BEST PRACTICE GUIDE

ixia | InSequence

Increased Visibility and Monitoring of Virtual Systems

915-3521-01 Rev. A, August 2014

Table of Contents

Executive Summary

As enterprises and governments continue to move from the use of physical servers to virtualized servers to improve efficiency, the use of resources in its operations and reduce costs, an increasingly large gap is developing in their capabilities to monitor, capture and analyze the network traffic between virtual machines.

Most networks currently use several commercial appliances to monitor, capture, and analyze the traffic on the physical network infrastructure. Unfortunately, if the traffic is between two virtual servers on the same physical host server, the traffic is routed through an internal virtual switch, and is never visible on the physical network to be captured by the current appliances. As they move toward increased virtualization, a major portion of the network traffic will become "invisible" to its current systems, increasing the risk that malicious or unauthorized traffic will go undetected.

Ixia has developed a solution to fill this gap within the virtual architecture and enable the capture of this traffic so that it can be monitored and analyzed using the current tools that network operators are using. Ixia's Phantom Virtualization Tap does not require the connection of a physical device to each host or software agents onto each virtual server. Instead it installs a component in the host's kernel which captures and sends the captured traffic out through a separate network connection for minimal impact to the existing production network. This approach does not interfere with the capabilities of the VMware vCenter product to manage the enterprise VMs. InSequence has installed a Phantom Virtual Tap in its laboratory environment and demonstrated the ability of the solution to capture this inter-virtual server traffic and provide it to the physical network for analysis with readily available tools.

Market research shows there is no other company or competing products that have this capability to install at the kernel level and allow the selective forwarding of captured traffic. The Phantom vTap can provide network operators with the capability to capture the virtual server to virtual server traffic that is being missed today, providing a more complete capability to monitor and protect its network and investment.

Many enterprises and government agencies currently face a growing gap in their capability to capture network traffic for monitoring and analysis to discover network flow problems, and protect the networks from malicious or unauthorized traffic.

Background

Many enterprises and government agencies currently face a growing gap in their capability to capture network traffic for monitoring and analysis to discover network flow problems, and protect the networks from malicious or unauthorized traffic. Specifically, they have already moved a significant portion of their server infrastructure to virtual machines (VMs) and are continuing to virtualize legacy servers and new servers as they are built to improve efficiency and reduce costs. As these servers are virtualized and put on virtual hosting systems that usually host multiple VMs, the network traffic that goes only between VMs on the same host never appears outside the host on the physical network. This traffic flows from one VM to another VM through a virtual switch (Vswitch) internal to the host.

These network operators currently use physical network taps to capture the traffic from the physical network infrastructure which is then fed to network monitoring appliances and computers for monitoring and analysis. The appliances and analysis computers use commercial or open source software tools to analyze the traffic for problems which may affect network performance and unauthorized or malicious traffic. These tools cannot capture data and thus do not receive any traffic that is not present on the physical network infrastructure for monitoring and analysis. As enterprises and governments increasingly move to virtualization, more and more of their network traffic will disappear from the monitoring and analysis screens.

InSequence, a system integrator focusing on federal agencies, is thoroughly aware of the increasing virtualization of the infrastructure as well as the potential vulnerabilities that go with this evolution and began looking for a solution to the problem.

"After some research and discussions with other interested individuals, we discovered the Ixia Phantom product. It was the only solution we could find that would not require a significant change to the VMware vCenter/ESX host architecture (the scenario in question). There are only a few vendors offering for this purpose, and all required modifications to the way the hosts worked within the vCenter infrastructure resulting in increased workloads," said James Filla, President of InSequence Inc.

Following is a list of some of the main features of the Phantom Virtual Tap system:

- vTap is a kernel module which is installed in the ESX kernel, which does not use or affect VM resources
- Does not install any agents or services onto the VMs
- The number of ESX hosts per Phantom HD is limited only by amount of traffic and available bandwidth
- The vTap captures a copy of inter-VM traffic determined by policies & rules created in Phantom Manager
- A dedicated NIC for vTap traffic is recommended on each host
- The product uses Generic Routing Encapsulation (GRE) for traffic thru the dedicated NIC
- Currently supports ESX 5.0/5.1
- Integrates with VM management software to manage multiple hosts
- Using a Network Packet Broker (NPB) such as Ixia xStream allows connections to multiple different tools for analysis

The Evaluation of the Proposed Virtual Traffic Monitoring Capability

In order to evaluate the Phantom solution for virtualized network traffic capture, InSequence decided to use its existing technology research lab environment, which is heavily virtualized, as a test case. This laboratory contains over 40 virtual servers and 8 virtual workstations as well as 5 physical workstations. Ixia agreed to provide the necessary hardware and software for Phantom and a team to help install and then configure the appliance for our network evaluation.

