Das Software-Defined Campus-Netzwerk (SD-Campus)

Traditionelle 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 sind dabei an der Tagesordnung und gefährden neben der Stabilität des Netzwerkes auch die Sicherheit der Unternehmensdaten. So werden beispielsweise fast 70%* aller Richtlinienverletzungen menschlichen Fehl-programmierungen zur Last gelegt. Gleichzeitig kämpfen die Unternehmen mit Personalmangel und Überalterung in den IT-Abteilungen.

Traditionell betriebene Netzwerke können den Anforderungen der Digitalisierung nicht standhalten!

Studien zufolge werden heute rund 70%** der IT-Budgets allein dafür aufgewandt, die Netzwerke am Laufen zu halten – Tendenz steigend. Da bleibt nicht viel Spielraum für Innovationen. Die Folgen der Digitalen Transformation erhöhen den Druck auf die Netzwerkbetreiber:

- Eine zunehmende Anzahl Endgeräte drängt in die Netze (z. B. durch Anwendungen im IoT). Eine manuelle Verwaltung ist kaum noch machbar.
- Cloud-zentrierte-IT und Mobile-first-Strategien verändern die Kommunikationsströme nachhaltig. Ohne Analysefunktionen sind die neuen Muster jedoch nicht zu verstehen.
- Fehlende Netzwerkagilität führt zu mangelnder Fähigkeit des Unternehmens, sich den Marktanforderungen anzupassen. Disruptiven Konzepten hat man so kaum etwas entgegen zu setzen.
- Die gewachsenen Infrastrukturen sind so komplex, dass eine Automatisierung kaum möglich ist. Prozesse und Tools müssen verschlankt werden.
- Mikrosegmentierung ist jetzt auch im Campus eine wesentliche IT-Security-Anforderung, die das Risiko der Ausbreitung von Sicherheitslecks reduziert.

* *Cisco SDA solution overview c22-739012 2017*

*** IDC WC20170525*

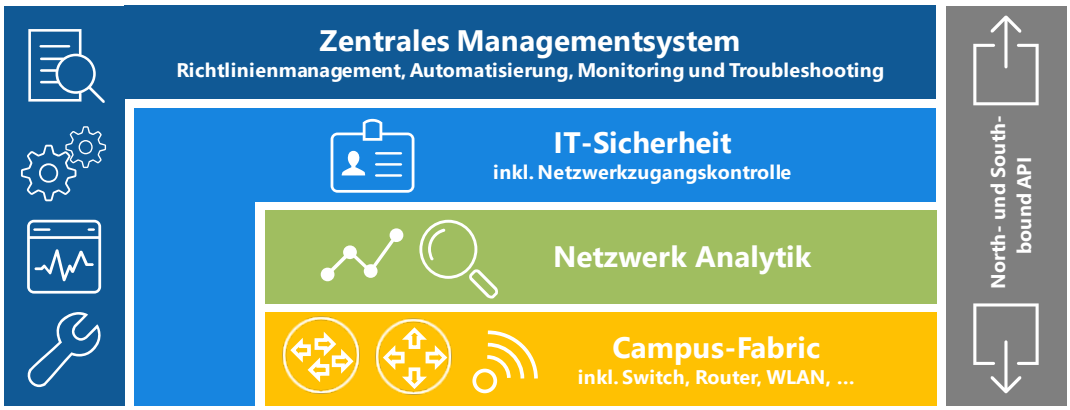
Die Idee eines automatisierten Campus-Netzwerkes verstehen

Der eigentliche Clou bei der Automatisierung des Campus ist, dass sich die Netzwerkkonfiguration zukünftig bedarfsgerecht und automatisch den jeweiligen Bedürfnissen (Endgerät, Anwender, Applikation, Policy) anpassen soll. Dazu müssen Netzwerkanalyse-Systeme und Policy-Control Hand-in-Hand arbeiten und u. a. Netzwerkzustände, Applikationsanforderungen und Access-Control-Vorgaben in Echtzeit erfassen und in der Netzwerkkonfiguration umsetzen können.

Das ist sicher noch ein Stück Zukunftsmusik, aber die Anfänge sind z. B. bei Zero-Touch-Provisioning oder durch mit dem Host wandernden VLAN-Konfigurationen gemacht und bringen bereits heute nachweislich eine Entlastung der Netzwerkadministratoren.

Administrative Vorteile

- Host-Mobility OHNE die Notwendigkeit umfangreicher VLAN-Konfiguration
- Granulare und verwaltbare Netzwerksegmentierung auch OHNE den Einsatz von MPLS
- Rollenbasierte Zugangskontrolle OHNE ACLs
- Gemeinsame Verwaltung von LAN und WLAN in derselben Managementsoftware



Voraussetzung ist eine Netzwerkarchitektur, die die Automatisierung aktiv unterstützt

Bestandteile eines automatisierten Campus-Netzwerkes:

Campus Fabric	Grundlegender Baustein, der Switches, Router und WLAN beinhaltet. Wenige Fabric-Protokolle ersetzen den komplexen Protokollstack traditioneller Architekturen
Zentrales Managementsystem	Konfiguration der Fabric auf Basis zuvor definierter Richtlinien (Policies), Automatisierung, Monitoring und Troubleshooting über eine zentrale Plattform
Netzwerk-Analyse-System	Erfassung des Netzwerkverhaltens als Basis der Automatisierung
Zugangskontrolle	Einbindung von rollen-, orts-, zeit- und geräte-bezogenem NAC in das zentrale Managementsystem
North- und South-bound APIs	Integration von Drittherstellern, neuer Apps und Services in die Campus-Fabric.

Vorteile für Unternehmen durch den Einsatz von Netzwerkautomatisierung

- Verbesserte Produktivität:
  Beschleunigung von Implementierung, Konfiguration, Troubleshooting, Applikationsbereitstellung
- Geringere Kosten für Änderungen:
  Deutlich weniger Fehlkonfigurationen, Updates im laufenden Betrieb
- Effizientere Administration:
  Automatische Identifikation und Verbindung von Anwendern und Geräten mit dem Netzwerk
- Steigerung der Netzwerk-Performance:
  Automatisierte Anpassung der Netzwerkumgebung an die tatsächlichen Erfordernisse
- Verbesserte Zuverlässigkeit und Elastizität:
  Load-Sharing, Load-Balancing und automatisiertes Re-Routing sind typische Eigenschaften einer Fabric
- Verbesserte Sicherheit:
  Mikrosegmentierung kann den Unterschied ausmachen zwischen Sicherheitsvorfall oder Stillstand des Betriebes
- Verbesserte Compliance:
  Zentrales Policy-Management ermöglicht den Nachweis der Einhaltung von Sicherheitsrichtlinien

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108
info@controlware.de
www.controlware.de