Automated Traffic Visibility for SDDC
Solution Guide

Contents

1 Introduction

This document is targeted at virtualization, security, and network architects interested in monitoring Cloud and Software Defined Data Center (SDDC) architectures based on VMware network virtualization solutions using Gigamon's Visibility Fabric™.

VMware NSX is the leading network virtualization platform that delivers the operational model of a virtual machine for the network. Similar to virtual machines for compute, virtual networks are programmatically provisioned and managed independent of underlying hardware. NSX reproduces the entire network model in software, enabling any network topology—from simple to complex multi-tier networks— to be created and provisioned in seconds.

Gigamon's Visibility Fabric architecture is an innovative solution that delivers pervasive and dynamic visibility of traffic traversing communication networks. The Visibility Fabric architecture significantly improves network flexibility by enabling static tools to connect to dynamic, virtualized applications, so users can efficiently and securely address their business needs.

VMware and Gigamon have collaborated on an integrated solution to enable organizations to realize the full potential of the Software Defined Data Center while providing "Active Visibility" into the virtual workloads and virtual networks. The joint solution addresses current challenges faced by data centers including:

- Lack of visibility into East-West (VM-to-VM) traffic
- Securing the physical and virtual traffic using the same monitoring policies
- Tenant level isolation and visibility for SLA monitoring

VMware NSX network virtualization platform provides the network virtualization pillar of the SDDC. The Gigamon Visibility Fabric consists of distributed physical (GigaVUE H Series platforms) and virtual (GigaVUE-VM) nodes that provide an advanced level of traffic intelligence. At the heart of the fabric is Gigamon's patented Flow Mapping® technology that identifies and directs incoming traffic to single or multiple tools based on user-defined rules implemented from a centralized fabric management console, GigaVUE-FM, which integrates tightly with VMware vCenter and NSX vSwitches.

The integrated solution provides several benefits:

- Automate traffic visibility for securing the micro-segmented SDDC
- Non-disruptive deployment over existing physical networks or next generation topologies
- Place and move virtual workloads independent of physical topology
- Use data center micro-segmentation to achieve tenant level isolation and security

- Pervasive visibility into virtual and physical network traffic by offloading intelligent and scalable filtering policies to Gigamon's Visibility Fabric while optimizing operational tool infrastructure
- Gain operational efficiency through automation using VMware NSX and NetX APIs and Gigamon's GigaVUE-VM Visibility in Motion policy migration.

2 VMware NSX Network Virtualization Overview

VMware NSX is foundational to the software-defined data center and completes the virtualization infrastructure, enabling IT to move as fast as the business demands without compromising the security or availability of critical applications. NSX embeds networking and security functionality typically handled in hardware directly into the hypervisor, delivering the operational model of a virtual machine for networking and security and unlocking the ability for IT to move at the speed of business.

Speed and agility, impenetrable security, and availability of applications are all critically important priorities for IT organizations to deliver. Most organizations have already virtualized compute components in their data centers, with the overwhelming majority virtualizing 50% to 100% of their servers. In addition, many businesses have also made the decision to virtualize storage, with more than 70% of businesses having already adopted or planning to adopt software-defined storage. This abstraction of functionality from hardware into software enables businesses to quickly provision applications, move virtual systems across and between data centers, and automate a number of processes.

Figure 1:SDDC Use Cases enabled by NSX

VMware NSX is the network virtualization platform of the software defined data center. It takes the functionality that was formerly embedded in network hardware—such as switching, routing, and firewalling—and abstracts it to the hypervisor. By doing this, NSX creates what can be thought of as a “network hypervisor” that is distributed throughout the data center. With it, IT is able to become an enabler of innovation for the organization, effectively saying “yes” to multiple stakeholders instead of treating their requests as competing and mutually exclusive.

An example of the initiatives where NSX can bring value are:

- Security: VMware NSX enables organizations to divide the data center into distinct security segments logically, down to the level of the individual workload – irrespective of the workload’s network subnet or VLAN.

- Automation: NSX addresses the challenge of lengthy network provisioning, configuration errors, and costly processes by automating labor-intensive, error-prone tasks. NSX creates networks in software, eliminating bottlenecks associated with hardware based networks.

- Application continuity: because NSX abstracts networking from the underlying hardware, networking and security policies are attached to their associated workloads. Organizations can easily replicate entire application environments to remote data centers for disaster recovery, move them from one corporate data center to another, or deploy them into a hybrid cloud environment.

3 NSX Architecture Components

The NSX-v system architecture consists of three main functional layers: the data plane, control plane and the management plane. In many real life deployments an additional cloud consumption layer sits on the top of the NSX Manager, leveraging the NSX API as configuration entry point.

