You make **possible**

Best Practices for Design and Deployment of Software Defined Access (SDA)

Imran Bashir - Technical Marketing Engineer
Nidhi Pandey – Technical Marketing Engineer

BRKCRS-2502

Barcelona | January 27-31, 2020

THE LAST MILE

Your Presenters today

Nidhi Pandey

Imran Bashir

Assumptions

IMPORTANT NOTICE

This session assumes you have received DNA Center & SD-Access Training

If not… please complete one or all of the following training materials:

- CiscoLive
- Learning@Cisco
- dCloud Lab
- SDA Design CVD
- SDA Deploy CVD
- DNAC Guides

This session is based

- Product Compatibility Matrix

For a list of current capabilities, restrictions, limitations & caveats refer to:

- DNAC Release Notes

Icons Used Throughout the BRKCRS-2502

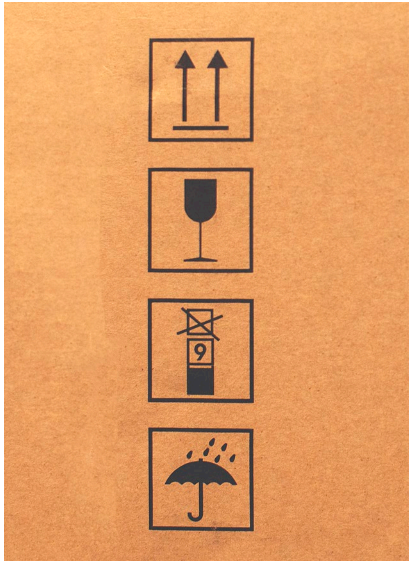
For your reference

- For Your Reference – These items will usually NOT be covered in detail during the session

- Content enlarging – when something is not visible enough, we highlight and enlarge this area.

- GUI navigation assistant – This special type of highlighting is used to help you in navigation in the Graphical User Interface of a product.

- Hidden Content – slides which won’t be presented during the session. Primarily, those slides are here to give you more detailed information.



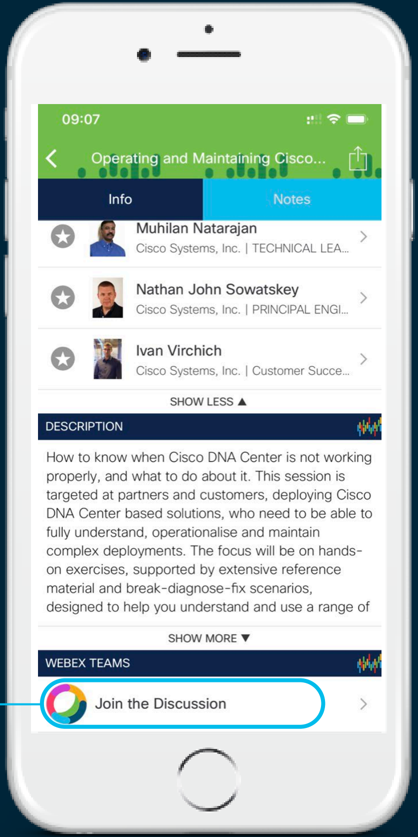
Cisco Webex Teams

Questions?

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

How

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



Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

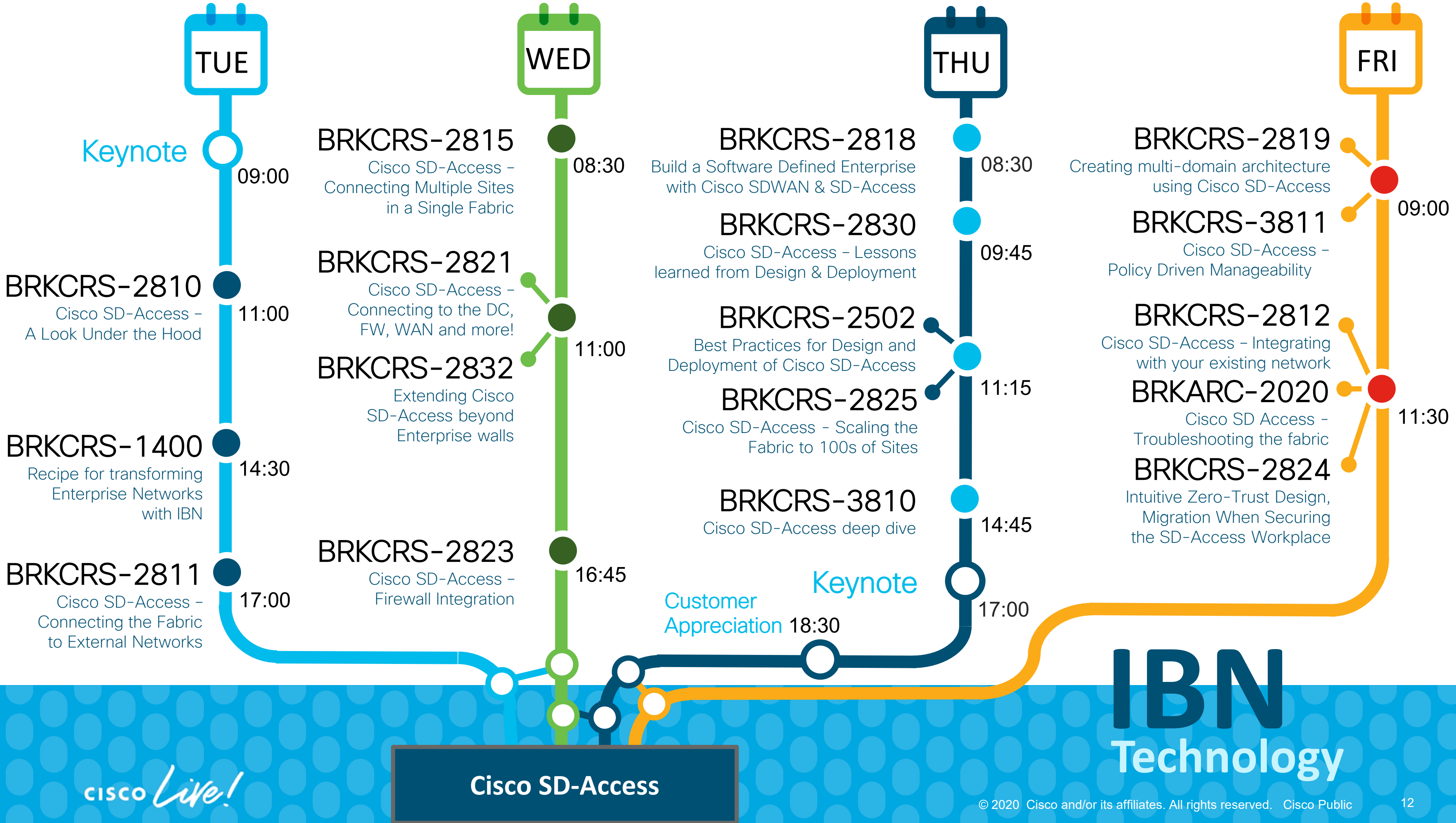
Agenda

- Introduction
- Sample Customer Requirements
- General Design Considerations
- Best Practices for Wired and Wireless
- Segmentation and Policy Best Practices
- Migration Considerations
- Security Best Practice
- Designing Customer Network
- Demo (if time permits)
- Conclusion

Are New to SD-Access ?

Have deployed SD-Access in lab or at customers place

Have design discussions with your customer about SD-Access



TUE

Keynote 09:00

BRKCRS-2810
Cisco SD-Access –
A Look Under the Hood
11:00

BRKCRS-1400
Recipe for transforming
Enterprise Networks
with IBN
14:30

BRKCRS-2811
Cisco SD-Access –
Connecting the Fabric
to External Networks
17:00

WED

BRKCRS-2815
Cisco SD-Access –
Connecting Multiple Sites
in a Single Fabric
08:30

BRKCRS-2821
Cisco SD-Access –
Connecting to the DC,
FW, WAN and more!
11:00

BRKCRS-2832
Extending Cisco
SD-Access beyond
Enterprise walls

BRKCRS-2823
Cisco SD-Access –
Firewall Integration
16:45

THU

BRKCRS-2818
Build a Software Defined Enterprise
with Cisco SDWAN & SD-Access
08:30

BRKCRS-2830
Cisco SD-Access – Lessons
learned from Design & Deployment
09:45

BRKCRS-2502
Best Practices for Design and
Deployment of Cisco SD-Access
11:15

BRKCRS-2825
Cisco SD-Access – Scaling the
Fabric to 100s of Sites

BRKCRS-3810
Cisco SD-Access deep dive
14:45

Keynote
17:00

Customer
Appreciation 18:30

FRI

BRKCRS-2819
Creating multi-domain architecture
using Cisco SD-Access
09:00

BRKCRS-3811
Cisco SD-Access –
Policy Driven Manageability

BRKCRS-2812
Cisco SD-Access – Integrating
with your existing network
11:30

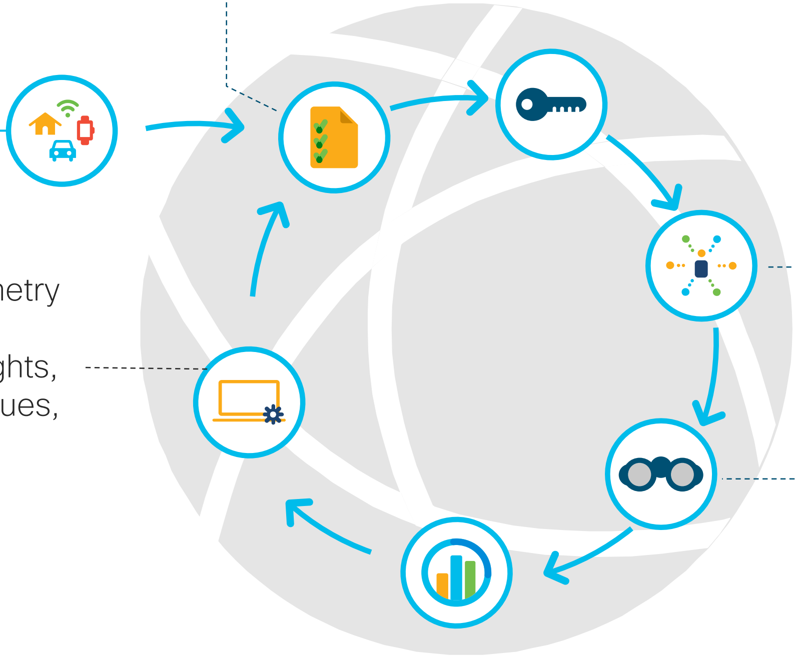
BRKARC-2020
Cisco SD Access –
Troubleshooting the fabric

BRKCRS-2824
Intuitive Zero-Trust Design,
Migration When Securing
the SD-Access Workplace

Cisco SD-Access

IBN
Technology

Rethink networking, think intent-based



Business intent: Deploy IoT sensors

1. **Network execution:** High security, high availability, normal priority
2. **Automate**: Translate intent to policy and configure network devices
3. **Secure**: Recognize IoT devices and place into appropriate network segments as per policy
4. **Assure**: Collect telemetry data from network, analyze, provide insights, discover potential issues, and remediate

SD-Access

Enabling your Journey to next-gen Digital Experiences

Always-On

Secure

Assured Experiences

Everything is Possible

Cisco SD-Access Customer Momentum

Fastest Ramping SD-X Solution!

wipro

ATM
TEXAS A&M
UNIVERSITY

70th Anniversary
70 Years of Beauty Creation
AMOREPACIFIC

SAFETY TREATMENT RESPONSIBILITY
DEPARTMENT OF
STATE HOSPITALS

RoyalCaribbean
INTERNATIONAL

MONTANA STATE UNIVERSITY
1893
BOZEMAN - MONTANA

DB BAHN

Meet your Customers

IBM
Network Services

felixplatterspital

AstraZeneca

UO
N
University of Northampton

ALABAMA
GREAT SEAL

Children's Hospital
LOS ANGELES
We Treat Kids Better

CISCO
Cisco IT

SCENTSY

LEGO

www.cisco.com/c/en/us/solutions/enterprise-networks/network-architecture-customer-success-stories.html

Customer Requirement – Healthcare Vertical

Customer will be onboarding two new clinical facilities and is striving towards a unified architecture to minimize operational overhead and to drive simplicity. Security is top of mind for the CIO.

Land & Layout

- 10,000 users/endpoints for facility 1 and 1000 users/endpoints in facility 2.

Existing Baseline Architecture

- Existing baseline architecture has VLAN based segmentation in place today (Corp users, ER, Medical Devices, Printers, Guest, Building Management, Cameras etc)
- Port-Security for limiting mac-address.
- MPLS circuit to connect other branches/sites. Internet breakout at everysite.
- OSPF for Campus Routing.
- No VRF based routing in backbone today; relies on GRT.
- Long term strategy is to consider SD-WAN for branch/DC interconnect.
- Microsoft AD for User, Computer Accounts.
- IOT devices with ”static” ip address, which need to operate in Layer2 domain.
- Wireless Guest Anchor for Guest Access.

Customer Requirement – Manufacturing Vertical

A manufacturing customer has 15 facilities in a Metro Area Network, all interconnected via dark fiber. They all connect back to Corporate HQ to access billing servers.

Local facilities have internet and DC breakouts.

Land & Layout

- Each local facilities have ~ 250 users
- HQ have ~1000 users.

Existing Baseline Architecture

- Uses ISE to profile headless endpoints – IOT, Printers, IP Phones.
- OSPF for Campus Routing.
- No VRF based routing in backbone today; relies on GRT.
- Local Guest Firewall at each facility
- Top of Mind

- Seamless policy propagation
- Seamless Mobility – wherever possible (Wired > Wired, Wired > Wireless) within a facility.
- Optimize Guest Traffic flow.
- Cross Domain policy propation/integration across sites.

Customer Requirement – Enterprise Vertical

Customer will be migrating the global centers to Fabric and also build fabric is few new sites.

Land & Layout

- Dual stack architecture, Datacenter and fabric integration

Top of Mind

- Existing baseline architecture has VLAN based segmentation in place today
- Port-Security for limiting mac-address.
- MPLS circuit to connect other branches/sites. Internet breakout at every site.
- OSPF for Campus Routing.
- Existing ISE and AD architecture
- Fabric wireless
- Seamless mobility
- Same subnet for static endpoints

The Challenge...

"I want to design and deploy a SD-Access network."

Optimization

On time

Business Critical

Scale

Endpoints

Design options

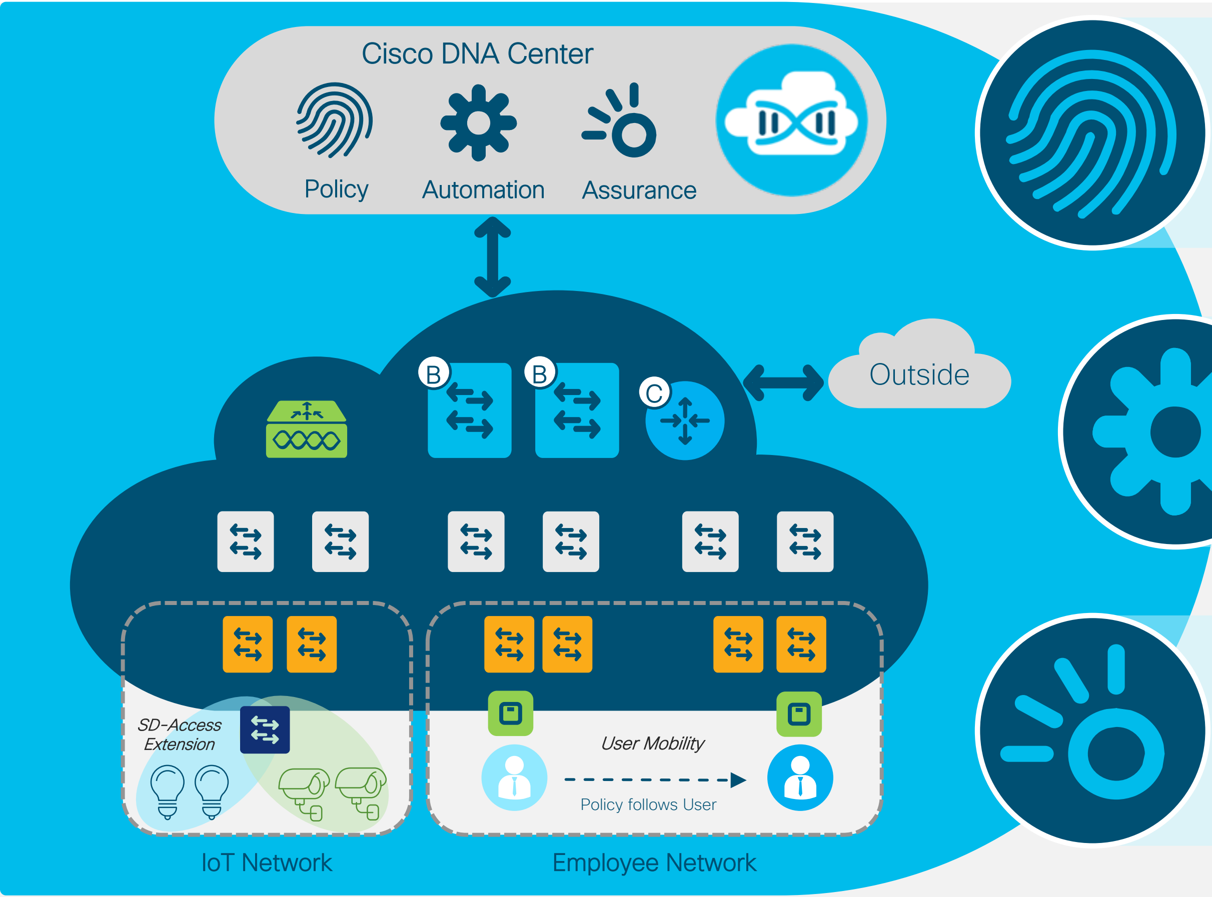
Platform choices

Software choices

SDA Technology Review

Cisco Software Defined Access

The Foundation for Cisco's Intent-Based Network



Identity-Based Policy and Segmentation

Policy definition decoupled from VLAN and IP address

Automated Network Fabric

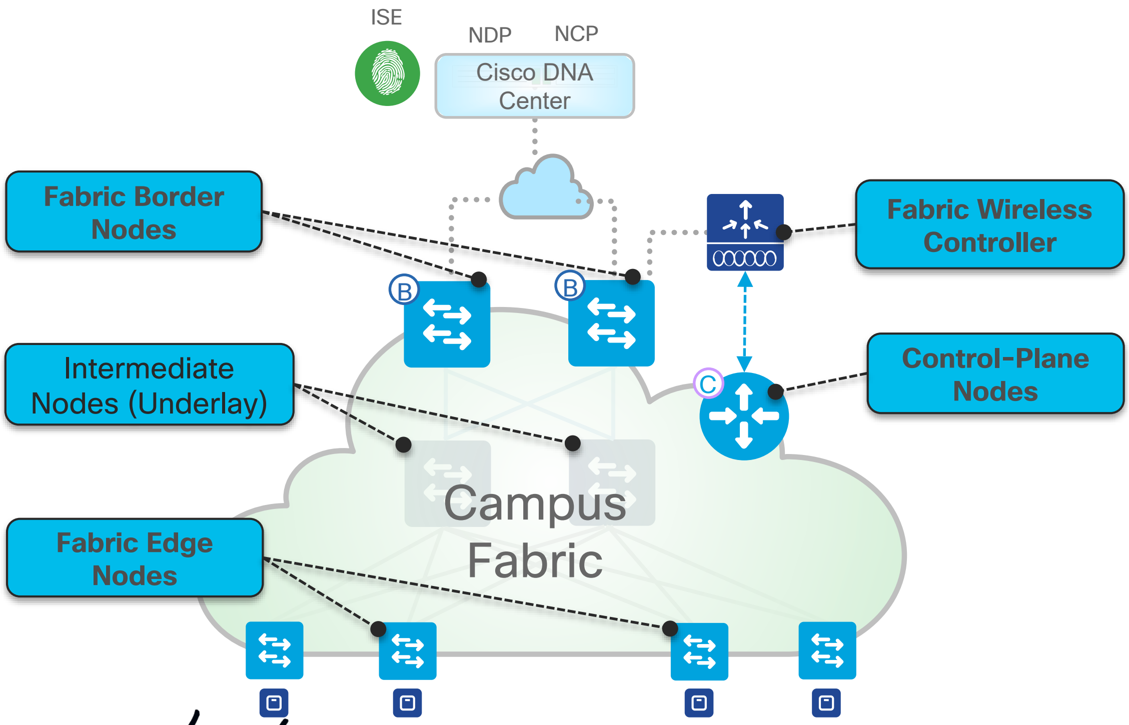
Single fabric for Wired and Wireless with full automation

Insights and Telemetry

Analytics and insights into User and Application experience

SD-Access Architecture

Fabric Roles & Terminology



- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships. This is a combination of the MS and MR.
- **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 APs and Wireless Endpoints to the SD-Access Fabric

SD-Access

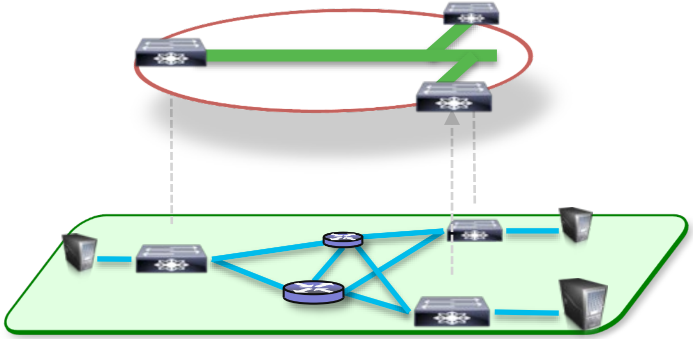
What exactly is a Fabric?

Recap

A Fabric is an Overlay

An *Overlay network* is a *logical topology* used to *virtually connect* devices, built over an arbitrary physical *Underlay* topology.

An *Overlay network* often uses *alternate forwarding attributes* to provide additional services, not provided by the *Underlay*.



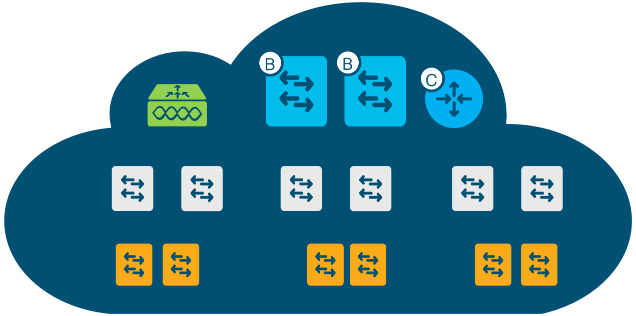
cisco Live!

SD-Access Fabric

Campus Fabric - Key Components

Recap

1. Control-Plane based on **LISP**
2. Data-Plane based on **VXLAN**
3. Policy-Plane based on **CTS**

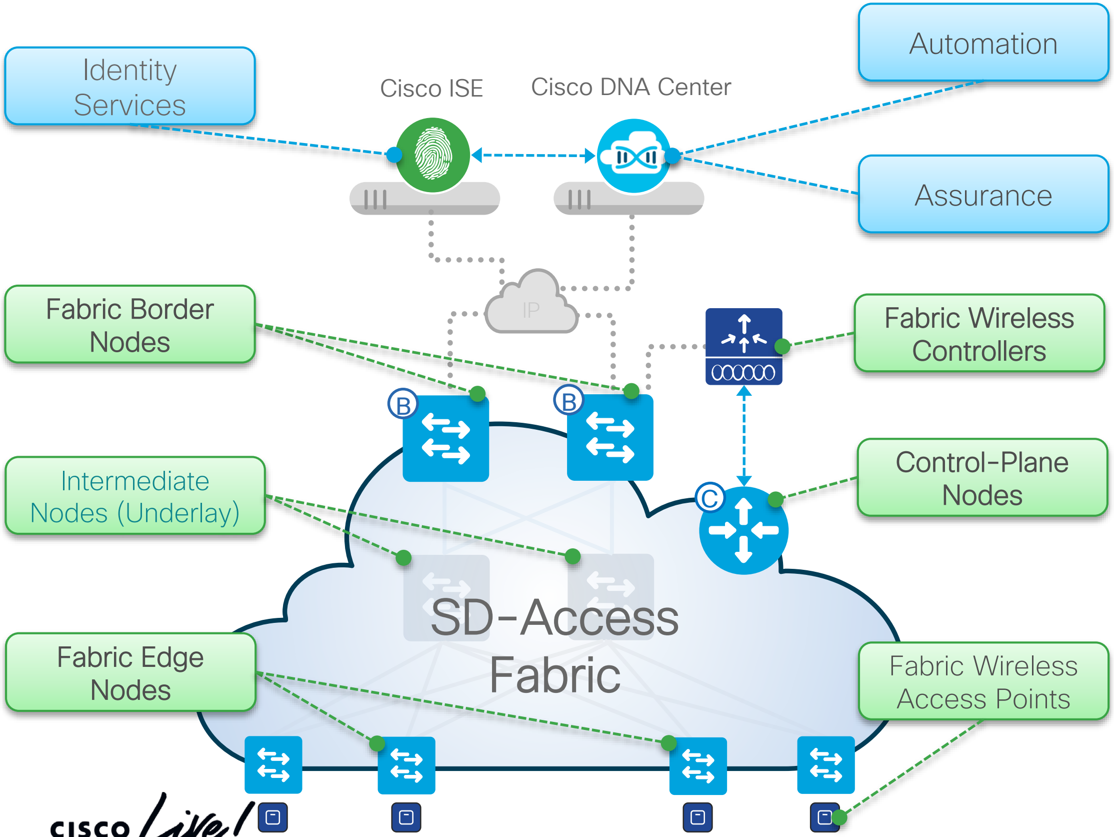


Key Differences

- L2 + L3 Overlay -vs- L2 or L3 Only
- Host Mobility with Anycast Gateway
- Adds VRF + SGT into Data-Plane
- Virtual Tunnel Endpoints (Automatic)
- NO Topology Limitations (Basic IP)

Cisco SD-Access

Fabric Roles & Terminology

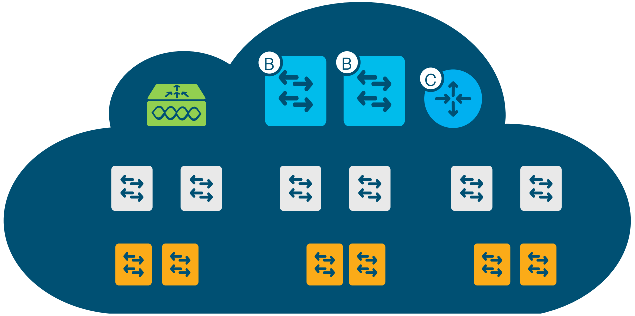


- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric network status
- **Identity Services** – NAC & ID Services (e.g. ISE) for dynamic Endpoint 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

SD-Access Fabric

Campus Fabric - Key Components



1. **Control-Plane** based on **LISP**
2. **Data-Plane** based on **VXLAN**
3. **Policy-Plane** based on **CTS**

SD-Access Fabric

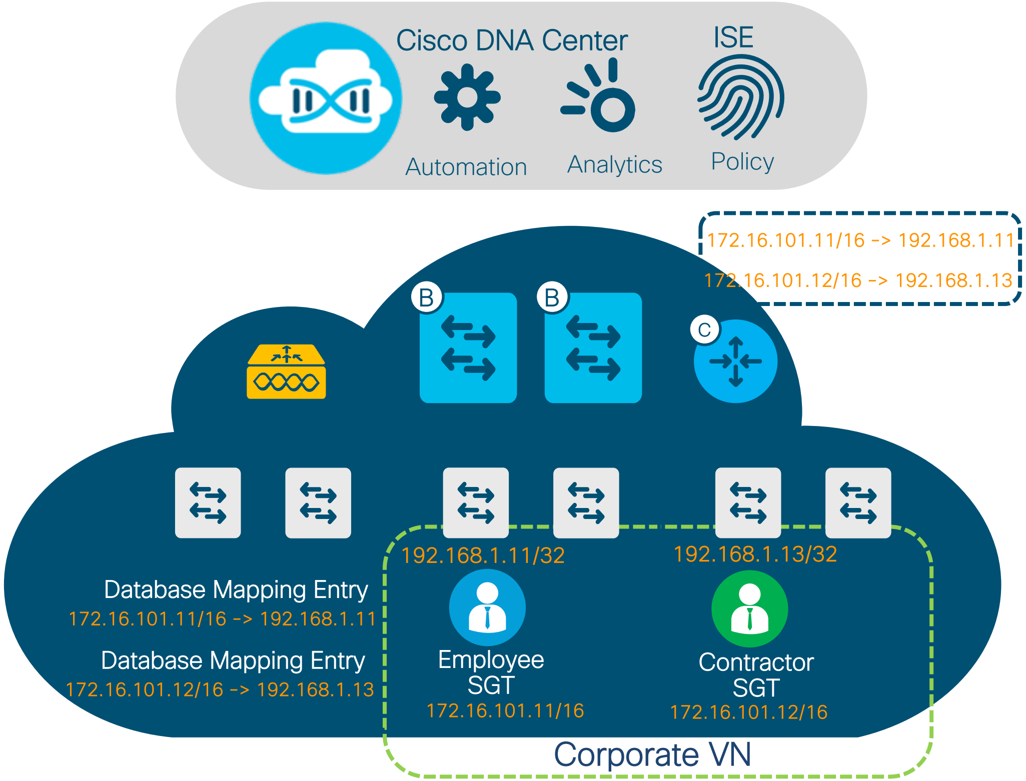
LISP Control Plane

Fabric nodes use LISP as a control plane for Endpoint Identifier (EID) and Routing Locator (RLOC) info

Fabric Control Plane node acts as a Map Server / Resolver for EID to RLOC mappings

Fabric Edge and Internal Border devices registers EIDs to the Map Server.

External Border node acts as PXTR (LISP Proxy Tunnel Router) and provides default gateway when no mapping exists.



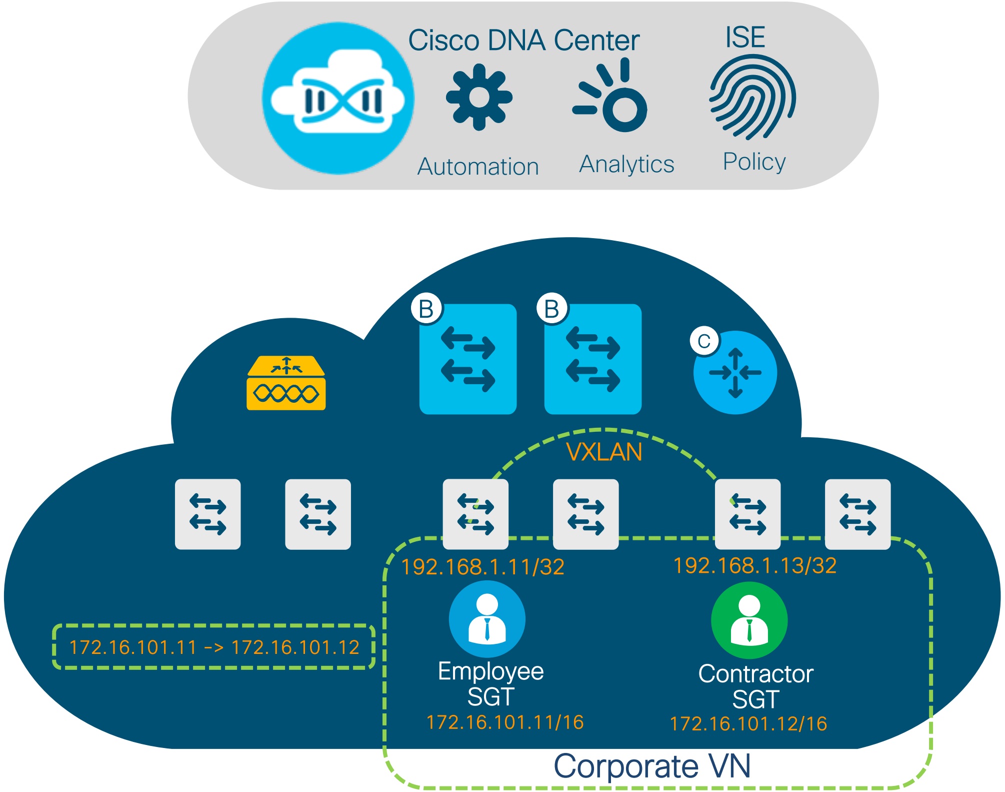
SD-Access Fabric

VXLAN Data Plane

Fabric nodes use VXLAN (Ethernet Based) as the data plane which supports both L2 and L3 overlay.

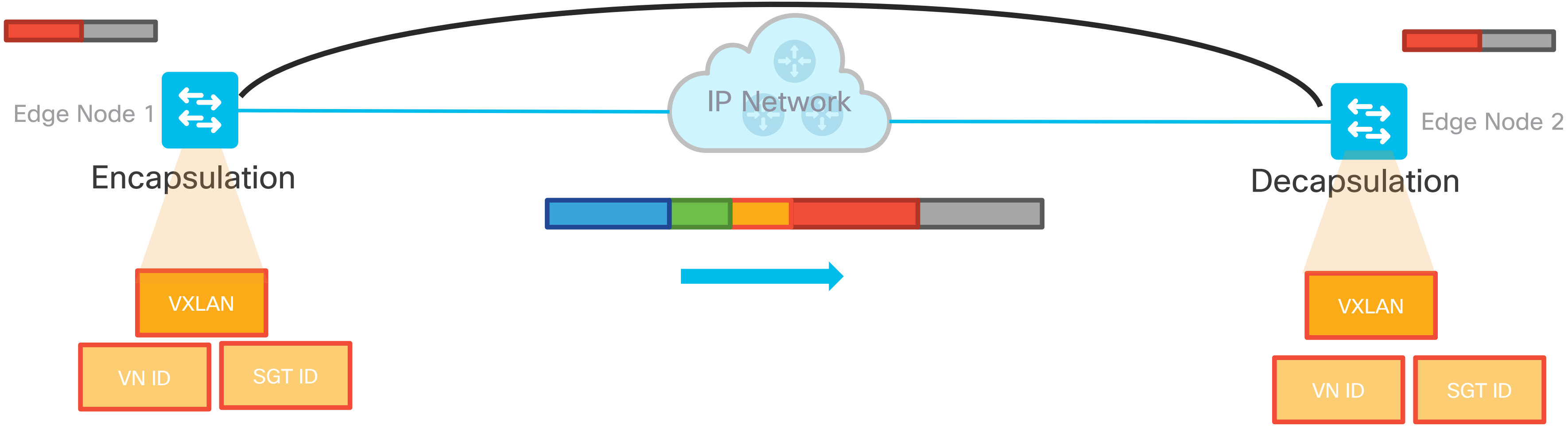
VXLAN header contains VNID (VXLAN Network Identifier) field which allows up to 16 million VNI

VXLAN header also has Group Policy ID for Scalable Group Tags (SGTs) allowing 64,000 SGTs.



Group-Based Policy

Ingress Classification & Egress Enforcement



Classification
Static or Dynamic VN and SGT assignments

Propagation
Carry VN and Group context across the network

Enforcement
Group Based Policies ACLs, Firewall Rules

SD-Access Fabric

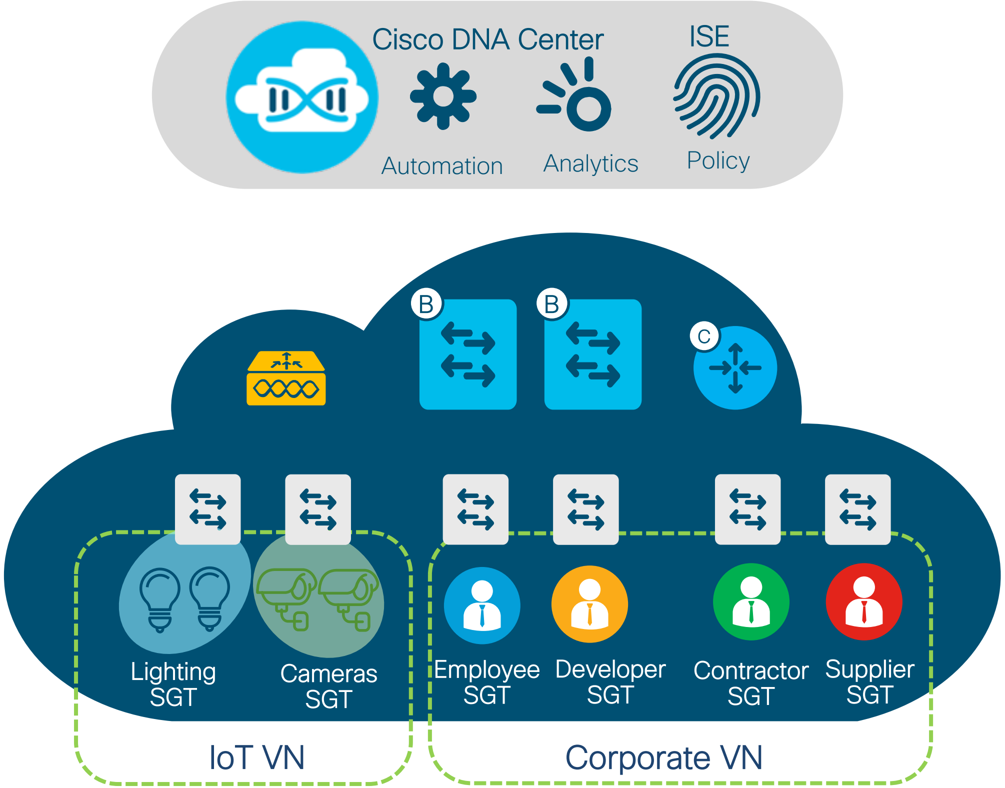
Cisco TrustSec Policy Plane

Scalable Group Tag (SGT) is a logical construct defined/identified based on the user and/or device context.

ISE dynamically assign SGTs to the users and devices coming to the network fabric.

Nodes add SGTs to the fabric encapsulation when communicating between the users and devices.

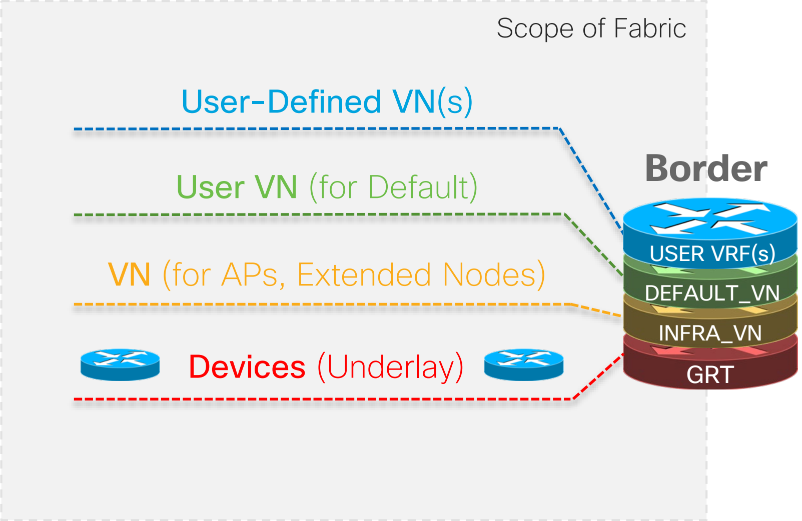
Edge and border nodes enforce the SGACL policies and contracts for the SGTs they protect locally.



