WHITE PAPER

How a Network Packet Broker Can Provide Pervasive Visibility into Distributed Network Environments

Introduction

Enterprises are extending their networks across physical, virtual and cloud environments, such as cloud Infrastructure-as-a-Service to take advantage of scalability, elasticity and availability. The final frontier for network packet brokers (at least for now) is providing visibility into applications and services on public and private cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, OpenStack and VMware. This visibility is particularly important, and challenging, because enterprises have difficulty in capturing network traffic in cloud deployments.

This white paper will examine the challenges of, and solutions for, providing visibility into physical, virtual and cloud environments. Readers will learn about virtual taps (vTAPs) and visibility nodes and discover how next-generation network packet brokers (NGNPBs) can integrate with management tools for all environments and orchestrate adjustment to changes.

Why Visibility is So Crucial – and So Difficult

Comprehensive visibility across all of your networked environments is crucial for seeing, managing and securing what matters. That's because, to be fully effective:

- Security tools need to spot indicators of compromise (IOCs) and malware everywhere on the network.
- Analytics tools must have a complete set of network data to build accurate baselines, detect anomalies and identify suspicious behaviors.
- Performance monitoring tools must have end-to-end visibility into application and network flows to develop meaningful metrics and troubleshoot problems.

In physical environments, the first step to network visibility is a Terminal Access Point (TAP), a basic building block of any visibility system. For complete coverage, many companies have adopted a TAP-ALL strategy as a best practice. This means that all critical links are set up with TAPs and/or Switch Port Analyzer (SPANs), even if the traffic is not under continuous monitoring. By having the TAP already in place, in the event of a security breach or troubleshooting requirement, the data is readily accessible.

In the past, tools would directly attach into the production network through these TAPs or through mirror/SPAN ports. However, with the growing volume of data and the increased mobility of users, devices and applications, tools are having a harder time providing accurate and timely analysis. For example:

- As network speeds/links are upgraded, tools that are directly connected into the network through TAP or SPAN ports are challenged as the tool interfaces do not necessarily keep up with network upgrade cycles. IT departments are now forced down a path of "rip and replace" for their monitoring infrastructure to connect tools to the higher speed links, even though these tools do not need to see all of the traffic.
- As the volume of traffic in the network grows, tools directly connected through TAPs or mirror/SPAN ports see growing volumes of traffic on that link, thereby forcing the tools to process increasingly large volumes of data. At some point the tools reach the limit of their processing capability, forcing traffic/data to be dropped and therefore becoming ineffective.
- As departments within IT organizations are being held to internal SLAs, these departments are now all contending for control of the TAPs or SPAN ports to connect their tools to. Given the limited number of TAPs or SPAN ports in any given segment of the network, this leads to contention across departments for access to those TAPs or SPAN ports.

In addition, as networks grow, the number and types of network analysis tools also grow. Networks are evolving to encompass various topologies, such as remote/branch offices, or private/public cloud. The approach of dropping tools directly into these networks significantly increases tool sprawl and the cost of the monitoring/management of infrastructure as well.

The kind of visibility afforded by a TAP in a physical environment has become much harder to achieve as enterprises migrate their computing workloads to virtual environments and cloud platforms. The methods developed for visibility into traditional datacenters no longer suffice. The major challenges created by these changes include:

- An inability to use conventional TAPs and SPAN portals to collect pervasive network traffic and metadata.
- A lack of advanced traffic intelligence for virtual and cloud environments.
- Continuous changes in the number and location of application instances.

These factors create major blind spots for security, analytics and performance monitoring tools. The truth is, it is very difficult to correlate cross-environment activity to detect lateral movement of threats. This leads some organizations to deploy different network data acquisition and monitoring tool sets for each environment, resulting in packet duplication and more complexity – leading to spiraling costs and inaccurate traffic analysis.

One of the hallmarks of next-generation network packet brokers is the ability to overcome these challenges and provide a single solution for collecting, processing and distributing network traffic across physical, virtual and cloud environments. The idea is to eliminate blind spots to reduce risk, manage complexity and minimize costs. Let's take a closer look.

Specific Challenges in Virtual Environments

In a conventional datacenter environment where application modules run on separate physical servers, TAPs and SPAN ports can be used to capture east-west traffic between application modules. However, when application modules run in virtual machines on the same physical server, the TAPS and SPAN ports have no visibility into the traffic between them

To add complexity, when demand increases, the hypervisor may automatically start up new instances of the software on the same host or on a different host. This happens too fast and too often for human administrators to observe the changes and reconfigure tools to monitor the new data flows.