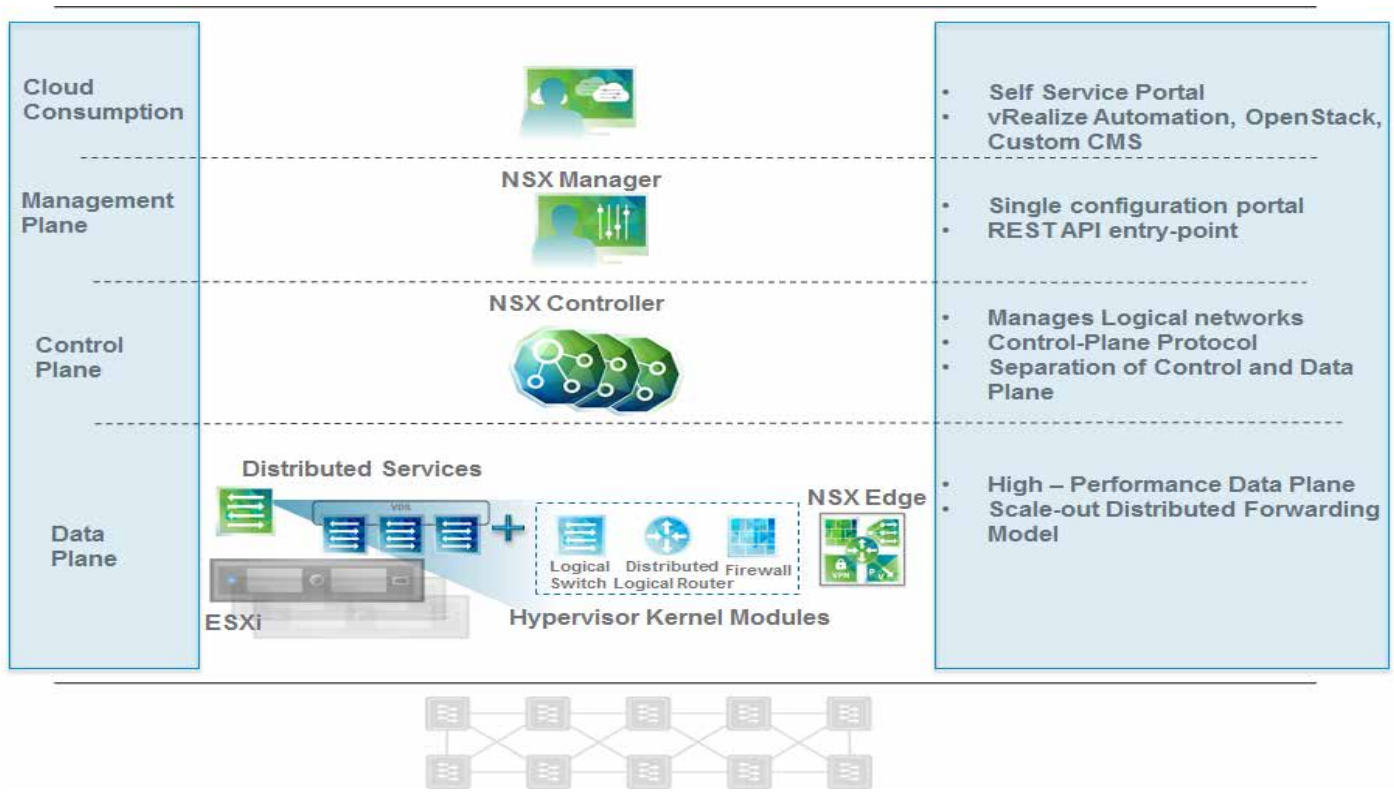

Figure 2: VMware NSX-V Solution Components

With the overall system architecture in mind, the specific role of each layer can be further described:

Cloud Consumption Layer

Typically, end-users tie in network virtualization to their cloud management platform for deploying applications. NSX provides a rich set of integration points into virtually any CMP via the REST API. In a vSphere environment NSX is integrated with the vSphere Web UI itself providing out of the box experience for deployment and consumption of the services.

Management Plane

The NSX management plane is built by the NSX manager with tight integration to vCenter. The NSX manager provides the single point of configuration and exposes REST API entry-points.

Control Plane

The NSX control plane runs in the NSX controller. In a vSphere-optimized environment with VDS the controller enables multicast free VXLAN and control plane programming of elements such as Distributed Logical Routing (DLR). In all cases, the controller is purely a part of the control plane and does not have any data plane traffic passing through it. The controller nodes are also deployed in a cluster of odd members in order to enable high-availability and scale. Any failure of the controller nodes does not impact any data plane traffic.

Data Plane

The NSX data plane consists of the NSX vSphere Distributed Switch (VDS) with add-on components such as distributed routing, distributed firewall, and VXLAN bridging support. These services run as kernel modules (VIBs), providing scalable and line rate performance. The NSX vSwitch (VDS) abstracts the physical network and provides access-level switching in the hypervisor. Key functions which are central to network virtualization and enable decoupling of logical networks from the underlying physical components include:

- VXLAN protocol-based support for overlay networks and centralized network configuration. Overlay networking enables extension of a layer 2 (L2) segment anywhere in the fabric without physical network design constraints.
- Distributed L3 Routing – Optimizes the forwarding of logical network segments (East-West) traffic while maintaining isolation between tenants.
- Distributed Firewall – Security enforcement is done at the kernel and vNIC level itself. This enables firewall rule enforcement in a highly scalable manner without creating bottlenecks onto physical appliances. The firewall is distributed in kernel allowing minimal CPU overhead and line rate performance.
- Traditional network features – such as Port Mirroring, NetFlow/IPFIX, Configuration Backup and Restore, Network Health Check, QoS, and LACP.
- Logical Load-balancing – Support for L4-L7 load balancing.

4 NSX and Partner Services

The natively available Service Insertion framework enables NSX to integrate with third-party solutions made available by VMware NSX partners like Gigamon.

With the latest enhancements, it is now possible for a monitoring service VM to receive a mirror copy of the traffic (packet copy service integration) and for a user to associate visibility policies directly into NSX Security Groups.

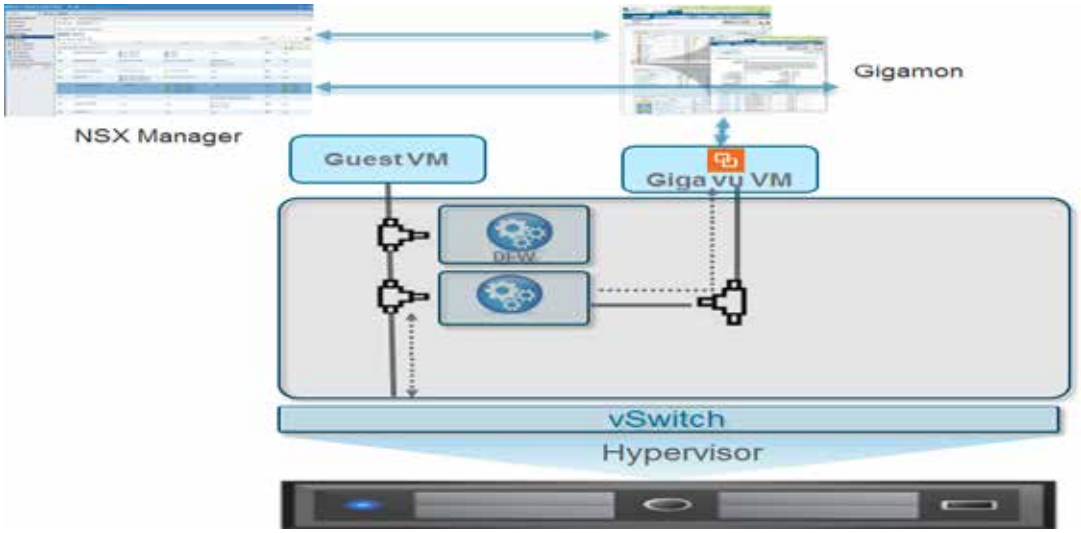

Figure 3: NSX Service Insertion Architecture

Traffic visibility is a very important use case not only because modern data center security tools depend on network traffic for analysis, but also because it nicely complements information available from log data and flow measurements which alone may not always provide the complete picture.

Gigamon's Fabric Manger, GigaVUE-FM, integrates with VMware NSX as a partner service, using NSX Service Insertion. Service Insertion allows partner services such as Gigamon Traffic Visibility to integrate with NSX. When the NSX Manager is registered in GigaVUE-FM, a Gigamon Traffic Visibility Service is registered with NSX. The Traffic Visibility Service is then installed on the NSX compute clusters through the vCenter UI. Installing the Gigamon Traffic Visibility Service deploys the GigaVUE-VM Service VMs to each host in the cluster. Security policies are then created that will make a copy of the network traffic using NetX APIs and tunneled across the production network to the Gigamon Visibility Fabric node. The traffic is de-capsulated here and sent to GigaSMART® engine for additional processing like slicing, masking, or net flow generation. Once done, it is now available to be sent to a tool farm that consists of your APM, NPM, and security appliances.

