VMware NSX+

Consistent multi-cloud networking and security

Key benefits

- Deploy consistent networking and security policies and features from a single console.
- Proactively minimize ransomware risk with scalable multi-cloud security.
- Achieve a true cloud operating model across private and public clouds.
- Migrate between clouds while maintaining granular network visibility and control.
- Simplify compliance, governance and policy management with a single vendor for purchase and support.

VMware NSX+™ is a fully managed cloud-based networking, security, and advanced load balancing as-a-service offering for VMware NSX®. It allows networking, security and operations teams to consume and operate enterprise-grade network services across private and public clouds from a single cloud console.

With NSX+, organizations can:

- Achieve consistent policy and simplified cloud consumption – Speed up app and network infrastructure deployments across private and public clouds with consistent networking, security, and advanced load balancing policies; API-driven multitenant consumption; and a multi-virtual private cloud (VPC) network architecture.
- Strengthen multi-cloud security and visibility – Establish comprehensive visibility into applications and traffic flows regardless of where they are deployed. Leverage security threat correlation across clouds to identify emerging threats and reduce the risk of ransomware.
- Simplify multi-cloud network operations – Gain granular visibility and resource monitoring, streamlined network upgrades, and improved day-2 operations with the ability to quickly identify trends, troubleshoot issues, and optimize performance.

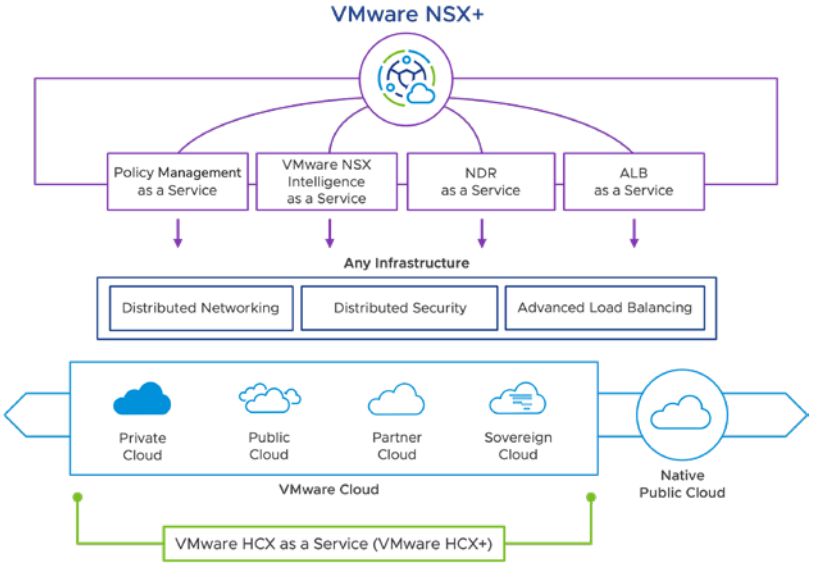

Figure 1: Multi-cloud networking, security, and advanced load balancing as a service with VMware NSX+.

Key features and capabilities	
Switching	Enable logical Layer 2 overlay extensions across a routed (Layer 3) fabric within 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.
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.
Context-aware micro-segmentation	Security groups and policies can be dynamically created and automatically updated based on attributes—beyond 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.
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, network address translation (NAT), and the like.
NSX distributed and gateway advanced security capabilities[1]	Several advanced security capabilities are available for NSX with security add-ons. These include: • Distributed security: – Distributed intrusion detection and prevention systems (IDPS) – Distributed network traffic analysis (NTA) – Network detection and response • Gateway security – URL filtering based on web categories and reputation • Malware detection

Key features and capabilities	
DPU-based acceleration for NSX	Delivers high-performance networking and security services implemented on DPUs[2] connected to the application hosts. Offloading NSX services from the hypervisor to DPU frees up host computing resources, enabling accelerated switching and routing, high-performance security, and enhanced observability while preserving your existing NSX user experience.
Multi-cloud policy	Centralized policy configuration and enforcement across multiple clouds from a single pane of glass, enabling network-wide consistent policy, operational simplicity, and simplified disaster recovery architecture.
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	API-first model exposing features through a RESTful API to allow scripting, integration with third parties, and DevOps consumption. Also offers OpenAPI specification and SDKs (Python, Java).
Operations	Native operations capabilities such as central CLI and traceflow to troubleshoot and proactively monitor the virtual network infrastructure.
Automation and cloud management	In addition to the API, the goal is to help by providing tooling for automation (SDK, Terraform provider, etc.). NSX is also integrated into numerous cloud management platforms, such as VMware Aria Automation™, VMware Cloud Director™, and others.
Multitenancy and cloud consumption	Divide the system into multiple projects to delegate access. This allows multiple users to manage networking and security in parallel on the same platform. Also provides a streamlined consumption model to simplify application deployments and segmentation with an NSX VPC.

VMware NSX+ editions

Standard

For organizations that need agile and automated networking plus micro-segmentation with centralized policy management, multiple VPCs across locations, keyless licensing, and network health monitoring capabilities.

Advanced

For organizations that need Standard edition capabilities plus advanced networking and security services with Layer 7 security, advanced load balancing with cloud services, and higher multi-cloud scale.

Enterprise

For organizations that need the most advanced capabilities NSX has to offer at the highest scale with additional multitenancy and multi-cloud features, and support for DPU-based acceleration.

	Standard	Advanced	Enterprise
Networking			
Distributed switching and routing	•	•	•
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		•	•
Dual stack (IPv4/IPv6) external management		•	•
Virtual routing and forwarding (VRF) (Tier-0 gateway VRFs)		•	•
Ethernet VPN (EVPN)			•
Multi-cloud			
Policy for local managers	•	•	•
Multitenancy	Limited	Limited	•
On-premises sites supported	Limited	Limited	•
Keyless activation	•	•	•
Cloud-based NSX infrastructure monitoring	•	•	•

Additional resources

VMware NSX Distributed Firewall datasheet

VMware NSX Advanced Threat Prevention™ datasheet

VMware NSX datasheet

VMware NSX Feature and Edition Guide

	Standard	Advanced	Enterprise
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		•	•
DPU-based acceleration			•
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)	•	•	•
Modern apps			
Container networking and security		•	•
Multisite			
Multi-vCenter® networking and security		•	•
Operations			
Policy API, central CLI, traceflow, overlay logical SPAN and IPFIX	•	•	•
Integrations			
DPU-based acceleration for NSX[3]			•
Integration with cloud management platforms[4]	•	•	•

Learn more

Learn more about VMware NSX+ at nsx-plus.com.

	Standard	Advanced	Enterprise
Associated products			
VMware Aria Operations™ for Logs (SaaS) for NSX[5]	Limited	Limited	Limited
VMware NSX Advanced Load Balancer™ Enterprise with Cloud Services[6]		Limited	Limited

1. For advanced security capabilities, please refer to the NSX Distributed Firewall datasheet.
2. Supports several leading DPU/NIC vendors and server OEMs. Please contact your VMware representative for more details.
3. For more information, please refer to the NSX Feature and Edition Guide.
4. L2, L3 and NSX gateway integration only. No consumption of security groups.
5. For more information, please read the VMware Aria Operations for Logs datasheet.
6. Limited quantities of NSX Advanced Load Balancer Enterprise with Cloud Services are included. Additional entitlements are available as an add-on license. For more information, please visit the NSX Advanced Load Balancer product page.