VMware NSX Cloud

Hybrid Cloud-Networking und -Sicherheit für Private und Public Clouds

AUF EINEN BLICK

VMware NSX® Cloud stellt einheitliche Networking- und Sicherheitsfunktionen für nativ in der Public Cloud ausgeführte Anwendungen bereit. NSX Cloud verwendet dieselbe Management- und Steuerungsebene wie NSX Data Center. Unternehmen profitieren damit von einer einzigen Networking- und Sicherheitslösung vom internen Rechenzentrum bis zur Public Cloud.

DIE WICHTIGSTEN VORTEILE

Einheitliche Networking- und Sicherheitsfunktionen für Public Clouds wie AWS und Azure für eine deutlich bessere Skalierbarkeit, Kontrolle und Transparenz bei gleichzeitig niedrigeren OpEx:

- Bereitstellungsflexibilität mittels NSX-Gebilden oder nativen Public Cloud-Gebilden
- Einfache Skalierbarkeit in virtuellen Netzwerken, Availability Zones, Regionen und Public Clouds
- Schutz und Standardisierung von Anwendungen durch eine präzise Kontrolle von Networking- und Sicherheitsservices
- Integrität und Compliance von Anwendungen in Public Clouds dank umfassender Networking- und Sicherheitstransparenz

PREISE

- Abonnementbasierte Preise, erhältlich im Rahmen befristeter Lizenzen (ein- oder dreijährig)
- Auf Basis von vCPUs, die von aktivierten Workloads innerhalb der Public Cloud verbraucht werden, unabhängig von der Anzahl der virtuellen Netzwerke; beispielsweise AWS Virtual Private Clouds (VPCs) und Azure Virtual Networks (VNets)
- Keine NSX Data Center-Lizenz für reine Cloud-Anwendungsbereiche erforderlich

Ein für Cloud-Prinzipien konzipiertes Netzwerk

VMware NSX Cloud bietet einheitliche Networking- und Sicherheitsfunktionen für Ihre nativ in Public Clouds ausgeführten Anwendungen. Zusammen mit der VMware NSX-Produktreihe bildet VMware NSX Cloud das Virtual Cloud Network – ein Software-Defined Networking-Ansatz, der sich über Rechenzentren, Clouds, Endpunkte und IoT-Komponenten erstreckt.

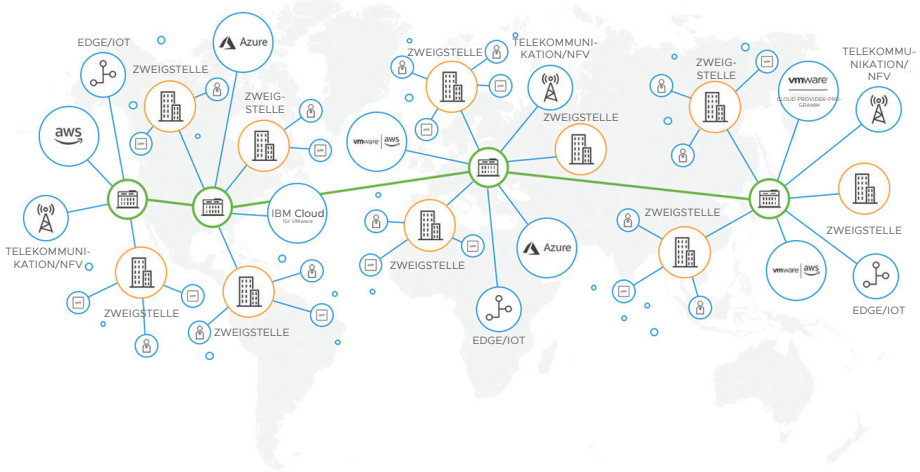

ABBILDUNG 1: Virtual Cloud Network.

