

ACP



ACP IT Solutions AG

Hauzenberg • Regensburg • Nürnberg

www.acp-gruppe.com

IT for
innovators.



Software Defined Networking

Use Cases und Erfahrungen aus der Praxis





Das Netzwerk der Zukunft –
automatisiert und sicher

Applica

SDN

11.11.2013

Network revolutionieren

Wird ACI vor

sws
BrainShare
2017

CISCO CERTIFIED
CCIE
ROUTING AND SWITCHING

Oliver Knon
CCIE #42421
Consultant
Oliver.knon@sws.de

Cisco Systems Networking SDN



for

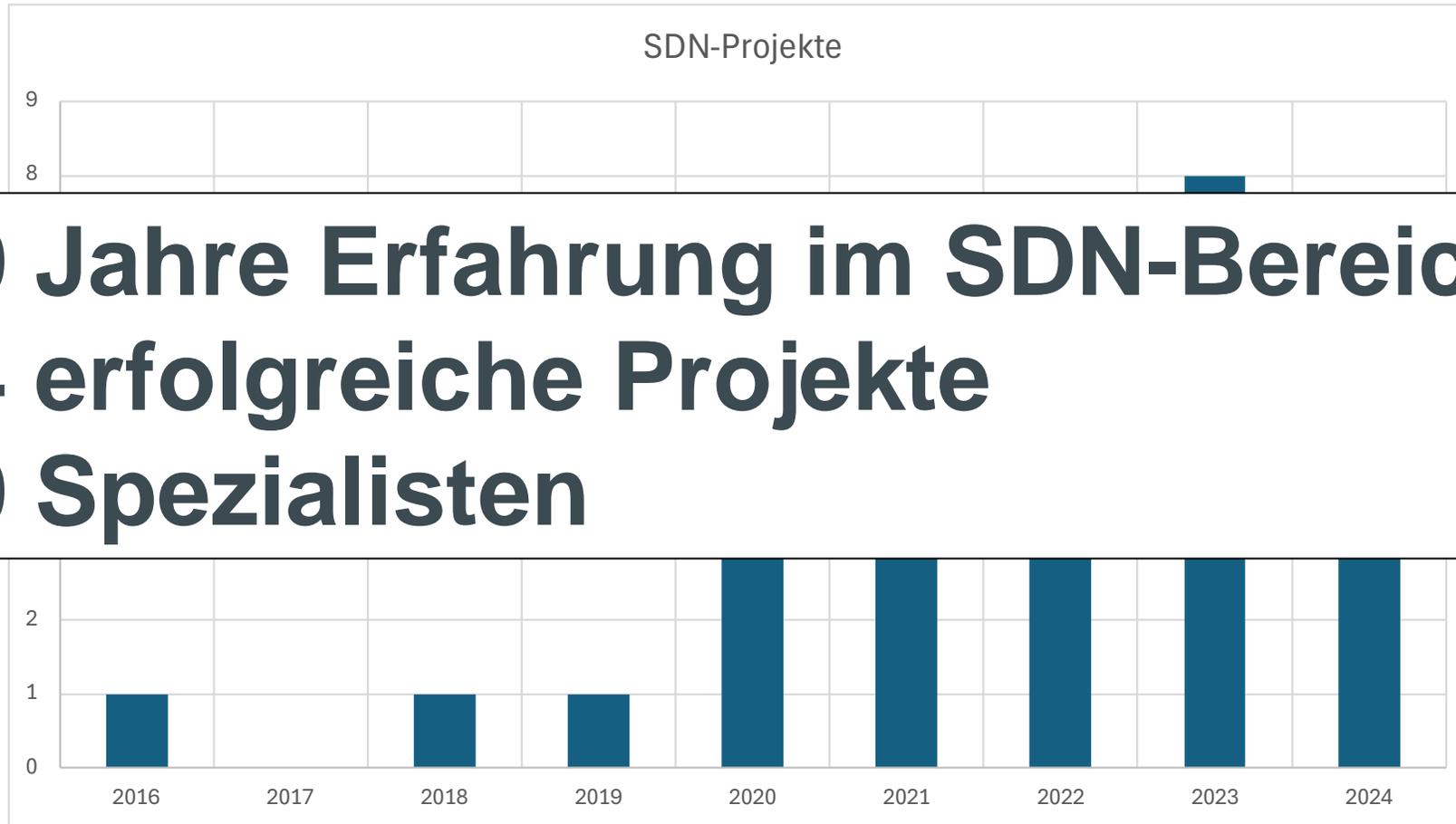
2018

Next Generation Network transparent, einfach und sicher



Oliver Knon
Senior Consultant
CCIE #42421
oliver.knon@sws.de

Intent-based networking is Cisco's big push for
Network Center – Cisco's IBN software



10 Jahre Erfahrung im SDN-Bereich
34 erfolgreiche Projekte
20 Spezialisten

ACP

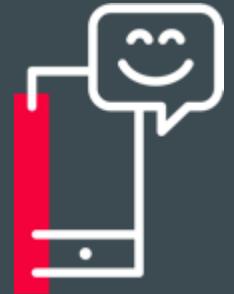


Software Defined Networking

Use Cases und Erfahrungen aus der Praxis

www.acp-gruppe.com

IT for
innovators.



Oliver Knon

Senior Solution Architect, CCIE #42421
Niederlassung Hauzenberg



oliver.knon@acp.de



+49 8586 9604 186

IT for
innovators.

Agenda

01

Einleitung

02

SD-Campus

03

SD-WAN

04

SD-Datacenter

05

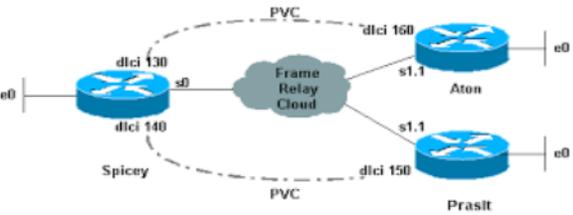
Ihre Fragen

IT for
innovators.

Einleitung

Classic Networking vs. Software Defined?

1990s

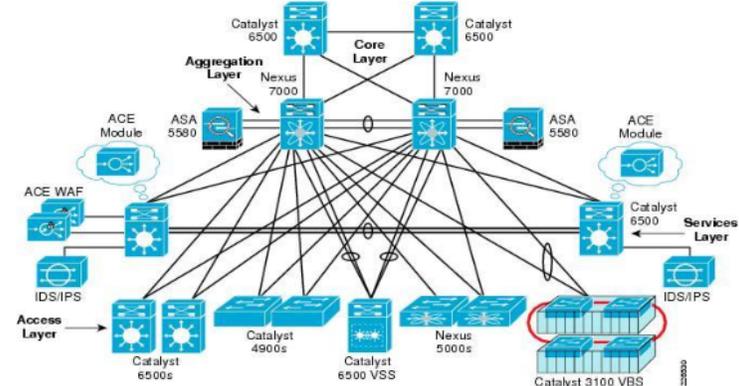


```

hq>enable
hq# config terminal
hq(config)# interface fastethernet 1/1
hq(config-if)# ip address
    1.1.1.1 255.255.255.0
hq(config-if)# no shutdown
hq(config-if)# exit
hq(config)# router eigrp
hq(config-router)# network 1.1.1.0
hq(config-router)# exit
hq(config)# exit
hq# copy run start
        
```

Today

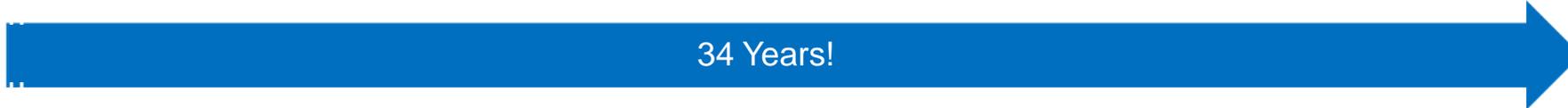
**What?
How?**



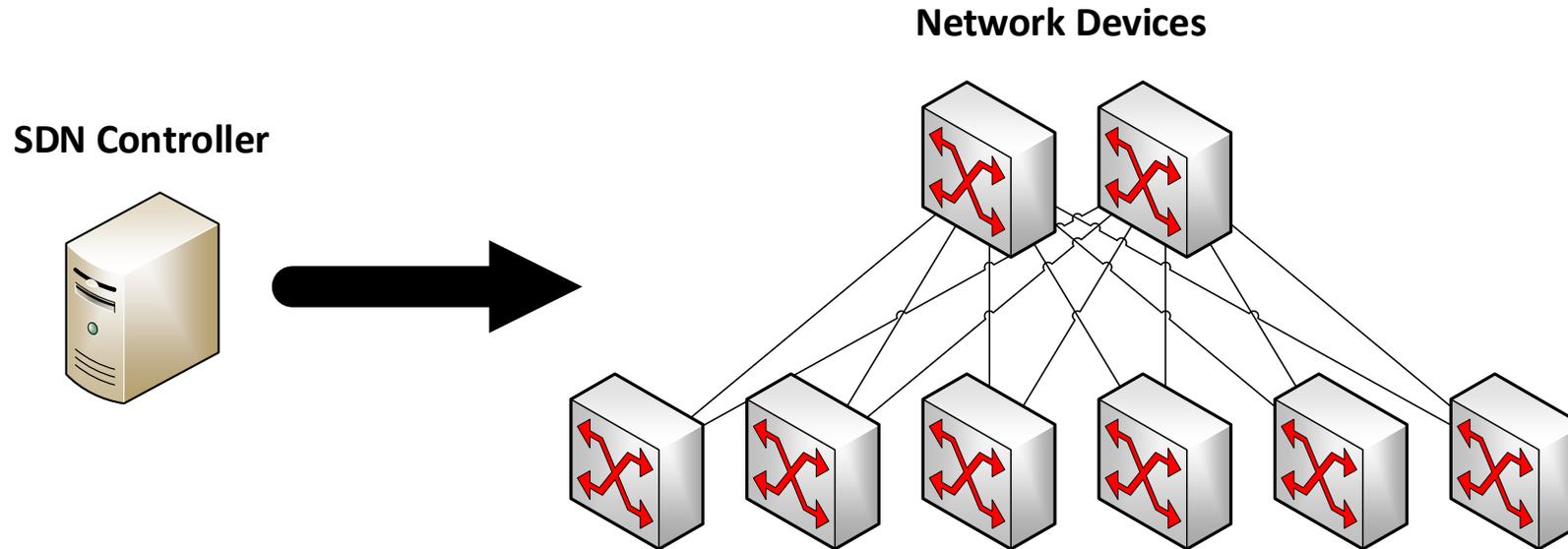
```

Catalyst>enable
Catalyst# config terminal
Catalyst(config)# interface
    Gigabitethernet 1/1/1
Catalyst(config-if)# no switchport
Catalyst(config-if)# ip address
    1.1.1.1 255.255.255.0
Catalyst(config-if)# no shutdown
Catalyst(config-if)# exit

Catalyst(config)# router eigrp Test1
Catalyst(config)# interface
    Te 1/1
Catalyst(config-if)# ip router
    eigrp Test1
Catalyst(config-if)# no shutdown
Catalyst(config-if)# end
Catalyst# copy run start
        
```



Classic Networking vs. Software Defined?



