Gigamon®

Whitepaper

The Road to SDN is Paved with Visibility and Many Good Intentions

Introduction

Network architectures are in the midst of massive transformation. Not too long ago traditional network designs began to strain under increased demand for compute and storage. This saw the advent of server and storage virtualization so that organizations could have on-demand access to resources required for supporting service oriented architectures and machine-to-machine communications. The increased agility and provisioning of virtualization showed the immense flexibility of decoupling key network components from the underlying hardware and catalyzed what is now a movement toward software defined networking (SDN).

While SDN and network virtualization (NV) rollouts are far from common, practically all organizations are making plans to accommodate this eventual architectural shift, which will transform networking in a way unseen in decades. As organizations consider how they benefit from SDN they will undoubtedly need to shore up their institutional knowledge and staff skill sets in the areas of software defined architectures and network function virtualization. In order to help, this paper brings together information from various sources to explain basic SDN concepts and terminology, lays out the benefits of SDN as well as offers market trends and practical advice for mapping the journey. The centerpiece of this guidance lies with pervasive network visibility. This paper concludes with explaining how starting today, organizations have access to this one unifying framework that is easy and fast to implement, and serves as a foundational building block to see them through server virtualization, to SDN, to cloud adoption and beyond.

Background

What is SDN

SDN architecture separates or decouples the control plane (i.e administration layer) from the data plane (i.e data forwarding layer). The resulting architecture is a highly programmable and scalable one where the control framework can view and provision the network as a single logical abstraction. In this kind of architecture, the orchestration and provisioning of services is easier to manage with desired configurations applied consistently and automatically. This unlocks whole new levels of scale and agility as well as choice in underlying hardware infrastructure. Beyond significant savings in CAPEX and OPEX the SDN architecture spurs innovation and accommodates change quickly and to the benefit of those it serves with little disruption and overhead.

How are Software-Defined Visibility and Network Function Virtualization related

Software defined networking (SDN) and network function virtualization (NFV) are complementary. For that matter, other complementary concepts are those of network virtualization (NV) and white box switching. In the end all of these concepts are about abstracting the software from the underlying hardware such that the functions of the former are portable and don't have a hardware dependence.

- SDN: the decoupling of the network control layer from the data or forwarding layer. This is at the highest level of abstraction and treats the network as a whole
- NFV: this is focused at specific network services a small representative list of which are DNS, network address translation, security services like firewalling, IPS, advanced threat detection, as well as WAN optimization and CDN
- NV: this is really about optimizing use of network bandwidth by treating it as an available whole that can be carved up and assigned to servers or more likely virtual machines as needed in near-real time

The role of OpenFlow

OpenFlow has been erroneously used as a synonym for SDN. It was in fact one of the first open standards to define the communications paths and interfaces between the control and forwarding plane of an SDN. The image below outlines the current structure of OpenFlow as put forward and managed by the Open Network Foundation (ONF).

In this structure, an SDN Controller functions as central command for the SDN. It communicates with routers and switches at the infrastructure layer via APIs like OpenFlow and the Open Virtual Switch Database (OVSDB). APIs are also the means by which the controller provisions applications.

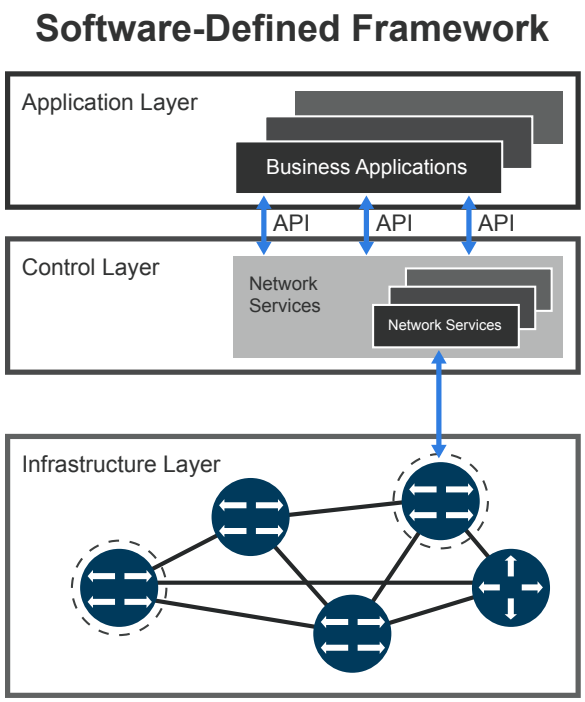

Figure 1: SDN architecture

The choice of protocols and SDN controller in particular have been at the source of a fierce industry battle that is still playing out among established networking vendors and newer players alike. The choices span open source controllers like NOX (developed by Nicira now VMware), POX, Beacon, and the more recent OpenDaylight, which enjoys broad market support from vendors large and small like Cisco, Citrix, Ericsson, HP, IBM and Juniper see list. Many of these vendors offer commercial versions of controllers that are open source derivatives while others have purpose-built proprietary offerings that may or may not be open sourced in the future. Firms like AT&T, Ciena, Fujitsu, Huawei, NTT, and Intel are also offering an alternative to OpenDaylight with the Open Network Operating System (ONOS).

