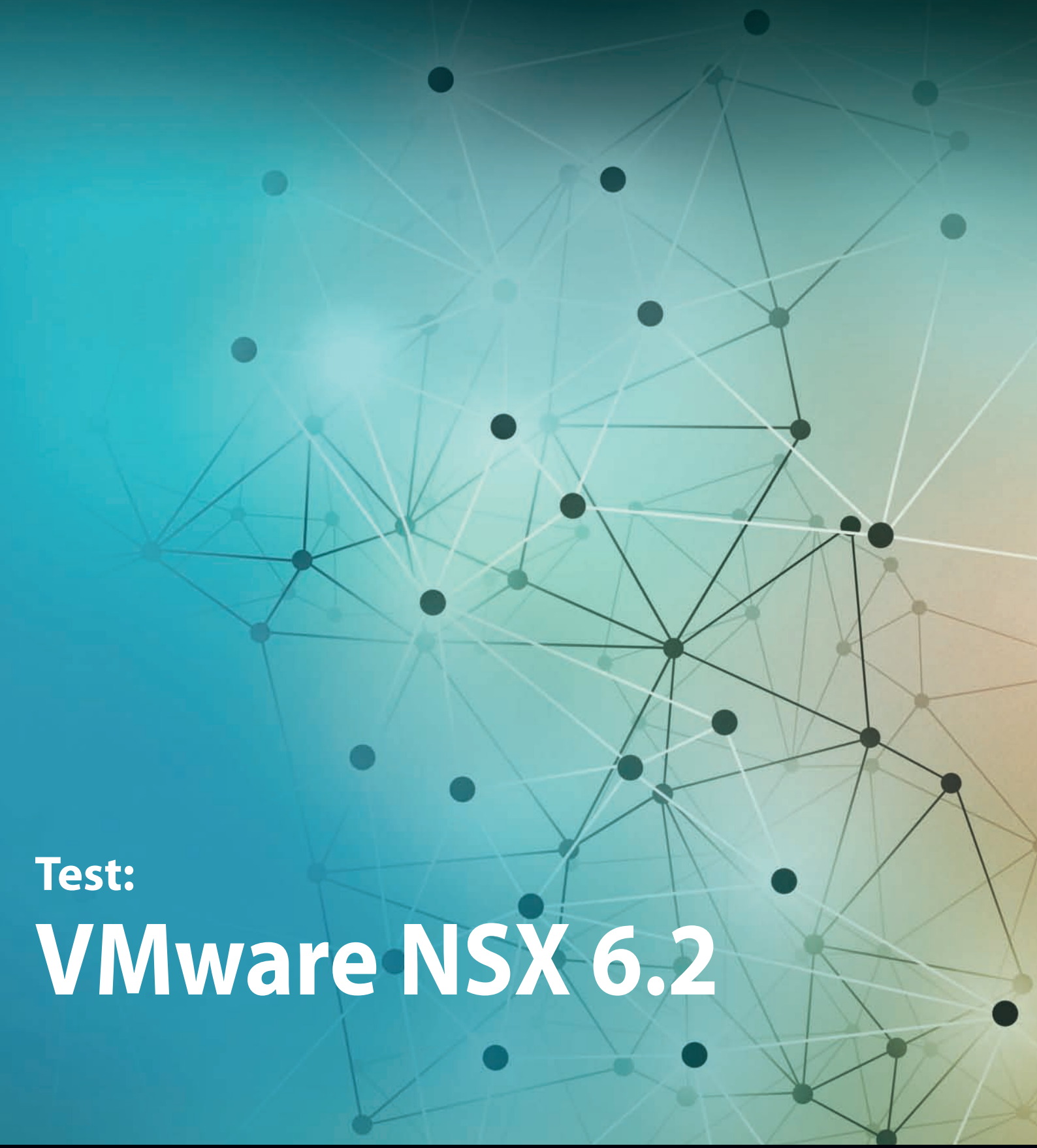
1 | 16 Sonderdruck

IT Administrator

Das Magazin für professionelle System- und Netzwerkadministration



Test:

VMware NSX 6.2

www.it-administrator.de


Quelle: grandeduc – 123RF

VMware NSX 6.2

Netzwerk-Revolutionär

von Jens Söldner

Mit VMware NSX wandeln Unternehmen ihr physisches Netzwerk zu einem virtuellen Pool von Transportkapazitäten, in dem sich Netzwerk- und Sicherheitsservices richtliniengesteuert einzelnen VMs zuweisen lassen – so die Marketingaussage von VMware. Konkret lässt sich mit der SDN-Plattform die Netzlandschaft im Rechenzentrum mittels Software und Regeln sehr schnell auf- und umbauen. Grund genug für IT-Administrator, VMwares NSX genauer unter die Lupe zu nehmen. Unser Test zeigt, dass NSX weit mehr ist als eine Overlay-Technik.

