VMWARE NSX

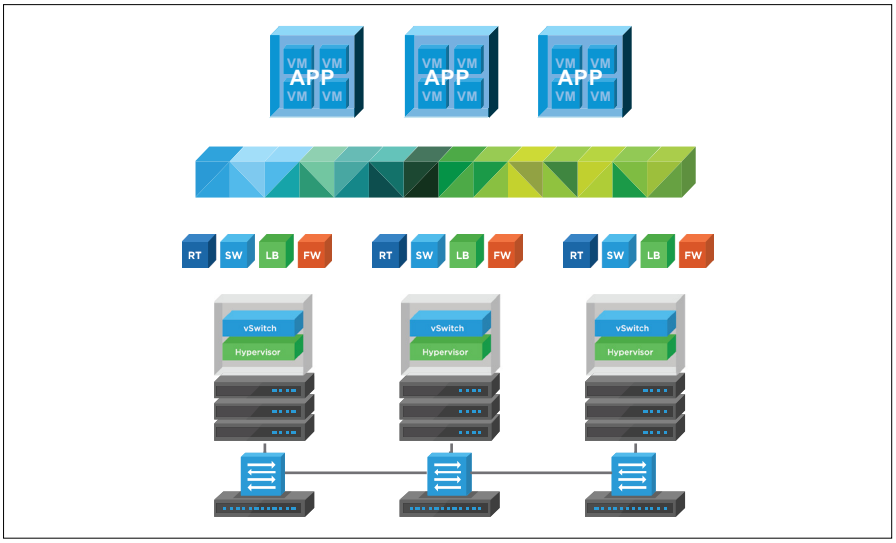
The Network Virtualization and Security Platform

AT A GLANCE

VMware NSX® is the network virtualization and security 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 networking and security 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.

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



Network Virtualization, Security, and the 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.

Key Features of NSX

Switching	Enable logical layer 2 overlay extensions across a routed (L3) fabric within and across data center boundaries. Support for VXLAN-based network overlays.
Routing	Dynamic routing between virtual networks performed in a distributed manner in the hypervisor kernel, scale-out routing with active-active failover with physical routers. Static routing and dynamic routing (OSPF, BGP) protocols supported.
Distributed Firewalling	Distributed stateful firewalling, embedded in the hypervisor kernel for up to 20Gbps of firewall capacity per hypervisor host. Support for Active Directory and activity monitoring. Additionally, NSX can also provide north-south firewall capability via NSX Edge™.

Load Balancing	L4–L7 load balancer with SSL offload and pass-through, server health checks, and App Rules for programmability and traffic manipulation.
VPN	Site-to-site and remote-access VPN capabilities, unmanaged VPN for cloud gateway services.
NSX Gateway	Support for VXLAN to VLAN bridging for seamless connection to physical workloads. This capability is both native to NSX and delivered by top-of-rack switches from an ecosystem partner.
NSX API	RESTful API for integration into any cloud management platform or custom automation.
Operations	Native operations capabilities such as central CLI, traceflow, SPAN, and IPFIX to troubleshoot and proactively monitor the infrastructure. Integration with tools such as VMware vRealize® Operations™ and vRealize Log Insight™ for advanced analytics and troubleshooting. NSX Application Rule Manager and Endpoint Monitoring enable end to end network traffic flow visualization up to Layer 7, allowing application teams to identify both intra and inter data center end points, and respond by creating the appropriate security rules.
Dynamic Security Policy	NSX service composer enables the creation of dynamic security groups. Beyond just IP address and MAC, membership of security groups can be based on VMware vCenter™ objects and tags, operating system type, and Active Directory roles to enable a dynamic security enforcement capability.
Cloud Management	Native integration with vRealize Automation™ and OpenStack.
3rd Party Partner Integration	Support for management, control plane, and data plane integration with third-party partners in a wide variety of categories such as next-generation firewall, IDS/IPS, agentless antivirus, application delivery controllers, switching, operations and visibility, advanced security, and more.
Cross vCenter Networking and Security	Extend networking and security across vCenter and data center boundaries irrespective of underlying physical topology—enabling capabilities such as disaster recovery and active-active data centers.
Log Management	Help resolve problems faster with added visibility from vRealize Log Insight for NSX. Visualize event trends, trigger alerts, and more, all in real-time.

Use Cases

Security

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. IT teams can then define security policies and controls for each workload based on dynamic security groups, which ensures immediate responses to threats inside the data center and enforcement down to the individual virtual machine. Unlike in traditional networks, if an attacker gets through data center perimeter defenses, threats can't move laterally within the data center.

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.

Native integration of NSX with cloud management platforms such as vRealize Automation or OpenStack enable further automation.

Application Continuity

Since 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—all in minutes, all without disrupting the applications, and all without touching the physical network.

VMware NSX Editions

Standard

For organizations needing agility and automation of the network

Advanced

For organizations needing Standard, plus a fundamentally more secure data center with micro-segmentation

Enterprise

For organizations needing Advanced, plus networking and security across multiple domains

ROBO

For organizations looking to virtualize and secure applications in the remote office or branch office.

FIND OUT MORE

For more information visit www.vmware.com/go/nsx.

Additional details on NSX licensing edition features can be found at https://kb.vmware.com/kb/2145269.

For information on all VMware products or to purchase, call 877-4VMWARE (outside North America, +1-650-427-5000), visit http://www.vmware.com/products, or search online for an authorized reseller.

	STANDARD	ADVANCED	ENTERPRISE	ROBO
Distributed Switching	•	•	•	•*
Distributed Routing	•	•	•	
NSX Edge firewall	•	•	•	•
NAT	•	•	•	•
Software L2 bridging to physical environment	•	•	•	
Dynamic routing with ECMP (active-active)	•	•	•	•
API-driven automation	•	•	•	•
Integration with vRealize and OpenStack	•	•	•	•
Log management with vRealize Log Insight for NSX	•	•	•	•
Automation of security policies with vRealize		•	•	•
NSX Edge load balancing		•	•	•
Distributed firewalling		•	•	•
Integration with Active Directory		•	•	•
Server activity monitoring		•	•	•
Service insertion (third-party integration)		•	•	•
Integration with VMware AirWatch®		•	•	•
Application Rule Manager		•	•	•
Cross vCenter NSX			•	
Multisite NSX optimizations			•	
VPN (IPSEC and SSL)			•	•
Remote gateway			•	
Integration with hardware VTEPs			•	
Endpoint Monitoring			•	

*VLAN backed

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com