A lot is riding on the choice of controller and the supported protocols since it will determine the SDN architecture and its interactions with infrastructure including existing routers and switches.

A word on OpenStack

Started in 2010 as a joint effort between RackSpace and NASA, OpenStack is now a global community of users and contributors administered by the OpenStack Foundation. The OpenStack goal is to bring the flexibility and scale of open source to the design of public and private clouds. Any service provider, company, government agency, or organization that wants to avoid vendor lock-in in the design and building of new data centers may want to consider the benefit that an OpenStack approach provides long term. As of this writing over 150 companies have agreed to contribute code and expertise to the OpenStack foundation effort.

The OpenStack architecture is modular and employs codenames for what are commonly known parts of a cloud computing architecture like compute, storage, networking and virtual machine monitoring to name a few (see below):

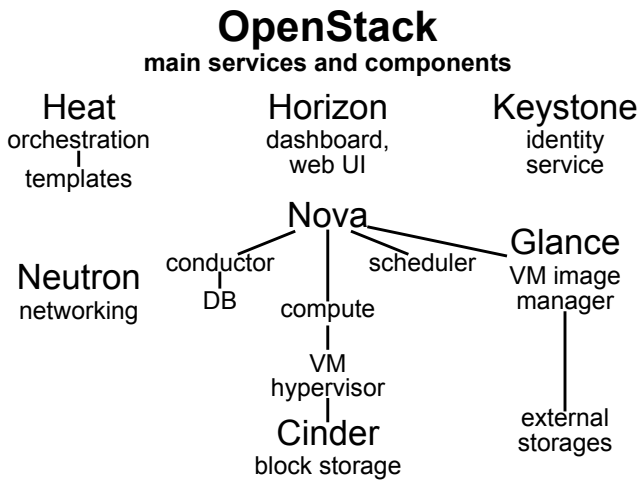

Figure 2: OpenStack main services and components[1]

In times past, many analysts and the industry at large have questioned the viability of OpenStack, citing an absence of broad use cases for the open source approach, a concern which is diminishing as enterprise use cases like Overstock.com, Paypal, and many others join FICO and NASA. Still, there are some concerns about scale-out, interoperability, and NFV to warrant research about which cloud architecture (i.e. proprietary, limited distribution, or open) option is right for your organization.

The business case for SDN and NFV

Network infrastructure has not seen massive change in decades. Part of the reason is that today's high performance networks run on purpose-built hardware with custom silicon that represents enormous investment on the part of the companies that have brought them to market. Implementers too have devoted significant resources in the people with specialized skills and certifications that are required to maintain today's network infrastructure. This state of affairs has made any kind of customization and network design flexibility extremely difficult until recently.

[1]Source: https://en.wikipedia.org/wiki/OpenStack

With SDN, customers have more options in their choice of infrastructure. Off the shelf hardware, with or without the OS and basic networking services installed, is available as are white box switches marketed precisely because of their flexibility and customizability. Network designers still have to make some trade offs in performance versus flexibility, but with more latitude than ever before, the innovation in this area continues rapidly. In fact, many vendors of purpose-built appliances for network and networking services now offer their functionality as software-only bundles and subscription services. In a nutshell, SDN and NFV:

1. Are serving as catalysts for innovation and accelerating its pace
2. Give customers more leverage in the sourcing of networking infrastructure
3. Open the door to new services and applications that may have been non-options because of hardware dependence
4. Reduce CAPEX through shared infrastructure use, which greatly expands the number of tenants and resources that can served
5. Reduce OPEX through centralized control and orchestration of network services and resources that expedites administration and service delivery
6. Make organizations more competitive and, in the case of public sector, more responsive through network flexibility and scaling that is business driven and at-will

Security challenges with SDN

Modern threats target traffic inside networks and data centers. They may enter the data center hiding within authorized devices or traffic streams, but once inside they propagate laterally, server-to-server. In theory, security controls and devices can be applied at each data center segment, but in reality this is impractical from a scale and performance perspective especially given growing network speeds and traffic volumes. When security is introduced it is rarely pervasive or granular. Also, despite some innovation in this area, the unification of security policies and application control across physical and virtual workloads is simply not a realistic deployment option at least today. As a result, data centers remain highly vulnerable and the favorite targets of attackers because they often house an organization's most valuable data. This situation becomes more acute in SDN architectures where reference designs and best practices don't exist yet and automation may unwittingly serve to proliferate threats more quickly and broadly in the network.

Customers and Adoption

SDN Market Forecast

In less than five years practically every network purchase will be scrutinized for SDN readiness and fit. See the 2015 SDN market report at SDXCentral: https://www.sdxcentral.com/flow/sdn-software-defined-networking/.

