
cisco Live!
ALL IN

The bridge to possible

Cisco ISE in SD-Access Network

Mahesh Nagireddy
Technical Marketing Engineering, Technical Leader
CCIE R&S

BRKENS-2814

cisco Live!

#CiscoLive

Cisco Webex App

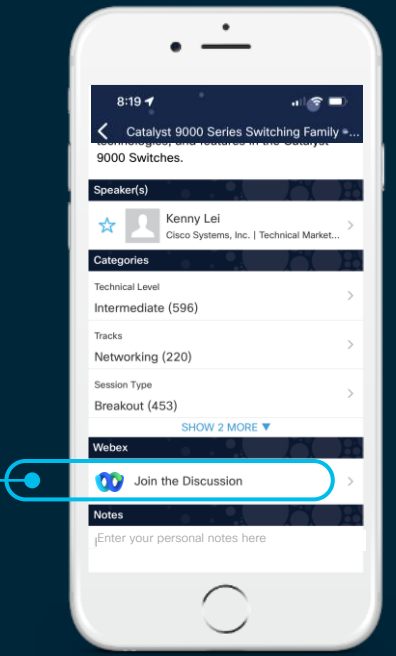
Questions?

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

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!

FINISH

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

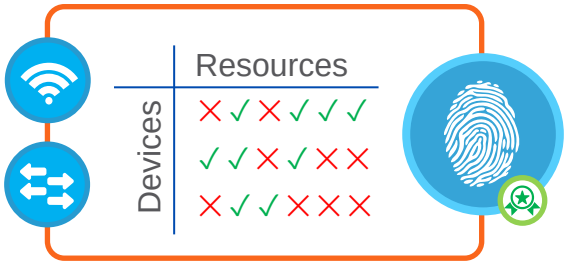
What are the challenges of networks without SD-Access?

Network deployment challenges

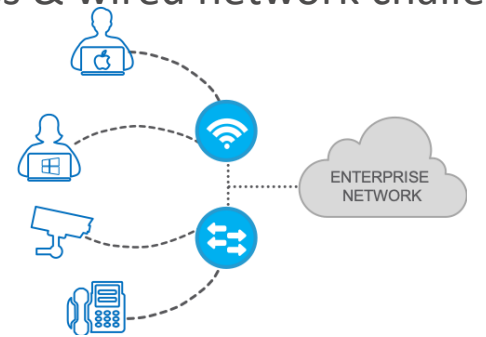
Network Infrastructure

Switching Routers Wireless

Network security challenges



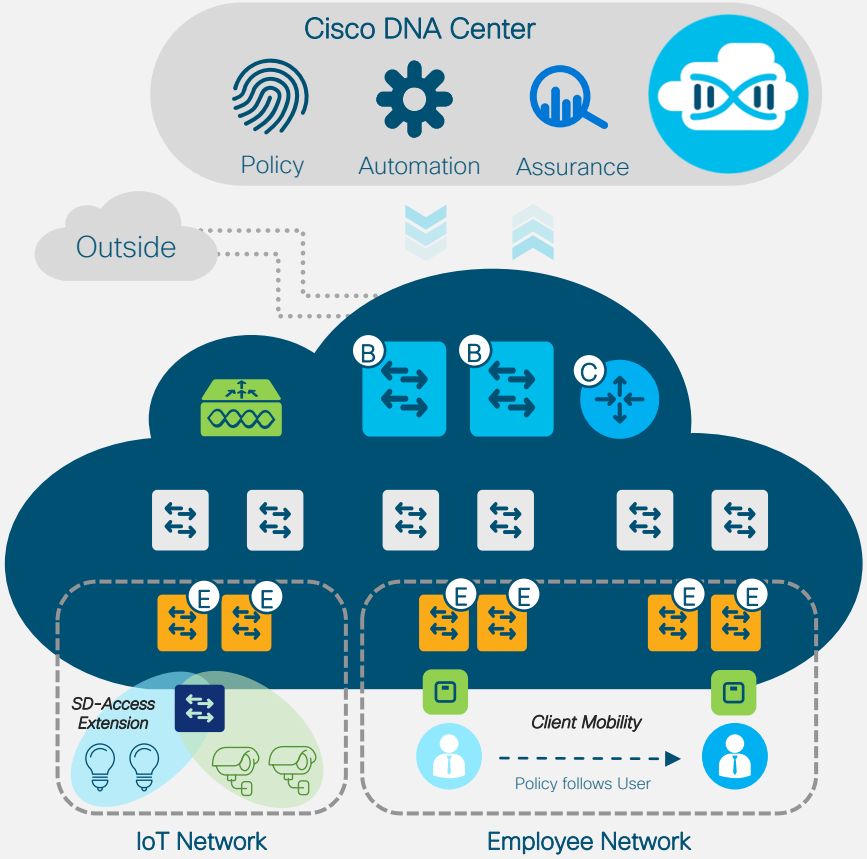
Wireless & wired network challenges



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

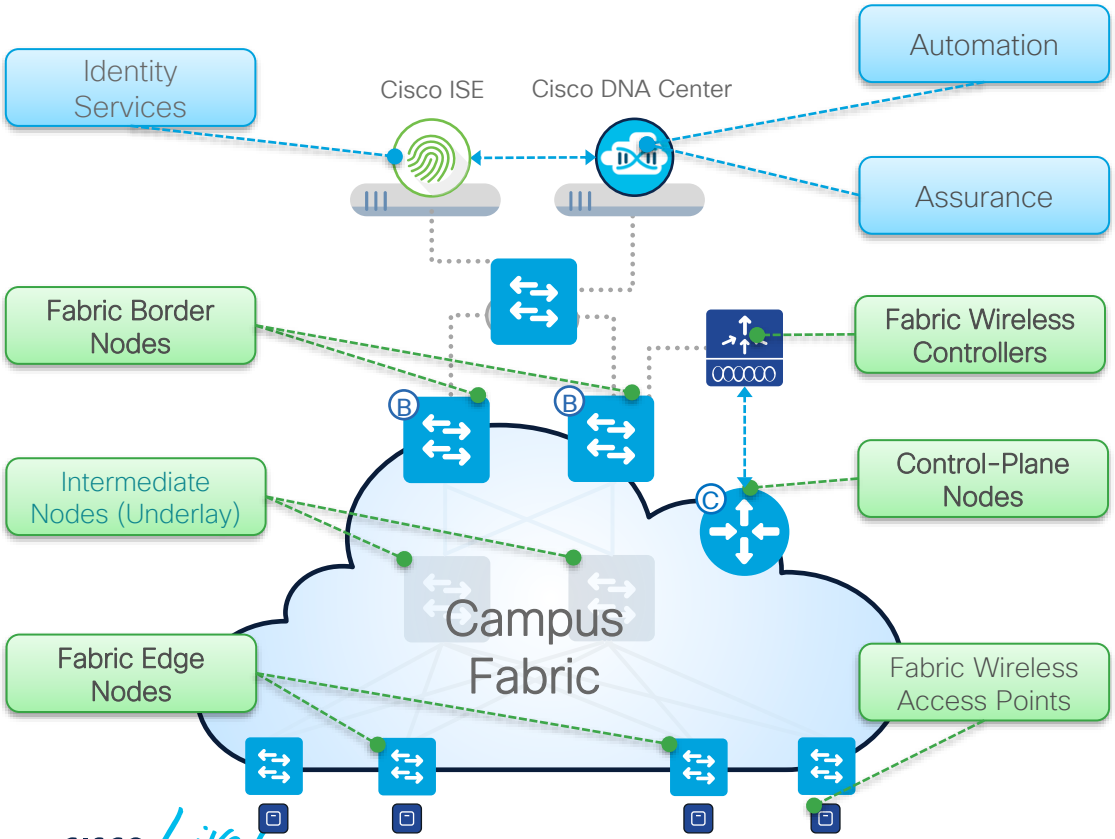
Enhance Security and Compliance

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

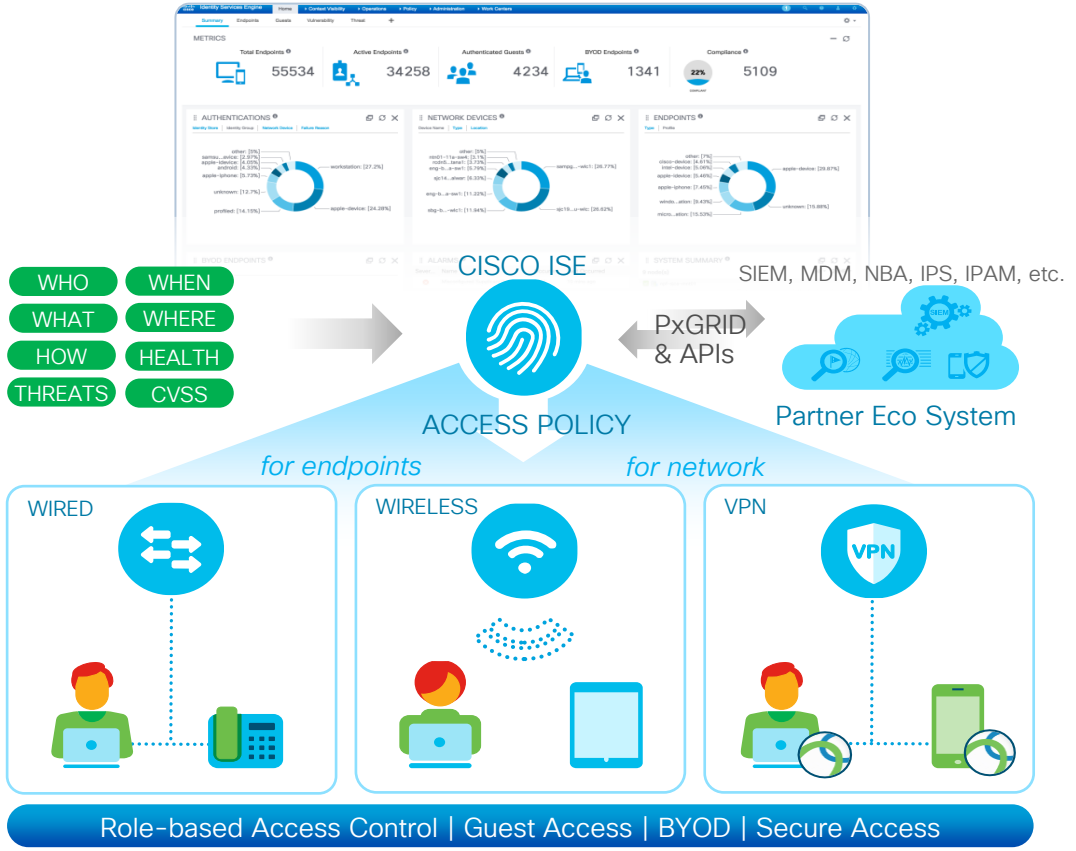
Cisco ISE Overview
Value of Cisco ISE

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

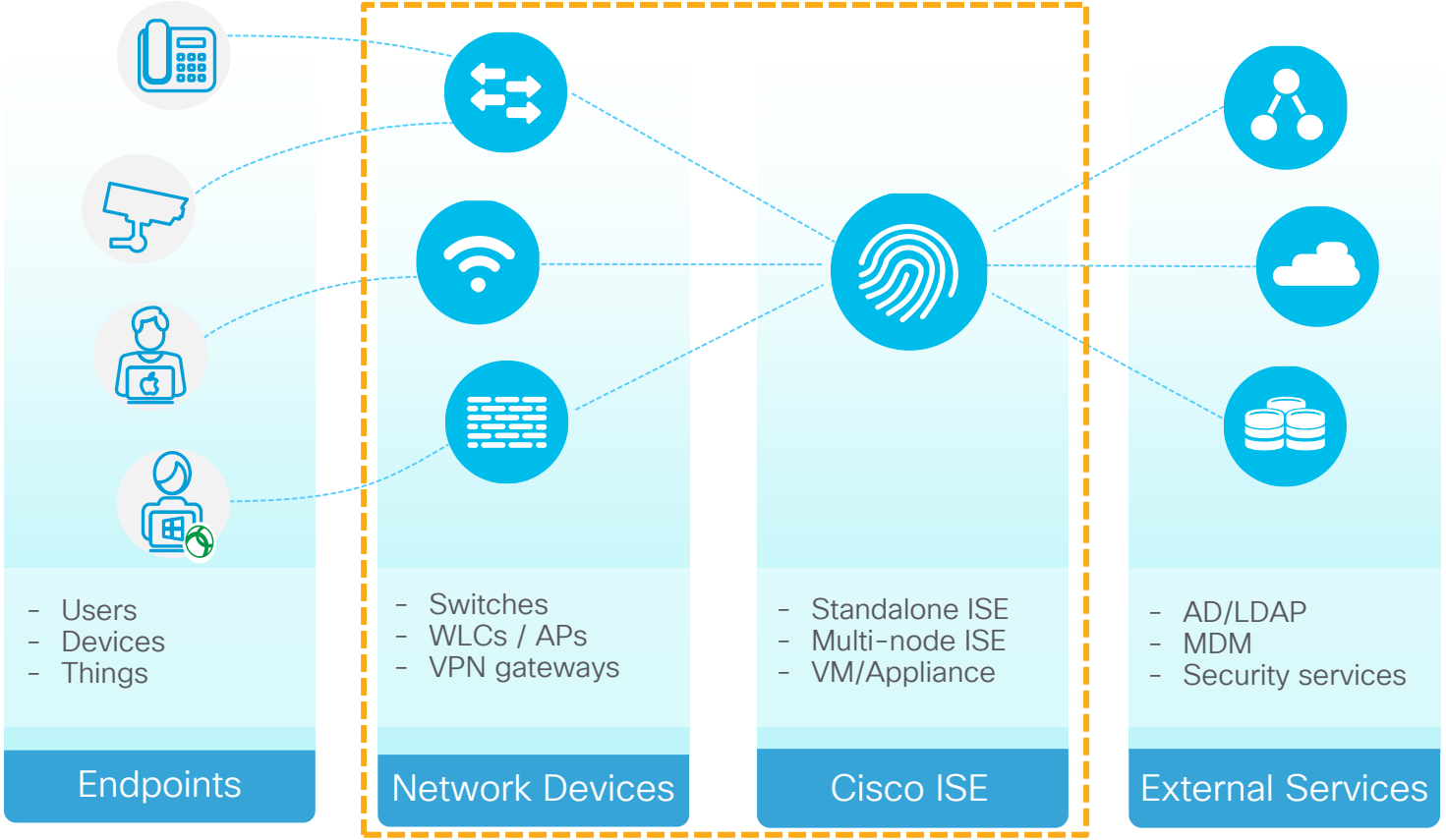
See
Users, endpoints and applications

Secure
By controlling network access and segmentation

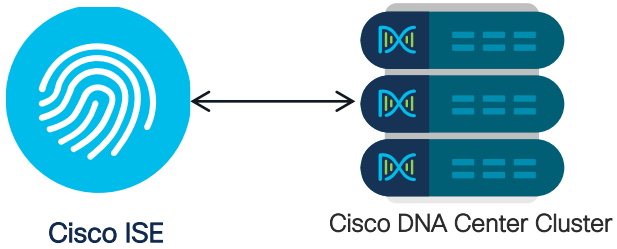
Share
Context with partners for enhanced operations



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

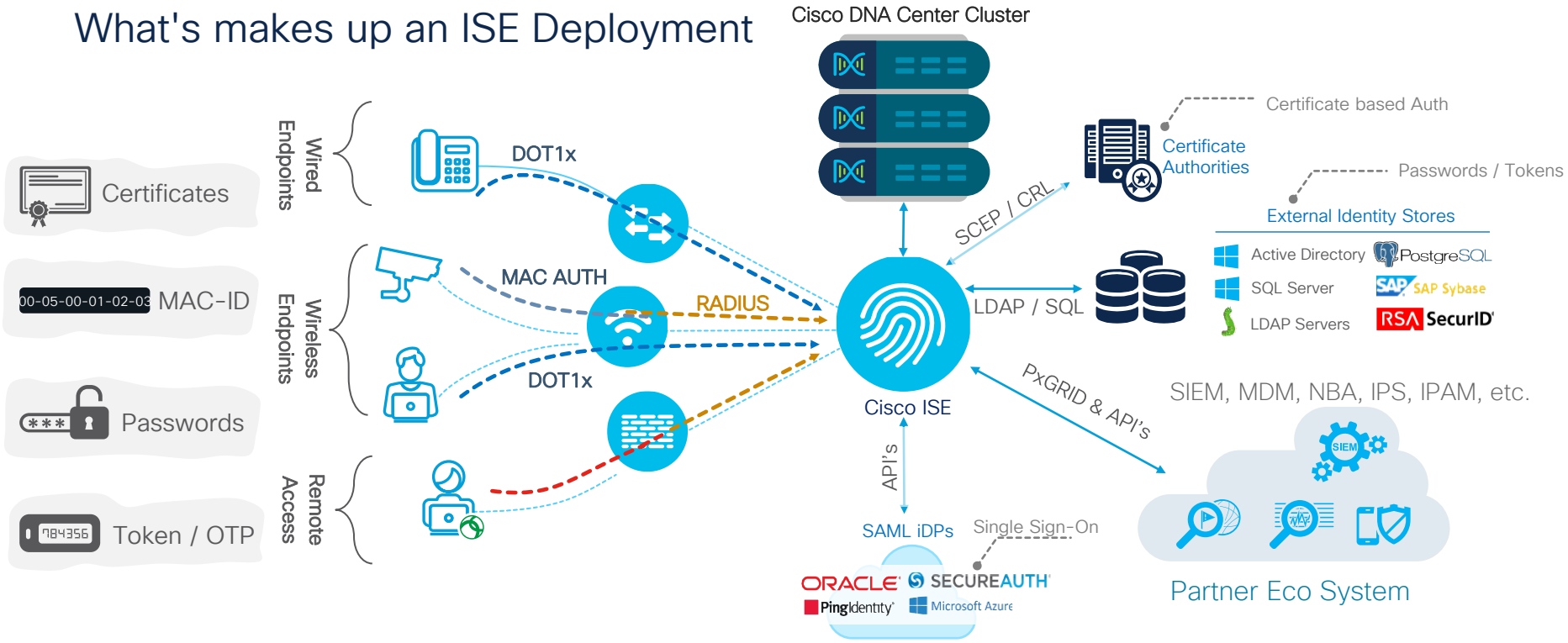
Guest Access Steps

Cisco WLC	Cisco ISE	DNA-Center
Create Guest WLAN	Setup Self-registration Guest Portal	Add a Guest Wireless SSID
ADD AAA Servers	Create Authorization Profile	Select Authentication Type(Web Auth) & ISE as Authentication Server
Enable AAA Override	Create Authentication Rules	Setup Self Registration Portal/Hotspot Portal
Create Redirect ACL		Setup Wireless Profile(Fabric SSID, Anchoring/Switching mode, VLAN,

ISE role in SD-Access Architecture

ISE in SD-Access

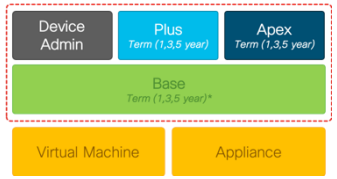
What's makes up an ISE Deployment

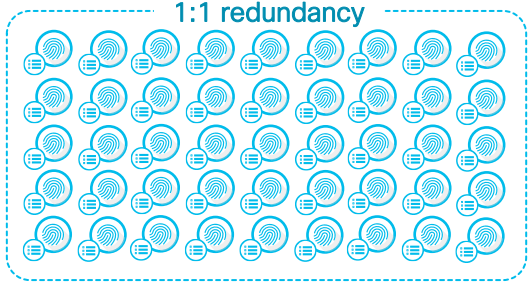


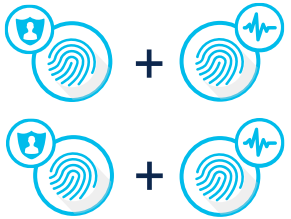
AAA, Policy-Based Segmentation and Context Sharing

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)

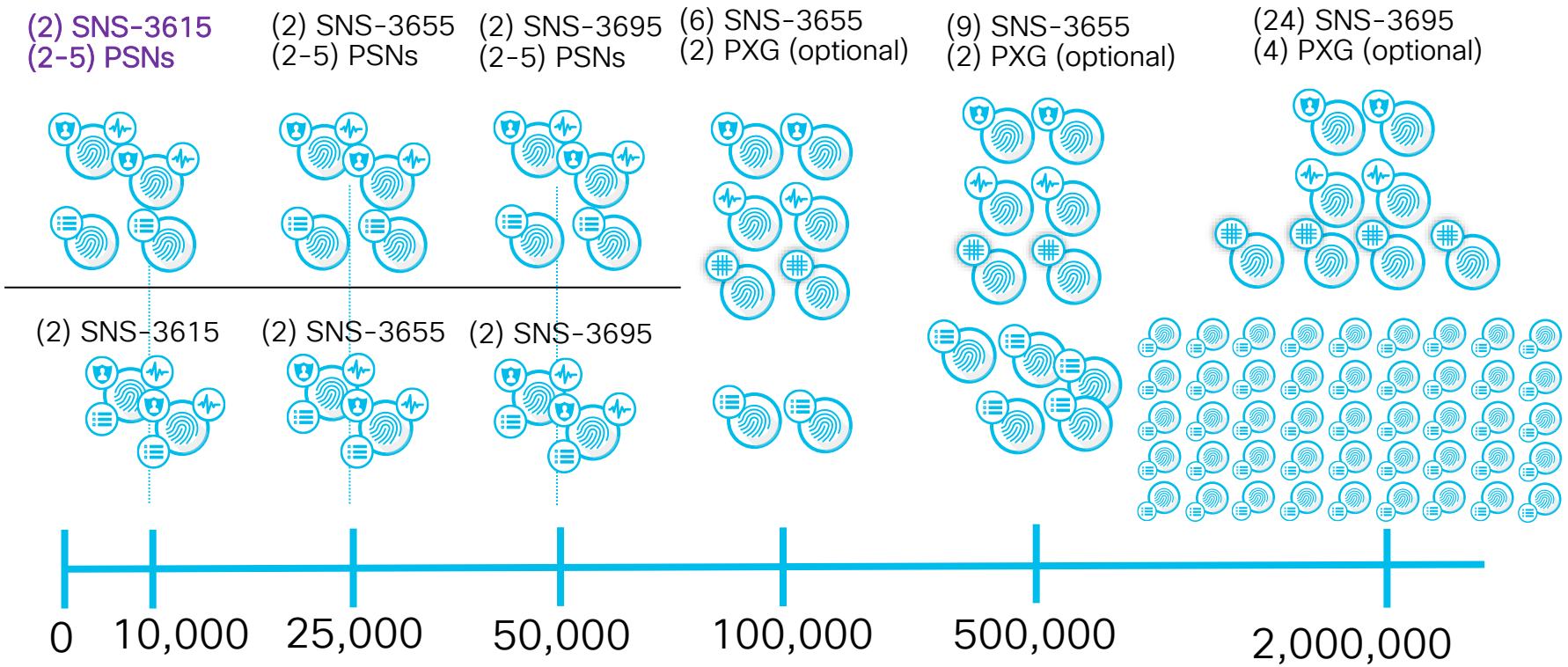
NEW

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

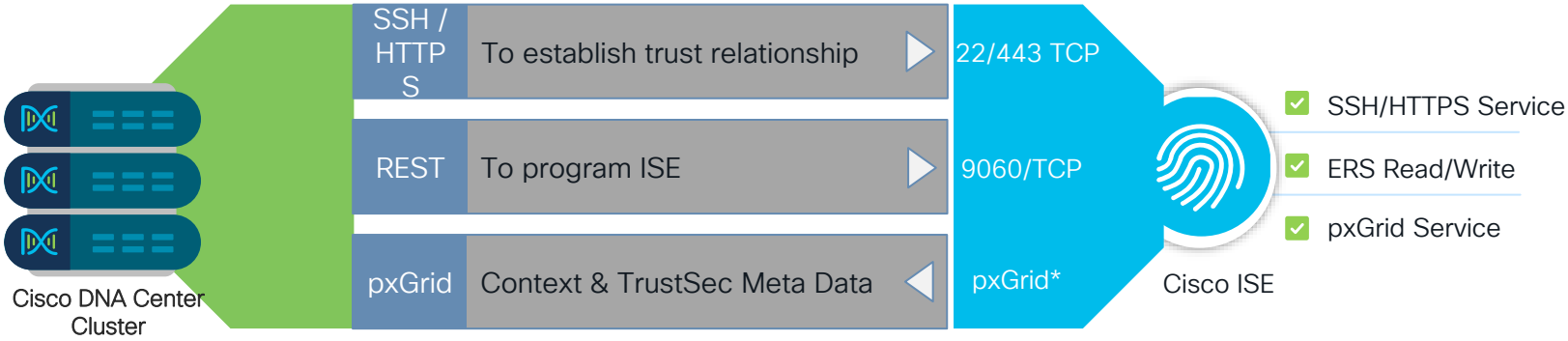
Session Scaling by Deployment Model 36xx

