VMware NSX Data Center

DIE WICHTIGSTEN VORTEILE

- Schutz von Anwendungen durch Mikrosegmentierung auf Workload-Ebene und detaillierte Sicherheit
- Reduzieren des Zeitaufwands für die Netzwerkbereitstellung von mehreren Tagen auf wenige Sekunden und höhere betriebliche Effizienz durch Automatisierung
- Konsistentes Management von Networking- und Sicherheitsrichtlinien, unabhängig von der physischen Netzwerktopologie innerhalb von sowie über Rechenzentren und native Public Clouds hinweg
- Detaillierte Virtualisierung der Anwendungstopologie, Empfehlungen für automatisierte Sicherheitsrichtlinien und durchgehende Überwachung von Abläufen.

VMware NSX® Data Center ist eine Plattform für Netzwerkvirtualisierung und Sicherheit, die die Grundlage des Virtual Cloud Network bildet. Dieser Software-Defined-Ansatz im Bereich Networking umfasst Rechenzentren, Clouds und Anwendungs-Frameworks. NSX Data Center verlagert Networking und Sicherheit näher an die Anwendung, unabhängig von deren Ausführungsort; von virtuellen Maschinen (VMs) über Container bis hin zu Bare-Metal-Systemen. Wie beim Betriebsmodell für VMs können auch Netzwerke unabhängig von der zugrunde liegenden Hardware bereitgestellt und verwaltet werden. NSX Data Center reproduziert das gesamte Netzwerkmodell als Software, sodass jede Netzwerktopologie – von einfachen bis zu komplexen mehrschichtigen Netzwerken – in Sekunden erstellt und bereitgestellt werden kann. Durch eine Kombination der Services von NSX oder zahlreichen Drittanbietern im Partnernetz (z.B. Firewalls der nächsten Generation oder Performance-Managementlösungen) können verschiedene virtuelle Netzwerke mit unterschiedlichen Anforderungen erstellt werden, was zu erhöhter Agilität und Sicherheit in Umgebungen aller Art führt. Diese Services können anschließend auf eine Reihe von Endpunkten innerhalb von Clouds sowie cloudübergreifend ausgedehnt werden.

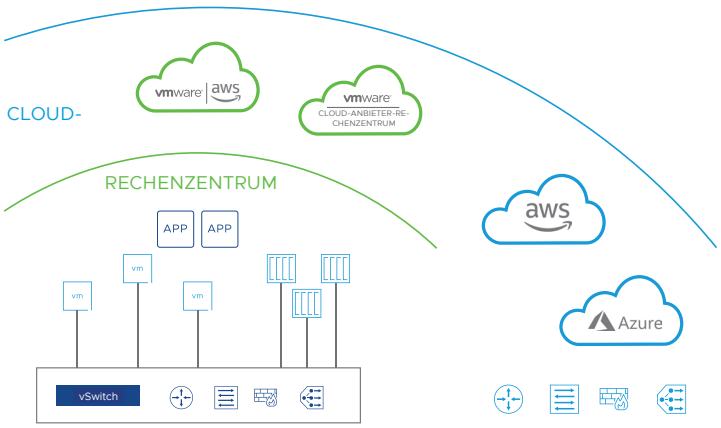

ABBILDUNG 1: NSX Data Center-Plattform für Netzwerkvirtualisierung und Sicherheit

Networking in Software

VMware NSX Data Center stellt ein völlig neues Networking-Betriebsmodell bereit, das in der Software definiert ist, die die Grundlage des Software-Defined Datacenter (SDDC) bildet und sich bis in ein Virtual Cloud Network ausdehnt. Betreiber von Rechenzentren profitieren jetzt von einem deutlich höheren Maß an Agilität, Sicherheit und Wirtschaftlichkeit, das in physischen Netzwerken bislang nicht erreicht werden konnte, weil das Netzwerk ausschließlich an physische Hardwarekomponenten gebunden war. NSX Data Center bietet umfassende logische Networking- und Sicherheitsfunktionen und entsprechende Services wie logisches Switching, Routing, Firewalling, Lastausgleich, virtuelles privates Netzwerk (VPN), Servicequalität (QoS) und Überwachung. Diese Services werden in virtuellen Netzwerken mithilfe einer Cloud-Management-Plattform bereitgestellt, die NSX Data Center-APIs nutzt. Virtuelle Netzwerke werden unterbrechungsfrei auf vorhandener Networking-Hardware bereitgestellt und können sich über Rechenzentren, Public und Private Clouds, Container-Plattformen und Bare-Metal-Server erstrecken.