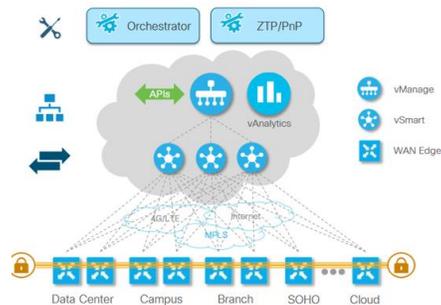
- einfaches und zentrales Management
- einheitliche Konfiguration nach Hersteller Best Practice
- zentrale und einheitliche Policies (Security/QoS)
- Automatisierung in:
 - Rollout
 - Betrieb (RMA + Updates!!!)
 - Konfiguration
 - Fehlersuche
- KI gestützte Trenderkennung und Fehlersuche

Cisco SD-Access



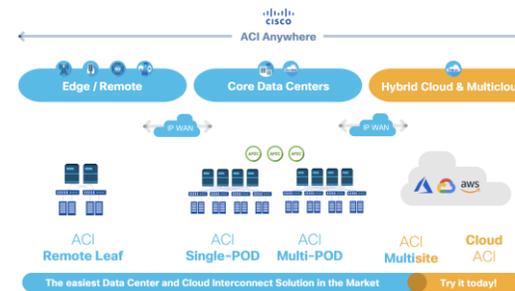
Campus

Cisco SD-WAN



WAN

Cisco ACI



Datacenter / Cloud

- 20 Cisco SD-Access Projekte von 200 bis 20.000 User
- 8 Cisco ACI Projekte von 500 bis 40.000 User
- 6 Cisco SD-WAN Projekte von 200 bis 2.500 Usern
- Branchen:
 - Industrie
 - Gesundheit
 - Versorger
 - Finanzen
 - Öffentlicher Dienst

02

SD-Campus (Cisco SDA)



Michael Sicklinger

Consultant

Niederlassung Hauzenberg



michael.sickliger@acp.de



+49 8586 9604 231

IT for
innovators.



„Das wurde wohl bei der Config vergessen...“

„Schon wieder ein neuer CVE?“

„Das ganze Wochenende updaten...hervorragend!“

„Segmentierung? Gern, aber wie?“

„Wo hängt der PC gleich wieder dran?“

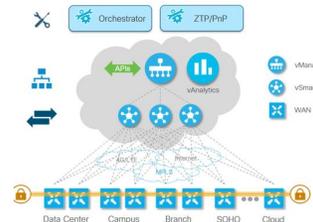
„Put your money where your mouth is“



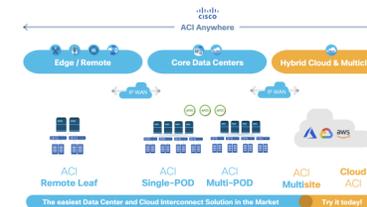
Cisco SD-Access



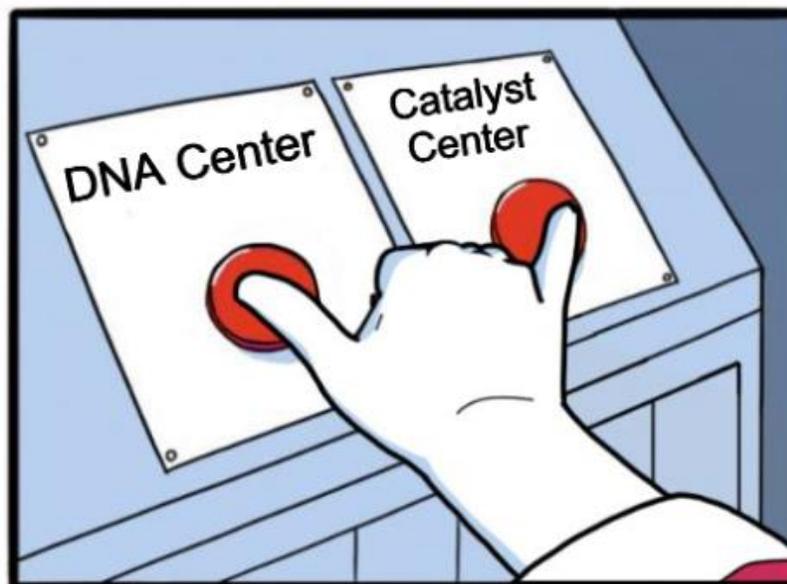
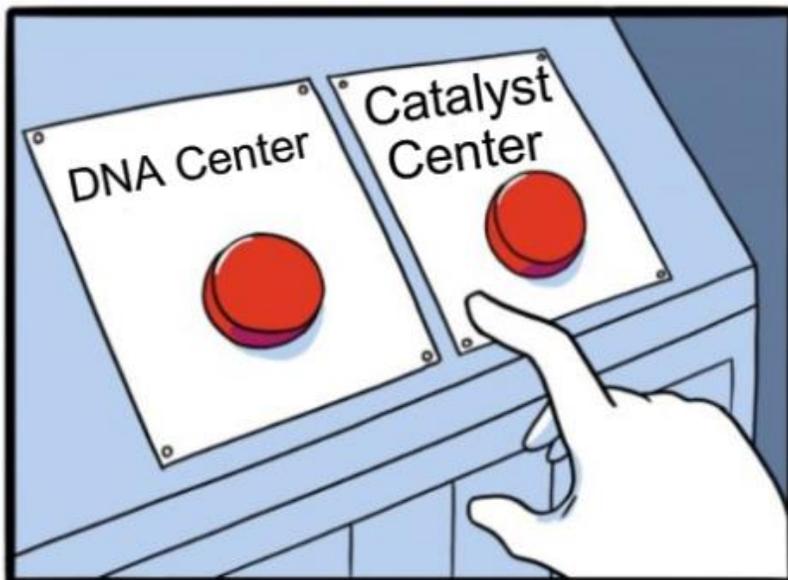
Cisco SD-WAN



Cisco ACI



First Things First



Cisco Software Defined Access

The Foundation for Cisco's Intent-Based Network



Technische Deep-Dives gratis am Secure Infrastructure Stand



Herausforderung: „Das wurde wohl bei der Config vergessen...“



Lösung: SD-Access LAN Automation

Ziel: (Voll-)automatisierte Inbetriebnahme der SDA-Switches

Ablauf:

1. Definieren der Uplink-Switches + Ports
2. Starten der LAN Automation
3. Neuen Switch einbauen und anstecken
4. Warten (ca. 30min.)



30min? Schon lang, oder...?

Moment!

Was passiert im Hintergrund:

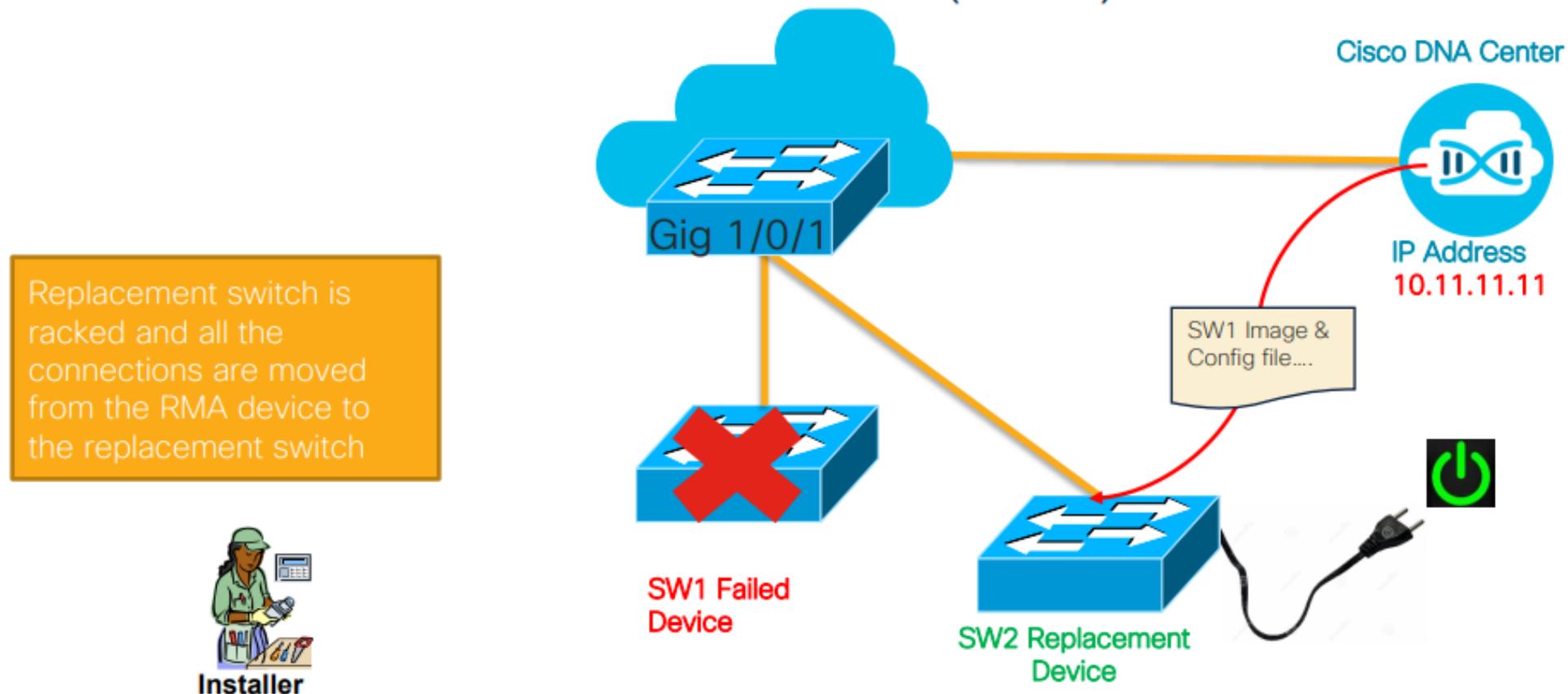
- Software-Update auf Kundenstandard
- Automatisierter Rollout der SDA Switch-Config nach CVD + Kundenparameter
→ Good Bye Copy-Paste-Fehler!

Unser Benefit:

**Netzwerkmigration an 30+ Standorten
(400+ Switches) in wenigen Monaten**

Use Case: RMA Workflow

Return Material Authorization (RMA) workflow



Unser Benefit: Kein Fachpersonal vor Ort benötigt

Use Case: CVE Management



Herausforderung: „Schon wieder ein neuer CVE?“



Lösung: DNA-Center Security Advisories

Use Case: CVE Management



ACP

Jeden Morgen 06 Uhr



Cisco DNA Center

Use Case: CVE Management



Cisco Security Advisory
Cisco DNA Center Access Contract Stored Cross-Site Scripting Vulnerability

Advisory ID:	2020-20099-000-001	CVE ID:	CVE-2020-1380	Download CVEF
First Published:	2020-09-04 14:48 CMT	CWE ID:	CWE-79	Download PDF
Version 1.0:	Final			Download
Workarounds:	No workarounds available.			
Cisco Bug ID:	CSCV31360			
CVSS Score:	Base 7.1 Click here to Copy Vector Score CVSS:3.0/AV:L/OW:L/RS:C/C:L/AN:N/A/C:R/X			

Medium

Summary
A vulnerability in the web-based management interface of Cisco DNA Center could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device.



