Softwaregesteuerte Campus-Netzwerke als Antwort auf die Anforderungen der Digitalisierung

Automatisierung der Campus-Netzwerke

Traditionell betriebene Netzwerke können den Anforderungen der Digitalisierung nicht mehr standhalten. Durch die Automatisierung des Campus soll die Netzwerkkonfiguration zukünftig bedarfsgerecht und selbstständig den jeweiligen Bedürfnissen anpasst werden.

Nach dem Einzug von Software-Defined-Technologien in Rechenzentren (SDN) und in den Weitverkehrsnetzen (SD-WAN) rücken jetzt die Campus-Infrastrukturen immer mehr in das Interesse der Unternehmen. Diesen Umstand haben auch die Hersteller erkannt und bieten mittlerweile entsprechende Lösungen. Annähernd zeitgleich bringen zwei der marktführenden Netzwerkanbieter eine Automatisierungs-Lösung für Campus-Netzwerke heraus.

Cisco Systems spricht dabei vom »Software-Defined Access«, Bestandteil der Digitalen Netzwerk-Architektur (DNA), die Mitte 2017 vorgestellt wurde. Bei Extreme Networks wird das neue Angebot, das maßgebliche Teile aus der Akquise von Avaya Networking enthält, als »Automated Campus« bezeichnet. Warum aber müssen wir uns mit der Automatisierung der Campus-Netze überhaupt beschäftigen und was steckt eigentlich hinter den Lösungen? Und vor allem, welche Vorteile sollen sich durch deren Einsatz ergeben?

Campus-Netzwerke sind typischerweise von komplexen VLAN-Strukturen, zerklüfteten Netzwerkbereichen und getrennten Richtlinienverwaltungen für das LAN und WLAN geprägt. Veränderungen im Netzwerk werden zu 95 % durch manuelle, CLI-basierte »hop-by-hop-Programmierung« auf jedem einzelnen Gerät vorgenommen. Fehler bei der Programmierung sind an der Tagesordnung und gefährden neben der Stabilität des Netzwerks mit direktem Impact auf die Business Continuity auch die Sicherheit der Unternehmensdaten. So werden beispielsweise fast 70 % aller Richtlinienverletzungen menschlichen Fehlprogrammierungen zur Last gelegt. Gleichzeitig kämpfen die Unternehmen mit Personalmangel und Überalterung in den IT-Abteilungen.

Die Anforderungen der digitalen Transformation. Studien zufolge werden heute rund 70 % der IT-Budgets alleine dafür verwendet, die Netzwerke am Laufen zu halten – Tendenz steigend. Da bleibt nicht viel Spielraum für Innovationen. Mit der digitalen Transformation verschärft sich die Problematik beim Betrieb der Netzwerke weiter, denn dadurch erhöhen sich die Anforderungen deutlich. Experten sind sich einig, dass traditionell betriebene Netzwerke den Anforderungen der Digitalisierung nicht standhalten können:

- Durch das Internet der Dinge (IoT) drängen immer mehr Endgeräte in die Netze.
- Anwender verfügen heute über eine Vielzahl von Endgeräten und haben den Anspruch, diese auch simultan im Netzwerk zu nutzen.
- Parallel steigen applikationsgetrieben die Anforderungen an Bandbreite und Quality-of-Service stetig an.
- Mobile-first-Strategien ebenso wie cloudzentrierte IT verändern die Kommunikationsströme nachhaltig. Netzwerkverantwortliche benötigen Echtzeitanalyse-Systeme, die es ihnen ermöglichen, dieses veränderte Kommunikationsverhalten zu verstehen und Netzwerkprobleme oder -trends frühzeitig zu erkennen und darauf zu reagieren.

> **Studien zufolge** werden heute rund 70 % der IT-Budgets alleine dafür verwendet, die Netzwerke am Laufen zu halten – Tendenz steigend. «

