VMWARE NSX

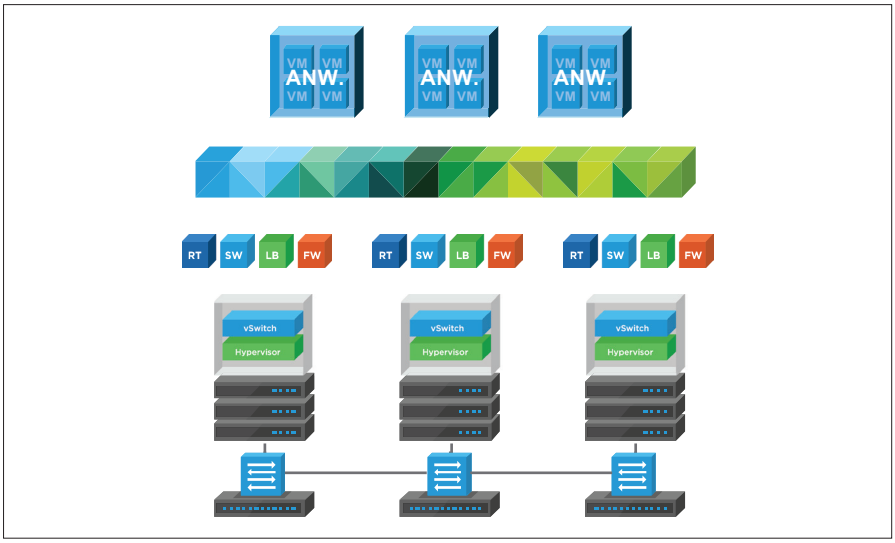
Die Plattform für die Netzwerkvirtualisierung

AUF EINEN BLICK

VMware NSX® ist eine Netzwerkvirtualisierungsplattform für das Software-Defined Datacenter (SDDC), die das Betriebsmodell einer virtuellen Maschine auf ganze Netzwerke anwendet. Mit NSX werden Netzwerkfunktionen wie Switching, Routing und Firewalling in den Hypervisor integriert und können über den Hypervisor in der gesamten Umgebung genutzt werden. Auf diese Weise entsteht eine Art „Netzwerk-Hypervisor", der als Plattform für virtuelle Netzwerke und Services fungiert. Wie beim Betriebsmodell für virtuelle Maschinen werden auch virtuelle Netzwerke programmatisch bereitgestellt und unabhängig von der zugrunde liegenden Hardware verwaltet. NSX reproduziert das gesamte Netzwerkmodell als Software, sodass jede Netzwerktopologie – von einfachen bis hin zu komplexen mehrschichtigen Netzwerken – in Sekunden erstellt und bereitgestellt werden kann. Durch Kombination der Services von NSX können verschiedene virtuelle Netzwerke mit unterschiedlichen Anforderungen erstellt und so die Sicherheit der genutzten Umgebungen verbessert werden.

DIE WICHTIGSTEN VORTEILE

- Mikrosegmentierung und detaillierte Sicherheit bis zur Ebene einzelner Workloads
- Reduzierung des Zeitaufwands für die Netzwerkbereitstellung von mehreren Tagen auf wenige Sekunden und höhere betriebliche Effizienz durch Automatisierung
- Workload-Mobilität unabhängig von der Topologie des physischen Netzwerks innerhalb von Rechenzentren und über Rechenzentren hinweg
- Erweiterte Sicherheit und leistungsfähige Netzwerkdienste durch Partnerschaft mit führenden Drittanbietern



Netzwerkvirtualisierung und das SDDC

VMware NSX stellt ein völlig neues Betriebsmodell für Netzwerke bereit, das die Grundlage eines Software-Defined Datacenter bildet. Da NSX Netzwerke in der Software abbildet, profitieren die Betreiber von Rechenzentren von einem deutlich höheren Maß an Agilität, Sicherheit und Wirtschaftlichkeit als bei physischen Netzwerken. NSX stellt umfassende logische Netzwerkelemente und -services bereit: logisches Switching, Routing, Firewalling, Lastausgleichsfunktionen, VPNs, Servicequalität (QoS) und Überwachung. Diese Services werden in virtuellen Netzwerken mithilfe einer Cloud-Managementplattform bereitgestellt, die die APIs von NSX nutzt. Virtuelle Netzwerke werden unterbrechungsfrei auf jeder vorhandenen Netzwerkhardware bereitgestellt.