The tools available today to monitor activities in virtual environments are simply not robust enough to meet the needs of multiple security, analytics and performance monitoring systems. Also, adding new tool sets for virtual environments means even more products to acquire, operate and integrate with existing systems.

Monitoring Virtual Environments (VMware)

Let's look at how NGNPBs solve these problems.

Acquire East-West Traffic

To obtain visibility into east-west traffic, NGNPBs deploy a visibility node, which is a lightweight footprint in a virtual machine (VM) on each host. The visibility node monitors network traffic into and out of individual virtual machines. The visibility node aggregates the traffic from the VMs, applies targeting policies created by an administrator and forwards the packets and metadata directly to an NGNPB platform for distribution to the physical tools.

NGNPBs Integrate with the Management Center

The NGNPB integrates with the management center of the virtual platform, for example, vCenter in a VMware environment. This integration allows the NGNPB to be notified when dynamic changes in the environment occur, so it can take appropriate actions. For example, when:

- Application instances are spun up on new virtual machines, the NGNPB can begin to monitor traffic to those VMs.
- An application instance is spun up on a new host, the NGNPB can deploy a visibility node on that host and start monitoring traffic there.
- A VM is moved from one host to another, the NGNPB can disable monitoring on the old host and enable monitoring in the location where the VM has landed.

Administrators would find it extremely difficult to keep up these changes using manual methods. For example, if a VM were moved from one hypervisor to another, the VM administrator would have to disable the existing vSwitch port mirror sessions and create a new port mirror session on the destination hypervisor. An NGNPB automates these tasks, providing continuous visibility into the traffic to the VM and freeing up the administrator for other critical tasks.

That's why an NGNPB can be a single solution for acquiring, aggregating and distributing network traffic and metadata for physical, virtual and cloud infrastructure. It provides pervasive visibility across the infrastructure, and provide traffic intelligence on all traffic, including SSL decryption and NetFlow generation.

Specific Challenges in Cloud Environments

When enterprises migrate applications to Amazon Web Services (AWS), Microsoft Azure and other Infrastructure-as-a-Service (IaaS) platforms, they gain agility and scalability and no longer have to install and manage hardware. However, they have to cope with a lack of access to east-west network traffic, highly dynamic environments and duplicate tool sets, just as when they run applications in virtual environments.

In fact, the situation is even more challenging. An enterprise has direct access to the virtual environments in its own datacenter. But the public cloud platform providers, who have to worry about privacy and security for many clients, put tight controls on the access they give outsiders.

That makes it very difficult to monitor applications on cloud platforms. For example, let's say east-west traffic flows back and forth between instances of the application modules in a three-tier web application. The enterprise can't put TAPs or SPAN ports between the tiers. And of course if you want to run applications on more than one cloud platform, you have to deal with even more tool sets, making end-to-end visibility that much harder to achieve.

Monitoring Applications on Cloud Platforms

Let's look at how NGNPBs provide comprehensive visibility across cloud platforms.

Visibility Modules and vTAPs in the Cloud

A NGNPB can deploy a visibility node in each cloud-based virtual private network, such as an Amazon Virtual Private Cloud (VPC) or an Azure Virtual Network (VNet). The visibility node uses vTAPs, which are lightweight software agents, to monitor network traffic on each instance in that private network or they can use the Public Cloud providers (IaaS), which have also introduced their own native vTAPs that are agentless. The vTAPs filter and send copies of the network packets securely to the visibility node.

The visibility node aggregates the traffic from the vTAPS, applies targeting rules created by an administrator and forwards the packets and metadata, typically via a Generic Routing Encapsulation (GRE) or VXLAN tunnel. The traffic can be routed to:

- A "tool tier" of security, analytics and performance monitoring tools running on the cloud platform.
- The central NGNPB platform in the enterprise datacenter, which in turn distributes the packets and metadata to the tools running there.

The NGNPB gives enterprises options to:

- Use security and performance monitoring tools that run on the cloud platform.
- Use existing tools in the datacenter so they can have one tool set across all environments.
- Do some of each based on the pros and cons for each type of tool.

Orchestration

NGNPBs typically include a central orchestration and management module. This module is integrated via REST APIs with monitoring and management tools from the platform vendors, such as AWS CloudWatch and Azure Network Watcher.

