Herausforderung IT Konsolidierung

Sichere, plattformübergreifende Kommunikation mit SD-WAN

Oliver Böhmer
Principal Architect – Cisco EMEAR

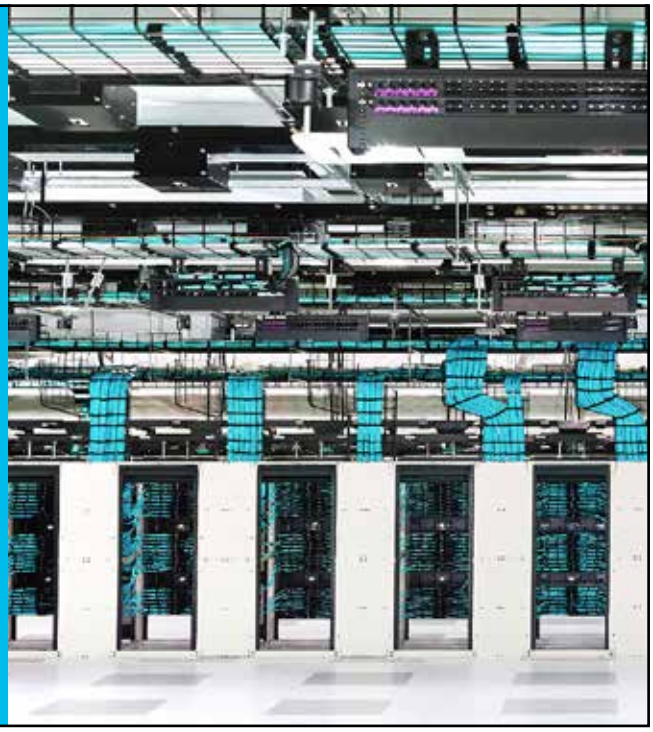
Klaus Lenssen
Chief Security Officer – Cisco Deutschland

21. Januar 2020

Agenda

- Einführung und Problemstellung
- SD-WAN - Übersicht
- Vertrauenswürdige Infrastruktur
- Automatisierung
- Zusammenfassung

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public



Einführung und Problemstellung

Herausforderung IT-Konsolidierung

- Flexible Zusammenschaltung unterschiedlicher Netze
- Schaffung von Netzbereichen mit unterschiedlichem Schutzbedarf
- Schutz vor Cyberangriffen
- Heterogenität der Anforderungen an die Weitverkehrsnetze der öffentlichen Verwaltung

- Ziel: **sichere und leistungsfähige Netzinfrastrukturen**

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Kritische Infrastrukturen

erfordern leistungsfähige & vertrauenswürdige Netzwerke

Kritische Infrastrukturen

erfordern neue Betriebsmodelle

95%

Network Changes Performed Manually

70%

Policy Violations Due to Human Error

75%

OpEx Spent on Network Changes and Troubleshooting

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Software-Defined WAN

... eine zentrale Komponente für kritische Infrastrukturen

SD-WAN is an acronym for software-defined networking in a wide area network (WAN). SD-WAN simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism. This concept is similar to how software-defined networking implements virtualization technology to improve data center management and operation.

https://en.wikipedia.org/wiki/SD-WAN

Software-defined networking (SDN) technology is an approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring making it more like cloud computing than traditional network management.