SD-Access Fabric

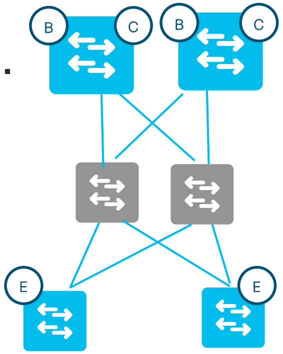
How VNs work in SD-Access

- **Fabric Devices (Underlay)** connectivity is in the Global Routing Table
- **INFRA_VN** is only for Access Points and Extended Nodes in GRT
- **DEFAULT_VN** is an actual "User VN" provided by default
- **User-Defined VNs** can be added or removed on-demand

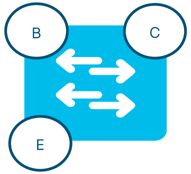


Fabric Roles

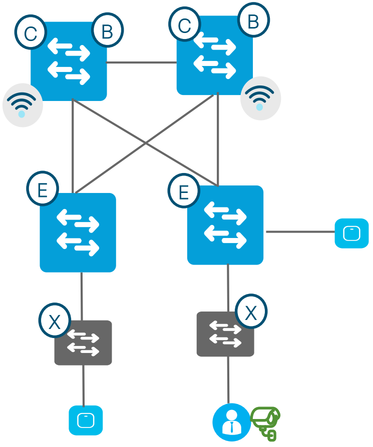
1.



2.



3.



- Border, Control Plane, Edge are fabric roles. One device can perform more than one function.

- WLC can be embedded in the 9k switches.

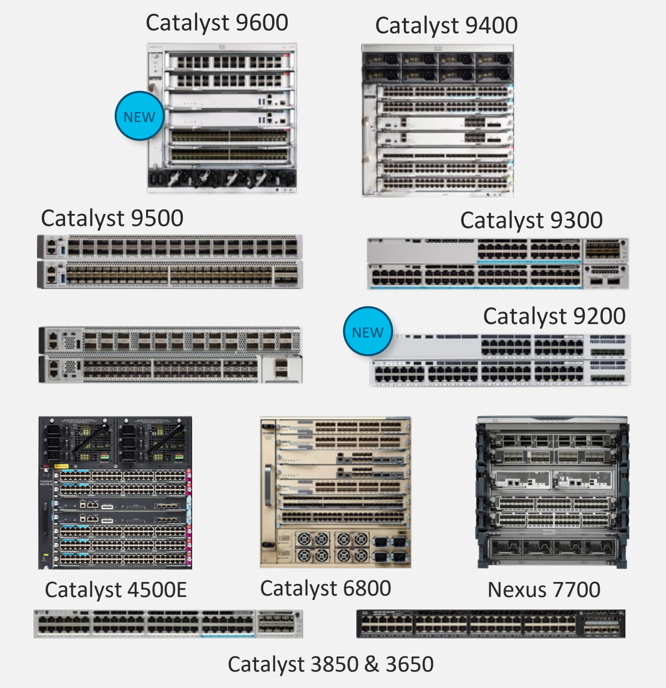
1. Co-located B/CP
2. FIAB
3. Embedded WLC

SD-Access Support

Digital Platforms for your Cisco Digital Network Architecture

For more details: cs.co/sda-compatibility-matrix

Switching



Catalyst 9600

Catalyst 9400

Catalyst 9500

Catalyst 9300

Catalyst 9200

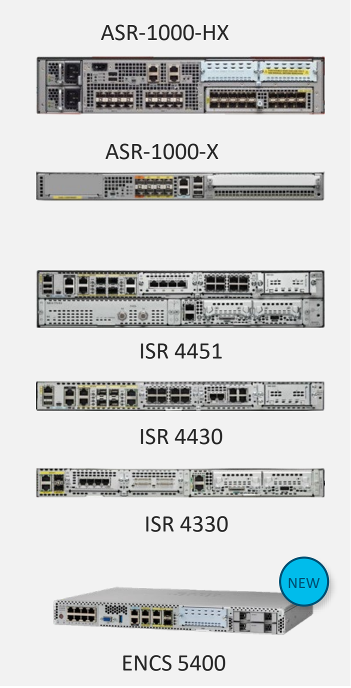
Catalyst 4500E

Catalyst 6800

Nexus 7700

Catalyst 3850 & 3650

Routing



ASR-1000-HX

ASR-1000-X

ISR 4451

ISR 4430

ISR 4330

ENCS 5400

Wireless

Catalyst 9800

Catalyst 9100 APs

AIR-CT8540

AIR-CT3504

AIR-CT5520

Aironet Wave 1 APs*

Aironet Wave 2 APs

Extended

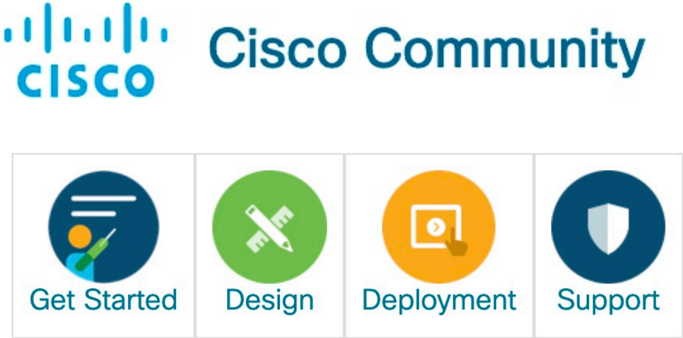
BETA

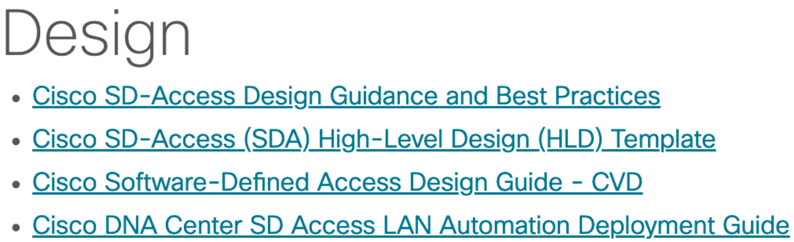
Cisco Digital Building

Catalyst 3560-CX

Cisco IE 4K/5K

Designing your SD-Access enabled Network



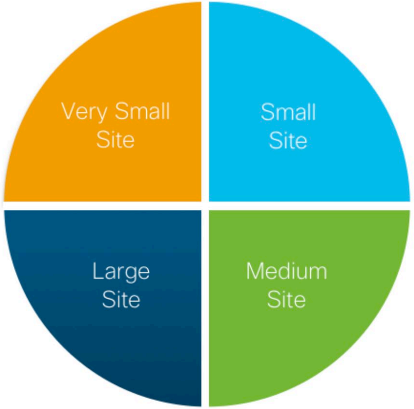


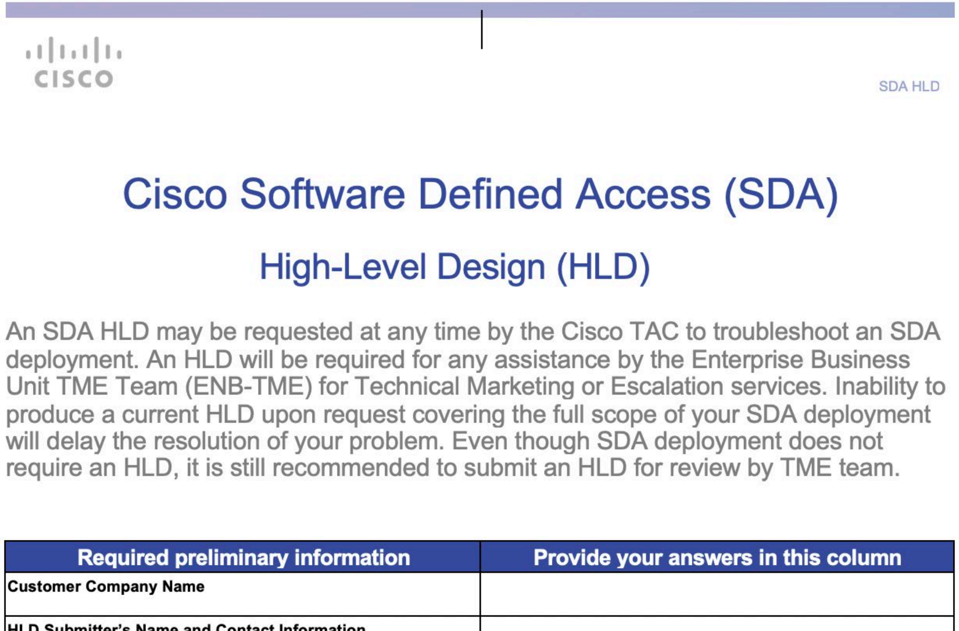
Design

- Cisco SD-Access Design Guidance and Best Practices
- Cisco SD-Access (SDA) High-Level Design (HLD) Template
- Cisco Software-Defined Access Design Guide - CVD
- Cisco DNA Center SD Access LAN Automation Deployment Guide

Types of SDA Designs

Fabric Design Categories





SDA HLD

Cisco Software Defined Access (SDA)

High-Level Design (HLD)

An SDA HLD may be requested at any time by the Cisco TAC to troubleshoot an SDA deployment. An HLD will be required for any assistance by the Enterprise Business Unit TME Team (ENB-TME) for Technical Marketing or Escalation services. Inability to produce a current HLD upon request covering the full scope of your SDA deployment will delay the resolution of your problem. Even though SDA deployment does not require an HLD, it is still recommended to submit an HLD for review by TME team.

Required preliminary information	Provide your answers in this column
Customer Company Name	
HLD Submitter's Name and Contact Information	

SD-Access Deployment Lifecycle

Evaluation

- Introduction to SD-Access and it’s features
- Foundational knowledge in deploying SD-Access
- Planning network design

Design

- Scoping design requirements
- Simulating and validating design requirements
- Review Design with Enterprise Networks TME

Implement

- Lab validation
- Production dry-runs
- Go-Live and Day 2 Support

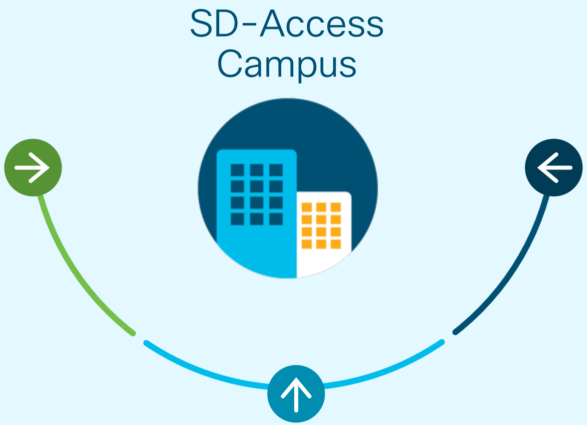
SDA Design Options

New Site

Migrate

SD-Access General Design Considerations

Drivers for Change
SDA Top Design Considerations



Wired Considerations

L2 > L3 – Architecture Change
New Subnets for SDA
Fusion device
Multicast – Native vs Underlay Multicast
External Connectivity – Transit types
VoIP CUCM
Flooding
Border Services – Firewall, etc ..

Security and Segmentation

Policy Enforcement in Fabric

East West & North South Segmentation
Policy in Multi-Domain
IP Transit vs SDA Transit
Enforcement at Border, Fusion or Firewall

Wireless

Embedded – MDNS support, Local WLC per site
OTT – Flex designs
Latency of AP > WLC (20 msec in fabric)

Design Questions - Requirements

Translating Business Intent into Technical Requirements

K

Key Questions

Focus on Business Intent & Global Scope

A

Connect Questions

Focus on Topology & Features
(Per Site + Transit)

B

Comply Questions

Focus on Access & App Policy
(Per Site + Transit)

Design Questions: Key Points

For your reference

Asking the right questions, to get things started

Is this a Single Site, or Multiple?

- Campus? Branch?
- WAN Considerations?

Is this a New or Existing Site?

- Parallel? Incremental?

Is this a Small, Medium or Large Site?

- How many Users / Devices?
- Scale Considerations?

Is this Site “Business Critical”?

- Redundancy Considerations?

What is More Important right now?

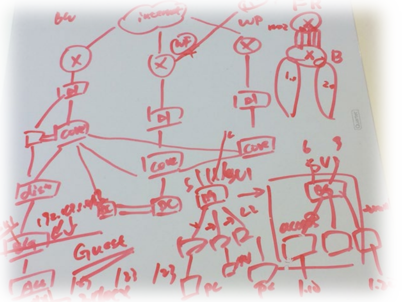
- Automation or Policy? Both?
- Visibility / Assurance?

Is Secure Network Access a top concern?

- Access Control?
- Segmentation?
- Intra or Inter-Site?

What are the Main Services?

- Centralized vs Distributed?
- Policy Implications (VN/SGT)



Design Questions: Connect Topics

For your reference

Connectivity Services

Where are Connect Services located?

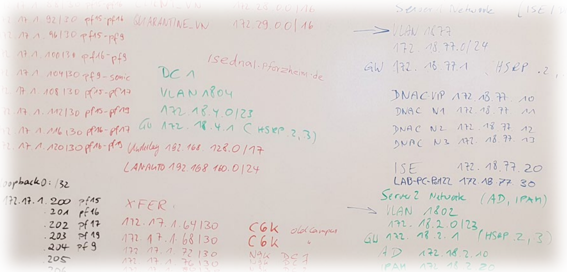
- Where is DNA Center?
- Where are DNS, DHCP, IPAM?
- Where is NTP?
- What is the IP Addressing?
- Local? DC? Over WAN?

What types of Network Services?

- Multicast / Broadcast?
- Voice / Video (Collaboration)?
- Client Services (mDNS)?
- Data Collection (SPAN/Netflow)?

Are Services in GRT or VRF?

- VRF Leaking (Fusion) involved?
- Firewall Rules (DMZ) involved?



Design Questions: Connect Topics

For your reference

Wired Considerations

How many Network Tiers?

- What type(s) of Core/Border/CP node?
- What type(s) of Access/Edge node?
- Are there any Distribution/Intermediate?

Which nodes will be Border?

- What type of hand-off? L2/L3?
- What is the outside Protocol(s)?
- Redundant Borders?
- Collocated or Distributed?

Which nodes will be Control Plane?

- Switch/Router/CSR?
- Collocated or Distributed?

Which nodes will be Edge?

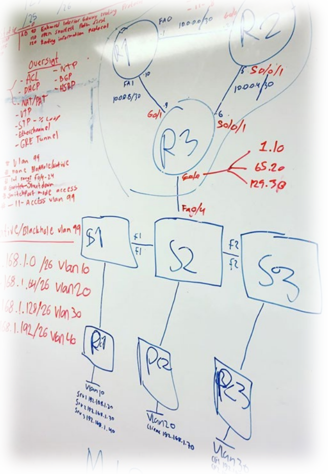
- How many Edge nodes?
- Any Edge @ Distribution?

Will there be Extended Nodes?

- How many Extended nodes?
- What type of Edge connection?

What is the Underlay?

- What is the IP Addressing?
- Automated Underlay?
- Manual Underlay? What Protocol?



Design Questions: Connect Topics

For your reference

Wireless Considerations

What type of Wireless?

- Fabric Enabled Wireless?
- Overlay Wireless (OTT)?
- Mixed Mode (both)?
- Cisco or 3rd Party?

Which types of WLC?

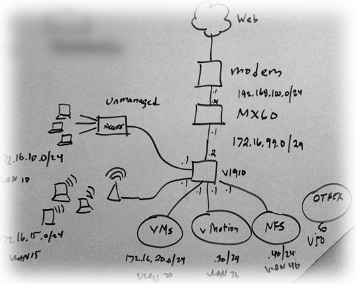
- How many Wireless Clients?
- Where is the WLC connected?
- Direct to Border? DC?
- Redundancy considerations?

Which types of APs?

- How many Wireless APs?
- What type of Edge connection?

What about Guest Wireless?

- Dedicated Guest VN?
- Dedicated Guest CP/Border?



Design Questions: Connect Topics

For your reference

Transit Considerations

What type of Transit?

- SDA Fabric Overlay?
- SD-WAN (Viptela)?
- DMVPN (IWAN)?
- Traditional IP/BGP?

What is the WAN/Edge node?

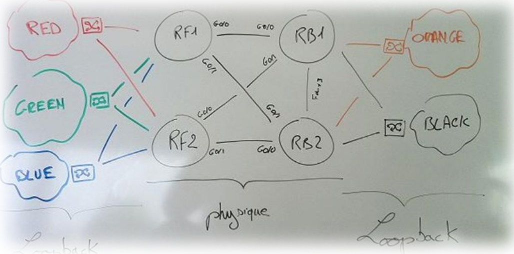
- Cisco or 3rd Party?
- Direct Internet Access?
- Redundancy considerations?

Is VRF hand-off required?

- All VRFs? Selective?
- 1:1? 1:N? M:N?
- Redundancy considerations?

Is Policy hand-off required?

- All SGTs? Selective?
- Inline SGT Tags? SXP?



Design Questions - Policy Topics

B0 - Policy Services

- Where are Policy Services located?
  - Where is Cisco ISE?
  - Other ID/NAC Services?
  - Local? DC? Over WAN?
  - Cloud hosted?
- Are Services in GRT or VRF?
  - VRF Leaking (Fusion) involved?
  - Firewall Rules (DMZ) involved?
- Is the Cisco ISE "Business Critical"?
  - Scale Considerations?
  - Redundancy Considerations?
- What types of Policy Services?
  - Identity Services?
  - Firewall Services?
  - VPN/Encrypt Services?
  - IDS/IPS or NaaS/NaaE?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Questions – Policy Topics

B1 – Identity Considerations

- Do you need Static Assignment?
  - Where/Why is Static Identity used?
  - Which parts are Static? VLAN, IP?
  - Will these migrate to Dynamic?
- Do you need Dynamic Authentication?
  - Wired? Wireless? Both?
  - Where is Dynamic Identity used?
  - Do you use Device Profiling?

- What type(s) of Authentication?
  - 802.1X (EAPOL)?
  - MAC Address Bypass (MAB)?
  - Web Authentication (CWA)?
  - Easy Connect (AD Integration)?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Design Questions - Policy Topics

Segmentation Considerations

- What areas need to be truly Isolated?
  - Separate Departments?
  - Secure Areas?
  - Guest Network?
  - Partners/Contractors?

- Where are VRFs Managed?
  - VRF Routing?
  - Firewalls? DMZ?
  - Local or End-2-End?
  - Scale considerations?
  - Redundancy considerations?

NOTE: This is NOT an exhaustive list of questions. Add more of your own! ☺

Sample Network with Multiple Sites

SDA Design is driven by Customer requirements

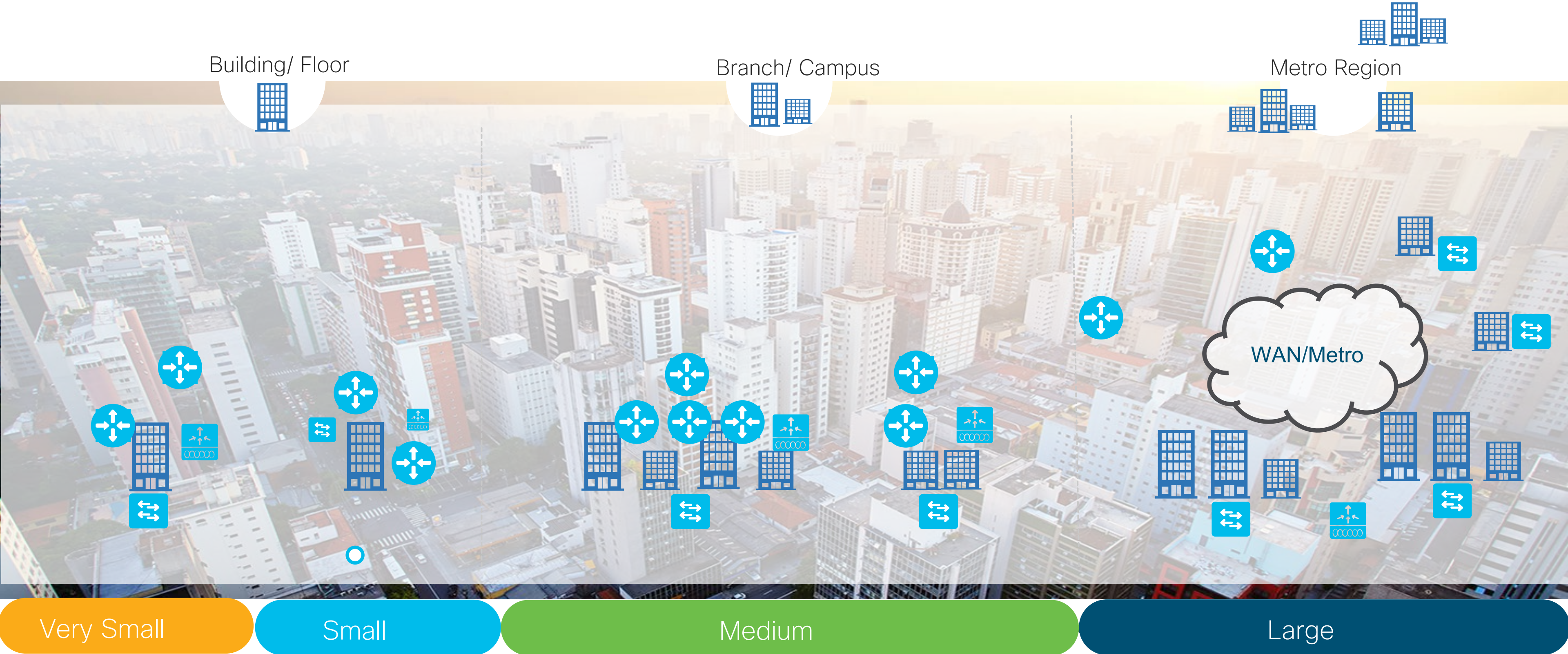
Use Cases

Mobility

Survivability

Scale

Segmentation and Policy



Types of SDA Designs

Fabric Design Categories

FIAB - Fabric In a Box

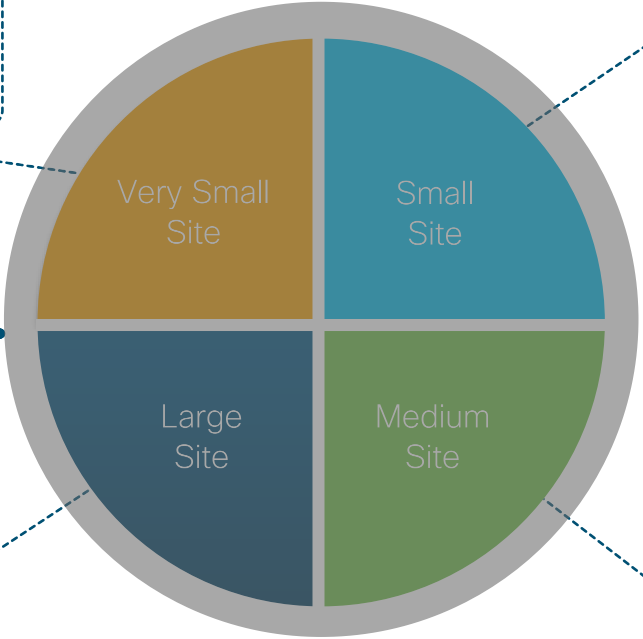
- Single wiring closet (MDF)
- Border, CP & FE and Wireless in a box
  - No Survivability
  - No Redundancy
- Stack supported (up to 8) with redundancy and survivability for Control plane
- Total endpoints < 2K (software limit)

Multiple Sites

- Multiple Sites is driven by customer design requirement
- Multiple Fabrics
- MAN or WAN Underlay
- Site Borders & Transit Area
- Distributed ISE

Large Site

- 2 dedicated CPs (w SDA Wireless) – 6 with Wired ONLY. Up to 4 Border nodes
  - Full Survivability for Border & CP
  - Full Redundancy for Border & CP
- Local WLC + HA
- ISE PAN - Local PSN



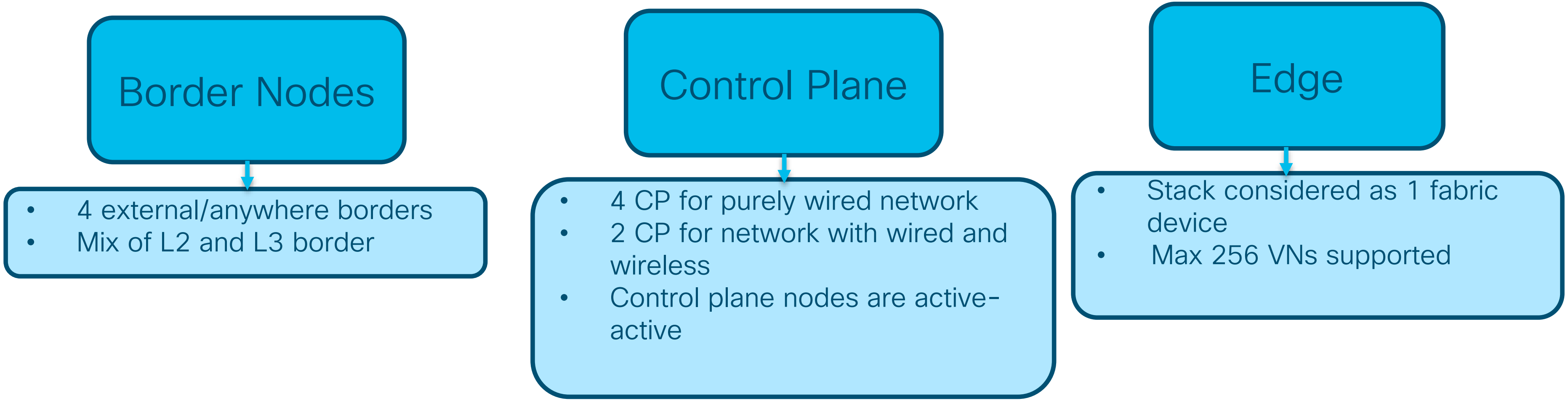
Small Site

- Multiple wiring closets (MDF's)
- 2 x (collocated Border & CP) (in a single box)
  - Limited Survivability for Border & CP
  - Limited Redundancy for Border & CP
- Dedicated Edge (no stacking)
- Local WLC
- Standalone ISE

Medium Site

- Dedicated CP's for higher survivability (Site, building, floor)
  OR
- 2 x collocated Border & CP (in a single box)
  - Full Survivability for CP
  - Limited Redundancy for Border
- Dedicated Edge (no stacking)
- Local WLC + HA
- ISE PAN - Local PSN

Scale Considerations for Fabric Nodes



Border Nodes

- 4 external/anywhere borders
- Mix of L2 and L3 border

Control Plane

- 4 CP for purely wired network
- 2 CP for network with wired and wireless
- Control plane nodes are active-active

Edge

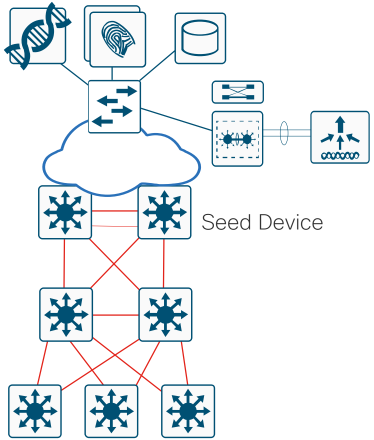
- Stack considered as 1 fabric device
- Max 256 VNs supported

Network Infrastructure – Underlay

SD-Access underlay options

Manual Underlay

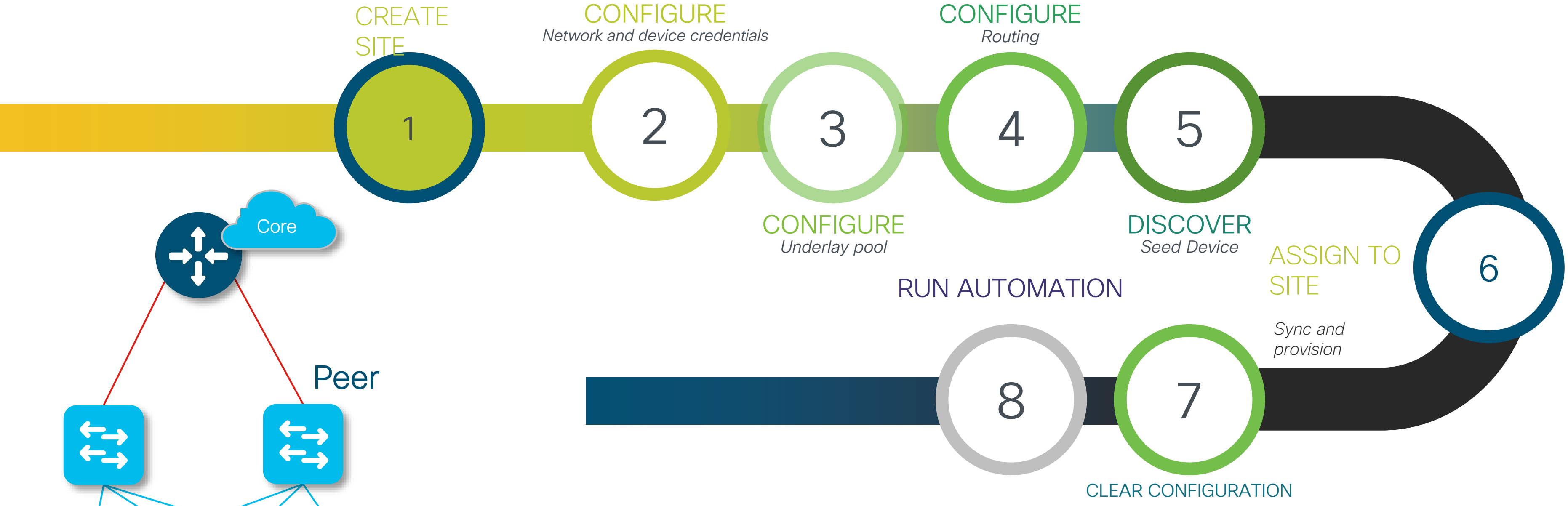
- Any Routed Network
- System MTU: 9100
- Loopback 0 with /32 subnet
- Resiliency – BFD, ECMP, NSF
- Multicast – ASM/SSM, sparse-mode
- CLI, SNMP credentials
- Discover & Manage network device
- Upgrade Software version



Automated Underlay

- Discover Seed Device
- Input IP Address Pool
- Start LAN Automation
  - ✓ Discover the network device
  - ✓ Onboard the network device
  - ✓ Upgrade software
- Stop LAN Automation
  - ✓ Complete Configuration (L3 interface, IS-IS)
  - ✓ Manage Device in Cisco DNAC-Center

Automated Underlay- LAN Automation



CREATE SITE

CONFIGURE
Network and device credentials

CONFIGURE
Underlay pool

CONFIGURE
Routing

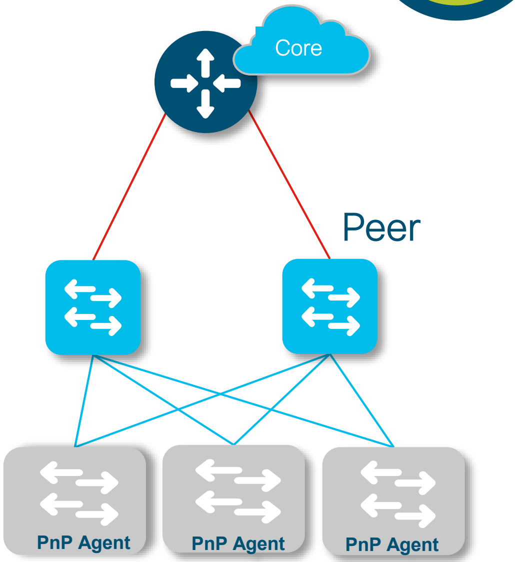
DISCOVER
Seed Device

RUN AUTOMATION

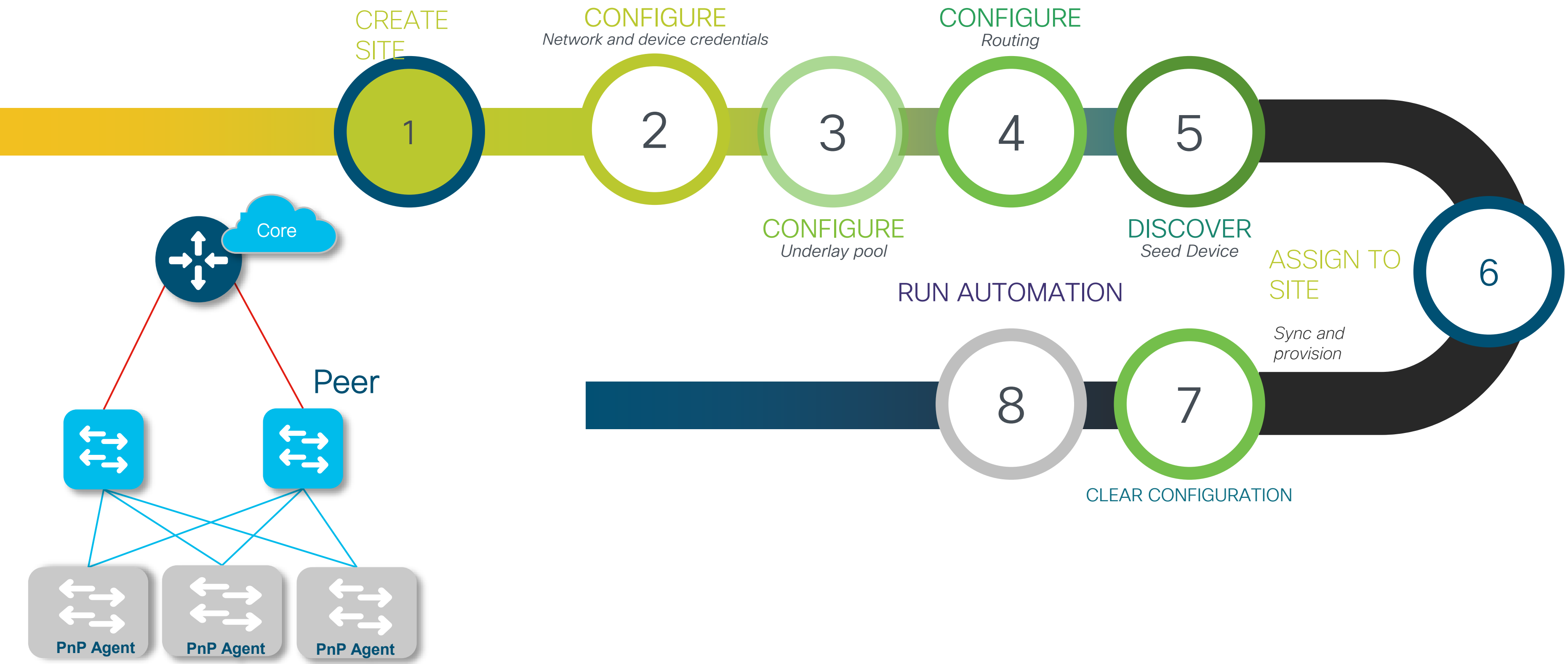
ASSIGN TO SITE

Sync and provision

CLEAR CONFIGURATION



Automated Underlay- LAN Automation



CREATE SITE

CONFIGURE
Network and device credentials

CONFIGURE
Underlay pool

CONFIGURE
Routing

DISCOVER
Seed Device

RUN AUTOMATION

ASSIGN TO SITE

Sync and provision

CLEAR CONFIGURATION

Overall Solution Scale is Driven by Cisco DNAC

For your reference

Cisco DNAC 1.3.1.0

DNA Center

	Cisco DNAC *(Overall Scale)*	Cisco DNAC *(Per Fabric Scale)*
No. of Endpoints Max concurrent endpoints	100,000	Same as overall
No. of Fabric Nodes Inc all managed devices Switches, Routers, WLC	1200	1200
Access Points No of AP's + Sensors	12,000	Same as overall
DNAC Sites No of Fabrics	2000	N/A
Virtual Networks No of VN's	256	256
IP Pools Max No. of IP Pools	N/A	600

Scale Numbers

DN1-HW-APL
Cisco UCS C220 M5
Rack Server
44 cores

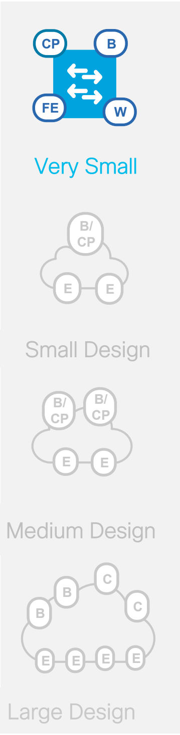
DN2-HW-APL
Cisco UCS C220 M5
Rack Server
56 cores

DN2-HW-APL-L
Cisco UCS C480 M5
Rack Server
112 cores

* = Higher numbers with newer appliance

Very Small Site

FIAB -- Fabric In A Box



Overview

FIAB - Fabric In a Box

- Total **endpoints < 2K** (software limit)
- Border, CP & FE and Wireless in a single box
  - **No Survivability for CP and Border**
- **Single wiring closet (MDF)**

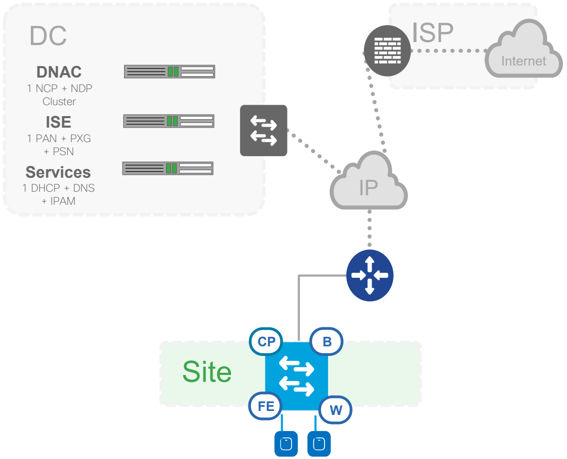
Benefits

- Reduces cost to deploy SDA for very small sites
- FE + FB + CP on same C9K
- Supports eWLC/ 9800 & Embedded-Wireless in 1.2.10 (16.10.1e for C9300)

	Border, Control and Edge 9300
End Points/Hosts Max number of Endpoints	< 2K
Fabric Nodes	1
Virtual Networks Maximum number of VN's	< 8
IP Pools	< 8
Access Points	200 (eWLC limit)
	B, CP & FE

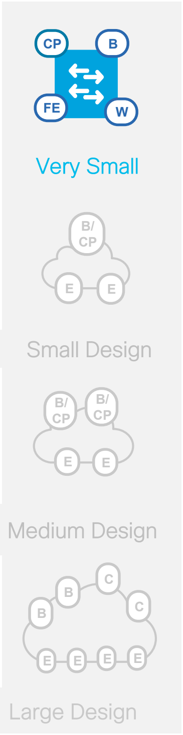
Note: Platforms numbers can be higher but consider these solution numbers for design

Sample Topology



Very Small Site

Stacks of FIAB



Overview

Stack of FIAB's

- Total **endpoints < 2K** (software limit)
- If a member of the Stack fails (with CP and Border), the next available member in the stack taker over the CP and Border functionality
  - Limited Survivability for CP and Border
- Single wiring closet (MDF)
- Max of 8 boxes can be in a Stack
- All the stack members must be the same platform