The Lab Environment

The InSequence lab environment was originally created to support an effort to implement a new software management capability using the FlexNet Manager (FNM) Suite for Enterprise software product. In conjunction with the software vendor, Flexera Software, the FlexNet Manager Suite for Enterprise was installed in the lab and work was started on development of installation scripts and software modifications for various customers. The lab environment currently has development, integration and a gold copy of the software that is used by the InSequence team. This gold copy is used to make and export of scripts and modifications to be imported to the product install at the operator's premises.

The InSequence lab environment was originally created to support an effort to implement a new software management capability using the FlexNet Manager (FNM) Suite for Enterprise software product.

Additional software that is used by the customer was also acquired by InSequence and installed in the Lab environment so it could simulate an environment for the testing of scripts and modifications. Software and hardware was also purchased and installed by InSequence to include the emerging Virtual Desktop Initiative (VDI) capabilities of a typical government agency in the environment for the FlexNet scripting and configuration.

Figure 1 shows the lab environment prior to the Phantom Virtual Tap deployment.

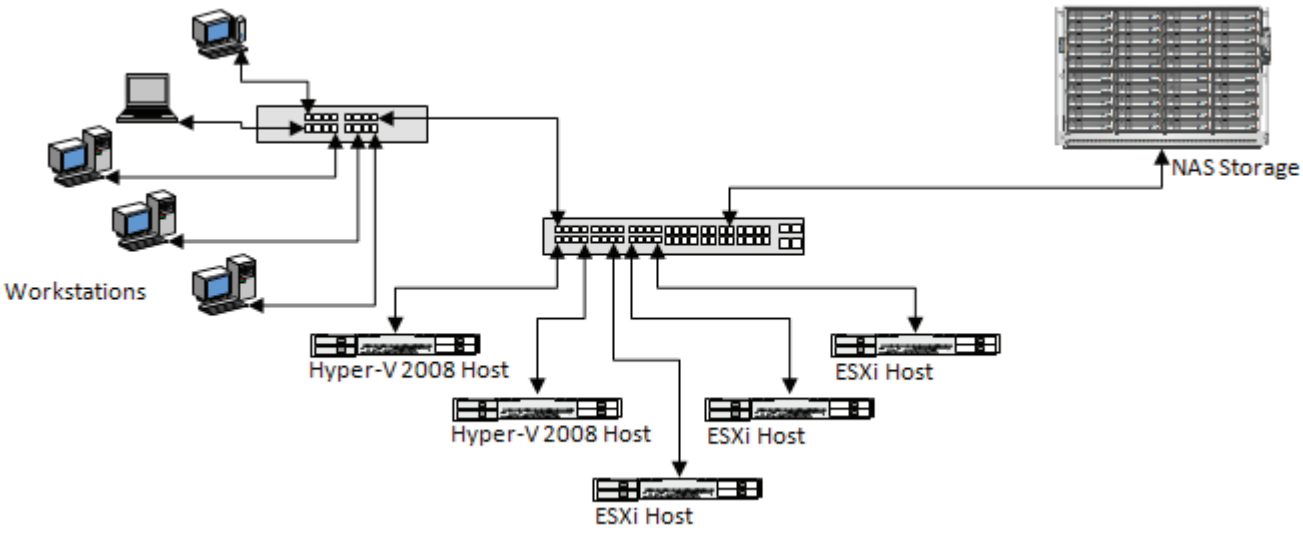

Figure 1 - Lab Environment before Phantom Virtual Tap deployment

Hardware

The following hardware was deployed for the original lab environment:

- Dell R710 servers (4) Dual Quad core (VM Host servers)
- Dell R 520 Server Dual Quad core (VM Host servers)
- Dell OptiPlex 755 workstations (2)
- Dell Pr4ecision 390 workstation
- HP t610 Thin Client (VDI client)
- MacBook Laptop
- Cisco Ethernet Switch
- Dell Ethernet Switch for workstations
- Aberdeen Sterling NAS