NEW



- 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***

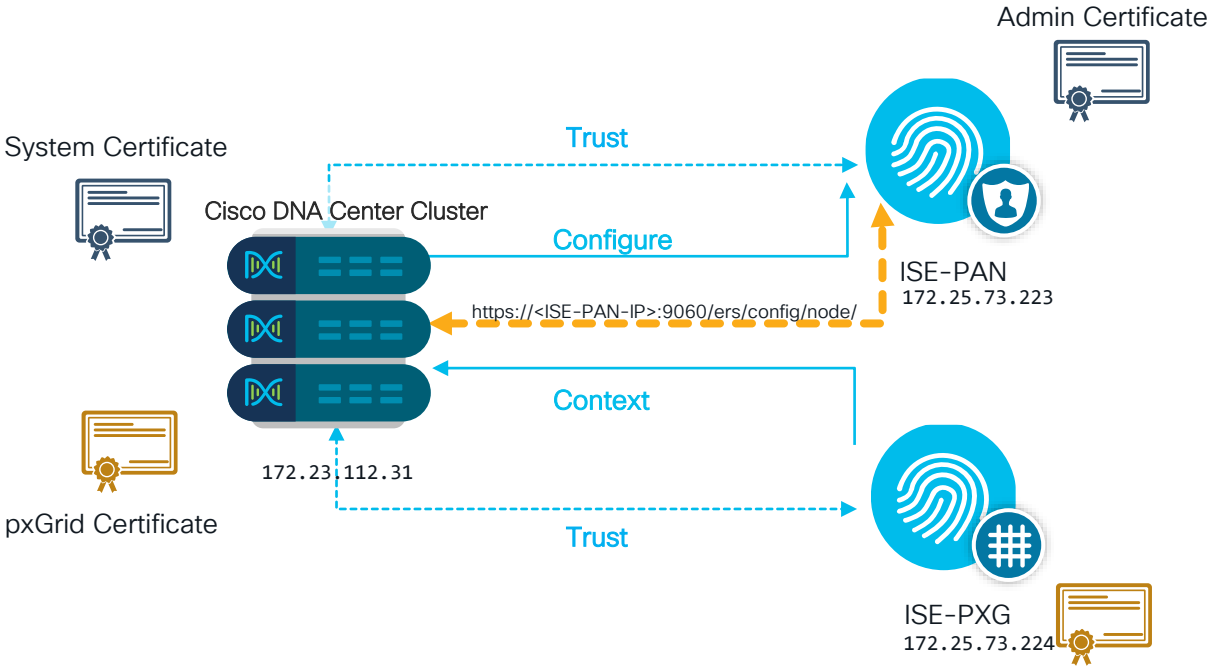
Enable *ERS for Read on* ***All other Nodes*** *incase of Distributed model*

ISE GUI password matches ISE CLI password

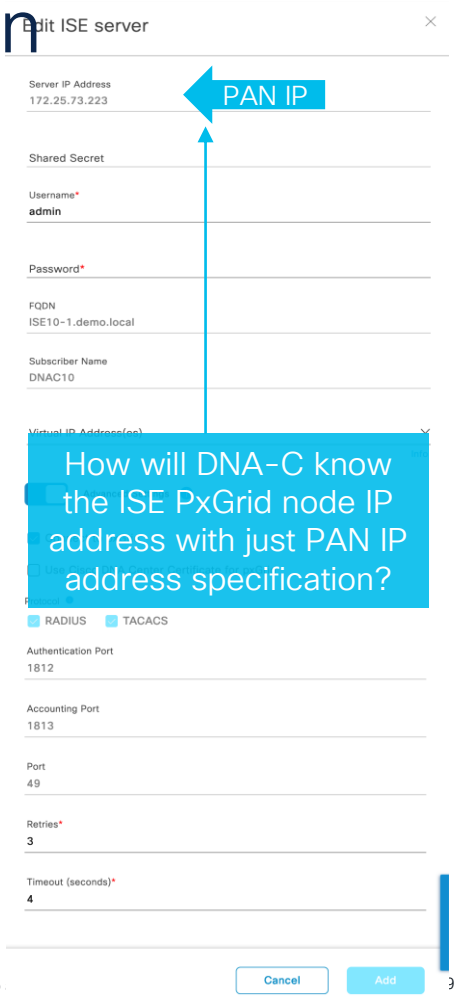
Cisco DNA Center and ISE Integration

How DNA Center Trust PxGrid Node

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

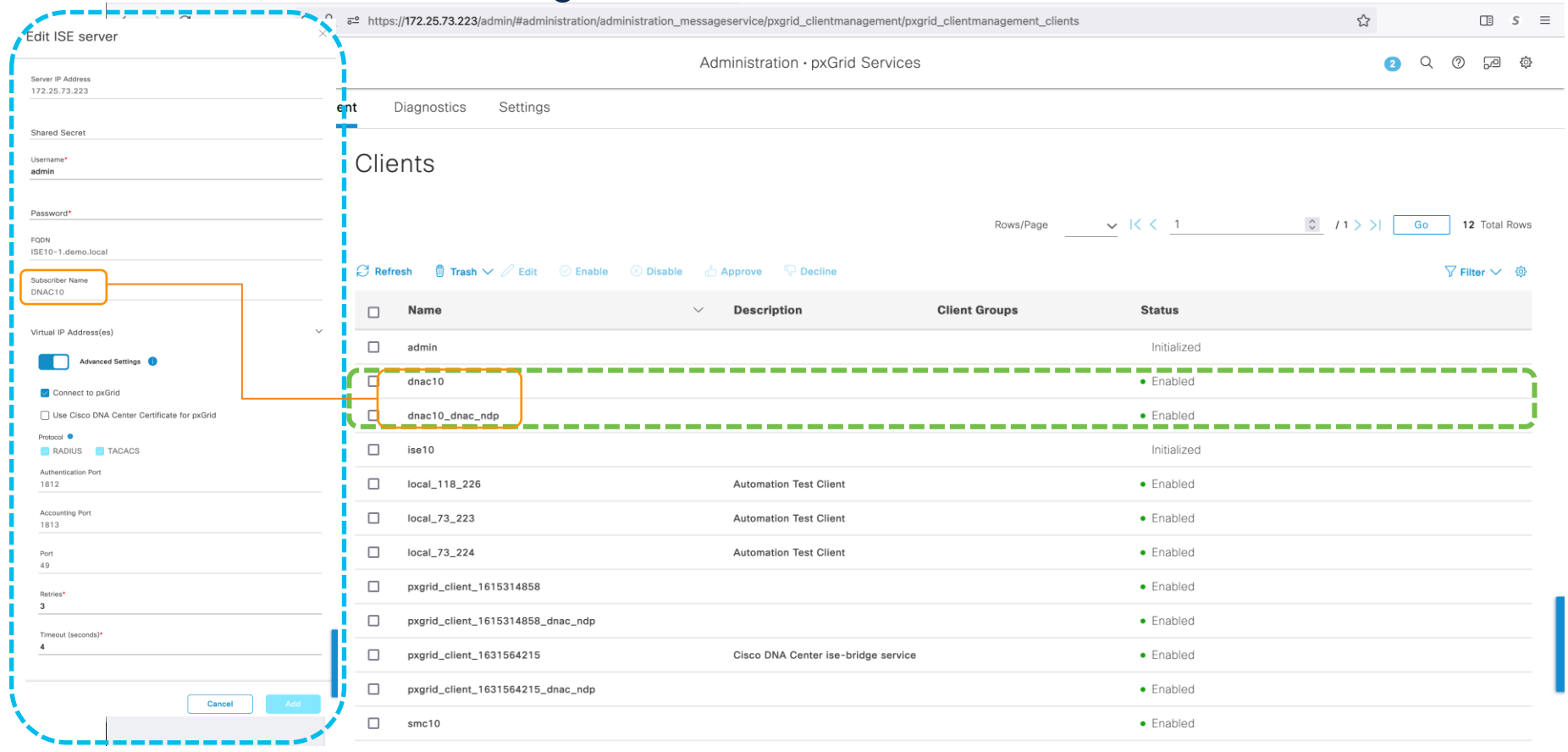


Add AAA/ISE server

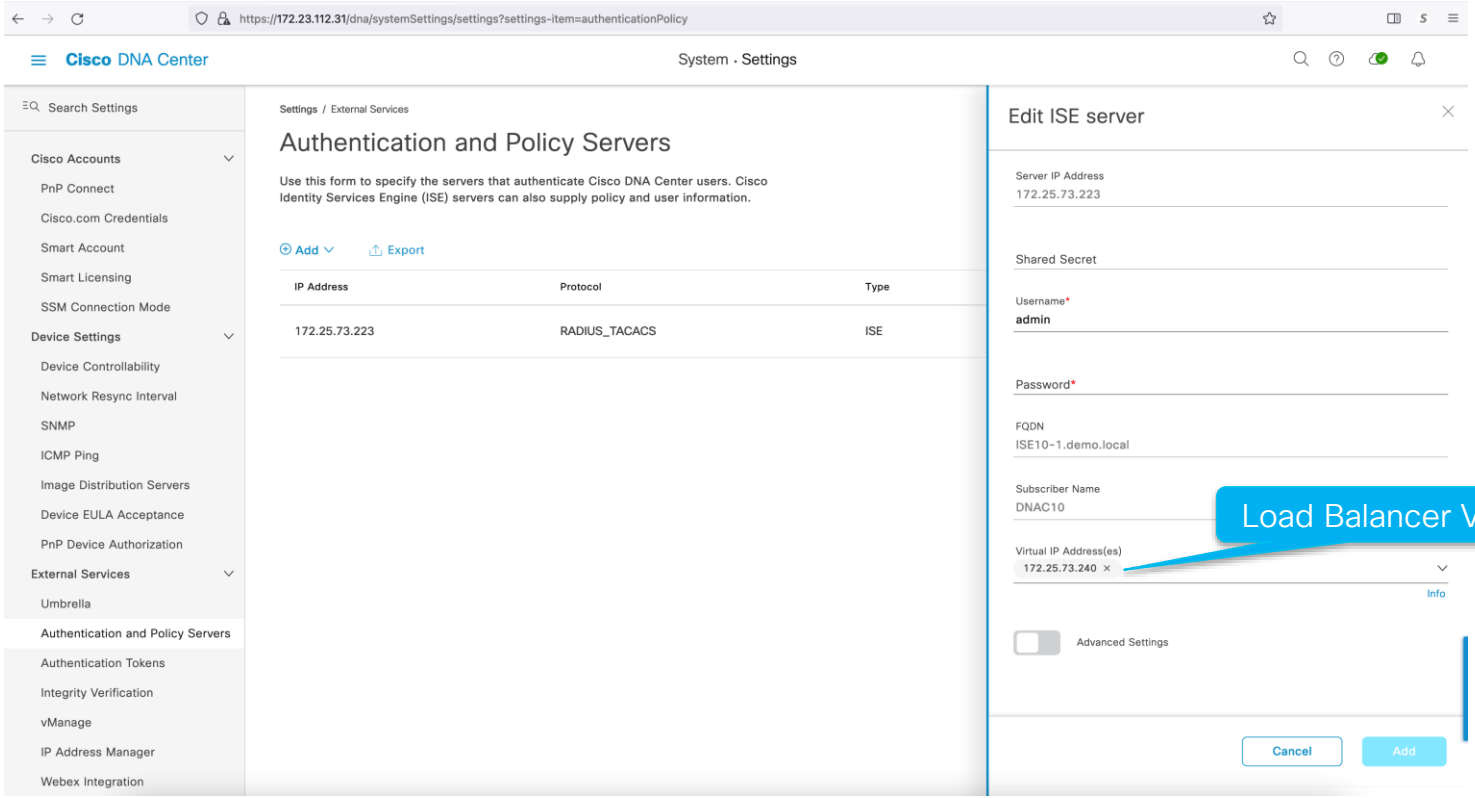


Cisco DNA Center Setting

DNA Center and ISE Integration

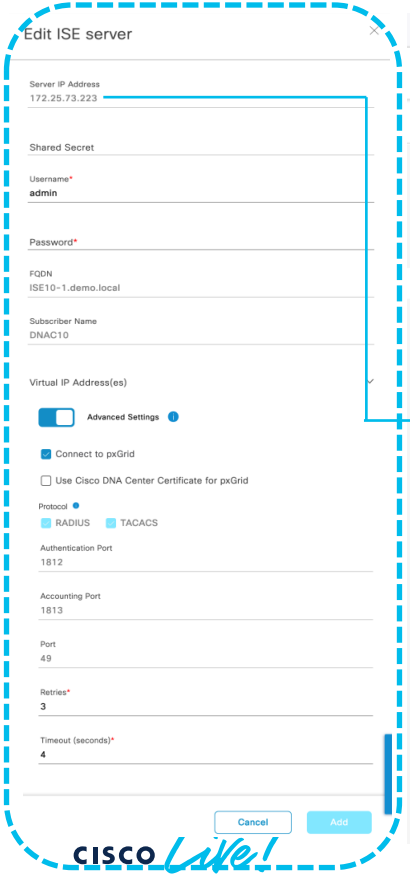


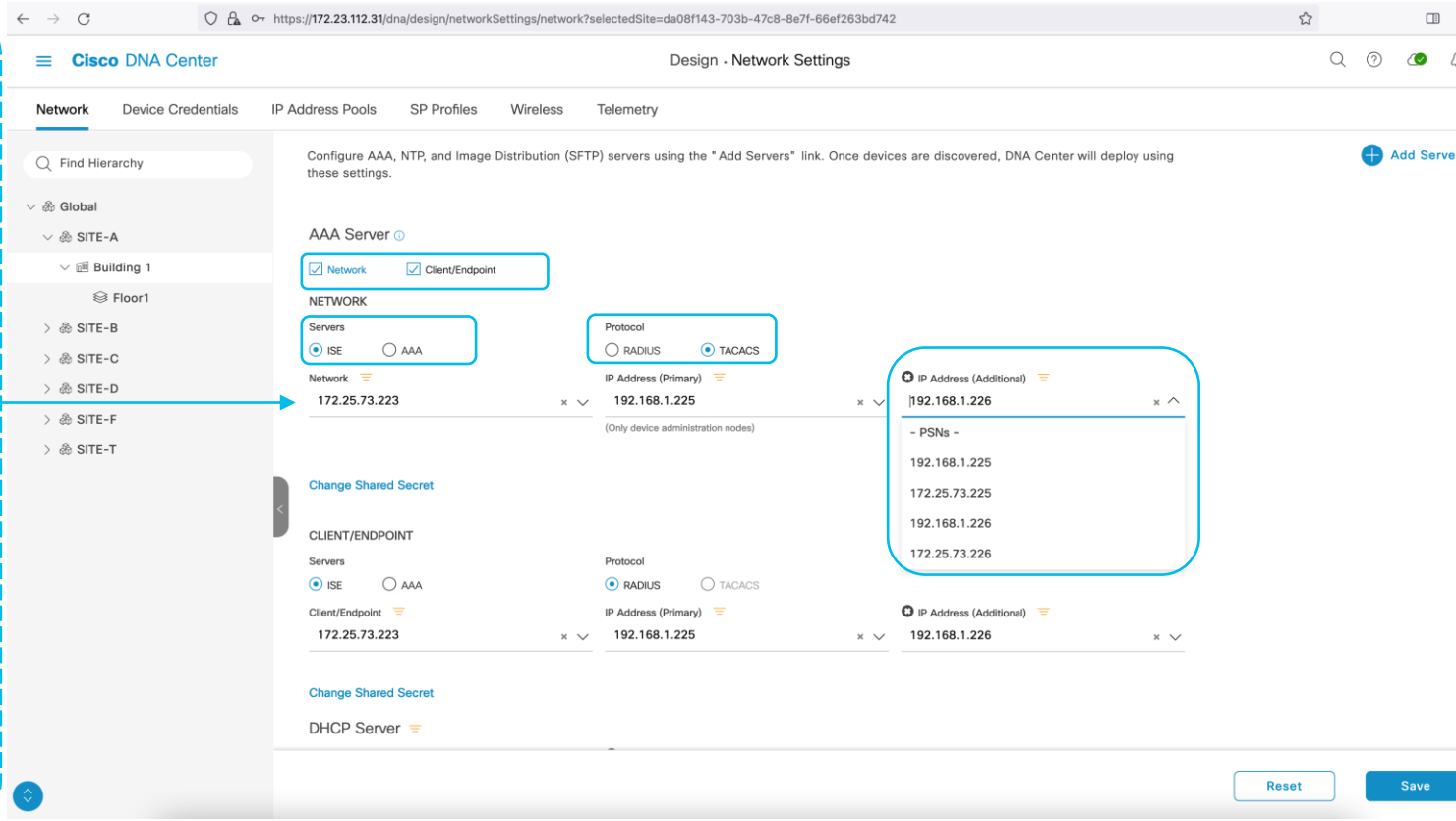
Cisco DNA Center Settings
Cisco ISE + Load Balancer



Cisco DNA Center Design

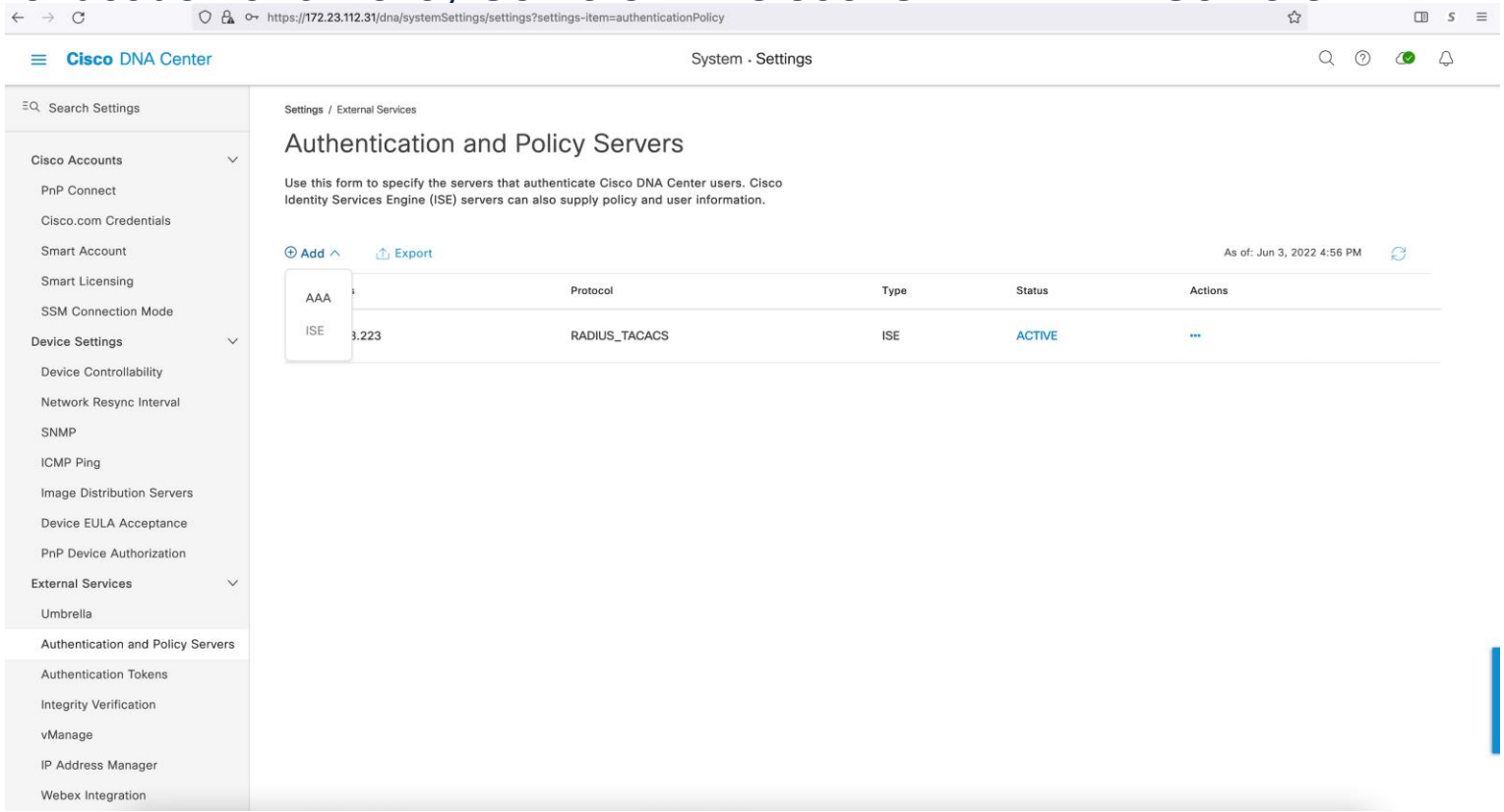
ISE as AAA Server for Client and Network





Cisco DNA Center Settings

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



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

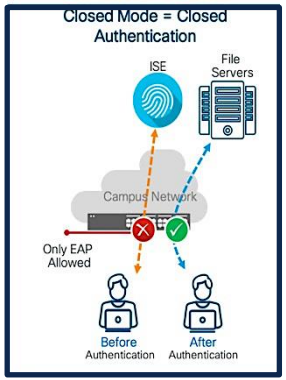
Cisco DNA Center — Design · Authentication Template

