How to leverage VMware NSX Platform to Secure Your Agency’s Software Defined Data Center

Software Defined Data Center – an Introduction

A Software Defined Data Center (SDDC) is arguably the Holy Grail end-state of the next-generation data center. The concept of SDDC envisions virtualization of all data center elements: compute, storage, networking, and security. Server consolidation, reduced physical complexity, increased operational efficiency, and the ability to dynamically re-purpose underlying resources to meet changing requirements are just a few reasons why many organizations are moving to SDDC architecture. Ultimately, SDDC helps fulfill the basic goals of enterprise IT:

• Simplification
• Consolidation
• Automation

Many organizations have taken the first step towards realizing the SDDC vision by virtualizing their servers with the help of VMware ESXi or Microsoft Hyper-V. Some are talking about storage virtualization. However, one of the most exciting areas of SDDC adoption is the field of Software Defined Networks (SDN), where VMware NSX is the largest and most mature player. Not only does VMware NSX provide a way to virtualize the classical network elements, it also provides some clever ways to safeguard your organization’s network, while also saving money.
There are many resources available on VMware NSX. However, they are either high level or very technical, and few focus on security. The goal of this whitepaper is to highlight the network security benefits of VMware NSX while providing enough technical details to help a Chief Information Security Officer (CISO) or a Security Operations Center (SOC) manager envision how NSX would integrate within the organization's information infrastructure.

VMware NSX – an Overview

The VMware NSX network virtualization platform is a critical component of VMware's SDDC architecture. NSX network virtualization delivers for networking what VMware has already delivered for compute and storage. In much the same way that server virtualization allows operators to programmatically create, snapshot, delete and restore software-based virtual machines (VMs) on demand, NSX enables virtual networks to be created, saved, deleted and restored on demand without requiring any reconfiguration of the physical network. The result fundamentally transforms the data center network operational model, reduces network provisioning time from days to minutes and dramatically simplifies network operations.

With network virtualization, the functional equivalent of a “network hypervisor” reproduces the complete set of Layer 2 to Layer 7 networking services (e.g., switching, routing, firewalling and load balancing) in software. As a result, these services can be programmatically assembled in any arbitrary combination, to produce unique, isolated virtual networks in a matter of seconds. The same way VMs are independent of the underlying x86 platform and allow IT to treat physical hosts as a pool of compute capacity, virtual networks are independent of the underlying IP network hardware and allow IT to treat the physical network as a pool of transport capacity that can be consumed and repurposed on demand.

NSX is a non-disruptive solution that can be deployed on any IP network, including existing data center network designs or next-generation fabric architectures from any vendor. With NSX, your organization already has the physical network infrastructure to stand up a full fledged SDDC.

NSX Security – a High-Level Explanation

The traditional, perimeter-based security model for the data center is becoming obsolete. Threats can still sneak through firewalls and Intrusion Prevention Systems (IPSs) while riding on legitimate access traffic. Once inside the defense perimeter, there are few controls in place to prevent malicious actors from moving laterally. With VMware NSX, there is a solution. NSX leverages the position of the hypervisor to securely acquire and share application context, the basis for distributed enforcement at each virtual interface. Furthermore, NSX uses network isolation, segmentation with firewalling, and advanced security services from ecosystem partners to implement unit-level trust and reduce the attack surface. Ultimately, VMware NSX makes possible a zero-trust security approach.

VMware NSX security is not like traditional firewall management. It is integrated and designed into NSX from the ground up. It operates in the kernel of every hypervisor. VMware NSX security policies can be applied more granularly than traditional firewalls. Instead of being tied primarily (or even solely) to IP addresses, rules can be enabled based on virtual containers, applications, and Active Directory identities – and they can be richer too, for example, by taking advantage of VM introspection capabilities.

Two other security gains also result from policy enforcement that becomes both more dynamic and more distributed:

**Dynamic network security** – With NSX virtual networks, security policies are automatically attached to workloads at the time of VM creation based on a flexible, hierarchical policy model. These policies will then “stick” with the VM through migrations and moves. Moreover, any centrally made changes to security policies are immediately distributed to each applicable virtual network.

**Distributed network security** – With NSX virtual networks, security policies are enforced at the very edges of the network (i.e., at the ingress/egress ports of each workload’s hypervisor-based vSwitch). This approach is far more effective than that used with traditional physical
networks, where organizations typically rely on a handful of centrally located security devices (which are blind to the majority of east-west traffic), or resort to an excessive amount of hairpinning to ensure that inter-VM traffic is properly controlled and inspected.

