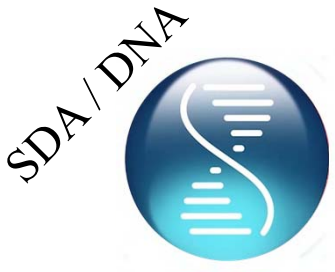
Create. Connect. Control.

anyweb

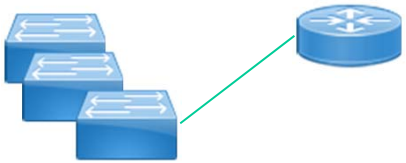
AnyWeb Practice Circle: Cisco ISE verbindet ACI und SDA

Wim van Moorsel
Fabian Aeppli
Maria Koceba
Edi Layritz

Create. Connect. Control.
anyweb



Security / Policy
Scalability



Campus

Data Center

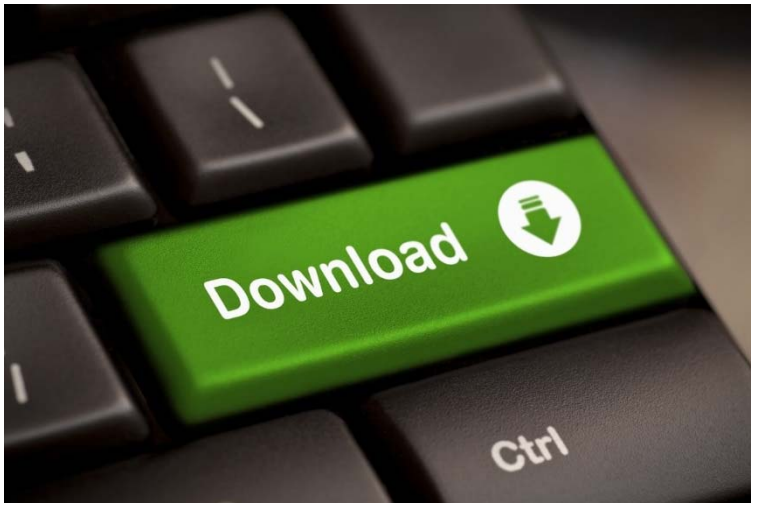
End-to-End

Create. Connect. Control.

Präsentationen

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

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



Create. Connect. Control.
anyweb

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

Create. Connect. Control.

anyweb

Setup

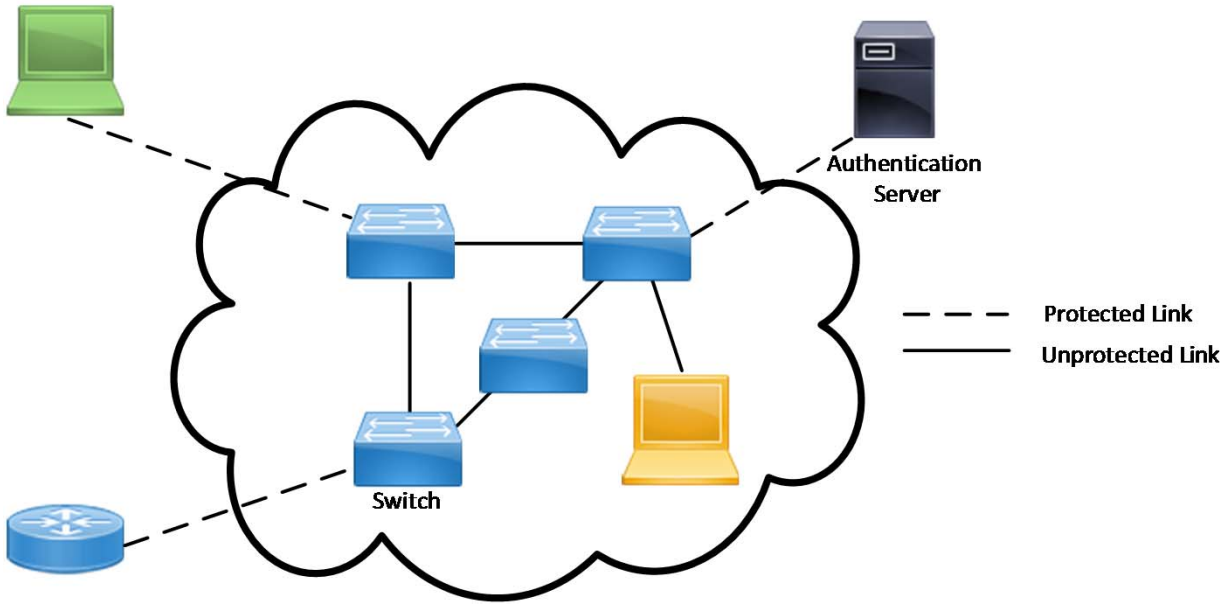
End-2-End Segmentierung mit Cisco TrustSec

Maria Koceba

Create. Connect. Control.

Cisco TrustSec

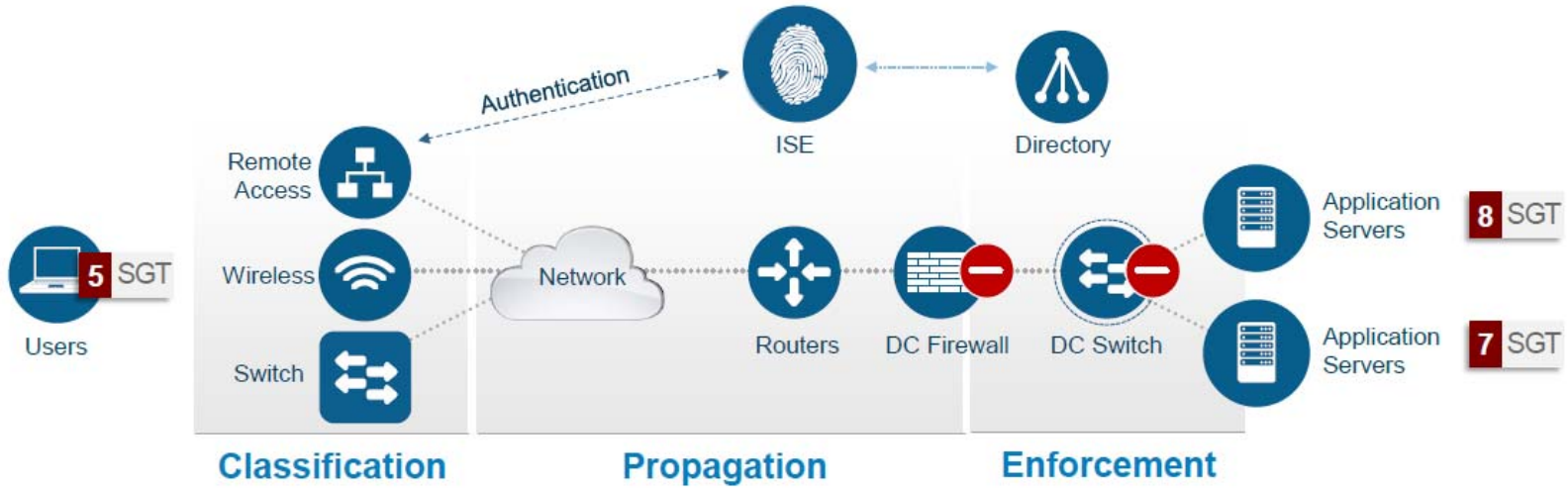
- Authentisierte Netzwerkinfrastruktur
- **Rollenbasierte Zugriffskontrolle**
- Sichere Kommunikation mit L2 Encryption



Create. Connect. Control.
anyweb

Rollenbasierte Zugriffskontrolle

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



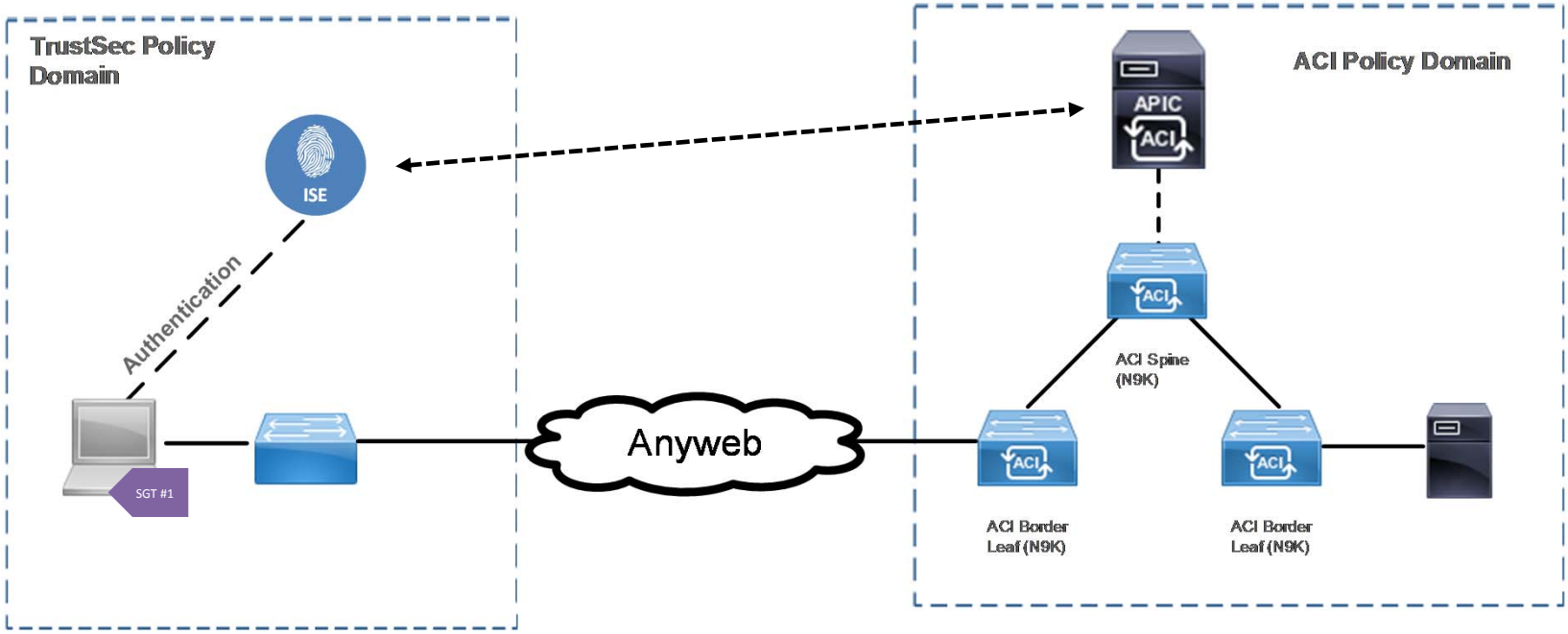
- statisch
- dynamisch

- Inline tagging
- SXP

- Group Based Policies ACLs
- Firewall Rules

Create. Connect. Control.
anyweb

Labor Aufbau

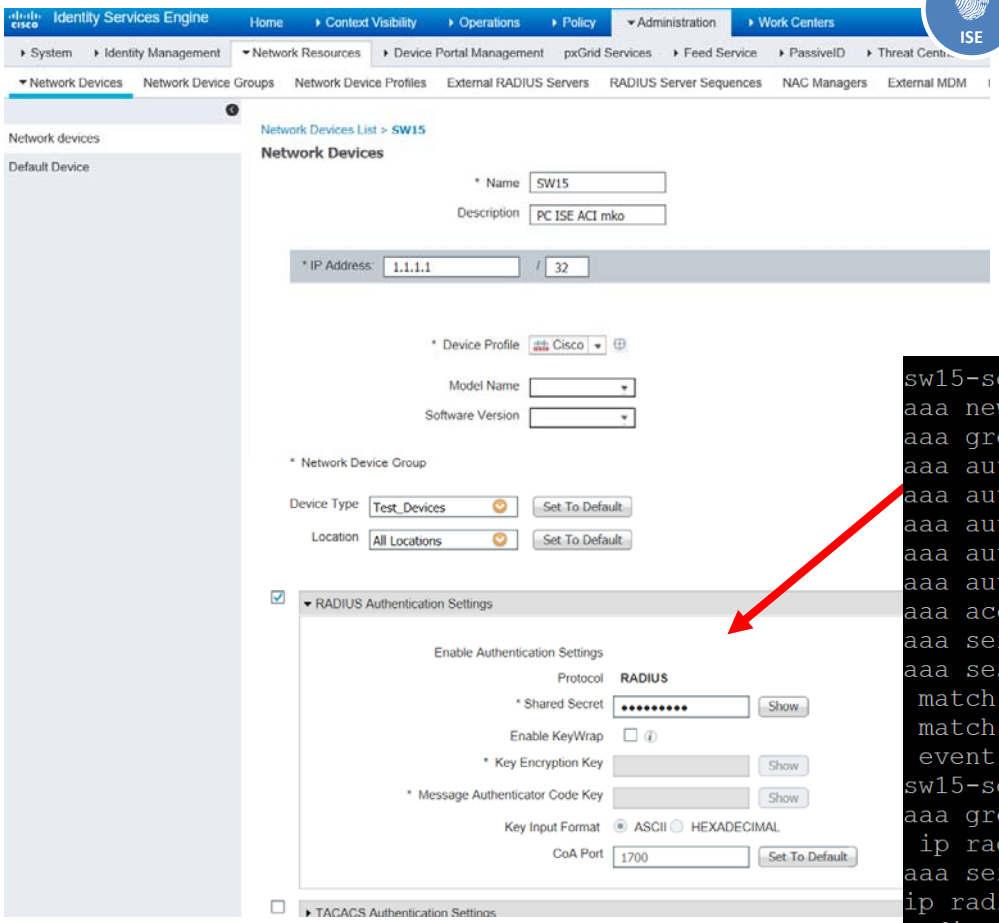


1. **Anbindung Switch – ISE (mit IBNS 2.0)**
2. **Anbindung ISE – ACI**
3. **Aufbau von TrustSec Domain**
4. **Klassifizierung**

Create. Connect. Control.
anyweb

1. Anbindung Switch - ISE

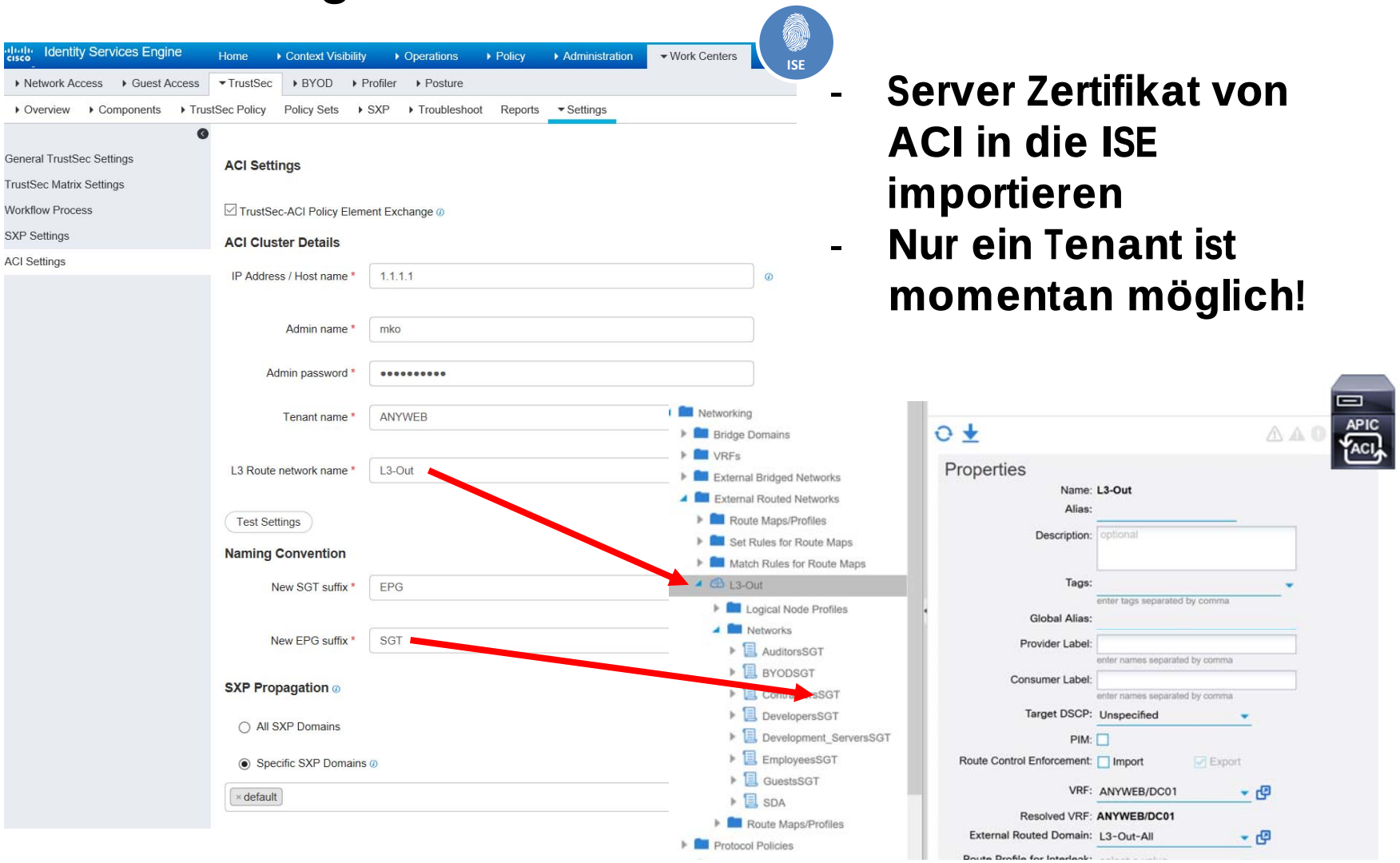
- **Switch in ISE erfassen**
- **RADIUS Konfiguration auf dem Switch**




```
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#
```

Create. Connect. Control.

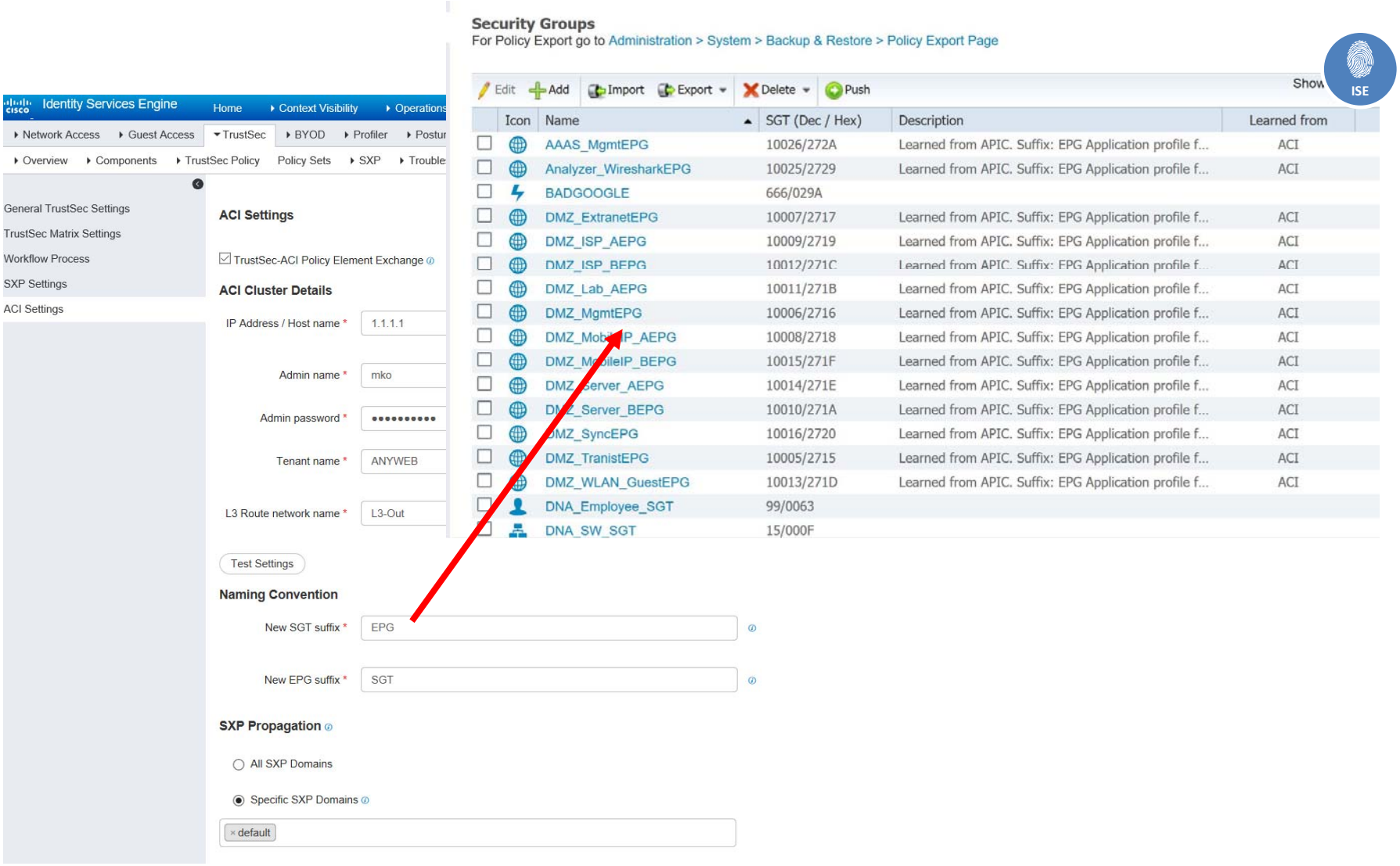
2. Anbindung ISE - ACI



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

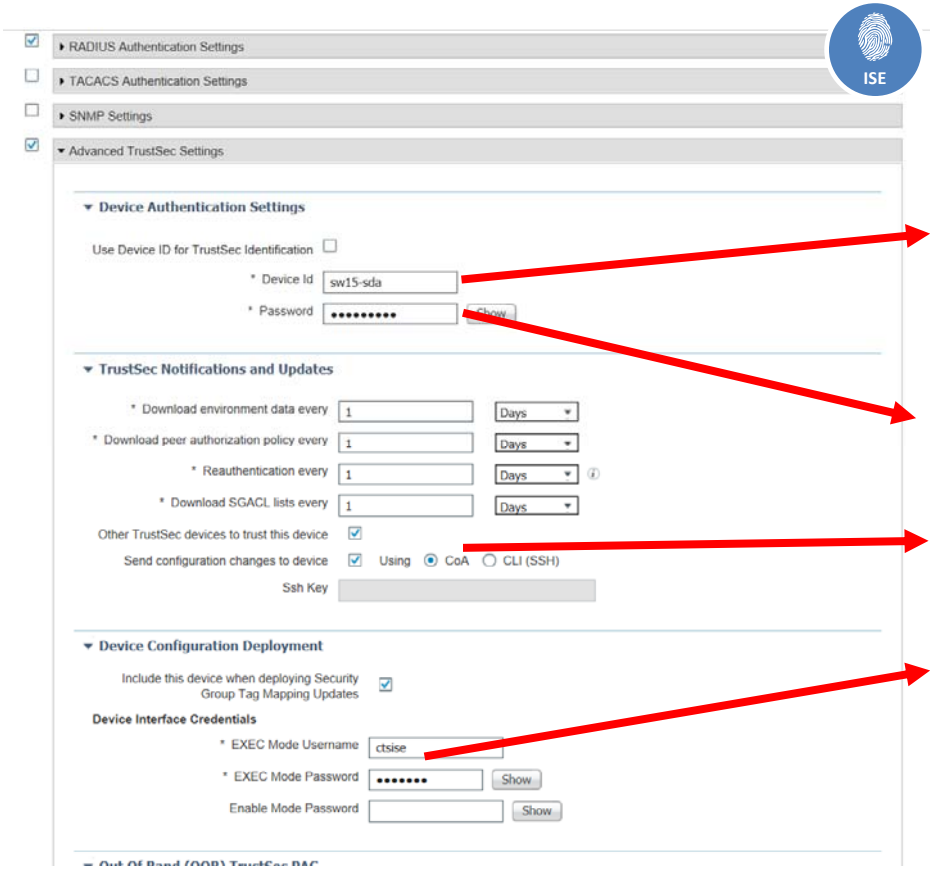
Create. Connect. Control.

