VMWARE NSX DATA CENTER

The Network Virtualization and Security Platform

AT A GLANCE

VMware NSX® Data Center is the network virtualization and security platform that enables the virtual cloud network, a software-defined approach to networking that extends across data centers, clouds, endpoints, and things. With NSX Data Center, network functions—including switching, routing, firewalling, and load balancing—are brought closer to the application and distributed across the environment. Similar to the operational model of virtual machines, networks can be provisioned and managed independent of underlying hardware. NSX Data Center 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 or from a broad ecosystem of third-party integrations ranging from Next-Generation Firewalls to performance management solutions to build inherently more agile and secure environments. These services can then be extended to a number of endpoints within and across clouds.

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

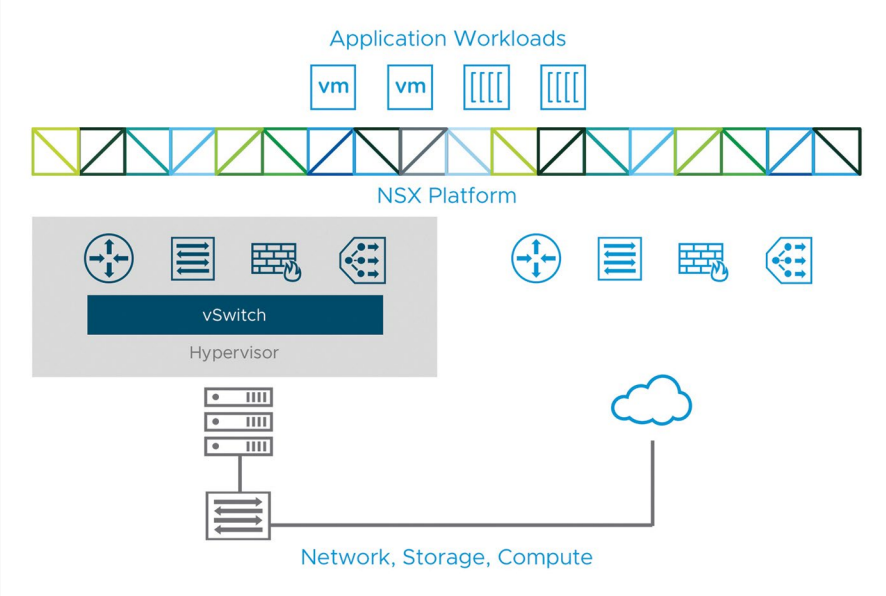

Figure 1: NSX Data Center: Network Virtualization and Security Platform

Network Virtualization, Security, and the Software-Defined Data Center

VMware NSX Data Center delivers a completely new operational model for networking defined in software, forming the foundation of the Software-Defined Data Center (SDDC). Data center operators can now achieve levels of agility, security, and economics that were previously unreachable when the data center network was tied to physical hardware components. NSX Data Center 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 Data Center APIs. Virtual networks are deployed nondisruptively over any existing networking hardware.

Key Features of NSX Data Center

Switching	Enable logical Layer 2 overlay extensions across a routed (Layer 3) 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 20 Gbps of firewall capacity per hypervisor host. Support for Active Directory and activity monitoring. Additionally, NSX Data Center 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 application 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 Data Center and delivered by top-of-rack switches from an ecosystem partner.
NSX Data Center 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. 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.
Context-Aware Micro-segmentation	NSX Data Center enables the creation of dynamic security groups and associated policies to be based on factors beyond just IP address and MAC, including VMware vCenter® objects and tags, operating system type, and Layer 7 application information to enable micro-segmentation based on the context of the application. Identity based policy using login information from VMs, Active Directory, and Mobile Device Management integration allows for security based on the user including session level security in remote and virtual desktop environments.
Cloud Management	Native integration with vRealize Automation™ and OpenStack.
Third-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.
Multi-site Networking and Security	Extend networking and security across data center boundaries irrespective of underlying physical topology—enabling capabilities such as disaster recovery and active-active data centers.

