

The background features a vibrant, abstract design with a rainbow color palette. On the left, there are horizontal, wavy bands of color transitioning from dark blue at the top to yellow and orange at the bottom. On the right, a bright white light source emits a series of sharp, triangular rays of color in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

# Role of Cisco ISE in SD-Access Network

## SD-Access LISP VXLAN Fabric

Mahesh Nagireddy  
Technical Marketing Engineering, Technical Leader  
CCIE R&S  
BRKENS-2814

**CISCO** *Live!*

#CiscoLiveAPJC

# Cisco Webex App

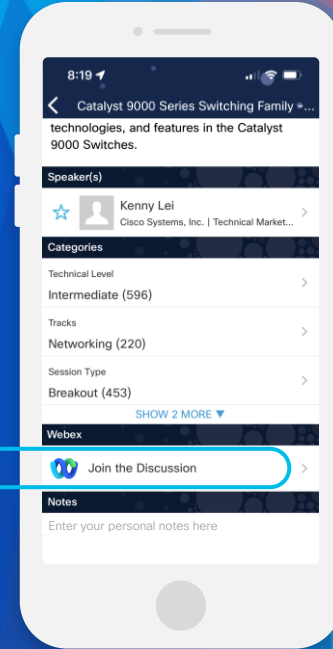
## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2814>

# Agenda

- Introduction
- Cisco ISE use cases in SD-Access Architecture
- Cisco Catalyst Center and ISE Integration
- Fabric Segmentation Strategy
- Multiple Cisco Catalyst Center
- Summary

# SD-Access LISP VXLAN Fabric

## Industry Leading Campus Architecture

3500+  
Deployments

70% Wireless Deployments

16,000 + Fabric sites  
1.43M+ Devices (switches + AP)

Adopted by 30% of Fortune25 Customers

Largest  
Deployments

761K Endpoints

2,907 Sites

3,227 Devices

Enabling Wins across Verticals

**UCLA Health**

*Higher Education & Research*

**Fiona Stanley Hospital**

*Healthcare*

**TOYOTA Americas**

*Manufacturing*

**BBVA**

*Financial*

**Volkswagen**

*Manufacturing*

**NHS**

*Healthcare*

# Modern, Open and Scalable Fabrics

IETF Standard based Protocols

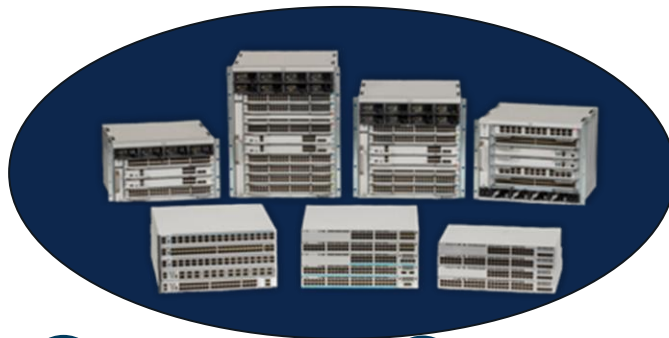
Cisco Catalyst Center

Cisco SD-Access

LISP VXLAN Fabric\*



Cisco Catalyst 9000



BGP EVPN VXLAN Fabric



Enterprise



Healthcare



Education



Financial



Public Sector



Manufacturing



Hospitality



Media



Transportation



Retail

**cisco** *Live!*

\*Cisco's Lead Motion

# Flexible Fabric Options Tailored to *Customer Outcomes!*

*SD-Access with  
LISP Control Plane  
VxLAN Data Plane*

*SD-Access with  
BGP EVPN Control Plane  
VxLAN Data Plane*

## Network Simplification

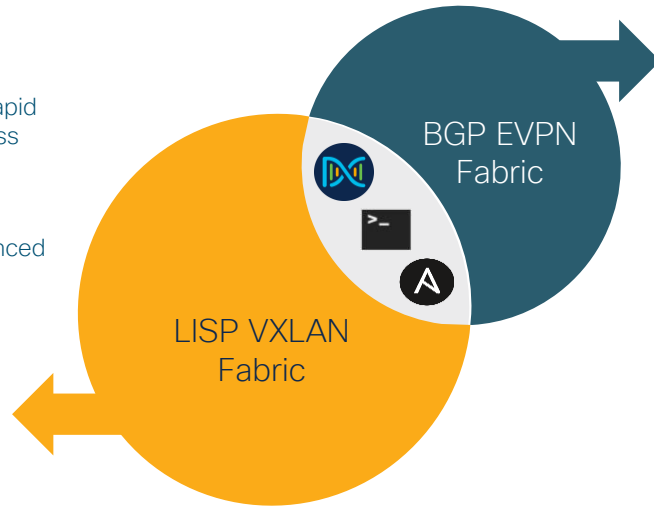
Lightweight, extensible, massive scale with rapid convergence. Single overlay for wired/wireless

## Mobility First Requirement

Fabric Integrated Wireless, L2 Mobility, Enhanced wireless performance

## Segmentation

Zero-Trust Architecture with Unified Wired + Wireless Policy



## One Fabric Architecture (Campus & DC)

Operational ease with a single familiar protocol

## Multi-vendor interoperability

Vendor-agnostic solution with unique Cisco differentiators

**One Infrastructure | Single Data plane | Consistent Zero-Trust Experience**

# Cisco ISE Overview

## Value of Cisco ISE

Cisco Identity Services Engine (ISE) is an industry leading, Network Access Control and Policy Enforcement platform, that lets you,



**See**

Users, endpoints and applications



**Secure**

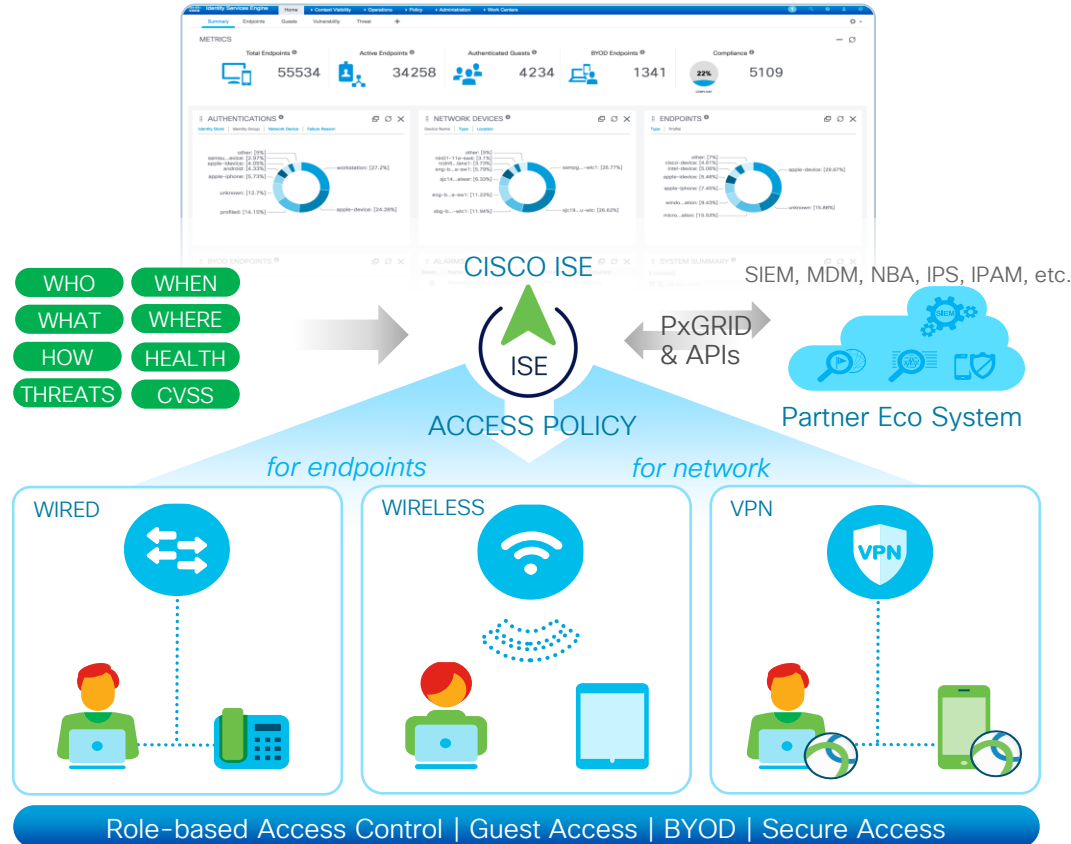
By controlling network access and segmentation



**Share**

Context with partners for enhanced operations

**CISCO** *Live!*

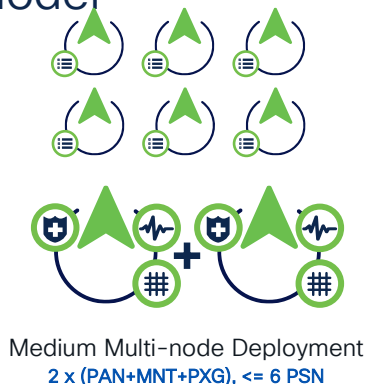
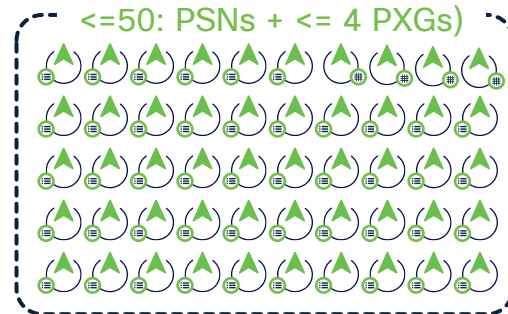


# ISE Deployment Scale

[cs.co/ise-scale](https://cs.co/ise-scale)

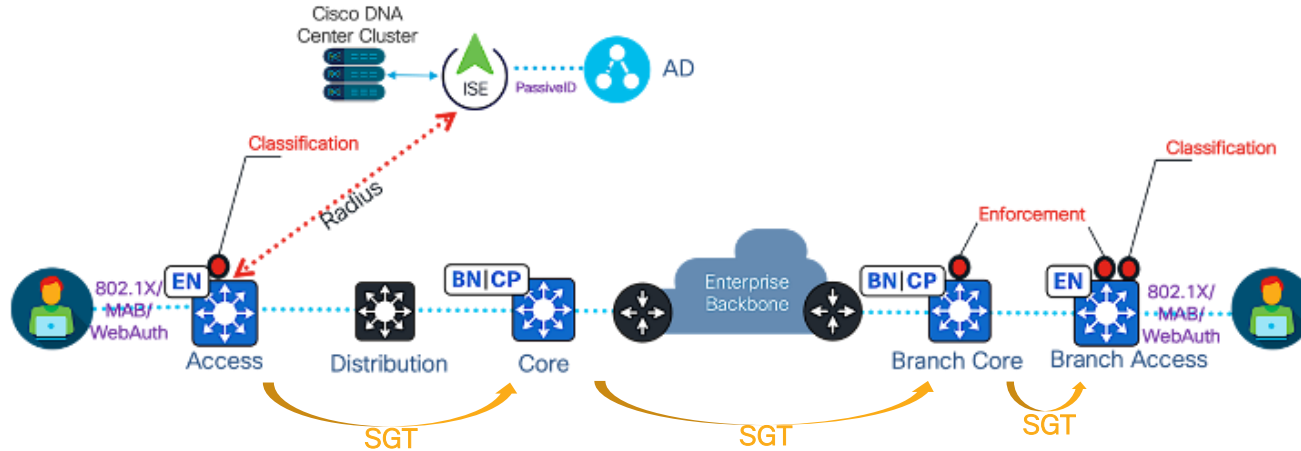
## Standalone to Distributed

- Same for physical and virtual deployments
- Compatible with load balancers
- No changes to current Licensing Model



|      |               |                        |                           |
|------|---------------|------------------------|---------------------------|
| 3700 | 100 Endpoints | Up to 50,000 Endpoints | Up to 2,000,000 Endpoints |
| 3600 | 100 Endpoints | Up to 50,000 Endpoints | Up to 2,000,000 Endpoints |
| 3595 | 100 Endpoints | Up to 20,000 Endpoints | Up to 500,000 Endpoints   |

# Cisco SD-Access Architecture

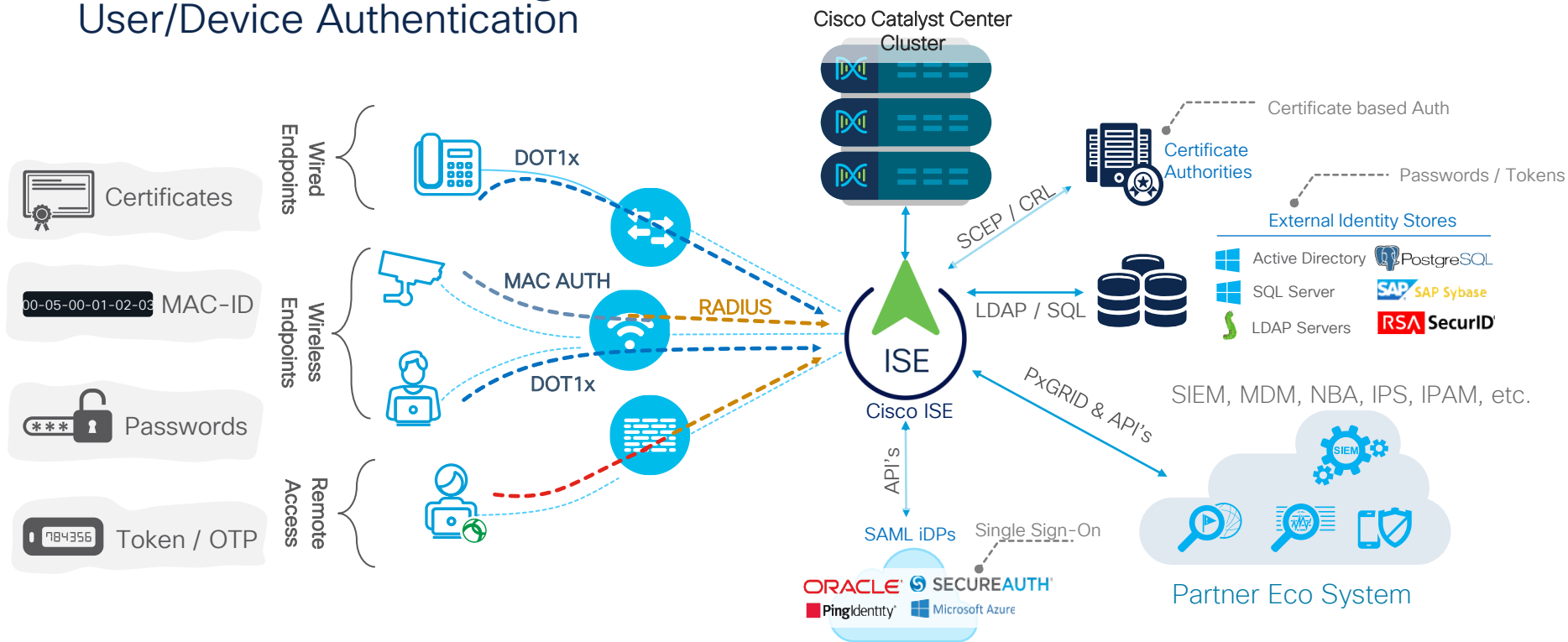


- Fully automated configuration from Cisco Catalyst Center as part of Fabric provisioning
- Centralized policy Management and visibility on Cisco Catalyst Center
- Macro and Micro segmentation for increased scale
- Use Tags vs Network constructs to assign policy

# Cisco ISE use cases in SD-Access Architecture

# Host Onboarding

## User/Device Authentication



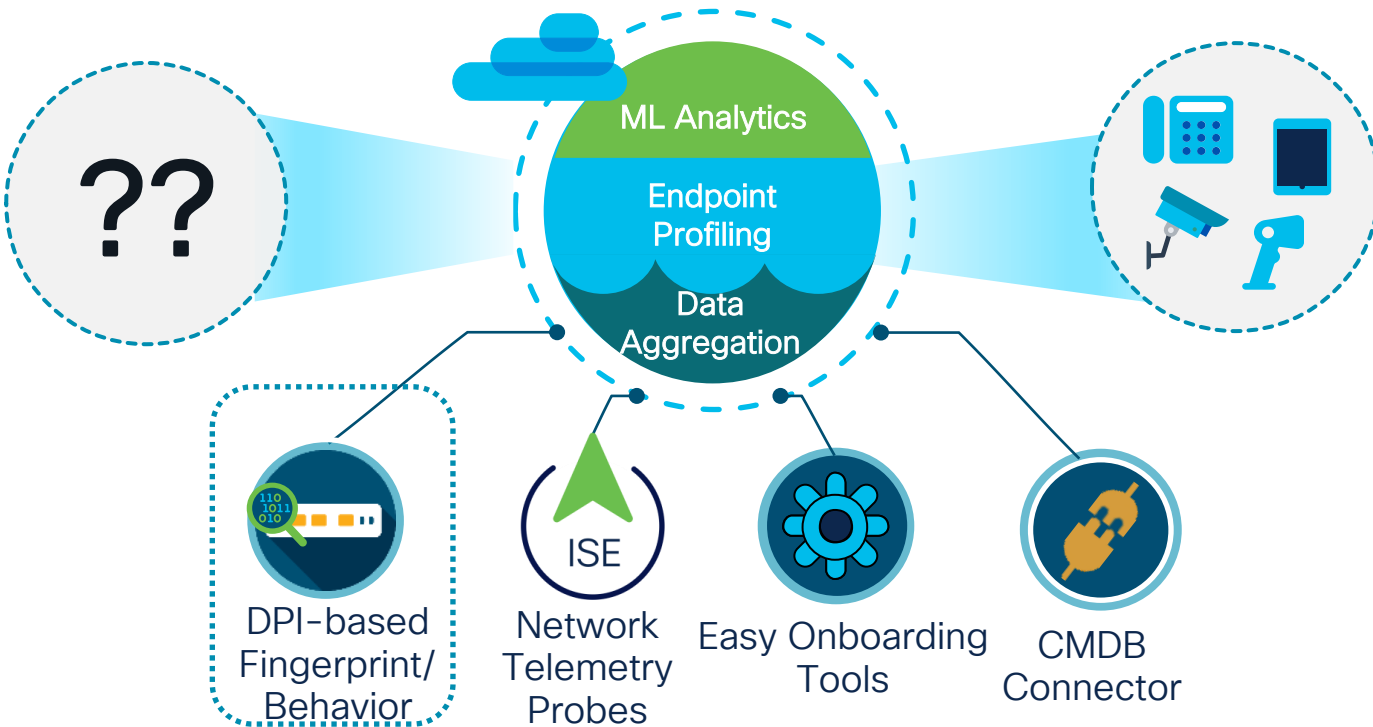
AAA, Policy-Based Segmentation and Context Sharing

# Cisco Endpoint Analytics

Endpoint profiling, data sources and ML Analytics

Rapidly reducing the unknowns by aggregating data from different sources

Starting  
Catalyst Center: 2.1.2.4 onwards  
Cisco ISE : 2.4P11 / 2.6 P5 / 2.7 P1 onwards  
IOS XE: 17.3.1 onwards  
License: DNA Advantage



## Classifying endpoints

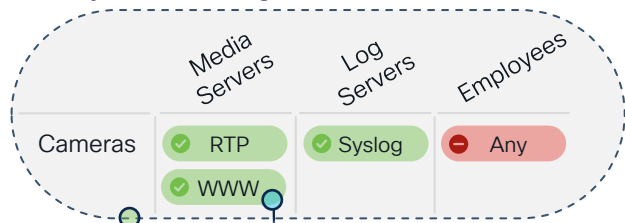
-  Device type
-  Hardware model
-  Hardware MFR
-  Operating system

# Cisco Policy Analytics

## Deploy group policies with confidence

Starting  
Catalyst Center: 2.1.1 onwards  
Cisco ISE : 2.4P7 / 2.6 P1 / 2.7 onwards  
Stealthwatch Version : 7.x onwards  
License: DNA Advantage

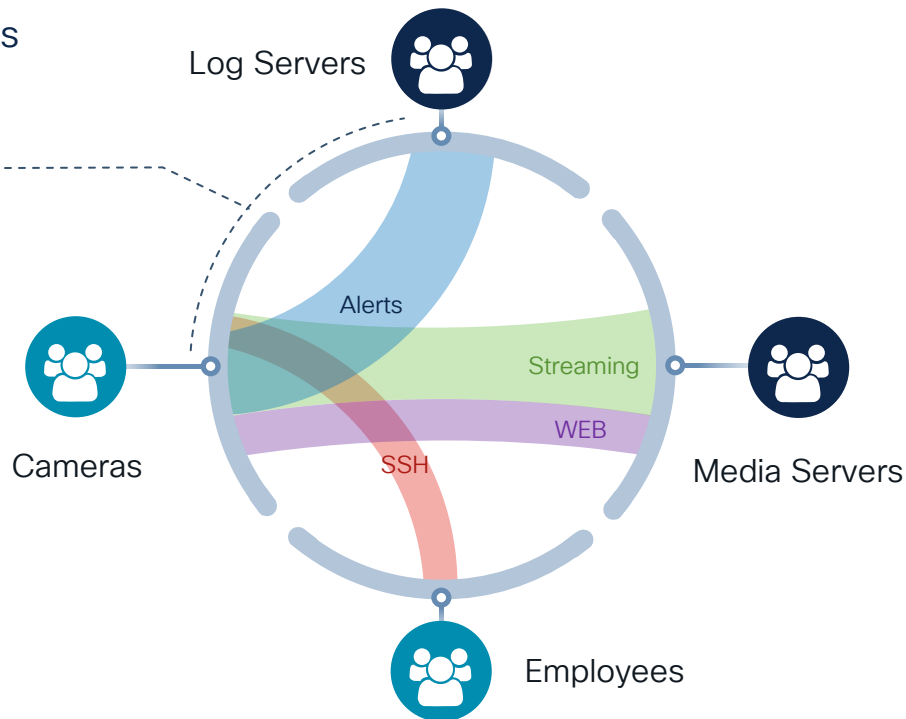
### Policy Modeling – With traffic patterns