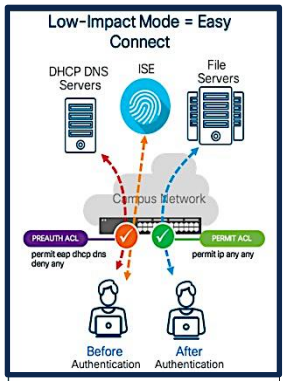
Last updated: 4:28 PM Refresh

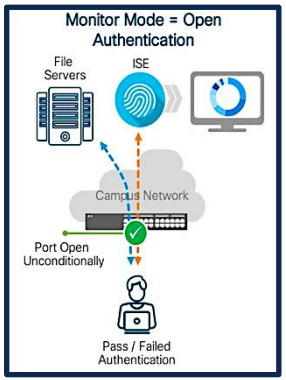
Filter

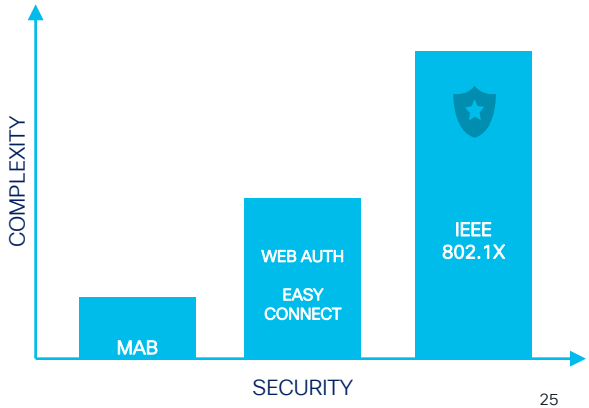
Find

Name	Type
Closed Authentication	Closed Authentication
Low Impact	Low Impact
Open Authentication	Open Authentication

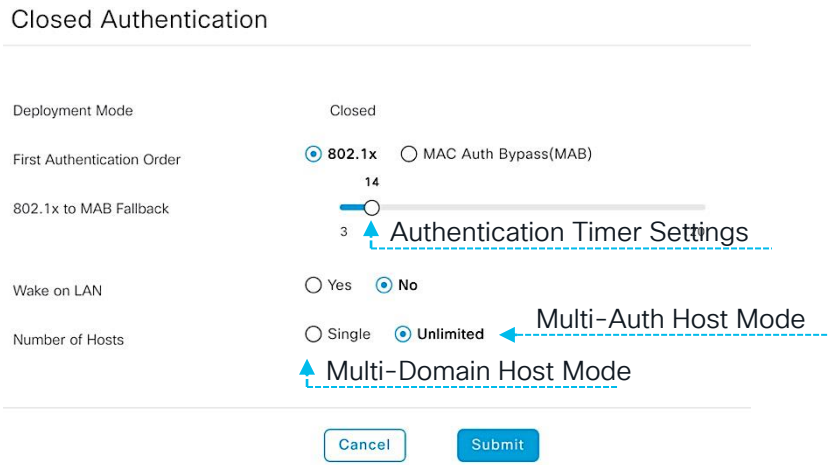


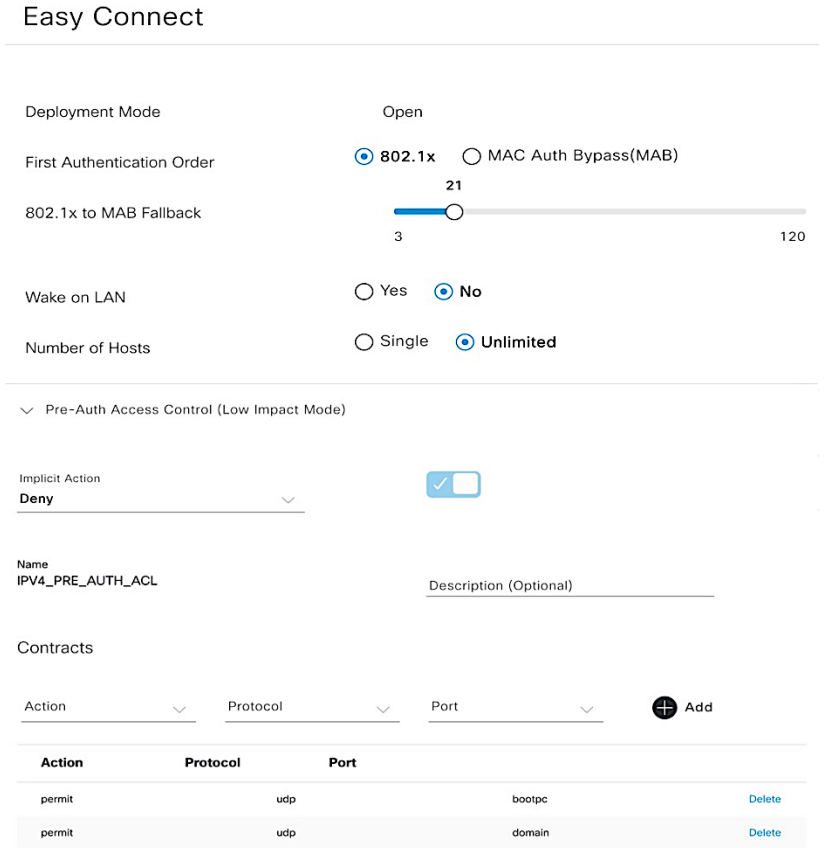






Cisco DNA Center Design
Closed Authentication Template





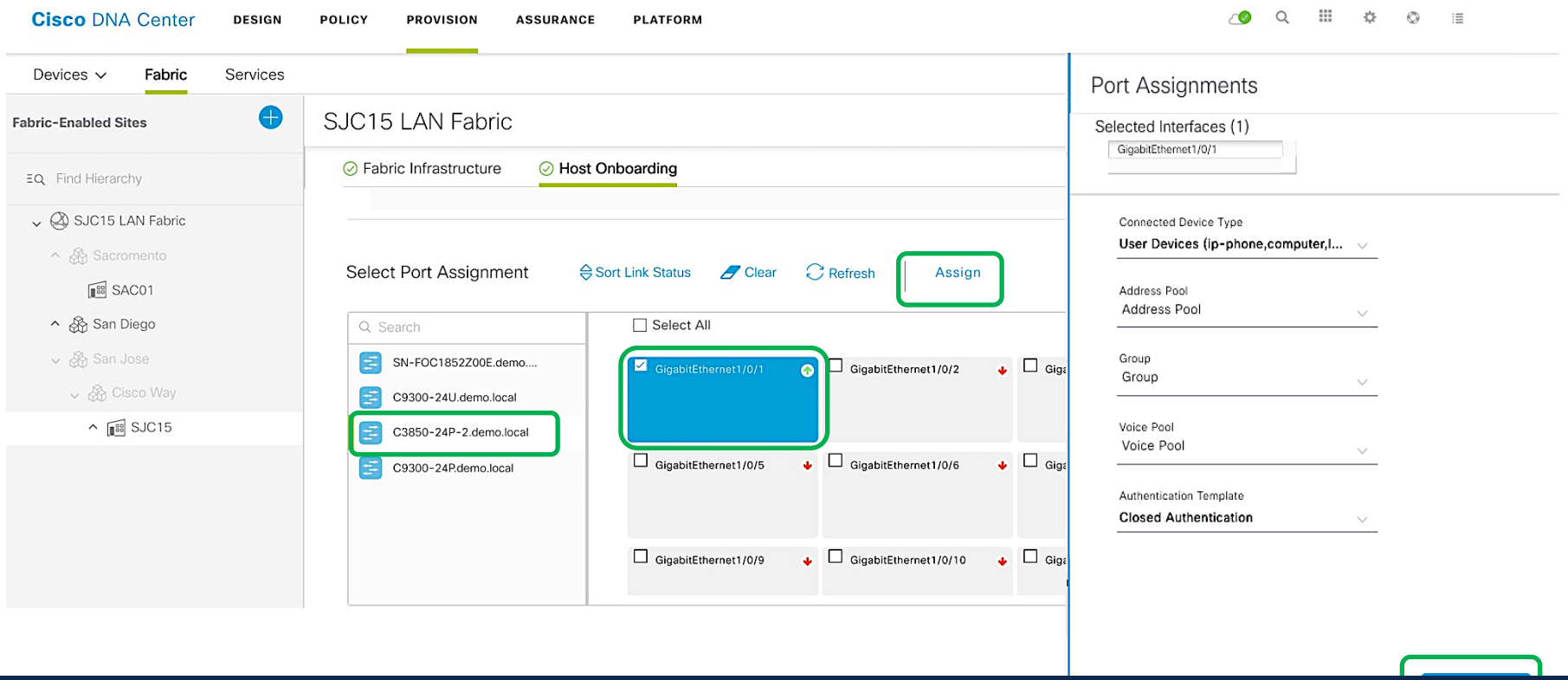
CLI's pushed with change in Fallback Timers

dot1x timeout tx-period 7

dot1x max-reauth-req 2

Cisco DNA Center Provision

Authentication Template(Global or Interface Specific)



Config Deployed

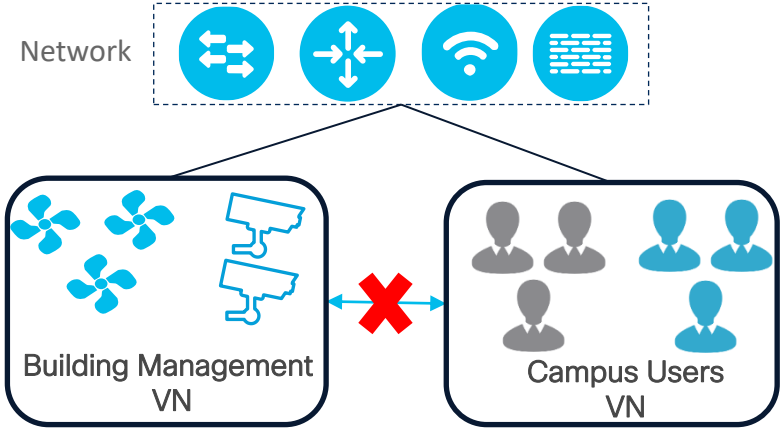
Template: default Access Vlans, IBNS 2.0 Service policy & Dot1x CLI's

Fabric Segmentation Strategy

cisco Live!

Cisco DNA Center Policy Segmentation Strategy

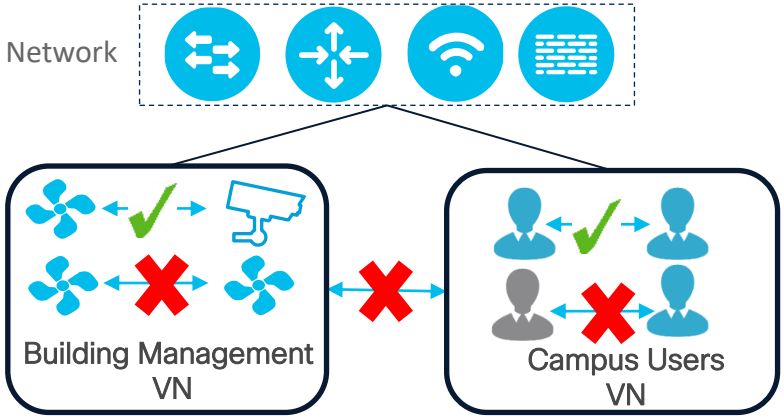
Macro Segmentation



Virtual Network (VN)

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

Micro Segmentation

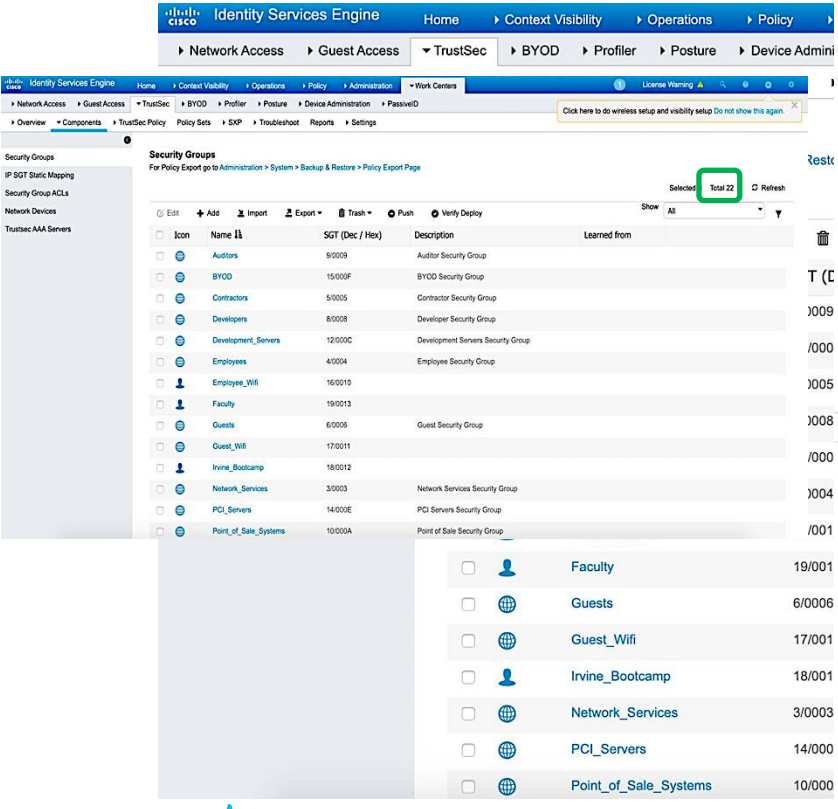


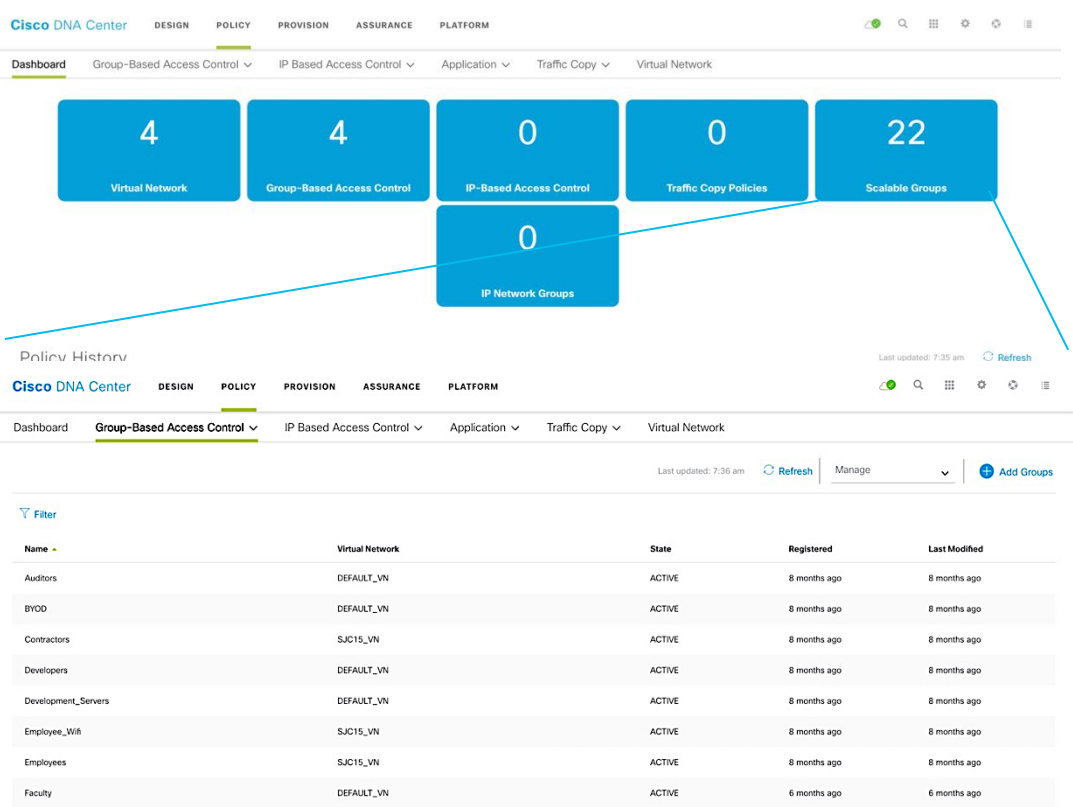
Scalable Group (SG)

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.

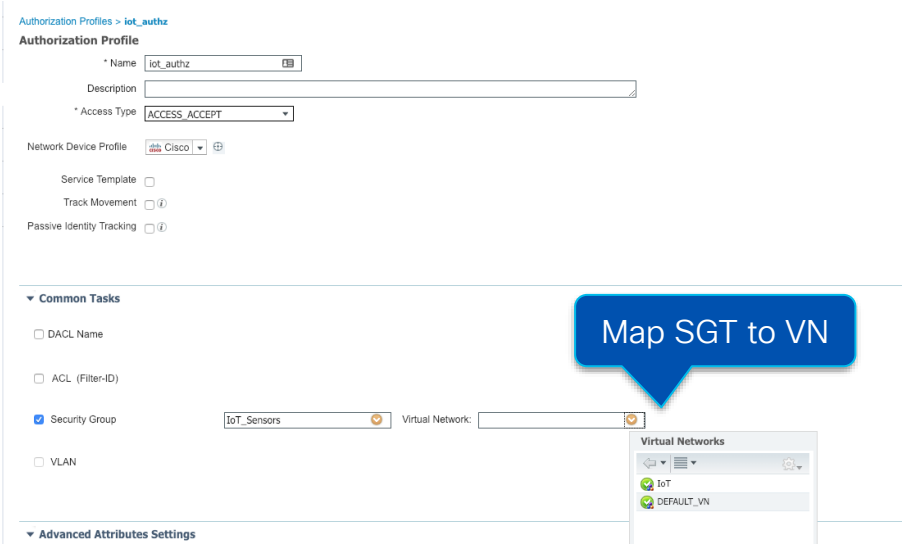
Cisco DNA Center Policy

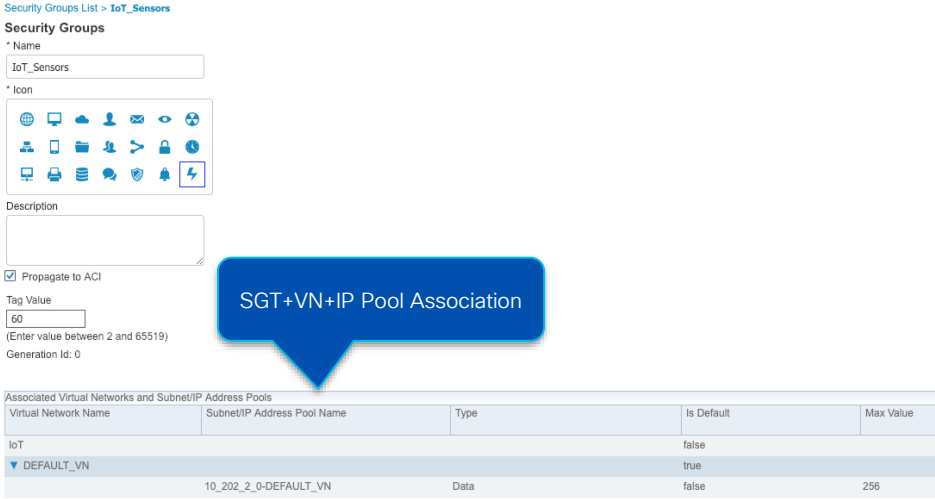
Security Groups => Scalable Groups





Assigning Endpoints to Correct VN

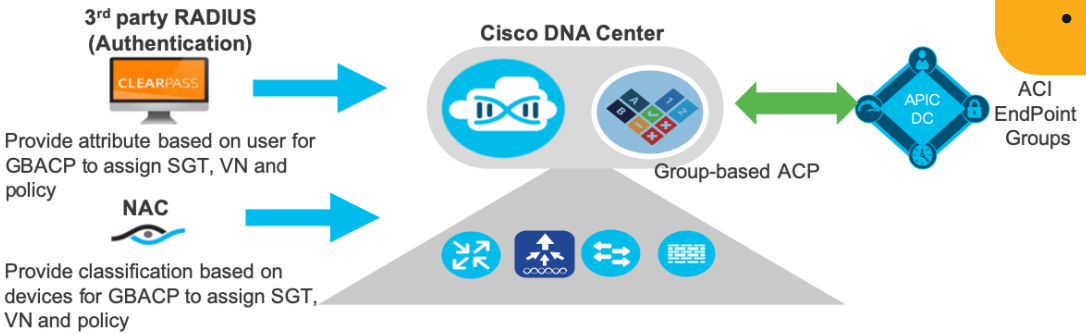




Cisco DNA Center Policy
Group-Based Access Control Policy

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

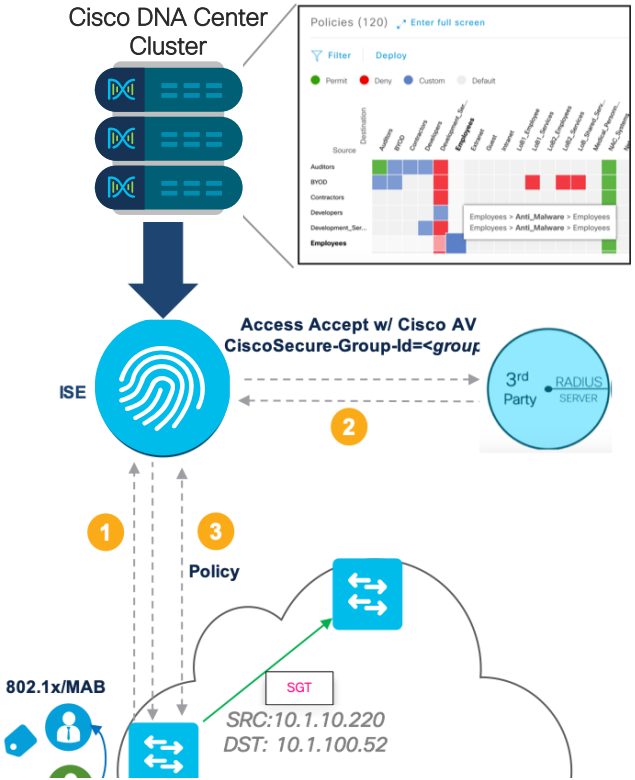
- Scalable Groups learned from ACI via ISE