VMwares Virtualisierungsplattform hat in puncto Netzwerk schon seit jeher viel zu bieten. Bereits der einfachste virtuelle Switch, der Standard vSwitch, bietet vielfältige Layer 2-Funktionen mit Unterstützung für VLAN-Segmentierung (802.1Q Tagging), NIC-Teaming, Sicherheitsrichtlinien und Traffic Shaping für ausgehende Netzwerkpakete. Allerdings kann der Standard vSwitch nicht zentral verwaltet werden, was insbesondere in größeren Umgebungen zu hohem Aufwand führt.

Diesen Schwachpunkt adressiert VMwares zentral verwalteter Distributed Switch, der bereits mit vSphere 4.0 im Jahr 2009 eingeführt wurde und mit jedem Release bis einschließlich vSphere 6.0 diverse Erweiterungen erfahren hat. So bietet der Distributed Switch in der aktuellen Version alle Features eines High-End-Switches: IPFIX/NetFlow-Unterstützung, RSPAN- und ERSPAN-Protokolle zur Remote-Netzwerkanalyse, Markieren von Paketen mit Quality-of-Service Tags sowie fein granularer Steuerung von Bandbreiten (Network I/O Control Version 3) und eine API für eigene Erweiterungen und die Integration von neuen Services. Dennoch ist er nach wie vor nur ein Layer 2-Switch – ein Routing zwischen VLANs kann der Distributed Switch selbst nicht liefern.

Auch daran arbeitet VMware schon länger. Der erste Wurf in Sachen erweiterter Layer 3- bis 7-Funktionalität kam im Jahr 2010 mit vShield 4.1, das VMware 2013 in "vCloud Networking and Security" (vCNS) umbenannt hatte. Diese vielversprechende Erweiterung setzte sich jedoch nicht auf breiter Front durch – primär deswegen, weil VMware die Sichtbarkeit im Datacenter Networking-Umfeld fehlte. Um endgültig im Datacenter-Networking wahrgenommen zu werden und um die hauseigene vShield-Technologie moderner zu gestalten, kaufte VMware im Jahr 2012 das Software-defined Networking (SDN)-Startup Nicira auf, dessen Technologie mit "vCloud Networking and Security" im Produkt "NSX for vSphere" (NSX-v) zusammengeführt wurde und seit August 2015 in Version 6.2 zur Verfügung steht.

NSX bohrt vSphere-Netzwerkfeatures auf

Herkömmliche Netzwerkelemente wie ein klassischer Layer 3-Switch lassen sich funktional in drei Ebenen unterteilen. Mit der Management-Ebene (Management Plane) interagiert der Netzwerkadministrator typischerweise über Konsolenkabel, SSH oder bei neueren Geräten auch über eine API. Die Control-Plane dient der Abstimmung zwischen Netzwerkgeräten – Protokolle wie Spanning Tree Protocol (STP) oder Open Shortest Path First (OSPF) sind dieser Ebene zugeordnet. Die Data Plane ist für die Erbringung der eigentlichen Funktion des Netzwerkgerätes zuständig. In einem herkömmlichen Netzwerkgerät sind die drei Ebenen nicht zentral gesteuert, was Automatisierung schwierig macht, da kein zentraler Controller vorgesehen ist, der das Gesamtnetzwerk verwaltet.

Die drei Funktionsebenen existieren prinzipiell auch in NSX-V, sind aber mit entsprechender Intelligenz angereichert, um die Steuerung des Gesamtnetzwerks zu ermöglichen. Die Management-Ebene wird vom NSX-Manager erbracht, einer virtuellen Appliance, die mit dem vCenter-Server verbunden wird. Der NSX-Manager stellt eine öffentlich zugängliche REST-API zur Verfügung, die vom vCenter-Server, aber auch von Cloud-Management-Systemen wie VMware vRealize Automation, VMware Integrated Open-Stack oder vCloud Director konsumiert werden kann.