For cases where an organization requires more advanced next-generation security services, NSX can work with third-party vendors. The VMware NSX controller consolidates all configuration and state information for all network connections and services and enables it to be consumable by another service. The key to remember is that NSX is a platform, not a competing security product. Many security vendors have already partnered with VMware to take advantage of NSX’s distributed enforcement and automated provisioning capability. The current list of supported vendors includes Intel Security / McAfee, Palo Alto, Rapid 7, Symantec, Trend Micro and many others.

NSX Functional Components
VMware NSX provides a faithful reproduction of network and security services in software. In this section we provide a brief review of each component (see Figure 1).

- **NSX Manager** – centralized network management component of NSX; installed as a virtual appliance on any ESXi host
- **NSX Controller** – central control point for all logical switches within a network and maintains information about all virtual machines, hosts, logical switches and VXLANs
- **NSX Edge** – virtual router and security gateway; provides common gateway services such as DHCP, L2/L3 VPN, NAT, dynamic routing and L4-L7 load balancing; usually provides security for north-south traffic
- **NSX vSwitch** – operates in server hypervisors to form a software abstraction layer between VM servers and the physical network; enables extension of L2 segment or IP subnet anywhere in the NSX fabric irrespective of the physical network design
- **Distributed Firewall** – hypervisor kernel-embedded firewall that provides visibility and control for virtualized workloads and networks; usually provides security for east-west traffic

---

**FIGURE 1 - VMWARE NSX FUNCTIONAL COMPONENTS**

1. **Controller configuration** (logical Switches and Logical Routers)
2. **Logical Router**
3. **Load Balancer, Firewall, VPN configuration**
4. **Routing Configuration**

---

Hypervisor Extension Modules

- vDS
- vXLAN
- Distributed Logical Router
- Firewall
NSX Distributed Firewall

VMware NSX Distributed Firewall (DFW) provides Layer 2 through Layer 4 stateful firewall services to any workload in the NSX environment. DFW runs in the kernel space and performs near line rate network traffic protection. DFW is VMware NSX component designed to protect workload-to-workload network traffic (Virtual-to-Virtual or Virtual-to-Physical). More concisely, DFW's main goal is to protect data center east-west traffic. Furthermore, since DFW policy enforcement is generally applied to the virtual Network Interface Card (vNIC) of a VM, DFW can also be used to secure communication between the SDDC VMs and actors external to the organization's network (north-south traffic). DFW is fully complementary with NSX Edge, which provides more traditional firewall capability. NSX Edge, or Edge Services Gateway (ESG), is usually the first entry point to the SDDC and also acts as SDDC perimeter firewall and IPS. ESG provides security for north-south and virtual-to-physical traffic. DFW and ESG distinct positioning roles are depicted in Figure 2.

NSX DFW operates at the VM vNIC level, meaning that a VM is always protected irrespective of the way it is connected to the logical network: VM can be connected to a VDS VLAN-backed port-group or to a Logical Switch (VXLAN-backed port-group). All these connectivity modes are fully supported. ESG Firewall can also be used to protect workloads sitting on physical servers and appliances, such as NAS.

The DFW system architecture is based on three distinct entities – each of them playing a clearly defined role:

- **vCenter Server** is the management plane of the solution. DFW policy rules are created through the vSphere Web client. Any vCenter container can be used in the source/destination field of the policy rule: cluster, VDS port-group, Logical Switch, VM, vNIC, Resource Pool, etc.

- **NSX Manager** is the control plane of the solution. It receives rules from the vCenter server and stores them in the central database. NSX Manager then pushes DFW rules down to all ESXi hosts that have been prepared for enforcement. Backup of DFW security policy rule table is performed each time the table is modified and published. NSX Manager can also receive DFW rules directly from REST API calls in case a Configuration Manager Proxy (CMP) is used for security automation.

- **ESXi Host** is the data plane of the solution. DFW rules are received from the NSX Manager and then translated into kernel space for real-time execution. VM network traffic is inspected and enforced per ESXi host. For instance, VM1 is located on ESXi host 1 and sends packets to VM2 that is located on ESXi host 2. Policy enforcement is done on ESXi host 1 for egress traffic (when packets leave VM1) and then on ESXi host 2 for ingress traffic (when packets reach to VM2).