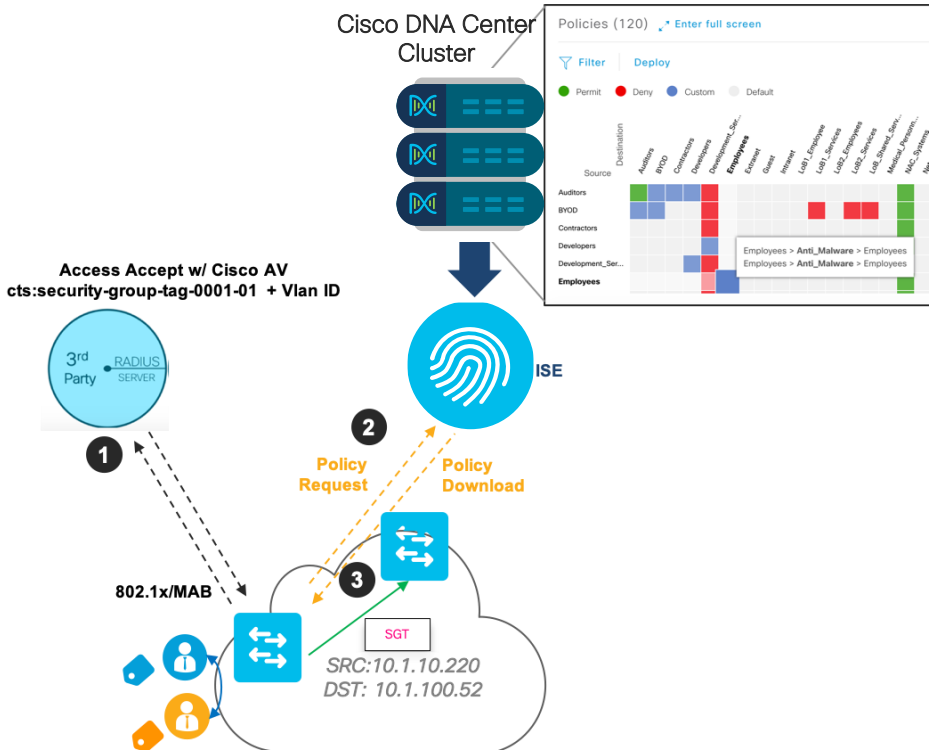
Third-Party AAA/RADIUS Server support

Improved Scale

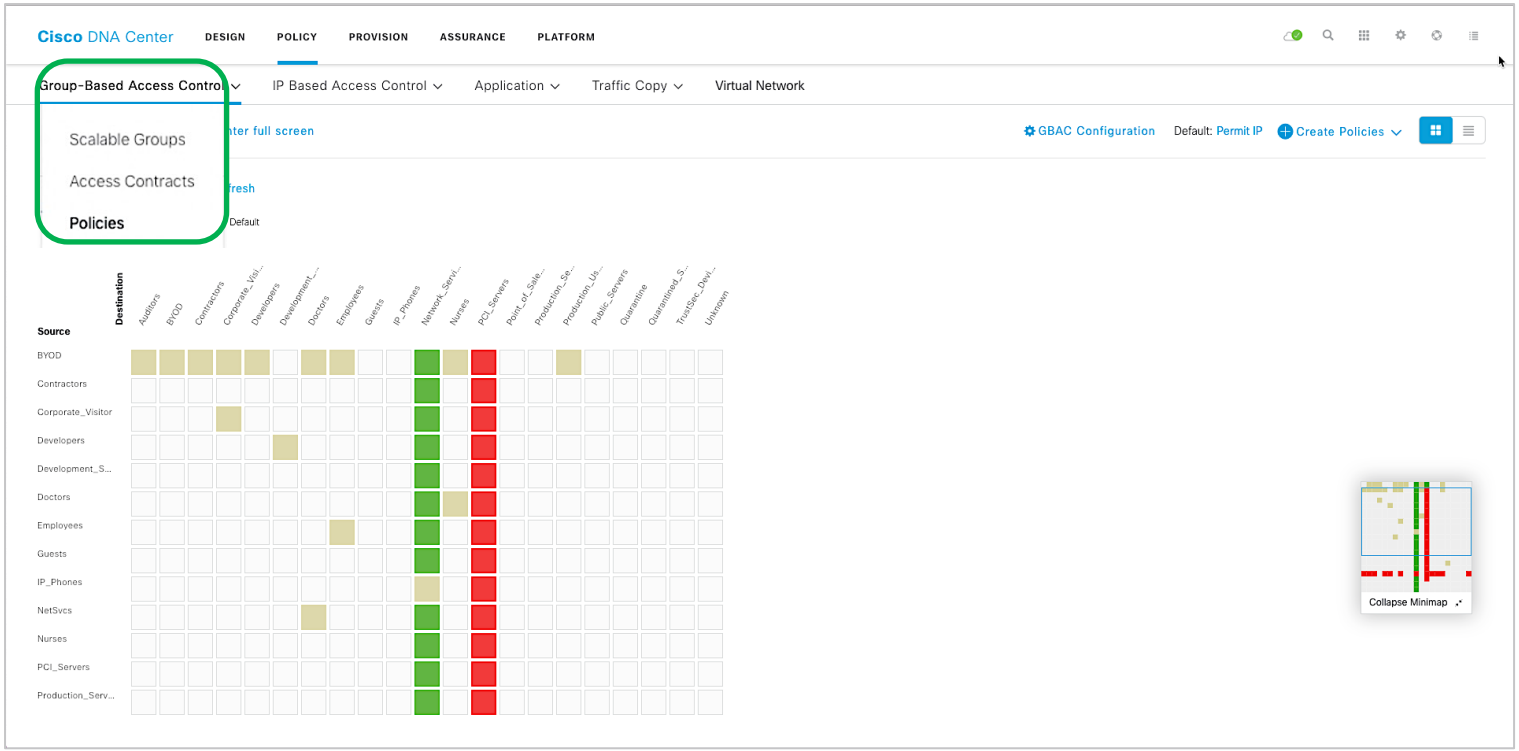
Up to 4000 Scalable Groups
Up to 500 Access Contracts
Up to 25,000 Policies

Cisco DNA Center Policy
Third-Party AAA/RADIUS Server support



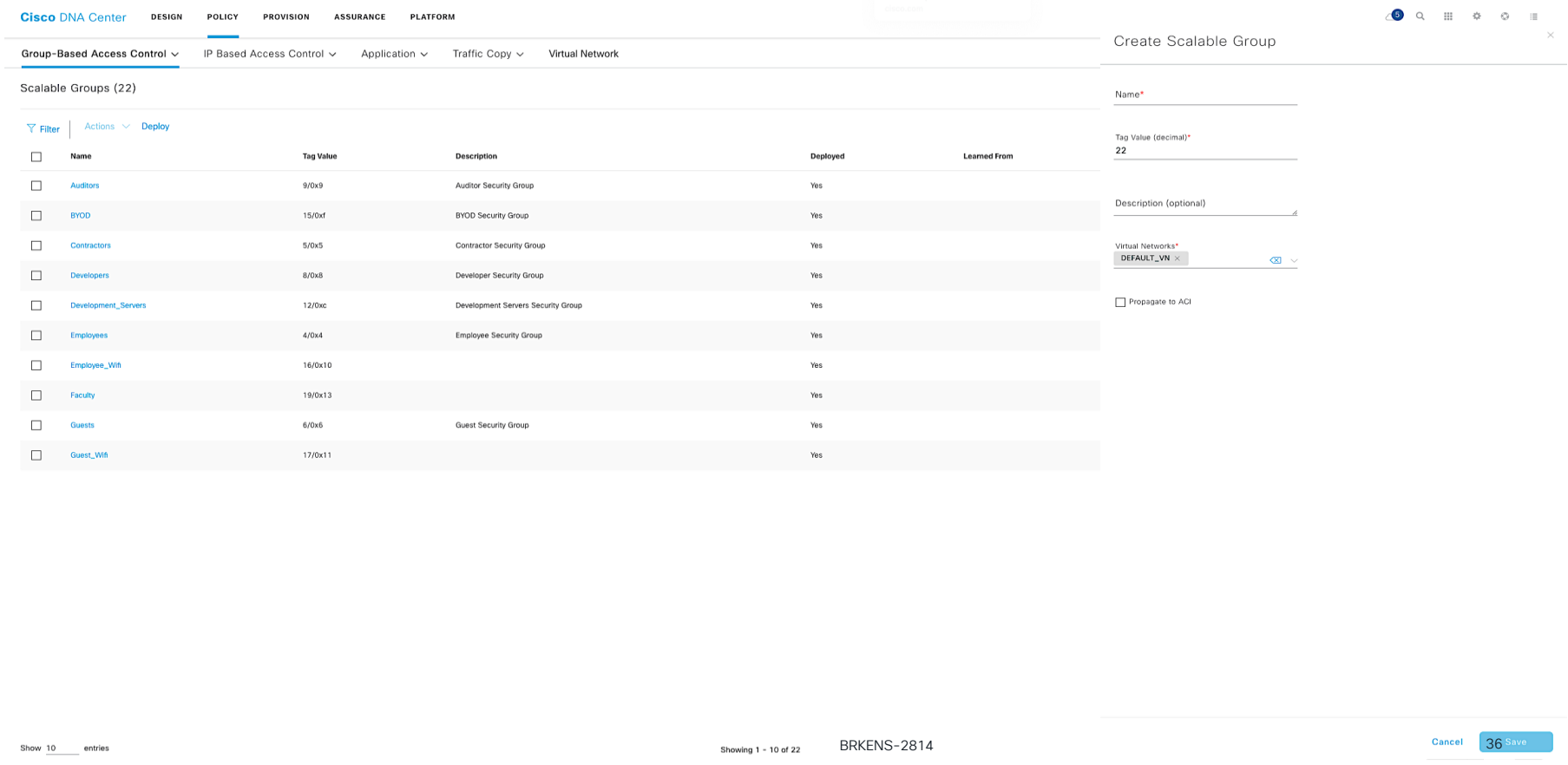


Cisco DNA Center Policy
Group-Based Access Control Policy



POLICY Landing Page & Matrix View

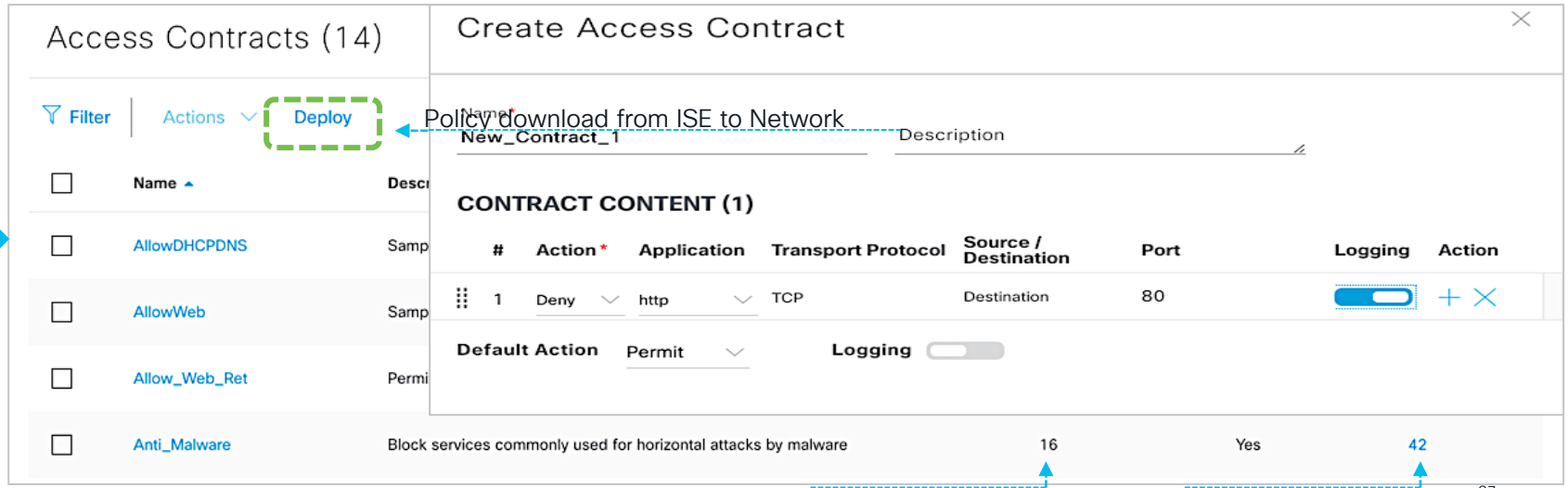
Cisco DNA Center Policy Scalable Groups



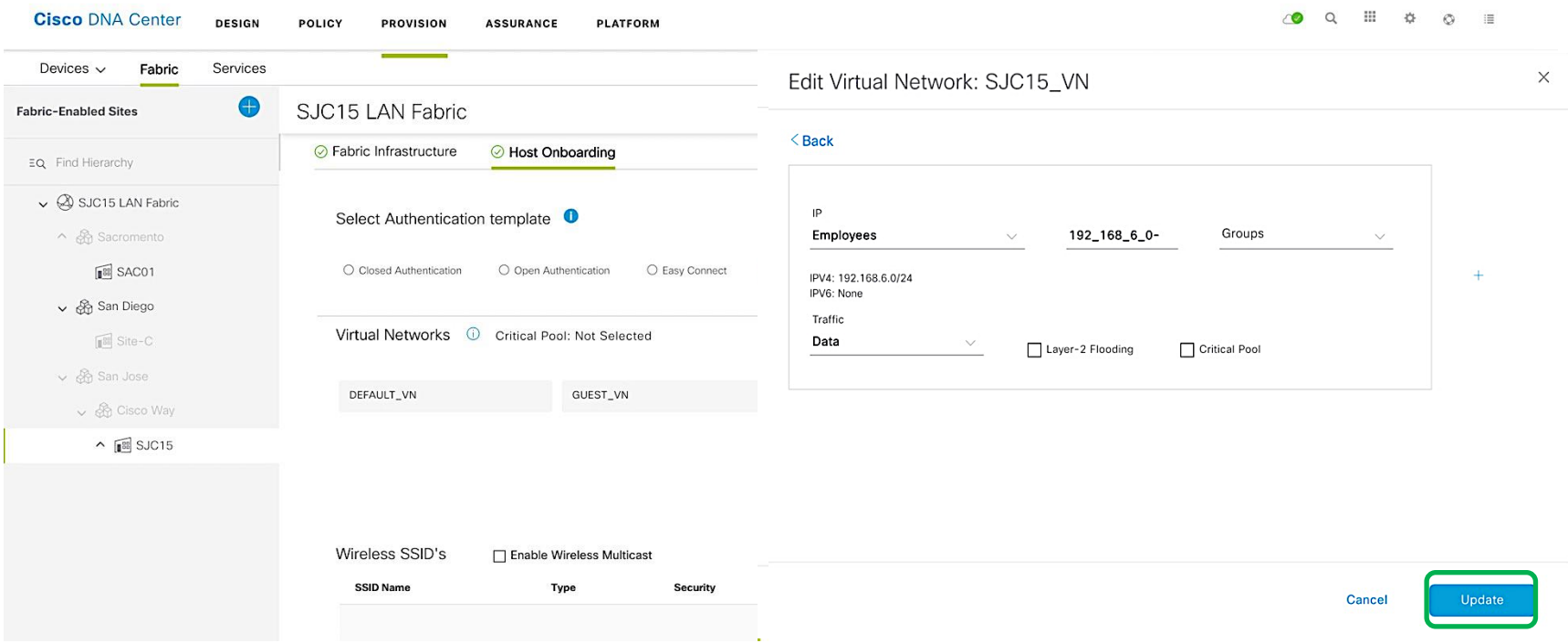
Cisco DNA Center Policy Access Contracts

Simple

Custom Contract



Cisco DNA Center Provision
Associate IP Pool to VN

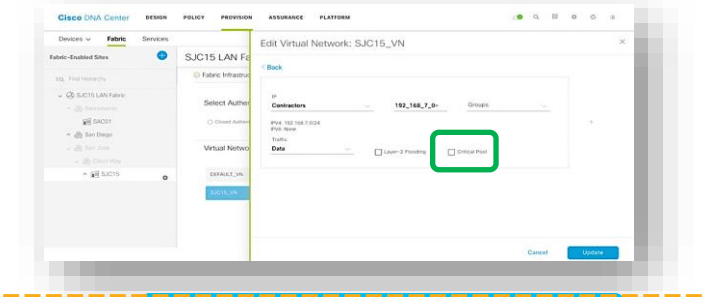


Config Deployed

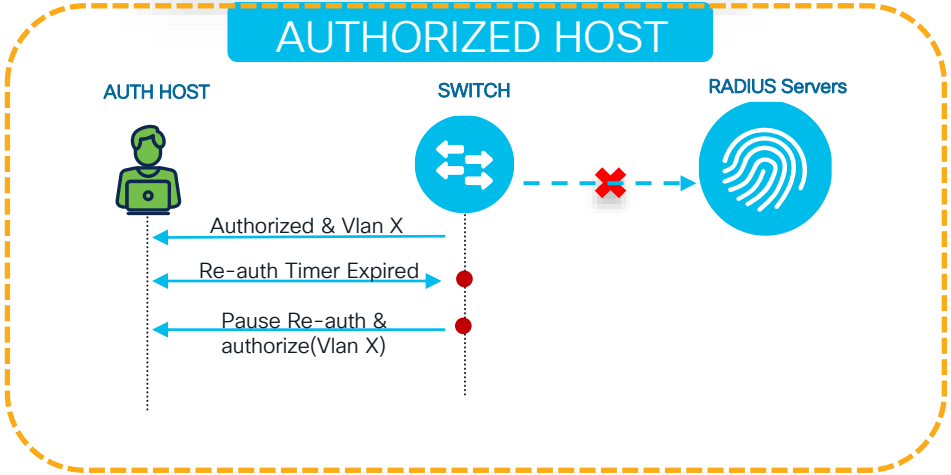
Vlan , SVI , Interface Template, LISP

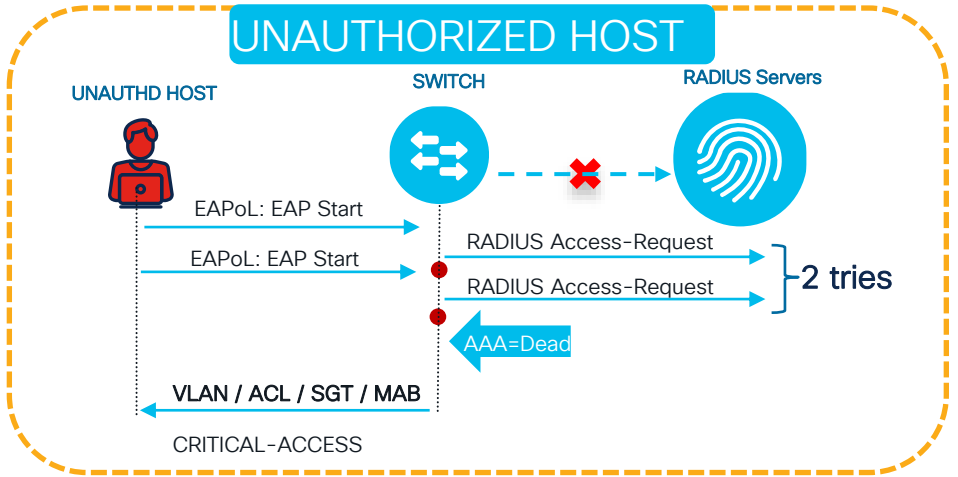
Cisco DNA Center Host Onboarding
Critical Vlan

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



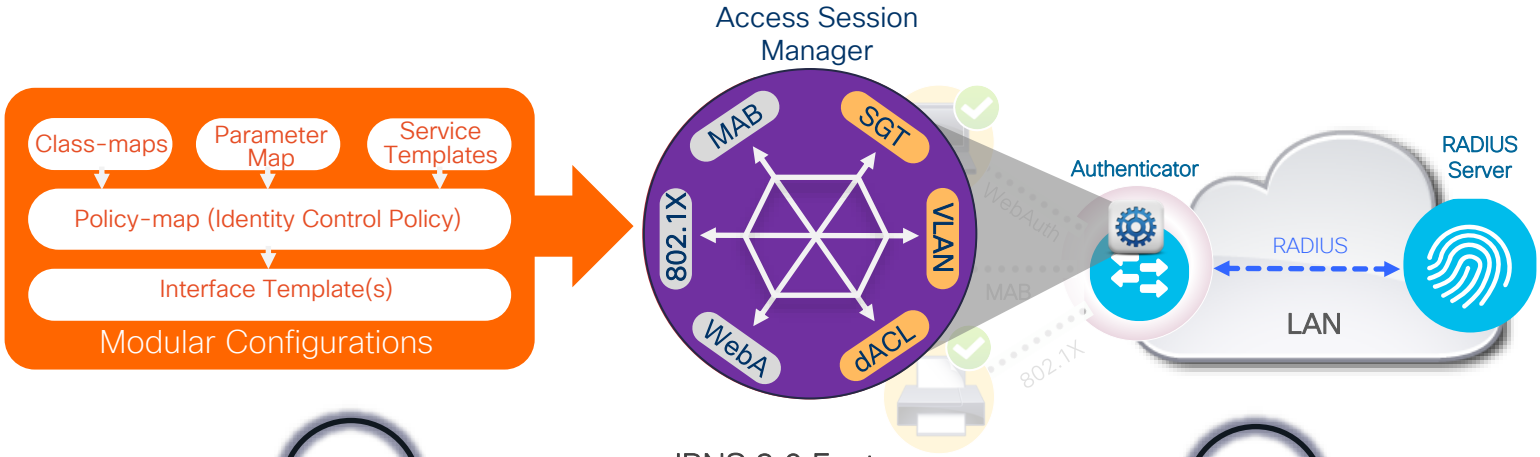
- Feature to locally activate an VLAN/ACL/ SGT/MAB during RADIUS Server outage.
- Default Critical Vlan - Data: 2047 & Voice : 2046
- No SVI created unless Critical pool selected
- Default for all Authentication Templates and Per Fabric Site
- Need more than one Critical Vlan for Data, use Static Port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

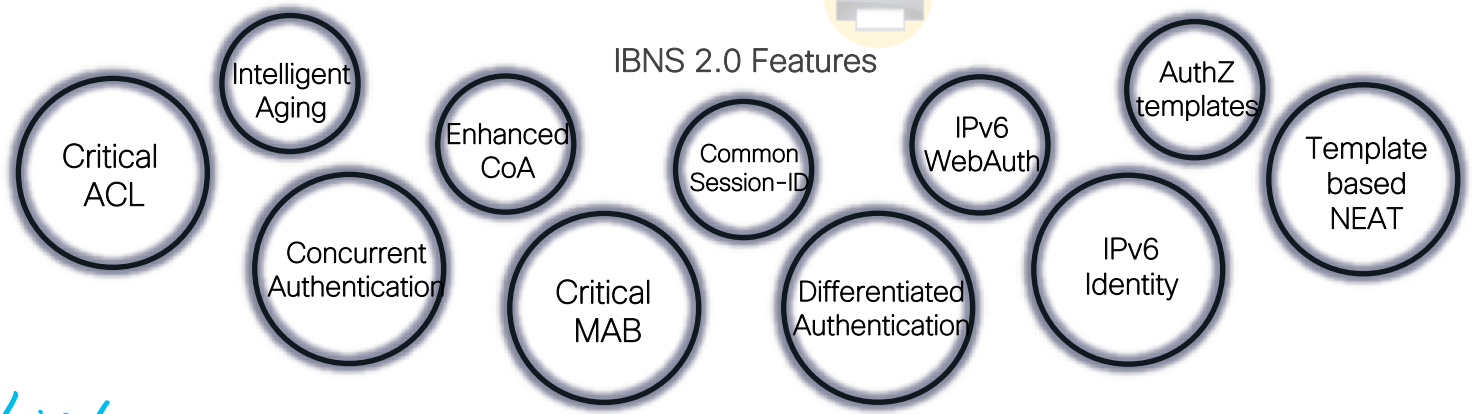




IBNS 2.0 Overview

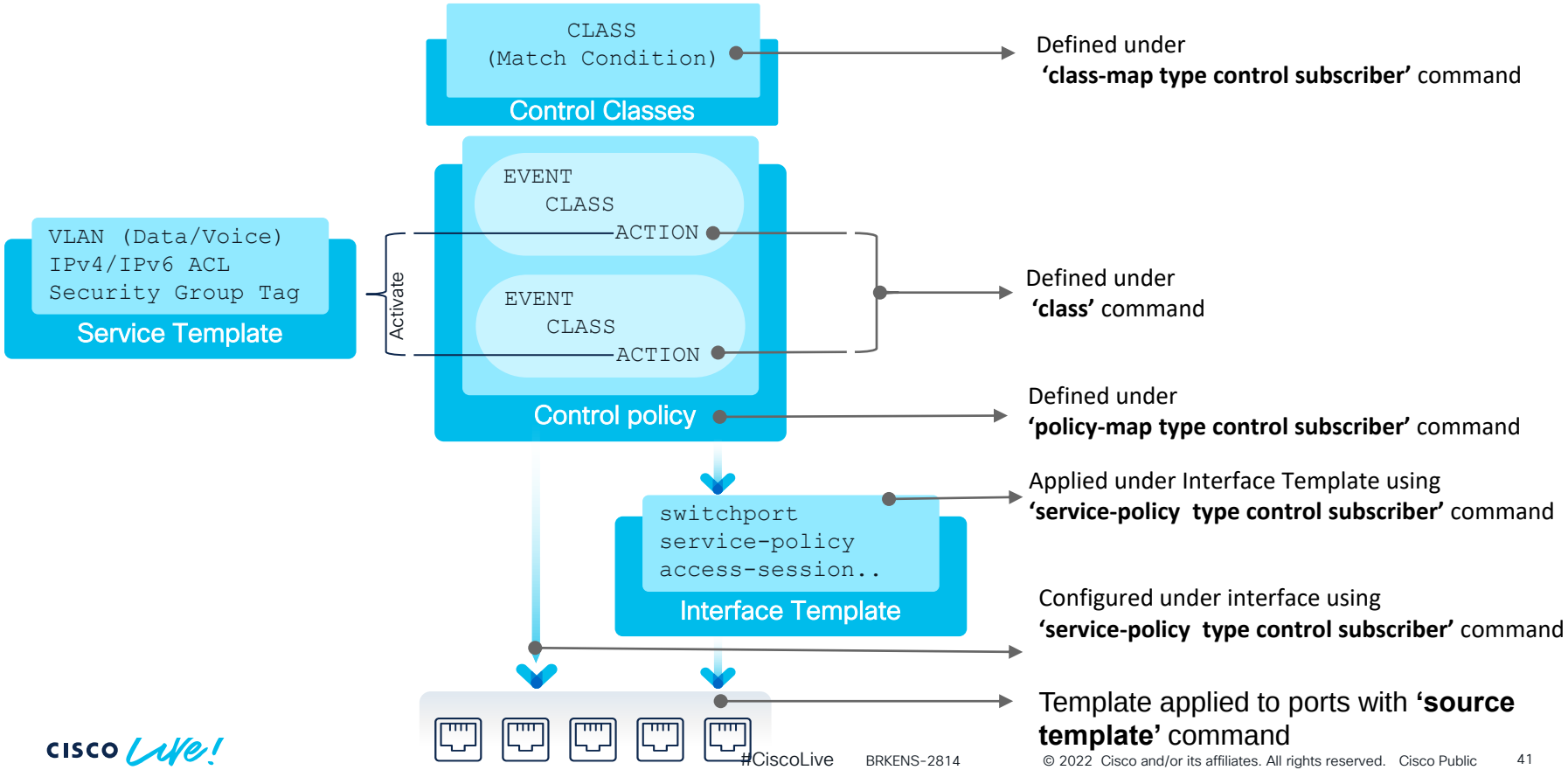
Any Authentication with Any Authorization on any Media (Wired / Wireless)