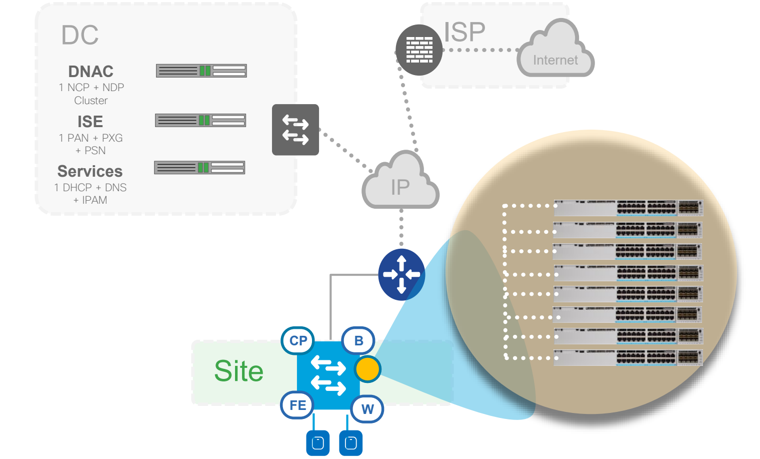
Benefits

- Get additional ports in a FIAB
- Still reduced cost to deploy SDA for very small sites
- FE + FB + CP on same C9K
- Supports eWLC/ 9800 & Embedded-Wireless in 1.2.10 (16.10.1e for C9300)

	Border, Control and Edge
	9300
End Points/Hosts Max number of Endpoints	< 2K
Fabric Nodes	1
Virtual Networks Maximum number of VN's	< 8
IP Pools	< 8
Access Points	200 (eWLC limit)
	B, CP & FE

Note: Platforms numbers can be higher but consider these solution numbers for design

Sample Topology



Small Site

CP
B
FE
W
Very Small
B/ CP
E
E
Small Design
B/ CP
B/ CP
E
E
Medium Design
B
C
B
C
E
E
E
E
Large Design

Overview

- Multiple wiring closets or even single.
- Border and CP are collocated in a single box
- Redundancy for Border or CP
- Limited Survivability
- Total endpoints < 10K (recommendation, but DNAC and platform scale can drive this number)

● = Scale Numbers are currently being tested

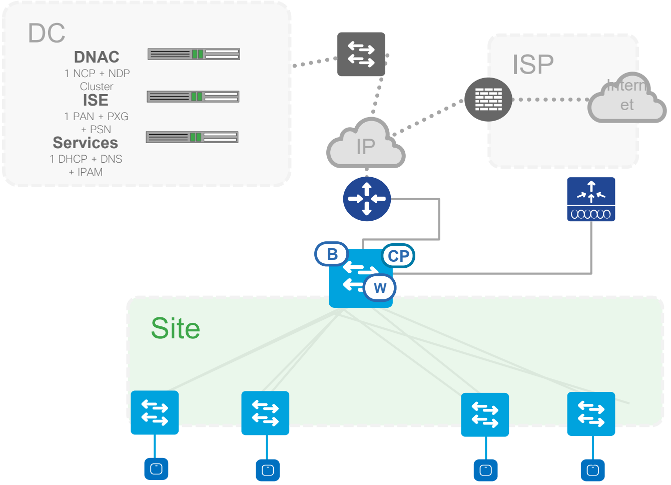
	Border, Control		Fabric Edge	
	9300	9500	9200	9300
End Points/Hosts Max number of Endpoints	< 10K	< 10K	●	< 10K
Fabric Nodes	2 (Collocated)	2 (Collocated)	●	< 25
Virtual Networks Maximum number of VN's	< 64	< 64	●	< 64
IP Pools	< 64	< 64	●	< 64
Access Points	200	200	●	200
	B, CP		FE	

Note: Platforms numbers can be higher but consider these solution numbers for design

Benefits

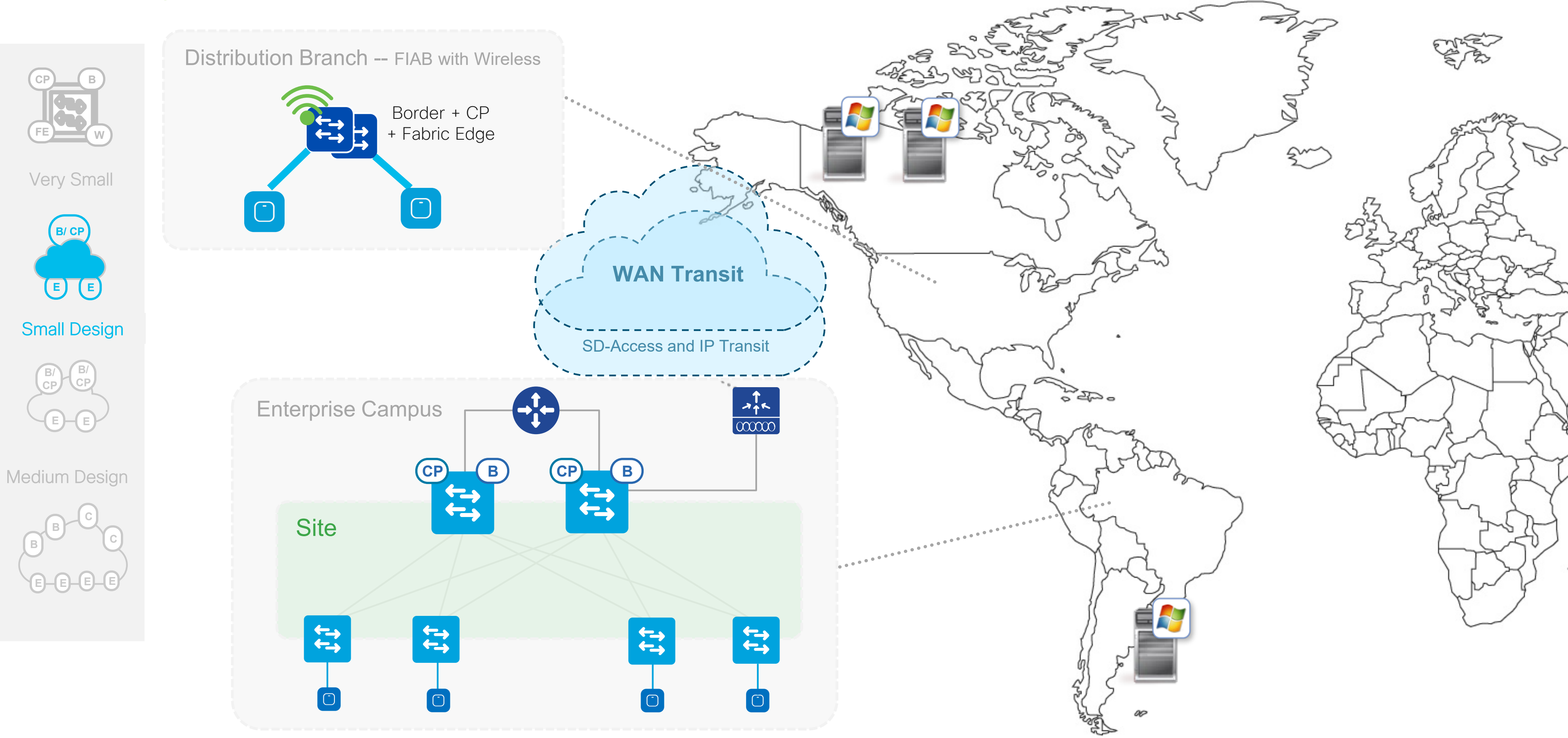
- Small site design
- Tends to be Building or Office with < 10,000 endpoints and < 100 IP Pools/Groups
- 1-2 Collocated CP + External Border (Single Exit)
- Tends to be local WLC connected to Border (e.g. Stack) + FEW
- Looking at <1000 dynamic authentications and <250 group based policies.
- FB + CP + eWLC (9300)with distributed Fabric Edges
- Supports eWLC/ 9800 & Embedded-Wireless in 1.2.10 (16.10.1e for C9300)

Sample Topology



Strategy for Cisco SD-Access in a small site

Design for a small site

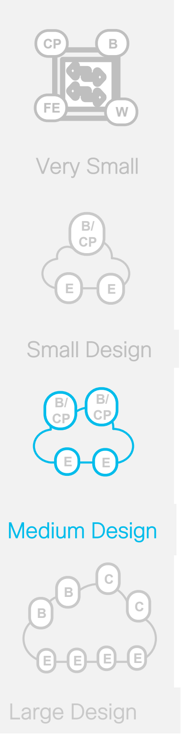


Medium Site

● = Scale Numbers are currently being tested

	Border, Control		Fabric Edge	
	9500	9600	9300	9400
End Points/Hosts Max number of Endpoints	< 25K	< 25K	●	< 25K
Fabric Nodes	4 (4 CP, 2 B))	4 (4 CP, 2 B)	●	<250
Virtual Networks Maximum number of VN's	< 64	< 64	●	< 64
IP Pools	< 64	< 64	●	< 64
Access Points	200	200	●	200
	B, CP		FE	

Note: Platforms numbers can be higher but consider these solution numbers for design



Overview

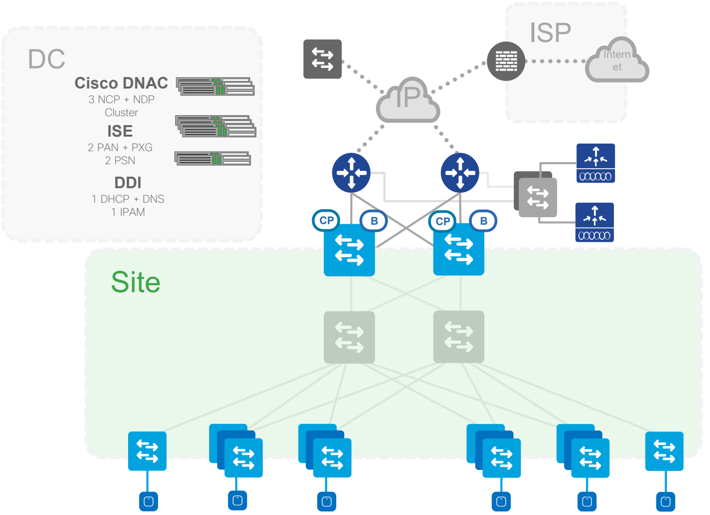
Medium Site

- Multiple wiring closets or even single.
- Dedicated CP's for higher survivability (Site, building, floor)
- 2 x collocated Border & CP (in a single box)
    - Full Survivability for CP
    - Limited Redundancy for Border
- Dedicated Edge (no stacking)
- **Recommended** total endpoints < 10K (recommendation, but DNAC and platform scale can drive this number).

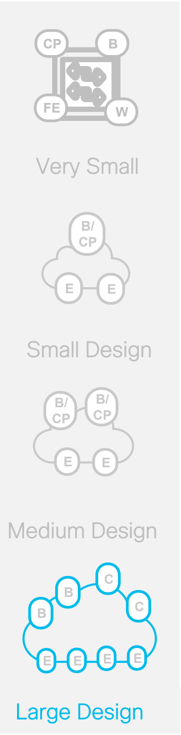
Benefits

- Next level up to a small design.
- Max Control Plane nodes = 6 (Wired Only); 4 with Wireless (2 Enterprise and 2 Guest CP's).
- Tends to be Multiple Buildings with < 25,000 endpoints
- Most likely a 3 Tier design, recommendation is to use 9400 & 9500 as intermediate nodes.
- Can choose a Co-located or a Distributed/Dedicated CP + Border(Single Exit) design.
- Tends to be WLC + FEW via Services Block or a local Data Center
- Looking at < 25,000 dynamic authentications and < 1000 group based policies

Sample Topology



Large Site



Overview

Large Site

- Multiple wiring closets (most likely).
- Max Control Plane nodes = 6 (Wired Only); 4 with Wireless (2 Enterprise and 2 Guest CP's).
- Max Border nodes = 4
- Dedicated CP's for higher survivability (Site, building, floor)
- Dedicated Borders for site exits
  - Full Survivability for CP
  - Full Redundancy for Border
- Dedicated Edge (no stacking)
- **Recommended** total endpoints < 25K (recommendation, but DNAC and platform scale can drive this number).

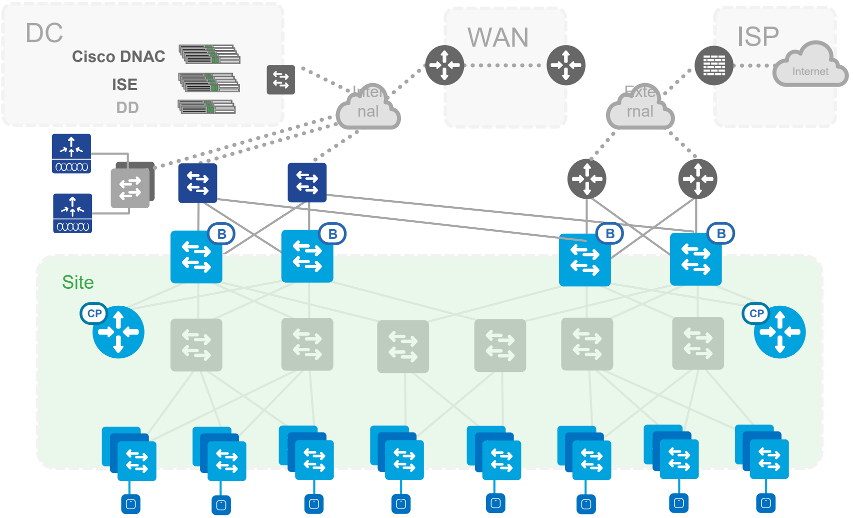
Benefits

- Dedicated borders can provide multiple exits to different DC's or destinations.
- Tends to be Many Buildings with < 25,000 endpoints and < 500 IP Pools/Groups
- Most likely a 3 Tier design, recommendation is to use 9500 as intermediate nodes.
- Can choose a Co-located or a Distributed/Dedicated CP + 2-4 Borders (Multiple Exits)
- Looking at < 25,000 dynamic authentications and < 2000 group based policies

● = Scale Numbers are currently being tested

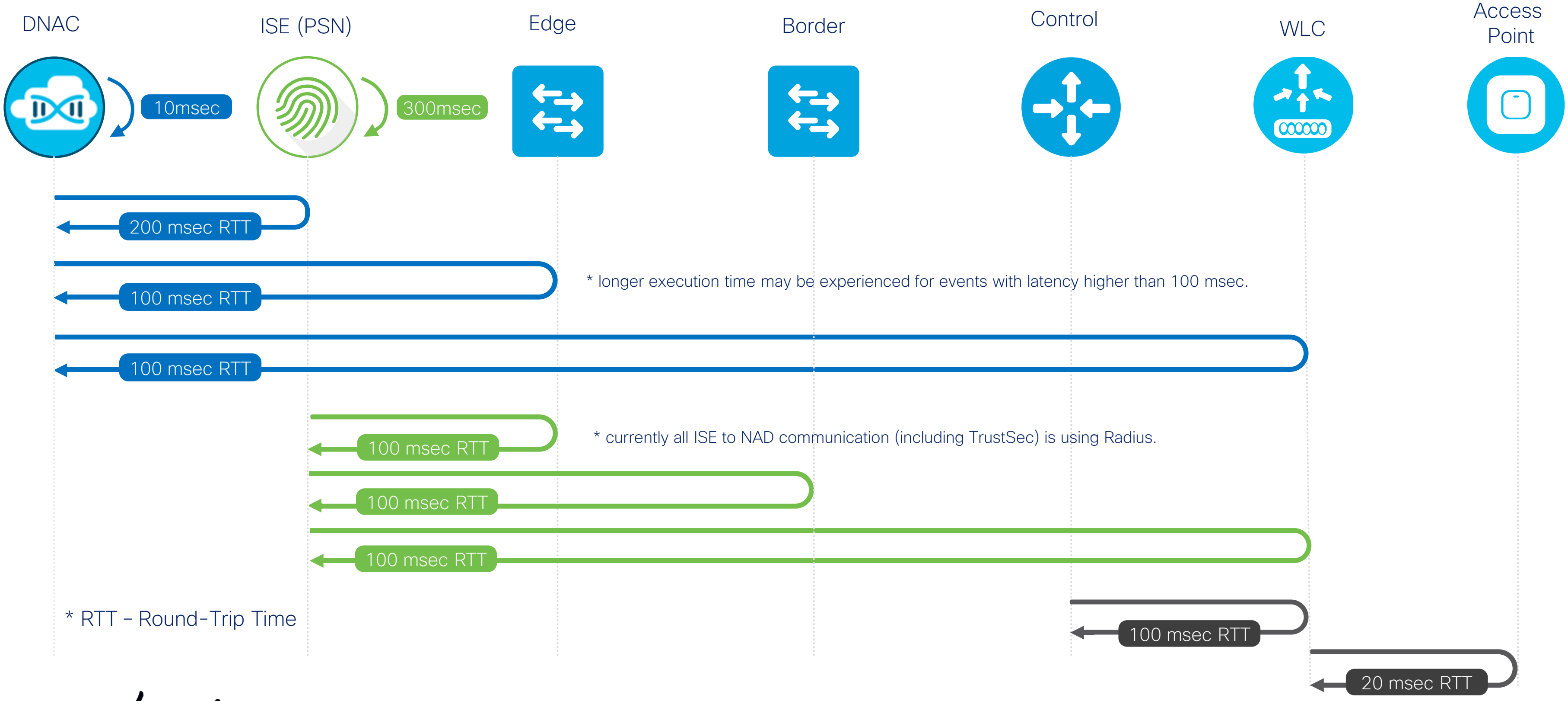
	Border, Control		Fabric Edge	
	9500	9600	9300	9400
End Points/Hosts Max number of Endpoints	< 25K	< 25K	●	< 25K
Fabric Nodes	6 + 4 (6 CP, 4 B)	6 + 4 (6 CP, 4 B)	●	<1000
Virtual Networks Maximum number of VN's	< 64	< 64	●	< 64
IP Pools	< 64	< 64	●	< 64
Access Points	200	200	●	200
	B, CP		FE	

Note: Platforms numbers can be higher but consider these solution numbers for design



Cisco SD-Access Network Requirements

Latency Requirements (RTT)



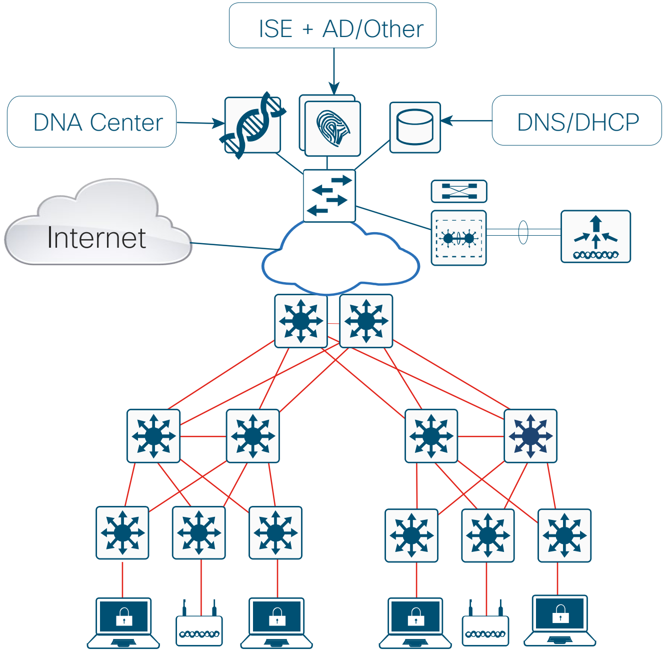
* longer execution time may be experienced for events with latency higher than 100 msec.

* currently all ISE to NAD communication (including TrustSec) is using Radius.

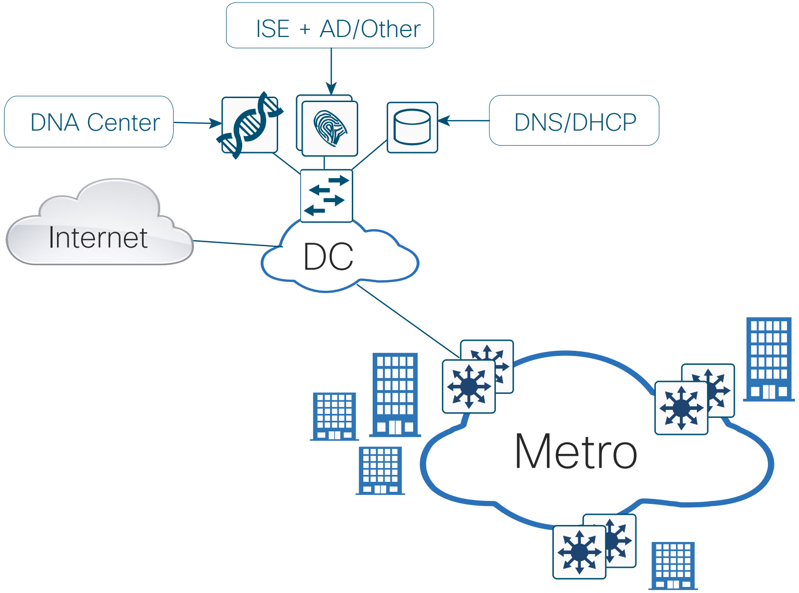
* RTT – Round-Trip Time

Cisco DNA Center Design- Where to Locate it

Local DC or Services Block



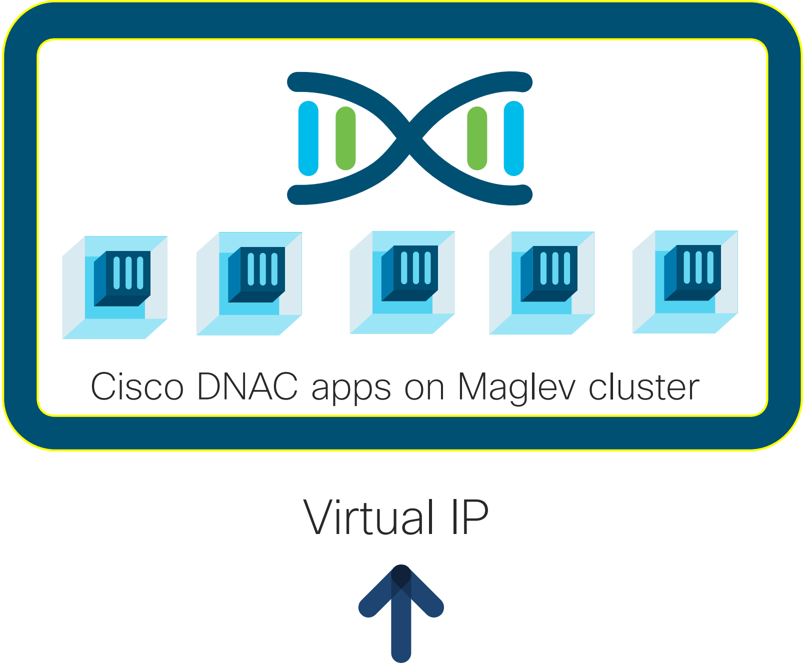
Remote DC (Over MAN/WAN)



NOTE: DNAC requires access to Internet

Scaling Strategy for Fabric within a site

Cisco DNA Center Design- Three Node High Availability



1 or 3 appliance HA Cluster

- Odd number to achieve quorum of distributed system
- Scale does not change

Seen as 1 logical Cisco DNAC instance

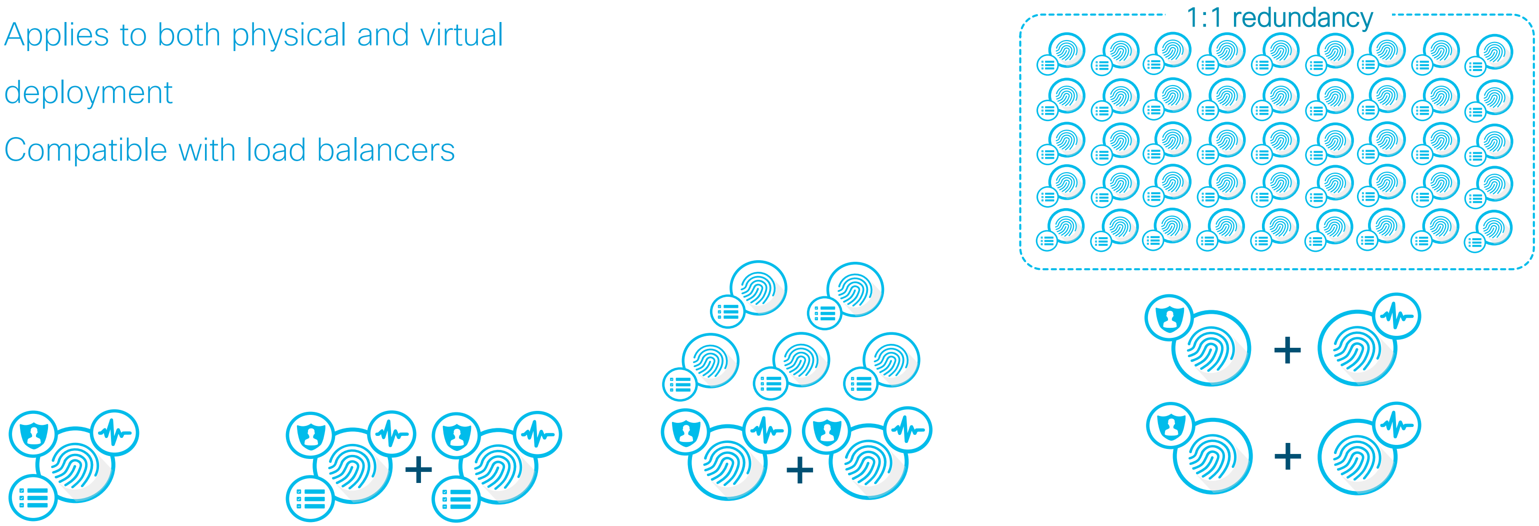
- Virtual (Cluster) IP

2 nodes active/sharing + 1 redundant

- Some services run multiple copies spread across nodes (e.g. databases)
- Other services run single copy and migrate from failed to redundant node

Cisco Identity Services Engine design

- Applies to both physical and virtual deployment
- Compatible with load balancers



Lab and
Evaluatio
n

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

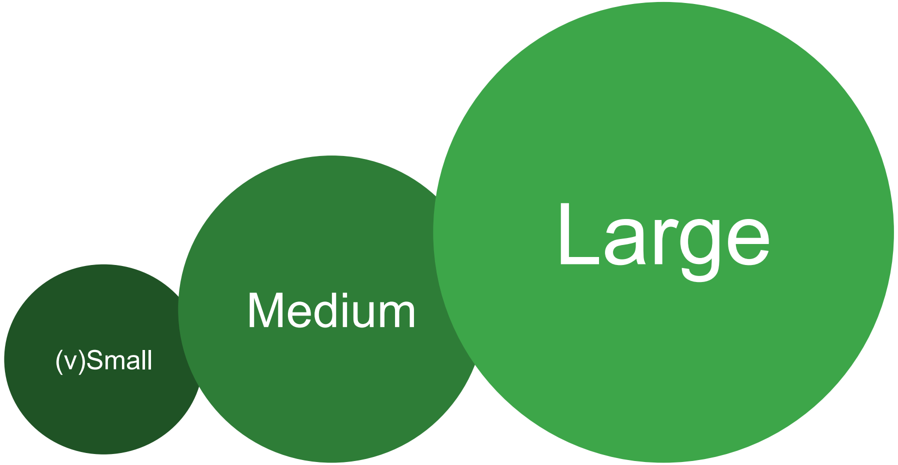
Small Multi-node
Deployment
2 x (PAN+MNT), <= 5 PSN

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

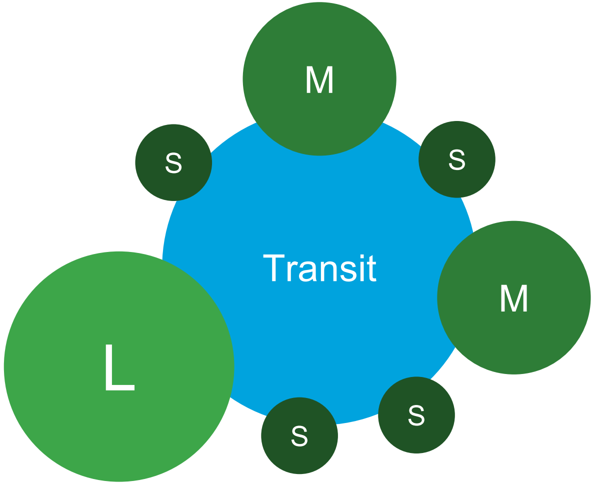
35xx	100 Endpoints	20,000 Endpoints	500,000 Endpoints
36xx	100 Endpoints	50,000 Endpoints	2,000,000 Endpoints(3695-PAN&MnT)

Why Multiple Sites?

Basic Goal is for *fewer, larger* Fabric Sites



Some Needs *require split* into Multiple Sites



- ✓ Higher scale due to more number of sites (Control plane per site)
- ✓ Wireless Client Roaming (< 20ms Latency)
- ✓ Direct Internet Access (@ Remote Sites)
- ✓ Survivable Remote Sites (Local CP/Borders)

Scaling Strategy across Multiple Sites

Why single site vs multi site ?

Advantages:

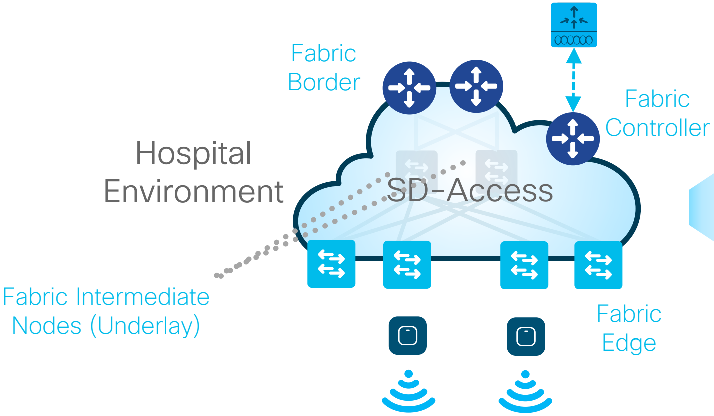
- ➢ Smaller or isolated Failure Domains
- ➢ Helps scaling number of Endpoints
- ➢ Cisco DNAC provides Automation and Single View of entire system
- ➢ Local breakout at each Site for Direct Internet Access (DIA)

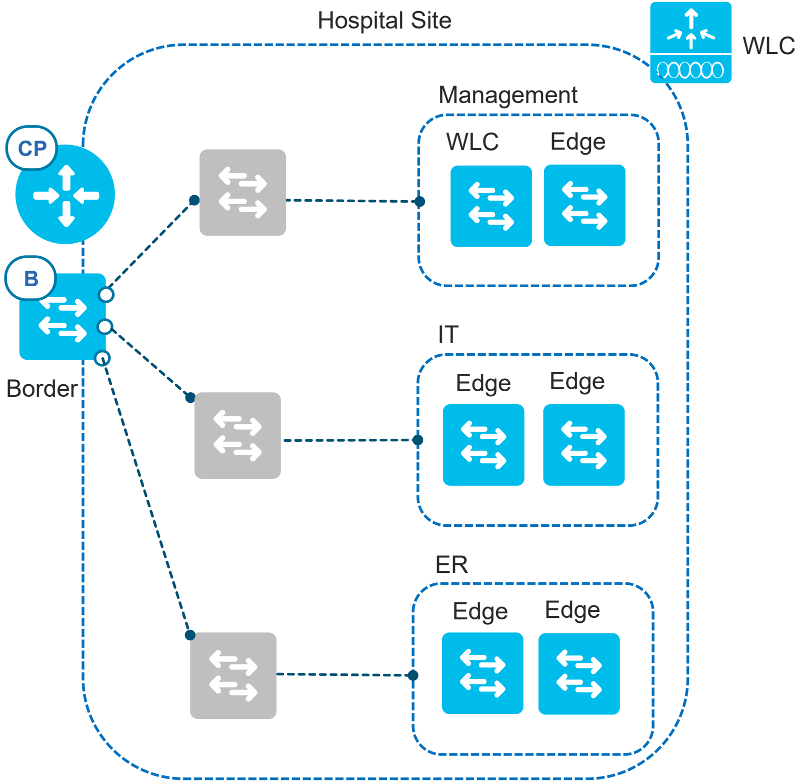
Why Multiple sites

Survivability or WAN separated networks

Use Case

- I need high survivability for my ER department



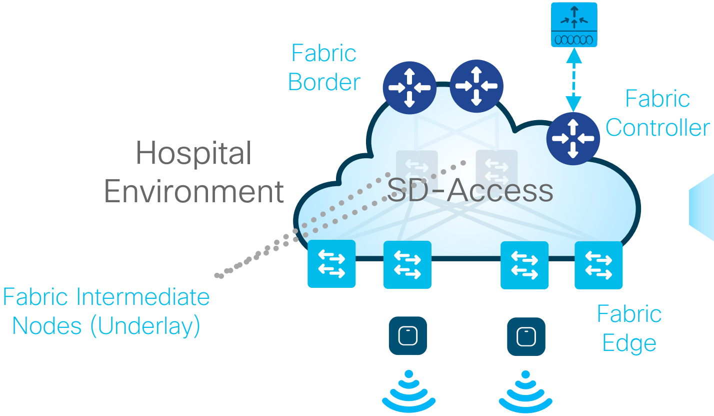


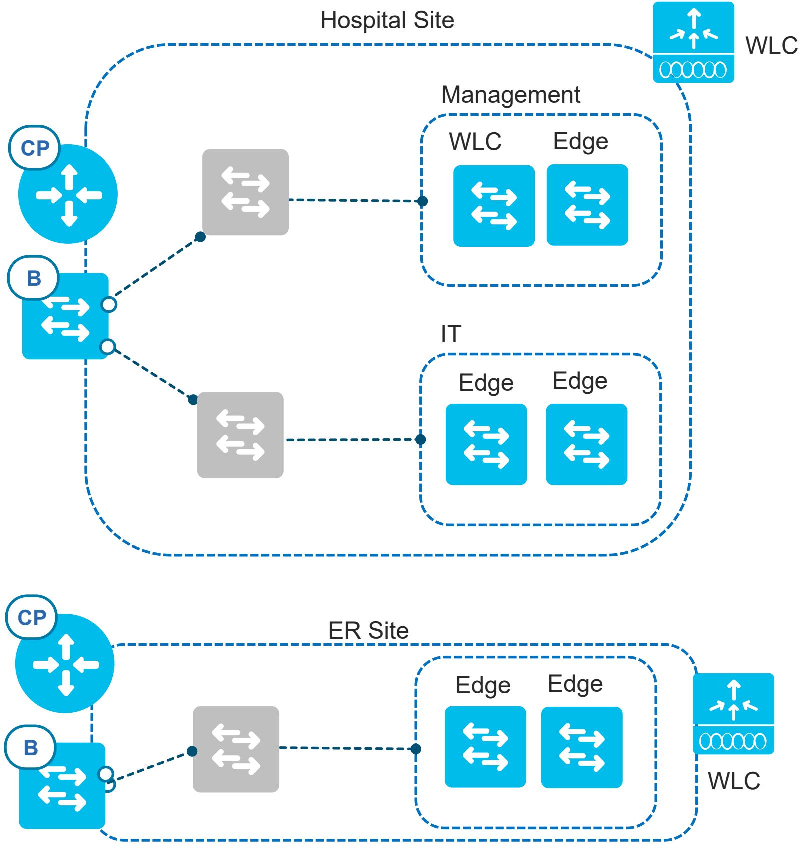
Why Multiple sites

Survivability or WAN separated networks

Use Case

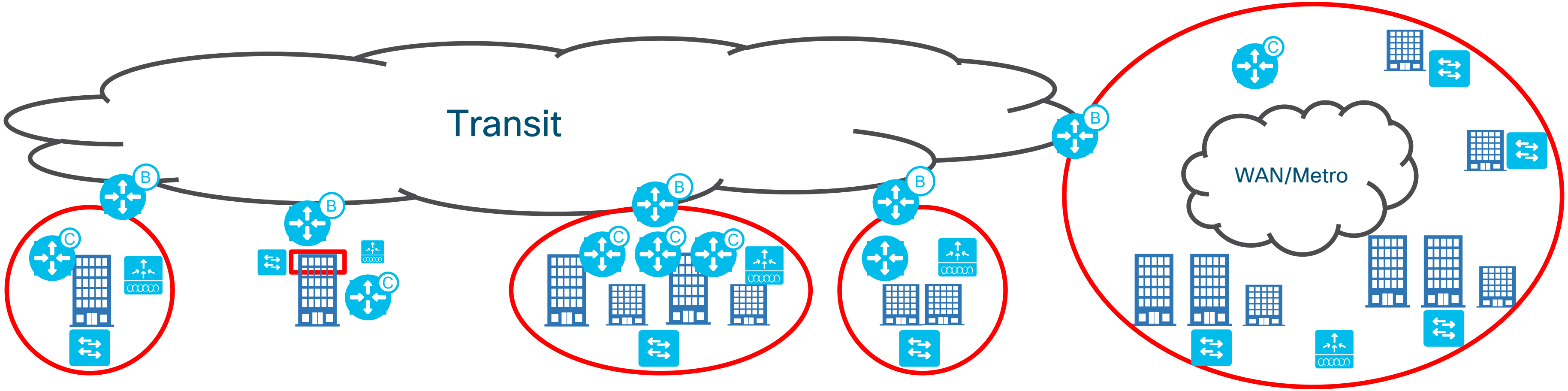
- I need high survivability for my ER department





Multiple Sites

Wireless Controller Scale



- Latency 20 ms
- Each site has a WLC associated with its Control Plane
- This will help scale the number of end points in the network

Sample Network with Multiple Sites

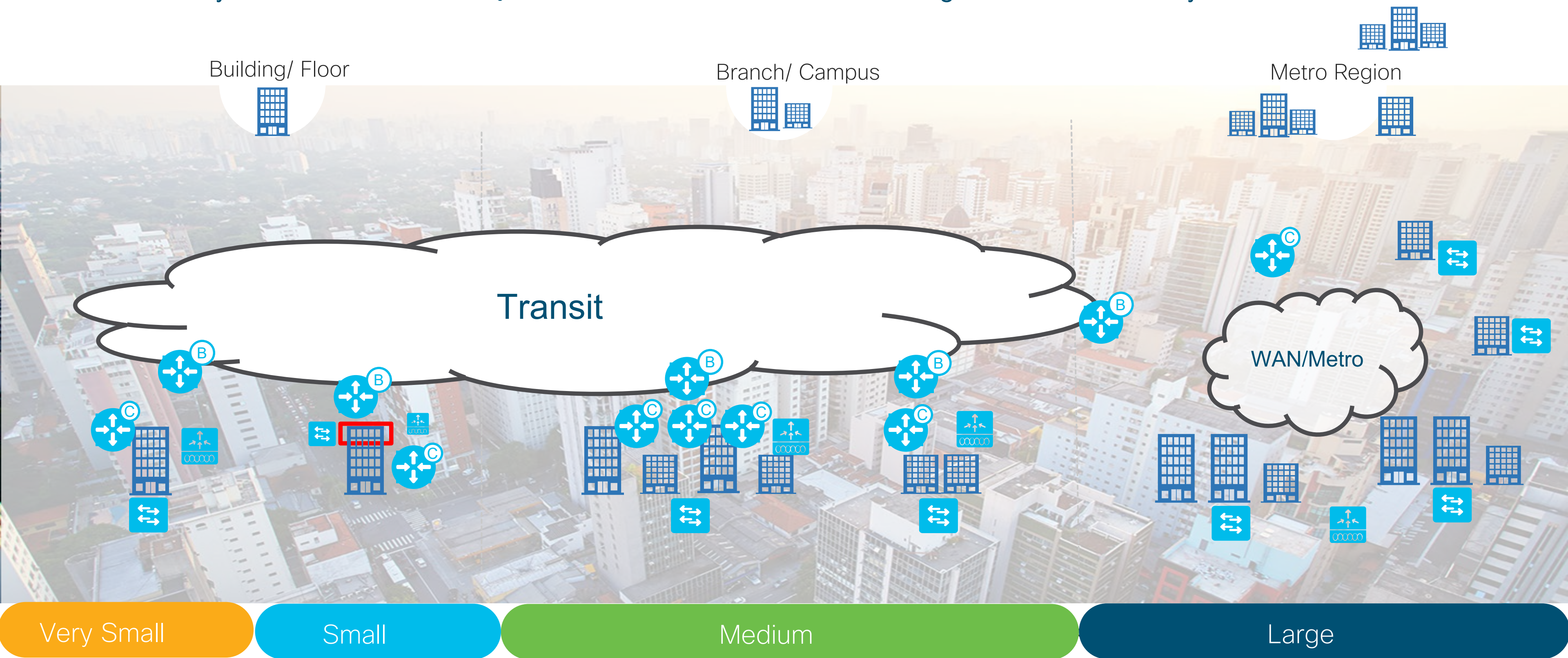
SDA Design is driven by Customer requirements

