

CISCO *Live!*



#CiscoLive



The bridge to possible

Cisco ISE in SD-Access Network

Mahesh Nagireddy

Technical Marketing Engineering, Technical Leader

CCIE R&S

BRKENS-2814



#CiscoLive

Cisco Webex App

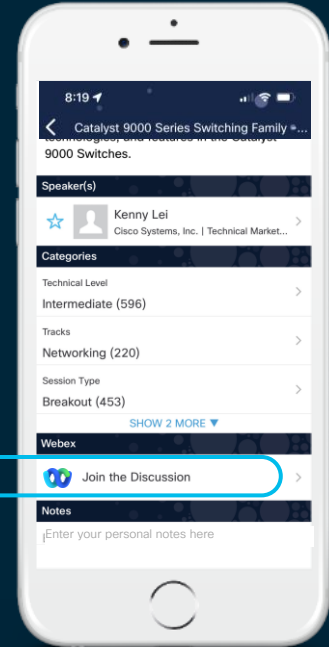
Questions?

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 June 17, 2022.



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

Networking

SD-Access

Learn about Cisco's Software Defined Access (SD-Access) solution that provides a secure, dynamic, and automated solution to meet the security and operational challenges faced by an ever-changing environment. The Cisco SD-Access sessions provide a comprehensive overview regarding best practices, design, deployment, migration and monitoring of a Cisco SD-Access architecture.

START

June 13 | 1:00 p.m.

BRKENS-2810

Cisco Software Defined Access - Under the Hood

June 13 | 2:30 p.m.

BRKENS-2811

Cisco SD-Access - Connecting to Firewall, Data Center, SD-WAN and More!

June 13 | 4:00 p.m.

BRKEWN-2308

Fabric Fundamentals - Integrating wireless into SD-Access (Fabric Enabled Wireless)

June 14 | 10:30 a.m.

BRKENS-2814

Role of Cisco ISE in SD-Access Network

June 14 | 1:00 p.m.

BRKENS-2832

Extending Cisco SD-Access Beyond Enterprise Walls

FINISH

June 15 | 10:30 a.m.

BRKENS-2502a

Cisco SD-Access Best Practices - Design & Deployment - Part 1

June 15 | 1:00 p.m.

BRKENS-2502b

Cisco SD-Access Best Practices - Design & Deployment - Part 2

June 15 | 2:30 p.m.

BRKENS-2850

What is Your First Step in Protecting Endpoints and Reducing the Attack Surface?

June 16 | 1:00 p.m.

BRKENS-3830

Tame Migration for Small to Large Campuses with SD-Access and SD-WAN at Scale - We did it for 150+ sites!

June 14 | 4:00 p.m.

BRKENS-3832

Lessons Learnt From Deployment of Large Scale Multi-Domain IBN Architectures in SDA, SDWAN and ACI

If you are unable to attend a live session, you can watch it On Demand after the event.

CISCO *Live!*



Agenda

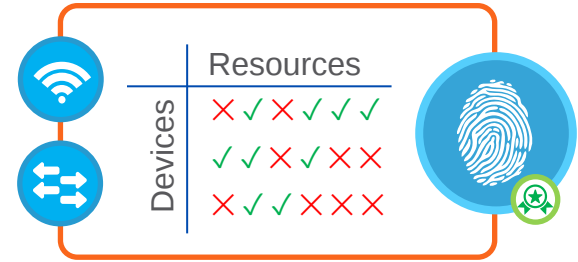
- Cisco ISE role in SD-Access Architecture
- Fabric Segmentation & Implementation
- Design & Integration

What are the challenges of networks without SD-Access?

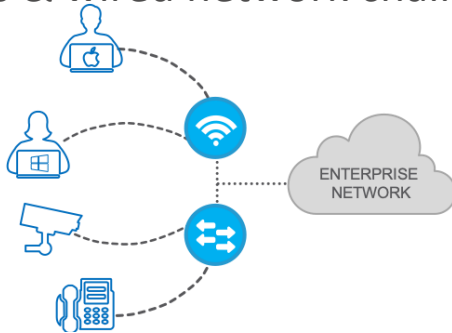
Network deployment challenges



Network security challenges



Wireless & wired network challenges

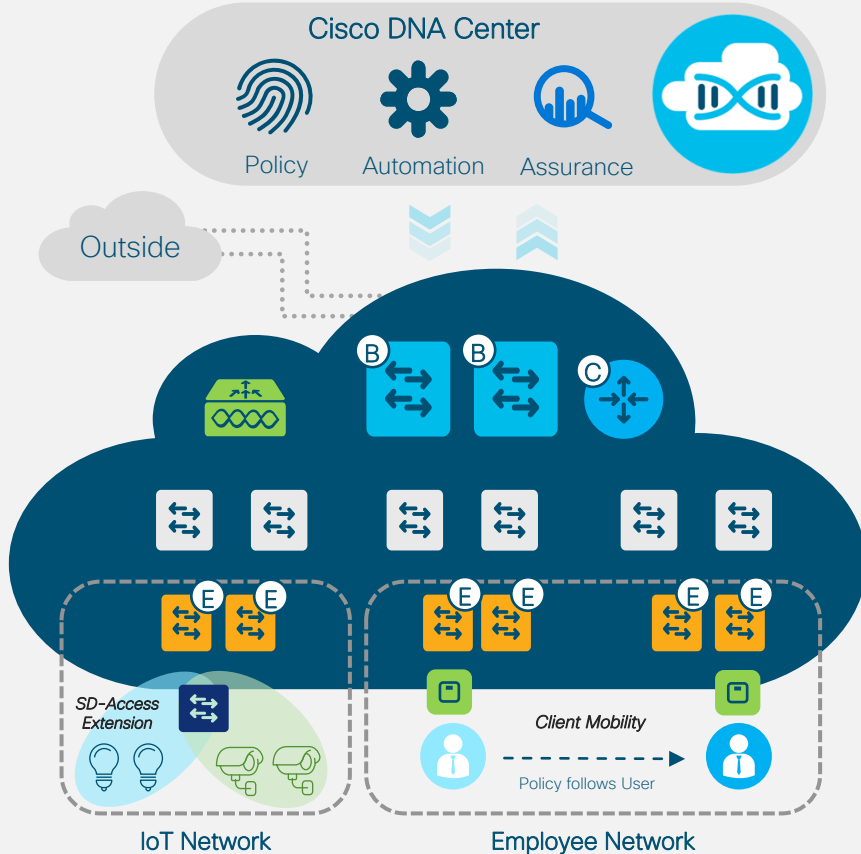


Network operations challenges



Cisco Software-Defined Access

The Foundation for Cisco's Intent-Based Network



One Automated Network Fabric

Single fabric for Wired and Wireless with full automation



Identity-Based Policy and Segmentation

Policy definition decoupled from VLAN and IP address



AI-Driven Insights and Telemetry

Analytics and visibility into User and Application experience

Benefits of SD-Access

Enhance Security and Compliance



Deliver consistent Experience



Boost operational effectiveness

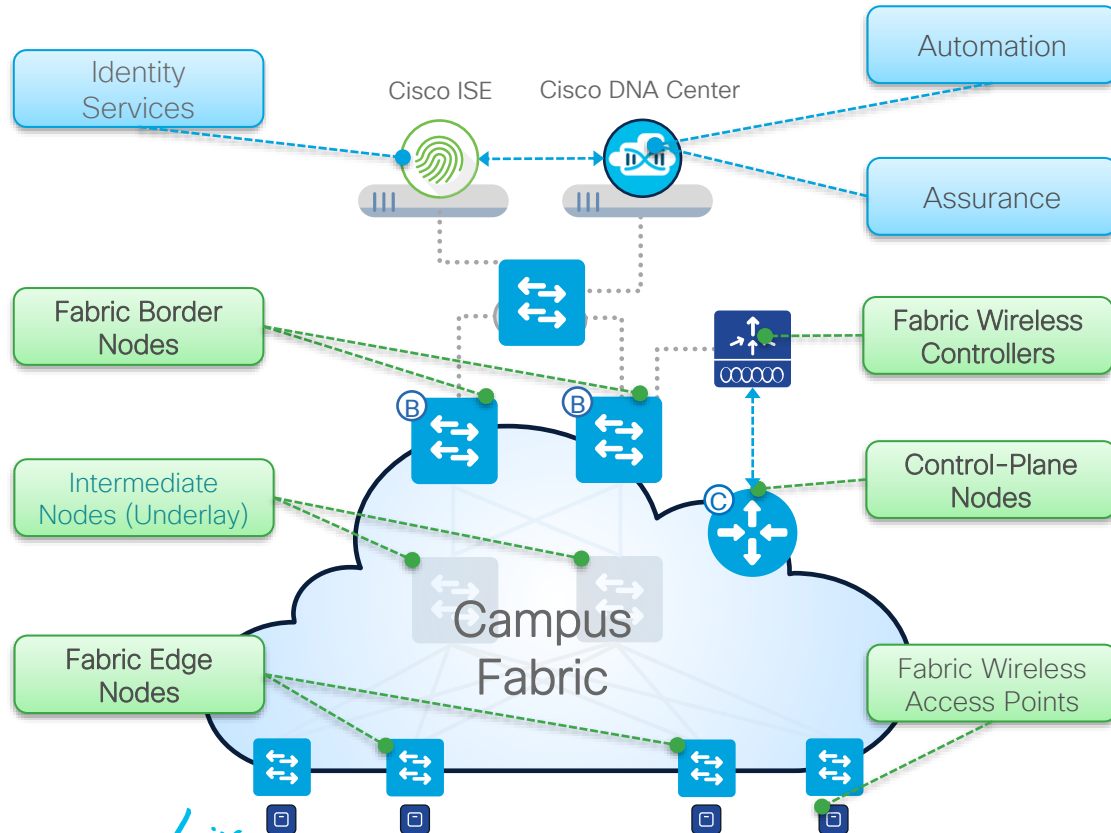


Gain network insights



Cisco SD-Access

Fabric Roles & Terminology



- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric device status
- **Identity Services** – NAC & ID Services (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- **Fabric Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric

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

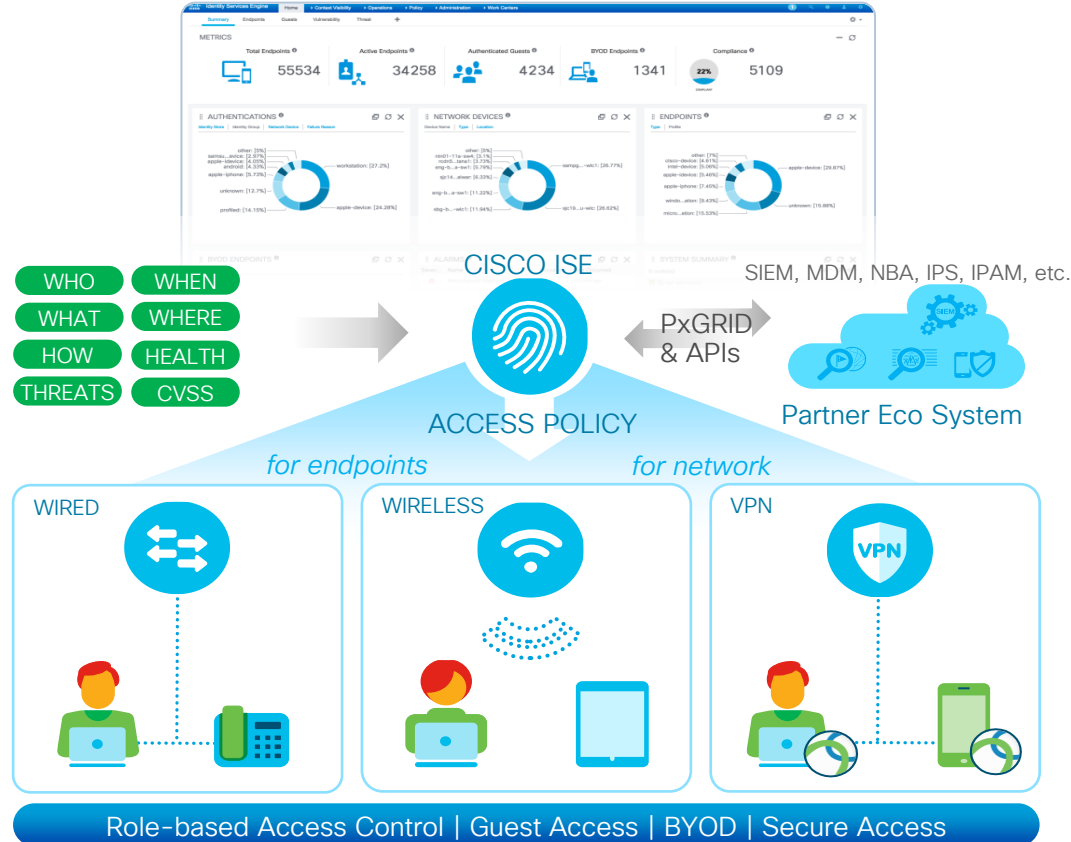
By controlling network access and segmentation



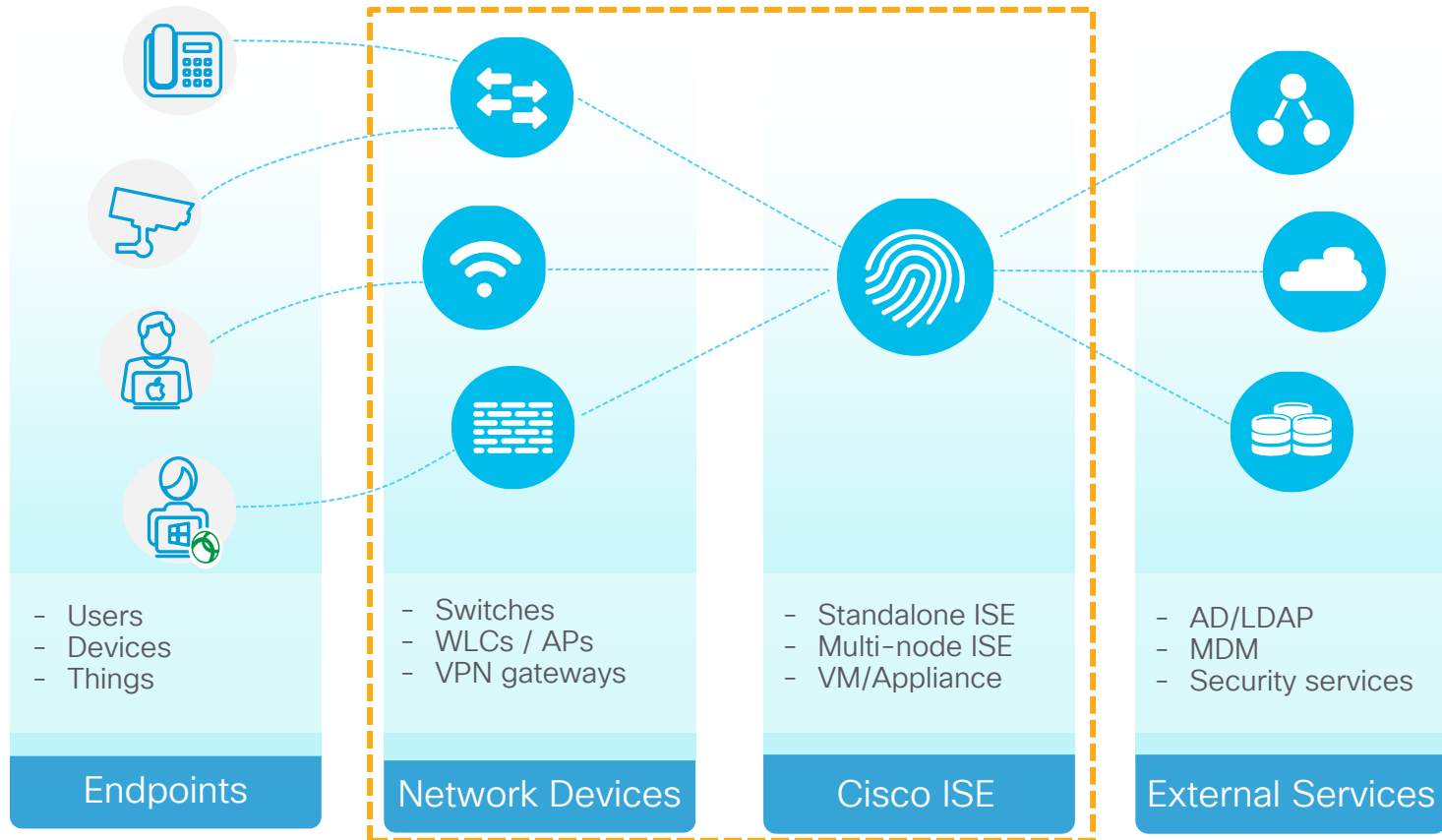
Share

Context with partners for enhanced operations

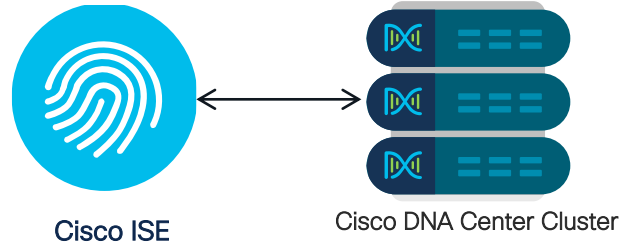
CISCO *Live!*



What's makes up an ISE Deployment



Cisco ISE Use Cases in SD-Access



Guest Access
Guest network automation

Host On-boarding
User authentication

Group Based Policies
SDA Segmentation

Assurance
Client 360

Device Administration
TACACS

Asset Visibility
Everything & Everyone on
Network

**Security Ecosystem
Integration**
Context Sharing

Guest Access Steps

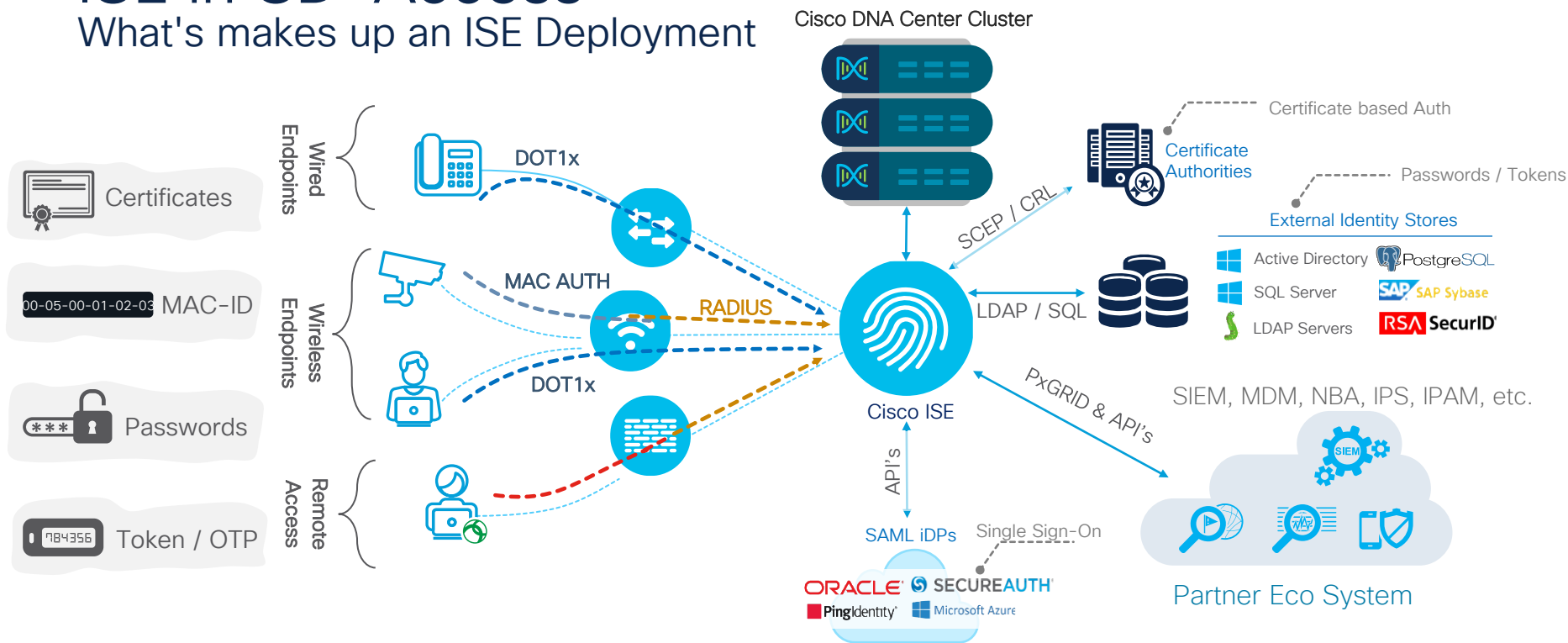
Cisco WLC 	Cisco ISE 
Create Guest WLAN	Setup Self-registration Guest Portal
ADD AAA Servers	Create Authorization Profile
Enable AAA Override	Create Authentication Rules
Create Redirect ACL	

