Cisco DNA-Center – SDN-basierte Netzwerkinfrastrukturen

- Start um 9:00 Uhr
- Ende 16:30 Uhr (Freitag um 15:30 Uhr)
- Mittagspause um 12 Uhr

Was ist SD-Access zusammengefasst?

SD-Access

Vereinheitlichung von LAN und WLAN

SD-Access revolutioniert die Netzwerklandschaft durch eine einheitliche Herangehensweise an LAN und WLAN. Diese Lösung eliminiert die traditionellen Unterschiede zwischen kabelgebundenen und drahtlosen Netzwerken im SDA-Umfeld. Sie schafft eine nahtlose Integration und Verwaltung für eine effizientere und konsistente Netzwerkleistung.

ZTNA (Zero Trust Network Access)

Sicherheitsfokus durch 802.1x/MAB und CCC/DNAC mit ISE

ZTNA, basierend auf 802.1x/MAB, ist ein zentraler Bestandteil der Sicherheitsstrategie. Durch die Verbindung mit dem Cisco Catalyst Center (CCC, alt: DNAC) und der Identity Service Engine (ISE) ermöglicht es einen strikten Sicherheitsfokus. Dieser Ansatz gewährleistet, dass jeder Netzwerkzugriff gründlich überprüft und autorisiert wird, um die Sicherheitsintegrität zu gewährleisten.

Makro- und Mikro-Segmentierung

Segmentierung für umfassende Sicherheit

SD-Access bietet eine umfassende Segmentierungslösung. Makro-Segmentierung erfolgt durch virtuelle Netzwerke (VN) und Virtual Routing and Forwarding (VRF), um Netzwerke in klar definierte Bereiche zu unterteilen. Zusätzlich bietet es Mikro-Segmentierung über Sicherheitsgruppen (SG), früher bekannt als TrustSec. Die Kombination beider Ebenen der Segmentierung ermöglicht eine feingranulare Kontrolle über Netzwerkzugriffe und maximiert die Sicherheit.

Over- und Underlays

Underlay

Grundlegende Netzwerk in welchem sich Switche befinden und die Datenkommunikation stattfindet

- Das Underlay umfasst Layer-3-Routing mit Link State Advertisements (LSA), Single Area Konfiguration, Authentifizierung und weitere Funktionen.
- Es bildet die Grundlage für die Fabric Edge Nodes.
- Es ermöglicht die Anbindung an herkömmliche Netzwerke über Virtual Routing and Forwarding (VRFs).

Overlay

Das Netzwerk in welchem Endgeräte miteinander kommunizieren

- Das Overlay ist eine Kombination aus Layer-3- und Layer-2-Overlay. Layer-2 wird für Legacy-Protokolle wie Wake-on-LAN (WoL) genutzt.
- Es erfolgt ein Mapping von Virtual Networks (VN) zu VRF-Instanzen über Border-Nodes.
- Endgeräte kommunizieren über dieses Overlay.
- Tunnelverbindungen zwischen den Endgeräten, vergleichbar mit Punkt-zu-Punkt-Verbindungen, basieren auf VXLAN.
- Die Verbindungen werden durch Locator/ID Separation Protocol (LISP) gefunden/identifiziert. Wer bildet das Tunnelende?
- Die Kommunikation findet innerhalb von LISP-Instanzen statt, wobei für jedes VN eine eigene Instanz existiert.
- Segmentierung erfolgt über Security Group Tags (SGTs).
- Die Kommunikation zwischen VNs findet ausschließlich über externe Systeme wie Firewalls oder Router (Fusion-Device) statt.

Revision #15
Created 2023-12-18 09:15:17 UTC by Joshua Lieder
Updated 2023-12-19 09:29:17 UTC by Joshua Lieder