Cisco DNA Center

ADVISORIES

0 Critical 2 High 0 Medium

SCAN CRITERIA ⓘ

15 Software Version 0 Custom 2 Advanced

Re-scan Network

Devices Advisories

SUMMARY

- > Impact
- > Custom Match Pattern

Advisories (2)

All **Affecting Devices**

Filter

Advisory ID	Advisory Title	CVSS Score ▾	Impact	CVE	Devices
cisco-sa-caf-3dXM8exv	Cisco IOx Application Framework Arbitrary File Creation Vulnerability	8.1	● High	CVE-2020-3238	2
cisco-sa-20190513-secureboot	Cisco Secure Boot Hardware Tampering Vulnerability	6.7	● High	CVE-2019-1649	2

Use Case: Software Updates

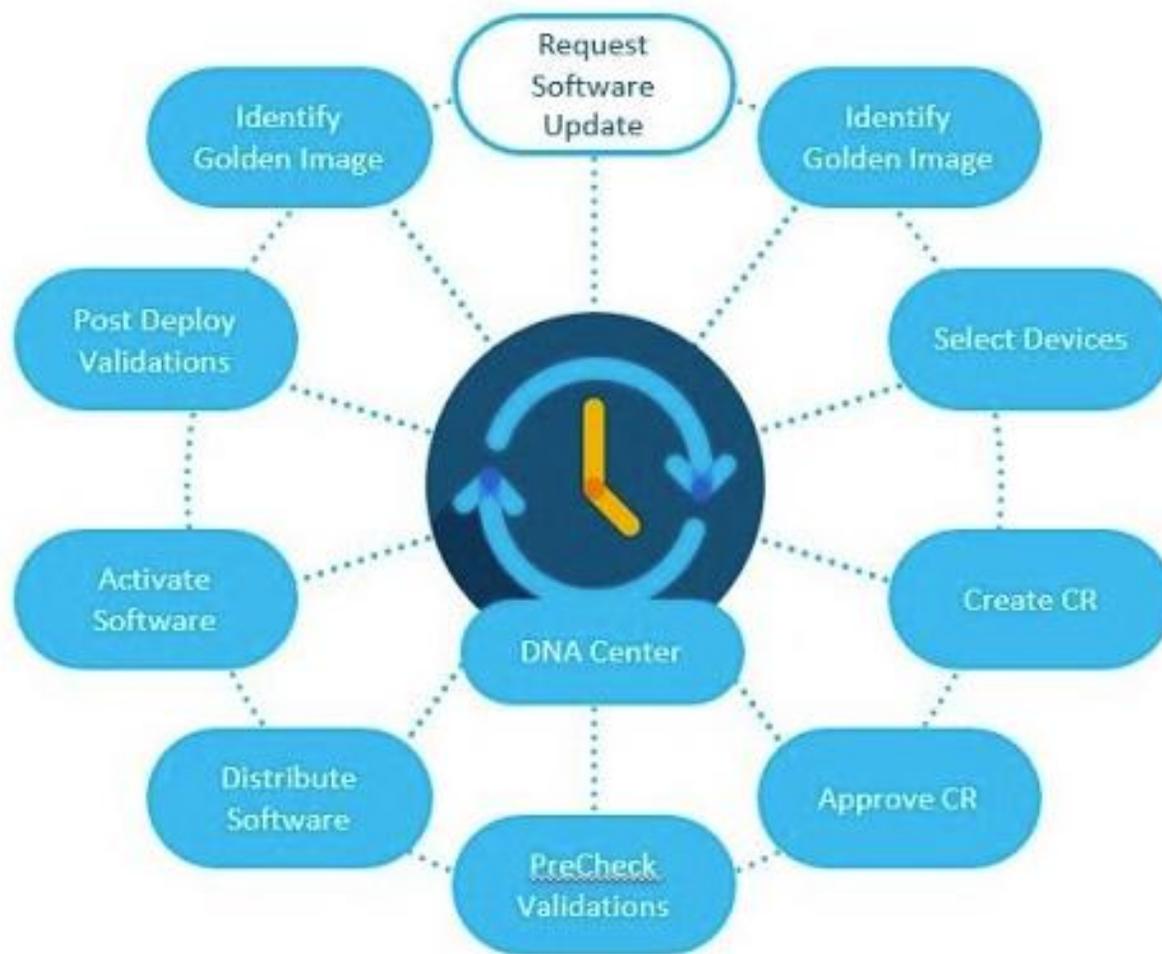


Herausforderung: „Das ganze Wochenende updaten...hervorragend!“



Lösung: DNA-Center Software Image Management

Use Case: Software Updates



Automate your software upgrade cycle

Use Case: SDA Segmentierung



Herausforderung: „Segmentierung? Gern, aber wie?“



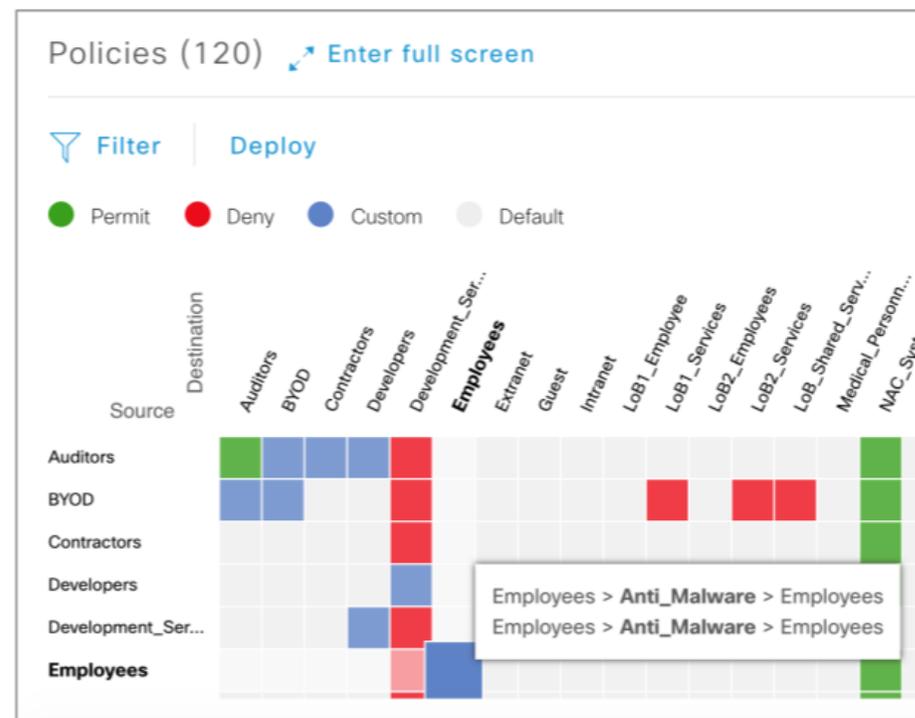
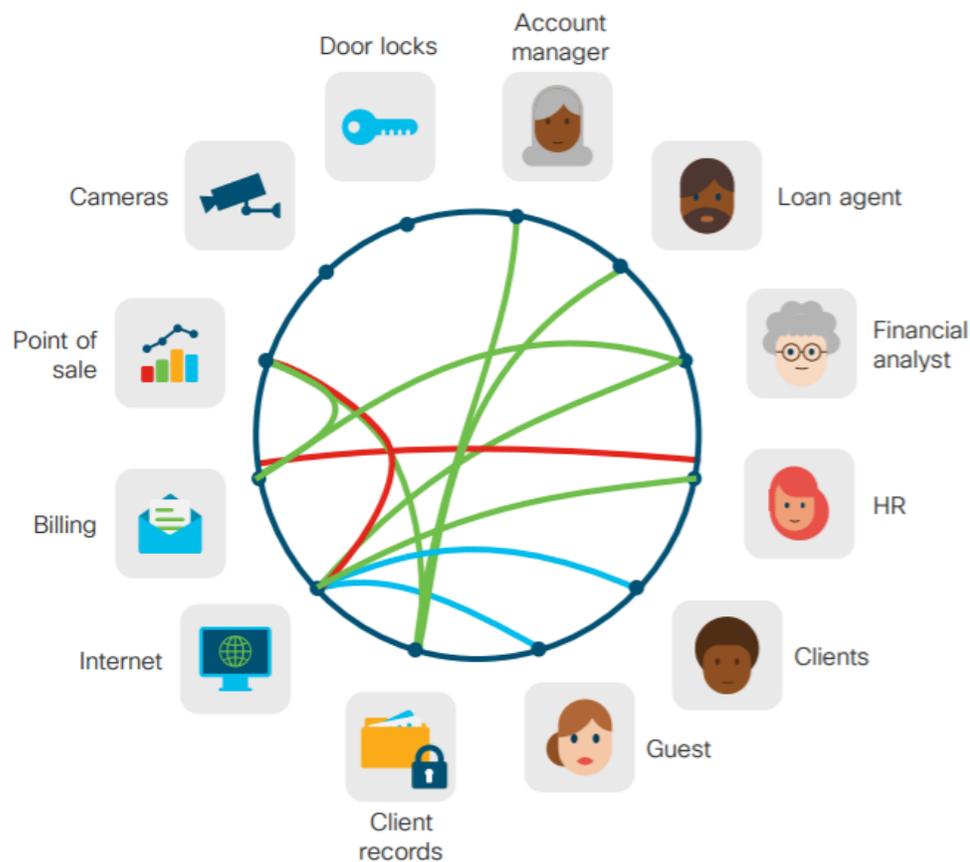
Lösung: SD-Access Segmentierung

Angriffsfläche verkleinern!



Macro-Segmentation and Micro-Segmentation

Group Based Access Control



Use Case: Assurance



Herausforderung: „Wo hängt der PC gleich wieder dran?“



Lösung: DNA-Center Assurance

Cisco DNA Assurance

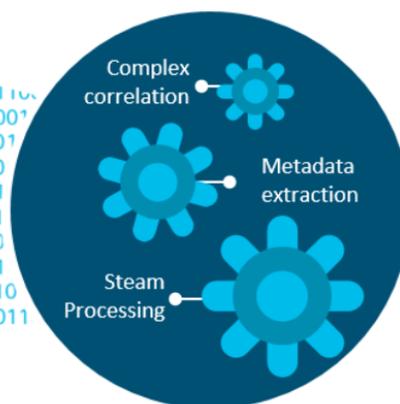
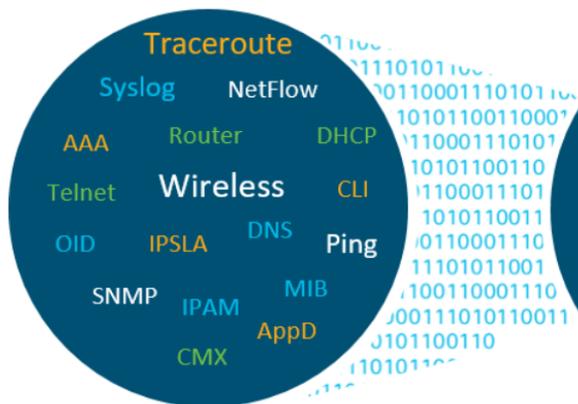
From network data to business insights

