



You make **possible**



Cisco SD-Access- Integration with Data Center Architectures

Fay-Ann Lee, Technical Marketing Engineer

BRKDCN-2489

CISCO *Live!*

Barcelona | January 27-31, 2020



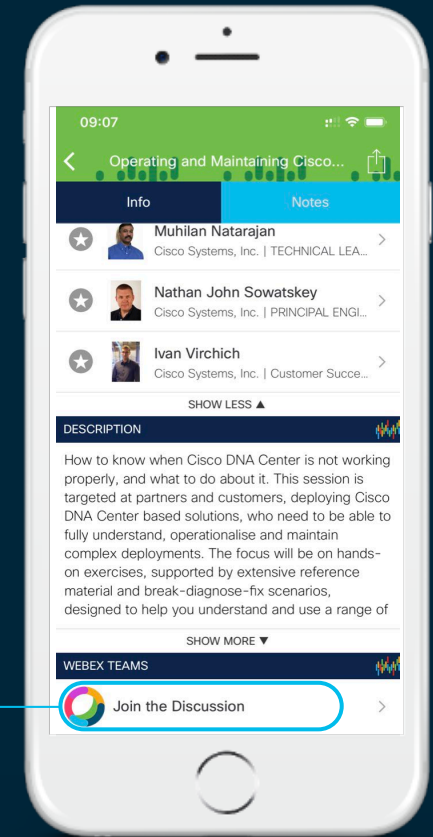
Cisco Webex Teams

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


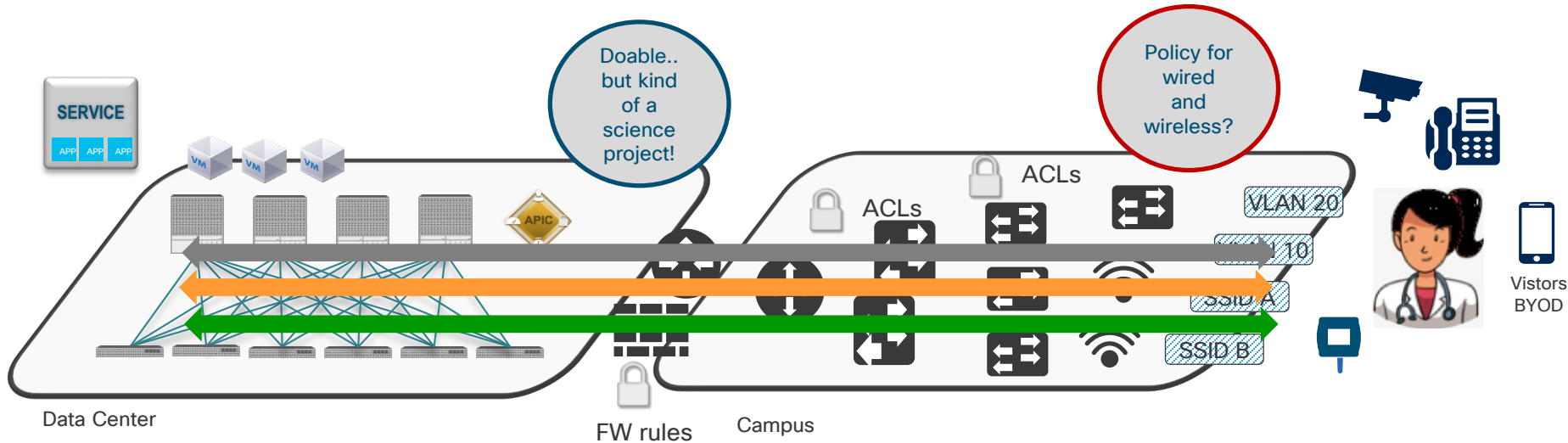


Agenda

- Introduction
- Integration
 - Policy Plane
 - Control Plane
 - Data Plane
- Demo
- Conclusion