Unearth critical access that must be allowed / denied

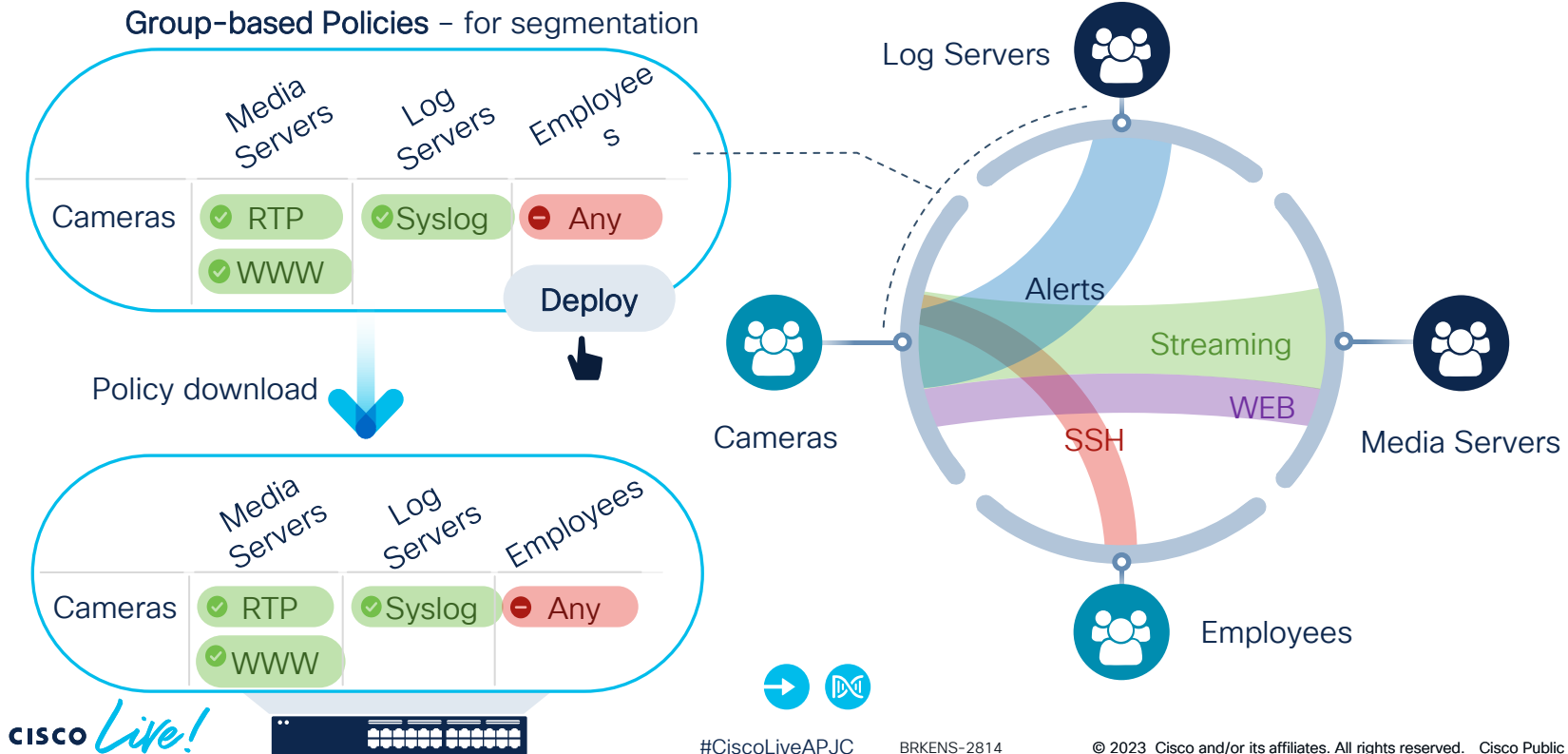
Observe and fine-tune for days/weeks

No policy on the network, yet



# Cisco Policy Analytics

## Deploy group policies with confidence



# Multiple Cisco Catalyst Center Solution Overview

## Cisco ISE Deployment (Cluster)

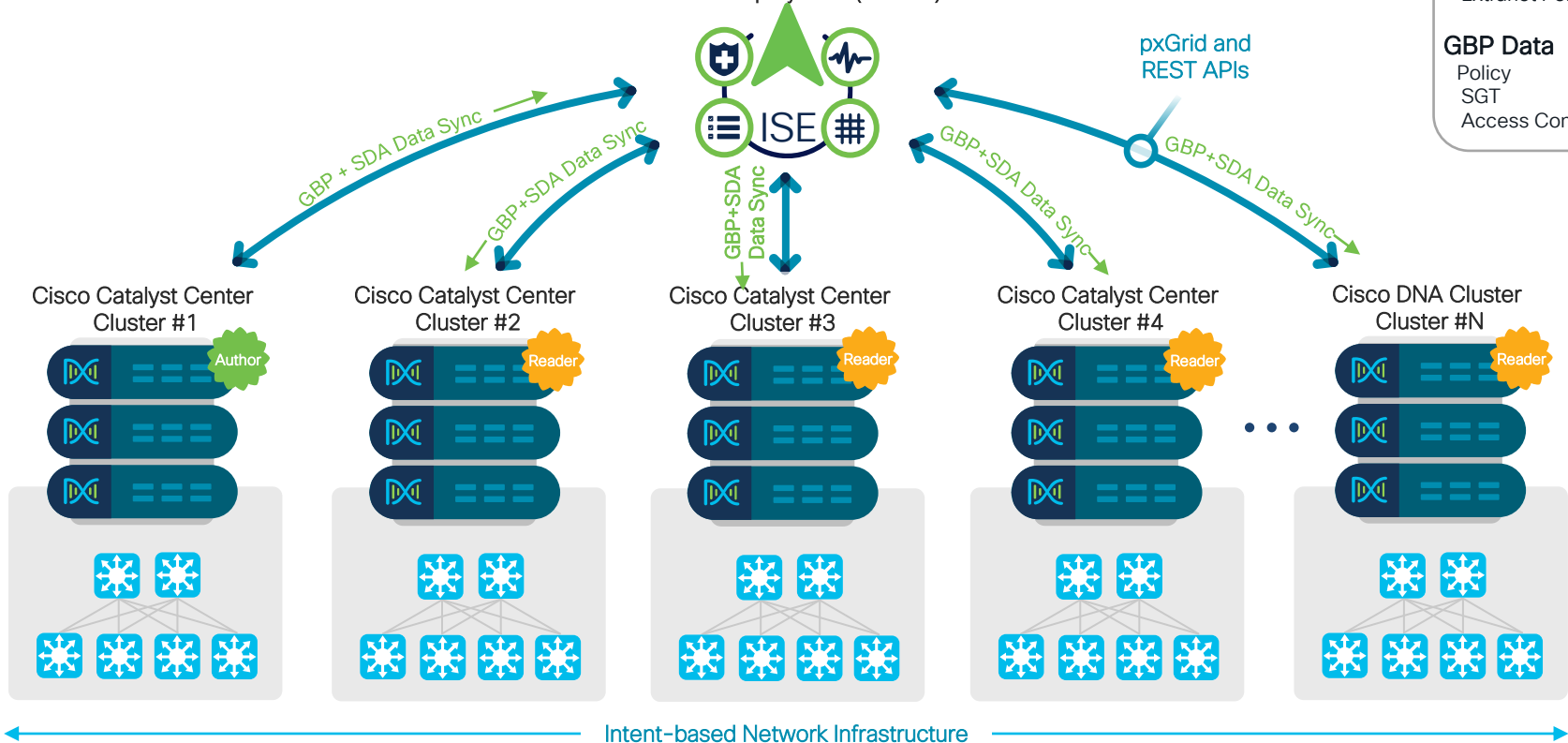
Starting Catalyst Center  
release : 2.2.3.x  
N=5

SD-Access Data

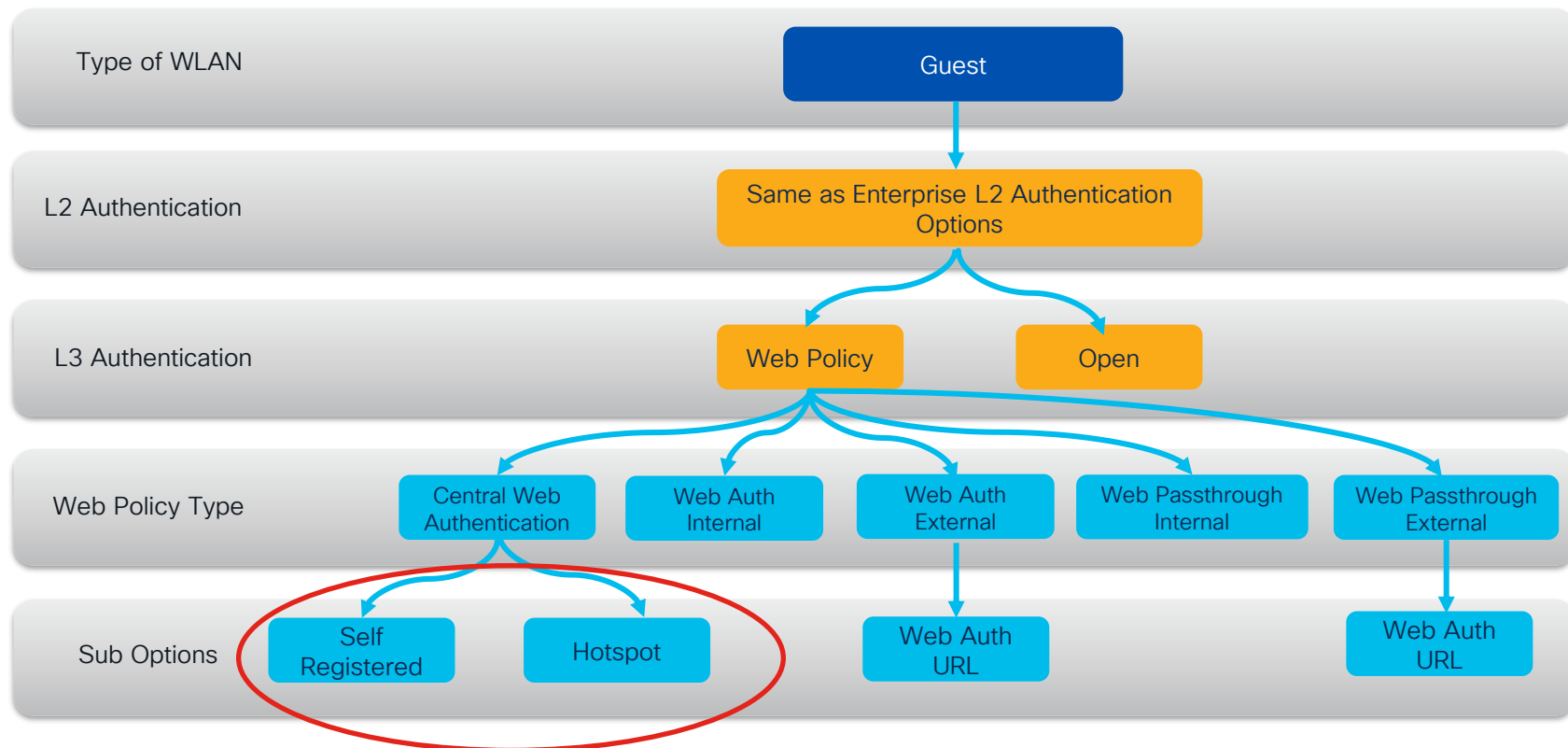
## Virtual Network Extranet Policy

## GBP Data

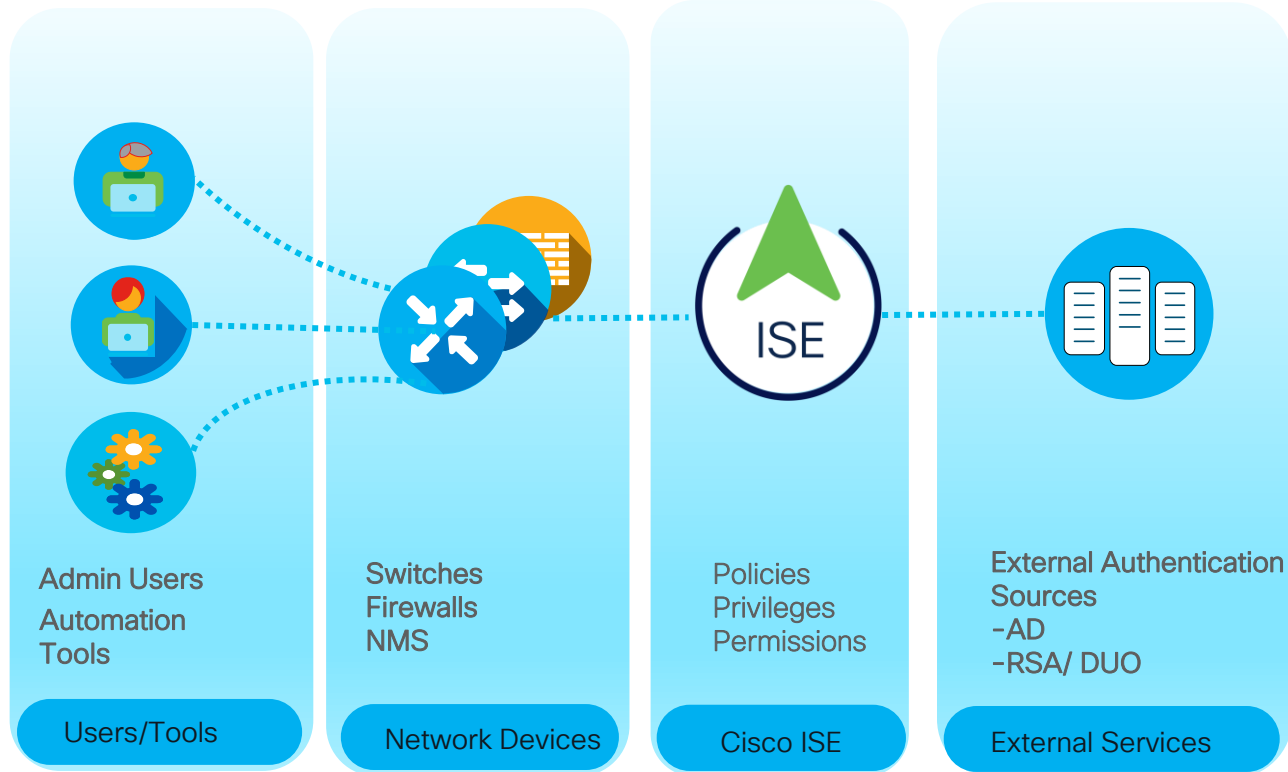
Policy  
SGT  
Access Contract



# Guest Workflow

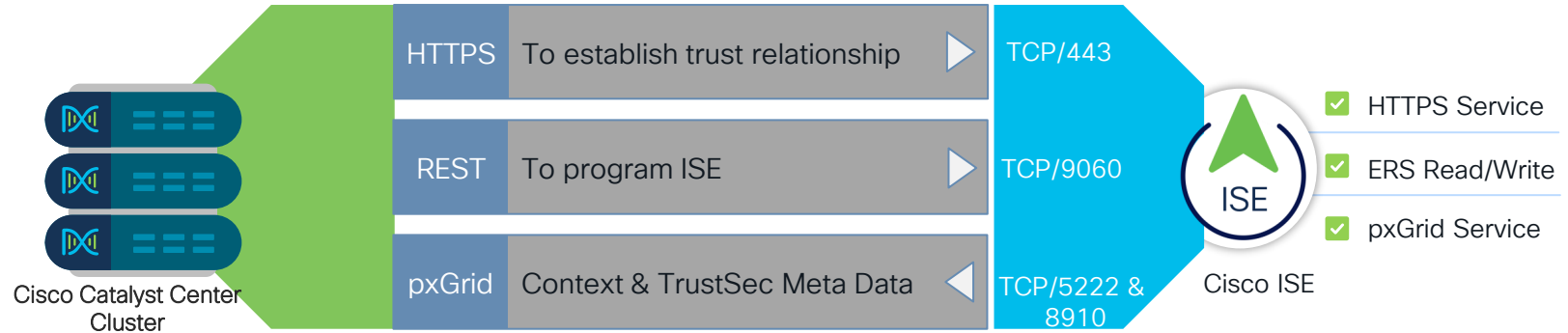


# ISE Deployment for Device Administration



# Cisco Catalyst Center and ISE Integration

# Cisco Catalyst Center & ISE Communication



## Cisco ISE: Enable below ISE Services

Administration > System > Deployment > Select ISE Host Name

Enable pxGrid Services

Administration > Settings > ERS Settings

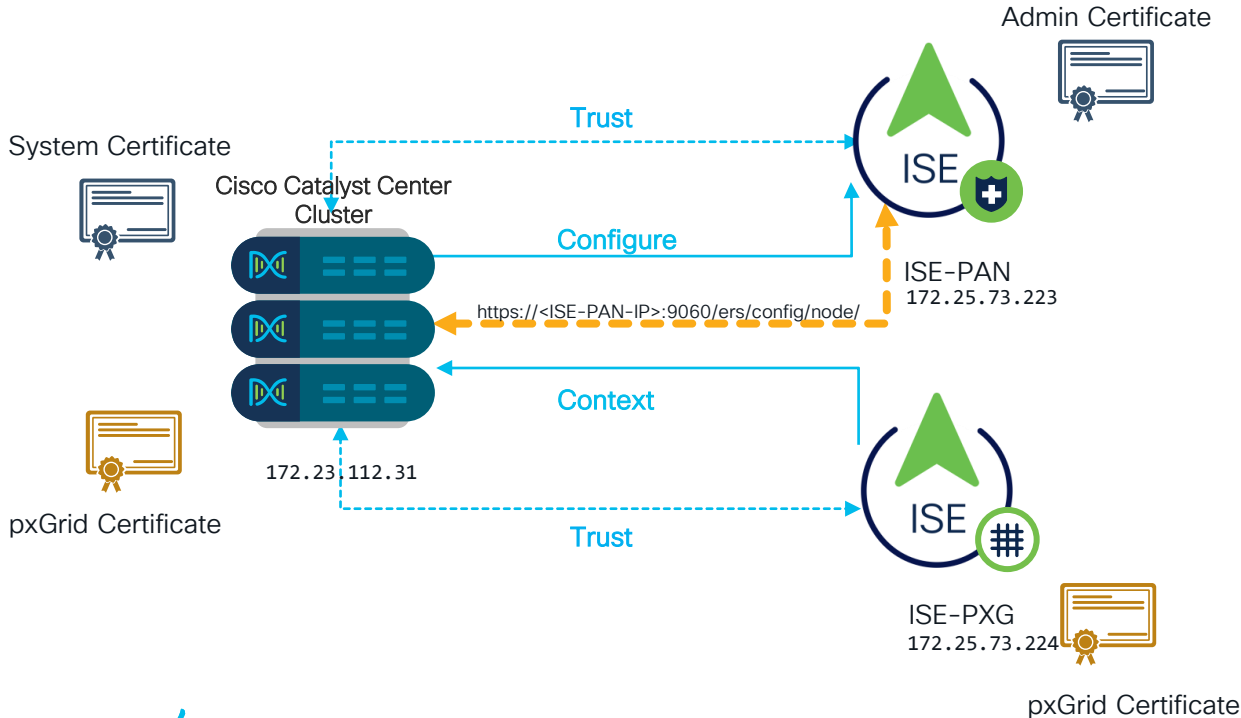
Enable *ERS for Read/Write on PAN*

*Enable ERS for Read on All other Nodes incase of Distributed model*

# Cisco Catalyst Center and ISE Integration

## How Catalyst Center Trust PxGrid Node

From the Cisco Catalyst Center [home](#) page, click **System > Settings > Authentication and Policy Servers** and then choose



### Edit ISE server

Server IP Address  
172.25.73.223

Shared Secret

Username\*  
admin

Password\*

FQDN  
ISE10-1.demo.local

Subscriber Name  
DNAC10

Virtual IP Address(es)

☒ Advanced Settings

☒ Connect to pxGrid

☐ Use Cisco DNA Center Certificate for pxGrid

Protocol

☒ RADIUS ☐ TACACS

Authentication Port  
1812

Accounting Port  
1813

Port  
49

Retries\*  
3

Timeout (seconds)\*  
4

Cancel

Add

# Cisco Catalyst Center Settings

## Cisco ISE + Load Balancer

The screenshot shows the Cisco DNA Center web interface. The left sidebar contains a search bar and a list of settings categories: Cisco Accounts, Device Settings, External Services, and Authentication and Policy Servers. The main content area is titled 'Authentication and Policy Servers' and contains a table of configured servers. The 'Edit ISE server' dialog is open on the right, showing fields for Server IP Address, Shared Secret, Username, Password, FQDN, Subscriber Name, and Virtual IP Address(es). A blue callout bubble points to the 'Virtual IP Address(es)' field, which contains the value '172.25.73.240'.