https://en.wikipedia.org/wiki/Software-defined_networking

Introducing Cisco SD-WAN
Powered by Viptela

Summary of Basic SD-WAN Capabilities

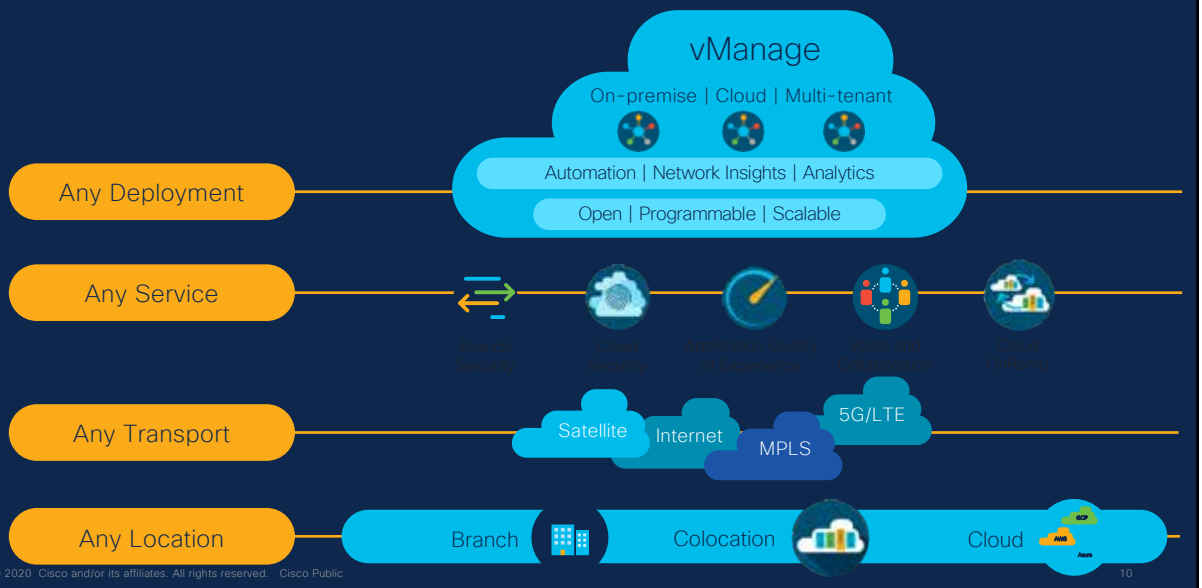
- Circuit Load Balancing
- Direct Internet Access
- Centralized Management & Orchestration
- Zero-Touch Provisioning

Cisco SD-WAN extended capabilities

- Multi-layered Security
  - Security & Segmentation
  - Analytics & Visibility
- Application Optimization
  - Voice Optimization
  - SaaS/IaaS Optimization
  - App Aware Dynamic Routing
- Enterprise Scale
  - Open and Programmable
  - Multi-Tenant/ Multi-Domain

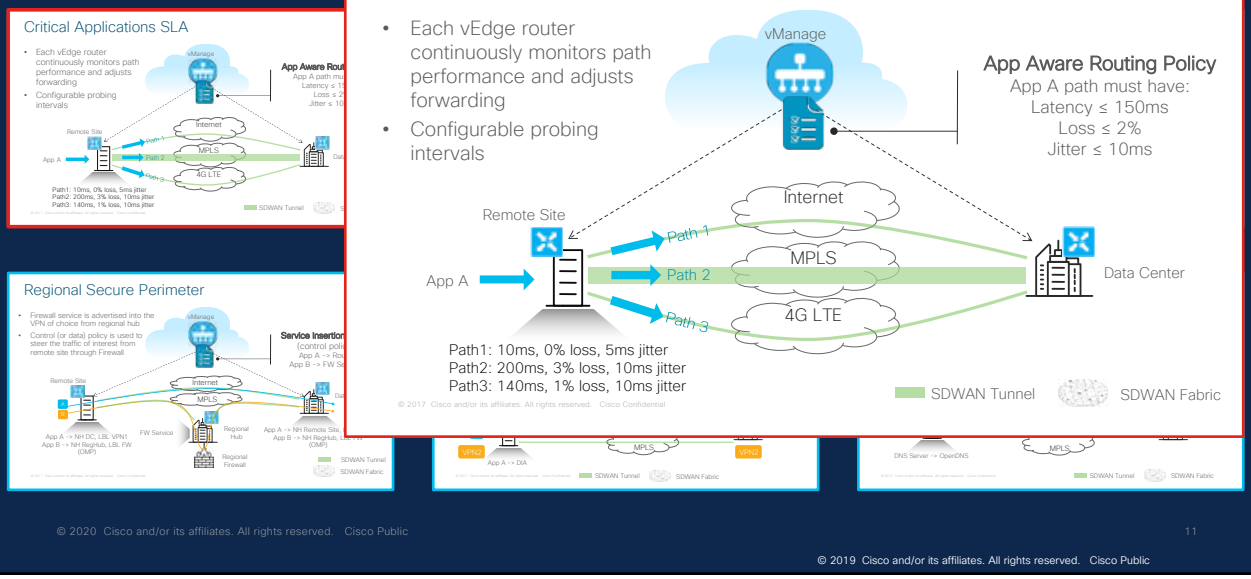
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Cloud Scale SD-WAN Architecture



