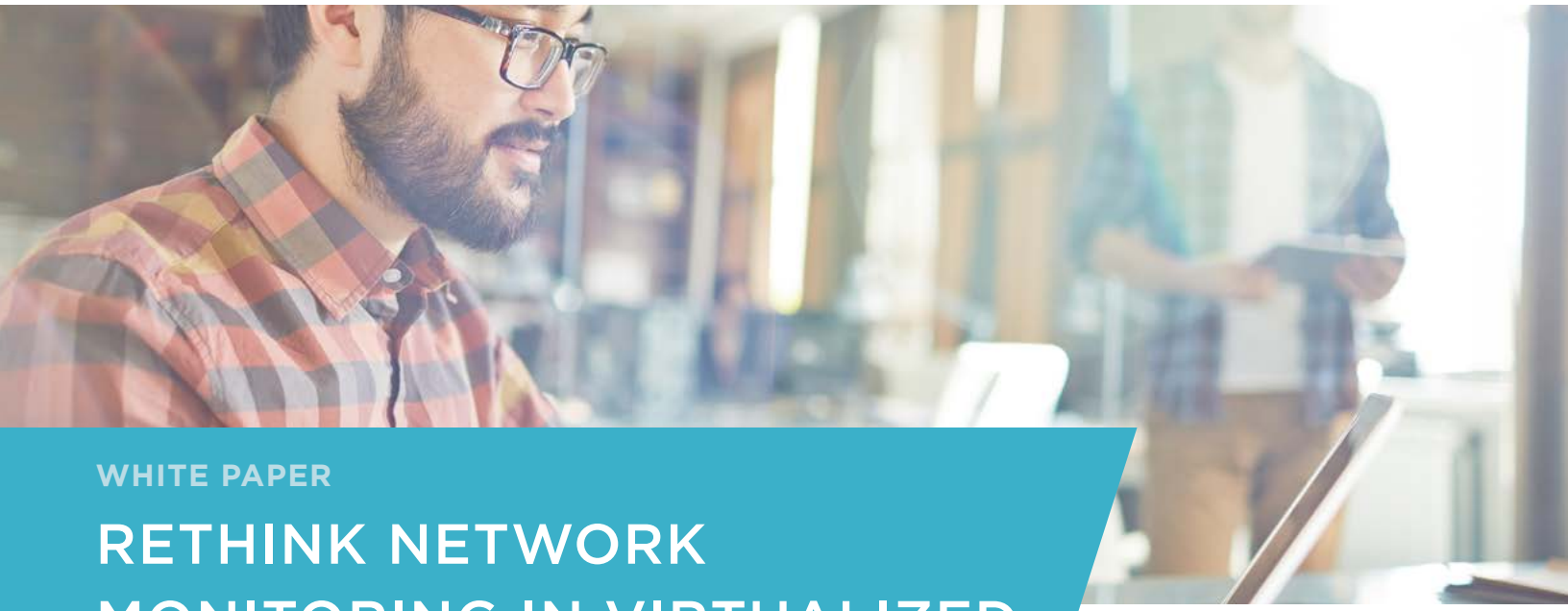
ixia



WHITE PAPER

RETHINK NETWORK MONITORING IN VIRTUALIZED ENVIRONMENTS

FIVE WAYS TO COPY VIRTUAL APPLICATION TRAFFIC

How to tap virtual machine packets so you can deliver them to security and network monitoring tools

Today, server virtualization accounts for a large percentage of compute resources. In 2015, 75% of workloads were virtualized.[1] A little less than 1 in 10 businesses claim greater than 90%.[2] Some organizations proudly boast 100% virtualization. No matter where you are with virtualization, one thing is true – the greater your percentage of virtualization, the more you have to rethink network monitoring to maintain application performance, security, and compliance. As you increase the percentage of virtualized servers, you should consider transitioning from physical to virtual monitoring tools. This means moving out-of-band analytical tools closer to your application data. This will lead to improved flexibility and efficiency.

OUR GOAL

TO HELP GUIDE YOU TO AN OBJECTIVE NETWORK MONITORING STRATEGY THAT FITS YOUR VIRTUALIZED ENVIRONMENT.