Use cases

Campus and branch—One of the key concerns in campus networks is network access control (NAC) or ensuring that users connect to networks securely and with access to only those services and applications required regardless of which device is used or where the connection takes place. The centralized control and provisioning capabilities within SDN can ensure that users' experience accessing required resources is seamless, independent of the underlying infrastructure, and that connectivity is consistent with the security and business profile that the organization has bestowed on the user. Changes in the security posture or accessibility needs can automatically trigger a rapid re-provisioning of the resources required without manual intervention or delays.

Data centers—With big data warehousing and massive increases in east/west and machine-to-machine traffic, data center designs are all about scale. SDN and NFV can extend the benefits of server and storage virtualization with on the fly service and application provisioning. Applications are spun up according to business need with the requisite amount of compute and security services automatically assigned as well.

Cloud—Private, hybrid, and even public clouds are really specialized data centers where agile resource allocation and infinite segmentation is key. With SDN and NFV architectures in play, clouds can be micro segmented giving tenants maximum control, ensuring resource privacy and the ability for threat containment. With the SDN data center and cloud provisioned as a logical whole, the management overhead is lower and the carbon footprint is maintained at the optimal level for the load.

Service providers—SDN and NFV offer many benefits for carriers and mobile network operators who want not only to scale, but to monetize every aspect of their infrastructure investments. With centralized control and provisioning, carriers can offer users and businesses services based on the customized bundles for desired applications, performance levels and security. On the fly and even self-service provisioning can mean huge gains in usage based revenue, competitive differentiation and customer loyalty. Also, the ability to source infrastructure with a variety and vendors and pricing models as an option can dramatically reduce the CAPEX or at least improve the ROI of SDN and NFV rollouts.

The State of Standards

SDN adoption might be proceeding faster were it not for the battle for standards and ensuing confusion this causes among adopters. Network and data center architects naturally want to make choices that will maximize the return on their investments and ensure that they capture the full benefit of SDN and NFV.

The diversity of SDN controllers outlined in a previous section of this document highlight the overabundance of choices and it is a situation which is replicated within NFV with options from ETSI, OPNFV, the OpenDaylight Project, the IETF, and the MEF. Still, there are options for stair-stepping into SDN and they do not require waiting for the standards dramas to play out in their entirety.

Migration to SDN

Detailing the path to SDN

While some organizations may be in a position to conduct net new build outs for SDN, the majority will likely build out hybrid networks of traditional infrastructure side by side with SDN capable routers and switches and dynamically provisioned workloads. In order to ensure successful operation of such an environment, visibility to traffic in both types of networks will be key, as will a way to correlate administration.

The hybrid network design is appealing in that it does not require whole cloth investment in SDN-ready gear, but stair stepping into SDN rather than changing the entire data center to the model, and can minimize the disruption to business operations that such a transition can have. At the same time, the portions of the network that are software defined will offer the benefits of automated and expedited provisioning as well as high quality of service (QoS) to those applications that are being served from it.

For most organizations, the vendors of their installed networking infrastructure, or those vendors under evaluation, will have offerings that allow for a gradual migration to an SDN architecture. This vendor list includes all of the large networking players such as Cisco, IBM, VMware, HP, Juniper, Brocade, and others, as well as start-ups. As mentioned earlier, since each may have implemented certain controllers and protocols, it is important to understand how the choice of today will impact the longer-term design options for the SDN that is being installed.

Timelines and considerations

The most important step in an SDN migration is arguably the planning phase. The overarching goal is to begin to reap SDN benefits in some measure while leveraging existing infrastructure to keep initial costs down and minimize disruption.

Asking key questions and documenting the responses in as much detail as possible will serve as the working blueprint of the SDN migration. Each organization is different so the number and types of questions may vary, but a representative list to be answered will include:

- Which business goals are driving the migration to SDN
- Which applications should be served from the SDN architecture initially
- Which vendors and/or protocols are being considered for the SDN infrastructure and why
- What are all the security controls that must be replicated from the legacy network at a minimum within the SDN
- Which are the milestones and timeframes that will define the phases of the migration
- Are there successful migrations which closely parallel desired architecture and goals and can serve as a frame of reference
- How will success be measured and communicated
- What resources are required for a successful migration

The Role of Visibility In SDN

Overview

SDN promises to transform our modern networks and data centers, turning them into highly agile frameworks that can be quickly reconfigured for changing business needs. Still, many organizations recognize that highly mobile workloads and auto-configured applications and services mean a likely loss of visibility to traffic and consequently loss of both performance optimization capabilities and security.

Network visibility is a foundational element in terrestrial networks and becomes more critical in highly dynamic SDN architectures. Loss of network visibility does not need to hinder firms from moving forward with SDN however. Companies like Gigamon® have taken steps to engage with both the standards community and the leading vendors of SDN architecture to ensure that application performance and security are maintained both during an SDN migration and after its completion.