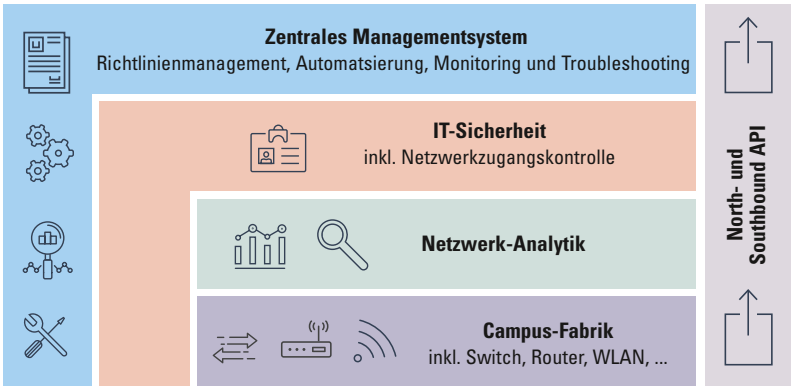
- Die mangelhafte Agilität der Netzwerkinfrastruktur ist nicht nur in den Rechenzentren ein immer wieder angeführter Kritikpunkt. Insbesondere die Umsetzungszeiten für Moves/Adds/Changes oder Upgrades müssen für eine optimale Unterstützung digitaler Initiativen von Tagen auf Minuten reduziert werden. Auch weisen die gewachsenen Infrastrukturen oft eine solche Komplexität auf, dass sie in der vorliegenden Form nicht oder nur mit erheblichem Aufwand automatisierbar sind. Daher ist es notwendig, dass ein Ziel darin besteht, die Tool-Landschaft und Prozesse auf ein handhabbares Maß zu verschlanken.
- Mehr Endgeräte und Anwendermobilität, funk- und cloudbasierte Netzwerke, sich ändernde Verkehrsmuster und eine allgemein zunehmende Bedrohungslage erfordern neue Verfahren, um den Unternehmensanforderungen an die IT-Security zu entsprechen. Der zunehmenden Bedeutung des Netzwerkes in einer digitalen Welt muss jedoch gleichzeitig auch durch Maßnahmen zur Erhöhung der Zuverlässigkeit, Ausfallsicherheit und Integrität Rechnung getragen werden.

Fabric, Policy, Management und Analytics. Betrachtet man die Kernelemente einer Campus-Automatisierung, erscheinen die Ansätze der beiden Hersteller Cisco Systems und Extreme Networks sehr ähnlich, auch wenn sie natürlich einige Unterschiede aufweisen, auf deren Details hier jedoch nicht näher eingegangen wird:

- In beiden Architekturen ist eine Campus Fabric der grundlegende Baustein und beinhaltet Switches, Router, Wireless Access Points und WLAN Controller. Während Cisco Systems zum Aufbau seiner Fabric auf LISP (Control-Plane), VXLAN (Data-Plane) und CTS (Policy-Plane) setzt, verwendet Extreme Networks IS-IS und Shortest Path Bridging (SPB), das inzwischen als IEEE 802.1aq standardisiert wurde. Beide Varianten bieten den Charme, dass die traditionell erforderlichen Protokolle zum Aufbau von Campus-Architekturen, wie beispielsweise IEEE 802.1, STP, VLAN, RIPv2, OSPF, EIGRP, PIM, BGP oder MPLS, hierfür nicht mehr erforderlich sind und damit ein großes Maß an Komplexität aus den Netzwerkkonfigurationen eliminiert werden kann.
- Die Campus Fabric wird mittels eines zentralen Managementsystems auf Basis zuvor definierter Richt-

Referenzarchitektur

Quelle: Controlware GmbH



Die Automatisierung des Campus-Netzwerks verbessert die Produktivität, verringert die Kosten, vereinfacht das Onboarding, steigert die Netzwerk-Performance, verbessert die Zuverlässigkeit, erhöht die Sicherheit und erleichtert die Compliance.

linien (Policies) konfiguriert. Cisco Systems verwendet dazu sein »DNA Center«, das gekoppelt mit dem SDN-Controller »APIC-EM« die Automatisierung, das Monitoring und Troubleshooting ermöglicht. Bei Extreme Networks kommt für dieselbe Aufgabenstellung das »Extreme Management Center« (vormals bekannt unter der Bezeichnung »NetSight«) zum Einsatz.

- Ergänzt wird die Architektur durch ein leistungsfähiges Netzwerk-Analytics-System (bei Cisco Systems »Network Data Platform«, bei Extreme Networks »ExtremeAnalytics«),
- eine weitreichende Zugangskontrolle (bei Cisco Systems »Identity & Access Policy« ISE, bei Extreme Networks »ExtremeControl«), die mit den implementierten Fingerprinting-Methoden zur Identifikation unter anderem von Nutzern, Geräten und Gerätestatus in beiden Fällen deutlich über IEEE 802.1X hinaus geht, und
- North- und Southbound API zur Einbindung von Drittherstellern, neuer Apps und Services – beispielsweise aus den Bereichen IT-Security, Mobility, Management und Orchestrierung sowie Analytics, Data Center und Cloud. Extreme Networks bietet etwa mit Fabric Attach die Möglichkeit, nicht-fabric-befähigte Geräte in die Campus Fabric zu integrieren und fabric-basierte Dienste direkt zu nutzen. Cisco Systems erweitert die Architektur zusätzlich um eine WAN-Integration und wird damit das Management von SD-Access und SD-WAN von einer einzigen Managementplattform aus ermöglichen.

Der eigentliche Clou bei der Automatisierung des Campus liegt darin, dass sich die Netzwerkkonfiguration zukünftig bedarfsgerecht und automatisch den jeweiligen Bedürfnissen (Endgerät, Anwender, Applikation, Policy) anpasst. Dazu müssen Netzwerkanalyse-Systeme und Policy-Control Hand-in-Hand arbeiten und unter anderem Netzwerkzustände, Applikationsanforderungen und Access-Control-Vorgaben in Echtzeit erfassen und in der Netzwerkkonfiguration umsetzen. Das ist sicher noch Zukunftsmusik, aber die Anfänge sind bereits gemacht, unter anderem bei Zero-Touch-Provisioning oder wandernden VLAN-Konfigurationen. Diese bringen den Netzwerkadministratoren schon heute eine beachtliche Entlastung.

