VMWARE NSX CLOUD

Einheitliche Netzwerk- und Sicherheitsfunktionen für native Anwendungen in Public Clouds

AUF EINEN BLICK

VMware NSX® Cloud stellt einheitliche Netzwerk- und Sicherheitsfunktionen für Anwendungen bereit, die nativ in der Public Cloud ausgeführt werden. NSX Cloud verwendet dieselbe Managementebene und dieselbe Steuerungsebene wie NSX Data Center. Unternehmen profitieren damit von einer einzigen Netzwerk- und Sicherheitslösung vom internen Rechenzentrum bis hin zur Public Cloud.

DIE WICHTIGSTEN VORTEILE

Einheitliche Netzwerk- und Sicherheitsfunktionen für Public Clouds wie AWS und Azure für eine deutliche bessere Skalierbarkeit, Kontrolle und Transparenz bei niedrigeren Betriebskosten

- Einfache Skalierbarkeit in allen virtuellen Netzwerken, Verfügbarkeitszonen, Regionen und Public Clouds
- Schutz und Standardisierung von Anwendungen durch eine präzise Kontrolle von Sicherheits- und Netzwerkservices
- Integrität und Compliance von Anwendungen in Public Clouds dank durchgängiger Transparenz von Netzwerk und Sicherheit

PREISE

- Als 1-Jahres- oder 3-Jahres-Abonnement erhältlich
- Gebühren richten sich nach der Anzahl der von aktiven Public Cloud-Workloads genutzten vCPUs, unabhängig von der Anzahl virtueller Netzwerke (z.B. AWS VPCs, Azure VNets)
- Keine NSX Data Center-Lizenz für reine Cloud-Nutzung erforderlich

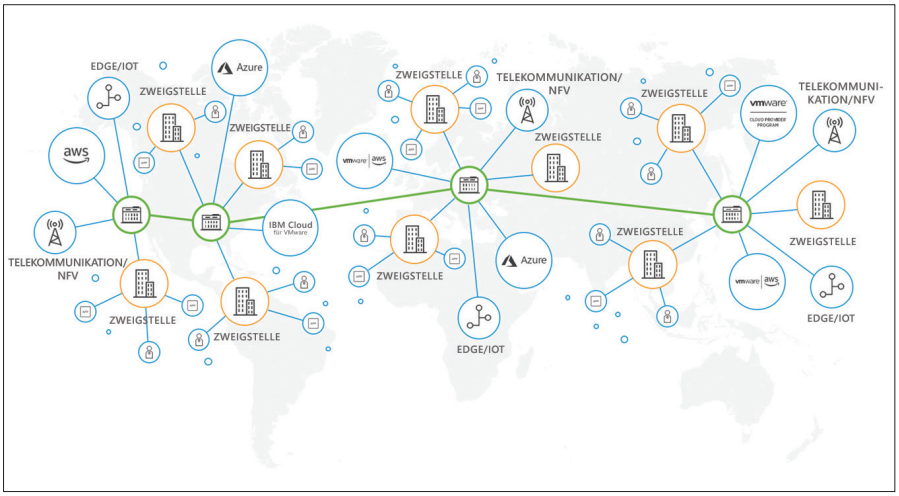

Abbildung 1: Das Virtual Cloud Network

Speziell für Cloud-Prinzipien entwickeltes Netzwerk

VMware NSX Cloud bietet einheitliche Netzwerk- und Sicherheitsfunktionen für Ihre Anwendungen, die nativ in Public Clouds ausgeführt werden. In Kombination mit der VMware NSX-Produktreihe bietet VMware NSX Cloud ein Virtual Cloud Network, also ein Software-Defined-Konzept für Netzwerke, das Rechenzentren, Clouds, Endpunkte und IoT-Komponenten umfasst.

Anwendungsbereiche

Konsistente Sicherheit für alle Clouds

NSX Cloud bietet Richtlinien für alle Workloads in unterschiedlichen Public Clouds. Da NSX Cloud dieselbe Steuerungsebene und dieselbe Managementebene wie NSX Data Center nutzt, lassen sich Richtlinien durchgängig in Rechenzentren und Clouds verwalten. Eine Richtlinie muss nur einmal definiert werden und kann dann überall auf Workloads angewendet werden – in unterschiedlichen virtuellen Cloud-Netzwerken, Regionen, Verfügbarkeitszonen und unabhängig vom Cloud-Anbieter. Sicherheitsrichtlinien werden abhängig von Anwendungsattributen und anwenderdefinierten Tags dynamisch auf die einzelnen Workloads angewendet. Gefährliche oder kompromittierte Workloads, auf die nicht die richtige Mikrosegmentierungs-Sicherheitsrichtlinien angewendet wurde, können automatisch in Quarantäne verschoben werden.