Anwendungsbereiche

Konsistente Sicherheit für alle Clouds

NSX Cloud bietet eine Richtlinie für Workloads, die in verschiedenen Public Clouds und On-Premises-Rechenzentren ausgeführt werden. Eine Richtlinie muss nur einmal definiert werden und kann dann von jedem Standort aus auf Workloads angewendet werden – in unterschiedlichen virtuellen Cloud-Netzwerken, Regionen, Availability Zones und unabhängig vom jeweiligen Cloud-Anbieter. Sicherheitsrichtlinien werden abhängig von Anwendungsattributen und anwenderdefinierten Tags dynamisch auf die einzelnen Workloads angewendet. Gefährliche oder kompromittierte Workloads lassen sich sogar automatisch in Quarantäne verschieben, wenn nicht die richtigen Mikrosegmentierungs-Sicherheitsrichtlinien angewendet wurden. NSX Cloud unterstützt eine North-South-Einbindung von Services. Dadurch kann bestimmter Datenverkehr zum erweiterten Schutz an Sicherheits-Appliances von Drittanbietern weitergeleitet werden.

Präzise Kontrolle über Cloud Networking

VMware NSX Cloud ist auf native Public Cloud-Umgebungen wie Amazon (AWS) und Microsoft Azure ausgelegt. NSX Cloud ergänzt die über Public Cloud-Anbieter verfügbaren nativen Services. Mit NSX Cloud können Sie die Infrastruktur- und Anwendungsservices für Workloads von Public Cloud-Anbietern ohne Einschränkungen weiter nutzen (z.B. AWS ELB/Azure Load Balancer, AWS Route 53/ Azure DNS, AWS Direct Connect/Azure ExpressRoute und Amazon RDS/Azure Database). Unter Verwendung Ihrer vorhandenen Automatisierungstools lassen sich außerdem Provisioning und Konfigurationsmanagement über REST-API-Anfragen automatisieren. NSX Cloud unterstützt darüber hinaus Gateway-Konsolidierung bei der Übertragung in VPCs/VNets. Dadurch wird der Betrieb vereinfacht und Sie können integrierte Services wie Site-to-Site-VPN sowie Edge-/Übertragungsservices von Drittanbietern nutzen.

Umfassende Kontrolle und Transparenz des Betriebs

VMware NSX Cloud stellt Standardschnittstellen und -protokolle für den Zugriff auf Netzwerk- und Sicherheitsdaten aus Cloud-Netzwerken bereit. Datenfluss-, Paket- und Ereignisinformationen sind über IPFIX, Traceflow, Portspiegelung und Syslog verfügbar. Diese Daten können von vorhandenen On-Premises-Betriebstools genutzt werden, um tief greifende, umfassende Transparenz für Überwachung, Fehlerbehebung und Auditing zu gewährleisten. Mit diesen umfangreichen Betriebsdaten lassen sich Netzwerkkonnektivitäts-, Performance- und Sicherheitsprobleme über die gesamte Hybrid Cloud-Bereitstellung hinweg – einschließlich On-Premises- und Public Cloud-Anwendungen – schneller ermitteln und beheben. NSX Cloud bietet detaillierte Transparenz im Hinblick auf Public Cloud-Workloads in sämtlichen VPCs/VNets, umfassende Such- und Filterfunktionen für einfacheres Management sowie die Möglichkeit zur Auswahl von Workloads, die mit NSX verwaltet werden sollen.

Wesentliche Merkmale

NSX-Durchsetzungsmodus – Verwenden Sie NSX-Tools für die einheitliche Einhaltung von Sicherheits- und Networking-Richtlinien bei allen On-Premises- und nativen Public Cloud-Workloads.

Nativer Cloud-Durchsetzungsmodus – Verwenden Sie die Sicherheits- und Networking-Gebilde eines Public Cloud-Anbieters für die einheitliche Einhaltung von Sicherheits- und Networking-Richtlinien bei allen On-Premises- und nativen Public Cloud-Workloads.

Erkennung und Schutz nativer Public Cloud Service-Endpunkte – Erkennen und schützen Sie native Public Cloud Service-Endpunkte sowie virtuelle Maschinen (VMs) und EC2-Instanzen.

Multi-Cloud-Networking und -Sicherheit an mehreren Standorten – Stellen Sie Endpunkten in mehreren Clouds Networking- und Sicherheitsfunktionen bereit. Gewährleisten Sie durch die Integration in NSX Data Center außerdem ein cloud- sowie rechenzentrumsübergreifendes Networking- und Sicherheitsmanagement.