Software

The following software list shows the major packages installed to the original lab environment:

- VMware ESXi 5.1 Virtual Hosting operating system (OS)
- Windows 2008 R2 (2) for the Virtual Hosting capabilities (Hyper-V)
- Windows server 2008 R2 for then main OS of most of the server VMs
- Fedora Linux for one of the license servers

- Red Hat Linux for one server
- Ubuntu 10.4 for one of the license servers
- Windows XP for virtual and physical workstations
- Windows 7 professional for several virtual and physical workstations
- FlexNet Manager Suite for Enterprises (components on several VM servers)
- VMware vCenter Essentials for management of ESXi servers
- Microsoft SCM 2007 – for software inventory and management (NGA system)
- XenApp server (several) for supplying applications to Virtual Desktop Infrastructure (VDI) clients
- XenDesktop 5 (for Windows Desktop Thin Clients) Virtual Desktop Infrastructure effort

The Phantom Virtual Tap Deployment to the Lab Environment

Prior to the arrival of the Phantom Tap software, InSequence added the two physical workstations to the lab environment to dedicate as analysis tools for the Phantom captured network traffic. The solution also used an Ixia-provided appliance, Ixia xFilter, that is a rack mounted unit and came completely ready to install and use. It was easy to install into the rack. InSequence replaced the normal 10GbE network interface SPF devices with 1GbE versions for their network. They then connected the dedicated Network Interface Connections (NICs) from each of the ESXi servers to the switch and from the switch to the ingress port on the xFilter, configured the four switch ports into a separate Virtual Local Area Network (VLAN), and connected the xFilter network interface to the Lab environment switch. After, they installed the Phantom Manager virtual appliance. InSequence then used the manager to deploy the virtual tap (vTap) to the ESXi kernel on the three ESXi host servers through the VMware vCenter appliance. No reboot of the ESX hosts was necessary.

Prior to the arrival of the Phantom Tap software, InSequence added the two physical workstations to the lab environment to dedicate as analysis tools for the Phantom captured network traffic.

As supplied, the xFilter appliance is configured with two ingress (input) and two egress (output) ports. The Ixia team reconfigured it for the desired setup of one ingress port and three egress ports for direct connection to analysis stations. Normally the egress ports would be connected to a Network Packet Broker (NPB) appliance which then feed the analysis workstations, but we do not have a NPB in the lab. InSequence wanted to connect three analysis workstations and only needed one, ingress considering the size of the lab network, and since the ingress capability is only limited by network bandwidth.

Several commonly used open source monitoring and analysis tools – including WireShark, JDSU on workstations, and Ntop on a server – were also installed into the test environment. Figure 2 shows the lab environment after the Phantom Virtual Tap deployment.