Accelerating SDN adoption with a Visibility Fabric

Gigamon is a company that pioneered network visibility delivering intelligent traffic forwarding as part of a centralized and highly scalable Visibility Fabric™. The company further extended the capabilities of the Visibility Fabric enabling its implementation as a Security Delivery Platform (SDP) or a central place from which security devices of all types can be deployed alongside solutions for packet capture, performance monitoring, and analytics.

Network visibility, as a pervasive layer, is nowhere more relevant or important than in SDN deployments. Specifically, detailed knowledge of the traffic flows and packets in these networks becomes vital for:

1. Monitoring the state of the SDN network itself
2. Monitoring the applications it enables
3. Ensuring security is maintained

Whether the SDN architecture of choice is built on OpenFlow or network virtualization abstractions like VMware's NSX and Cisco's ACI, or still some other framework, the key requirements above remain. In SDN, control and forwarding layers are managed independently yet need to function together. Synchronization issues between these layers due to network latency or vendor variance in networking infrastructure can cause bottlenecks and disrupt operations. When it comes to SDN applications and services, the benefits of on-demand provisioning are undeniable. But this sort of dynamic configuration can result in unpredictable traffic patterns that become hard to troubleshoot via traditional means, which place performance management tools at predictable places in the network. Visibility to such traffic in the SDN realm needs to be constant and the tools centralized so that they can receive all traffic flows and packets. Similar logic applies to the need for security. Whereas security devices could be placed on critical network segments in traditional networks, this is not possible in SDNs because the critical points of the network are not known but rather change and quite frequently as new resources and communications rules are provisioned. Centralized placement and total access to all inter-SDN traffic gives security technologies the best statistical chance of surfacing embedded malware and anomalous patterns.

To explain the point further, three specific SDN uses cases are outlined below.

The VMware NSX Software Defined Data Center (SDDC)

One of the key elements of making the move to the SDDC is the ability of IT to manage, monitor and secure the SDDC while continuing to leverage investments in existing tools. Network virtualization solutions like VMware's NSX and Cisco ACI introduce the concepts of overlay and underlay networks. Overlay networks are typically virtual networks that provide tenant isolation as well as service isolation in addition to the separation of location and identity. The physical network infrastructure typically serves as the underlay network. Virtual overlays can be instantiated, extended and removed dynamically based on tenant subscriptions, service guarantees and VM mobility; all of which makes the underlying physical infrastructure more efficient.

However, they also make the job of troubleshooting and monitoring more complex. The dynamic nature of the overlays, the need to correlate and track traffic between the underlay and overlays, the existing departmental silos between the server and network teams—particularly when the overlays are instantiated in the server/hypervisor domain, but are routed over a physical underlay network—can all be barriers to rapid troubleshooting, performance optimization, and security. Furthermore, they introduce multiple planes of traffic to be monitored and secured. Similarly, VM migration now occurs over a segmented Layer 3 underlay network through the use of network overlays, thereby maintaining session continuity. This allows the underlying physical infrastructure to scale out through Layer 3 segmentation. However, it also poses a challenge from the perspective of application performance management (APM) and security