In the physical world, application traffic is analyzed by capturing copies of production traffic. The copies are forwarded directly to analysis tools or to a dedicated monitoring network physically separated from the production traffic. The separation of monitoring from production network traffic makes it possible to limit the impact on the production environment to a one-time physical topology or switch configuration change.

In virtual compute environments, a significant portion of the network traffic never hits a physical link. Much of the VM to VM communication is buried deep inside of physical hosts. This VM to VM traffic, sometimes referred to as east-west traffic (server to server), creates blind spots for your network performance and security monitoring tools. Ultimately, the same network monitoring tactics used in a physical environment will not work in a virtual one.

Another obstacle is the inability to isolate production from monitoring traffic. In a virtual environment, there are compute costs and possibly I/O tradeoffs to consider when making copies of the VM's network traffic. CPU, memory, and network resources available to applications are also used to capture and process the monitored traffic. In the end, while the requirements on security and monitoring have not changed, the ability to secure and monitor traffic has.

In 2011, Gartner predicted that up to 80% of traffic in the data center would be east-west traffic by 2014.[3] Gartner's estimate in 2011 appears to be the norm today. According to Cisco, about 73% of data center traffic will come from within the data center by 2019.[4] If you only have physical network monitoring in place, your network, application, and security monitoring tools may see only 20-25% of the traffic in your data center. This is your blind spot and it could limit your tool's vision into an application's poor performance or fail to spot malicious agents. To eliminate blind spots, monitoring tools need access to VM traffic no matter where it originates, terminates, or travels in between.

IN 2015, 75% OF WORKLOADS WERE VIRTUALIZED.

GARTNER

BY 2019, 73% OF DATA CENTER TRAFFIC WILL COME FROM WITHIN THE DATA CENTER.

CISCO

PHASES OF VIRTUAL MONITORING

Virtual monitoring is accomplished in phases:

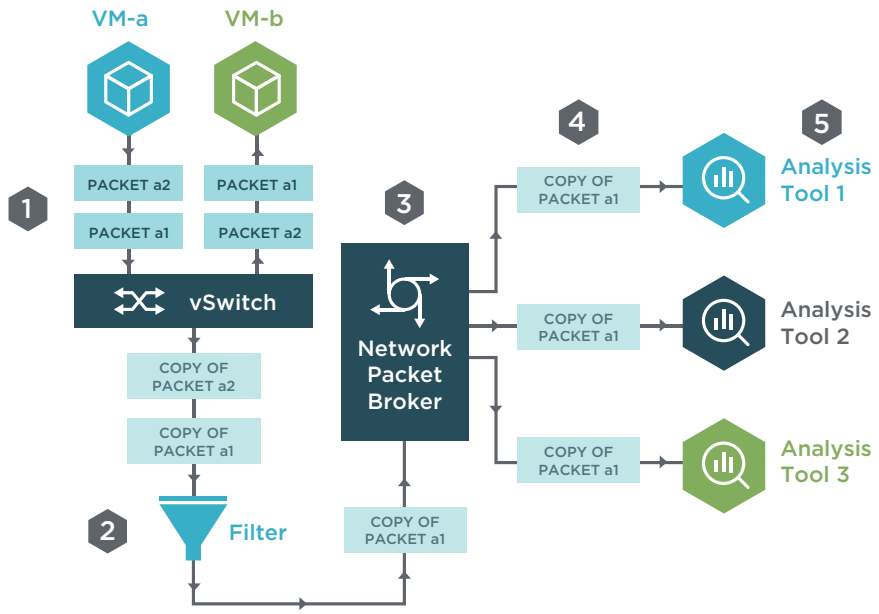
1 *Copy traffic from the VMs of interest* – Configure the vSwitch or virtual switching layer to copy VM traffic. An alternative approach is to add a packet capture agent to the monitored VM.

2 *Perform basic filtering* – Filtering virtual traffic before it impacts host resources is an important consideration in any production-scale deployment. East-west traffic can be many times larger than north-south traffic entering and exiting the host. Thus, too much monitored traffic can quickly overwhelm a host's I/O if you are not careful.

