LANCOM Whitepaper

Cloud Management & Software-defined Networking

Traditionelle, statische Netzwerkarchitekturen sind nicht mehr in der Lage, den stetig wachsenden Anforderungen moderner Unternehmensinfrastrukturen Stand zu halten: Neben einem explosionsartigen Anstieg der Anzahl an Endgeräten und Netzwerkanwendungen sowie vielen verteilten Standorten sind IT-Administratoren zugleich mit zunehmenden Ansprüchen der Anwender mit Bezug auf Sicherheit und Geschwindigkeit konfrontiert. Die notwendige manuelle Konfiguration einzelner Netzwerkkomponenten erzeugt große Arbeitsaufwände und daraus folgend Ressourcenengpässe. Die Lösung für dieses Dilemma liegt in der Auslagerung dieser Komplexität in ein intelligentes Cloud-basiertes Managementsystem auf der Grundlage von Software-defined Networking. Dieses Whitepaper zeigt auf, wie die Administration von Unternehmensnetzwerken mit Hilfe von Cloud-Management und Software-defined Networking dramatisch vereinfacht wird.

Einschränkungen aktueller Netzwerkarchitekturen

Ein typisches Unternehmensnetzwerk muss eine Vielzahl an Anforderungen erfüllen: Zum einen stellen verschiedene Server den Benutzern die Daten für die tägliche Arbeit zur Verfügung. Zum anderen wird darüber intern und auch extern kommuniziert, sowohl kabelgebunden als auch kabellos über WLAN – und das an verteilten Standorten mit unterschiedlichen Anwendungsanforderungen. Zusätzlich wird für Gäste und Mitarbeiter ein WLAN-Hotspot angeboten, aber sicher getrennt vom internen Produktivnetz. Sicherheit, sowohl vor Ausfällen als auch Angriffen, muss dabei auch jederzeit gewährleistet sein.

Um all diese Anforderungen zu erfüllen, müssen die Konfigurationen aller eingesetzten Netzwerkkomponenten perfekt aufeinander abgestimmt sein – Router, Switches, Access Points und Firewalls mit abgestimmten Kommunikationsprotokollen, VLANs, QoS-Einstellungen, Firewallregeln, Authentifizierungsmethoden und vielem mehr. Die traditionelle Einzelgerätekonfiguration macht die Bereitstellung eines einfach funktionierenden Netzwerks selbst für erfahrene, zertifizierte Netzwerkadministratoren zu einer komplexen Aufgabe: Aufwand und Fehleranfälligkeit steigen exponentiell zur Geräteanzahl, was bei Konfigurationsfehlern ein langwieriges Troubleshooting zur Folge hat. Darüber hinaus verlangen bestimmte Applikationen vor Ort mehr Bandbreite und optimierteres QoS. Diese Anforderungen lassen sich nur automatisiert unter Berücksichtigung der jeweiligen Applikation bedienen.

Ganzheitliche Netzwerk-Orchestrierung

Netzwerke werden aufgrund der bestehenden und zukünftigen Anforderungen immer komplex bleiben. Um diese Komplexität beherrschbar zu machen, müssen die bisherigen Konfigurations- und Administrationswege überdacht werden. Software-defined Networking ersetzt

LANCOM Systems

die bisher manuelle Einzelgerätekonfigurationen durch eine automatisierte Netzwerk-Orchestrierung. Der Administrator gibt über eine einfache, zentrale Oberfläche nur noch die Rahmenbedingungen für das gesamte Netzwerk-Design vor. Die Konfiguration und der Rollout von Konfigurationsänderungen übernimmt ein zentrales Managementsystem – vollautomatisch und auf alle Netzwerkkomponenten (Router, Gateways, Switches und Access Points) abgestimmt. Dadurch werden die Fähigkeiten der eingesetzten Netzwerkkomponenten optimal ausgenutzt, insbesondere im Bereich Virtualisierung. Hinzu kommt die strikte Trennung von Management- (Control Plane) und Datenverbindungen (Data Plane): Während die Datenverbindungen (z. B. VPN-Tunnel) direkt zwischen den VPN-Gateways aufgebaut werden, wird jede einzelne Netzwerkkomponente direkt über eine unabhängige Managementverbindung mit dem Cloud-basierten Management verbunden. Das bedeutet: Nutzdaten bleiben für das Managementsystem verborgen und das Management und Monitoring der Netzwerkkomponenten erfolgt (fast vollkommen) unabhängig vom Zustand der Datenverbindungen. Das Ganze erfolgt zudem vollautomatisch und ohne gesonderte vorherige Konfiguration der Geräte (Zero-touch / Autokonfiguration), durch einen gesicherten Verbindungsaufbau vom Gerät zum Managementsystem.

