



ELIMINATE NETWORK BLIND SPOTS CREATED BY VIRTUALIZATION AND IMPROVE ROI REALIZATION

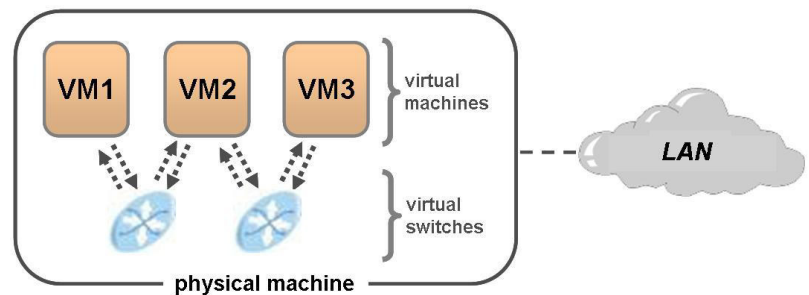
Server virtualization delivers many benefits, including lower hardware maintenance and energy costs, recovered data center floor space, higher availability, reduced disaster recovery costs, faster server deployments, maximized server capacity and increased flexibility for development and testing environments. However, Enterprises are discovering many network traffic and security concerns associated with migrating to virtualized server environments.

Server Virtualization Concerns

Virtualization introduces new challenges for Enterprises to monitor and secure virtual networks. Because virtual machine-to-virtual machine (VM2VM) communications inside a physical server cannot be monitored by traditional network and security devices, this lack of visibility complicates problem identification and resolution, potentially erasing any cost-savings associated with virtual environments. Virtualization creates visibility issues and raises the following questions:

How do I

- ▶ Protect the cost savings gained by migrating to the virtual environment?
- ▶ Identify when a virtual server is generating an excessive amount of traffic?
- ▶ Determine services consumed or served by each VM?
- ▶ Secure VMs without introducing undue administrative burden or performance issues?
- ▶ Track and identify network events that trigger VMotion?
- ▶ Baseline the virtual network to better understand traffic patterns and anomalous traffic?
- ▶ Manage virtual network to limit VM sprawl?
- ▶ Discover misconfigured firewalls?



What Can Be Done to Address These Concerns?

"VM behavioral analysis and monitoring is needed. NAC at VM connection only ensures [that VMs] comply to policy as they connect. A critical part of the NAC process is the ongoing observation of machine behavior to determine if the VM itself becomes compromised." ¹

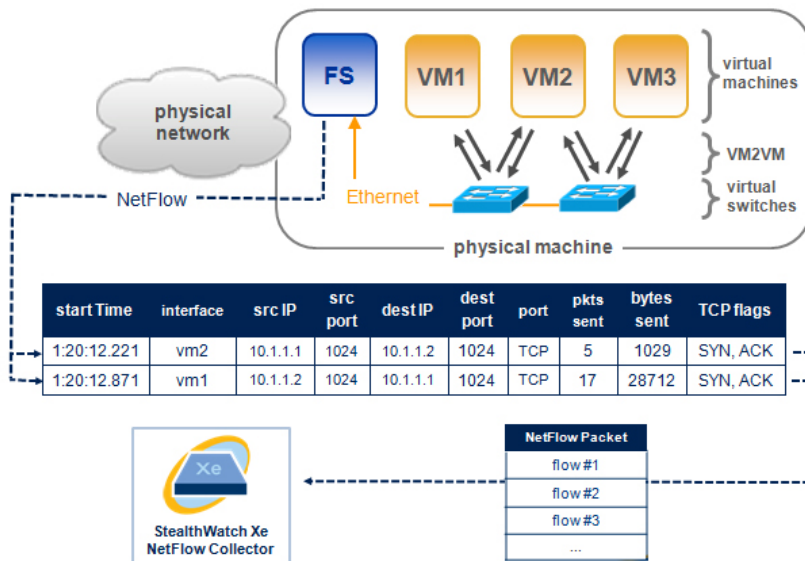
Just as internal security and post-admission controls are necessary elements of any security strategy, so too are monitoring and securing virtual environments. When VM2VM communications should not occur, as is often the case, only a monitoring tool can alarm on this activity, which can be indicative of VM compromise or security policy violation, such as unauthorized VM access. In addition, the ability to mitigate via the VM infrastructure offers efficient and expedient resolution for virtual network incidents.

¹ Gartner, March 6, 2007

Virtualization Blind Spots	Results	Lancope Solution
<ul style="list-style-type: none"> Intra-virtual machine communications (VM2VM) go unnoticed Out of the line-of-site of traditional security and network tools 	<ul style="list-style-type: none"> Compliance issues General inability to audit communications between virtual resources 	Capture and export all communications information from the virtual environment to restore PCI and forensic capabilities
Inability to monitor and troubleshoot network service levels within the virtual environment	<ul style="list-style-type: none"> Finger pointing SLA violations Slow fault reaction time 	Capture key network performance metrics that detail service levels and provide reports designed to troubleshoot virtual network issues
Host security postures go unmonitored and unaccounted	<ul style="list-style-type: none"> Rogue virtual machines Undetected VM2VM attacks License violations Unauthorized applications and/or OSs 	Apply over 160 flow-based behavioral algorithms to the virtual environment, enabling detection of a wide range of network attacks and policy violations

How It Works

The StealthWatch FlowSensor™ VE, deployed on each virtual server, captures traffic, security, user and application behaviors within NetFlow v9 templates. These VM2VM communications contained within lightweight NetFlow PDUs but hidden from traditional physical network monitoring solutions, are then sent out of the virtual server across the network to the StealthWatch Xe for NetFlow collector. As flows arrive at the collector, StealthWatch performs behavior analysis to reveal network congestion issues, policy violations, worm outbreaks and other security and traffic volume related incidents. Because the majority of processing and analysis occurs at the collector rather than within the Virtual Flow Sensor itself, virtual server resources are conserved and virtualization cost savings protected. A single StealthWatch Xe for NetFlow collector supports up to 1000 VMs simultaneously.



About Lancope, Inc.

Lancope®, Inc. is the leader in NetFlow Analysis and the provider of the StealthWatch® for flow-based anomaly detection and network performance monitoring. Delivering unified visibility across physical and virtual networks, StealthWatch eliminates network blind spots and reduces total network and security management costs.

Lancope Headquarters

3650 Brookside Parkway
Suite 400
Alpharetta, GA 30022

+1.770.225.6500 (US)
888.419.1462 (Toll Free)
+1.770.698.8827 (International)

Website: www.lancope.com

E-mail: sales@lancope.com

©2009 Lancope, Inc. All rights reserved. Lancope, StealthWatch, and other trademarks are registered or unregistered trademarks of Lancope, Inc. All other trademarks are properties of their respective owners. StealthWatch is covered by U.S. Patent Nos. 7,290,283; 7,185,368; 7,475,426; 7,512,980 and other U.S. and foreign patents pending.

DS11182009