Von der virtuellen Maschine zum virtuellen Rechenzentrum

Der Virtual-Reality-Hype ist derzeit in aller Munde. Doch es gibt auch noch eine andere virtuelle Realität: virtuelle Maschinen, virtuelle Netzwerke und sogar virtuelle Rechenzentren. Alle mit ihren eigenen Grenzen und Spezialitäten.

DER AUTOR

Marc Chauvin
CTO, Cyberlink

Wollte man früher eine Applikation in der Cloud laufen lassen, standen einzelne virtuelle Maschinen (VM) bei Hosting-Providern zur Verfügung. Diese VM waren mit einer öffentlichen IP-Adresse direkt an das Internet angeschlossen.

Danach kamen erste Angebote für ganze virtuelle Rechenzentren (VDC). Es ist vergleichbar mit einem physischen Datacenter, worin beliebig viele VM hochgefahren werden können. Zusätzlich können virtuelle Netzwerke (SDN) abgebildet werden.

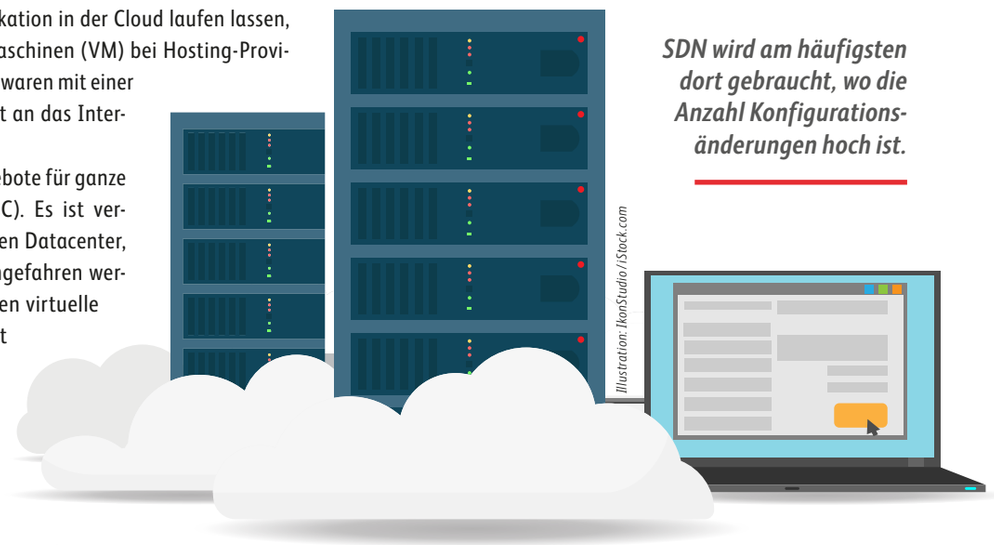

Illustration: IkonStudio / iStock.com

SDN wird am häufigsten dort gebraucht, wo die Anzahl Konfigurationsänderungen hoch ist.

Software-defined Networking (SDN)

SDN-Plattformen erlauben die programmatische Konfiguration von Netzwerkdiensten. Software kümmert sich um die (De)Provisionierung von Netzwerkkomponenten. Somit werden unter anderem Cloud-Umgebungen, Netzwerkfabriken, Cores und Router zentral und automatisch konfiguriert. Die Inbetriebnahme neuer Dienste verläuft schnell und fehlerfrei.

SDN-Lösungen verfolgen das Ziel, neben der Automatisierung auch die Vielfalt der darunterliegenden Technologien herstellerunabhängig zu reduzieren. Jede SDN-Lösung hat jedoch Grenzen und Spezialitäten, daher ist die Auswahl der richtigen SDN-Plattform sehr anspruchsvoll.

Virtuelle Netzwerkfunktionen (NFV)

Die virtuellen Netzwerkfunktionen sind mit denen der physischen Welt identisch: Firewalls, NAT-Gateways, DHCP-Server, VPN-Gateways, Router, Loadbalancer und viele mehr. Mit der Virtualisierung dieser Funktionen ist gemeint, diese softwarebasiert, vollständig zentralisiert und automatisch konfigurierbar zu betreiben. Einige SDN-Hersteller bieten die entsprechenden Tools für NFV.

Virtuelle Netzwerkfunktionen werden oft in Zusammenhang mit virtualisierten Serverumgebungen gebracht, sind jedoch nicht nur dort vorhanden. Auch die physische Core-Infrastruktur wird immer häufiger damit ausgestattet. Sogar der Router beim Kunden (CPE) bietet vermehrt solch zentral verwaltete Funktionen, vCPE (virtual Customer Premise Equipment), an. Neben Firewall, DHCP, VPN und NAT gehören auch Traffic-Management und QoS zu den virtuellen Netzwerkfunktionen.

SDN und NFV in der Cloud

SDN wird am häufigsten dort gebraucht, wo die Anzahl Konfigurationsänderungen hoch ist und die Provisionierung durch systemfremde Entitäten (Kunden, Apps, API) gesteuert werden muss. Eine Cloud-Plattform ist somit prädestiniert für SDN. Auch in Multi-Cloud-Umgebungen können gewisse Funktionen zentral konfiguriert werden. Es ist heutzutage üblich, ein virtuelles LAN zwischen der eigenen virtualisierten Umgebung und Microsoft Azure oder auch Amazon (AWS) zu teilen und zentral zu konfigurieren. Dazu kommen virtuelle Router des jeweiligen SDN-Herstellers zum Einsatz.