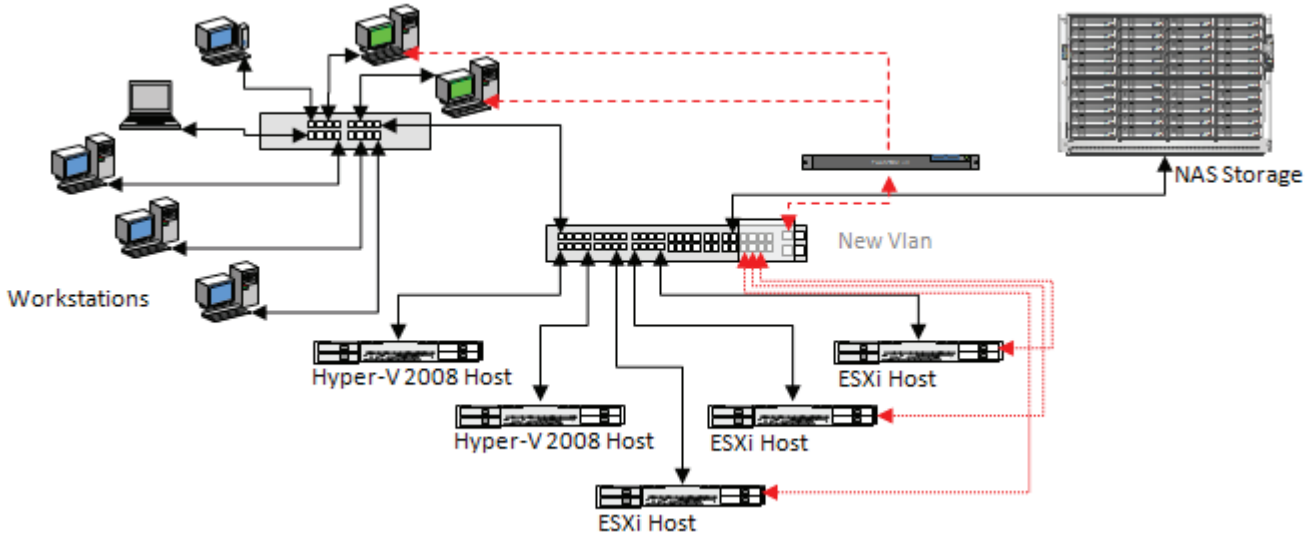

Figure 2 - Lab Environment after Phantom Virtual Tap deployment

Hardware

The following hardware was added to the lab environment for the evaluation and demonstration:

- Ixia xFilter, the basic appliance for distribution of the captured network traffic
- Dell OptiPlex 755workstations for analysis tools.
- Dell PowerEdge 1950 dual core servers (2) for future evaluation of Windows Hyper-V 2012 capabilities

Software

The following software was added for the evaluation and demonstration:

- Phantom Manager virtual appliance to manage the Phantom vTaps
- vTap software to the ESXi hosting kernel software
- Ixia ixChariot network traffic generator appliance VM
- WireShark network monitoring software (workstations)
- JDSU network monitoring software (workstations)
- ntop network monitoring software (Linux server)
- Windows Server 2012 R2 for the Hyper-V capability

The Phantom Virtual Tap Evaluation

InSequence configured the xFilter to collect the traffic from most of the VMs in the lab on the three ESXi hosts through the Phantom Manager appliance web interface (see Figure 3)

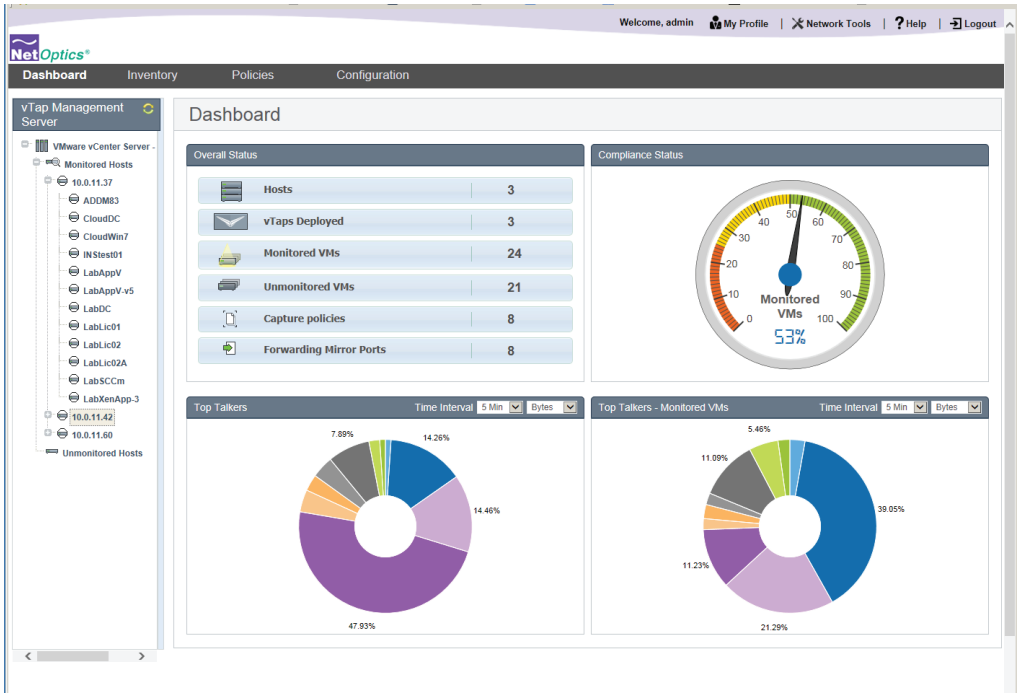

Figure 3 - Phantom Manager Dashboard page showing VMs and Hosts detected and monitored after configuration

Hosts to be managed were selected through the inventory tab from the available hosts automatically discovered through the vCenter server, see Figure 4.