Network telemetry
contextual data

Complex event
processing

Correlated
insights

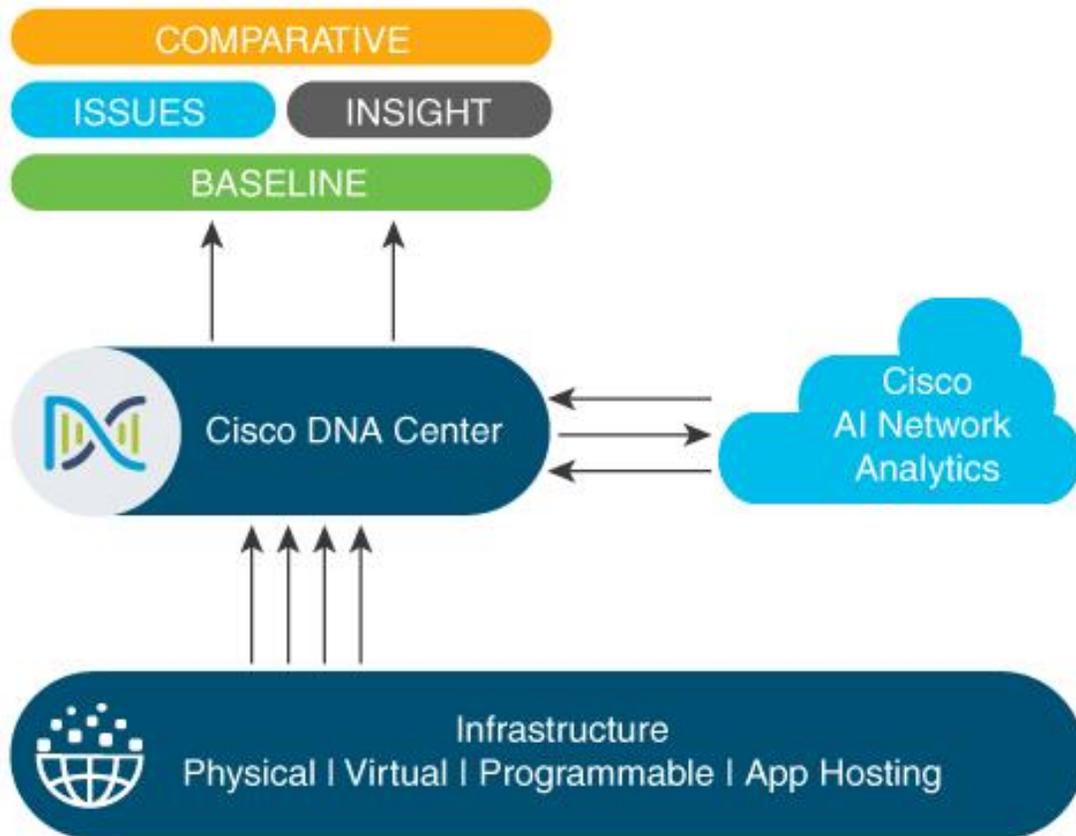
Suggested
remediation



Everything as a sensor

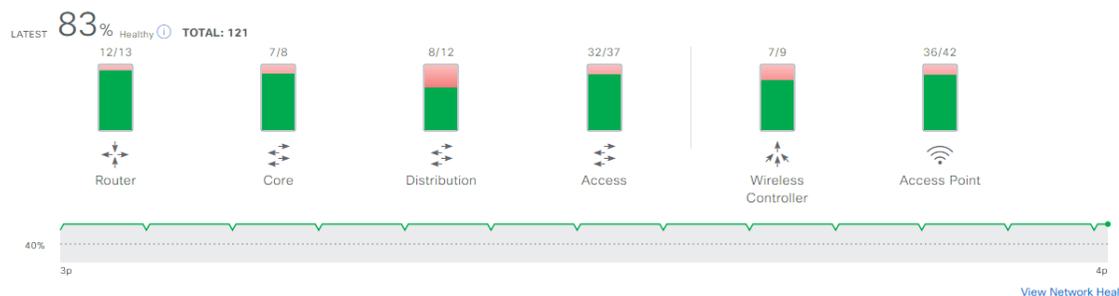
Over 150 actionable insights

Clients | Applications | Wireless | Switching | Routing

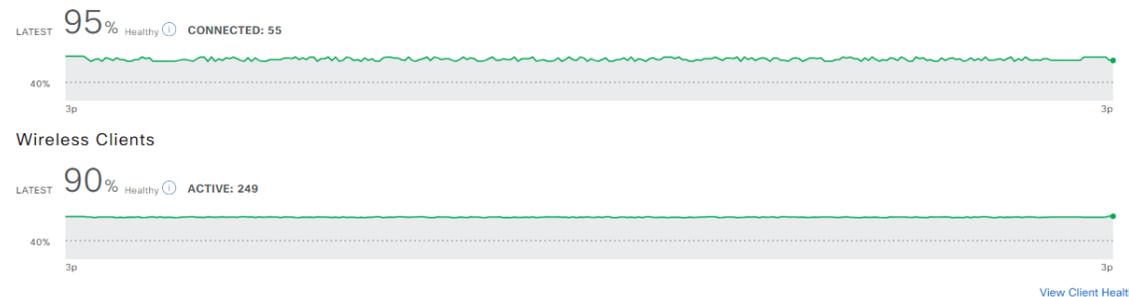


Actions

Network Devices



Wired Clients



Site Analytics ⓘ

Data For: Jun 23, 2024 12:30 PM - Jun 24, 2024 12:30 PM

Onboarding Attempts ⓘ

97%

1. San Jose (24%)

Onboarding Duration ⓘ

95%

1. San Jose (24%)

Connection Speed ⓘ

71%

1. San Jose (71%)

Roaming Attempts ⓘ

99%

1. San Jose (62%)

Roaming Duration ⓘ

96%

1. San Jose (62%)

[View Site Analytics](#)

Network Services ⓘ

AAA (8 SERVERS)



DNS (1 SERVER)



DHCP (6 SERVERS)



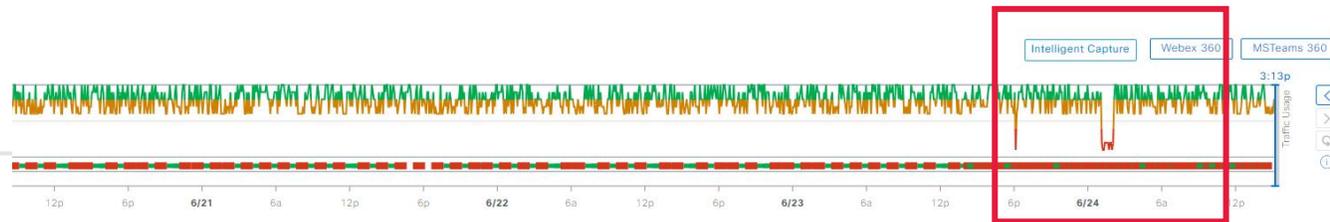
Client / Client 360

Gordon.Thomson-iPad

7 Days

Time Range

3 Hours 24 Hours 7 Days



Jun 17, 2024 3:13 PM - Jun 24, 2024 3:13 PM

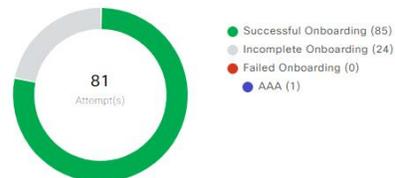
Device: Apple-iPad OS: Apple-iPad MAC: 6C:19:C0:BD:87:C7 IPv4: 10.30.100.41 IPv6: fe80::4aa:40a6:6cf8:4ea2 L3 Virtual Network: -- L2 Virtual Network: -- VLAN ID: 120 Status: Connected Capability: 11ac Last seen: Jun 24, 2024 3:20:51 PM Connected Network Device: AP4800 SSID: c9800AP11AC [View All Details](#)

Issues Onboarding Path Trace Application Experience Device Info Connectivity RF iOS Analytics Event Viewer

Summary Jun 23, 2024 3:13 PM - Jun 24, 2024 3:13 PM

- Onboarding failed during Authentication (1 out of 1), due to 'Auth Key Exchange Timeout' (1)
- Roaming failed during Authentication (4 out of 4), mostly due to 'Auth Key Exchange Timeout' (3)

Onboarding



[View Details](#)

Roaming



[View Details](#)

Connectivity

RF QUALITY

RSSI 93% of the time is Good
SNR 100% of the time is Good

[View Details](#)

TRAFFIC

Retries 10% of the data traffic
Data Rate 100% of the time is Good

Issues (4)

P1 Application Network Latency for Application 'webex-meeting' is Above the Threshold Value of 262ms. Instance Count: 45

Jun 24, 2024 3:20 PM



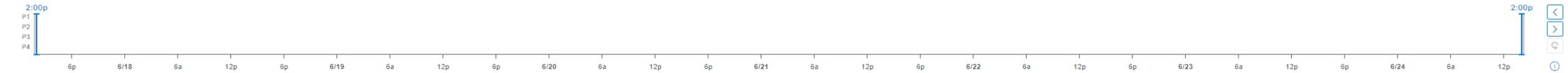
Use Case: Assurance & AI/MR



Issues ▾ Events

Global 7 Days ▾

Jun 17, 2024 2:00 PM - Jun 24, 2024 2:00 PM



Most Impacted Areas by Issue Priority: Global

San Jose: 431 P1 | 2328 Open

San Francisco: 49 P1 | 185 Open

All | P1: 482 | P2: 553 | P3: 1582 | P4: 7 | AI-Driven: 5

Total Open: 2624

Export

Search Table

Priority ▲	Issue Type ▲	Device Role	Category	Issue Count ▼	Site Count (Area)	Device Count	Last Occurred Time ▼
P1	Fabric Devices Connectivity - ISE Server	BORDER ROUTER	Connected	48	1	1	Jun 24, 2024 1:32 PM
P1	WLC unreachable	WLC	Availability	47	1	1	Jun 24, 2024 1:26 PM
P1	Fabric Devices Connectivity - Control Border Underlay	BORDER ROUTER	Connected	47	1	1	Jun 24, 2024 1:24 PM
P1	Switch unreachable	BORDER ROUTER	Availability	57	1	1	Jun 24, 2024 1:22 PM
P1	Fabric Devices Connectivity - DHCP Underlay	BORDER ROUTER	Connected	47	1	1	Jun 24, 2024 1:10 PM
P1	Fabric Devices Connectivity - DNS Underlay	BORDER ROUTER	Connected	69	1	1	Jun 24, 2024 1:06 PM

[BGP session Status to Peer Device](#) / [Issue Instance](#)

P1 BGP v4 neighborship on Fabric Border 'hzb-vt0_sw-bn01.acp.de' in Fabric Site 'Global/Hauzenberg/Brueckenstr' with '172.28.153.210' is down ✕

Status: Open ▾Issue Profile: global [Edit Issue Settings](#)

INSIGHTS

BGP v4 neighborship on Fabric Border 'hzb-vt0_sw-bn01.acp.de' in 'LISP/BGP' Fabric Site 'Global/Hauzenberg/Brueckenstr' with '172.28.153.210' is down.

Device [hzb-vt0_sw-bn01.acp.de](#)

Time Jul 3, 2024 11:27 AM

Location Global/Hauzenberg/Brueckenstr/EG

Fabric Site Global/Hauzenberg/Brueckenstr

INITIAL ASSESSMENT

-- Impacted Clients

Problem Details

Suggested Actions

Suggested Actions (3)

[Preview All](#)

> 1 Verify the BGP session status.

[Run](#)

> 2 Verify reachability to the BGP neighbor

[Run](#)

> 3 If you are unable to resolve the issue, contact Cisco TAC for support.

Problem Details

Suggested Actions (3)

[Preview All](#)

Suggested Actions

1 ✓ Verify the BGP session status.