Need for Speed

In einer virtualisierten Umgebung spielen SDN und NFV noch eine weitere wichtige Rolle: Eine drastisch hohe Leistung im Routing- und Firewalling-Bereich wird gefordert. Typischerweise bleiben in einer virtualisierten Umgebung zirka 70 Prozent des gesamten Netzwerkverkehrs lokal. Es handelt sich um den sogenannten Ost-West-Verkehr zwischen den Servern respektive den VM. Als Nord-Süd-Verkehr bezeichnet man den Datentausch zwischen der eigenen Umgebung und fremden Netzwerken wie etwa dem Internet.

« Viele Managementfunktionen sind plötzlich verwundbar »

Wieso Netzwerke selbst konfigurieren, wenn das auch eine Software erledigen kann? Marc Chauvin, CTO von Cyberlink, sagt im Interview, warum das Unternehmen auf Software-defined Networking (SDN) setzt und welche Vorteile virtuelle Netzwerkfunktionen bieten. Interview: Joël Orizet

Warum beschäftigt sich Cyberlink mit softwaredefinierten Netzwerklösungen?
Marc Chauvin: Wir sehen gleich mehrere Vorteile in dieser Erfolg versprechenden Technologie. Hochgradige Automatisierung erleichtert das Provisionieren von Netzwerkdiensten und erlaubt gleichzeitig die direkte Anbindung an den Billing-Prozess. Netzwerkdienste werden dadurch zeitnah, fehlerfrei und konsistent aufgeschaltet. SDN ermöglicht es dem Kunden in einem Selfservice-Portal seine Services ohne den Eingriff eines Cyberlink-Mitarbeiters zu verwalten und je nach Bedarf zu verändern. Zusätzlich können wir mithilfe von SDN auch unseren Lieferanten besser in die Geschäftsprozesse einbinden. Änderungen oder Schutzmechanismen – wie etwa im Fall einer DDoS-Attacke – werden auch im Netz der Lieferanten automatisiert und ohne Verzögerung umgesetzt. Um am Markt erfolgreich zu sein, müssen wir uns stetig neu erfinden. Neue Technologien wie SDN sind dabei ein wichtiger Grundstein für unsere Innovationskraft.

Wo setzt Cyberlink solche Lösungen konkret ein?
Als Erstes haben wir unsere Cloud-Plattform – Virtual Datacenter – komplett mit SDN ausgestattet und mit NFV erweitert. Nun arbeiten wir daran, unsere Core-Infrastruktur – Router und Switches – beim Kunden zu virtualisieren und mit SDN zu kontrollieren, was uns letztlich erlaubt, Netzwerkdienste wie SD-WAN, MPLS, VPN und weitere einheitlich und automatisch auszurollen.

Welche Vorteile verspricht sich Cyberlink von einem softwaredefinierten Netzwerk?
Ein SDN ermöglicht es uns, schneller auf die Bedürfnisse unserer Kunden einzugehen und agile Netzwerkdienste anzubieten. Dadurch erreichen wir mehr Flexibilität, bessere Qualität unserer Services und können zusätzlich die operativen Kosten durch Automatisierung signifikant reduzieren.

Was sind die Fallstricke bei der Bereitstellung von virtuellen Netzwerkfunktionen?
Es gibt viele SDN-Plattformen auf dem Markt. Die geeignete Plattform zu finden ist nicht ganz einfach. Man muss die Vor- und Nachteile von Vendor-locked und offener Open-Source-Software abwägen. Zudem muss die Kompatibilität zu den derzeitigen und zukünftigen Hardwarekomponenten im Netz sichergestellt werden. Nicht zu unterschätzen ist auch der erhöhte Bedarf an Infrastruktursicherheit. Viele Managementfunktionen, die früher von aussen unerreichbar waren, sind heute durch Portale und APIs plötzlich öffentlich zugänglich und stellen eine neue Angriffsfläche dar.

Wie können IT-Dienstleister solche Fallstricke vermeiden?
Man sollte sich über die Technologie sehr gut informieren und bei Bedarf externe Ressourcen beiziehen. Eine umfangreiche Evaluation der verschiedenen SDN-Softwarehersteller ist auf jeden Fall wichtig. Wer eine geplante Roadmap und ein definiertes Lifecycle-Management der eingesetzten Infrastruktur und Dienstleistungen hat, ist im Vorteil. SDN soll Stück für Stück und vorsichtig eingeführt werden. Fehlt die notwendige Fachkompetenz in den eigenen Reihen, bietet sich die Möglichkeit, Netzwerkservices von Dienstleistern wie Cyberlink zu beziehen und sich selbst auf seine Kernkompetenzen zu fokussieren.

« Man sollte sich über die Technologie gut informieren und bei Bedarf externe Ressourcen beiziehen. »

Marc Chauvin, CTO, Cyberlink