DNA-Center 
Add a Guest Wireless SSID
Select Authentication Type(Web Auth) & ISE as Authentication Server
Setup Self Registration Portal/Hotspot Portal
Setup Wireless Profile(Fabric SSID, Anchoring/Switching mode, VLAN,

ISE role in SD- Access Architecture

ISE in SD-Access

What's makes up an ISE Deployment

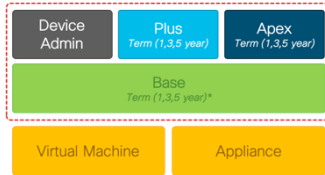


AAA, Policy-Based Segmentation and Context Sharing

ISE Scale

Standalone and Distributed

- Applies to both physical and virtual deployment
- Compatible with load balancers
- No changes to current Licensing Model



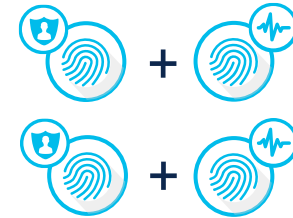
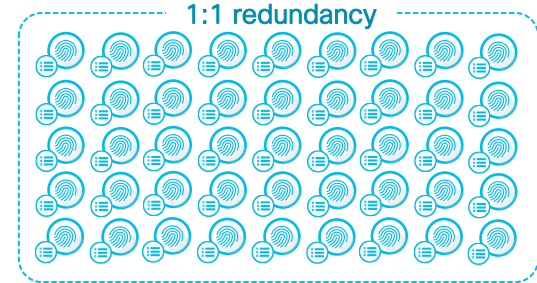
Lab and Evaluation



Small HA Deployment
2 x (PAN+MNT+PSN)



Small Multi-node Deployment
2 x (PAN+MNT), <= 5 PSN



Large Deployment
2 PAN, 2 MNT, <=50 PSN

35xx	100 Endpoints	20,000 Endpoints	500,000 Endpoints
36xx	100 Endpoints	50,000 Endpoints	2,000,000 Endpoints(3695-PAN & MNT)

ISE Performance & Scale

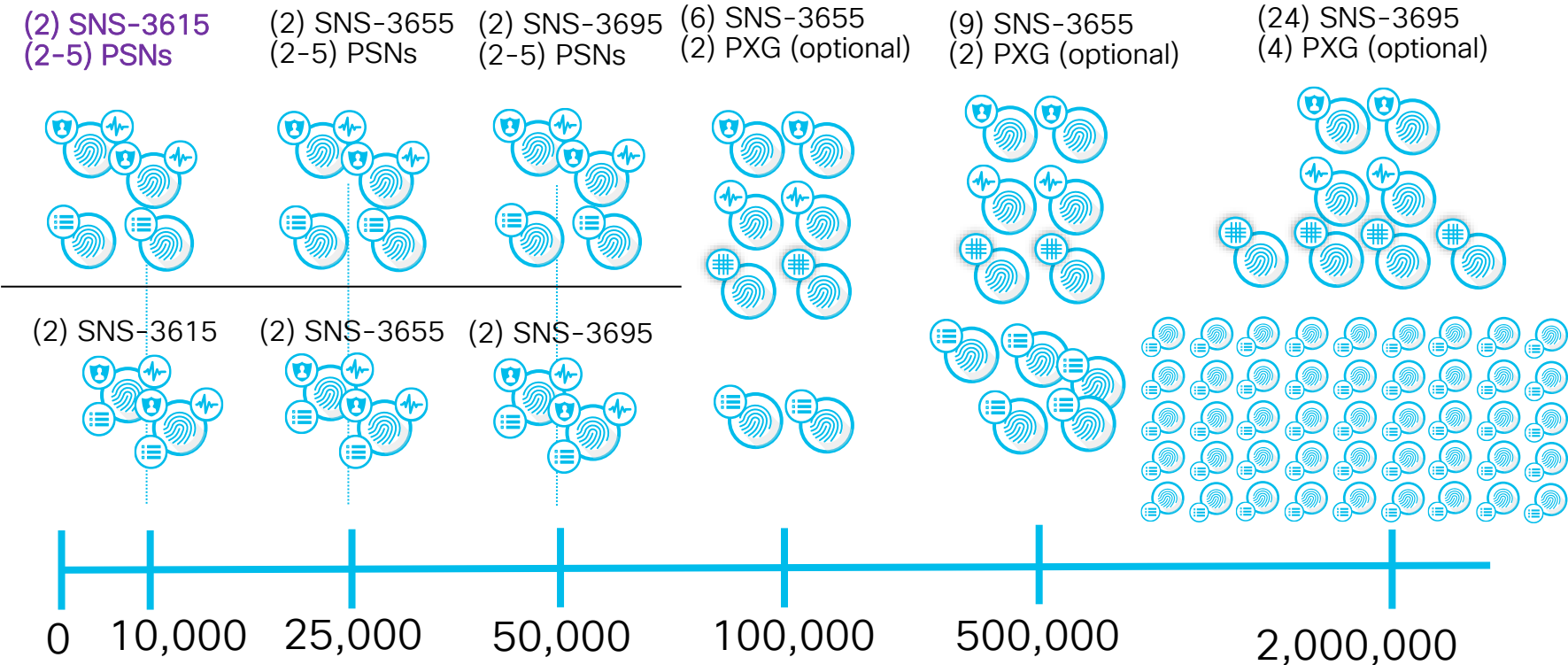
https://www.cisco.com/c/en/us/td/docs/security/ise/performance_and_scalability/b_ise_perf_and_scale.html





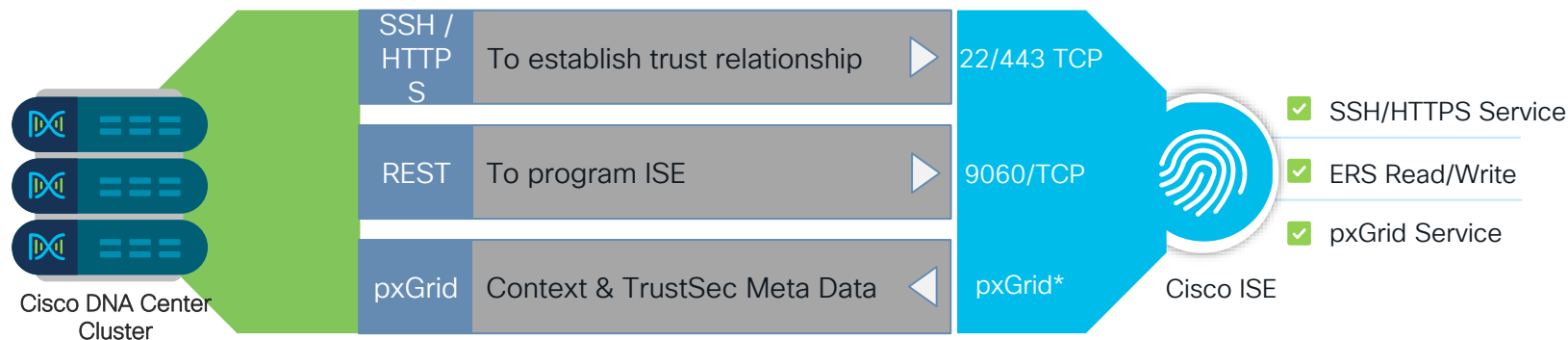
Cisco ISE Scaling

Session Scaling by Deployment Model 36xx



- 5222/TCP, 7400/TCP, 8910/TCP, 12001/TCP,
- Details: <http://bit.ly/pxgrid-ports-23>

Cisco DNA Center & ISE Communication



Cisco ISE: Enable below ISE Services

Administration > System > Deployment > Select ISE Host Name

Enable SXP Service, Passive Identity Service, and pxGrid.

Administration > Settings > ERS Settings

Enable *ERS for Read/Write on PAN*

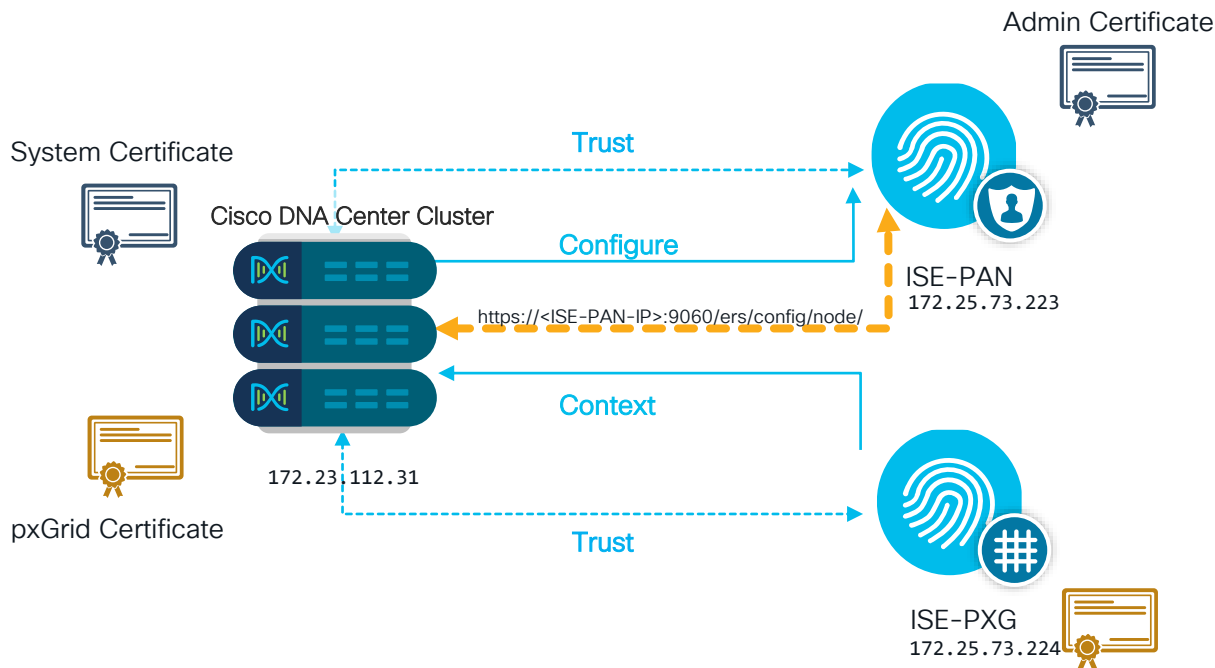
Enable ERS for Read on All other Nodes incase of Distributed model

ISE GUI password matches ISE CLI password

Cisco DNA Center and ISE Integration

How DNA Center Trust PxGrid Node

From the Cisco DNA Center home page, ick and then choose
System > Settings > Authentication and Policy Servers



Edit ISE server

Server IP Address
172.25.73.223

PAN IP

Shared Secret

Username*
admin

Password*

FQDN
ISE10-1.demo.localSubscriber Name
DNAC10

Virtual IP Address(es)

How will DNA-C know the ISE PxGrid node IP address with just PAN IP address specification?

☐ RADIUS ☐ TACACS
Authentication Port
1812Accounting Port
1813Port
49Retries*
3Timeout (seconds)*
4

Cancel

Add

Cisco DNA Center Setting

DNA Center and ISE Integration

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

https://172.25.73.223/admin/#administration/administration_messageservice/pxgrid_clientmanagement/pxgrid_clientmanagement_clients

Administration · pxGrid Services

ent Diagnostics Settings

Clients

Rows/Page 1 / 12 Total Rows

Refresh Trash Edit Enable Disable Approve Decline Filter

☐	Name	Description	Client Groups	Status
☐	admin			Initialized
☐	dnac10			• Enabled
☐	dnac10_dnac_ndp			• Enabled
☐	ise10			Initialized
☐	local_118_226	Automation Test Client		• Enabled
☐	local_73_223	Automation Test Client		• Enabled
☐	local_73_224	Automation Test Client		• Enabled
☐	pxgrid_client_1615314858			• Enabled
☐	pxgrid_client_1615314858_dnac_ndp			• Enabled
☐	pxgrid_client_1631564215	Cisco DNA Center ise-bridge service		• Enabled
☐	pxgrid_client_1631564215_dnac_ndp			• Enabled
☐	smc10			• Enabled

Cisco DNA Center Settings

Cisco ISE + Load Balancer

The screenshot shows the Cisco DNA Center web interface. The browser address bar displays `https://172.23.112.31/dna/systemSettings/settings?settings-item=authenticationPolicy`. The page title is "System · Settings". 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 includes a table of configured servers. A right-hand panel titled "Edit ISE server" is open, 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 field, which contains the value "172.25.73.240".

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 DNA Center Design

ISE as AAA Server for Client and Network

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

https://172.23.112.31/dna/design/networkSettings/network?selectedSite=da08f143-703b-47c8-8e7f-66ef263bd742

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

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 DNA Center Settings

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

The screenshot shows the Cisco DNA Center web interface. The browser address bar displays the URL: `https://172.23.112.31/dna/systemSettings/settings?settings-item=authenticationPolicy`. The page title is "System - Settings". The left sidebar contains a search bar and a list of settings categories: "Cisco Accounts" (with sub-items: PnP Connect, Cisco.com Credentials, Smart Account, Smart Licensing, SSM Connection Mode), "Device Settings" (with sub-items: Device Controllability, Network Resync Interval, SNMP, ICMP Ping, Image Distribution Servers, Device EULA Acceptance, PnP Device Authorization), "External Services" (with sub-items: Umbrella, Authentication and Policy Servers), "Authentication Tokens", "Integrity Verification", "vManage", "IP Address Manager", and "Webex Integration". The main content area is titled "Authentication and Policy Servers" and includes a description: "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." Below the description are "Add" and "Export" buttons. A table lists the configured servers, with a timestamp "As of: Jun 3, 2022 4:56 PM" and a refresh icon. The table has columns for "Protocol", "Type", "Status", and "Actions".

Protocol	Type	Status	Actions
AAA			
ISE 3.223	RADIUS_TACACS	ACTIVE	...

Cisco DNA 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.