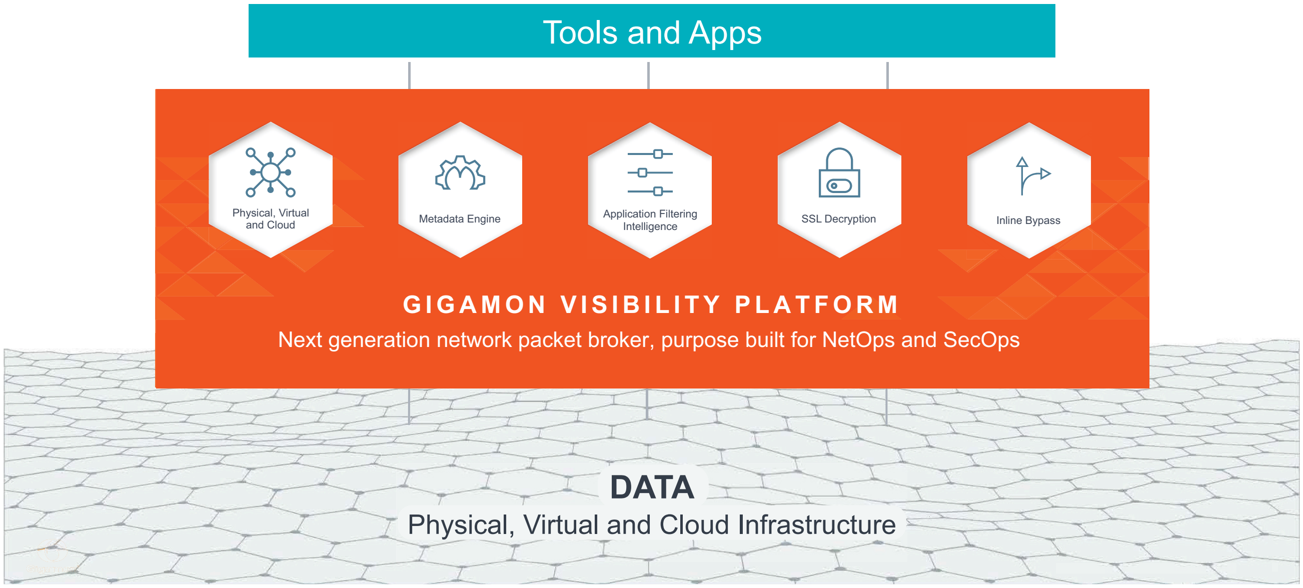
The integration allows the NGNPB to be notified when changes take place in the cloud-based virtual private network. It can then take appropriate actions, such as deploying a vTAP when application instances are created on a new virtual private network.

The orchestration and management module can also be a central point of control to create and manage policies collecting and filtering data from the workloads in the cloud.

Introducing the Gigamon Visibility Platform, a Next-Generation Network Packet Broker

The Gigamon® Visibility Platform is a next-generation network packet broker, designed to provide the right traffic to your inline and out-of-band tools. Whether a network setup is on-premises, virtual or in the cloud, a network packet broker provides the perfect visibility foundation to support:

- Threat prevention
- High resiliency of inline network security tools
- Large numbers of out-of-band threat detection tools
- Accuracy of network monitoring tools
- Analysis of network performance
- Aggregation of high-speed network TAPs


Tools and Apps
Physical, Virtual and Cloud
Metadata Engine
Application Filtering Intelligence
SSL Decryption
Inline Bypass
GIGAMON VISIBILITY PLATFORM
Next generation network packet broker, purpose built for NetOps and SecOps
DATA
Physical, Virtual and Cloud Infrastructure

With the Gigamon Visibility Platform, the right tools get the right traffic at the right time. It is designed from the ground up to:

- Enable network and security tools to keep up with increasing network speed
- Gain insight into network traffic
- Reduce tool sprawl and help lower costs

Summary

Your network relies on tools to keep it running, secured and optimized, but none of those tools receive a complete picture because of blind spots that prevent complete visibility and control of your infrastructure. Bridge your network and management tools by intelligently delivering relevant network traffic and powerful visibility so you can see, secure and empower what really matters.

About Gigamon

Gigamon is the recognized leader in network visibility solutions, delivering the powerful insights needed to see, secure and empower enterprise networks. Our solutions accelerate threat detection and incident response while empowering customers to maximize their infrastructure performance across physical, virtual and cloud networks. Since 2004 we have cultivated a global customer base which includes leading service providers, government agencies as well as enterprise NetOps and SecOps teams from more than 80 percent of the Fortune 100.

To learn how to gain pervasive visibility across all types of networks, visit www.gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com