3 *Perform advanced packet manipulation and grooming* – Advanced and intelligent visibility consists of packet manipulation, advanced packet grooming, and brokering. This phase can lead to much greater tool efficiency and additional security protections.

4 *Deliver the filtered and groomed traffic to analysis tools* – Effective monitoring requires efficient delivery of copied network traffic to either physical or virtual analysis tools. In some cases, analysis may be done on the same host or may need to exit the host using a tunneling protocol.

5 *Analyze the traffic for insights* – Out-of-band security and performance monitoring tools capture packets for analysis and alerting. Inline security tools analyze packets for threats.



ANALYZING ACTUAL PACKETS OFFERS THE BEST WAY TO UNDERSTAND WHAT IS GOING ON.

NOTE: This white paper focuses solely on Phases 1 and 2.

VIRTUAL MONITORING CHALLENGES

It can be challenging to find the right balance of system resource usage for virtual applications versus virtual monitoring. Increased visibility in the host will in turn take processing, memory, and network bandwidth away from the monitored applications. There are three important rules of monitoring that will guide the monitoring options presented and should guide you as you develop your virtual monitoring strategy.

1. Applications have priority. Monitoring is secondary.
2. Monitoring should minimally affect the operation of the application.
3. Monitoring should not add additional failure nodes to the application.

Analyzing actual packets offers the best way to understand what is going on. There are other indirect ways to monitor applications and user experience, such as analyzing logs and metadata. Consider these indirect methods only as a complementary solution or as a secondary option when virtual tapping is unfeasible. This paper will focus solely on packet-based monitoring. For concept and reading ease, we will use the term packet to describe frames or packets.

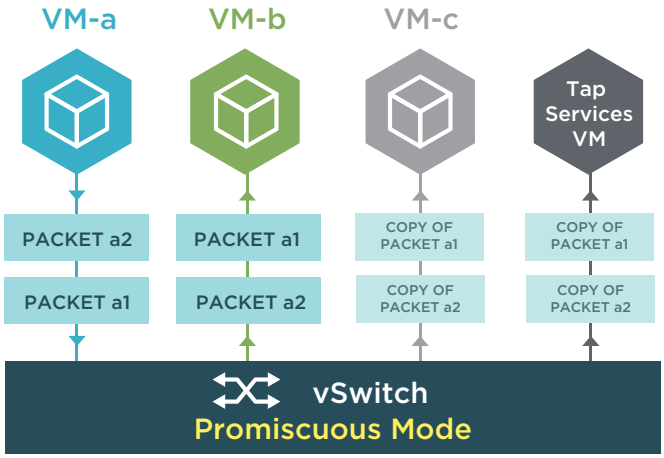
FIVE WAYS TO COPY VIRTUAL APPLICATION TRAFFIC

There are a number of vSwitches available for use in a variety of hypervisors. Each has its own set of capabilities. For this paper, we will focus on the most commonly used in VMware and KVM. In VMware, they are the virtual Standard Switch (vSS) and virtual Distributed Switch (VDS). In KVM environments, the most common is Open vSwitch (OVS). We will explore five options available today as potential virtual tapping solutions. The five options are listed in no particular order.

OPTION 1

ADDING A TAP SERVICE VM TO A MONITORED HOST USING vSWITCH PROMISCUOUS MODE

This option copies all vSwitch traffic and forwards it to a tap services VM running on the host. To do this, the vSwitch uses a technique called promiscuous mode. Promiscuous mode essentially copies all traffic on the vSwitch and forwards it to the tap services VM. Once the tap services VM has received the packet, basic filtering and local analysis can be performed.



A SECURITY NOTE ABOUT PROMISCUOUS MODE

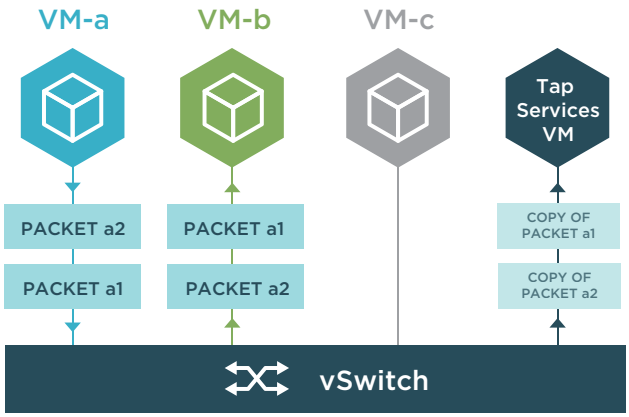
Placing a vSwitch in promiscuous mode has the similar effect to replacing the vSwitch with a virtual hub. This means any VM connected to that vSwitch could listen to all traffic regardless of destination. In addition, a VM's virtual network adapter typically operates by filtering-out frames not intended for the VM before sending it to its CPU. For the tap services VM to receive all traffic, normal filtering performed by the virtual network adapter is disabled. As a result, enabling promiscuous mode on a vSwitch should be done with great care and planning.

ENABLING PROMISCUOUS MODE ON A VSWITCH SHOULD BE DONE WITH GREAT CARE AND PLANNING.

OPTION 2

ADDING A TAP SERVICE VM TO A MONITORED HOST USING vSWITCH PORT MIRRORING

This option copies select vSwitch traffic and forwards it to a tap services VM running on the host. To do this, the vSwitch uses a technique called port mirroring. Configure a port on the vSwitch to receive mirrored copies of traffic (destination port) from another port (source port). Once the tap services VM has received the packet, basic filtering and local analysis can be performed.



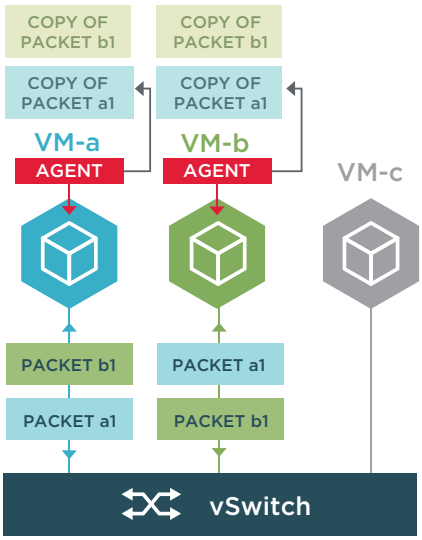
OPTION 3

ADDING A TAP AGENT TO A MONITORED VM

This option uses the monitored VM itself to copy packets moving through the virtual network interface controller (vNIC). To do this, add a tap agent into an application or into the operating system (OS) on each monitored VM, which will sniff the network data moving to and from it. This process is commonly known as packet capture (PCAP) or remote packet capture (RPCAP).

This option works well in virtual environments where you do not have control over the vSwitch. This is common in public cloud environments. It also natively supports VM motion as the VM's vNIC performs the packet capture and copy. However, capturing and copying packets on the monitored VM directly affects the monitored application. Basic filtering is also limited as multiple VMs may store a copy of the same packet.

ADDING A TAP AGENT WORKS WELL IN VIRTUAL ENVIRONMENTS WHERE YOU DO NOT HAVE CONTROL OVER THE VSWITCH.



ixia

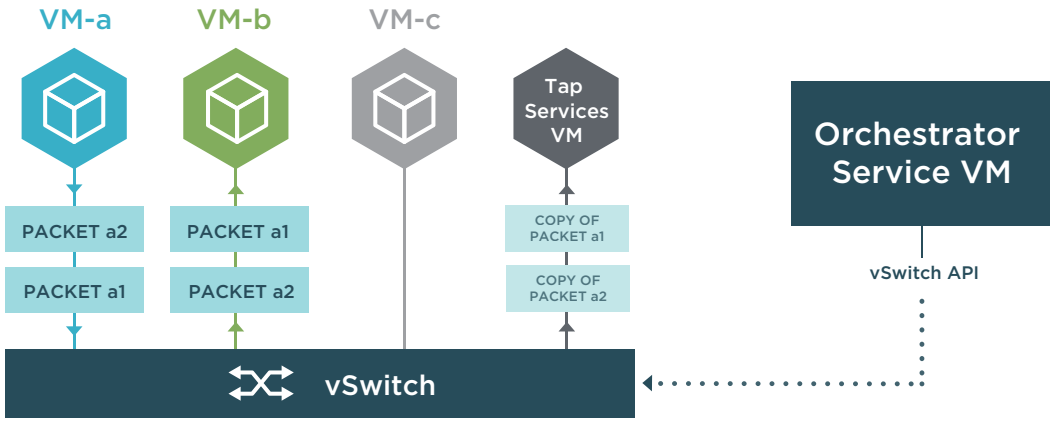
OPTION 4

ORCHESTRATING REMOTE CONTROLS TO vSWITCH INFRASTRUCTURE

This option copies select packets on the vSwitch and forwards it to a tap services VM running on the host. To do this, an orchestrator service VM is introduced that instructs the vSwitch to copy select traffic based on rules you set. This capability provides you with more granular control over which packets are copied so you can eliminate unneeded traffic. Set filters based on source IP, source port, destination IP, destination port, and layer 4 protocols like TCP and UDP.

One orchestrator service VM can instruct vSwitches across multiple hosts using advanced API capabilities. The orchestrator function requires vSwitch privileges, which works well in the private cloud, but does not in the public cloud. However, as a public cloud service provider, you could use this option to implement Tap-as-a-Service to your tenants. Option 4 provides a unified console for orchestrating capture, filter, and forwarding policies across all managed hosts.

THE ORCHESTRATOR FUNCTION REQUIRES VSWITCH PRIVILEGES, WHICH WORKS WELL IN THE PRIVATE CLOUD, BUT DOES NOT IN THE PUBLIC CLOUD.



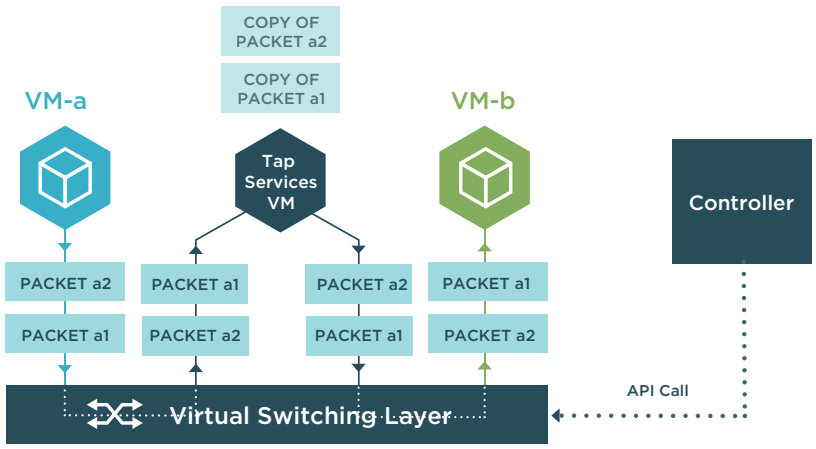
ixia

OPTION 5

FLOW STEERING

This option instructs the virtual switching layer to steer VM to VM segment traffic flow to a tap services VM first. The tap services VM copies select packets and then forwards the original packet to its destination. To do this, a controller instructs the virtual switching layer using an API to steer select traffic to a tap services VM based on rules you set. The tap services VM can be on the same physical host as the monitored VM or on another host.

Flow steering differs from the traditional tapping methodology of out-of-band, non-intrusive packet capture, copy, and forward. Flow steering makes the tapping function an integral part of the flow traversal. This option offers high flexibility, control, and automation capabilities. But, there are tradeoffs. The downside is that the inline tap services VM creates an additional failure node in the application data path between the VMs. The upside is that in orchestrated virtual environments, detection and recovery from VM failures are more robust than in a physical environment.



DID YOU KNOW?