System · Settings

Search Settings

Cisco Accounts

- PnP Connect
- Cisco.com Credentials
- Smart Account
- Smart Licensing
- SSM Connection Mode

Device Settings

- Device Controllability
- Network Resync Interval
- SNMP
- ICMP Ping
- Image Distribution Servers
- Device EULA Acceptance
- PnP Device Authorization

External Services

- Umbrella

Authentication and Policy Servers

- Authentication Tokens
- Integrity Verification
- vManage
- IP Address Manager
- Webex Integration

Settings / External Services

### Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

[Add](#) [Export](#)

| IP Address    | Protocol      | Type |
|---------------|---------------|------|
| 172.25.73.223 | RADIUS_TACACS | ISE  |

#### Edit ISE server

Server IP Address  
172.25.73.223

Shared Secret

Username\*  
admin

Password\*

FQDN  
ISE10-1.demo.local

Subscriber Name  
DNAC10

Virtual IP Address(es)  
172.25.73.240

Advanced Settings

Cancel Add

Load Balancer VIP

# Cisco Catalyst Center Design

## ISE as AAA Server for Client and Network

**Edit ISE server**

Server IP Address  
172.25.73.226

Shared Secret

Username\*  
admin

Password\*

FQDN  
ISE10-1.demo.local

Subscriber Name  
DNAC10

Virtual IP Address(es)

☐ Advanced Settings

☐ Connect to pxGrid

☐ Use Cisco DNA Center Certificate for pxGrid

Protocol  
☒ RADIUS ☐ TACACS

Authentication Port  
1812

Accounting Port  
1813

Port  
49

Retries\*  
3

Timeout (seconds)\*  
4

**Cisco DNA Center** Design · Network Settings

Network Device Credentials IP Address Pools SP Profiles Wireless Telemetry

Find Hierarchy

- Global
  - SITE-A
    - Building 1
      - Floor1
        - SITE-B
        - SITE-C
        - SITE-D
        - SITE-F
        - SITE-T

Configure AAA, NTP, and Image Distribution (SFTP) servers using the "Add Servers" link. Once devices are discovered, DNA Center will deploy using these settings.

**AAA Server**

☒ Network ☒ Client/Endpoint

**NETWORK**

Servers  
☒ ISE ☐ AAA

Protocol  
☐ RADIUS ☒ TACACS

Network  
172.25.73.223

IP Address (Primary)  
192.168.1.225  
(Only device administration nodes)

IP Address (Additional)  
192.168.1.226

- PSNs -  
192.168.1.225  
172.25.73.225  
192.168.1.226  
172.25.73.226

**CLIENT/ENDPOINT**

Servers  
☒ ISE ☐ AAA

Protocol  
☒ RADIUS ☐ TACACS

Client/Endpoint  
172.25.73.223

IP Address (Primary)  
192.168.1.225

IP Address (Additional)  
192.168.1.226

[Change Shared Secret](#)

[Change Shared Secret](#)

DHCP Server

CISCO *Live!*

# Cisco Catalyst Center Settings

## Authentication and Policy Servers – 1 Cisco ISE + N AAA Servers

☰ Cisco DNA Center

System · Settings

🔍 ? 🟢 🔔

🔍 Search Settings

Cisco Accounts

PnP Connect

Cisco.com Credentials

Smart Account

Smart Licensing

SSM Connection Mode

Device Settings

Device Controllability

Network Resync Interval

SNMP

ICMP Ping

Image Distribution Servers

Device EULA Acceptance

PnP Device Authorization

External Services

Umbrella

Authentication and Policy Servers

Authentication Tokens

Integrity Verification

vManage

IP Address Manager

Webex Integration

Settings / External Services

Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

✔ Settings updated successfully.

⊕ Add

📄 Export

As of: Jun 7, 2022 12:22 PM

| IP Address    | Protocol      | Type | Status | Actions |
|---------------|---------------|------|--------|---------|
| 172.25.73.223 | RADIUS_TACACS | ISE  | ACTIVE | ⋮       |
| 172.25.73.251 | TACACS        | AAA  | ACTIVE | ⋮       |
| 172.25.73.250 | RADIUS        | AAA  | ACTIVE | ⋮       |

# Cisco Catalyst Center Design Authentication Template

← → ↺ <https://172.23.112.31/dna/design/authTemplate> ☆ ⬇ 📄 ☰

☰ Cisco DNA Center

Design · Authentication Template

🔍 ? 🟢 🔔

Last updated: 4:28 PM [Refresh](#)

🔍 Filter

🔍 Find

Name ▾

Type

[Closed Authentication](#)

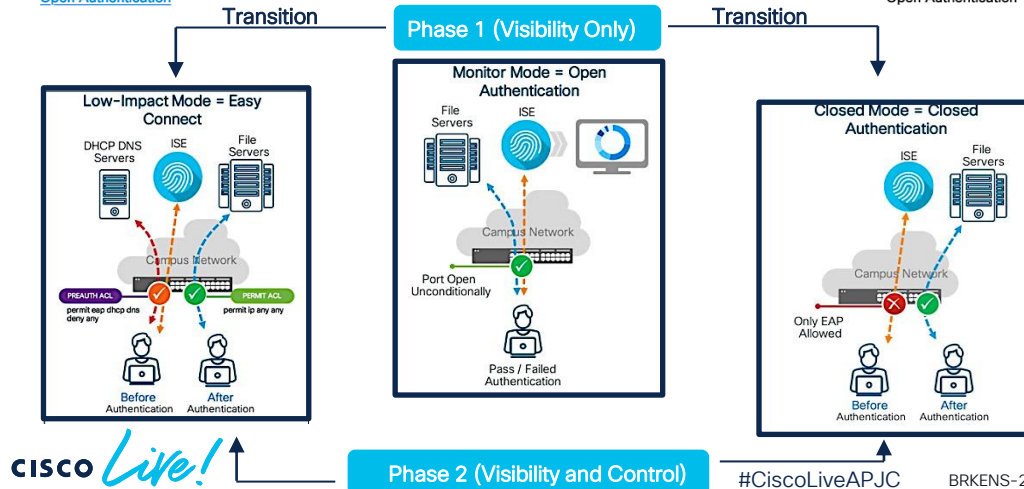
Closed Authentication

[Low Impact](#)

Low Impact

[Open Authentication](#)

Open Authentication



CISCO *Live!*

Phase 2 (Visibility and Control)

#CiscoLiveAPJC

BRKENS-2814

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

26

# Cisco Catalyst Center Design

## Closed Authentication Template

### Closed Authentication

Deployment Mode: Closed

First Authentication Order: ☒ 802.1x ☐ MAC Auth Bypass(MAB)

802.1x to MAB Fallback:  3 to 14

Wake on LAN: ☐ Yes ☒ No

Number of Hosts: ☐ Single ☒ Unlimited

Authentication Timer Settings

Multi-Auth Host Mode

Multi-Domain Host Mode

### Easy Connect

Deployment Mode: Open

First Authentication Order: ☒ 802.1x ☐ MAC Auth Bypass(MAB)

802.1x to MAB Fallback:  3 to 21

Wake on LAN: ☐ Yes ☒ No

Number of Hosts: ☐ Single ☒ Unlimited

Pre-Auth Access Control (Low Impact Mode)

Implicit Action: ☒ Deny

Name: IPV4\_PRE\_AUTH\_ACL

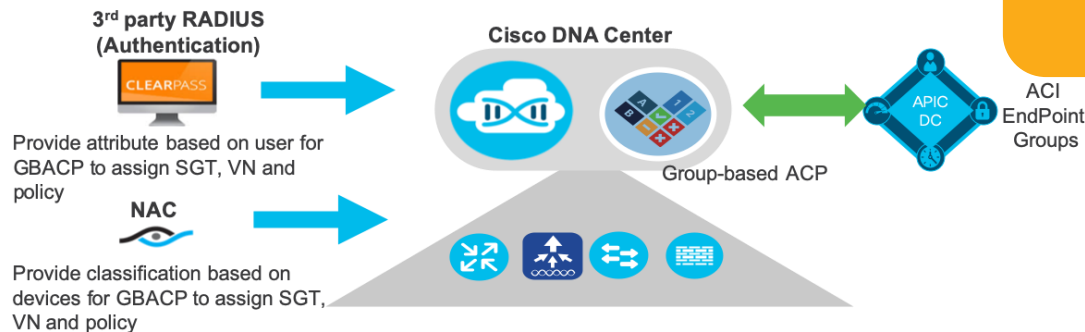
Description (Optional):

Contracts

| Action | Protocol | Port   |        |
|--------|----------|--------|--------|
| permit | udp      | bootpc | Delete |
| permit | udp      | domain | Delete |

# Cisco Catalyst Center Policy

## Group-Based Access Control Policy



Starting Cisco Catalyst Center Release : 1.3.1.0

ISE minimum versions

- ISE 2.4 patch 7
- ISE 2.6 patch 1

- Group-Based Access Control Policy is a component in Cisco Catalyst Center for providing
  - GBAC Policy Authoring in Cisco Catalyst Center
  - Policy data synchronized to ISE
  - ISE provides runtime policy services to network
- Group-Based Access Control Terminology
  - **Scalable Groups\*** (Cisco Catalyst Center) = Security Groups (ISE)
  - Access Contracts (Cisco Catalyst Center) ~ SGACLs (ISE)
  - Policies (Cisco Catalyst Center) = Egress Policies (ISE)

\* - Its Security Groups on Newer Cisco Catalyst Center releases

# Cisco Catalyst Center Policy

## Group-Based Access Control Policy Benefits



### New User Policy Experience

- Scalable Groups directly created/managed in Catalyst Center. ISE TrustSec UI is **READ-ONLY**
- Policy Matrix view (in addition to policy list view)



### Enhanced Policy Definition

- **Default-Deny policy support**
- Access Contract support for ICMP, Filtering on Source Ports and Logging Capabilities
- Policy-Level “Monitor Mode”



### Seamless Integration

- Scalable Groups learned from ACI via ISE



### Third-Party AAA/RADIUS Server support



### Improved Scale

Up to 4000 Scalable Groups  
Up to 500 Access Contracts  
Up to 25,000 Policies

# Cisco Catalyst Center Policy

## Manage Group-Based Access Control policy

☰ Cisco DNA Center

[Overview](#) / [Configurations](#)

Policy Settings

Analytics Settings

### Policy Settings

#### Administration Mode

Manage Group-Based Access Control in

- ☒ Cisco DNA Center, policy UI in Cisco Identity Services Engine will be read-only

For emergent cases, such as Cisco DNA Center not responding, you can override the read-only mode in Cisco Identity Services Engine Security Group settings so that you can make policy changes directly in Cisco Identity Services Engine. Be cautious that this will casue both sides out of sync. A full re-sync might be necessary after recovery.

[Re-sync policy data](#) ▼

- ☐ Cisco Identity Services Engine, Group-Based Access Control UI in Cisco DNA Center will be inactive

### Managing Policy on Cisco Catalyst Center

- Cisco ISE is Read-Only
- Single Matrix support on Cisco ISE
- Default Permit/Deny applicable to all sites
- Single SGACL enforcement per policy

### Managing Policy on Cisco ISE

- No Matrix view on Catalyst Center
- Multi-Matrix support on Cisco ISE
- Per Site Default Permit/Deny available with multi-Matrix
- Multi SGACL enforcement per policy

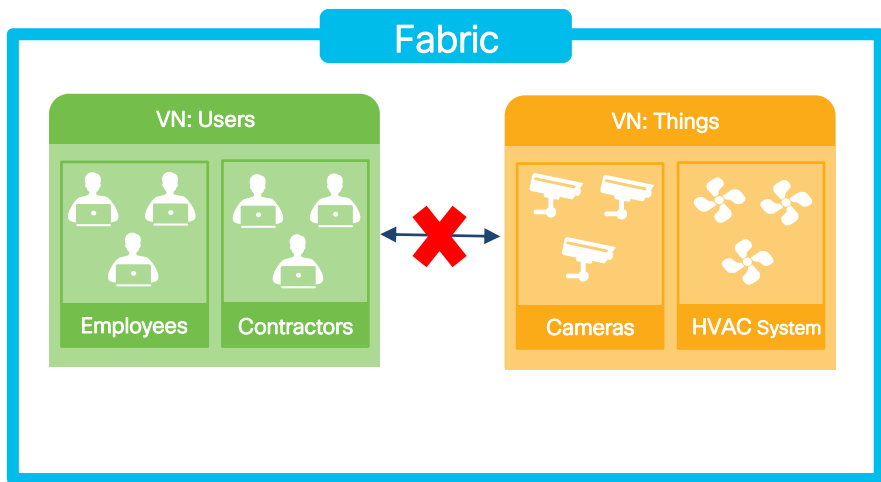
# Fabric Segmentation Strategy



# Cisco SD-Access Segmentation

## Segmentation Strategy

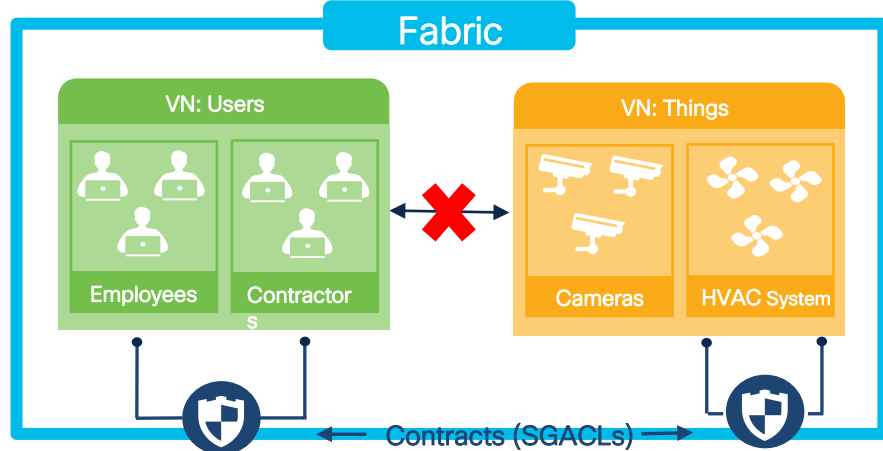
### Macro Segmentation



#### Virtual Network (VN)

- VN = VRF = LISP Instance ID
- Complete Isolation between VN's
- Default Policy: No communication

### Micro Segmentation

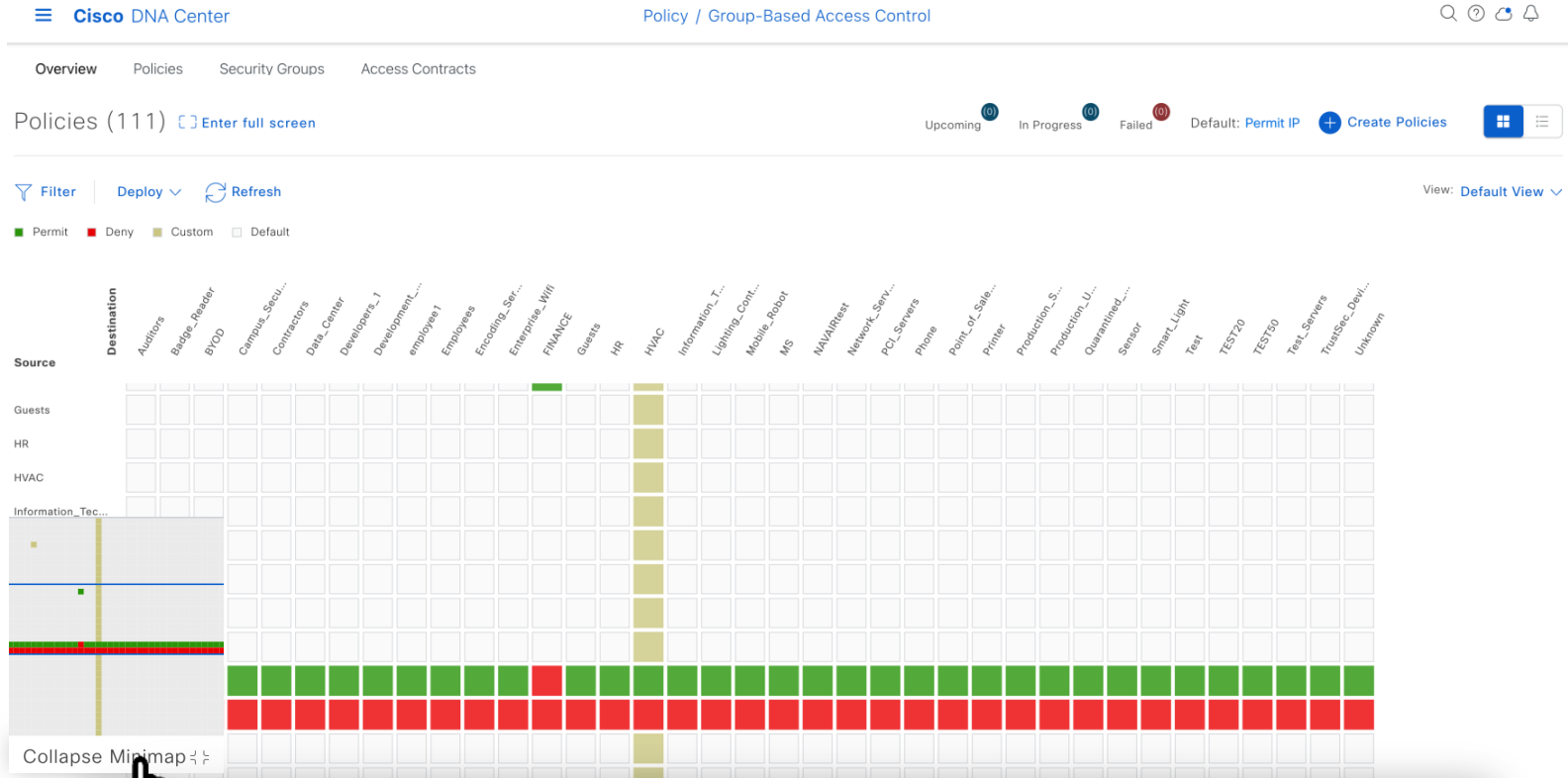


#### Security Group Tag (SGT)

- Location Independent Policy
- Simple Permit/Deny/Contracts
- Default Policy: Permit/Deny

# Cisco Catalyst Center Policy

## Group-Based Access Control Policy



POLICY Landing Page & Matrix View

# Cisco Catalyst Center Policy Scalable Groups

☰ Cisco DNA Center

Policy / Group-Based Access Control



Overview Policies **Security Groups** Access Contracts

Security Groups (37)

Upcoming <sup>30</sup>

🔍 Search Table

0 Selected [Delete](#) [Deploy](#) [Edit](#)

| <input type="checkbox"/> | Name                | Tag Value | Description                        |
|--------------------------|---------------------|-----------|------------------------------------|
| <input type="checkbox"/> | Auditors            | 9/0x9     | Auditor Scalable Group             |
| <input type="checkbox"/> | Badge_Reader        | 30/0x1e   |                                    |
| <input type="checkbox"/> | BYOD                | 15/0xf    | BYOD Security Group                |
| <input type="checkbox"/> | Campus_Security     | 21/0x15   | CS Group                           |
| <input type="checkbox"/> | Contractors         | 5/0x5     | Contractor Security Group          |
| <input type="checkbox"/> | Data_Center         | 27/0x1b   |                                    |
| <input type="checkbox"/> | Developers_1        | 8/0x8     | Developer Scalable Group           |
| <input type="checkbox"/> | Development_Servers | 12/0xc    | Development Servers Security Group |
| <input type="checkbox"/> | employee1           | 28/0x1c   |                                    |
| <input type="checkbox"/> | Employees           | 4/0x4     | Employee Security Group            |

## Create Security Group

Name\*

Tag Value (decimal)\*

37

Description (optional)

☐ Propagate to ACI [?](#)

Cancel

Save Now



# Cisco Catalyst Center Policy Access Contracts

Cisco DNA Center

Policy / Group-Based Access Control



Access Contract

Name\* Description ☐ Modeled Access Contract ⓘ

## CONTRACT CONTENT (1)

| #   | Action *    | Application * | Transport Protocol | Source / Destination | Port | Logging                  | Action |
|-----|-------------|---------------|--------------------|----------------------|------|--------------------------|--------|
| ⋮ 1 | Select... ▼ | Select... ▼   |                    | Destination          |      | <input type="checkbox"/> | + ×    |

Default Action Permit ▼

Logging ☐

Cancel

Save Now



contract

# Cisco Catalyst Center Provision

## Network Device Addition to ISE

### Discover your Network



Scans the devices in network and sends the list of discovered devices to Inventory!

#### • 3 Ways to Discover

- Use Cisco Discovery Protocol (CDP)
- Specify a range of IP addresses
- Use Link Layer Discovery Protocol (LLDP)

#### • Key Considerations

- Discovery Credentials(CLI, SNMP etc.)
- Preferred Management IP Address
- Preferred protocol to connect to device.

#### • 3 Ways to Onboard devices

- Lan Automation
- Plug n Play
- Manual Discovery

### Provision your Network



Onboard devices and deploy the policies across them!

