

Create. Connect. Control.



AnyWeb Practice Circle: Cisco ISE verbindet ACI und SDA

Wim van Moorsel

Fabian Aeppli

Maria Koceba

Edi Layritz



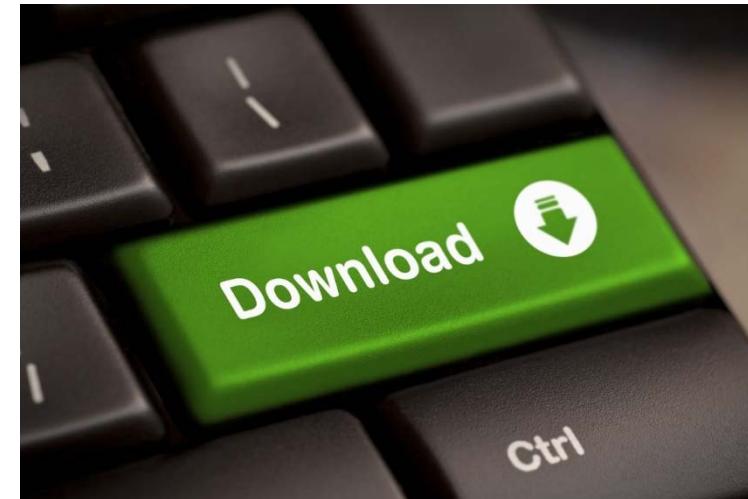
End-to-End

A horizontal double-headed green arrow spanning the distance between the Campus and Data Center icons.

Präsentationen

Die Präsentationen stehen nach der Veranstaltung auf der AnyWeb Homepage zum Download bereit:

<https://www.anyweb.ch/events/>



Agenda Practice Circle, 30. Oktober 2017

- **Begrüßung und Einführung** 13:30
- Use case: Segmentierung und Zonierung 13:45
- Labor Aufbau: End-zu-End Segmentierung 14:00
- DNA/SDA Einstieg 14:30
- Kurze Pause 14:45
- Einführung DNA Center mit Demo 15:00
- ACI vergleichbar mit SDA 15:30
- End-zu-End Geschichte mit DNA 15:45
- DNA Readiness (Migration) 16:00
- Networking und Apéro 16:15
 - Austausch mit den Spezialisten

Setup

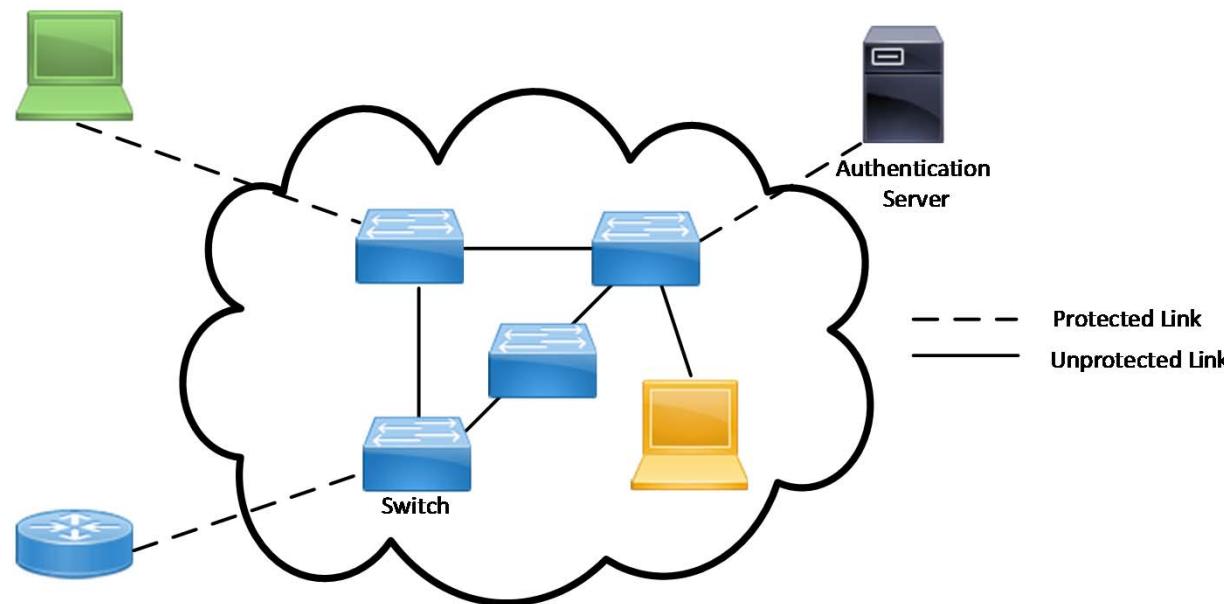
End-2-End Segmentierung mit Cisco TrustSec

Maria Koceba

Source	Destination				
	Employee	Suppliers	App Servers	Shared Services	Non-Compliant
Employee	✓	✗	✓	✓	✗
Suppliers	✗	✓	✗	✓	✗
App Servers	✓	✗	✓	✗	✗
Shared Services	✓	✓	✗	✓	✗
Non-Compliant	✗	✗	✗	✗	✗

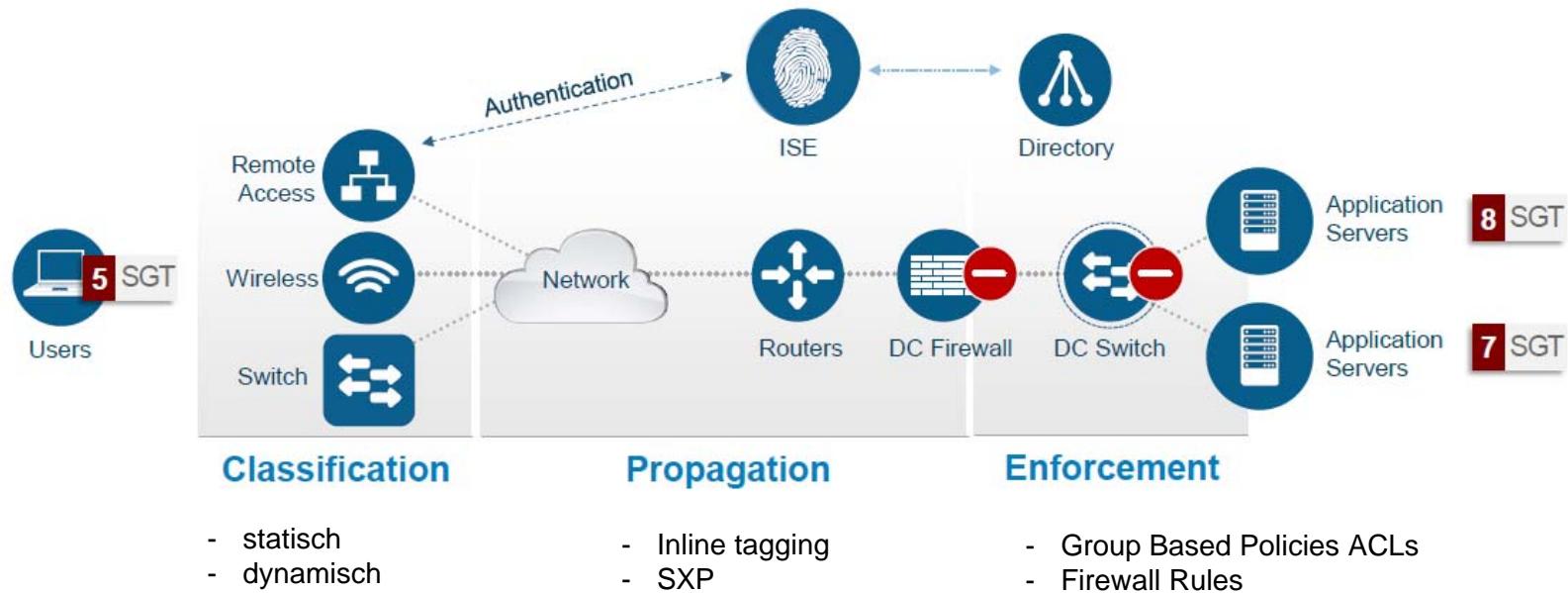
Cisco TrustSec

- Authentisierte Netzwerkinfrastruktur
- Rollenbasierte Zugriffskontrolle
- Sichere Kommunikation mit L2 Encryption

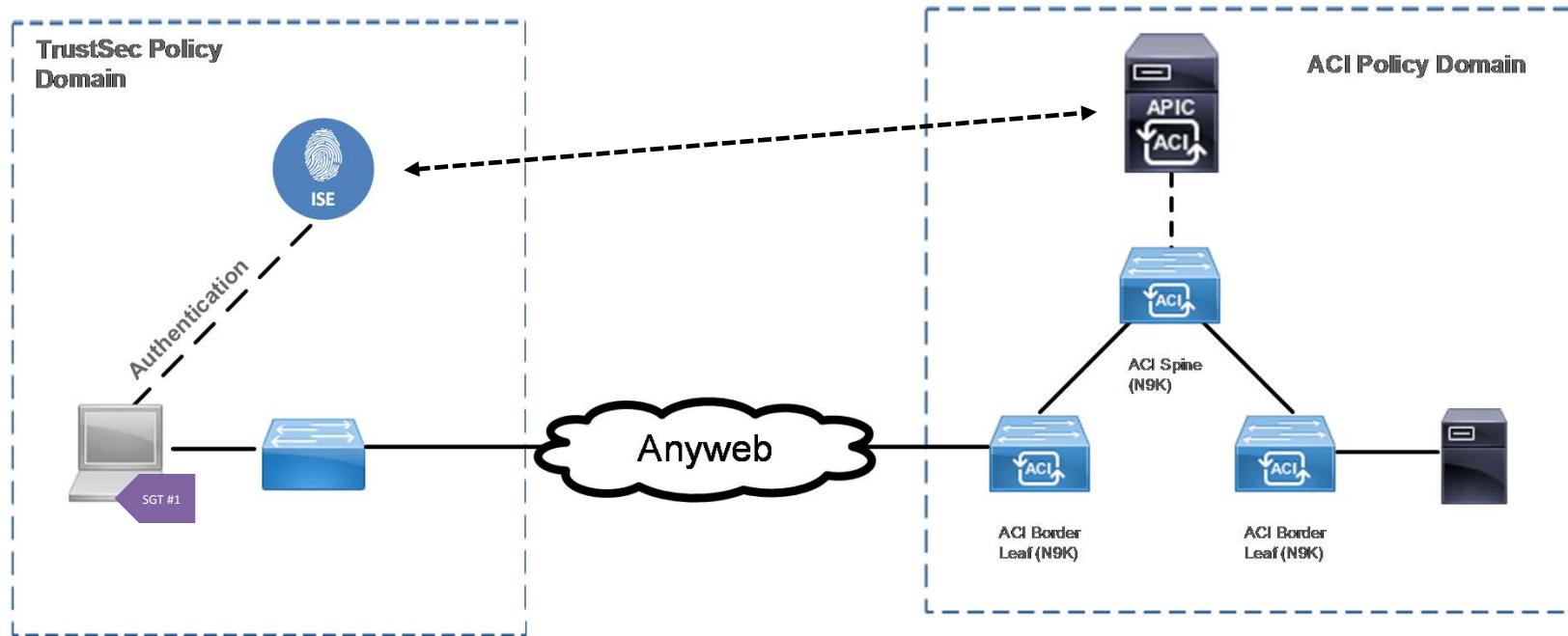


Rollenbasierte Zugriffskontrolle

- Die Lösung ist Netzwerktopologie unabhängig
- basiert auf Security Group Tags – einer Software definierten Segmentierung (SDN)



Labor Aufbau



1. Anbindung Switch – ISE (mit IBNS 2.0)
2. Anbindung ISE – ACI
3. Aufbau von TrustSec Domain
4. Klassifizierung

1. Anbindung Switch - ISE

The screenshot shows the ISE web interface for managing network devices. In the center, there's a configuration form for a device named 'SW15' with IP address '1.1.1.1'. The 'RADIUS Authentication Settings' section is expanded, showing fields for Protocol (set to RADIUS), Shared Secret (redacted), KeyWrap, Key Encryption Key, Message Authenticator Code Key, Key Input Format (ASCII selected), and CoA Port (1700). A red arrow originates from this section and points to a terminal window on the right.

- Switch in ISE erfassen
- RADIUS Konfiguration auf dem Switch

```

sw15-sda#sh run | in aaa
aaa new-model
aaa group server radius NAC
aaa authentication login default local
aaa authentication enable default none
aaa authentication dot1x default group NAC
aaa authorization network default group NAC
aaa authorization network TRUSTSEC group NAC
aaa accounting identity default start-stop group NAC
aaa server radius dynamic-author
aaa session-id common
match result-type aaa-timeout
match result-type aaa-timeout
event aaa-available match-all
sw15-sda#sh run | in radius
aaa group server radius NAC
ip radius source-interface Vlan90
aaa server radius dynamic-author
ip radius source-interface Vlan90
radius-server dead-criteria time 10 tries 2
radius-server retry method reorder
radius-server timeout 2
radius-server deadtime 5
radius server ANYISE
sw15-sda#

```

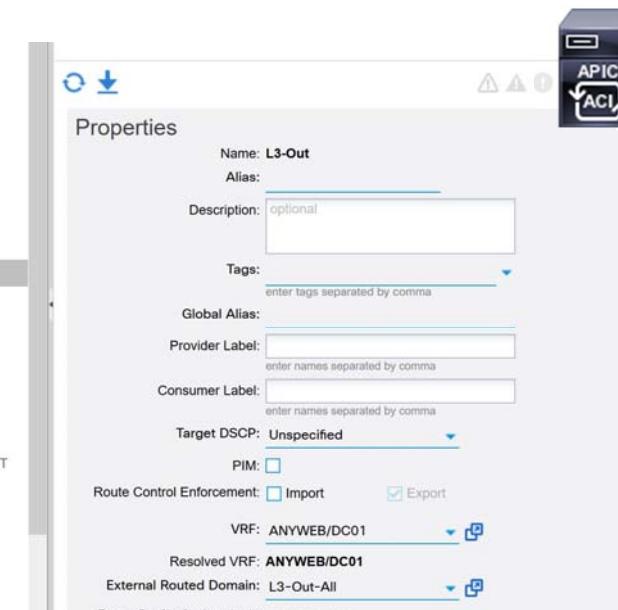
2. Anbindung ISE - ACI

The screenshot shows the ISE web interface with the following details:

- ACI Settings** section:
 - IP Address / Host name: 1.1.1.1
 - Admin name: mko
 - Admin password: (redacted)
 - Tenant name: ANYWEB
 - L3 Route network name: L3-Out
 - New SGT suffix: EPG
 - New EPG suffix: SGT
- SXP Propagation** section:
 - All SXP Domains (radio button)
 - Specific SXP Domains (radio button)
 - default

A red arrow points from the 'L3 Route network name' field to the 'Properties' dialog box on the right.

- Server Zertifikat von ACI in die ISE importieren
- Nur ein Tenant ist momentan möglich!



2. Anbindung ISE - ACI

The Cisco ISE UI shows the 'ACI Settings' section under 'TrustSec'. It includes fields for 'IP Address / Host name' (1.1.1.1), 'Admin name' (mko), 'Admin password' (redacted), 'Tenant name' (ANYWEB), and 'L3 Route network name' (L3-Out). Below this, there's a 'Naming Convention' section with 'New SGT suffix' (EPG) and 'New EPG suffix' (SGT). Under 'SXP Propagation', the 'Specific SXP Domains' option is selected, with a text input field containing 'x default'.

The table lists security groups (SG) learned from APIC, categorized by 'Learned from' (ACI). A red arrow points from the 'New SGT suffix' field in the ISE UI to the 'Name' column of the table, specifically highlighting the entry 'DMZ_MobileIP_AEPG'.

Icon	Name	SGT (Dec / Hex)	Description	Learned from
	AAAS_MgmtEPG	10026/272A	Learned from APIC. Suffix: EPG Application profile f...	ACI
	Analyzer_WiresharkEPG	10025/2729	Learned from APIC. Suffix: EPG Application profile f...	ACI
	BADGOOGLE	666/029A		
	DMZ_ExtranetEPG	10007/2717	Learned from APIC. Suffix: EPG Application profile f...	ACI
	DMZ_ISP_AEPG	10009/2719	Learned from APIC. Suffix: EPG Application profile f...	ACI
	DMZ_ISP_BEPG	10012/271C	Learned from APIC. Suffix: EPG Application profile f...	ACI
	DMZ_Lab_AEPG	10011/271B	Learned from APIC. Suffix: EPG Application profile f...	ACI
	DMZ_MgmtEPG	10006/2716	Learned from APIC. Suffix: EPG Application profile f...	ACI
	DMZ_MobileIP_AEPG	10008/2718	Learned from APIC. Suffix: EPG Application profile f...	ACI
	DMZ_MobileIP_BEPG	10015/271F	Learned from APIC. Suffix: EPG Application profile f...	ACI
	DMZ_Server_AEPG	10014/271E	Learned from APIC. Suffix: EPG Application profile f...	ACI
	DMZ_Server_BEPG	10010/271A	Learned from APIC. Suffix: EPG Application profile f...	ACI
	DMZ_SyncEPG	10016/2720	Learned from APIC. Suffix: EPG Application profile f...	ACI
	DMZ_TransitEPG	10005/2715	Learned from APIC. Suffix: EPG Application profile f...	ACI
	DMZ_WLAN_GuestEPG	10013/271D	Learned from APIC. Suffix: EPG Application profile f...	ACI
	DNA_Employee_SGT	99/0063		
	DNA_SW_SGT	15/000F		

3. Aufbau von TrustSec Domain

The screenshot shows the Cisco ISE web interface under 'Advanced TrustSec Settings'. It includes sections for Device Authentication Settings, TrustSec Notifications and Updates, and Device Configuration Deployment. Red arrows point from the 'Device Id' field ('sw15-sda'), the 'Radius Server' section, and the 'EXEC Mode Username' field ('ctsise') to three separate terminal windows displaying the generated CLI commands.

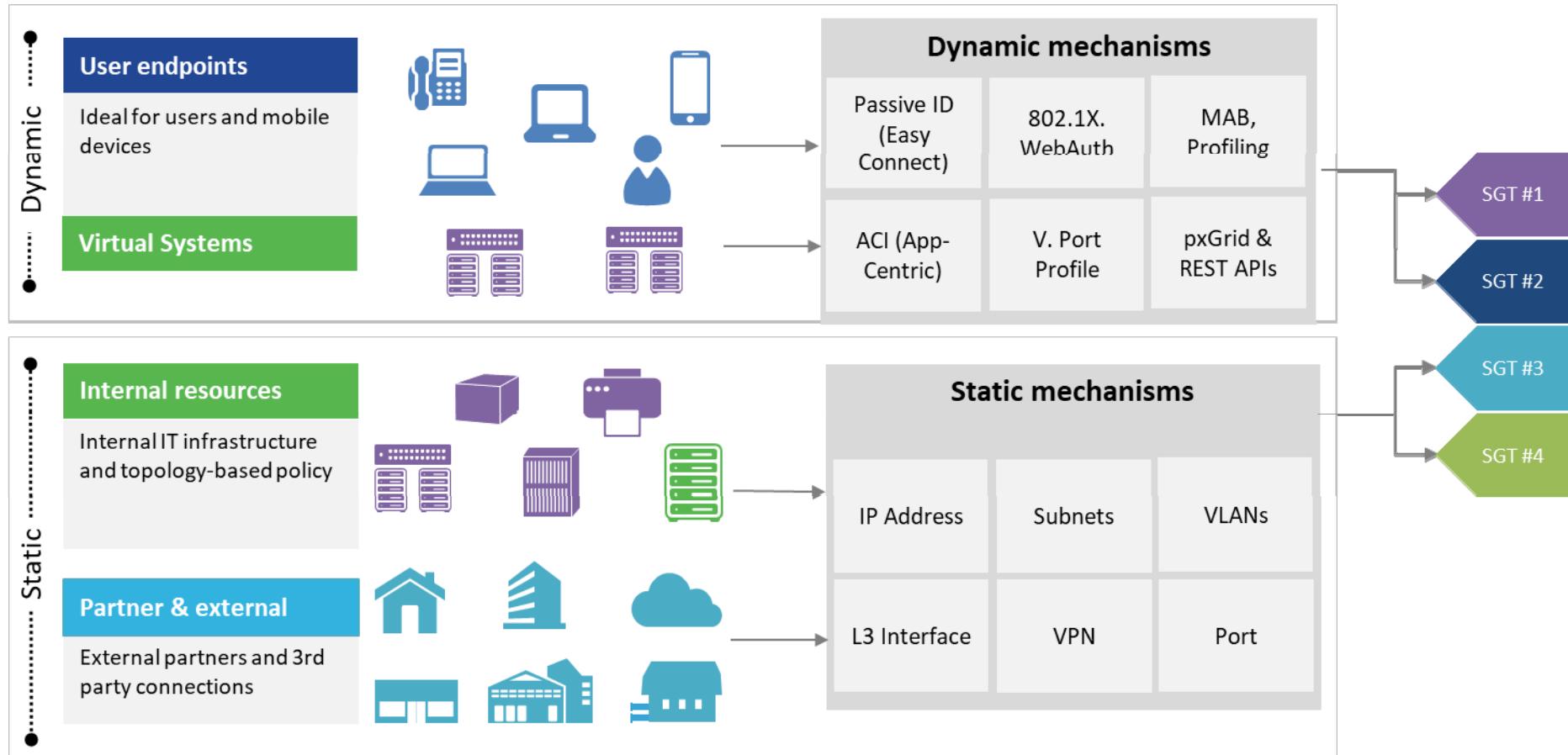
```

sw15-sda#sh run | in TRUSTSEC
aaa authorization network TRUSTSEC group NAC
cts authorization list TRUSTSEC
!
radius server ANYISE1
address ipv4 1.1.1.1 auth-port 1812 acct-port 1813
pac key CISCODNA
!
!
aaa server radius dynamic-author
client 1.1.1.1 server-key CISCODNA
!
username ctsise privilege 15 secret 5 $1$KX6X$zFs5G
!