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
```

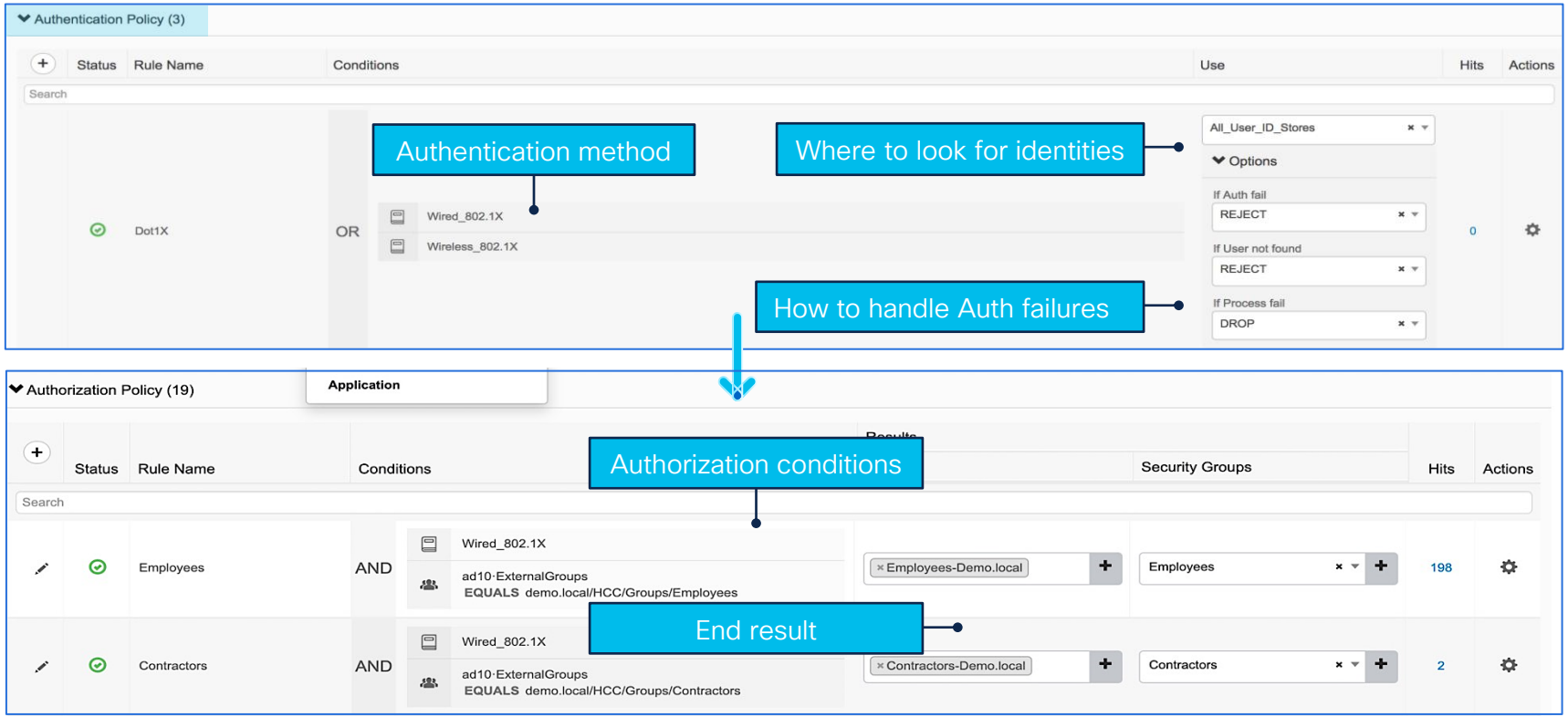
Interface Templates

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

Policy-Map

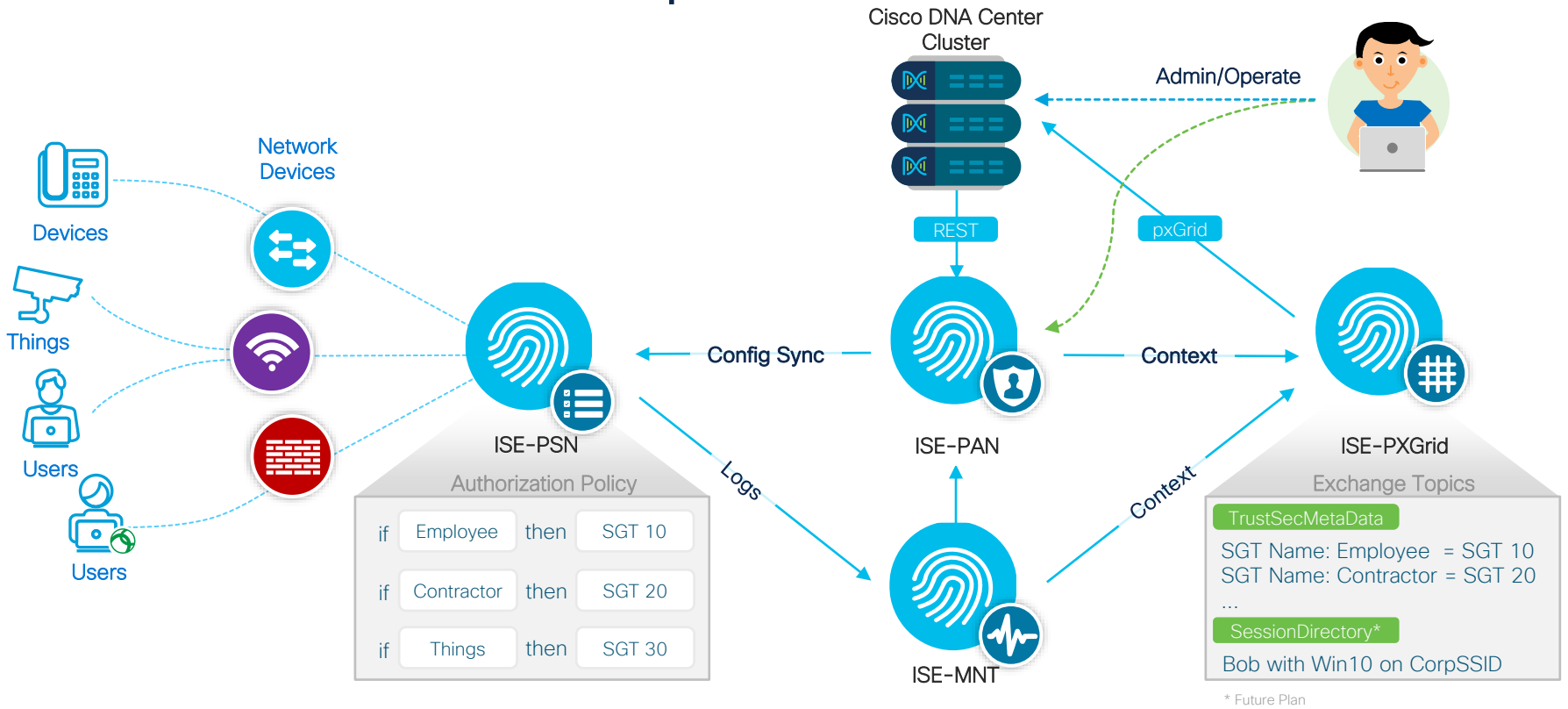
```
policy-map type control subscriber PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
policy-map type control subscriber PMAP_DefaultWiredDot1xClosedAuth_MAB_1X
policy-map type control subscriber PMAP_DefaultWiredDot1xLowImpactAuth_1X_MAB
policy-map type control subscriber PMAP_DefaultWiredDot1xLowImpactAuth_MAB_1X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

ISE Authentication and Authorization policy

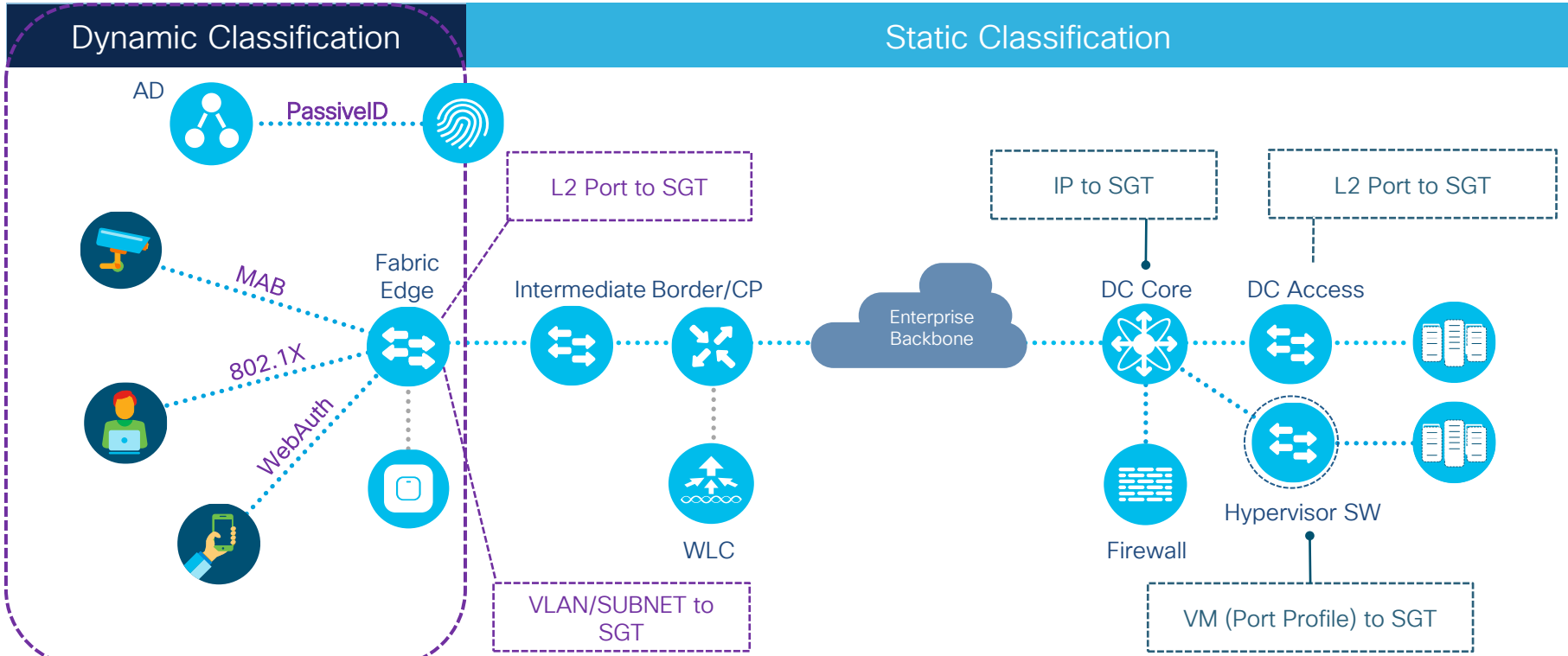


Configured by Administrator

Cisco DNA Center Operation



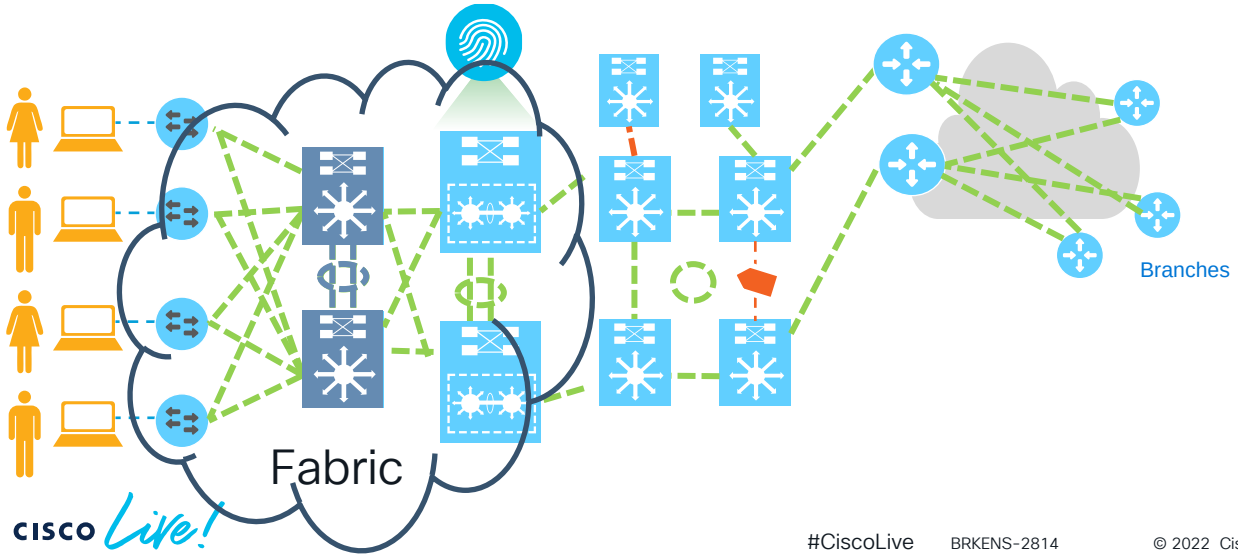
Security Group Tags(SGT)
Classification Mechanism



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**

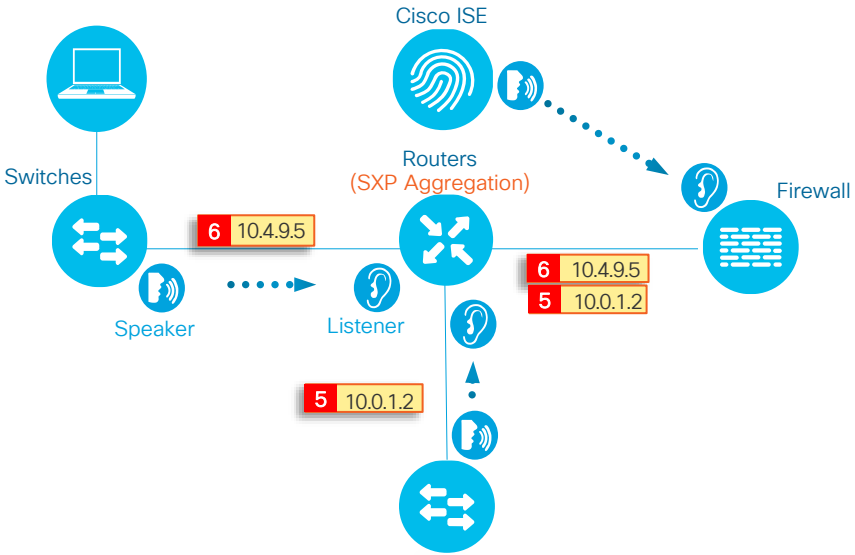
Supporting devices

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

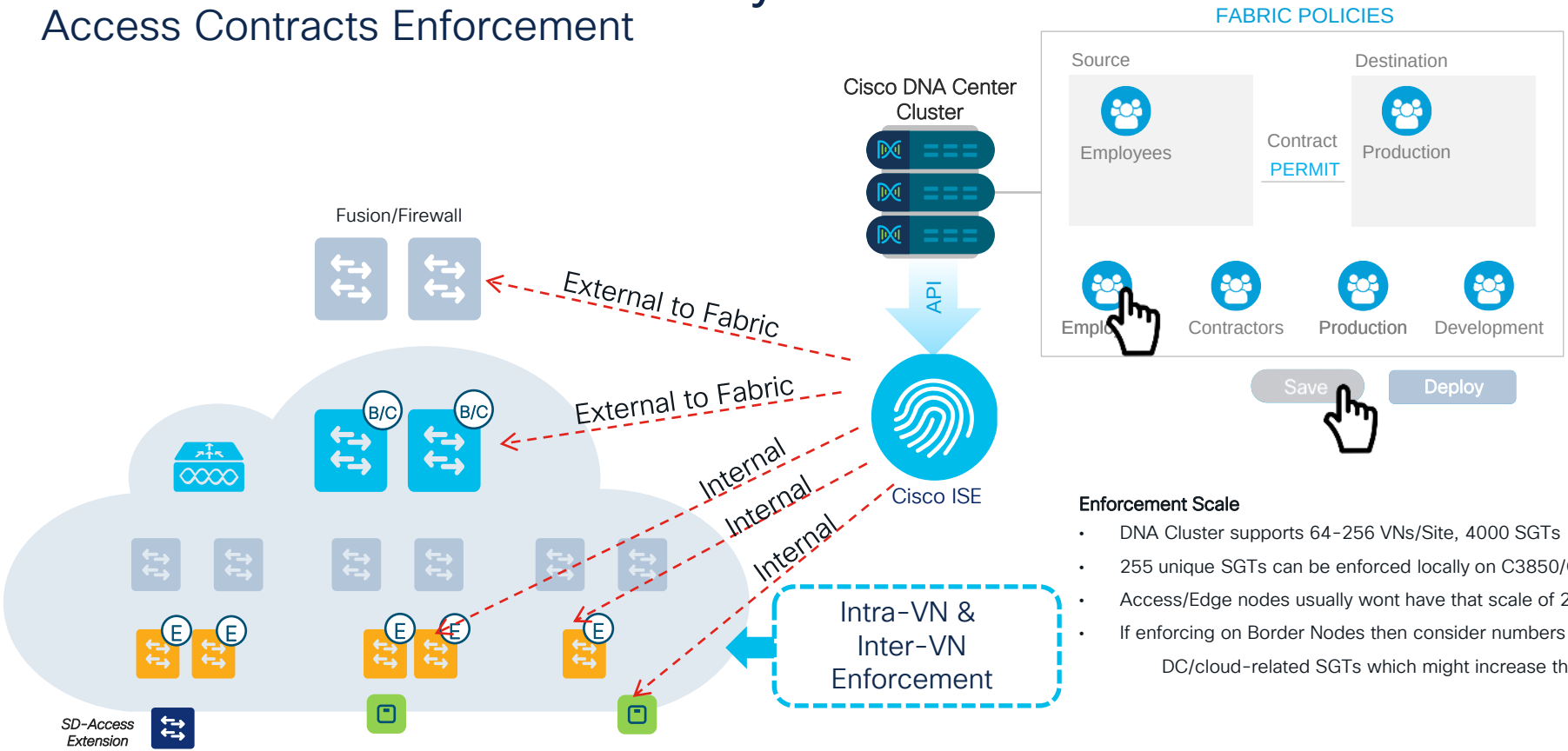
Scalable Group Tags(SGT)
Propagation Mechanism