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)
- Device addition to ISE Database
- Create Fabric Domains and add devices to Fabric

Config Deployed

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

Cisco DNA 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](#)

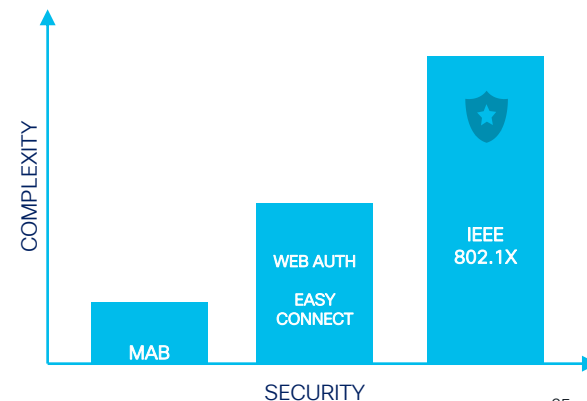
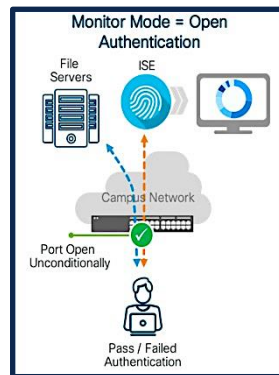
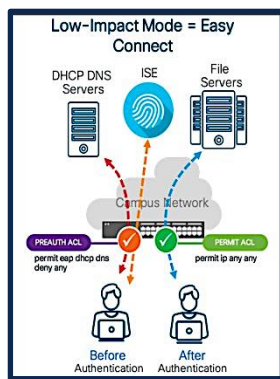
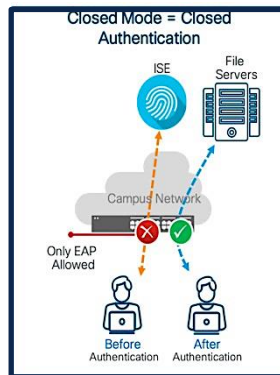
Closed Authentication

[Low Impact](#)

Low Impact

[Open Authentication](#)

Open Authentication



Cisco DNA 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

CLI's pushed with change in Fallback Timers

dot1x timeout tx-period 7

dot1x max-reauth-req 2

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 DNA Center Provision

Authentication Template(Global or 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	Select All
 SN-FOC1852Z00E.demo....	☒ GigabitEthernet1/0/1 
 C9300-24U.demo.local	☐ GigabitEthernet1/0/2 
 C3850-24P-2.demo.local	☐ GigabitEthernet1/0/5 
 C9300-24Pdemo.local	☐ GigabitEthernet1/0/6 
	☐ GigabitEthernet1/0/9 
	☐ GigabitEthernet1/0/10 

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

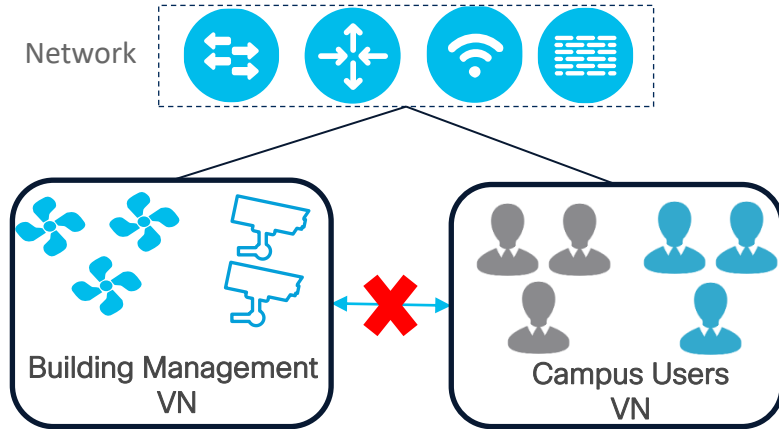
Template: default Access Vlans, IBNS 2.0 Service policy & Dot1x CLI's

Fabric Segmentation Strategy



Cisco DNA Center Policy Segmentation Strategy

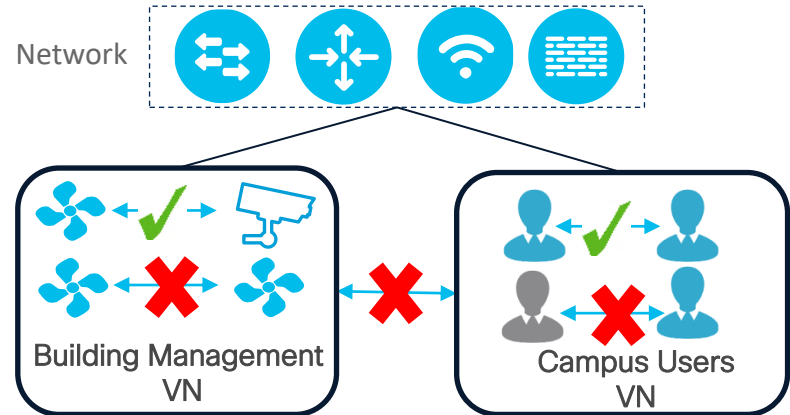
Macro Segmentation



Virtual Network (VN)

First level Segmentation ensures **zero** communication between specific groups. Ability to consolidate multiple networks into one management plane.

Micro Segmentation



Scalable Group (SG)

Second level Segmentation **ensures role based access control** between two groups within a Virtual Network. Provides the ability to segment the network into either line of businesses or functional blocks.

Cisco DNA Center Policy

Security Groups => Scalable Groups

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. The 'Policy' section is expanded, showing 'Network Access', 'Guest Access', 'TrustSec', 'BYOD', 'Profiler', 'Posture', and 'Device Admin'. The 'TrustSec' section is selected, and the 'Security Groups' page is displayed. The page shows a list of security groups with columns for 'Icon', 'Name', 'SGT (Dec / Hex)', 'Description', and 'Learned from'. A 'Total 22' badge is visible in the top right corner of the list. A 'Click here to do wireless setup and visibility setup Do not show this again' message is also present.

Icon	Name	SGT (Dec / Hex)	Description	Learned from
☐	Auditors	9/0009	Auditor Security Group	
☐	BYOD	15/000F	BYOD Security Group	
☐	Contractors	5/0005	Contractor Security Group	
☐	Developers	8/0008	Developer Security Group	
☐	Development_Servers	12/000C	Development Servers Security Group	
☐	Employees	4/0004	Employee Security Group	
☐	Employee_Wifi	16/0019		
☐	Faculty	19/0013		
☐	Guests	6/0006	Guest Security Group	
☐	Guest_Wifi	17/0011		
☐	Irvine_Bootcamp	18/0012		
☐	Network_Services	3/0003	Network Services Security Group	
☐	PCI_Servers	14/000E	PCI Servers Security Group	
☐	Point_of_Sale_Systems	10/000A	Point of Sale Security Group	

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes 'DESIGN', 'POLICY', 'PROVISION', 'ASSURANCE', and 'PLATFORM'. The 'POLICY' section is selected, and the 'Group-Based Access Control' page is displayed. The page shows a dashboard with five blue boxes representing different policy types: Virtual Network (4), Group-Based Access Control (4), IP-Based Access Control (0), Traffic Copy Policies (0), and Scalable Groups (22). Below the dashboard, there is a 'Policy History' section with a table of policy entries. A blue line connects the 'Scalable Groups' box to the 'Policy History' table.

Name	Virtual Network	State	Registered	Last Modified
Auditors	DEFAULT_VN	ACTIVE	8 months ago	8 months ago
BYOD	DEFAULT_VN	ACTIVE	8 months ago	8 months ago
Contractors	SJC15_VN	ACTIVE	8 months ago	8 months ago
Developers	DEFAULT_VN	ACTIVE	8 months ago	8 months ago
Development_Servers	DEFAULT_VN	ACTIVE	8 months ago	8 months ago
Employee_Wifi	SJC15_VN	ACTIVE	8 months ago	8 months ago
Employees	SJC15_VN	ACTIVE	8 months ago	8 months ago
Faculty	DEFAULT_VN	ACTIVE	6 months ago	6 months ago
Guest_Wifi	GUEST_VN	ACTIVE	8 months ago	8 months ago
Guests	DEFAULT_VN	ACTIVE	8 months ago	8 months ago

Assigning Endpoints to Correct VN

Authorization Profiles > [iot_authz](#)

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

Common Tasks

☐ DACL Name

☐ ACL (Filter-ID)

☒ Security Group Virtual Network:

☐ VLAN

Advanced Attributes Settings

Map SGT to VN

Virtual Networks

- IoT
- DEFAULT_VN

Security Groups List > [IoT_Sensors](#)

Security Groups

* Name

* Icon

Description

☒ Propagate to ACI

Tag Value

(Enter value between 2 and 65519)

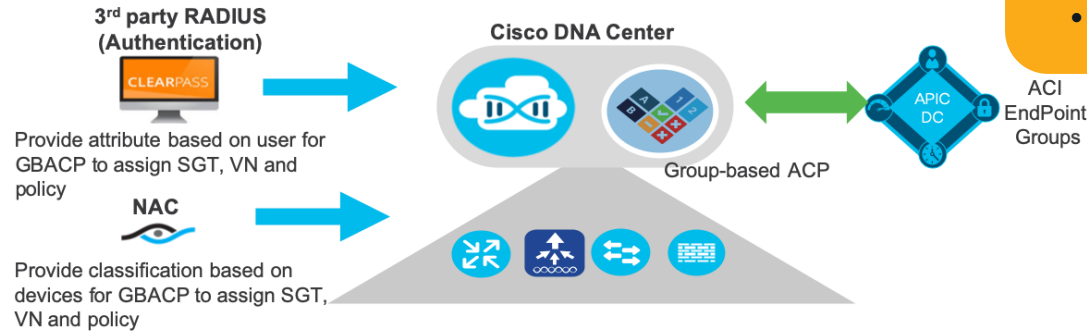
Generation Id: 0

SGT+VN+IP Pool Association

Associated Virtual Networks and Subnet/IP Address Pools

Virtual Network Name	Subnet/IP Address Pool Name	Type	Is Default	Max Value
IoT			false	
▼ DEFAULT_VN			true	
	10_202_2_0-DEFAULT_VN	Data	false	256

Cisco DNA Center Policy Group-Based Access Control Policy



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

* - Its Security Groups on Newer Cisco DNA Center releases

Cisco DNA Center Policy

Group-Based Access Control Policy Benefits



New User Policy Experience

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



Enhanced Policy Definition

- **White-listing 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

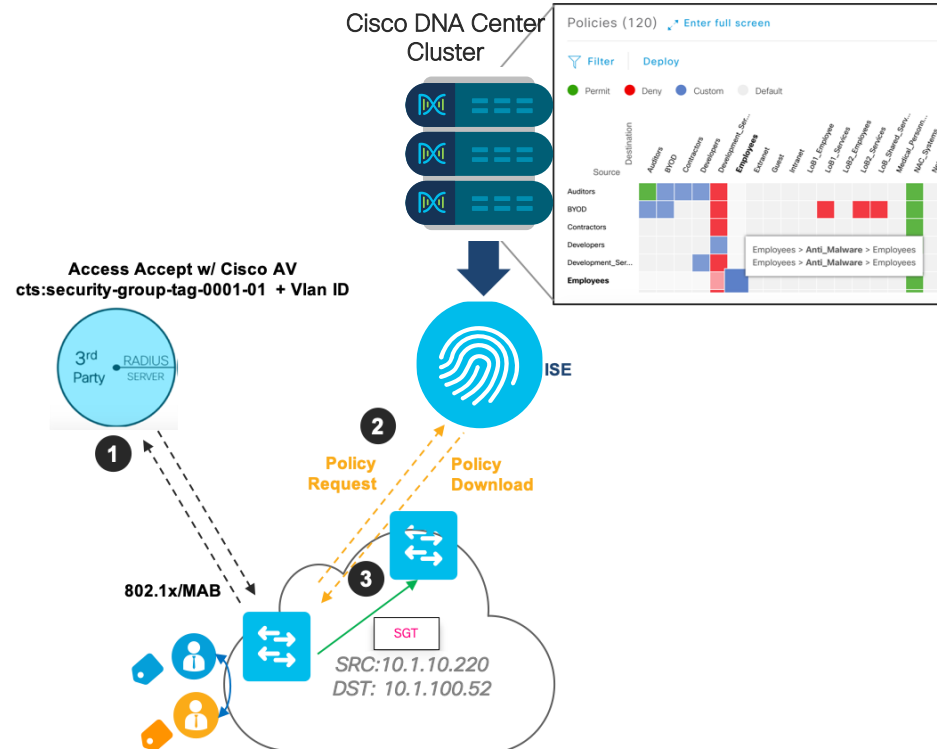
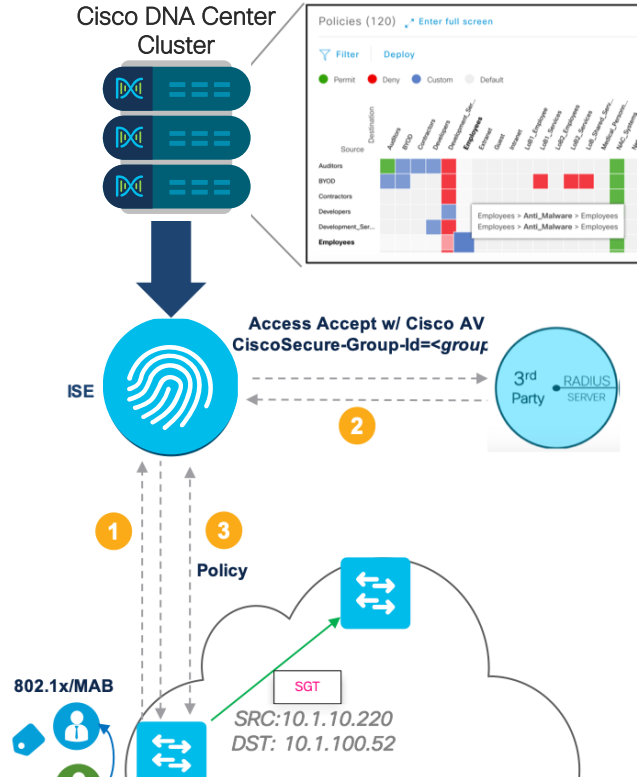


Improved Scale

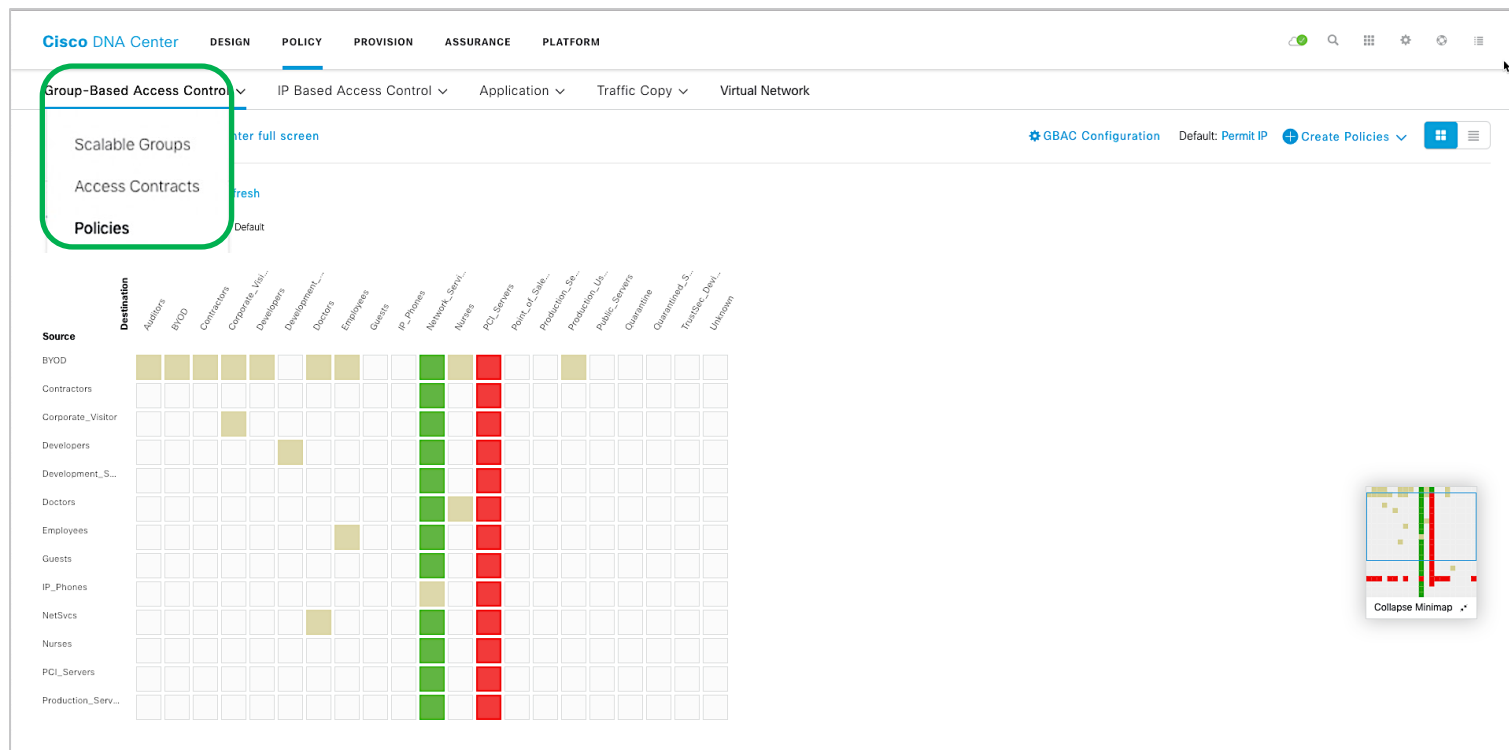
Up to 4000 Scalable Groups
Up to 500 Access Contracts
Up to 25,000 Policies

Cisco DNA Center Policy

Third-Party AAA/RADIUS Server support



Cisco DNA Center Policy Group-Based Access Control Policy



POLICY Landing Page & Matrix View

Cisco DNA Center Policy Scalable Groups

Scalable Groups (22)

Filter Actions Deploy

	Name	Tag Value	Description	Deployed	Learned From
☐	Auditors	9/0x9	Auditor Security Group	Yes	
☐	BYOD	15/0xf	BYOD Security Group	Yes	
☐	Contractors	5/0x5	Contractor Security Group	Yes	
☐	Developers	8/0x8	Developer Security Group	Yes	
☐	Development_Servers	12/0xc	Development Servers Security Group	Yes	
☐	Employees	4/0x4	Employee Security Group	Yes	
☐	Employee_WiFi	16/0x10		Yes	
☐	Faculty	19/0x13		Yes	
☐	Guests	6/0x6	Guest Security Group	Yes	
☐	Guest_WiFi	17/0x11		Yes	

Create Scalable Group

Name*

Tag Value (decimal)*

22

Description (optional)

Virtual Networks*

DEFAULT_VN

☐ Propagate to ACI

Cisco DNA Center Policy Access Contracts

Simple

FABRIC POLICIES

Source: Employees

Destination: Production

Contract: PERMIT

Employees Contractors Production Development

Save

Access Contracts (14)

Filter Actions **Deploy**

☐	Name	Description
☐	AllowDHCPDNS	Sample
☐	AllowWeb	Sample
☐	Allow_Web_Ret	Permi
☐	Anti_Malware	Block services commonly used for horizontal attacks by malware

Create Access Contract

Name: New_Contract_1

Description

CONTRACT CONTENT (1)

#	Action *	Application	Transport Protocol	Source / Destination	Port	Logging	Action
1	Deny	http	TCP	Destination	80	☒	+ -
Default Action		Permit	Logging		☐		

of ACE Lines

of Policies using Group

Cisco DNA Center Provision

Associate IP Pool to VN

Cisco DNA Center

DESIGN POLICY **PROVISION** ASSURANCE PLATFORM

Devices ▾ **Fabric** Services

Fabric-Enabled Sites 

EQ 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

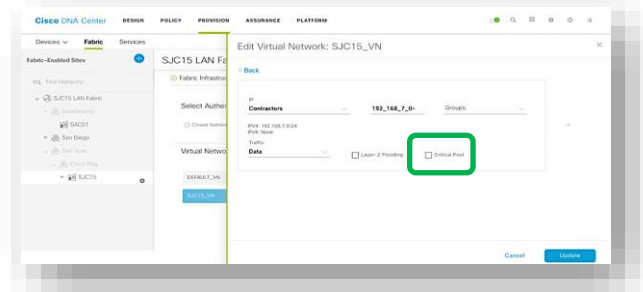
[Cancel](#) [Update](#)

