NetOptics®

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

White Paper

Driven by the promise of dramatic reductions in the number of physical servers needed (Consolidation ratios of 10:1, 15:1, and even 20:1 have been reported), more and more enterprises are deploying virtualization techniques in their data centers. Virtualization, however, is not without its drawbacks.

One of the biggest challenges is monitoring. Tap solutions have been used for years to facilitate traffic capture, analysis, replay, and logging, helping IT professionals effectively manage their complex networks and meet compliance. But neither traditional Taps, nor any other solution, is able to capture all the traffic that flows between virtual machines (VMs).

This lack of visibility can have an enormous impact on the business, increasing the risk of intrusion and disruption. Data passing between VMs cannot be captured for auditing, and sources of issues cannot be pinpointed in a timely manner. IT professionals need a solution that can provide comprehensive visibility of all the data, including packets passing between VMs.

The Challenge of the Virtual Environment

Virtualization consists of deploying multiple computing environments onto a single server managed by Hypervisor. Hypervisor software manages multiple operating systems 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 endless elasticity and expandability with 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 ESX 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 not seen—it is a black box from a monitoring perspective. As a result, inter-VM traffic is invisible to physical security and monitoring devices.

Monitoring tools on the market today are, unfortunately, not capable of providing a comprehensive, raw view of all the traffic because they cannot see that 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 sizable burden on the Hypervisor and still do not provide the full visibility required. This lack of visibility creates “black holes” in tightly managed, regulated, and mission-critical environments that pose a potential threat to security and compliance. It also creates operational challenges in high-speed, high-frequency environments (e.g., trading systems) where latency (delay) is unacceptable. Alternative solutions, such as adding an inspection VM on the ESX, are costly, intrusive, and difficult to manage.

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 that capture traffic and direct it somewhere to smart clients that capture traffic using smart filters and deliver the monitored streams to some destination. The problem with this solution is that these clients must be installed and images built on every VM. This often creates a loss of performance.

The ideal solution is one that would deliver the following capabilities:

- Provide complete visibility to virtual network traffic
- Operate without negatively impacting the performance of the virtual environment
- Enable the enforcement of the same stringent compliance regulations across the converged, virtualized and physical infrastructure
- Integrate with virtualization technologies without requiring architectural changes or a large footprint.
- Support the elasticity of the infrastructure and be able to “follow” machines as the are moved around for optimized performance (vMotion)

Enter the Virtual Tap

To provide complete visibility into traffic flowing between VMs on hypervisor stacks, Net Optics has developed the Phantom Virtual Tap, which is purpose-built for virtualized environments. The Virtual Tap software is situated low on the ESX stack, at the hypervisor 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.

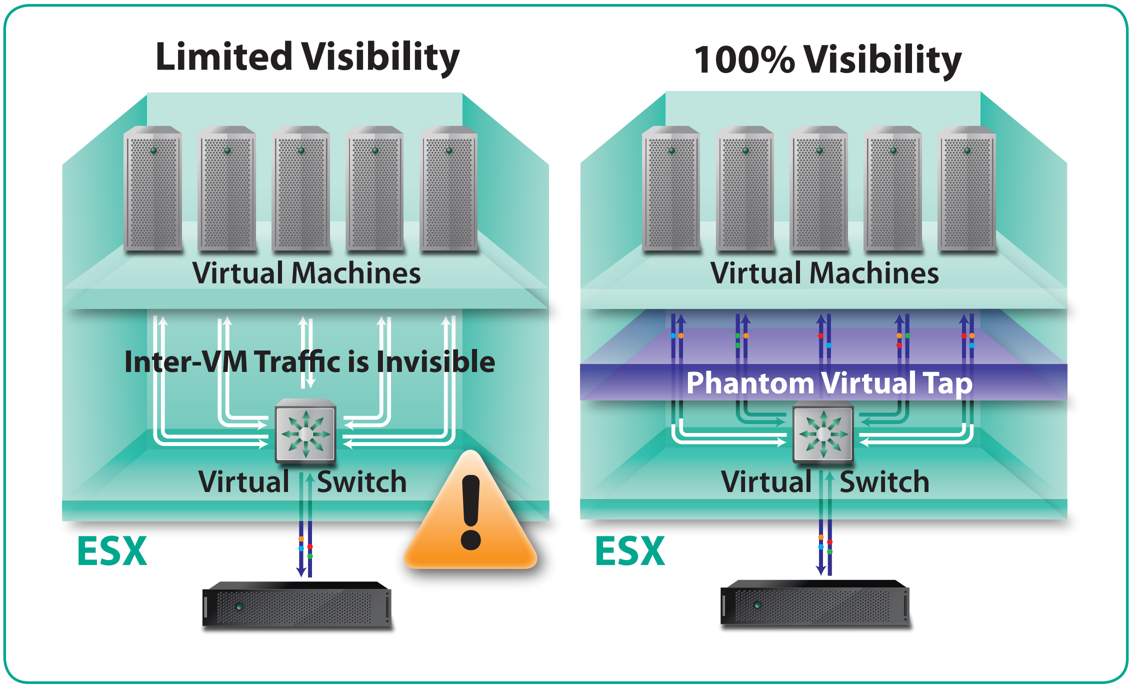

Figure 1. Phantom Virtual Tap

Furthermore, the Virtual Tap can differentiate between specific VM instances in replicated environments and continue to monitor and log VMs, even as they move between hypervisors.

The Virtual Tap is also 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 implementing. Memory and resource demand on the ESX are minimal.

The Phantom Virtual Tap was developed for VMware version 4.x and is both VMware ESX and ESXi 4.x-certified. It is fully integrated at the Hypervisor kernel and supports leading virtual switch solutions, including VMware, DNS, and Cisco.

The Virtual Tap also integrates with VMware vMotion and high-availability/load balancing solutions. These solutions allow running virtual machines to migrate from one physical server to another with no impact on end users. The Virtual TAP continues to monitor traffic and maintain access control, even as virtual instances transition between ESX 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).