VMware NSX Data Center

KEY BENEFITS

- Protect applications with micro-segmentation at the workload level and granular security.
- Reduce network provisioning time from days to seconds and improve operational efficiency through automation.
- Gain consistent management of networking and security policies independent of physical network topology within and across data centers and native public clouds.
- Obtain detailed application topology visualization, automated security policy recommendations and continuous flow monitoring.
- Enable advanced, lateral threat protection on east-west traffic using the built-in, fully distributed threat prevention engine.

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, and application frameworks. With NSX Data Center, networking and security are brought closer to the application wherever it's running, from virtual machines (VMs) to containers to bare metal. Like the operational model of VMs, 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 variety of endpoints within and across clouds.

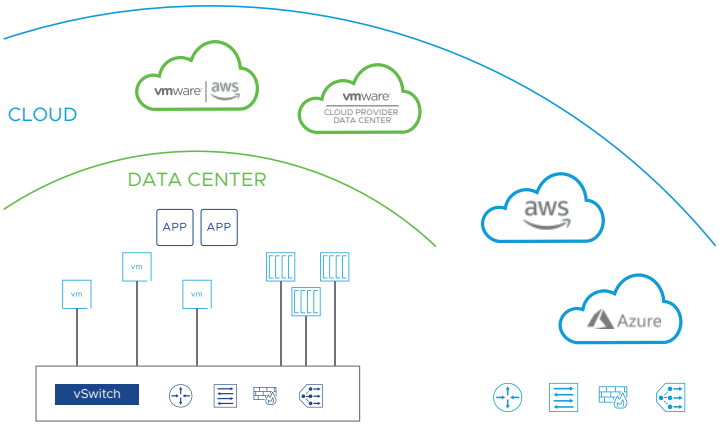

FIGURE 1: NSX Data Center network virtualization and security platform.

Networking in software

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) and extending to a virtual cloud network. Data center operators can now achieve levels of agility, security and economics that were previously unreachable when the data center network was tied solely to physical hardware components. NSX Data Center provides a complete set of logical networking and security capabilities and services, including logical switching, routing, firewalling, load balancing, virtual private network (VPN), quality of service (QoS) and monitoring. These services are provisioned in virtual networks through any cloud management platform leveraging NSX Data Center APIs. Virtual networks are deployed non-disruptively over any existing networking hardware and can extend across data centers, public and private clouds, container platforms and bare-metal servers.

Key features

Switching	Enable logical Layer 2 overlay extensions across a routed (Layer 3) fabric within and across data center boundaries. Support for VXLAN- and GENEVE-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 protocols supported, including support for IPv6.
Gateway Firewall	Stateful firewalling up to Layer 7 (including app identification and distributed FQDN whitelisting), embedded in the NSX gateway, distributed across entire environment with centralized policy and management.
Distributed Firewall	Stateful firewalling up to Layer 7 (including app identification and distributed FQDN whitelisting), embedded in the hypervisor kernel, distributed across entire environment with centralized policy and management. In addition, the NSX Distributed Firewall integrates directly into cloud native platforms such as Kubernetes and Pivotal Cloud Foundry, native public clouds such as AWS and Azure, as well as bare-metal servers.
Load Balancing	L4–L7 load balancer with SSL offload and pass-through, server health checks (and passive health checks), and application rules for programmability and traffic manipulation via GUI or API.
VPN	Site-to-site and remote-access VPN capabilities, unmanaged VPN for cloud gateway services.
NSX Gateway	Support for bridging between VLANs configured on the physical network and NSX overlay networks, for seamless connectivity between virtual and physical workloads.
NSX Intelligence™	NSX Intelligence provides automated security policy recommendations and continuous monitoring and visualization of every network traffic flow for enhanced visibility, enabling a highly and easily auditable security posture. As part of the same UI as NSX-T™ Data Center, NSX Intelligence provides a single pane of glass for both network and security teams.
NSX Distributed Threat Prevention (NSX Distributed IDS/IPS[1])	NSX Distributed IDS/IPS™ is an advanced threat detection engine purpose-built to detect lateral threat movement on east-west traffic. The unique distributed architecture, combined with precise application context, enables security teams to replace discrete appliances while easily achieving regulatory compliance and creating virtual security zones without physical separation of infrastructure.
Federation	Centralized policy configuration and enforcement across multiple locations from a single pane of glass, enabling network-wide consistent policy, operational simplicity and simplified disaster recovery architecture.
Virtual Routing and Forwarding (VRF)	Complete data plane isolation among tenants with a separate routing table, NAT and edge firewall support in each VRF on the NSX Tier 0 gateway.
NSX Data Center API	RESTful API based on JSON for integration with cloud management platforms, DevOps automation tools and custom automation.
Operations	Native operations capabilities such as central CLI, traceflow, overlay logical SPAN and IPFIX to troubleshoot and proactively monitor the virtual network infrastructure. Integration with tools such as VMware vRealize® Network Insight™ for advanced analytics and troubleshooting.
Context-Aware Micro-Segmentation	Security groups and policies can be dynamically created and automatically updated based on attributes—beyond just IP addresses, ports and protocols—to include elements such as machine name and tags, operating system type and Layer 7 application information to enable adaptive micro-segmentation policy. Policies based on identity information from Active Directory and other sources enable user-level security down to the individual user session level in remote desktop services and virtual desktop infrastructure (VDI) environments.