Wesentliche Merkmale

Switching	Unterstützung logischer Layer-2-Overlay-Erweiterungen in einer gerouteten Fabric (Layer 3) innerhalb und außerhalb des Rechenzentrums. Unterstützung von VXLAN- und GENEVE-basierten Netzwerk-Overlays.
Routing	Dynamisches, verteiltes Routing zwischen virtuellen Netzwerken im Hypervisor-Kernel, horizontal skalierbares Routing mit Aktiv-Aktiv-Failover auf physischen Routern; Unterstützung von Protokollen für statisches und dynamisches Routing, einschließlich IPv6-Unterstützung.
Gateway-Firewall	Stateful Firewalling bis zu Layer 7 (einschließlich Anwendungserkennung und URL-Whitelisting), eingebettet im NSX-Gateway, verteilt über die gesamte Umgebung mit zentralisierten Richtlinien und Management.
Verteilte Firewall	Stateful Firewalling bis zu Layer 7 (einschließlich Anwendungserkennung und URL-Whitelisting), eingebettet in einen Hypervisor-Kernel, verteilt über die gesamte Umgebung mit zentralisierten Richtlinien und Management. Darüber hinaus integriert sich die NSX Distributed Firewall direkt in cloudnative Plattformen, wie Kubernetes und Pivotal Cloud Foundry, native Public Clouds, wie AWS und Azure, sowie Bare-Metal-Server.
Lastausgleich	L4-L7-Lastausgleich mit SSL-Offload und Pass-Through, Server-Systemdiagnosen (und passive Systemdiagnosen) und Anwendungsregeln für Programmierbarkeit und Manipulation des Datenverkehrs über GUI oder API.
VPN	Funktionen für Site-to-Site- und Remote-Zugriff via VPN, nicht verwaltetes VPN für Cloud-Gateway-Services
NSX-Gateway	Unterstützung von Bridging zwischen im physischen Netzwerk konfigurierten VLANs und NSX-Overlay-Netzwerken für nahtlose Konnektivität zwischen virtuellen und physischen Workloads.
NSX Intelligence™	NSX Intelligence stellt Empfehlungen für automatisierte Sicherheitsrichtlinien sowie durchgehende Überwachung und Virtualisierung jedes einzelnen Datenflusses im Netzwerk bereit und bietet somit eine erhöhte Transparenz, durch die der Sicherheitsstatus hochgradig und unkompliziert überprüfbar wird. Als Teil derselben Benutzeroberfläche wie NSX-T™ Data Center stellt NSX Intelligence eine zentrale Oberfläche für Netzwerk- und Sicherheitsteams bereit.
NSX Data Center-API	Auf JSON basierende RESTful API zur Integration von Cloud-Management-Plattformen, DevOps-Automatisierungstools und anwenderdefinierter Automatisierung.
Betrieb	Native Betriebsfunktionen, z.B. eine zentrale CLI, Traceflow, logische Overlay-SPAN und IPFIX zur Fehlerbehebung und proaktiven Überwachung der virtuellen Netzwerkinfrastruktur. Integration in Tools wie VMware vRealize® Network Insight™ zur erweiterten Analyse und Fehlerbehebung.
Kontextbezogene Mikrosegmentierung	Dynamisches Erstellen und automatisches Aktualisieren von Sicherheitsgruppen und Richtlinien auf Basis von Attributen, die über IP-Adressen, Ports und Protokolle hinausgehen. Dazu gehören beispielsweise Elemente wie Maschinenname und Tags, Betriebssystemtyp und Layer 7-Anwendungsdaten, die eine adaptive Mikrosegmentierungsrichtlinie gestatten. Auf Identitätsdaten aus Active Directory und anderen Quellen basierte Richtlinien bieten Sicherheit auf Anwenderebene bis hinunter zur einzelnen Sitzungsebene in RDS und Umgebungen mit virtueller Desktop-Infrastruktur (VDI).
Automatisierung und Cloud-Management	Native Integration in vRealize Automation™/VMware Cloud™ Automation Services, OpenStack und diverse andere. Vollständig unterstützte Ansible-Module, vollständig unterstützter Terraform-Anbieter und PowerShell-Integration.
Integration von Partnerprodukten	Integration von Partnerprodukten in die Management-, Steuerungs- und Datenebene in zahlreichen Kategorien, z.B. Firewall der nächsten Generation, System zur Erkennung von Eindringversuchen (IDS)/Abwehr von Eindringversuchen (IPS), agentenlose Virenschutzsoftware, Funktionen für Switching, Betrieb und Transparenz, erweiterte Sicherheit und vieles mehr.
Multi-Cloud-Networking und -Sicherheit	Konsistentes Networking und Sicherheitsfunktionen über die Grenzen von Rechenzentren und Private und Public Clouds hinaus, unabhängig von der zugrunde liegenden physischen Topologie oder Cloud-Plattform.
Networking- und Sicherheitsfunktionen für Container	Unterstützung von Lastausgleich, Mikrosegmentierung (verteiltes Firewalling), Routing und Switching für Container auf Plattformen, die auf Kubernetes und Cloud Foundry basieren und entweder in VMs oder auf Bare-Metal-Hosts ausgeführt werden. Bietet Transparenz für Container-Netzwerkdatenverkehr (logische Ports, SPAN/Mi, IPFIX und Traceflow).