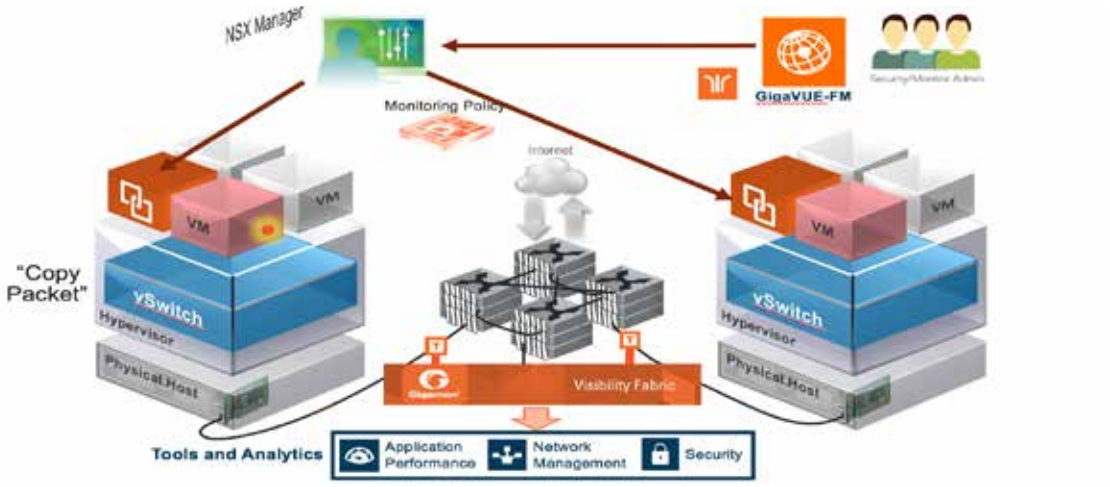

Figure 4 – Dynamic Traffic Visibility Service Insertion

5 Gigamon Visibility Fabric Overview

The Unified Visibility Fabric is an innovative and complete visibility solution to bridge communication networks. For truly pervasive visibility, this must include physical, virtual and emerging SDN/NFV environments.

The Gigamon Unified Visibility Fabric is a layered architecture (see Figure 5: Gigamon Unified Visibility Fabric) that includes the following tiers:

- Visibility Fabric Nodes Tier
- Fabric Services and Traffic Intelligence Tier
- Fabric Control (Management) Tier
- Application Tier

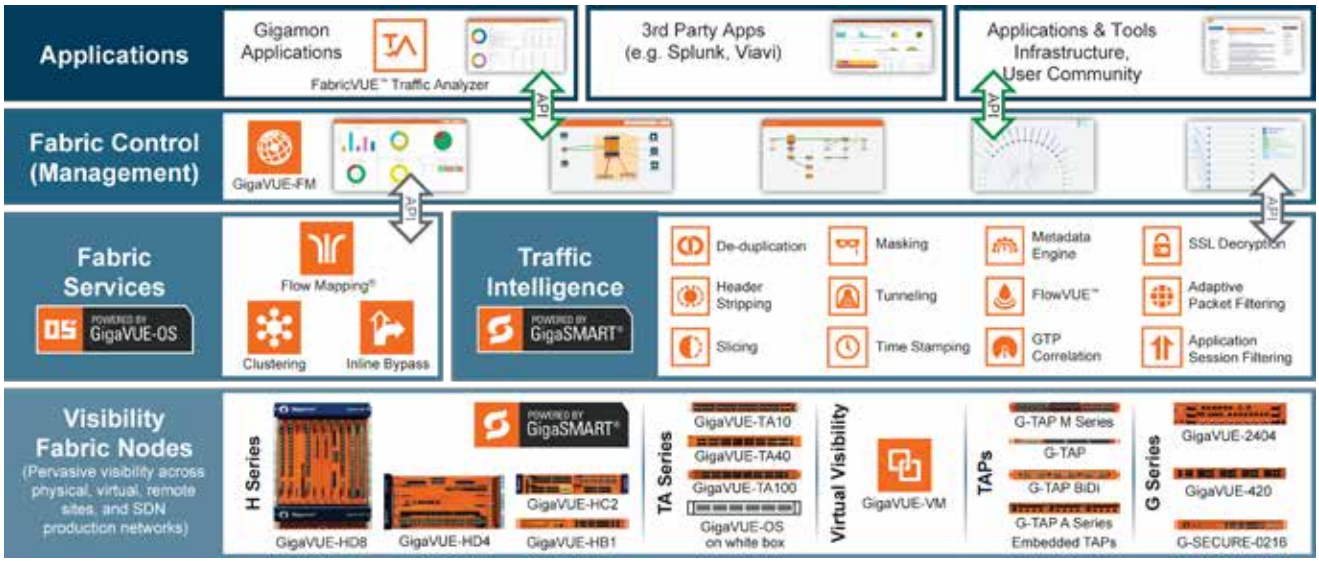

Figure 5: Gigamon Unified Visibility Fabric

Visibility Fabric Nodes Tier

Distributed nodes provide pervasive visibility across physical, virtual, and remote sites, as well as future SDN/NFV production networks. Gigamon provides the industry's broadest portfolio of visibility nodes that provide an advance level of filtering intelligence.

- GigaVUE H Series forms the foundation of a distributed fabric. The high-performance fabric nodes are modular and extensible for a range of scale and performance requirements from 1Gb 1RU nodes to larger 2.4Tb chassis-based solutions.
- GigaVUE-VM forms the virtual edge of the visibility infrastructure and extends visibility within virtual networks and monitors traffic between virtual machines.

Fabric Services and Traffic Intelligence Tier

The Visibility Fabric nodes offer two distinct set of services, Fabric Services powered by GigaVUE-OS and Traffic Intelligence powered by GigaSMART.

Gigamon's patented Flow Mapping technology identifies and directs incoming traffic flows of interest to single or multiple tools based on user-defined rules implemented from a centralized management system. Flow Mapping allows multi-tenant access and segregation of monitored traffic and policies by providing advanced role-based management.

GigaSMART provides stateful and packet-level optimization and normalization functions that run as software applications on high-performance compute engines in the fabric nodes. GigaSMART applications span a variety of functions and include:

- **Packet Slicing / Masking** – Slice/mask confidential information in a packet before sending it to a monitoring tool.
- **Header Stripping** – Remove extraneous headers to deliver normalized IP packets to monitoring tools. This is especially useful when adopting network virtualization or SDN.
- **Adaptive Packet Filtering** – Intelligent protocol aware filtering across advanced encapsulation headers including VXLAN, VN-Tag, MPLS, etc.
- **De-duplication** – Remove duplicate instances of the same packet to avoid unnecessary traffic processing by tools.
- **NetFlow and Metadata Generation** – Generates and Exports records to collectors supporting Netflow v5/v9 and/or IPFIX as well extensions for other metadata such as URL, HTTP response code, SIP, DNS, and Certificates.
- **Application Session Filtering** – Provide complete visibility into traffic flows by forwarding all packets from session initiation to termination. Also can classify flows of interest using signatures to filer applications such as video streaming, email, Web 2.0 and other business applications.
- **SSL Decryption** – Decrypt SSL encrypted traffic to offload tools from the decryption function. This function is useful to detect any malware that is encrypted in the SSL traffic.

Fabric Control (Management) Tier

GigaVUE-FM provides centralized management and a common policy framework for the Visibility Fabric. GigaVUE-FM delivers a single-pane-of-glass view of all the physical and virtual nodes across the Visibility Fabric, while also providing an easy-to-use wizard-based approach for configuring patented Flow Mapping and GigaSMART traffic policies. The GigaVUE-FM solution provides a set of REST APIs to integrate with third-party applications and tools to enable dynamic changes in the Visibility Fabric.