Cloud-basiertes Management

Die Verlagerung der Control Plane, also des Netzwerkmanagements, in eine zentrale Cloud bietet den Vorteil eines permanenten, standortunabhängigen Out-of-band-Managements und einer zentralen, Web-basierten Adminstrationsoberfläche für alle Geräte, alle Standorte und alle Anwendungen. Hierbei ist zu beachten, dass es verschiedene Konzepte zum Hosting einer Cloud-basierten Lösung gibt. Allen gemein ist, dass die Inhalte nur für den Administrator zugänglich sind, aber der Standort und der Zugriff auf die Server unterschiedlich gehandhabt werden. Folgende Varianten werden unterschieden:

- Public Cloud
  Das Cloud-basierte Managementsystem wird vom Anbieter gehostet. Dieses Managementsystem steht dabei allen Kunden gleichermaßen zur Verfügung, es erfolgt keine Trennung nach Fachhändler oder Endkunden. Selbstverständlich sorgt die Public Cloud dafür, dass Kunden und Fachhändler jeweils nur „ihren" Netzwerkbereich sehen und verwalten können. Der große Vorteil dieser Lösung ist: Es entfallen alle Einrichtungskosten und -aufwände. Mit dem Erwerb der jeweiligen Netzwerkprodukte und Cloud-Lizenzen kann sofort die Installation und Einrichtung des Netzwerks beginnen. Wichtig: Generell ist zu empfehlen, bei der Auswahl eines Cloud-Hosting-Dienstleisters auf die Vertrauenswürdigkeit des Dienstleisters selbst sowie auf den Standort des Rechenzentrums zu achten. Das Hosting der Public Cloud in der EU garantiert hohe Datensicherheit und rechtssicheres Handling.
- Private Cloud
  Das Cloud-basierte Managementsystem wird im Rechenzentrum eines Systemhauses betrieben. Das Systemhaus verwaltet mit diesem System dann die Netzwerkinfrastruktur seiner Kunden. Der große Vorteil dieser Lösung: Erhebliche Skalierungsverbesserung, da ein Managementsystem für alle Kunden eines Systemhauses genutzt werden kann. Es bietet zudem eine entsprechende Privatsphäre, da die Konfigurationsdaten des Netzwerks im den Kunden bekannten Rechenzentrum des Systemhauses verbleiben und die Verantwortung hierüber beim Systemhaus liegt.
- Self-hosted Cloud
  Das Cloud-basierte Managementsystem wird direkt im Rechenzentrum des Endkunden selbst installiert und betrieben. Diese Variante bedeutet einerseits die höchstmögliche Privatsphäre (Konfigurationsdaten verlassen den Netzwerkbereich des Kunden nicht), andererseits aber doch deutlichen Aufwand, da hier ein Managementsystem für genau einen Kunden installiert und betrieben werden muss.

Software-defined Networking

Die Orchestrierung des vollständigen Netzwerks umfasst die Bereiche WAN, LAN, WLAN und SECURITY sowie alle zugehörigen Netzwerkfunktionen (Abb. 1). Aus diesem Grund haben sich die Begriffe SD-WAN, SD-LAN, SD-WLAN und SD-SECURITY etabliert. Grundprinzip für Software-defined Networking (SDN) ist dabei die Abkehr vom gerätezentrischen, hin zu einem netzwerkzentrischen Ansatz. Damit werden nur noch Netzwerke und Verkehrsbeziehungen definiert. Die konkrete Umsetzung obliegt der zentralen, automatisierten Intelligenz und den Geräten.