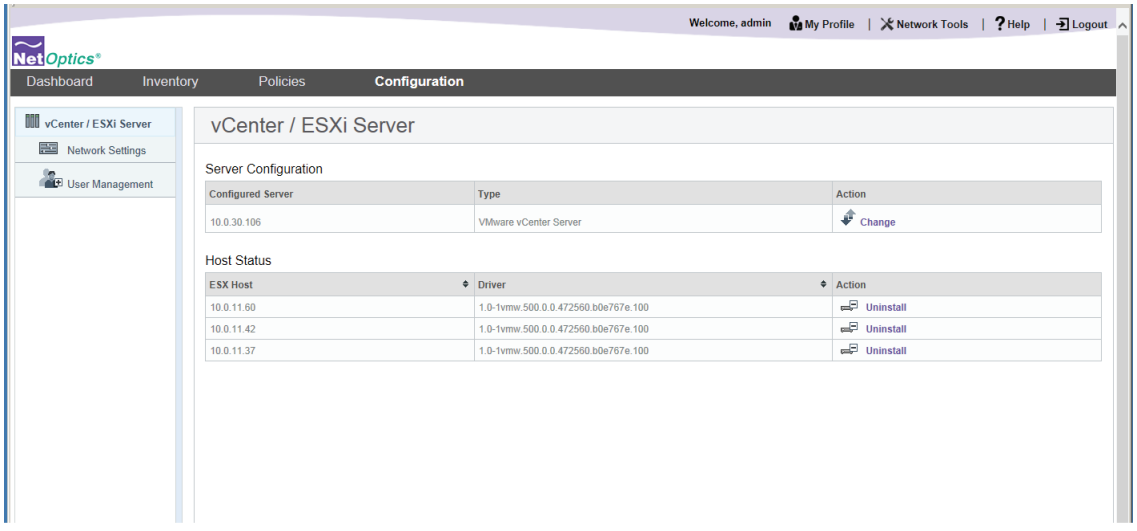

Figure 4 - Determine Hosts to be monitored

InSequence created the policies for forwarding the capture data and which VMs to collect from through the Policies tab. (see Figure 5).

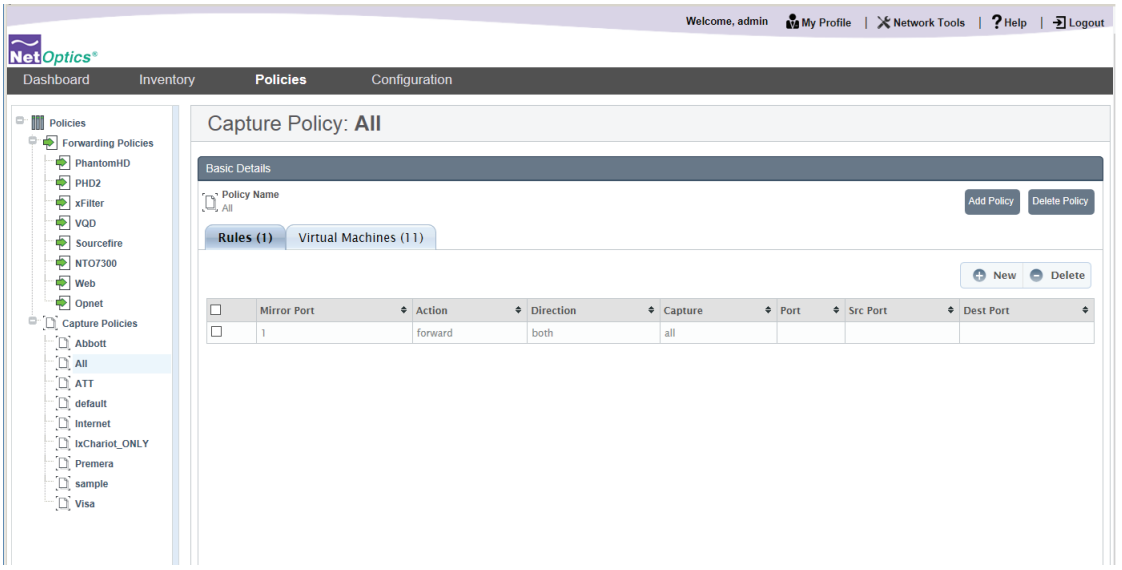

Figure 5 - Create Policies for Data Collection and Forwarding

InSequence then selected the VMs to forward the data from. Again, the VMs were automatically discovered through the connection to the vCenter server (see Figure 6)