Mobility

Survivability

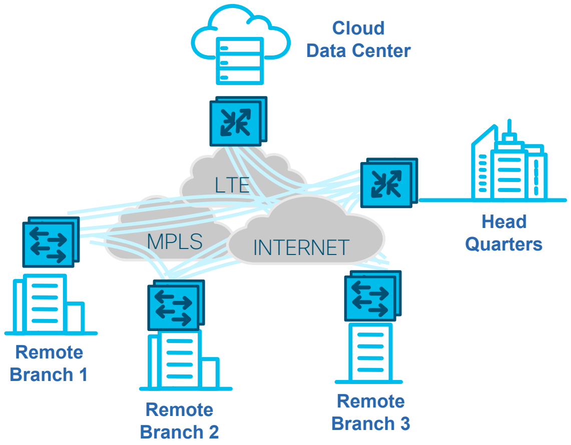
Scale

Segmentation and Policy

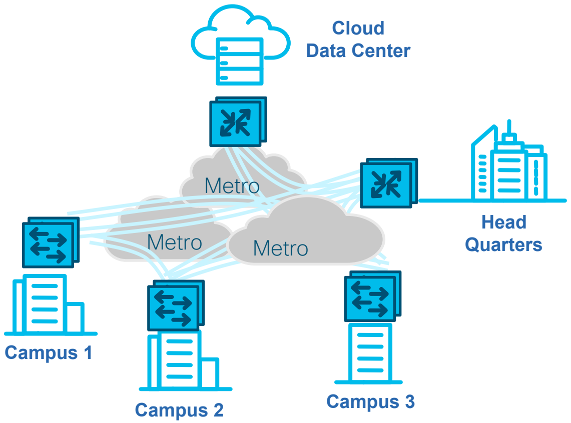


Types of Transit

Transit Design – IP vs SDA transit



Why IP Transit	Use-cases
Customers already using existing WAN or have adopted SD-WAN	Internet Handoff P2P IPSEC encryption
Less than <1G circuits from Provider(s)	Policy Based Routing WAN Accelerators
Higher latencies because sites are in different regions (many miles apart)	Traffic engineering Mobile Backhaul LTE



Why SDA Transit	Use-cases
Smaller or isolated Failure Domains Helps scaling number of Endpoints	Consistent policy and end-to-end segmentation using VRFs and SGTs
DNAC provides Automation and Single View of entire system	Smaller and Isolated fault domains
VNs and SGTs gets pushed to all sites (consistent policy) Local breakout at each Site for Direct Internet Access (DIA)	Resiliency and Scalability

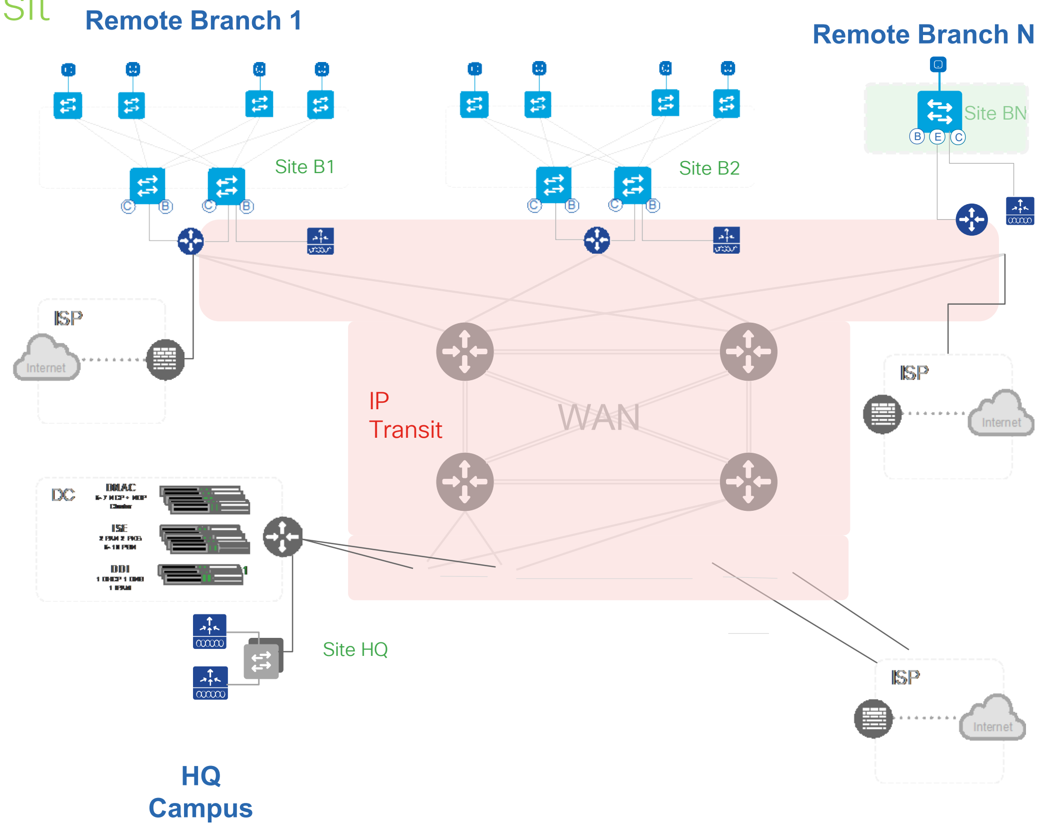
IP Transit

Design for a multi site with IP Transit

Overview

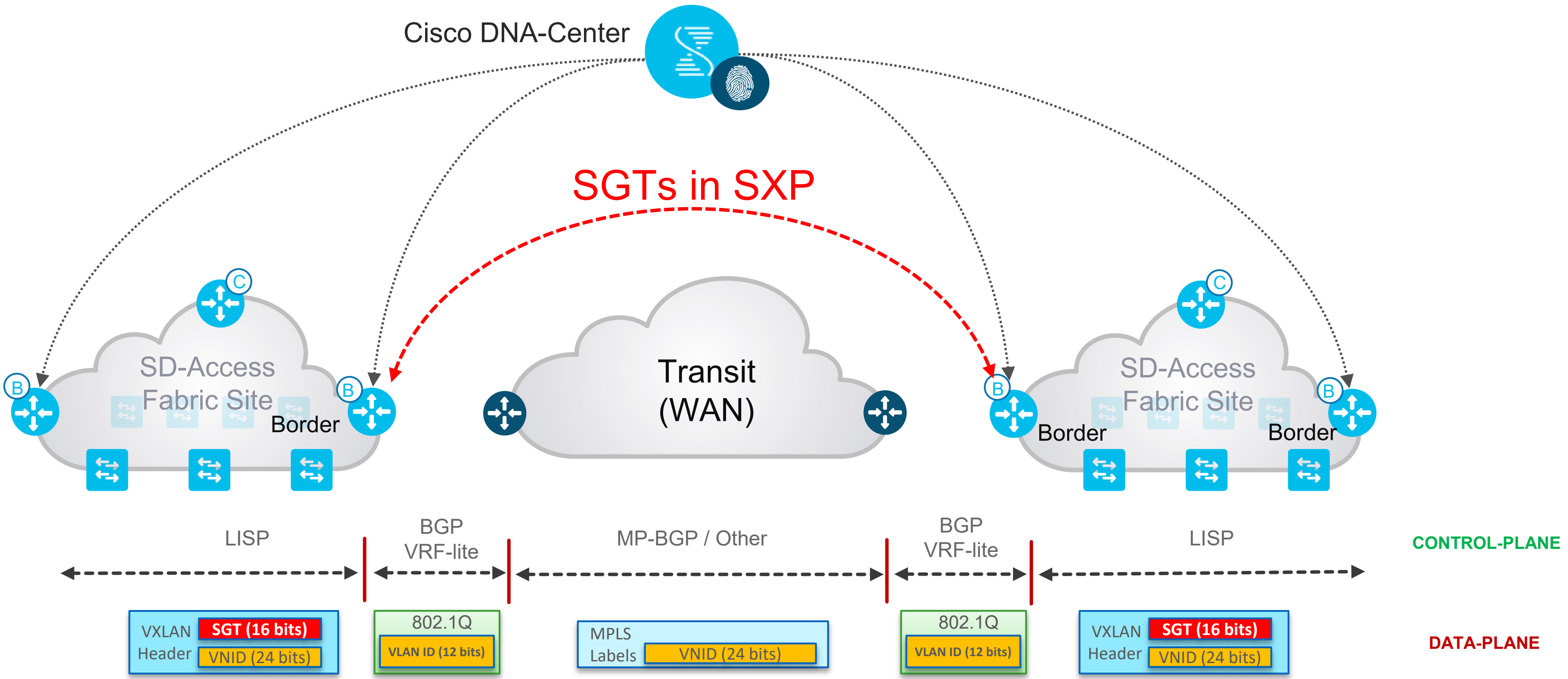
- Tends to be many remote branch offices connected
- Customers already using existing WAN or have adopted SD-WAN
- Higher latencies because sites are in different regions (many miles apart)

- Typical use cases
  - Internet Handoff
  - P2P IPSEC encryption
  - Policy Based Routing
  - WAN Accelerators
  - Traffic engineering
  - Mobile Backhaul LTE



Cisco SD-Access for Distributed Campus IP Based WAN Transit

Management and Policy



cisco Live!

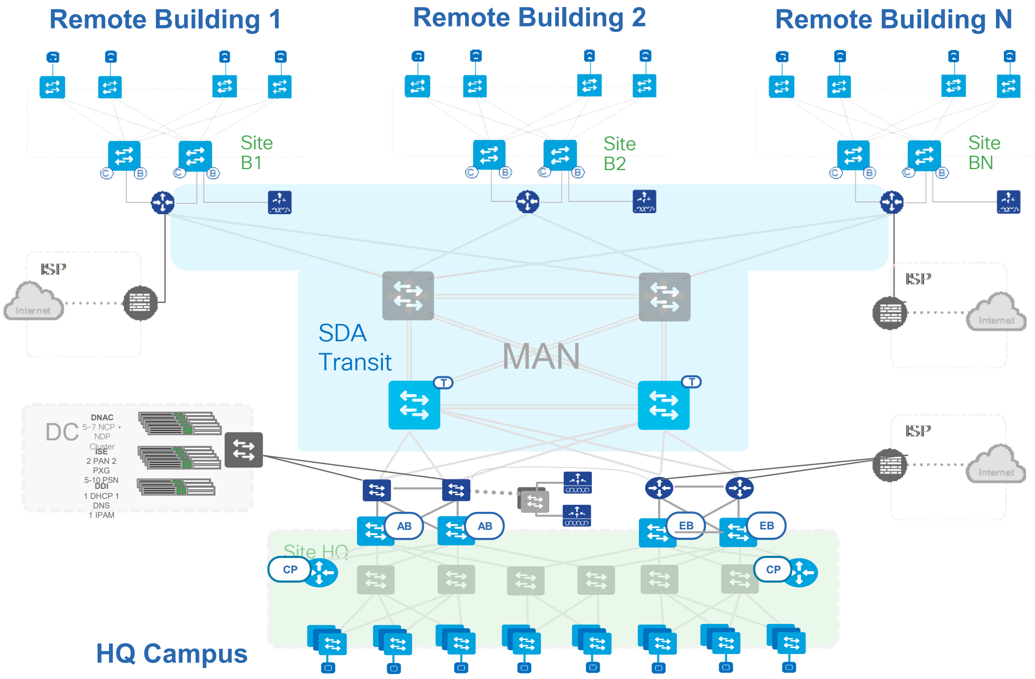
SDA Transit

Design for a multi site with SDA Transit

Overview

- Customers have multiple sites connect via “Dark Fiber” links or DWDM links
- Sites are in same Metropolitan area (a few hundred miles apart)

- Typical use cases
  - Consistent policy and end-to-end segmentation using VRFs and SGTs
  - Smaller and Isolated fault domains
  - Resiliency and Scalability

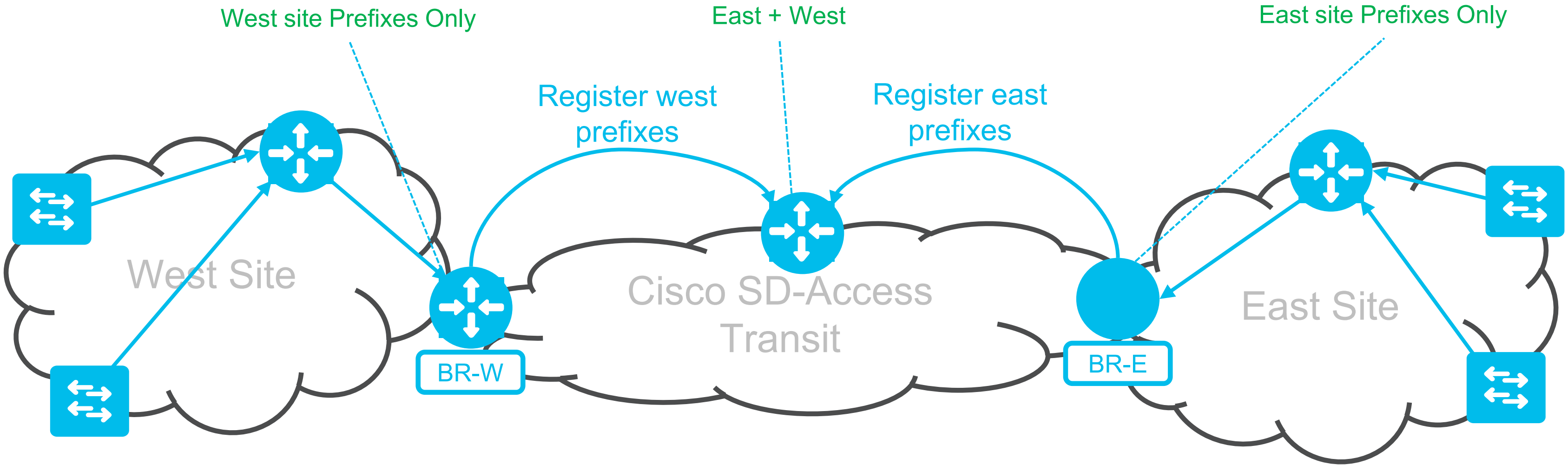


Cisco SD-Access Distributed Site Control Plane for Global Scale

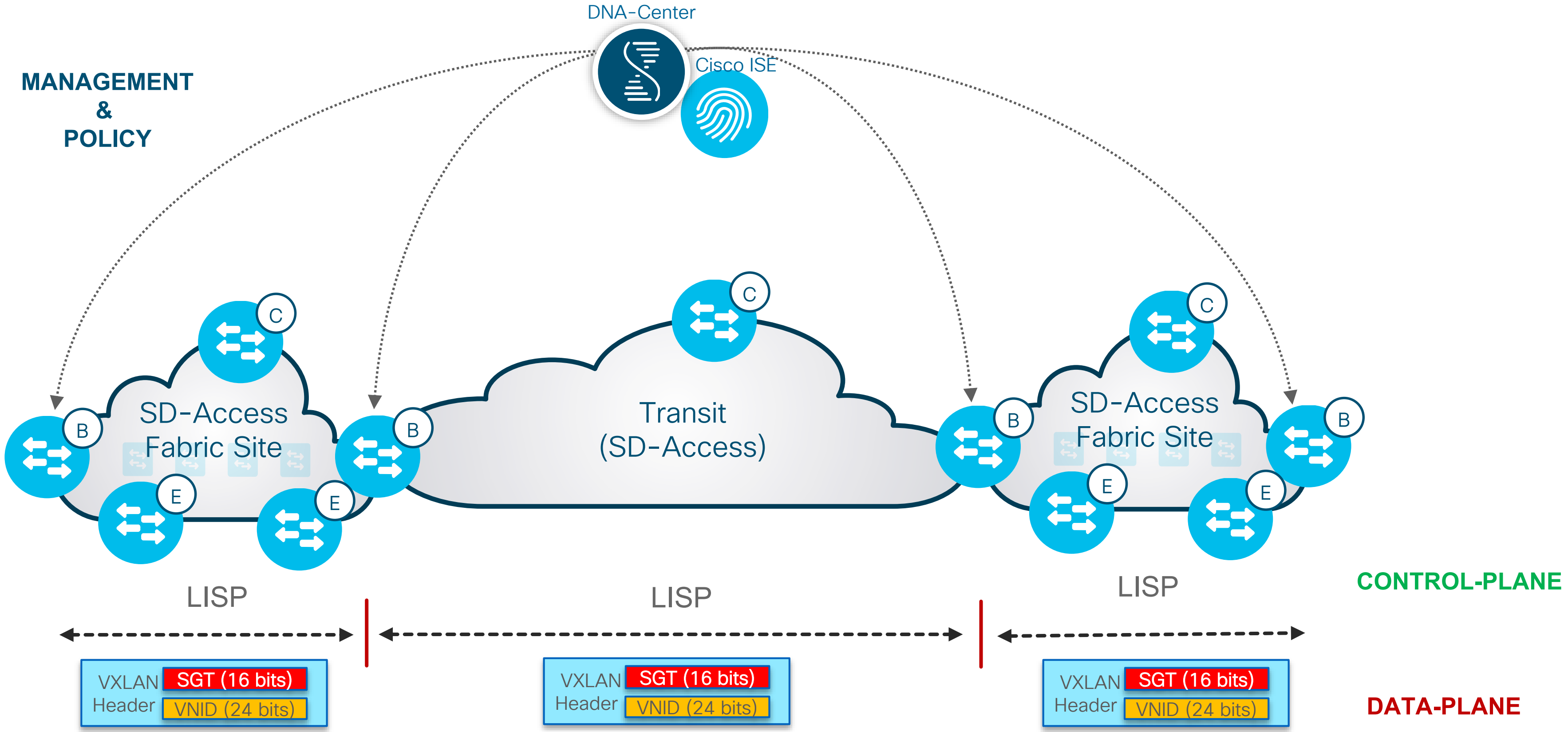
Multiple SD-Access Fabric Sites

Use Case

- Each site only maintains state for in-site end-points.
- Off site traffic follows default to transit.
- Survivability, each site is a fully autonomous resiliency domain
- Each Site has its own unique subnets



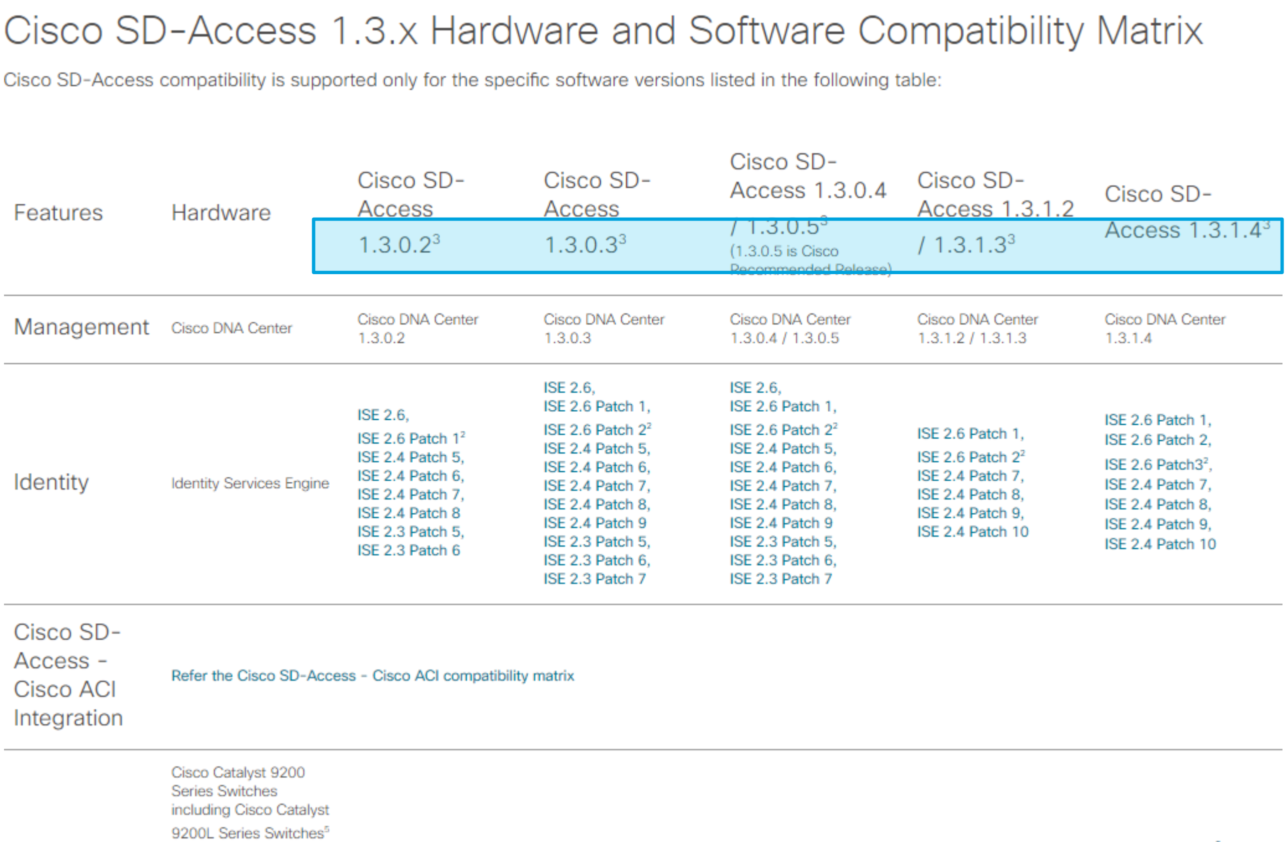
Native SD-Access Transit with Multi-Site Design



Device Compatibility

For your reference

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html



Cisco SD-Access 1.3.x Hardware and Software Compatibility Matrix

Cisco SD-Access compatibility is supported only for the specific software versions listed in the following table:

Features	Hardware	Cisco SD-Access 1.3.0.2[3]	Cisco SD-Access 1.3.0.3[3]	Cisco SD-Access 1.3.0.4 / 1.3.0.5[3] (1.3.0.5 is Cisco Recommended Release)	Cisco SD-Access 1.3.1.2 / 1.3.1.3[3]	Cisco SD-Access 1.3.1.4[3]
Management	Cisco DNA Center	Cisco DNA Center 1.3.0.2	Cisco DNA Center 1.3.0.3	Cisco DNA Center 1.3.0.4 / 1.3.0.5	Cisco DNA Center 1.3.1.2 / 1.3.1.3	Cisco DNA Center 1.3.1.4
Identity	Identity Services Engine	ISE 2.6, ISE 2.6 Patch 1[2] ISE 2.4 Patch 5, ISE 2.4 Patch 6, ISE 2.4 Patch 7, ISE 2.4 Patch 8 ISE 2.3 Patch 5, ISE 2.3 Patch 6	ISE 2.6, ISE 2.6 Patch 1, ISE 2.6 Patch 2[2] ISE 2.4 Patch 5, ISE 2.4 Patch 6, ISE 2.4 Patch 7, ISE 2.4 Patch 8, ISE 2.4 Patch 9 ISE 2.3 Patch 5, ISE 2.3 Patch 6, ISE 2.3 Patch 7	ISE 2.6, ISE 2.6 Patch 1, ISE 2.6 Patch 2[2] ISE 2.4 Patch 5, ISE 2.4 Patch 6, ISE 2.4 Patch 7, ISE 2.4 Patch 8, ISE 2.4 Patch 9 ISE 2.3 Patch 5, ISE 2.3 Patch 6, ISE 2.3 Patch 7	ISE 2.6 Patch 1, ISE 2.6 Patch 2[2] ISE 2.4 Patch 7, ISE 2.4 Patch 8, ISE 2.4 Patch 9, ISE 2.4 Patch 10	ISE 2.6 Patch 1, ISE 2.6 Patch 2, ISE 2.6 Patch3[2], ISE 2.4 Patch 7, ISE 2.4 Patch 8, ISE 2.4 Patch 9, ISE 2.4 Patch 10
Cisco SD-Access - Cisco ACI Integration	Refer the Cisco SD-Access - Cisco ACI compatibility matrix					
	Cisco Catalyst 9200 Series Switches including Cisco Catalyst 9200L Series Switches[5]					

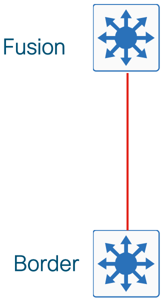
SD-Access Wired Design Considerations

Fusion Configuration

Connecting Fabric to Traditional Infrastructure

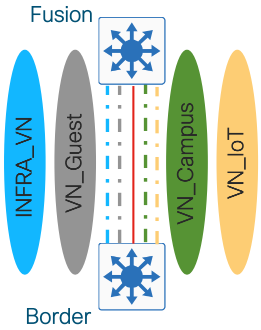
Extend

- Configure VRF
- Interfaces for each VN matching Border configuration



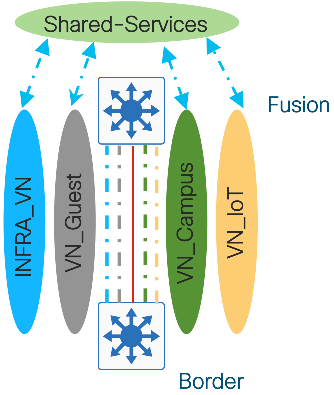
eBGP

- eBGP neighbors for each VN between Fusion and Border



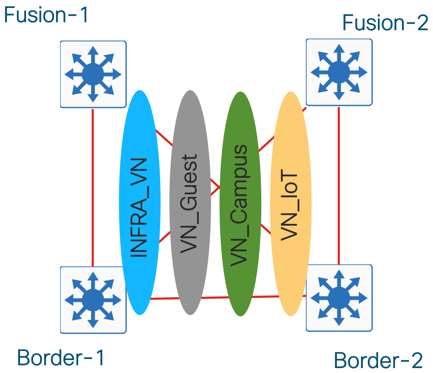
Route Leak

- Route-leak shared-services subnets to each VN
- Route-leak VN subnets into Global



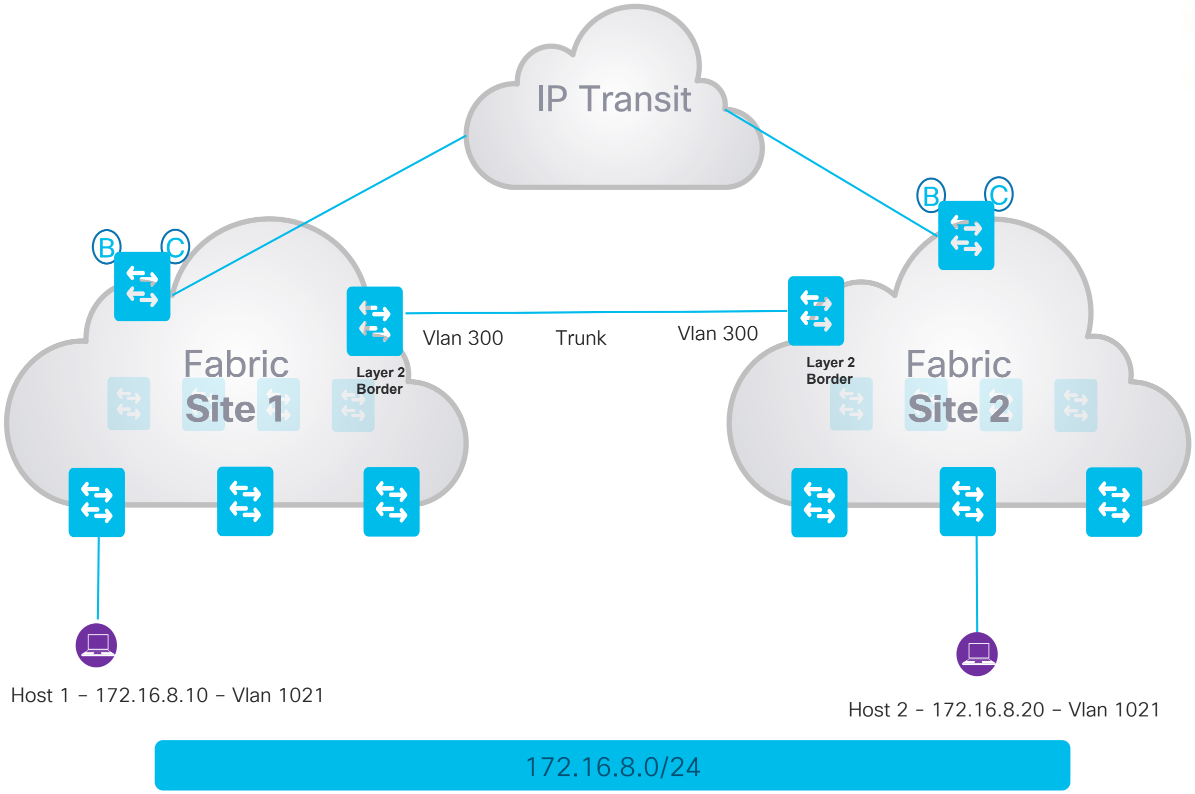
iBGP

- iBGP neighbors for each VN between Border nodes



- If Border / Fusion network device is Routing platform, L3 sub-interfaces will be used to extend Virtual Networks
- If Border / Fusion network device is Switching platform, VLANs & Trunk will be used to extend Virtual Networks

L2 Intersite Handoff- 1.3.3



- This feature can be used when inter site communication for Layer 2 traffic such as ARP, Broadcast, Link local multicast is needed for a subnet across fabric site.
- This can be achieved by configuring a handoff on Layer 2 Border across multiple fabric sites for a specific VLAN.
- This creates a Trunk between both fabric sites on a given interface.
- For Border which is doing L3 handoff towards IP Transit, we export /32 routes for that VN that is extended across fabric sites.
- Wireless hosts mobility is not possible with this feature.

SD-Access Extension

- Key Benefits for IoT and Business

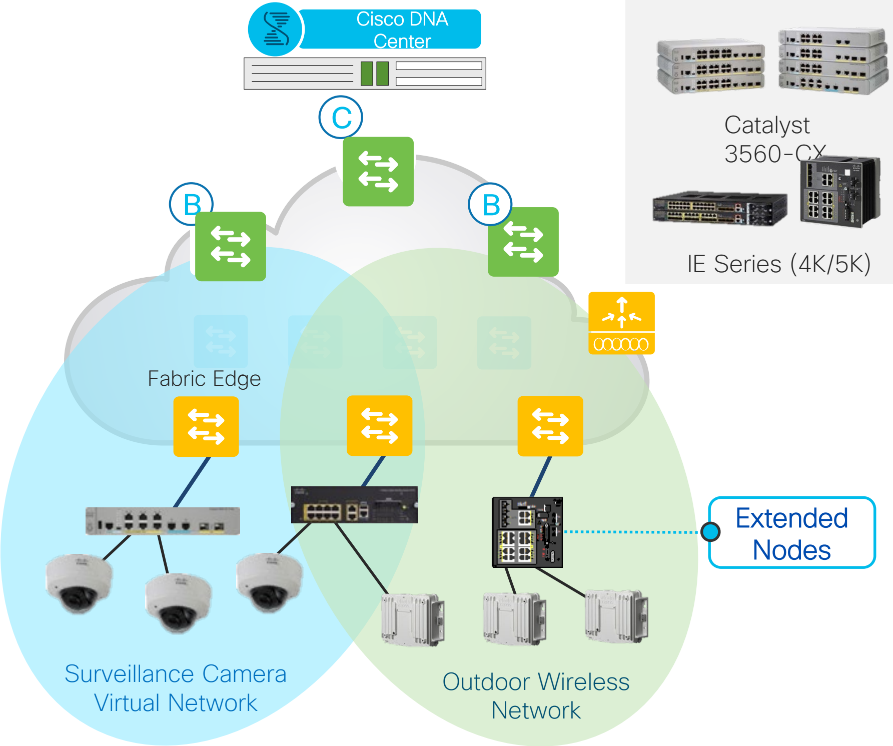
Extending Wireless

- Outdoors areas like Parking , Warehouse etc.
- OT areas in Plants , Manufacturing etc.

Benefits

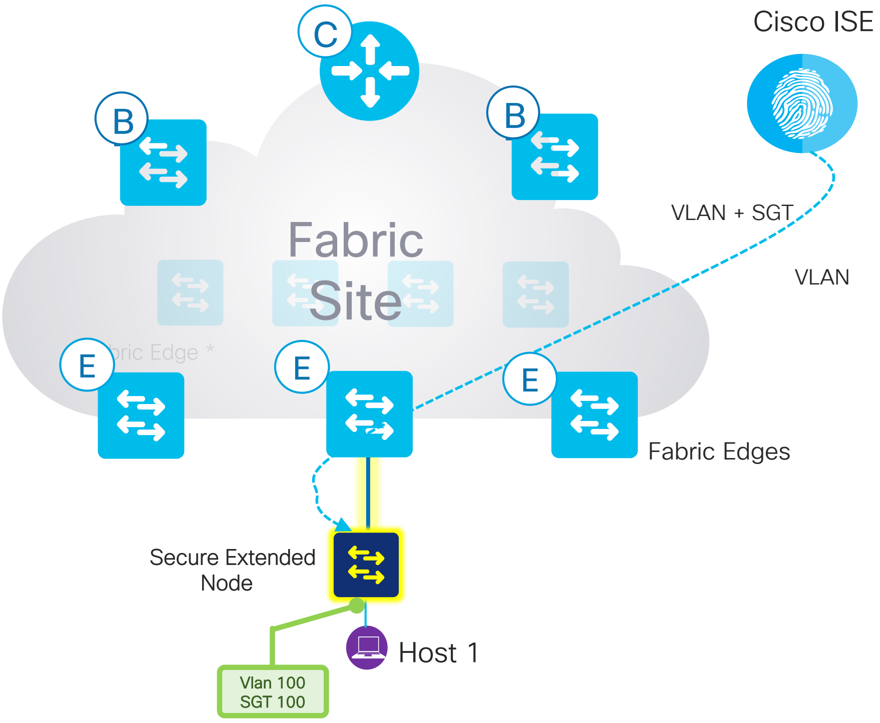
- Operational IOT simplicity for
  - IT designed and managed or
  - IT designed and OT managed
- Greater visibility to wide set of IoT devices
- Improved threat detection and containment

Extended Nodes extend SD-Access beyond the Fabric edge Edge



Platform Support

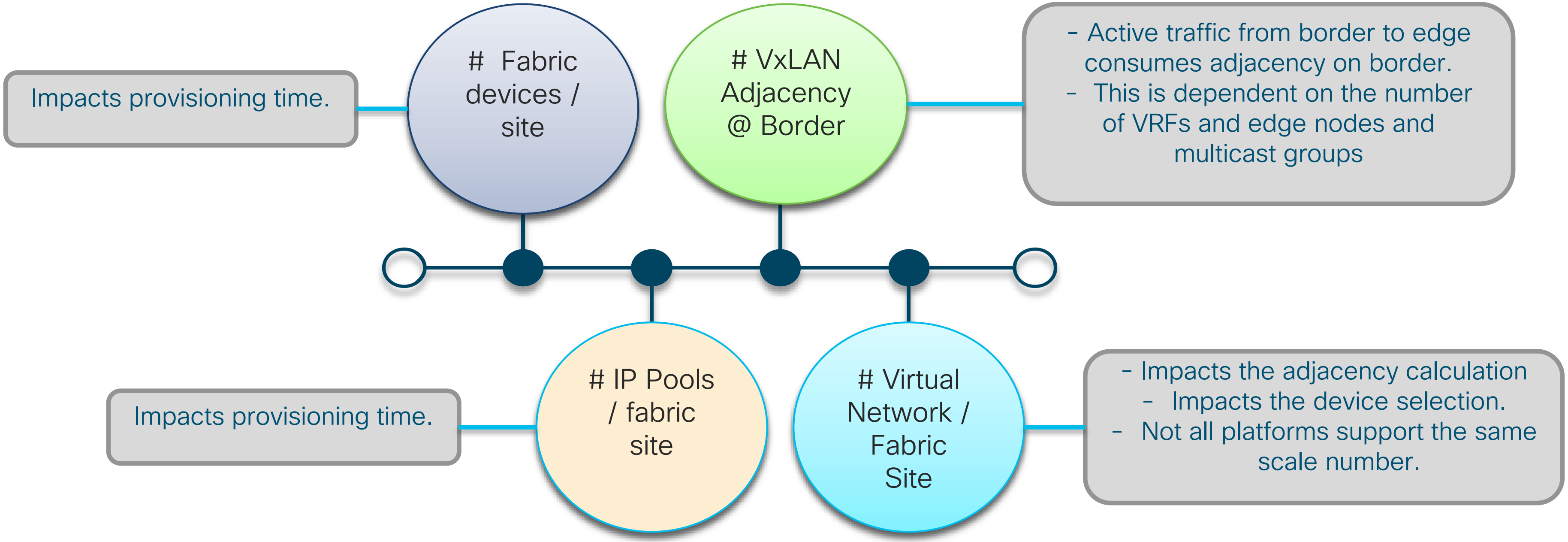
Policy Extended Node – 1.3.3



Supported Platform:
IE3400, IE3400H

- *Policy Extended Node* will have 802.1x/MAB Authentication enabled to communicate with ISE to download the VLAN and **Scalable Group Tag** attributes for end points.
- Link connecting Edge to Secure Extended node is configured with inline tagging so that SGT is propagated.
- Secure Extended nodes performs SGACL enforcement.
- Current Fabric Edge behavior of downloading VLAN/SGT tag is now possible with secure extended node.

Per Site Scale Factors to Consider in Fabric.



Impacts provisioning time.

# Fabric devices / site

# VxLAN Adjacency @ Border

- Active traffic from border to edge consumes adjacency on border.
- This is dependent on the number of VRFs and edge nodes and multicast groups

Impacts provisioning time.

# IP Pools / fabric site

# Virtual Network / Fabric Site

- Impacts the adjacency calculation
- Impacts the device selection.
- Not all platforms support the same scale number.

