VMware NSX

Key benefits

- Reduce network provisioning time from days to seconds and improve operational efficiency through automation.
- Protect applications with micro-segmentation and advanced threat prevention at the workload level and granular security.
- 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 prevention on east-west traffic using the built-in, fully distributed threat prevention engine.

VMware NSX® is the network virtualization and security platform that enables VMware's cloud networking solution with a software-defined approach to networking that extends across data centers, clouds and application frameworks. With NSX, networking and security are brought closer to the application wherever it's running, from virtual machines (VMs) to containers to physical servers. Like the operational model of VMs, networks can be provisioned and managed independent 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 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.

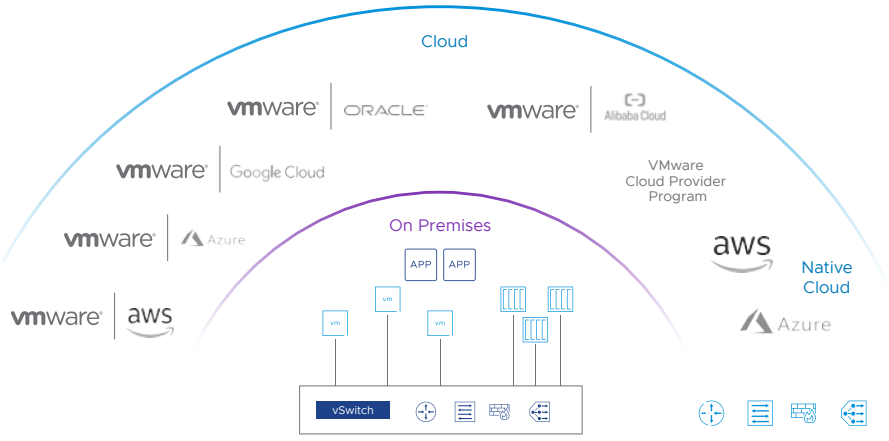

Figure 1: The NSX network virtualization and security platform.

Networking in software

VMware NSX 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 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 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 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 physical servers.

Key features	
Switching	Enable logical Layer 2 overlay extensions across a routed (Layer 3) fabric within and across data center boundaries.
Routing	Dynamic routing between virtual networks that is performed in a distributed manner in the hypervisor kernel, and scale-out routing with active-active failover with physical routers. Static routing and dynamic routing protocols are supported, including support for IPv6.
Load balancing[1]	VMware NSX Advanced Load Balancer™ provides enterprise-grade multi-cloud load balancing, global server load balancing (GSLB), application security and web application firewall, application analytics and container ingress services from the data center to the cloud.
Virtual routing and forwarding (VRF)	Complete data plane isolation among tenants with a separate routing table, network address translation (NAT), and edge firewall support in each VRF on the NSX Tier-0 gateway.
Distributed firewall	Stateful firewalling of Layer 2 up to Layer 7 (including app identification, user identification, and distributed FQDN allowlisting) is embedded in the hypervisor kernel, and distributed across the 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 physical servers.

Key features	
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.
VMware NSX Intelligence™	Get 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 VMware NSX, NSX Intelligence provides a single pane of glass for network and security teams.
NSX gateway	Support for bridging between VLANs configured on the physical network and NSX overlay networks, for seamless connectivity between virtual and physical workloads.
Gateway firewall	A full-featured, enterprise-grade network firewall provides protection using a full stateful L4–L7 firewall. This includes L7 application identification, user identification, NAT, and the like.
VPN	Site-to-site and unmanaged VPN for cloud gateway services.
NSX distributed and gateway advanced security capabilities[2]	Several advanced security capabilities are available for NSX with security add-ons. These include: • Distributed security: – Distributed intrusion detection and prevention systems (IDPS) – Distributed malware prevention – Distributed network traffic analysis (NTA) – Network detection and response • Gateway security – URL filtering based on web categories and reputation • Malware detection
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.

Key features	
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	VMware NSX Container Plugin provides container networking for VMware Tanzu® Kubernetes Grid™, VMware Tanzu Application Service™, VMware vSphere® with Tanzu, Red Hat OpenShift, and upstream Kubernetes. VMware Container Networking™ with Antrea™ provides in-cluster networking and Kubernetes network policy with commercial support and signed binaries. Integration with NSX provides multi-cluster network policy management and centralized connectivity troubleshooting via traceflow through the NSX management plane.
NSX 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® Log Insight™ for highly scalable log management, and VMware vRealize Network Insight™ for advanced analytics and troubleshooting.
Automation and cloud management	Native integration with VMware vRealize Automation™/ vRealize Automation Cloud™ 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/intrusion prevention system (IDS/IPS), agentless antivirus, switching, operations and visibility, advanced security, and more.

Use cases

Security

NSX 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 enables micro-segmentation to define and enforce network security policy at the individual workload level.

Multi-cloud networking

NSX delivers a network virtualization solution that brings networking and security consistently across heterogeneous sites to streamline multi-cloud operations. As a result, NSX 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 enables faster provisioning and deployment of full-stack applications by removing the bottleneck of manually managed networking and security services and policies. NSX natively integrates with cloud management platforms and other automation tools, such as vRealize Automation/vRealize Automation Cloud, 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 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 traditional and new applications.

VMware NSX editions

Professional

For organizations that need agile and automated networking 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 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.

	Professional	Advanced	Enterprise Plus	ROBO
Networking[3]				
Distributed switching and routing	•	•	•	•[4]
Software L2 bridging to physical environments	•	•	•	
Dynamic routing with ECMP (active-active)	•	•	•	•
IPv6 with static routing and static IPv6 allocation	•	•	•	
IPv6 with dynamic routing, dynamic IPv6 allocation and services		•	•	
VRF (Tier-0 gateway VRFs)		•	•	
Ethernet VPN (EVPN)			•	
Distributed security				
Distributed firewalling for VMs and workloads running on physical servers	•	•	•	•
Context-aware micro-segmentation (L7 application identification, RDSH, protocol analyzer)		•	•	
Distributed FQDN allowlisting		•	•	
Distributed advanced security capabilities	Additional distributed security capabilities are available with NSX security add-on licenses. Please refer to the NSX Distributed Firewall datasheet.			
Gateway security				
NSX Gateway Firewall™ (stateful)	•	•	•	•
NSX gateway NAT	•	•	•	•
VPN (L2 and L3)	•	•	•	•
Gateway advanced security capabilities	Additional gateway security capabilities are available with NSX security add-on licenses. Please refer to the NSX security datasheet.			

Additional resources

VMware NSX Distributed Firewall datasheet

VMware Container Networking with Antrea datasheet

	Professional	Advanced	Enterprise Plus	ROBO
Modern apps				
Container networking and security		•	•	
Multisite				
Multi-vCenter® networking and security		•	•	
Federation			•	
Operations				
Policy API, central CLI, traceflow, overlay logical SPAN and IPFIX	•	•	•	•
Integrations				
Integration with NSX Cloud™[5] for AWS and Azure support	•	•	•	•
Integration with cloud management platforms[6]	•	•	•	•
Integration with distributed firewall (Active Directory, VMware AirWatch®, endpoint protection and third-party service insertion)		•	•	•

	Professional	Advanced	Enterprise Plus	ROBO
Associated products				
VMware vRealize Log Insight for NSX[7]	•	•	•	•
VMware vRealize Network Insight Advanced[8]			•	
VMware HCX Advanced[8]			•	
VMware NSX Advanced Load Balancer – Basic Edition[1] (L4–L7 load balancing with SSL offload and pass-through, server health checks, application rules for programmability and traffic manipulation via GUI or API)		•	•	•
VMware NSX Intelligence (VM-to-VM traffic flow analysis, firewall visibility, automated security policy, rule and group recommendation analytics)			•	

1. VMware recommends customers use NSX Advanced Load Balancer for load balancing. NSX Advanced Load Balancer – Basic Edition is included with the NSX Advanced and Enterprise Plus editions. Advanced features of NSX Advanced Load Balancer are available as an add-on license. For more information, please visit the NSX Advanced Load Balancer product page.
2. For advanced security capabilities, please refer to the NSX Distributed Firewall datasheet.
3. A license to use VMware NSX includes an entitlement to use the VMware Workspace ONE® Access™ feature, but only for certain functionalities. For detailed feature capabilities, please refer to the knowledge base articles on NSX Data Center for vSphere features and NSX features, including the article, Product Offerings for NSX-T Data Center 3.2 for the latest information.
4. Switching only, VLAN backed.
5. NSX Cloud subscription required for public cloud workloads.
6. L2, L3 and NSX gateway integration only. No consumption of security groups.
7. For more information, please read the vRealize Log Insight datasheet.
8. NSX 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 VMware HCX datasheet.

Item No: 1356650aq-ds-nsx-a4 3/22