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

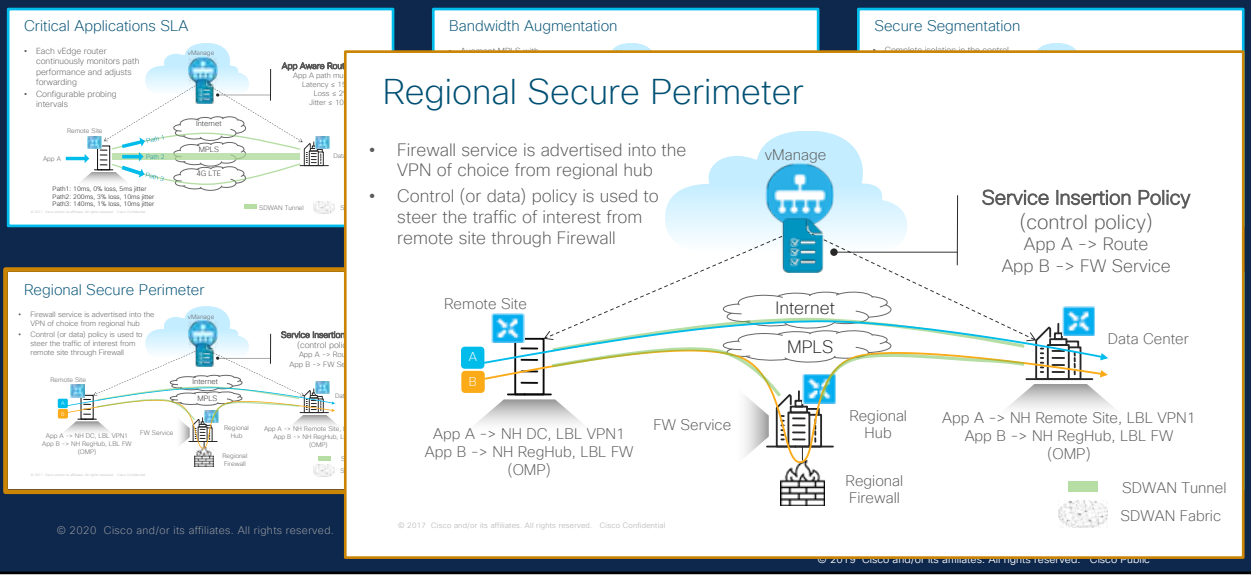
Sample SD-WAN Use Cases



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

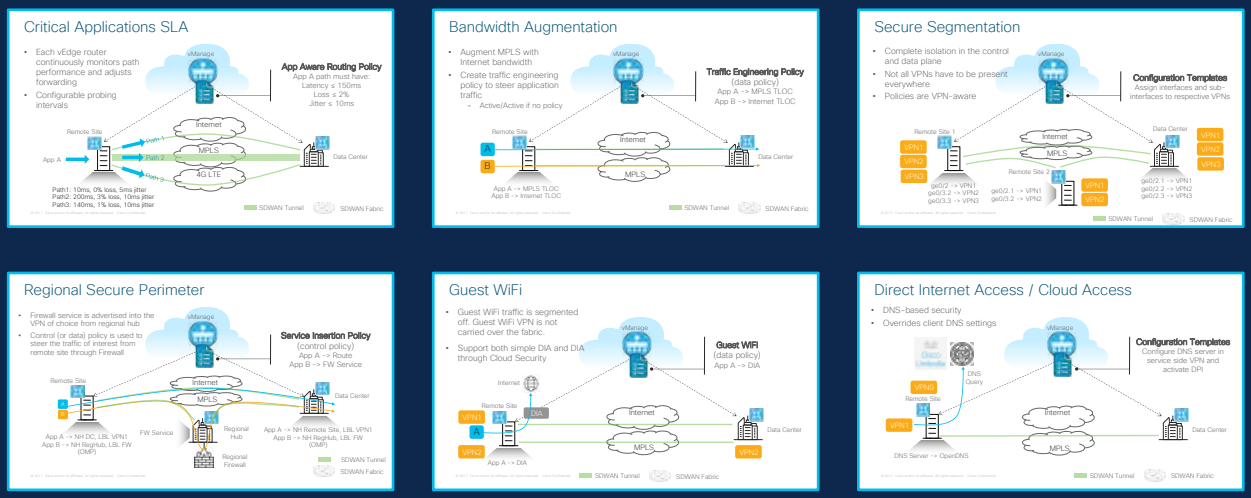
Sample SD-WAN Use Cases



© 2020 Cisco and/or its affiliates. All rights reserved.

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

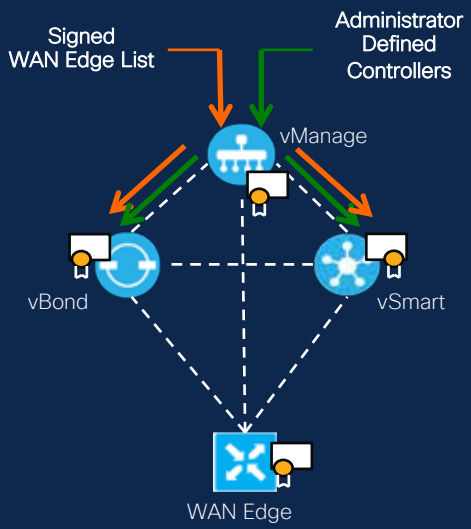
Sample SD-WAN Use Cases



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero-Trust Fabric



- Bi-directional certificate-based trust between all elements
  - Public or Enterprise PKI
- Administrator uploads digitally signed WAN Edge list
  - White-list for both physical and virtual vEdge
  - Downloadable from Cisco License portal
- Result:
  - Only explicitly authorized Devices can join the network
  - Authorization can easily and centrally be revoked

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Trustworthy Technologies

Sicherheit: Warum ist Vertrauen wichtig?

Aufbau einer vertrauenswürdigen Plattform

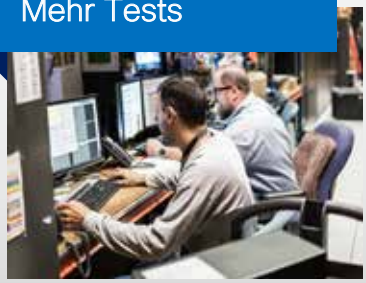
Die Netzwerkinfrastruktur muss auf einer Plattform vertrauenswürdiger Technologien aufgebaut sein, um sicherzustellen, dass die Geräte authentisch sind und nachprüfbar belegt werden kann, dass sie nicht verändert wurden.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Kundenanforderungen steigen

Nachweis der Vertrauenswürdigkeit

Mehr Tests



Mehr Transparenz

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Vertrauenswürdige Lösungen

Sicherheit in jedem Schritt …

Sicherheit eingebettet in den gesamten Lebenszyklus jeder Lösung im gesamten Portfolio

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Würden Sie einem Gerät vertrauen, das Ihnen sagt, dass es vertrauenswürdig ist?