Application Tier

The Applications Tier interfaces with GigaVUE-FM through a set of APIs. These APIs allow third-party development of applications, integration with SDN controllers, integration with other specialized IT applications, and tools infrastructure. The GigaVUE-FM features integration with VMware vCenter APIs that allows continuous visibility without administrator intervention.

6 Components of Data Center Visibility

The Gigamon Visibility Fabric provides monitoring for both the physical and virtual network end points by capturing the traffic (TAP or SPAN) and delivering it to the centralized tool infrastructure as shown in Figure 6 and 7.

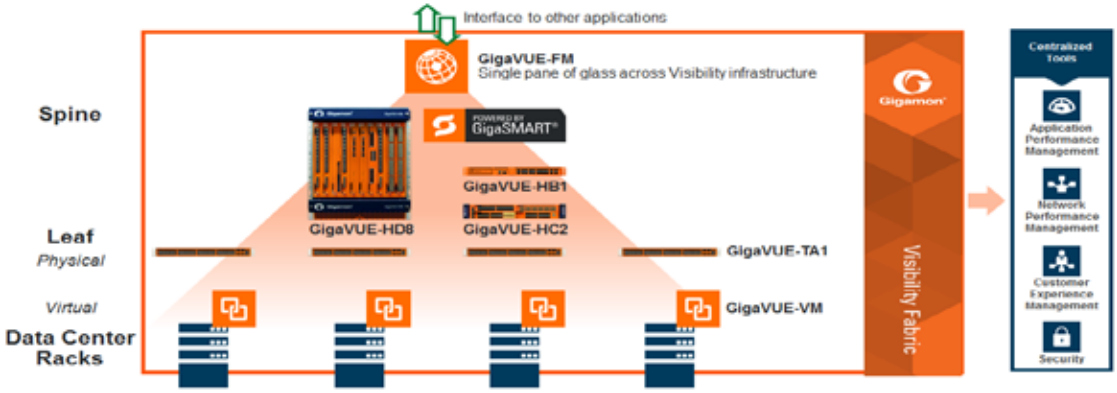

Figure 6: Components of Data Center Visibility

The TAP modules are strategically placed to capture all north-south traffic, while the GigaVUE-VM virtual node is used to selectively capture the virtual east-west traffic.

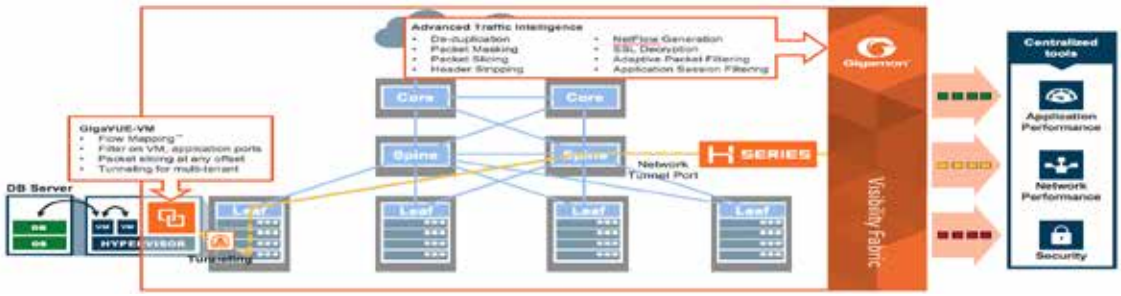

Figure 7: Capture and delivering traffic in a SDDC

GigaVUE-VM - Intelligent Traffic Replication and Filtering for Virtual Machines

With more than 80% of the workloads in the Data Center expected to be virtual in 2016, and 80% of this DC traffic being East-West, a primary challenge for the centralized monitoring infrastructure is to access this virtual traffic for Application, Network and Security analysis.

Gigamon's GigaVUE-VM Visibility Fabric node provides an intelligent filtering technology that allows virtual machine (VM) traffic flows of interest to be selected, forwarded, and delivered to the monitoring infrastructure centrally attached to the GigaVUE platforms, thereby eliminating any traffic blind spots in the virtualized data center.

As a VMware vSphere guest VM, the light footprint GigaVUE-VM fabric node is installed without the need for special software, invasive agents, kernel modules, or changes to the hypervisor. With this solution, your organization can now achieve the same packet-level traffic visibility between virtualized applications as is normally available between discrete

physical applications and servers. VMware using NETX API provides a copy of the virtual traffic to GigaVUE-VM providing active visibility into an agile and dynamic Software-Defined Data Center (SDDC). GigaVUE-VM fabric nodes tightly integrate with Virtual Distributed Switch (vDS) and logical network.

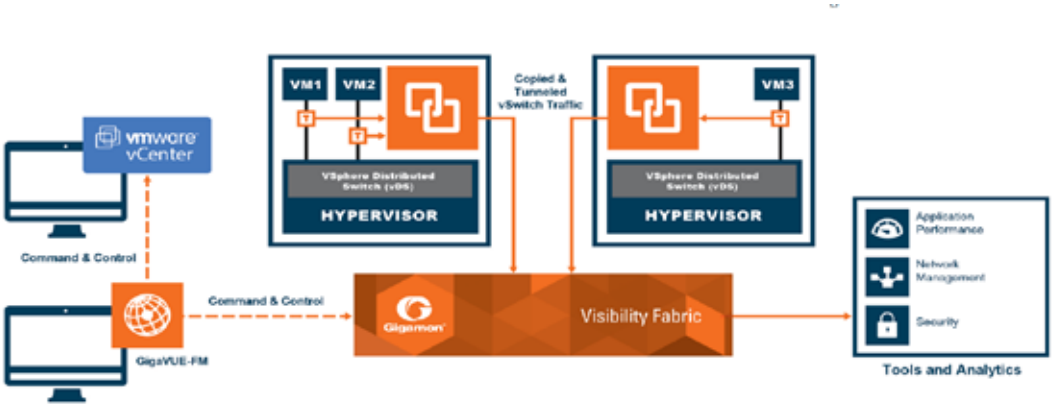

Figure 8: GigaVUE-VM Traffic Capture

Having an end-to-end solution that provides traffic visibility into both the physical and virtualized infrastructures empowers the infrastructure administrators and operators with the insight needed to ensure service quality, security compliancy, and maintain business continuity.

GigaVUE-FM – Visibility Fabric Control and Management

GigaVUE-FM delivers a single pane-of-glass view of all the physical and virtual nodes across the Visibility Fabric, while also providing an easy-to-use wizard-based approach for configuring patented Flow Mapping and GigaSMART traffic policies.

The summarized and customizable dashboard allows operators to view and pro-actively identify hot spots with quick-access links to node status, events, port, and traffic usage exceptions. This information can also be exported as HTML or PDF reports for offline review, repository, compliancy, and capacity planning

A single instance of GigaVUE-FM can manage hundreds of visibility nodes across multiple locations, containing more than a quarter of a million physical ports in addition to managing VMware virtual infrastructures.