Präzise Kontrolle über Cloud-Netzwerke

VMware NSX Cloud ist für native Public Cloud-Umgebungen wie Amazon (AWS) und Microsoft Azure konzipiert. NSX Cloud ergänzt die über Public Cloud-Anbieter verfügbaren nativen Services. Mit NSX Cloud können Sie die Infrastruktur und Anwendungsservices eines Public Cloud-Anbieters ohne Einschränkungen weiter nutzen (z.B. AWS ELB/Azure Load Balancer, AWS Route53/Azure DNS, AWS Direct Connect/Azure ExpressRoute und Amazon RDS/Azure Database). Unter Verwendung Ihrer vorhandenen Automatisierungstools können Sie außerdem das Provisioning und Konfigurationsmanagement über REST API-Anfragen automatisieren.

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 www.vmware.com/de/products/nsx-cloud.html oder http://www.vmware.com/de/products besuchen und online nach einem autorisierten Händler suchen.

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, Port Mirroring und Syslog verfügbar. Sie können mit Ihren vorhandenen internen Betriebstools auf diese Daten zugreifen, um einen umfassenden und durchgängigen Einblick zu erhalten sowie Überwachung, Fehlerbehebung und Prüfung zu verbessern. Dank der umfassenden Betriebsdaten können Probleme mit der Netzwerkkonnektivität, der Performance und der Sicherheit in der gesamten Hybrid Cloud-Infrastruktur einschließlich interner Anwendungen und der Public Cloud deutlich schneller identifiziert und behoben werden.

Wesentliche Leistungsmerkmale

Standortübergreifende Multi-Cloud-Netzwerke und -Sicherheit: NSX Cloud stellt Netzwerk- und Sicherheitsfunktionen für Endpunkte in unterschiedlichen Clouds zur Verfügung und bietet durch die Integration in NSX Data Center ein cloud- und rechenzentrumsübergreifendes Netzwerk- und Sicherheitsmanagement.

Mikrosegmentierung: Kontrollierter East-West-Traffic zwischen Anwendungs-Workloads, die nativ in Public Clouds ausgeführt werden

Sicherheitsgruppen: Sicherheitsgruppen und -regeln können basierend auf umfassenden Richtlinienkonstrukten definiert werden, darunter Instanzname, Betriebssystemtyp, AMI-ID und anwenderdefinierte Tags.

Dynamische Richtlinie: Die Sicherheitsrichtlinie wird basierend auf Instanzattributen und anwenderdefinierten Tags automatisch angewendet und durchgesetzt. Die Richtlinien folgen den Instanzen automatisch, wenn diese innerhalb der Cloud und cloudübergreifend verschoben werden.

Quarantäneinstanzen: Verschieben Sie gefährliche oder kompromittierte Workloads, die ohne Sicherheit durch Mikrosegmentierung in der Public Cloud ausgeführt werden, in Quarantäne. Quarantäneinstanzen können nicht mit dem Cloud-Netzwerk kommunizieren.

Verteilte Architektur: Durch die verteilte Firewalling-Architektur von NSX Cloud entfallen zusätzliche Netzwerk-Hops und zusätzlicher Datenverkehr, da Richtlinien auf der virtuellen Netzwerkschnittstelle jeder Instanz durchgesetzt werden, anstatt sie über eine externe Firewall zu leiten.

Edge Firewalling: NSX Cloud bietet Stateful Firewalling, eine Funktion, die den North-South-Traffic zwischen Instanzen in virtuellen Netzwerken und im öffentlichen Internet filtert.

RESTful API: Mithilfe von RESTful API und Automatisierungstools werden Netzwerk- und Sicherheitsinfrastruktur programmgesteuert und bedarfsorientiert bereitgestellt und konfiguriert.

Vorlagen: Mit vorhandenen Automatisierungs- und Orchestrierungstools lassen sich standardisierte Anwendungsvorlagen erstellen, die das Provisioning und Management von Netzwerk- und Sicherheitsservices innerhalb von Public Clouds vereinfachen.

Transparenter East-West-Traffic: 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 Prüfung von Sicherheitsereignissen wie Zulassen/Verweigern und Quarantäne-Incidents. Die 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 Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de