Config Deployed
Vlan , SVI , Interface Template, LISP

Cisco DNA Center Host Onboarding

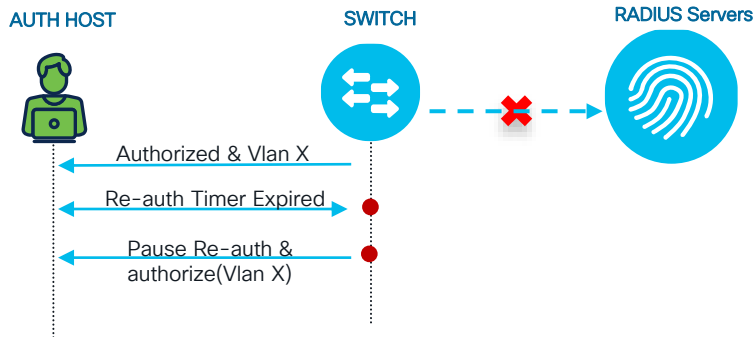
Critical Vlan

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

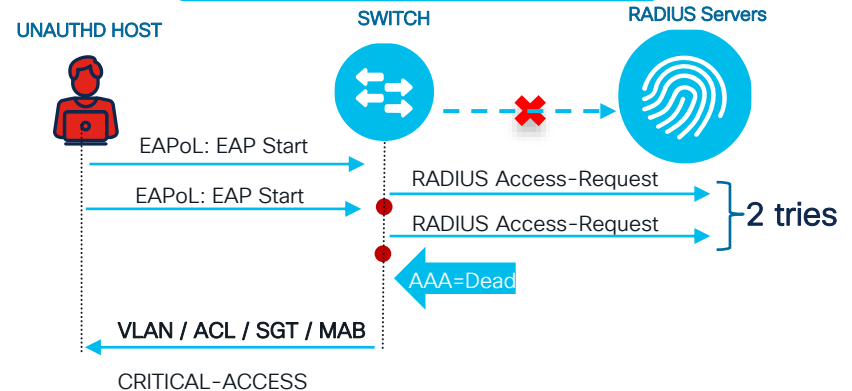


- Feature to locally activate an VLAN/ACL/ SGT/MAB during RADIUS Server outage.
- Default Critical Vlan - Data: 2047 & Voice : 2046
- No SVI created unless Critical pool selected
- Default for all Authentication Templates and Per Fabric Site
- **Need more than one Critical Vlan for Data, use Static Port assignment with dynamic Vlan mapping from Cisco ISE**

AUTHORIZED HOST

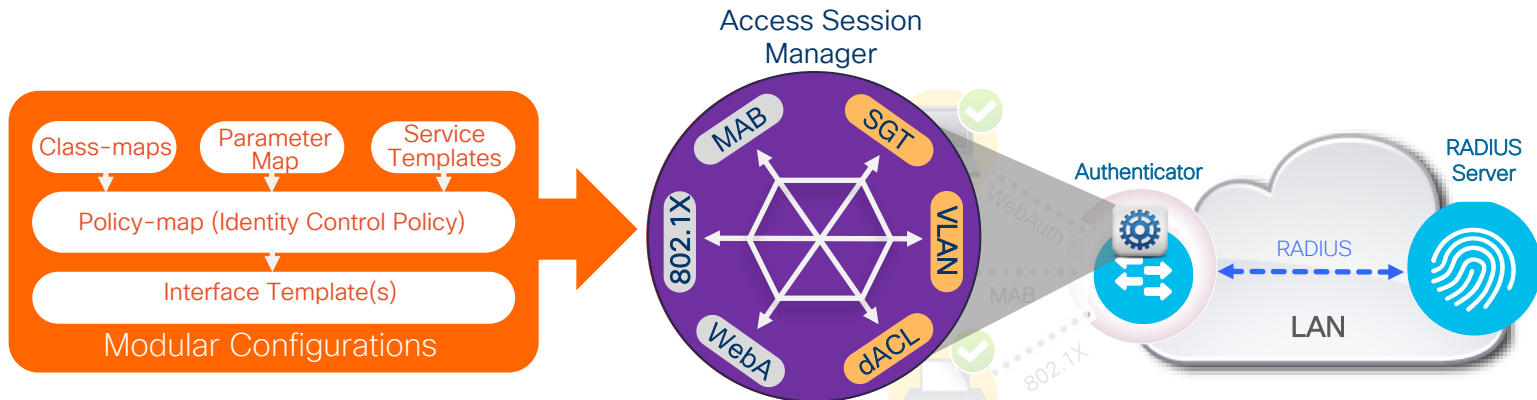


UNAUTHORIZED HOST

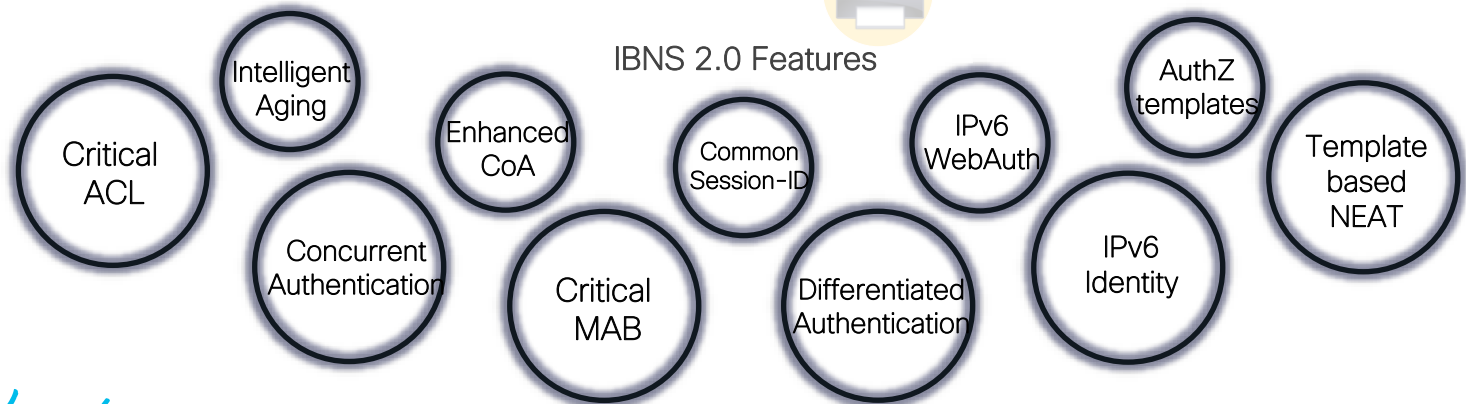


IBNS 2.0 Overview

Any Authentication with Any Authorization on any Media (Wired / Wireless)