2. Anbindung ISE - ACI



Create. Connect. Control.
anyweb

3. Aufbau von TrustSec Domain




```
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
!
```

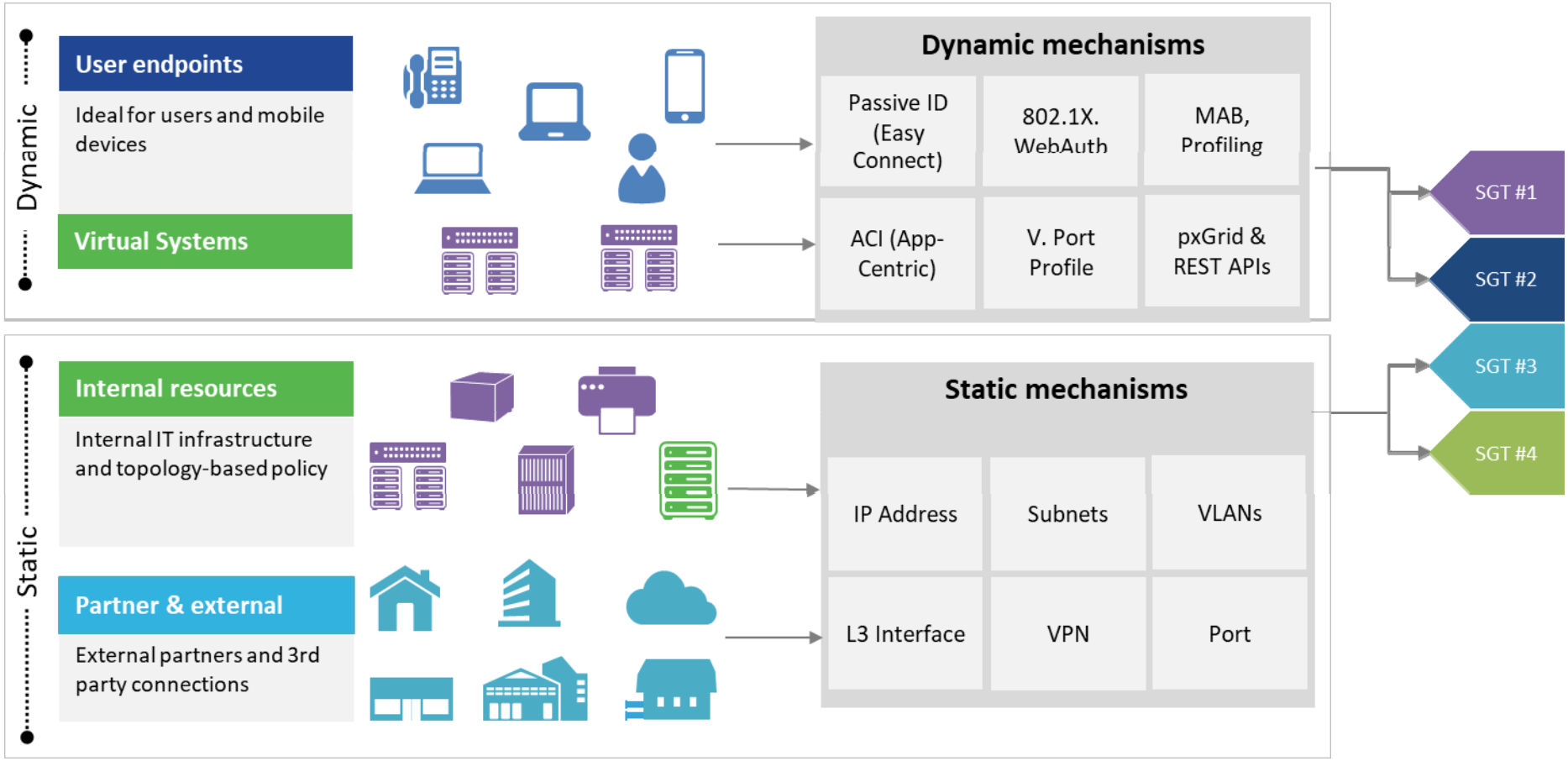
```
!
aaa server radius dynamic-author
 client 1.1.1.1 server-key CISCODNA
```

```
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**

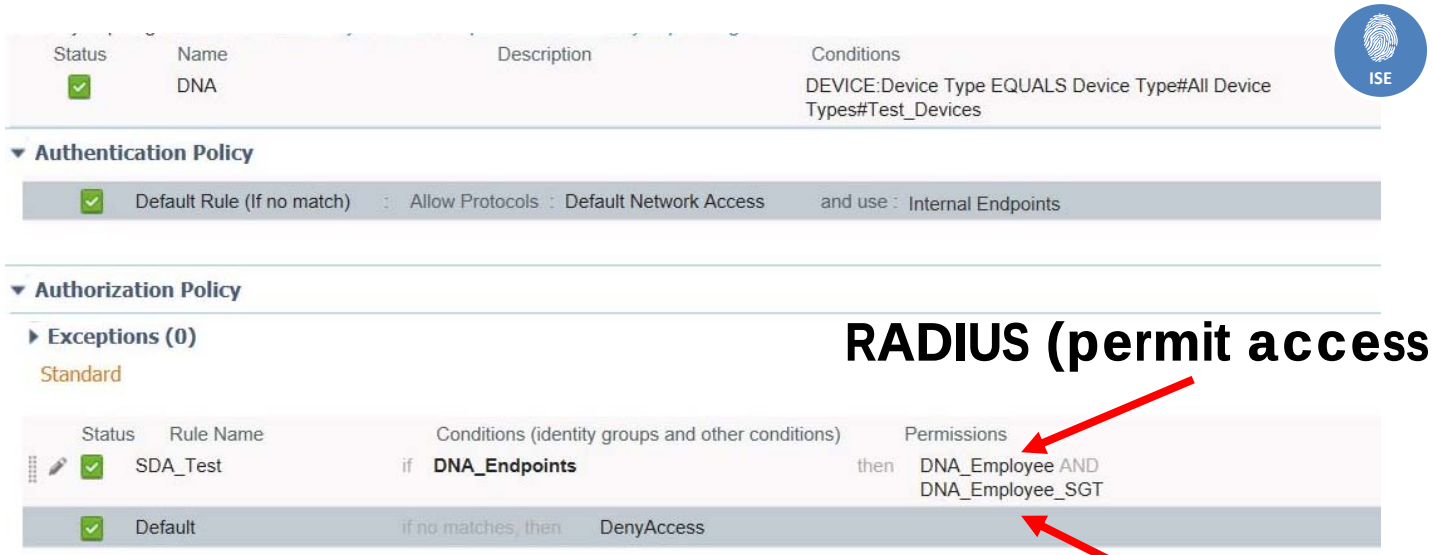
Create. Connect. Control.

Klassifizierungsmethoden



Create. Connect. Control.
anyweb

AuthN/AuthZ Policy



RADIUS (permit access + VLAN ID)

TrustSec (Tag)

```
!
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
!
```

Switchport Konfiguration mit dem IBNS 2.0

Create. Connect. Control.

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:AC17965300000010573F
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Typ	(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

ISE

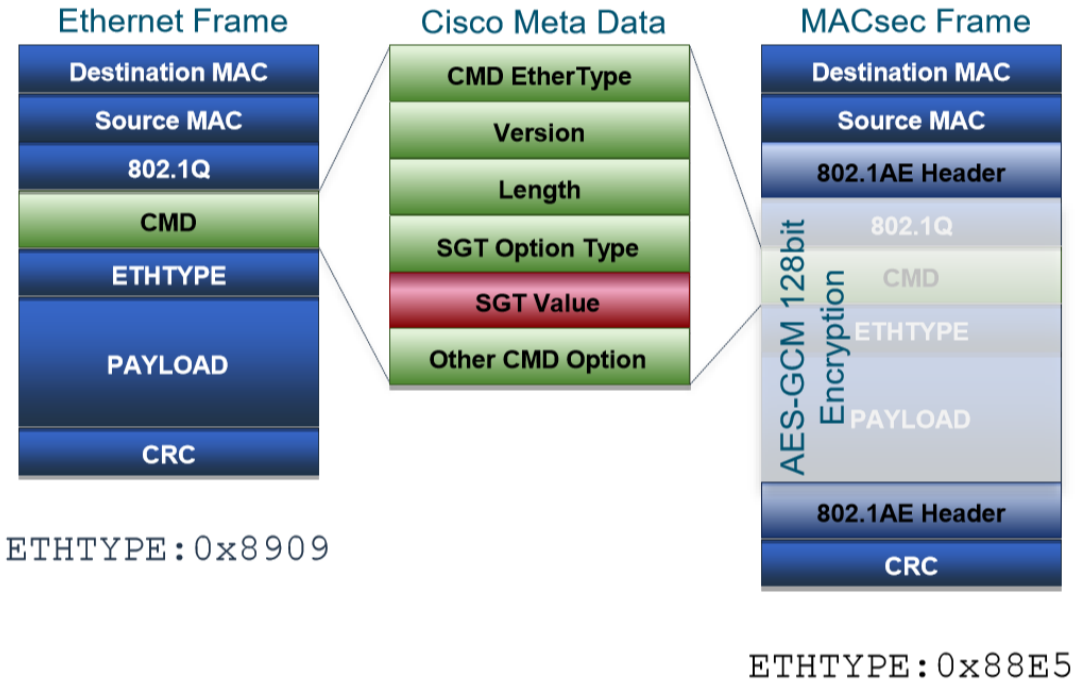
Source Timestamp	2017-10-26 07:54:35.973
Received Timestamp	2017-10-26 07:54:35.973
Policy Server	ise01
Event	5200 Authentication succeeded
Username	04:7D:7B:30:F0:62
User Type	Host
Endpoint Id	04:7D:7B:30:F0:62
Calling Station Id	04-7D-7B-30-F0-62
Endpoint Profile	Unknown
Authentication Identity Store	Internal Endpoints
Identity Group	DNA_Endpoints
Audit Session Id	AC17965300000010573F1C98
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

Create. Connect. Control.
anyweb

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**

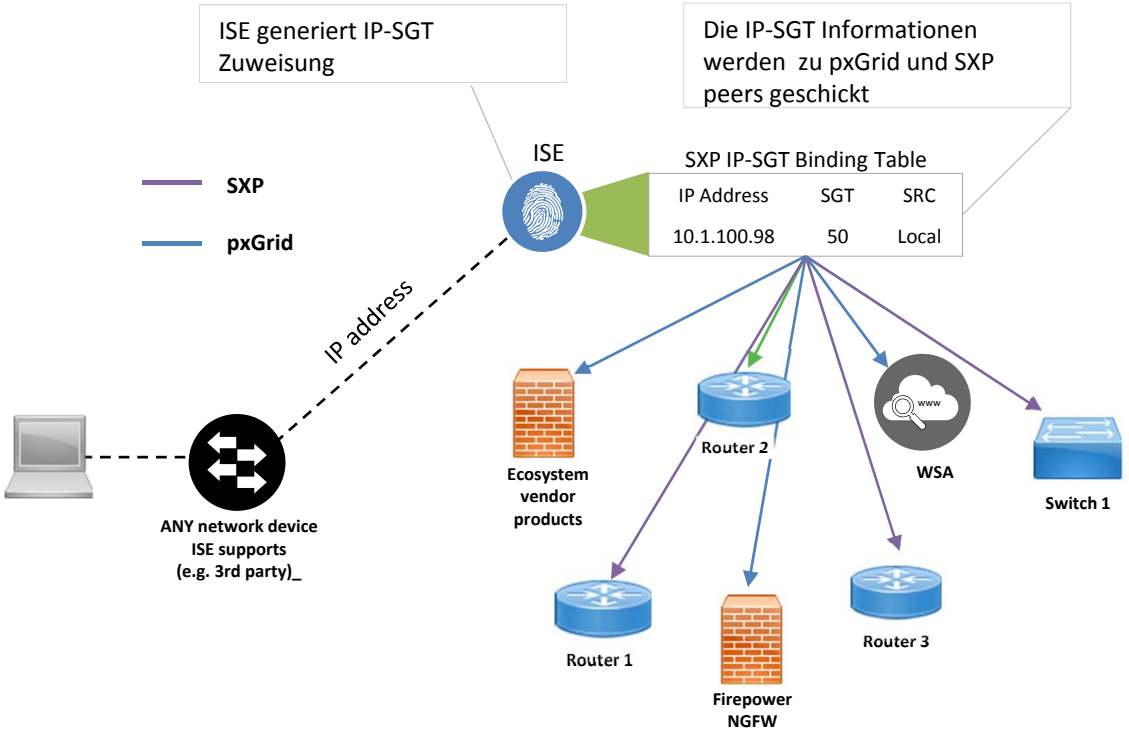


Create. Connect. Control.
anyweb

Propagation – SXP (SGT eXchange Protokoll)

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

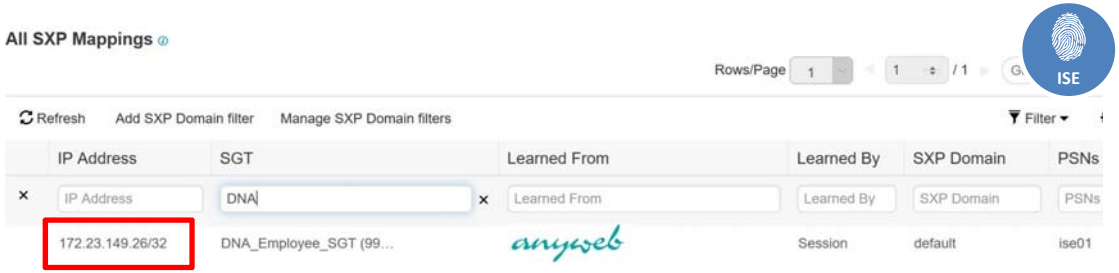
- **Nachteile:**
- **Eine Tabelle mehr…**
- **Skaliert nicht so gut**



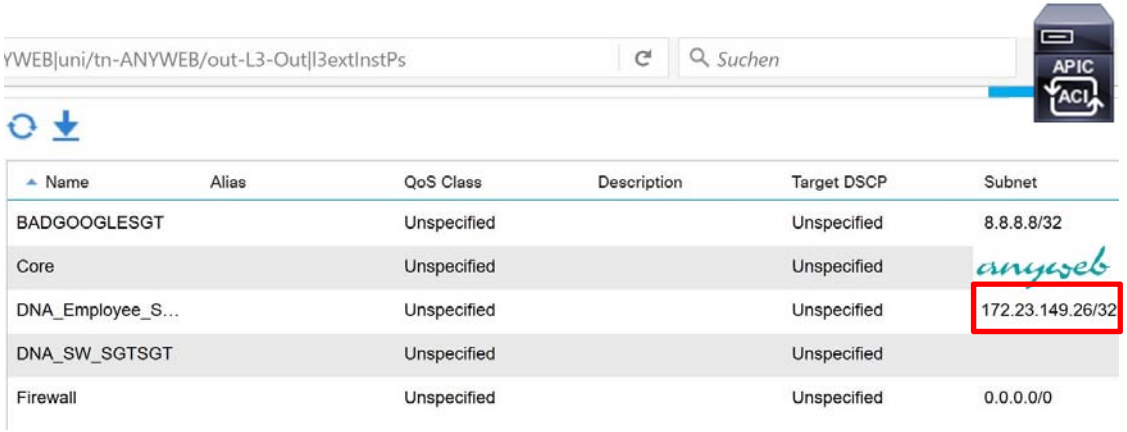
Create. Connect. Control.

Propagation – SXP (SGT eXchange Protokoll)

- **ISE erfährt IP zu SGT Zuweisung (von Switch) in AAA Accouting Paket**



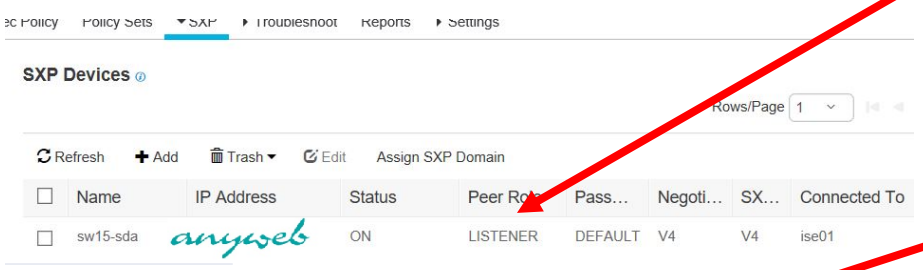
- **IP zu SGT Informationen werden dann mittels SXP zu ACI weitergegeben.**

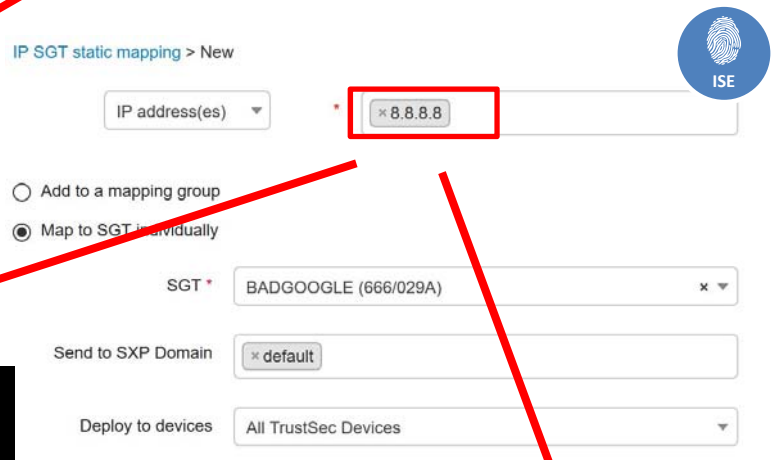


Create. Connect. Control.

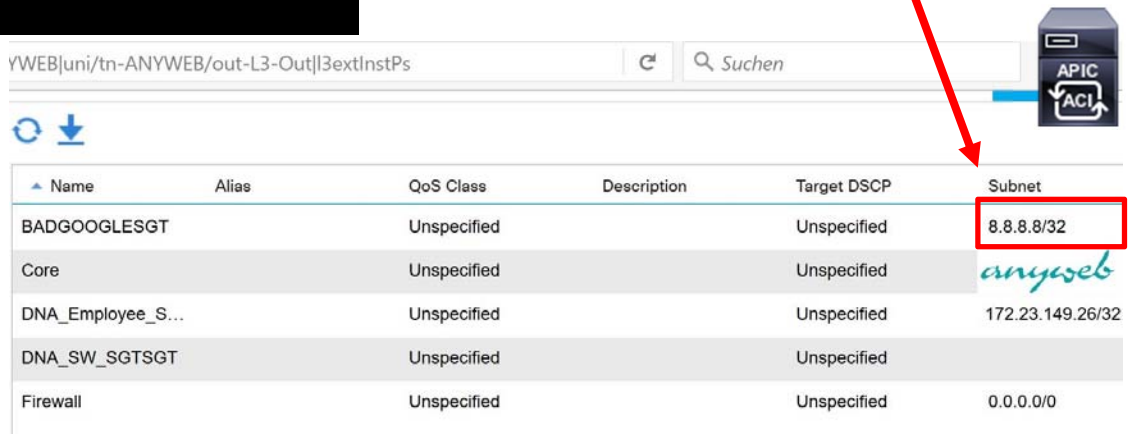
Propagation – SXP (SGT eXchange Protokoll)

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





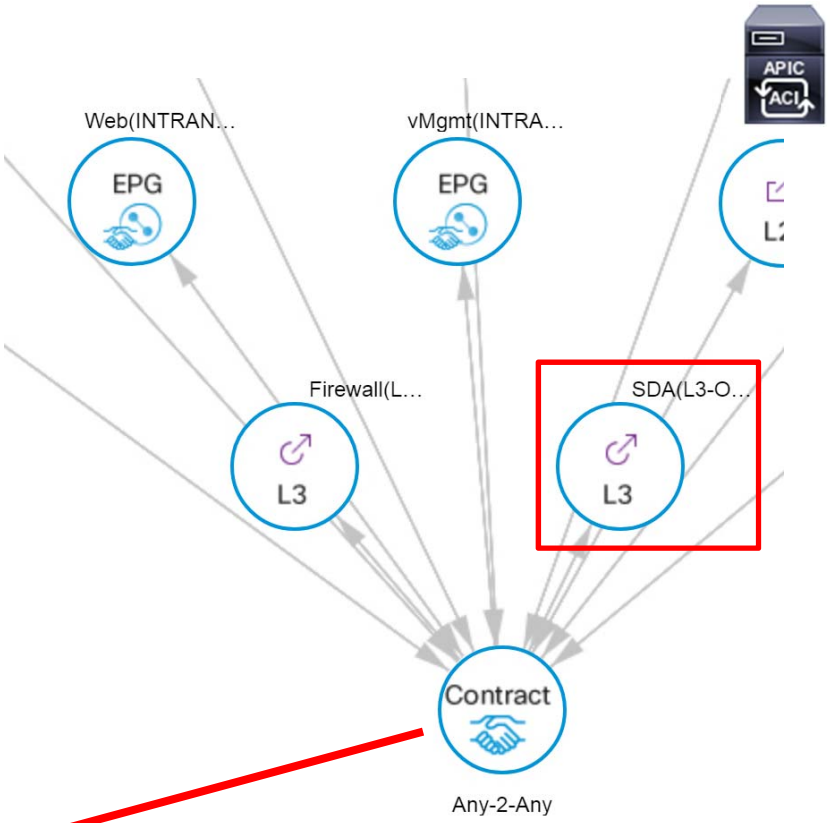

```
sw15-sda#       sh cts sxp sgt-map
SXP Node ID(generated):0xAC179653(172.23.150.83)
IP-SGT Mappings as follows:
IPv4,SGT: <8.8.8.8 , 666:BADGOOGLE>
source  : SXP;
Peer IP : 1.1.1.1
```



Create. Connect. Control.
anyweb

Enforcment auf ACI

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



Contract ≈ ACL

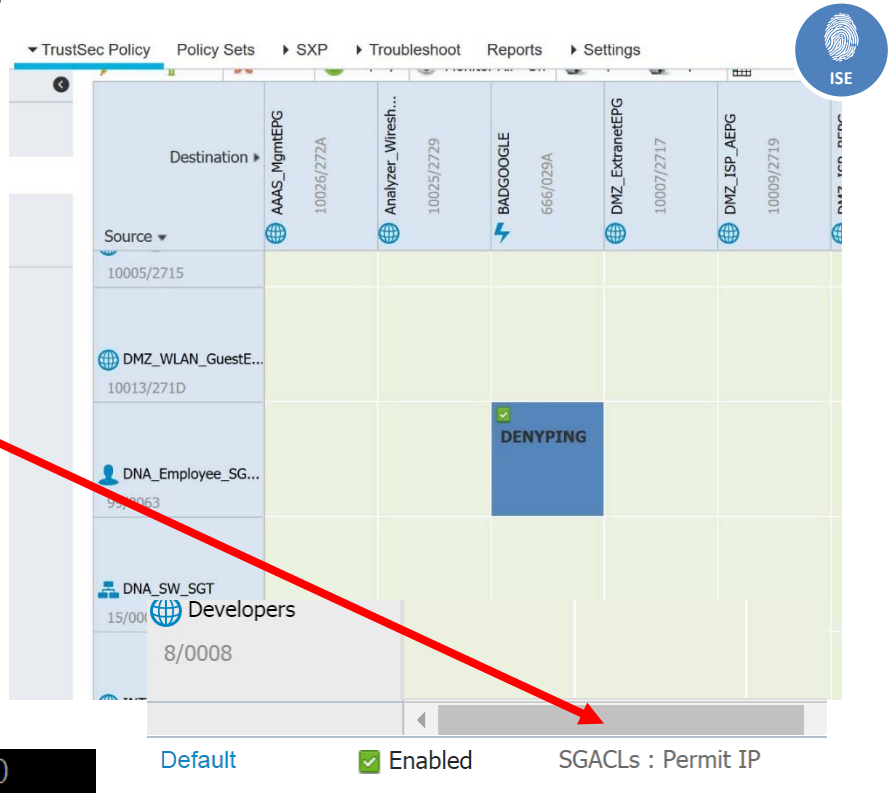
Filter Entries:

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

Create. Connect. Control.

Enforcment auf dem Switch

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

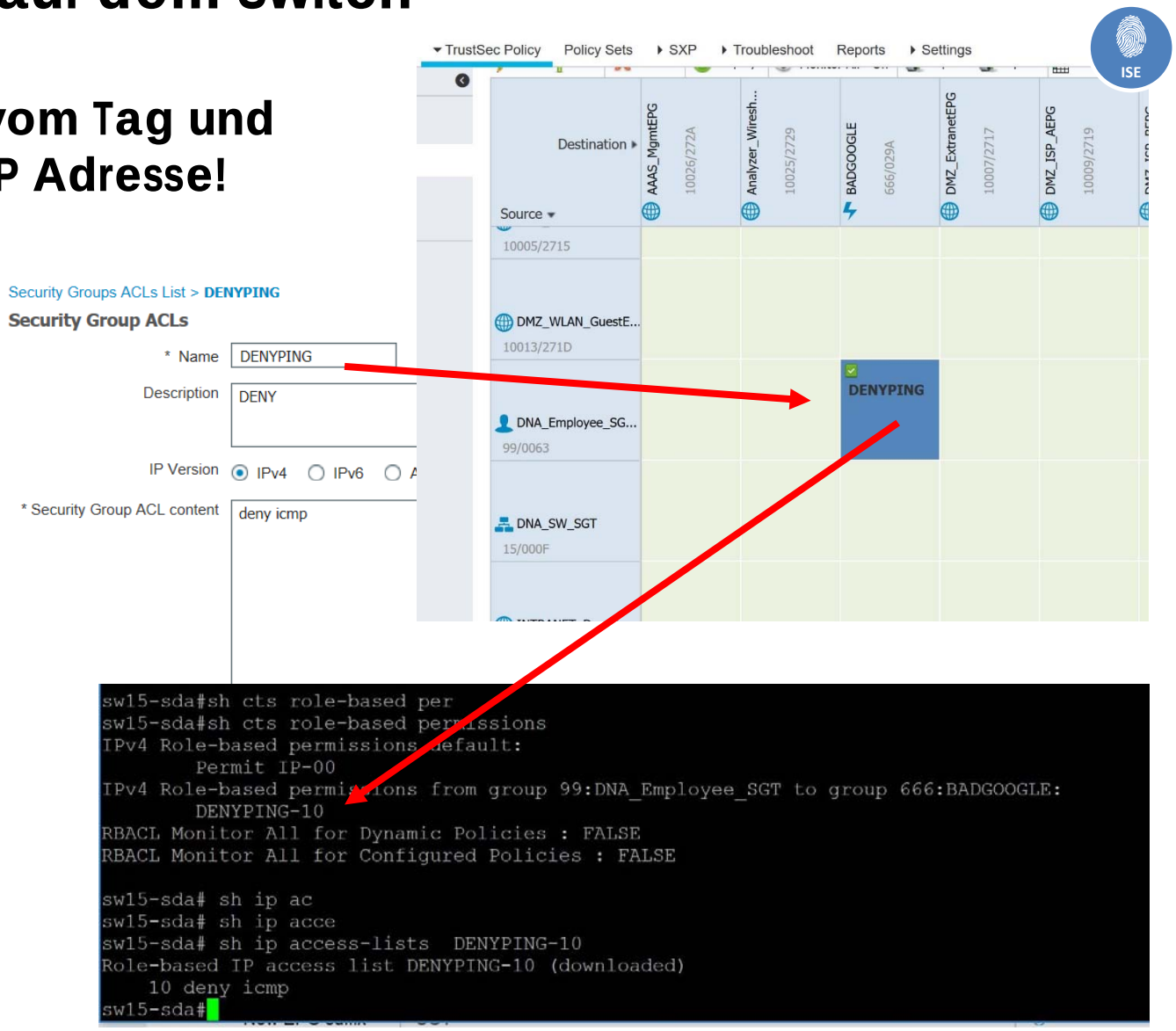