Das Fundament vertrauenswürdiger Lösungen

Cisco SDL

Secure Development

Supply/Value Chain Security

Sicherheit über den gesamten Produkt-Lifecycle

Trustworthy Technologies

Secure Boot und Run Time Defenses

Software Integrität

Trust Anchor Modul und SUDI

Hardware Integrität

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wichtige vertrauenswürdige Technologien

Secure Boot signierter SW

- Verhindert das Booten von bösartigem Code
- Automatisierte Integritätsprüfungen
- Überwacht den Startvorgang und schaltet sich bei einer Gefährdung ab
- Schnellere Identifizierung von Bedrohungen

Trust Anchor module (TAm)

- Manipulationssicherer Chip mit X.509 Zertifikat, während der Fertigung installiert
- Bietet eindeutige Geräteidentität und Schutz vor Produktfälschungen
- Sichere, nichtflüchtige Speicherung und RNG/Crypto-Dienste
- Ermöglicht Zero-Touch-Provisioning und minimiert die Bereitstellungskosten

Runtime Defenses (RTD)

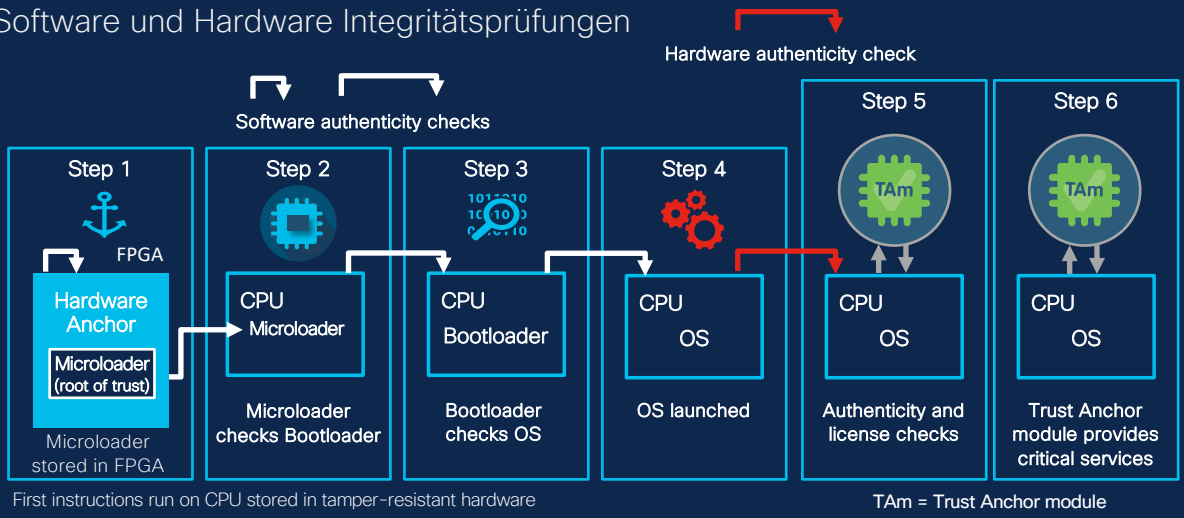
- Schützt vor dem Einschleusen von bösartigem Code in laufende Software
- Macht es für Angreifer schwieriger, Schwachstellen in laufender Software auszunutzen
- Zu den Laufzeittechnologien gehören ASLR, BOSC und X-Space

Vertrauenswürdige Technologien erhöhen Sicherheit und Resilienz der Cisco-Lösungen

