MEDIALINE

Datacenter

VMware NSX

Network virtualization and security platform for software-defined data centers

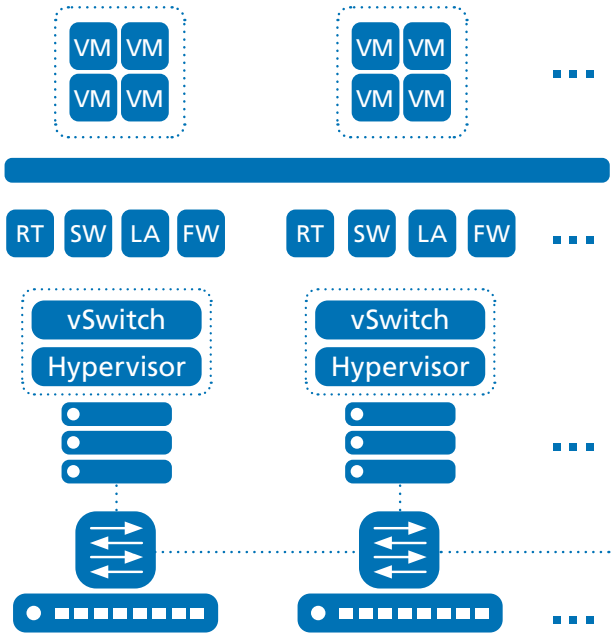
What is NSX?

VMware NSX is a network virtualization and security platform for a software-defined data center (SDDC). It applies the operational model of a virtual machine to entire networks.
By integrating switching, routing, and firewalling into the hypervisor, these network functions can be utilized throughout the environment, creating a type of network hypervisor. As an operator of one or more data centers, you can benefit from increased agility, security, and cost-effectiveness through the implementation of NSX networks as software.
Virtual networks can be provisioned seamlessly on existing network hardware.

Benefits of NSX

- High security even on individual workloads
- Network deployments in seconds
- Ensuring security and network service through partnerships with leading third-party providers

Concept NSX



Main Functions

- Switching: Collaboration of logical 2-overlay extensions in a routed fabric in connection with the data center.
- Routing: Support for dynamic and static routing
- Distributed Firewalling: With a capacity of up to 20Gbit/s per hypervisor host and deployment for north-south and east-west traffic
- Load Balancing: Server system diagnostics and application rules for programmability and manipulation of traffic data
- VPN: Features for site-to-site and remote access VPNs
- NSX Gateway: Collaboration for seamless connection with physical workloads
- Operations: Support for native operational functions such as central CLI, Traceflow, SPAn, and IPFX, as well as proactive monitoring of the infrastructure. NSX Application Rule Manager and Endpoint Monitoring allow visualization of end-to-end network traffic
- Context-Aware Micro-Segmentation: Creation of dynamic security groups and corresponding policies.
- Integration with Partner Products: Support and collaboration for integration at the management, control and data levels, and much more
- Network and Security Features: Use beyond the boundaries of vCenter and data centers
- Protocol Management: Real-time triggers and troubleshooting made faster through transparency is possible

Application areas:

Security:

The logical structure of your data center enables NSX to create individual security segments, even down to the level of individual workloads. IT teams can immediately respond to threats in the data center by defining dynamic security groups.

Automation:

Challenges related to time-consuming network deployment, configuration errors, and expensive automation processes can be addressed with NSX. Typical bottlenecks in hardware-based networks can be avoided with NSX.

Application continuity:

Network and security policies can be linked to workloads thanks to the abstraction of hardware. This enables companies to replicate complete application environments for disaster recovery purposes in remote data centers, move them to data centers, or provide them in a hybrid cloud.

VMware NSX Editions:

Standard:

For companies that want to automate their network and make it more agile

Advanced:

For companies that need additional security features for their data center with micro-segmentation beyond the functionality of the Standard Edition

Enterprise:

For companies that need additional network and security features for various domains beyond the functionality of the Advanced Edition

ROBO:

For companies that want to virtualize and protect applications at remote locations or in branch offices

as of: 03/2021