```
cts role-based enforcement vlan-list 20
```

Create. Connect. Control.

Enforcment auf dem Switch

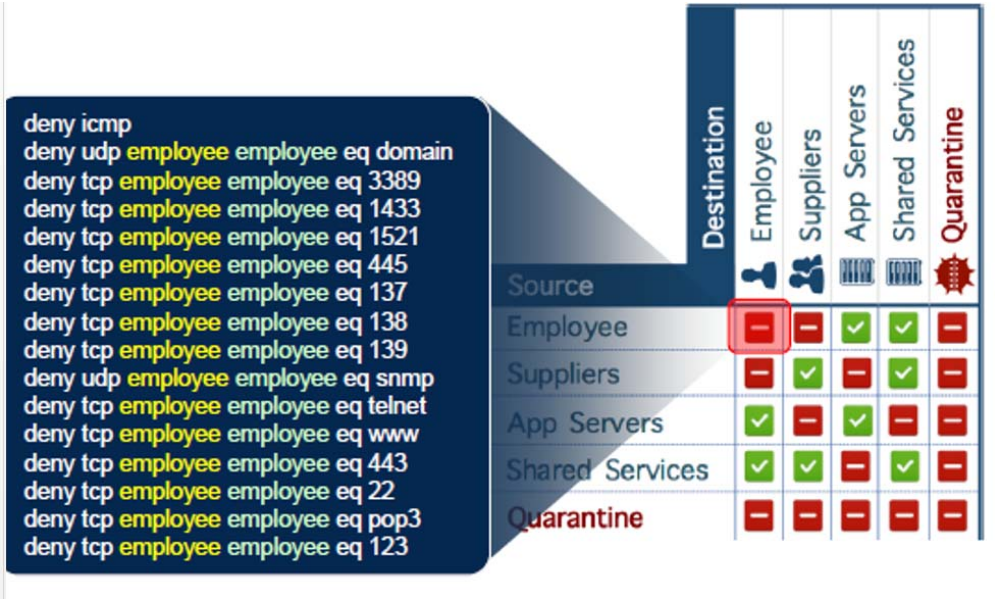
- **Aufgrund vom Tag und nicht von IP Adresse!**



Create. Connect. Control.
anyweb

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**

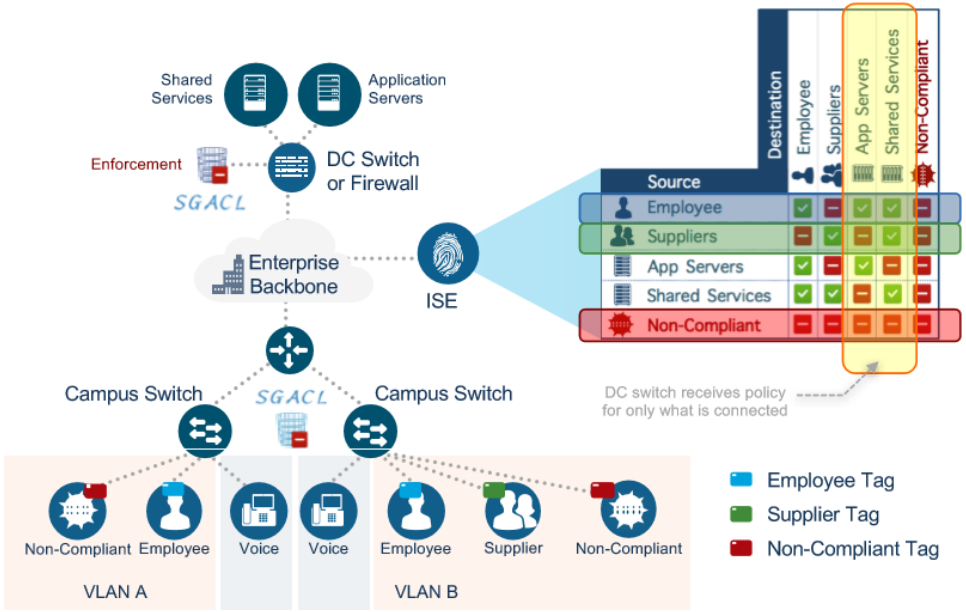


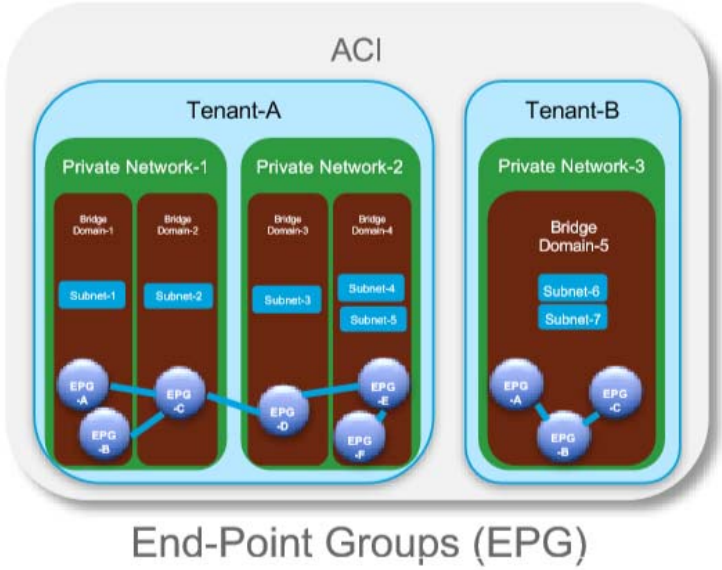
- **Aber immer noch relativ viel initiale (manuelle) Konfiguration auf den Switches**

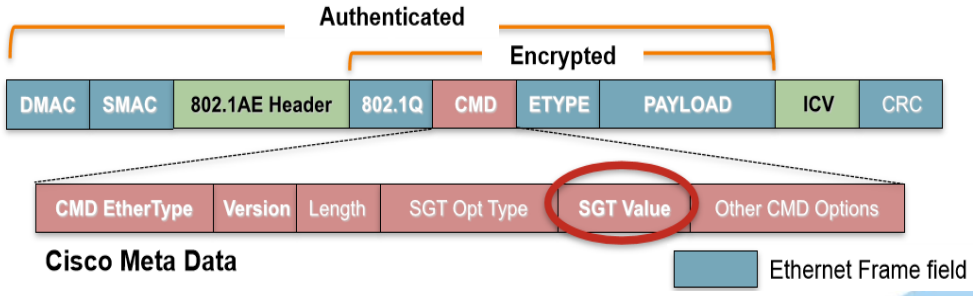
```
sw15-sda#sh run
Building configuration...