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

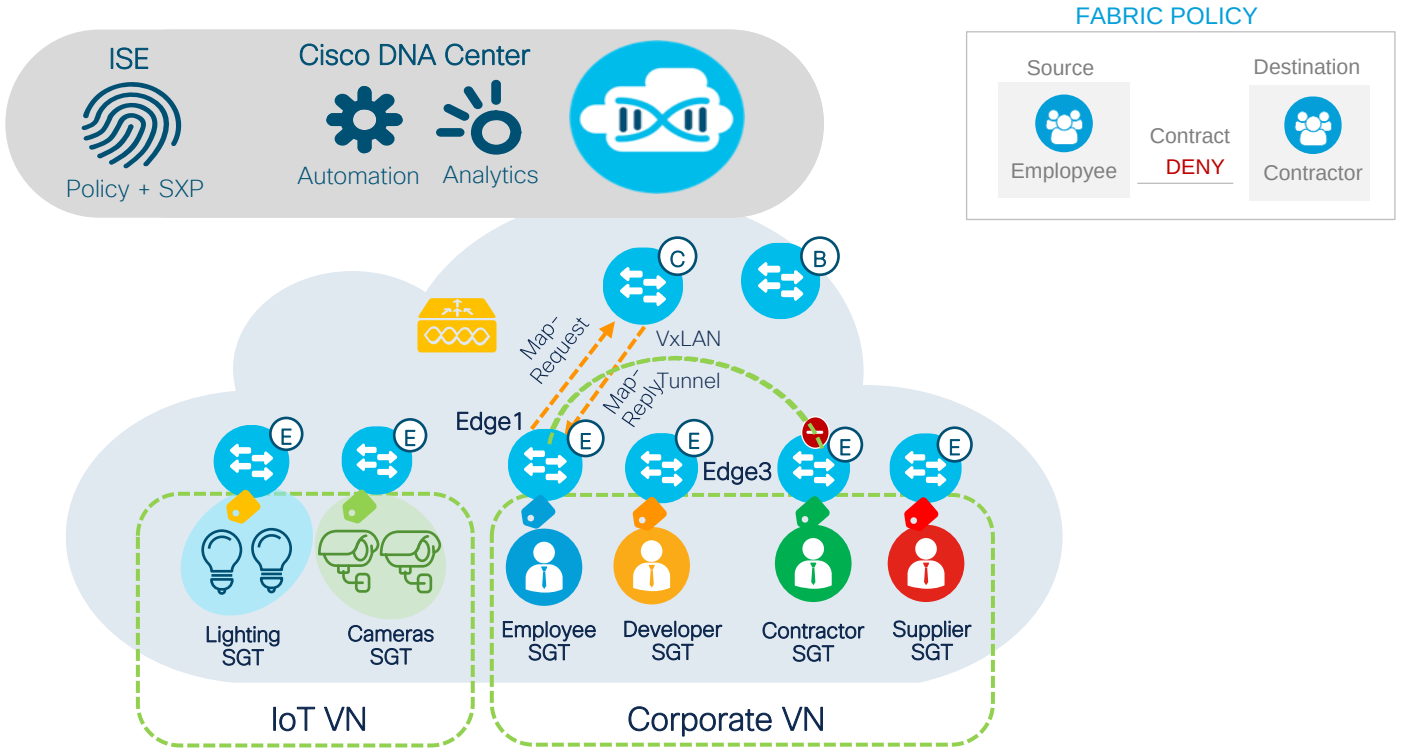


Enforcement Scale

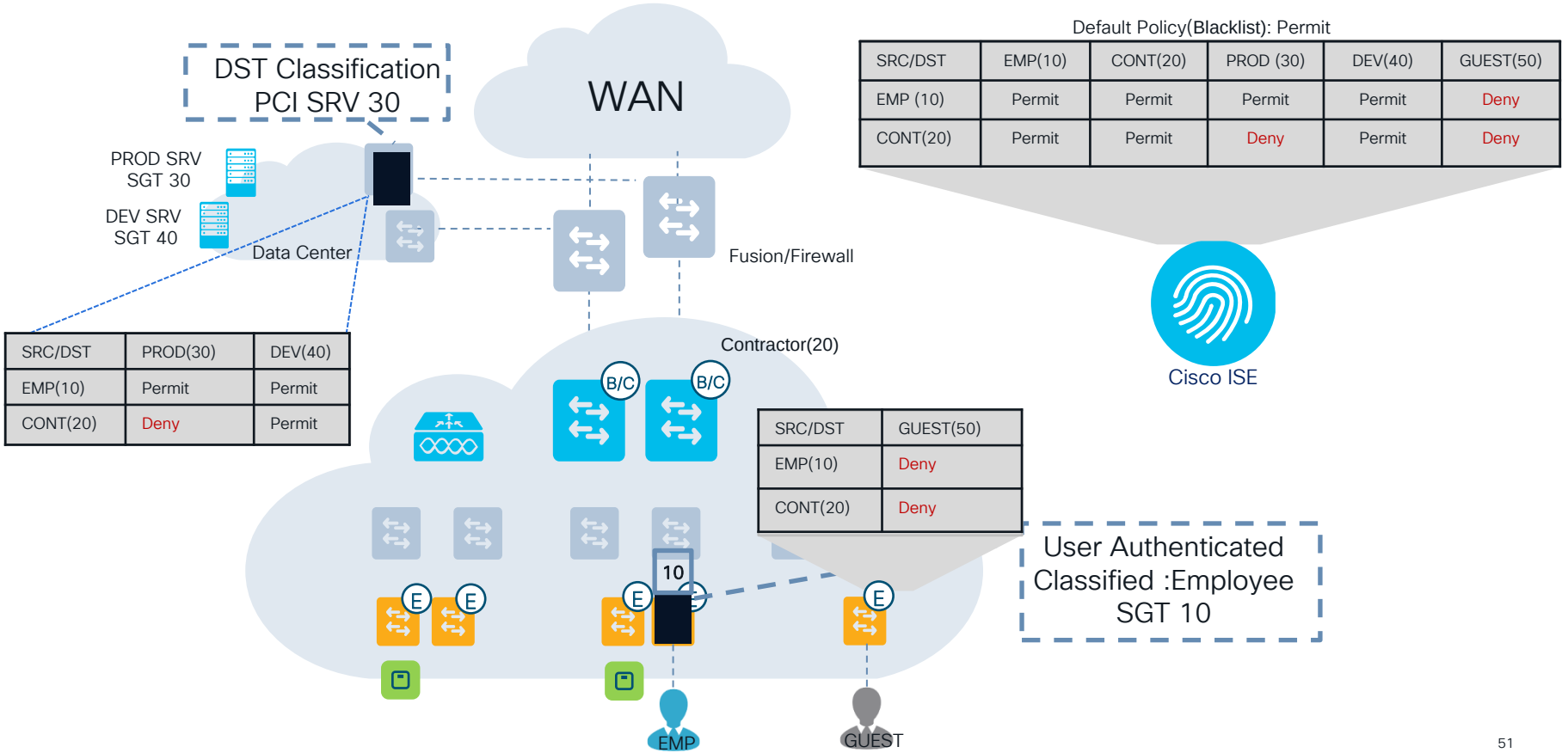
- DNA Cluster supports 64-256 VNs/Site, 4000 SGTs
- 255 unique SGTs can be enforced locally on C3850/C9k
- Access/Edge nodes usually wont have that scale of 255+
- If enforcing on Border Nodes then consider numbers of DC/cloud-related SGTs which might increase the SG

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



Cisco SGT
SGT Tagging & SGACL Download



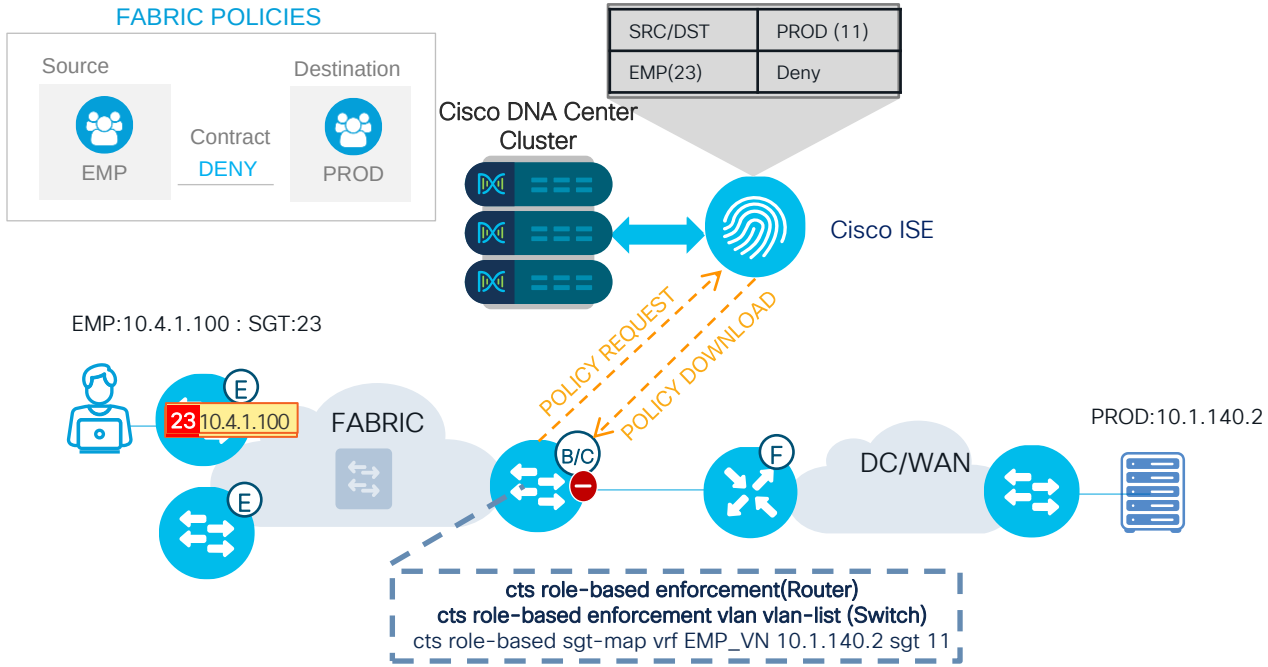
SRC/DST	EMP(10)	CONT(20)	PROD (30)	DEV(40)	GUEST(50)
EMP (10)	Permit	Permit	Permit	Permit	Deny
CONT(20)	Permit	Permit	Deny	Permit	Deny

SRC/DST	PROD(30)	DEV(40)
EMP(10)	Permit	Permit
CONT(20)	Deny	Permit

SRC/DST	GUEST(50)
EMP(10)	Deny
CONT(20)	Deny

Cisco DNA Center Policy
Access Contracts Enforcement on Border

1. Statically/Manually adding policy on Border via CLI

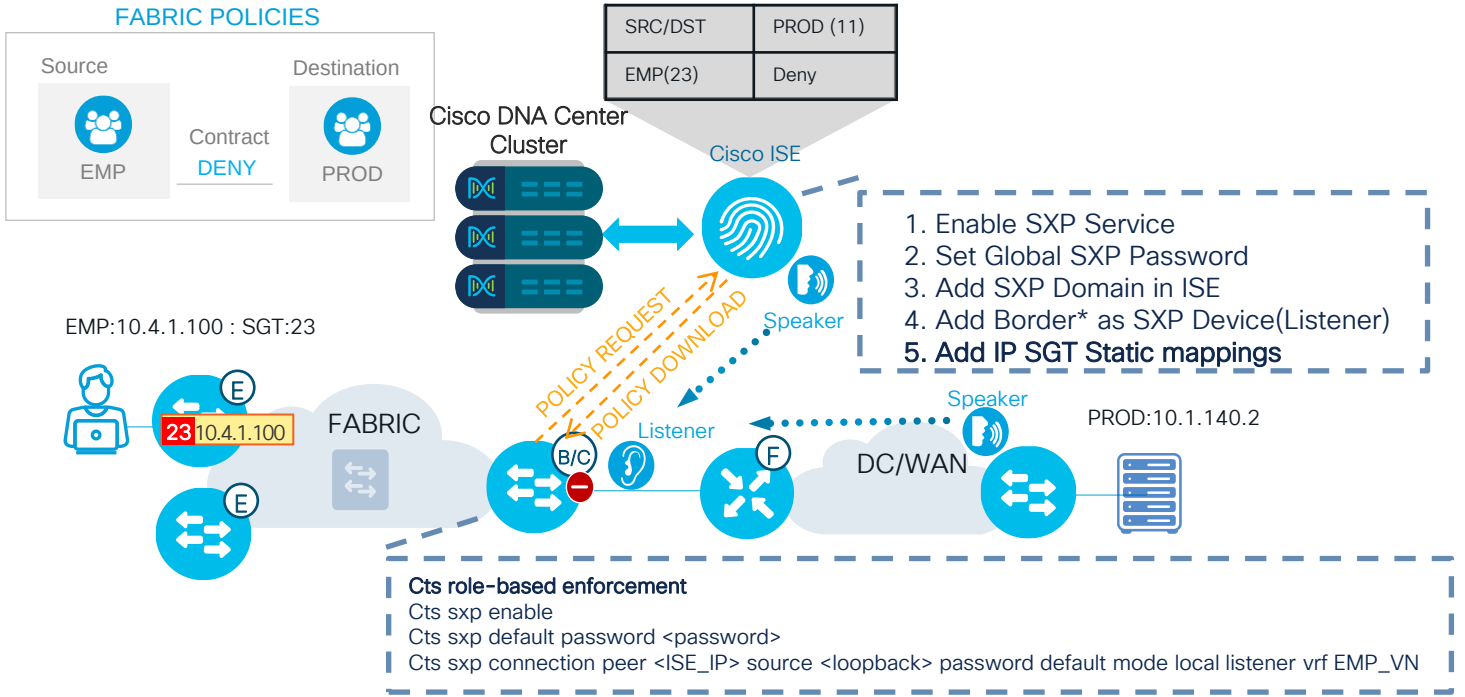


User able to Ping PROD Server
Add Server Mapping statically on the Border using CLI

Cisco 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)



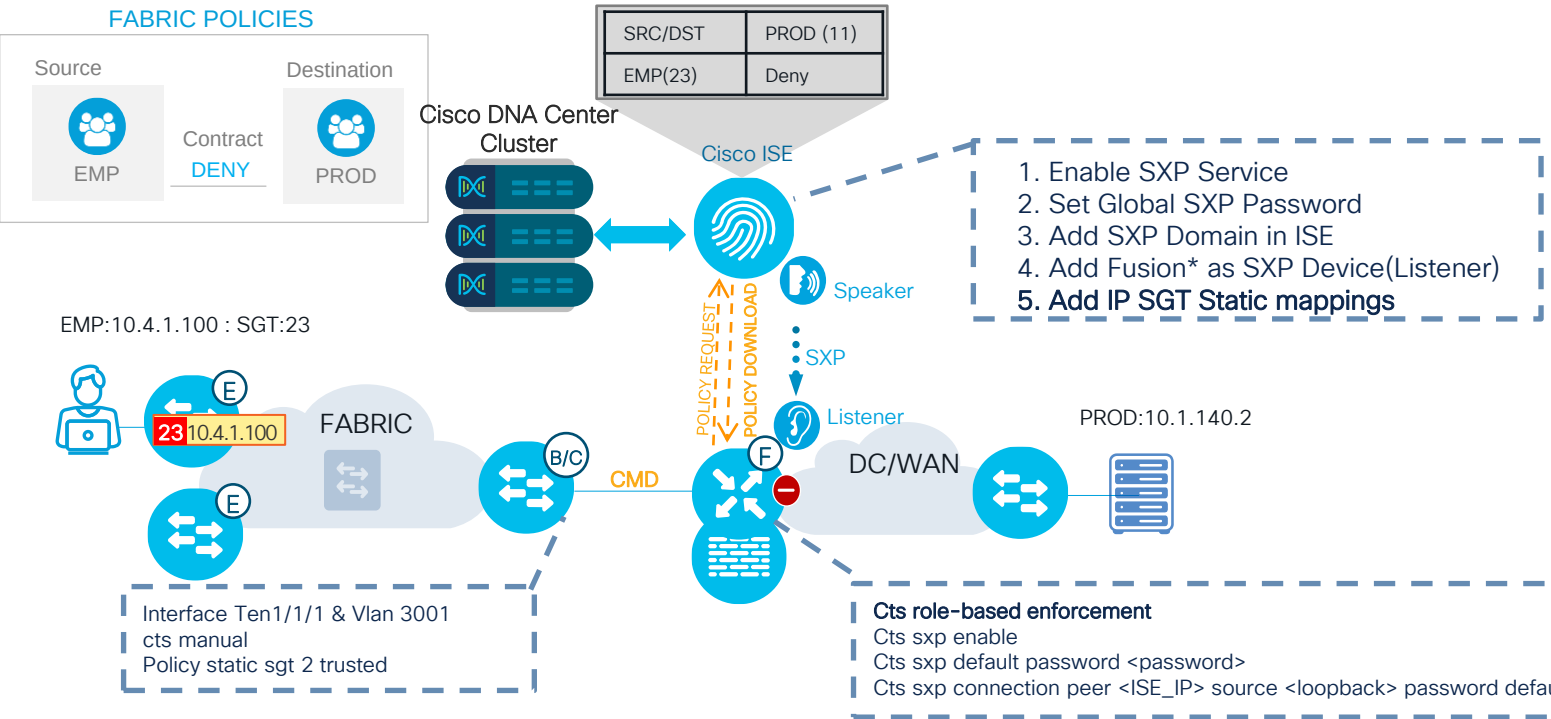
Scale	C9200L	C9200	C3850	C9300	C9400	C9500	C6800	N7700	ASR1K
IP-SGT	8,000	10,000	12,000	10,000	40,000	40,000	256,000	200,000	750,000
Max SGT	255	255	255	255	255	255	No Limit	No Limit	No Limit

Cisco DNA Center Policy

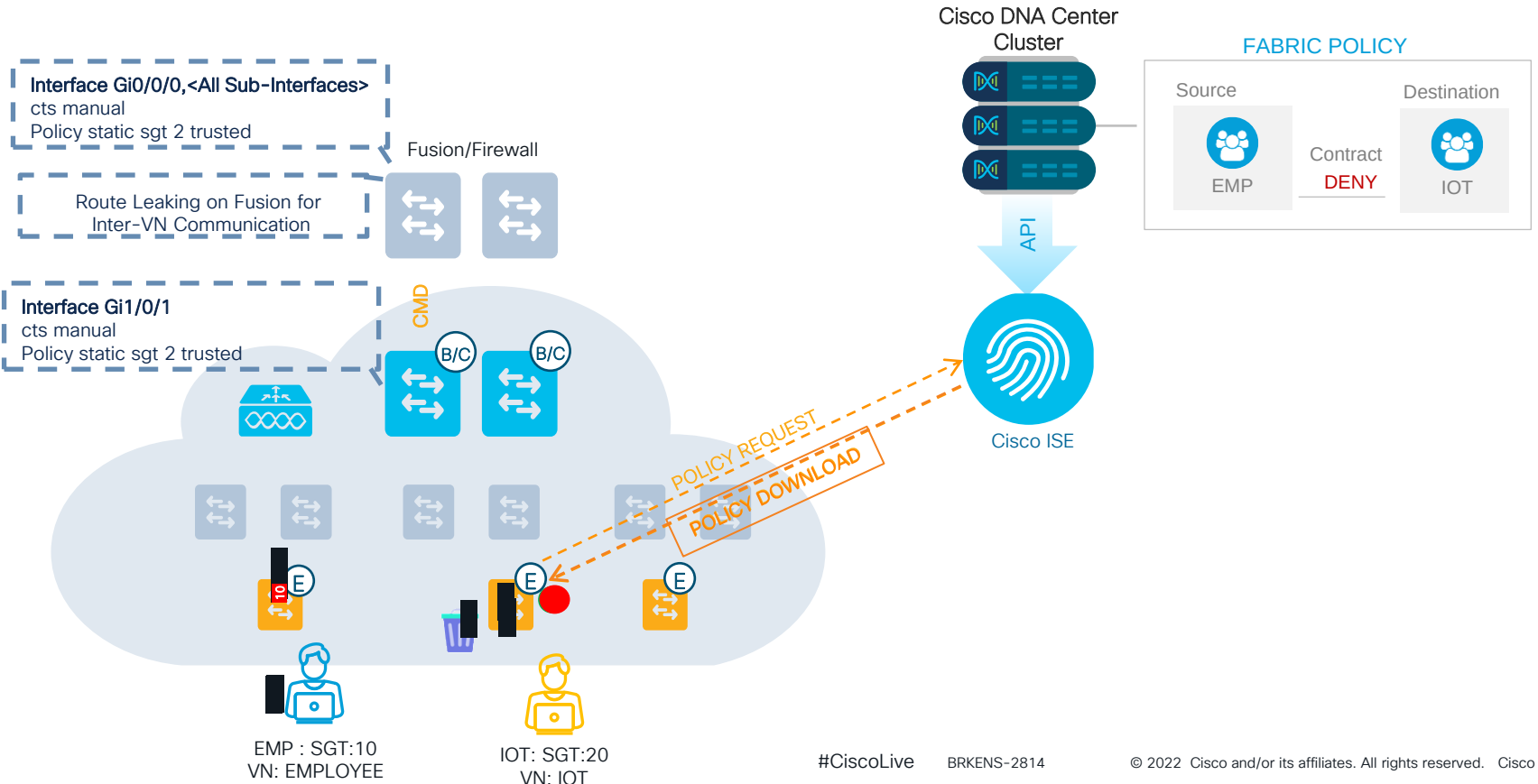
Access Contracts Enforcement on Fusion

SRC & DST SGTs learnt via SXP(Cisco ISE)

VxLAN to CMD Conversion(Border)

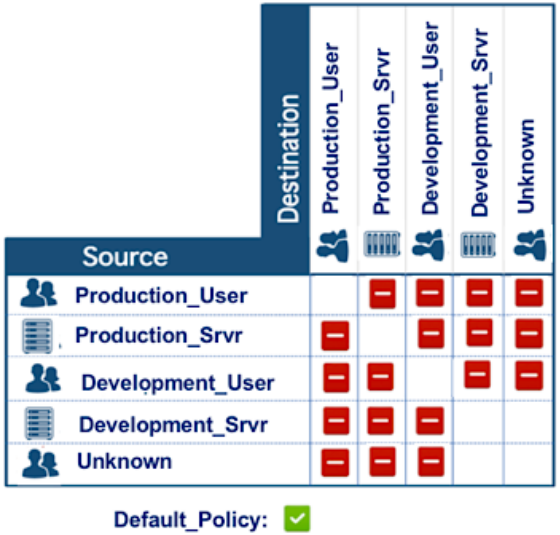


Cisco DNA Center Policy
VN-2-VN Policy Enforcement

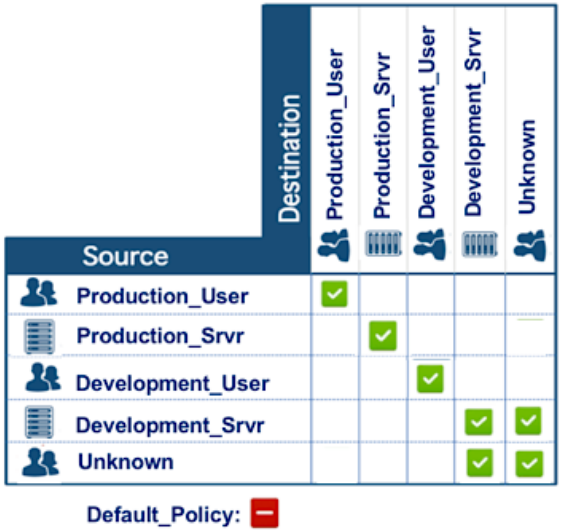


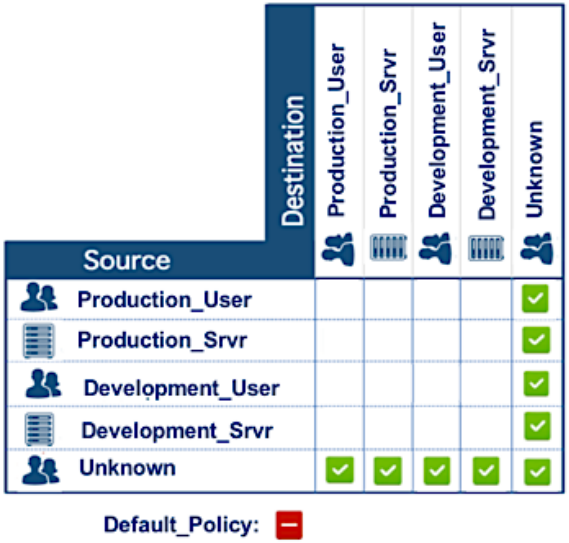
Cisco DNA Center Policy Whitelist vs Blacklist Model