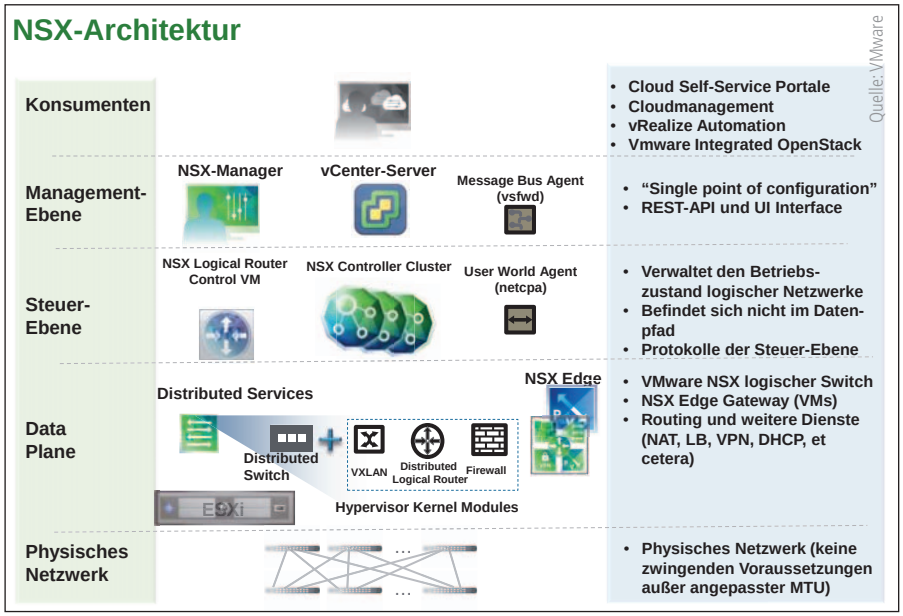


Bild 1: Mit NSX erweitert VMware seine schon zuvor mächtigen Netzwerkfeatures noch einmal deutlich.

Ein herkömmliches User Interface wird als Plug-in für VMwares Web-Client bereitgestellt und erlaubt so die Verwaltung der NSX-Umgebung. Nur wenige, spezielle Aktionen sind nicht in der GUI abgebildet, aber über die API verfügbar. Der NSX-Manager sollte in einem vSphere HA-Cluster betrieben werden. Steht er kurzzeitig nicht zur Verfügung, beispielsweise bedingt durch den Ausfall eines ESXi-Servers oder bei einem Update, läuft die NSX-Umgebung wie gewohnt weiter, lediglich Änderungen an den von NSX verwalteten Objekten wie logischen Switchen, Routern oder Firewall-Regeln sind währenddessen nicht möglich.

Für die Steuer-Ebene zeichnen sich primär die NSX-Controller verantwortlich, ein Software-Cluster aus drei virtuellen Maschinen, die sich um die zentrale Verwaltung der Netzwerktopologie, der logischen Netzwerke auf Basis des Overlay-Protokolls VXLAN und um die Koordination der logischen Router kümmern. Sind logische Router in der Umgebung vorhanden, so erhalten diese zusätzlich eine Kontroll-VM, die sich um den Austausch von Routen über dynamische Routingprotokolle wie OSPF und BGP kümmert und diese über die NSX Controller an den User World-Agenten übermittelt, der auf den ESXi Servern läuft. Die Komponenten der Steuer-Ebene befinden sich nicht im Datenpfad der logischen Switche und Router, sondern werden mit dem Management-Netzwerk verbunden, an dem auch das vCenter, der NSX Manager sowie die Management-seitigen VMkernel-Ports der ESXi-Server hängen. Die Kommunikation zwischen dem NSX-Manager und den NSX-Controllern erfolgt verschlüsselt über eine interne REST-API. Auch die Kommunikation zwischen allen anderen NSX-Komponenten läuft verschlüsselt ab.

Die Datenübertragungsebene stellen einzelne ESXi-Server bereit, indem ein Distributed Switch mit zusätzlichen Kernelmodulen für VXLAN, Routing und kernelbasierter Firewall erweitert wird. So entsteht ein optimierter Datenpfad für Verkehr innerhalb des Rechenzentrums, der idealerweise die logischen VXLAN-Netzwerke nicht verlässt. Für den Datenaustausch mit der Außenwelt jenseits des Rechenzentrums sind weder VXLAN-Netzwerke noch der kernelbasierte Router optimal, da früher oder später der Verkehr in physische Netzwerke auf VLAN-Basis eingespeist werden muss. Hierfür stellt VMware die schon von der Vorgängerversion vShield bekannten Edges bereit, die ideal den Übergang von der logisch-virtuellen VXLAN-Welt in die physische VLAN-Welt koordinieren können.

Zu guter Letzt wird natürlich auch noch ein physisches Netzwerk benötigt, ohne das auch NSX nicht auskommen kann. Hier kann der IT-Verantwortliche prinzipiell mit jedem Netzwerkausrüster zusammenarbeiten, besondere technische Abhängigkeiten bestehen nicht, außer dass die Maximum Transfer Unit (MTU) um 50 Bytes nach oben korrigiert werden muss, um den Overhead des VXLAN-Protokolls zu berücksichtigen. Selbstredend ist ein leistungsfähiges und stabiles physisches "Underlay"-Netzwerk eine wesentliche Basis der NSX Netzwerk-Virtualisierung.