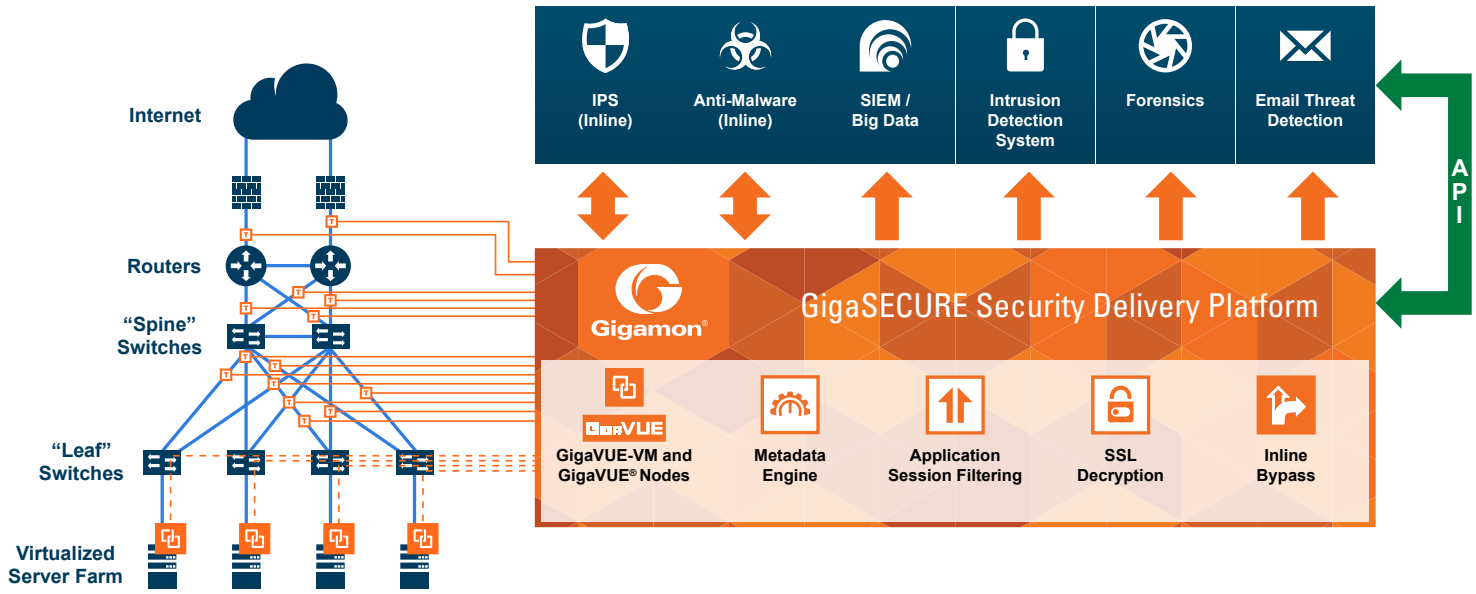

Figure 3: Visibility Fabric for hybrid SDN preserves tool investments, traffic monitoring for physical and SDN segments

monitoring. This is because the tools that depend on traffic visibility for analyzing application performance or for managing and limiting the threat envelope, can encounter blind spots when VMs move to different locations and their traffic is no longer visible to the tool at its original location.

Gigamon's integrated VMware solution addresses these challenges in both hybrid and green-field SDN deployments. As shown in the diagram below, a Gigamon Security Delivery Platform sits between the SDN architecture and existing security and performance management tools bringing SDN visibility to all of them. Virtualized TAPs deliver the traffic, flows, and packets to the SDP that then forwards copies of that traffic to all the tools requiring it. And integration with NSX Manager and vCenter enables automated deployment of the virtual components or TAPs in the GigaSECURE® Security Delivery Platform, while also enabling dynamic provisioning of visibility traffic policies within software defined data centers.

The VMware NSX Multi-Tenant SDDC/Cloud

In the multi-tenant SDDC, resources are partitioned into logical entities mapping to customers' organizations, otherwise known as cloud "tenants". In this instance the data center or cloud operator needs to manage the virtualized network as a whole delivering security inspection and monitoring services to all tenants while ensuring isolation of tenant resources from each other. In the deployment shown below, the integration of VMware's cloud management platform (vRealize Automation) and/or NSX Manager with Gigamon's Security Delivery Platform enables

- Insertion of a Visibility Service using the GigaSECURE Virtual Visibility component, GigaVUE-VM
- Definition of security or traffic policies that select, filter, and forward the tenant's virtual traffic to security and monitoring tools for analysis

The service and the traffic policies are auto-updated as new tenants come onboard or existing tenants' security groups scale dynamically.