With a single user interface, there is no longer a need to access each node individually, reducing OPEX value.

7 How the Integrated VMware NSX and Gigamon Visibility Fabric solution works

The following figure shows step-by-step workflow on how GigaVUE-VM provides automated traffic visibility for virtual workloads in NSX environment using VMware NSX and NetX APIs.

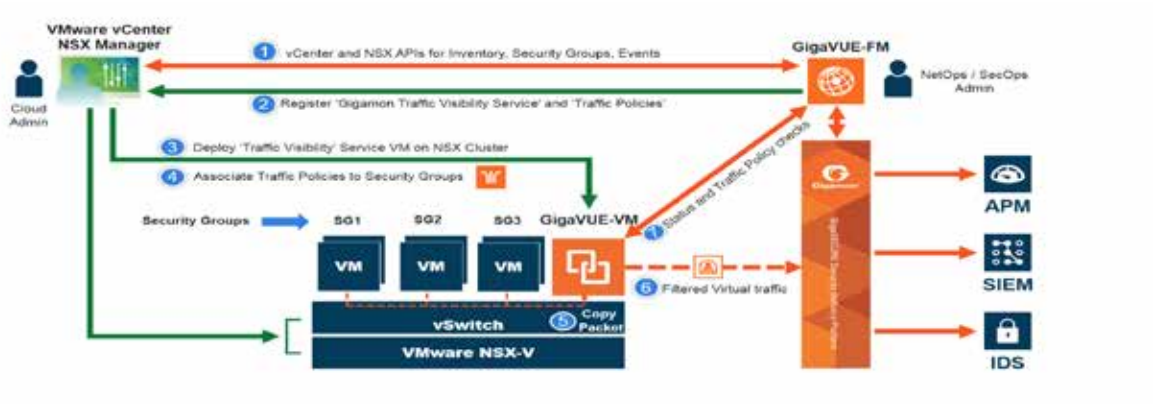

Figure 9: GigaVUE-VM for NSX - Workflow

Steps for integrating GigaVUE-VM with NSX

The following lists the steps for integrating GigaVUE-FM and VMware NSX. For additional information on how to configure these steps and prerequisites. Please refer to the *GigaVUE FM and GigaVUE-VM User's Guide* available at ***https://gigamoncp.force.com/gigamoncp/SWDownloadCommunity***

Step 1: Create Users in VMware vCenter and GigaVUE-FM

For VMware NSX and GigaVUE-FM to communicate, a Gigamon-FM user must be created in VMware and an NSX user must be created in Gigamon-FM. Also, a GigaVUE-FM user must be created in VMware vCenter for GigaVUE-FM to perform vCenter inventory functions. For VMware NSX and GigaVUE FM to communicate, users with the proper permissions must be created in both GigaVUE-FM and VMware NSX.

Step 2: Register the NSX vCenter and NSX Manager in GigaVUE-FM

There is a one-to-one mapping between vCenters and NSX Managers. Both the vCenter registered with the NSX Manager and the NSX Manager must be added to GigaVUE-FM.

When the NSX Manager is registered in GigaVUE-FM, it registers the Gigamon Traffic Visibility Service in NSX as a Network Introspection Service. (Refer Figure 10.) The Gigamon Traffic Visibility service is used to install GigaVUE-VM Service Virtual Machines and define profiles for forwarding traffic to the GigaVUE Visibility Fabric.

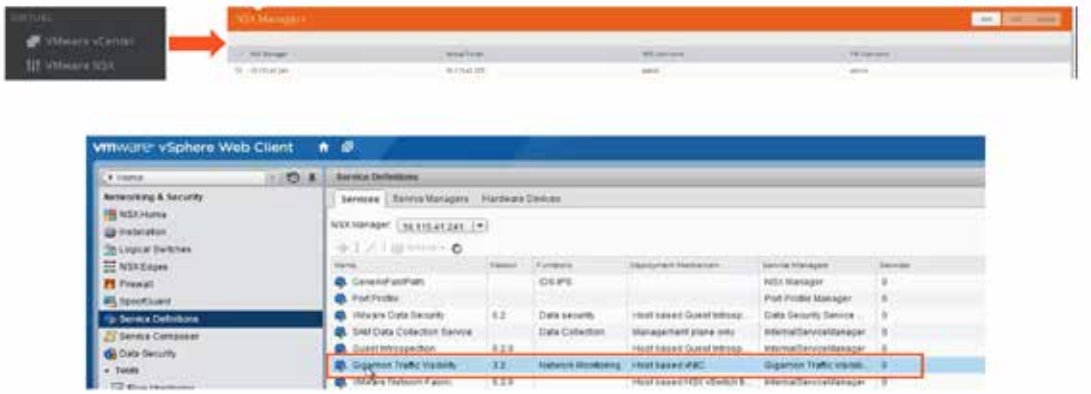

Figure 10: Dynamic Service Insertion with GigaVUE-FM

Step 3: Install the Gigamon Traffic Viability Service on vCenter Clusters.

The Gigamon Traffic Visibility service must be installed on each of the clusters in the NSX environment. Installing the Gigamon Traffic Visibility service installs the GigaVUE-VM Service VM on each of the hosts in the cluster. The Cloud Administrator should perform this Gigamon Traffic Visibility service installation. Refer to Figure 11.

The GigaVUE-VM node has 3 network interfaces:

- Network Adapter 1 – Used for management communication between the Fabric Manager and GigaVUE-VM
- Network Adapter 2 – Used for tunneling virtual network traffic to the Gigamon Visibility Fabric nodes
- Network Adapter 3 – Used for internal traffic communication within the GigaVUE-VM

When the GigaVUE-VM is deployed by NSX, the network port group selected for the Network configuration is applied to all 3 network adapters. Gigamon recommends that separate port groups be used for management communication and tunneled network traffic. This can be changed manually or through the use of a script. Although, Network Adapter 3 is only used for internal communication, it still must be in the connected state. It doesn't matter which port group Network Adapter 3 is connected to.

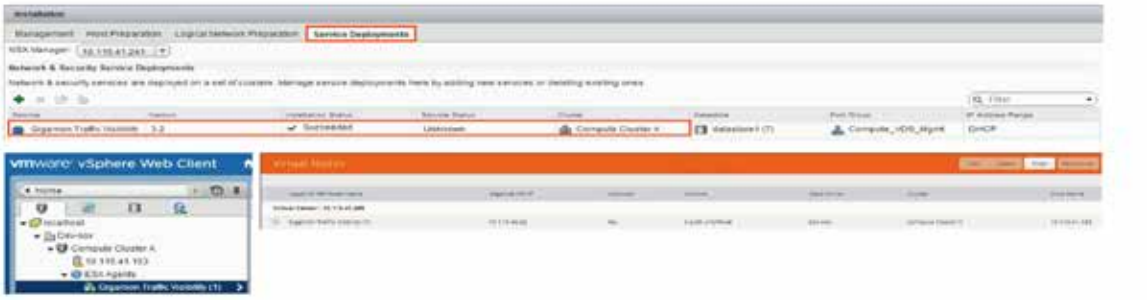

Figure 11: Service Virtual Machine (GigaVUE-VM) Deployment

Step 4: Configuring GigaVUE-FM Tunnels and Virtual Maps

NSX traffic needs to be sent to the H-Series node. A tunnel must be created in the Tunnels Library that defines the destination port to which the traffic is sent. The tunnel type supported are GMIP, L2GRE, and ERSPAN. For more detail on each of these tunnel typle, refer to the *GigaVUE FM and GigaVUE-VM User's Guide*.