Die Architektur von NSX wirkt stimmig. Gegenüber dem Vorgänger vCloud Networking and Security (vShield) hat VMware auf allen Ebenen kräftig nachgelegt. Komplett neu sind die NSX-Con-

VMware NSX 6.2

Produkt
Plattform zur Virtualisierung von Netzwerkfunktionen mit integrierten Sicherheitsfeatures.

Hersteller
VMware
www.vmware.com/de/

Preis
Eine Lizenz VMware NSX for vSphere kostet pro physischem Prozessor 4005 Euro. Als Add-on für Unternehmen, die bereits die vCloud Suite lizenziert haben, reduziert sich der Preis auf 3337 Euro pro Prozessor.

Systemvoraussetzungen
Basis für die Installation von NSX ist vSphere 5.5 und aufwärts. Da das Produkt vornehmlich in größeren Umgebungen mit einem dedizierten Management-Cluster zum Einsatz kommt, ist dessen Einsatz empfehlenswert, um die NSX-Komponenten von den ESXi-Servern zu separieren. Des Weiteren benötigt die Netzwerkvirtualisierung mittels Overlay-Protokoll VXLAN eine erhöhte Maximum Transfer Unit (MTU) von 1600 Bytes auf den physischen Switchen, über die die VXLAN-Overlay-Netzwerke transportiert werden. In größeren Umgebungen muss natürlich über ein passendes Netzwerkdesign der physischen Infrastruktur im Vorfeld nachgedacht werden (Stichwort: Spine-Leaf-Architektur). Da das VMotion-Netzwerk inzwischen seit vSphere 6.0 geroutet werden darf, müssen sich die ESXi-Server nicht mehr zwingend im gleichen Layer 2-Netzwerk befinden. Zu guter Letzt ist die Verwendung von Distributed Switchen zwingende Voraussetzung für den Betrieb von NSX.

Technische Daten
www.it-administrator.de/downloads/datenblätter

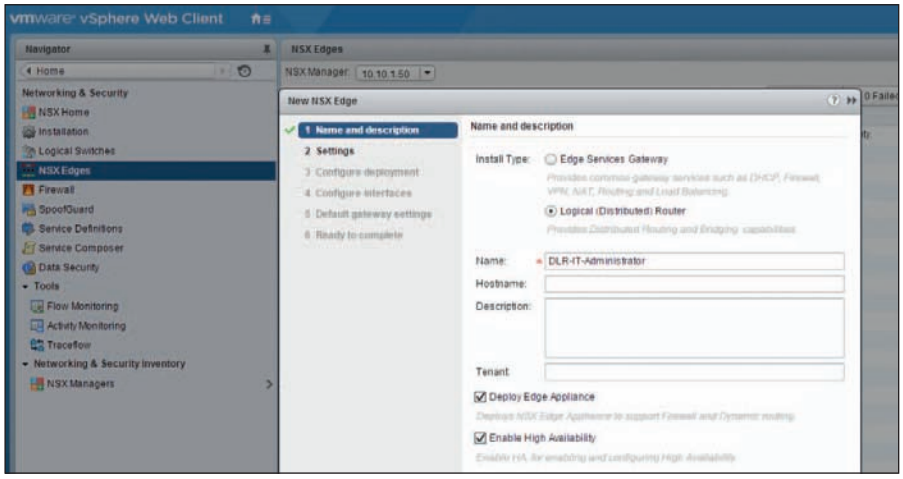


Bild 2: Das Erzeugen eines verteilten logischen Routers ist über das Web-Interface in wenigen Schritten vorgenommen.

troller, das Routing und die Bereitstellung von Firewall-Funktionen im Kernel. Das bereits in der Vorgängerversion vorhandene Overlay-Protokoll VXLAN kann NSX dank der Intelligenz der Controller nun deutlich effizienter handhaben und zudem die lästige Voraussetzung von Multicast, die vCNS noch kannte, abschaffen.

Rebootfreie Installation

Die Installation der NSX-Komponenten selbst gestaltet sich sehr einfach. Zunächst muss der NSX-Manager installiert werden, eine virtuelle Appliance, die VMware im OVA-Format ausliefert. Sie beinhaltet sämtliche Komponenten (Kernel-Treiber und weitere Appliances) für den Betrieb von NSX. Die Installation gelingt über den herkömmlichen Assistenten zur Installation von OVF/OVA-Komponenten problemlos, lediglich Netzwerkinformationen und das Passwort für den Admin User müssen angegeben werden. Die NSX-Appliance beansprucht für sich vier vCPUs und 16 GByte RAM. Zu Troubleshooting-Zwecken ist ein Login auf dem NSX-Manager direkt über die VMware Remote Console oder über SSH möglich.