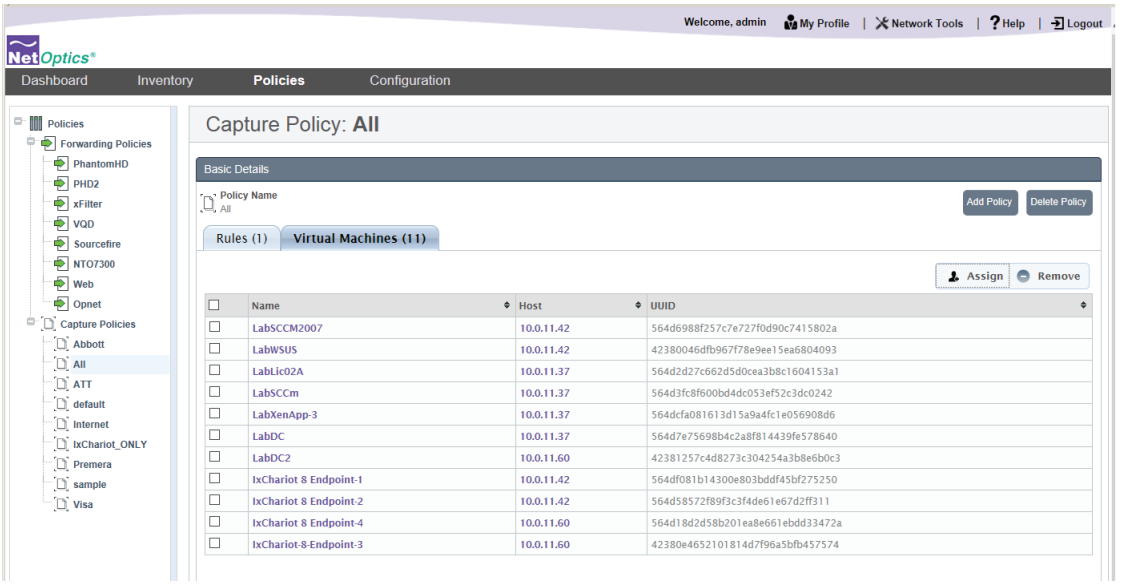

Figure 6 - Selection of Virtual Machines to forward to data collected from

InSequence then confirmed that traffic was being captured from each of the VMs (see Figure 7).