Vorteile bei Business-Outcomes. Klar ist, dass niemand seine Campus-Infrastruktur weitreichend verändern wird, wenn sich dadurch nicht ein deutlich erkennbarer Mehrwert ergibt. Relativ schnell sind einige Vereinfachungen im Netzwerkbetrieb erkennbar:

- die bereits angesprochene Host Mobility ohne die Notwendigkeit umfangreicher hop-by-hop-Programmierung von VLANs,
- auch ohne die Implementierung von MPLS wird eine granulare und verwaltbare Netzwerk-Segmentierung möglich,
- die Einbindung einer rollenbasierten Zugangskontrolle ohne die Notwendigkeit der komplexen und aufwendigen Pflege von Access Control Lists (ACL),
- die Verwaltung der Richtlinien für verkabelte und kabellose Infrastrukturen in derselben Management-Software,
- die Verwaltung von Konfigurationen für Geräte im Campus, im WAN und an entfernten Standorten mit nur einem Tool (Cisco WAN-Integration).

Doch unabhängig von einer rein technischen Betrachtung, bietet die Automatisierung des Campus-Netzwerks erhebliche Vorteile, die sogar das Geschäftsergebnis positiv beeinflussen können:

Verbesserte Produktivität und geringere Kosten bei Änderungen/Anpassungen:
Der Fabric-basierte Ansatz ermöglicht eine Beschleunigung bei der Implementierung, Konfiguration, Applikationsbereitstellung und dem Troubleshooting verbunden mit deutlich weniger Fehlkonfigurationen. Dadurch ergibt sich eine deutlich größere Netzwerkstabilität. Änderungen und Updates lassen sich zudem im laufenden Betrieb durchführen.

Vereinfachtes Onboarding:
Durch die Kombination aus Fabric und Policy ist es möglich, Identifikationen und automatische Verbindungen von Anwendern und Endgeräten zu realisie-

ren – unabhängig davon, von wo aus sich diese mit dem Netzwerk verbinden. Gerade im Hinblick auf die zunehmende User-Mobility und die massive Zunahme von IoT-Geräten bedeutet dies eine enorme Entlastung der Administratoren bei zeitgleich schneller und stabiler Konnektivitätsbereitstellung, verbunden mit einer hohen Sicherheit für das Unternehmensnetzwerk.

Steigerung der Netzwerk-Performance:
In einer Netzwerkumgebung, die sich selbstständig den Erfordernissen anpasst, erhält jede Applikation genau die benötigte Bandbreite und den erforderlichen Quality-of-Service.

Verbesserte Zuverlässigkeit und Elastizität:
Load-Sharing, Load-Balancing und die Fähigkeit im Fehlerfall automatisches Re-Routing vorzunehmen, sind wesentliche Eigenschaften einer Fabric. Ein stabiles und verfügbares Netzwerk wiederum ist die Grundvoraussetzung für einen reibungslosen Geschäftsbetrieb.

Verbesserte Sicherheit:
In Zeiten einer zunehmenden Bedrohung der IT-Sicherheit und der Erkenntnis, dass eine reine Perimetersicherheit schon lange nicht mehr ausreicht, reduziert verwaltbare Hyper-Segmentierung das Risiko der Ausbreitung eines Sicherheitslecks erheblich. Dies kann den entscheidenden Unterschied zwischen einem Sicherheitsvorfall oder dem Stillstand des gesamten Geschäftsbetriebs ausmachen.

Verbesserte Compliance:
Nicht nur für kritische Infrastrukturen und die Kreditkartenindustrie ist der Nachweis der Einhaltung von Sicherheitsrichtlinien enorm wichtig. Eine Campus-Fabric mit zentral verwalteten Sicherheits-Policies erleichtert es, die vorgegebenen Regelwerke im Netzwerk effektiv durchzusetzen.

Sind Sie für die Digitalisierung gerüstet? Bei der Konzeption und Realisierung von Automatisierungsprojekten im Bereich der Campus-Netzwerke ist es ratsam, sich eingehend mit den Eigenschaften einer Campus-Fabric auseinanderzusetzen. Nur so finden Sie heraus, welche Möglichkeiten sich Ihnen bieten und welches Potenzial Sie mit der jeweiligen Lösung ausschöpfen können. Ein erfahrener Systemintegrator wie Controlware steht Ihnen hier als Partner zur Seite. Eigene SDN-Labore, langjährige Partnerschaften mit den Herstellern und höchster Partnerstatus – nicht nur bei Cisco Systems und Extreme Networks – gewährleisten Kompetenz, die sich für Sie auszahlt.

Rolf Bachmann

Rolf Bachmann,
Business Development Manager Network Solutions

www.controlware.de