Wichtigste Funktionen von NSX

Switching	Unterstützung logischer Layer 2-Overlay-Erweiterungen in einer gerouteten (L3) Fabric innerhalb und außerhalb des Rechenzentrums. Unterstützung für VXLAN-basierte Netzwerk-Overlays.
Routing	Dynamisches Routing zwischen virtuellen Netzwerken im Hypervisor-Kernel, skalierbares Routing mit Aktiv/Aktiv-Failover auf physische Router. Unterstützung von Protokollen für statisches Routing und dynamisches Routing (OSPF, BGP).
Verteiltes Firewalling	Verteilte Stateful Firewall, eingebettet in den Hypervisor-Kernel für eine Firewall-Kapazität von bis zu 20 Gbit/s pro Hypervisor-Host. Unterstützung von Active Directory und Aktivitätsüberwachung. NSX kann mithilfe von NSX Edge™ außerdem Nord-Süd-Firewall-Funktionen bereitstellen.

Lastausgleich	L4-L7-Lastausgleich mit SSL-Offload und Pass-Through, Server-Systemdiagnosen und Anwendungsregeln für Programmierbarkeit und Manipulation des Datenverkehrs
VPN	Funktionen für Site-to-Site- und Remote-Zugriffs-VPNs, nicht gemanagtes VPN für Cloud-Gateway-Services
NSX-Gateway	Unterstützung für VXLAN-zu-VLAN-Bridging für die nahtlose Verbindung mit physischen Workloads. Diese Funktion ist in NSX eingebettet und wird zudem auch über Top-of-Rack-Switches von Partnern bereitgestellt.
NSX API	RESTful API für die Integration in beliebige Cloud-Managementplattformen oder für die benutzerdefinierte Automatisierung
Betrieb	Native Betriebsfunktionen wie eine zentrale CLI, Traceflow, SPAN und IPFIX für die Fehlerbehebung und proaktive Überwachung der Infrastruktur. Integration in Tools wie VMware vRealize® Operations™ und vRealize Log Insight™ für die erweiterte Analyse und Fehlerbehebung. NSX Application Rule Manager und Endpoint Monitoring ermöglichen die Visualisierung des End-to-End-Netzwerkdatenverkehrs bis Layer 7, sodass Anwendungsteams innerhalb von Dateien und über Dateien hinweg Endpunkte in Rechenzentren aufzeigen und durch entsprechende Sicherheitsregeln reagieren können.
Dynamische Sicherheitsrichtlinie	Der NSX Service Composer ermöglicht die Erstellung dynamischer Sicherheitsgruppen. Die Zugehörigkeit zu Sicherheitsgruppen kann nicht nur auf Basis der IP- und MAC-Adresse, sondern auch auf Basis von VMware vCenter™-Objekten und -Tags, Betriebssystemtyp und Active Directory-Rollen definiert werden und ermöglicht so die Durchsetzung dynamischer Sicherheitsrichtlinien.
Cloud-Management	Direkte Integration in vRealize Automation™ und OpenStack.
Integration in Partnerprodukte	Unterstützung für die Integration von Drittanbieterprodukten in die Management-, Steuerungs- und Datenebene in zahlreichen Kategorien wie Firewalls der nächsten Generation, IDS/IPS, agentenlose Virenschutzsoftware, Controller für die Anwendungsbereitstellung, Funktionen für Switching, Betrieb und Transparenz, erweiterte Sicherheit und vieles mehr.
Cross vCenter Networking and Security	Nutzung von Netzwerk- und Sicherheitsfunktionen über die Grenzen von vCenter und Ihrer Rechenzentren hinaus, unabhängig von der zugrunde liegenden physischen Topologie. Dadurch werden Funktionen wie Disaster Recovery und Aktiv/Aktiv-Rechenzentren ermöglicht.
Protokollmanagement	Lösen Sie Probleme schneller durch die zusätzliche Transparenz von vRealize Log Insight für NSX. Veranschaulichen Sie Ereignistrends, lösen Sie Warnungen aus und profitieren Sie von vielen weiteren Vorteilen – in Echtzeit.