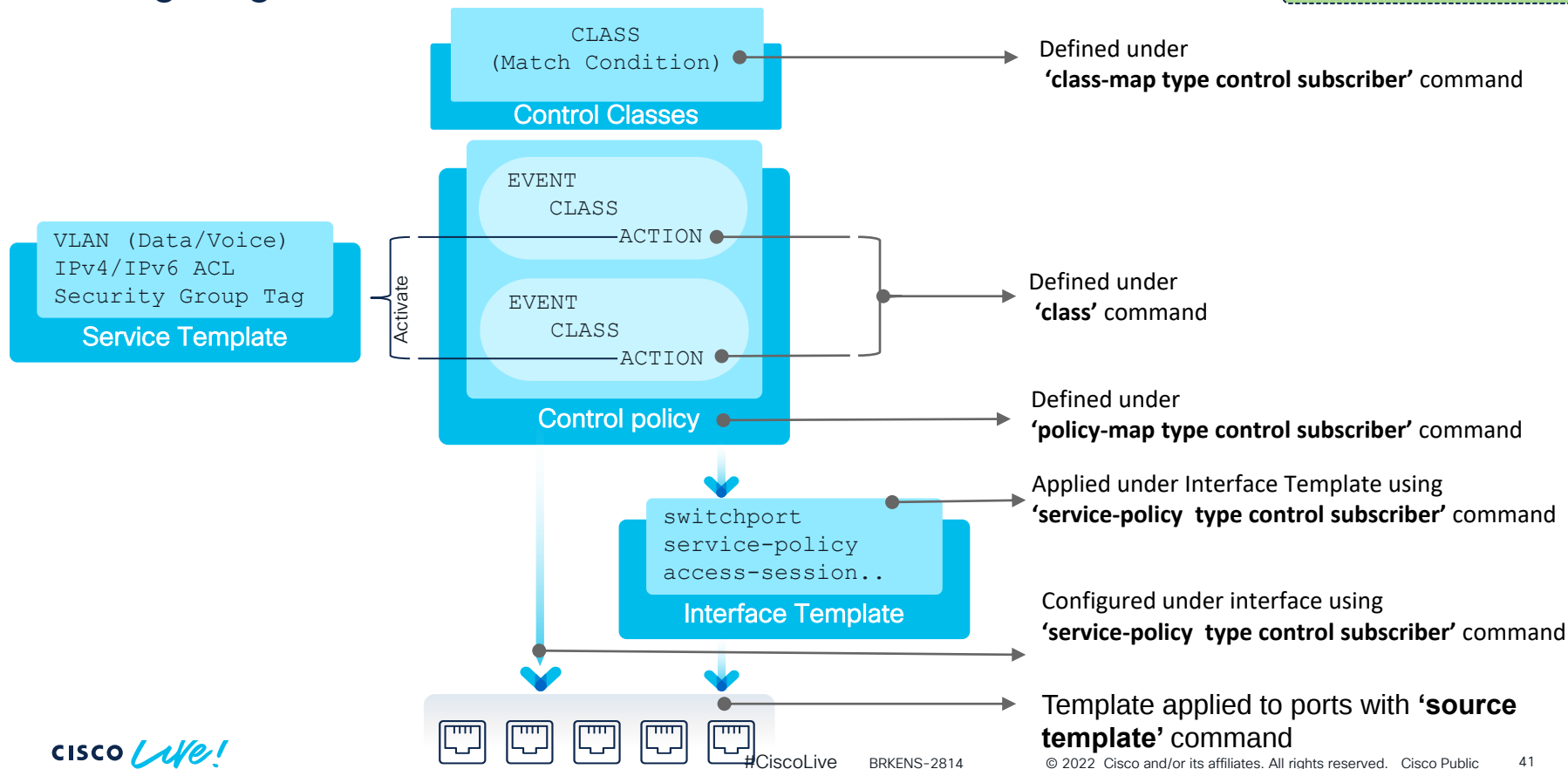
IBNS 2.0 Features



Cisco DNA Center Provision

Configuring IBNS 2.0

Global AAA and RADIUS
server configurations



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 DNA 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
```

ISE Authentication and Authorization policy

The image displays two screenshots of the Cisco ISE configuration interface, illustrating the setup of Authentication and Authorization policies. Annotations in blue boxes highlight key components.

Authentication Policy (3)

- Authentication method:** Points to the list of methods (Wired_802.1X, Wireless_802.1X) under the 'Conditions' column.
- Where to look for identities:** Points to the 'All_User_ID_Stores' dropdown menu under the 'Options' section.
- How to handle Auth failures:** Points to the 'If Auth fail', 'If User not found', and 'If Process fail' dropdown menus, which are set to REJECT, REJECT, and DROP respectively.

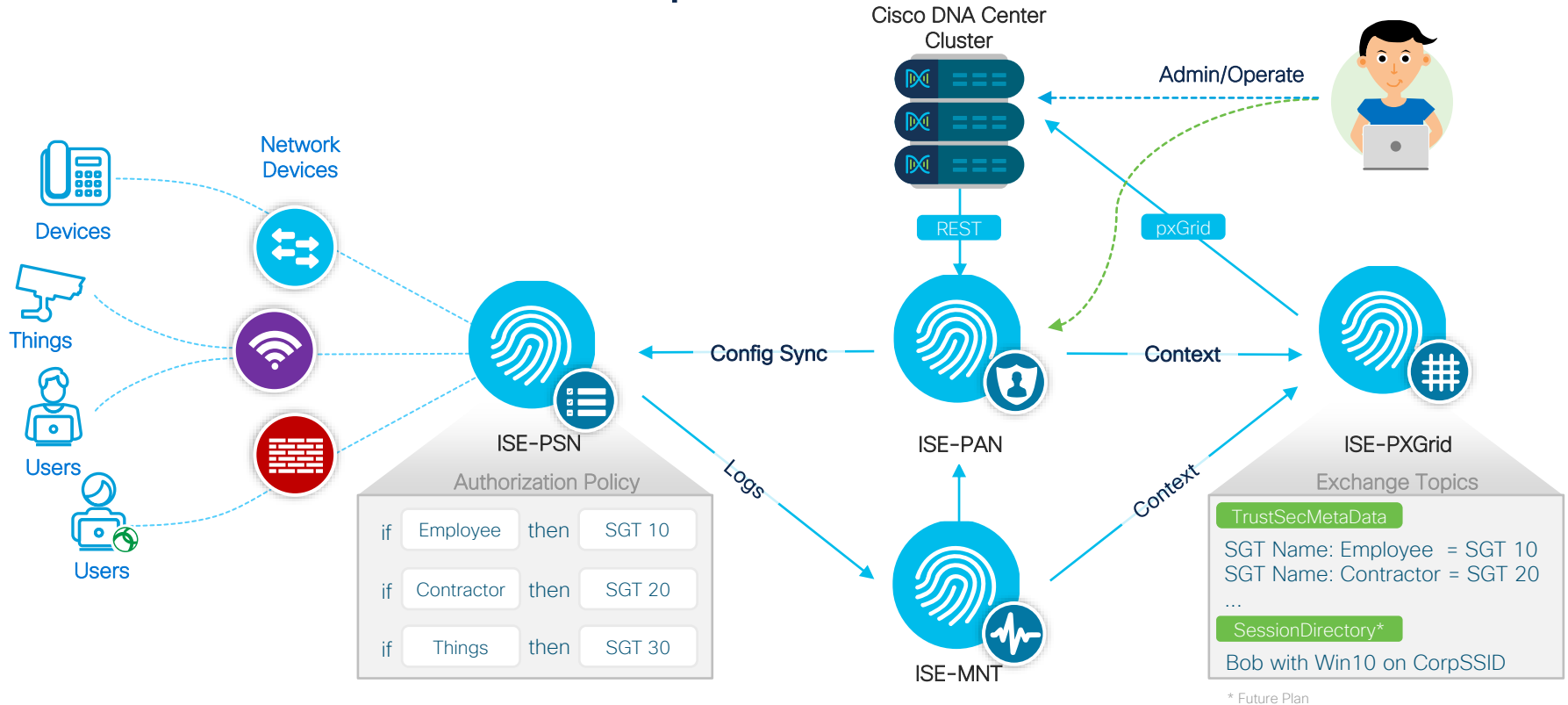
Authorization Policy (19)

- Authorization conditions:** Points to the 'Conditions' column, which shows the logical combination of network access methods and user groups (e.g., Wired_802.1X AND ad10-ExternalGroups EQUALS demo.local/HCC/Groups/Employees).
- End result:** Points to the 'Security Groups' column, which shows the resulting groups (Employees-Demo.local, Contractors-Demo.local) and the number of hits (198, 2).

A blue arrow points from the 'How to handle Auth failures' annotation in the Authentication Policy section down to the 'Authorization conditions' annotation in the Authorization Policy section, indicating the flow of configuration.

Configured by Administrator

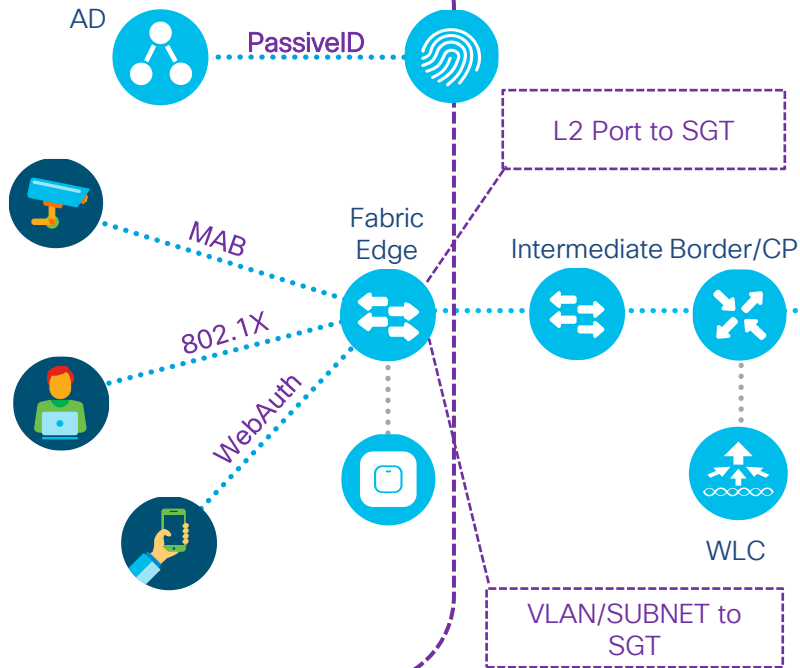
Cisco DNA Center Operation



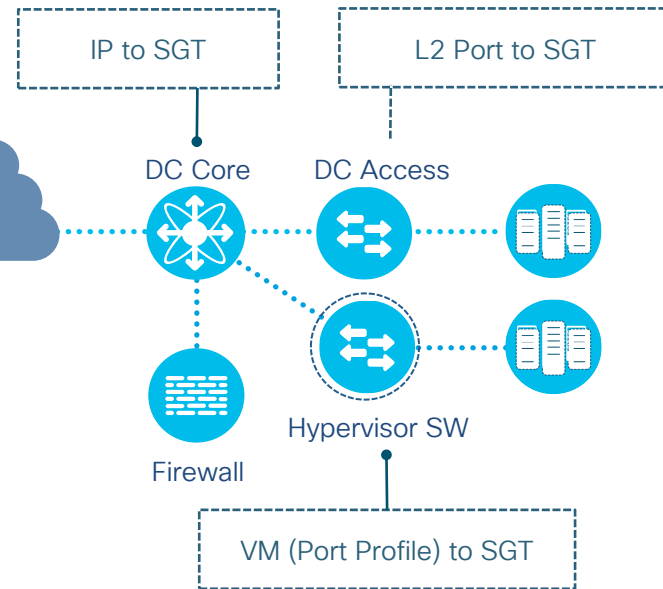
Security Group Tags(SGT)

Classification Mechanism

Dynamic Classification



Static Classification

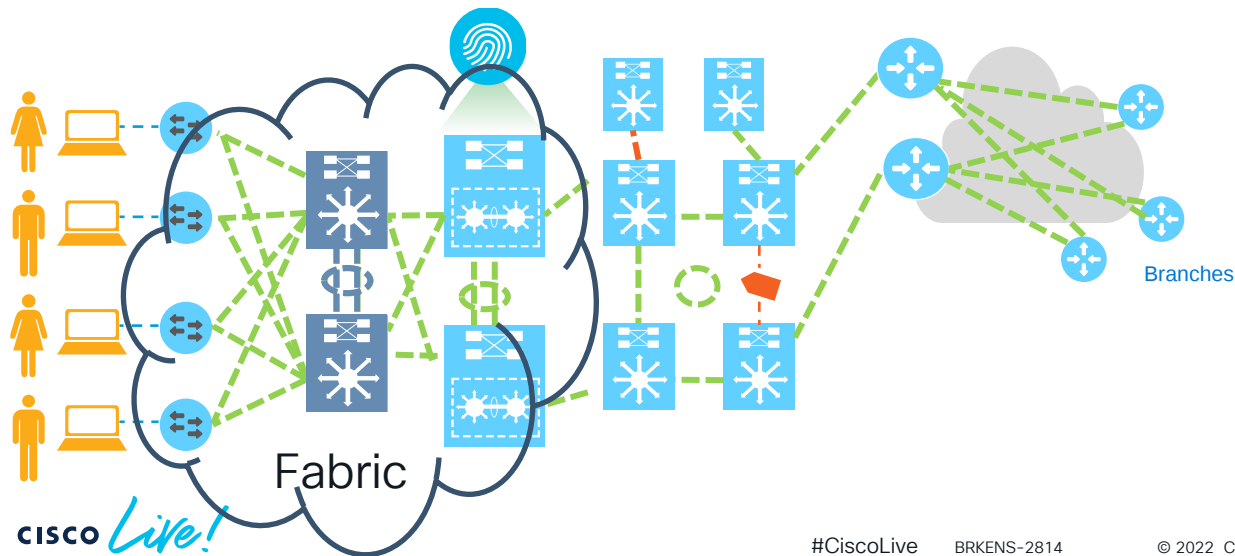


Scalable Group Tags(SGT)

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

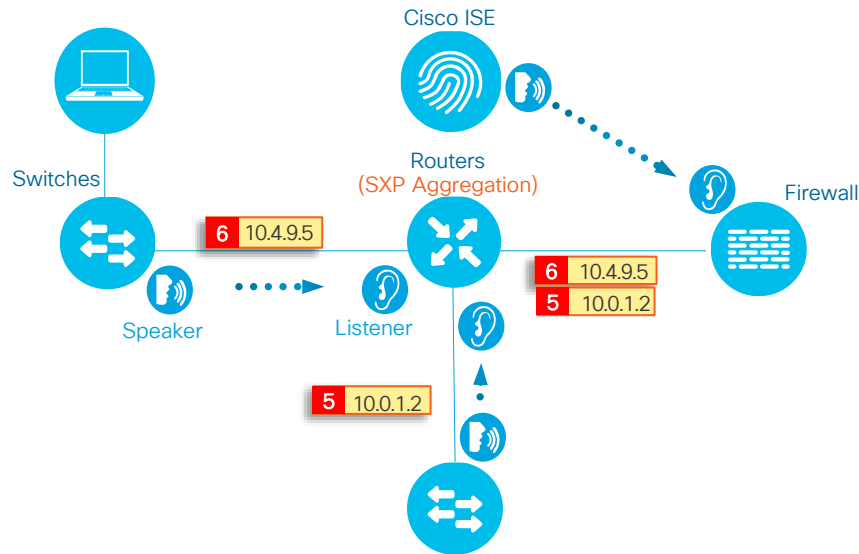
- Catalyst switches
- WLAN controllers
- Nexus switches
- Integrated Service Routers
- Industrial Ethernet Switches
- ASR 1000
- ASA 5500-x
- Firepower Threat Defense

Scalable Group Tags(SGT)

Propagation Mechanism

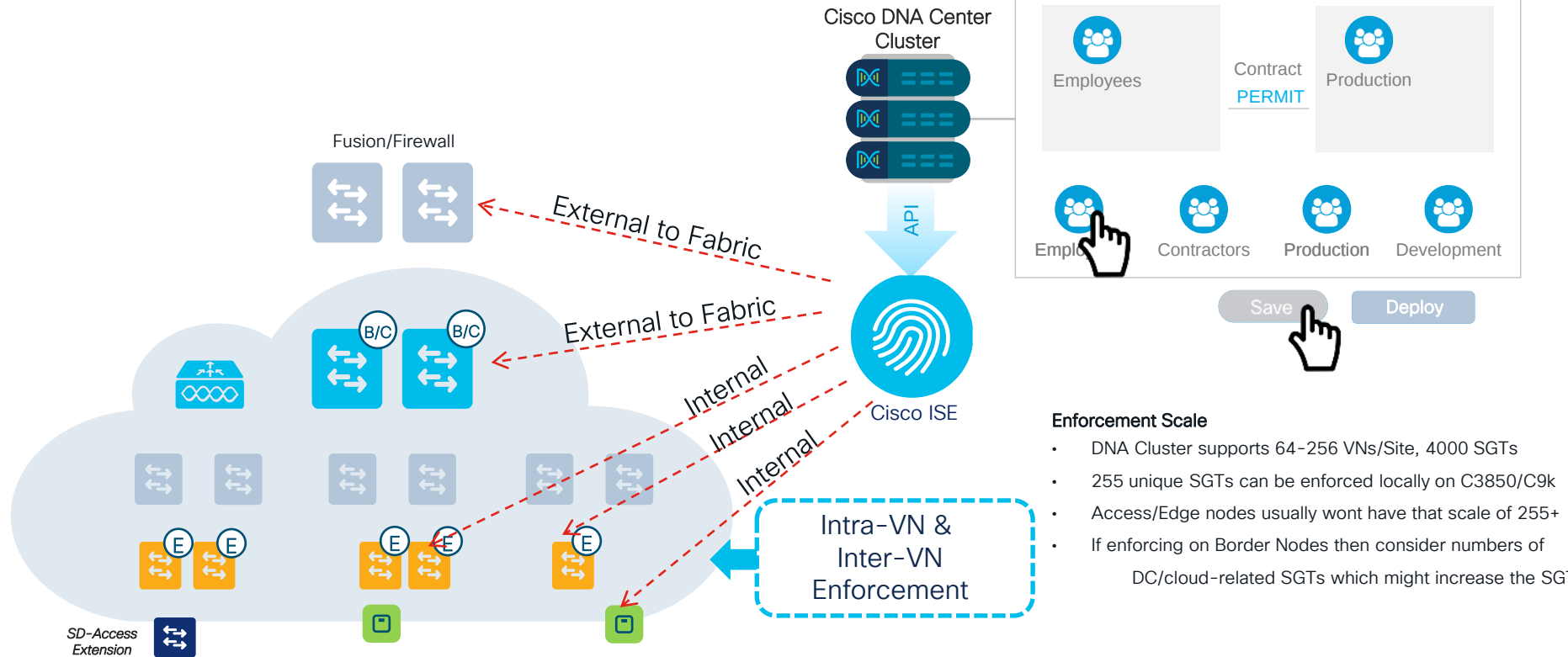
SGT Exchange Protocol (SXP)

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



Cisco DNA Center Policy

Access Contracts Enforcement



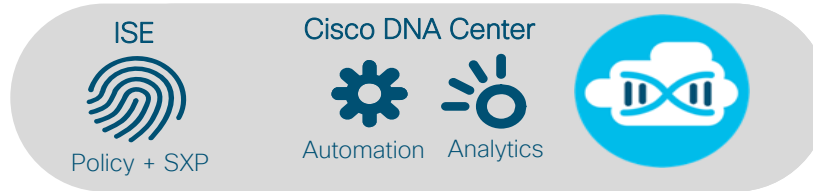
Enforcement Scale

- 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 SG

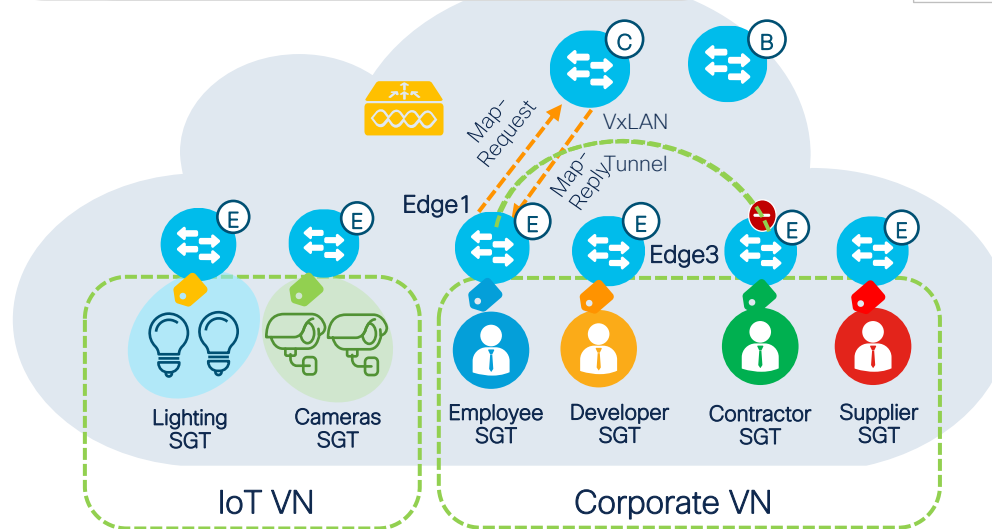
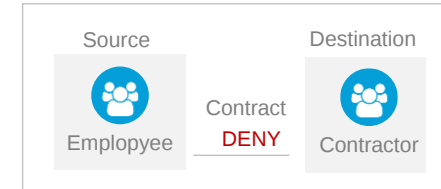