Der nächste Schritt ist die Konfiguration der Appliance. Sie benötigt Zeitsynchronisation über NTP und eine Verbindung mit dem vCenter-Server. Nach dem Herstellen der Verbindung zwischen dem NSX-Manager und dem vCenter installiert NSX ein Plug-in in "VMwares Web Client", über den die weitere Konfiguration und Administration stattfindet. Optional kann über das Verwaltungsinterface des NSX-Managers noch eine Sicherung und gegebenenfalls Wiederherstellung der NSX-Datenbank über einen FTP Server konfiguriert werden.

Nachdem der NSX-Manager im Management-Cluster aufgesetzt wurde und mit dem vCenter verbunden ist, erfolgen die nächsten Schritte im Web-Client. Prinzipiell könnten alle administrativen Aktionen auch über die REST-Schnittstelle des NSX-Managers stattfinden: Dies erlaubt eine weitgehende Automatisierung, zum Beispiel durch VMwares vRealize Orchestrator. Prinzipiell ist es sogar so, dass nicht alle Konfigurationsmöglichkeiten über den Web-Client angeboten werden. So sind etwa das Wechseln des UDP-Ports für das VXLAN-Protokoll oder andere spezielle Aktionen sogar nur über die REST-Schnittstelle der API durchführbar.

Nächster Installationsschritt ist nun die Bereitstellung des NSX-Controller-Clusters, eine Technologie, die der NSX-Vorgänger vShield beziehungsweise vCNS noch nicht aufwies. Die NSX-Controller stellen das "Gehirn" der NSX-Umgebung dar, sie koordinieren NSX-weit die Konfiguration der logischen (VXLAN)-Netzwerke und der logischen (kernelbasierten) Router. Für die verteilte Firewall (DFW) jedoch spielen sie keine Rolle, diese wird direkt zwischen dem NSX-Manager und den ESXi-Servern gesteuert.

Die Installation der NSX-Controller erfolgt entweder menugeführt im Web-Client oder über API-Aufrufe in der REST-Schnittstelle des NSX-Managers. Wie bereits beim NSX-Manager handelt es sich auch bei den NSX-Controllern um virtuelle Appliances, die einen Ressourcenbedarf von vier vCPUs und 4 GByte RAM pro Controller aufweisen. Bei der Installation muss der Administrator den Ausführungs- und Speicherort der NSX-Controller angeben (also Management-Cluster und Datastore) sowie das Management-Netzwerk, mit dem die NSX-Controller verbunden werden. Über dieses Netz müssen sie das vCenter, den NSX-Manager und die ESXi-Server erreichen. Darüber hinaus ist die Angabe eines IP-Pools notwendig. Dies ist ein Objekt, das im NSX-Manager gespeichert wird und die IP-Konfiguration für die NSX-Controller vorhält.

Dann hinterlegt der IT-Verantwortliche noch beim ersten NSX-Controller ein Passwort für den dort verwendeten eigenständigen Admin-User (also nicht der gleiche Account wie beim NSX-Manager). Dieses Passwort kommt dann für die weiteren zwei NSX-Controller ebenfalls zum Einsatz. Dieser Prozess wird noch zweimal wiederholt, bis alle drei Controller installiert sind, laufen, und ihr Status im Web-Client auf "Normal" steht.

Als Nächstes werden die ESXi-Server vorbereitet, die die NSX-Funktionen "logisches Switching" (Bereitstellung von Overlay-Netzwerken auf VXLAN-Basis), "logisches/verteiltes Routing" (Routerfunktionalitäten im Kernel der ESXi Server) und "verteilte Firewall" (Firewallabarbeitung im ESXi-Kernel) nutzen sollen. Hierfür benötigen die ESXi-Server Kernelmodule (VIBs), was auch der NSX-Manager vornimmt. Die Installation der Kernelmodule erfolgt clusterweise, nicht pro ESXi-Server.

Zudem benötigen die ESXi-Server für die VXLAN-Overlay-Funktionalität einen dedizierten VMkernel-Port ("VTEP", VXLAN oder "Virtual Tunnel End Point"), der mit dem VXLAN-Transport-Netzwerk, einem dedizierten VLAN, das die höhere MTU von 1600 erlaubt, verbunden wird. Die VTEPs bedürfen einer IP-Konfiguration, die wiederum über im NSX-Manager gespeicherte IP-Pools oder alternativ DHCP erfolgt.