✓ Verify the BGP session status

show ip bgp ipv4 unicast summary

Success

```
show ip bgp ipv4 unicast summary
BGP router identifier 172.28.156.73, local AS number 65002
BGP table version is 773, main routing table version 773
76 network entries using 18848 bytes of memory
109 path entries using 14824 bytes of memory
12/9 BGP path/bestpath attribute entries using 3552 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
1 BGP community entries using 24 bytes of memory
```

✓ Verify the BGP session for the neighbor 172.28.153.210

show ip bgp vpv4 all neighbors 172.28.153.210

Success

```
show ip bgp vpv4 all neighbors 172.28.153.210
BGP neighbor is 172.28.153.210, vrf STAGING_VN, remote AS 65001, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active, down for never
  Last update received: n/a
  Neighbor sessions:
    0 active, is not multiseession capable (disabled)
  Stateful switchover support enabled: NO for session 0
```

„Was man nicht im Kopf hat, hat man im DNAC!“



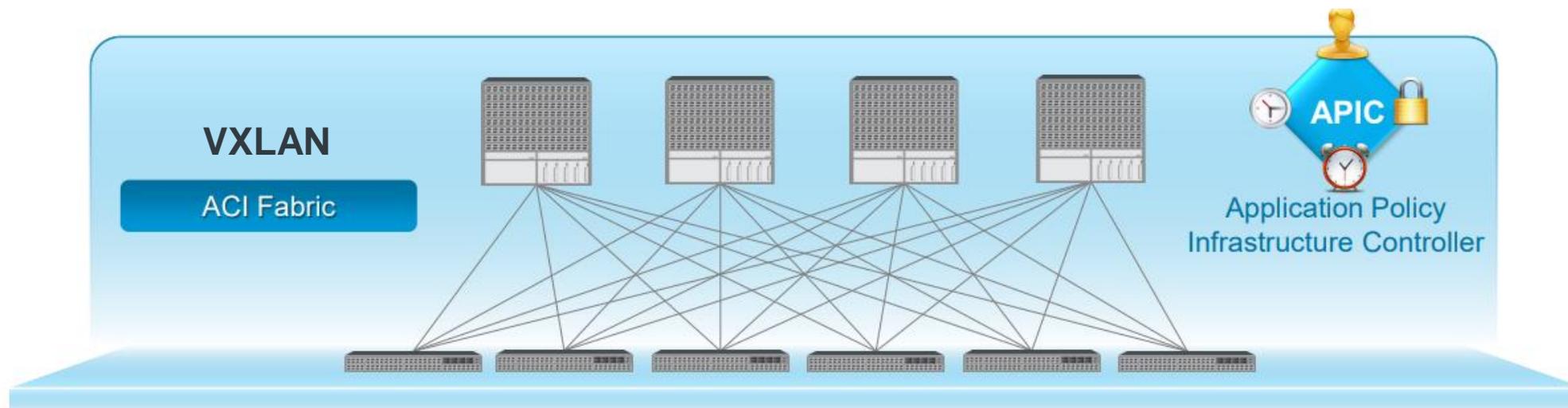
„Dass Vieles einfach über eine Oberfläche betreut werden kann, unterstützt logischerweise beim Troubleshooting und macht es effizienter.“

„Durch die Mikrosegmentierung ist es für uns sehr einfach Geräte diverser Hersteller im gleichen Netz voneinander zu separieren und gezielt Freischaltungen zu machen.“

„Von der Assurance bin ich ziemlich begeistert, es kommt ja doch hin und wieder vor, dass ein Client ein Netzwerkproblem hat und da können wir super nachvollziehen, wo das Problem ist bzw. sein könnte.“

03

SD-Datacenter (Cisco ACI)



Georedundates Datacenter

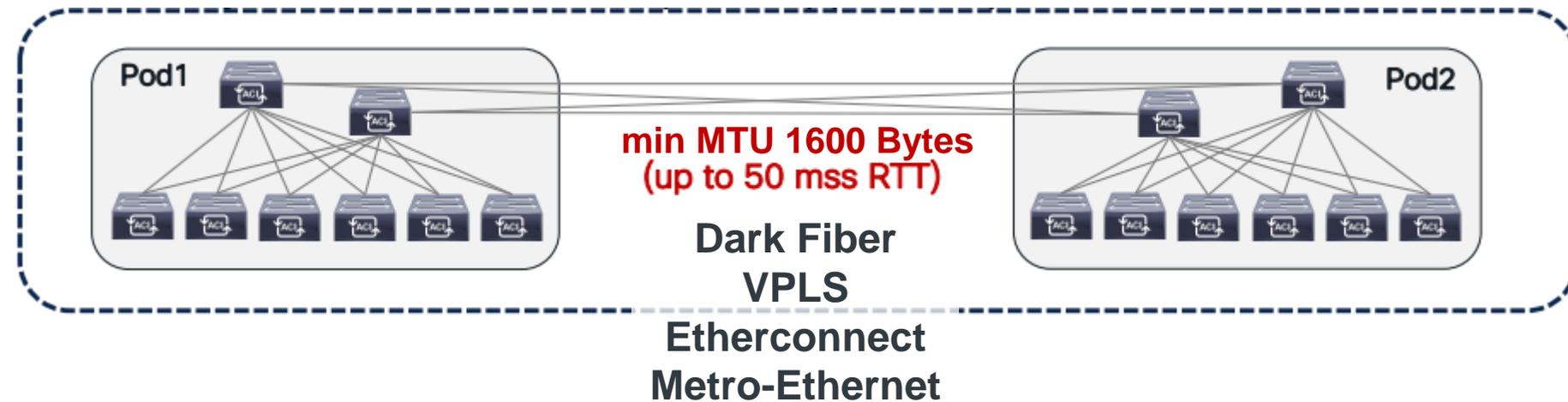
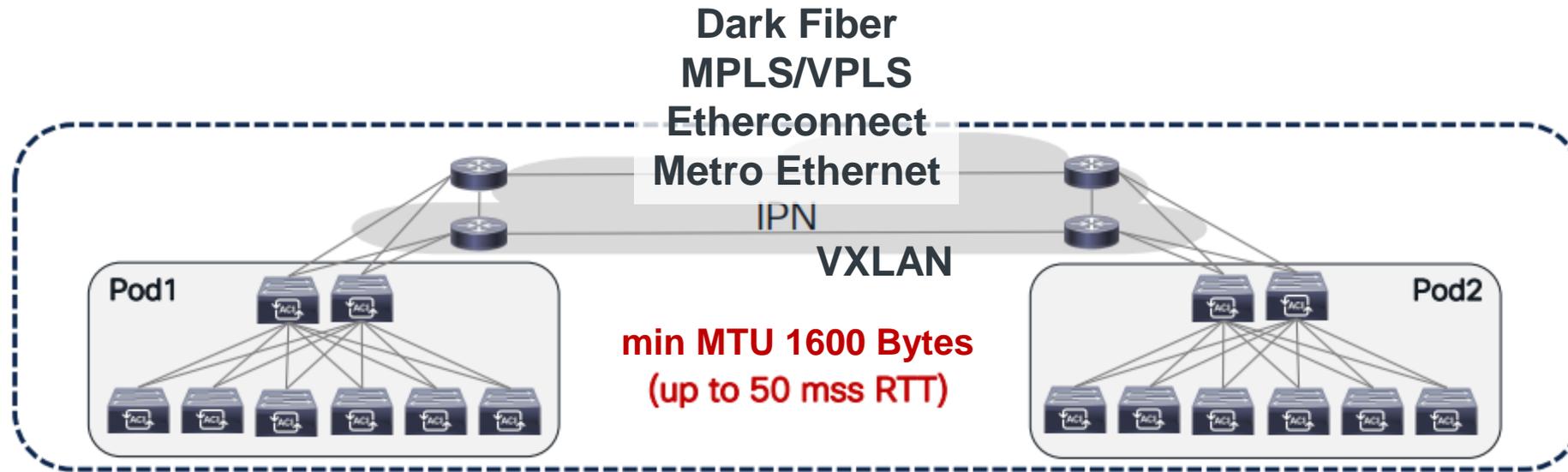


?

Dark Fiber
Etherconnect
MPLS
Metro Ethernet

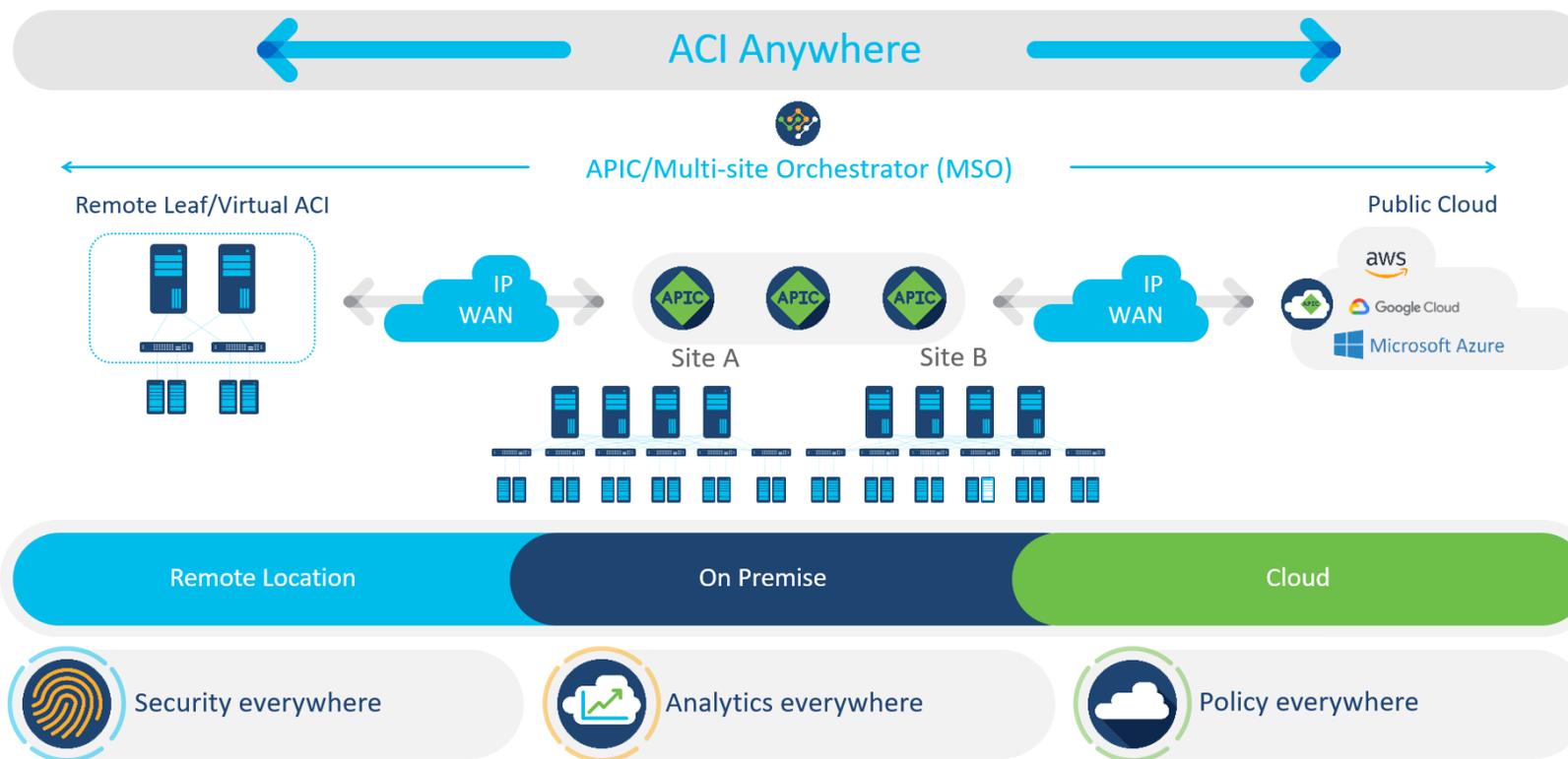


Georedundates Datacenter (ACI Multipod)