<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/software-system-bulletin.pdf>

Cisco DNA Center Policy

Segmentation within the Fabric

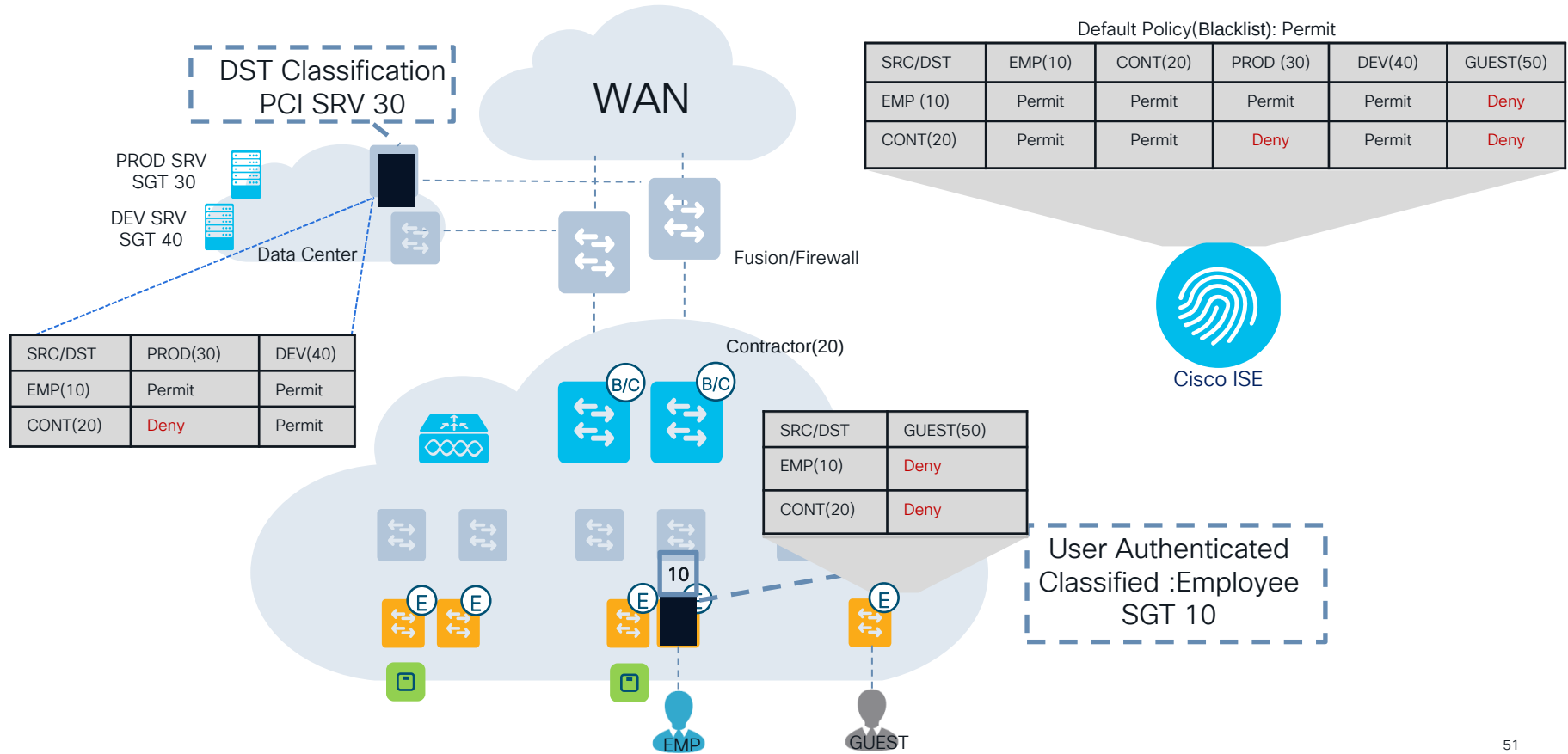


FABRIC POLICY



Cisco SGT

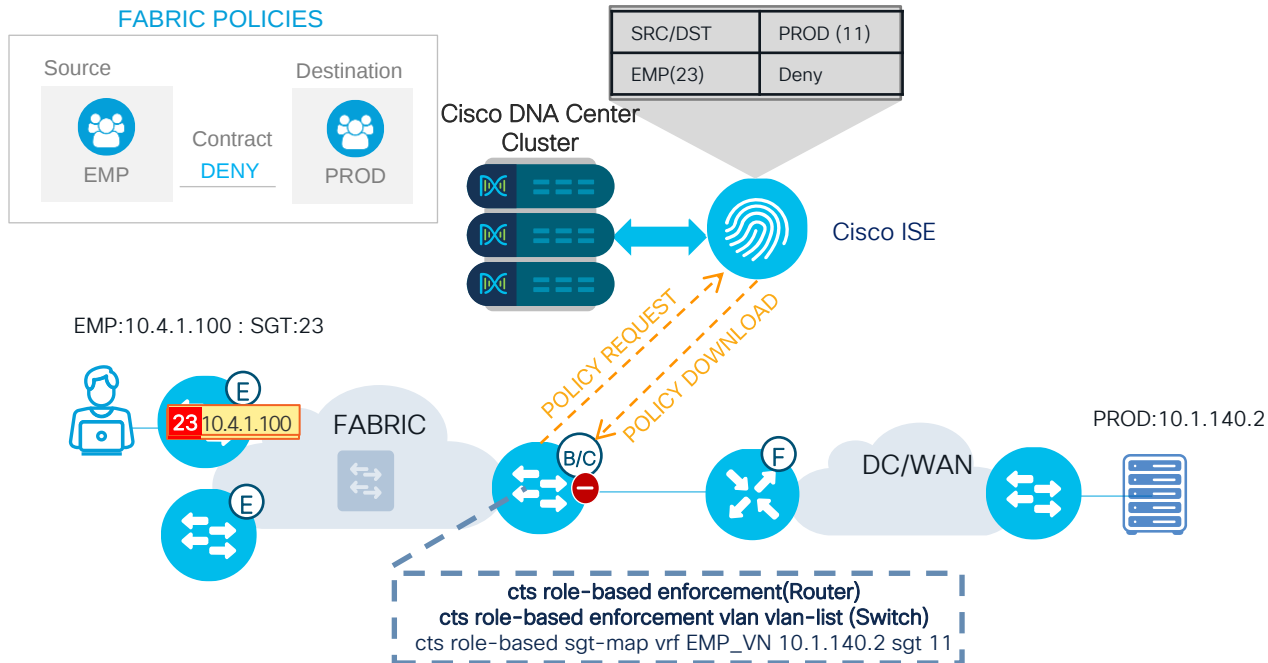
SGT Tagging & SGACL Download



Cisco DNA Center Policy

Access Contracts Enforcement on Border

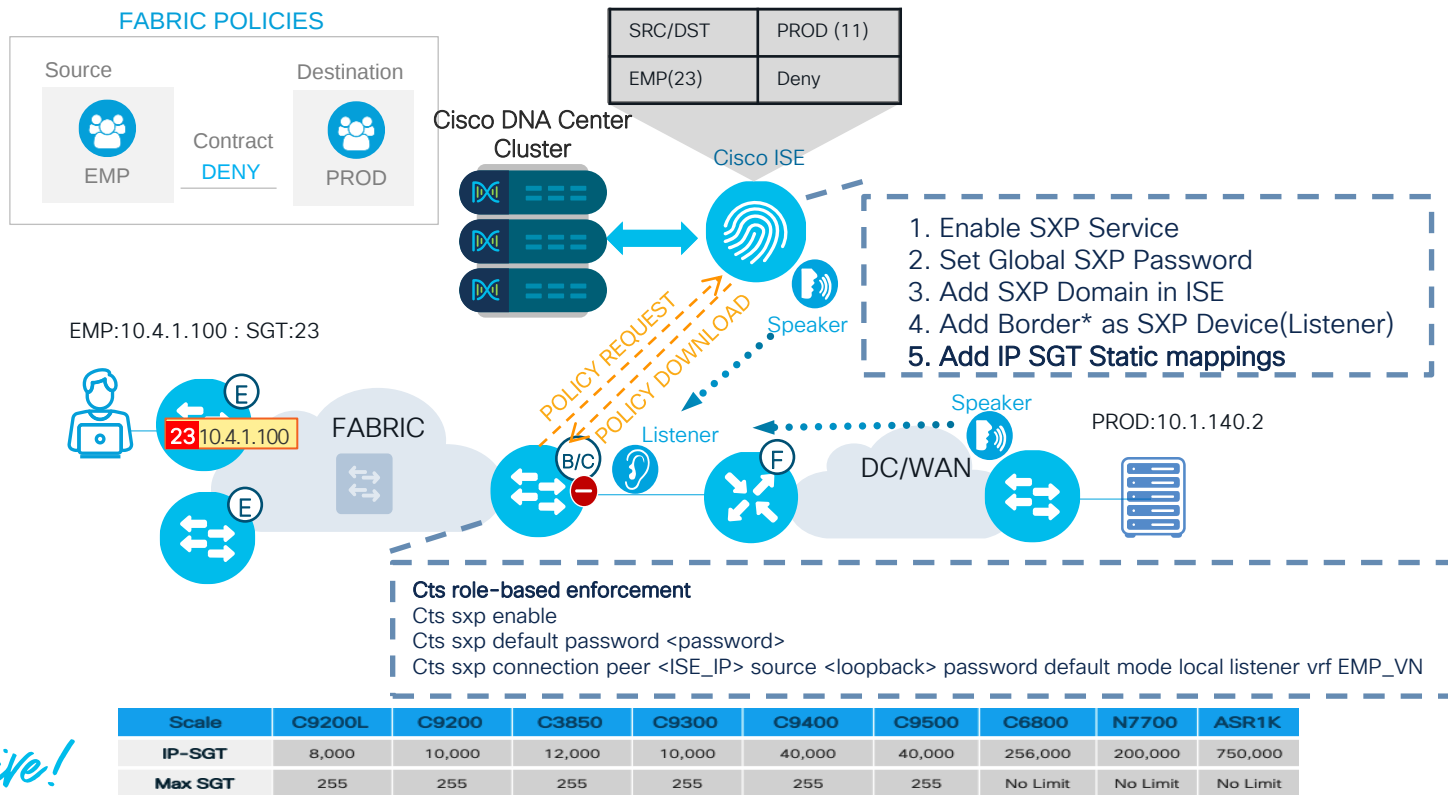
1. Statically/Manually adding policy on Border via CLI



Cisco DNA Center Policy Access Contracts Enforcement on Border

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

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

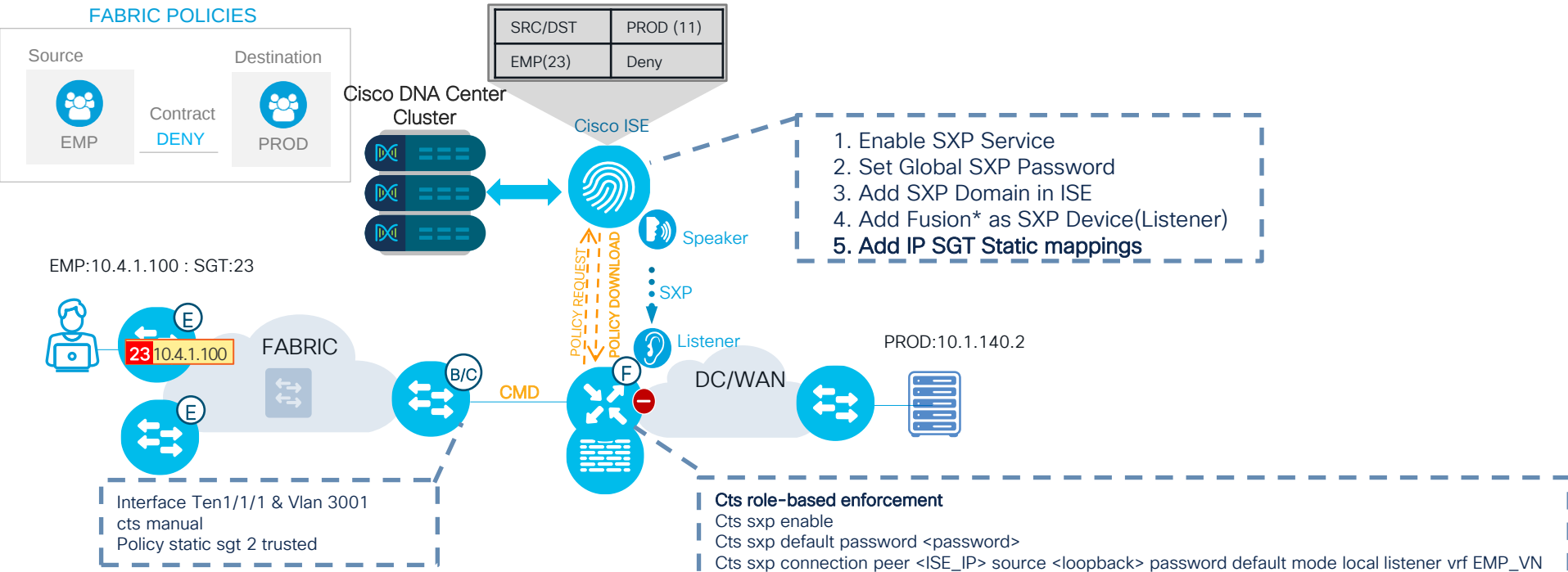


Cisco DNA Center Policy

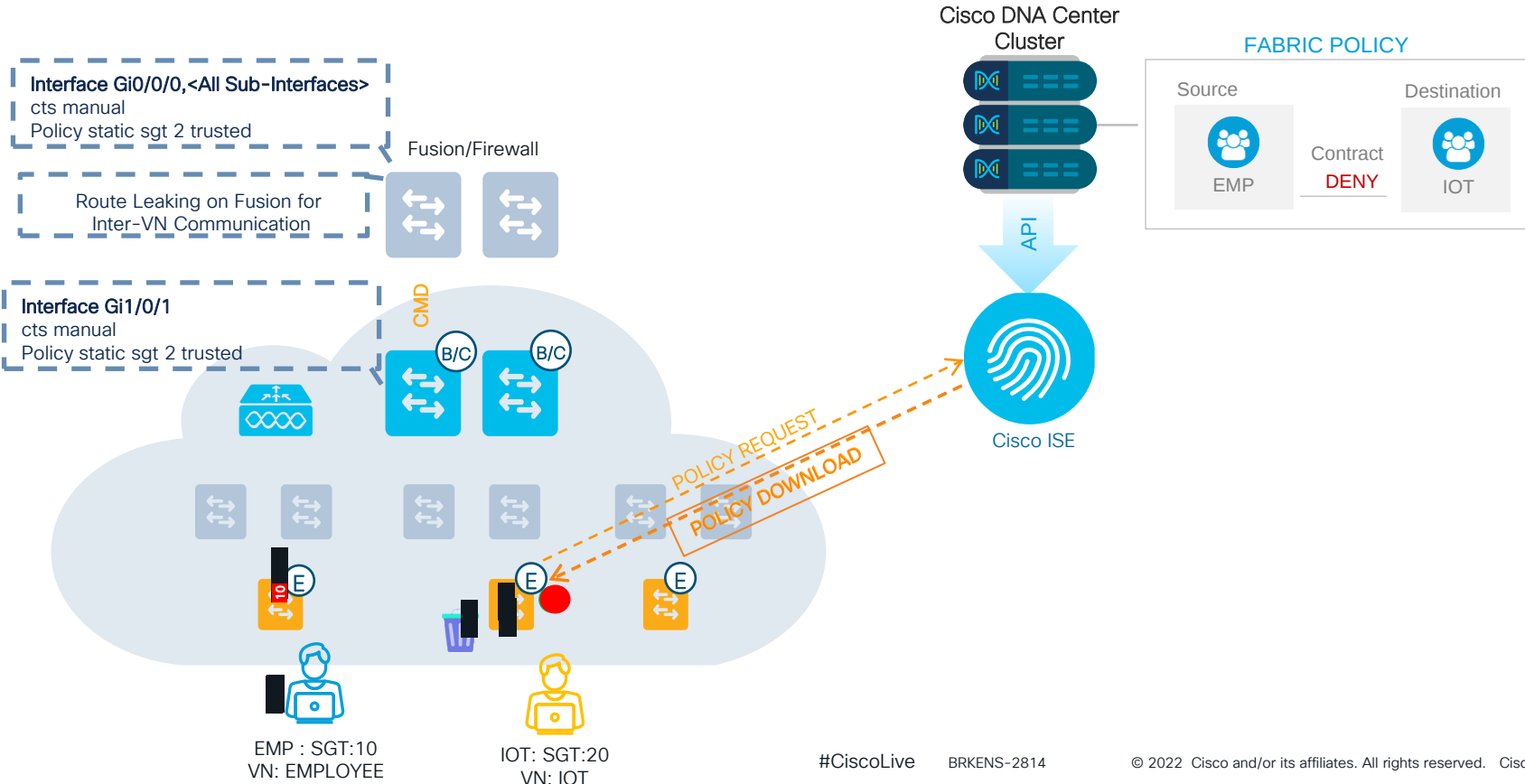
Access Contracts Enforcement on Fusion

SRC & DST SGTs learnt via SXP(Cisco ISE)

VxLAN to CMD Conversion(Border)



Cisco DNA Center Policy VN-2-VN Policy Enforcement



Cisco DNA Center Policy Whitelist vs Blacklist Model

Blacklist Model

Source		Destination				
		Production_User	Production_Srvr	Development_User	Development_Srvr	Unknown
Production_User						
Production_Srvr						
Development_User						
Development_Srvr						
Unknown						

Default_Policy:

Whitelist Model

Source		Destination				
		Production_User	Production_Srvr	Development_User	Development_Srvr	Unknown
Production_User						
Production_Srvr						
Development_User						
Development_Srvr						
Unknown						

Default_Policy:

Source		Destination				
		Production_User	Production_Srvr	Development_User	Development_Srvr	Unknown
Production_User						
Production_Srvr						
Development_User						
Development_Srvr						
Unknown						

Default_Policy:

Initial Brownfield Deployment

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

Cisco DNA Center Policy Whitelist vs Blacklist Model

Cisco DNA Center DESIGN **POLICY** PROVISION

Group-Based Access Control ▾ IP Based Access Control ▾ Traffic Copy ▾ Virtual Network

Policies (0) [Enter full screen](#) [GBAC Configuration](#)

Filter Deploy Refresh

■ Permit

■ Deny

■ Custom

□ Default

Source	Destination														
	Auditors	BYOD	Contractors	Developers	Development...	Employees	Extranet	Guests	Intranet	Network_Servi...	PCI_Servers	Point_of_Sale_...	Production_Ser...	Production_Us...	Quarantined_S...
Auditors															
BYOD															
Contractors															
Developers															
Development_Se...															

Default Policy

Action

Permit IP

Deny IP

Deny_IP_Log

Permit IP

Permit_IP_Log

Cancel

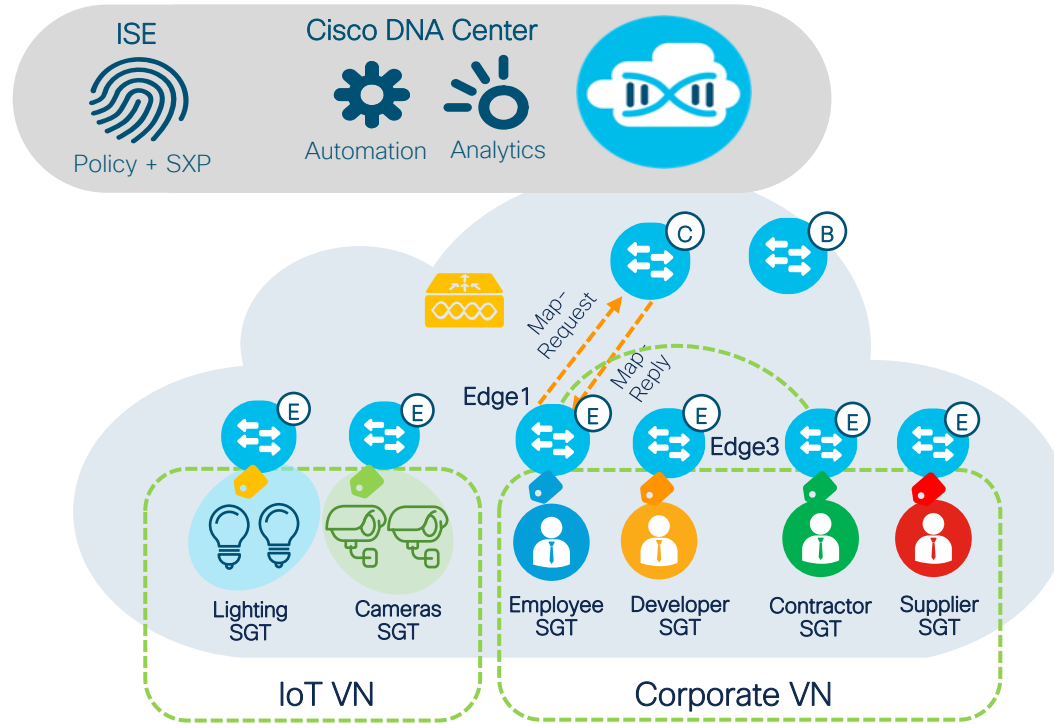
Save

Design & Integration

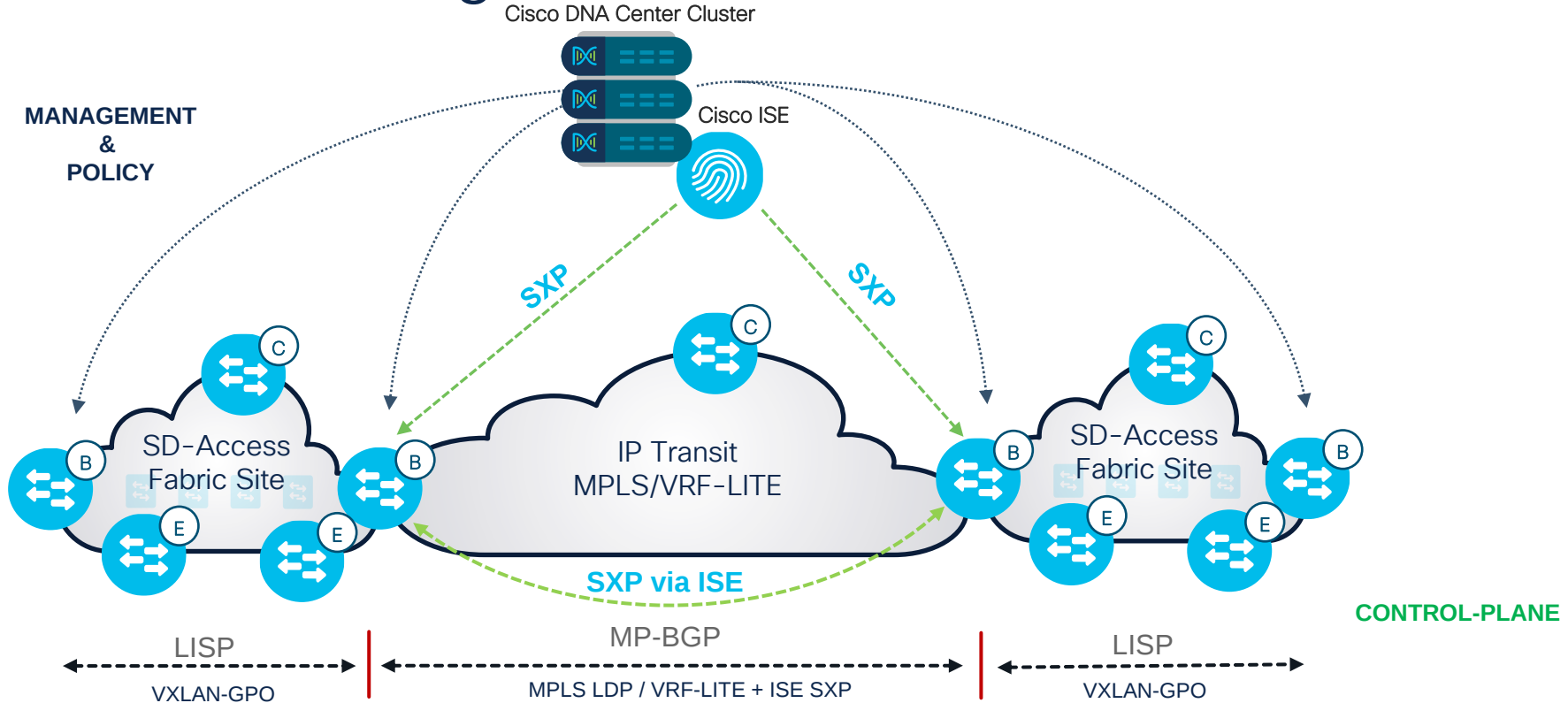


Single Site Design

Segmentation within the Fabric

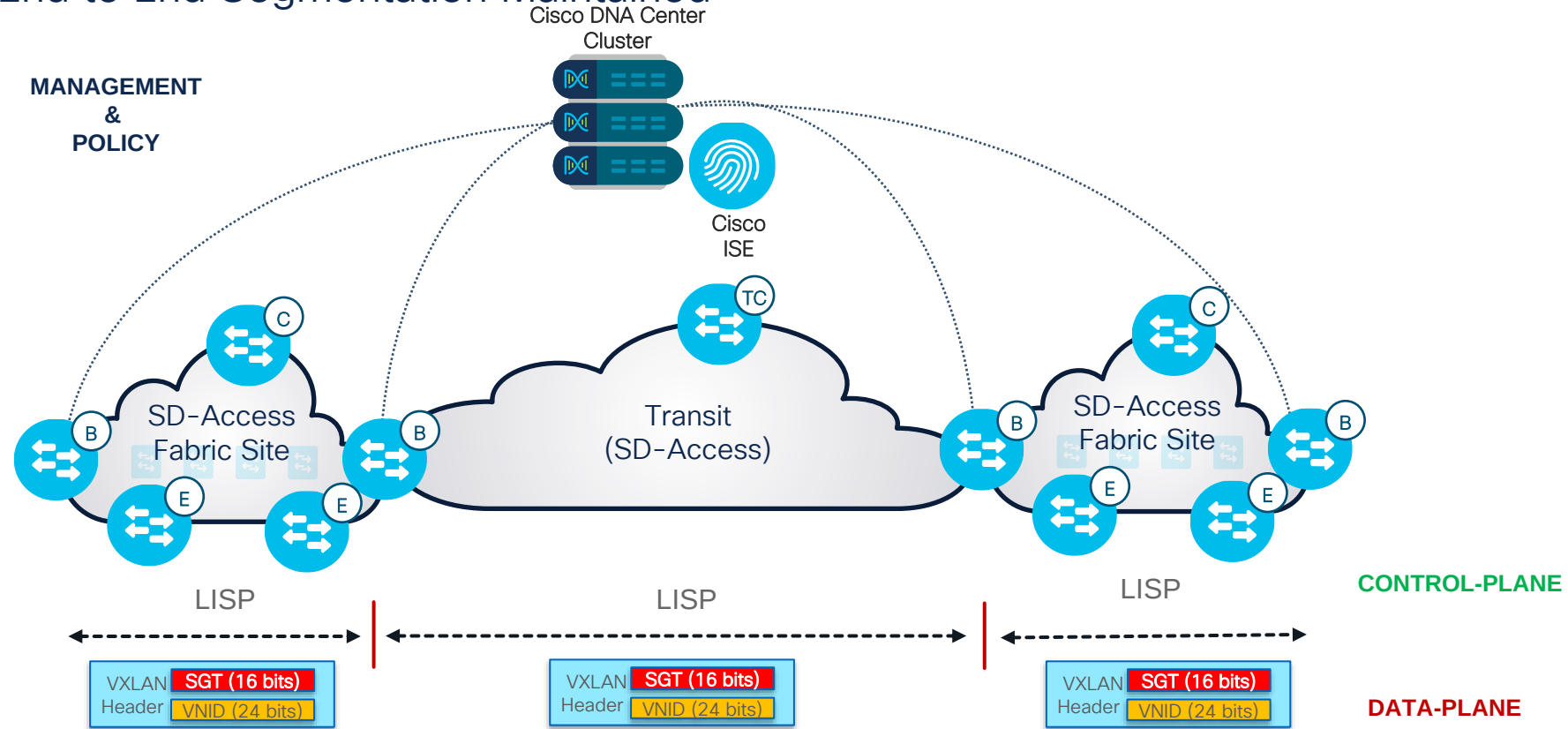


Multi-Site Design with IP Transit



