VMware NSX
The Network Virtualization Platform

AT A GLANCE

VMware NSX® is the network virtualization platform for the Software-Defined Data Center, delivering the operational model of a virtual machine for entire networks. With NSX, network functions including switching, routing, and firewalls are embedded in the hypervisor and distributed across the environment. This effectively creates a “network hypervisor” that acts as a platform for virtual networks and services. Similar to the operational model of virtual machines, virtual networks are programmatically provisioned and managed independent of underlying hardware. NSX reproduces the entire network model in software, enabling any network topology—from simple to complex multi-tier 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 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, firewalls, 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 non-disruptively over any existing networking hardware.

Key Features of NSX

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switching</td>
<td>Enable logical layer 2 overlay extensions across a routed (L3) fabric within and across data center boundaries. Support for VXLAN based network overlays.</td>
</tr>
<tr>
<td>Routing</td>
<td>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.</td>
</tr>
<tr>
<td>Distributed Firewalling</td>
<td>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 can also provide north-south firewall capability via NSX edge.</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>L4-L7 load balancer with SSL offload and pass-through, server health checks, and App Rules for programmability and traffic manipulation.</td>
</tr>
<tr>
<td>VPN</td>
<td>Site-to-Site and Remote-Access VPN capabilities, unmanaged VPN for cloud gateway services.</td>
</tr>
<tr>
<td>NSX Gateway</td>
<td>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.</td>
</tr>
<tr>
<td>NSX API</td>
<td>RESTful API for integration into any cloud management platform or custom automation.</td>
</tr>
</tbody>
</table>
VMware NSX

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
New NSX offerings enable more customers to match the needs of their specific network virtualization requirements to start on the path to the Software-Defined Data Center.

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

Use Cases

Security
VMware 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.
### VMware NSX

<table>
<thead>
<tr>
<th>Feature</th>
<th>Standard</th>
<th>Advanced</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed switching and routing</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSX Edge firewall</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SW L2 bridging to physical environment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic routing with ECMP (Active-active)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>API-driven automation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration with vRealize and OpenStack</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automation of security policies with vRealize</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSX Edge load balancing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed firewalling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration with Active Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server activity monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service insertion (3rd party integration)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cross vCenter NSX</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Multi-Site NSX optimizations</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>VPN (IPSEC and SSL)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Gateway</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration with HW VTEPs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Find Out More

For more information visit [www.vmware.com/go/nsx](http://www.vmware.com/go/nsx).

Additional details on NSX licensing edition features can be found at: [http://www.vmware.com/products/nsx/licensing.html](http://www.vmware.com/products/nsx/licensing.html)

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](http://www.vmware.com/products), or search online for an authorized reseller.