#### Key Aspects

- Add devices to sites
- Deploying the required network settings to devices(**NTP,AAA,Radius,Tacacs,Syslog,SNMP,DNS & Domain**)

#### Config Deployed

Add Device to ISE Network Devices(Default NDG)

#### Config Deployed

NTP , Global AAA, Radius , Tacacs\* , Radius , Syslog, SNMP, DNS,Domain & IP SLA

# Cisco Catalyst Center Host Onboarding Authentication Template(Global)

Cisco DNA Center

Fabric Sites

Find Hierarchy

Global

SITE-A

Building 1

Fabric Sites > SITE-A

## SITE-A

Fabric Infrastructure Host Onboarding More Actions Show Task Status

Authentication Virtual Networks Wireless SSIDs Port Assignment

Select Authentication Template ⓘ

Settings will be applied to all Fabric Edge host ports, unless overridden by a static port assignment.

- ☐ Open Authentication ⓘ Edit
- ☒ Closed Authentication ⓘ Edit
- ☐ Low Impact ⓘ Edit
- ☐ No Authentication ⓘ

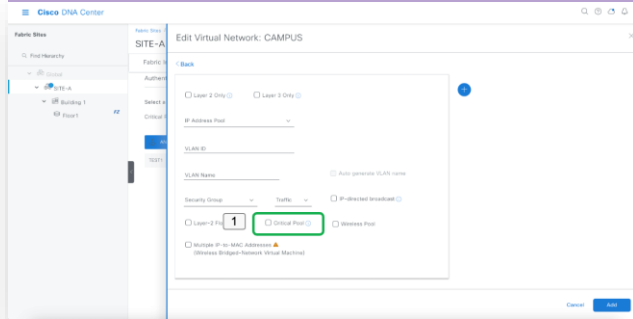
Deploy

Config Deployed

IBNS 2.0(Class-maps, Policy-maps), Service Templates, Interface specific configs

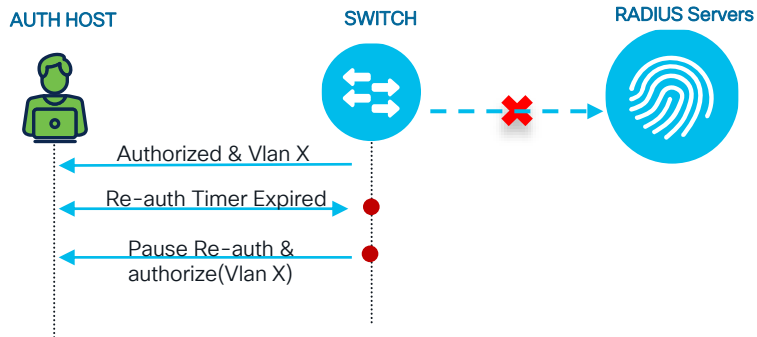
# Cisco DNAC Provision Critical Vlan

Navigate to **PROVISION > Fabric>Created Fabric>Host Onboarding > Virtual Network**

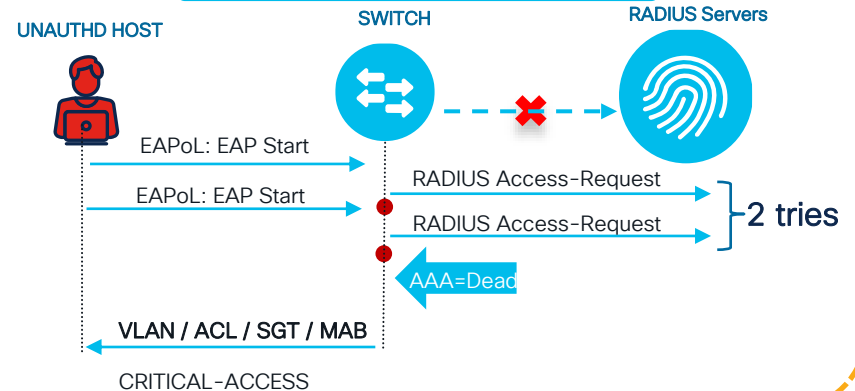


- Feature to locally activate an VLAN/ACL/ SGT/MAB during RADIUS Server outage.
- **Default Critical Vlan** - Data: 2047 & Voice : 2046
- No SVI created unless Critical pool selected
- **Default for all Authentication Templates**
- **Enabled Per Site**
- **Dedicated VN with Limited Network access is recommended**

## AUTHORIZED HOST



## UNAUTHORIZED HOST

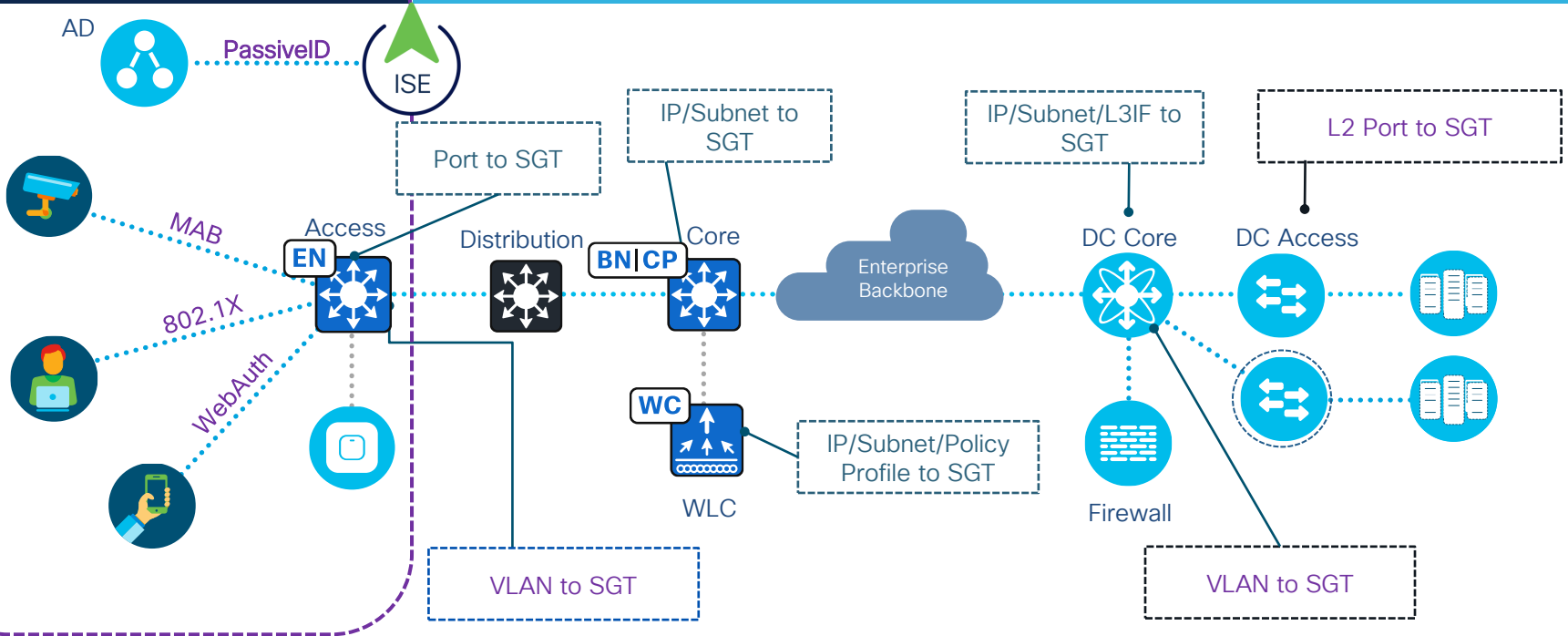


# Security Group Tags(SGT)

## Classification Mechanism

### Dynamic Classification

### Static Classification



# Cisco Catalyst Center Provision

## Associate IP Pool to VN

Cisco DNA Center

DESIGN POLICY **PROVISION** ASSURANCE PLATFORM

Devices ▾ **Fabric** Services

Fabric-Enabled Sites +

Find Hierarchy

- SJC15 LAN Fabric
  - Sacramento
    - SAC01
  - San Diego
    - Site-C
  - San Jose
  - Cisco Way
  - SJC15

SJC15 LAN Fabric

Fabric Infrastructure Host Onboarding

Select Authentication template ⓘ

☐ Closed Authentication ☐ Open Authentication ☐ Easy Connect

Virtual Networks ⓘ Critical Pool: Not Selected

DEFAULT\_VN GUEST\_VN

Wireless SSID's ☐ Enable Wireless Multicast

| SSID Name | Type | Security |
|-----------|------|----------|
|-----------|------|----------|

Edit Virtual Network: SJC15\_VN

< Back

IP

Employees 192\_168\_6\_0- Groups

IPV4: 192.168.6.0/24  
IPV6: None

Traffic

Data ☐ Layer-2 Flooding ☐ Critical Pool

Cancel Update

**Config Deployed**  
Vlan , SVI , Interface Template, LISP

# Cisco Catalyst Center Host Onboarding Authentication Template(Interface Specific)

**Cisco DNA Center** DESIGN POLICY **PROVISION** ASSURANCE PLATFORM

Devices ▾ **Fabric** Services

**Fabric-Enabled Sites**

Find Hierarchy

- ✓ SJC15 LAN Fabric
  - ^ Sacramento
    - SAC01
  - ^ San Diego
  - ✓ San Jose
  - ✓ Cisco Way
  - ^ SJC15

**SJC15 LAN Fabric**

✓ Fabric Infrastructure ✓ **Host Onboarding**

Select Port Assignment **Assign**

Search

- SN-FOC1852Z00E.demo....
- C9300-24U.demo.local
- C3850-24P-2.demo.local**
- C9300-24Pdemo.local

☐ Select All

|                                                          |                                                |                                                |
|----------------------------------------------------------|------------------------------------------------|------------------------------------------------|
| <input checked="" type="checkbox"/> GigabitEthernet1/0/1 | <input type="checkbox"/> GigabitEthernet1/0/2  | <input type="checkbox"/> GigabitEthernet1/0/3  |
| <input type="checkbox"/> GigabitEthernet1/0/5            | <input type="checkbox"/> GigabitEthernet1/0/6  | <input type="checkbox"/> GigabitEthernet1/0/7  |
| <input type="checkbox"/> GigabitEthernet1/0/9            | <input type="checkbox"/> GigabitEthernet1/0/10 | <input type="checkbox"/> GigabitEthernet1/0/11 |

**Port Assignments**

Selected Interfaces (1)

GigabitEthernet1/0/1

Connected Device Type

**User Devices (ip-phone,computer,I...** ▾

Address Pool

Address Pool ▾

Group

Group ▾

Voice Pool

Voice Pool ▾

Authentication Template

**Closed Authentication** ▾

**Config Deployed**

Template: default Access Vlans, IBNS 2.0 Service policy & Dot1x CLI's

Session start = new MAC address learnt on the port

Authenticate dot1x +Do-until-failure: No matter the endpoint is capable of 802.1x or not unconditionally expect for EAPOL Frames

On no response from end-point, terminate 802.1x and attempt MAB auth with priority 20

Activate when port receives EAPOL frame.

### policy-map type control subscriber POLICY-A

event session-started match-all

10 class always do-until-failure

10 authenticate using dot1x priority 10

event authentication-failure match-first

5 class DOT1X\_FAILED do-until-failure

10 terminate dot1x

20 authenticate using mab priority 20

10 class DOT1X\_NO\_RESP do-until-failure

10 terminate dot1x

20 authenticate using mab priority 20

20 class MAB\_FAILED do-until-failure

10 terminate mab

20 authentication-restart 60

30 class always do-until-failure

10 terminate dot1x

20 terminate mab

30 authentication-restart 60

event agent-found match-all

10 class always do-until-failure

10 terminate mab

20 authenticate using dot1x priority 10

- 10 : Class Sequence number
- always: Execute action unconditionally
- do-until-failure: Execute action sequentially until failure

An Authentication Failure event, Exit on first match and activate respective action.

If dot1x failed, execute below actions sequentially until failure.  
Terminate dot1x & attempt MAB auth with priority 20.

If MAB failed, execute below actions sequentially until failure.  
Terminate MAB & wait for 60 secs to retry authentication

Similar to **authentication priority dot1x mab** command, if EAP frames received after MAB, then stop MAB and do 802.1x

# Cisco Catalyst Center Provision

## IBNS 2.0 Related Configuration

### Service Templates

```
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
sgt 3999
vlan 2047
service-template DefaultCriticalVoice_SRV_TEMPLATE
voice vlan
service-template DefaultCriticalAccess_SRV_TEMPLATE
access-group IPV4_CRITICAL_AUTH_ACL
access-group IPV6_CRITICAL_AUTH_ACL
```

### Interface Templates

```
template ApAutzTemplate
template DefaultWiredDot1xClosedAuth
template DefaultWiredDot1xLowImpactAuth
template DefaultWiredDot1xOpenAuth
template SWITCH_INTERFACE_TEMPLATE
```

### Policy-Map

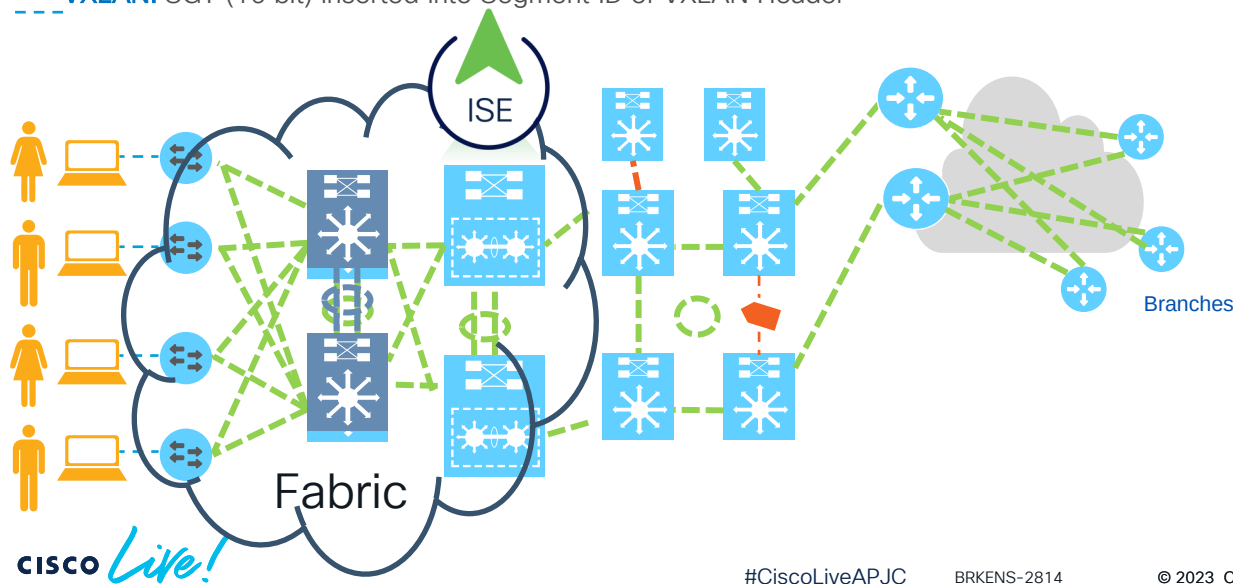
```
policy-map type control subscriber PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
policy-map type control subscriber PMAP_DefaultWiredDot1xClosedAuth_MAB_1X
policy-map type control subscriber PMAP_DefaultWiredDot1xLowImpactAuth_1X_MAB
policy-map type control subscriber PMAP_DefaultWiredDot1xLowImpactAuth_MAB_1X
policy-map type control subscriber PMAP_DefaultWiredDot1xOpenAuth_1X_MAB
policy-map type control subscriber PMAP_DefaultWiredDot1xOpenAuth_MAB_1X
```

# Scalable Group Tags(SGT)

## Propagation Mechanism

### Inline Tagging Methods

- **Ethernet Inline Tagging:** (EtherType:0x8909) 16-Bit SGT encapsulated within Cisco Meta Data (CMD) payload.
- **IPSec / L3 Crypto:** Cisco Meta Data (CMD) uses protocol 99, and is inserted to the beginning of the ESP/AH payload.
- **LISP:** SGT (16 bit) insertion in the Nonce field (24 bit)
- **VXLAN:** SGT (16 bit) inserted into Segment ID of VXLAN Header



### Propagation options

- Cisco MetaData (CMD)
- Ethernet
- MACsec
- IPsec
- DM-VPN
- GET-VPN
- **VXLAN**

### Supporting devices

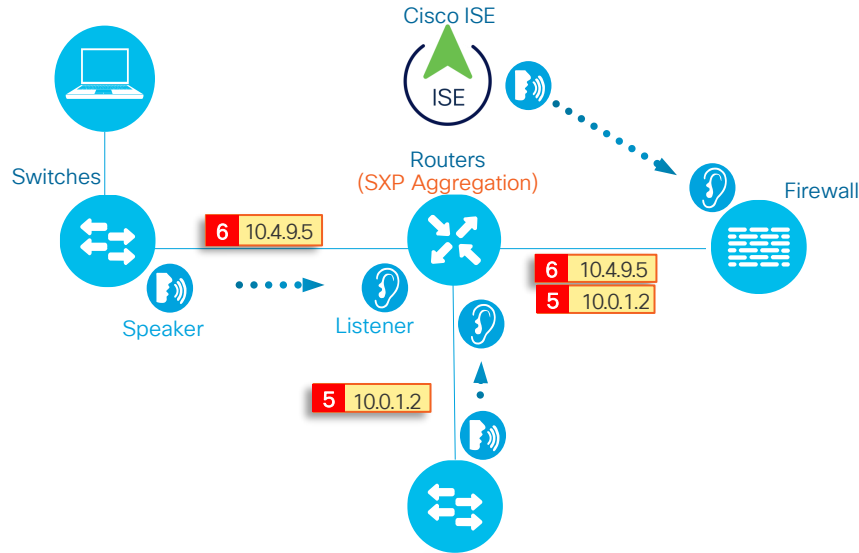
- Catalyst switches
- WLAN controllers
- Nexus switches
- Integrated Service Routers
- Industrial Ethernet Switches
- ASR 1000
- ASA 5500-x
- Firepower Threat Defense

# Scalable Group Tags(SGT)

## Propagation Mechanism

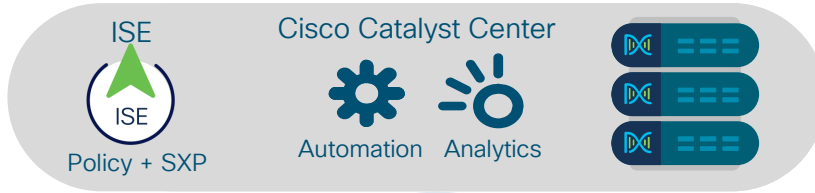
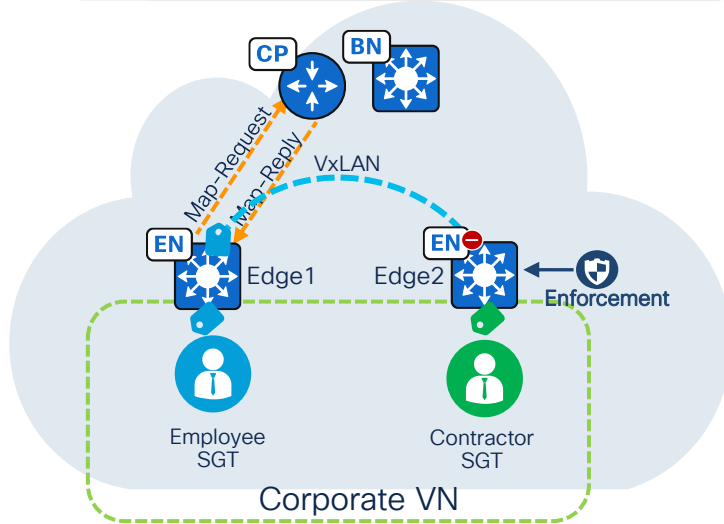
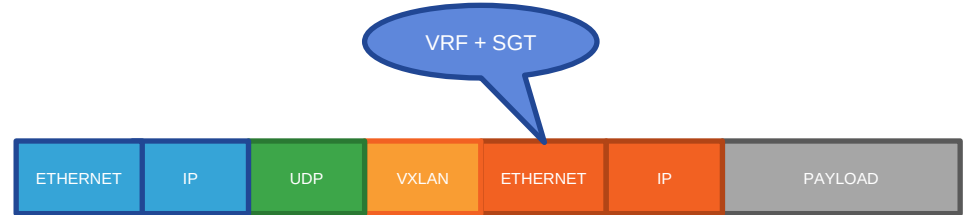
### SGT Exchange Protocol (SXP)

- **IP-to-SGT** binding exchange over 64999/TCP
- **Cisco ISE** can be a SXP speaker / Listener