Der letzte Schritt ist das Anlegen der VXLAN-Transport-Zone, die den Umfang der VXLAN-Ausdehnung innerhalb der vSphere-Installation definiert. Sie benötigt einen Replikationsmodus (Multicast, Unicast oder Hybrid), der die Funktionsweise des VXLAN-Protokolls wesentlich beeinflusst und auch einen Einfluss auf die Skalierbarkeit der Umgebung hat. So erlebt der IT-Verantwortliche insgesamt eine einfache und zügige Installation, die ohne Reboot der ESXi-Server auskommt.

Überzeugendes Layer 2-Switching in VXLANs

Steht die NSX-Installation inklusive der VXLAN-Transportzone, ist es an der Zeit, entweder manuell über den Web-Client oder über die REST-API des NSX-Managers logische VXLAN-Netzwerke anzulegen. Die Bezeichnung "logische Netzwerke" resultiert aus der Tatsache, dass sie keine weitere Konfiguration im physischen Underlay mehr benötigen, wenn dieses einmal korrekt aufgesetzt wurde. Insbesondere können logische Netzwerke jederzeit angelegt, verwendet und gelöscht werden, ohne dass herkömmliche VLANs in physischen Netzwerken mehr angelegt werden müssen. Denn alle logischen Netzwerke werden in einem einzigen physischen Netzwerk über VXLAN gekapselt übertragen, was ein absolutes Muss für die Mandanten-Fähigkeit in der Cloud.

Erstellt der Administrator ein logisches Netzwerk via API oder manuell, so wird auf allen Distributed Switchen, die zur VXLAN-Transport-Zone gehören, eine entsprechende Portgroup für das VXLAN-Netzwerk angelegt. Der VM-Datenverkehr an dieser Portgruppe muss über den VXLAN Tunnel End Point (VMkernel-Port) übertragen werden, wenn die Maschinen auf unterschiedlichen ESXi-Servern laufeb. Befinden Sie sich im gleichen VXLAN und im gleichen ESXi-Server, erfolgt die Kommunikation direkt im Hauptspeicher des ESXi-Servers, ohne dass eine zusätzliche Tunnelung notwendig ist. Wichtig dabei ist, dass Quell- und Zielhost sich selbst nicht zwingend im gleichen physischen Layer 2-Netzwerk befinden müssen, da VXLAN in UDP und IP eingepackt wird und somit routbar ist, was das Netzwerkdesign flexibilisiert und insgesamt deutlich größere Installationen ermöglicht. Das Erzeugen von logischen Netzwerken erfolgt selbst sekundenschnell. Beim Anlegen des logischen Layer 2-Netzwerks hat der Administrator erneut die Möglichkeit, den Replikationsmodus (Multicast/Unicast/Hybrid) der Transport Zone zu übernehmen oder einen davon abweichenden für diesen logischen Switch festzulegen. Alles in allem zeigt sich das Layer 2-Switching als absolut überzeugend und sehr einfach zu verwenden.

Zwei Arten für Layer 3-Routing, IPv6 ausgenommen

Etwas komplexer wird es beim Bereitstellen der Routing-Funktionalität, denn hier lässt VMware dem Administrator die Wahl zwischen zwei unterschiedlichen Architekturen. Der kernelbasierte Router "DLR" (Distributed Logical Router) ist ideal, wenn nur zwischen logischen VXLAN-Netzwerken geroutet werden muss. Die Eckdaten können sich durchaus sehen lassen: Da ein DLR nicht als virtuelle Maschine betrieben wird, gelten deren Limitierungen nicht für ihn. So kann er mit logischen Interfaces (LIF) bis zu 999 Netzwerke – idealerweise logische VXLAN-Netze – miteinander verbinden.

Die manuelle Bereitstellung von DLRs ist nicht schwer und wird über einen Assistenten vorgenommen. Nach dem Erzeugen lässt sich der DLR jederzeit über den Web-Client oder die API weiter anpassen. Weniger gut geeignet ist der DLR, wenn er VLANs routen soll, was beim Weg aus dem Rechenzentrum heraus aber früher oder später passieren muss. Hierfür stellt VMware die vom Vorgänger bekannten Edge-VMs bereit, die in NSX weiter hinsichtlich Funktionen und Leistung verbessert wurden. Die Edge ist eine herkömmliche virtuelle Maschine und somit auf ein Maximum von zehn virtuellen Netzwerkkarten begrenzt. Zudem läuft sie in einem ESXi-Server im User Space und nicht im Kernel, was ihren maximalen Durchsatz bremst. Will der IT-Verantwortliche den Datenpfad zwischen dem Rechenzentrum und der Außenwelt optimieren, so ist es möglich, bis zu acht Edges über ECMP (Equal Cost Multipathing) zusammenzubinden. Auch das Layer 3-Routing zeigte sich als einfach in Betrieb zu nehmen. Wir vermissten allerdings die Unterstützung von OSPFv3 und somit von IPv6-Routing.