A single DFW instance is created per vNIC. So if a new VM with 3 vNICs is created, 3 instances of DFW will be allocated to this VM. Configuration of these DFW instances can be identical or completely different, depending on the given operational scenario. Generally, a user can select a Point of Enforcement (PEP) for a specific DFW configuration (also referred to as “DFW rule”), which can have the scope ranging from a vNIC to a logical switch. By default, a DFW rule is propagate to all DFW instances.
DFW policy rules can be written in two ways: using L2 rules (Ethernet) or L3/L4 rules (General).

- **2 rules are mapped to L2 OSI model:** only MAC addresses can be used in the source and destination fields – and only L2 protocols can be used in the service fields (like ARP for instance).
- **L3/L4 rules are mapped to L3/L4 OSI model:** policy rules can be written using IP addresses and TCP/UDP ports.

It is important to remember that L2 rules are always enforced before L3/L4 rules. For example, if the L2 default policy rule is modified to ‘block’, then all L3/L4 traffic will be blocked as well.

DFW performance and throughput scale linearly by adding new ESXi hosts, up to the maximum limit supported by NSX, which is 20 Gbps per host. DFW is activated as soon as the host preparation process is completed. If a VM needs no DFW service at all, it can be added in the exclusion list (by default, NSX Manager, NSX Controllers and ESGs are automatically excluded from DFW function).

Third-Party Security Vendor Integration

The NSX network virtualization platform provides L2-L4 stateful firewall features to deliver segmentation within virtual networks. In some environments, there is a requirement for more advanced network security capabilities than provided by VMware's native DFW. Every security team uses a unique combination of network security products to meet the needs of its environment. The VMware NSX platform is being leveraged by VMware's entire ecosystem of security solution providers. Network security teams are often challenged to coordinate network security services from multiple vendors in relationship to each other. A powerful benefit of the NSX approach is its ability to build policies that leverage NSX service insertion, chaining, and steering to drive service execution in the logical services pipeline, based on the result of other services, making it possible to coordinate otherwise completely unrelated network security services from multiple vendors.

How might a typical integration with third-party security vendors proceed? For example, VMware integrates with a network security service provider by leveraging...
the VMware NSX platform to distribute the provider’s next-generation firewall (NGFW), making the advanced features locally available on each hypervisor. Network security policies, defined for application workloads that are provisioned or moved to that hypervisor, are inserted into the virtual network’s logical pipeline. At runtime, the service insertion leverages the locally available NGFW feature set of the service provider to deliver and enforce application, user, and context-based control policies at the workloads virtual interface.

To dive a little deeper, NSX distributes network security services into a vNIC context to form a logical pipeline of services applied to virtual network traffic. Third-party network security services can be inserted into this pipeline, allowing physical or virtual services to be consumed. Between guest VM and Virtual Distributed Switch (VDS), there is a service space implemented into the vNIC context, each with a unique Slot-ID. As depicted in Figure 3, slot 2 is allocated to DFW and slot 4 to the network security service’s firewall. Another set of slots is available to plug in more third-party services. Traffic exiting the guest VM always follows the path with increasing slot-ID number (i.e., a packet is redirected to slot 2 and then slot 4). Traffic reaching the guest VM follows the path in the reverse slot-ID order (slot 4 and then slot 2).

Summary

VMware NSX network virtualization platform addresses current challenges with physical network infrastructure. However, more importantly, IT managers focused on NSX’s efficiency-related enhancements may overlook its equally significant security benefits. In fact, NSX can strengthen organizational security in a variety of ways, such as containerization to prevent lateral movement. With VMware NSX, organizations can take advantage of available resources wherever they’re located, and move them with the resources as required for automation. This allows for a more secure environment that matches the automation goals of SDDC.

NSX brings enhanced flexibility, scalability and security to the SDDC by decoupling the virtual network from the physical network. NSX enables unrestricted workload mobility, placement, and security enforcement. With NSX, workloads can freely move (or “vMotion”) across subnets and availability zones, and their placement is not dependent on the physical topology and availability of physical network services in a given location. Everything a VM needs from a networking and security perspective is provided to it by NSX, wherever it physically resides. Among the important benefits of this capability is that it’s no longer necessary for organizations to over-provision server capacity within each application/network pod or deal with tedious firewall rule changes. Instead, organizations can take advantage of available resources wherever they’re located, thereby allowing substantially greater optimization of resource utilization, security granularity, and consolidation.