```

- Ermöglicht Download von Environment Data (SG, SGACLs) von ISE
- Die AAA Konfiguration des Seed Devices unterscheidet sich von Non-Seed Devices

Klassifizierungsmethoden



AuthN/AuthZ Policy

Status	Name	Description	Conditions													
<input checked="" type="checkbox"/>	DNA		DEVICE:Device Type EQUALS Device Type#All Device Types#Test_Devices													
▼ Authentication Policy <div style="background-color: #f0f0f0; padding: 5px;"> <input checked="" type="checkbox"/> Default Rule (If no match) : Allow Protocols : Default Network Access and use : Internal Endpoints </div>																
▼ Authorization Policy <div style="background-color: #f0f0f0; padding: 5px;"> Exceptions (0) Standard </div>																
RADIUS (permit access + VLAN ID)																
<table border="1"> <thead> <tr> <th>Status</th> <th>Rule Name</th> <th>Conditions (identity groups and other conditions)</th> <th>Permissions</th> </tr> </thead> <tbody> <tr> <td> <input checked="" type="checkbox"/></td> <td>SDA_Test</td> <td>if DNA_Endpoints</td> <td>then DNA_Employee AND DNA_Employee_SGT</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>Default</td> <td>if no matches, then</td> <td>DenyAccess</td> </tr> </tbody> </table>					Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	 <input checked="" type="checkbox"/>	SDA_Test	if DNA_Endpoints	then DNA_Employee AND DNA_Employee_SGT	<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions													
 <input checked="" type="checkbox"/>	SDA_Test	if DNA_Endpoints	then DNA_Employee AND DNA_Employee_SGT													
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess													

```
!
interface GigabitEthernet1/0/1
switchport mode access
device-tracking attach-policy Test
no logging event link-status
authentication periodic
authentication timer reauthenticate server
access-session control-direction in
access-session port-control auto
mab
no snmp trap link-status
dot1x pae authenticator
spanning-tree portfast
spanning-tree bpduguard enable
service-policy type control subscriber PC_POLICY_INITIAL
!
```

TrustSec (Tag)

Switchport Konfiguration
mit dem IBNS 2.0

AuthN/AuthZ Results

```
sw15-sda#sh access-session int gi1/0/1 de
      Interface: GigabitEthernet1/0/1
      IIF-ID: 0x1466C5D4
      MAC Address: 047d.7b30.f062
      IPv6 Address: fe80::3d2a:7fff:2807:5da6
      IPv4 Address: 172.23.149.26
      User-Name: 04-7D-7B-30-F0-62
      Status: Authorized
      Domain: DATA
      Oper host mode: multi-auth
      Oper control dir: in
      Session timeout: N/A
      Common Session ID: AC17965300000010573F1C98
      Acct Session ID: 0x00000007
      Handle: 0xeb000006
      Current Policy: PC_POLICY_INITIAL
```

Server Policies:

Vlan Group: Vlan: 20
SGT Value: 99

Class	CACS:AC1796530000010573F1C98
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) 20
cisco-av-pair	cts:security-group-tag=0063-0
cisco-av-pair	profile-name=Unknown
LicenseTypes	Base license consumed

Authentication Details

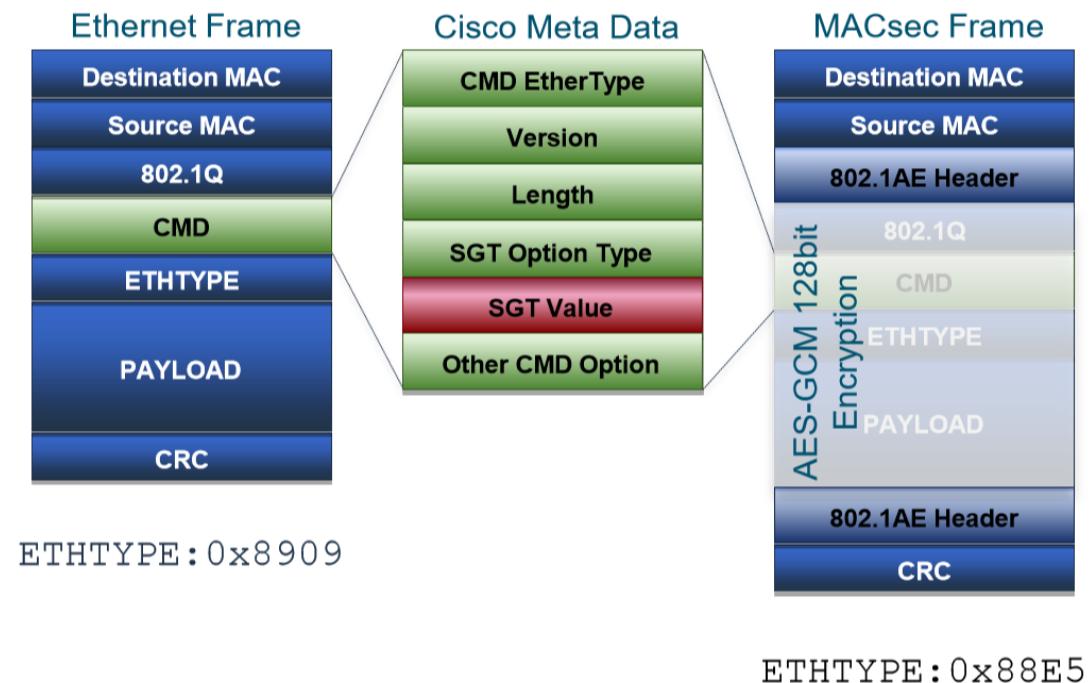


Source Timestamp	2017-10-26 07:54:35.973
Received Timestamp	2017-10-26 07:54:35.973
Policy Server	ise01
Event	5200 Authentication succeeded
Username	04:7D:7B:30:F0:62
User Type	Host
Endpoint Id	04:7D:7B:30:F0:62
Calling Station Id	04-7D-7B-30-F0-62
Endpoint Profile	Unknown
Authentication Identity Store	Internal Endpoints
Identity Group	DNA_Endpoints
Audit Session Id	AC1796530000010573F1C98
Authentication Method	mab
Authentication Protocol	Lookup
Service Type	Call Check
Network Device	SW15
Device Type	All Device Types#Test_Devices
NAS IPv4 Address	anyweb
NAS Port Id	GigabitEthernet1/0/1
NAS Port Type	Ethernet
Authorization Profile	DNA_Employee,DNA_Employee_SGT
Security Group	DNA_Employee_SGT
Response Time	9

Propagation – inline tagging

- **Vorteile:**
- **Gute Skalierbarkeit**
- **SGT Information bleibt im Data Paket**

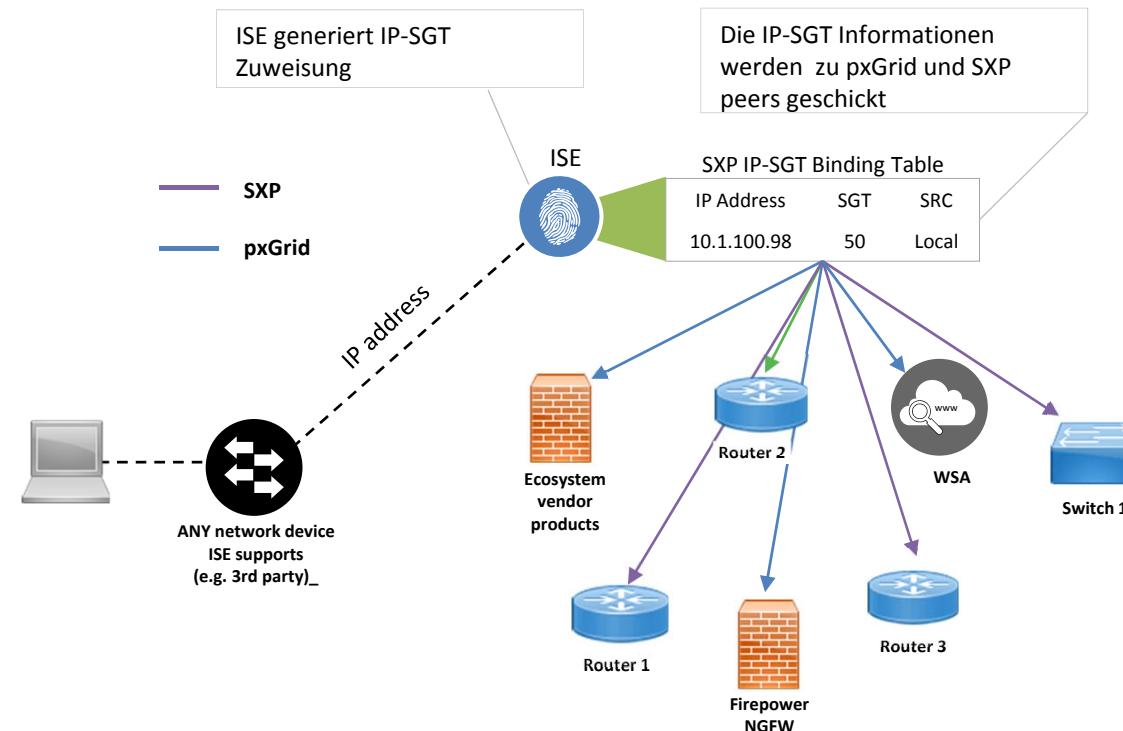
- **Zu beachten:**
- **Einfluss auf L2 Frame (MTU Grösse)**
- **Es muss durch Hardware unterstützt werden**



Propagation – SXP (SGT eXchange Protokoll)

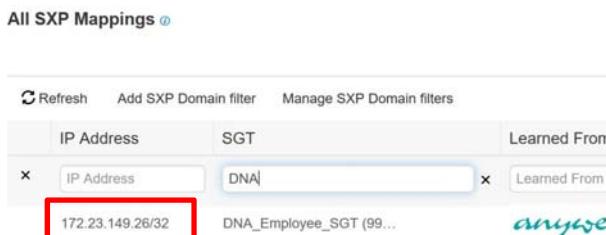
- **Vorteile:**
- **Einfach implementierbar**
- **Keine Hardware Abhängigkeit**

- **Nachteile:**
- **Eine Tabelle mehr...**
- **Skaliert nicht so gut**

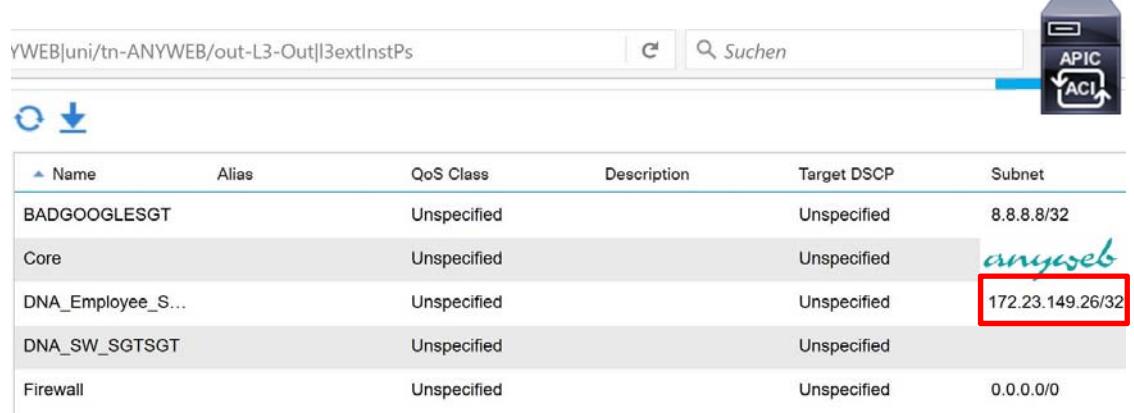


Propagation – SXP (SGT eXchange Protokoll)

- ISE erfährt IP zu SGT Zuweisung (von Switch) in AAA Accounting Paket
- IP zu SGT Informationen werden dann mittels SXP zu ACI weitergegeben.



IP Address	SGT	Learned From	Learned By	SXP Domain	PSNs
172.23.149.26/32	DNA	DNA_Employee_SGT (99...)	anyweb		



Name	Alias	QoS Class	Description	Target DSCP	Subnet
BADGOOGLES GT		Unspecified		Unspecified	8.8.8.8/32
Core		Unspecified		Unspecified	anyweb
DNA_Employee_S...		Unspecified		Unspecified	172.23.149.26/32
DNA_SW_SGTSGT		Unspecified		Unspecified	
Firewall		Unspecified		Unspecified	0.0.0.0/0

Propagation – SXP (SGT eXchange Protokoll)

```
sw15-sda#sh run | in xp
cts xp enable
cts xp default password CISCODNA
cts xp connection peer 1.1.1.1 password default mode peer speaker hold-time 0 0
```

The diagram illustrates the propagation of SGT (Switched Group Tag) information across three network components:

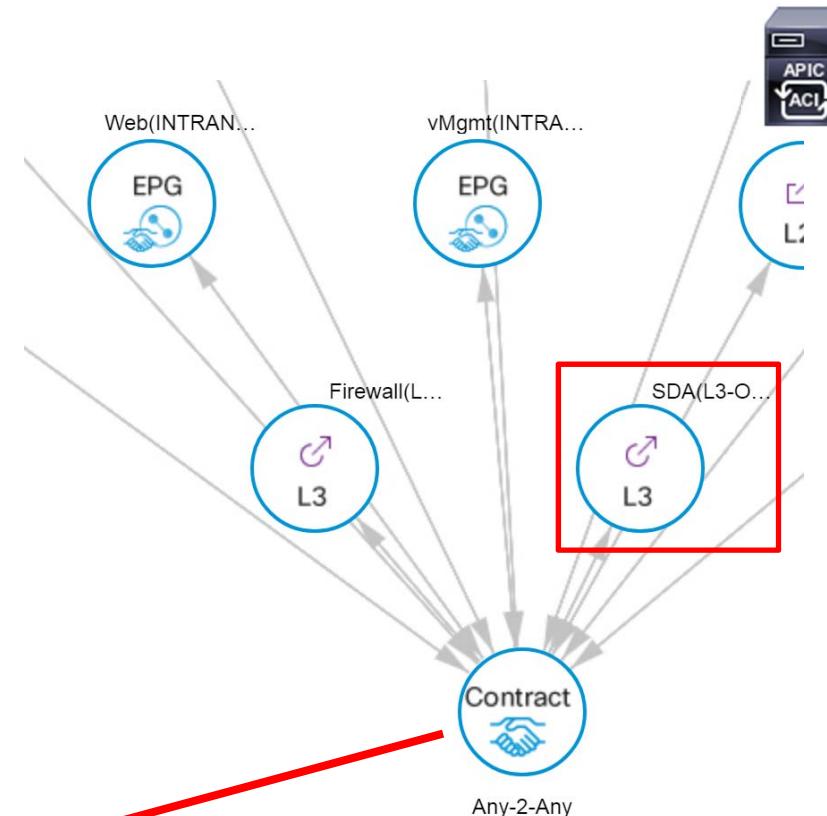
- Cisco Switch Configuration:** A terminal window shows the command `sh run | in xp` being executed on a Cisco switch (sw15-sda). The output includes `cts xp enable` and `cts xp connection peer 1.1.1.1 password default mode peer speaker hold-time 0 0`.
- APIC-ACI Configuration:** A screenshot of the APIC-ACI interface shows a table for "YWEB|uni/tn-ANYWEB/out-L3-Out||3extInstPs". The table lists several entries, with the last entry highlighted by a red arrow pointing to the "Subnet" column, which contains the value "8.8.8.32".
- ISE Device Configuration:** A screenshot of the "IP SGT static mapping > New" interface on an ISE device. It shows a form where the "IP address(es)" field is set to "8.8.8.8". A red arrow points from this field to the "SGT" field, which is set to "BADGOOGLE (666/029A)".

Red arrows indicate the flow of SGT information from the Cisco switch configuration through the APIC-ACI interface to the ISE device configuration.

Name	Alias	QoS Class	Description	Target DSCP	Subnet
BADGOOGLESGT		Unspecified		Unspecified	8.8.8.32
Core		Unspecified		Unspecified	
DNA_Employee_S...		Unspecified		Unspecified	172.23.149.26/32
DNA_SW_SGTSGT		Unspecified		Unspecified	
Firewall		Unspecified		Unspecified	0.0.0.0/0

Enforcement auf ACI

- ACI default Verhalten:
gibt es kein Contract zwischen zwei EPGs – wird der Verkehr geblockt.



Contract ≈ ACL

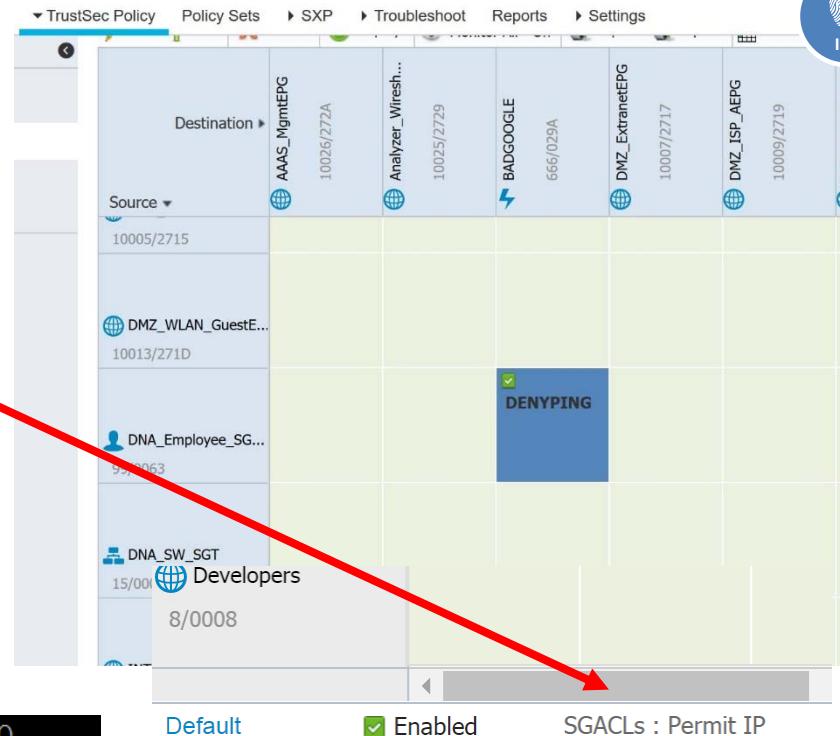
Filter Entries:

Name	EtherType	ARP Flag	IP Protocol	Match Only Fragmen	Stateful	Source Port / Range		Destination Port / Range		TCP Session Rules
						From	To	From	To	
SSH	IP		tcp	False	False	unspecified	unspecified	22	22	Unspecified

Enforcement auf dem Switch

- Default Verhalten: gibt es keine Policy zwischen zwei SG – wird der Verkehr zugelassen.
- Enforcement auf dem Switch muss noch ausdrücklich erlaubt werden

`cts role-based enforcement vlan-list 20`



The screenshot shows a policy matrix in the AnyWeb TrustSec Policy interface. The columns represent Destinations and the rows represent Sources. A blue cell in the row for 'DNA_Employee_SG...' and column for 'Developers' contains the text 'DENYPING'. At the bottom of the matrix, there is a row of controls: 'Default', a checked checkbox labeled 'Enabled', and a dropdown menu labeled 'SGACLs : Permit IP'.