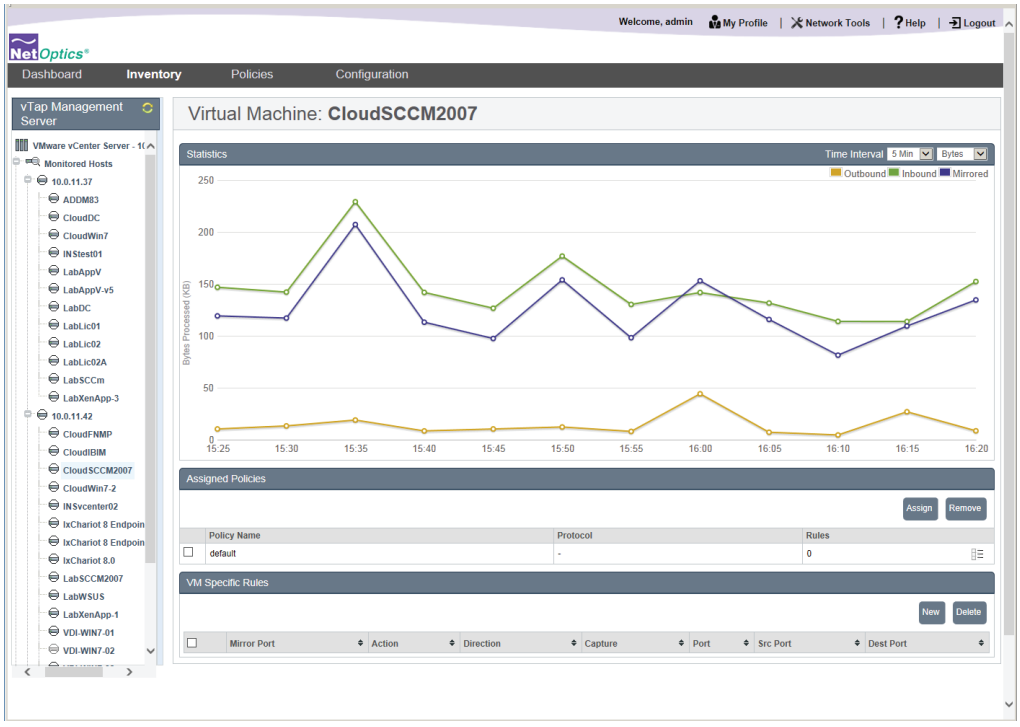

Figure 7 - Phantom Manager page showing traffic statistics for one of the VMs

Next, they wrote a simple script on one existing VM servers to request a file from another existing VM server on the same ESXi host. This script was set to repeat the request until stopped, generating a request once every 5 seconds. InSequence then started two instances of the WireShark tool, side by side on one of the monitoring and analysis workstations. One instance was set to monitor the feed from the Phantom HD appliance. The other instance was set to monitor traffic on the local lab environment physical network connection.

It was clear there was much more traffic on the Phantom HD instance than the local network instance during the same short time period, 5071 vs. 124 packets (see Figure 8). This traffic was inter-VM traffic between VMs on the same hosts and was being captured from all three hosts.

It was clear there was much more traffic on the Phantom HD instance then the local network instance during the same short time period, 5071 vs. 124 packets

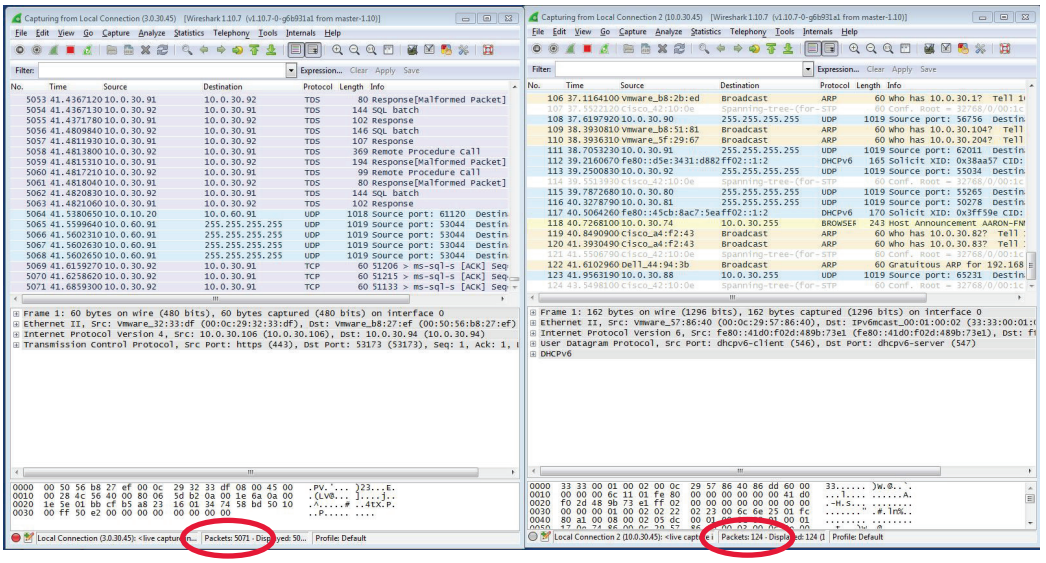

Figure 8 - Comparison of the Phantom HD feed and local Physical network traffic

Next, InSequence applied a filter to each instance to show only the traffic generated by the script generating the inter VM file request. This showed that while the Phantom Virtual Tap was capturing this inter-VM host traffic, none of this traffic was visible to be captured on the local physical network (see Figure 9). This was a clear demonstration of how a virtual tap can expose blind spots and the hidden information within those blind spots.