Revolutionäre Security and Firewalling

Eine große Stärke und einer der Haupttreiber der NSX-Adaption durch Unternehmen ist die neu eingeführte kernelintegrierte "Distributed Firewall". Diese setzt am Übergang der virtuellen Maschine zum virtuellen Switch an, also an der vNIC, und somit außerhalb des Betriebssystems der VM. Die Firewall-Regeln werden zentral im NSX-Manager über die GUI oder die REST-API verwaltet und vom NSX-Manager ohne Umweg über die NSX-Controller an die ESXi-Server weitergegeben, die sie im Kernel durchsetzen.

Die Distributed Firewall agiert auf Ebene zwei bis vier des OSI-Stacks und kann Regeln nicht nur anhand von MAC-Adressen, IP-Adressen, TCP- und UDP-Portnummern umsetzen, sondern auch VMware-Objekte wie virtuelle Maschinen, logische Switche, Cluster oder Ähnliches in die Regelumsetzung einbeziehen. Wird eine VM zum Beispiel durch VMotion verschoben oder aufgrund von HA neu gestartet, folgt die Regelumsetzung natürlich der VM auf den neuen ESXi-Server. Zudem kann der Administrator auch fortgeschrittene Security Groups definieren und diese über Security Policies absichern, die neben Firewall-Regeln auch Third-Party Services zum Virenschutz, Vulnerability Scanning

VPN, LB und NAT mit Edges

Die Edges sind nicht nur auf Routingfunktionen beschränkt, dank ihres VM-Betriebsmodells eignen sie sich auch gut für die Bereitstellung weiterer Netzwerkfunktionalitäten. So bieten die Edges neben Routing auch NAT (Source und Destination NAT), eine Firewall, Loadbalancer-Funktionen (technologische Grundlage hierfür ist das Open Source-Projekt "HAProxy") sowie drei VPN-Spielarten: Site-to-Site VPN auf IPsec Basis, SSL VPN für Remote-Benutzer auf Basis der 2011 durch VMware übernommenen Technologie von NeoAccel und ein L2-VPN, über das sich auch Rechenzentren miteinander verbinden lassen. Alles in allem stehen dem Administrator hier sehr nützliche Zusatzfeatures zur Verfügung.

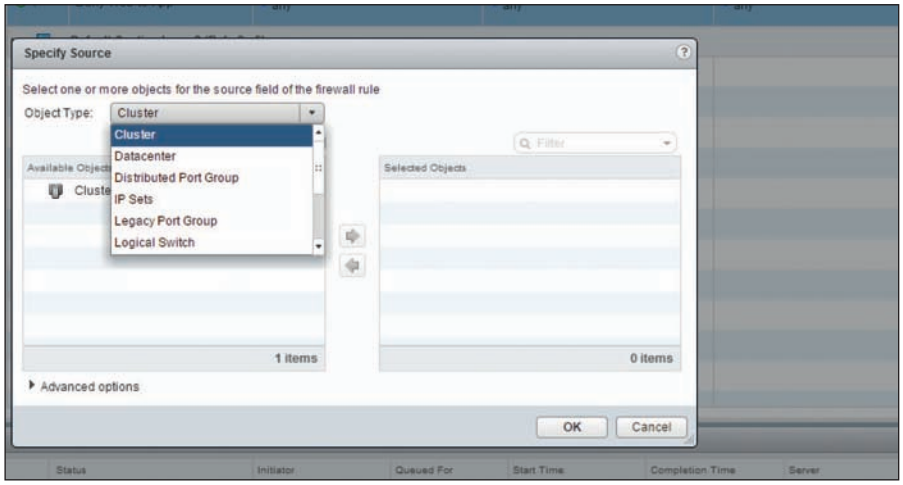


Bild 3: Die Distributed Firewall kann neben IP-Adressen und TCP-/UDP-Ports auch eine Vielzahl von VMware-Objekten wie Cluster, Datacenter oder VXLAN Switches in Regeln berücksichtigen.

oder eine Next-Generation Firewall wie Palo Alto mit einbinden können. Auch Cloud-Managementsysteme wie VMware Integrated OpenStack docken direkt an das Security Group-Feature an. Performanceseitig gibt VMware den Durchsatz der Distributed Firewall mit 20 GBit/s pro Hostsystem an, ein Wert, der sich durchaus sehen lassen kann. Die Distributed Firewall sucht momentan seinesgleichen. Reichen die Funktionen der Distributed Firewall nicht aus, lassen sich über Thrid-Party-Integration weitreichende Funktionen nachlegen.