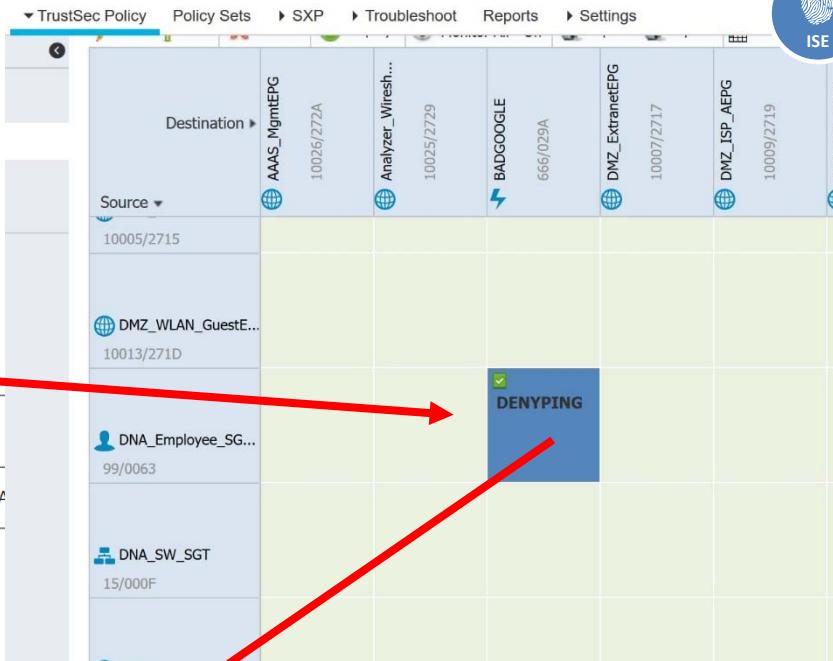
Enforcement auf dem Switch

- Aufgrund vom Tag und nicht von IP Adresse!

Security Groups ACLs List > DENYPING

Security Group ACLs

* Name	DENYPING
Description	DENY
IP Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> A
* Security Group ACL content	deny icmp



```

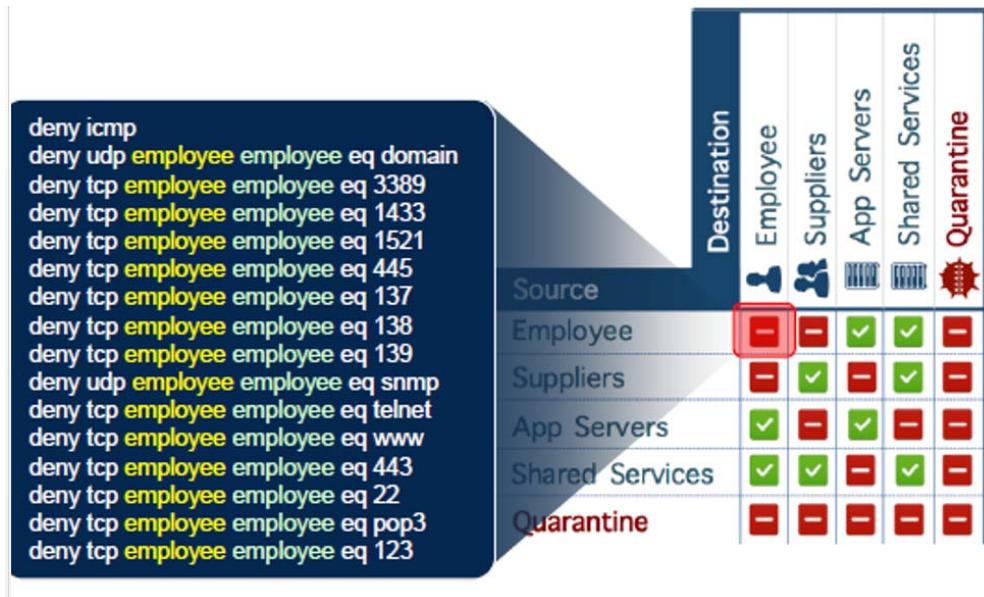
sw15-sda#sh cts role-based per
sw15-sda#sh cts role-based permissions
IPv4 Role-based permissions default:
    Permit IP-00
IPv4 Role-based permissions from group 99:DNA_Employee_SGT to group 666:BADGOOGLE:
    DENYPING-10
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

sw15-sda# sh ip ac
sw15-sda# sh ip acce
sw15-sda# sh ip access-lists DENYPING-10
Role-based IP access list DENYPING-10 (downloaded)
    10 deny icmp
sw15-sda#

```

Vorteile von Cisco TrustSec

- Zentral definierte Policy (auf dem ISE) mit dezentralen Forcierung
- Komplexe Policies sind einfach zum Umsetzen
- Flexibilität beim Erstellen neuen Client Gruppen
- Aber immer noch relativ viel initiale (manuelle) Konfiguration auf den Switches

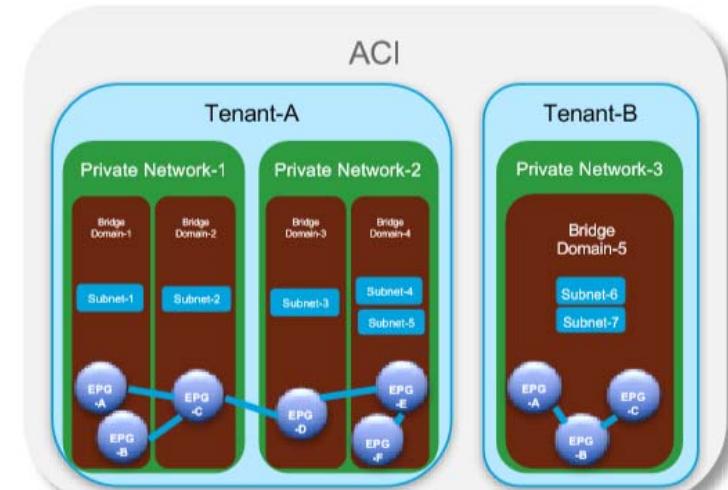
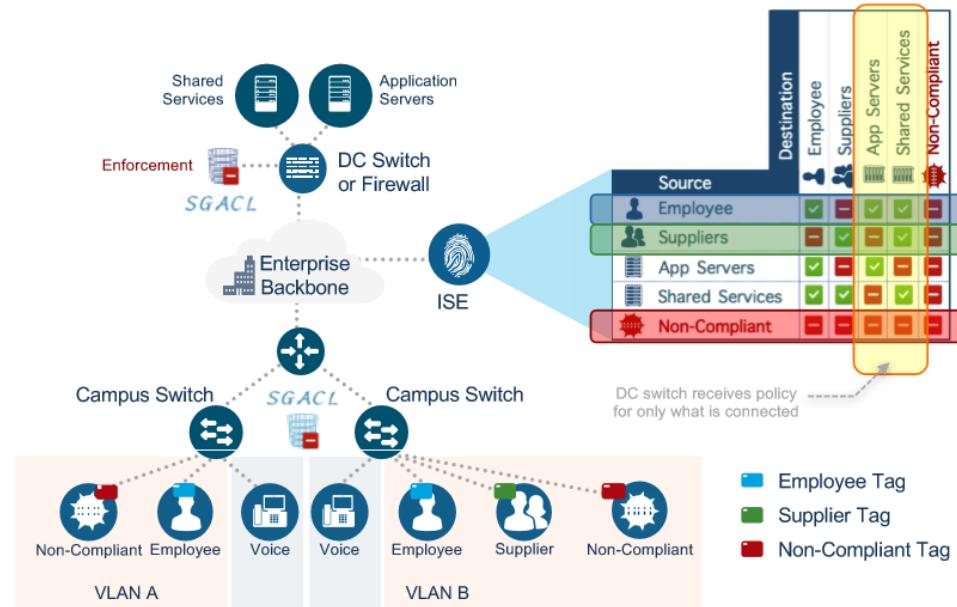


```

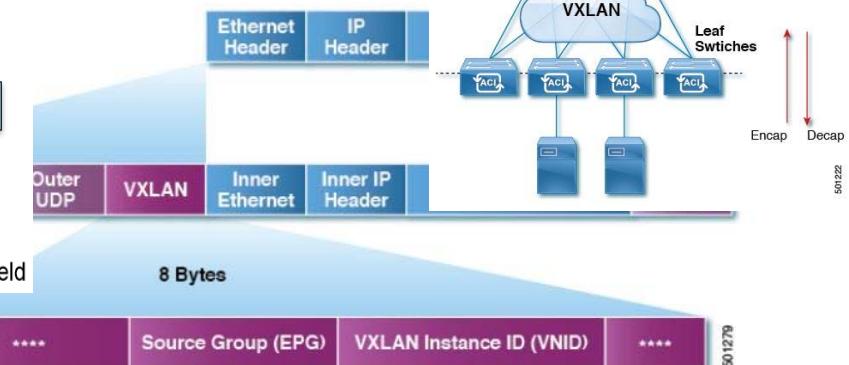
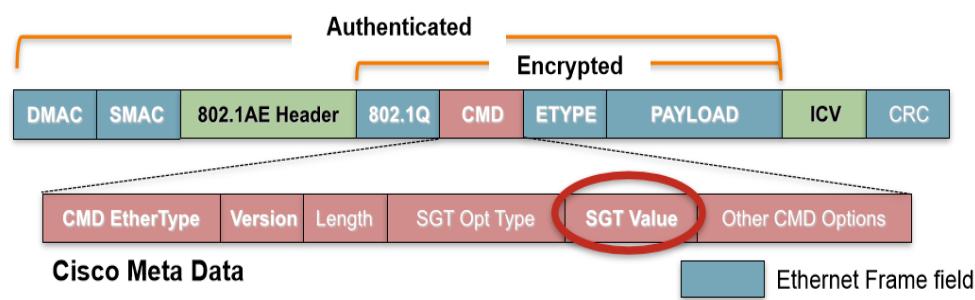
sw15-sda#sh run
Building configuration...
!
Current configuration : 11891 bytes
!
! Last configuration change at 09:35:23 UTC Thu Oct 26 2017 by
!
version 16.6
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec

```

Wie geht es weiter???



End-Point Groups (EPG)



Create. Connect. Control.



... cool ... aber geht's auch einfacher?

Cisco DNA / SDA

Edi Layritz

Was möchten wir?

- Weniger tippen
- Gleiche Konfiguration auf allen Client Switchen
- Hohe Sicherheit
 - End to End Policies
 - Sicherer Zugang zum Netz
 - Segmentierung / Zonierung
- Gleiche IOS Version auf allen Switchen
- ...

→ Automatisierung kann uns helfen

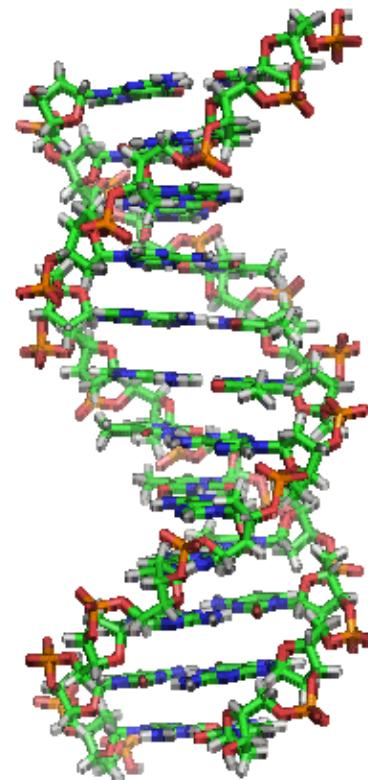
DNA / SDA



It's a
Journey ...

Isches no wiit? Nei, nei!!!!

DNA / SDA - Begriffe



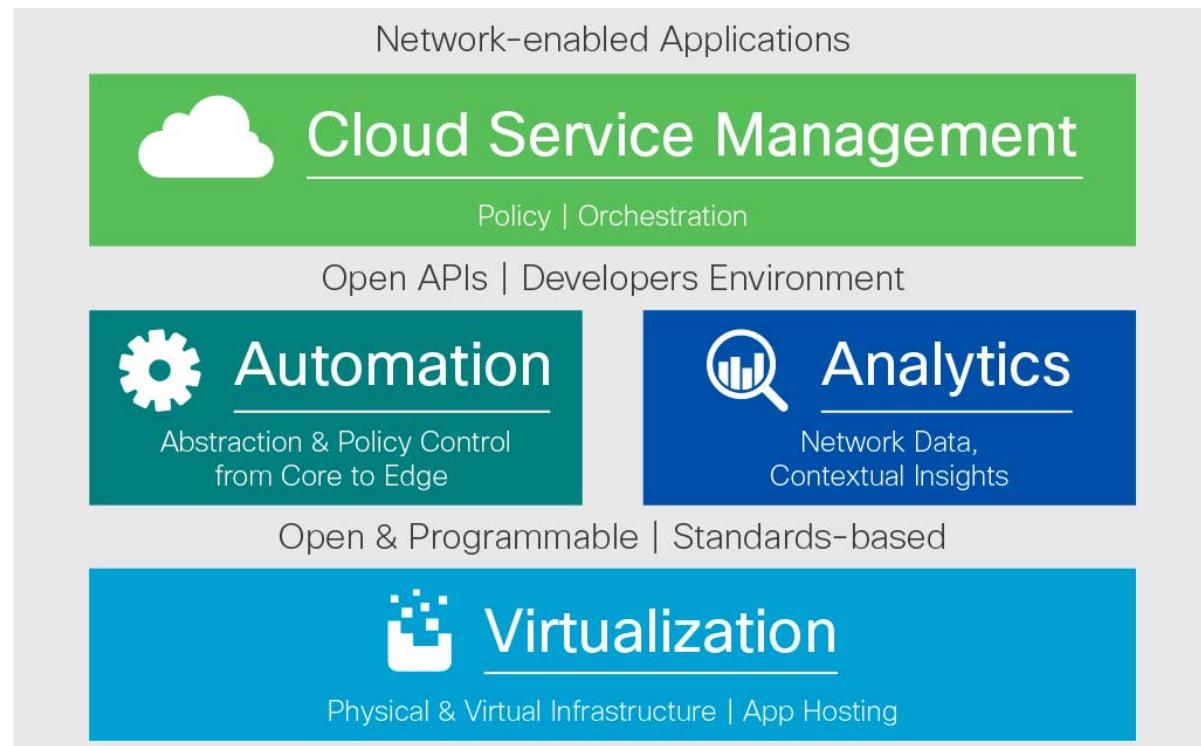
DNA ist nicht
Desoxyribonukleinsäure ;-)

DNA / SDA - Begriffe



DNA – Digital Network Architecture

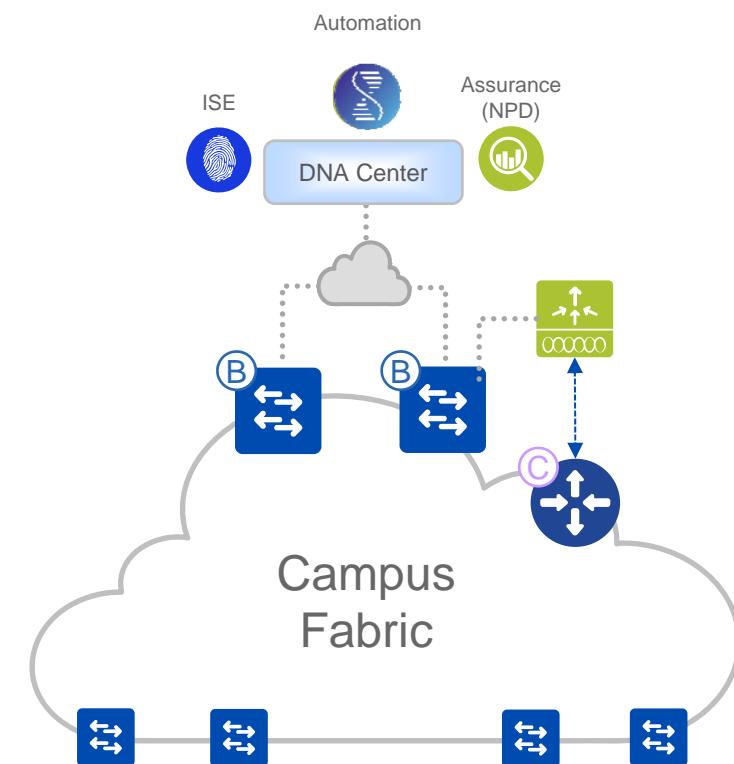
Eine Architektur:



DNA / SDA - Begriffe

SDA – Software Defined Access

Die Umsetzung:



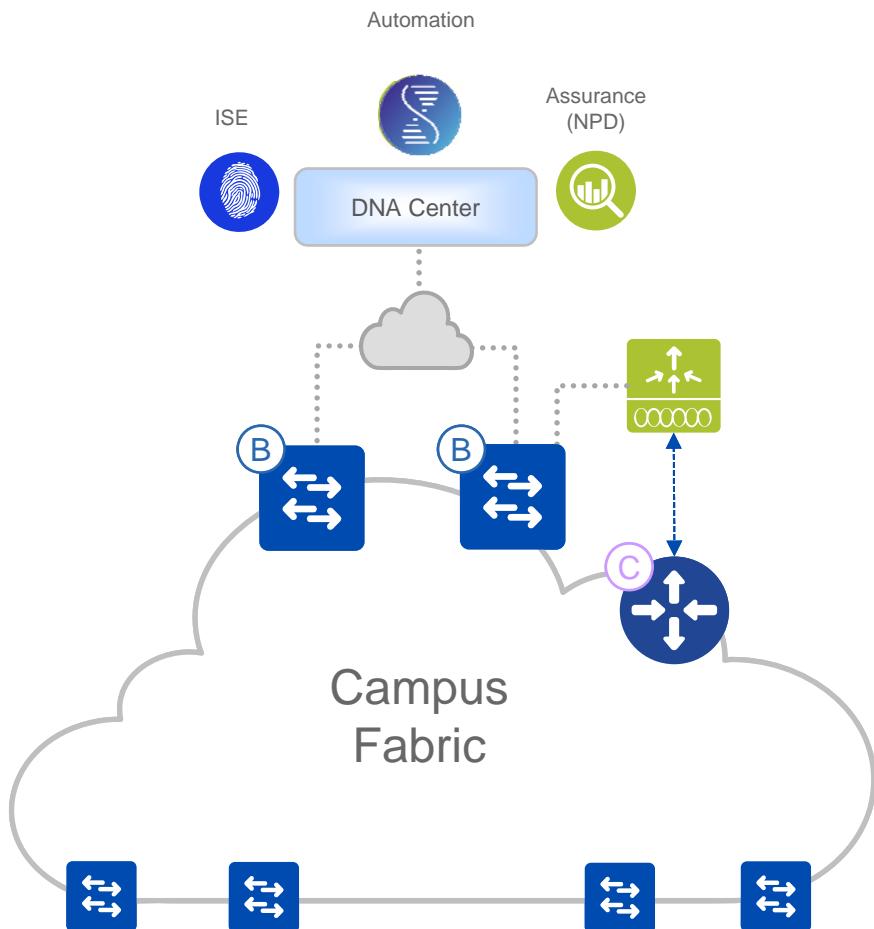
Was bietet DNA?