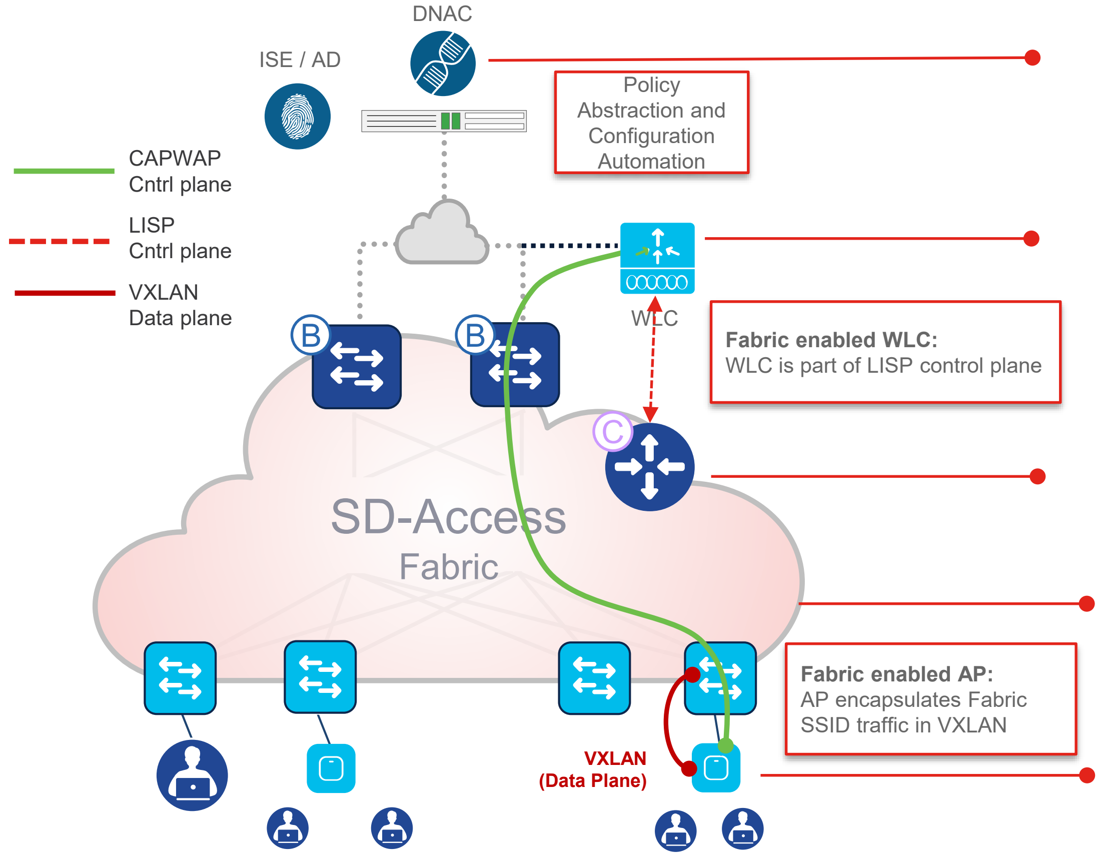
Adjacency calculation – (no of active VRF x edge nodes) + multicast groups

A bit about your Speaker

- Nidhi Pandey
- Technical Marketing Engineer at Cisco Systems.
- ~10 Years with Cisco Systems
- Focus on Enterprise & Security
- Ask me about : Indian History, Good Reads, Bangalore and Bollywood

SD-Access Wireless Design Considerations

SD-Access Wireless Architecture



Fabric enabled WLC:
WLC is part of LISP control plane

Fabric enabled AP:
AP encapsulates Fabric SSID traffic in VXLAN

Automation

- DNAC simplifies the Fabric deployment,
- Including the wireless integration component

Centralized Wireless Control Plane

- WLC still provides client session management
- AP Mgmt, Mobility, RRM, etc.
- Same operational advantages of CUWN

LISP control plane Management

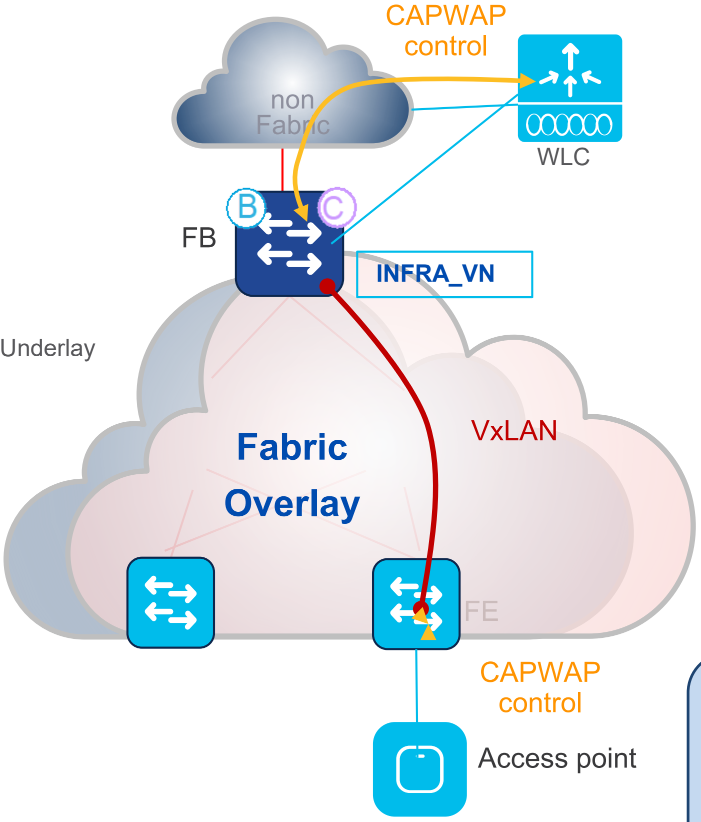
- WLC integrates with LISP control plane
- WLC updates the CP for wireless clients
- Mobility is integrated in Fabric thanks to LISP CP

Optimized Distributed Data Plane

- Fabric overlay with Anycast GW + Stretched subnet
- VLAN extension with no complications
- All roaming is Layer 2

VXLAN from the AP

- Carrying hierarchical policy segmentation starting from the edge of the network



Access Points

- AP is directly connected to FE (or to an extended node switch)
- AP is part of Fabric overlay
- AP belongs to the INFRA_VN which is mapped to the global routing table (new in DNAC 1.1)
- AP joins the WLC in Local mode

WLC

- WLC is connected outside Fabric (optionally directly to Border)
- WLC needs to reside in global routing table – to talk to CP!
- No need for inter-VRF leaking for AP to join the WLC
- WLC can only belong to one FD. WLC talks to one CP (two for HA)

Design Notes:
1) Fabric AP is in local mode, need < 20ms latency between AP & WLC
2) If WLC is used also for non-Fabric (mixed mode), considered MAC and ARP table scale of the directly-connected Border device

What are my Options for Wireless with SDA ?

Over the Top (OTT)

Fabric Enabled Wireless (FEW)

Mixed Mode

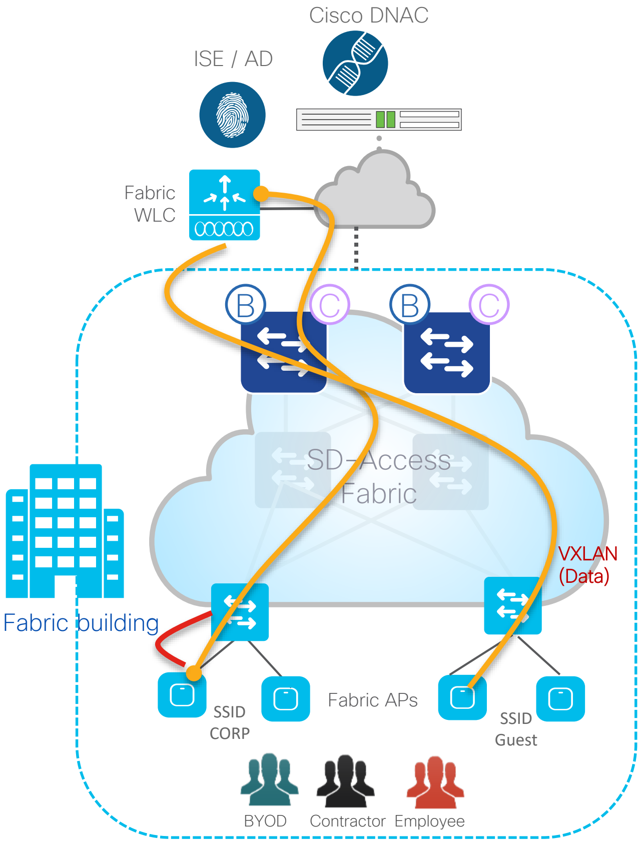
Design Consideration

Common for Greenfield & Brownfield

Network Hierarchy	Site Location Mapping, ISE, IP Services
Scale	Network Scale and Wireless
Underlay Readiness	Global Routing Table, Infra VN & CAPWAP
Device Discovery	WLC Discovery & Assurance, Brownfield Support, PnP

Cisco SD-Access Wireless Adoption

- Fabric Enabled Wireless



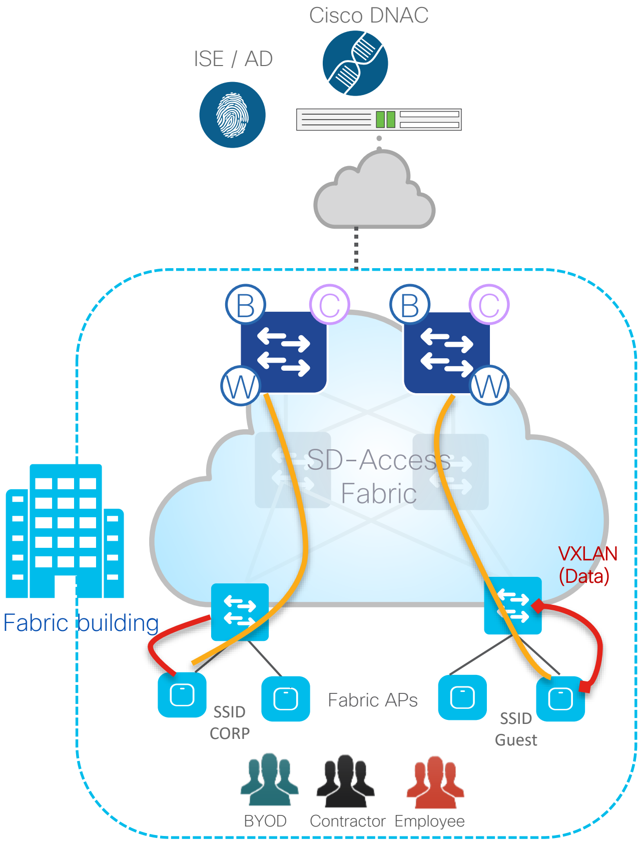
Full Cisco SD-Access Wireless value

- Cisco DNA Center with Automation & Assurance
- Virtual Networks for Segmentation (ex Employee, IoT, Guest)
- ISE for SGT Access Control within VRF (ex. Contractor, BYOD, Employees)
- Subnet extension across Campus with distributed data plane
- Optimized path for Guest and no Anchor WLC
- And more…

🟧	CAPWAP Control
🟥	VXLAN

Cisco SD-Access Wireless Adoption

- Fabric Enabled Wireless with eWLC



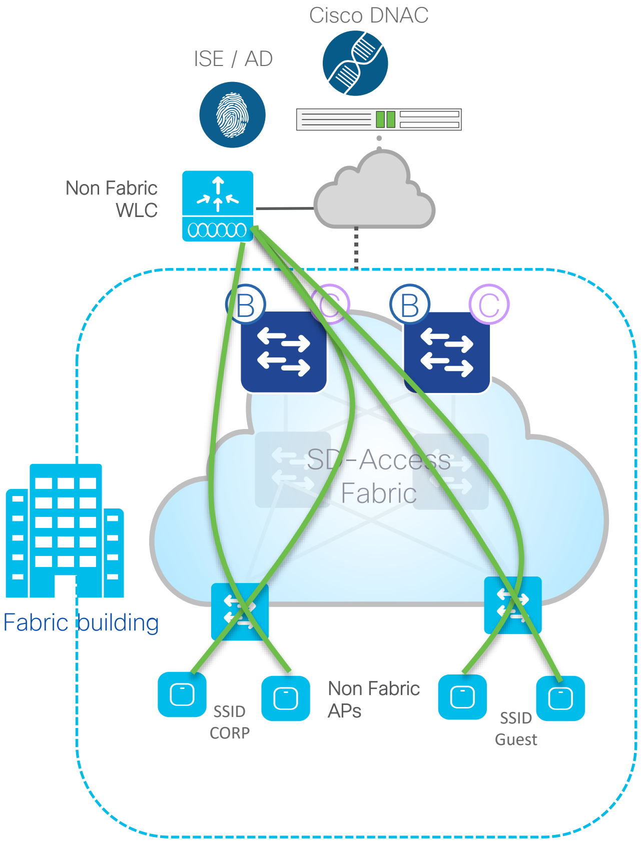
Full Cisco SD-Access Wireless value with eWLC

- Cisco DNA Center with Automation & Assurance
- Virtual Networks for Segmentation (ex Employee, IoT, Guest)
- ISE for SGT Access Control within VRF (ex. Contractor, BYOD, Employees)
- Subnet extension across Campus with distributed data plane
- Optimized path for Guest and no Anchor WLC
- And more…

🟧 CAPWAP Control
🟥 VXLAN

Cisco SD-Access Wireless Adoption

- Over the Top (OTT)



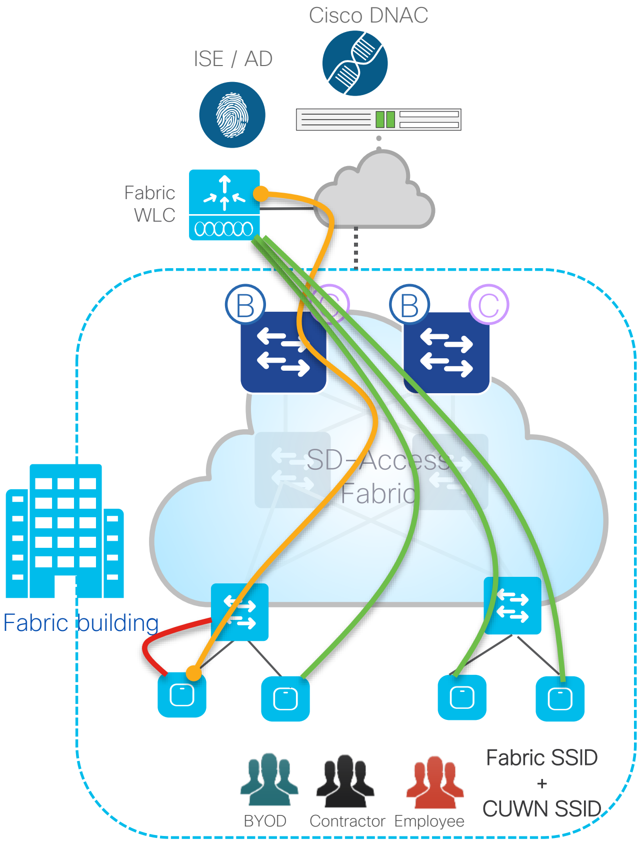
OTT Use Cases

- No SDA advantages for wireless
- Migration step to full SD-Access
- Customer wants/need to first migrate wired (different Ops teams managing wired and wireless, get familiar with Fabric, different buying cycles, etc.) and leave wireless “as it is”
- Customer cannot migrate to Fabric yet (older APs, need to certify the new software, etc.)

🟩 CAPWAP Control and Data

Cisco SD-Access Wireless Adoption

- Mixed Mode

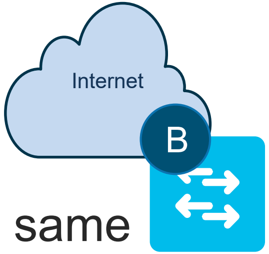


- Mix of Fabric and non-Fabric (centralized) SSIDs
- Mixed mode is supported both on the same AP or different APs
- Non Fabric SSID : Client Traffic is CAPWAP encapsulated
- Fabric SSID : Client Traffic is VXLAN encapsulated

🟩	CAPWAP Control and Data
🟧	CAPWAP Control
🟥	VxLAN

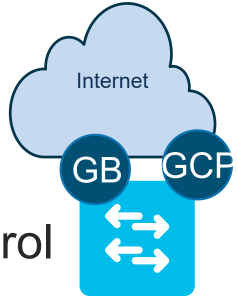
Guest Access Deployment

Guest as VN



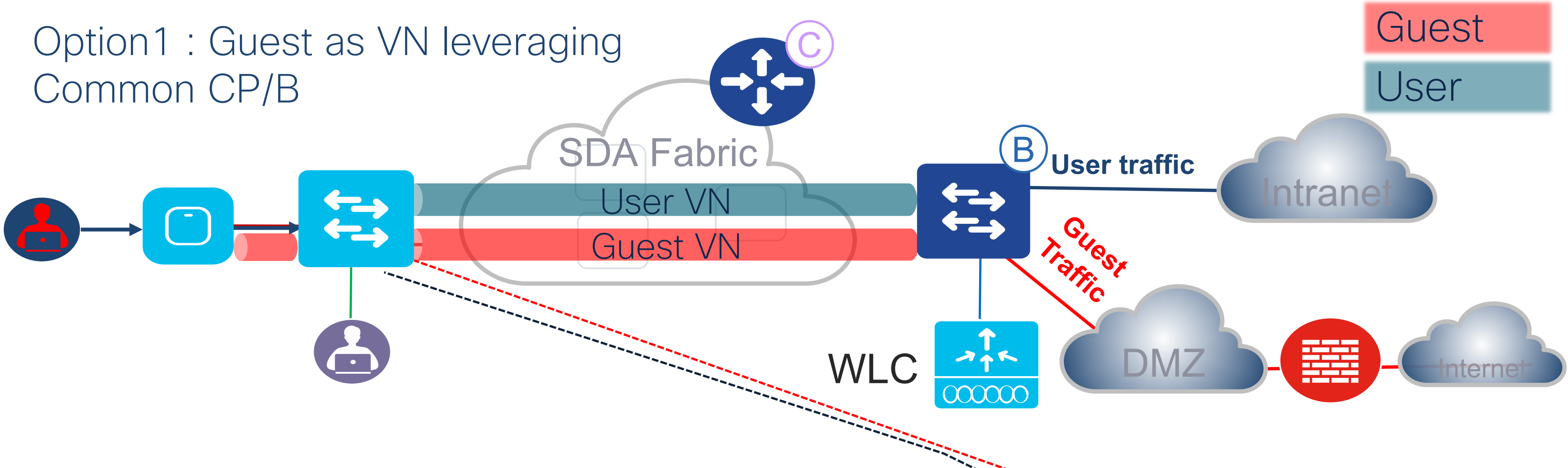
- Guest traffic using the same Border /Control plane as like any other VN
- Work flow automated from DNAC
- Simplified design
- External handoff via VRF-Lite

Dedicated GB/GCP



- A dedicated Border and Control plane for Guest VN
- Deploy as co-located or distributed nodes.
- Manual work flows required
- Identical to traditional Guest Anchor solution.
- Ideal for stringent compliance requirements

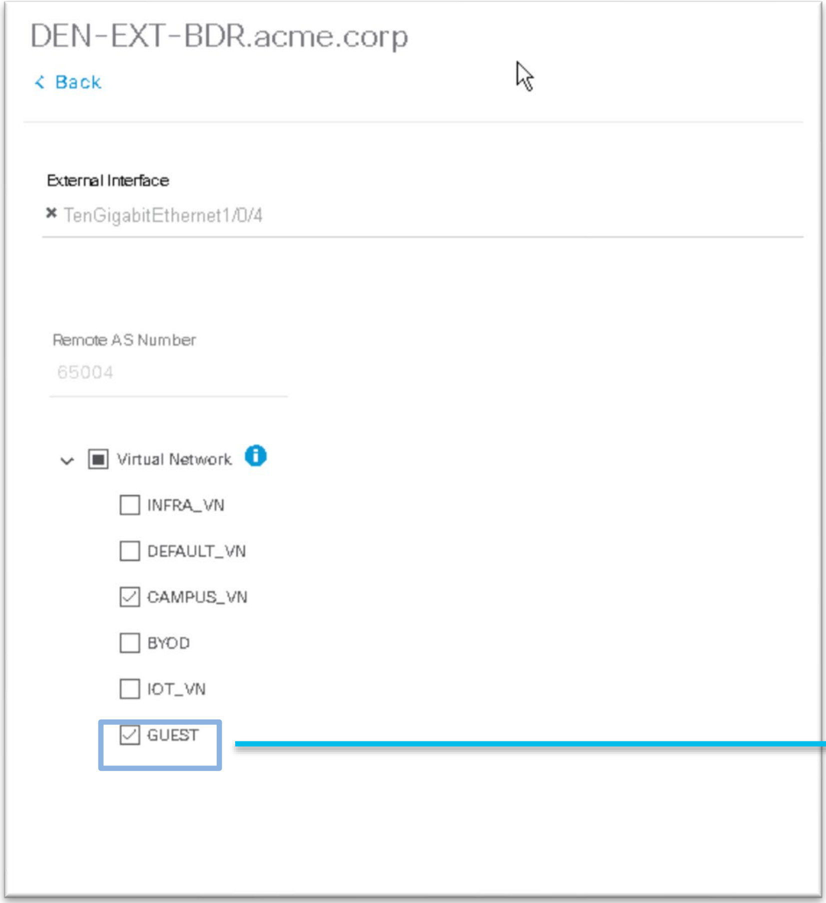
Option1 : Guest as VN leveraging Common CP/B



- Common border /CP between user VN and Guest VN
- Traffic steering at the border for Guest into DMZ using vrf-lite
- eBGP handoff workflow automated through DNAC
- Segmentation within fabric achieved by VNID(macro segementation)

```
router lisp
locator-table default
locator-set edge
  IPv4-interface Loopback0
priority 10 weight 10
!
ipv4 use-petr 3.1.1.1
```

Guest VN Border Handoff



DEN-EXT-BDR.acme.corp

< Back

External Interface

× TenGigabitEthernet1/0/4

Remote AS Number

65004

⌄ ■ Virtual Network

□ INFRA_VN

□ DEFAULT_VN

☑ CAMPUS_VN

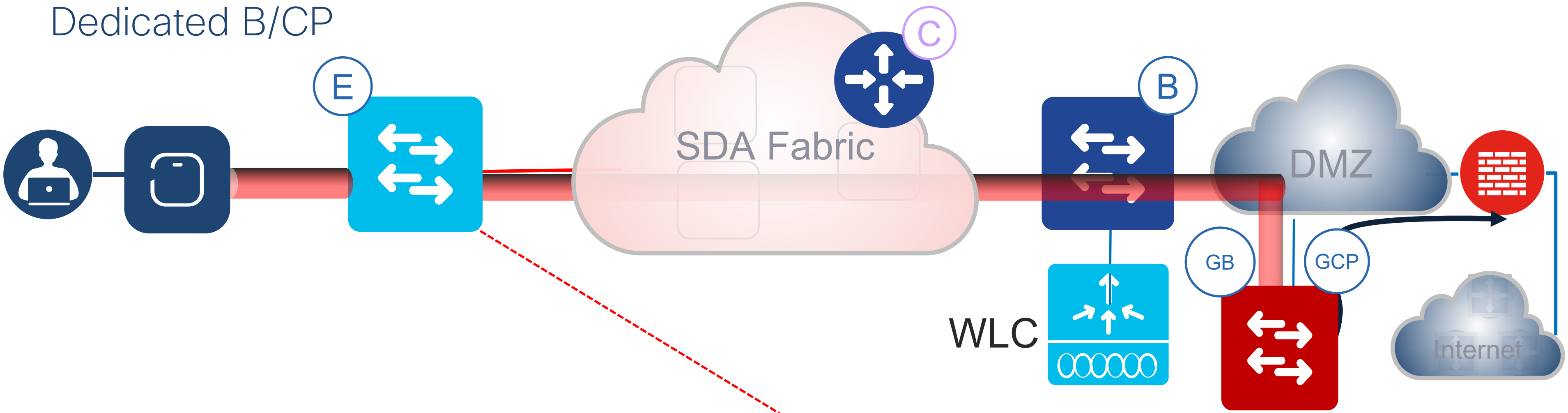
□ BYOD

□ IOT_VN

☑ GUEST

Extend Guest VN

Option 2: Guest as VN with Dedicated B/CP

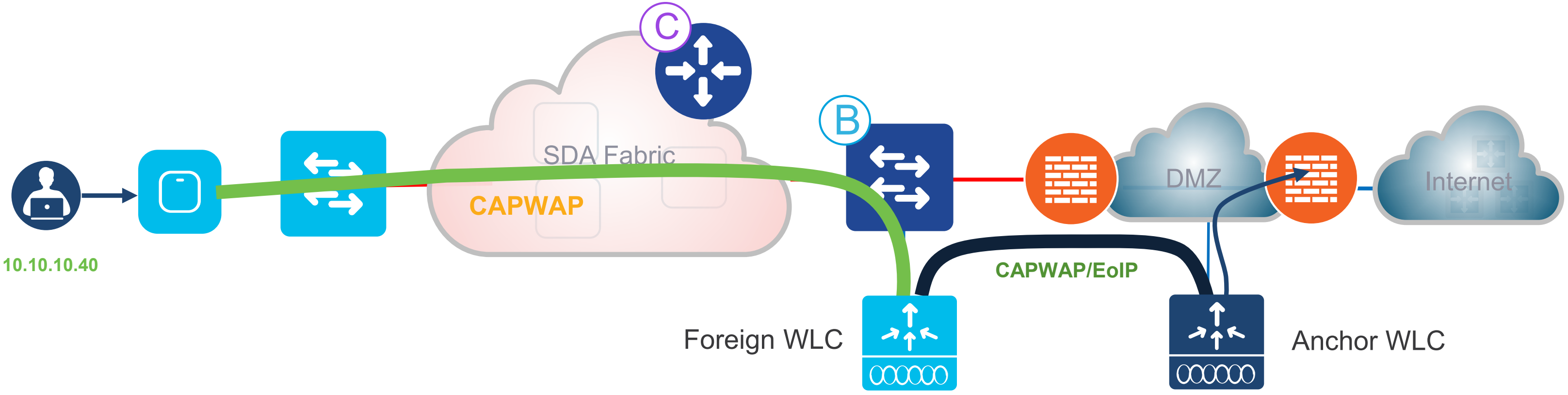


- Guest border RLOC should be reachable in the Underlay
- End to End MTU of 9100
- Register Guest EIDs to Guest control plane(GCP)
- All Guest traffic terminated on a dedicated guest border(GB)
- East to west isolation can be achieved by micro segmentation.

```
router lisp
service ipv4
   eid-table vrf GUEST
   map-cache 0.0.0.0/0 map-request
   itr map-resolver 192.168.10.2
   etr map-server 192.168.10.2 key 7 02130752
   etr map-server 192.168.10.2 proxy-reply
   etr
   sgt
   use-petr 192.168.10.2
   proxy-itr 192.168.41.5
   exit-service-ipv4
```

SD-Access Wireless Guest Design

- Anchor-Foreign CUWN Solution



- Guest WLAN anchored at Guest Anchor in DMZ
- Well proven CUWN solution, protecting investment
- Separate solution for Wired Guest, Anchor WLC managed differently

Fabric in a Box Scale and DNAC Scale

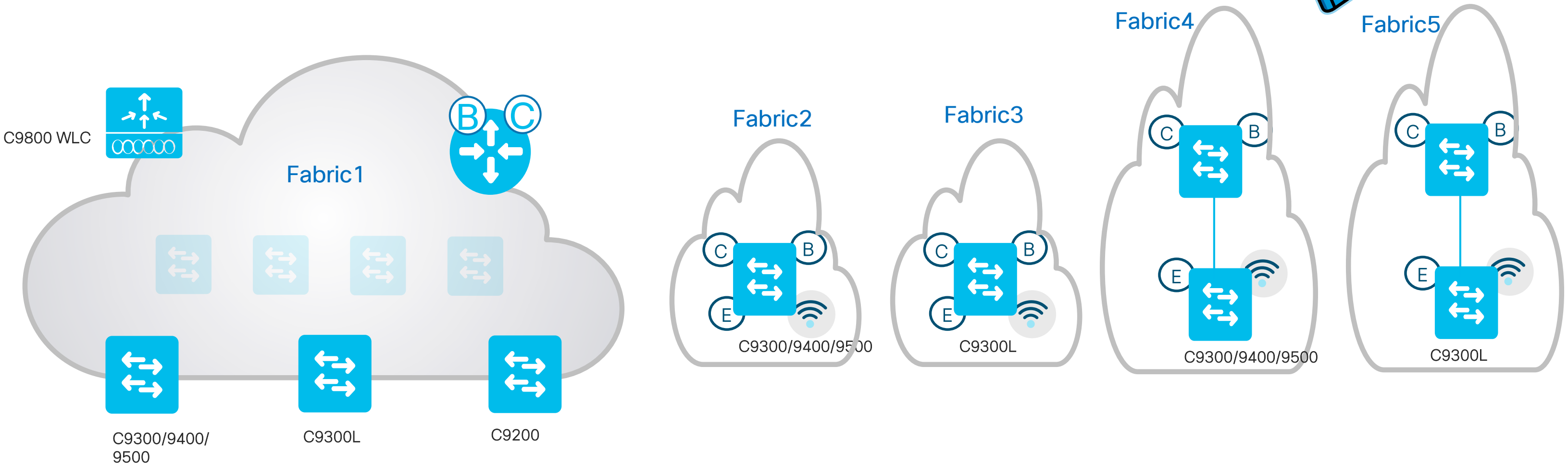
For your reference

DNAC 1.3 Release

Parameters	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
No of Devices (Switch/Route/WLC)	1000	2000	5000
No of Access Points	4000	6000	12000
No of Endpoints (Concurrent)	25,000	40,000	100,000
No of endpoints – wired: wireless ratio	Any	Any	Wired: 40,000 Wireless: 60,000
Number of Site Elements	500	1000	2000
No of WLC	500	1000	2000

Fabric Wireless Scale

For your reference



	C9300/9400/ 9500 as edge	C9300L as edge	C9200 as edge	C9300/9400/9500 (with embedded wireless) FiAB	C9300L (with embedded wireless) FiAB	C9300/9400/9500 (with embedded wireless) as edge	C9300L (with embedded wireless) as edge
Access Points	200	50	25	100	50	200	50
Clients	4000	1000	500	2000	1000	4000	1000

Wireless Controller Scale

For your reference

Platform	Number of AP’s	Number of end points	SDA Design
3504	150	3000	Small
5520	1500	20,000	Small or Medium
8504	6000	40,000	Medium or Large
Catalyst 9800	Up To 6000	Up To 64,000	Small, Medium or Large
Catalyst 9k (Embedded WLC) *except cat92xx	200	4000	Small, Medium

For more details: cs.co/sda-compatibility-matrix

SD-Access Platforms

SD-Access Wireless

AireOS WLC

- AIR-CT3504
- AIR-CT5520
- AIR-CT8540

Catalyst 9800

NEW

- Catalyst 9800-40/80
- Catalyst 9800-CL
- Catalyst 9800 Embedded WLC

Wi-Fi 6, 11ac Wave 2 Wave 1*AP

- Catalyst 9100
- AIR-AP1800, 2800, 3800, and 4800

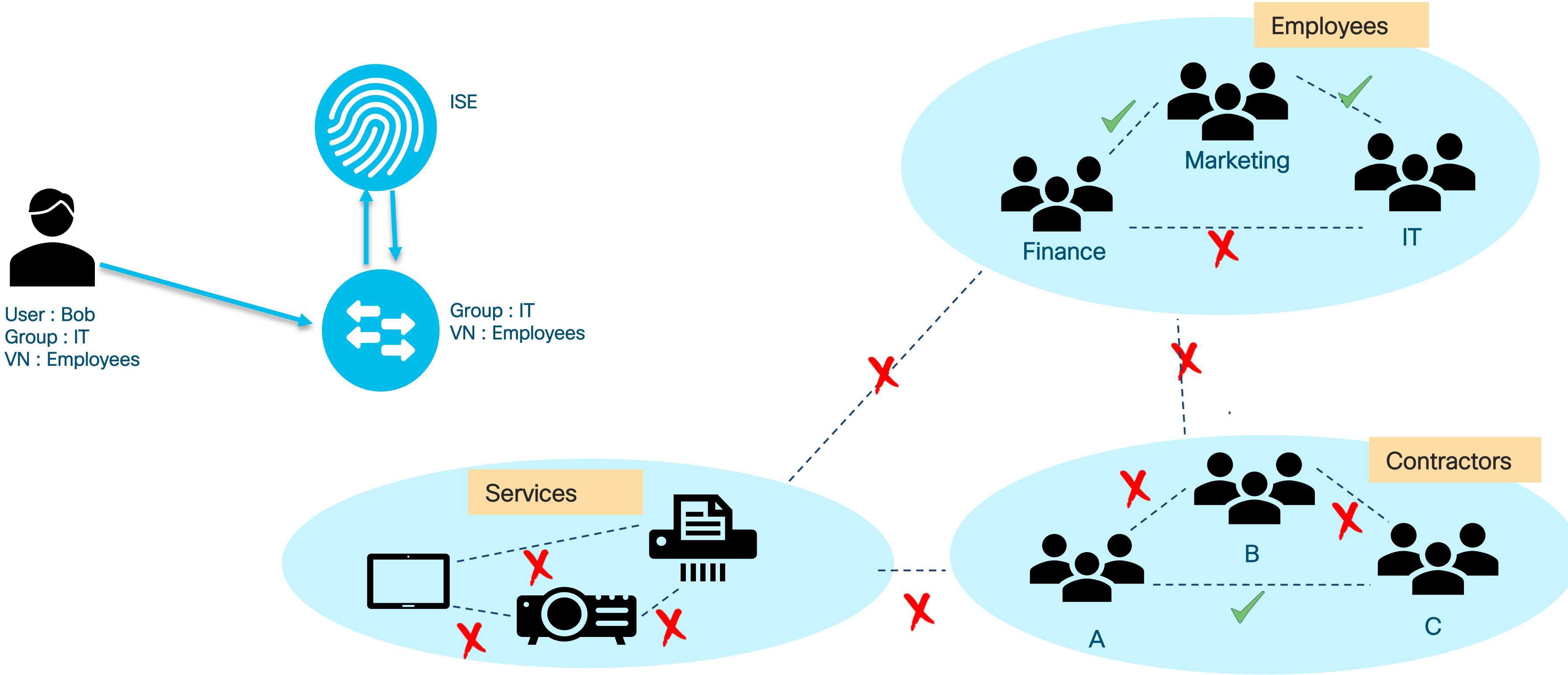
- AIR-CAP1700, 2700 and 3700
- AIR-AP1540, 1560

* No IPv6, AVC, FNF

cisco Live!

Segmentation and Policy Best Practices

Segmentation Overview



Default access between groups in a VN is Permit All

Access between groups across VNs can be achieved using a stateful device (i.e Firewall)

Getting Started

Identify assets to protect

e.g., your Crown Jewels:
Cardholder data
Medical records
Intellectual Property
Prod vs Dev Separation
Vulnerable systems

Protect employees from lateral movement of threats

Map assets to policy groups

Users/Devices : Define dynamic SGT classification based on context

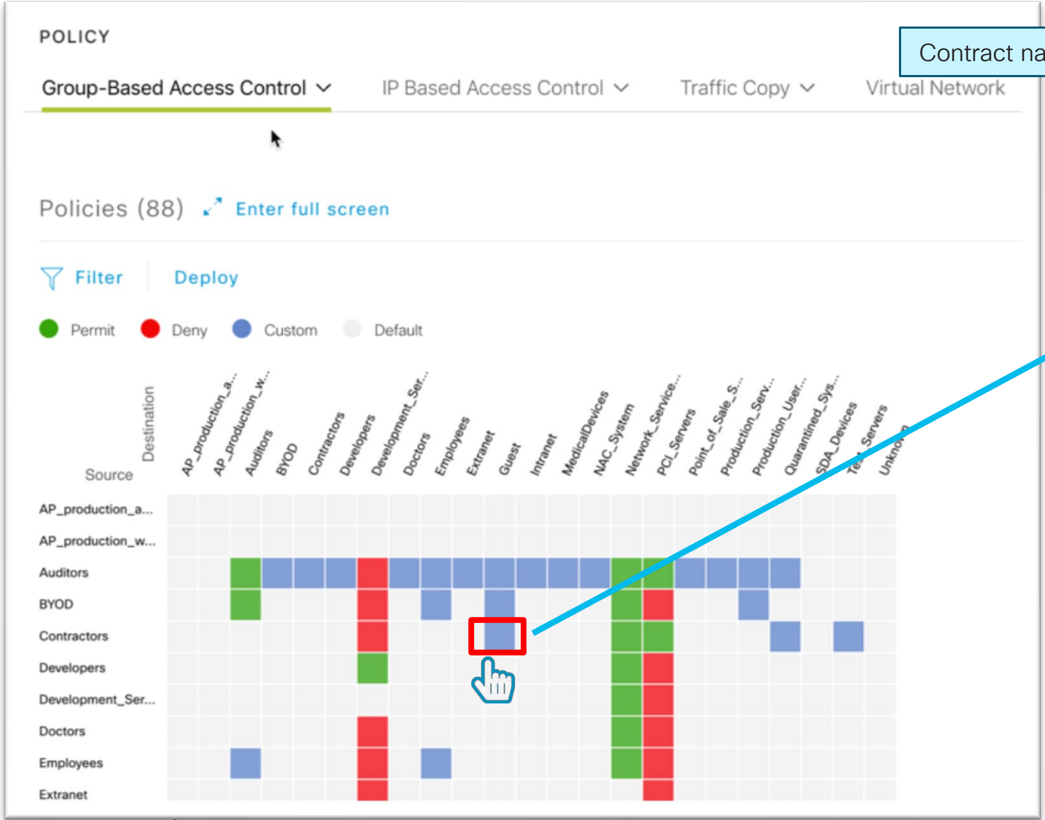
Protected Apps/Resources:

- Define DC resources
- Learn from ACI DC
- Learn from Cloud

Policy Enforcement

- Define how groups can interact
- Enforcement on automatically on Edge Nodes for E-W
- Choose other enforcement points based on the use-case

New Policy View (post 1.3.1.0)



POLICY

Group-Based Access Control ⌄ | IP Based Access Control ⌄ | Traffic Copy ⌄ | Virtual Network

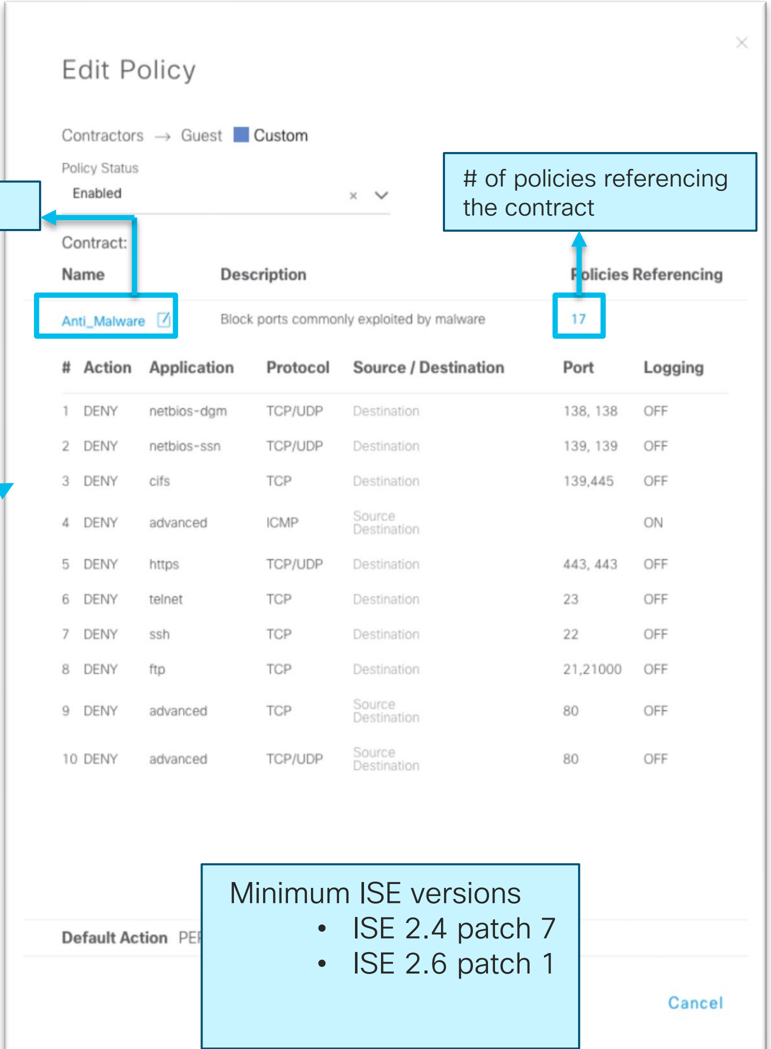
Policies (88) Enter full screen

Filter | Deploy

● Permit ● Deny ● Custom ● Default

Destination

Source	AP_production_a...	AP_production_w...	Auditors	BYOD	Contractors	Developers	Development_Ser...	Doctors	Employees	Extranet	Guest	Intranet	MedicalDevices	NAC_System	Network_Service...	PCI_Servers	Point_of_Sale_S...	Production_Serv...	Production_User...	Quarantined_Sys...	SDA_Devices	Test_Servers	Unknown
AP_production_a...																							
AP_production_w...																							
Auditors			🟩	🟦	🟦	🟦	🟥	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟦	🟦	🟦	🟦			
BYOD			🟩				🟥		🟦		🟦				🟩	🟥			🟦				
Contractors							🟥				🟦				🟩	🟩				🟦		🟦	
Developers							🟩								🟩	🟥							
Development_Ser...															🟩	🟥							
Doctors							🟥								🟩	🟥							
Employees			🟦				🟥		🟦						🟩	🟥							
Extranet							🟥									🟥							



Edit Policy ×

Contractors → Guest 🟦 Custom

Policy Status
Enabled × ⌄

Contract:

Name	Description	Policies Referencing
Anti_Malware	Block ports commonly exploited by malware	17

#	Action	Application	Protocol	Source / Destination	Port	Logging
1	DENY	netbios-dgm	TCP/UDP	Destination	138, 138	OFF
2	DENY	netbios-ssn	TCP/UDP	Destination	139, 139	OFF
3	DENY	cifs	TCP	Destination	139,445	OFF
4	DENY	advanced	ICMP	Source Destination		ON
5	DENY	https	TCP/UDP	Destination	443, 443	OFF
6	DENY	telnet	TCP	Destination	23	OFF
7	DENY	ssh	TCP	Destination	22	OFF
8	DENY	ftp	TCP	Destination	21,21000	OFF
9	DENY	advanced	TCP	Source Destination	80	OFF
10	DENY	advanced	TCP/UDP	Source Destination	80	OFF

Default Action PE

Cancel

Contract name

# of policies referencing the contract

Minimum ISE versions

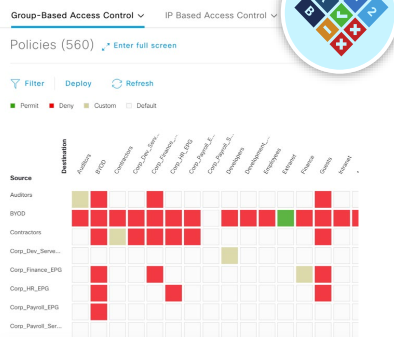
- ISE 2.4 patch 7
- ISE 2.6 patch 1

cisco Live!