Blacklist Model



Whitelist Model

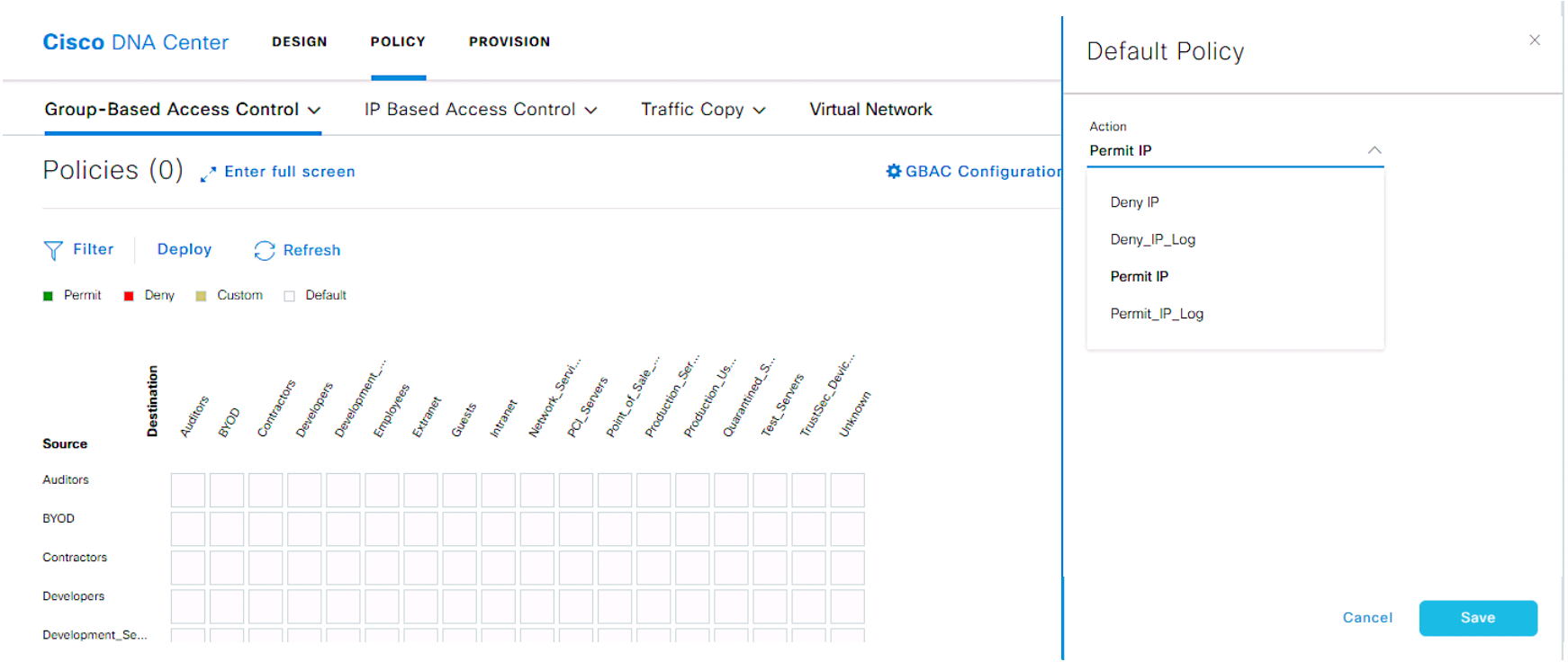




Initial Brownfield Deployment

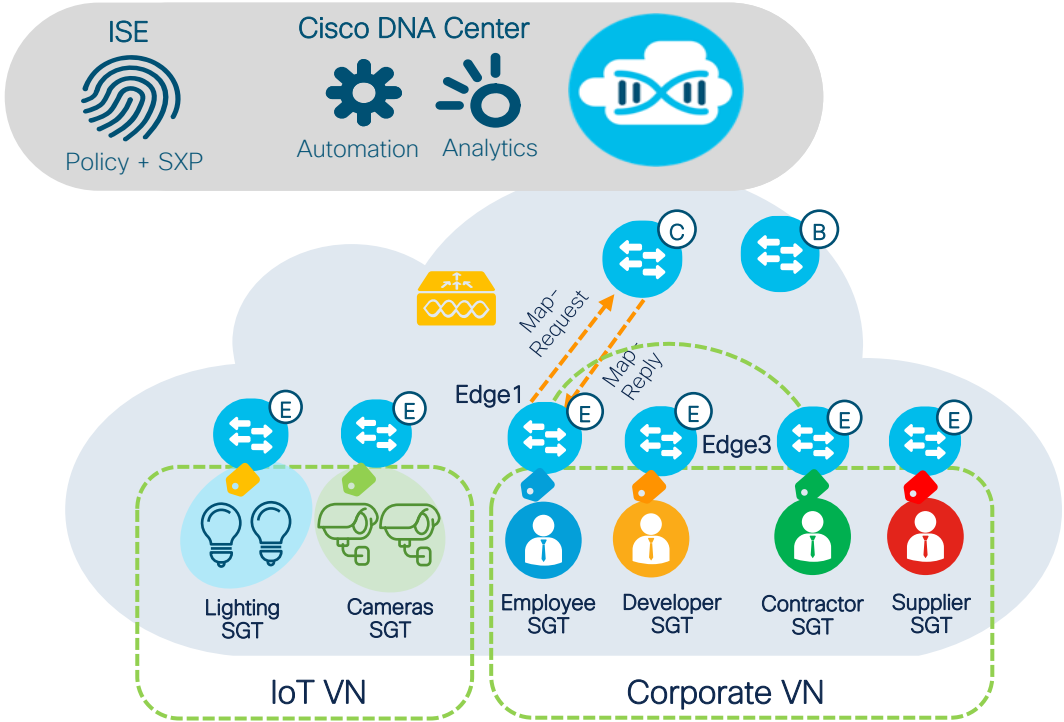
From TrustSec_Devices SGT 2 -> TrustSec_Devices SGT 2, permit ip
From TrustSec_Devices SGT 2 -> Unknown SGT 0, permit ip
From Unknown SGT 0 -> TrustSec_Devices SGT 2, permit ip

