WHITE PAPER

Illuminating Data Center Blind Spots

New Approaches to Overcoming Access and Visibility Deficits in the Virtualized Environment

915-6636-01 Rev. A, July 2014

Table of Contents

New Approaches to Overcoming Access and Visibility Deficits in the Virtualized Environment 1

Abstract 4

Momentum: Virtualization's Biggest Challenge 4

Hunting the Blind Spot 4

SPAN Port Shortfalls 6

The IT Visibility Wish List 6

Visibility Approaches That Work: Monitoring, Access, and Control in a Virtualized Environment 7

Enter the Phantom vTap 7

A Multipurpose Virtual Visibility Solution 7

Summary 8

Abstract

Server virtualization has seen phenomenal acceptance and growth throughout recent years. This innovation promises even greater efficiencies of shared resources (CPU, RAM, Storage), cost savings, and flexibility to come. Making better use of x86 computer/server systems to meet a burgeoning set of demands promises substantial benefit—as long as visibility and other challenges can be overcome. With up to 80 percent of data center traffic now traveling between VMs within the same hypervisor, end-to-end visibility has become a major concern. This paper details strategies to give users confidence that their virtualizing data centers offer full visibility into inter-VM ("east-west") traffic, so that the organization can realize the tremendous benefits of virtualization.

Momentum: Virtualization's Biggest Challenge

As virtualized environments expand and mature, it is vital that system administrators have constant access to reliable information on how data are being used. Virtualization deploys several computing environments onto a single server, which is then managed by a hypervisor. This hypervisor's software is able to manage several operating systems and enable consolidation of physical servers onto a virtual stack on a single server.

As virtualized environments expand and mature, it is vital that system administrators have constant access to reliable information on how data are being used.

Among the benefits of this approach are nearly limitless elasticity, shared expandability, and the need for 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.

Among the drawbacks is the growing concern of virtual machine "sprawl" that arises from the ease of virtual machine (VM) creation and cloning. As VMs are added, the task of keeping track of them grows difficult. Unmanaged VMs may also be running obsolete security policies or software that has not been appropriately upgraded.

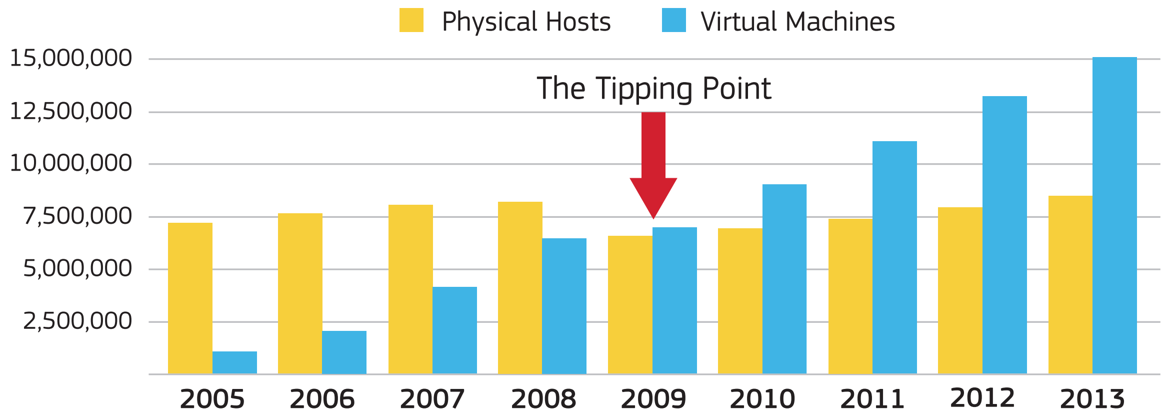
Just as with physical networks, access audit trails are necessary in the virtualized environment to document compliance with regulations. Also, because virtual machines can act as file shares, databases, web servers, application servers, etc., Virtual environments require the same access control and identification measures needed for physical servers.

Hunting the Blind Spot

The most daunting downside to virtualization is inarguably the "blind spot." In the network, a loss of visibility into the functions and traffic flow between guest VMs is common on a virtualized host. Blind spots are a favored "hangout" for malicious intruders; performance issues lurk there unsuspected as well.