Better Utilization of VN and SGTs to avoid the SGACL scale limitations.

# of VNs supported per site – 256 (Cat 9500)
If Each VLAN = variable <SGT>
Then
    SGACL = {count <SGT>}^{2}

Result = [Large SGACL matrix]



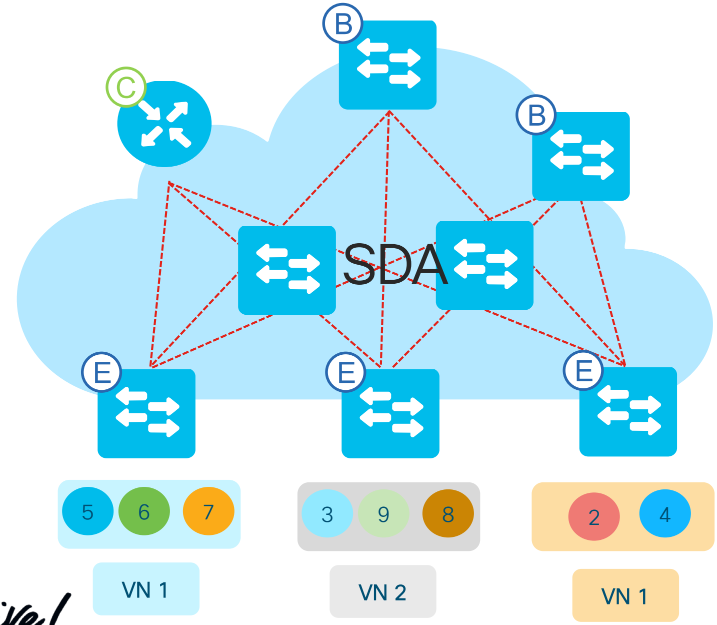
Group-Based Access Control ⌄   IP Based Access Control ⌄

Policies (560) Enter full screen

Filter | Deploy | Refresh

🟩 Permit 🟥 Deny ▨ Custom □ Default

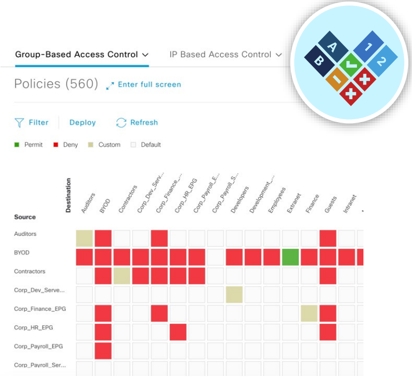
Source \ Destination	Auditors	BYOD	Contractors	Corp_Dev_Serv...	Corp_Finance_...	Corp_HR_EPG	Corp_Payroll_E...	Corp_Payroll_S...	Developers	Development_...	Employees	Extranet	Finance	Guests	Intranet	
Auditors	▨	🟥	□	□	🟥	□	□	□	□	□	□	□	□	🟥	□	□
BYOD	🟥	🟥	🟥	🟥	🟥	🟥	🟥	□	🟥	🟥	🟥	🟩	🟥	🟥	🟥	🟥
Contractors	□	🟥	▨	🟥	🟥	🟥	🟥	□	□	□	□	□	□	🟥	□	□
Corp_Dev_Serve...	□	□	□	□	□	□	□	□	▨	□	□	□	□	□	□	□
Corp_Finance_EPG	□	🟥	□	□	🟥	□	□	□	□	□	□	□	▨	🟥	□	□
Corp_HR_EPG	□	🟥	□	□	□	🟥	□	□	□	□	□	□	□	🟥	□	□
Corp_Payroll_EPG	□	🟥	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Corp_Payroll_Ser...	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□



Recommendation-

- Combination of VN and SGTs to limit the SGACLs
- Considerations to be given for VN and SGT constructs
- Start small

Shared SGTs across VNs



Group-Based Access Control ⌄ IP Based Access Control ⌄

Policies (560) Enter full screen

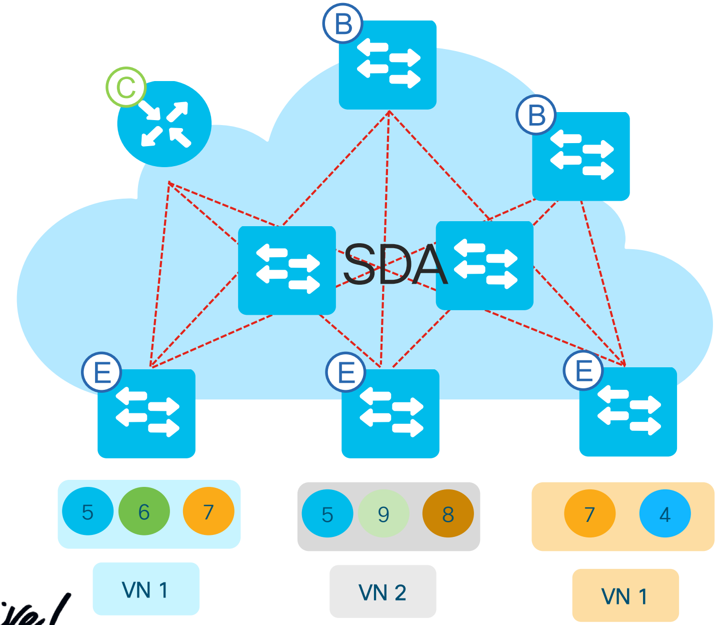
Filter | Deploy | Refresh

🟩 Permit 🟥 Deny ▨ Custom □ Default

Source \ Destination	Auditors	BYOD	Contractors	Corp_Dev_Serv...	Corp_Finance_...	Corp_HR_EPG	Corp_Payroll_E...	Corp_Payroll_S...	Developers	Development_...	Employees	Extranet	Finance	Guests	Intranet	
Auditors	▨	🟥	□	□	🟥	□	□	□	□	□	□	□	□	🟥	□	□
BYOD	🟥	🟥	🟥	🟥	🟥	🟥	🟥	□	🟥	🟥	🟥	🟩	🟥	🟥	🟥	🟥
Contractors	□	🟥	▨	🟥	🟥	🟥	🟥	□	□	□	□	□	□	🟥	□	□
Corp_Dev_Serve...	□	□	□	□	□	□	□	□	▨	□	□	□	□	□	□	□
Corp_Finance_EPG	□	🟥	□	□	🟥	□	□	□	□	□	□	□	▨	🟥	□	□
Corp_HR_EPG	□	🟥	□	□	□	🟥	□	□	□	□	□	□	□	🟥	□	□
Corp_Payroll_EPG	□	🟥	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Corp_Payroll_Ser...	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Use Case:

- Scale for SGTs and VNs cross the supported limit.
- Access requirements across VNs
- Default access between VNs is deny.

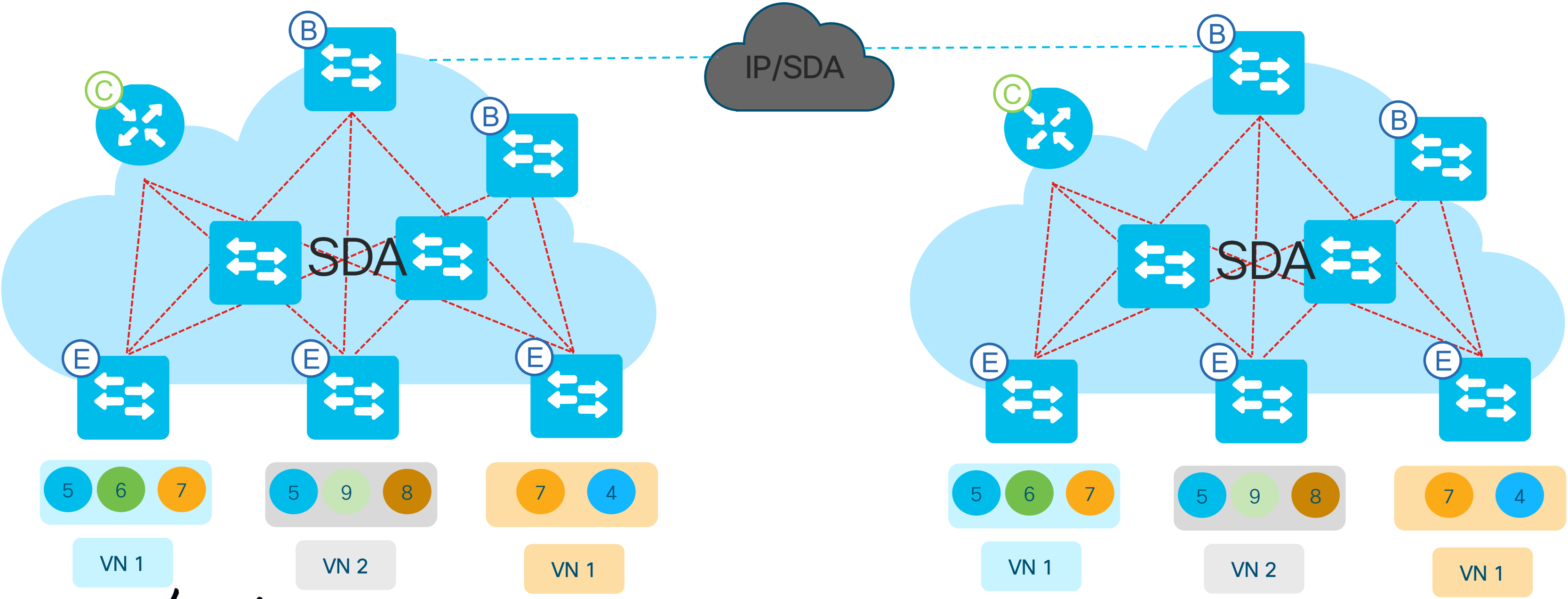


Recommendation- same SGTs in different VNs

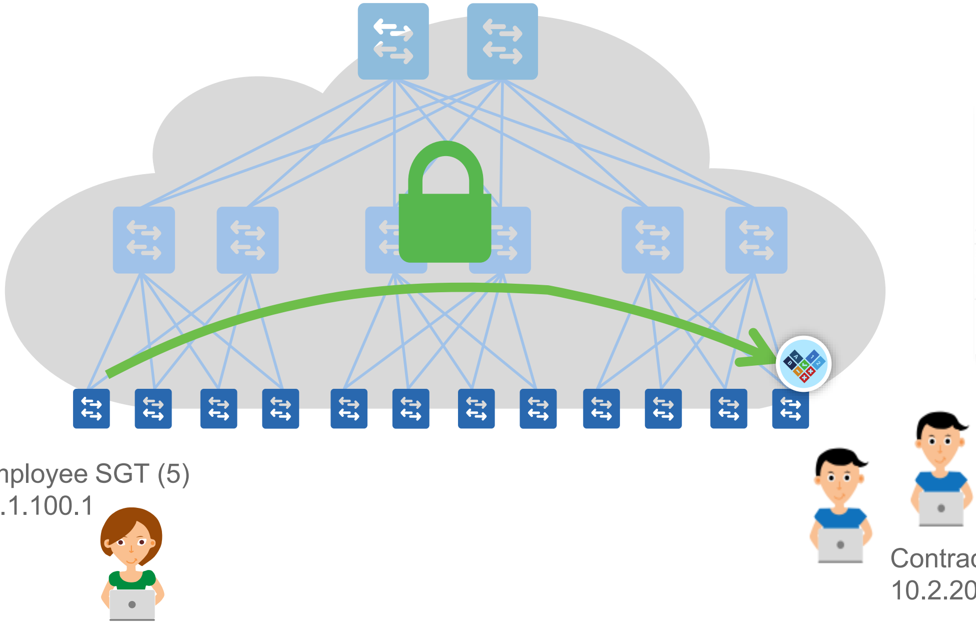
Supported in single site and multi-site designs

Multi-Site Policy Considerations

Need for Multisite deployment
Same SGTs can be shared across sites
Inline tagging supported by default in SDA transit
Make use of SXP domains



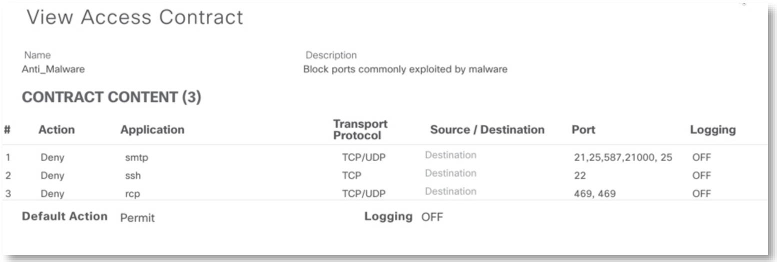
Enforcement Scale: IP/Group Mappings



Employee SGT (5)
10.1.100.1

Employee SGT (5)
10.2.200.6

Contractor SGT (10)
10.2.200.6



View Access Contract

Name
Anti_Malware

Description
Block ports commonly exploited by malware

CONTRACT CONTENT (3)

#	Action	Application	Transport Protocol	Source / Destination	Port	Logging
1	Deny	smtp	TCP/UDP	Destination	21,25,587,21000, 25	OFF
2	Deny	ssh	TCP	Destination	22	OFF
3	Deny	rcp	TCP/UDP	Destination	469, 469	OFF

Default Action Permit **Logging** OFF

Scale	C3850	C9300	C9400	C9500	C6800	N7700	ASR1K
IP-SGT	12,000	10,000	40,000	40,000	256,000	200,000	750,000

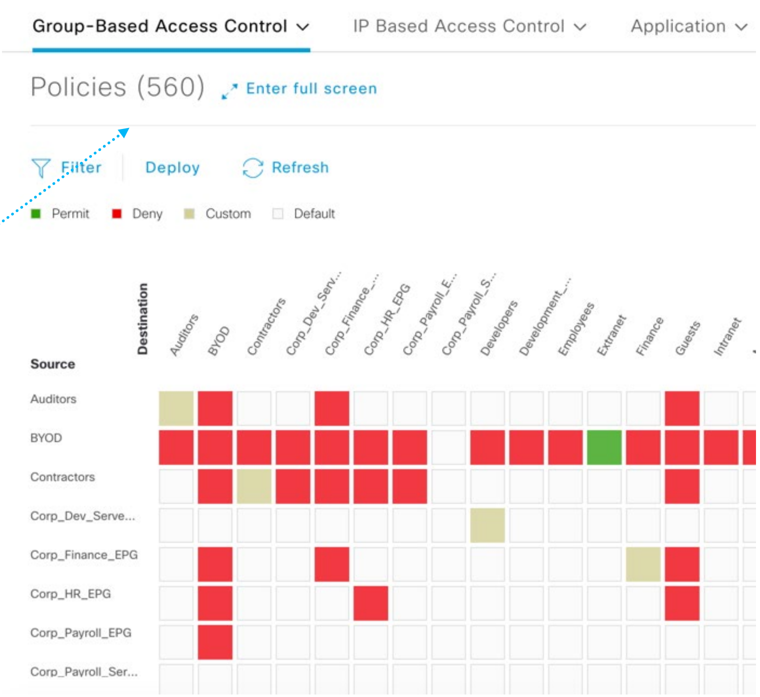
Policy Table Size

SGT, DGT table utilization = number of **populated** cells downloaded to individual fabric nodes

Blank cells (default policy) do not consume table entries

DNAC/ISE shows populated cells for whole environment

Max populated cells on switch/router =SGT,DGT Table



Policies (560)

🟩 Permit 🟥 Deny ▨ Custom □ Default

Destination

Source	Auditors	BYOD	Contractors	Corp_Dev_Serv...	Corp_Finance_...	Corp_HR_EPG	Corp_Payroll_E...	Corp_Payroll_S...	Developers	Development_...	Employees	Extranet	Finance	Guests	Intranet
Auditors	▨	🟥			🟥									🟥	
BYOD	🟥	🟥	🟥	🟥	🟥	🟥	🟥		🟥	🟥	🟥	🟩	🟥	🟥	🟥
Contractors		🟥	▨	🟥	🟥	🟥	🟥							🟥	
Corp_Dev_Serve...									▨						
Corp_Finance_EPG		🟥			🟥								▨	🟥	
Corp_HR_EPG		🟥				🟥								🟥	
Corp_Payroll_EPG		🟥													
Corp_Payroll_Ser...															

Scale	Catalyst 3850	Catalyst 9300	Catalyst 9400	Catalyst 9500	Catalyst 6800	Nexus N7700	ASR1K/ ISR4K
SGT/DGT Table	4K	8K	8K	8K	30K	16K	62K

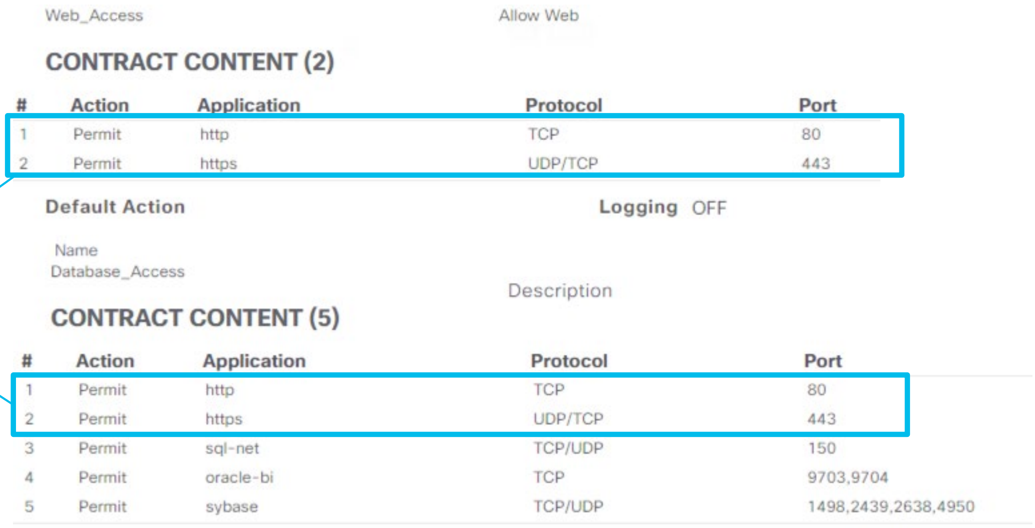
SDA group based policy scale- 25000 Policies

Policy Entries

Key parameter for IOS platforms is number of unique permissions (Access Control Entries)

When permissions reused in multiple contracts with IOS - no additional TCAM used/ACEs counted

Number of unique permissions used = ACE count



Web_Access

Allow Web

CONTRACT CONTENT (2)

#	Action	Application	Protocol	Port
1	Permit	http	TCP	80
2	Permit	https	UDP/TCP	443

Default Action **Logging** OFF

Name

Database_Access

Description

CONTRACT CONTENT (5)

#	Action	Application	Protocol	Port
1	Permit	http	TCP	80
2	Permit	https	UDP/TCP	443
3	Permit	sql-net	TCP/UDP	150
4	Permit	oracle-bi	TCP	9703,9704
5	Permit	sybase	TCP/UDP	1498,2439,2638,4950

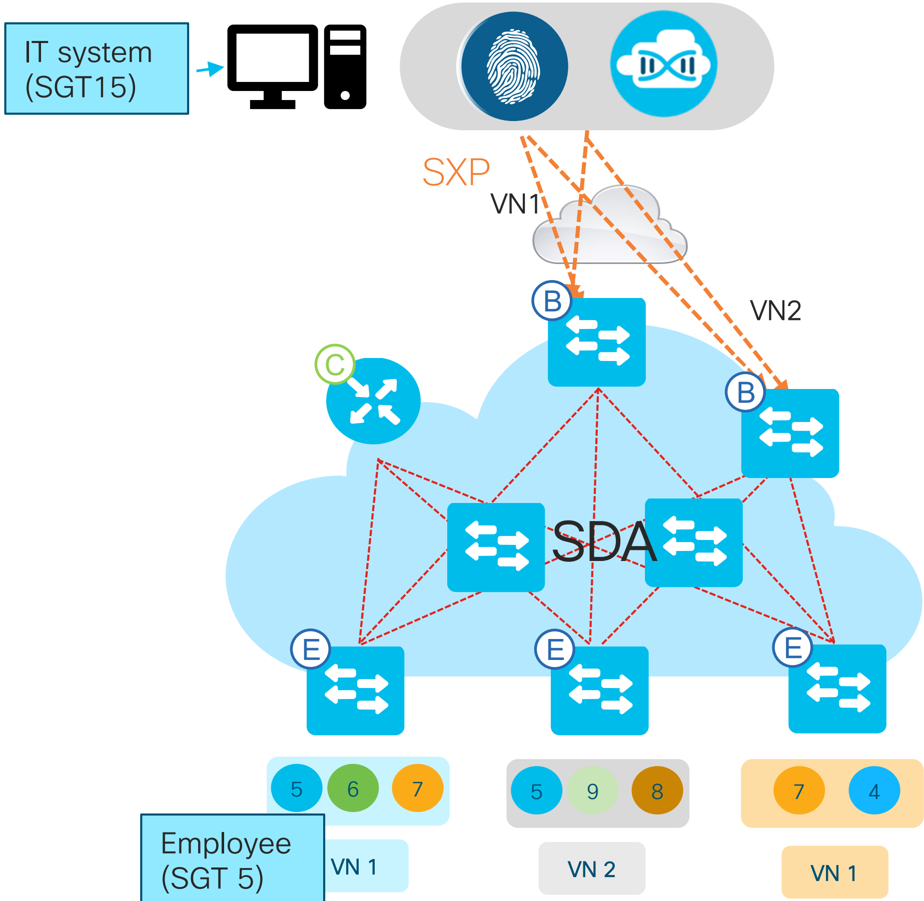
Scale	Catalyst 3850	Catalyst 9300	Catalyst 9400	Catalyst 9500	Catalyst 6800	Nexus N7700*	ASR1K/ ISR4K
SGT/DGT Table	4K	8K	8K	8K	30K	16K	62K

SGACLs (Security ACEs)	1500	5K	18K	18K	30K(XL)
					12K(non XL)
						128K	64K

* N7700 does NOT reuse TCAM entries – permissions in multiple contracts use multiple TCAM entries

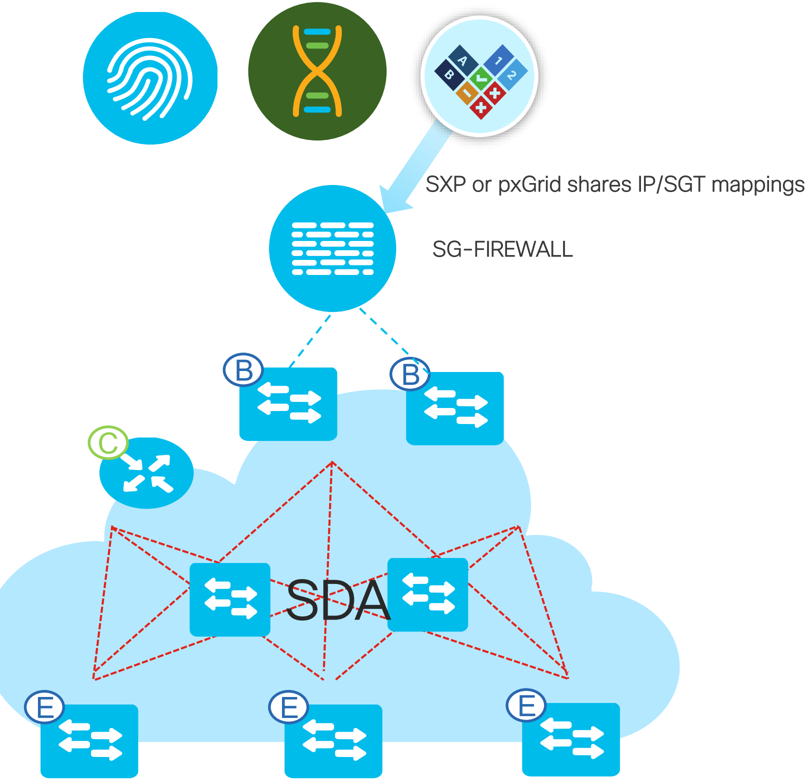
North/South Policy Enforcement (Border Nodes)

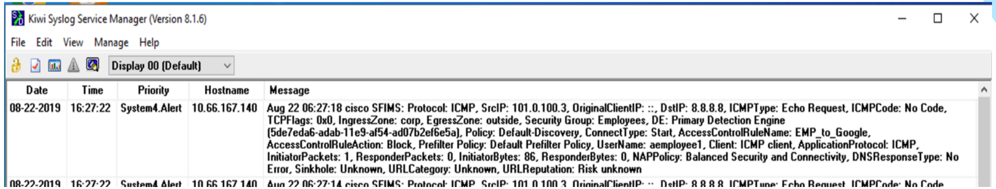
- Enforcement not enabled automatically on Borders currently (config template in DNAC available for this)
- Static Classifications for destinations outside of fabric share with border nodes using SXP protocol or manual configuration on border.
- SXP connection per VN



Firewall as Fusion

- Comprehensive inter-VN policy, stateful inspection, AVC
- Source SGT to Destination SGT policy
- Rich reporting in FTD
- TrustSec policies not downloaded from ISE to firewall




Kiwi Syslog Service Manager (Version 8.1.6)
File Edit View Manage Help
Display 00 (Default)

```
Date        Time      Priority       Hostname        Message
08-22-2019  16:27:22  System4.Alert  10.66.167.140   Aug 22 06:27:18 cisco SFIMS: Protocol: ICMP, SrcIP: 101.0.100.3, OriginalClientIP: ::, DstIP: 8.8.8.8, ICMPType: Echo Request, ICMPCode: No Code,
                                                     TCPFlags: 0x0, IngressZone: corp, EgressZone: outside, Security Group: Employees, DE: Primary Detection Engine
                                                     (5de7eda6-adab-11e9-af54-ad07b2ef6e5a), Policy: Default-Discovery, ConnectType: Start, AccessControlRuleName: EMP_to_Google,
                                                     AccessControlRuleAction: Block, Prefilter Policy: Default Prefilter Policy, UserName: aemployee1, Client: ICMP client, ApplicationProtocol: ICMP,
                                                     InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 86, ResponderBytes: 0, NAPPolicy: Balanced Security and Connectivity, DNSResponseType: No
                                                     Error, Sinkhole: Unknown, URLCategory: Unknown, URLReputation: Risk unknown
08-22-2019  16:27:22  System4.Alert  10.66.167.140   Aug 22 06:27:14 cisco SFIMS: Protocol: ICMP, SrcIP: 101.0.100.3, OriginalClientIP: ::, DstIP: 8.8.8.8, ICMPType: Echo Request, ICMPCode: No Code
```

Border Scale Parameters

For your reference

Scale	Catalyst 3850 (XS)	Catalyst 9300	Catalyst 9300L	Catalyst 9400	Catalyst 9500	Catalyst 9500 H	Catalyst 9600	Catalyst 6800	Nexus N7700	ASR1k/ ISR4k	CSR1KV
Virtual Networks	64	256	256	256	256	256	1k	500	500	4k	n.a
Group Tag Table (SGT/DGT)	4k	8k	8k	8K	8K	16K	32K	30K	16K	62K	n.a
SGACLs (Security ACEs)	1500	5K	5K	18K	18K	13K IPv4	27K	30K(XL) 12K (LE)	1k	64K	n.a
IPv4 Fabric Routes (LPM IP/mask)	8K	8K	8K	SUP1XL= 20K	48K	48K	200K	1M (XL) 256K (LE)	500k	4M (16GB) 1M (8GB)	200K

IPv4 Host Entries (Host /32)	16K	16K	16K	SUP1XL= 80K	80K	150k	150k	1M (XL)
								512K (L)
									32k	1M(8 GB)
										4M(16 GB)
											100k

Edge Scale Parameters

For your reference

Fabric Constructs	Catalyst 3650	Catalyst 3850	Catalyst 9200L	Catalyst 9200	Catalyst 9300	Catalyst 9300L	Catalyst 4K (Sup8E)	Catalyst 9400	Catalyst 9500
Virtual Networks	64	64	1*	4*	256	256	64	256	256
Local End Points/Hosts	2K	4K	2k	4k	4K	4K	4K	4K	4K
SGT/DGT Table	4K	4K	2k	2k	8K	8K	2K	8K	8K
SGACLs (Security ACEs)	1350	1350	1k	1k	5K	5K	1350	18K	18K

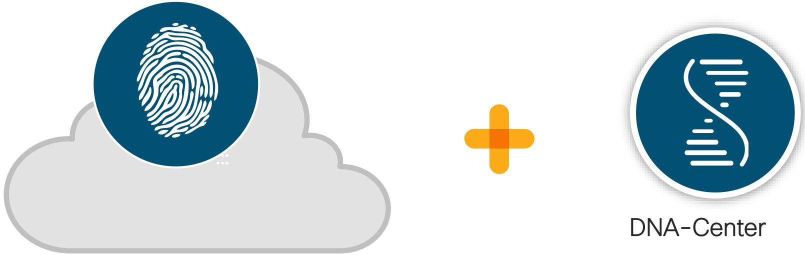
*9200L = 1 Default_VN + 1 Infra_VN (global routing table). No extra User VN possible
9200 = 3 User Configured VNs + 1 DEFAULT_VN + 1 INFRA_VN

Migration Best Practices

Migration Approaches: Parallel vs Incremental

Parallel *IMPLEMENTATION* *RESOURCES*	Incremental *RESOURCES* IMPLEMENTATION
Best for Branch (small) deployments	Best for Campus (any size)
Requires enough cable runs to create a new parallel network	Requires a couple of cables from new access and distribution switches
Power and outlets for a parallel network	Incremental power and outlet requirement
Legacy hardware in existing network	Legacy hardware in existing network
Upgrade most of the wired network	Upgrade some of the wired network
Clean slate (leave behind any complexity in the old design)	Must carry forward the constraints of the old design in the underlay
Test users in a complete new network	Test of functionality is partial
Easy Rollback of migrated users	Easy Rollback of migrated users

Integrating DNAC with existing ISE



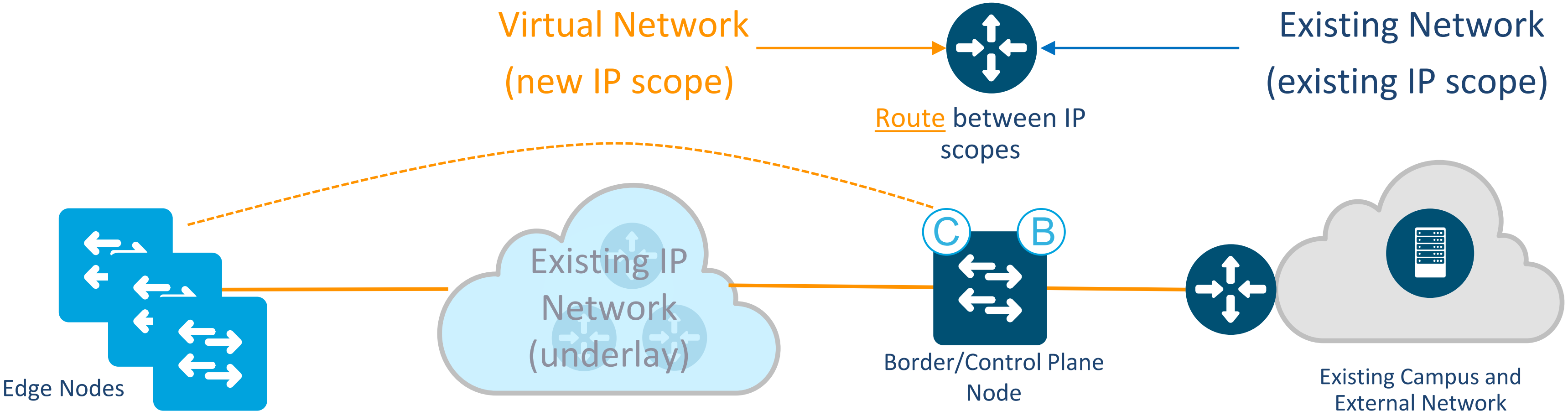
Existing Campus and External Network

DNA-Center

- Benefit from the already integrated systems
- Supplicant configuration need not be changed
- Policies and rules can be can be reused

- Check the compatibility matrix
- Integrate DNAC with Existing ISE preferably with no existing trustsec configuration
- Make sure to take the backup of existing ISE cluster
- Group based access control with 1.3.1

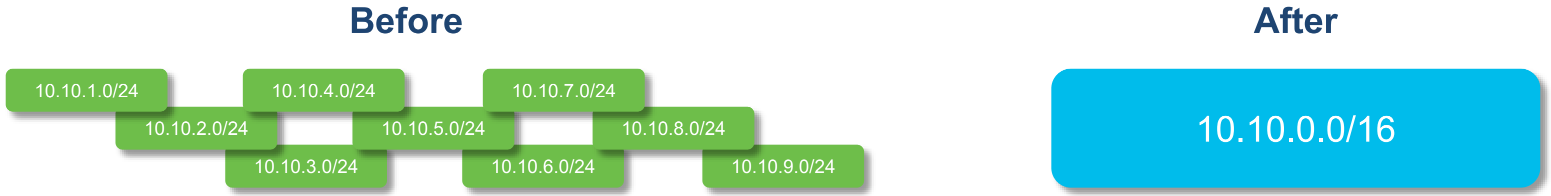
Incremental Migration – High Level concept



- **Deploy a Border/Control Plane node and an Edge node**
- A virtual network with new address is formed over the existing network
- **Incrementally** add Fabric Edge nodes
- The virtual network connects to the existing/external network via the border

Using New Subnets for Migration

- Immediately realize the advantages of bigger subnets, but lesser subnets that are optimized for SD-Access
- Design for the present and the future
- Add DHCP scope and size
- Update existing firewall rules for that one big subnet
- Not a big issue for endpoints with IP stacks that work well with DHCP



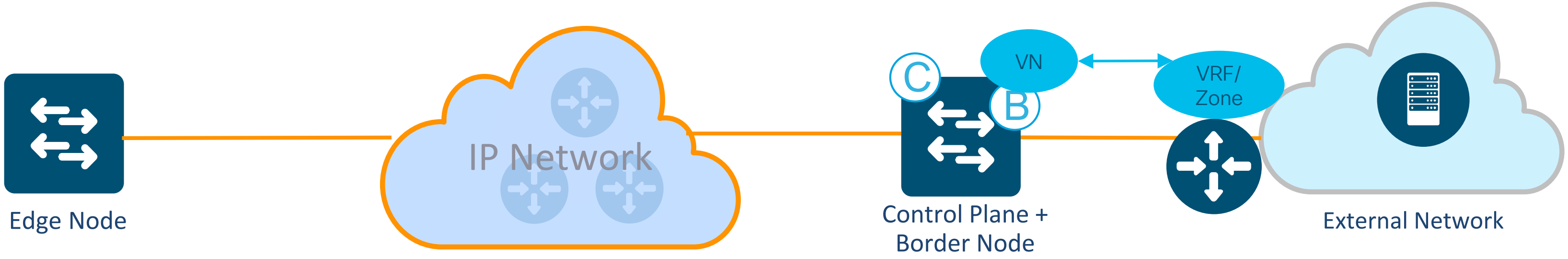
Before

10.10.1.0/24
10.10.2.0/24
10.10.3.0/24
10.10.4.0/24
10.10.5.0/24
10.10.6.0/24
10.10.7.0/24
10.10.8.0/24
10.10.9.0/24