Cisco DNA Center Policy Whitelist vs Blacklist Model

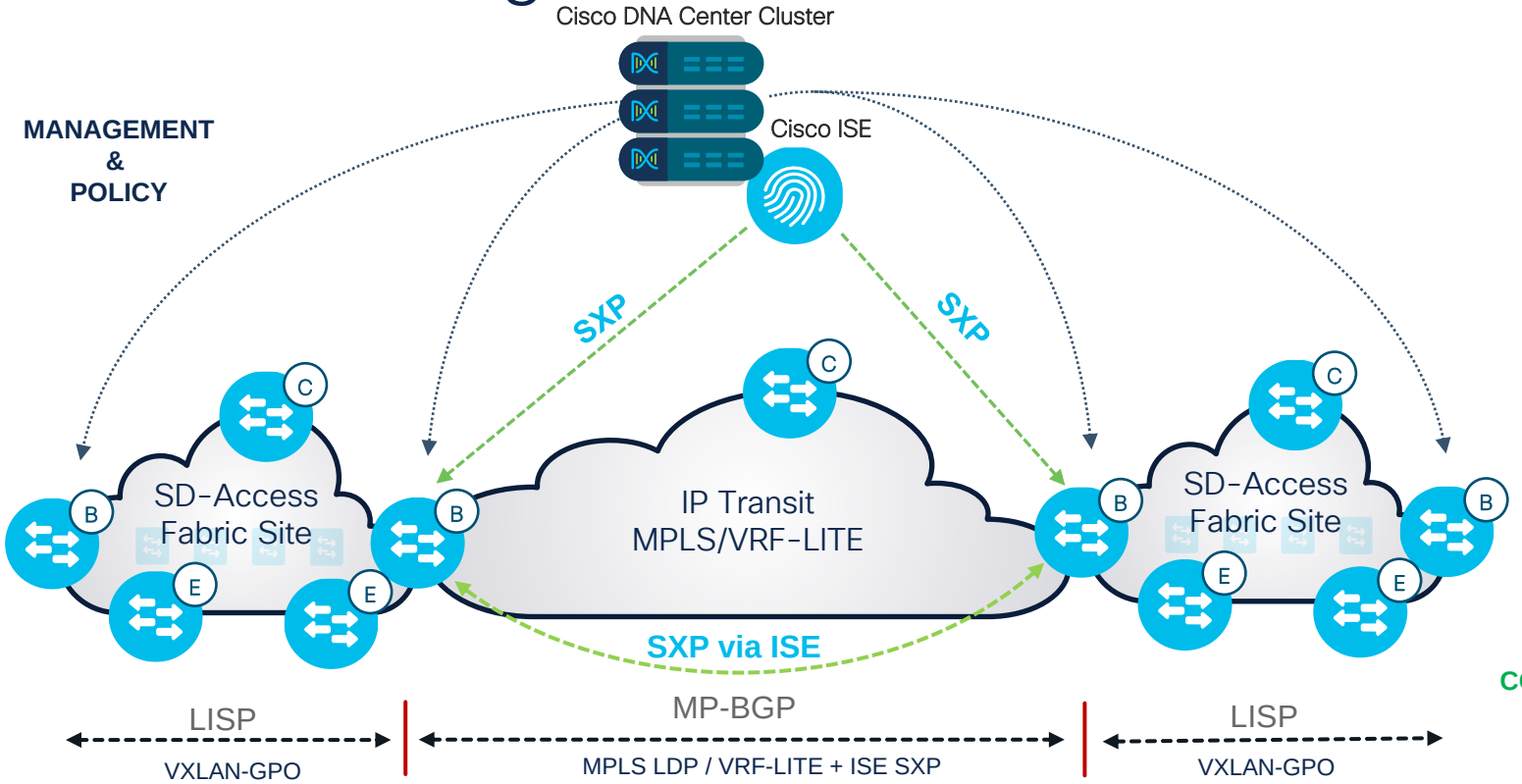


Design & Integration

Single Site Design
Segmentation within the Fabric

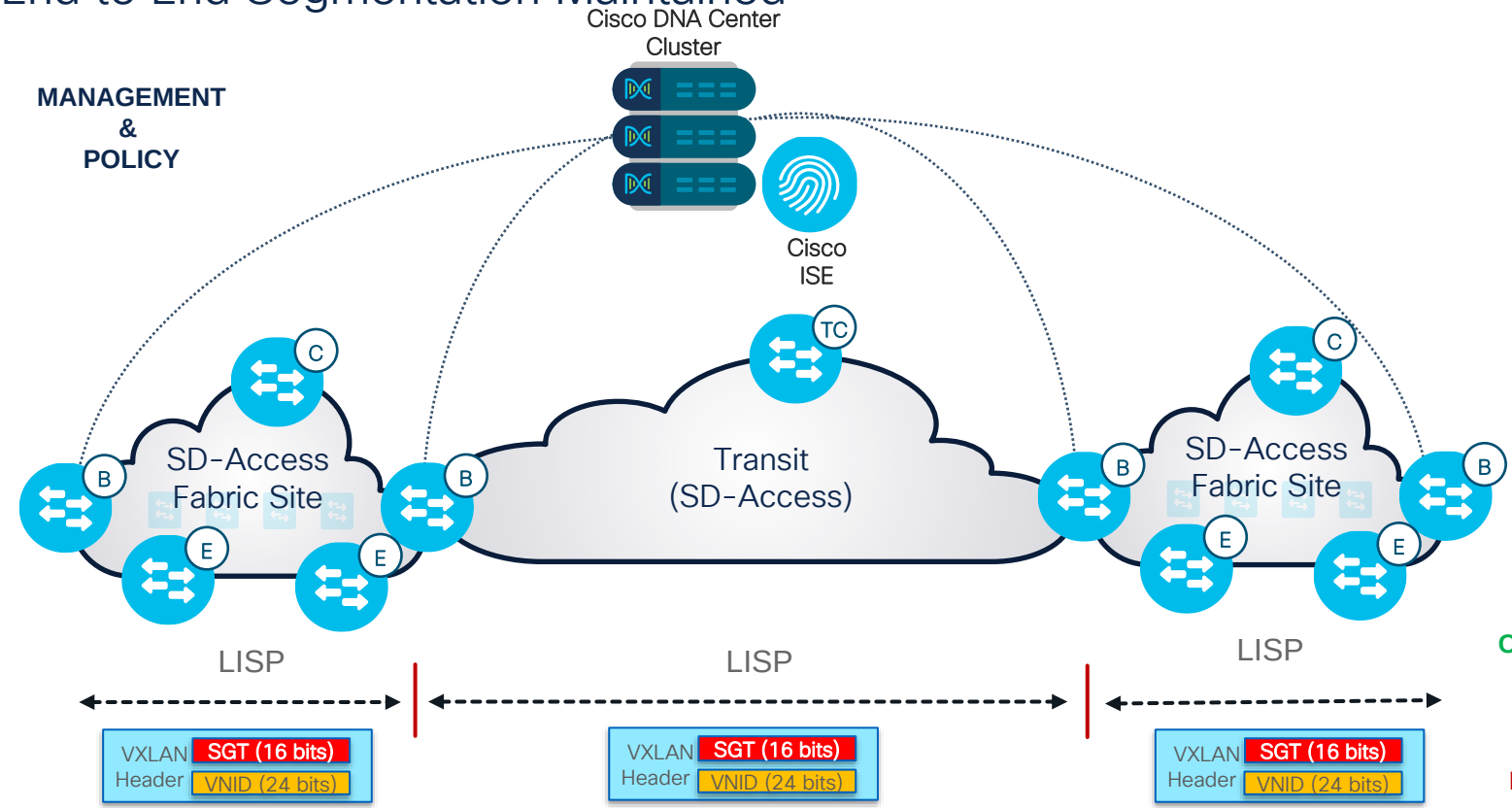


Multi-Site Design with IP Transit

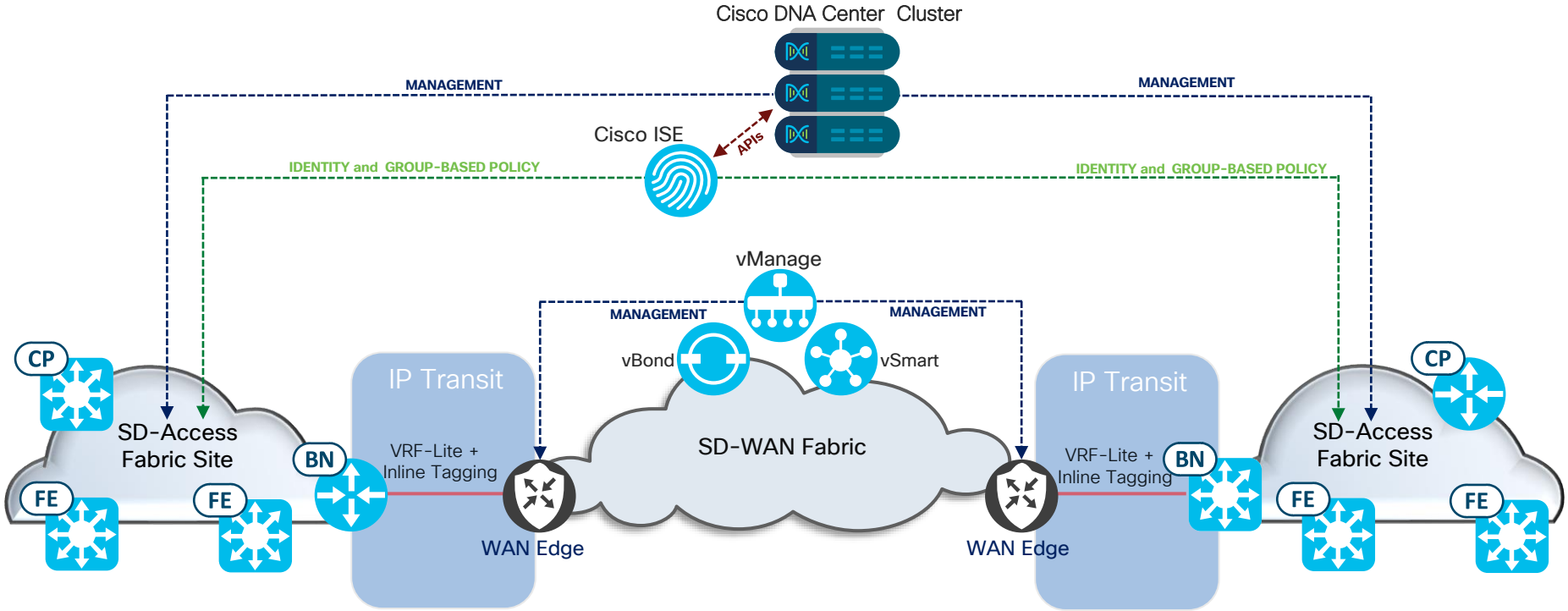


Multi-Site Design with SD-Access Transit

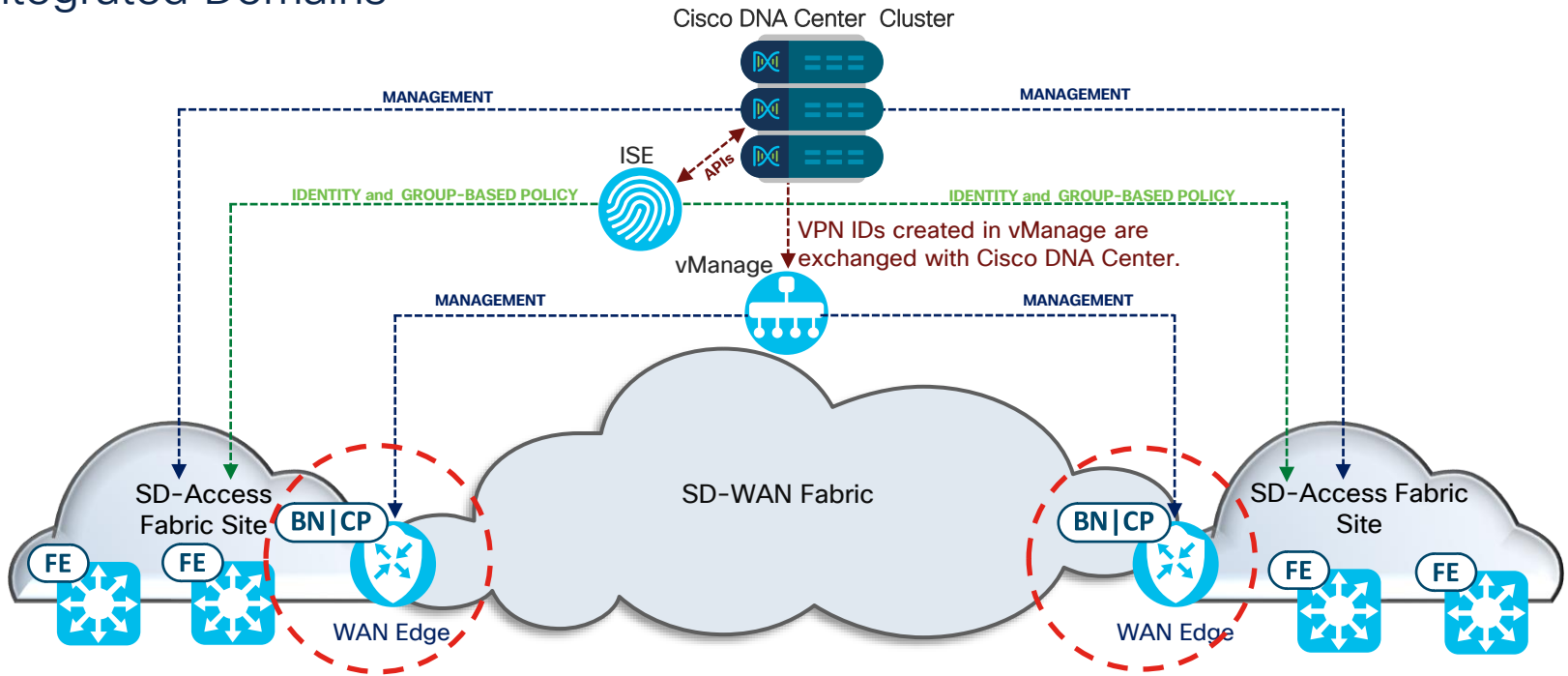
End to End Segmentation Maintained



Multi-Site Design with SD-WAN Transport
Independent Domains

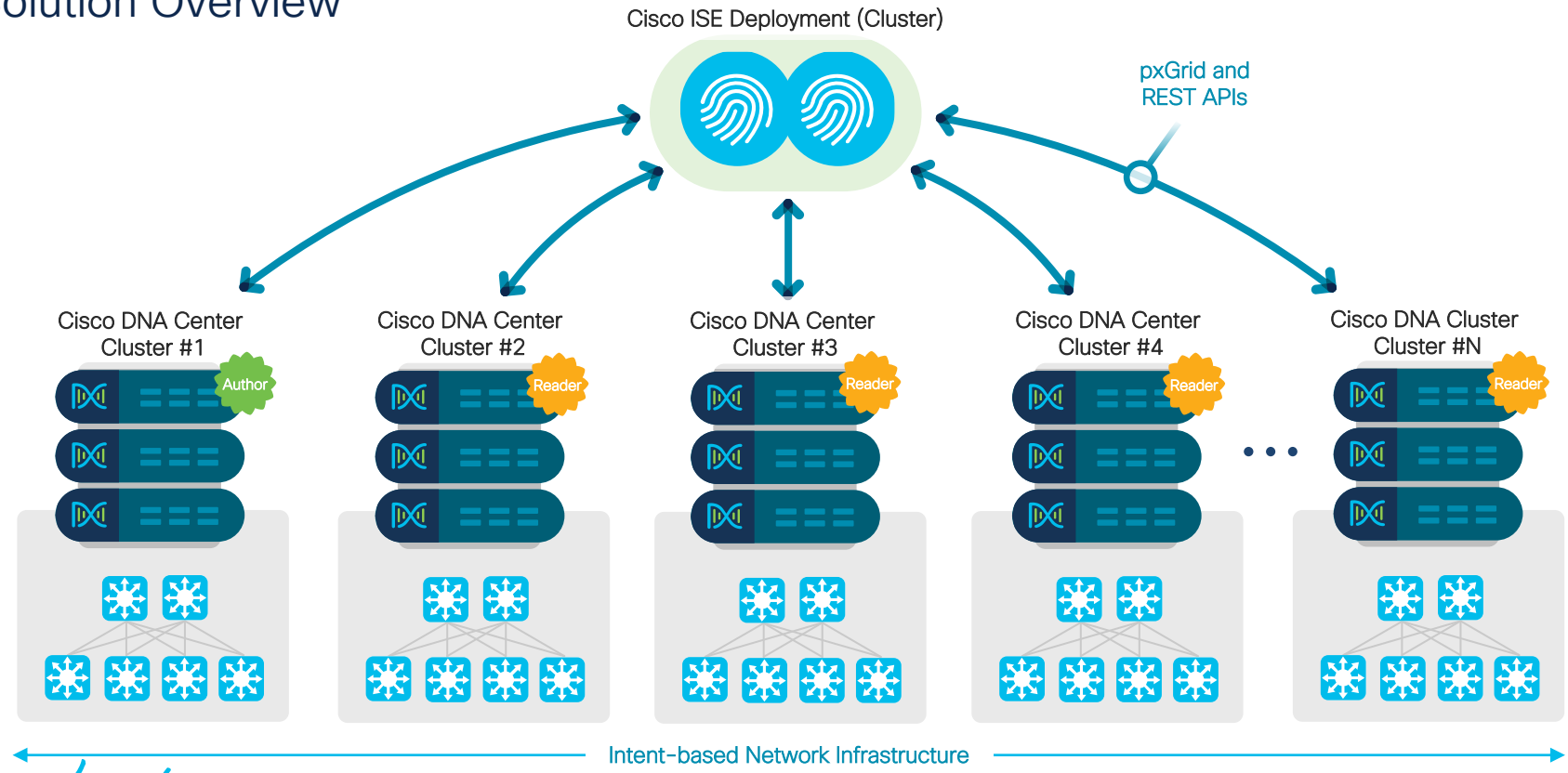


Multi-Site Design with SD-WAN Transit
Integrated Domains*

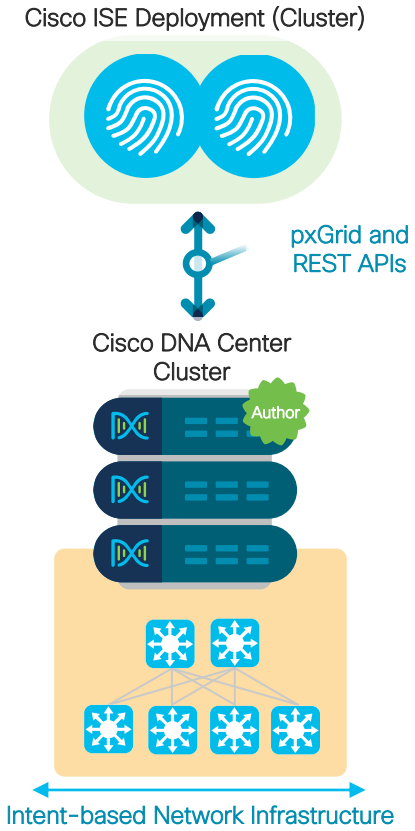


* - Limited Availability

Multiple Cisco DNA Center
Solution Overview

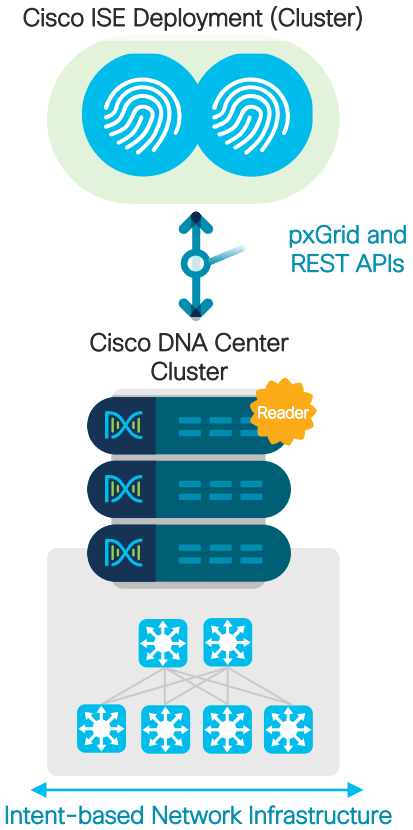


Multiple Cisco DNA Center
Author Node Cluster



- 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



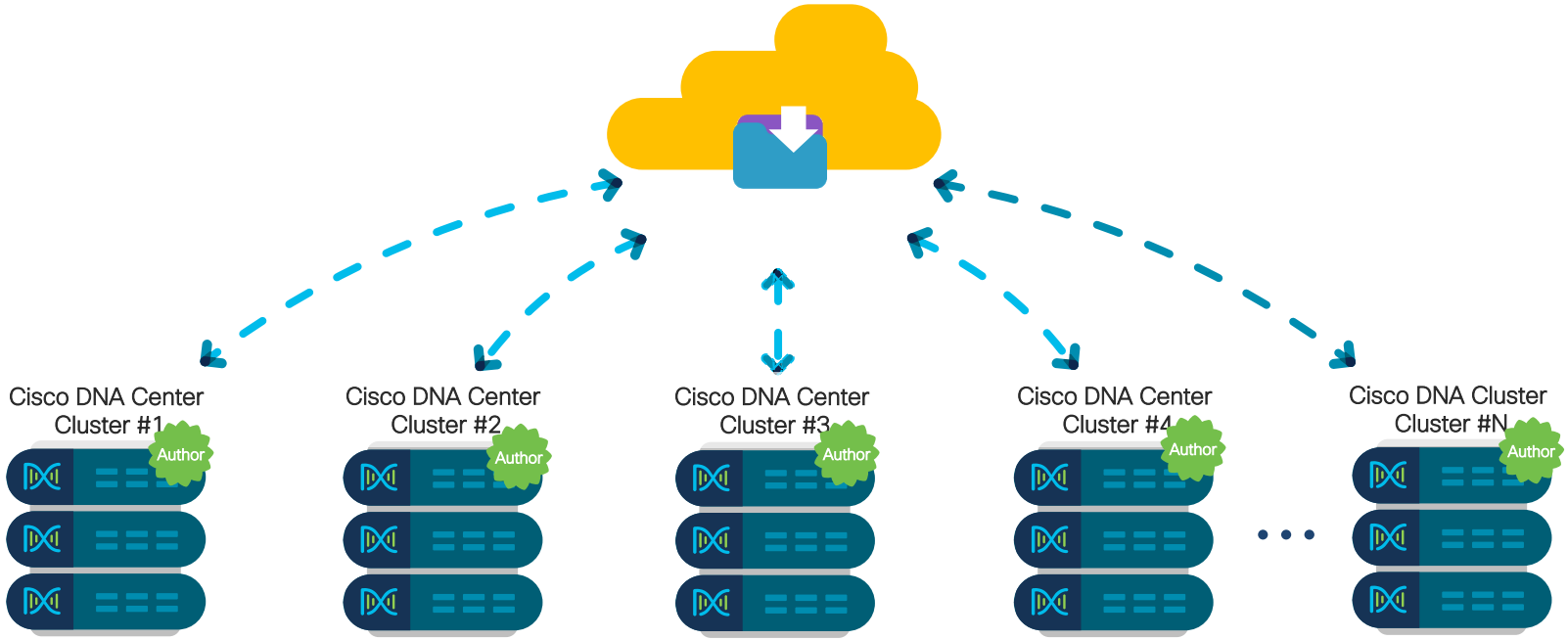
- Subsequent DNA Cluster to integrate with Cisco ISE
- Up to 4 Cisco DNA Center Center Clusters can be added as Reader Node Clusters.
- Read only view of VN, SGTs, Access Contracts, GBAC Policy and VN-SGT Associations
- Can only be a Greenfield Cisco DNA Center Cluster

Multiple Cisco DNA Center

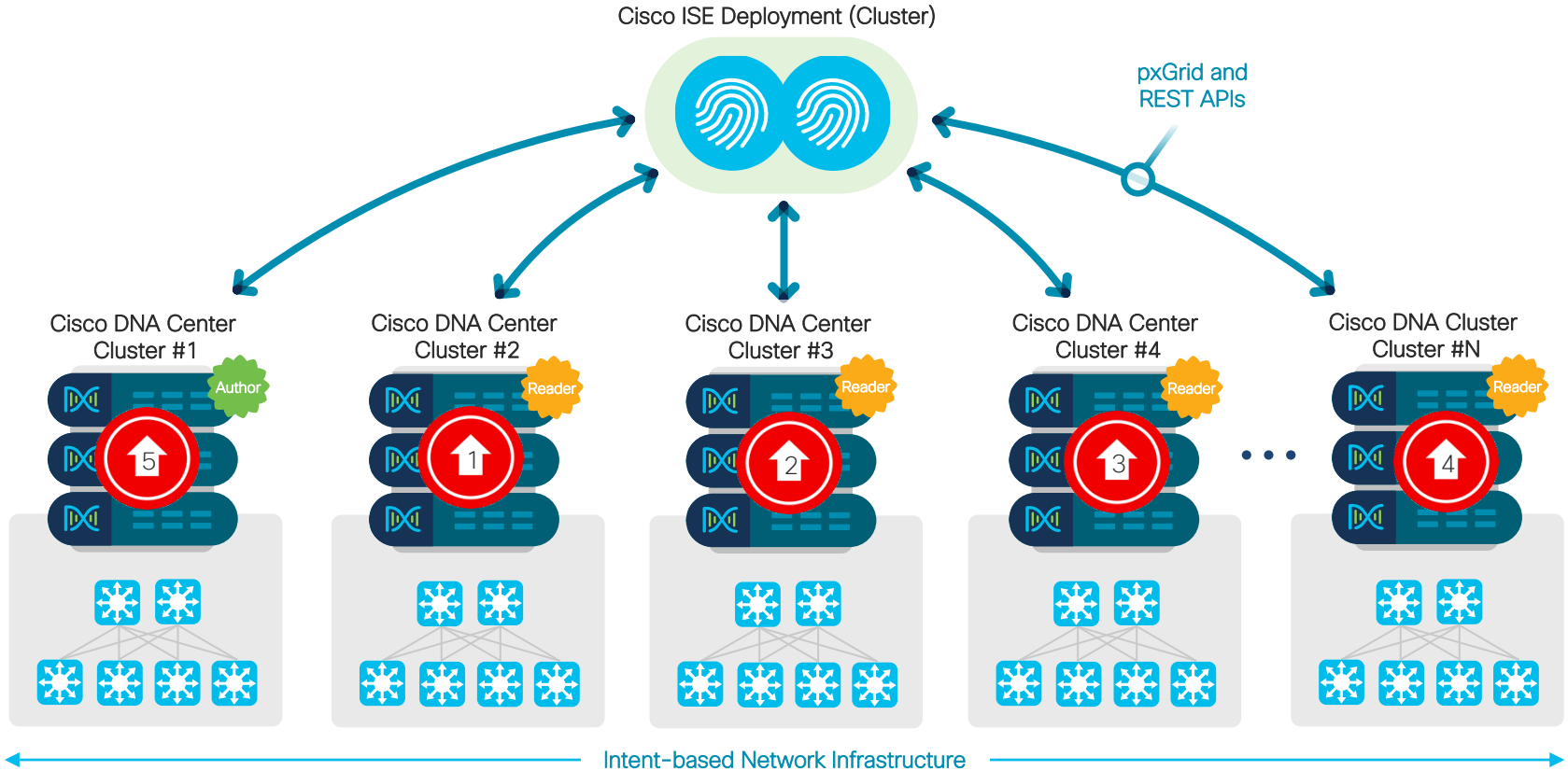
Multiple Cisco DNA Center Package and Installation

Connect with your Cisco Sales Representative or Channel Partner for:

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



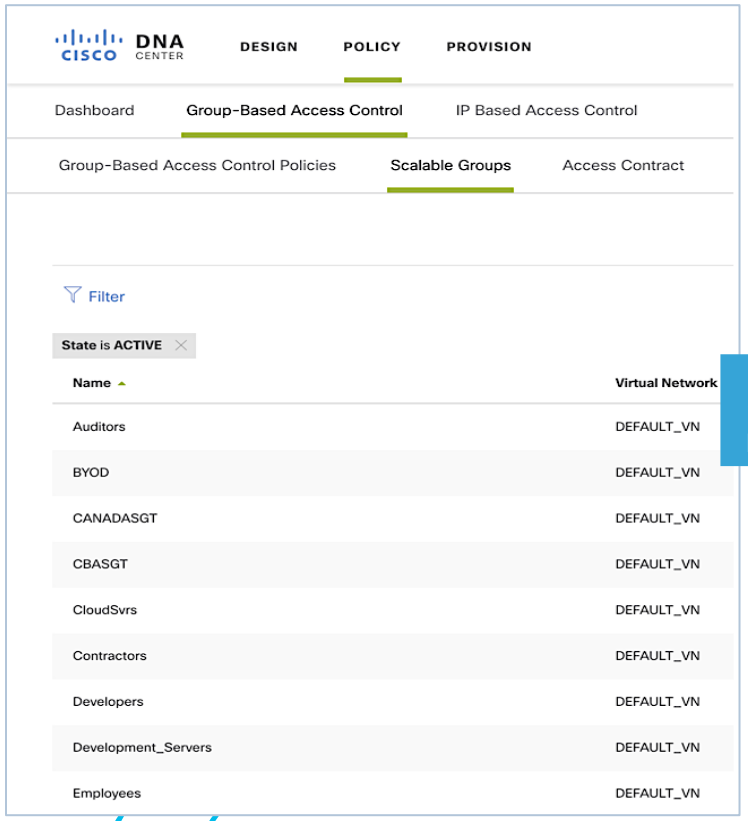
Multiple Cisco DNA Center
Upgrade Recommendations



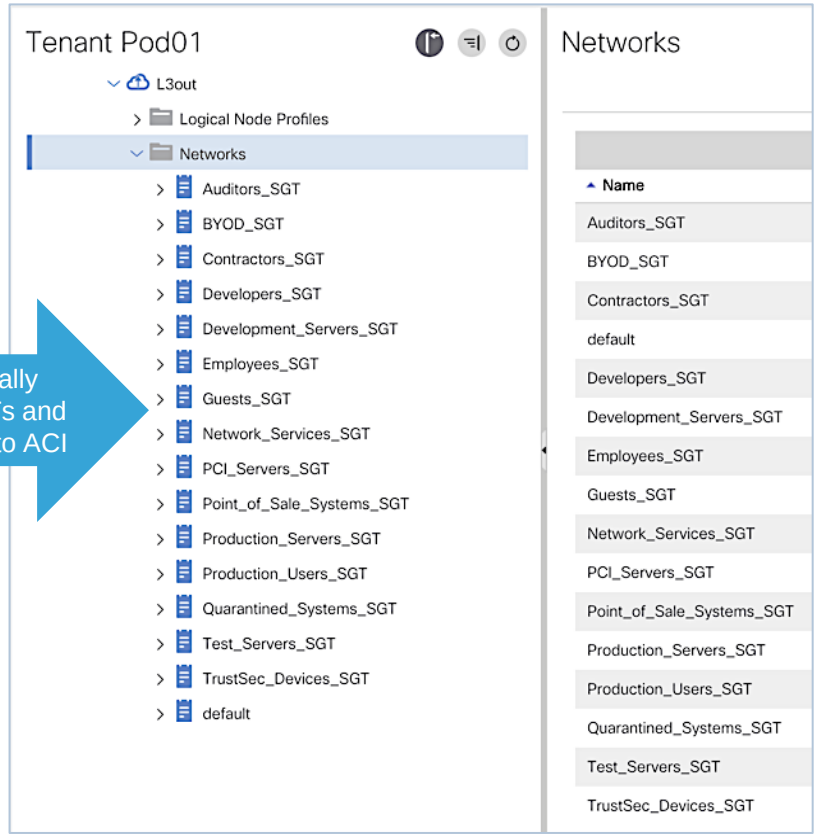
Cisco ISE and APIC
Consistent Polices Across Enterprise

- 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

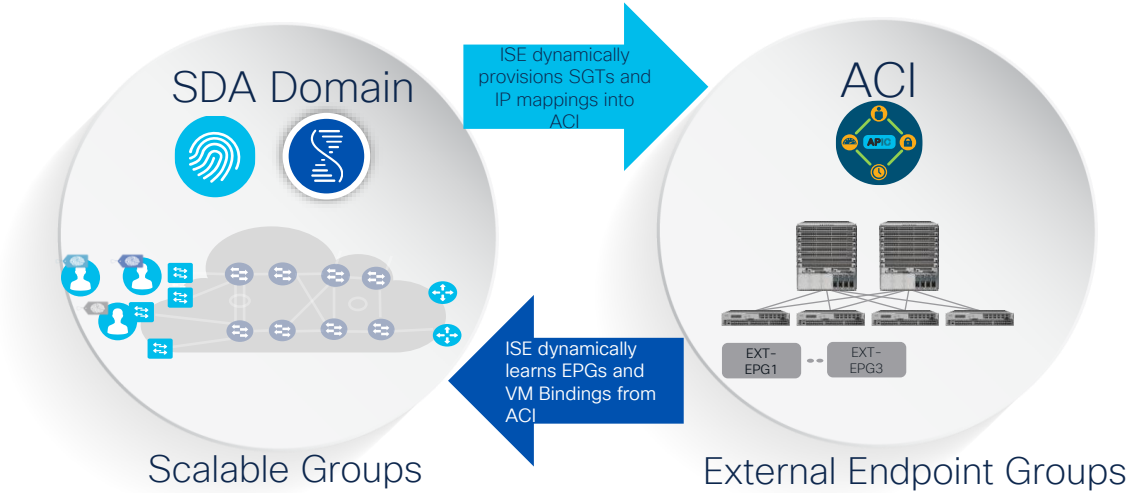


ISE dynamically provisions SGTs and IP mappings into ACI



Recommend
ISE 2.4 patch 6 or 2.6

Cisco ISE and APIC
Enforcement Scale in ACI



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

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

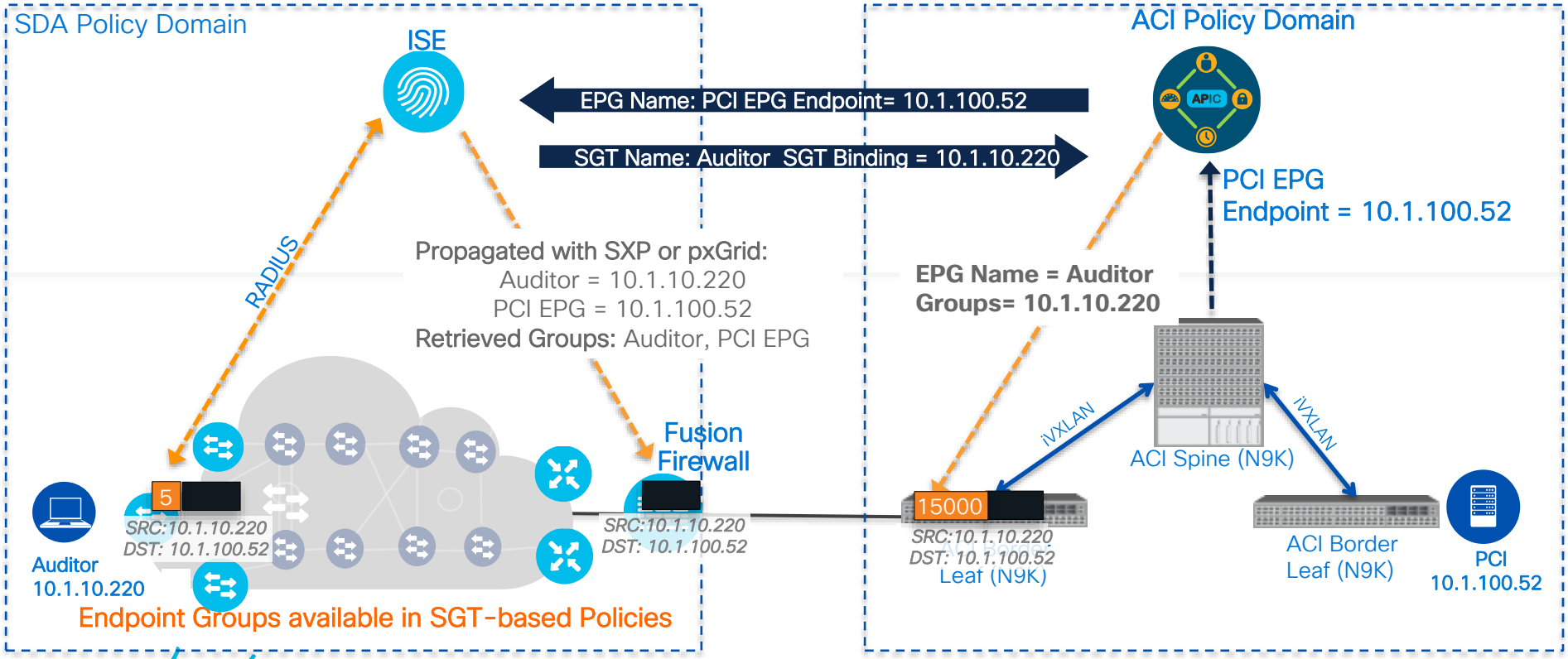
*Per pair of ISE SXP Nodes
** Per ISE pxGrid node

ACI 3.2 Scale EX, FX and FX2 Hardware

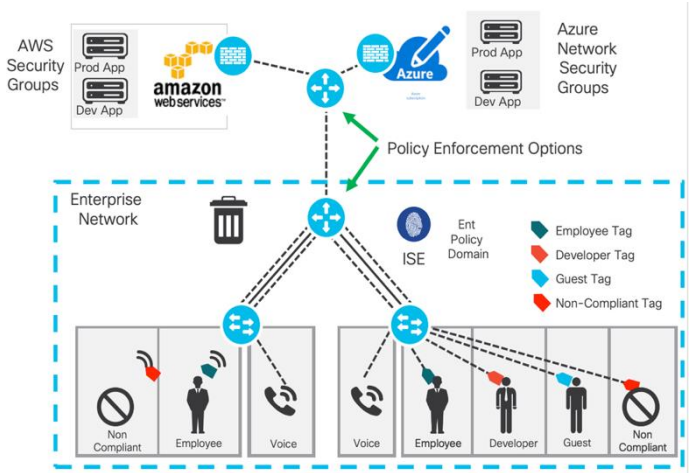
SGT -> External EPG	250
Number of Mappings	64,000
Mappings per External EPG	8000
Transaction rate (target)	100/s

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

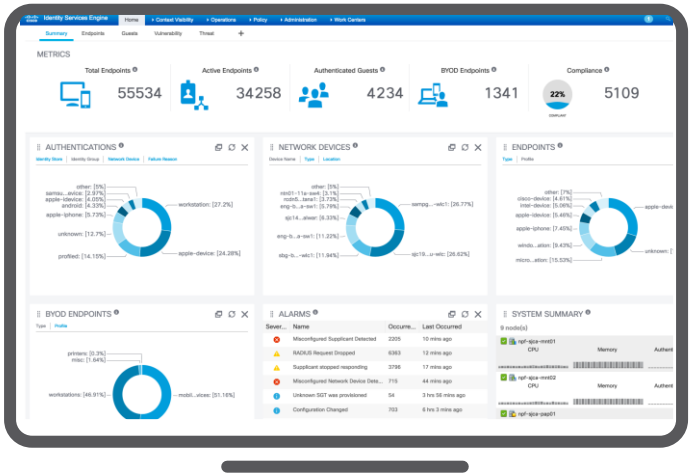
Increase Efficiency

Regulatory Compliance

Reduce OPEX

SUMMARY

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



MOBILITY

MICRO SEGMENTATION

SECURITY

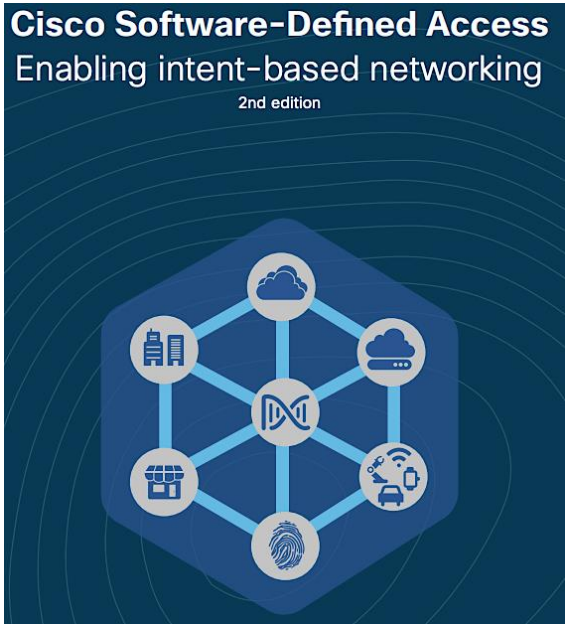
DEVICE ADMIN (TACACS+)

MULTI DOMAIN INTEGRATION

Cisco Solution e-books

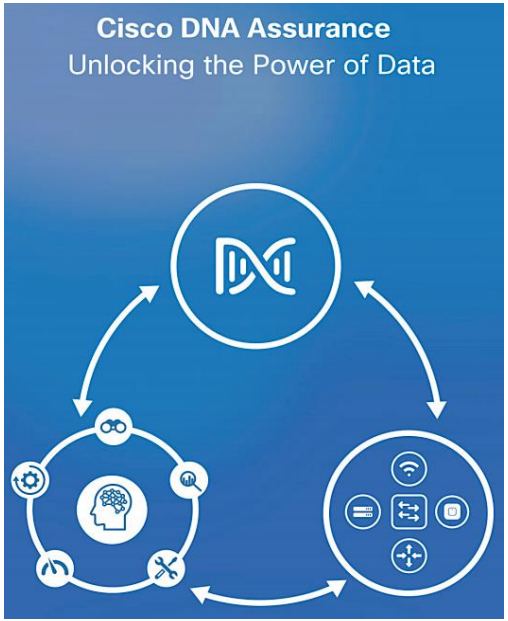
Cisco Software-Defined Access

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

Thank you


cisco Live!
ALL IN