Bereitstellungszeiten von Anwendungen verkürzen

Wesentlicher Nutzenaspekt von NSX ist die programmatische Konsumierbarkeit seiner Funktionen über die vom NSX-Manager bereitgestellte REST-API. Dies macht sich unter anderem VMwares Cloud-Plattform "vRealize Automation" zunutze – im Zusammenspiel ist es möglich, nicht nur Gruppen von VMs automatisiert zu deployen, sondern auch die von den VMs benötigten Netzwerkkomponenten wie logische Netzwerke, Router oder Loadbalancer sowie Sicherheitsfunktionen automatisch mitbereitzustellen.

Dies reduziert die Bereitstellungszeit komplexer Applikationen dramatisch, da nun nicht mehr auf zugelieferte Tätigkeiten des Netzwerkteams gewartet werden muss. Auch VMwares OpenStack-Distribution VIO ist dank des Neutron Projekts eng auf das Zusammenspiel mit NSX abgestimmt.

Großes Partnernetzwerk

Reichen die im NSX enthaltenen Funktionen nicht aus, steht eine breite Partnerlandschaft von etwa 30 bekannten Netzwerk- und Securityherstellern bereit, um fortgeschrittene Next-Generation Firewall-Funktionen, Virenschutz, erweitertes Loadbalancing oder Hardware-VTEP-Integration nachzulegen.

Lediglich Netzwerk-Branchenprimus Cisco hat sich nicht als Partner von NSX aufgestellt, da dessen Plattform "Application Centric Infrastructure" (ACI) als Gegenmodell zu NSX positioniert wird und die Beziehung zwischen beiden Herstellern seit der Ankündigung von NSX merklich abgekühlt ist. Dennoch stellt VMware Whitepaper und Handreichungen bereit, um NSX in einer Cisco-lastigen Umgebung mit UCS und Nexus-Switchen optimal bereitzustellen.

Fazit

VMware ist mit NSX for vSphere ein beeindruckender Wurf in Sachen SDN gelungen. Das Produkt deckt die wesentlichen Layer 2 bis 7-Features ab, für Spezialanforderungen stehen Partnerprodukte bereit. Die Integration in die VMware-Produktsuite ist als nahtlos zu bezeichnen und NSX mit etwas Know-how einfach zu bedienen – eine ausführliche Schulung vorausgesetzt, da das Produkt am Anfang doch sehr komplex wirkt. Vor allem das passende Design der zugrundeliegenden Netzwerkinfrastruktur erfordert Spezialwissen. Eine Schwachstelle von NSX ist die rudimentäre Unterstützung von IPv6. Zwar können die Firewall und das Produkt selbst mit IPv6 umgehen, aber die NSX-Implementierung der dynamischen Routingprotokolle OSPF und BGP selbst noch nicht. Für ein vernünftiges Monitoring der Plattform, das über die Verwendung eines Syslog-Servers hinausgeht, werden VMware-Zusatzprodukte wie vRealize Operations und Log Insight benötigt.

Positiv hervorzuheben ist das einfache Management über eine klar zu bedienende GUI. In Version 6.2 hat VMware zudem noch nachgelegt und weitere Trouble-shooting-Tools wie eine zentrale CLI, Unterstützung für Traceflow und vor allem den Support großer Umgebungen mit mehreren vCenter nachgelegt, indem logische Switche, Router und die Firewall nun "universell" über vCenter-Grenzen verwendbar sind. *(jp)* IT

So urteilt IT-Administrator

SDN-Architektur	10
Distributed Firewall	10
Routing und Switching	8
NAT/VPN/Loadbalancer	7
Inbetriebnahme	9

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für Unternehmen, die eine private Cloud auf Basis von vRealize Automation oder VMware Integrated OpenStack aufbauen möchten. Das gilt auch für Unternehmen, die ihre virtuellen Netzwerke automatisiert bereitstellen und verwalten möchten oder Bedarf an den neuartigen Sicherheitsfunktionen der Distributed Firewall haben.

bedingt für klassische kleinere VMware-Infrastrukturen, bei denen eine weitgehende Automatisierung des Netzwerks nicht im Vordergrund steht, aber die Sicherheitsfunktionen der Distributed Firewall und die Partnerintegration gut zum Einsatz kommen können.

nicht für Unternehmen, die eine heterogene Hypervisor-Infrastruktur betreiben.