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
```

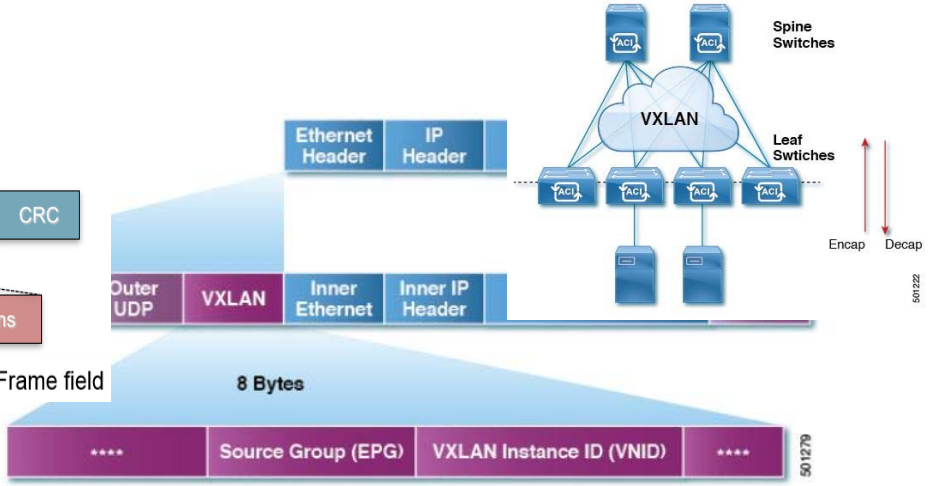
Create. Connect. Control.
anyweb

Wie geht es weiter???









Create. Connect. Control.

anyweb

… cool … aber geht’s auch einfacher?

Cisco DNA / SDA

Edi Layritz

Create. Connect. Control.
anyweb

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**
- **…**

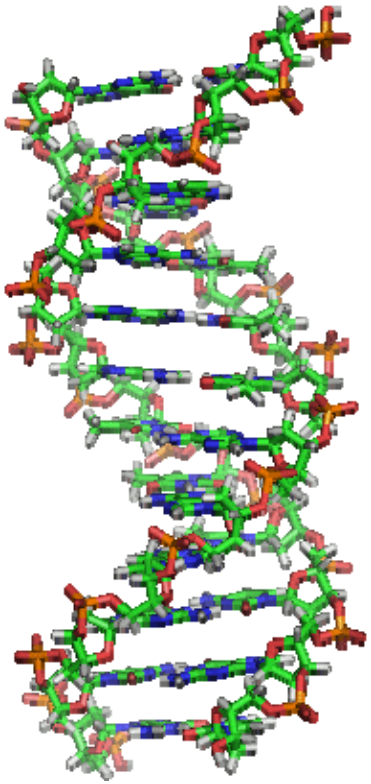
→ Automatisierung kann uns helfen

Create. Connect. Control.
anyweb

DNA / SDA

Create. Connect. Control.
anyweb

DNA / SDA - Begriffe



DNA ist nicht

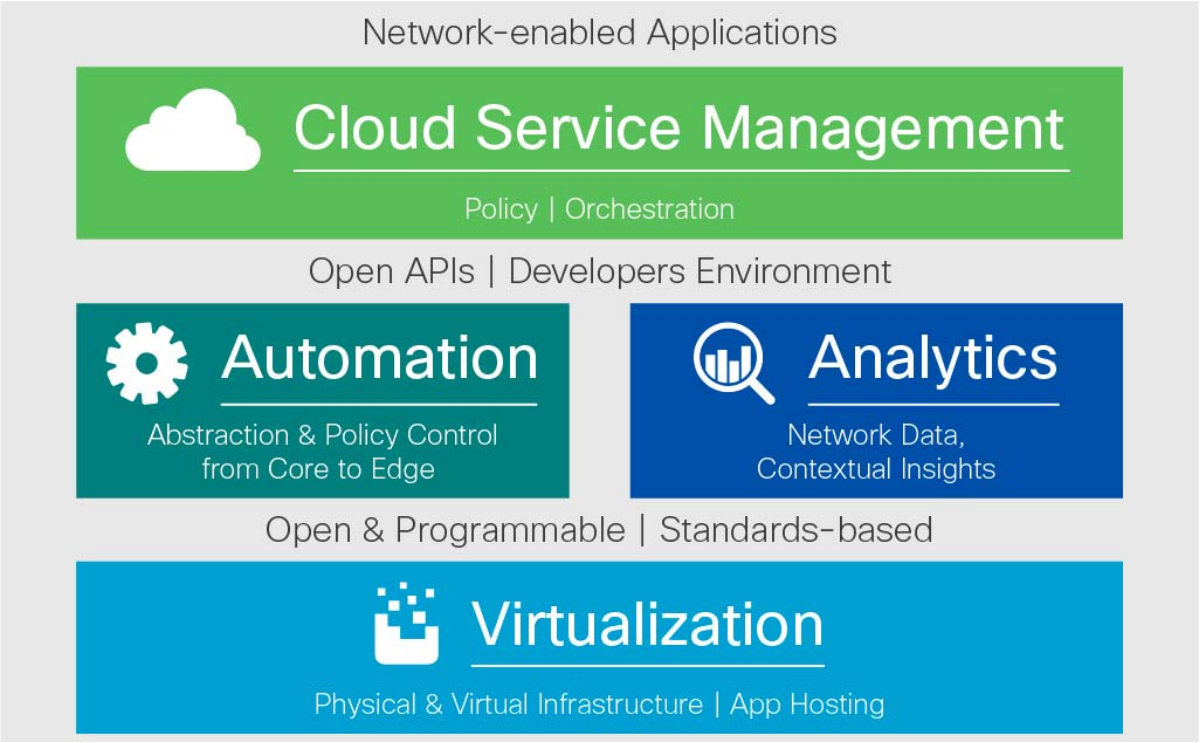
Desoxyribonukleinsäure ;-)

Create. Connect. Control.
anyweb

DNA / SDA - Begriffe

DNA – Digital Network Architecture

Eine Architektur:

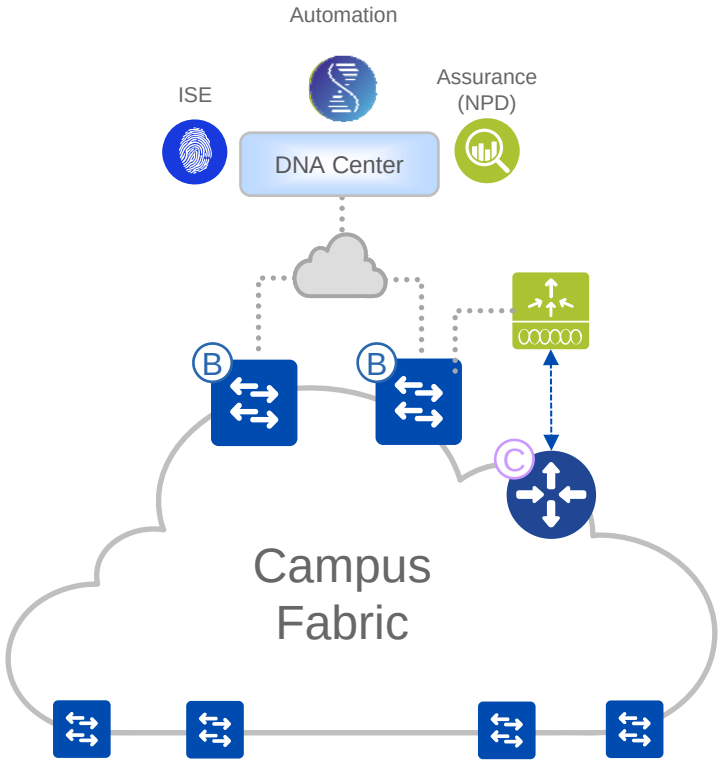


Create. Connect. Control.

DNA / SDA - Begriffe

SDA – Software Defined Access

Die Umsetzung:



Create. Connect. Control.
anyweb

Was bietet DNA?

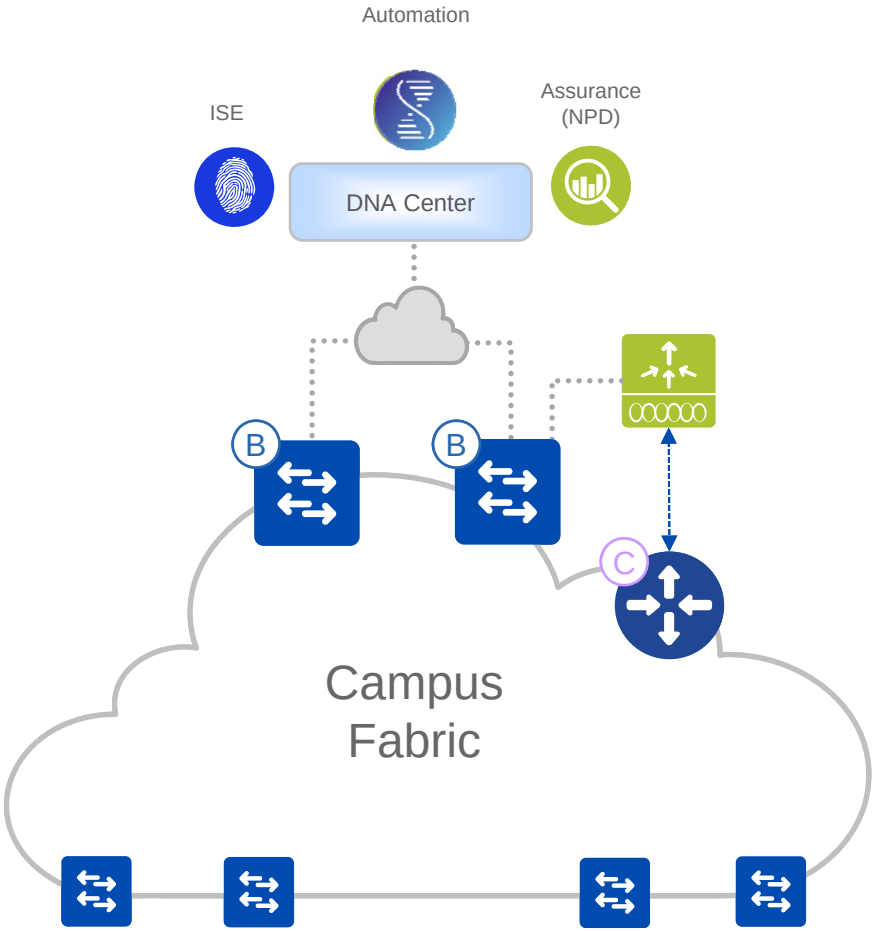
- **Ein homogenes Netz**
  - **Access - Control**
  - **Segmentierung**
  - **Policy Enforcement**
  - **Insights & Telemetrie – Ende November 2017**
- **Automatisierung beim Ausrollen**
- **Einfacher Betrieb**

Create. Connect. Control.
anyweb

It’s a journey

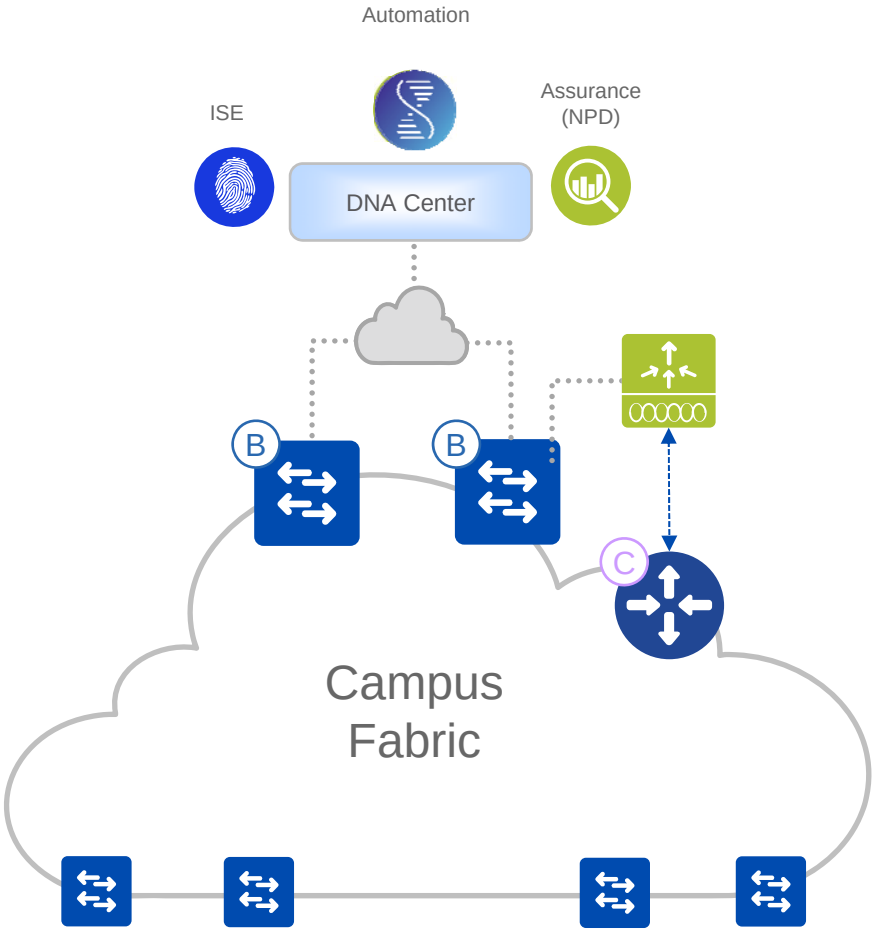
Create. Connect. Control.
anyweb

SDA – Campus Fabric



Create. Connect. Control.
anyweb

SDA – Campus Fabric

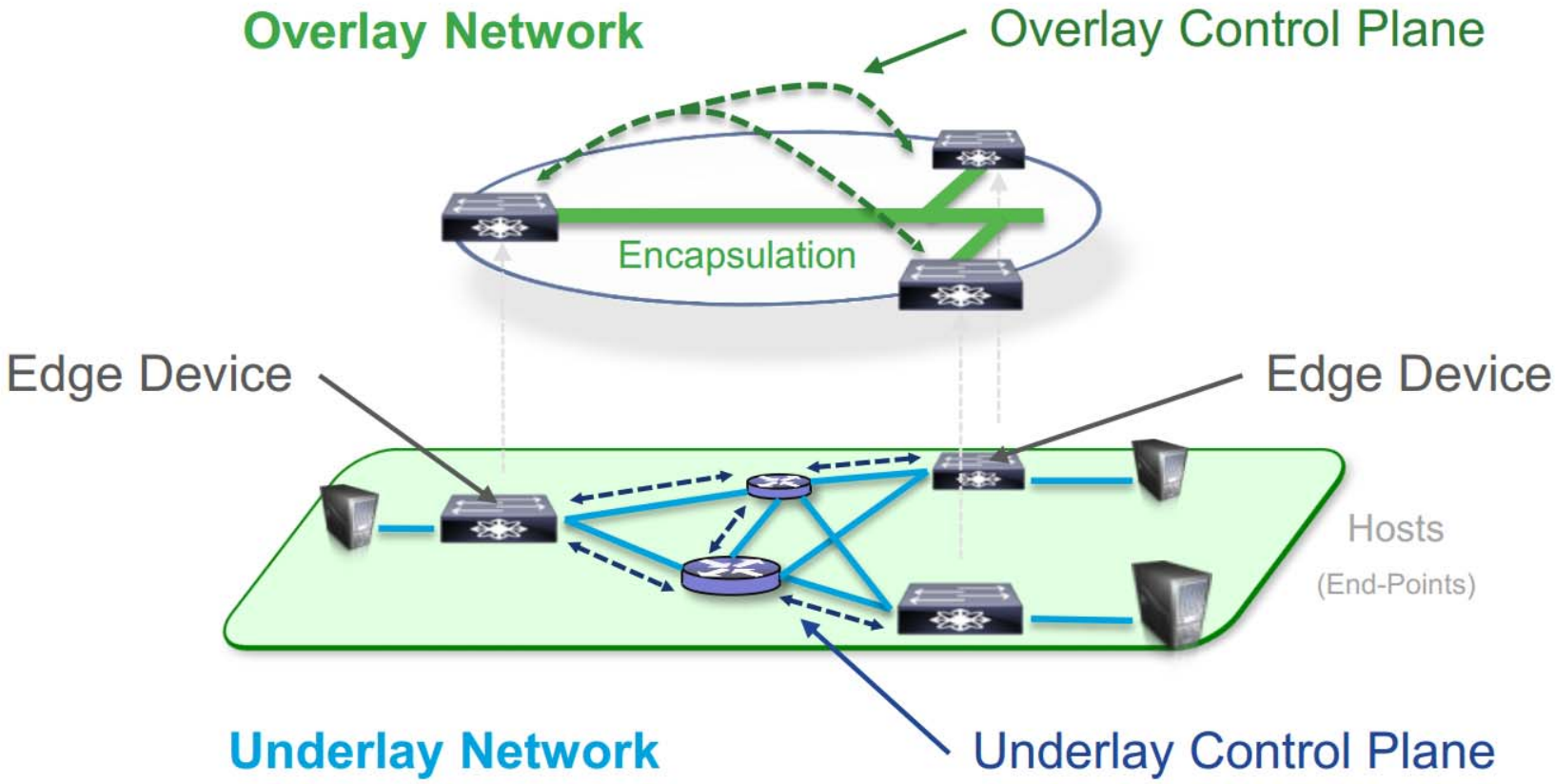


- **Campus Fabric**

Create. Connect. Control.
anyweb

SDA – Campus Fabric

Die Fabric bildet ein Overlay Netz



Create. Connect. Control.
anyweb

SDA – Campus Fabric

- Ein Overlay Netz bildet eine virtuelle Topologie um Geräte miteinander zu verbinden

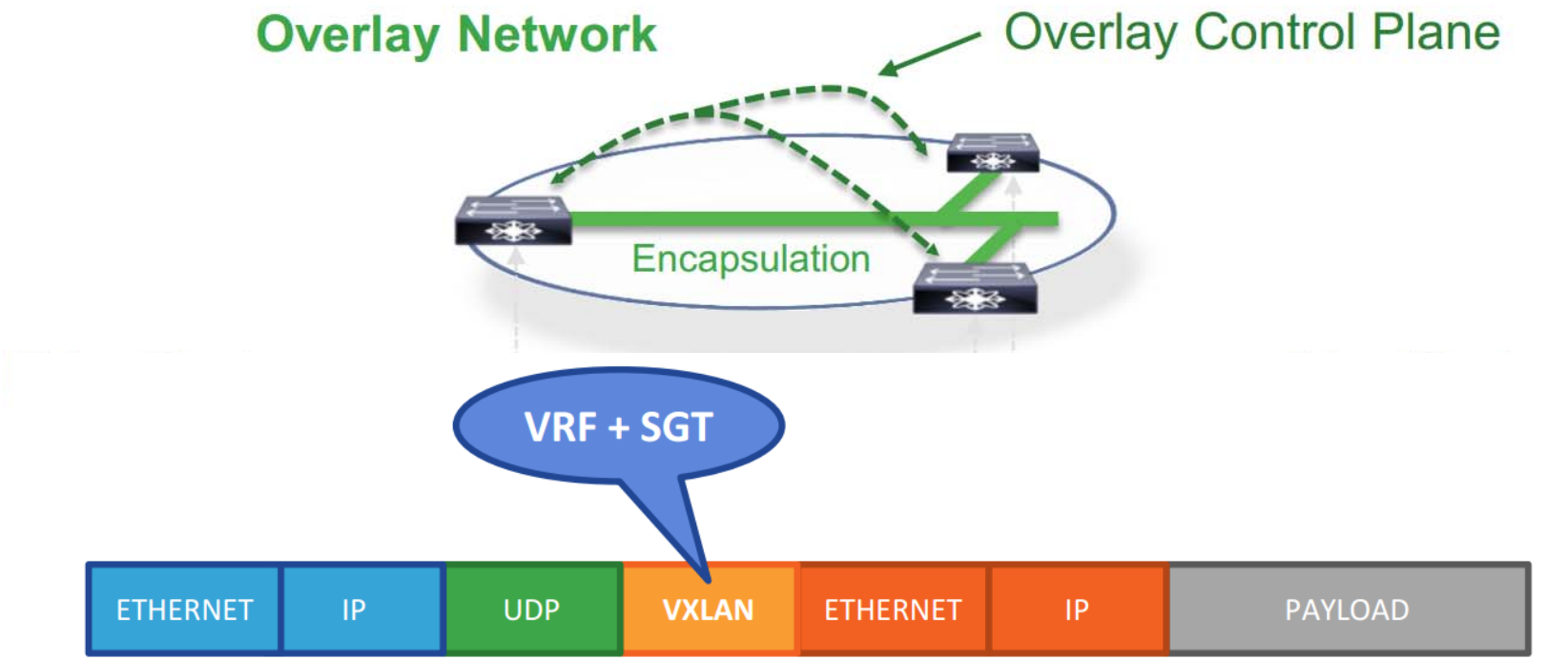
  Beispiele: MPLS VPN, DMVPN, CAPWAP

- 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

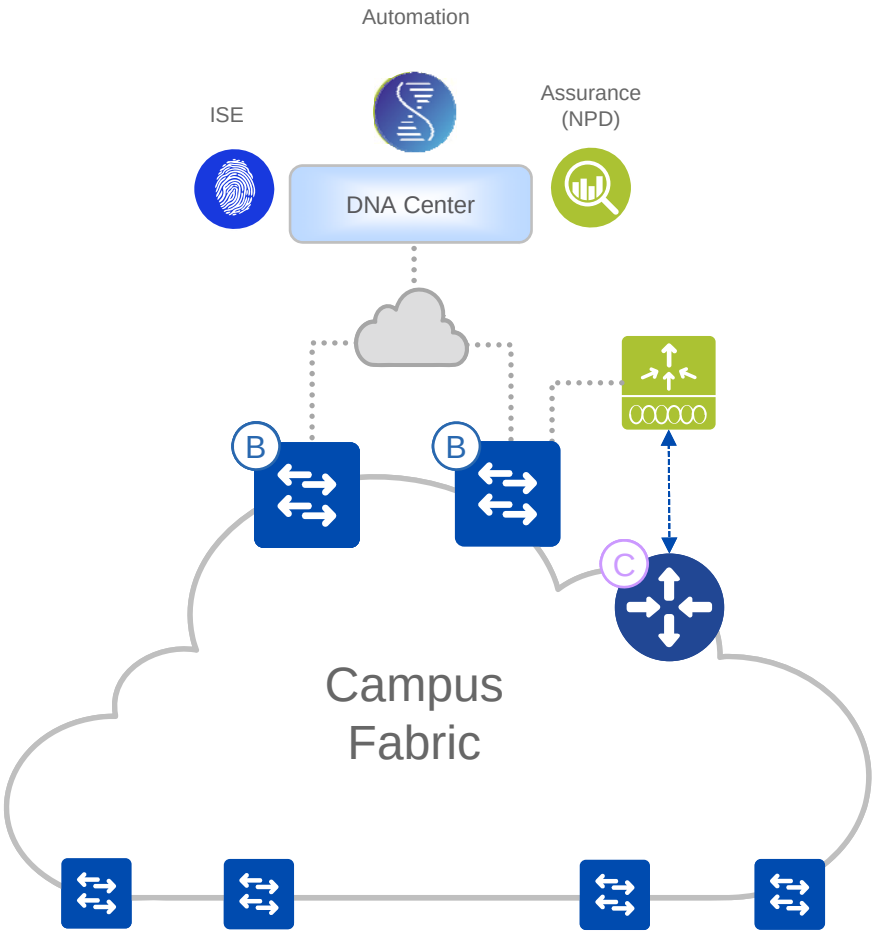
Create. Connect. Control.
anyweb

SDA – Campus Fabric



Create. Connect. Control.
anyweb

SDA – Campus Fabric



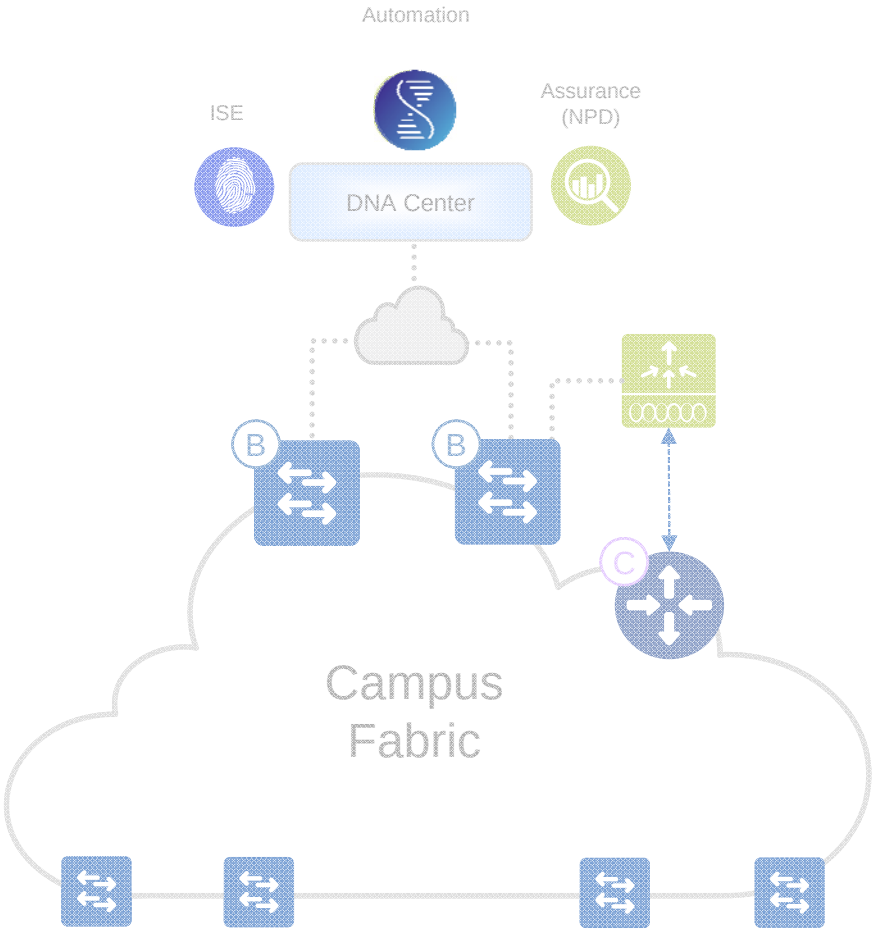
- Edge Node
  - Hier werden die Endgeräte angeschlossen

- 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

Create. Connect. Control.
anyweb

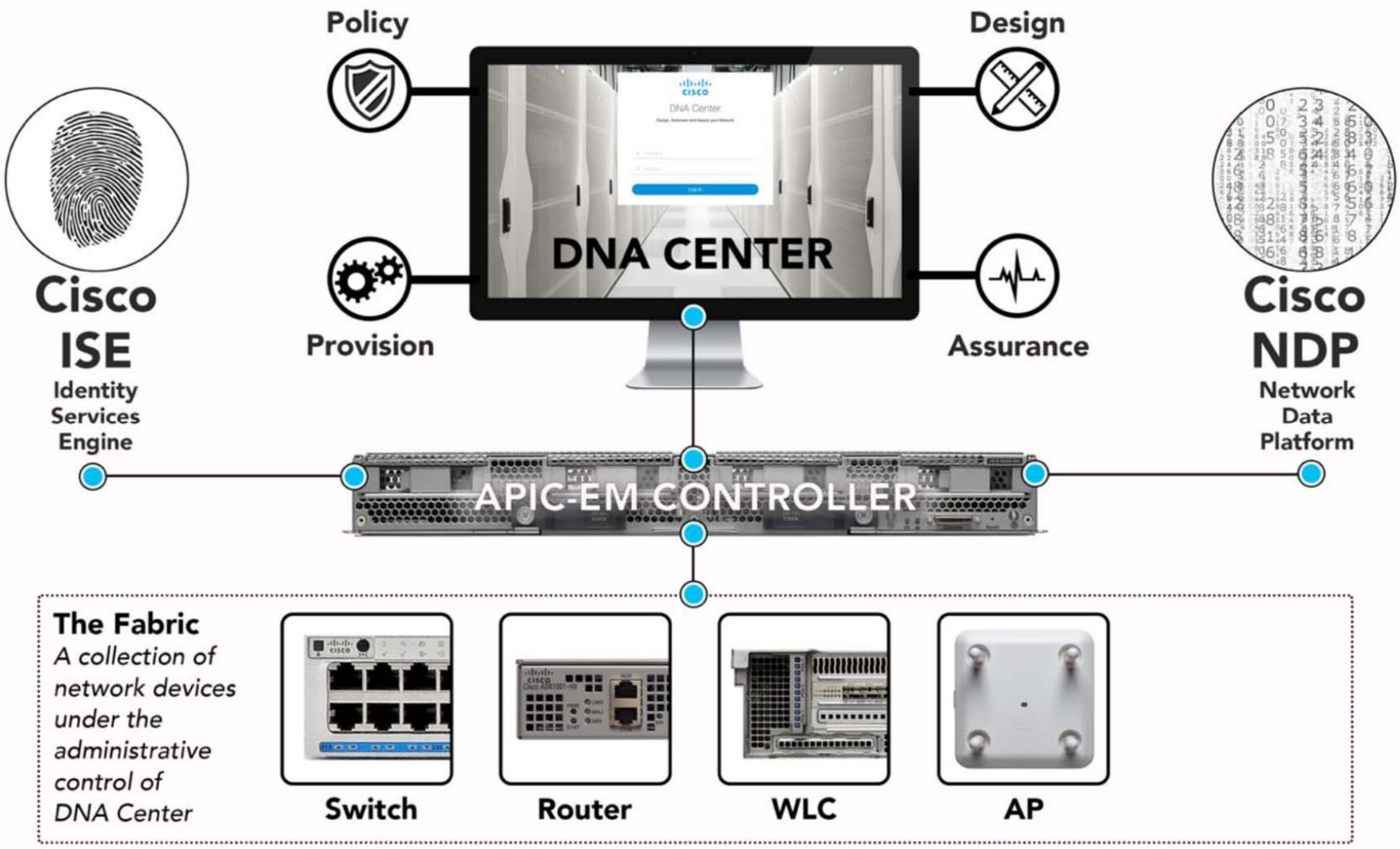
SDA – DNAC



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

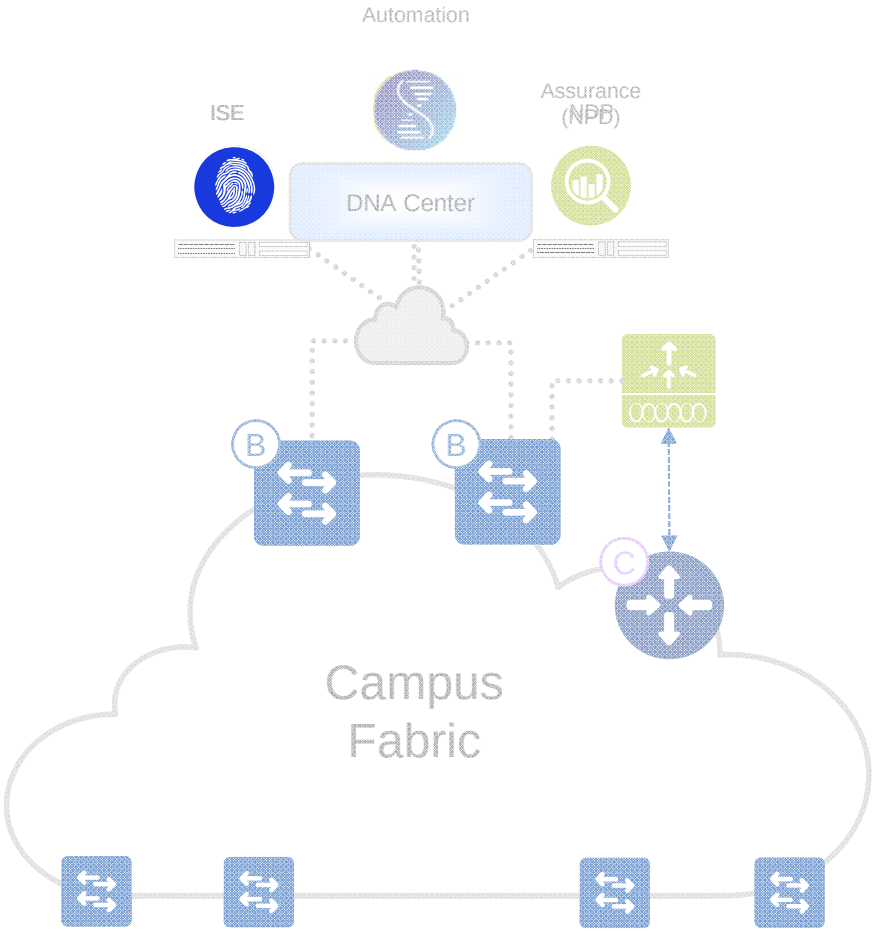
Create. Connect. Control.
anyweb

SDA – DNAC



Create. Connect. Control.
anyweb

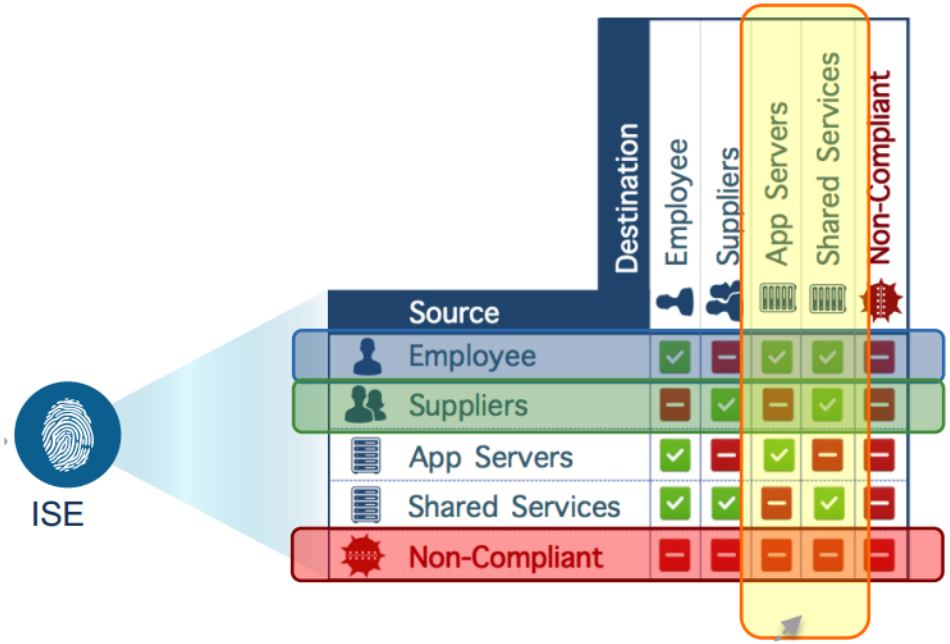
SDA – ISE



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

Create. Connect. Control.

SDA – ISE

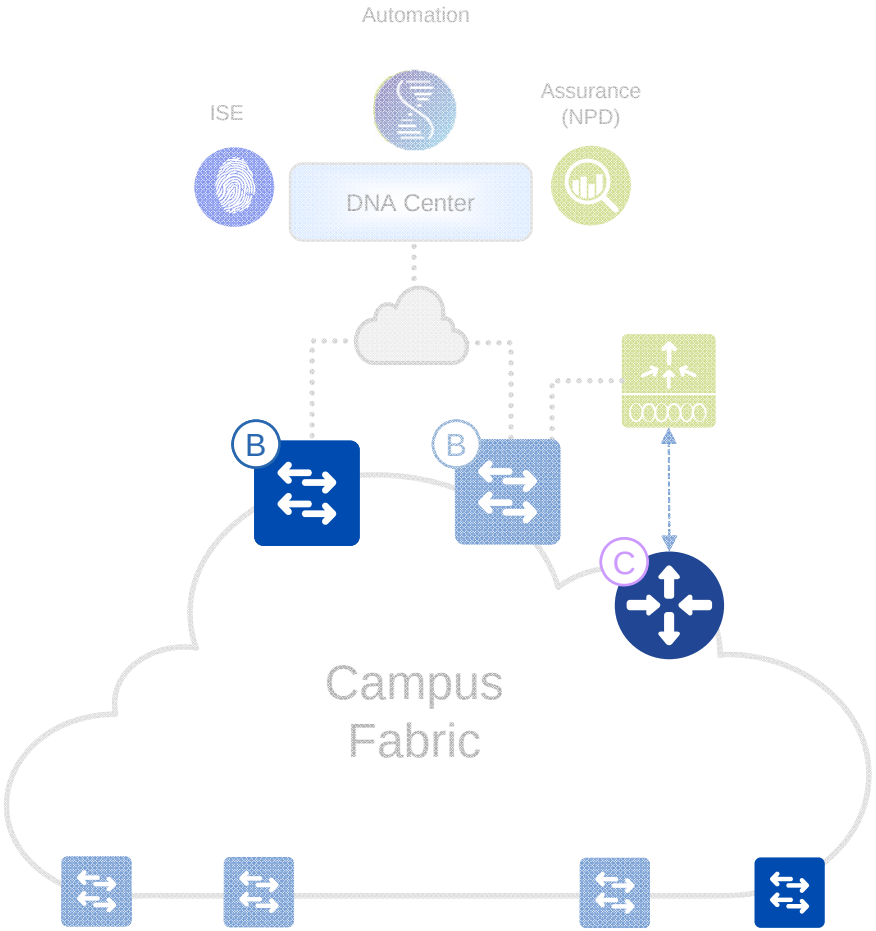


Create. Connect. Control.

It’s a journey

Create. Connect. Control.
anyweb

SDA - Hardware

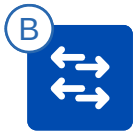


- **Campus Fabric**
- **DNA-Center**
- **Hardware**

Create. Connect. Control.
anyweb

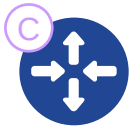
SDA - Hardware

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

Create. Connect. Control.
anyweb

SDA - Hardware

DNA-Center

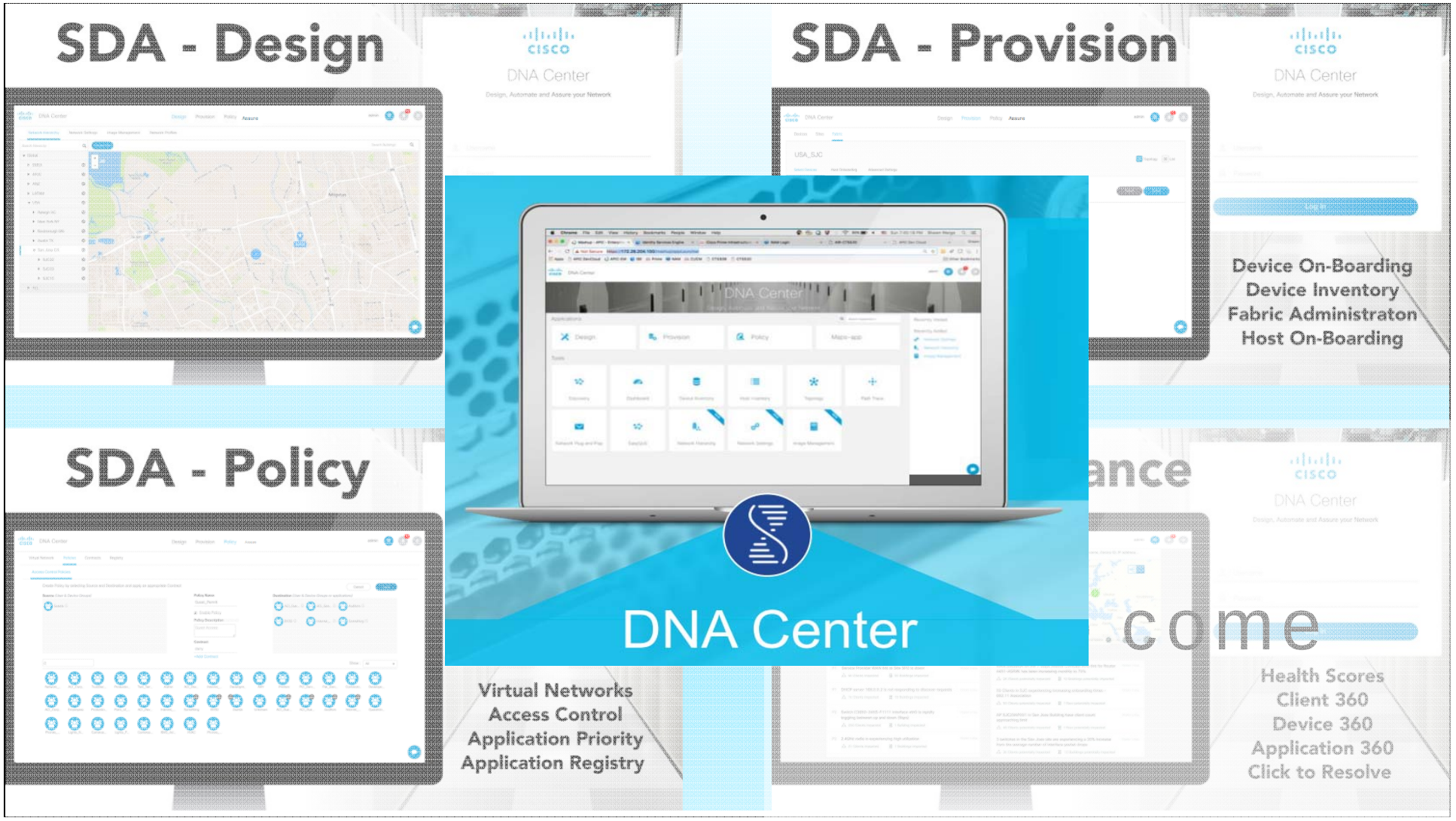
Zum jetzigen Zeitpunkt nur als Appliance lieferbar

Gründe dafür nach Cisco

- Braucht viel Leistung
- Leistung ist so garantiert

Create. Connect. Control.
anyweb

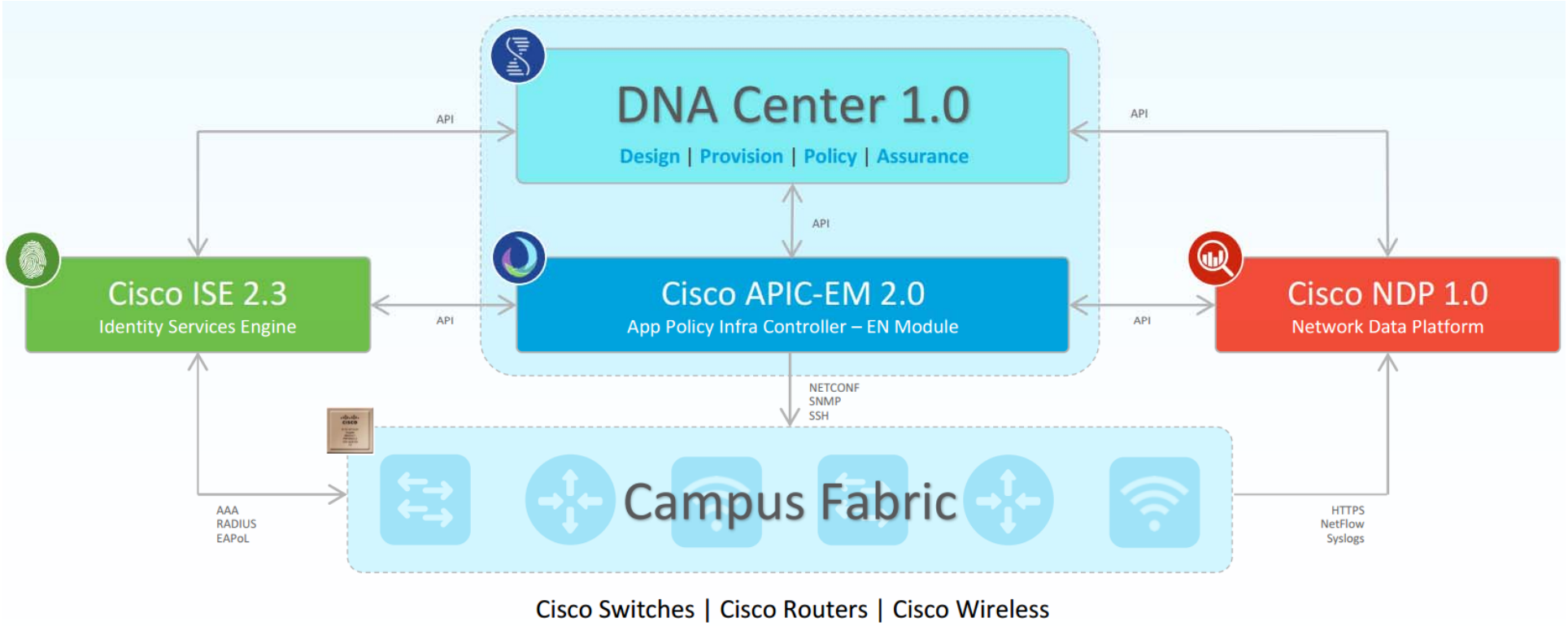
DNA Center



Create. Connect. Control.
anyweb

DNA Center

Einbindung vom DNA Center



Create. Connect. Control.
anyweb

DNA Center

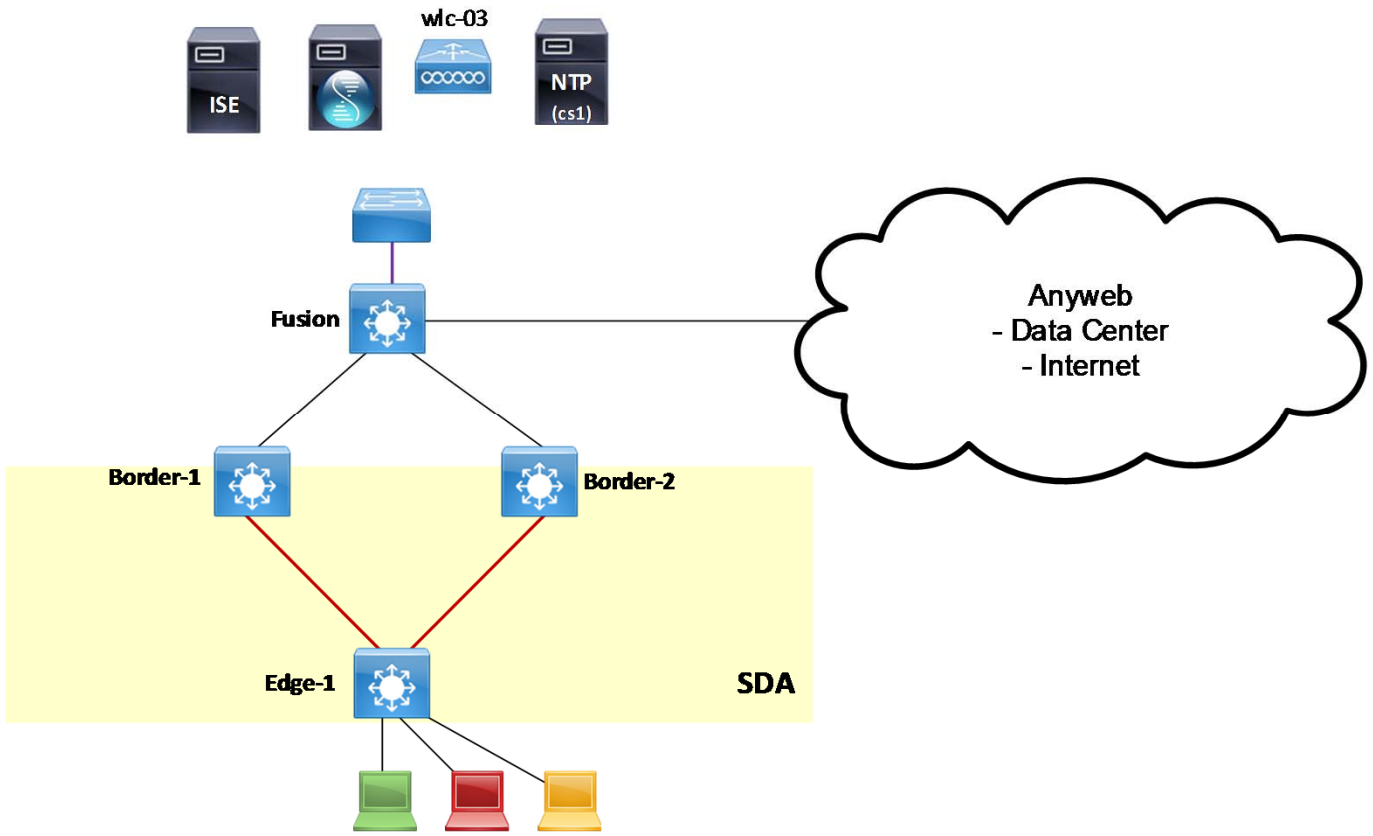
DNA-Center lernt die SGT's vom ISE oder dem AD

SGT: Scalable Groups, Scalable Group Tags

Create. Connect. Control.
anyweb

DNA Center

SDA@AnyWeb – Laboraufbau



Create. Connect. Control.
anyweb

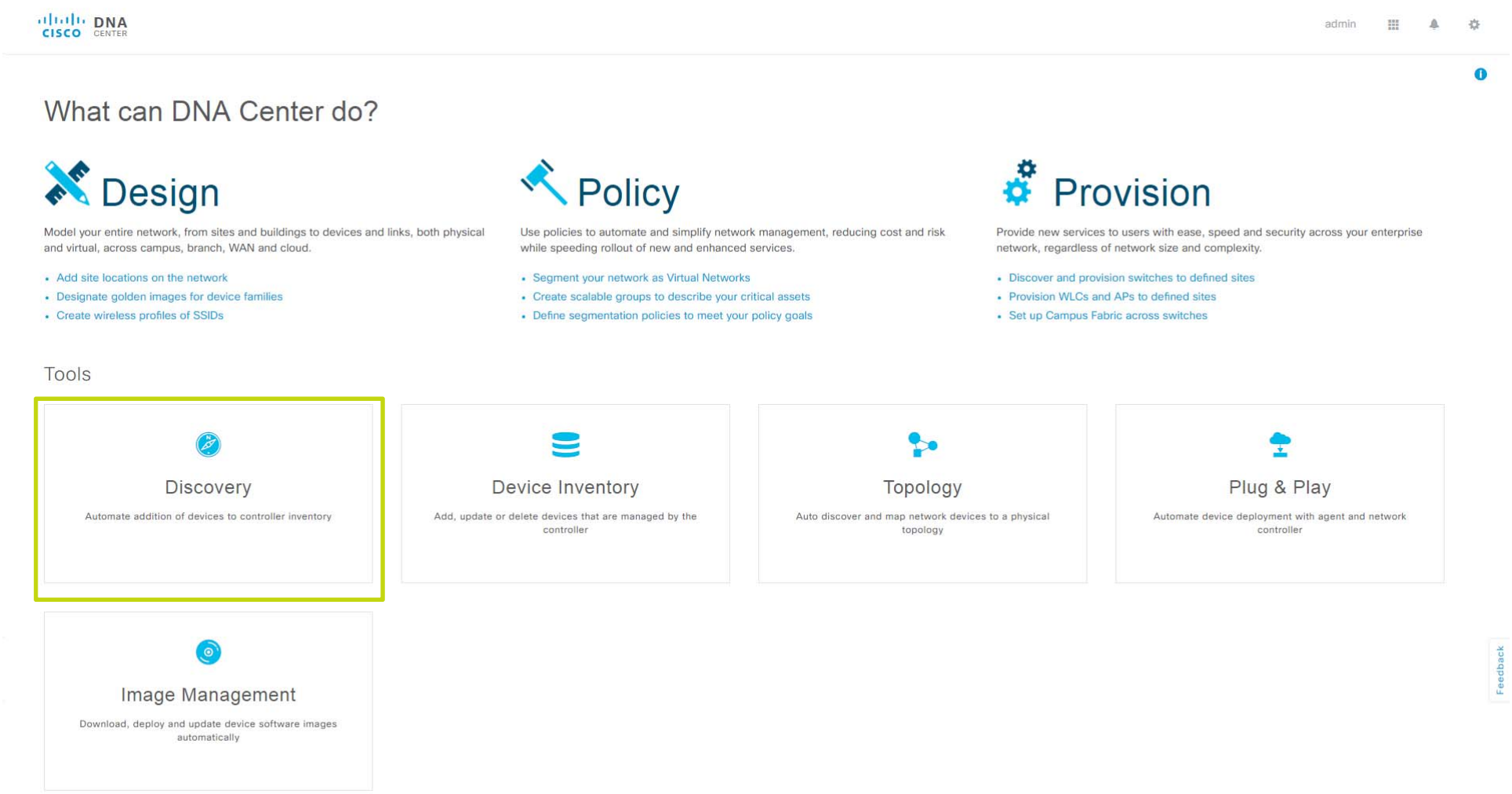
DNA Center

Aufbau eines SDA mit DNA Center

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

Create. Connect. Control.
anyweb

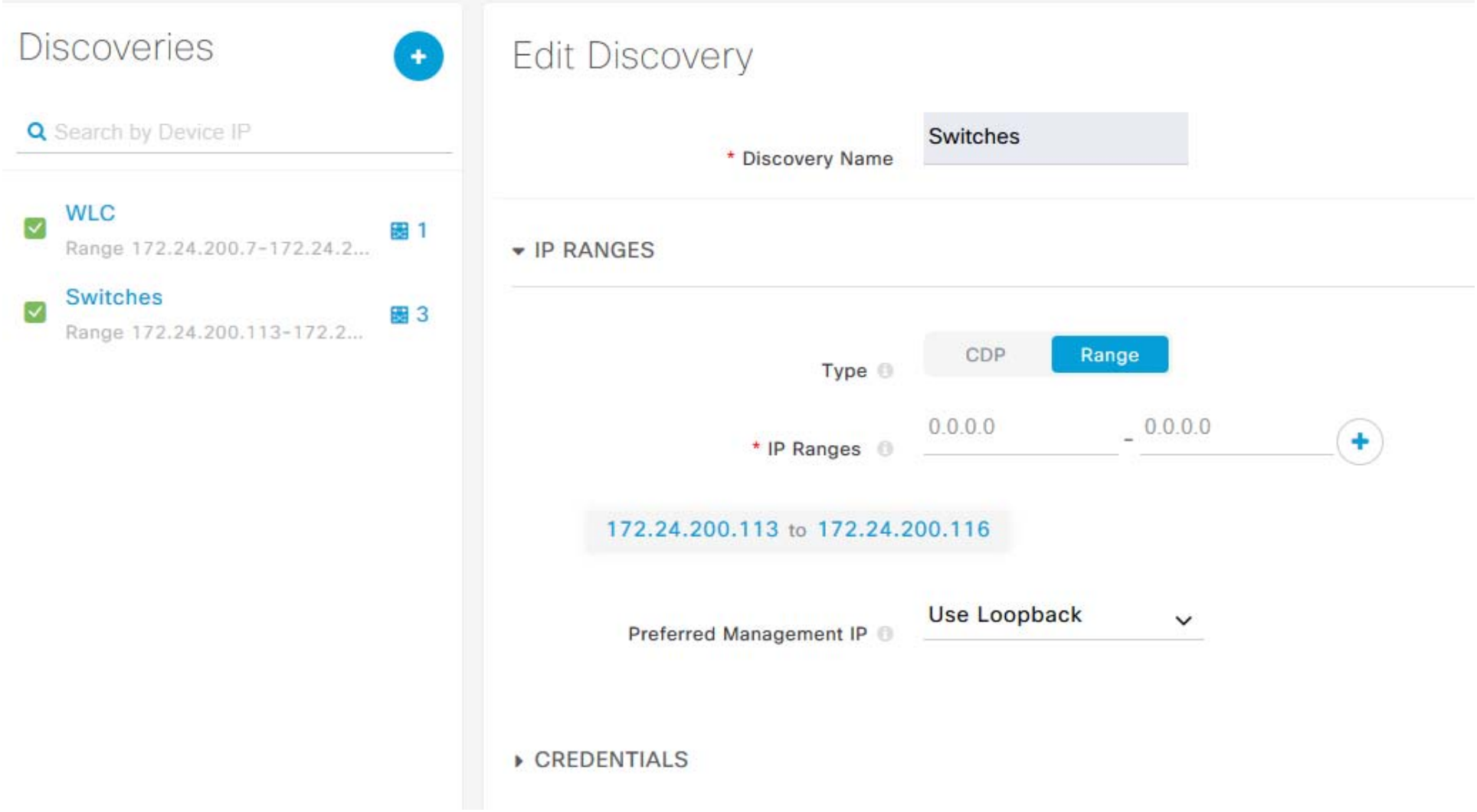
DNA Center



Create. Connect. Control.
anyweb

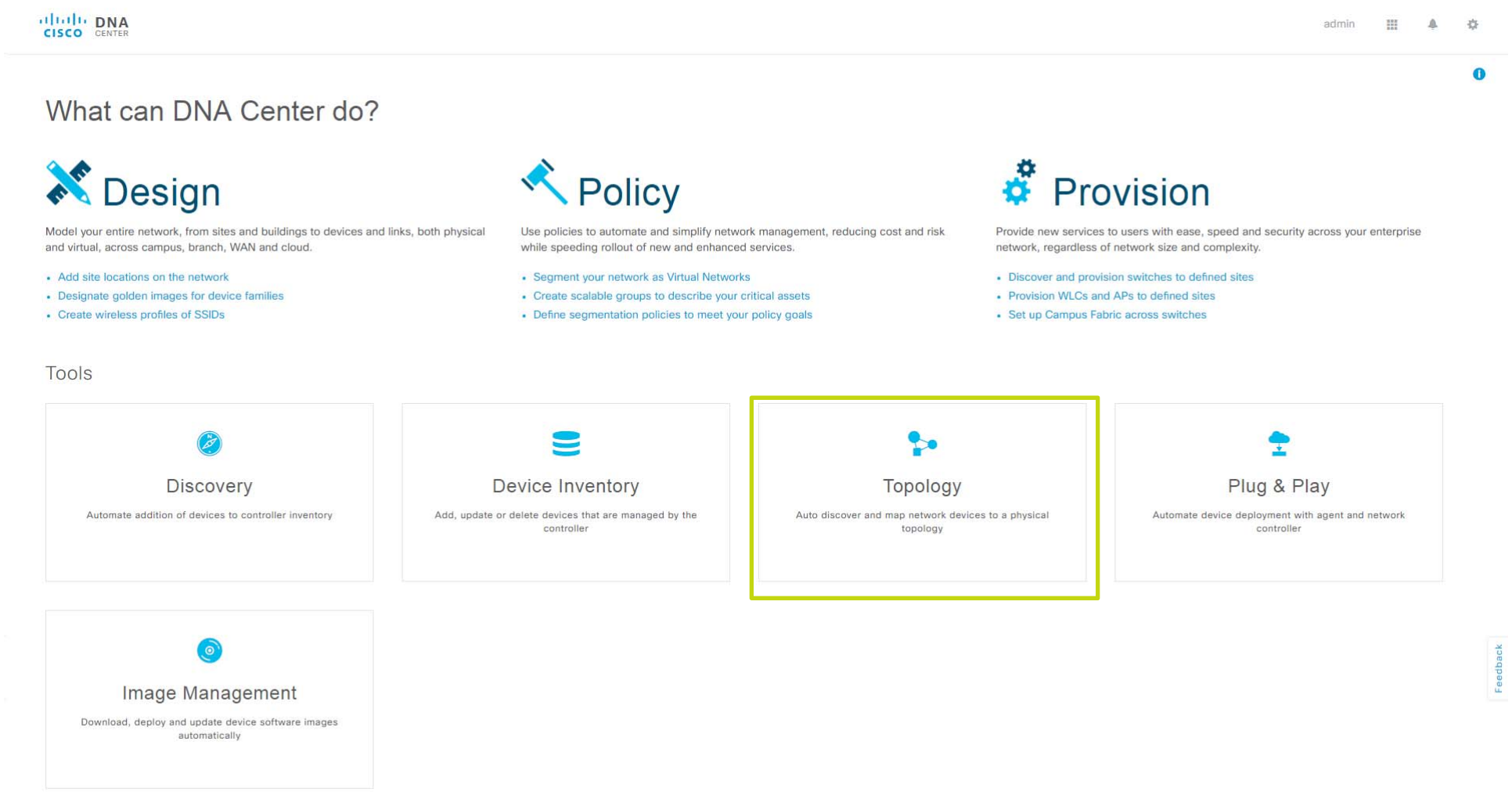
DNA Center

Discover | Topology | Design | Policy | Provision



Create. Connect. Control.
anyweb

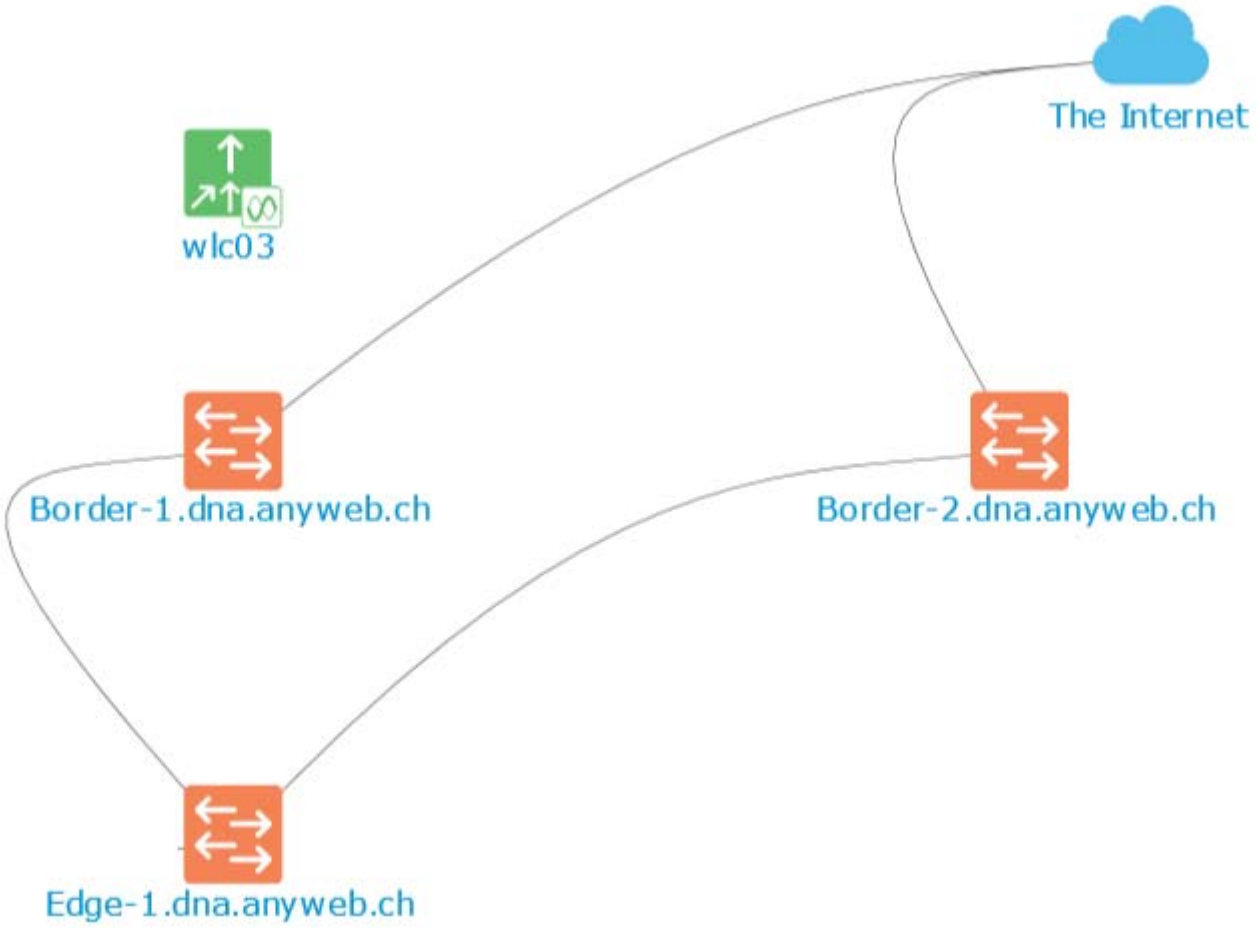
DNA Center



Create. Connect. Control.
anyweb

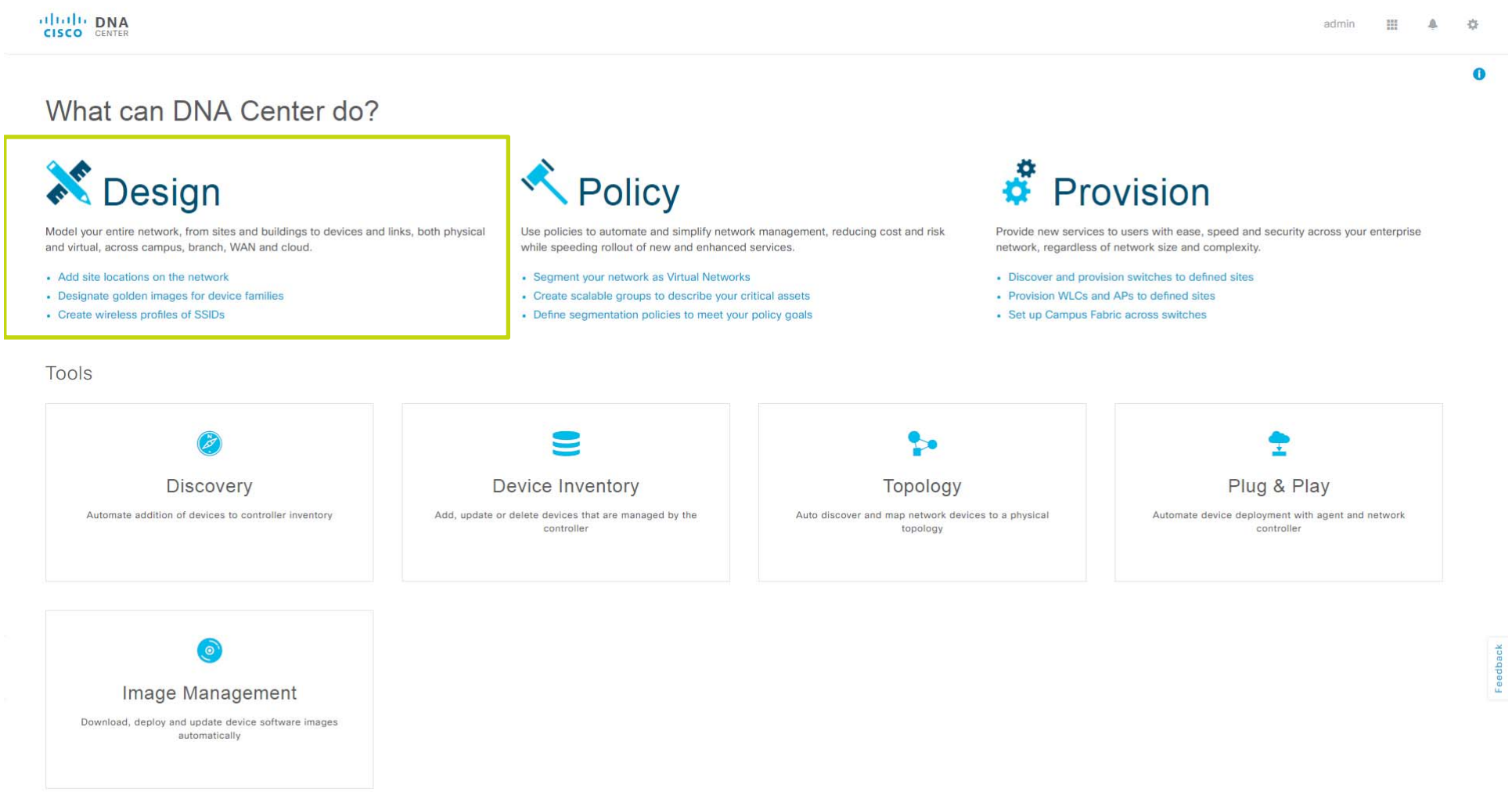
DNA Center

Discover | Topology | Design | Policy | Provision



Create. Connect. Control.
anyweb

DNA Center

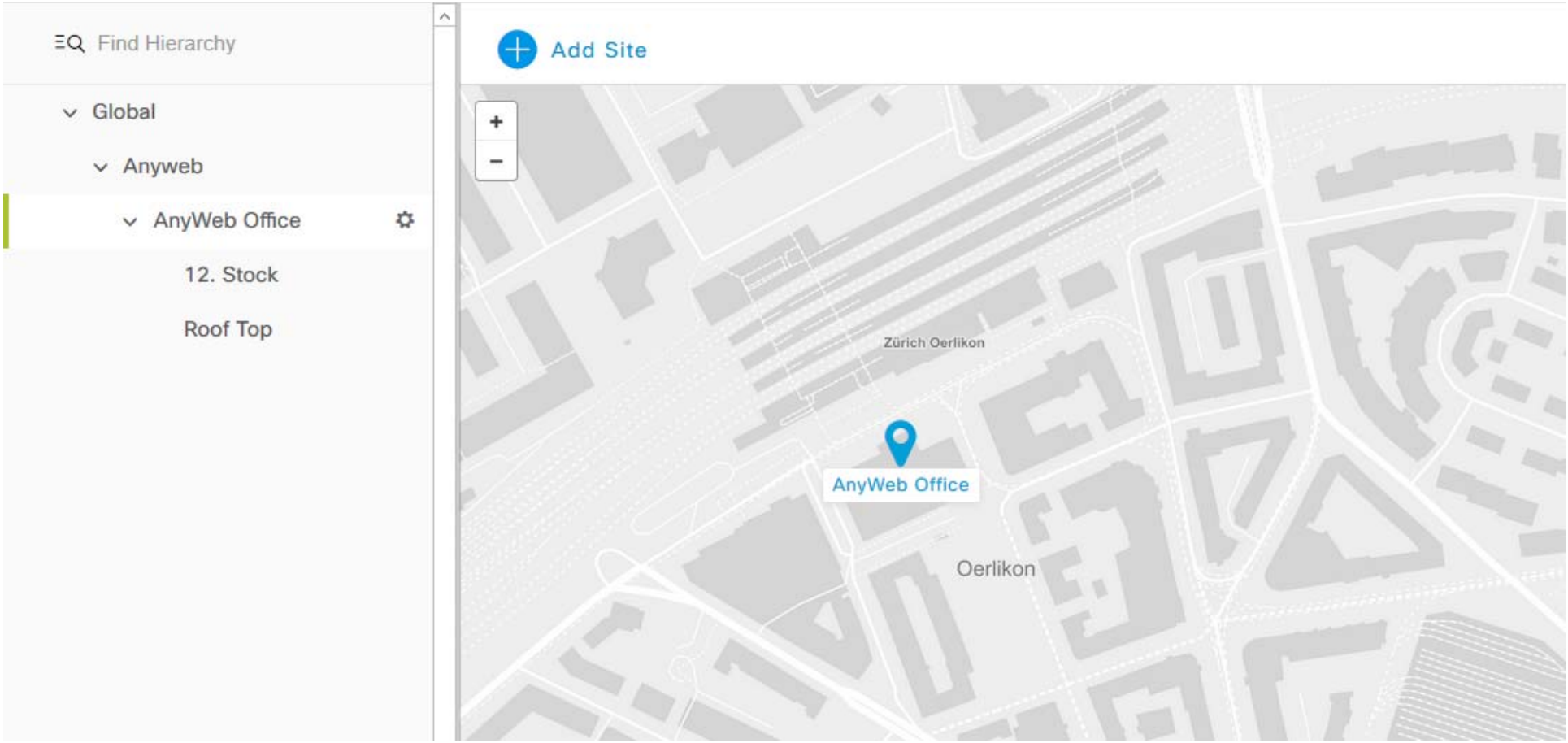


Create. Connect. Control.

DNA Center

Discover | Topology | Design | Policy | Provision

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

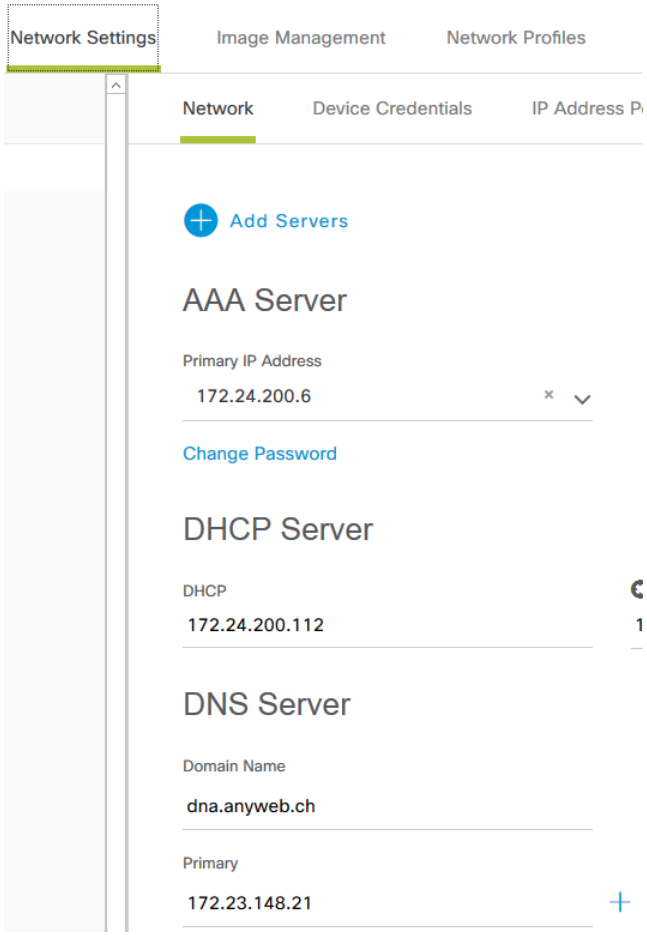


Create. Connect. Control.
anyweb

DNA Center

Discover | Topology | Design | Policy | Provision

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

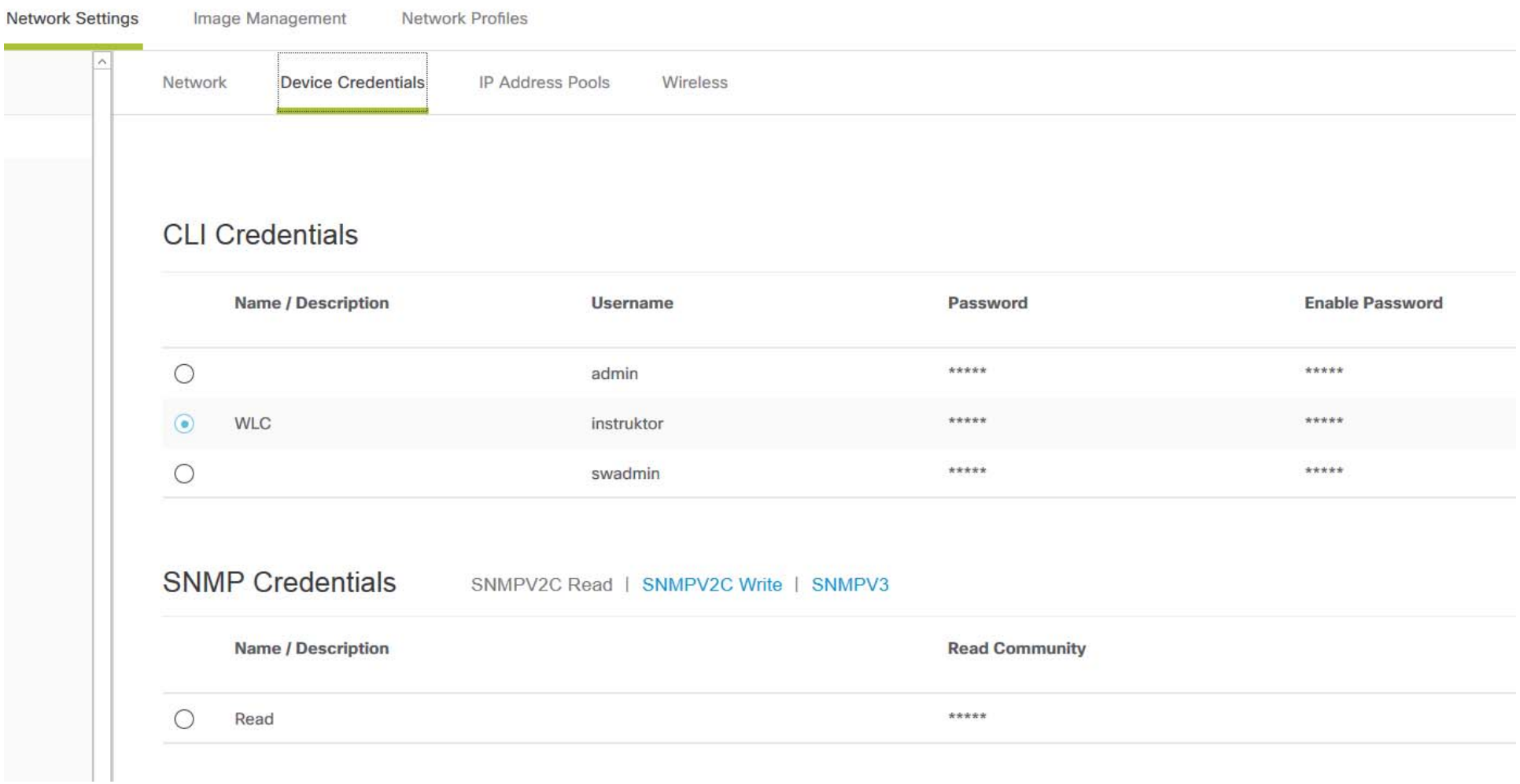


Create. Connect. Control.
anyweb

DNA Center

Discover | Topology | Design | Policy | Provision

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

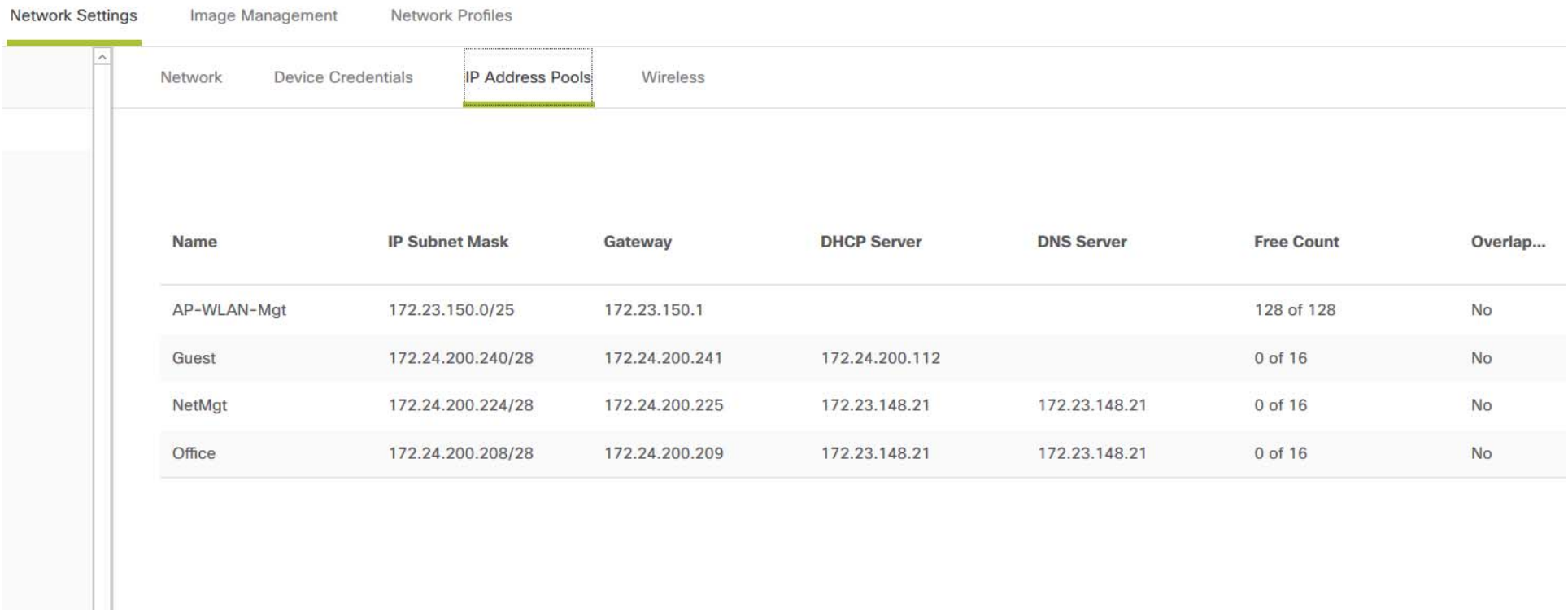


Create. Connect. Control.
anyweb

DNA Center

Discover | Topology | Design | Policy | Provision

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



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

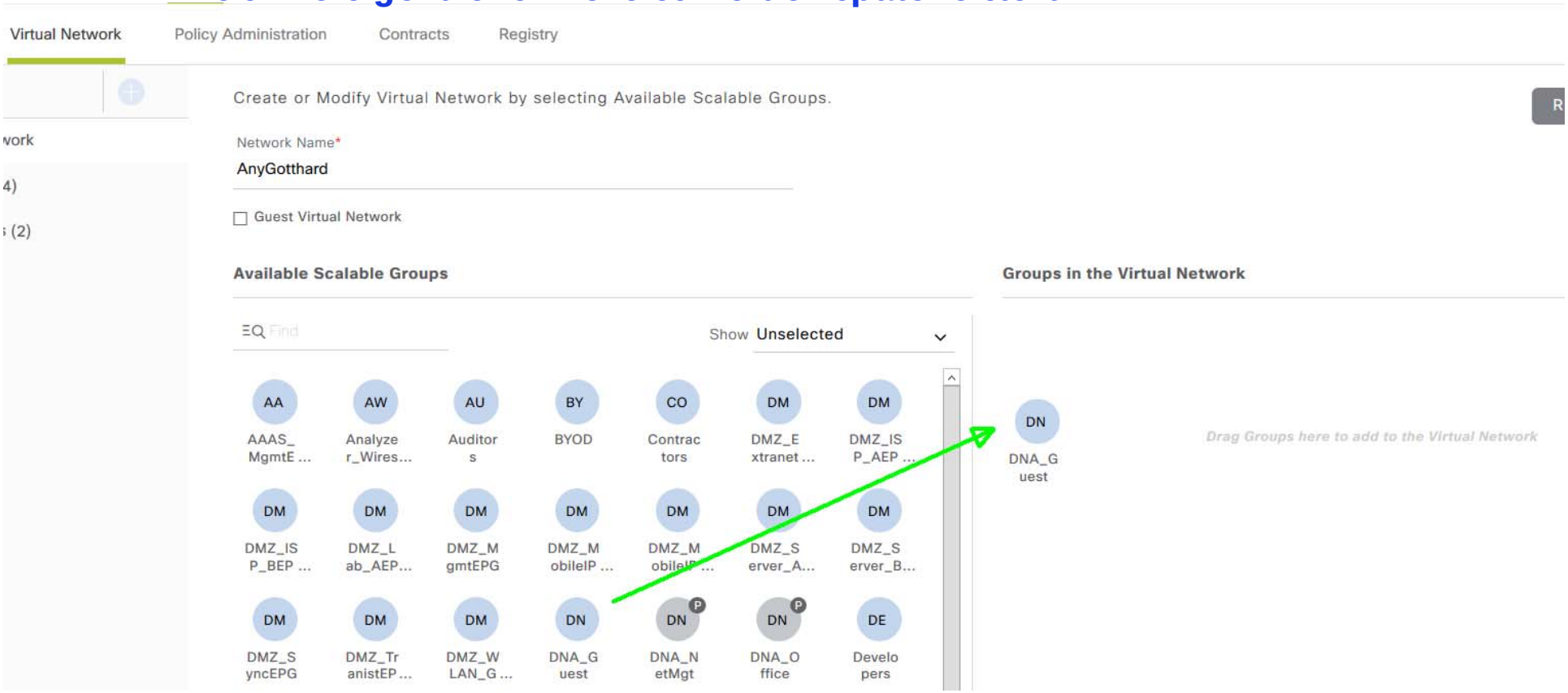
Create. Connect. Control.

DNA Center

Discover | Topology | Design | Policy | Provision

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

Hinweis: Die eigentlichen Policies werden später erstellt

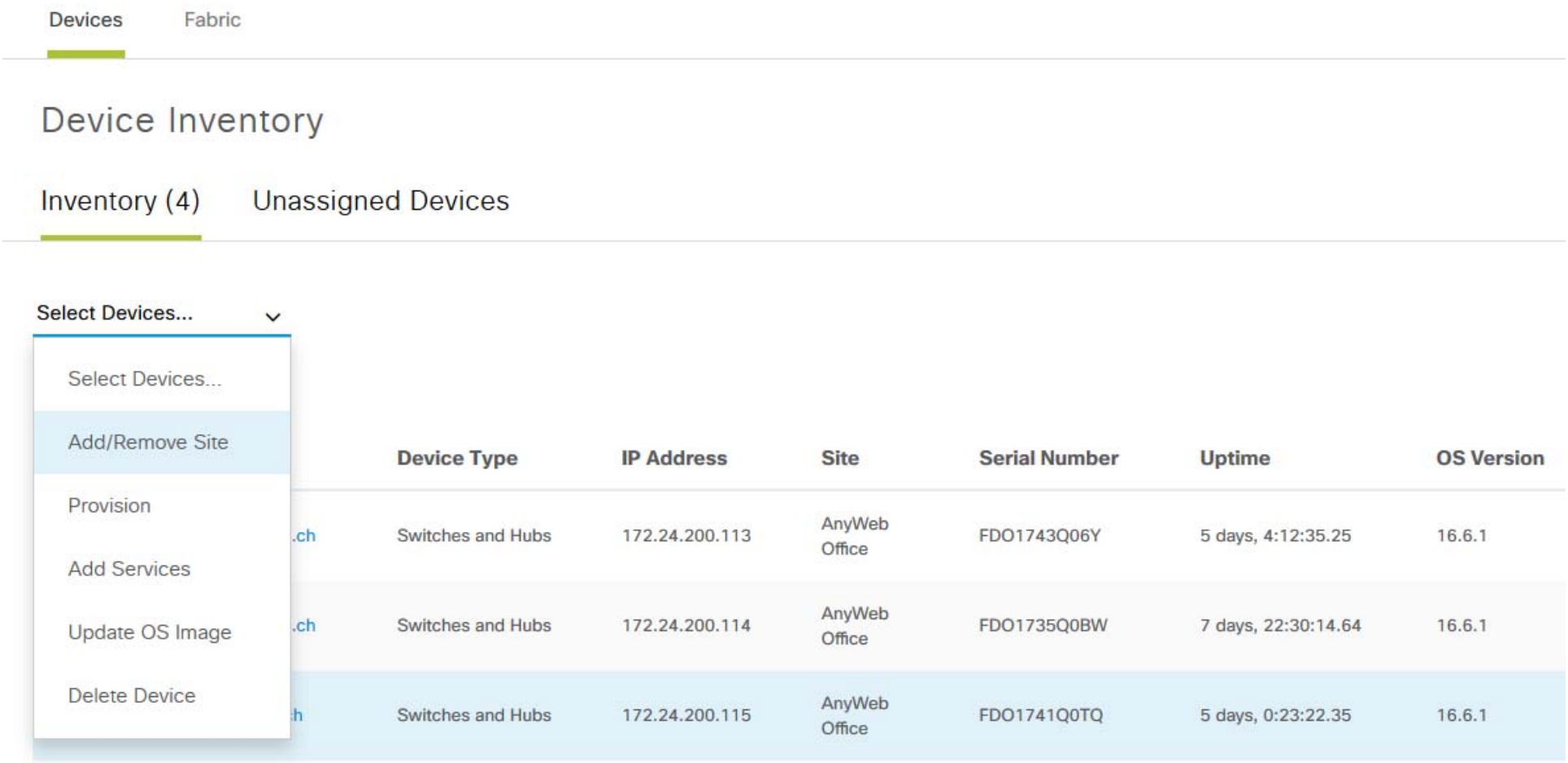


Create. Connect. Control.

DNA Center

Discover | Topology | Design | Policy | Provision

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

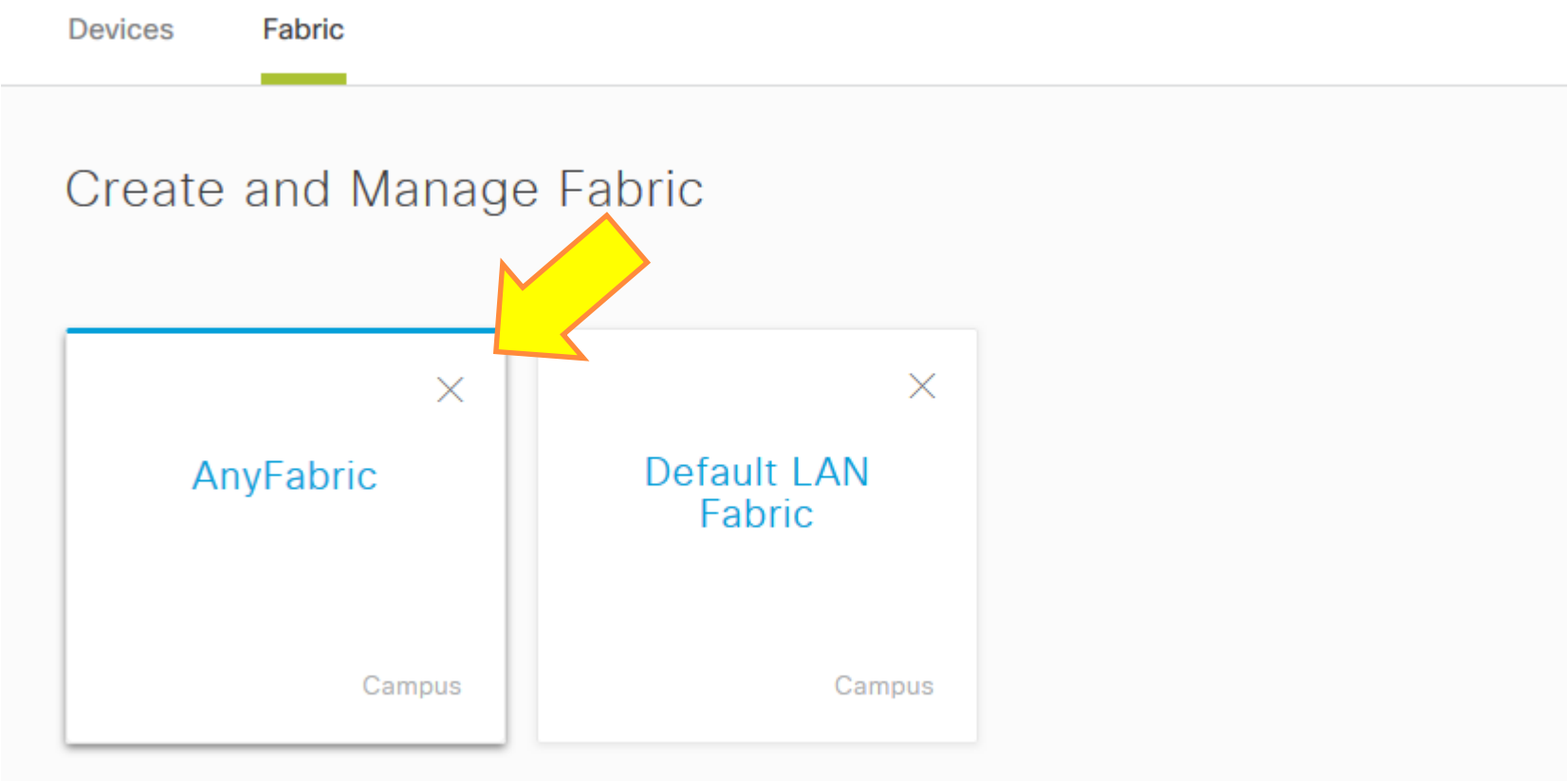


Create. Connect. Control.

DNA Center

Discover | Topology | Design | Policy | Provision

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

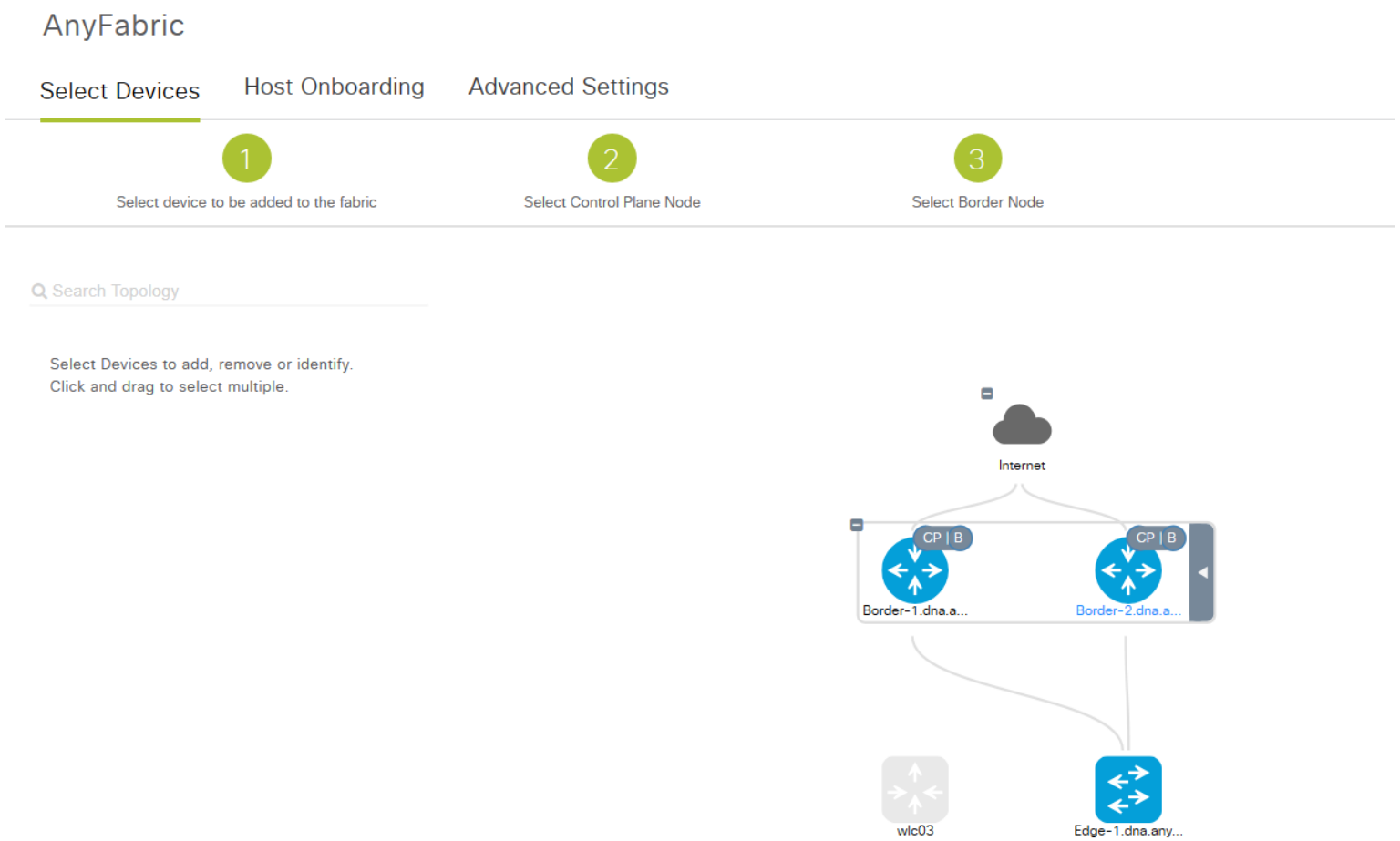


Create. Connect. Control.

DNA Center

Discover | Topology | Design | Policy | Provision

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

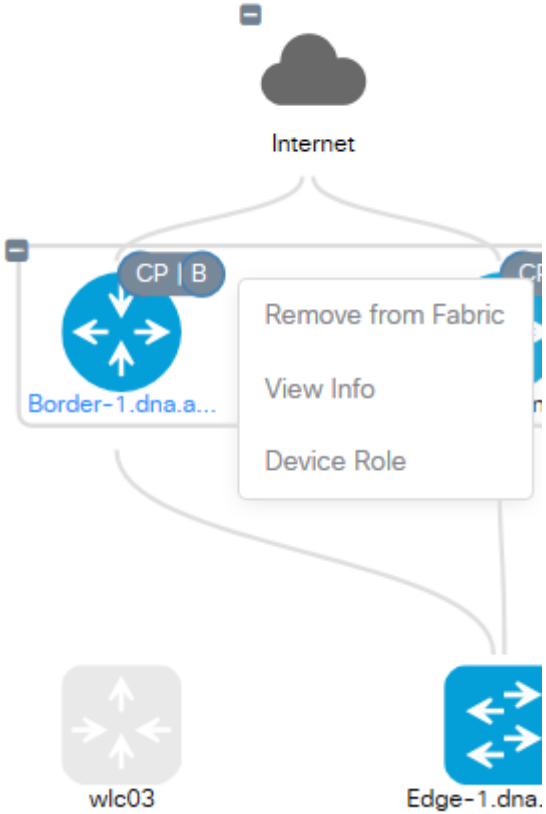


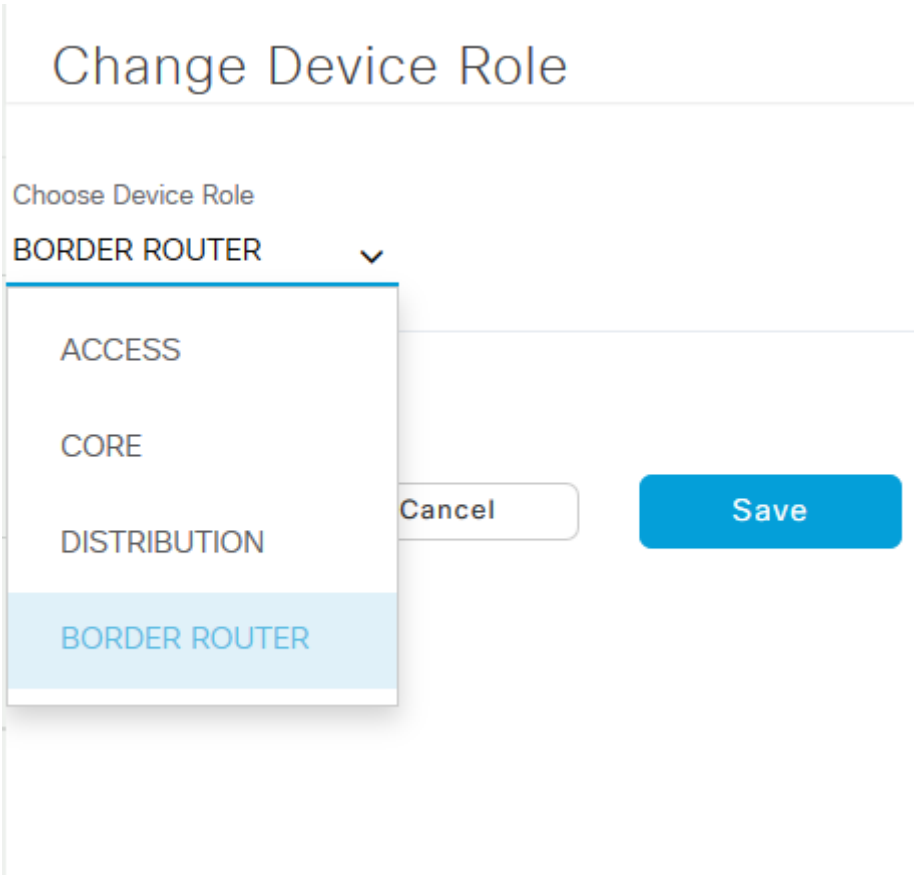
Create. Connect. Control.
anyweb

DNA Center

Discover | Topology | Design | Policy | Provision

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





Create. Connect. Control.
anyweb

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:

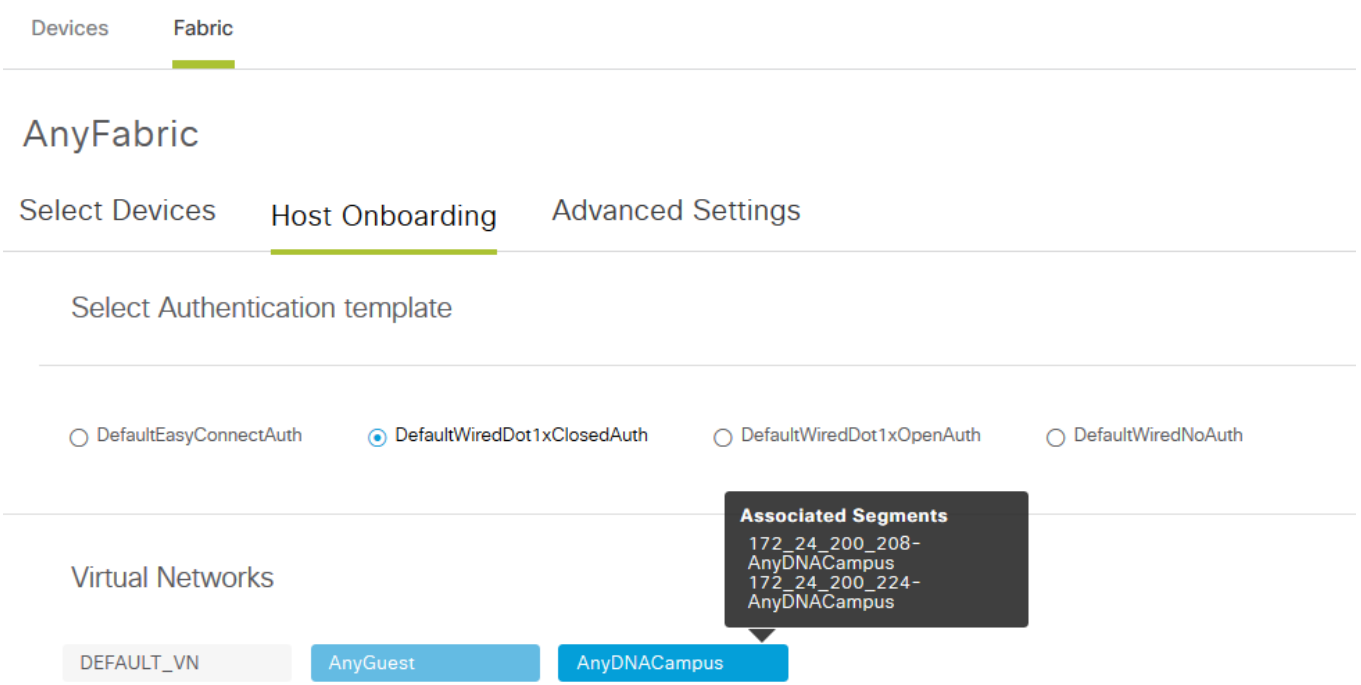
- Dynamisch
- Statisch

Create. Connect. Control.

DNA Center

Discover | Topology | Design | Policy | Provision

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



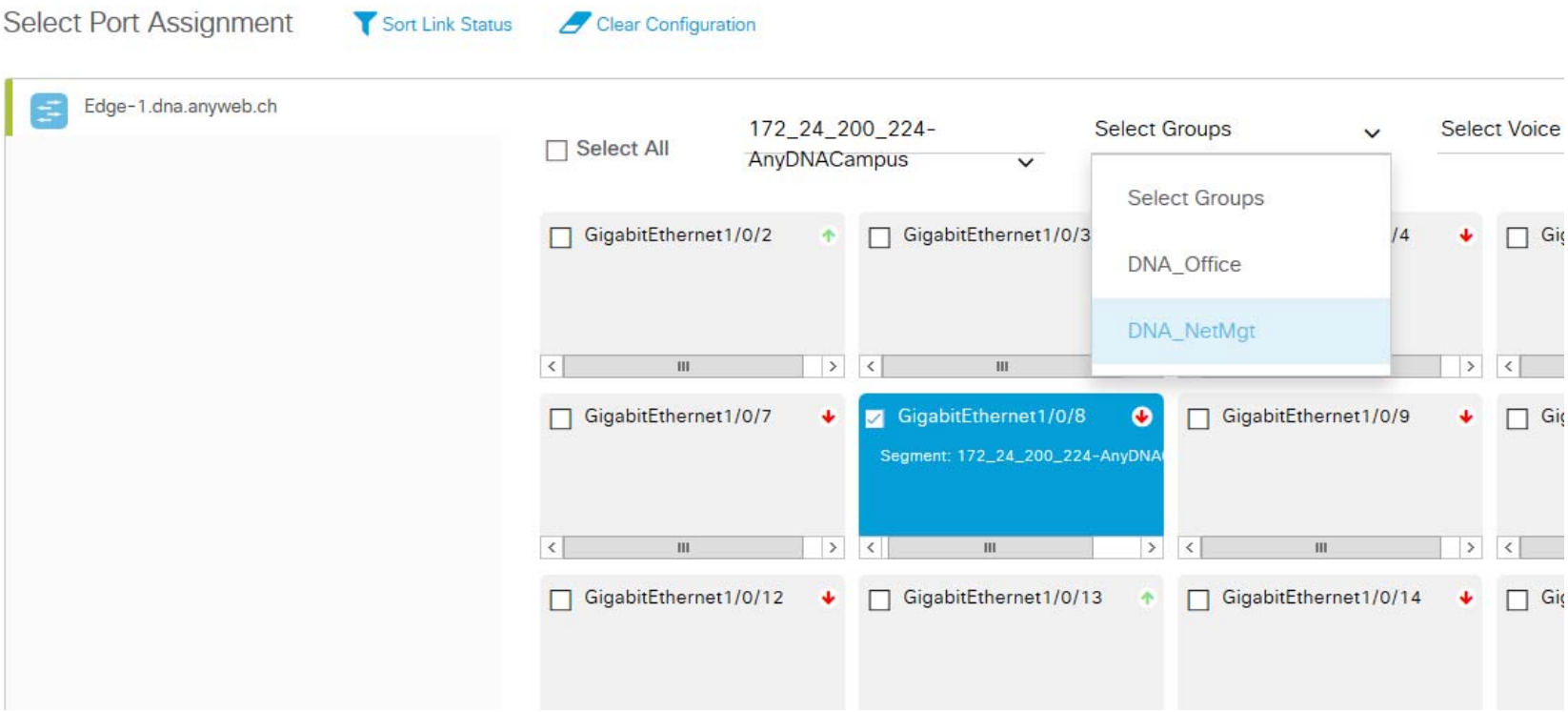
Dynamische Zuweisung des VLAN basierend auf der Rolle

Create. Connect. Control.

DNA Center

Discover | Topology | Design | Policy | Provision

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



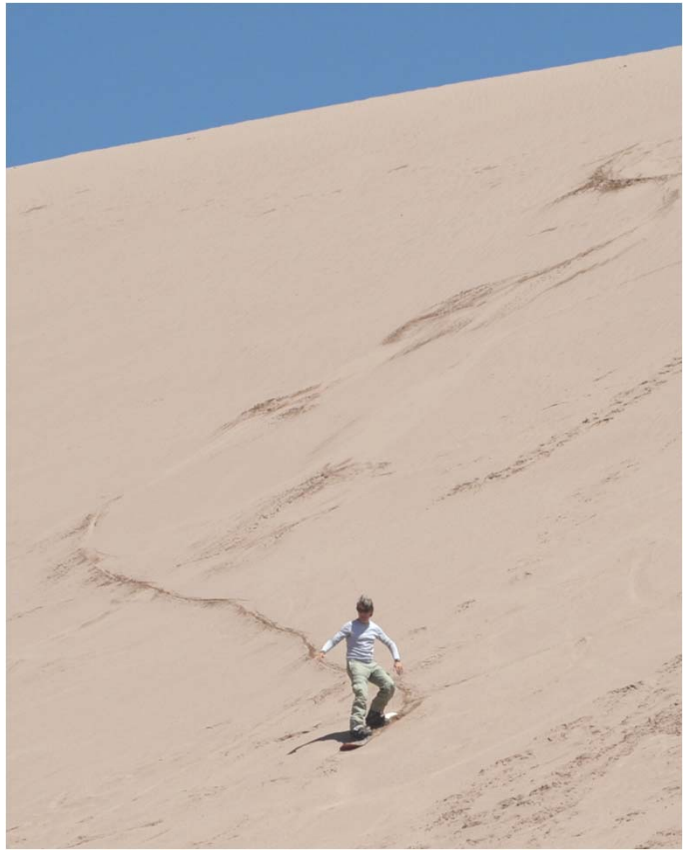
Statische Zuweisung des VLAN zu einem Port

Create. Connect. Control.
anyweb

It’s a journey

So

oder



so?

Create. Connect. Control.
anyweb

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!

Create. Connect. Control.
anyweb

DNA Center

Hands-on DNA-Center

Create. Connect. Control.
anyweb

DNA Center

Hands-on: Host Onbarding festlegen

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

Aktueller Zustand: dynamisch

Ziel: Port ist für einen Office Benutzer ohne Dot1x eingerichtet

Create. Connect. Control.
anyweb

DNA Center - Hands-on: Host Onbarding festlegen

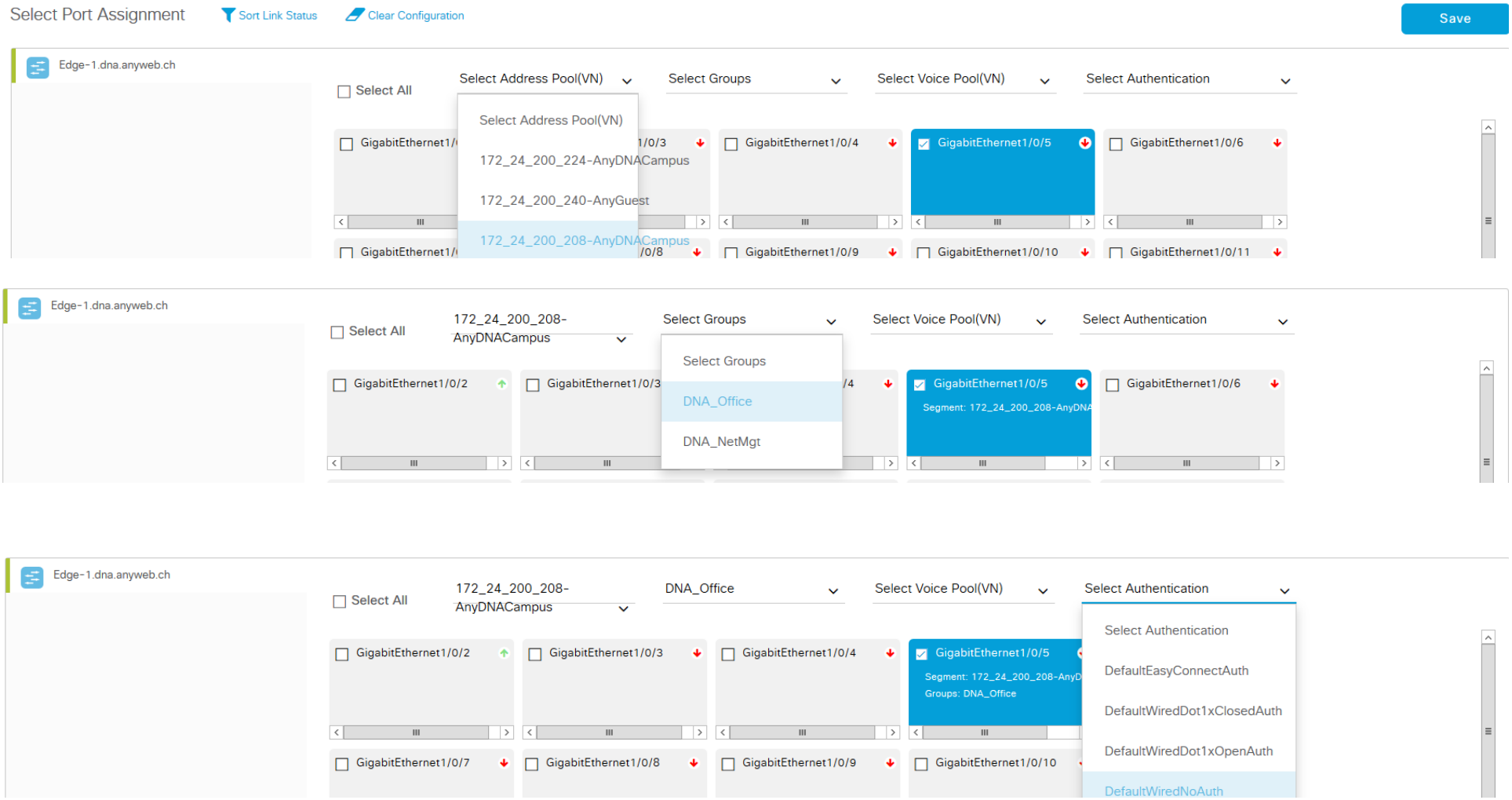
Konfig auf Switch-Port vor der Änderung:

```
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
```

Create. Connect. Control.

DNA Center - Hands-on: Host Onbarding festlegen

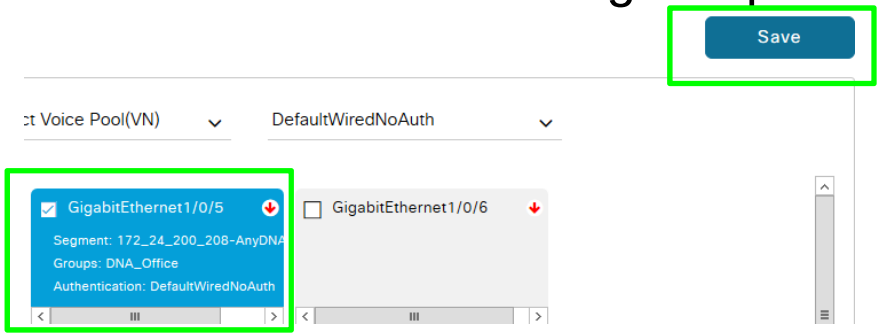
Port Gi 1/0/5 konfigurieren:



Create. Connect. Control.
anyweb

DNA Center - Hands-on: Host Onbarding festlegen

Port Gi 1/0/5 Änderungen speichern:



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
```