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 www.vmware.com/products, or search online for an authorized reseller.

Use Cases

Security

NSX Data Center enables organizations to divide the data center into distinct security segments, down to the level of the individual workload—independent from where the workload is running. IT teams can define policies for each workload based on application and user context, which ensures immediate responses to threats inside the data center and enforcement down to the application. Unlike in traditional networks, attacks that penetrate perimeter defenses can't move laterally within the data center.

Automation

VMware NSX Data Center virtualizes all networking and security functions to enable faster deployment and complete lifecycle automation of traditional and new applications consistently across sites and clouds. Automating tedious tasks, new cloud-native application roll-out, and ongoing operations empowers IT organizations and developers to move at the increasing speed of business.

Multi-Cloud Networking

Because NSX Data Center 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 workloads rapidly from one data center to another, or deploy them into a hybrid cloud environment—all in minutes, without disrupting the applications or touching the physical network.

Networking and Security for Cloud-Native Apps

VMware NSX Data Center provides native full stack networking and security for containerized applications and microservices, delivering granular policy on a per-container basis as new applications are developed. This enables native container-to-container L3 networking, micro-segmentation for microservices, and end-to-end visibility of networking and security policy across both traditional and new applications.

VMware NSX Data Center Editions

Standard

For organizations needing agility and automation of the network

Professional

For organizations needing Standard, plus micro-segmentation, and may have public cloud endpoints

Advanced

For organizations needing Professional, plus advanced networking and security services and integration with a broad ecosystem, and may have multiple sites

Enterprise Plus

For organizations needing the most advanced capabilities NSX Data Center has to offer, plus network visibility and security operations with vRealize Network Insight™, and hybrid cloud mobility with NSX Hybrid Connect

ROBO

For organizations looking to virtualize networking and security for applications in the remote office or branch office

	STANDARD	PROFESSIONAL	ADVANCED	ENTERPRISE PLUS	ROBO
NSX DATA CENTER[1]					
Distributed Switching and Routing	•	•	•	•	•[5]
NSX Edge Firewall	•	•	•	•	•
NSX Edge NAT	•	•	•	•	•
SW L2 Bridging to Physical Environments	•	•	•	•	
Dynamic Routing with ECMP (Active-active)	•	•	•	•	•
Integration with Cloud Management Platforms[3]	•	•	•	•	•
Distributed Firewalling		•	•	•	•
VPN (L2 and L3)		•	•	•	•
Integration with NSX Cloud[4]		•	•	•	•
NSX Edge Load Balancing			•	•	•
Integrations with Distributed Firewall (Active Directory, AirWatch® & Third-Party Service Insertion)			•	•	•
Application Rule Manager			•	•	•
Container Networking and Security			•	•	
Multi-site Networking and Security			•	•	
Integration with Hardware Gateways			•	•	
Endpoint Monitoring				•	
Context-aware Micro-segmentation (Application Identification, RDSH)				•	
+vREALIZE NETWORK INSIGHT ADVANCED[2]					
Traffic (IPFIX) Visibility & Network Monitoring				•	
Firewall Planning and Management				•	
NSX Operations and Troubleshooting				•	
+NSX HYBRID CONNECT ADVANCED[2]					
Large Scale Workload Migration				•	
WAN Optimization for Workload Migration				•	
Traffic & Load Management Across Multiple Links				•	

[1] For detailed feature capabilities please refer to the Knowledge Base articles on NSX Data Center for vSphere features and NSX-T™ Data Center features to get the latest information.

[2] NSX Data Center Enterprise Plus includes full versions of vRealize Network Insight Advanced and NSX Hybrid Connect Advanced.

[3] L2, L3, and NSX Edge integration only. No consumption of security groups.

[4] NSX Cloud subscription required for public cloud workloads.

[5] Switching only, VLAN backed.

vmware®

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