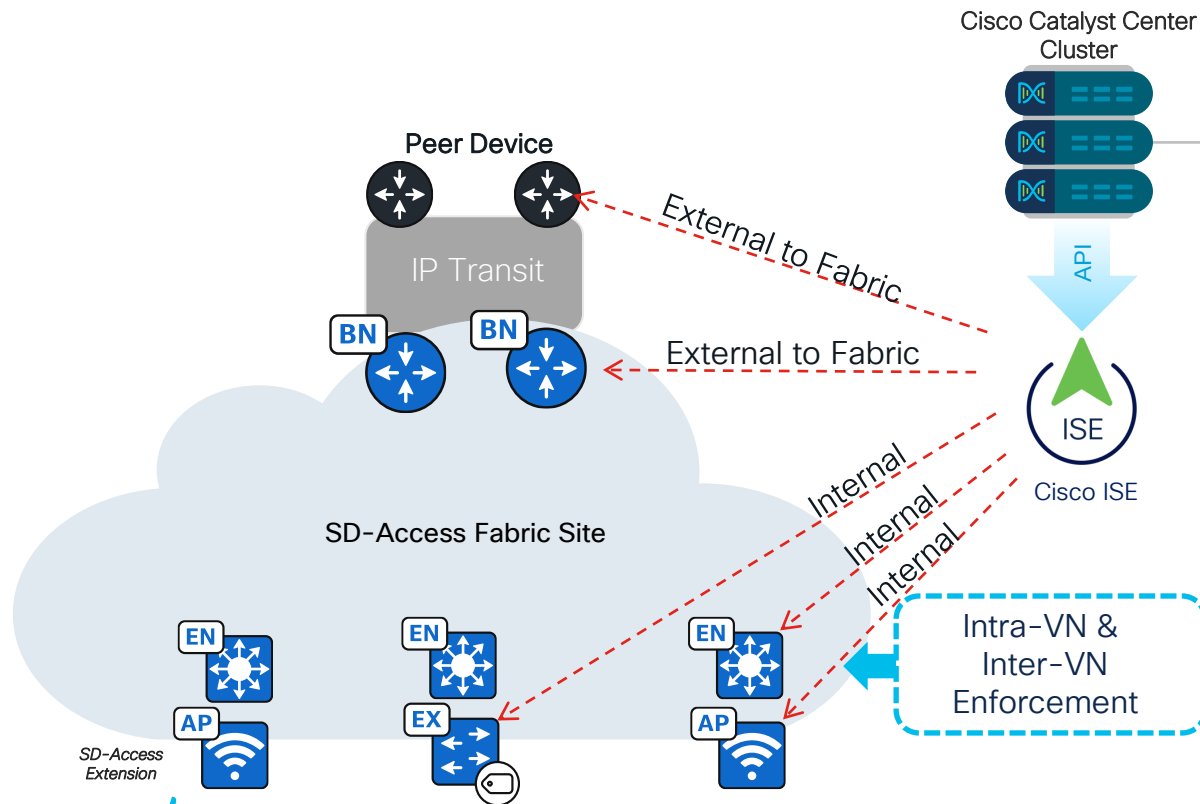
# Single Site Architecture

## Segmentation within a Fabric Site

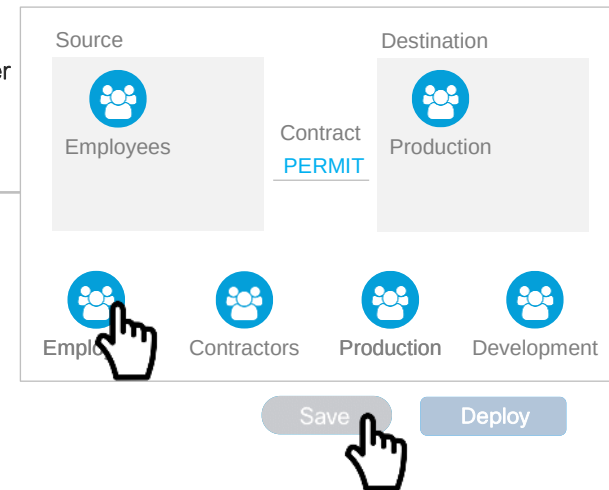


# Cisco Catalyst Center Policy

## Access Contracts Enforcement



### FABRIC POLICIES

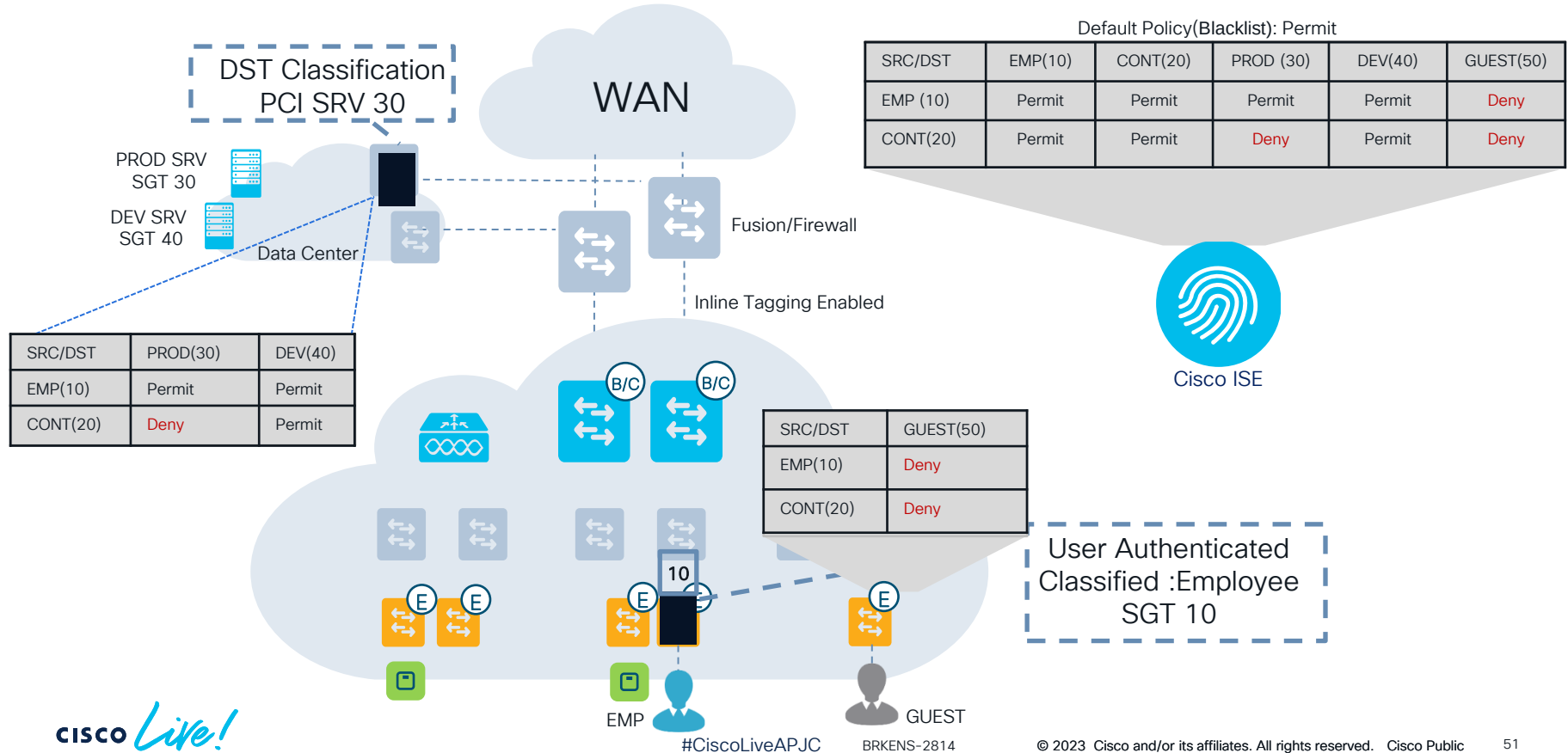


### Enforcement Scale

- DNA Cluster supports 64-256 VNs/Site, 4000 SGTs
- 255 unique SGTs can be enforced locally on C3850/C9k
- Access/Edge nodes usually won't have that scale of 255+
- If enforcing on Border Nodes then consider numbers of DC/cloud-related SGTs which might increase the SGT counts

# Cisco SGT

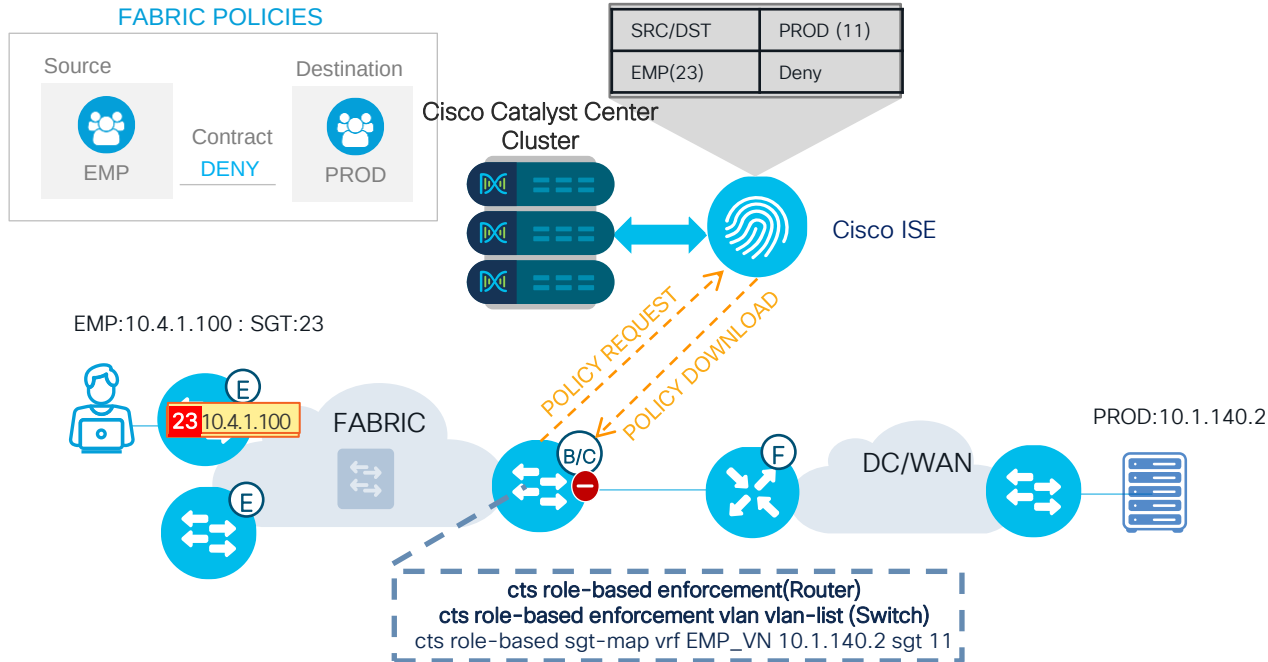
## SGT Tagging & SGACL Download



# Cisco Catalyst Center Policy

## Access Contracts Enforcement on Border

### 1. Statically/Manually adding policy on Border via CLI



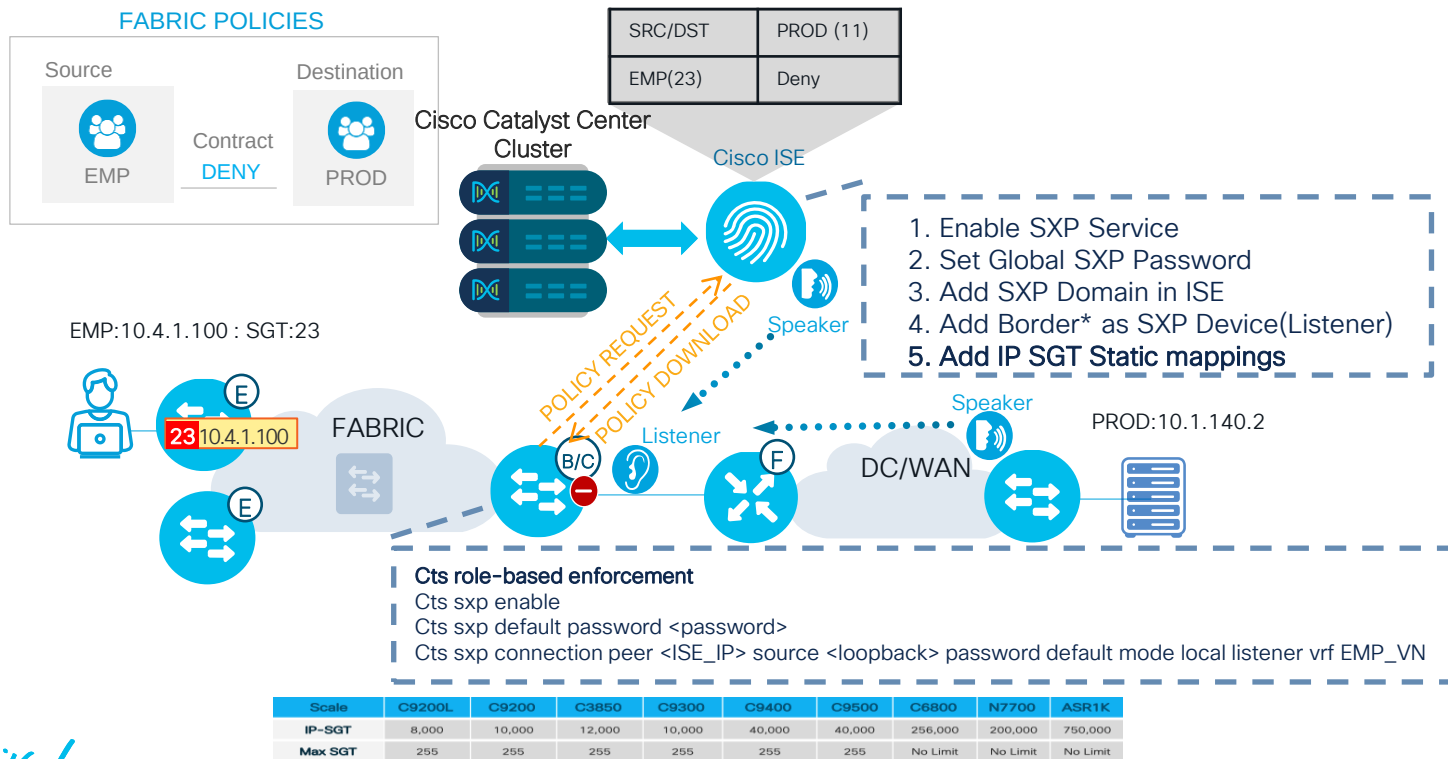
User able to Ping PROD Server  
Add Server Mapping statically on the Border using CLI

# Cisco Catalyst Center Policy

## Access Contracts Enforcement on Border

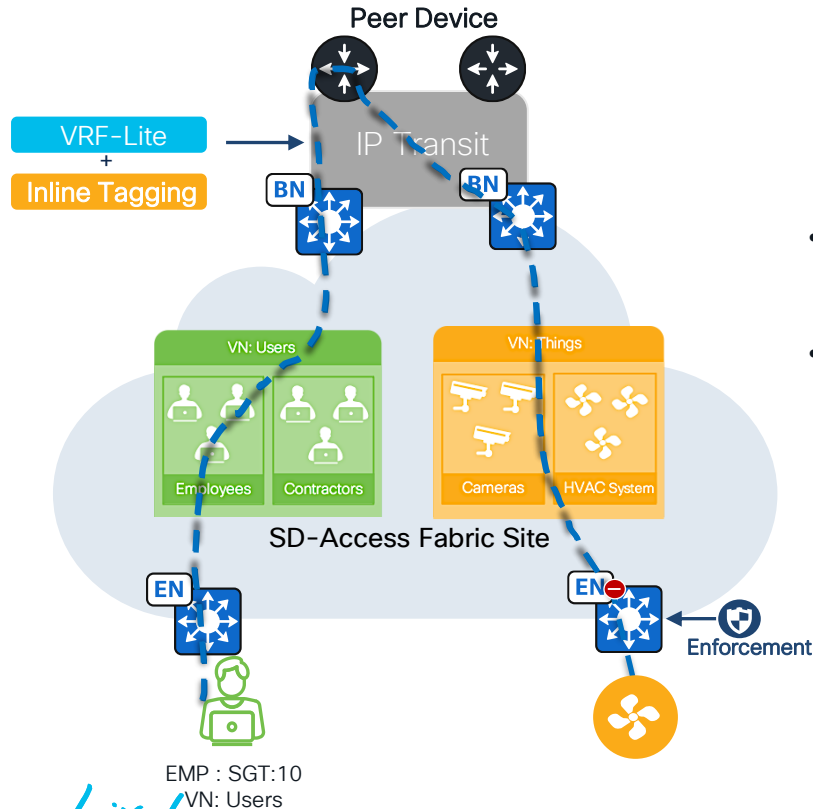
### 2. IP-SGT bindings via SXP(Cisco ISE)

### 3. IP-SGT bindings via SXP(N/W Device)



# Cisco Catalyst Center Policy

## VN-2-VN Policy Enforcement



- By default, Endpoint context(VRF+SGT) information is not carried across the IP Transit network.
- Additional configuration like VRF-Lite across dot1q trunk or Sub-interface + SGT inline tagging are required to carry endpoint context information

# Cisco Catalyst Center Policy

## Default Permit vs Default Deny Model

### Default Permit Model

|                                                                                                  |  | Destination                                                                       |                                                                                   |                                                                                   |                                                                                   |                                                                                   |
|--------------------------------------------------------------------------------------------------|--|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Source                                                                                           |  | Production_User                                                                   | Production_Srvr                                                                   | Development_User                                                                  | Development_Srvr                                                                  | Unknown                                                                           |
|  Production_User  |  |                                                                                   |  |  |  |  |
|  Production_Srvr  |  |  |                                                                                   |  |  |  |
|  Development_User |  |  |  |                                                                                   |  |  |
|  Development_Srvr |  |  |  |  |                                                                                   |                                                                                   |
|  Unknown          |  |  |  |  |                                                                                   |                                                                                   |

Default\_Policy: 

### Default Deny Model

|                                                                                                    |  | Destination                                                                        |                                                                                     |                                                                                     |                                                                                     |                                                                                     |
|----------------------------------------------------------------------------------------------------|--|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Source                                                                                             |  | Production_User                                                                    | Production_Srvr                                                                     | Development_User                                                                    | Development_Srvr                                                                    | Unknown                                                                             |
|  Production_User  |  |  |                                                                                     |                                                                                     |                                                                                     |                                                                                     |
|  Production_Srvr  |  |                                                                                    |  |                                                                                     |                                                                                     |                                                                                     |
|  Development_User |  |                                                                                    |                                                                                     |  |                                                                                     |                                                                                     |
|  Development_Srvr |  |                                                                                    |                                                                                     |                                                                                     |  |  |
|  Unknown          |  |                                                                                    |                                                                                     |                                                                                     |  |  |

Default\_Policy: 

|                                                                                                      |  | Destination                                                                         |                                                                                     |                                                                                     |                                                                                     |                                                                                     |
|------------------------------------------------------------------------------------------------------|--|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Source                                                                                               |  | Production_User                                                                     | Production_Srvr                                                                     | Development_User                                                                    | Development_Srvr                                                                    | Unknown                                                                             |
|  Production_User  |  |                                                                                     |                                                                                     |                                                                                     |                                                                                     |  |
|  Production_Srvr  |  |                                                                                     |                                                                                     |                                                                                     |                                                                                     |  |
|  Development_User |  |                                                                                     |                                                                                     |                                                                                     |                                                                                     |  |
|  Development_Srvr |  |                                                                                     |                                                                                     |                                                                                     |                                                                                     |  |
|  Unknown          |  |  |  |  |  |  |

Default\_Policy: 

From TrustSec\_Devices SGT 2 -> TrustSec\_Devices SGT 2, permit ip  
 From TrustSec\_Devices SGT 2 -> Unknown SGT 0, permit ip  
 From Unknown SGT 0 -> TrustSec\_Devices SGT 2, permit ip

Initial Brownfield Deployment

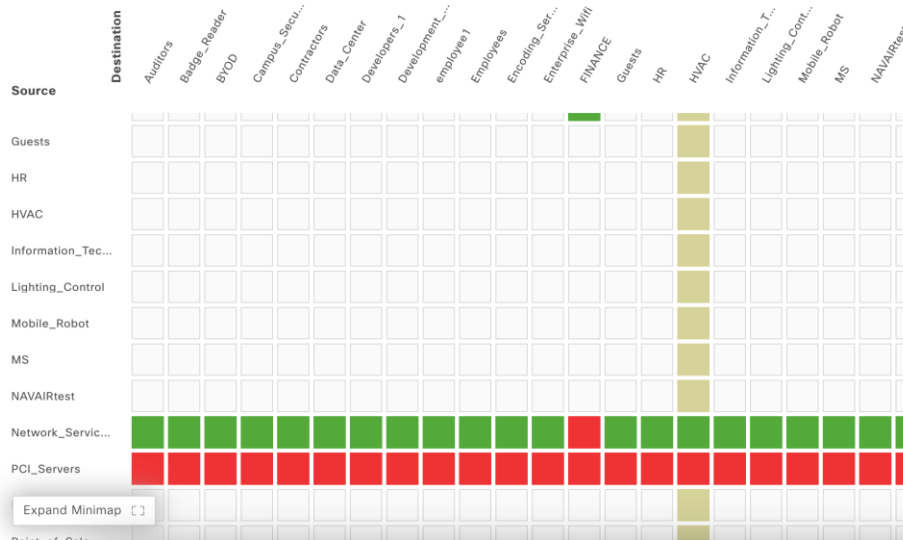
# Cisco Catalyst Center Policy

## Whitelist vs Blacklist Model

Policies (111) [Enter full screen](#)

[Filter](#) | [Deploy](#) [Refresh](#)

■ Permit ■ Deny ■ Custom ■ Default



Upcoming [In Progress](#) [Failed](#) [Default: Permit IP](#) [Create Policies](#)

Default Policy

Action

Permit IP

Deny IP

Deny\_IP\_Log

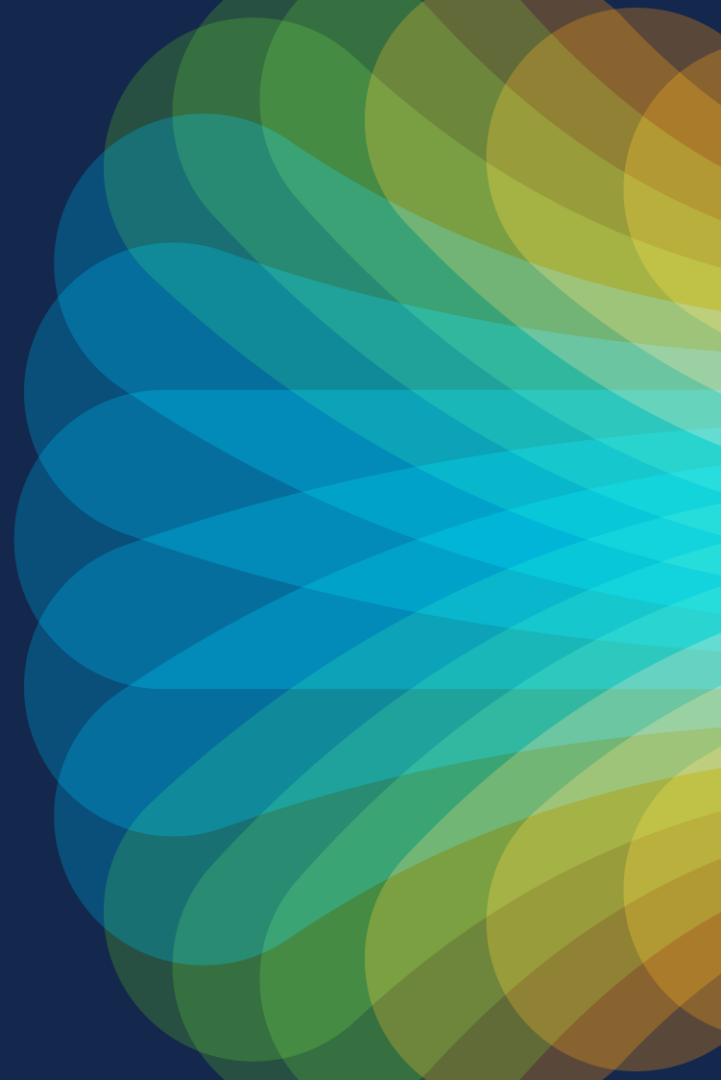
Permit IP

Permit\_IP\_Log

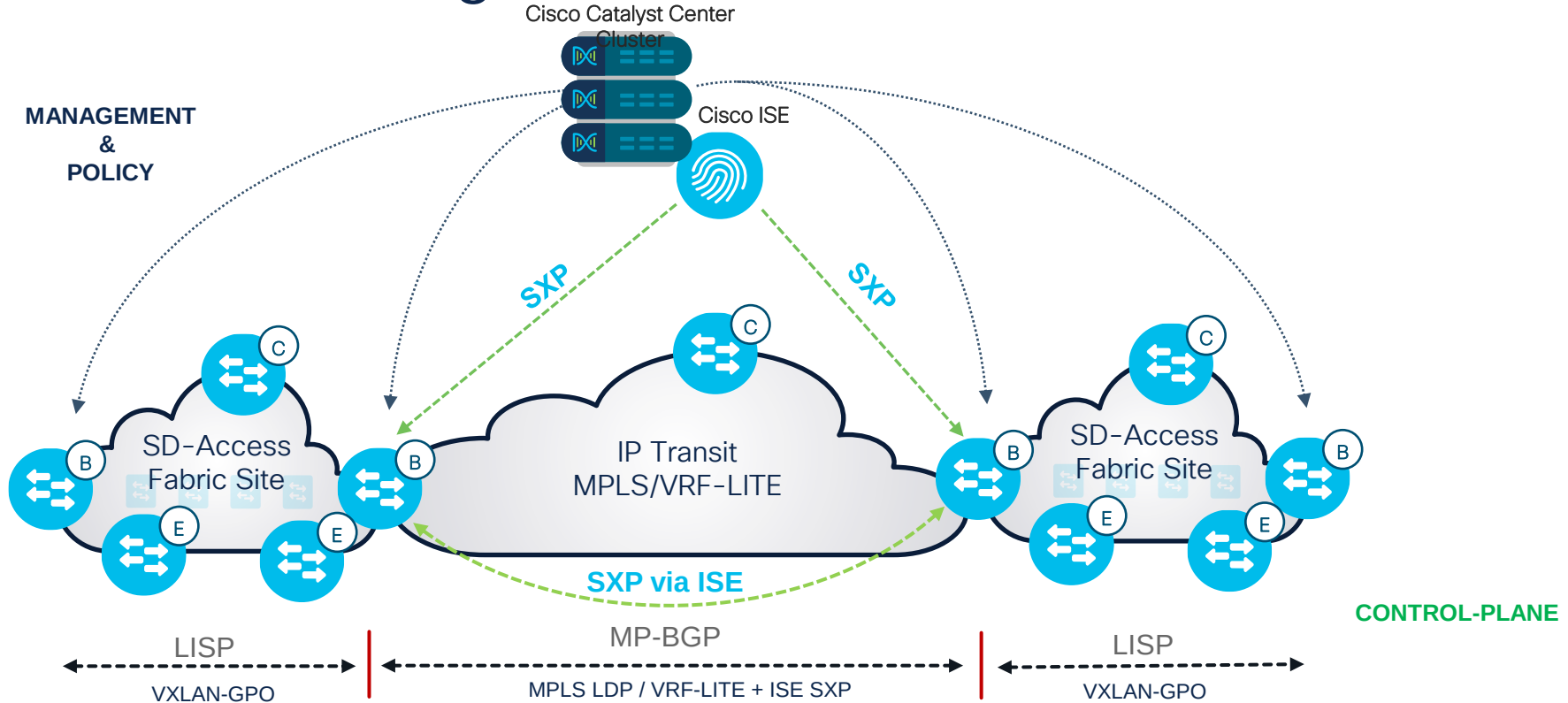
Cancel

Save Now

# Design & Integration

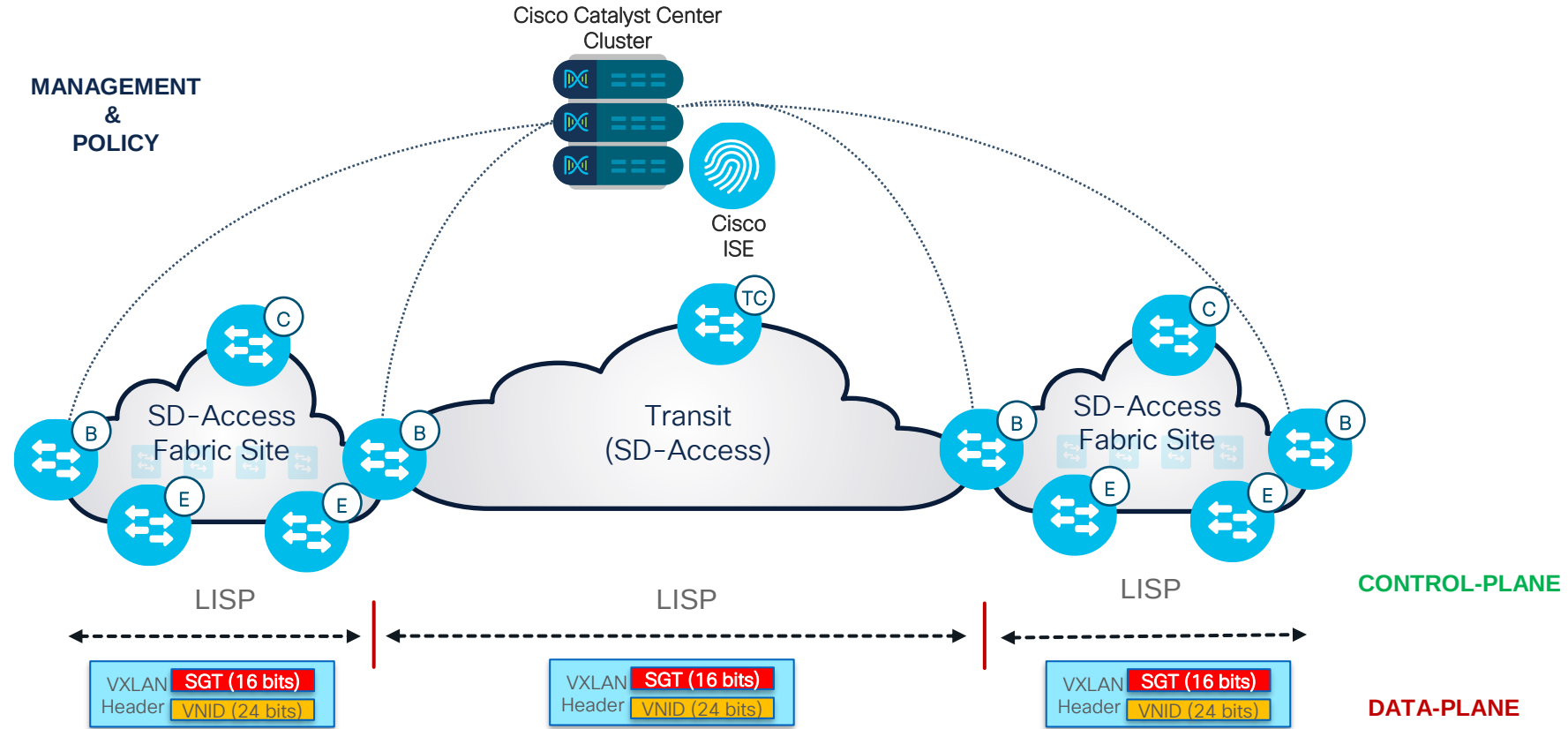


# Multi-Site Design with IP Transit



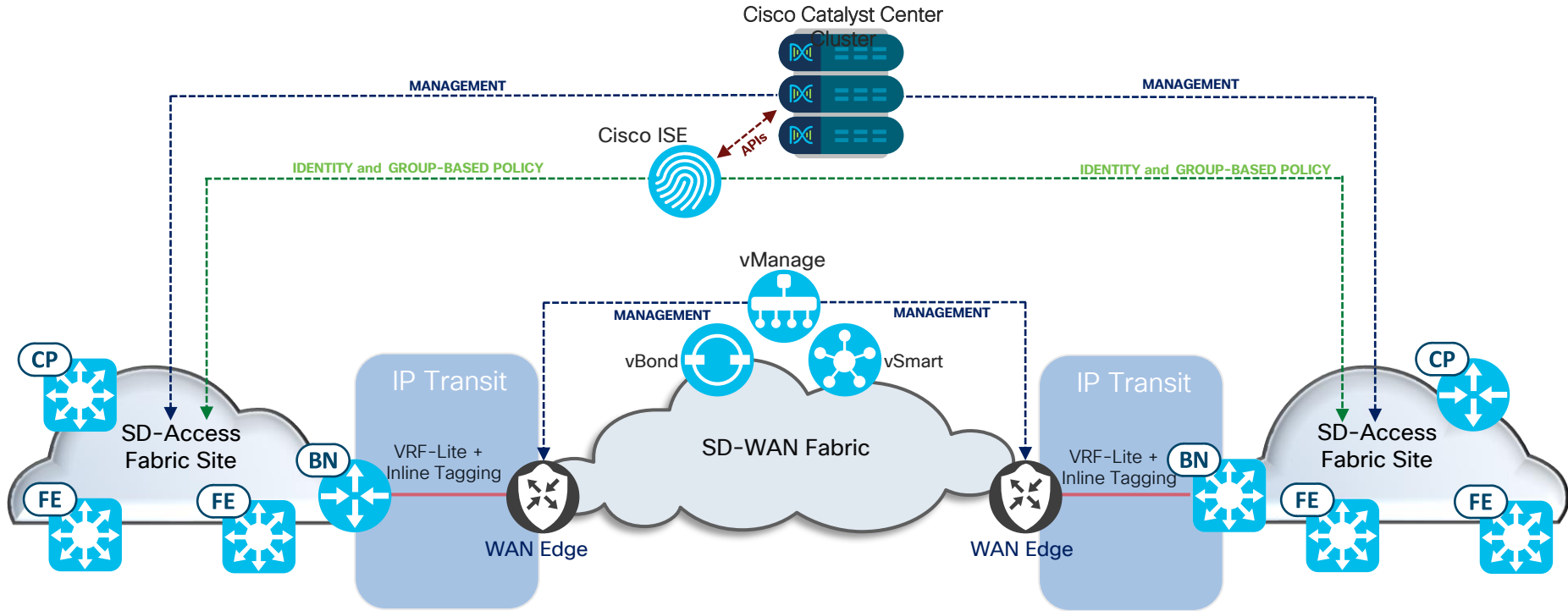
# Multi-Site Design with SD-Access Transit

## End to End Segmentation Maintained



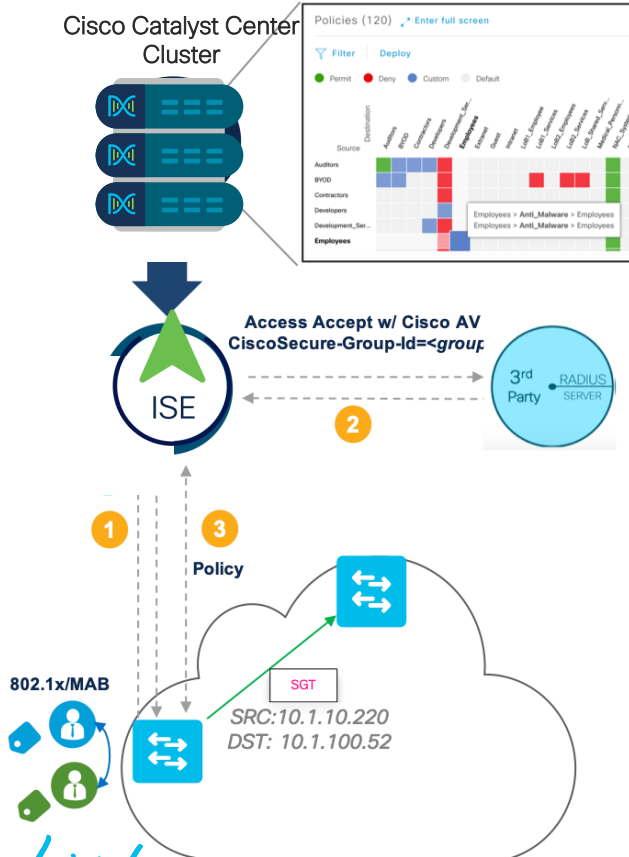
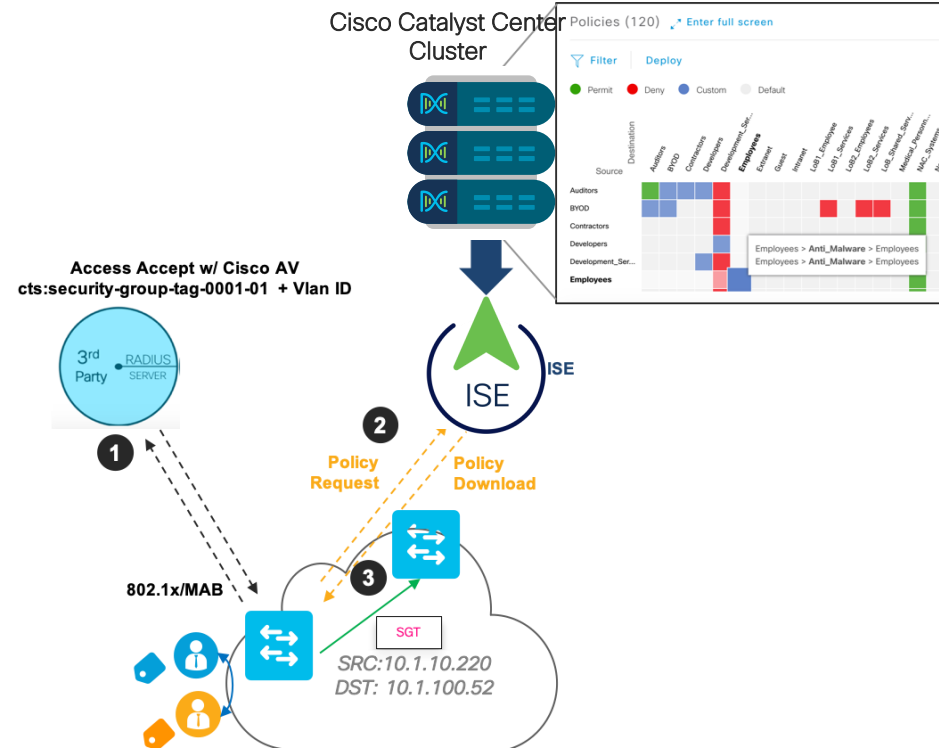
# Multi-Site Design with SD-WAN Transport

## Independent Domains



# Cisco Catalyst Center Policy

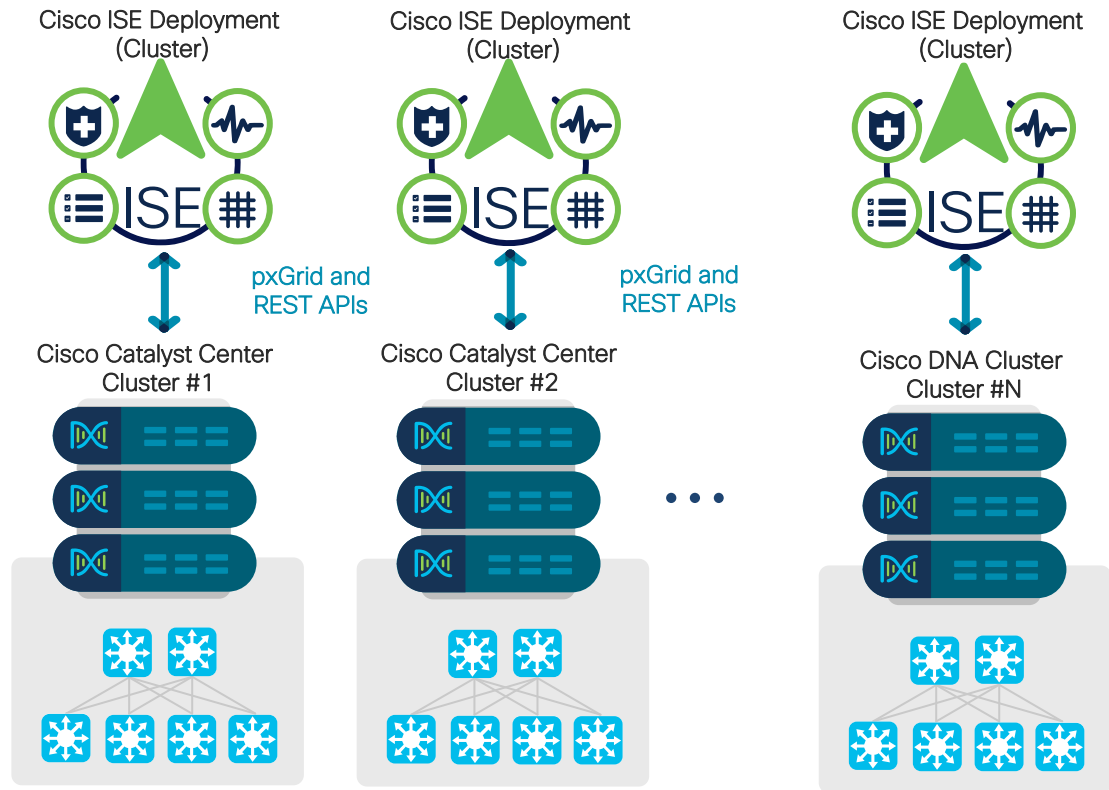
## Third-Party AAA/RADIUS Server support