After

10.10.0.0/16

Prerequisites



Set following on the Fabric nodes and other nodes in the underlay

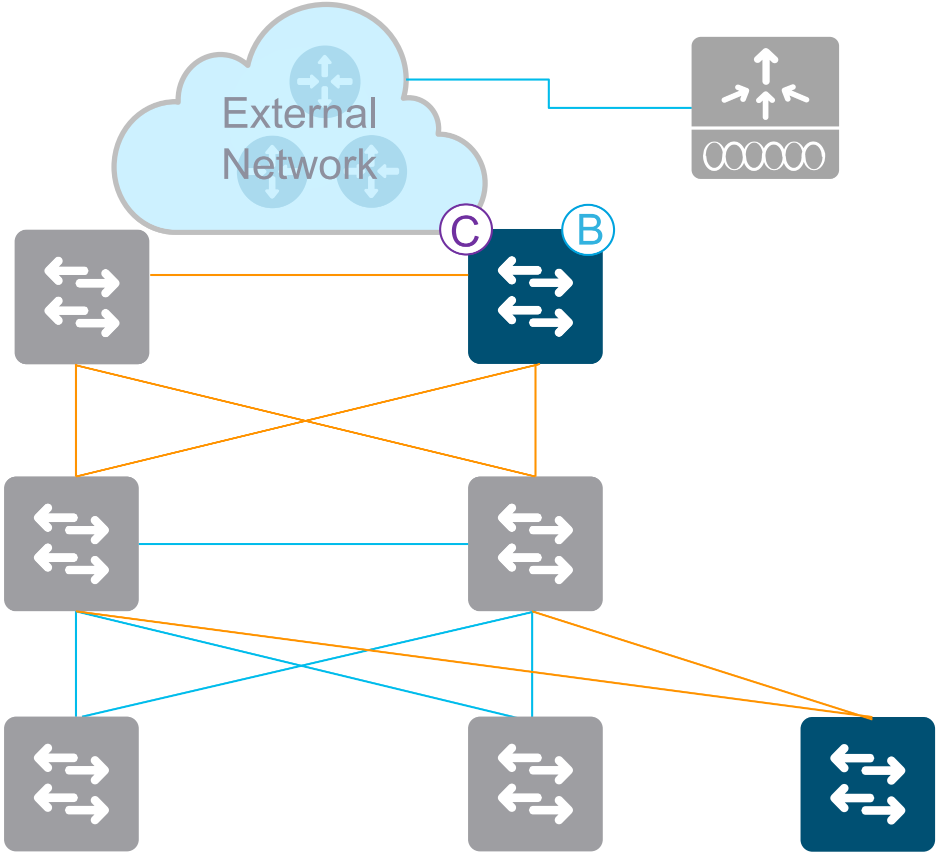
- Set MTU to 9100 on the switch and the existing network.
- Configure ‘ip routing’
- Set ‘username’ and ’password’ for device access
- Configure VTY and console lines for device access
- Configure NTP
- Configure SNMP, syslog
- Configure Loopback0 (/32) for RLOC, and underlay IP addresses

Understand the VN requirements

- Understand the different domains needed.
- Understand the security mapping needed
- Difficult to modify later

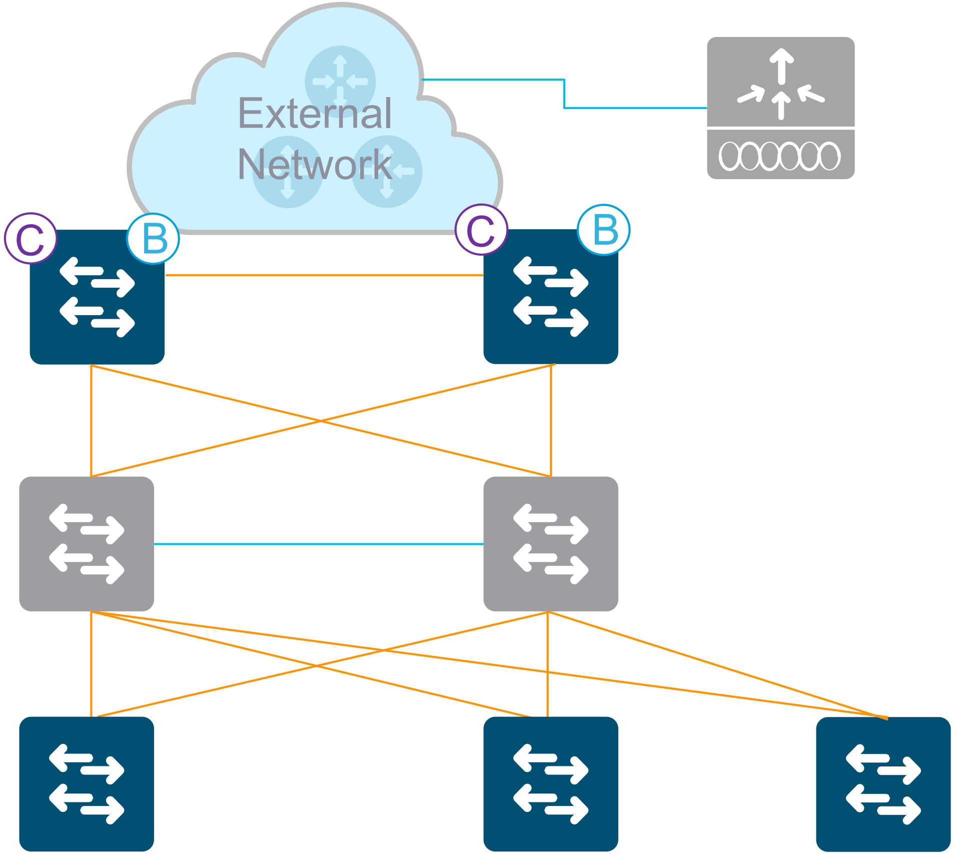
Current State of the Network

- Now configure the rest of the access switches links from L2 to L3 routed access
- Configure them as fabric edge switches
- Also configure the secondary core as the fabric border/control plane for redundancy



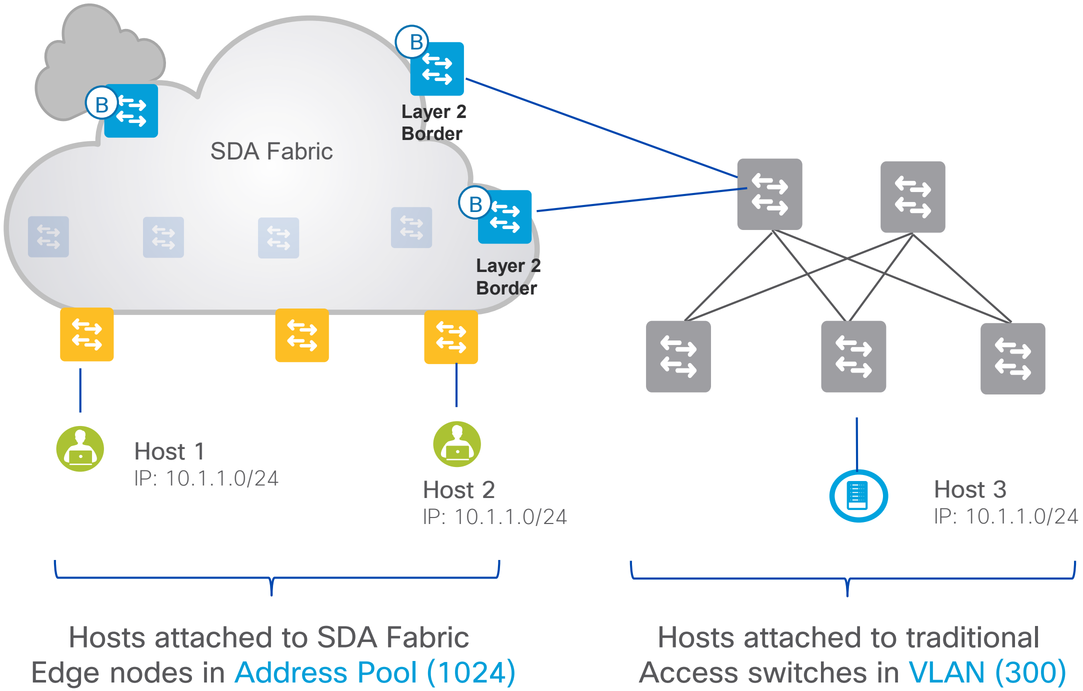
After the Migration

- Add border redundancy
- Configure BFD
- Per-VRF BGP configuration
- Configure eBGP for N-S traffic
- Recommended to have iBGP for E-W traffic
- Test the fabric for critical production traffic
- Test failover scenarios
- Test multiple paths
- Enable L2 flooding on need basis
- All link MTU should support VxLAN header



Routed Access Design Considerations

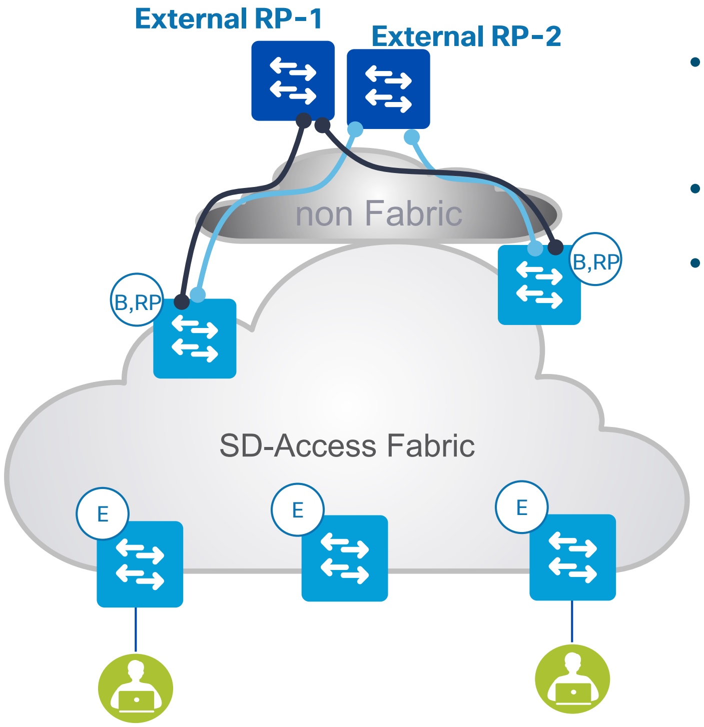
- Shutdown existing SVI
- Provision existing subnet from DNA-Center (10.1.1.0/24 in this case)
- Verify connectivity
- Use dedicated L2 border to avoid issues from legacy network
- VLAN ID cannot overlap



Hosts attached to SDA Fabric Edge nodes in Address Pool (1024)

Hosts attached to traditional Access switches in VLAN (300)

Multicast with RP outside the fabric – 1.3.3



- New multicast workflow support RP internal or external to the fabric
- Configuration as part of the ASM workflow
- Maximum 2 RPs supported.

What is the Best WLC/AP Migration model for You

Greenfield or Brownfield

Building From Scratch

Introduce New Compactable HW & build a new infrastructure.

(Suitable for new Sites/Buildings)

Parallel Build

Build a Infrastructure Parallel to the Traditional Infrastructure.

(Suitable for a migration from different vendors)

Migrate Existing Setup

Migrate the Existing HW to compactable HW models.

(Suitable for sites with devices running out of support)

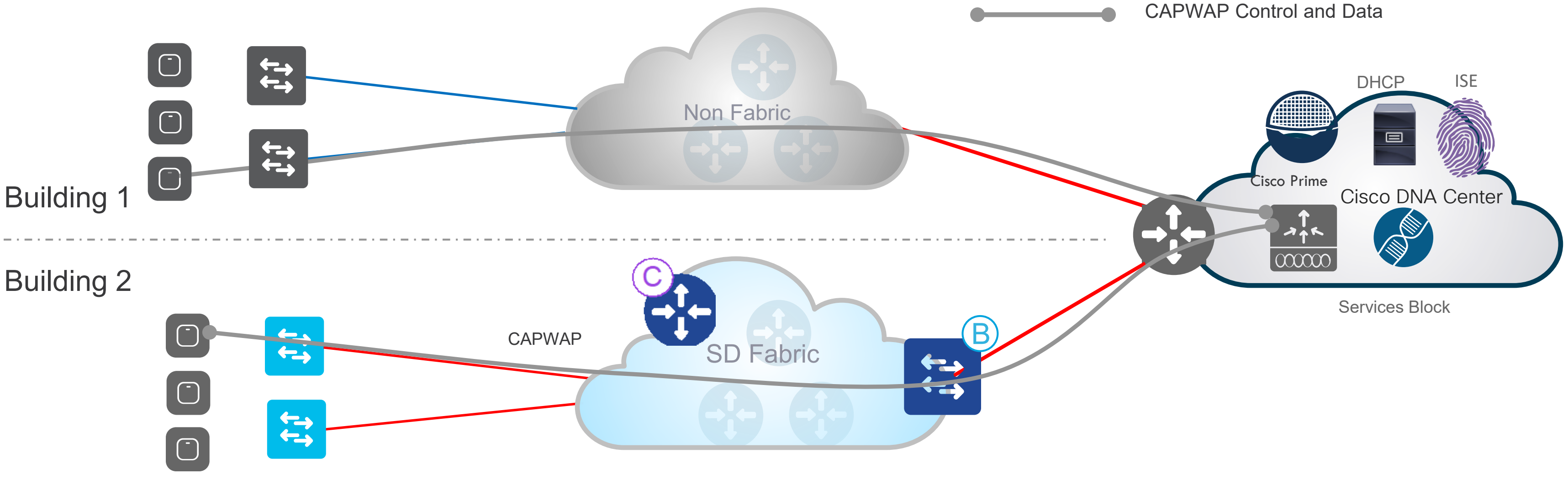
Split Existing Setup

Split the HA and use one WLC for building new Infrastructure.

(Best approach for those who have compactable HW available in existing Infrastructure)

SD-Access Wireless Migration

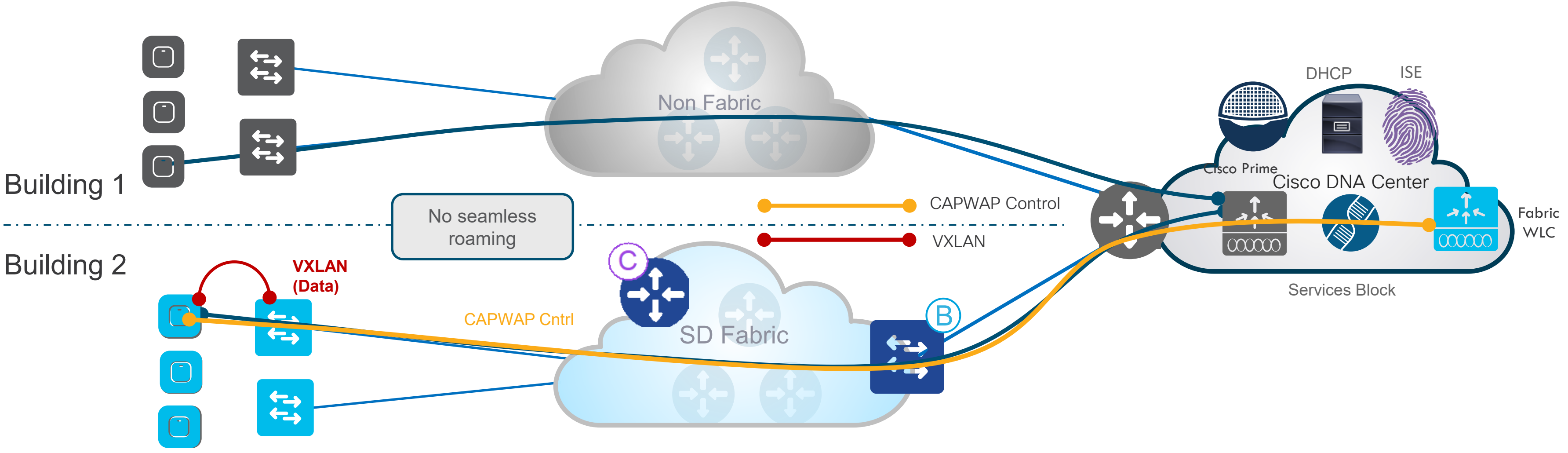
Migration for an existing CUWN deployment



1. Add Cisco DNA Center and ISE (if not present already)
2. First, Migrate wired network to SD-Access Fabric
3. Wireless is over the top of Fabric

SD-Access Wireless Migration

Migration for an Existing CUWN Deployment



4 ▪ Discover existing WLC to Cisco DNA Center – Learn configuration (e.g. SSIDs) and populate Cisco DNA Center

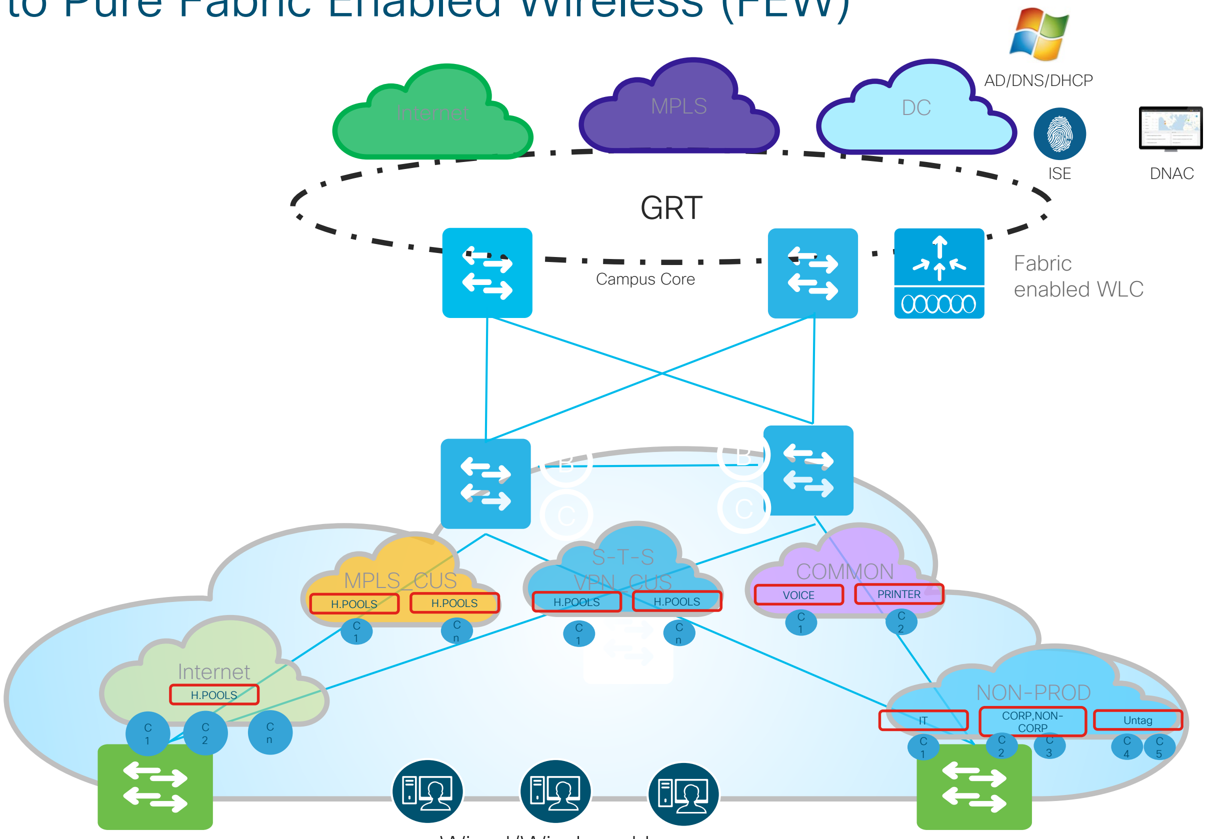
5 ▪ Assign a separate WLC for SD-Access and provision it to the site (re-use the configuration inherited from old WLC)

6 ▪ on CUWN WLC, configure the APs in the area to join the new Fabric WLC

7 ▪ APs in the area will join Fabric WLC. From Cisco DNA Center provision APs to the Fabric site

Migration Scenario 1

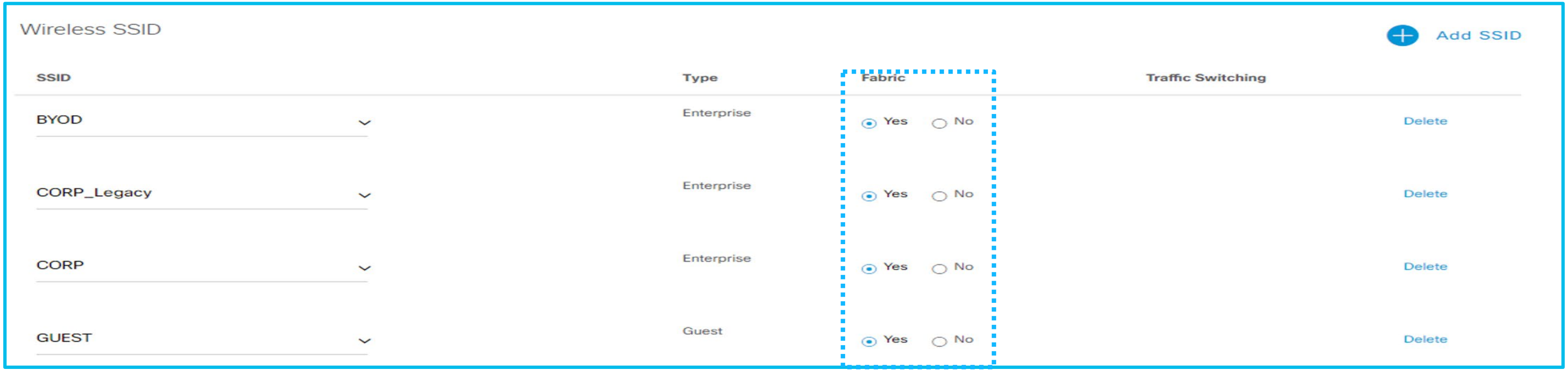
Traditional to Pure Fabric Enabled Wireless (FEW)



Wired/Wireless Users

Scenario One (All SSIDs are FEW)

For your reference



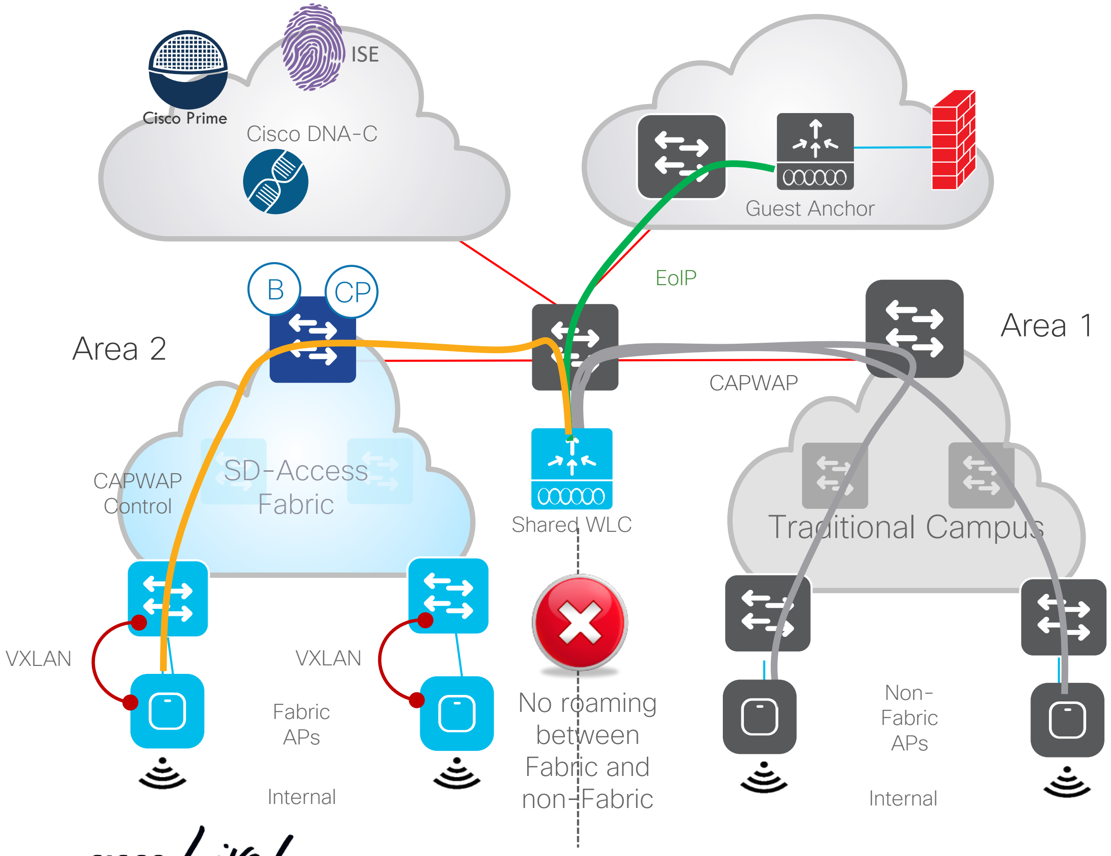
Wireless SSID

Add SSID

SSID	Type	Fabric	Traffic Switching	
BYOD	Enterprise	● Yes ○ No		Delete
CORP_Legacy	Enterprise	● Yes ○ No		Delete
CORP	Enterprise	● Yes ○ No		Delete
GUEST	Guest	● Yes ○ No		Delete

Migration Scenario 2

Shared WLC for FEW & Non-FEW



Shared controller for SDA and CUWN

- Shared WLC can manage Fabric and non-Fabric APs but **needs upgrade to 8.5**
- New code = more risk for existing non-Fabric buildings

Management:

- **DNAC 1.2 can manage non-Fabric WLC** in brownfield scenarios
- But not all wireless settings are available

WLAN Design:

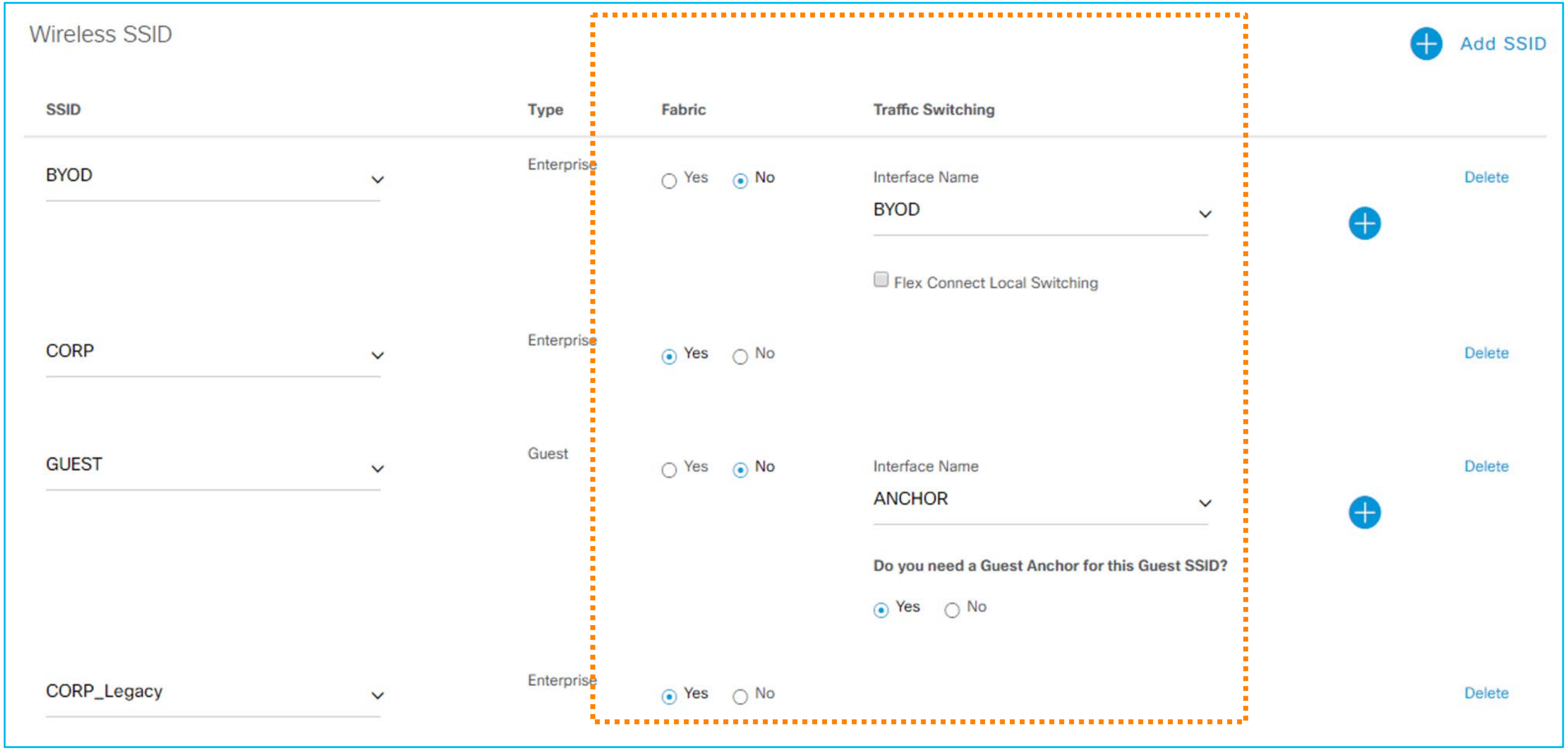
- Fabric is enabled per SSID
- To have same SSID name in both areas:
  1. Need to define and apply AP Groups
  2. APs need to be re-booted

Guest and Policy:

- Can leverage existing Guest Anchor also for Fabric area/building
- Can leverage ISE for both

Scenario Two (FEW & Non-FEW)

For your reference



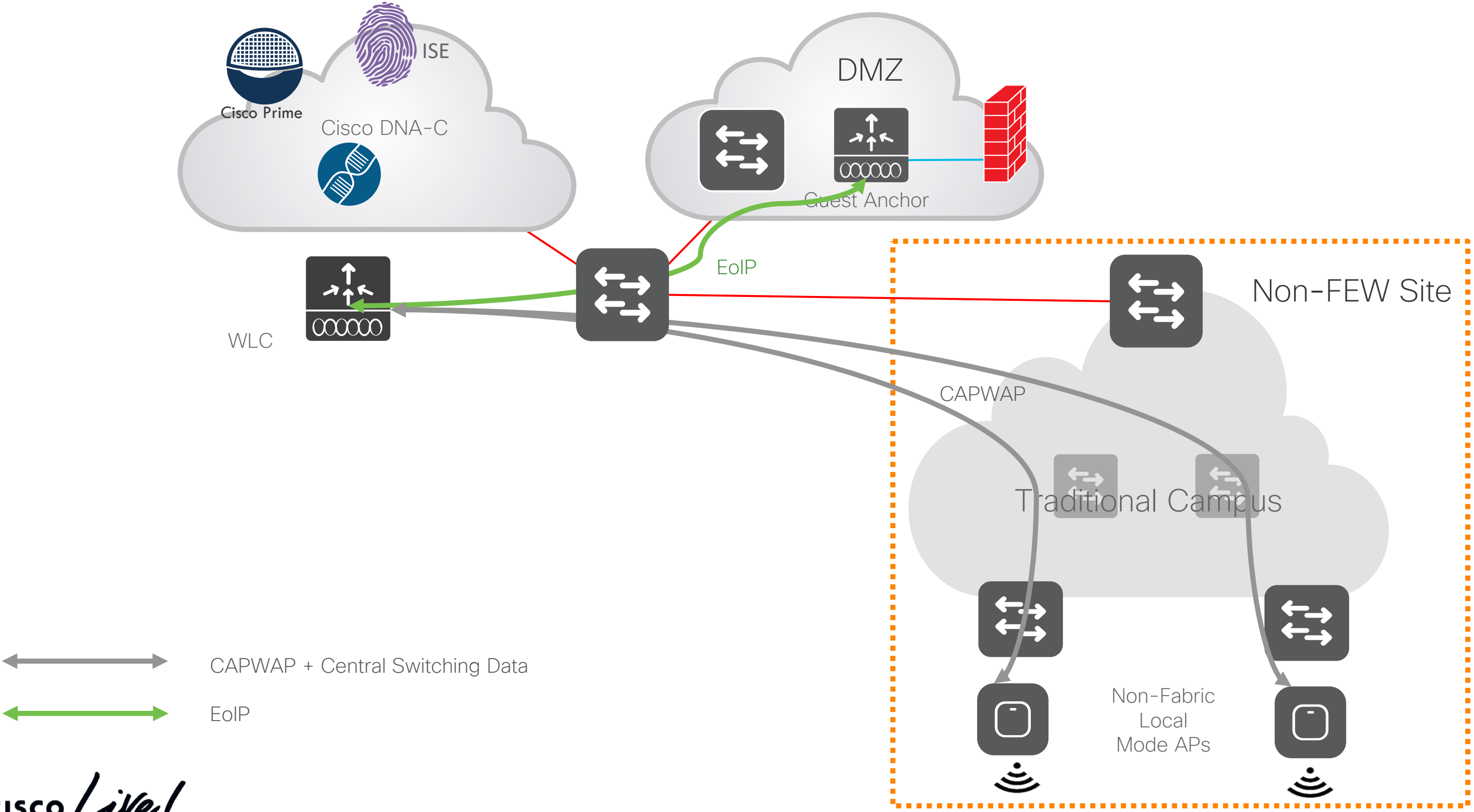
Wireless SSID

⊕ Add SSID

SSID	Type	Fabric	Traffic Switching		
BYOD	Enterprise	○ Yes ● No	Interface Name: BYOD □ Flex Connect Local Switching	⊕	Delete
CORP	Enterprise	● Yes ○ No			Delete
GUEST	Guest	○ Yes ● No	Interface Name: ANCHOR **Do you need a Guest Anchor for this Guest SSID?** ● Yes ○ No	⊕	Delete
CORP_Legacy	Enterprise	● Yes ○ No			Delete

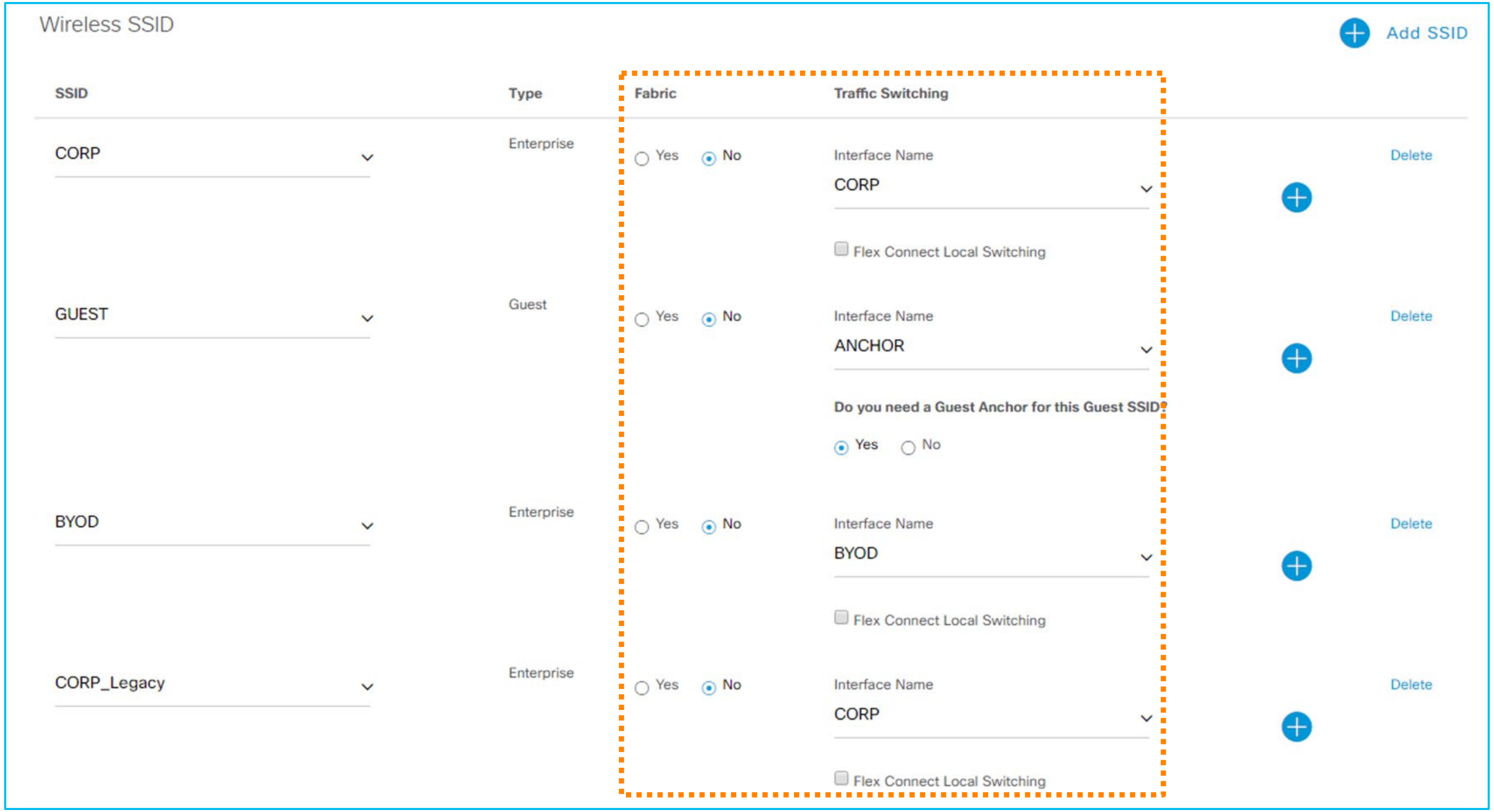
Migration Scenario Three

Onboarding Traditional Site using Cisco DNA-C



Scenario Three: Non-FEW & Local Mode AP

For your reference



SSID	Type	Fabric	Traffic Switching
CORP	Enterprise	○ Yes ● No	Interface Name CORP □ Flex Connect Local Switching
GUEST	Guest	○ Yes ● No	Interface Name ANCHOR Do you need a Guest Anchor for this Guest SSID? ● Yes ○ No
BYOD	Enterprise	○ Yes ● No	Interface Name BYOD □ Flex Connect Local Switching
CORP_Legacy	Enterprise	○ Yes ● No	Interface Name CORP □ Flex Connect Local Switching

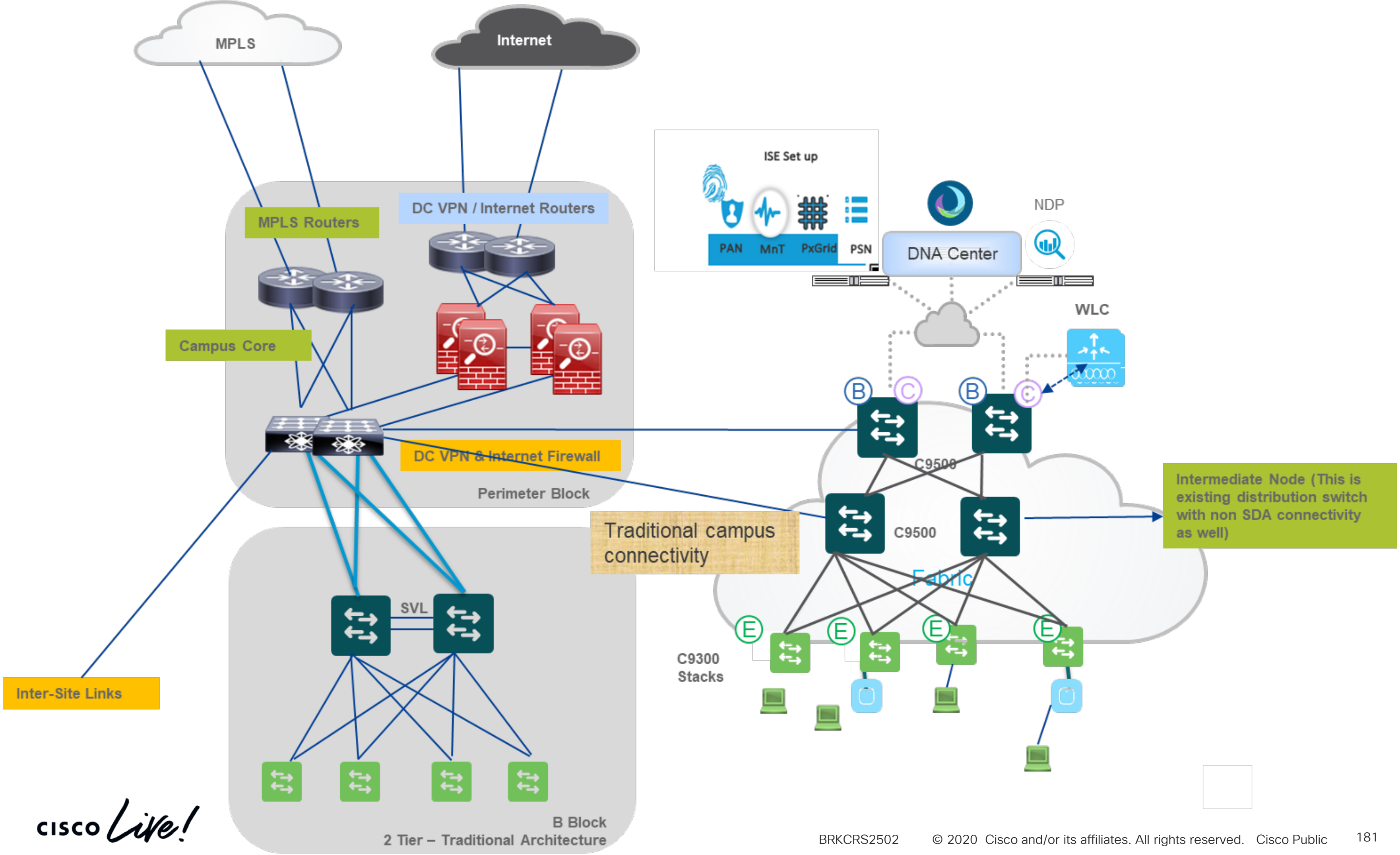
Migration Example

Requirement :

Customer would want to utilize existing network infrastructure while moving specific ODCs to SDA. User count is 5000 users. Fabric enabled wireless for the ODC in SDA.