- Ein homogenes Netz
 - Access - Control
 - Segmentierung
 - Policy Enforcement
 - Insights & Telemetrie – Ende November 2017
- Automatisierung beim Ausrollen
- Einfacher Betrieb

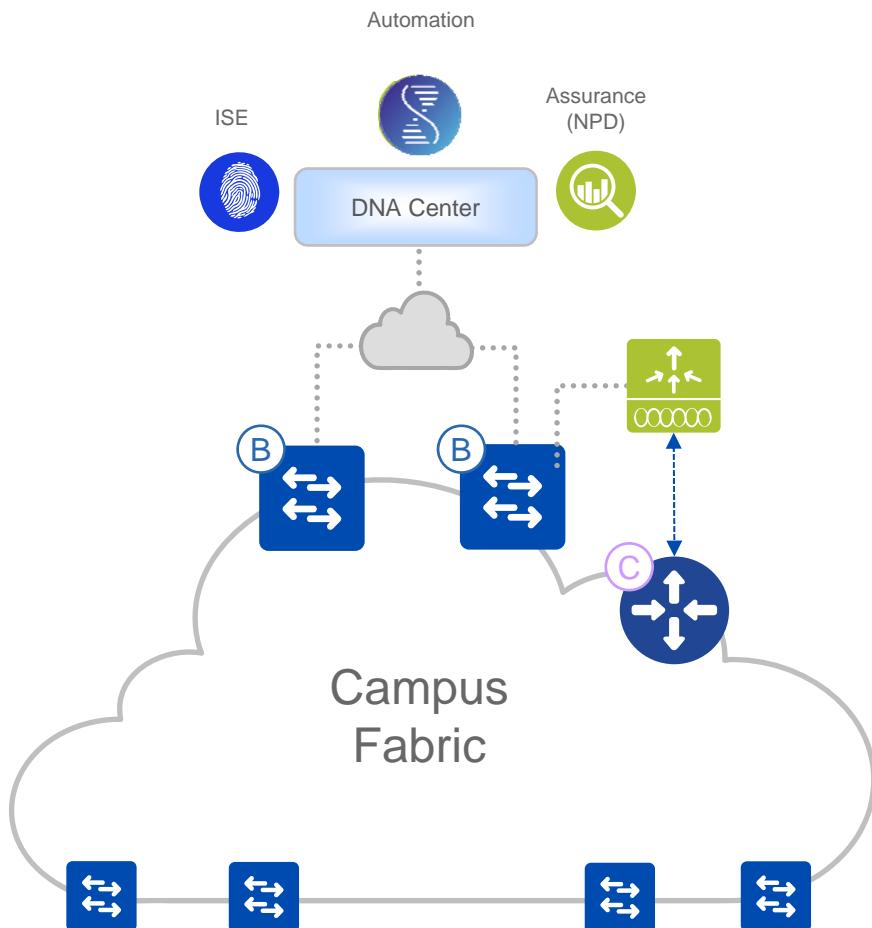
It's a journey



SDA – Campus Fabric



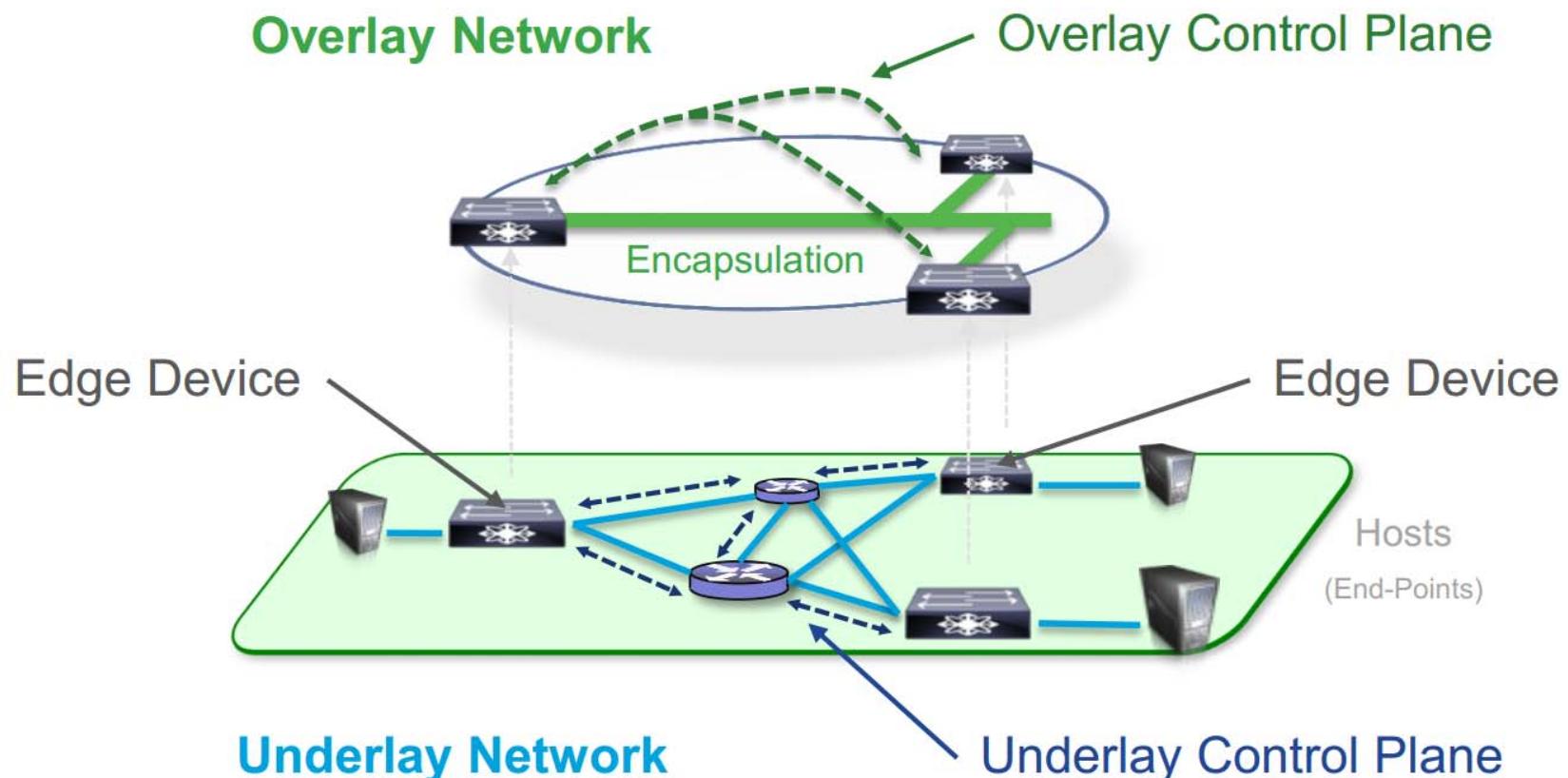
SDA – Campus Fabric



- **Campus Fabric**

SDA – Campus Fabric

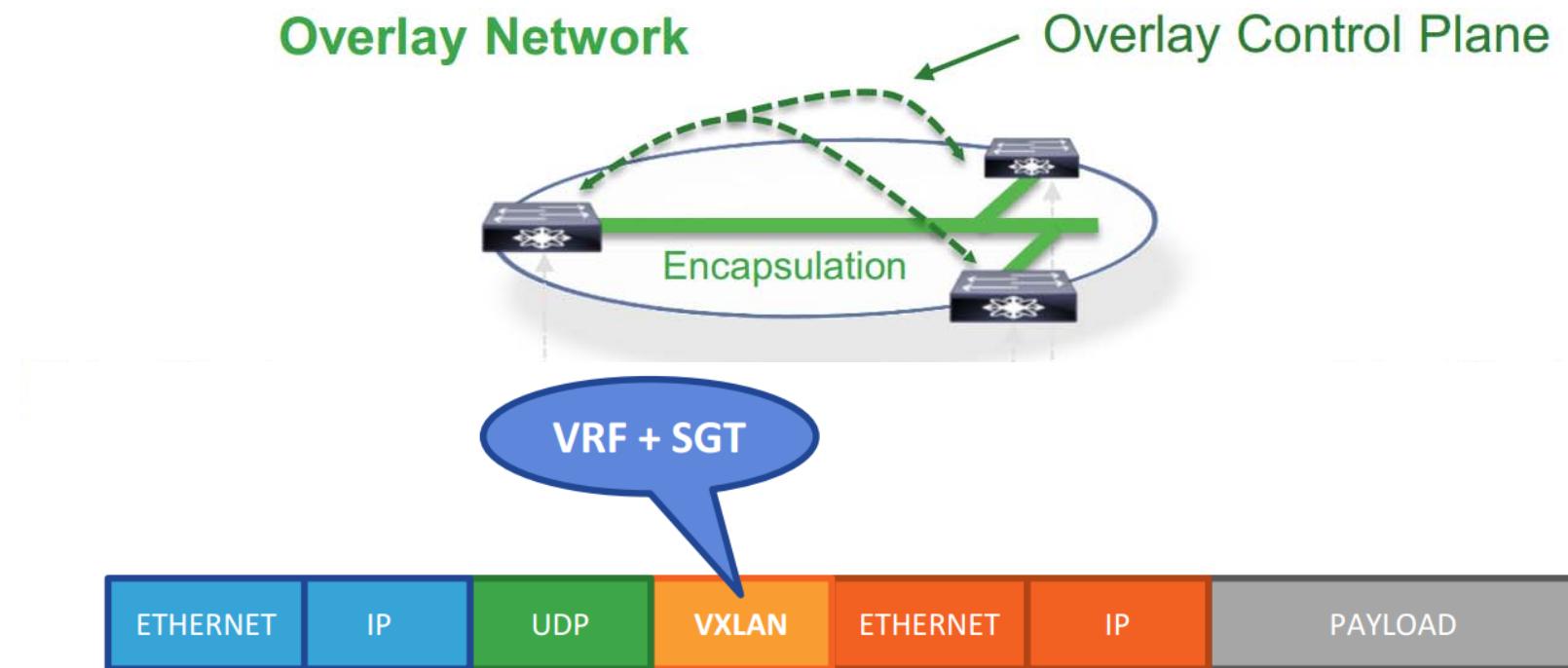
Die Fabric bildet ein Overlay Netz



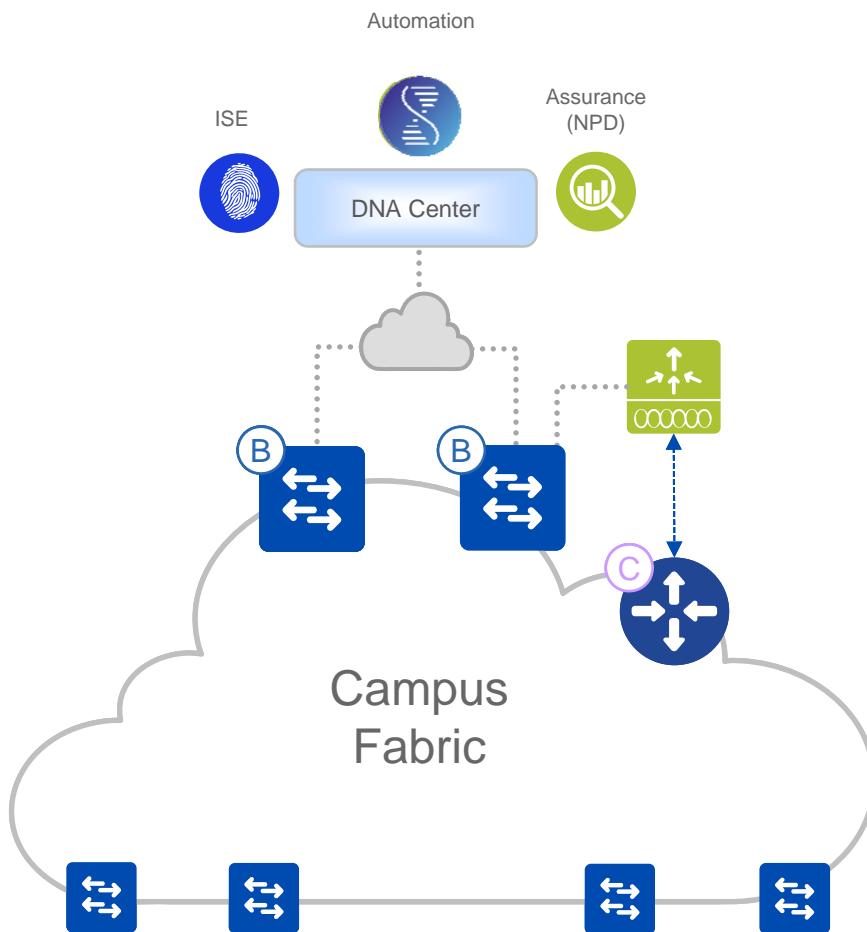
SDA – Campus Fabric

- Ein Overlay Netz bildet eine virtuelle Topologie um Geräte miteinander zu verbinden
Beispiele: MPLS VPN, DMVPN, CAPWAP
- Campus Fabric verwendet LISP
 - Dies ermöglicht die fixe Zugehörigkeit von IP Adressen und Standort (L3-Device) Einfacher Betrieb
→ IP Mobility
 - LISP – Locator ID Separation Protocol
- Zur Enkapsulierung wird VXLAN mit SGT verwendet
→ Jedes Packet wird mit der Gruppenzugehörigkeit des Absender markiert
- Layer 3 bis in den Access

SDA – Campus Fabric

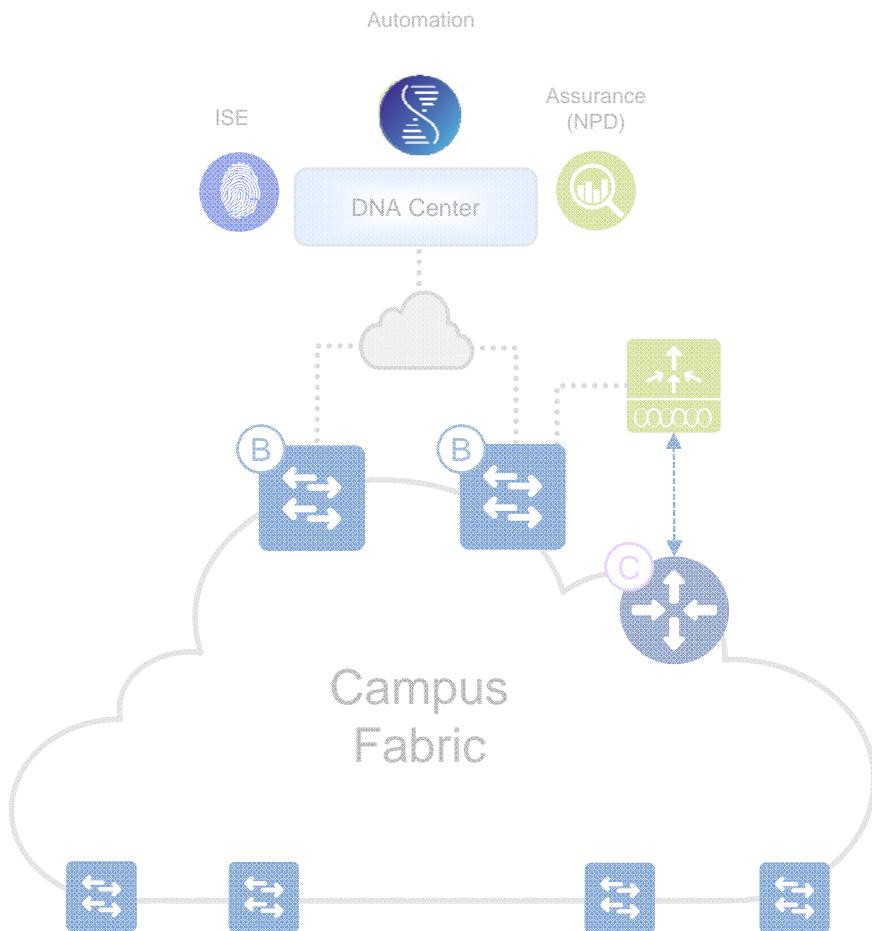


SDA – Campus Fabric



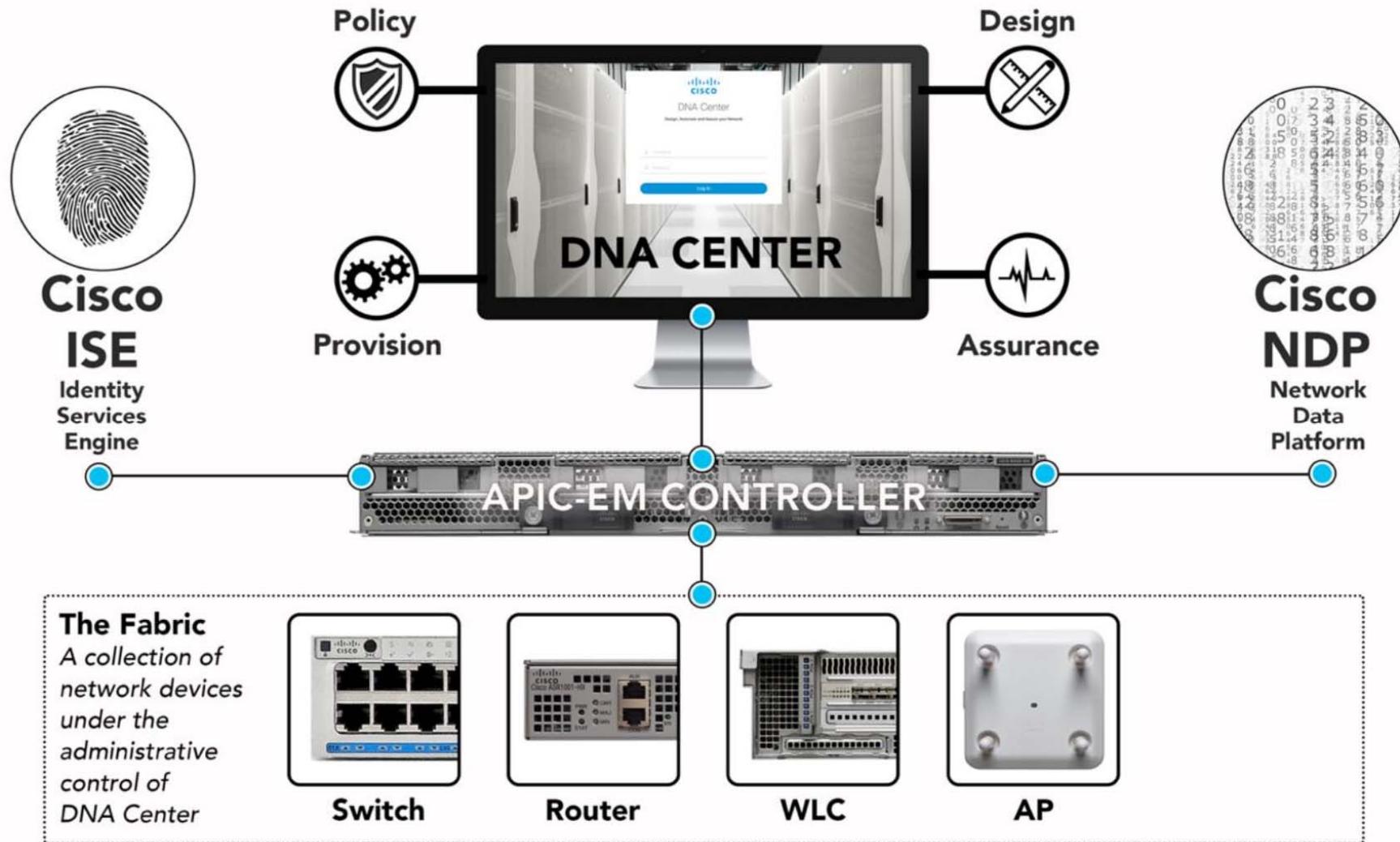
- Edge Node
 - Hier werden die Endgeräte angeschlossen
- Border Node
 - Stellt den Übergang zum restlichen Netz, dem DC und dem Internet sicher
- Control Node
 - Führt Buch darüber wo sich eine IP Adresse befindet

SDA – DNAC

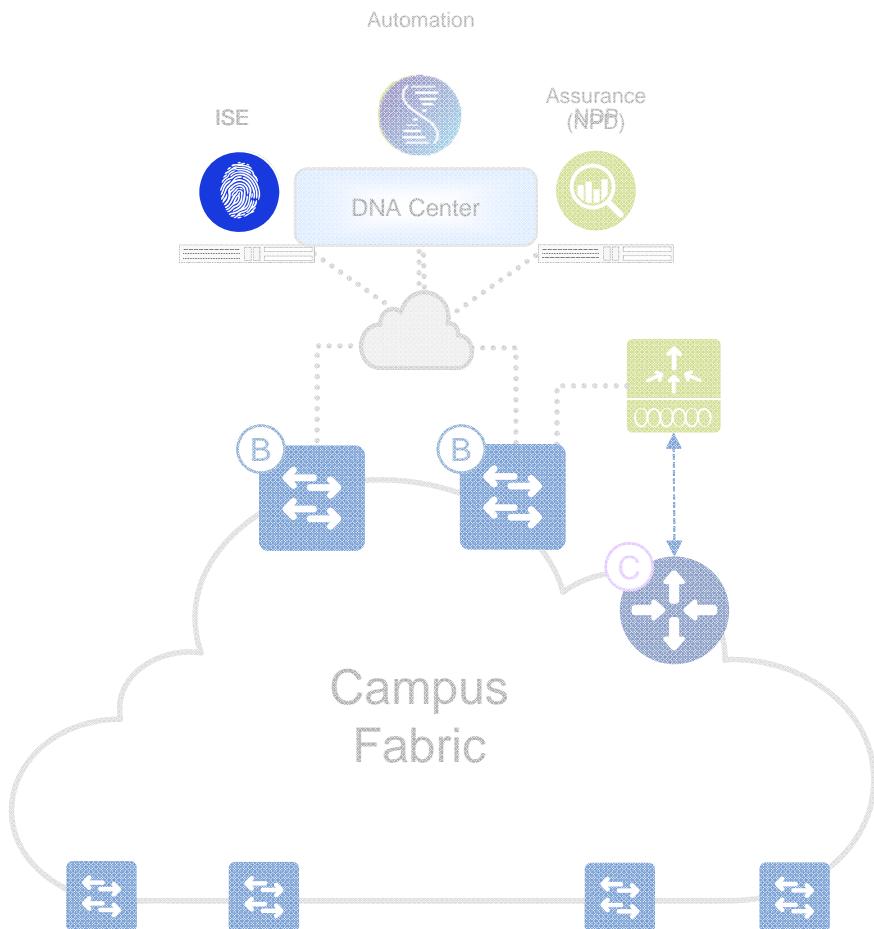


- **Campus Fabric**
- **DNA-Center**

SDA – DNAC

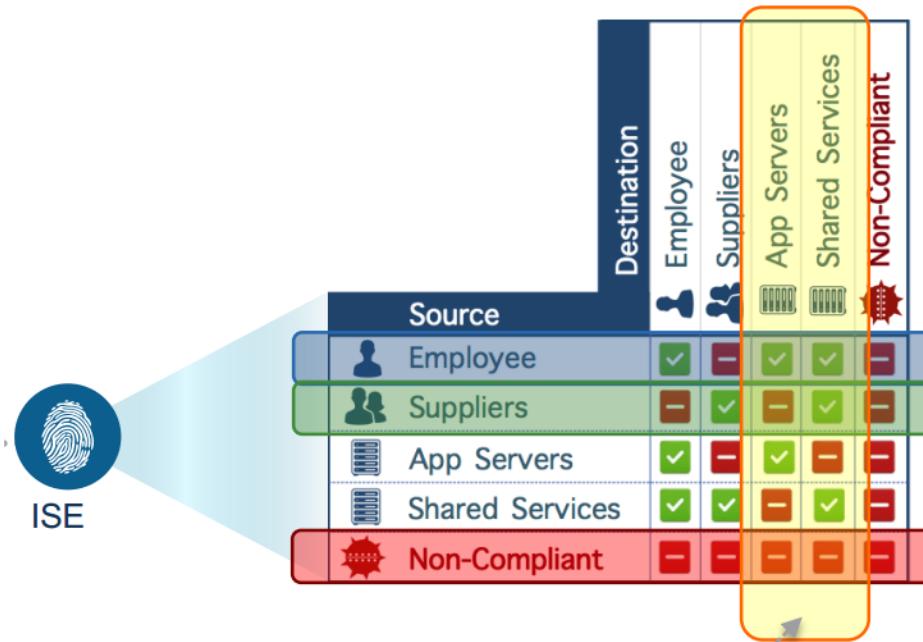


SDA – ISE



- **Campus Fabric**
- **DNA-Center**
- **ISE**

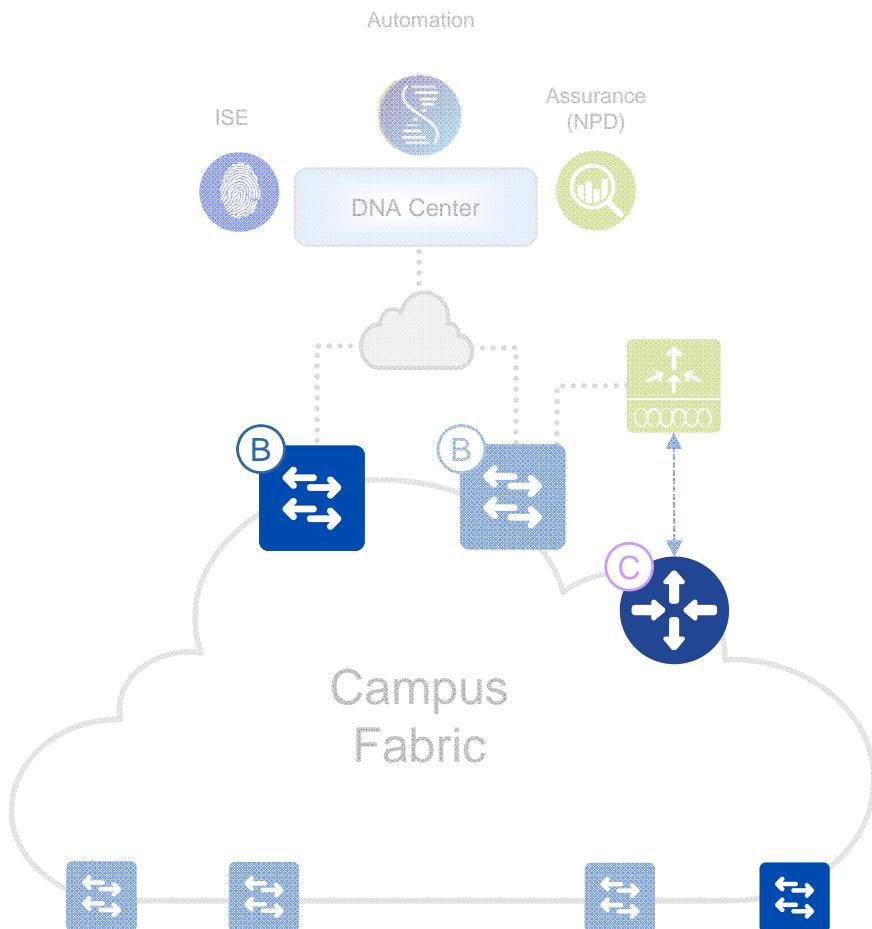
SDA – ISE



It's a journey



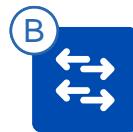
SDA - Hardware



- **Campus Fabric**
- **DNA-Center**
- **Hardware**

SDA - Hardware

Switches



Border Node

- Cat 9500
- Cat 3850
- Cat 6800
- ASR 1000
- ISR 4430/4450
- Nexus 7700
 - M3 Cards



Control Node

- Cat 9500
- Cat 3850
- Cat 6800
- ASR 1000
- ISR 4430/4450



Edge Node

- Cat 9300/9400
- Cat 3650/3850
- Cat 4500



WLC

- 3504
- 5520
- 8540

SDA - Hardware

DNA-Center



Zum jetzigen Zeitpunkt nur als Appliance lieferbar

Gründe dafür nach Cisco

- Braucht viel Leistung
- Leistung ist so garantiert



DNA Center

SDA - Design

SDA - Provision

SDA - Policy

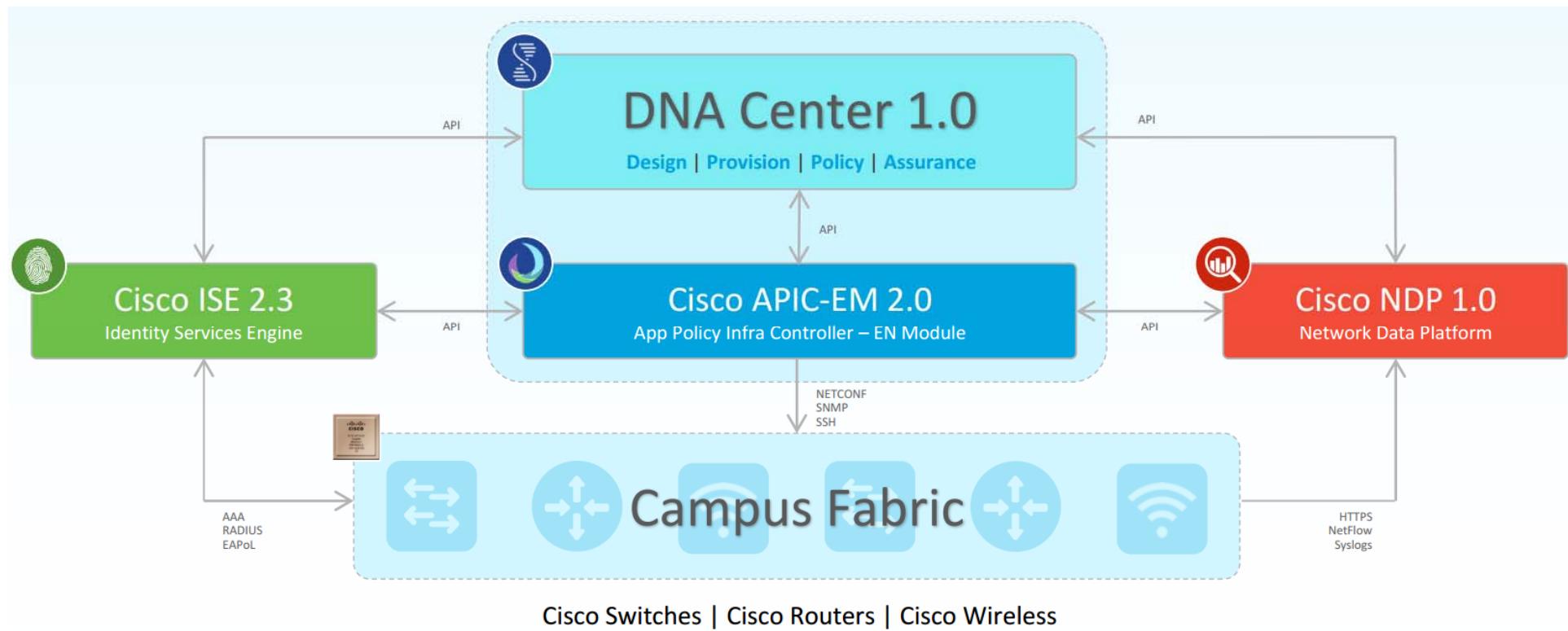
DNA Center

Virtual Networks
Access Control
Application Priority
Application Registry



DNA Center

Einbindung vom DNA Center

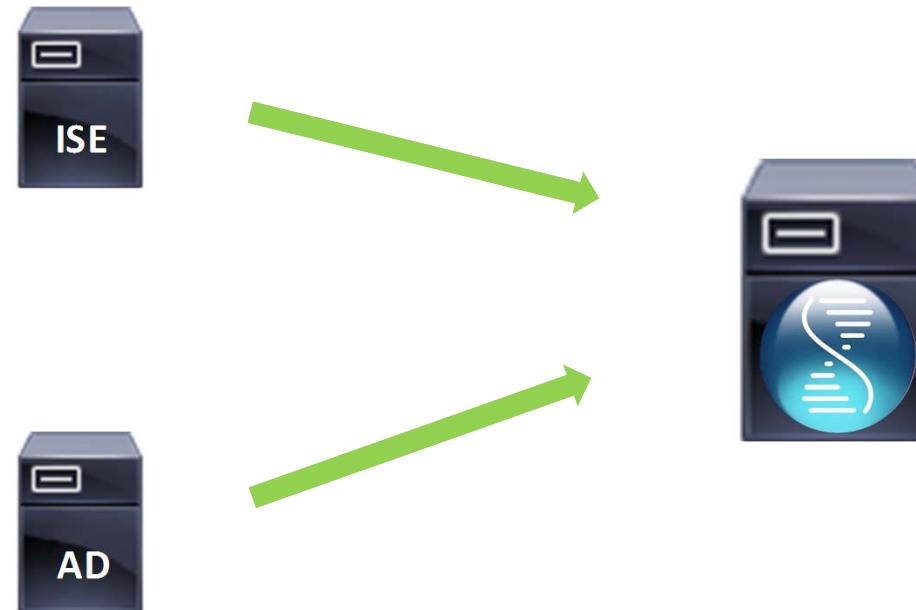




DNA Center

DNA-Center lernt die SGT's vom ISE oder dem AD

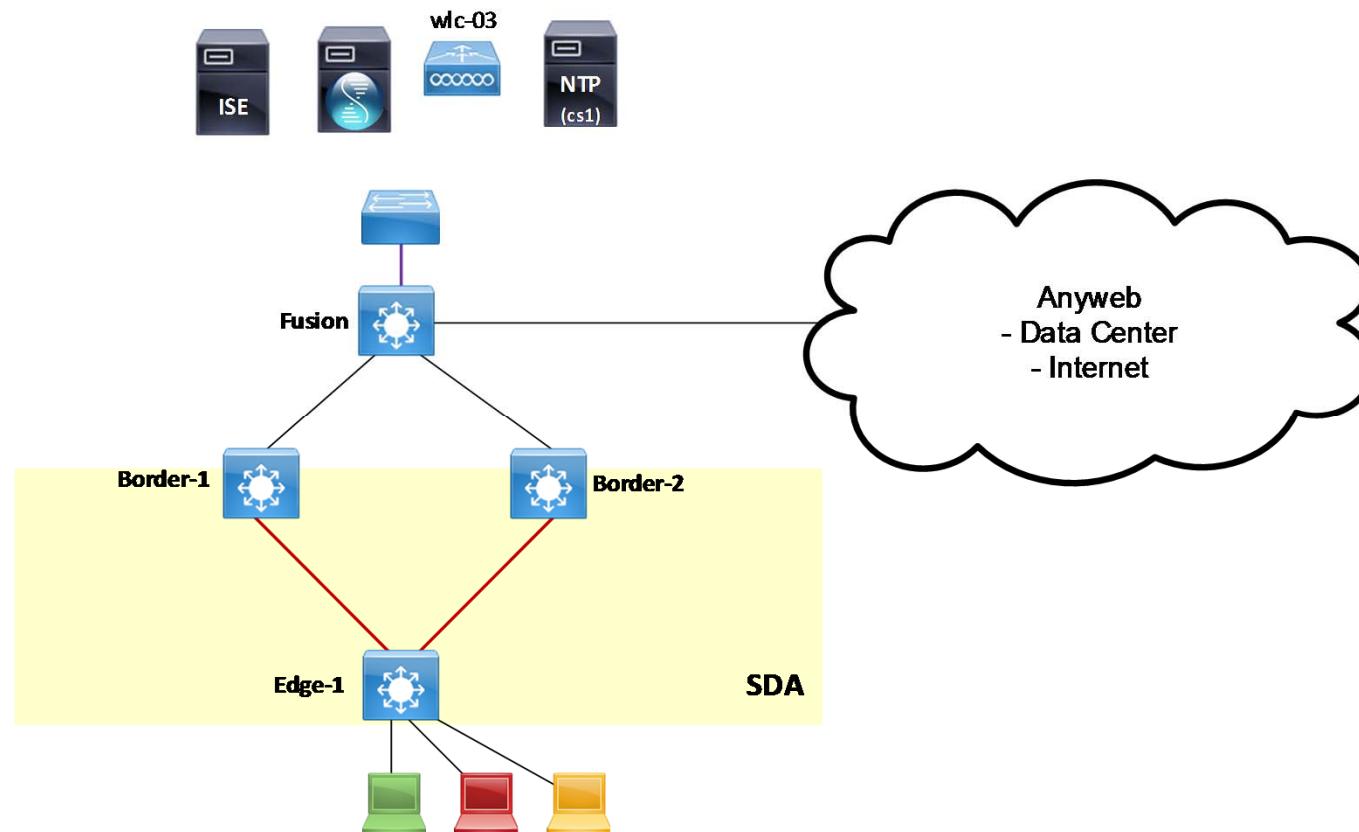
SGT: Scalable Groups, Scalable Group Tags





DNA Center

SDA@AnyWeb – Laboraufbau





DNA Center

Aufbau eines SDA mit DNA Center

- Vorbereitungen → Manuel
 - Grundkonfiguration der Switches
- Netzwerkeinstellungen → DNAC
- Einfache Policies → DNAC
- Komplexe Policies → ISE
- Restliche Konfiguration → DNAC



DNA Center

CISCO DNA CENTER
admin
grid
bell
gear
info

What can DNA Center do?

Design

Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.

- Add site locations on the network
- Designate golden images for device families
- Create wireless profiles of SSIDs

Policy

Use policies to automate and simplify network management, reducing cost and risk while speeding rollout of new and enhanced services.

- Segment your network as Virtual Networks
- Create scalable groups to describe your critical assets
- Define segmentation policies to meet your policy goals

Provision

Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.

- Discover and provision switches to defined sites
- Provision WLCs and APs to defined sites
- Set up Campus Fabric across switches

Tools

Discovery

Automate addition of devices to controller inventory

Device Inventory

Add, update or delete devices that are managed by the controller

Topology

Auto discover and map network devices to a physical topology

Plug & Play

Automate device deployment with agent and network controller

Image Management

Download, deploy and update device software images automatically

Feedback



Discover | Topology | Design | Policy | Provision

Discoveries



 Search by Device IP

- WLC**  1
Range 172.24.200.7-172.24.2...
- Switches**  3
Range 172.24.200.113-172.2...

Edit Discovery

Switches

* Discovery Name

▼ IP RANGES

Type 

CDP

Range

* IP Ranges 

0.0.0.0

0.0.0.0



172.24.200.113 to 172.24.200.116

Preferred Management IP 

Use Loopback



► CREDENTIALS



What can DNA Center do?

Design

Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.

- Add site locations on the network
- Designate golden images for device families
- Create wireless profiles of SSIDs

Policy

Use policies to automate and simplify network management, reducing cost and risk while speeding rollout of new and enhanced services.

- Segment your network as Virtual Networks
- Create scalable groups to describe your critical assets
- Define segmentation policies to meet your policy goals

Provision

Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.

- Discover and provision switches to defined sites
- Provision WLCs and APs to defined sites
- Set up Campus Fabric across switches

Tools



Discovery

Automate addition of devices to controller inventory



Device Inventory

Add, update or delete devices that are managed by the controller



Topology

Auto discover and map network devices to a physical topology



Plug & Play

Automate device deployment with agent and network controller

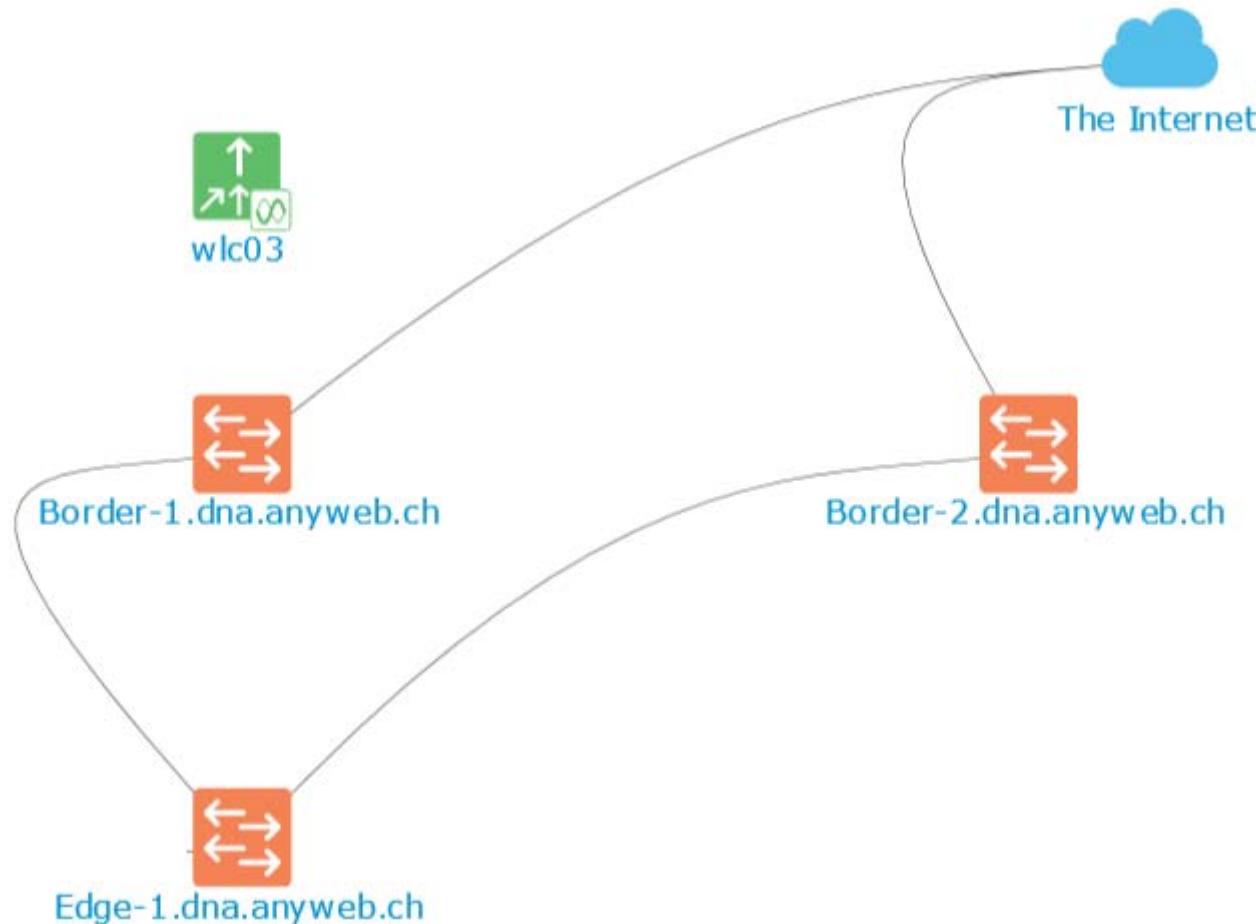


Image Management

Download, deploy and update device software images automatically



Discover | Topology | Design | Policy | Provision





DNA Center

DNA CENTER
admin
grid
bell
gear
info

What can DNA Center do?

Design

Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.

- Add site locations on the network
- Designate golden images for device families
- Create wireless profiles of SSIDs

Policy

Use policies to automate and simplify network management, reducing cost and risk while speeding rollout of new and enhanced services.

- Segment your network as Virtual Networks
- Create scalable groups to describe your critical assets
- Define segmentation policies to meet your policy goals

Provision

Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.

- Discover and provision switches to defined sites
- Provision WLCs and APs to defined sites
- Set up Campus Fabric across switches

Tools

Discovery

Automate addition of devices to controller inventory

Device Inventory

Add, update or delete devices that are managed by the controller

Topology

Auto discover and map network devices to a physical topology

Plug & Play

Automate device deployment with agent and network controller

Image Management

Download, deploy and update device software images automatically

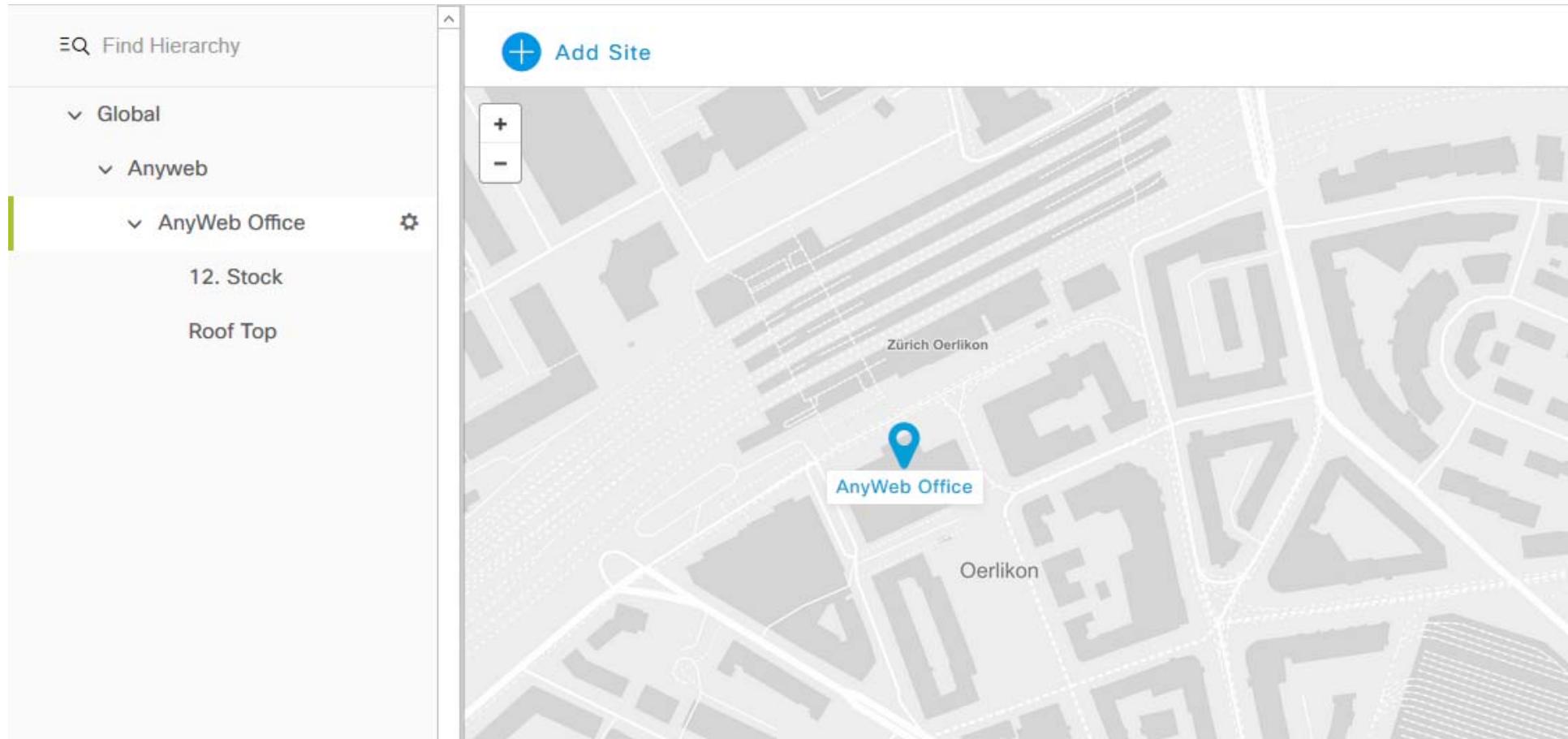
Feedback



DNA Center

Discover | Topology | Design | Policy | Provision

Add Location | set common Network Params | Device Credentials | IP Pools



The screenshot shows the Cisco DNA Center Design interface. On the left, there's a sidebar titled "Find Hierarchy" with a search bar and a tree view. The tree structure is as follows:

- Global
- Anyweb
 - AnyWeb Office
 - 12. Stock
 - Roof Top

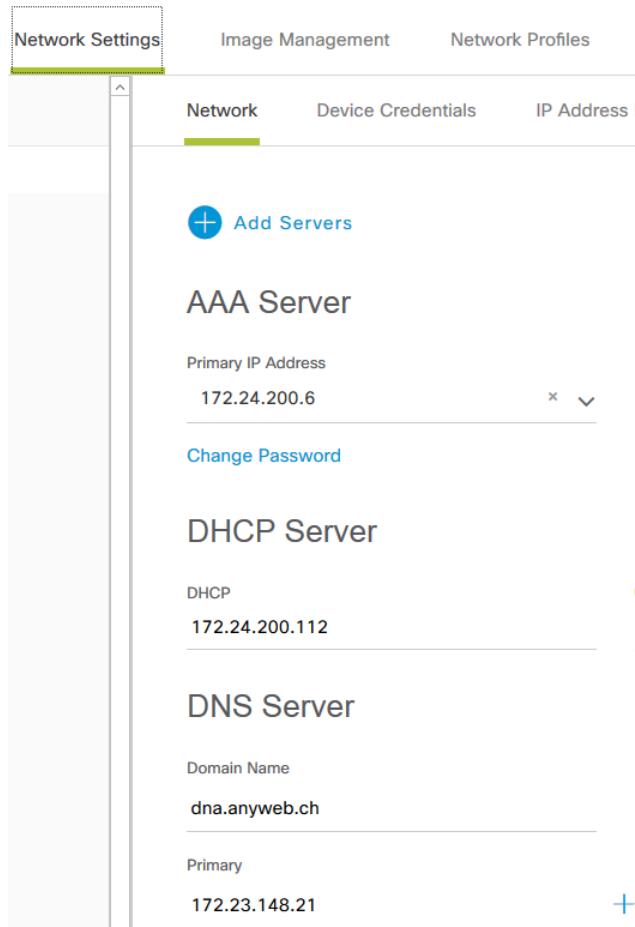
To the right of the sidebar is a map of a city area labeled "Zürich Oerlikon". A blue location pin marks the "AnyWeb Office" location. The map shows various buildings and streets. At the top of the main content area, there's a button labeled "Add Site" with a plus sign. To the left of the map, there are zoom controls (+ and -).



DNA Center

Discover | Topology | Design | Policy | Provision

Add Location | set common Network Params | Device Credentials | IP Pools



The screenshot shows the Network Settings page in DNA Center. The top navigation bar includes tabs for Network Settings, Image Management, and Network Profiles. The sub-navigation bar under Network Settings includes Network, Device Credentials, and IP Address Pools, with Network selected. A prominent 'Add Servers' button is located at the top left of the main content area. Below it, the 'AAA Server' section is displayed, showing a primary IP address of 172.24.200.6. A 'Change Password' link is also present. The 'DHCP Server' section shows one entry with an IP address of 172.24.200.112. The 'DNS Server' section shows one entry with a domain name of dna.anyweb.ch and a primary IP address of 172.23.148.21. A blue plus sign icon is located at the bottom right of the DNS server list.

AAA Server
Primary IP Address 172.24.200.6
Change Password

DHCP Server
DHCP 172.24.200.112

DNS Server
Domain Name dns.anyweb.ch
Primary 172.23.148.21



Discover | Topology | Design | Policy | Provision

Add Location | set common Network Params | Device Credentials | IP Pools

Network Settings Image Management Network Profiles

Network **Device Credentials** IP Address Pools Wireless

CLI Credentials

Name / Description	Username	Password	Enable Password
<input type="radio"/>	admin	*****	*****
<input checked="" type="radio"/> WLC	instruktor	*****	*****
<input type="radio"/>	swadmin	*****	*****

SNMP Credentials

SNMPV2C Read | [SNMPV2C Write](#) | [SNMPV3](#)

Name / Description	Read Community
<input type="radio"/> Read	*****



Discover | Topology | Design | Policy | Provision

Add Location | set common Network Params | Device Credentials | IP Pools

Network Settings Image Management Network Profiles

Network Device Credentials IP Address Pools Wireless

Name	IP Subnet Mask	Gateway	DHCP Server	DNS Server	Free Count	Overlap...
AP-WLAN-Mgt	172.23.150.0/25	172.23.150.1			128 of 128	No
Guest	172.24.200.240/28	172.24.200.241	172.24.200.112		0 of 16	No
NetMgt	172.24.200.224/28	172.24.200.225	172.23.148.21	172.23.148.21	0 of 16	No
Office	172.24.200.208/28	172.24.200.209	172.23.148.21	172.23.148.21	0 of 16	No



DNA Center

Discover | Topology | Design | Policy | Provision

Ein virtuelles Netzwerk (vrf) erstellen und Scalable Groups (VLAN) zufügen

Hinweis: Die eigentlichen Policies werden später erstellt

Virtual Network Policy Administration Contracts Registry

Create or Modify Virtual Network by selecting Available Scalable Groups.

Network Name*
AnyGotthard

Guest Virtual Network

Available Scalable Groups

AA AAAS_MgmtE ...	AW Analyzer_Wires...	AU Auditors	BY BYOD	CO Contractors	DM DMZ_Extranet...	DM DMZ_ISP_AEP ...
AAAS_MgmtE ...	Analyze r_Wires...	Auditor s	BYOD	Contractors	DMZ_Extranet...	DMZ_ISP_AEP ...
DM DMZ_ISP_BEP ...	DM DMZ_Lab_AEP...	DM DMZ_MgmtEPG	DM DMZ_MobileIP ...	DM DMZ_MobileIP ...	DM DMZ_Server_A...	DM DMZ_Server_B...
DM DMZ_SyncEPG	DM DMZ_TransitEP...	DM DMZ_WLAN_G ...	DN DNA_Guest	DN DNA_NetMgt	DN DNA_Office	DE Developers

Groups in the Virtual Network

Drag Groups here to add to the Virtual Network

DN
DNA_Guest



DNA Center

Discover | Topology | Design | Policy | Provision

Assign Switch to Site | Add a Fabric | Assign Roles to Switches | onboard Hosts

Devices Fabric

Device Inventory

Inventory (4) Unassigned Devices

Select Devices... ▾

Select Devices...

Add/Remove Site

Provision

Add Services

Update OS Image

Delete Device

	Device Type	IP Address	Site	Serial Number	Uptime	OS Version
.ch	Switches and Hubs	172.24.200.113	AnyWeb Office	FDO1743Q06Y	5 days, 4:12:35.25	16.6.1
.ch	Switches and Hubs	172.24.200.114	AnyWeb Office	FDO1735Q0BW	7 days, 22:30:14.64	16.6.1
.ch	Switches and Hubs	172.24.200.115	AnyWeb Office	FDO1741Q0TQ	5 days, 0:23:22.35	16.6.1



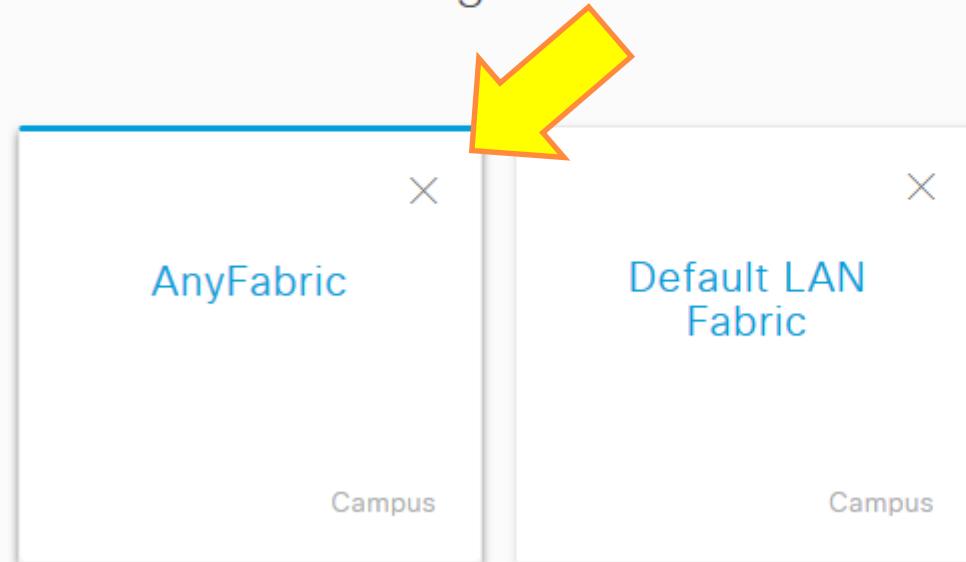
DNA Center

Discover | Topology | Design | Policy | Provision

Assign Switch to Site | Add a Fabric | Assign Roles to Switches | onboard Hosts

Devices **Fabric**

Create and Manage Fabric



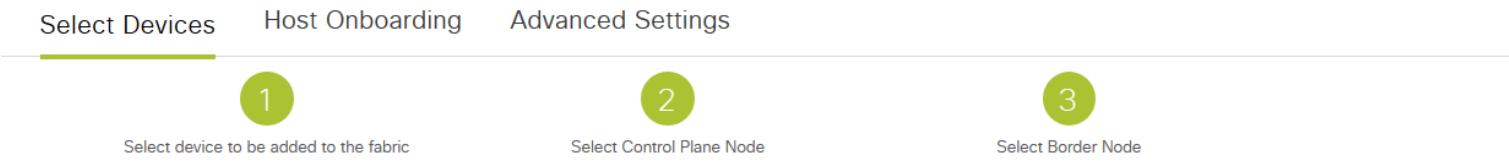


DNA Center

Discover | Topology | Design | Policy | Provision

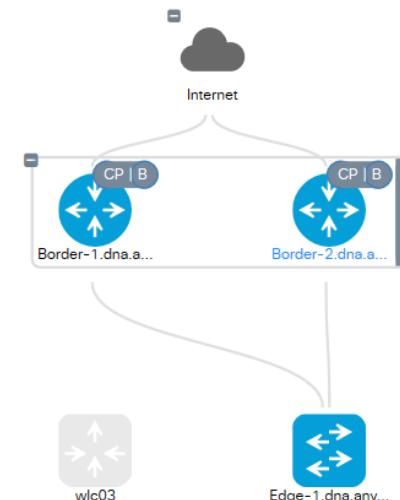
Assign Switch to Site | Add a Fabric | Assign Roles to Switches | onboard Hosts

AnyFabric



 Search Topology

Select Devices to add, remove or identify.
Click and drag to select multiple.

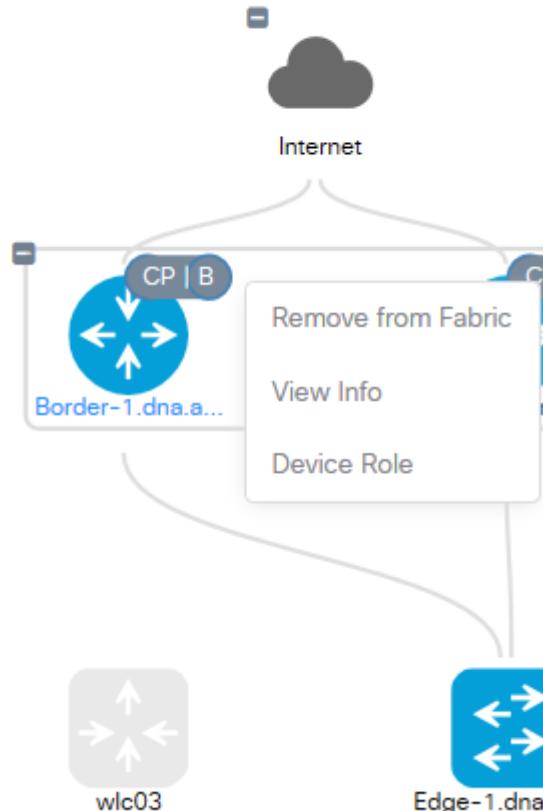




DNA Center

Discover | Topology | Design | Policy | **Provision**

Assign Switch to Site | Add a Fabric | **Assign Roles to Switches** | onboard Hosts



Change Device Role

Choose Device Role

BORDER ROUTER

- ACCESS
- CORE
- DISTRIBUTION
- BORDER ROUTER**

Cancel Save



DNA Center

Discover | Topology | Design | Policy | Provision

Assign Switch to Site | Add a Fabric | Assign Roles to Switches | onboard Hosts

Hier wird festgelegt, wie die Hosts der richtigen Gruppe zugewiesen werden
zur Auswahl stehen:

- Dynamisch
- Statisch



DNA Center

Discover | Topology | Design | Policy | **Provision**

Assign Switch to Site | Add a Fabric | Assign Roles to Switches | **onboard Hosts**

Devices **Fabric**

AnyFabric

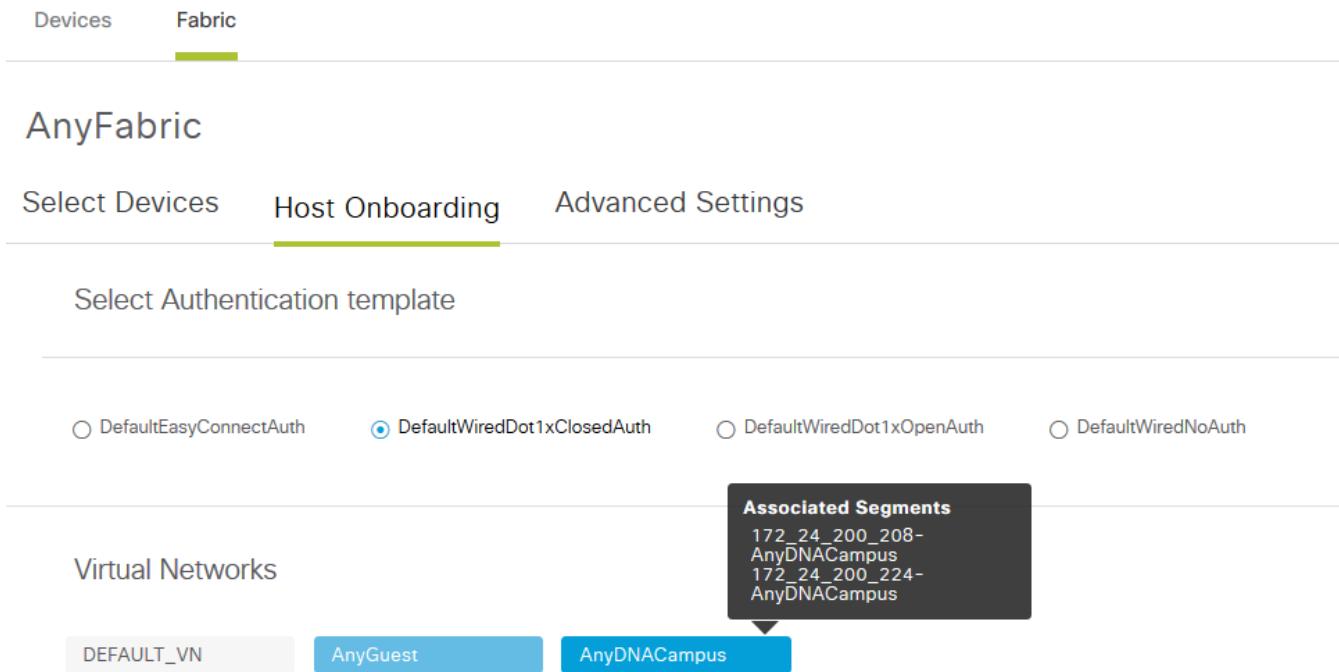
Select Devices **Host Onboarding** Advanced Settings

Select Authentication template

DefaultEasyConnectAuth DefaultWiredDot1xClosedAuth DefaultWiredDot1xOpenAuth DefaultWiredNoAuth

Virtual Networks

Associated Segments
172_24_200_208-
AnyDNACampus
172_24_200_224-
AnyDNACampus



DEFAULT_VN **AnyGuest** AnyDNACampus

Dynamische Zuweisung des VLAN basierend auf der Rolle



DNA Center

Discover | Topology | Design | Policy | **Provision**

Assign Switch to Site | Add a Fabric | Assign Roles to Switches | **onboard Hosts**

Select Port Assignment  Sort Link Status  Clear Configuration

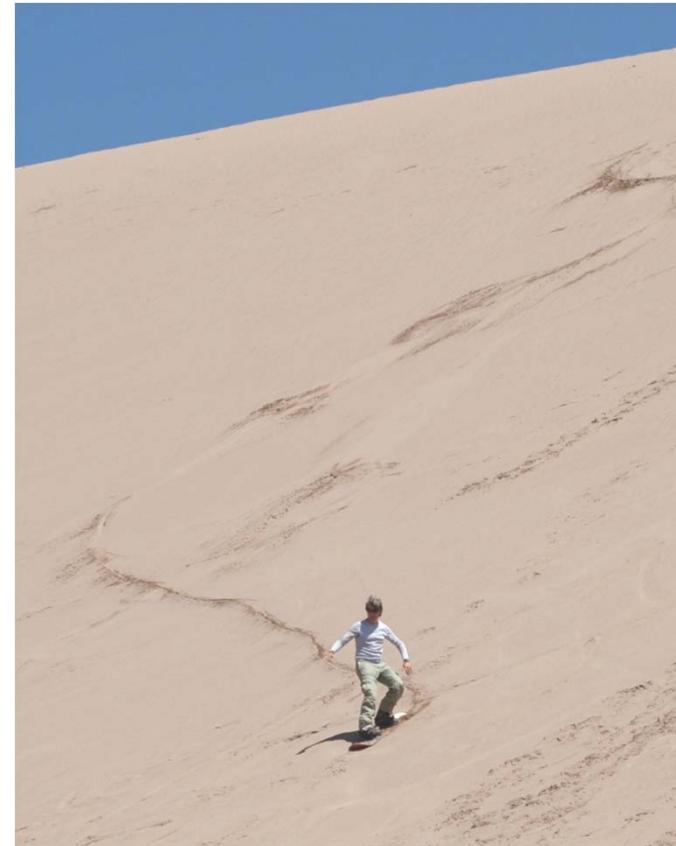
Edge-1.dna.anyweb.ch

Select All 172_24_200_224-
AnyDNACampus Select Groups Select Voice

Port	Status	Group	Voice
GigabitEthernet1/0/2	Up	DNA_Office	<input type="checkbox"/>
GigabitEthernet1/0/3	Up	DNA_NetMgt	<input type="checkbox"/>
GigabitEthernet1/0/7	Down	Segment: 172_24_200_224-AnyDNA	<input type="checkbox"/>
GigabitEthernet1/0/8	Up	Segment: 172_24_200_224-AnyDNA	<input checked="" type="checkbox"/>
GigabitEthernet1/0/9	Down		<input type="checkbox"/>
GigabitEthernet1/0/12	Down		<input type="checkbox"/>
GigabitEthernet1/0/13	Up		<input type="checkbox"/>
GigabitEthernet1/0/14	Down		<input type="checkbox"/>

Statische Zuweisung des VLAN zu einem Port

It's a journey



So

oder

so?



DNA Center

Mit dem DNA-Center bauen wir ein Netzwerk auf

- Einfach Klicken?
- Es werden:
 - Adressen festgelegt
 - Segmentierungen und Zonen festgelegt
 - DHCP Server ... bekanntgegeben
 - ...

→ Ein Konzept ist wichtiger denn je!



Hands-on DNA-Center



Hands-on: Host Onboarding festlegen

Interface Gi1/0/5 auf Switch Edge-1 statisch zuweisen

Aktueller Zustand: dynamisch

Ziel: Port ist für einen Office Benutzer ohne Dot1x eingerichtet



DNA Center - Hands-on: Host Onboarding festlegen

Konfig auf Switch-Port vor der Änderung:

```
Edge-1#show run interface gi1/0/5
Building configuration...

Current configuration : 625 bytes
!
interface GigabitEthernet1/0/5
    switchport mode access
    switchport voice vlan 4000
    device-tracking attach-policy IPDT_MAX_10
    authentication control-direction in
    authentication event server dead action authorize vlan 3999
    authentication event server dead action authorize voice
    authentication host-mode multi-auth
    authentication order dot1x mab
    authentication priority dot1x mab
    authentication port-control auto
    authentication periodic
    authentication timer reauthenticate server
    authentication timer inactivity server dynamic
    mab
    dot1x pae authenticator
    dot1x timeout tx-period 10
    spanning-tree portfast
end
```



DNA Center - Hands-on: Host Onboarding festlegen

Port Gi 1/0/5 konfigurieren:

Select Port Assignment

Edge-1.dna.anyweb.ch

Select Address Pool(VN) Select Groups Select Voice Pool(VN) Select Authentication

GigabitEthernet1/0/1 1/0/3 GigabitEthernet1/0/4 GigabitEthernet1/0/5 GigabitEthernet1/0/6
172_24_200_224-AnyDNACampus

GigabitEthernet1/0/2 172_24_200_240-AnyGuest GigabitEthernet1/0/9 GigabitEthernet1/0/10 GigabitEthernet1/0/11
172_24_200_208-AnyDNACampus

GigabitEthernet1/0/8 GigabitEthernet1/0/3 GigabitEthernet1/0/5 GigabitEthernet1/0/6
Segment: 172_24_200_208-AnyDNA

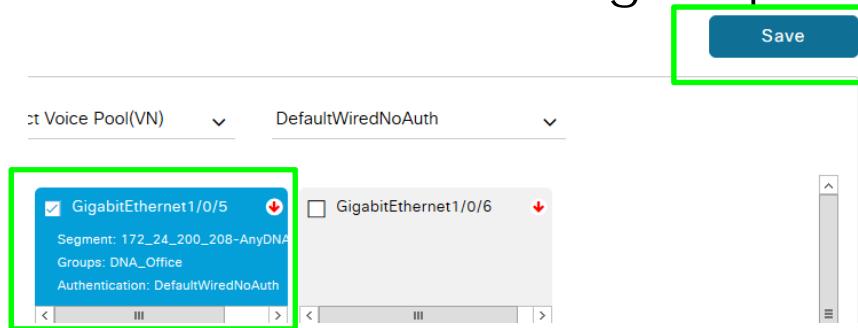
GigabitEthernet1/0/2 GigabitEthernet1/0/3 GigabitEthernet1/0/4 GigabitEthernet1/0/5 GigabitEthernet1/0/6
Segment: 172_24_200_208-AnyDNA

GigabitEthernet1/0/7 GigabitEthernet1/0/8 GigabitEthernet1/0/9 GigabitEthernet1/0/10 GigabitEthernet1/0/11
Segment: 172_24_200_208-AnyDNA



DNA Center - Hands-on: Host Onboarding festlegen

Port Gi 1/0/5 Änderungen speichern:



The screenshot shows the DNA Center interface for configuring a port. At the top, there are dropdown menus for 'Voice Pool(VN)' set to 'Default' and 'Authentication' set to 'DefaultWiredNoAuth'. Below these, a list of ports is displayed. The first port, 'GigabitEthernet1/0/5', is selected and highlighted with a green box. Its details are shown in a modal: Segment: 172_24_200_208-AnyDNA, Groups: DNA_Office, Authentication: DefaultWiredNoAuth. To the right of the port list is a vertical scrollbar. A large blue 'Save' button is located at the bottom right of the configuration area, also highlighted with a green box.

Port Gi 1/0/5 nach der Änderung

```
Edge-1#show run interface gi1/0/5
Building configuration...

Current configuration : 231 bytes
!
interface GigabitEthernet1/0/5
  switchport access vlan 1022
  switchport mode access
  device-tracking attach-policy IPDT_MAX_10
  load-interval 30
  cts manual
  policy static sgt 16
  no propagate sgt
  spanning-tree portfast
end
```

It's a journey





Hands-on: Policy erstellen

Benutzer der Gruppe Office sollen PC's der Gruppe NetMgt nicht erreichen können

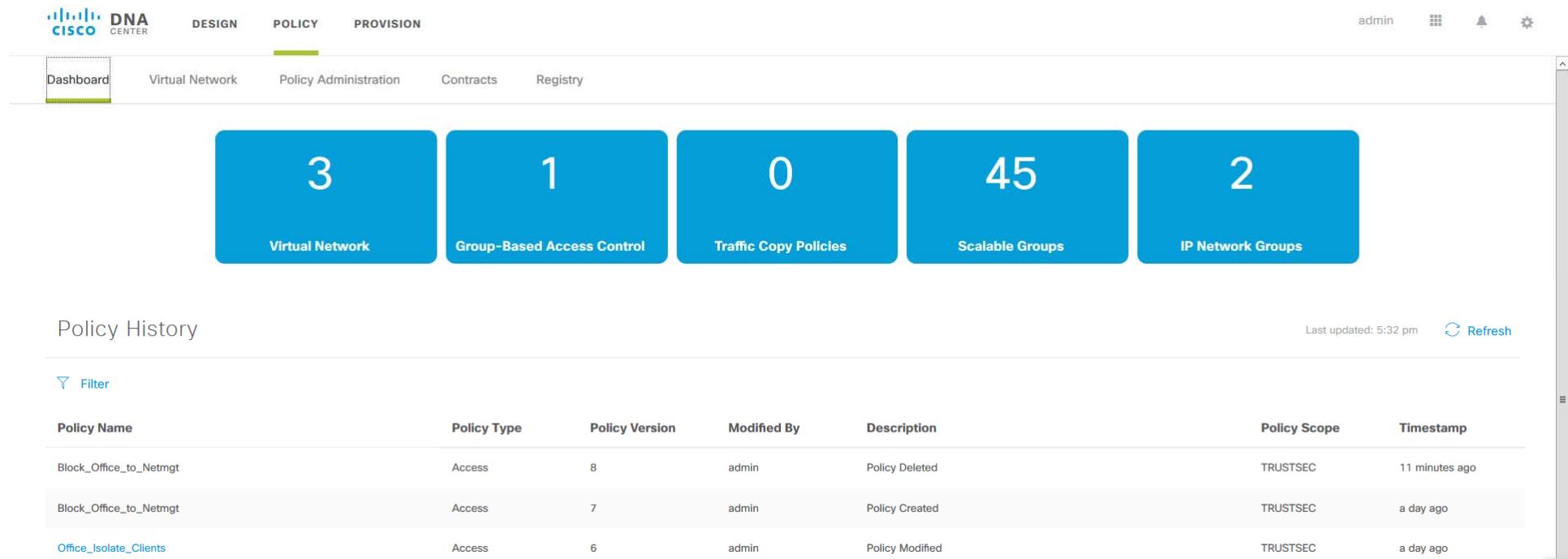
Aktueller Zustand: Beide Gruppen sind im gleichen Virtuellen Netz, als im gleichen VRF. Verkehr zwischen diesen beiden Gruppen ist im SDA erlaubt

Ziel: Eine Policy die den Verkehr verhindert



DNA Center - Hands-on: Policy erstellen

Policy Dashboard



The screenshot shows the Cisco DNA Center Policy Dashboard. At the top, there are tabs for DESIGN, POLICY (which is selected), and PROVISION. Below the tabs, there are links for Dashboard, Virtual Network, Policy Administration, Contracts, and Registry. On the right side, there are user status (admin) and navigation icons. The main area features five blue cards with white text: 3 Virtual Network, 1 Group-Based Access Control, 0 Traffic Copy Policies, 45 Scalable Groups, and 2 IP Network Groups. Below this, the Policy History section displays a table of recent policy changes. The table has columns for Policy Name, Policy Type, Policy Version, Modified By, Description, Policy Scope, and Timestamp. The data in the table is as follows:

Policy Name	Policy Type	Policy Version	Modified By	Description	Policy Scope	Timestamp
Block_Office_to_Netmgt	Access	8	admin	Policy Deleted	TRUSTSEC	11 minutes ago
Block_Office_to_Netmgt	Access	7	admin	Policy Created	TRUSTSEC	a day ago
Office_Isolate_Clients	Access	6	admin	Policy Modified	TRUSTSEC	a day ago



DNA Center - Hands-on: Policy erstellen

Add a Policy

- Policy Name
- Source- und Destination-gruppe bestimmen

Dashboard Virtual Network **Policy Administration** Contracts Registry

Group-Based Access Control Traffic Copy Policies

Create Policy by selecting Source, Destination, and applying a Contract

Policy Name* **Description (Optional)** **Contract*** [Add Contract](#)

Enable Policy Enable Bi-directional [i](#)

Available Scalable Groups

[Find](#)

AA	AW	AU	BY	CO	DM	DM
AAAS_MgmtEP ...	Analyzer_Wiresh ...	Auditors	BYOD	Contractors	DMZ_ExtranetEP ...	DMZ_ISP_AEPG
DM	DM	DM	DM	DM	DM	DM
DMZ_ISP_BEPG	DMZ_Lab_AEPG	DMZ_MgmtEPG	DMZ_MobileEP_ ...	DMZ_MobileEP_ ...	DMZ_Server_A ...	DMZ_Server_B
DM	DM	DM	DN	DN	DN	DE
DMZ_SyncEPG	DMZ_TransitEP ...	DMZ_WLAN_Guest	DNA_Guest	DNA_NetMgt	DNA_Office	Developers

Source Scalable Groups

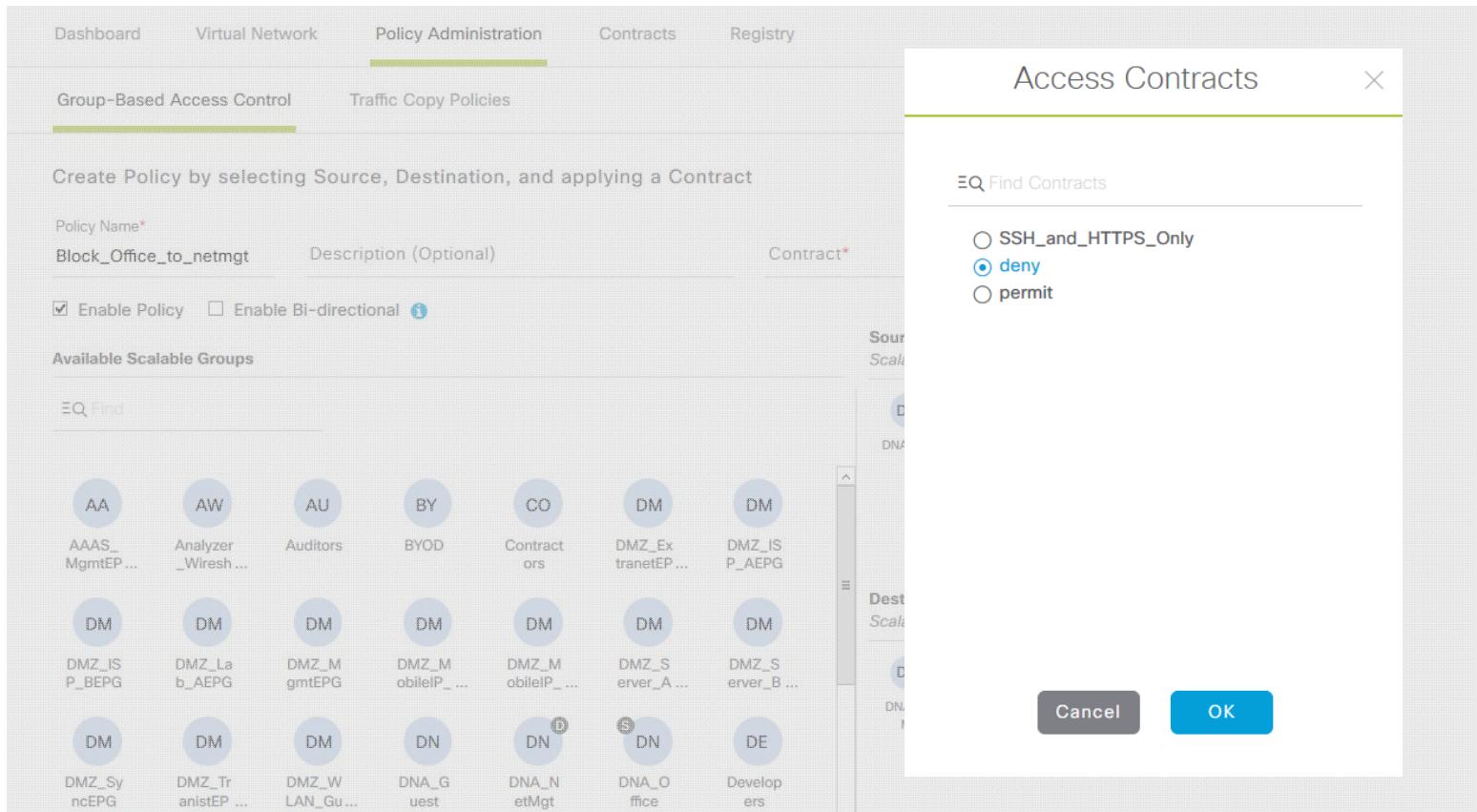
Destination Scalable Groups



DNA Center - Hands-on: Policy erstellen

Add a Policy

- Deny Contract zufügen



The screenshot shows the Cisco DNA Center interface with the 'Policy Administration' tab selected. A modal window titled 'Access Contracts' is open, allowing the creation of a new policy. The 'Contract*' field is set to 'deny'. The 'Source Scalable Groups' section lists various network entities represented by icons and names. The 'Dest Scalable Groups' section is partially visible. At the bottom right of the modal are 'Cancel' and 'OK' buttons.

Create Policy by selecting Source, Destination, and applying a Contract

Policy Name*
Block_Office_to_netmgt

Description (Optional)

Contract*
 SSH_and_HTTPS_Only
 deny
 permit

Available Scalable Groups

Source Scalable Groups

Group Type	Group Name	Description
AA	AAAS_MgmtEP ...	
AW	Analyzer_Wiresh ...	
AU	Auditors	
BY	BYOD	
CO	Contractors	
DM	DM_ExtranetEP ...	
DM	DM_ISP_AEPG	
DM	DM_ISP_BEPG	
DM	DM_Lab_AEPG	
DM	DM_MgmtEPG	
DM	DM_MobileIP_...	
DM	DM_MobileIP_...	
DN	DN_Server_A ...	
DN	DN_Server_B ...	
DN	DN_SyncEPG	
DN	DN_TrainistEP ...	
DN	DN_WLAN_Guest	
DE	Developers	
DN	DNA_NetMgt	
DN	DNA_Office	

Dest Scalable Groups

Group Type	Group Name	Description
DN	DN_Auditors	
DN	DN_BYOD	
DN	DN_Contractors	
DN	DN_ExtranetEP ...	
DN	DN_ISP_AEPG	
DN	DN_ISP_BEPG	
DN	DN_Lab_AEPG	
DN	DN_MgmtEPG	
DN	DN_MobileIP_...	
DN	DN_MobileIP_...	
DN	DN_Server_A ...	
DN	DN_Server_B ...	
DN	DN_SyncEPG	
DN	DN_TrainistEP ...	
DN	DN_WLAN_Guest	
DE	DE_Developers	

Access Contracts

Find Contracts

SSH_and_HTTPS_Only
 deny
 permit

OK **Cancel**



DNA Center - Hands-on: Policy erstellen

Add a Policy

- Policy speichern

Group-Based Access Control Traffic Copy Policies

Create Policy by selecting Source, Destination, and applying a Contract

Policy Name* Description (Optional)
 Enable Policy Enable Bi-directional 

Contract*  Add Contract  Cancel  Save

Enable Policy Enable Bi-directional 

Available Scalable Groups

Source Scalable Groups

Destination Scalable Groups

Find 

AA	AW	AU	BY	CO	DM	DM
AAAS_MgmtEPG ...	Analyzer_Wiresh ...	Auditors	BYOD	Contract ors	DMZ_ExtranetEP ...	DMZ_ISP_AEPG
DM	DM	DM	DM	DM	DM	DM
DMZ_ISP_BEPG	DMZ_Lab_AEPG	DMZ_MgmtEPG	DMZ_MobileEP ...	DMZ_MobileEP ...	DMZ_Server_A ...	DMZ_Server_B ...
DM	DM	DM	DN	DN	DN	DE
DMZ_SyncEPG	DMZ_TrainistEP ...	DMZ_WLAN_Gu ...	DNA_Guest	DNA_NetMgt	DNA_Office	Develop ers
DS	EM	GU	IN	IN	IN	IN
Develop	Employe	Guests	INTRAN	INTRAN	INTRAN	INTRAN