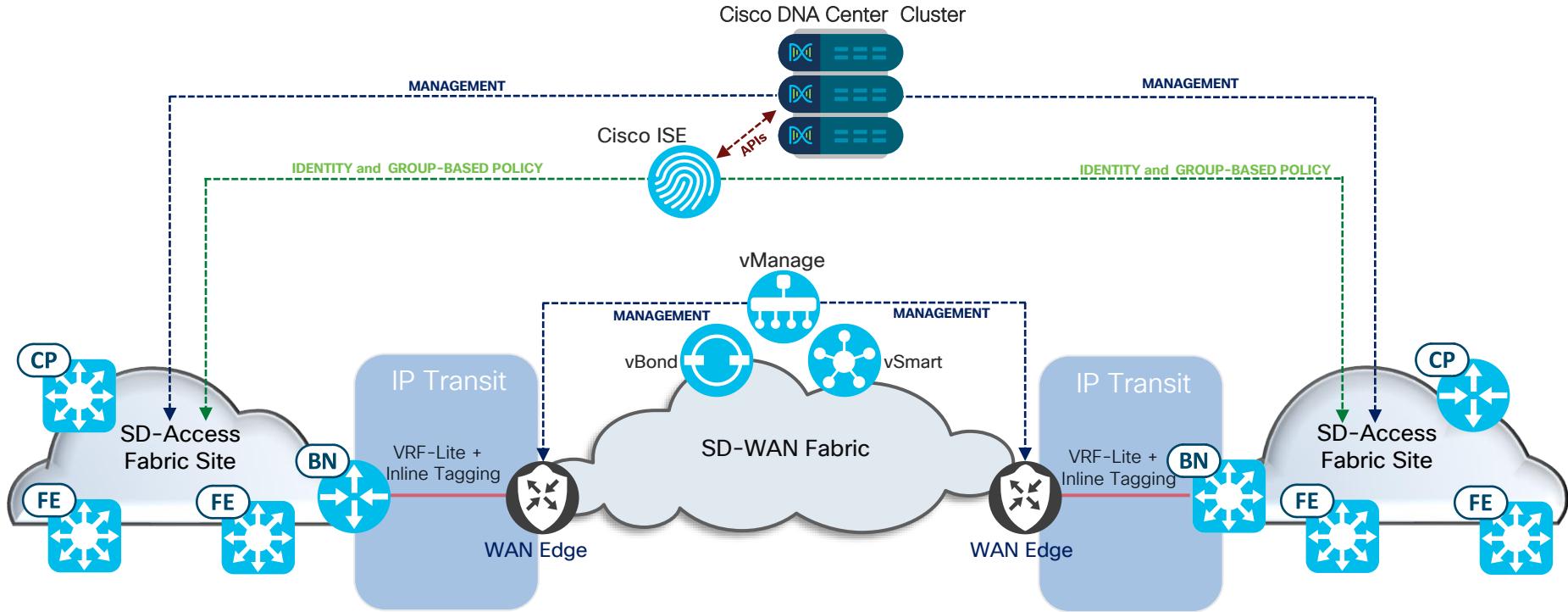
Multi-Site Design with SD-Access Transit

End to End Segmentation Maintained



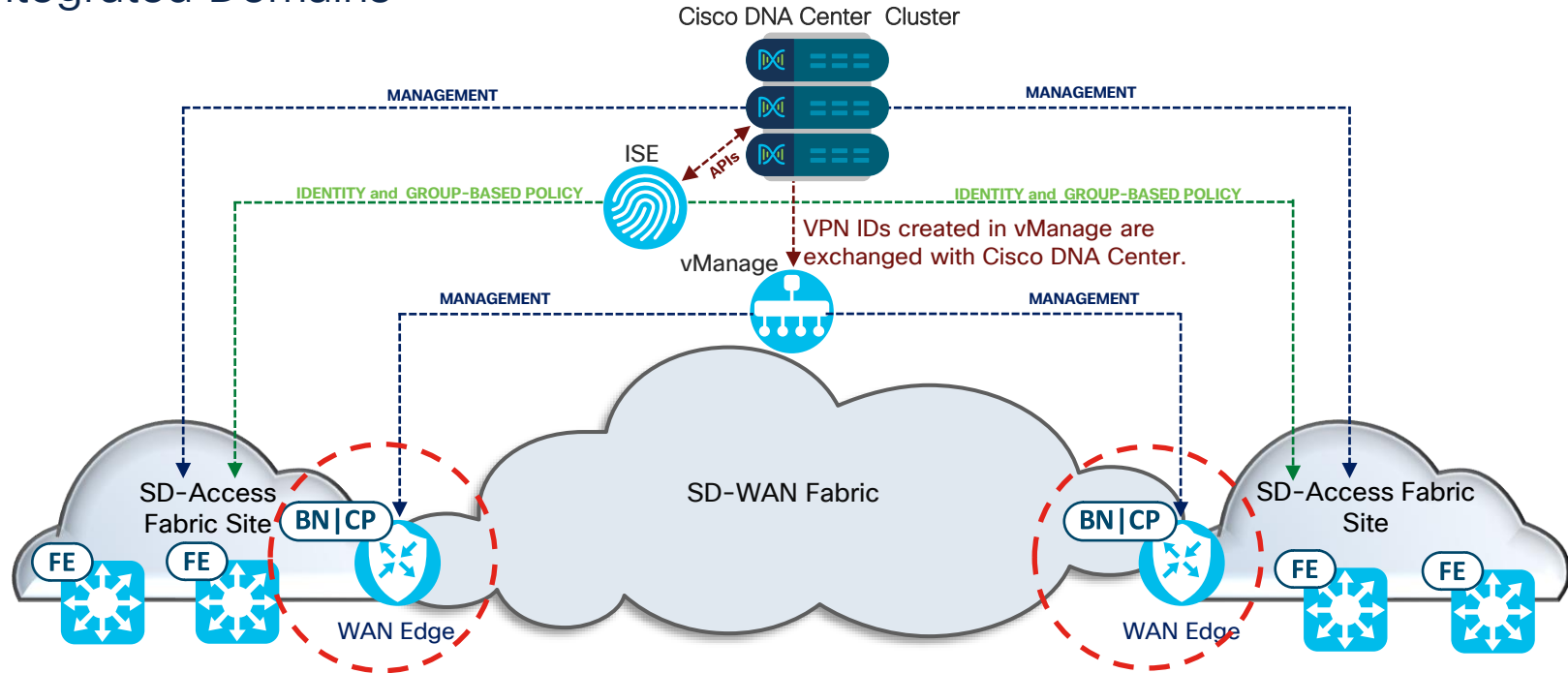
Multi-Site Design with SD-WAN Transport

Independent Domains



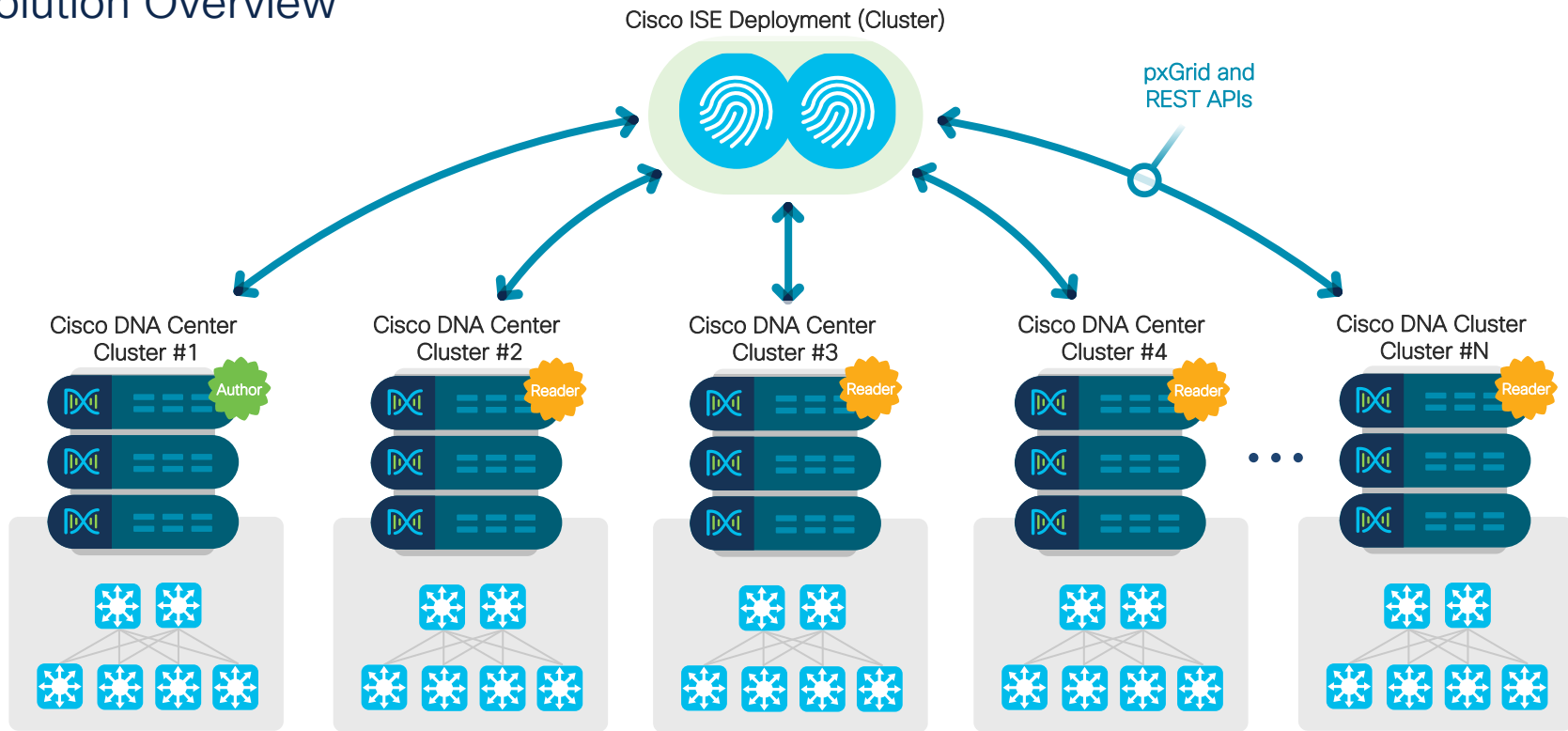
Multi-Site Design with SD-WAN Transit

Integrated Domains*



* - Limited Availability

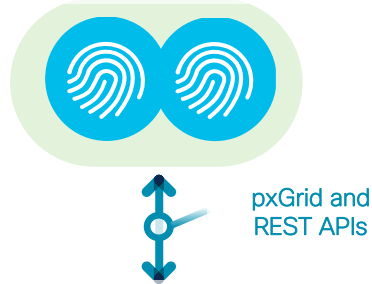
Multiple Cisco DNA Center Solution Overview



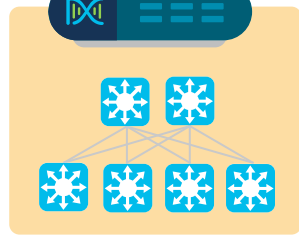
Multiple Cisco DNA Center

Author Node Cluster

Cisco ISE Deployment (Cluster)



Cisco DNA Center Cluster



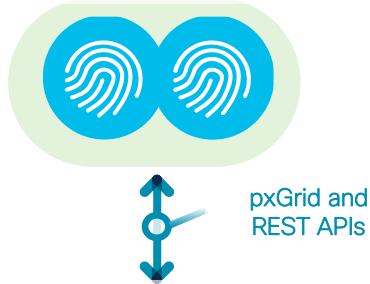
Intent-based Network Infrastructure

- 1st Cisco DNA Cluster to integrate 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 DNA Center Cluster

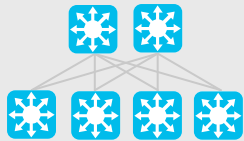
Multiple Cisco DNA Center

Reader Node Cluster

Cisco ISE Deployment (Cluster)



Cisco DNA Center Cluster



Intent-based Network Infrastructure

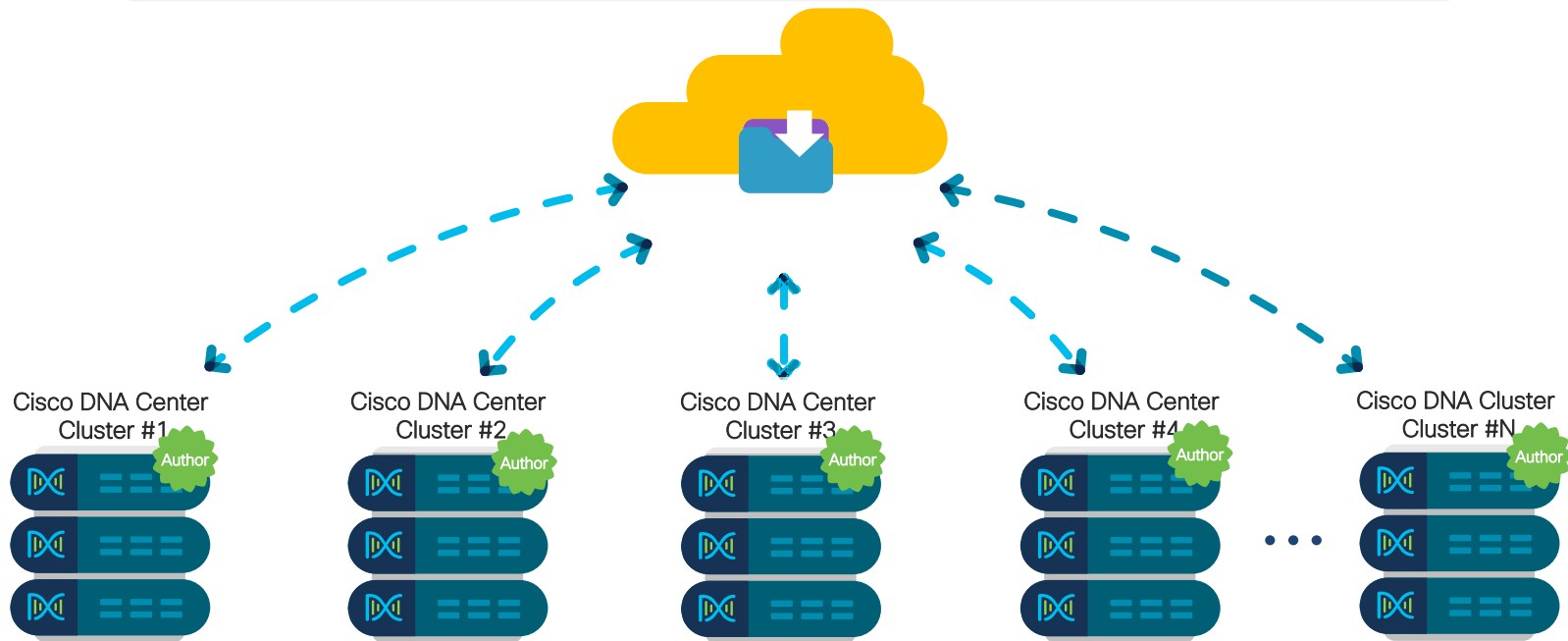
- Subsequent DNA Cluster to integrate with Cisco ISE
- Up to 4 Cisco DNA Center Center Clusters can be added as Reader Node Clusters.
- Read only view of VN, SGTs, Access Contracts, GBAC Policy and VN-SGT Associations
- Can only be a Greenfield Cisco DNA Center Cluster

Multiple Cisco DNA Center

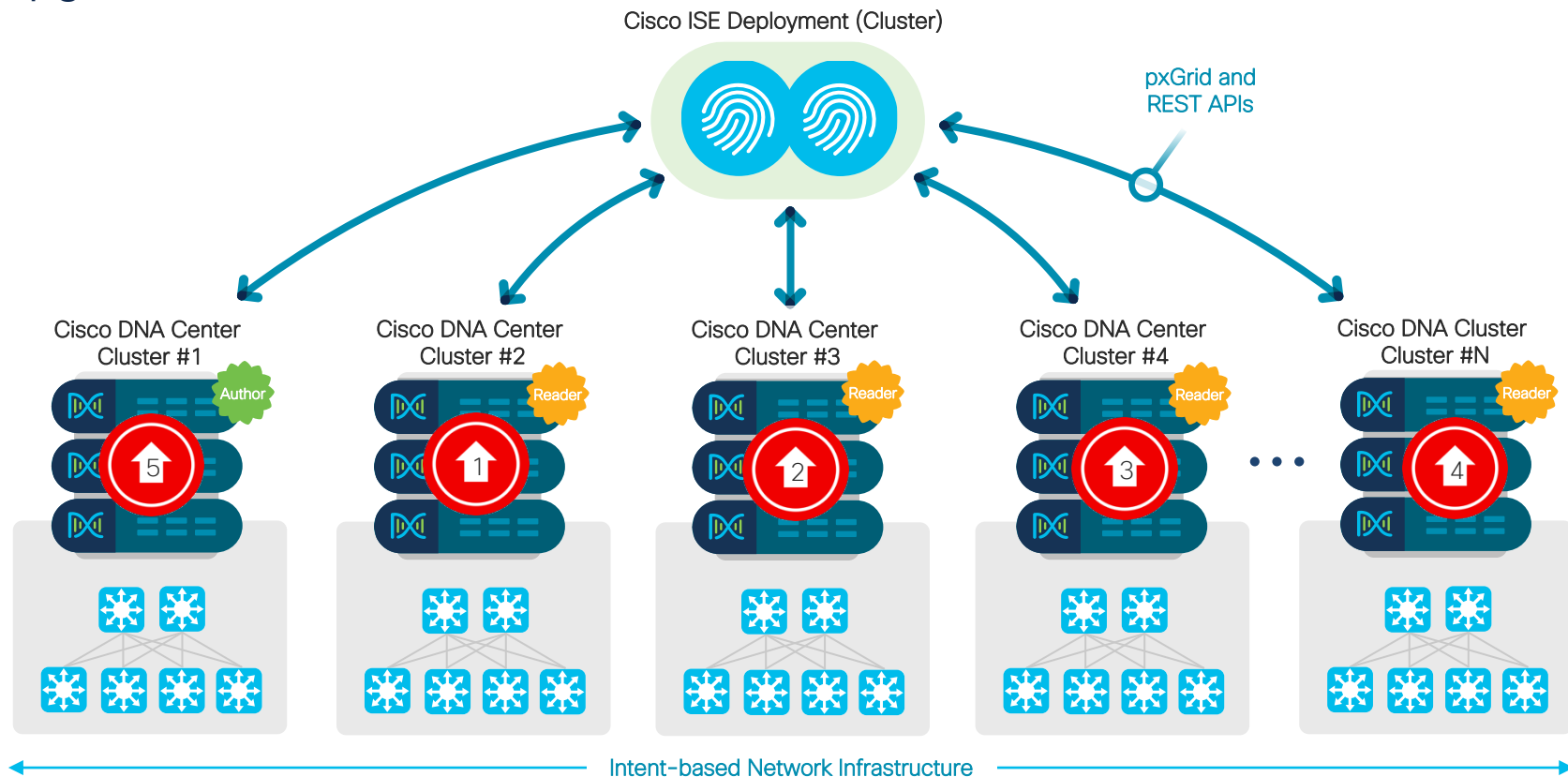
Multiple Cisco DNA Center Package and Installation

Connect with your Cisco Sales Representative or Channel Partner for:

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



Multiple Cisco DNA Center Upgrade Recommendations



Cisco ISE and APIC

Consistent Policies Across Enterprise

Identity Services Engine / DNA Center



Security



APIC-DC, Controller for ACI

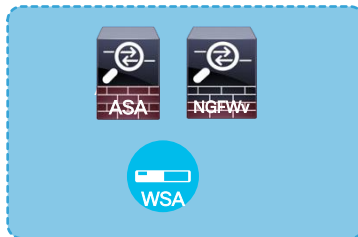


Common Policy Groups

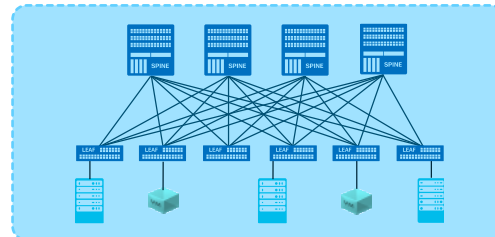
Campus & Branch Networks



Security Apps



ACI DC/Cloud



- Consistent Security Policy Groups in SD-Access and ACI domains
- Groups from SD-Access used in ACI policies, groups from ACI available in SD-Access policies

Cisco ISE and APIC

Groups provisioned from SD-Access to ACI

DNA CENTER DESIGN POLICY PROVISION

Dashboard **Group-Based Access Control** IP Based Access Control

Group-Based Access Control Policies **Scalable Groups** Access Contract

Filter

State is ACTIVE

Name	Virtual Network
Auditors	DEFAULT_VN
BYOD	DEFAULT_VN
CANADASGT	DEFAULT_VN
CBASGT	DEFAULT_VN
CloudSvrs	DEFAULT_VN
Contractors	DEFAULT_VN
Developers	DEFAULT_VN
Development_Servers	DEFAULT_VN
Employees	DEFAULT_VN

ISE dynamically provisions SGTs and IP mappings into ACI

Tenant Pod01

L3out

Logical Node Profiles

Networks

- Auditors_SGT
- BYOD_SGT
- Contractors_SGT
- Developers_SGT
- Development_Servers_SGT
- Employees_SGT
- Guests_SGT
- Network_Services_SGT
- PCI_Servers_SGT
- Point_of_Sale_Systems_SGT
- Production_Servers_SGT
- Production_Users_SGT
- Quarantined_Systems_SGT
- Test_Servers_SGT
- TrustSec_Devices_SGT
- default

Networks

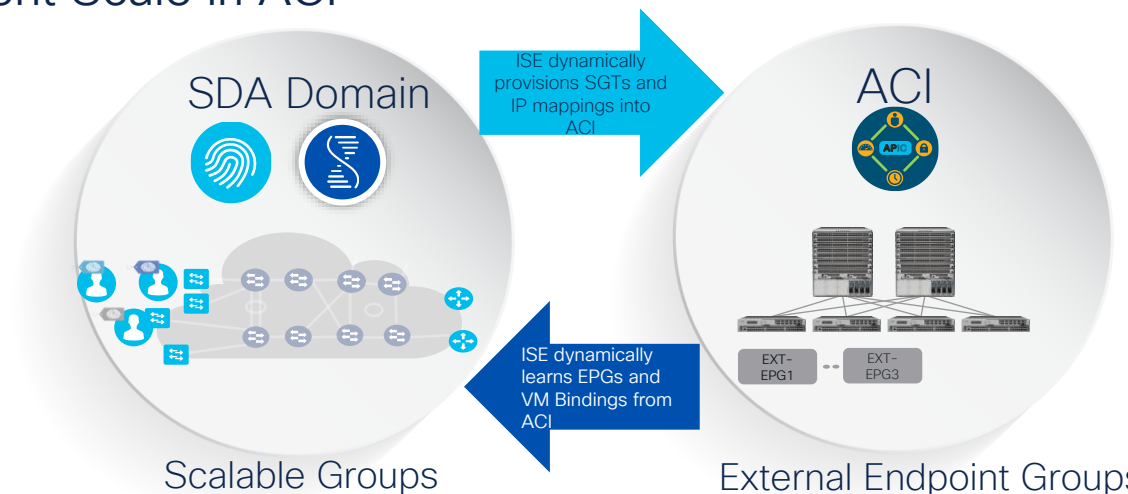
Name

- Auditors_SGT
- BYOD_SGT
- Contractors_SGT
- default
- Developers_SGT
- Development_Servers_SGT
- Employees_SGT
- Guests_SGT
- Network_Services_SGT
- PCI_Servers_SGT
- Point_of_Sale_Systems_SGT
- Production_Servers_SGT
- Production_Users_SGT
- Quarantined_Systems_SGT
- Test_Servers_SGT
- TrustSec_Devices_SGT

Cisco ISE and APIC

Enforcement Scale in ACI

Recommend
ISE 2.4 patch 6 or 2.6



Fusion platforms capable of > 250k Mappings include:
ASR, ISR4k, C6800, ASA and FirePower Appliances

ACI 3.2 Scale EX, FX and FX2 Hardware

ISE/SD-Access Scale	
Numbers of Groups	1000
Number of Mappings*	250k
SXP Peers*	200
pxGrid Peers**	200

*Per pair of ISE SXP Nodes

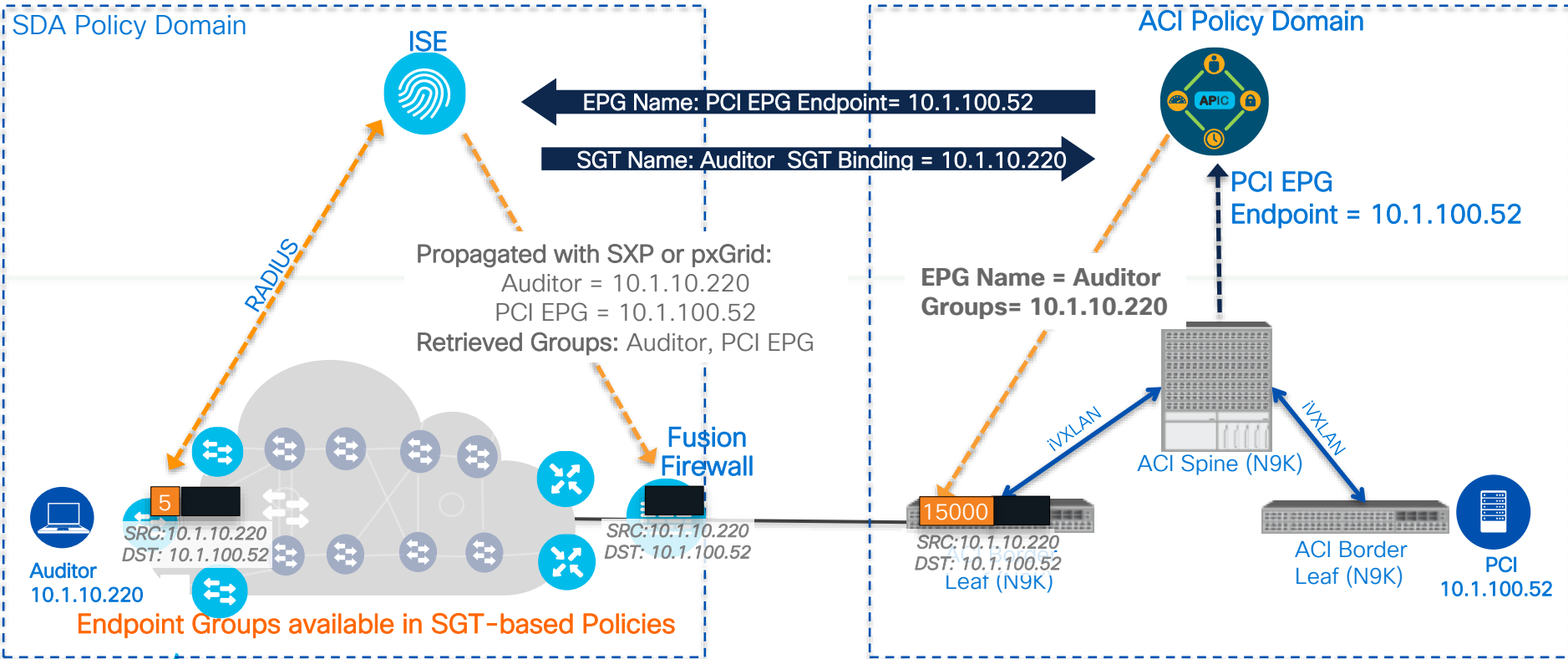
** Per ISE pxGrid node

BRKENS-2814

SGT -> External EPG	250
Number of Mappings	64,000
Mappings per External EPG	8000
Transaction rate (target)	100/s

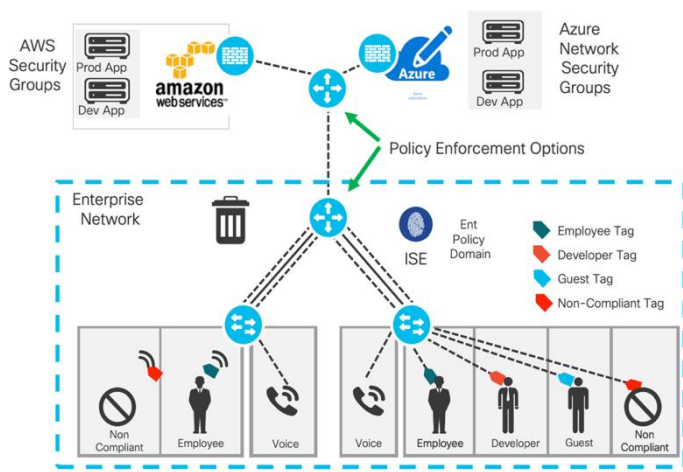
Cisco ISE and APIC

ACI Groups used in SD-Access(Border or Fusion)



Access Control :

SD-Access to Cloud



- Policy enforced in enterprise network OR Virtual Firewall or SGACL-capable virtual routers in cloud environments • e.g ASAv, CSR-1000v, ISRv
- Workloads / groups provisioned by Cisco or 3rd party orchestration tools • Orchestration tool can push IP-SGT bindings to ISE REST APIs
- ISE SXP updates enforcement points
- Avoids policy changes as new workloads are provisioned in clouds

Business Benefits



Simplify
Policy



Increase
Efficiency



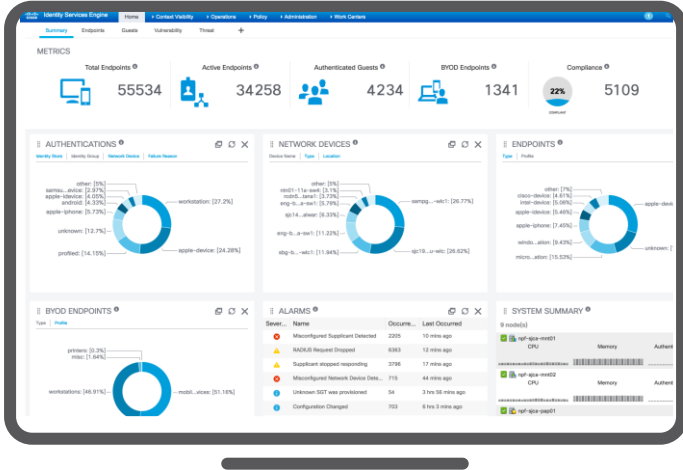
Regulatory
Compliance



Reduce
OPEX

CISCO *Live!*

Cisco ISE is a key piece in the SD-Access Architecture



MOBILITY 

MICRO SEGMENTATION

SECURITY 

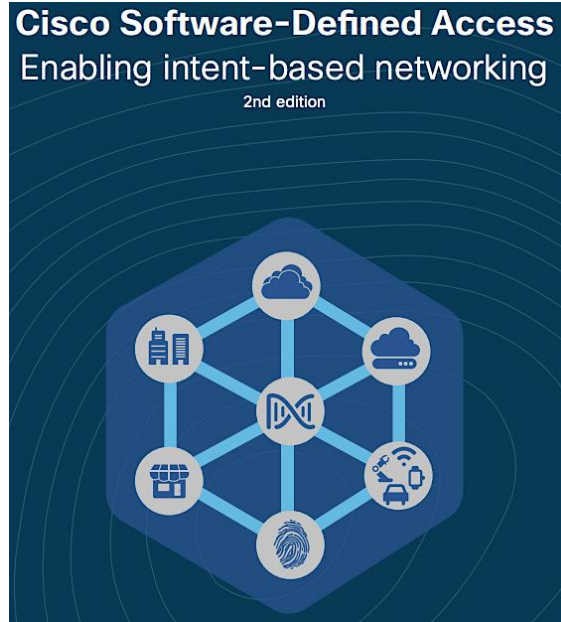
DEVICE ADMIN (TACACS+)

MULTI DOMAIN INTEGRATION 

Cisco Solution e-books

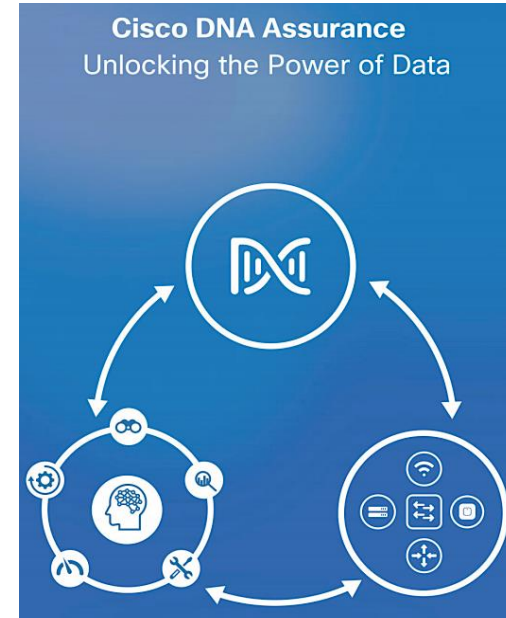
Cisco Software-Defined Access

Enabling intent-based networking



Cisco DNA Assurance

Unlocking the Power of Data



Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



Learn

Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train

Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify

Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

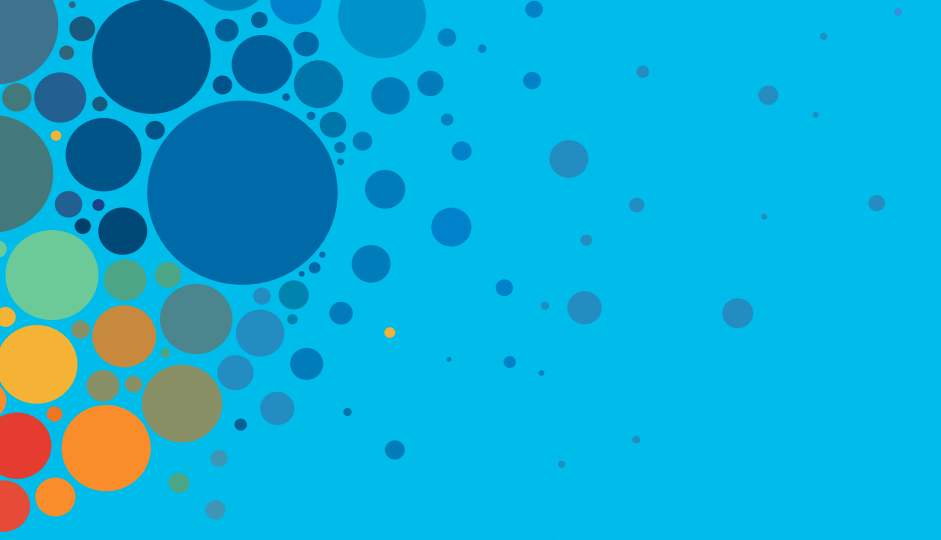
Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer 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



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive