

Application and Network Performance Monitoring in a Virtualized Environment

As organizations implement virtualized environments, knowing how to monitor and maintain them becomes yet another challenge for today's network professional. Monitoring network and application traffic in an environment containing one-to-many relationships between physical hardware devices (virtual hosts) and virtual application servers (virtual machines) presents a number of concerns.

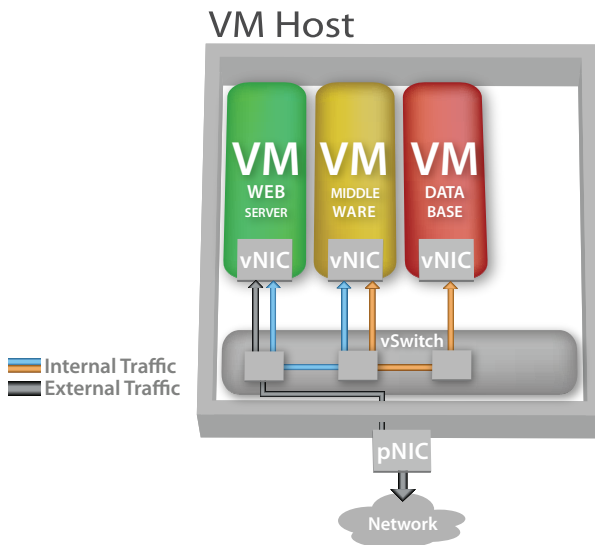
This white paper presents various visibility options and their ramifications, and outlines new technology that allows visibility into both external and internal traffic within a virtual environment.

Introduction

Before discussing monitoring options within a virtual environment, let's take a moment to discuss how the traffic flows within it.

Virtual environments are designed to include a virtual adapter (vNIC) for each virtual machine within the system. The vNIC is logically connected to a virtual switch, which is managed by the virtual host system (see the diagram below). This addresses communication which would remain in the VM host. In order to enable communication into and out of the VM host, a logical connection between the vNIC and the pNIC must be established.

Within the VMware ESX and ESXi environments, a virtual adapter can be set in "promiscuous mode." When promiscuous mode is enabled on a virtual adapter, all traffic flowing through the virtual switch—including local traffic between virtual machines and remote traffic originating from outside the virtual host—is sent to the promiscuous virtual adapter.



Challenges

A number of challenges are presented when attempting to monitor applications with a virtualized environment.

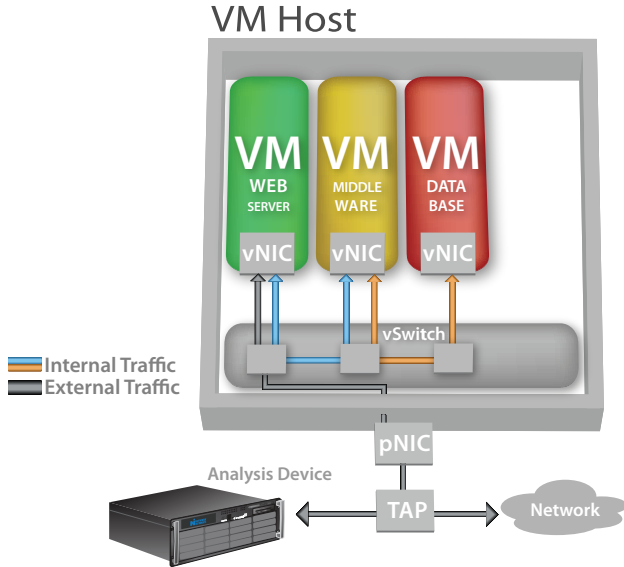
1. **Lack of visibility.** Traffic between virtual machines within a virtual host will not be visible outside of the host. This causes a number of problems:
 - a. Network engineers cannot monitor multi-tier applications partially or wholly located on multiple virtual machines within a single host.
 - b. Should a virtual machine be compromised by malicious code or security breach, other virtual machines within the same host may also be compromised.
2. **Lack of analysis functionality.** A separate solution is required to push data streams flowing within virtual machines out to an external tool or a purpose-built device. This functionality is necessary for network and application monitoring and analysis, compliance, and security audits. Virtual TAPs (software applications placed inside a virtual machine to export all data through a designated pNIC to an external device) can alleviate this problem.

**The Visibility Gap:
Virtual Environments
present new
visibility challenges
to monitoring and
analysis devices.**

Options

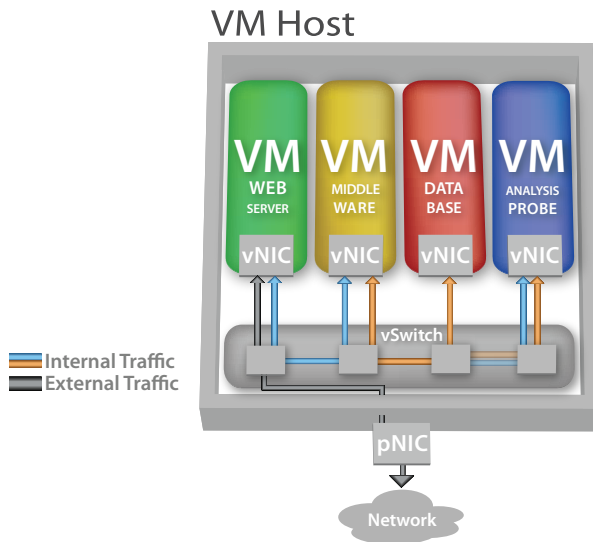
There are three primary ways to monitor both traffic flow from within applications on virtual machines and from the virtual host:

1. Monitor the host using an external analysis device as you would any other system, via SPAN technology or a physical TAP.



This option works well for environments not needing to track internal virtual machine-to-machine traffic within a host. However, it may not catch a security breach compromising multiple virtual machines within a host.

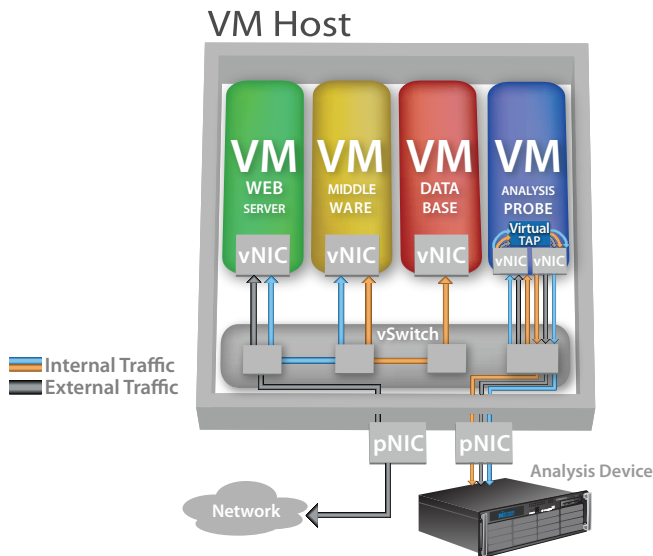
2. Monitor all virtual machines in a host by establishing a new virtual machine within the host. This option assumes the ability to SPAN or set in promiscuous mode the virtual switch within the host.



This option provides visibility at the statistics and packet levels of all traffic within a virtual host. It does not, however, allow packet-level traffic to be analyzed by an external physical device (IDS, retrospective analysis device, etc.).

The goal is to not only see all traffic flowing within a VM host but also export that data for powerful analytics and reporting.

3. Use a Virtual TAP to collect and redirect all internal virtual machine traffic to a dedicated virtual NIC within the monitoring virtual machine that is connected to an external purpose-built device for analysis or compliance enforcement.



Depending on the functionality of the external device the traffic is being copied to, this option may provide all the functionality of option two while taking advantage of the physical capabilities of the purpose-built external device.

Option two combined with option three offers the most extensive and comprehensive monitoring solution. In a VMware environment, one can utilize promiscuous mode on the internal virtual switch, and direct a copy of all traffic from all virtual machines to a virtual machine monitoring instance.

This offers several benefits:

- a. Collect metrics and perform real-time analysis.
- b. Using a Virtual TAP, re-direct packet streams out a separate NIC to be recorded by a Retrospective Network Analysis (RNA) device or other purpose-built security or analysis tool.

Benefits of the Virtual TAP

Mirroring all traffic within a virtual host to an external device provides a number of advantages, including total visibility into VM application traffic and the ability to run greater analytics for comprehensive reporting and faster problem resolution.

For example:

1. **Application Performance Monitoring.** Feed VM traffic to an enterprise reporting engine for comprehensive monitoring of virtualized environments. Set and track performance baselines and respond quickly when performance deviates from the norm. Tracking VM traffic over time helps determine if your VM server load has increased to the point of requiring action.
2. **Application Performance Troubleshooting.** The Virtual TAP can also output data to a Retrospective Network Analysis device, which stores it for later access. RNA devices have an intuitive time-navigation interface to help easily isolate problems within your virtual environment and troubleshoot these issues using Application Analytics.

The Virtual TAP option bridges the Visibility Gap, allowing complete real-time analysis, Retrospective Network Analysis, and full-scale reporting on all virtualized traffic.

The Virtual TAP removes the limitation of having to access or respond to VM traffic in real time. By eliminating the visibility gap the TAP provides greater control of your virtual environment and helps you better maintain overall application performance.

Conclusion

Depending on the virtual server technology you have decided to implement, you will have a number of options for network and application traffic visibility, and for the use of external devices for analysis. If all virtual machine communications take place between the virtual machines and the “outside” (i.e. outside the physical host), then monitoring the data flow from outside the host server may be the least complicated method by which to gain flow visibility.

If there is any internal communication between virtual machines, the only way to monitor this data is by using a monitoring virtual machine (separate or existing) with an analysis service (i.e. probe) gathering data from the internal virtual switch. Should you need to analyze or store data on an external purpose-built device, installing a Virtual TAP within the monitoring virtual machine will provide complete visibility into all data flowing on the internal virtual switch.



Operative Software Products

7219 Kentwood Avenue • Los Angeles, CA 90045
telephone US only (866) 204-6289 or (310) 410-9350

www.operativesoft.com/html/observer_virtual.htm