Figure 12: Virtual Traffic Delivery to the Physical Fabric Node

Virtual maps are also needed to monitor NSX traffic. A separate map needs to be created for each separate GigaSMART tunnel destination to send NSX traffic, or if specific map rules or slicing is required. If the same parameters will be applied for all NSX traffic, only one map is needed to handle all NSX traffic. Creating a map creates a corresponding profile in NSX that will be used to associate the NSX traffic with the virtual map during security policy creation.

Step 5: Create the NSX Security Group and Security Policy

An NSX security group and security policy must be created to redirect network traffic to the Gigamon Traffic Visibility service. A security group defines which VMs will be monitored. The security policy associates the Gigamon Traffic Visibility service and map profile to the security group. Finally, apply the security policy to the security group to tie together monitored VM and security policy with visibility service. The cloud tenant user should create the security group and security policy. (Refer to Figure 13 and Figure 14.) With this NSX service profile and security group gets associated with virtual traffic policy created in GigaVUE-FM. Refer Figure 15.

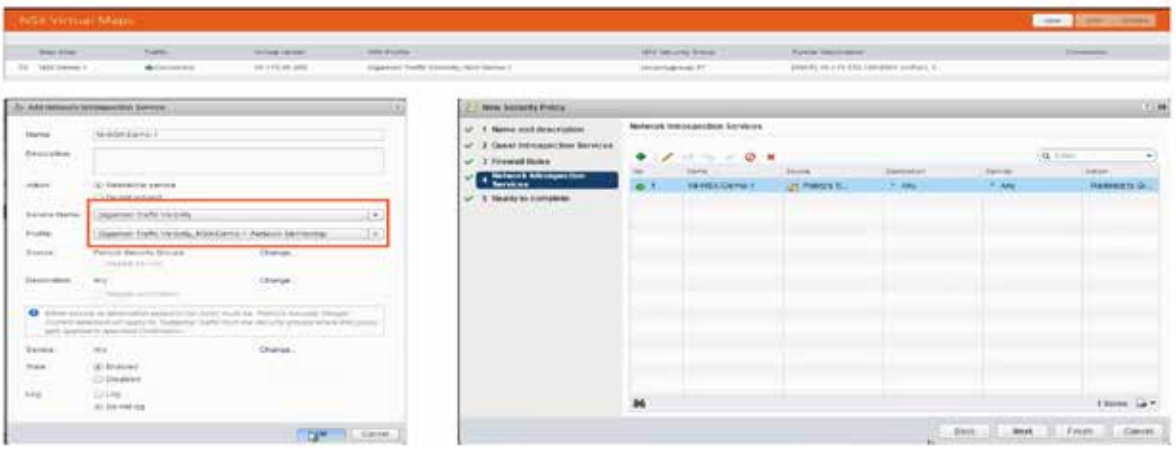

Figure 13: Add Gigamon Virtual Map to NSX Service Profile

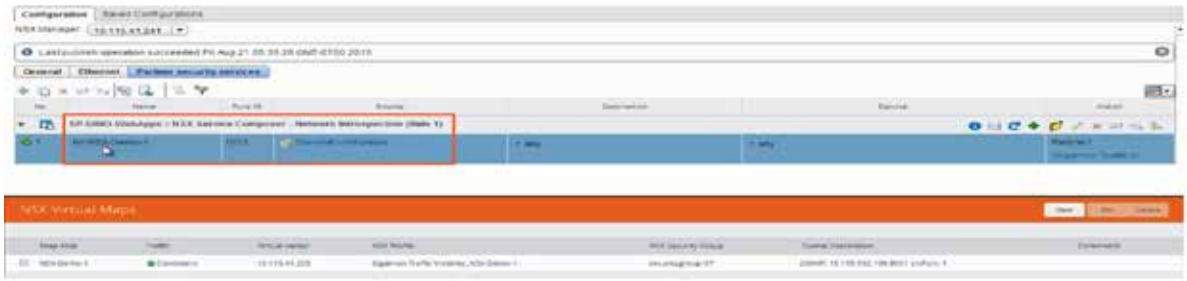

Figure 14: Map a Traffic Policy to Security Group

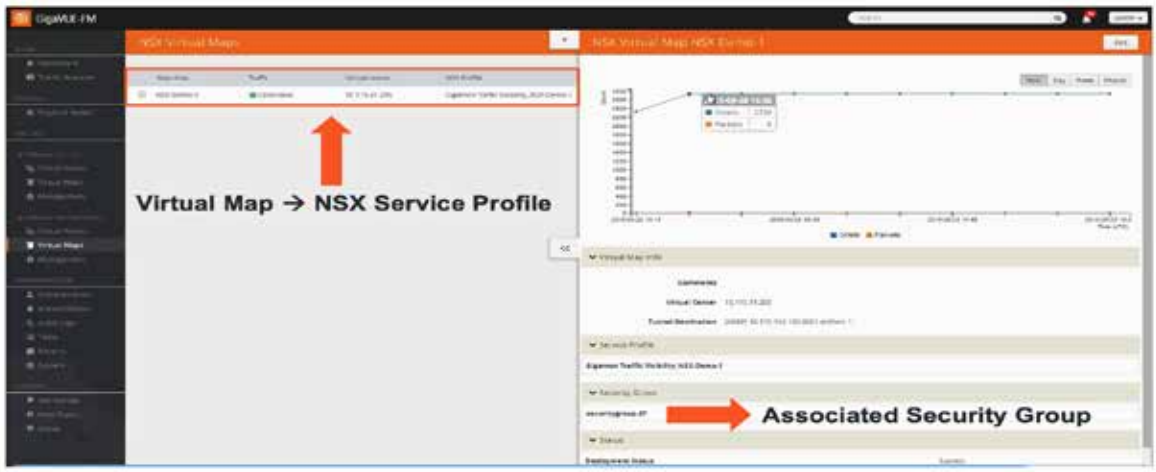

Figure 15: NSX Service profile and security group associated with Traffic Policy in GigaVUE-FM

Troubleshooting with GigaVUE-FM

GigaVUE-FM can be leveraged for troubleshooting by network operators. Various dashboards and widgets provide reports and graphs for top N network and tool ports by traffic consumption, CPU usage, GigaSMART operations, and so on. Also, a user can check the individual port statistics, which show how many packets were received, how many sent out, how many discards, and how many dropped.