When visibility is obscured, tools such as Intrusion Detection/Prevention systems (IDSs and IPSs), Data Leak Protection systems (DLPs), and application-layer and UTM firewalls become far less effective. Network performance and debugging tools cannot see into the virtual switch layer.

Applications On Virtualized Infrastructure



Source: IDC

The statistics of security breaches caused by lack of visibility blare from the headlines nearly every day, with huge financial losses and tens of millions of accounts compromised. This is indisputable evidence that a new solution is necessary. Additionally, lack of compliance risks heavy fines, costly legal complexities and bad publicity. With customers increasingly expectant of their SLAs, high availability and seamless performance, loss of visibility risks loss of goodwill and consequent customer flight.

Most data center traffic used to flow between servers and the Internet ("north-south") traffic. But the growth of virtualization, the demand for ever-higher bandwidth, and the drive toward 10G has changed that path, so that a majority of new traffic is local communication within the data center. This is referred to as "east-west" traffic, e.g., VM migration and access to local storage.

East-west traffic between two VMs on the same virtual server is notoriously tricky to monitor. Customarily, traffic would be visible on the wire connected to the monitoring tools. This would make it relatively easy to segment network traffic using dedicated hardware for different applications, data sets, and departments.

Under virtualization, however, balancing loads efficiently and separating network traffic becomes more of a challenge. VMs move between physical servers, increasing the possibility of untrusted VMs communicating with sensitive VMs on the same virtual switch. Under virtualized conditions, Inter-VM traffic is managed by the hypervisor's virtual switch technology (virtual standard switch, virtual distributed switch, or other 3rd party virtual switches), and never gets out to the physical wire at all – or to the third-party monitoring tools. So unseen Inter-VM traffic constitutes a blind spot that is simply invisible to tools and, as a result, goes unmonitored.

Under virtualization, however, balancing loads efficiently and separating network traffic becomes more of a challenge.

In point of fact, there are even more ways in which monitoring tools can become blinded in a virtualized environment. For traffic on blade servers, in which each blade hosts multiple VMs, the connectivity between blades is a hardware backplane (another potential blind spot). A blade server with 10 blades running 20 VMs on each blade totals up to 200 unmonitored VMs!

All of these factors limit or prevent actionable information from reaching the tools. Monitoring plans also fall behind in migration cycles; overwhelmed systems make it hard, if not impossible, to keep up with traffic and filter data at rates that they were not designed to handle.

Virtual machine security requires technologies designed specifically to protect and monitor this layer. These are highly scalable resources that illuminate the blind spot while providing control and minimizing network complexity. Ideally, such an approach would allow IT administrators to continue using current security and performance monitoring tools to optimize the substantial investment in these tools.

SPAN Port Shortfalls

Running in promiscuous mode is the virtualization equivalent of physical network SPAN ports. Malicious intruders can set this mode on a network device to capture private information not intended for them. Promiscuous mode degrades performance, opens up a world of possible security breaches, and offers no way to filter specific traffic – a major red flag for multi-tenancy environments.

The need to proactively detect and resolve performance issues is further complicated by the many tools, probes, interfaces, processes, functions, and servers involved. This complexity, added to overburdened tools, overwhelms infrastructure defenses. The result is even more unmonitored data areas.

Network and security teams need visibility without interference—a way for traffic of interest to be exported from VMs to monitoring tools.

The IT Visibility Wish List

Network and security teams need visibility without interference – a way for traffic of interest to be exported from VMs to monitoring tools. Such a solution would terminate GRE headers and allow for full inspection and audit of network packets in unaltered (raw) state to meet SLAs and comply with regulatory mandates.

In their efforts to solve this virtual visibility problem, organizations have explored adding an inspection VM on the ESX – which turns out to be costly, intrusive, and difficult to manage. As an alternative, installing clients such as sniffers on virtual machines could capture traffic and direct it elsewhere; smart clients could capture traffic using smart filters and deliver the monitored streams to another destination. However, these clients must be installed and images built on every VM. This mandate places a sizeable burden on the hypervisor, strains performance, and still fails to provide the total visibility required.