With flow steering, you can have multiple tools sequentially perform tasks. This is known as service chaining. The most common illustration is adding inline security tools to create a virtual security zone. For example, a virtual firewall could be added inline to intercept the VM to VM communication, analyze the traffic, and either drop or forward the packet to the next tool after inspection.

BEST PRACTICES

SINCE FLOW STEERING ADDS A NODE INLINE, WE RECOMMEND ADDING HIGH-AVAILABILITY AND LOAD BALANCING CAPABILITIES.

ixia

FIVE WAYS TO COPY VIRTUAL APPLICATION TRAFFIC

SCORECARD

Great ⬢⬢⬢ Average ⬢⬢ Poor ⬢ | HIGH ● ◕ ◑ ◔ ○ LOW

	OPTION 1	OPTION 2	OPTION 3	OPTION 4	OPTION 5
	Adding a Tap Service VM to a Monitored Host using vSwitch Promiscuous Mode	Adding a Tap Service VM to a Monitored Host Using vSwitch Port Mirroring	Adding a Tap Agent to a Monitored VM	Orchestrating Remote Controls to vSwitch Infrastructure	Flow Steering
BENEFIT RATING					
Ease of Configuration	⬢⬢	⬢⬢⬢	⬢⬢	⬢⬢	⬢⬢⬢
Flexibility	⬢⬢⬢	⬢⬢	⬢	⬢⬢⬢	⬢⬢⬢
Scalability	⬢⬢⬢	⬢⬢	⬢⬢	⬢⬢⬢	⬢⬢
Virtual Motion Capability	⬢⬢⬢	⬢	⬢⬢⬢	⬢⬢⬢	⬢⬢⬢
Secure Multitenant	⬢	⬢⬢	⬢⬢⬢	⬢⬢⬢	⬢⬢⬢
COST RATING					
Impact on Host Resources (Memory, CPU)	◑	◕	●	◑	◔
Impact on vSwitch Resources	◑	◕	◔	◔	○
Impact on VM being monitored	◔	◔	●	◔	◔
LOCATION					
Your Datacenter	✓	✓	✓	✓	✓
Public Cloud			✓		✓
Private Cloud	✓	✓	✓	✓	✓
SUPPORTED PLATFORMS					
VMware 5.1	✓	✓	✓	✓	
VMware 5.5	✓	✓	✓	✓	
VMware 6.0	✓	✓	✓		
VMware NSX	✓	✓	✓	✓	✓
KVM	✓	✓	✓	✓	✓ *
Microsoft Hyper-V	✓	✓	✓	✓	
Microsoft Azure			✓		✓
Amazon Web Services (AWS)			✓		✓
SUPPORTED vSWITCHES					
vSS	✓		✓	✓	
vDS		✓	✓	✓	
OVS	✓	✓	✓	✓	

* Not all versions of KVM are supported.

CONCLUSION

Eliminating virtual blind spots bring new challenges to IT performance and security monitoring professionals. In the software-defined-everything world, processing cycles are a shared resource that tapping, filtering, and forwarding use in parallel with production workloads. Choosing the best strategy that meets performance and security monitoring goals can depend on the application you are monitoring, where you are running the application, the virtualization software you are using, and the outcome you want to achieve.

As a leader in network visibility, Ixia offers solutions for virtualized environments that make network, application, and security monitoring tools perform better. We can help you choose a strategy for monitoring the performance and security of your virtualized applications to fit your virtualization software investment, your cloud initiatives, and help you achieve your goals.

For more information on virtual visibility or to try our software, visit www.ixiacom.com. Together, we can help you develop trust in your virtualized infrastructure.

[1] "Magic Quadrant for x86 Server Virtualization Infrastructure", ID:G00268538, Gartner. July 14, 2015.
[2] "The State of Virtualization for Visibility Architectures," Ixia survey report. March 2015.
[3] "Your Data Center Network is Heading for Traffic Chaos, Bjarne Munch," 27 April 2011 / ID Number: G00210674, Gartner.
[4] "Cisco Global Cloud Index, 2015" 28 October 2015, Cisco.

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) 1.818.871.1805

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
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127