Create. Connect. Control.
anyweb

It’s a journey

Create. Connect. Control.
anyweb

DNA Center

Hands-on: Policy erstellen

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

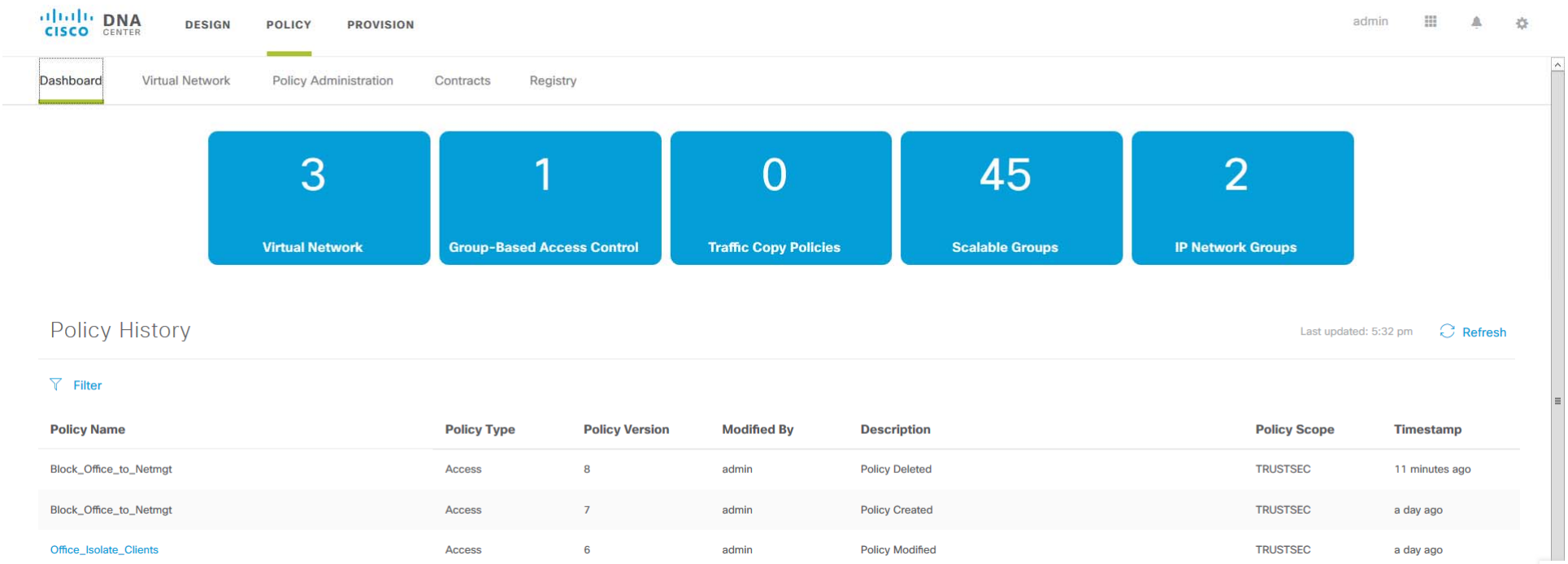
Aktueller Zustand: Beide Gruppen sind im gleichen Virtuellen Netz, als im gleichen VRF. Verkehr zwischen diesen beiden Gruppen ist im SDA erlaubt