Anwendungsbereiche

Sicherheit

NSX Data Center macht die betriebliche Umsetzung von Zero-Trust-Sicherheit für Anwendungen in Private und Public Cloud-Umgebungen realisierbar und effizient. Wenn es darum geht, kritische Anwendungen zu sperren, eine logische Demilitarized Zone (DMZ) in Software zu erstellen oder die Angriffsfläche einer virtuellen Desktop-Umgebung zu verkleinern, bietet NSX Data Center Mikrosegmentierung, um Netzwerksicherheitsrichtlinien auf Ebene der einzelnen Workloads zu definieren und durchzusetzen.

Multi-Cloud-Networking

NSX Data Center stellt eine Lösung zur Netzwerkvirtualisierung bereit, die konsistente Networking- und Sicherheitsfunktionen für heterogene Standorte bietet, um den Multi-Cloud-Betrieb zu optimieren. Dadurch eignet sich NSX Data Center für zahlreiche Multi-Cloud-Anwendungsbereiche, von nahtloser Rechenzentrumserweiterung über die Erstellung von Ressourcenpools für mehrere Rechenzentren bis zu schneller Workload-Mobilität.

Automatisierung

Durch die Virtualisierung von Networking- und Sicherheitsservices beschleunigt NSX Data Center die Bereitstellung von Full-Stack-Anwendungen, indem es die Engpässe manuell verwalteter Networking- und Sicherheitsservices und -richtlinien beseitigt. NSX Data Center ist nativ in Cloud-Management-Plattformen und andere Automatisierungstools wie vRealize Automation/VMware Cloud Automation Services, OpenStack, Terraform, Ansible und andere integrierbar, sodass Entwickler und IT-Teams in der Lage sind, Anwendungen mit dem notwendigen Tempo bereitzustellen und zu verwalten.

Networking und Sicherheit für cloudnative Anwendungen

NSX Data Center bietet umfassende, integrierte Networking- und Sicherheitsfunktionen für containerbasierte Anwendungen und Mikroservices und stellt detaillierte Richtlinien auf Container-Basis bereit, sobald neue Anwendungen verfügbar sind. Dies ebnet den Weg für natives Container-to-Container-L3-Networking, Mikrosegmentierung für Mikroservices sowie End-to-End-Transparenz von Networking- und Sicherheitsrichtlinien für herkömmliche und neue Anwendungen.