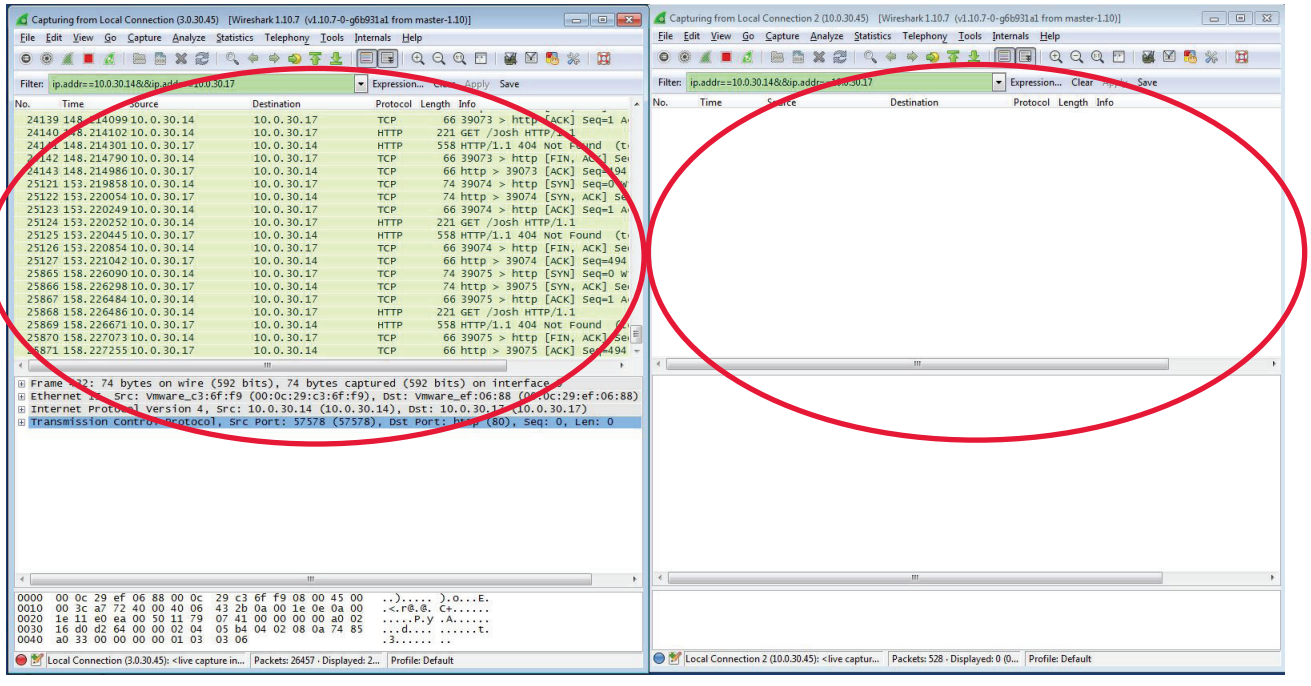

Figure 9 – inter VM Traffic on the same Host is not Available on the Physical Network

Finally, InSequence was able to replicate these results on several different occasions and different monitoring/analysis stations. They also saw the same results using the JDSU and ntop tools on the other monitoring/analysis stations.

Conclusion

Most virtualized data centers are currently not capturing a significant amount of traffic that goes between virtualized servers. This limits their ability to monitor and analyze the complete network traffic for problems and unauthorized or malicious traffic. Couple this with the increasing emphasis within most enterprises and government agencies to tighten up security and administrative privileges across the enterprise in light of recent world events, there is an increasing vulnerability to exploitation within the virtual to virtual communication of the enterprise.

The Ixia Phantom Virtual Tap solution can provide the customer the capability to capture the traffic between virtual servers and other systems that it is currently missing. This can be done in a relatively short period of time and can be done in a phased approach starting with a proof of concept on a single network to demonstrate the utility of the product in helping the customer eliminate the gap of monitoring network traffic between VMs.

As part of any holistic approach to a visibility architecture, InSequence recommends that IT operators see a demonstration of this capability as the first step in moving toward a more secure virtual infrastructure and enterprise. This capability can be demonstrated at the InSequence facility at any time.

Ixia Worldwide Headquarters
26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

Ixia European Headquarters
Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom

Sales +44 1628 408750
(Fax) +44 1628 639916

Ixia Asia Pacific Headquarters
21 Serangoon North Avenue 5
#04-01
Singapore 554864

Sales +65.6332.0125
Fax +65.6332.0127

InSequence
13454 Sunrise Valley Dr.
Suite #210

Herndon, VA 20171

Tel 571.643.0262
Fax 571.643.0269
www.insequenceinc.com

915-3521-01 Rev. A, August 2014