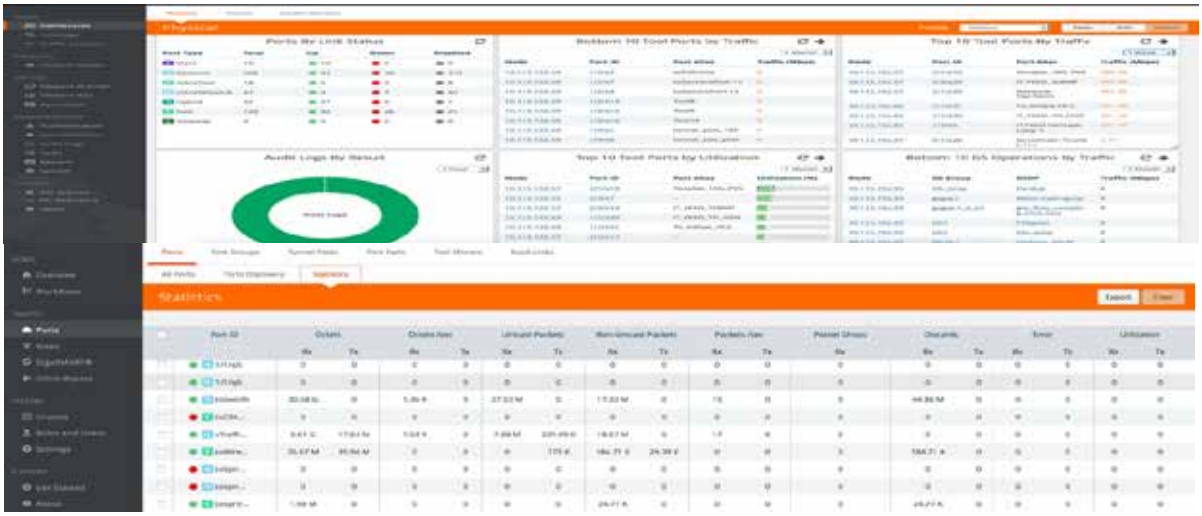

Figure 16: Visibility Metrics within GigaVUE-VM

Conserve Network Backhaul

Some monitoring tools may not require the entire payload and could do most of their analytics using the headers. In which case, the DC or tool administrator can conserve the network backhaul by “Slicing” the filtered traffic prior to delivery.

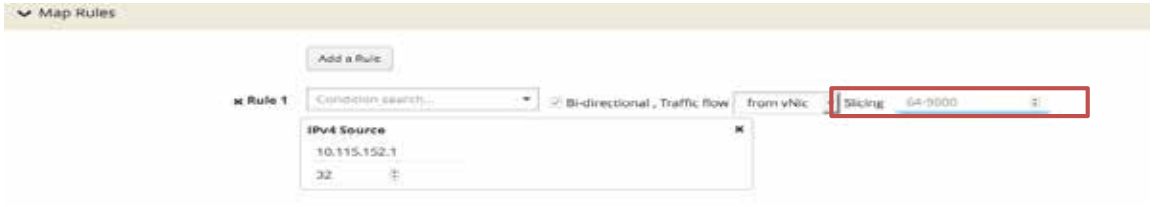

Figure 17 Conserve Network Backhaul

GigaSMART Service Chaining

A combination of GigaSMART services can be chained as seen in Figure 18 with “tenant filtering” to provide additional visibility

- Metadata (NetFlow/IPFIX) to generate billing or monitor network SLAs.
- SSL Decryption to “decrypt SSL packets”, thereby optimizing the monitoring infrastructure.
- Masking to hide sensitive information, such as SSN or credit card numbers .

Figure 18: Sample GigaSMART Service Chaining

8 Use Cases

SDDC provide a different approach to enable fast provisioning of networking and security services, simplified operations and fundamentally better security to data centers. Gigamon and VMware have developed an integrated solution that leverages Gigamon's SDP enabled by the unified visibility Fabric and VMware NSX network virtualization. This solution delivers. Below are couple of uses cases to showcase how the integrated solution delivers pervasive and automated visibility of traffic traversing both physical and virtual workloads and networks

Use Case 1: Securing Micro-segments with Automated Traffic Visibility

IT Security teams continue to mitigate security threats with traditional security devices. But virtualization has caused the enterprise to explore new ways to extend the reach of security tools into the virtual infrastructure. With today's distributed application architecture that led to the growth in East-West traffic inside the hypervisor, security architects are looking for more efficient ways to gain visibility to that traffic on behalf of their existing and next-generation security appliances, such as IDS/IPS, Web server security, integrity monitoring and malware inspection, along with several other tools.

Security tools such as perimeter firewalls and IDS/IPS sensors are commonly deployed at the perimeter of the network, where they inspect network traffic between untrusted zones like the Internet and trusted zones such as the core data center or end-user networks. However, today's security threat mitigation can no longer be accomplished with just a firewall and IPS sensor. Comprehensive security must encompass all threat vectors including but not limited to, e-mail scanning, Web application security, malware detection and granular application control. These tools rely on live packet streams on the wire. They also rely on end to end packet flows between network segments, servers and end-users. As the infrastructure is virtualized and the traffic migrates inside the virtual switch, tools examining that traffic can go dark—the virtual network becomes a hidden silo of IT.

With most Web application traffic hosted in the virtualized data center using SSL, the data center administrator now has multiple blind spots to deal with.

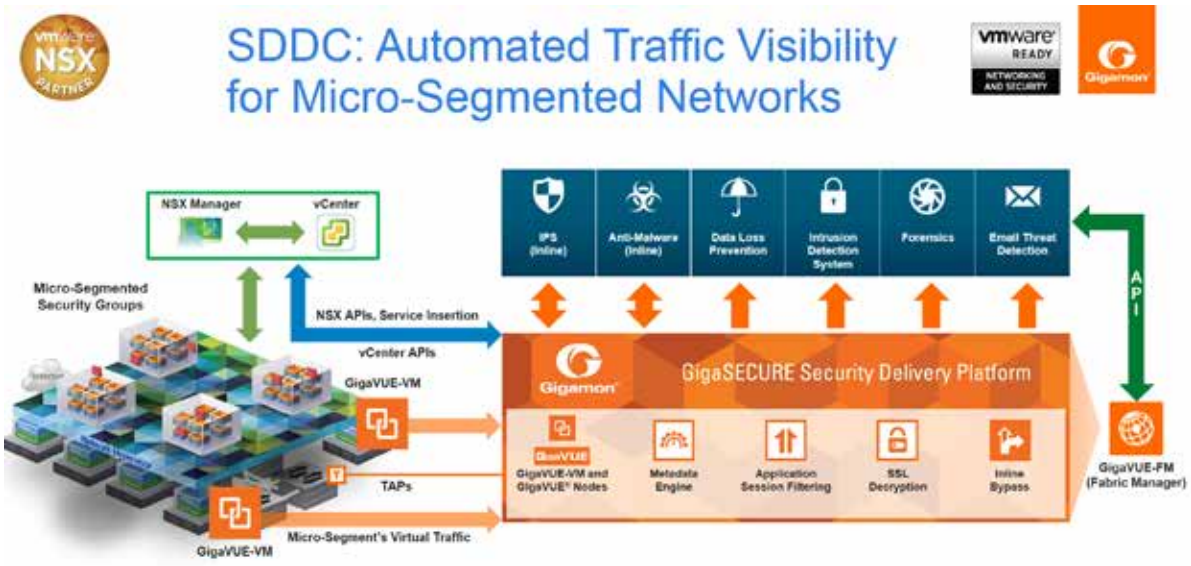

Figure 19: Automating Traffic Visibility for Micro-Segmented Networks

Gigamon's GigaVUE-VM provides automated traffic visibility for SDDCs using dynamic service insertion. GigaVUE-FM is used to discover the inventory of the SDDC managed by vCenter and NSX Manager using NSX APIs. This registers Gigamon "Traffic Visibility Service" and "Traffic Policies" with NSX. vCenter security user can then define and associate traffic policies to NSX Security Group using NSX APIs. Finally, VMware NetX APIs is used to filter and copy the tenant's virtual traffic to GigaVUE-VM.