# Multiple Cisco Catalyst Center

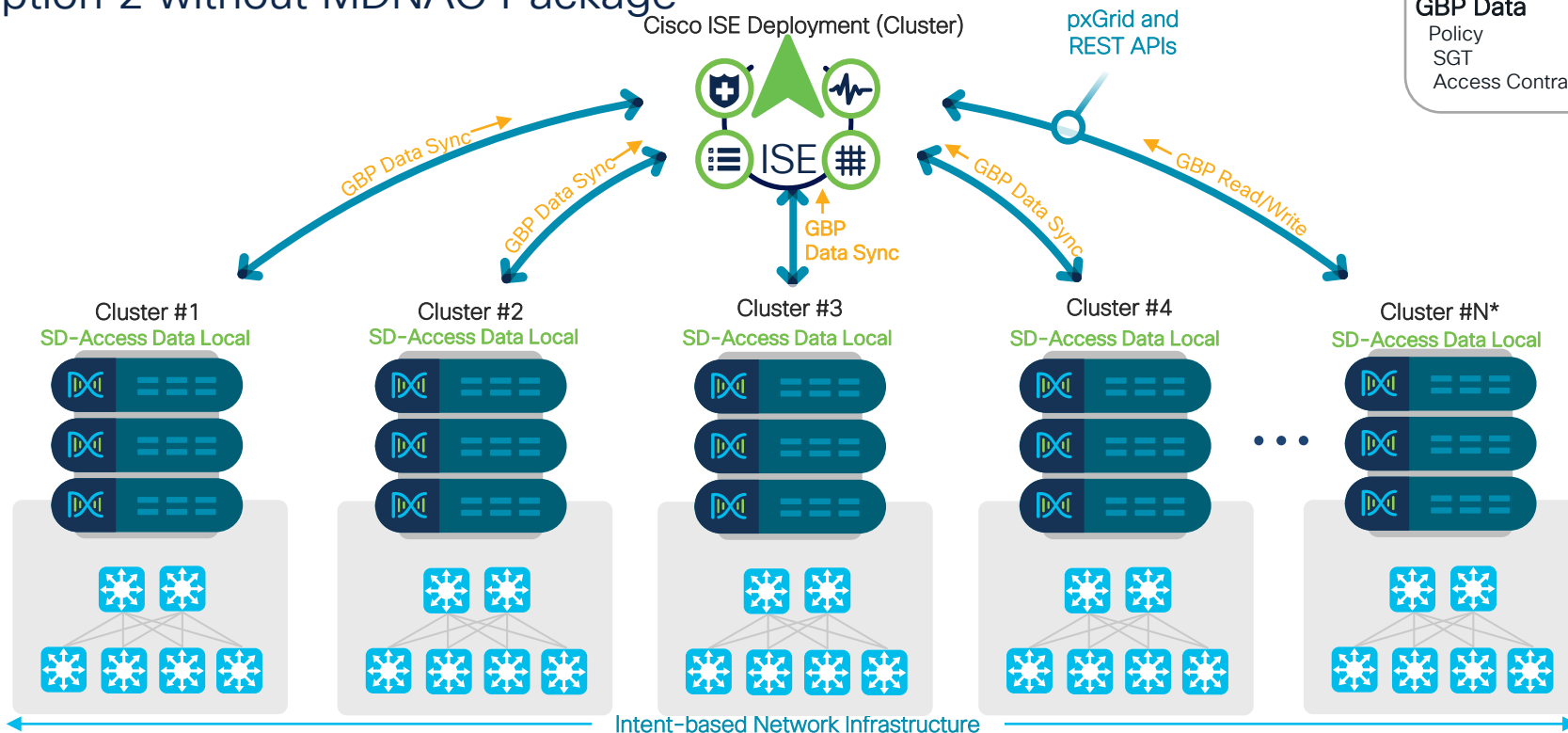
# Integrating Cisco Catalyst Center with ISE

## Option 1



## Option 2 without MDNAC Package

**GBP Data**  
Policy  
SGT  
Access Contract



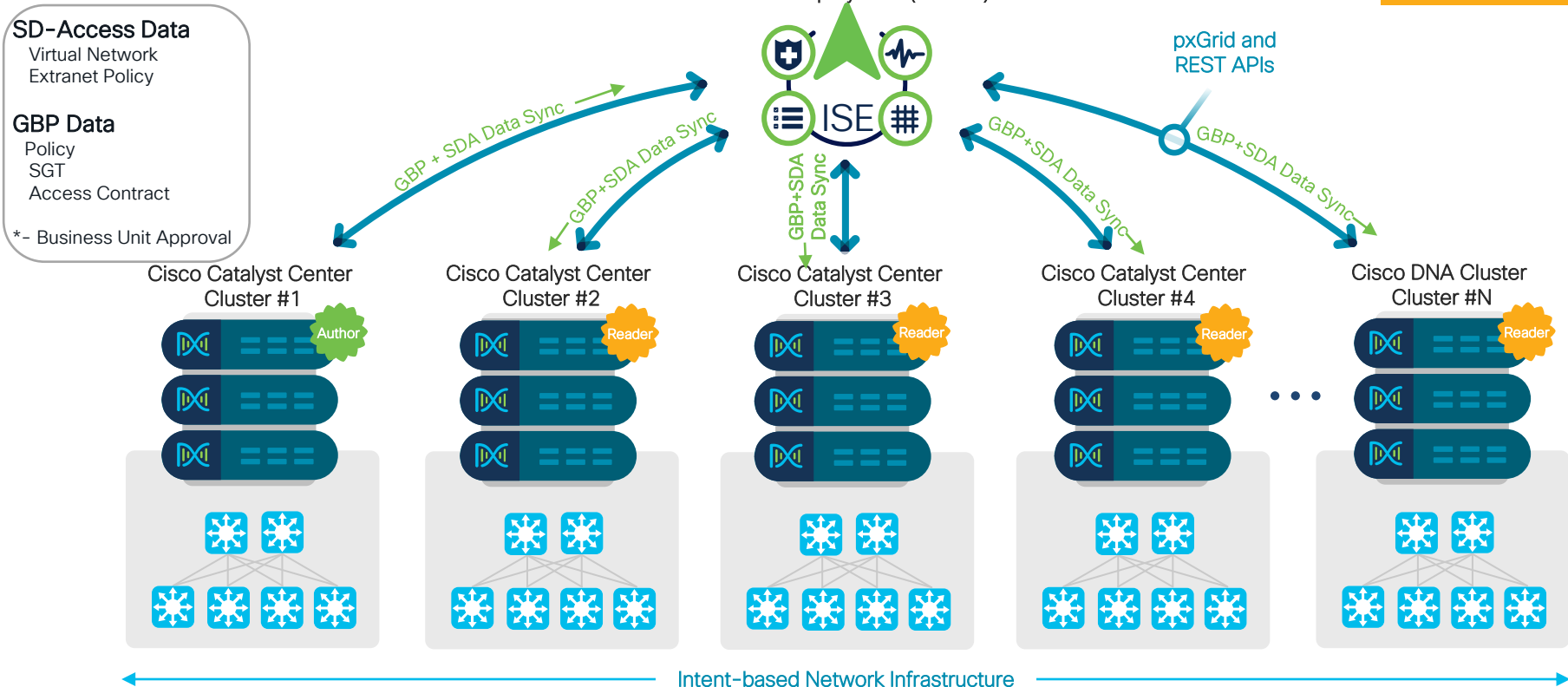
# Integrating Cisco Catalyst Center with ISE

## Option 3- Multiple Cisco Catalyst Center Solution Overview\*

Starting Catalyst Center  
release : 2.2.3.x  
N=5

Limited Availability(LA)  
Feature

Cisco ISE Deployment (Cluster)



# Multiple Cisco Catalyst Center to Single ISE

## Why Multiple Cisco Catalyst Center?

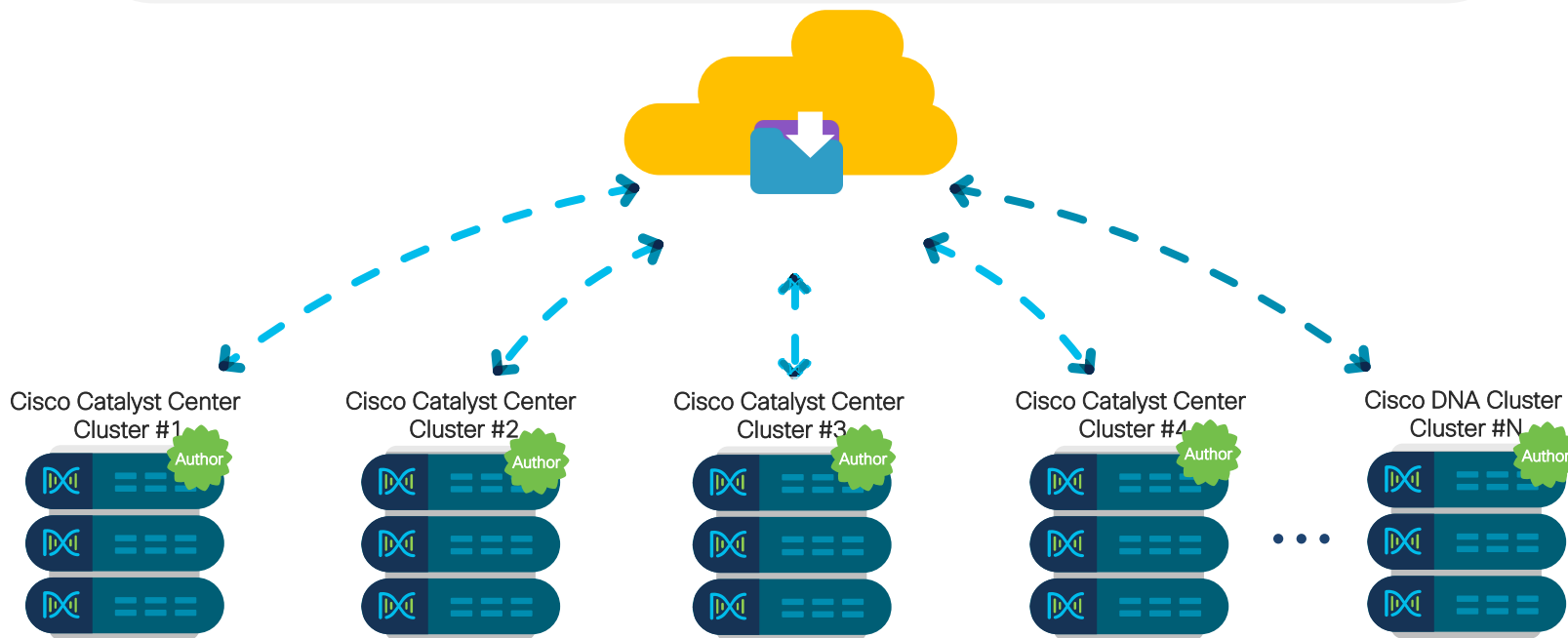
- Globally consistent Group-based Access Control Policy
- Central management of Virtual Network, Scalable Groups, Policies, Access Contracts.
- Shared SD-Access Transit across Multiple Cisco Catalyst Center Clusters
- LISP Extranet Policy or VN Policy for Multisite Fabric with SD-Access Transit

# Multiple Cisco Catalyst Center

## Multiple Cisco Catalyst Center Package and Installation

Connect with your Cisco Sales Representative or Channel Partner for:

- High-Level Design review
- Multiple Cisco Catalyst Center Package release



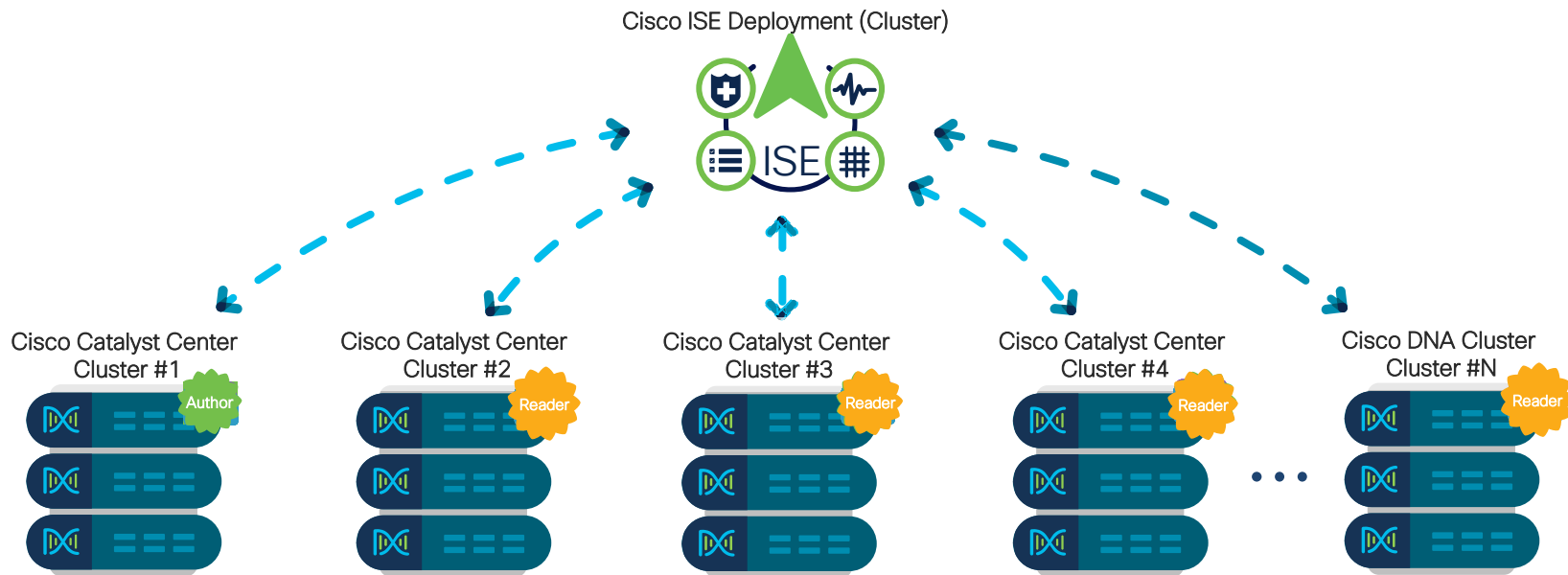
# Multiple Cisco Catalyst Center

## Multiple Cisco Catalyst Center Enhancements(Package part of ISO)

Starting  
Catalyst Center : 2.3.6.x  
Cisco ISE. : >3.2  
Max Cluster : 5

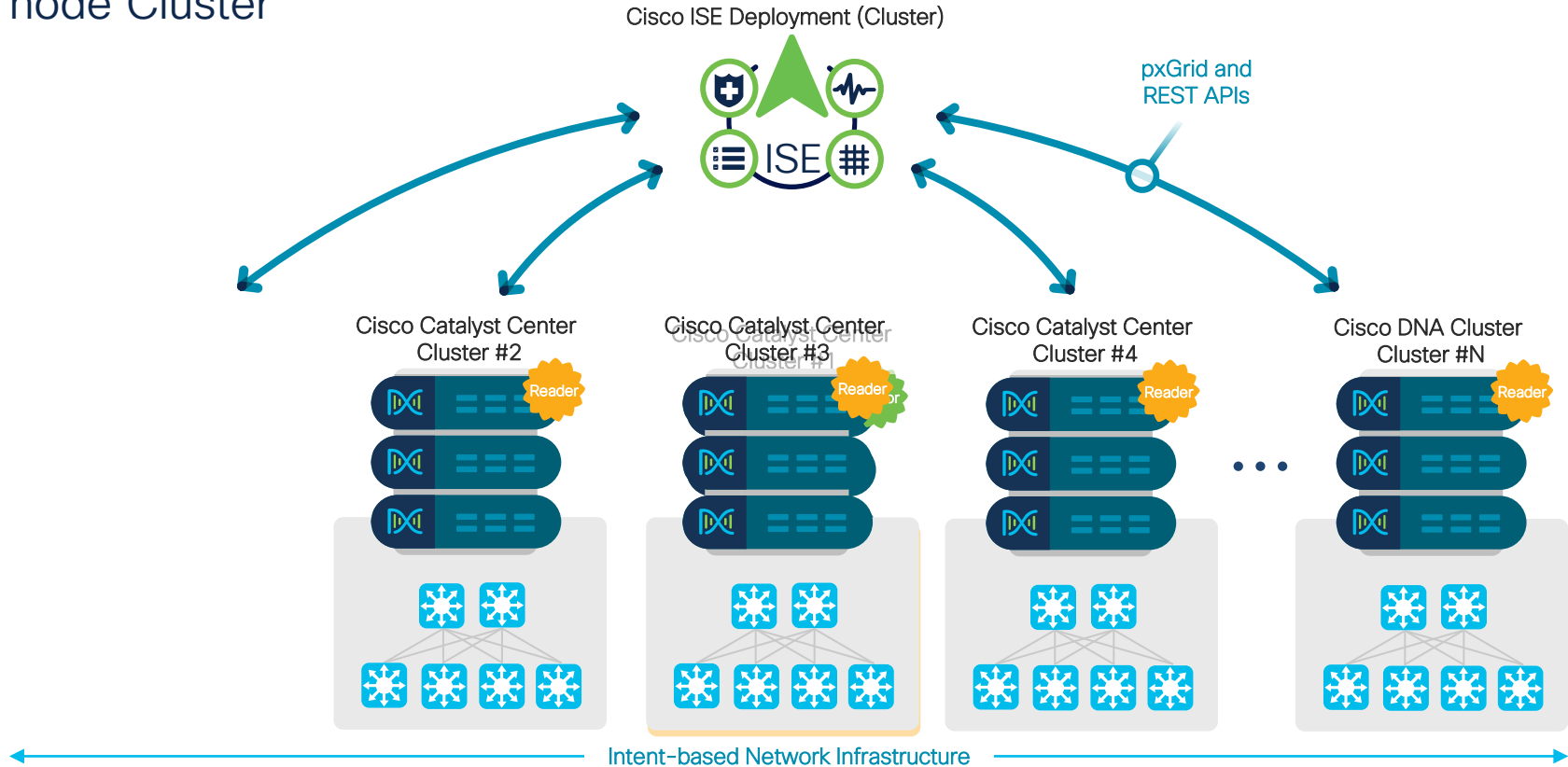
Connect with your Cisco Sales Representative or Channel Partner for:

- High-Level Design review



# Multiple Cisco Catalyst Center

Integrating other Cisco Catalyst Center Clusters with Cisco ISE as Reader node Cluster



# Multiple Cisco Catalyst Center Author Node Cluster

Cisco ISE Deployment (Cluster)

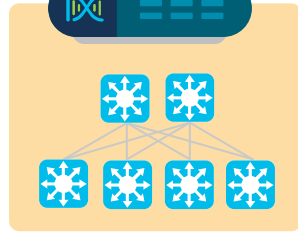


pxGrid and  
REST APIs

Cisco Catalyst Center  
Cluster



- 1<sup>st</sup> Cisco DNA Cluster to integrate/reintegrate with Cisco ISE
- Only ONE cluster can be designated as Author Node
- Manages VN, SGTs, Access Contracts, GBAC Policy and VN-SGT Associations
- Creation, modification or deletion of policy components performed on Author
- Can be a **Greenfield or Brownfield** Cisco Catalyst Center Cluster



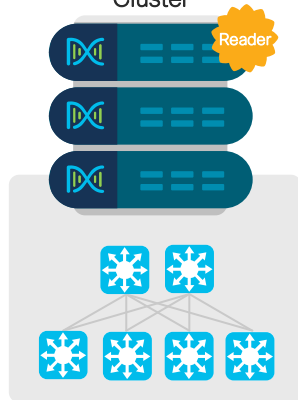
Intent-based Network Infrastructure

# Multiple Cisco Catalyst Center Reader Node Cluster

Cisco ISE Deployment (Cluster)