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Boot

Software und Hardware Integritätsprüfungen

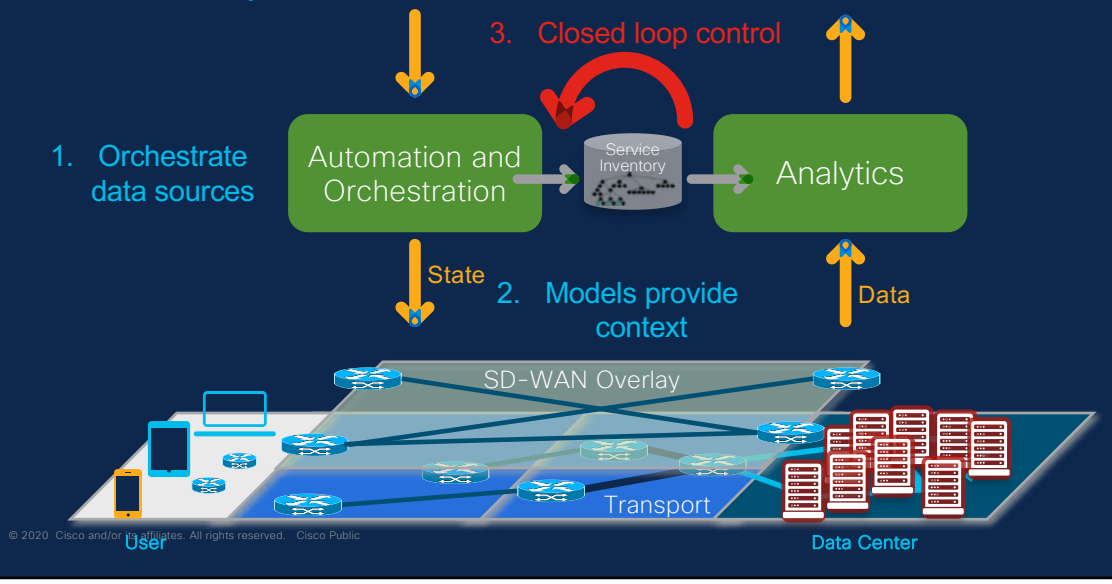


Secure boot checks images and verifies that software is authentic and unmodified before it is allowed to boot

Automatisierung

... viel mehr als eine zentrale Management-Console

Orchestration and Analytics Related as Loosely Coupled Systems – Closed Loop Assurance



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Beispiele für Closed Loop Assurance

- Außerbetriebnahme von Verbindungen bei zu hoher Fehlerrate
- Verkehrs- oder Topologie-optimierung in Spitzenlastzeiten
- Automatische Skalierung von zentralen Diensten
- Außerbetriebnahme oder Re-initialisierung bei Zweifel der Vertrauenswürdigkeit
- Automatisches Überschreiben manueller (d.h. nicht-autorisierter) Konfigurationsänderungen
- Quarantäne von verdächtigem Verkehr/Nutzern

Keine Zukunftsmusik – solche Lösungen sind bereits im Einsatz

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Crosswork Trust Insights

Cloud-basiertes SaaS-Angebot: Keine Gemeinkosten für Bereitstellung, Verwaltung und Betrieb

Vertrauenswürdigkeit visualisieren

- Report der Vertrauensdaten von Cisco IOS XR-Geräten
- HW/SW auf Produktionssystemen mit kryptografischem Nachweis überprüfen
- Report der Sicherheitsfunktionen von IOS-XR-Routing-Geräten

Inventar verfolgen und verifizieren

- Automatische Rückverfolgbarkeit von Hardware, Software und Patches
- Verfolgung und Nachweis der Behebung von SW/HW-Problemen für die Einhaltung und Prüfung
- Forensik zu HW/SW-Änderungen mit umfangreicher Geschichte

Vertrauenswürdige Daten für die Automatisierung

- Automatische Erfassung und Analyse des Hardware- und Software-Bestands
- Bereitstellung von API für Bestandsdaten
- Basis für vertrauenswürdige Automatisierungssysteme

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public


Kritische Infrastrukturen brauchen vertrauenswürdige und agile Netzwerke
Betriebszustände und Vertrauensmechanismen individueller Geräte müssen über Automatisierung zu einem Gesamtstatus der Infrastruktur aggregiert werden um sinnvoll (Sec)Ops nutzbar zu sein.
Secure Dev. Lifecycle
Trust Anchor Secure Boot
Remote Attestation
Automation
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public
28

Fragen?

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public