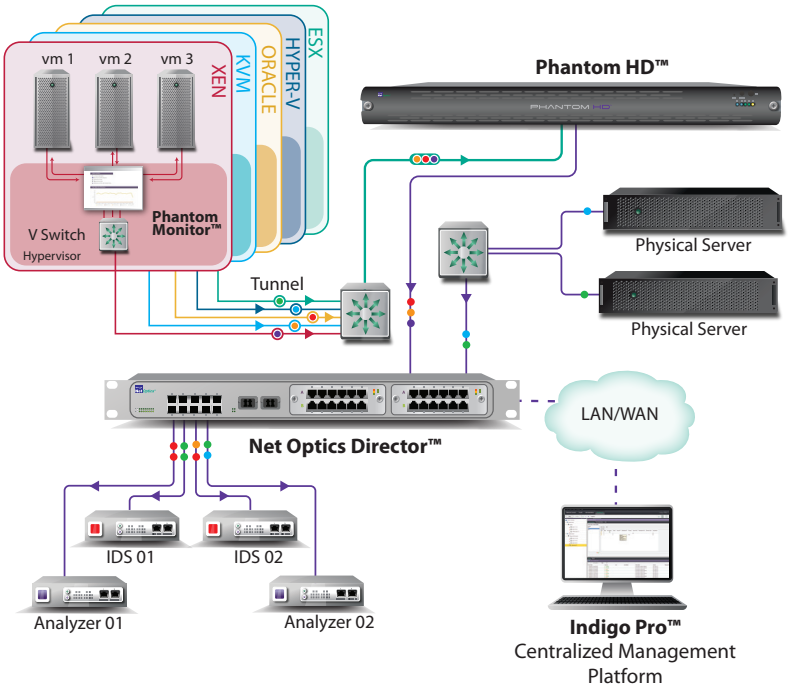

Figure 1. Phantom Virtual Tap

Enter the Phantom Virtualization Tap

To provide complete visibility into traffic flowing between VMs on hypervisor stacks, Net Optics developed the Phantom Virtualization Tap™, which is purpose-built for hypervisors and cloud environments. The virtualization Tapping software is situated low on the hypervisor stack, at the kernel level, as shown in Figure 1 below. As a result, all packets are visible prior to any failures, errors, or other causes of packet loss. Not one packet is dropped or altered by the system.

Furthermore, the Phantom Virtualization Tap can differentiate between specific VM instances in replicated environments and continue to monitor and log individual VMs, even as they move between hypervisor. The Phantom Virtualization Tap is non-intrusive and non-disruptive; it requires no virtual appliances, promiscuous probes, network manipulation, or counterintuitive traffic-shaping and routing. There is no need to modify the existing environment before implementation. Memory and resource demand on the hypervisor are minimal.

Requiring no changes and creating no single point of failure, the Phantom Virtualization Tap supports all best-of-breed hypervisors—including vSphere5, Microsoft Hyper-V, Citrix Xen, Oracle VM, and KVM. These solutions allow running VMs to migrate from one physical server to another with no impact on end users. The Phantom Virtualization Tap continues to monitor traffic and maintain access control, even as virtual instances transition between hypervisor stacks.

For further information about Phantom Virtual Tap:

http://www.netoptics.com
Net Optics, Inc.
5303 Betsy Ross Drive
Santa Clara, CA 95054
(408) 737-7777
info@netoptics.com

Customer First!

Disclaimer: Information contained herein is the sole and exclusive property of Net Optics Inc. The information within this document or item is confidential; it shall not be disclosed to a third party or used except for the purpose of the recipient providing a service to Net Optics Inc. or for the benefit of Net Optics Inc. Your retention, possession or use of this information constitutes your acceptance of these terms. Please note that the sender accepts no responsibility for viruses and it is your responsibility to scan attachments (if any).