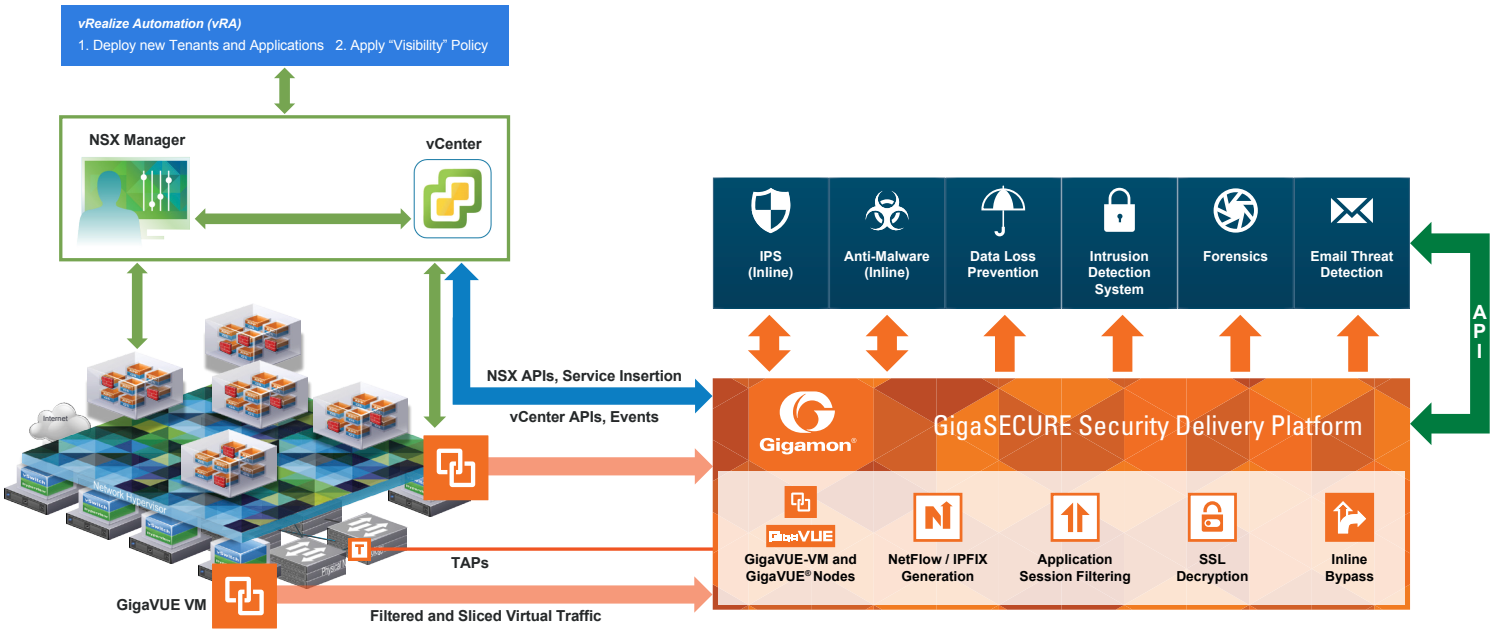

Figure 4: Securing the VMware NSX Software Defined Data Center (SDDC)

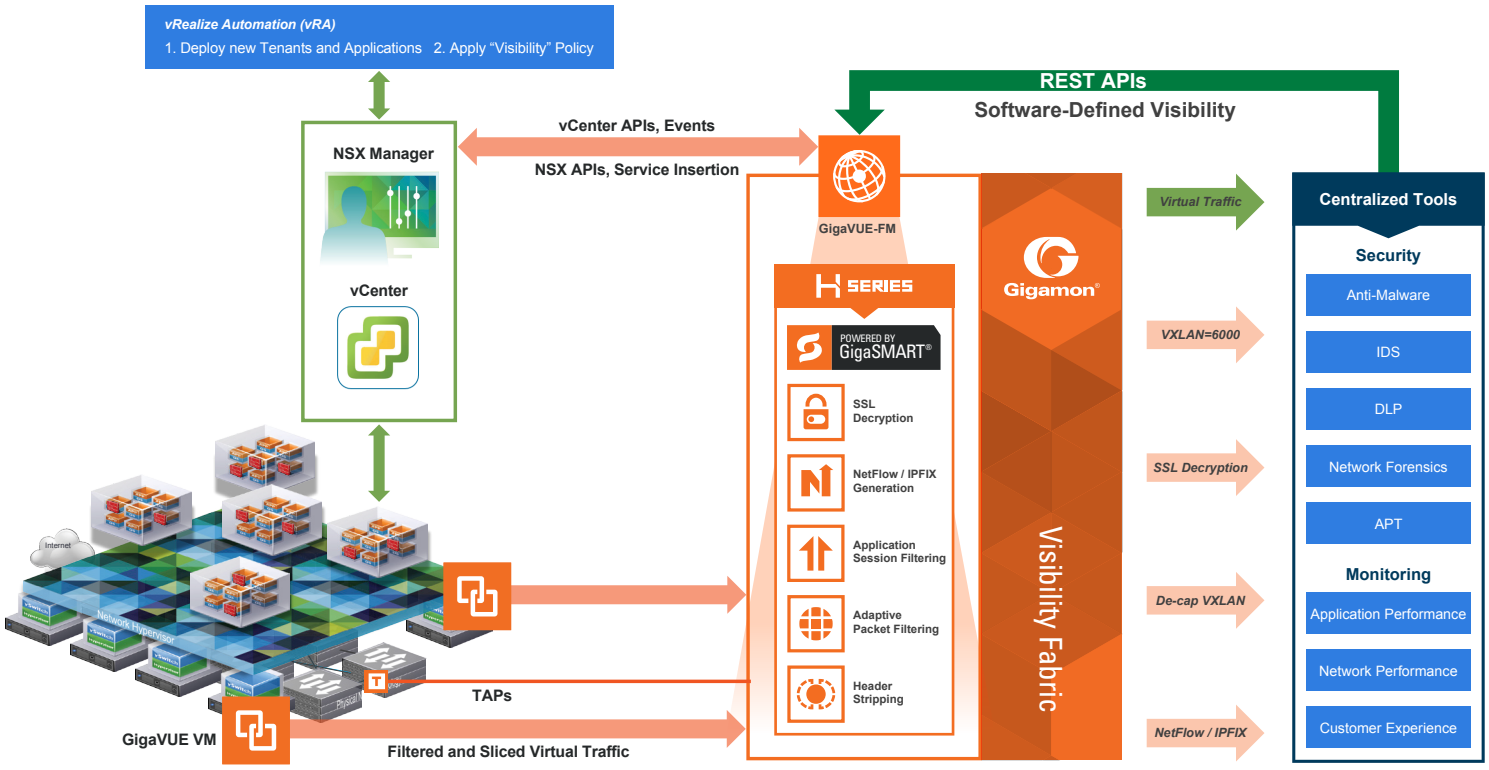

Figure 5: Tenant-level traffic visibility for monitoring for VMware NSX SDDCs

The Cisco ACI Software Defined Network

The ACI architecture also uses the overlay/underlay concepts of network virtualization. The Application Policy Infrastructure Controller (APIC) is the unified point of policy enforcement and translates the application-centric policies to network policy configuration that is programmed into the underlying ACI fabric. For a network administrator, it is important to have the necessary visibility into the communication between the APIC and the physical/virtual nodes to immediately determine if the APIC and the infrastructure state go out of sync. Further, being able to correlate network traffic activity to what the controller expects the switches to be doing is a vital aspect of ensuring the success of SDN deployments.

