IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 1, Ver. IV (Jan.-Feb. 2017), PP 70-72
www.iosrjournals.org

Comparison between Cisco ACI and VMWARE NSX

Palash Ijari
(Computer Science, Kle Technological University, India)

Abstract: *Software-Defined Networking(SDN) allows you to have a logical image of the components in the data center, also you could arrange the components logically and use them according to the software application needs. This paper gives an overview about the architectural features of Cisco's Application Centric Infrastructure (ACI) and Vmware's NSX and also compares both the architectures and their benefits.*
Keywords: *ACI, NCX, Nexus, Vmware, VLAN, VXLAN, NVGRE SDDC.*

I. Introduction

Software Defined Network (SDN) is an emerging network framework that it separates the control plane from the data plane. There are three layers in the SDN network architecture: application, control, and infrastructure layers. The application layer uses application programming interfaces (APIs) to communicate with controllers. Open Flow protocol is the first standardized protocol defined between the control and the infrastructure layer, and it allows network administrators to make decisions about how data flows should be routed between switches and network entities in networks. With the characteristics of the flexibility property and the central management, the wireless networks can obtain benefits from the SDN evolution to fulfill the 5G capacity booming. This paper aims to compare the SDN of two leading companies, CISCO and VMware. The parameters taken into consideration are functionality, efficiency, security and speed. New parties looking to adopt either of these systems can choose the most suitable system.

II. Cisco ACI

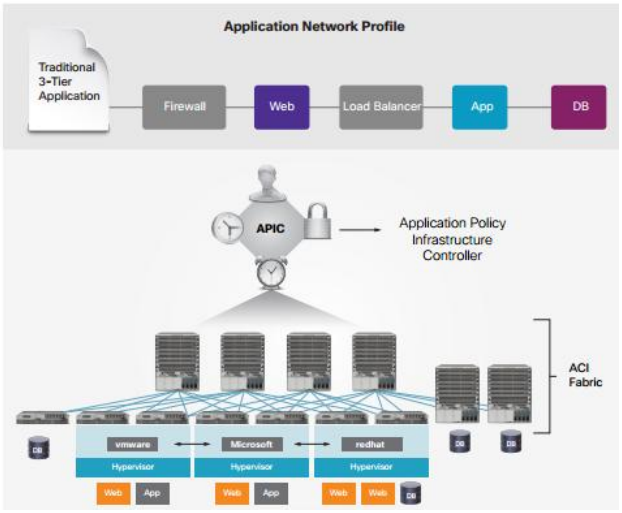
Cisco ACI is a tightly coupled policy-driven solution that integrates software and hardware. The hardware for Cisco ACI is based on the Cisco Nexus 9000 family of switches. The software and integration points for ACI include a few components, including Additional Data Center Pod**,** Data Center Policy Engine, and Non-Directly Attached Virtual and Physical Leaf Switches. While there isn't an explicit reliance on any specific virtual switch, at this point, policies can only be pushed down to the virtual switches if Cisco's Application Virtual Switch (AVS) is used, though there has been talk about extending this to Open vSwitch in the near future.

To a large extent, the network for Cisco ACI is no different than what has been deployed over the past several years in enterprise data centers. What is different, however, is the management and policy framework, along with the protocols used in the underlying fabric.

In a leaf-spine ACI fabric, Cisco is provisioning a native Layer 3 IP fabric that supports equal-cost multi-path (ECMP) routing between any two endpoints in the network, but uses overlay protocols, such as virtual extensible local area network (VXLAN) under the covers to allow any workload to exist anywhere in the network. Supporting overlay protocols is what will give the fabric the ability to have machines, either physical or virtual, in the same logical network (Layer 2 domain), even while running Layer 3 routing down to the top of each rack. Cisco ACI supports VLAN, VXLAN, and network virtualization using generic routing encapsulation (NV-GRE), which can be combined and bridged together to create a logical network/domain as needed.

From a management perspective, the central SDN Controller of the ACI solution, the Application Policy Infrastructure Controller (APIC) manages and configures the policy on each of the switches in the ACI fabric. Hardware becomes stateless with Cisco ACI, much like it is with Cisco's UCS Computing Platform. This means no configuration is tied to the device. The APIC acts as a central repository for all policies and has the ability to rapidly deploy and re-deploy hardware, as needed, by using this stateless computing model.

Cisco ACI also serves as a platform for other services that are required within the data center or cloud environment. Through the use of the APIC, 3rd party services can be integrated for advanced security, load balancing, and monitoring. Vendors and products, such as Source Fire, Embrane, F5, Cisco ASA, and Citrix can integrate natively into the ACI fabric and be part of the policy defined by the admin. Through the use of northbound APIs on the APIC, ACI can also integrate with different types of cloud environments.