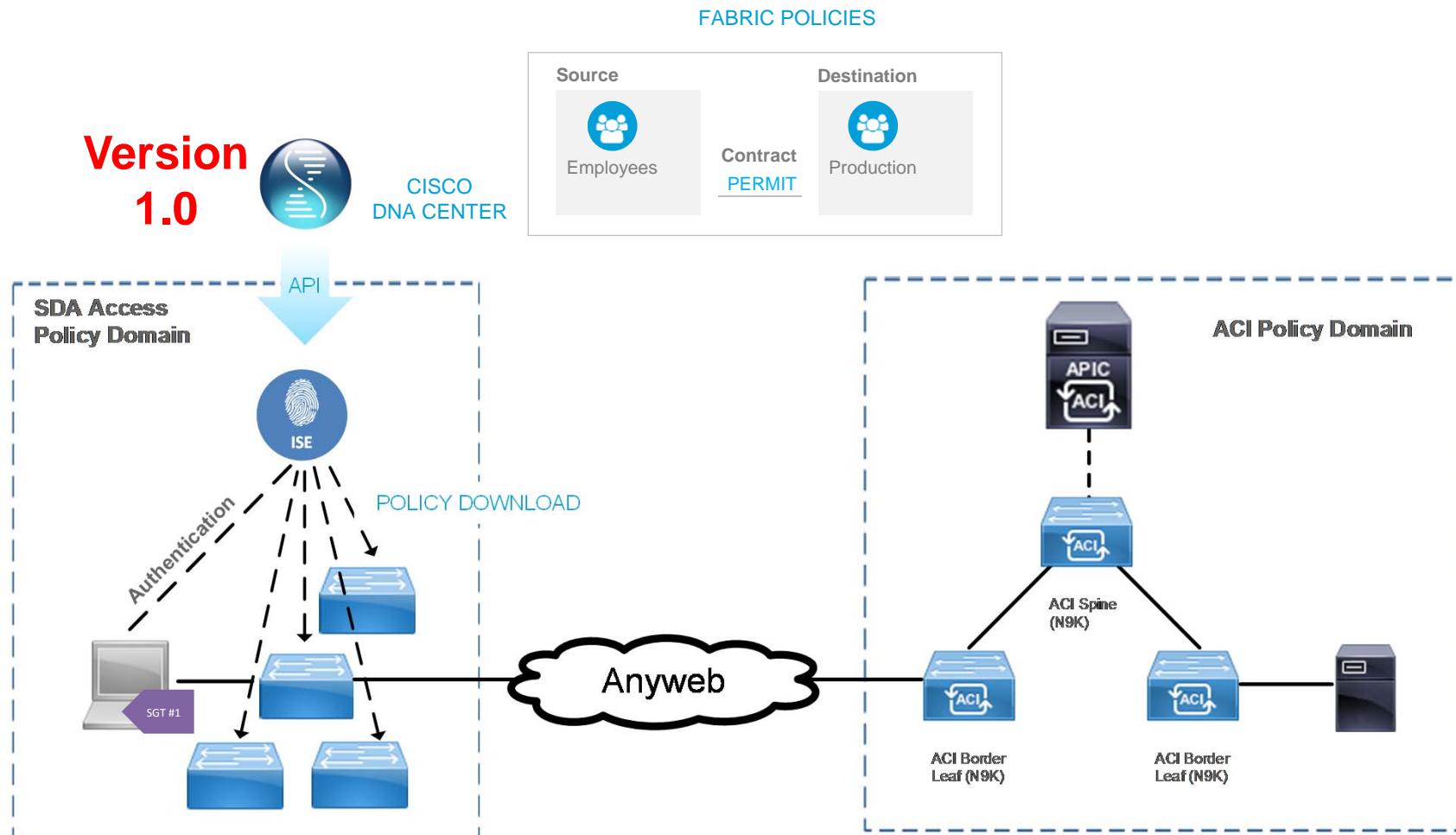
Setup

End-2-End Segmentierung mit Cisco DNA

Maria Koceba

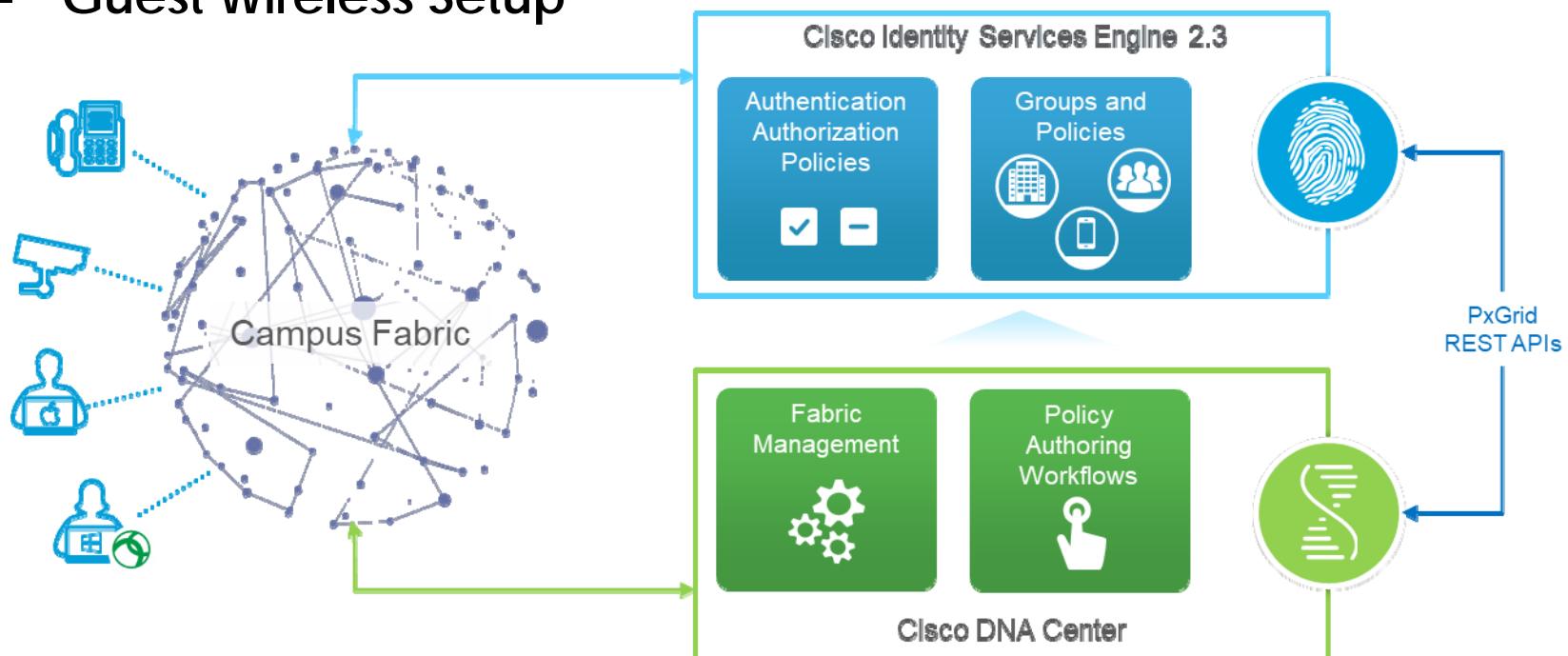
Source	Destination				
	Employee	Suppliers	App Servers	Shared Services	Non-Compliant
Employee	✓	✗	✓	✓	✗
Suppliers	✗	✓	✗	✓	✗
App Servers	✓	✗	✓	✗	✗
Shared Services	✓	✓	✗	✓	✗
Non-Compliant	✗	✗	✗	✗	✗

Putting it together..

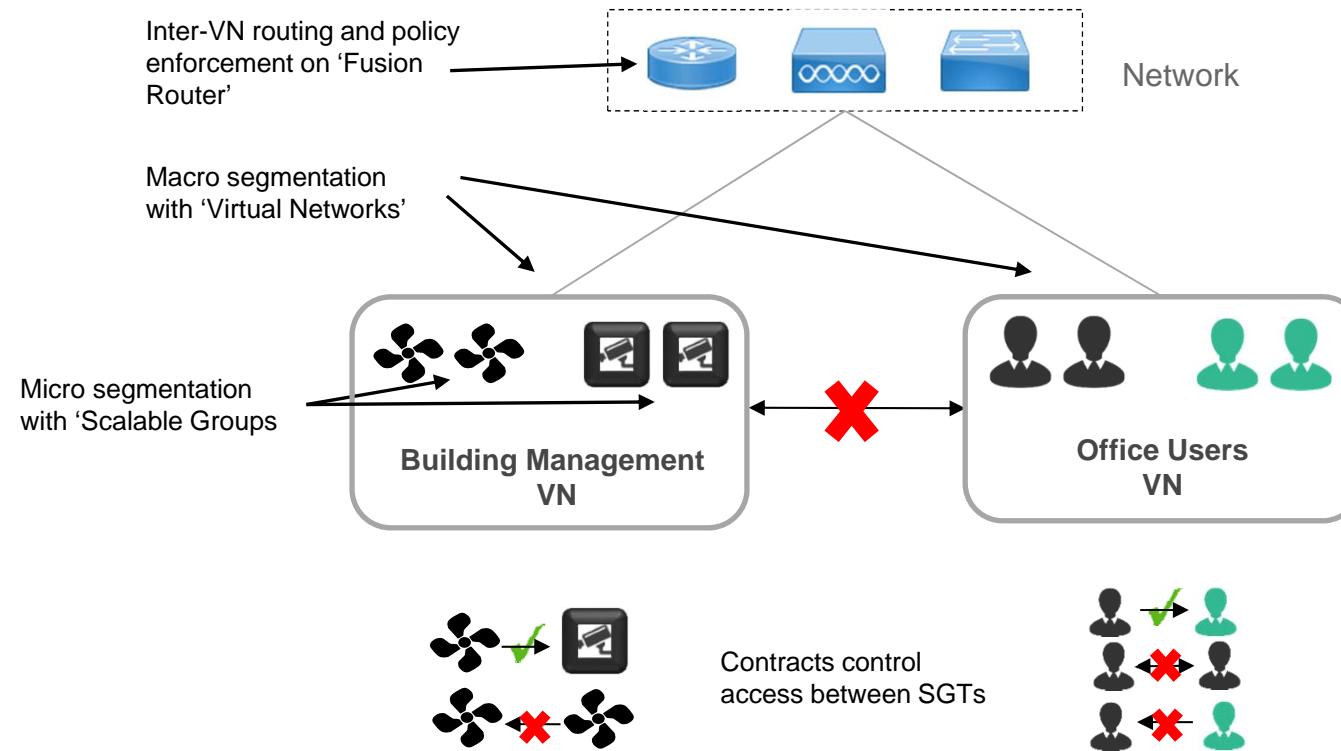


Rolle von ISE in DNA Center

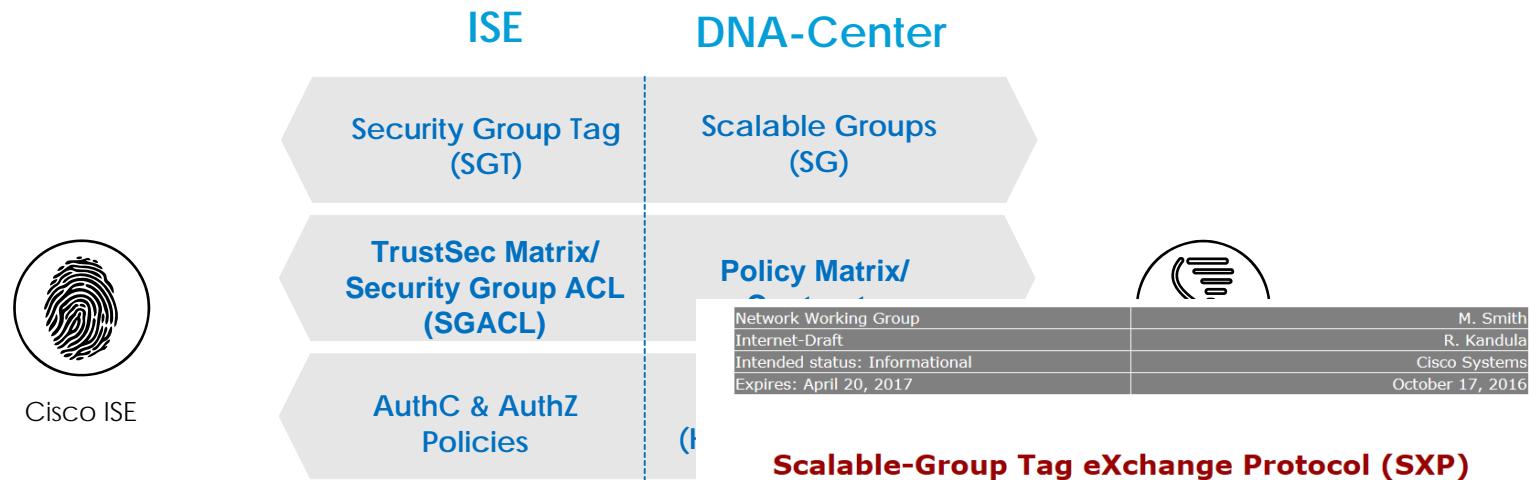
- Access Control/Host On-boarding (User/Device Authentication)
- Role-based Segmentation
- Guest Wireless Setup



Macro- und Micro-Segmentierung dank DNA



ISE & DNA Begriffe



Cisco TrustSec (CTS) builds secure networks by establishing domains of trust. Communication between devices in the domain is secured with a combination of encryption, authentication, and access control.

The Security Group Tag (SGT) Exchange Protocol (SXP) is one of several protocols developed for propagating IP-to-SGT binding information across network devices that are connected to upstream devices in the network. This process allows security services on sev-

- [Finding Feature Information](#)
- [Prerequisites for Cisco TrustSec SGT Exchange Protocol IPv4](#)
- [Restrictions for Cisco TrustSec SGT Exchange Protocol IPv4](#)
- [Information About Cisco TrustSec SGT Exchange Protocol IPv4](#)
- [How to Configure the Cisco TrustSec SGT Exchange Protocol IPv4](#)

This document discusses scalable-group tag exchange protocol (SXP), a control protocol to propagate IP address to Scalable Group Tag (SGT) binding information across network devices.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

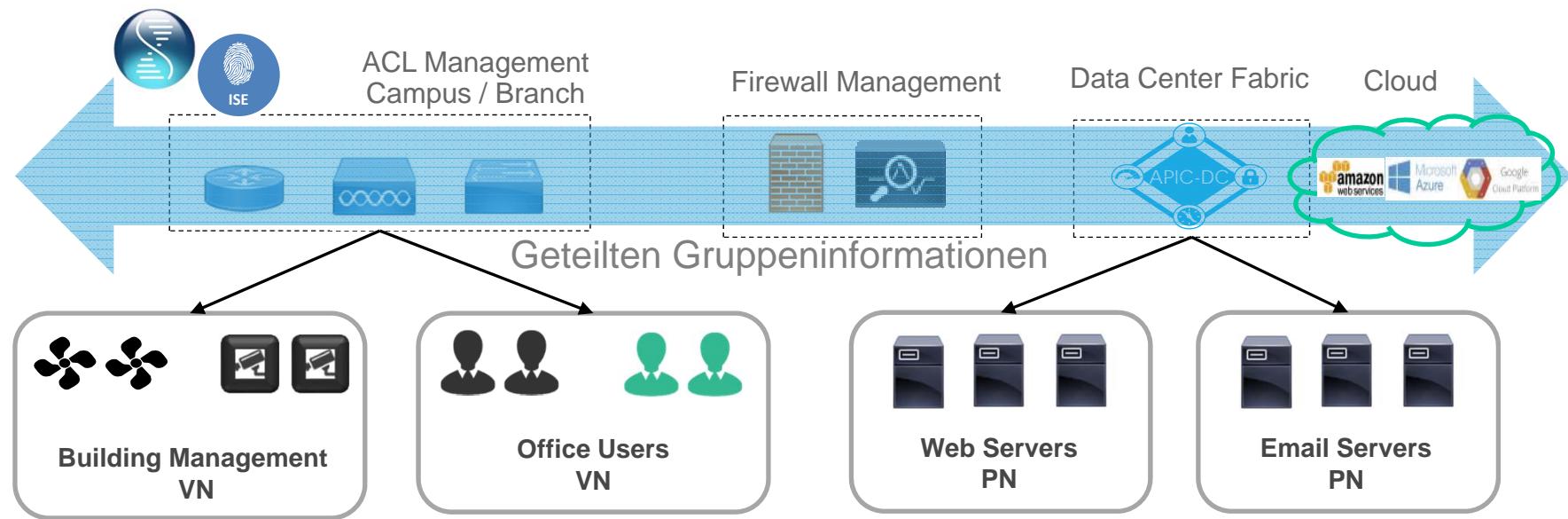
Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

Vision



DNA Readiness

Wie kann DNA / SDA eingeführt werden?

→ It's a journey



It's a journey



DNA Readiness

Wie kann DNA / SDA eingeführt werden?

- Warten auf Release 1.1 → November 2017
- Ziele festlegen
- HW auf readiness prüfen inklusive IOS Stand
- Vorgehen festlegen
- Konzept erarbeiten
- Aufbau, Test, Migration

DNA Readiness

Ziele festlegen

- Welche Bereiche des Netzwerkes sollen umgestellt werden
 - Ergibt u.a. eine Liste der betroffenen Komponenten
- Soll das Data Center eingebunden werden
- Wird WLAN eingebunden
- Zeitrahmen festlegen
 - Kann das Projekt mit dem regulären Lifecycle realisiert werden
 - SDA Einführung Lifecycle anpassen oder umgekehrt

DNA Readiness

Ziele festlegen

- Welche Funktionen sollen im SDA unterstützt werden?

- Soll ein Proof of Concept durchgeführt werden
 - Anyweb empfiehlt das klar

DNA Readiness

Betroffene Komponenten (Switches, WLC, ...) prüfen

- Welche Hardware wird unterstützt?
- Passt die Lizenz?
- Materialliste erstellen
 - DNA-Center Appliance
 - ISE 2.3
 - Switches?
 - WLC?

DNA Readiness

Vorgehen festlegen

- PoC / PoV
 - Aufbau
 - Tests
- Migration
 - Schrittweise
 - Alles auf einmal – nicht empfohlen
- Materialbestellung

DNA Readiness

Konzept erarbeiten

Das Netz wird neu gebaut!

- Dem Konzept kommt eine grosse Bedeutung zu
- Konzeptionelle Änderungen sind auch mit SDA nicht cool
- Viele Bereiche des Netzwerkes inklusive Segmentierung und Benutzeroberfläche sind betroffen

DNA Readiness

Aufbau, Tests, Migration

- Grundlemente aufbauen
 - DNA-Center
 - ISE einbinden
- Border vorbereiten
 - Wenn möglich eine nicht auf einem produktiven Router
- Erster Edge/Access Switch einbinden
- Ausführlich Testen
- (schrittweise) Migration

It's a journey

Mars needs network engineers



Ischs no wiit?

Nei, jetzt immer da Schatz!

Weitere Schritte

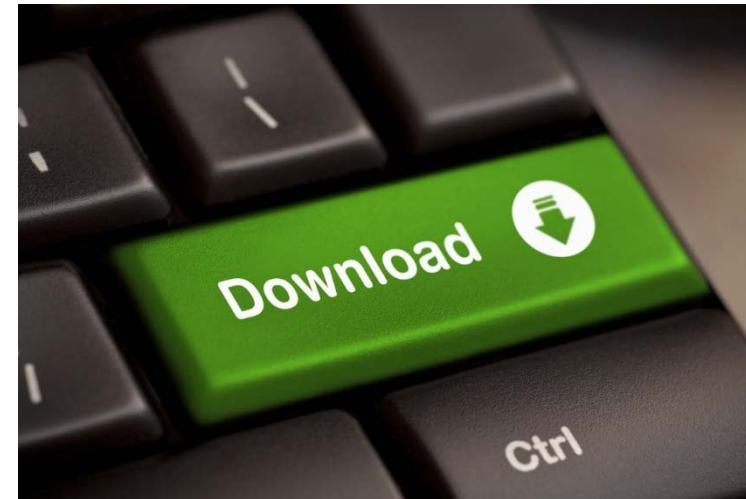
- **Ausbildung**
 - Standardkurse
 - Network Programm
 - Zugeschnitten
- **Planungsworkshop**
 - Design
 - PoC
- **Quick start**
 - Mentoring
- **Mache den ersten Sch**
 - ACI
 - DNA
 - ISE

Cisco Kurse				
Basis Cisco Training (CCENT)				
Routing & Switching CCNA / CCNP				
Wireless CCNA / CCNP				
Enterprise Networking Solutions				
Network Programmability & SDN				
Kurscode	Titel	Dauer	Verfügbare Daten	Status
PYN	Python for Networkers	3 Tage	28.11.2017	
			16.01.2018	
			03.04.2018	
			15.05.2018	
APIC-EM INTRO	APIC-EM Introduction	1 Tag	03.11.2017	
			13.04.2018	
			13.07.2018	
NPI	Introduction to Cisco Network Programmability	3 Tage	24.01.2018	
			07.05.2018	
NPDES1	Designing and Implementing Cisco Network Programmability	5 Tage	05.02.2018	
			28.05.2018	
Security CCNA / CCNP				
ASA & ISE Training				
Collaboration (Voice) CCNA / CCNP				
Data Center CCNA / CCNP				
ACI Training				
Service Provider CCNA / CCNP				



Präsentationen

- Die Präsentationen stehen nach der Veranstaltung auf der AnyWeb Homepage zum Download bereit
 - <http://www.anyweb.ch/events/>





30. November: AnyWeb Practice Circle Cyber Security

AnyWeb AG

Practice Circle Oktober 2017

Page 102



Networking und Apéro