Like VMware, Cisco ACI uses VXLAN tagging to segment traffic in the virtualized network. And like the VMware NSX environment, Gigamon's Security Delivery Platform bridges the visibility gap retrieving traffic from physical and virtualized network segments and sending it to the attached tooling. GigaSECURE policy-based forwarding optionally strips VXLAN tags for traffic being sent to those security and application management tools that don't support them and would otherwise be non-functional in the SDN.

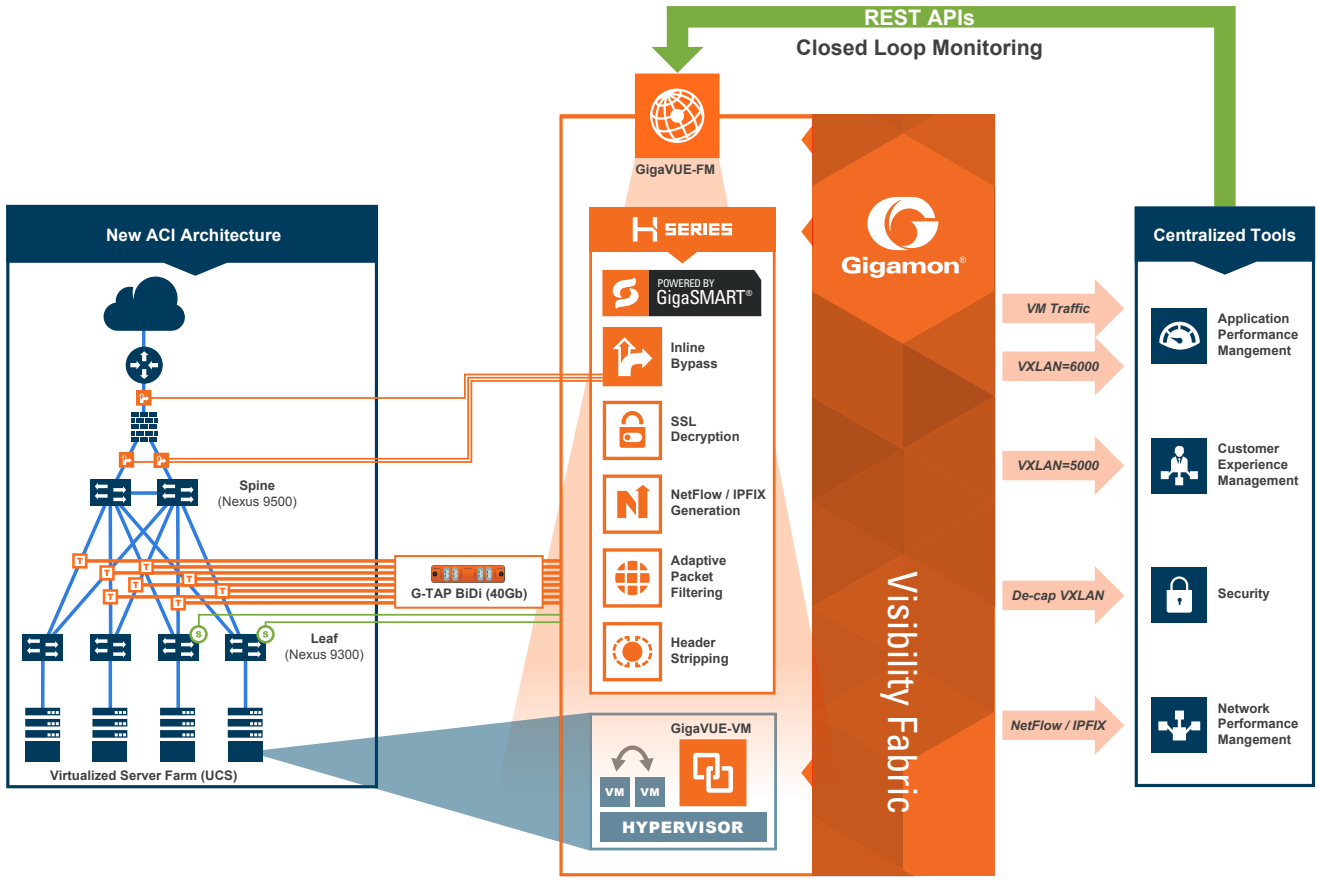

Figure 6: Monitoring and security for Cisco ACI

OpenStack Clouds And Visibility

The number of OpenStack deployments in production status has nearly doubled since 2013. As adoption becomes increasingly mainstream, users must consider the following:

1. How security for prevention, detection and forensics will be implemented
2. Whether migrated applications still meet SLA and compliance mandates
3. How analysis and troubleshooting will work, especially in SP clouds
4. Can existing architecture for performance management and security be reused

One of the basic ways to meet several of these design goals is to ensure visibility to traffic flows in OpenStack clouds. As the leader in network visibility, Gigamon has conducted pioneering work in the area of public cloud visibility which it calls Tap-as-a-Service (TaaS) and offers as part of the OpenStack open source framework.