The solution not only provides traffic visibility for existing virtual workloads but also what also provides automated traffic visibility for new VMs in the Security Group as n-tier applications scale out. Traffic monitoring policies associated with the Security Group are automatically applied and visibility is available almost immediately for new VMs. GigaVUE-VM adds additional L2-L4 filtering and packet slicing optimizations and forwards the traffic to the Gigamon Security Delivery Platform which provides addition traffic optimization such as netflow/metadata generation or SSL decryption before delivery the traffic to monitoring tool farm.

Use Case 2: Virtual Network (Tenant) Filtering and Monitoring

VXLAN helps solve the data center networking challenge. It provides the capability to create isolated, multi-tenant broadcast domains across data center fabrics and enables customers to create elastic, logical networks that span physical network boundaries. Thus virtualizing the network and creating networks that meet the agility, performance, and scale requirements of virtualized applications and data.

This method not only allows very large numbers of isolated Layer 2 VXLAN networks to coexist on a common Layer 3 infrastructure, it also allows virtual machines to reside on the same Layer 2 virtual network but be on two different Layer 3 networks.

With a 24-bit segment ID to uniquely identify broadcast domains, VXLAN enables multi-tenant environments at cloud scale and extends the Layer 2 network across physical boundaries by encapsulating the original frames in a MAC-in-UDP encapsulation.

The VXLAN encapsulated traffic can be sent to the Visibility Fabric architecture, which can utilize the processing capabilities provided by GigaSMART to filter on the segment-ID (Adaptive Packet Filtering) to forward and/or de-capsulate (Header Stripping) specific traffic flows before forwarding to the monitoring tools that need access to this information.

The network and security analyzers that need critical visibility into the UDP encapsulated traffic can now monitor the security and performance of the VXLAN virtual overlay network without any hardware or software modifications.

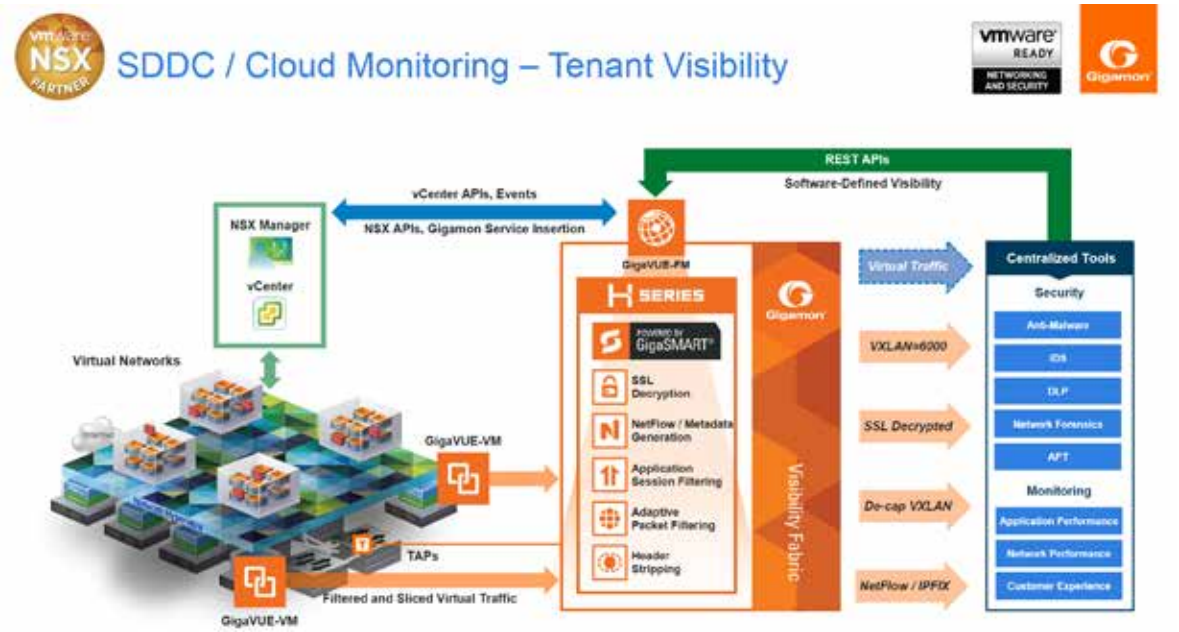

Figure 20: SDDC / Cloud Monitoring – Tenant and Application Visibility

Monitoring performance of VXLAN endpoints is the key to enabling network and security operations teams to control and comprehend the "virtual" domains floated on top of the common networking and virtualization infrastructure.

9 Conclusion

The VMware network virtualization solution addresses current challenges with physical network infrastructure and brings flexibility, agility, and scale through VXLAN-based logical networks. Along with the ability to create on-demand logical networks using VXLAN, the vCloud Networking, and Security Edge gateway helps users deploy various logical network services such as firewall, DHCP, NAT, and load balancing on these networks.

The VMware NSX and Gigamon integrated solution extends the monitoring delivered by the NSX virtualization platform. The joint solution provides an integrated data center solution that allows IT organizations to unlock all the benefits of the software defined data center, from greater flexibility and agility to optimized capacity utilization and operational efficiencies, without compromising security. IT administrators can now provide comprehensive visibility and safe enablement of all data center traffic, including intra-server virtual machine communications.

About VMware

VMware is radically transforming IT with technologies that make your business more agile, efficient, and profitable. A pioneer in virtualization and policy-driven automation, VMware simplifies IT complexity across the entire data center. VMware delivers value to more than 500,000 customers through virtualization software, professional services, and a robust ecosystem of more than 55,000 partners that drive application interoperability and customer choice.

For more information about VMware NSX visit:
www.vmware.com/nsx*http://www.vmware.com/nsx*

http://www.vmware.com/nsx

About Gigamon

Gigamon provides active visibility into physical and virtual network traffic, enabling stronger security and superior performance. Gigamon's Visibility Fabric™ and GigaSECURE®, the industry's first Security Delivery Platform, deliver advanced intelligence so that security, network, and application performance management solutions in enterprise, government, and service provider networks operate more efficiently. As data volumes and network speeds grow and threats become more sophisticated, tools are increasingly overburdened. One hundred percent visibility is imperative. Gigamon is installed in more than three-quarters of the Fortune 100, more than half of the Fortune 500, and seven of the 10 largest service providers.

For more information about the Gigamon Unified Visibility Fabric visit: ***www.gigamon.com***

See Inside Your Network™

4088-01 08/16