

*Visibility and the Virtual Environment:*

# Increasing Real Security using Net Optics' Phantom Virtual Tap

*by Joel Snyder, Senior Partner, Opus One*

Information security practitioners are in an increasing tug-of-war to maintain visibility into the data flowing across enterprise networks. Factors such as the increase in SSL encryption and the highly-switched, highly-redundant, and very distributed nature of data center networks have affected the ability of security tools to see traffic on the wire. When visibility is obscured, tools such as Intrusion Detection/Prevention systems (IDS/IPSeS), Data Leak Protection systems (DLPs), and application-layer and UTM firewalls are ineffective. Network forensics tools don't save useful information, and network performance and debugging tools become ineffective.

The rise of server virtualization has thrown yet another monkey wrench into the machinery used to provide network and security visibility. The fundamental issue is that best practices in server virtualization call for the creation of large clusters of homogeneous virtual host processing elements linked to high speed Storage Area Networks (SANs). The virtualization service manager spreads guest virtual machines (VMs) across these virtual hosts using a combination of resource reservation and load balancing, optimizing use of the virtual hosts and SAN. The server team manages scarce resources of CPU, memory, and disk—and doesn't want to be constrained by network topology, subnets, and VLANs.

In other words, world-class server virtualization almost guarantees that the network and security teams will lose visibility into traffic flowing between guest VMs. Security and network teams can insist that certain types of guest VMs be tied to certain virtual hosts, which would force some inter-VM traffic out a virtual host onto a physical network connection that can be tapped and monitored. However, these constraints de-optimize and reduce the effectiveness of virtualization. That's a heavy "tax" for the server team to pay so that the network and security teams can do their job.

Network and security teams must find approaches to maintain visibility without interfering in the design and deployment of virtual services.

## Gaining Visibility in Virtual Environments

Net Optics' Phantom Virtual Tap is an ideal tool for the security manager who needs visibility in highly virtualized environments. Phantom, especially when used with the Net Optics' Director product, provides the same services that security teams have come to expect from hardware tap and port mirroring technologies commonly used in enterprise networks. Net Optics effectively bridges the gap between physical and virtual environments, re-enabling security tools such as IDS, DLP, and Network Forensics recorders without affecting or complicating the virtual environment.

Unlike alternative approaches to tapping virtual environments, one of the goals of Phantom is to get the packets out of the virtual environment as quickly and as inexpensively as possible. By hooking directly into the ESX hypervisor (only VMware vSphere is supported at this time), Phantom is able to copy packets as they pass between guest VMs with a minimum of overhead. A small virtual machine is placed on each virtual host that receives configuration information and passes selected packets out of the virtual environment, but no significant processing (and thus no performance impact) occurs on the virtual host itself. Phantom also does not put the vSwitch within the virtual host into promiscuous mode, as this would significantly affect performance.

A key feature for taps in virtual environments is support for vMotion, the apparently random movement of guest VMs from one virtual server to another. When Phantom is

installed on each virtual server, the tapping of traffic from selected guest VMs is not interrupted and vMotion events are essentially transparent.

Alternative approaches, such as placing guest VMs with security features onto each virtual server, have an undesirable and expensive performance impact, and greatly complicate existing security and network management environments. These approaches may work in very small virtual environments, but when 10, 50, or more virtual hosts are involved, the only reasonable approach is to use tapping technology that does not impact performance or increase management overhead. Phantom easily meets the requirements of enterprises needing visibility into virtual environments.

## Testing Results

In Opus One's testing of a release candidate of Phantom, we were able to quickly integrate Phantom into a four-node vSphere environment. An important note: while installing Phantom can occur during normal operations, de-installing Phantom does require an ESX server reboot! We configured Phantom using the included central management appliance. Phantom is very well integrated into vSphere, which minimizes the amount of work. For example, Phantom's central management automatically learns all ESX hosts, guest VMs, and virtual networks from vSphere. This simplifies management and helps reduce missed systems and human error.

While the web-based interface is fairly simple, some training is helpful because not every option is where you'd expect to find it. One bonus of the central management appliance is that Phantom taps send Netflow information (which can be distributed to specialized collectors) to the appliance, giving easy access to simple traffic graphs and statistics, such as top talkers and protocols in use on each guest VM.

Each Phantom virtual tap can send selected traffic to up to four devices, encapsulated in a GRE tunnel. Ideally, Net Optics' Director would be used to aggregate and further distribute tapped traffic to security and network performance devices. In our testing, we used a Unix client to receive and de-encapsulate the GRE traffic, a poor substitute for the Director.

One nice feature of Phantom is the ability to define simple IP-based policy on which traffic to tap and which to ignore. This can reduce unwanted traffic sent to security devices (such as internal file sharing or backup traffic, not commonly inspected), or can be used to send different types of traffic to different devices (such as sending debugging traffic for a single host to a protocol analyzer). Even if policy seems excessive, it's actually fairly important, because without careful policy definition, it's easy to get two copies of every packet when guest VMs are on different hypervisors. (When guest VMs are on the same hypervisor, the tap automatically avoids duplicating packets.)

Phantom easily solves the problem of tapping traffic, but it doesn't do anything for the security manager who wants in-line capabilities for network-based IPS or DLP blocking features. Security products that require true in-line placement will require a different technology than Phantom offers.

Phantom will be released March, 2011, and this much-needed add-on should be on the short list for evaluation by every security manager looking for visibility into large virtual environments.

## About Opus One

Opus One has provided IT testing and consulting services in the area of messaging, security, and networking to clients on six continents for thirty years.