Ziel: Eine Policy die den Verkehr verhindert

Create. Connect. Control.
anyweb

DNA Center - Hands-on: Policy erstellen

Policy Dashboard

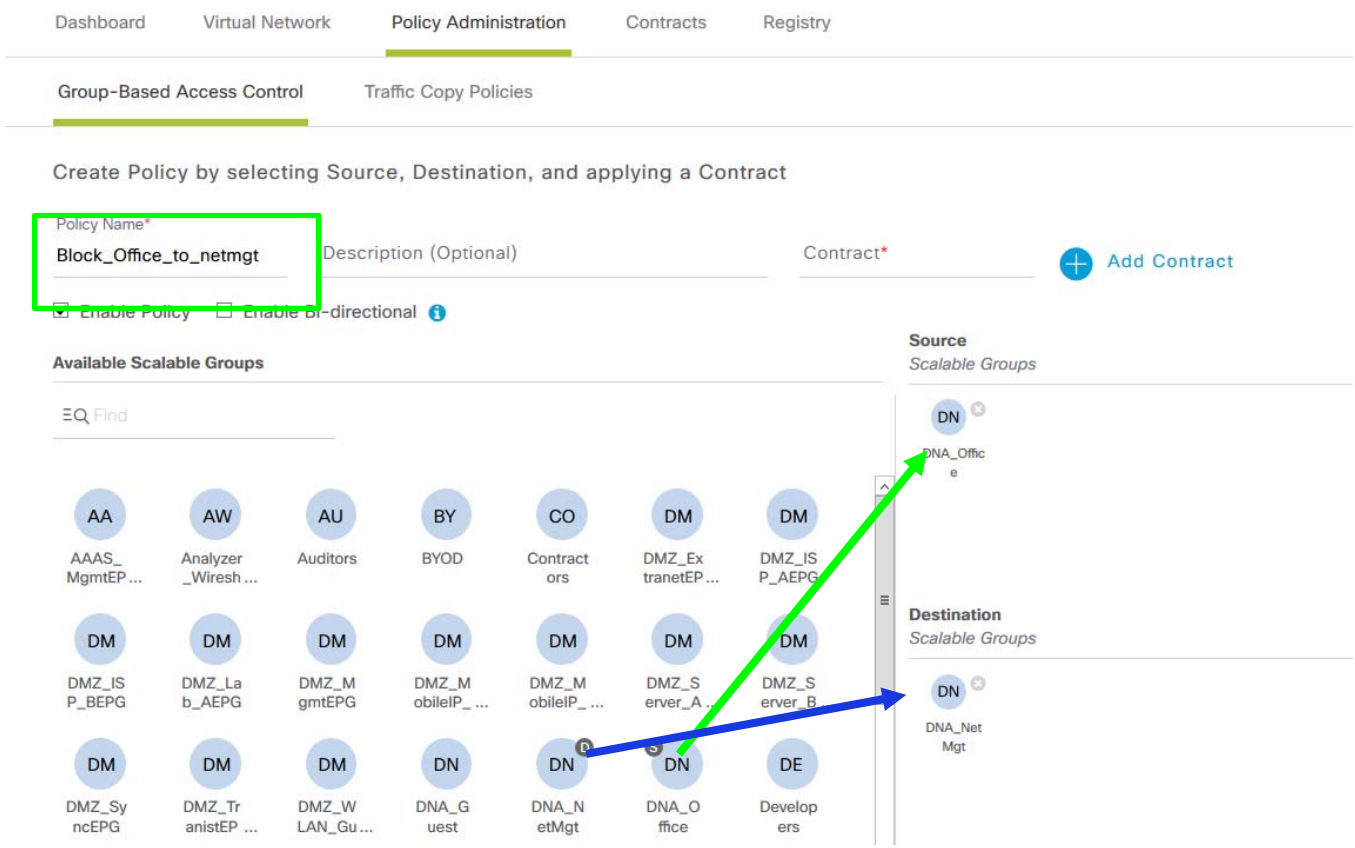


Create. Connect. Control.
anyweb

DNA Center - Hands-on: Policy erstellen

Add a Policy

- Policy Name
- Source- und Destination-gruppe bestimmen

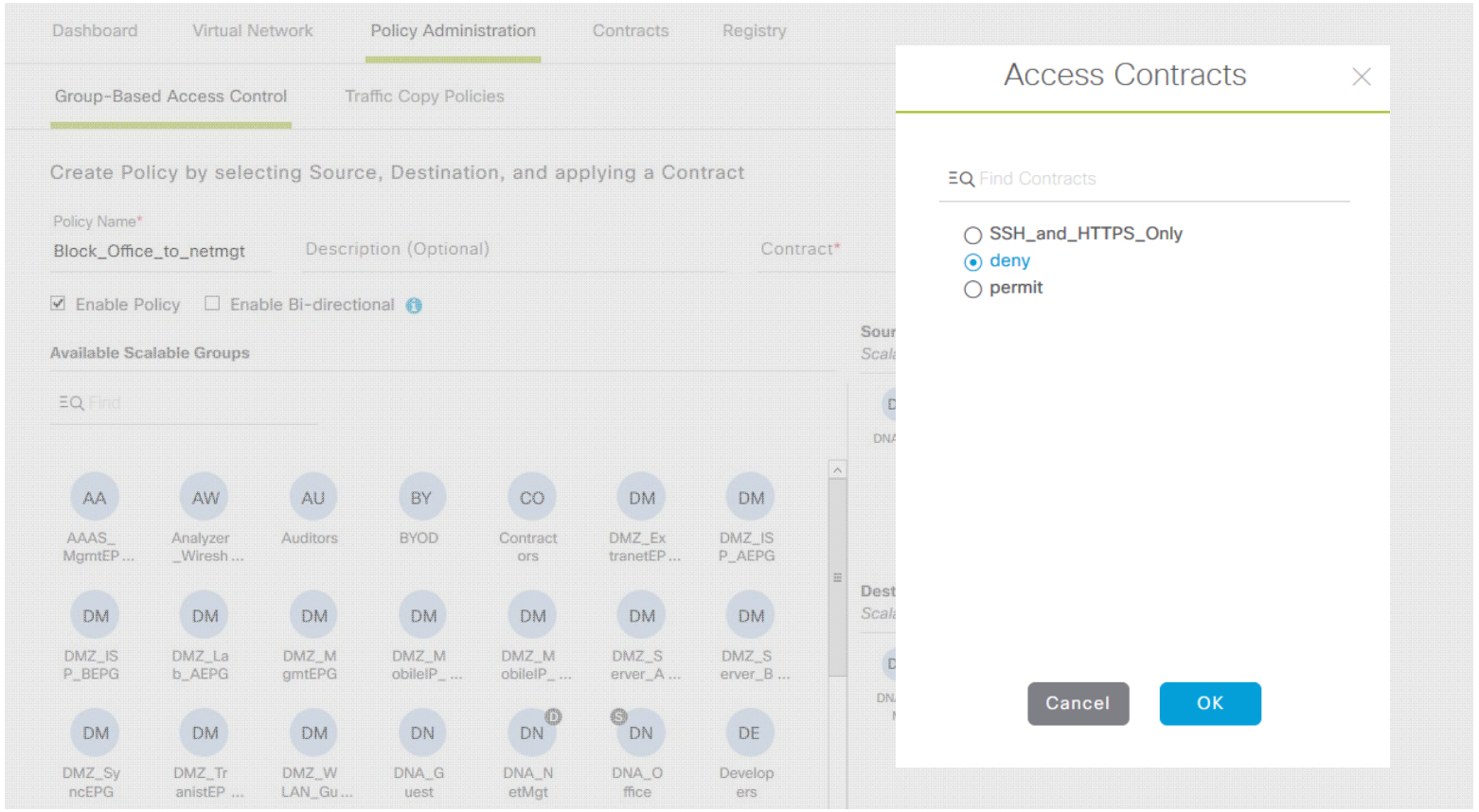


Create. Connect. Control.
anyweb

DNA Center - Hands-on: Policy erstellen

Add a Policy

- Deny Contract zufüge

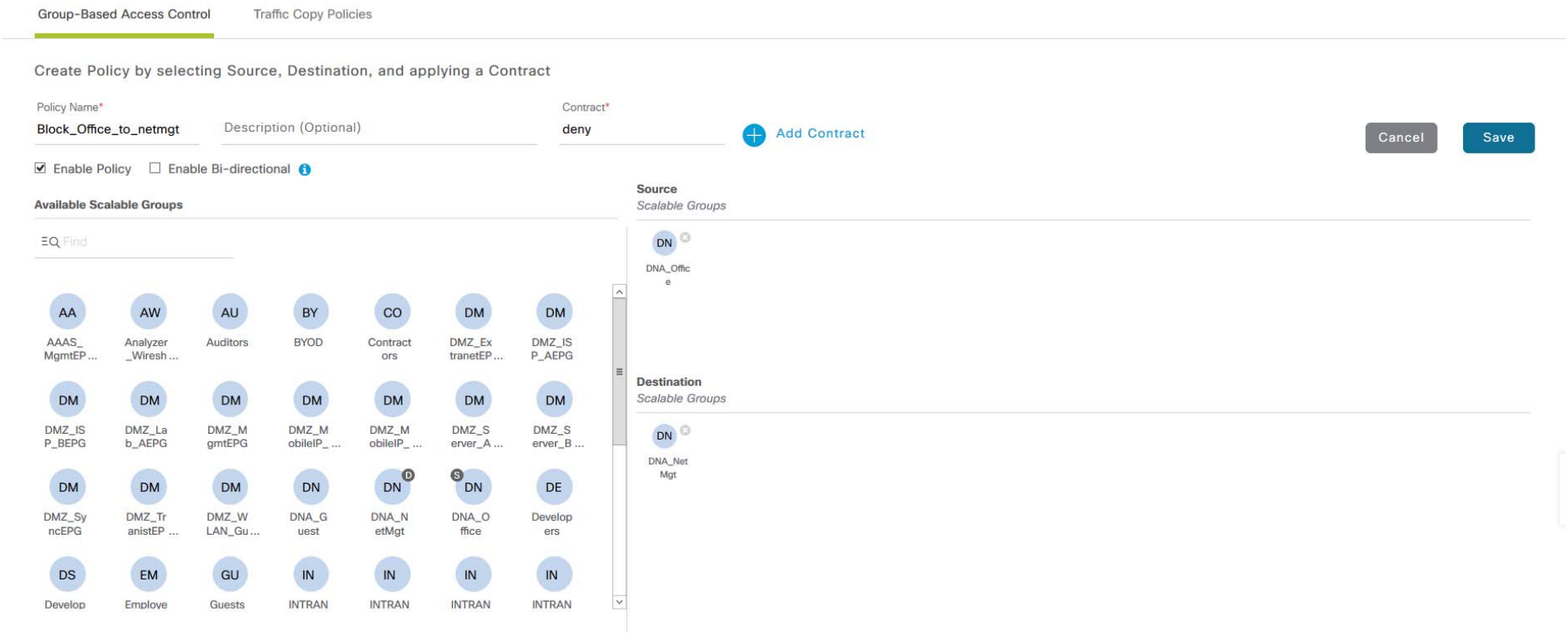


Create. Connect. Control.
anyweb

DNA Center - Hands-on: Policy erstellen

Add a Policy

- Policy speichern



Create. Connect. Control.

anyweb

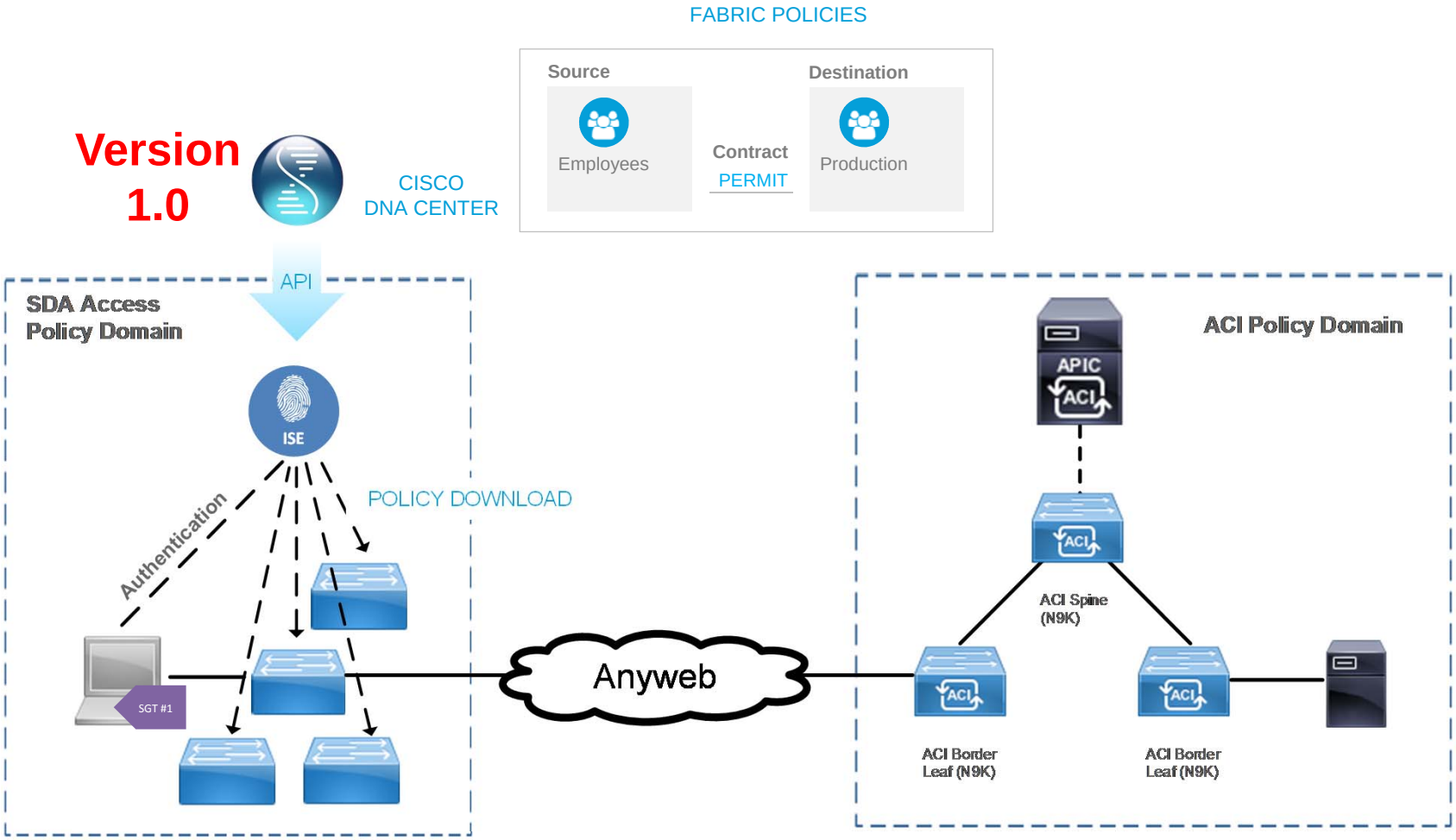
Setup

End-2-End Segmentierung mit Cisco DNA

Maria Koceba

Create. Connect. Control.
anyweb

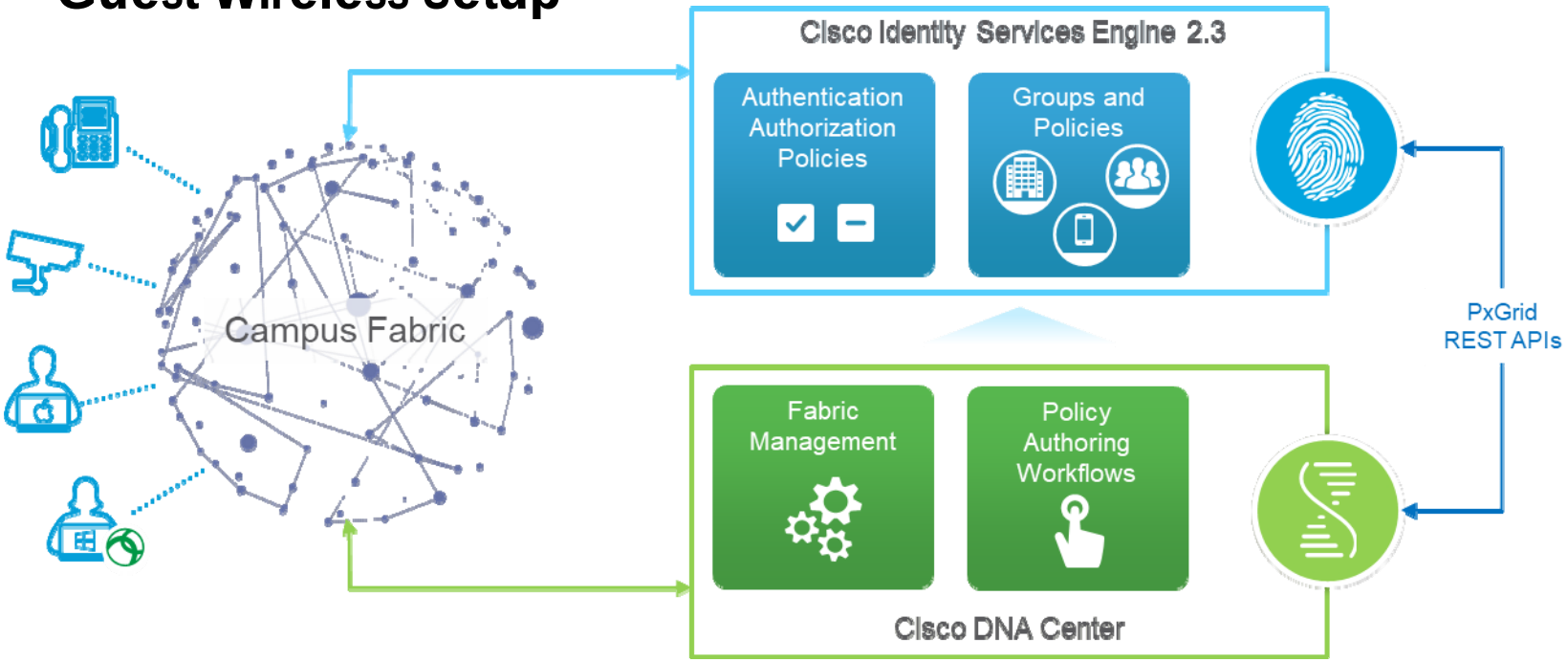
Putting it together..



Create. Connect. Control.
anyweb

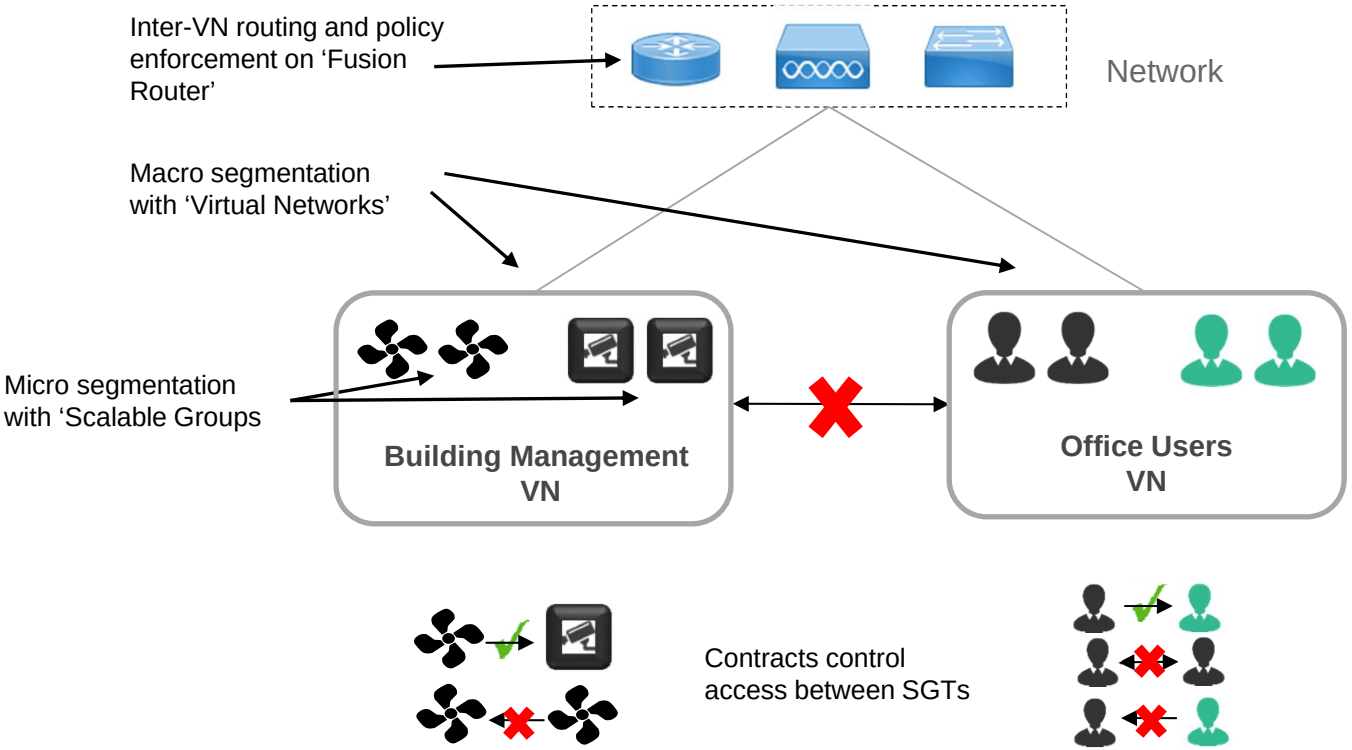
Rolle von ISE in DNA Center

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



Create. Connect. Control.
anyweb

Macro- und Micro-Segmentierung dank DNA



Create. Connect. Control.
anyweb

ISE & DNA Begriffe

ISE	DNA-Center
Security Group Tag (SGT)	Scalable Groups (SG)
TrustSec Matrix/ Security Group ACL (SGACL)	Policy Matrix/
AuthC & AuthZ Policies	

Cisco ISE

Cisco TrustSec (CTS) builds secure networks by establishing domains of tru
between devices in the domain is secured with a combination of encryption,

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

- 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

Network Working Group	M. Smith
Internet-Draft	R. Kandula
Intended status: Informational	Cisco Systems
Expires: April 20, 2017	October 17, 2016

Scalable-Group Tag eXchange Protocol (SXP)

draft-smith-kandula-sxp-05

Abstract

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

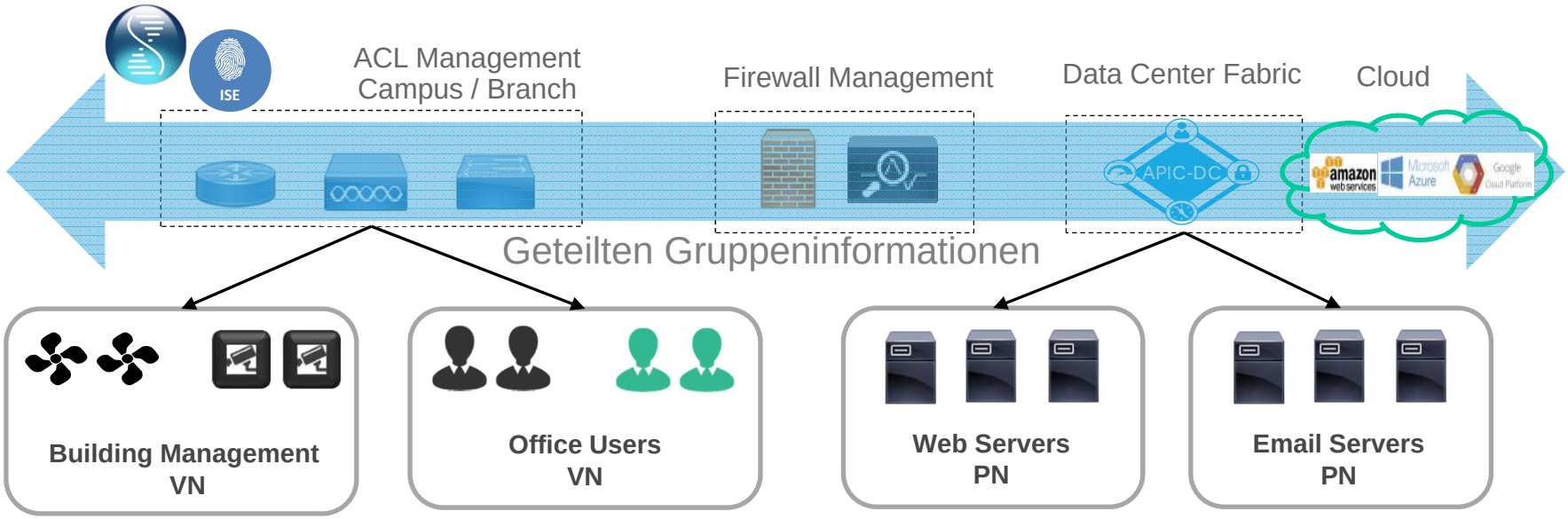
This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

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."

Create. Connect. Control.
anyweb

Vision



Create. Connect. Control.
anyweb

DNA Readiness

Wie kann DNA / SDA eingeführt werden?

→ It's a journey 

Create. Connect. Control.
anyweb

It’s a journey

Create. Connect. Control.
anyweb

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

Create. Connect. Control.
anyweb

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

Create. Connect. Control.

DNA Readiness

Ziele festlegen

- Welche Funktionen sollen im SDA unterstützt werden?
- Soll ein Proof of Concept durchgeführt werden
  - Anyweb empfiehlt das klar

Create. Connect. Control.
anyweb

DNA Readiness

Betroffene Komponenten (Switches, WLC, …) prüfen

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

Create. Connect. Control.
anyweb

DNA Readiness

Vorgehen festlegen

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

Create. Connect. Control.
anyweb

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 Benutzerauthentication sind betroffen

Create. Connect. Control.
anyweb

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

Create. Connect. Control.
anyweb

It’s a journey

Mars needs network engineers

Ischs no wiit?

Nei, jetzt simmer da Schatz!

Create. Connect. Control.
anyweb

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	✓ +
NPDESI	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

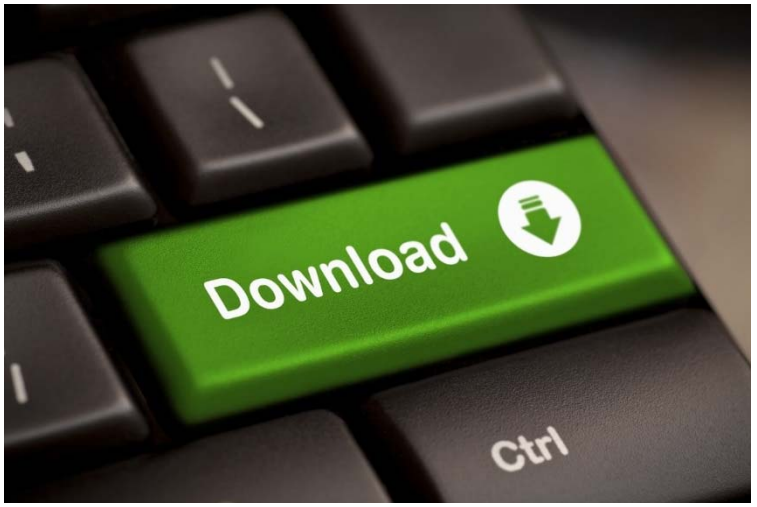
Service Provider CCNA / CCNP

Create. Connect. Control.
anyweb

Create. Connect. Control.
anyweb

Präsentationen

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



Create. Connect. Control.
anyweb

30. November: AnyWeb Practice Circle Cyber Security

Create. Connect. Control.
anyweb

Networking und Apéro