Automation and Cloud Management	Native integration with vRealize Automation™/vRealize Automation Cloud™, OpenStack and more. Fully supported Ansible modules, fully supported Terraform provider and PowerShell integration.
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, intrusion detection system (IDS)/intrusion prevention system (IPS), agentless antivirus, switching, operations and visibility, advanced security and more.
Multi-Cloud Networking and Security	Enable consistent networking and security across data center sites, and across private and public cloud boundaries, irrespective of underlying physical topology or cloud platform.
Container Networking and Security	Supports load balancing, micro-segmentation (distributed firewalling), routing and switching for containers on platforms built on Kubernetes and Cloud Foundry, running on either VMs or bare-metal hosts. Provides visibility for container network traffic (logical ports, SPAN/Mi, IPFIX and traceflow).

Use cases

Security

NSX Data Center makes operationalizing zero-trust security for applications attainable and efficient in private and public cloud environments. Whether the goal is to lock down critical applications, create a logical demilitarized zone (DMZ) in software or reduce the attack surface of a virtual desktop environment, NSX Data Center enables micro-segmentation to define and enforce network security policy at the individual workload level.

Multi-cloud networking

NSX Data Center delivers a network virtualization solution that brings networking and security consistently across heterogeneous sites to streamline multi-cloud operations. As a result, NSX Data Center enables multi-cloud use cases ranging from seamless data center extension to multi–data center pooling to rapid workload mobility.

Automation

By virtualizing networking and security services, NSX Data Center enables faster provisioning and deployment of full stack applications by removing the bottleneck of manually managed networking and security services and policies. NSX Data Center natively integrates with cloud management platforms and other automation tools, such as vRealize Automation/vRealize Automation Cloud, OpenStack, Terraform, Ansible and more, to empower developers and IT teams to provision, deploy and manage apps at the speed business demands.

Networking and security for cloud native apps

NSX Data Center provides integrated 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 that need agile and automated networking.

Professional

For organizations that need Standard edition capabilities, plus micro-segmentation, and may have public cloud endpoints.

Advanced

For organizations that need Professional edition capabilities, plus advanced networking and security services and integration with a broad ecosystem, and may have multiple sites.

Enterprise Plus

For organizations that need the most advanced capabilities NSX Data Center has to offer, plus network operations with vRealize Network Insight, hybrid cloud mobility with VMware HCX®, and traffic flow visibility and security operations with NSX Intelligence.

Remote Office Branch Office (ROBO)

For organizations that need to virtualize networking and security for applications in the remote office or branch office.

	STANDARD	PROFESSIONAL	ADVANCED	ENTERPRISE PLUS	ROBO
NSX DATA CENTER[2]					
Distributed Switching and Routing	•	•	•	•	•[6]
NSX Gateway Firewall (Stateful)	•	•	•	•	•
NSX Gateway NAT	•	•	•	•	•
Software L2 Bridging to Physical Environments	•	•	•	•	
Dynamic Routing with ECMP (Active-Active)	•	•	•	•	•
Integration with Cloud Management Platforms[3]	•	•	•	•	•
IPv6 with Static Routing and Static IPv6 Allocation	•	•	•	•	
Distributed Firewalling for VMs and Workloads Running on Bare Metal		•	•	•	•
VPN (L2 and L3)		•	•	•	•
Integration with NSX Cloud™[4] for AWS and Azure Support		•	•	•	•
Load Balancing			•	•	•
Integration with Distributed Firewall (Active Directory, VMware AirWatch®, Endpoint Protection and Third-Party Service Insertion)			•	•	•
Container Networking and Security			•	•	
Multi-vCenter® Networking and Security			•	•	
IPv6 with Dynamic Routing, Dynamic IPv6 Allocation and Services			•	•	
Context-Aware Micro-Segmentation (L7 Application Identification, RDSH, Protocol Analyzer)			•	•	
Distributed FQDN Whitelisting			•	•	
NSX Distributed IDS/IPS[1]			•	•	
VRF (Tier 0 Gateway VRFs)			•	•	
Federation				•	

	STANDARD	PROFESSIONAL	ADVANCED	ENTERPRISE PLUS	ROBO
NSX INTELLIGENCE					
VM-to-VM Traffic Flow Analysis				•	
Firewall Visibility				•	
Automated Security Policy				•	
Rule and Group Recommendation Analytics				•	
vRealize Network Insight Advanced[5]				•	
VMware HCX Advanced[5]				•	

1. NSX Distributed IDS/IPS requires an additional subscription. Please note: NSX-T 3.0 only includes IDS functionality.
2. For detailed feature capabilities, please refer to the knowledge base articles on NSX Data Center for vSphere® features and NSX-T Data Center features, including the *Product Offerings for NSX-T Data Center 3.0* article, for the latest information.
3. L2, L3 and NSX Gateway integration only. No consumption of security groups.
4. NSX Cloud subscription required for public cloud workloads.
5. NSX Data Center Enterprise Plus includes full versions of vRealize Network Insight Advanced and VMware HCX Advanced. For more information, please see the *vRealize Network Insight datasheet* and the *HCX datasheet*.
6. Switching only, VLAN backed.

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