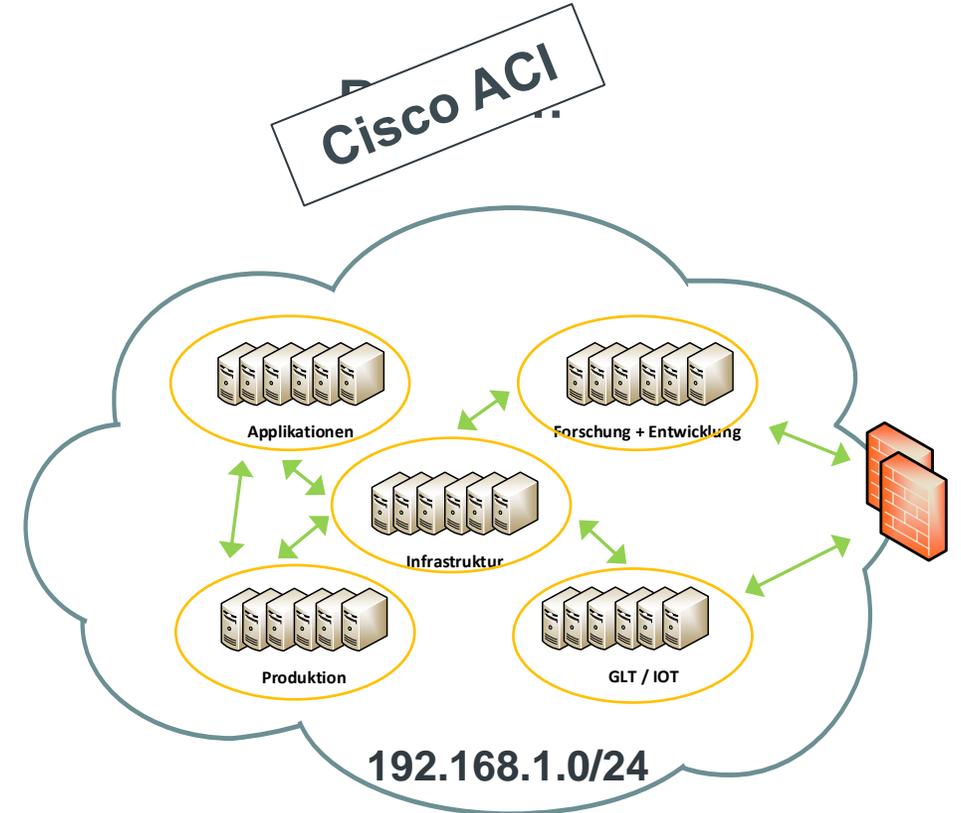
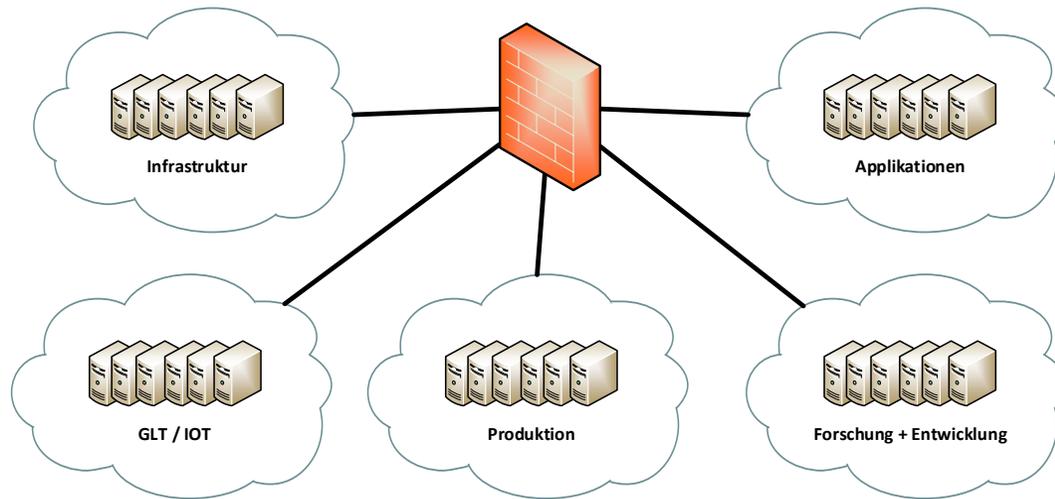


Cisco ACI Anywhere

Any Workload, Any Location, Any Cloud



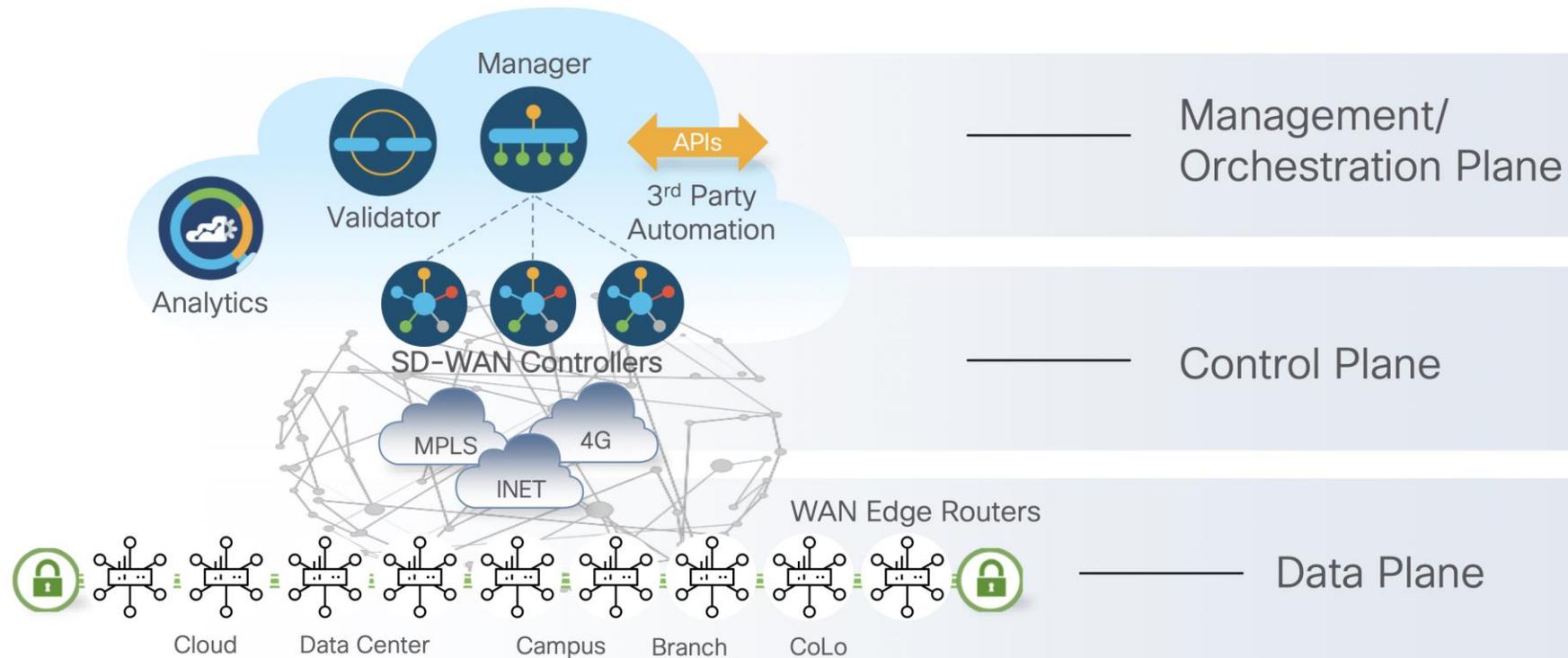
Expectation...



04

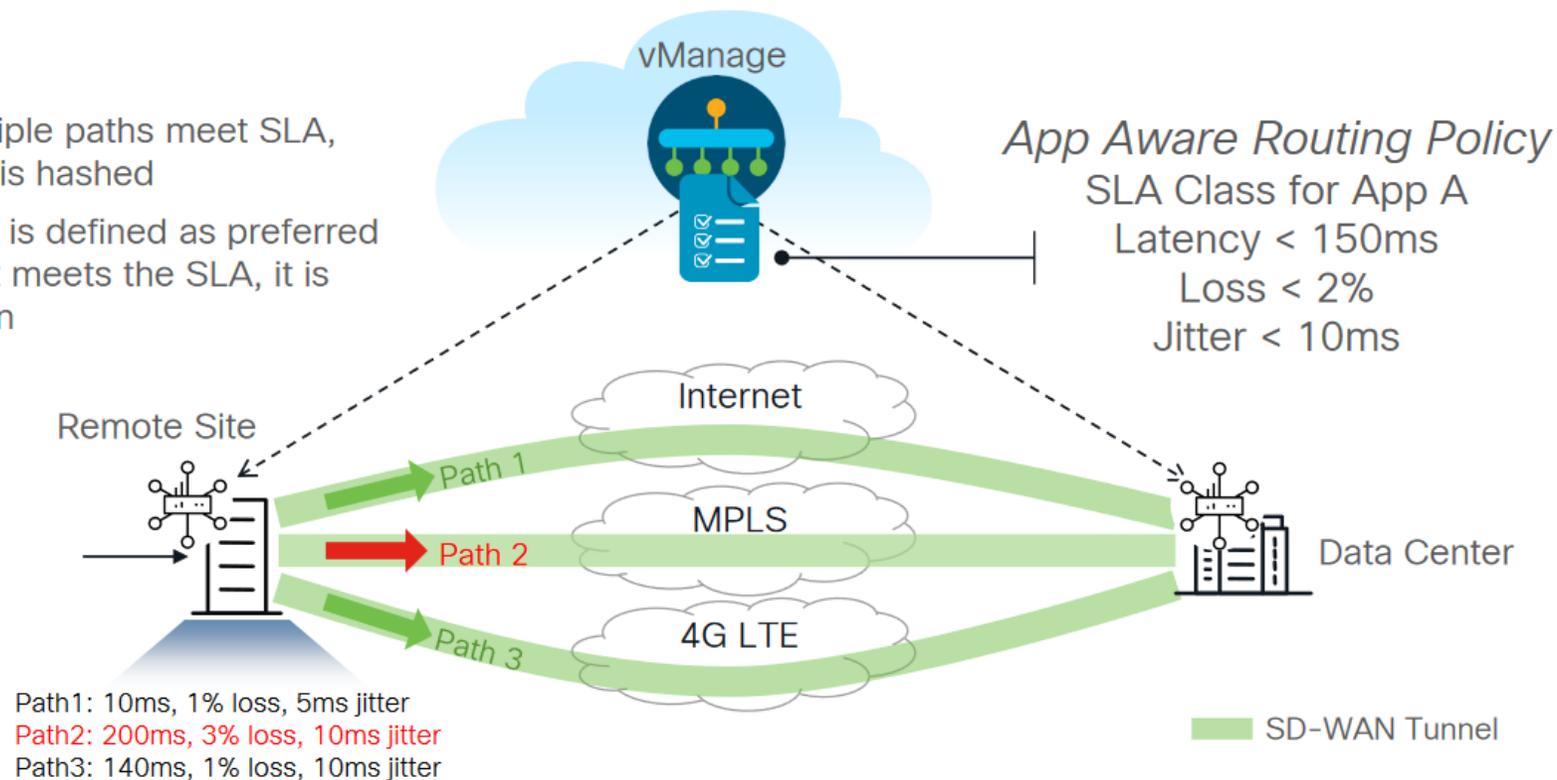
SD-WAN (Cisco SD-WAN)