Plan :

1. Use a pair of Border+Control plane node (Catalyst 9500)
2. 3 tier architecture
3. DNAC appliance - DN2-HW-APL
4. ISE – 4 node hybrid deployment (3655)
5. Manual underlay
6. Add 2 WLC to SDA (platform)
7. Campus core switches to be used for Fusion


MPLS
Internet
MPLS Routers
DC VPN / Internet Routers
Campus Core
DC VPN & Internet Firewall
Perimeter Block
Inter-Site Links
SVL
B Block
2 Tier – Traditional Architecture
Traditional campus connectivity
ISE Set up
PAN
MnT
PxGrid
PSN
DNA Center
NDP
WLC
B
C
B
C
C9500
C9500
Fabric
E
E
E
E
C9300 Stacks
Intermediate Node (This is existing distribution switch with non SDA connectivity as well)

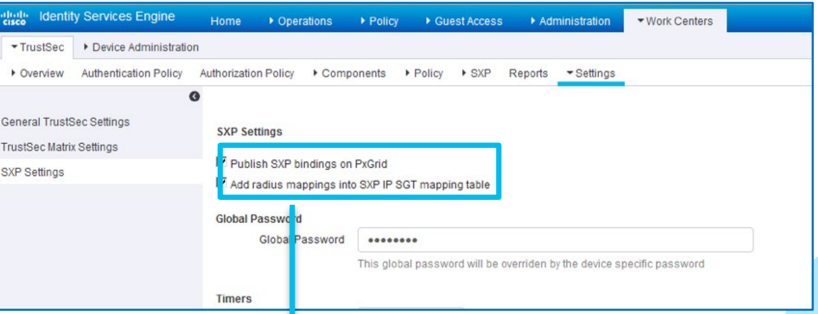
Security Best Practices

Firewall Integration for Inter-VN Policy

Requirement for Inter-VN policy enforcement

SXP or pxGrid always needed to enable group-based FW rules

SGT/VXLAN to SGT/Eth is optional



SXP Settings

☑ Publish SXP bindings on PxGrid

☑ Add radius mappings into SXP IP SGT mapping table

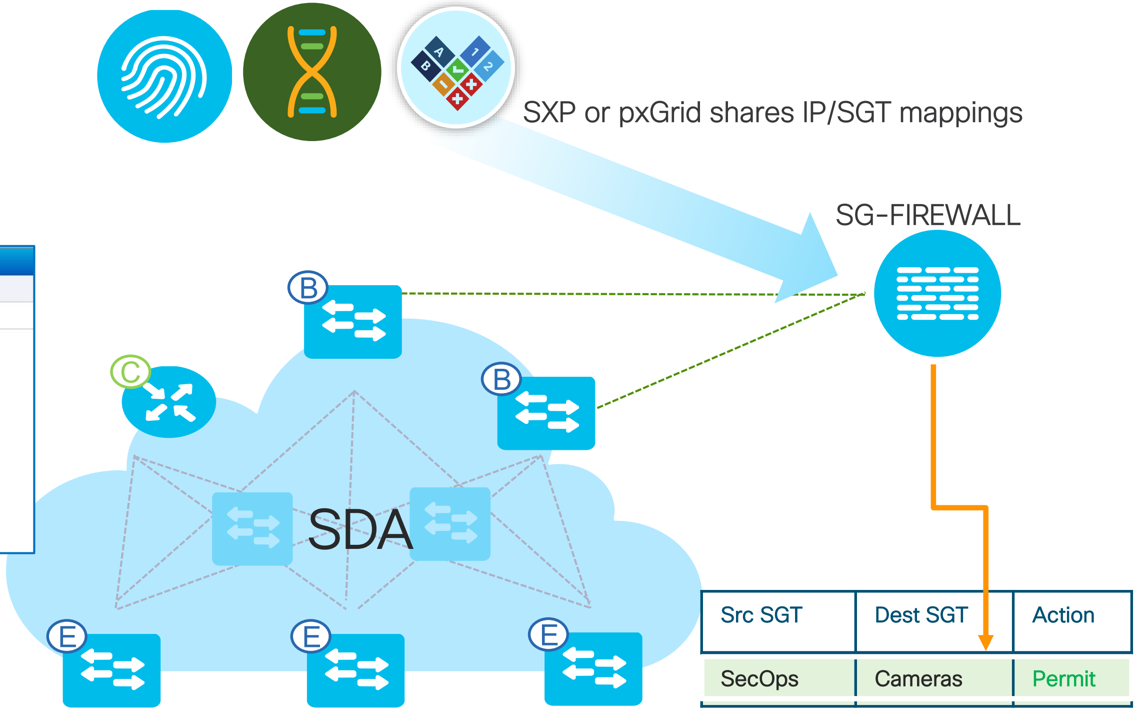
Global Password

Global Password ••••••••

This global password will be overriden by the device specific password

Timers

Mappings can be shared with SXP Peers



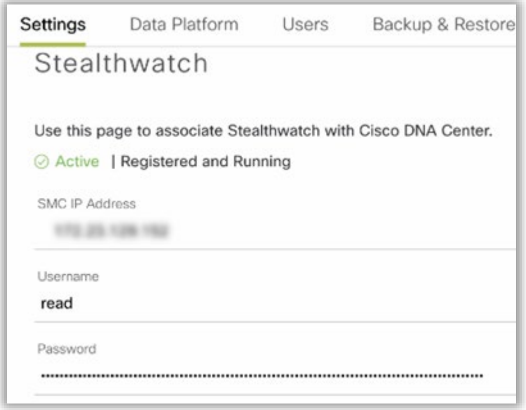
Src SGT	Dest SGT	Action
SecOps	Cameras	Permit

Note: FTD 6.5 on needed to use SGT as Dest Criteria

Cisco DNA Center Automates ETA/Netflow

Using the Stealthwatch Security Analytics App

Integrate Stealthwatch SMC with Cisco DNA Center



Stealthwatch

Use this page to associate Stealthwatch with Cisco DNA Center.

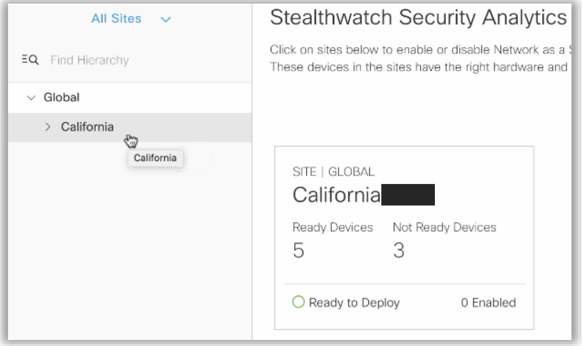
Active | Registered and Running

SMC IP Address: [redacted]

Username: read

Password: ••

Select the Site to enable ETA



Stealthwatch Security Analytics

Click on sites below to enable or disable Network as a
These devices in the sites have the right hardware and

SITE | GLOBAL

California [redacted]

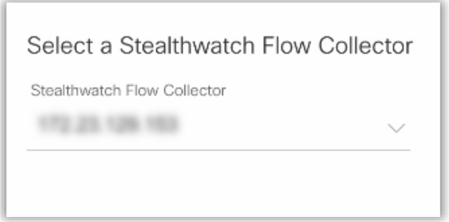
Ready Devices: 5

Not Ready Devices: 3

Ready to Deploy

0 Enabled

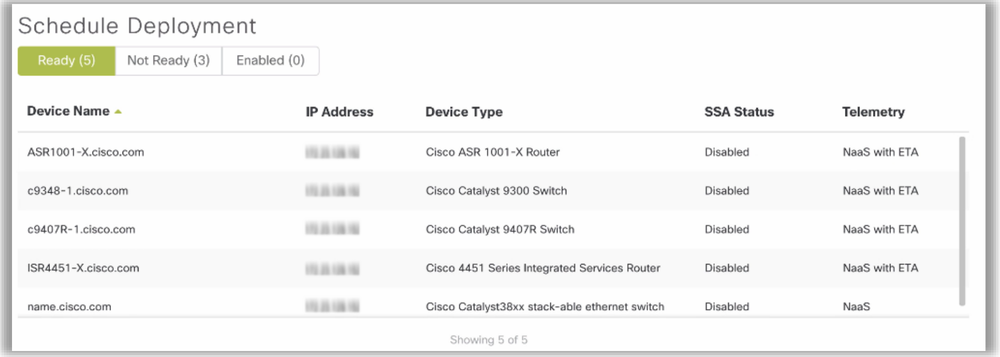
Select Flow Collector from drop-down list



Select a Stealthwatch Flow Collector

Stealthwatch Flow Collector: [redacted]

Deploy ETA or NetFlow to all capable devices within the Site

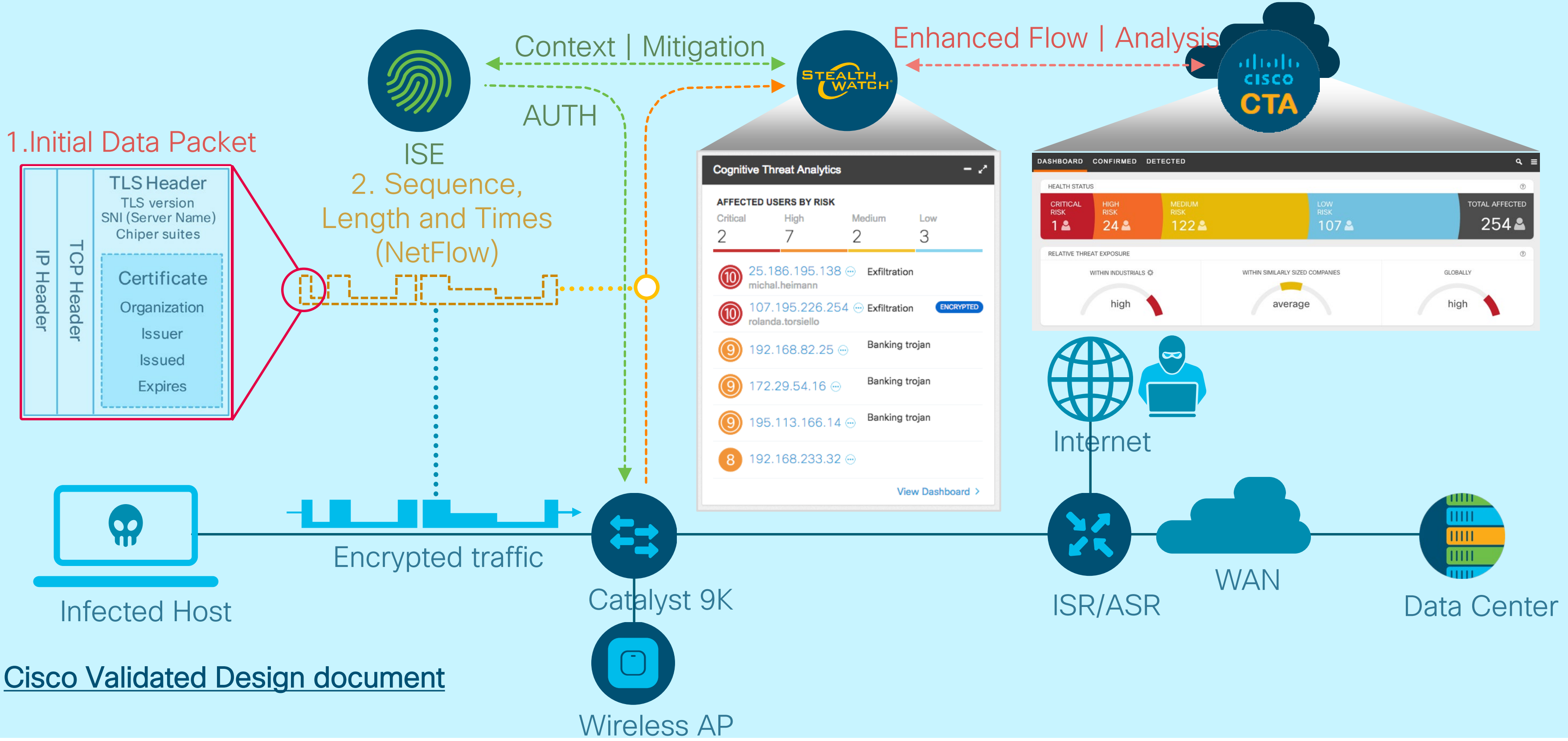


Schedule Deployment

Device Name	IP Address	Device Type	SSA Status	Telemetry
ASR1001-X.cisco.com	[redacted]	Cisco ASR 1001-X Router	Disabled	NaaS with ETA
c9348-1.cisco.com	[redacted]	Cisco Catalyst 9300 Switch	Disabled	NaaS with ETA
c9407R-1.cisco.com	[redacted]	Cisco Catalyst 9407R Switch	Disabled	NaaS with ETA
ISR4451-X.cisco.com	[redacted]	Cisco 4451 Series Integrated Services Router	Disabled	NaaS with ETA
name.cisco.com	[redacted]	Cisco Catalyst38xx stack-able ethernet switch	Disabled	NaaS

Showing 5 of 5

The “system” for ETA



Cognitive Threat Analytics

AFFECTED USERS BY RISK

Critical	High	Medium	Low
2	7	2	3

10	25.186.195.138 michal.heimann	Exfiltration	
10	107.195.226.254 rolanda.torsiello	Exfiltration	ENCRYPTED
9	192.168.82.25	Banking trojan	
9	172.29.54.16	Banking trojan	
9	195.113.166.14	Banking trojan	
8	192.168.233.32		

View Dashboard >

DASHBOARD CONFIRMED DETECTED

HEALTH STATUS

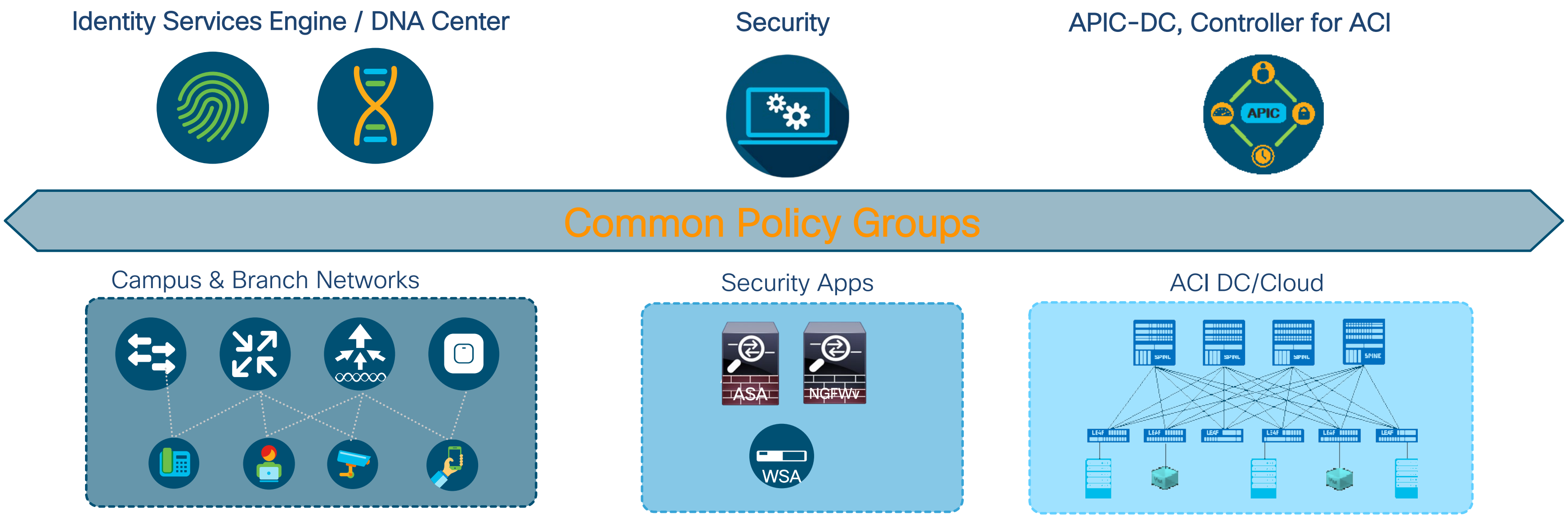
CRITICAL RISK	HIGH RISK	MEDIUM RISK	LOW RISK	TOTAL AFFECTED
1	24	122	107	254

RELATIVE THREAT EXPOSURE

WITHIN INDUSTRIALS	WITHIN SIMILARLY SIZED COMPANIES	GLOBALLY
high	average	high

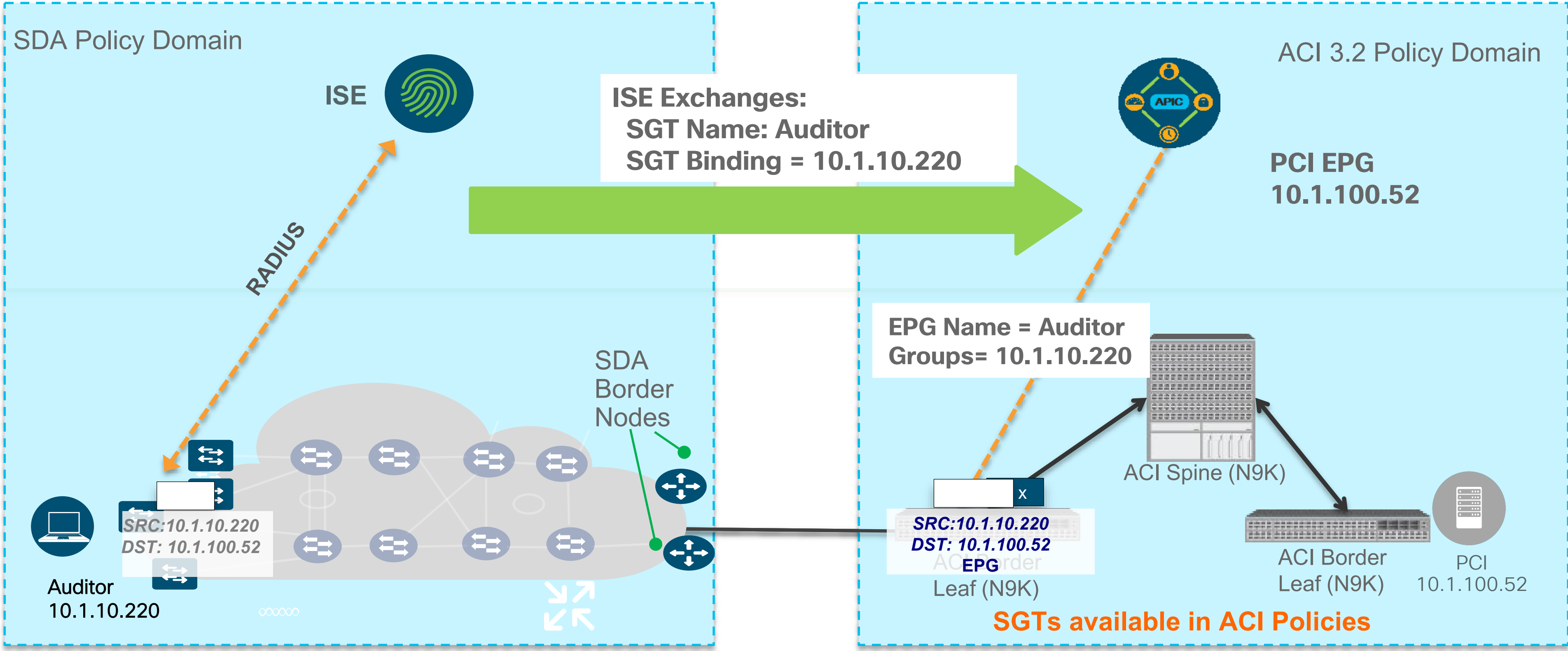
Cisco Validated Design document

Consistent Policies Across the Enterprise



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

Groups from SDA Used in ACI



SDA Policy Domain

ISE

RADIUS

ISE Exchanges:
SGT Name: Auditor
SGT Binding = 10.1.10.220

ACI 3.2 Policy Domain

APIC

PCI EPG
10.1.100.52

EPG Name = Auditor
Groups= 10.1.10.220

SDA Border Nodes

ACI Spine (N9K)

SRC:10.1.10.220
DST: 10.1.100.52

Auditor
10.1.10.220

SRC:10.1.10.220
DST: 10.1.100.52
EPG

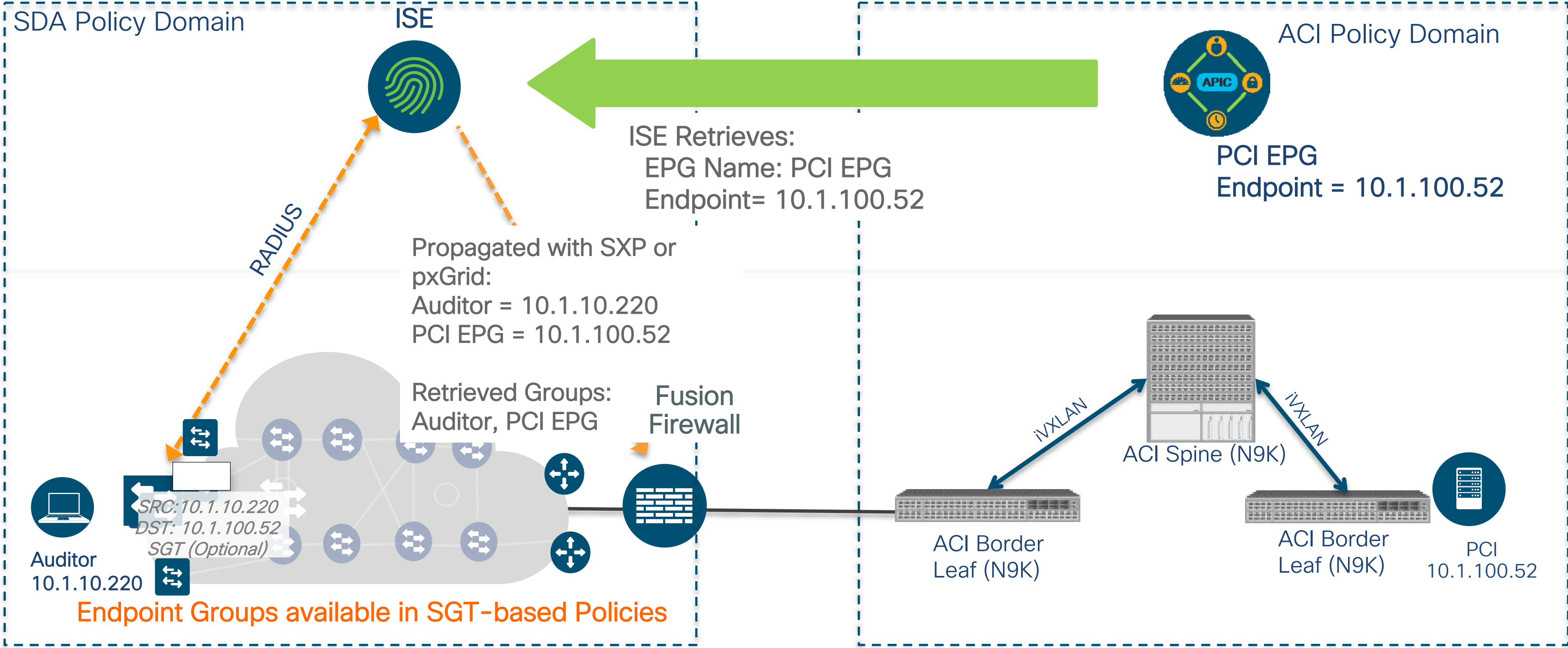
ACI Border Leaf (N9K)

ACI Border Leaf (N9K)

PCI
10.1.100.52

SGTs available in ACI Policies

ACI Groups Used in SDA (Border or Fusion)



ISE Retrieves:
EPG Name: PCI EPG
Endpoint= 10.1.100.52

PCI EPG
Endpoint = 10.1.100.52

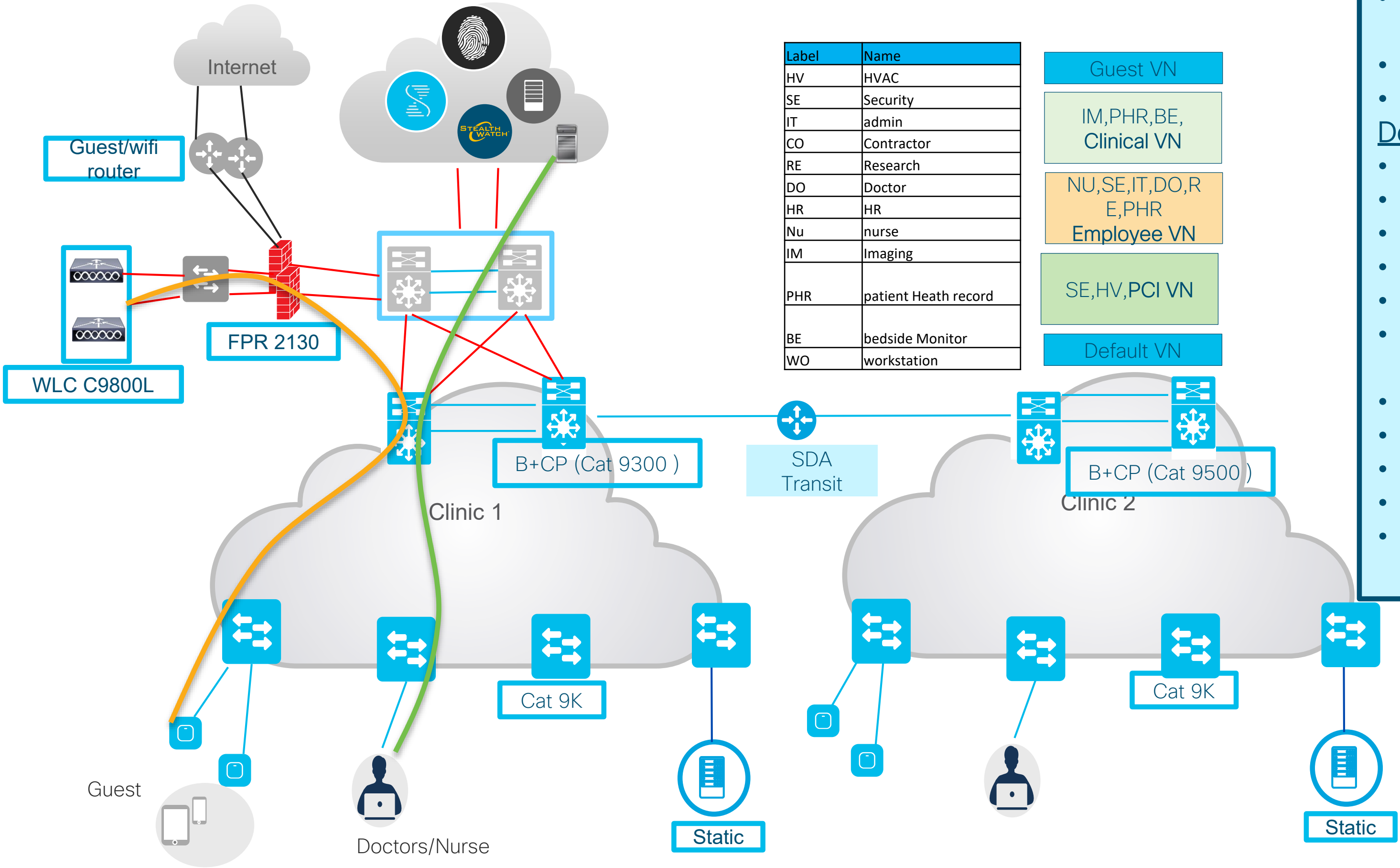
Propagated with SXP or pxGrid:
Auditor = 10.1.10.220
PCI EPG = 10.1.100.52

Retrieved Groups:
Auditor, PCI EPG

Endpoint Groups available in SGT-based Policies

How Did Our Customers Deploy

Healthcare



Label	Name
HV	HVAC
SE	Security
IT	admin
CO	Contractor
RE	Research
DO	Doctor
HR	HR
Nu	nurse
IM	Imaging
PHR	patient Heath record
BE	bedside Monitor
WO	workstation

Guest VN

IM,PHR,BE, Clinical VN

NU,SE,IT,DO,RE,PHR Employee VN

SE,HV,PCI VN

Default VN

Requirement:

- Port Security,
- 2 new facilities. 10K ep in site 1 and 1K in site2
- Static endpoints
- Guest Anchor solution

Design:

- DNAC-L appliance
- Border – 9300 (2 for redundancy)
- Edge – 9300 Stack
- IP Pools – 20
- Fusion – ASR
- Border type – internal+external,eBGP
- Underlay – LAN Automation
- Wireless – OTT
- Transit- SDA
- Policy – Mix of VN and SGT
- Security - Stealthwatch

Manufacturing

Label	Name
HV	HVAC
SE	Security
PL	Plant Operation
EM	Employee
SU	Supplier
AP	Industrial Application
OP	Operators
BA	Base Control
PR	Process
PT	Printer

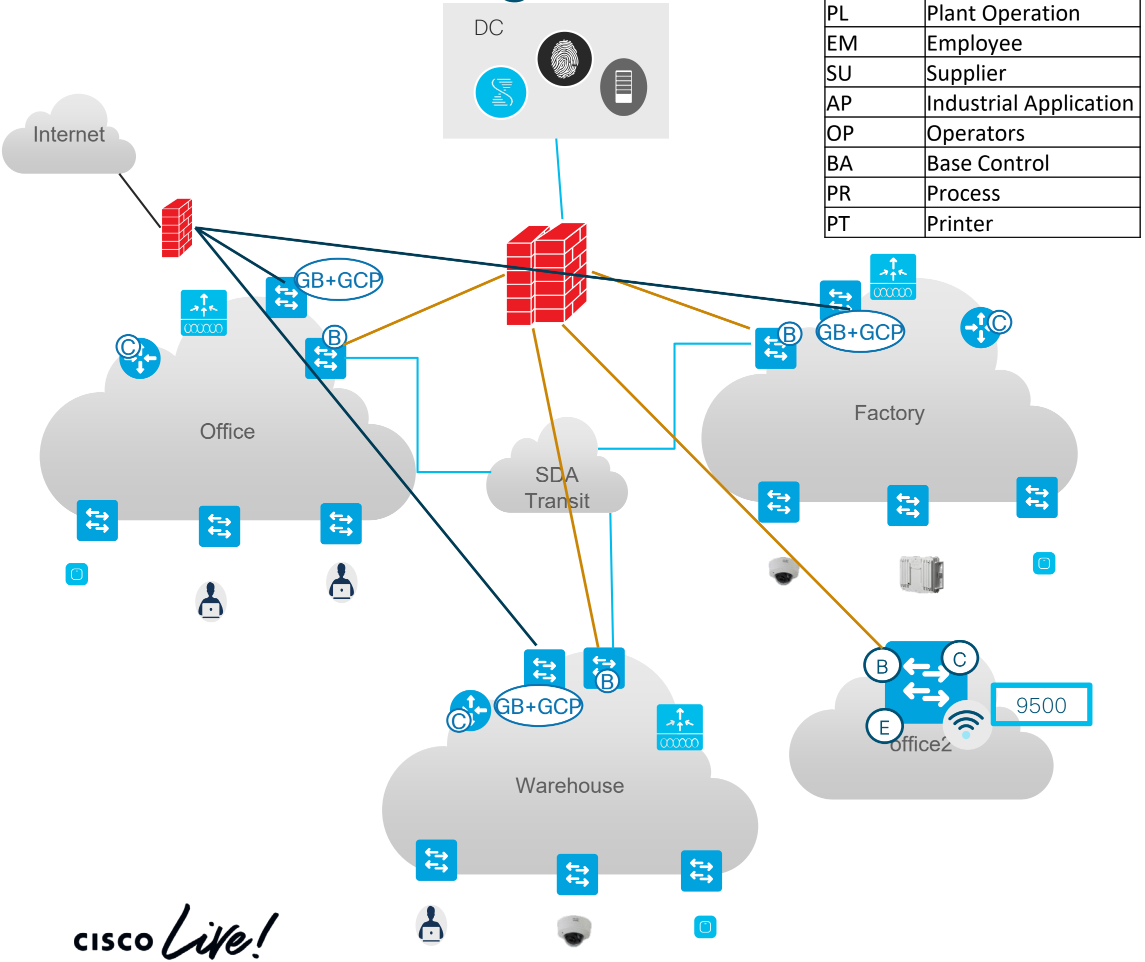
Guest VN

EM,AP,PT
Enterprise VN

HV,SE
Building VN

OP,BA,PL
Factory VN

Default VN



Requirement:

- 15 facilities
- 250 users per facility
- Existing Ise deployment
- Seemless mobility and policy propagation
- Cross domain policy
- Optimize guest traffic

Design:

- DNAC XL for multisite
- Latency consideration
- Border -9500, CP -9300
- Smaller sites have FiAB (9500)
- WLC- 9800 per site
- Separate border and control plane for Mobility requirement
- GB and GCP for optimizing Guest traffic
- Firewall connecting the sites for interVN traffic

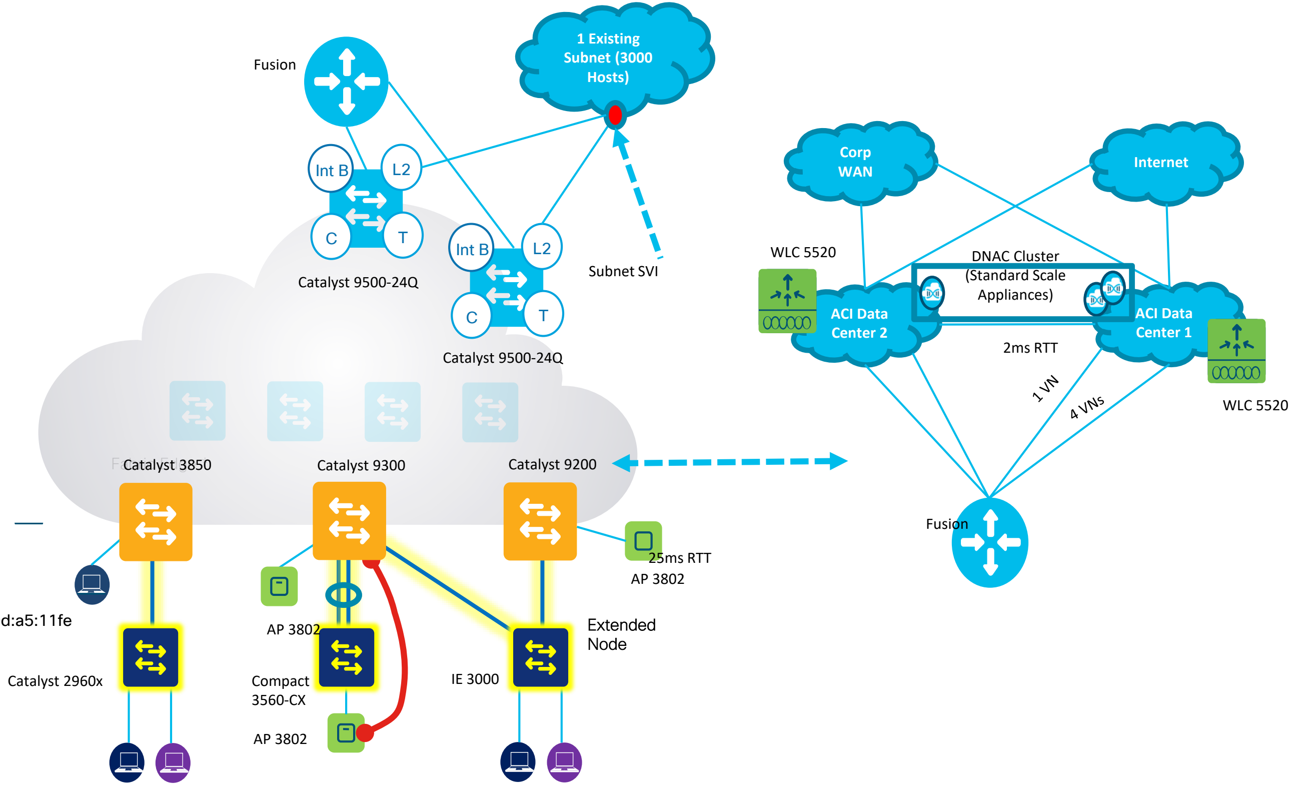
Enterprise

Fabric Requirements

130 Buildings (3 floors each average)
L2 Overlays
Integration with ACI
Multi-Site with SD-Access Transit
5 Virtual Networks
DNA Center Cluster
Common VLAN Name Across Sites
25,000 Clients (Inc v4/v6 .. V6 with 3 addresses per device)

Targeted Code Releases

DNAC 1.3.1
IOS XE 16.9.3s
ISE 2.6 patch 1



Take aways

- Understand the requirements before getting started
- Consider the scale requirements
- Choose the right platforms for fabric devices
- Start small, then expand

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

Please fill out the survey

Thank you

You make **possible**