VMware NSX Data Center Editions

Standard

Für Unternehmen, die agiles, automatisiertes Networking benötigen

Professional

Für Unternehmen, die über den Funktionsumfang der Standard Edition hinaus Mikrosegmentierung benötigen und ggf. über Public Cloud-Endpunkte verfügen

Advanced

Für Unternehmen, die über den Funktionsumfang der Professional Edition hinaus erweiterte Networking- und Sicherheitsservices sowie Integration in verschiedene Partnerlösungen benötigen und ggf. über mehrere Standorte verfügen

Enterprise Plus

Für Unternehmen, die neben allen hochentwickelten Funktionen von NSX Data Center auch Netzwerkbetrieb mit vRealize Network Insight, Hybrid Cloud-Mobilität mit VMware HCX® und Datenverkehrstransparenz und Sicherheitsvorgänge mit NSX Intelligence benötigen.

Remote Office/Branch Office (ROBO)

Für Unternehmen, die Networking- und Sicherheitsservices für Anwendungen an Remote-Standorten oder in Zweigstellen virtualisieren müssen

	STANDARD	PROFESSIONAL	ADVANCED	ENTERPRISE PLUS	ROBO
NSX DATA CENTER[1]					
Verteiltes Switching und Routing	•	•	•	•	•[5]
NSX Gateway Firewall (Zustandsbehaftet)	•	•	•	•	•
NSX Gateway NAT	•	•	•	•	•
Software-L2-Bridging zu physischen Umgebungen	•	•	•	•	
Dynamisches Routing mit ECMP (Aktiv-Aktiv)	•	•	•	•	•
Integration in Cloud-Management-Plattformen[3]	•	•	•	•	•
Verteiltes Firewalling für auf Bare-Metal ausgeführte VMs und Workloads		•	•	•	•
VPN (L2 und L3)		•	•	•	•
Integration in NSX Cloud[4] for AWS und Azure-Unterstützung		•	•	•	•
Lastausgleich			•	•	•
Integration in verteilte Firewall (Einbindung von Active Directory, VMware AirWatch®, Endgeräteschutz und Drittanbieterservices)			•	•	•
Networking- und Sicherheitsfunktionen für Container			•	•	
Standortübergreifende Networking- und Sicherheitsfunktionen			•	•	
IPv6			•	•	
Kontextbezogene Mikrosegmentierung (Anwendungsidentifikation, RDSH, Protokollanalysefunktion)				•	
Erweiterte NSX Gateway-Firewall (Anwendungsidentifikation, Protokollanalysefunktion)				•	
URL-Filterung				•	
+NSX INTELLIGENCE					
Analyse des Datenverkehrs zwischen VMs				•	
Firewall-Transparenz				•	
Automatisierte Sicherheitsrichtlinie				•	
Analysefunktionen für Empfehlungen zu Regeln und Gruppen				•	
+vREALIZE NETWORK INSIGHT ADVANCED[2]					
Datenverkehrstransparenz (IPFIX) und Netzwerküberwachung				•	
Firewall-Planung und -Management				•	
NSX – Betrieb und Fehlerbehebung				•	
+VMWARE HCX ADVANCED[2]					
Workload-Migration in großem Umfang				•	
WAN-Optimierung zur Workload-Migration				•	
Verbindungsübergreifendes Datenverkehrs- und Lastmanagement				•	

1. Detaillierte, aktuelle Informationen zu den Funktionen und Merkmalen finden Sie in den jeweiligen Knowledgebase-Artikeln zu NSX Data Center for vSphere®- sowie NSX-T Data Center-Funktionen.
2. NSX Data Center Enterprise Plus umfasst Vollversionen von vRealize Network Insight Advanced und VMware HCX Advanced.
3. Nur L2-, L3- und NSX Gateway-Integration. Keine Nutzung von Sicherheitsgruppen.
4. Für Public Cloud-Workloads ist ein NSX Cloud-Abonnement erforderlich.
5. Nur Switching, VLAN-gestützt.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel.: 877-486-9273 Fax: 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Willy-Brandt-Platz 2 81829 München Tel.: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de