Anwendungsbereiche

Sicherheit

NSX ermöglicht Unternehmen die logische Gliederung ihres Rechenzentrums in einzelne Sicherheitssegmente – bis hinab auf die Ebene einzelner Workloads und unabhängig vom Netzwerksubnetz oder VLAN der Workloads. Die IT-Teams können dann für jeden Workload Sicherheitsrichtlinien und -kontrollen auf der Grundlage dynamischer Sicherheitsgruppen definieren, wodurch eine sofortige Reaktion auf Bedrohungen im Rechenzentrum und die Durchsetzung von Richtlinien auf Ebene einzelner virtueller Maschinen möglich wird. Gelingt es einem Angreifer, die Sicherheitsmaßnahmen am Perimeter des Rechenzentrums zu überwinden, können sich die Bedrohungen nicht wie in herkömmlichen Netzwerken lateral im Rechenzentrum ausbreiten.

Automatisierung

Mit NSX lassen sich Herausforderungen im Zusammenhang mit der zeitaufwendigen Netzwerkbereitstellung, Konfigurationsfehlern und kostspieligen Prozessen durch die Automatisierung arbeitsintensiver und fehleranfälliger Aufgaben bewältigen. NSX ermöglicht die Erstellung softwarebasierter Netzwerke, wodurch sich die typischen Engpässe hardwarebasierter Netzwerke vermeiden lassen.

Dank der nativen Integration von NSX in Cloud-Managementplattformen wie vRealize Automation oder OpenStack kann die Automatisierung weiter verbessert werden.

Anwendungskontinuität

Da NSX Netzwerkfunktionen von der zugrunde liegenden Hardware abstrahiert, werden Netzwerkvorgänge und Sicherheitsrichtlinien mit den jeweiligen Workloads verknüpft. Dadurch können Unternehmen auf einfache Weise vollständige Anwendungsumgebungen für Disaster Recovery-Zwecke in Remote-Rechenzentren replizieren, zwischen einzelnen Rechenzentren verschieben oder in einer Hybrid Cloud-Umgebung bereitstellen – und dies innerhalb weniger Minuten, ohne Beeinträchtigung des Anwendungsbetriebs und ohne Eingriff in das physische Netzwerk.

Editions von VMware NSX

Neue NSX-Angebote ermöglichen es noch mehr Kunden, ihre individuellen Anforderungen an die Netzwerkvirtualisierung zu erfüllen und mit dem Umstieg auf ein Software-Defined Datacenter zu beginnen.

Standard

Für Unternehmen, die die Agilität und Automatisierung ihres Netzwerks verbessern möchten

Advanced

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

Enterprise

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

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter http://www.vmware.com/go/nsx.

Einzelheiten zur Lizenzierung der Funktionen der einzelnen NSX-Editions finden Sie unter https://kb.vmware.com/kb/2145269.

Wenn Sie ein VMware-Produkt erwerben möchten oder weitere Informationen über alle VMware-Produkte benötigen, setzen Sie sich unter 0800 100 6711 direkt mit VMware in Verbindung. Sie können auch unsere Website unter http://www.vmware.com/de/products besuchen oder online nach einem autorisierten Händler suchen.

	STANDARD	ADVANCED	ENTERPRISE
Verteiltes Switching und Routing	•	•	•
NSX Edge-Firewall	•	•	•
NAT	•	•	•
Software-L2-Bridging zur physischen Umgebung	•	•	•
Dynamisches Routing mit ECMP (Aktiv/Aktiv)	•	•	•
API-gesteuerte Automatisierung	•	•	•
Integration in vRealize und OpenStack	•	•	•
Protokollmanagement mit vRealize Log Insight für NSX	•	•	•
Automatisierung von Sicherheitsrichtlinien mit vRealize		•	•
NSX Edge-Lastausgleich		•	•
Verteiltes Firewalling		•	•
Integration in Active Directory		•	•
Überwachung der Serveraktivität		•	•
Service-Integration (Integration von Drittanbieterprodukten)		•	•
Integration von VMware AirWatch®		•	•
Application Rule Manager		•	•
Cross vCenter NSX			•
NSX-Optimierungen für mehrere Standorte			•
VPN (IPSEC und SSL)			•
Remote-Gateway			•
Integration von Hardware-VTEPs			•
Endpoint-Überwachung			•

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Freisinger Str. 3 85716 Unterschleißheim/Lohhof Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de