Such approaches 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 tactics 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 affect performance or increase management overhead. The Ixia Phantom vTap easily meets the requirements of enterprises needing visibility into virtual environments.

Today, vendors are competing to provide visibility solutions that can serve the white-hot demand for total traffic visibility in virtualized networks. The solution must:

- Operate without negatively affecting the performance of the virtual environment.
- Enable regulatory enforcement across the converged physical and virtualized infrastructures
- Integrate smoothly with virtualization technologies and not require architectural changes or add a large footprint.
- Support the elasticity of the infrastructure and “follow” machines as they are moved around for optimized performance.

Visibility Approaches That Work: Monitoring, Access, and Control in a Virtualized Environment

In the past, traditional taps 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.

Enter the Phantom vTap

Now, Ixia's Visibility Architecture delivers a new perspective on network visibility. As part of that architecture, the Phantom vTap captures data passing between VMs and sends traffic of interest to physical or virtual monitoring tools. Supporting major hypervisors, this tap can mirror traffic of interest by using TapFlow filtering, and then send only traffic of interest to any monitoring appliance of choice.

The Phantom vTap effectively bridges the gap between physical and virtual environments, enabling security tools such as IDS, DLP, and Network Forensics Recorders without affecting or complicating the virtual environment. A major goal of the Phantom vTap is to get the packets out of the virtual environment in real time with the least amount of impact on the virtual switch. The tap can mirror packets as they pass between guest VMs with a minimum of overhead and no significant processing (and thus no performance impact) on the virtual host itself.

The Phantom vTap works in conjunction with a portfolio of high-performance network taps, bypass switches, network packet brokers (NPBs) and monitoring tools. The purpose of the architecture is to speed application delivery and effective troubleshooting and monitoring for network security, application performance, and service level agreement (SLA) fulfillment—and to allow IT to meet compliance mandates. The Ixia Virtual Visibility Framework provides a single platform for virtual visibility and troubleshooting. It enables inter-VM traffic monitoring to help eliminate blind spots using existing network, application, and security visibility tools.

Used with a network packet broker, the Phantom vTap provides the superior functionality that security teams always received from the hardware tap and port mirroring technologies used in enterprise networks.

A Multipurpose Virtual Visibility Solution

Used with a network packet broker, the Phantom vTap provides the superior functionality that security teams always received from the hardware tap and port mirroring technologies used in enterprise networks. The tap integrates directly into the hypervisor kernel and rests low on the hypervisor stack. This allows full access to the entire network stack, without the performance penalty of running the vSwitch in promiscuous mode and prevents loss of important network-layer errors, which may be cleaned before sharing in promiscuous mode. Such errors may actually hold the key when troubleshooting a performance or interoperability issue.

As a result, all packets are visible prior to failures, errors, or other causes of packet loss. Furthermore, the Phantom vTap can differentiate between specific VM instances in replicated environments, monitoring and logging individual VMs, even as they move among hypervisors. Because its VM-based monitoring follows the Universally Unique Identifier (UUID) of the VM, the Phantom vTap offers the same network visibility as that which is pre-defined from the source location.

Finally, the Phantom vTap is tool agnostic, allowing network packets to be sent to any existing security or performance monitoring tool; it accomplishes this by means of direct connection with a network packet broker switch. This approach allows application of smart filters to packet streams so that only data of interest is sent to downstream management systems.

The Phantom vTap is non-intrusive, non-disruptive, and hypervisor-agnostic. 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 vTap supports all best-of-breed hypervisors. It continues to monitor traffic and maintain access control, even as virtual instances transition between hypervisor stacks.

Summary

The Ixia Visibility Architecture's Phantom vTap represents a ground-breaking advance in restoring lost visibility into virtualized server infrastructure consistent with best practices for effective monitoring. This approach has proven the most promising for establishing rigorous network management visibility and control over sprawling virtual server infrastructures. In short, the Phantom vTap is a major step towards mainstreaming server virtualization.

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