Cisco Catalyst SD-WAN

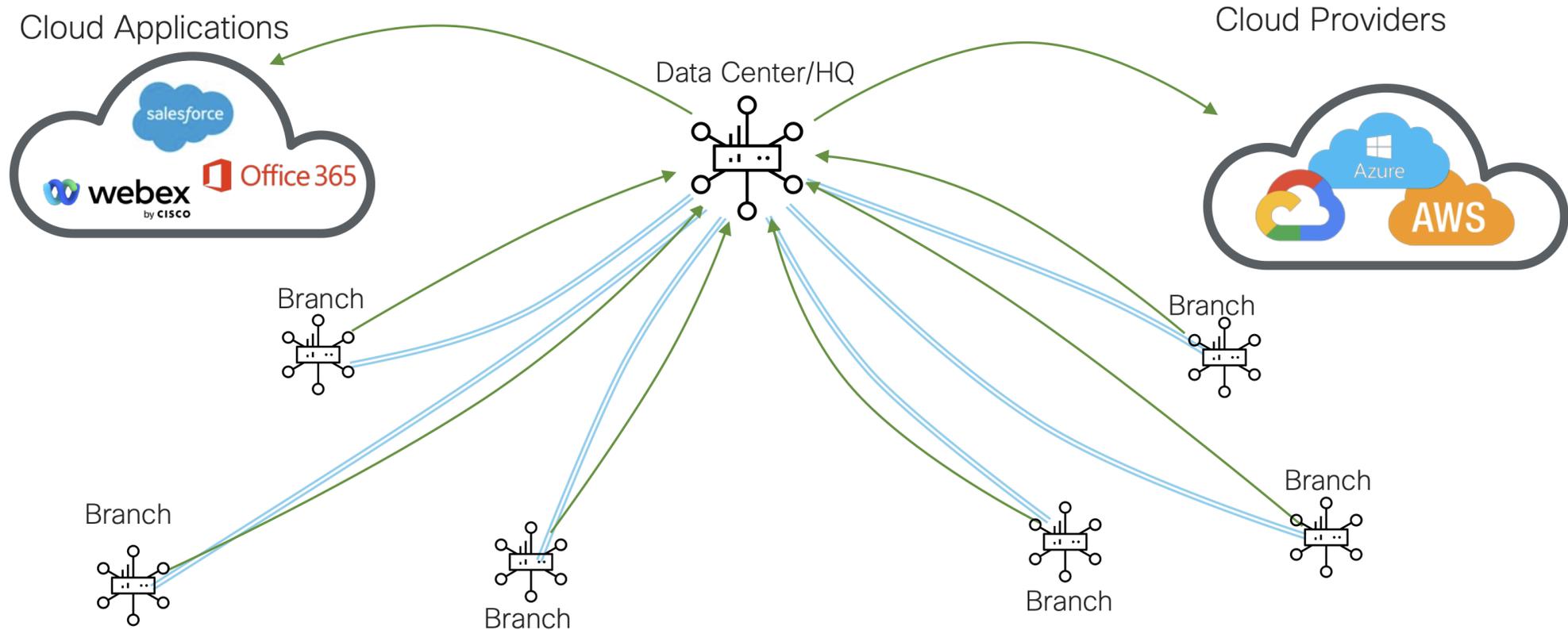


Application Aware Routing

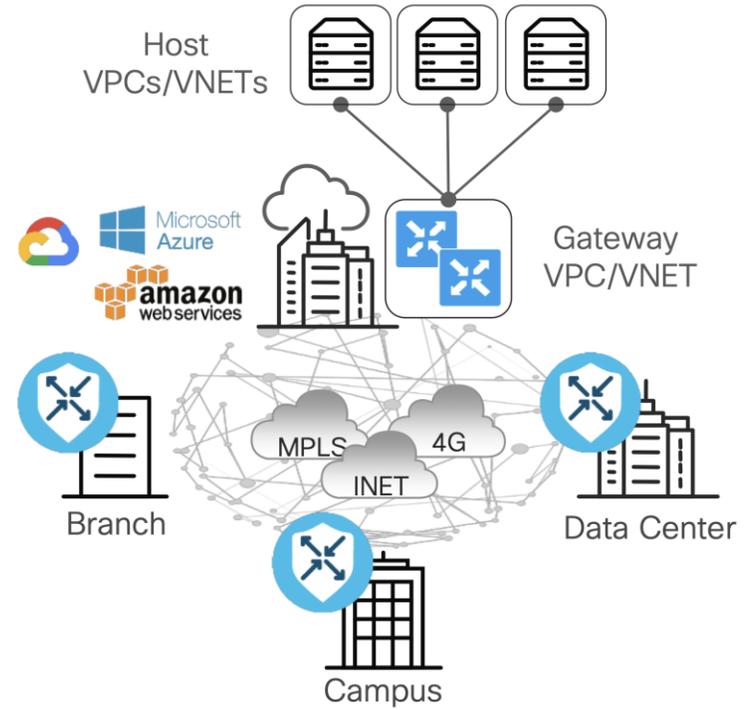
- If multiple paths meet SLA, traffic is hashed
- If path is defined as preferred AND it meets the SLA, it is chosen