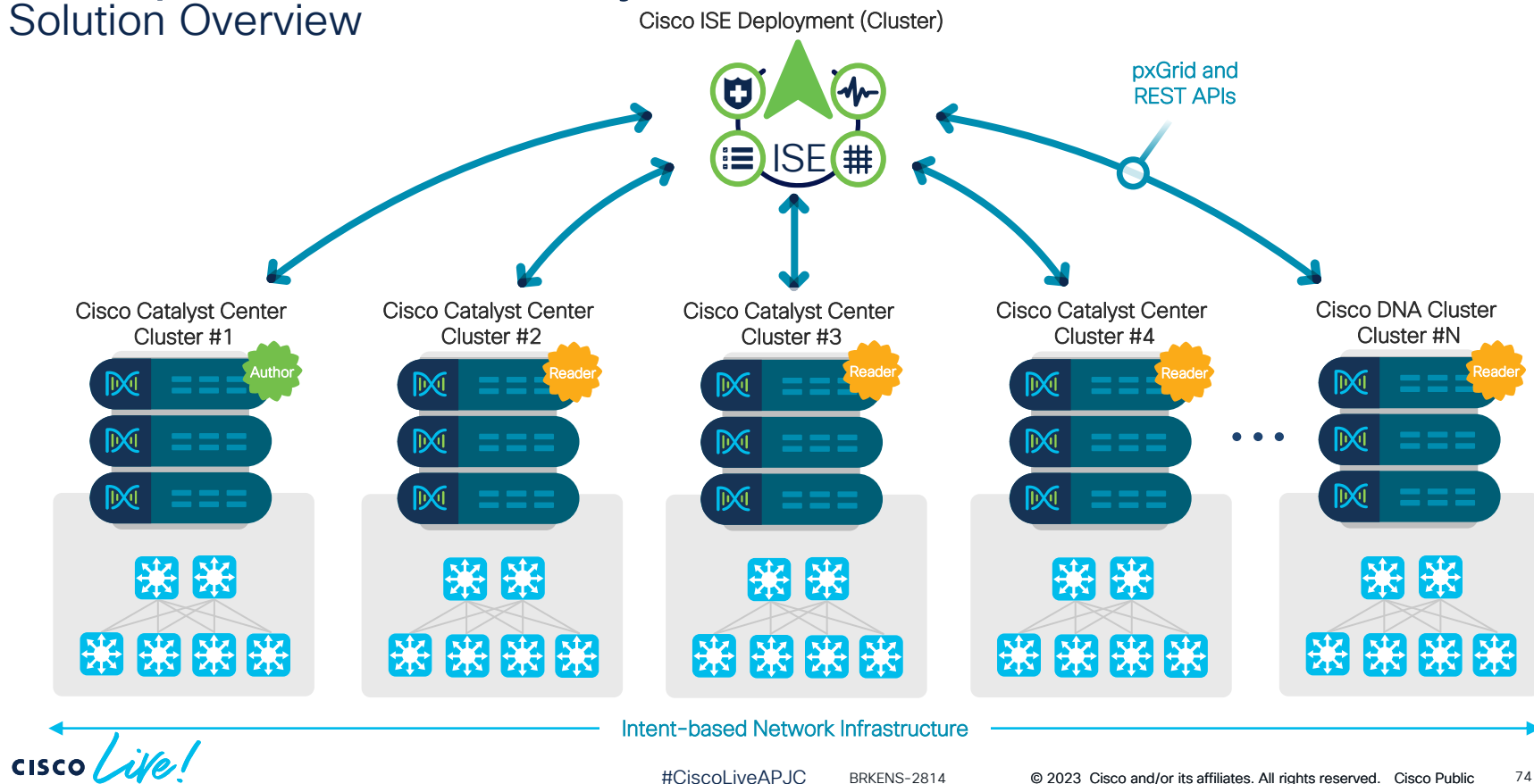
Cisco Catalyst Center  
Cluster



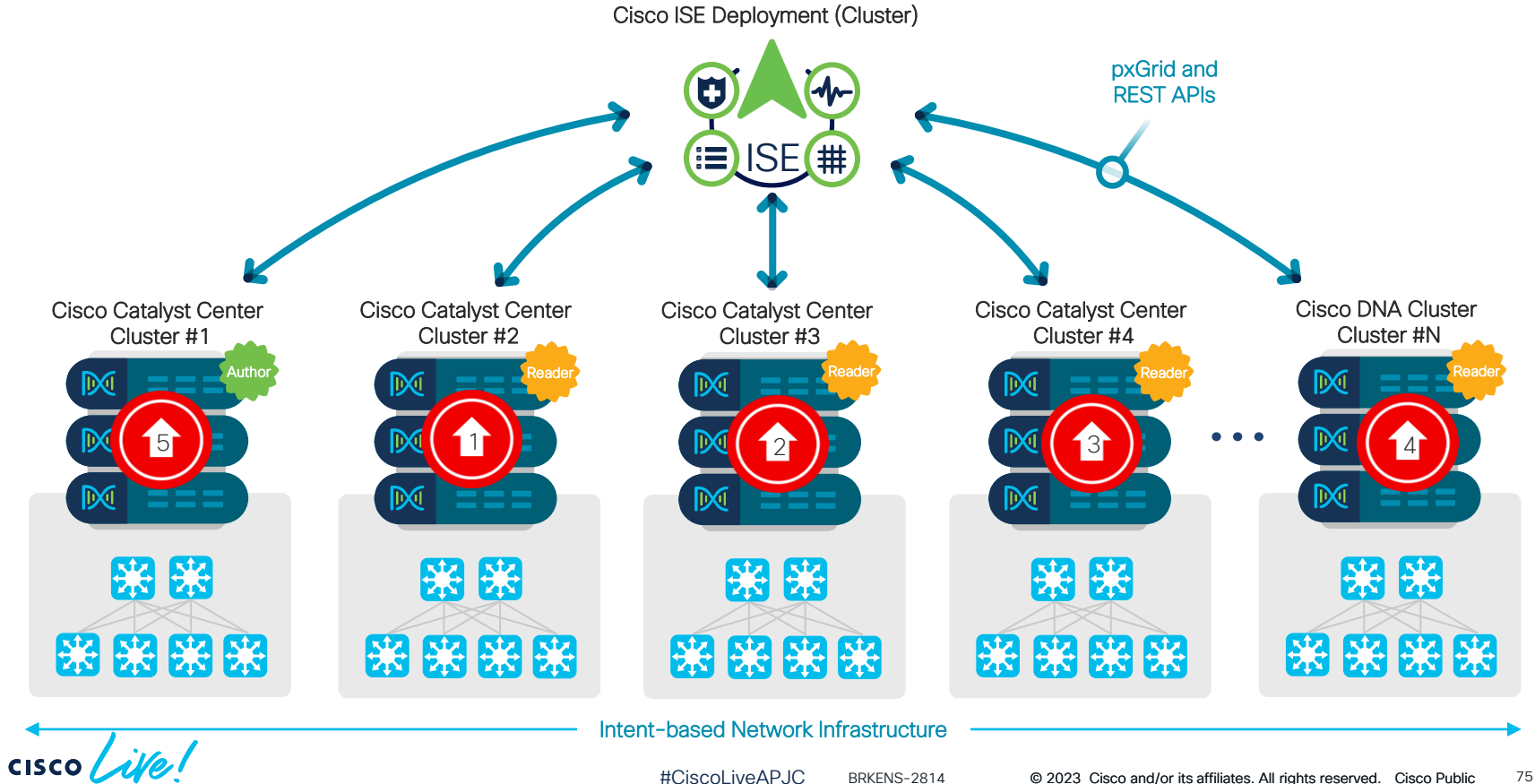
- Subsequent Catalyst Center Cluster to integrate with Cisco ISE
- Up to 4 Cisco Catalyst Center Clusters can be added as Reader Node Clusters.
- Read only view of VN, SGTs, Access Contracts, GBAC Policy and VN-SGT Associations
- Can only be a **Greenfield** Cisco Catalyst Center Cluster

Intent-based Network Infrastructure

# Multiple Cisco Catalyst Center Solution Overview

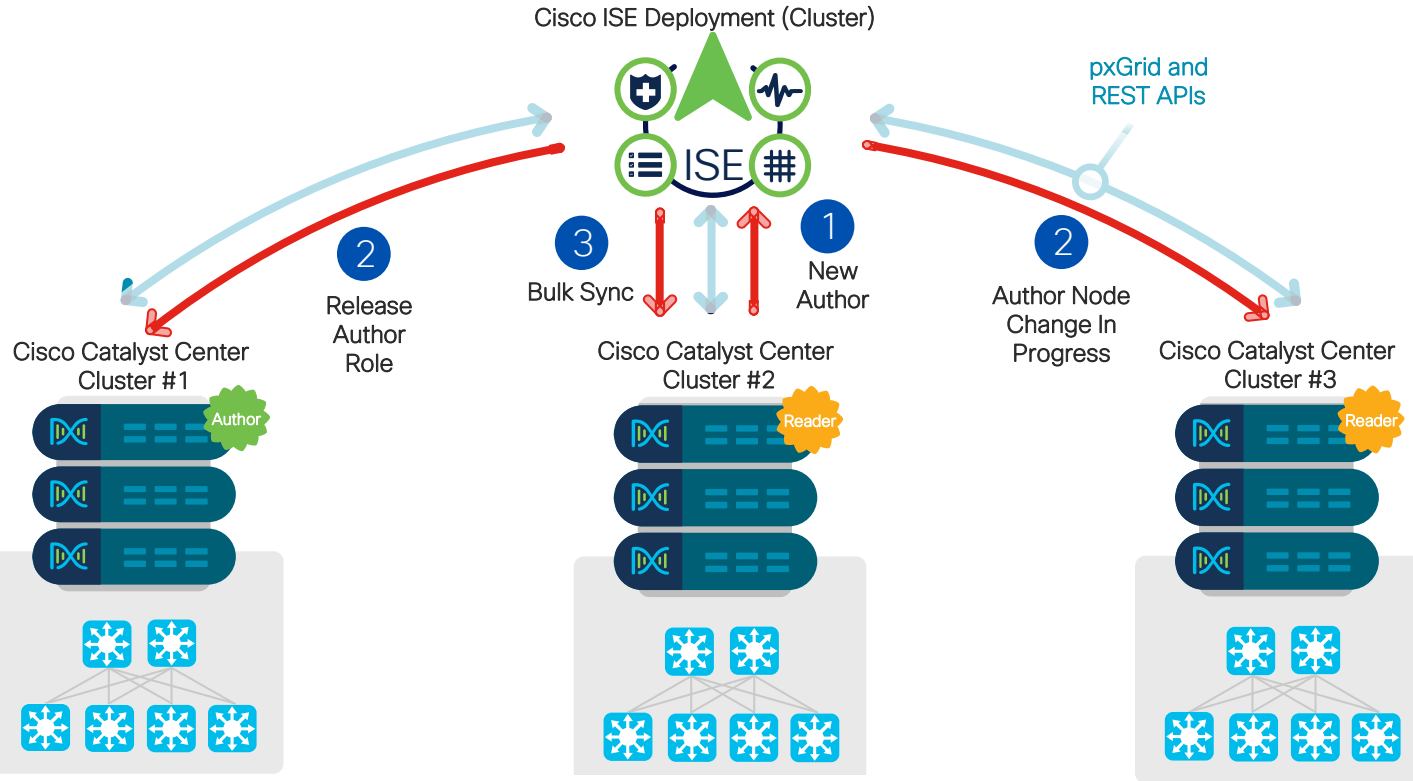


# Multiple Cisco Catalyst Center Upgrade Recommendations

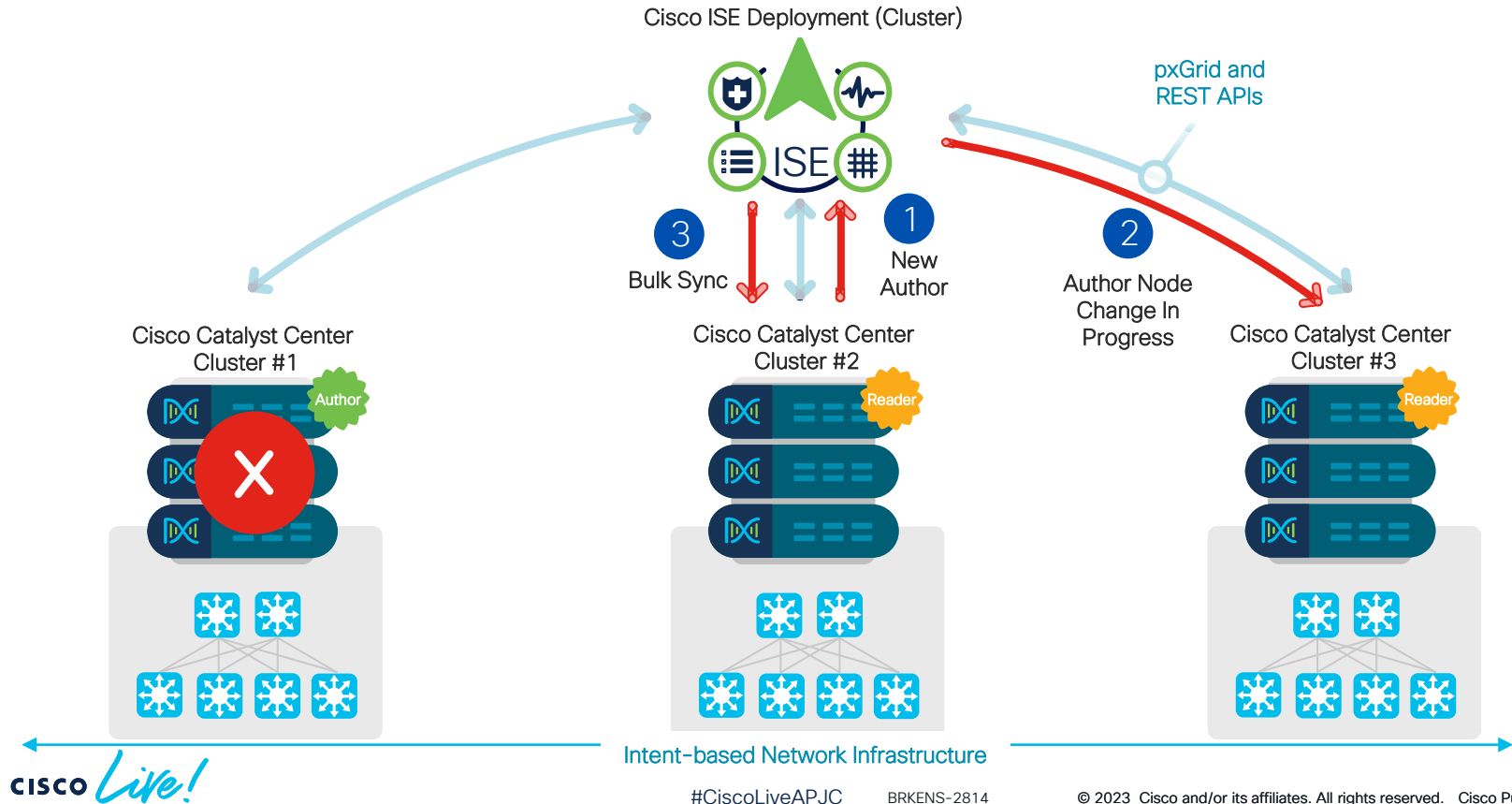


# Multiple Cisco Catalyst Center

## Graceful Promotion of Reader to Author Role



# Multiple Cisco Catalyst Center Force Promotion of Reader to Author Role



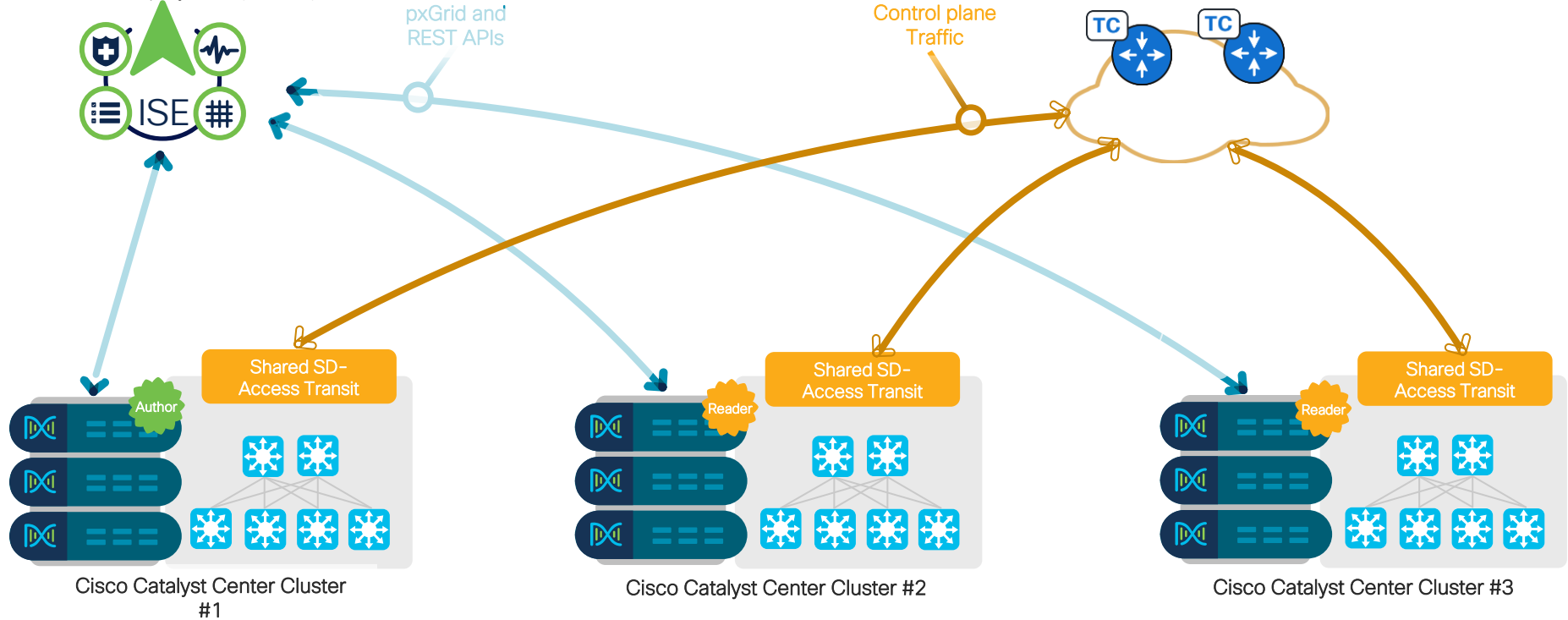
# Multiple Cisco Catalyst Center Use Case

## Shared SD-Access Transit

Shared SD-Access Transit  
Starting Catalyst Center: 2.2.3.x

4 TCP Node supported  
Starting Catalyst Center : 2.3.3.0

Cisco ISE Deployment (Cluster)



SD-Access Transit shared across multiple Cisco Catalyst Center Clusters

[illegible]

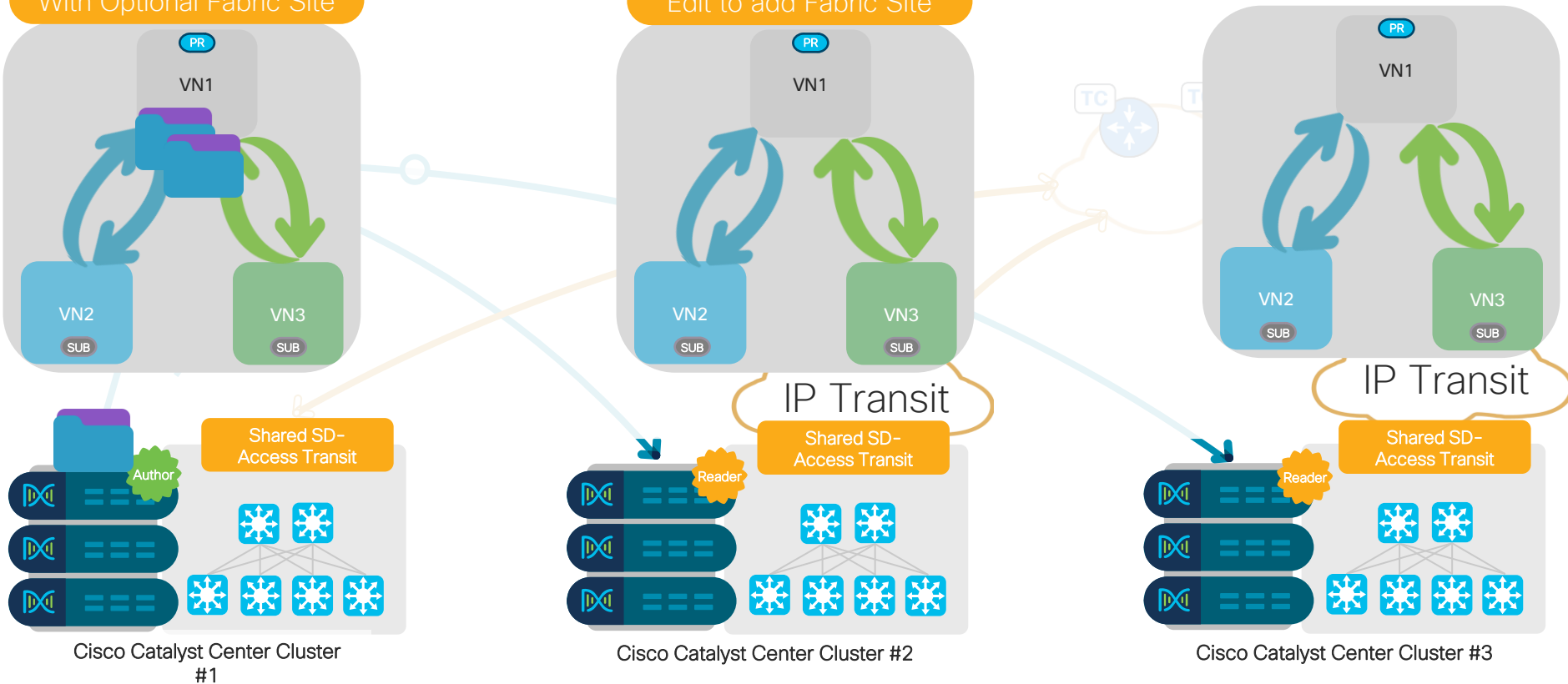
## SD-Access Transit shared across multiple Cisco Catalyst Center Clusters

# Multiple Cisco Catalyst Center

## LISP Extranet Policy- Scenario 2(Local cluster Policy)

With Optional Fabric Site

Edit to add Fabric Site



SD-Access Transit shared across multiple Cisco Catalyst Center Clusters

# Cisco SD-Access Collaterals



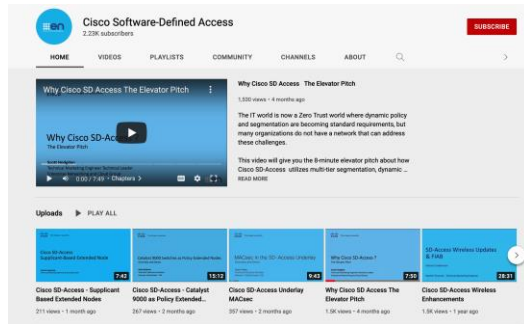
## [Cisco Software-Defined Access for Industry Verticals](#)



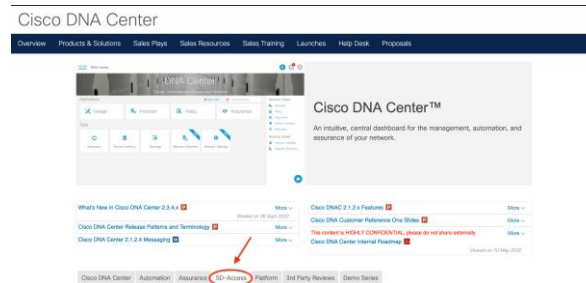
## [Cisco Software-Defined Access Enabling intent-based networking](#)



## [Cisco SD-Access YouTube Link](#)



## [Cisco SD-Access SalesConnect Link](#)



## [SD-Access BU Engagement Form](#)

## [SD-Access BU Design Council Form](#)

## [Multiple Cisco Catalyst Center LA Form](#)

## [Cisco SD-Access Design Tool](#)

## [EN&C Validated Designs](#)

# Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



# Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC