

# VMware NSX

Netzwerkvirtualisierungs- & Sicherheitsplattform für Software-Defined Datacenter

## Was ist NSX?

VMware NSX ist eine Netzwerkvirtualisierungs- und Sicherheitsplattform für ein Software-Defined Datacenter (SDDC). Es wendet das Betriebsmodell einer virtuellen Maschine auf ganze Netzwerke an.

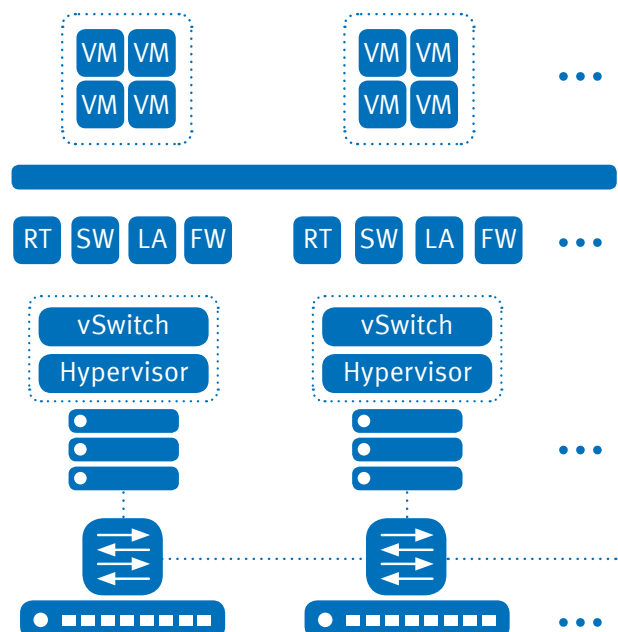
Durch die Integration von Switching, Routing und Firewalling in den Hypervisor können diese Netzwerkfunktionen in der gesamten Umgebung genutzt werden. Dadurch entsteht eine Art Netzwerk-Hypervisor. Als Betreiber von einem oder mehreren Rechenzentren profitiert man von gesteigerter Agilität, Sicherheit und Wirtschaftlichkeit durch die Abbildung von NSX-Netzwerken als Software.

Auf vorhandener Netzwerkhardware können virtuelle Netzwerke unterbrechungsfrei bereitgestellt werden.

## Vorteile von NSX

- Höchste Sicherheit auch auf einzelnen Workloads
- Netzwerkbereitstellungen in Sekunden
- Gewährleistung von Sicherheit und Netzwerkservice durch Partnerschaften mit führenden Drittanbietern

## Konzept NSX



## Hauptfunktionen

- **Switching:** Kooperation logischer 2-Overlay- Erweiterungen in einer gerouteten Fabric in Verbindung mit dem Rechenzentrum
  - **Routing:** Unterstützung von dynamischen & statischen Routings
  - **Verteiltes Firewalling:** mit einer Kapazität bis zu 20Gbit/s pro Hypervisor Host und Bereitstellung für Nord-Süd und Ost-West Traffic.
  - **Lastausgleich:** Systemdiagnosen des Servers und Anwendungsregeln für Programmierbarkeit und Manipulation des Datenverkehrs
  - **VPN:** Funktionen für Site-to-Site und Remote-Zugriffs-VPNs
  - **NSX-Gateway:** Kooperation für die nahtlose Verbindung mit physischen Workloads
  - **Betrieb:** Unterstützung nativer Betriebsfunktionen wie z.B.: zentrale CLI, Traceflow, SPAn und IPFX, sowie proaktive Überwachung der Infrastruktur.
- **NSX Application Rule Manager und Endpoint Monitoring** erlauben Visualisierung des End-to-End Netzwerkdatenverkehrs
  - **Kontextbezogene Mikrosegmentierung:** Erstellung dynamischer Sicherheitsgruppen und passender Richtlinien
  - **Integration in Partnerprodukte:** Unterstützung und Kooperationen für Integration in der Management-, Steuerungs- und Datenebene & vieles mehr
  - **Netzwerk und Sicherheitsfunktionen:** Benutzung über die Grenzen von vCenter und Rechenzentren hinaus
  - **Protokollmanagement:** Echtzeitauslösungen und Problembehebung durch Transparenz schneller möglich

## Anwendungsbereiche:

### Sicherheit:

Die logische Gliederung Ihres Rechenzentrums ermöglicht NSX durch einzelne Sicherheitssegmente – unterteilt bis hin zu einzelnen Workloads. Auf Bedrohungen im RZ kann durch das Festlegen dynamischer Sicherheitsgruppen durch die IT-Teams sofort reagiert werden.

### Automatisierung:

Herausforderungen im Zusammenhang mit zeitaufwendiger Netzwerkbereitstellung, Konfigurationsfehlern und teuren Prozessen zur Automatisierung lassen sich durch NSX bewältigen. Typische Engpässe hardwarebasierter Netzwerke lassen sich durch NSX vermeiden.

### Anwendungskontinuität:

Netzwerk- und Sicherheitsrichtlinien können dank der Abstrahierung der Hardware mit den jeweiligen Workloads verknüpft werden. Dies ermöglicht Unternehmen vollständige Anwendungsumgebungen für Disaster Recovery Zwecke in Remote-Rechenzentren zu replizieren, diese in Rechenzentren zu verschieben oder in einer Hybrid Cloud bereitzustellen.

## VMware NSX Editions:

### Standard:

Für Unternehmen, die ihr Netzwerk agiler gestalten und automatisieren möchten

### Advanced:

Für Unternehmen, die über den Funktionsumfang der Standard Edition hinaus zusätzliche Sicherheitsfunktionen für ihr Rechenzentrum mit Mikrosegmentierung benötigen

### Enterprise:

Für Unternehmen, die über den Funktionsumfang der Advanced-Edition hinaus zusätzliche Netzwerk- und Sicherheitsfunktionen für verschiedene Domänen benötigen

### ROBO:

Für Unternehmen, die Anwendungen an Remote-Standorten oder in Zweigstellen virtualisieren und schützen möchten



IT  
Infrastructure



Managed &  
Cloud Services



Business  
Solutions