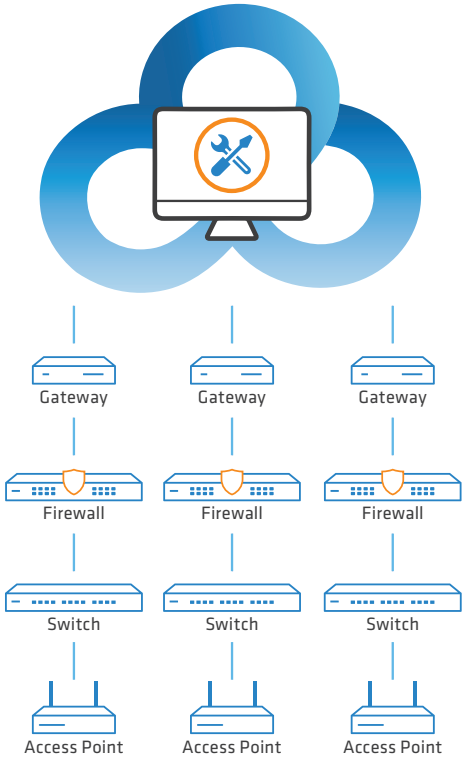

Abb. 1 Software-defined Networking

SD-WAN

SD-WAN ermöglicht die automatische Einrichtung sicherer IPSec-VPN-Verbindungen zwischen Standorten inklusive Netzwerkvirtualisierung auch über die Weitverkehrsstrecken: Die VPN-Funktionalität wird per Mausklick aktiviert und die gewünschten VLANs werden für den jeweiligen Standort ausgewählt. Die aufwändige Einzelkonfiguration der einzelnen Tunnelendpunkte entfällt vollständig.

SD-LAN

SD-LAN orchestriert die Port-Profile aller Switches und weist die notwendige Netzwerkkonfiguration automatisch zu, wie beispielsweise VLANs. Jedes VLAN steht hierbei für ein Segment des Netzes. So werden alle Switch-Konfigurationen standortübergreifend und passend zu den Access Points und Routern aufeinander abgestimmt und gleichzeitig per Mausklick ausgerollt oder aktualisiert.

SD-WLAN

SD-WLAN erlaubt die automatische Konfiguration mehrerer WLANs (Multi-SSID) inklusive einer Netztrennung z. B. für Hotspots. Diese unterschiedlichen WLAN-Netzwerke können als Segmente innerhalb des Gesamtnetzwerkes betrachtet werden. Dabei müssen nur SSID, Authentifizierungsmethode und nach Bedarf Bandbreitenlimitierung pro WLAN definiert werden. So erstellte WLAN-Profile werden im Anschluss einfach per Mausklick auf beliebig viele Access Points und WLAN-Router an den gewünschten Standorten ausgerollt oder aktualisiert.

SD-SECURITY

SD-SECURITY stellt hochgradig automatisierte Sicherheitsfunktionen von Cloud-managed Next Generation UTM-Firewalls sicher. Mit der zentralen Administration von Vorgaben für Netzwerksicherheit, Compliance und Bandbreitennutzung können so zum Beispiel Applikationen geblockt oder ein direkter Zugriff erlaubt werden.

Fazit

Software-defined Networking ersetzt die bisher manuelle Gerätekonfiguration durch eine automatisierte Netzwerk-Orchestrierung. Zudem ermöglicht ein zentrales, Cloud-basiertes Managementsystem, auf der Grundlage von SDN-Technologie, ein ganzheitliches „hyper-integriertes" Management. Sprich: Alle Geräte fallen darunter: Router, Switches, Access Points und Firewalls. Dies reduziert massiv die Betriebskosten (OPEX): Die aufwändige Einzelgerätekonfiguration entfällt, neue Standorte werden schnell und sicher in Betrieb genommen, Netzwerkfehler können schnell erkannt und ohne teure Außendiensteinsätze proaktiv behoben werden. Zudem können die einzelnen Netzsegmente global bearbeitet und die Änderungen automatisch auf alle betroffenen Geräte ausgerollt und anschließend vollständig überwacht werden. Administrative Tätigkeiten, die vorher Stunden oder Tage in Anspruch genommen haben, reduzieren sich auf wenige Minuten oder Klicks. Das Resultat: Komplexe Vernetzungsszenarien werden spielend einfach beherrschbar und Netzwerke – wie auch IT-Services – werden auf ein neues Leistungsniveau gehoben.