Mikrosegmentierung – Sichern Sie sich die Kontrolle über den East-West-Traffic zwischen nativ in Public Clouds ausgeführten Anwendungs-Workloads. NSX Cloud bietet zudem Mikrosegmentierung von virtuellen Desktops, die über VMware Horizon® Cloud on Azure bereitgestellt werden.

Umfangreiche Abstrahierung zum Festlegen von Sicherheitsrichtlinien – Legen Sie Sicherheitsgruppen und -regeln anhand umfangreicher Richtliniengebilde wie Instanzname, OS-Typ, AMI-ID und benutzerdefinierten Tags fest.

Dynamische Richtlinie – Automatische Anwendung und Durchsetzung von Sicherheitsrichtlinien anhand von Instanzattributen und benutzerdefinierten Tags: Richtlinien folgen Instanzen automatisch, wenn diese innerhalb von Clouds und cloudübergreifend verschoben werden.

Quarantäneinstanzen – Stellen Sie gefährliche oder kompromittierte Workloads, die ohne Sicherheit durch Mikrosegmentierung in der Public Cloud ausgeführt werden, unter Quarantäne. Unter Quarantäne gestellte Instanzen werden an der Kommunikation im Cloud-Netzwerk gehindert. Dabei werden mehrere Sicherheitsstufen bereitgestellt.

Service-Einbindung – Leiten Sie bestimmten North-South-Traffic mithilfe von richtlinienbasiertem Routing an eine Drittanbieter-Firewall-Appliance der nächsten Generation weiter.

Site-to-Site-VPN – Nutzen Sie die integrierte VPN-Unterstützung für Backhaul-Datenverkehr zu On-Premises-Rechenzentren.

WENN SIE EIN VMWARE-PRODUKT ERWERBEN MÖCHTEN ODER WEITERE INFORMATIONEN BENÖTIGEN,

setzen Sie sich unter der folgenden Telefonnummer direkt mit VMware in Verbindung: 0800 100 6711. Sie können auch unsere Website unter *vmware.com/de/products/nsx-cloud* oder *vmware.com/de/products* besuchen oder online nach einem autorisierten Händler suchen.

Verteilte Architektur – Mit der verteilten Firewalling-Architektur der NSX Cloud lassen sich zusätzliche Netzwerk-Hops und überschüssiger Datenverkehr beseitigen. Sie setzt Richtlinien an der virtuellen Netzwerkschnittstelle jeder einzelnen Instanz durch, anstatt durch eine externe Firewall zu routen.

Gemeinsam genutztes Gateway bei der Übertragung in VPCs/VNets – Nutzen Sie Gateway-Konsolidierung bei der Übertragung in VPCs/VNets, was zu einer einfacheren Administration und schnellerem Onboarding von Computing-VPCs/VNets führt und das Einbinden von Drittanbieter-Services gestattet.

Edge Firewalling – Nutzen Sie Stateful Firewalling zum Filtern des North-South-Traffics zwischen Instanzen in virtuellen Netzwerken und im öffentlichen Internet.

RESTful API – Mithilfe von RESTful API und Automatisierungstools werden Networking- und Sicherheitsinfrastrukturen programmgesteuert und bedarfsorientiert bereitgestellt und konfiguriert.

Vorlagen – Mit vorhandenen Automatisierungs- und Orchestrierungstools können Sie standardisierte Anwendungsvorlagen erstellen, die das Provisioning und Management von Networking- und Sicherheitsservices in Public Clouds vereinfachen.

East-West-Traffic-Transparenz – Nutzen Sie Ihre vorhandenen Tools für Tag 2-Abläufe, um Einblick in den East-West-Traffic innerhalb von und zwischen VPCs zu erhalten.

Sicherheitsprotokollierung – Profitieren Sie von Echtzeittransparenz und der Prüfung von Sicherheitsereignissen, z.B. Zulassen/Verweigern und Quarantänevorfälle. Informationen zu Sicherheitsereignissen können an einen Syslog- oder SIEM-Server gesendet werden.

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