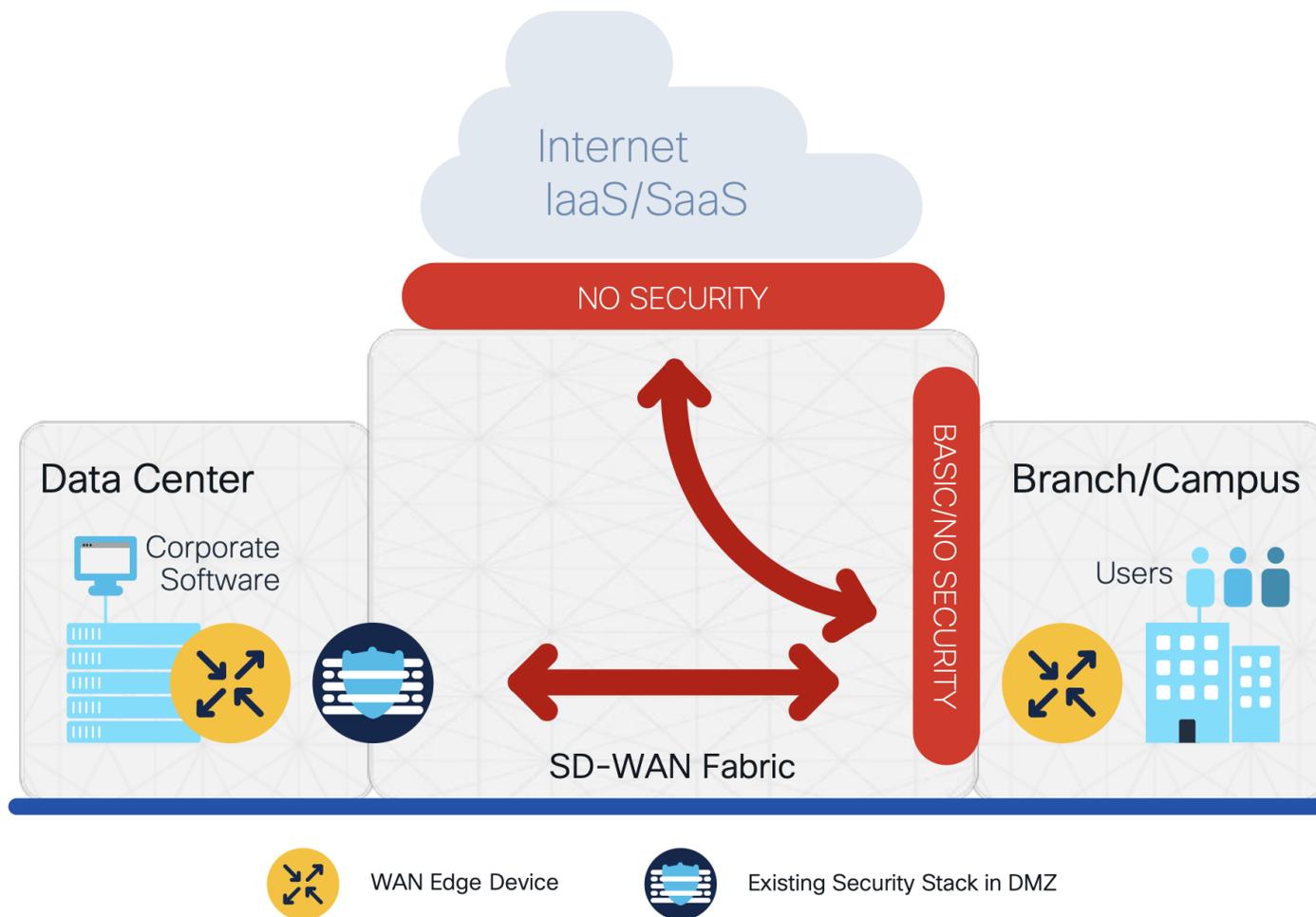
SaaS / IaaS



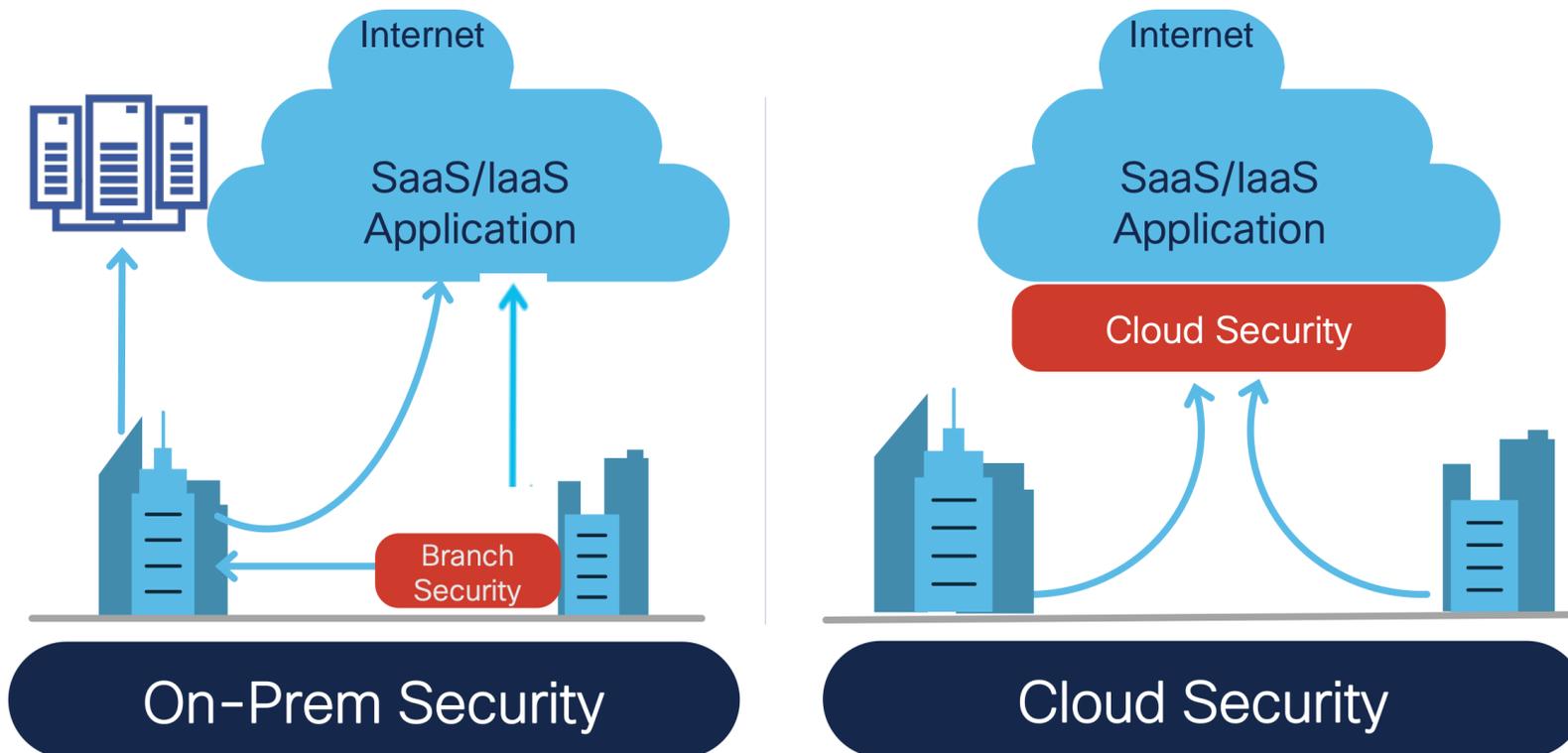
Cloud On Ramp for SaaS / IaaS

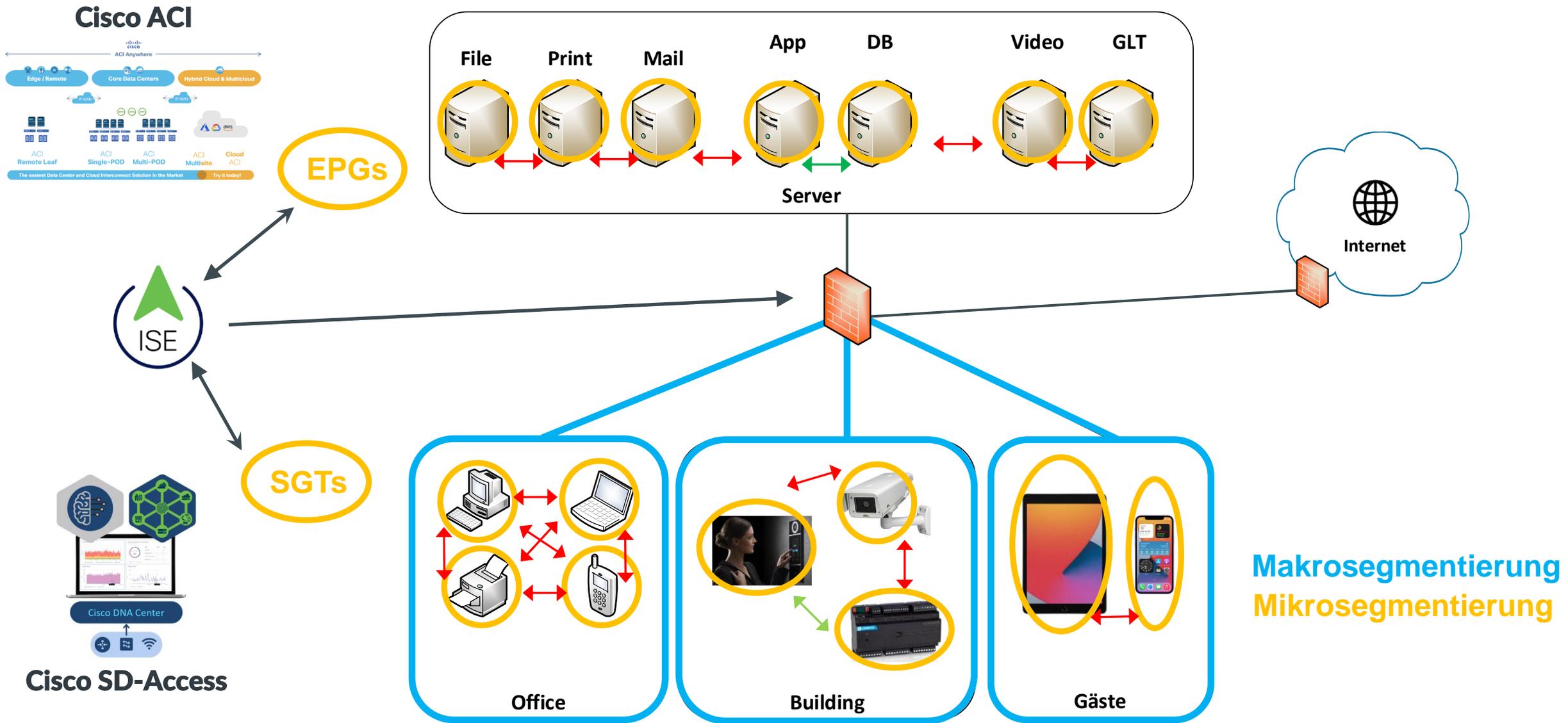


Direct Internet Access (DIA)

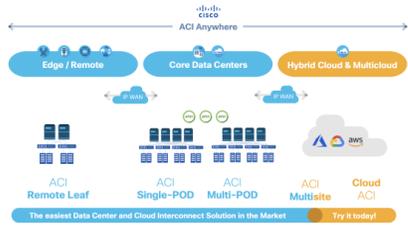


Direct Internet Access (DIA)





Cisco ACI



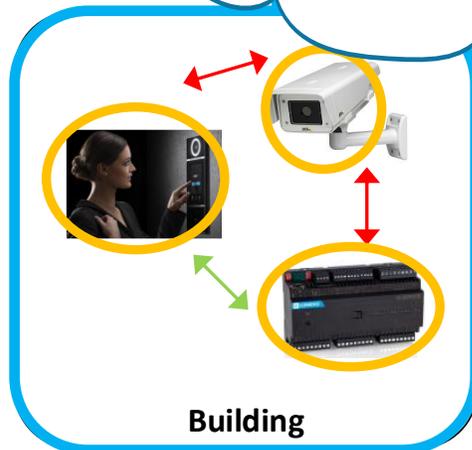
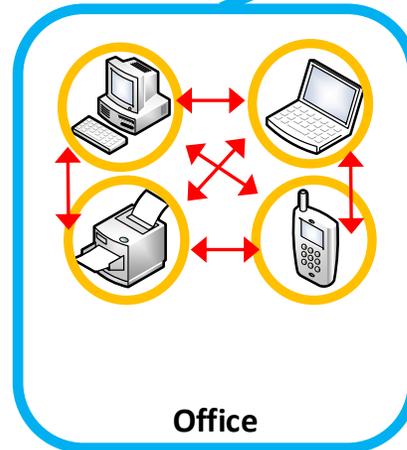
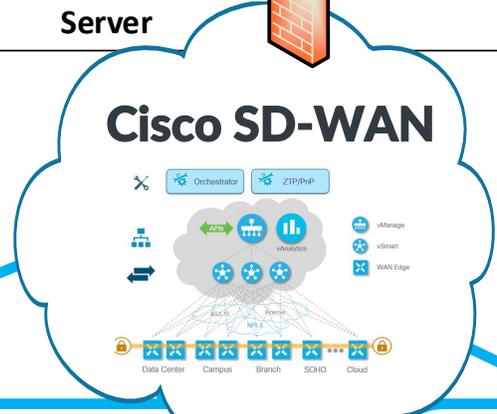
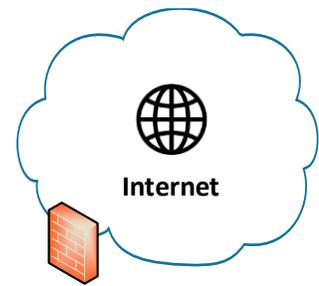
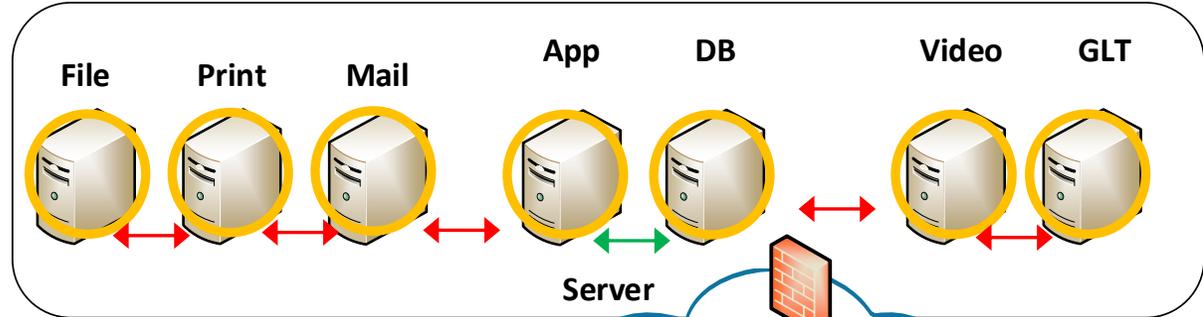
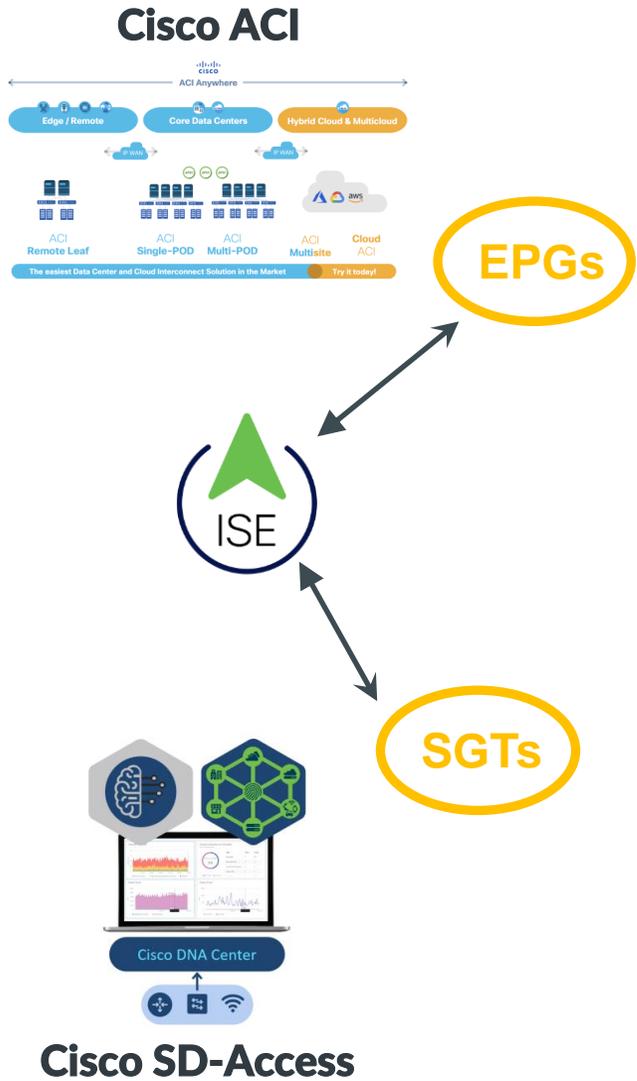
EPGs

SGTs

Cisco SD-Access

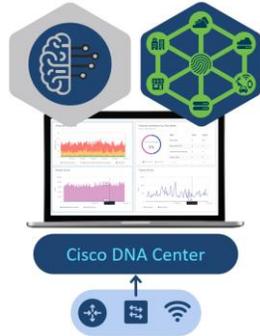
Makrosegmentierung
Mikrosegmentierung

Cisco Multidomain Segmentation



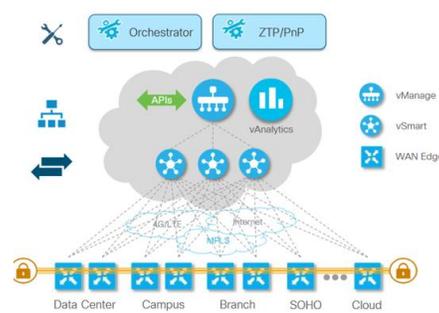
Makrosegmentierung
Mikrosegmentierung

Cisco SD-Access



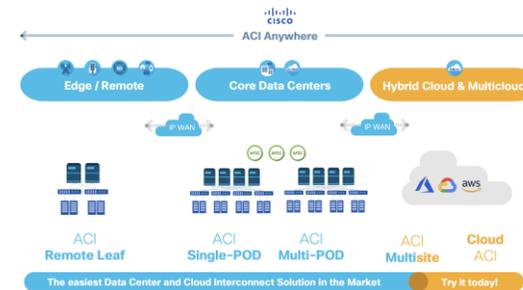
Campus

Cisco SD-WAN



WAN

Cisco ACI



Datacenter / Cloud

ACP Professional Services + Managed Services (24x7)

- Automatisierung und Compliance
- CVE-Management + Updates
- Mikrosegmentierung
- Applikationsbasiertes Routing
- Security für lokalen Internetbreakout
- Flexibler DCI für georedundantes DC
- Seamless Public Cloud Integration

- höhere IT-Sicherheit / weniger Risiken
- höhere Compliance
- bessere Konnektivität und Applikationsperformance
- gesteigerte Anwenderproduktivität
- geringere Betriebskosten



**Fragen?
Antworten!**