CISCO ACI Architecture

III. VMWARE NSX

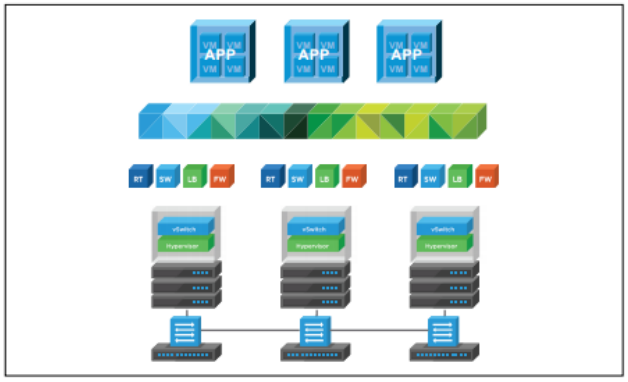
VMware NSX is the network virtualization platform for the Software-Defined Data Center (SDDC), delivering the operational model of a virtual machine for entire networks. With NSX, network functions including switching, routing, and firewalling are embedded in the hypervisor and distributed across the environment. This effectively creates a "network hypervisor" that acts as a platform for virtual networks and services. Similar to the operational model of virtual machines, virtual networks are programmatically provisioned and managed independently of underlying hardware. NSX reproduces the entire network model in software, enabling any network topology— from simple to complex multitier networks— to be created and provisioned in seconds. Users can create multiple virtual networks with diverse requirements, leveraging a combination of the services offered via NSX to build inherently more secure environments.

3.1 Network virtualization and SDDC

VMware NSX delivers a completely new operational model for networking that forms the foundation of the Software-Defined Data Center. Because NSX builds networks in software, data center operators can achieve levels of agility, security, and economics that were previously unreachable with physical networks. NSX provides a complete set of logical networking elements and services—including logical switching, routing, firewalling, load balancing, VPN, quality of service (QoS), and monitoring. These services are provisioned in virtual networks through any cloud management platform leveraging the NSX APIs. Virtual networks are deployed nondisruptively over any existing networking hardware.

3.2 Key Benefits

- Micro-segmentation and granular security delivered to the individual workload.
- Reduced network provisioning time from days to seconds and improved operational efficiency through automation
- Workload mobility independent of physical network topology within and across data centers
- Enhanced security and advanced networking services through an ecosystem of leading third-party vendors



VMware NSX Architecture

IV. Comparison of ACI And NSX

Starting with assessing NSX, the first step is to understand that with or without NSX, a physical network will be required to actually move packets between devices. In addition to this, modern data centers are only about 70% virtualized from a workload perspective. Legacy applications still exist on bare metal, while modern applications are written to utilize bare metal without the cost and overhead of a hypervisor. This means that you'll want to ensure you're able to provide network services and security to all existing workloads, without artificially choking traffic through hypervisors or server-based gateway devices.

Because NSX provides no management or visibility into the physical network that the NSX application utilizes, you'll want to ensure that any network chosen for NSX provides native automation for provisioning and network change, as well as advanced visibility and telemetry tools for troubleshooting and day-two operations. These tools should not be limited to simple databases for mapping virtual tunnels to VLANs, but offer more comprehensive visibility and automation, including firmware and patch management. Without this, your network will become more complex with two management and monitoring systems for performance and failure troubleshooting.

You'll next want to look at the hypervisors you're using, or could potentially use moving forward. More than half of data centres use multiple hypervisors, so you'll want to take this into account. When choosing NSX, you must choose between the VMware-only NSX for vSphere, or the multi-hypervisor version, VMware NSX-MH, which uses a VMware-proprietary distribution of Open vSwitch (OVS). Additionally, at the time of this writing, NSX-MH is being phased out. The two products are not compatible, and the features vary greatly between the two. Additionally, you'll want to consider licensing costs and future licensing model changes that may occur.

You'll next want to consider what the business objective/requirement is for NSX. Are you looking for an SDN solution to speed up deployment of new applications and services, the ability to move to cloud computing models, or the ability to move to agile software deployment models? If so, NSX may not be the right tool, because it focuses on only the VM-to-VM traffic pattern, with no ability to move traffic between VMs on different physical devices.

4.1 Security capabilities

If your goal is to tighten security and move beyond legacy perimeter-based defense postures, then NSX may be a solid choice for virtual traffic. This is especially true if you've chosen to standardize 100% on the VMware hypervisor and are (or intend to be) a 100% VMware-based virtualization environment. In this case, NSX offers segmentation abilities within the hypervisor by providing basic semi-stateful firewall capabilities within the virtual environment.

It's important to remember that even in this second scenario you'll need to have a separate set of security tools for physical environments. Even 100% VMware virtualized environments need security for vMotion, hypervisor management, IP storage ports, NSX management, gateway servers, and BUM (broadcast, unknown unicast, and multicast) appliances that are run as physical servers, etc. You'll also still utilize perimeter security, typically consisting of physical appliances that do not tie into NSX solutions

V. Conclusion

As with any major technology shift and product decision, it's important to gain a strong understanding of what the products offer, and what the business goals are for technological shift. It's best not to look at ACI and NSX as competing solutions, because they truly aren't. If your business requires a dynamically provisioned, scalable and programmable network, ACI is the leading choice. If your business requires hypervisor-level micro-segmentation for VM-to-VM traffic, NSX is a solid choice. If both are required by the business, the two can work together to meet those requirements.

References

Journal Papers:

[1]. Muzzamil Aziz, Sdn-Enabled Application-Aware Networking For Data Center Networks, Electronics, Circuits And Systems (Icecs)