TaaS is a platform-oriented solution, designed to operate as an extension of Neutron, the OpenStack network service. TaaS offers a simple API that will enable a tenant (or the cloud administrator) to monitor ports in Neutron-provisioned networks. Since it is vital that tenant boundaries are not compromised, a tenant can only monitor its own ports, i.e. any port on one of its private virtual networks or a port created by it on a shared virtual network. The TaaS workflow begins with the creation of a tap-service instance that has a Neutron port serving as the destination side of a port-mirror session. A monitoring virtual machine is usually attached to this port to consume the mirrored traffic. Later, one or more tap-flows can be added to the tap-service instance. A tap-flow represents the association between a (source) port that is being monitored and a tap-service instance. TaaS allows a mirror session to span across multiple hosts, by virtue of remote port-mirroring, thereby ensuring that location independence is preserved.

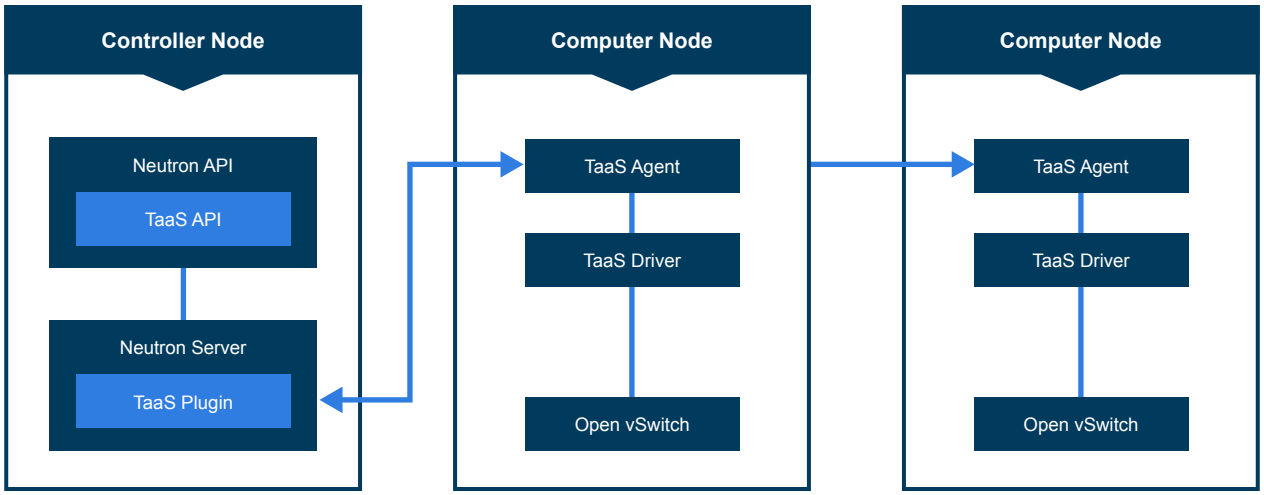

Figure 7: Tap-as-a-Service (TaaS) offers a simple API that will enable a tenant to monitor ports in Neutron-provisioned networks

Port mirroring used to be a switch layer function. Tap-as-a-Service has effectively virtualized this capability and made it available for the users of Neutron provisioned networks. Gigamon sees TaaS as the basic building block on top of which more complex traffic visibility solutions can be engineered for a diverse set of use cases, ranging from network administration and trouble-shooting to application/network security, data analytics and more.

Summary

SDN, NFV, and network virtualization are finally a reality and they are transforming networking permanently and for the better. Most organizations will make the transition embracing one, two, or all three concepts. Those that will make the journey with the least disruption are those who understand how fundamental traffic visibility is to that end. On demand networking brings unprecedented, agility, scale and dynamism to network design. Understanding traffic pathways and baselines before during and after the SDN migration means knowing how well the transition is delivering on CAPEX and OPEX promises as well as potential for higher security.

The Gigamon Security Delivery Platform centered on a Visibility Fabric works in conjunction with the SDN deployment to create an imperative third layer to the control and forwarding planes. With it the layers of SDN can collaborate, automate, and provision reducing errors and eliminating security blind spots.

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 and effectively. For more information visit **www.gigamon.com**

3185-03 02/16

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