The Barriers

Use Case: New Service Rollout

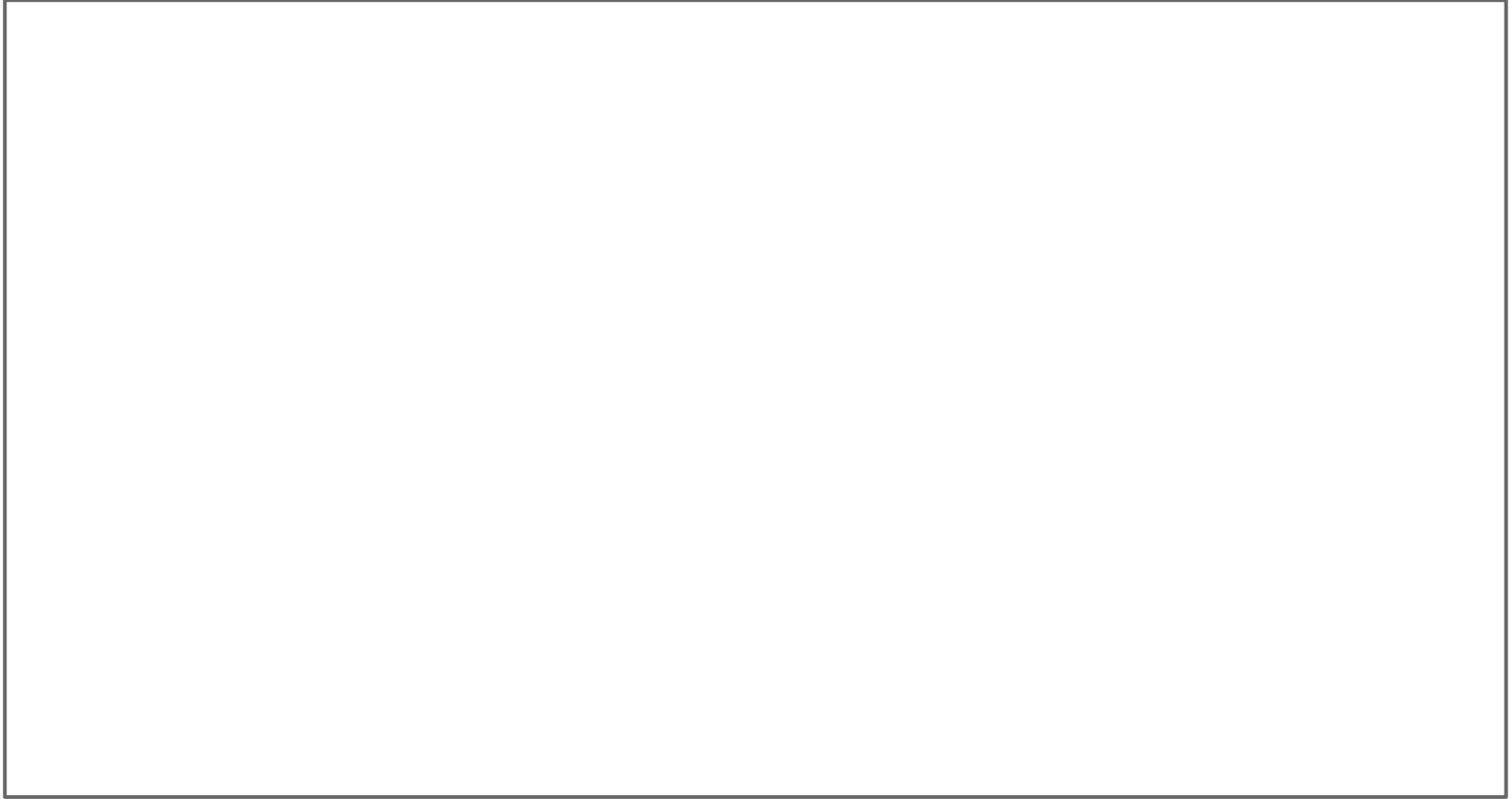


Spawning new VMs is probably the easiest part

How to grant the right access to the right resources for the right users and devices?

Today: Multiple VLANs, SSIDs, ACLs

Can you see the business intent here?



Policy Based on Context

IOT



~~192.168.3.47~~

Physicians



~~192.168.12.213~~

More than just an IP address

Group-Based Policies



Intent-Based Segmentation

Intent-Based Segmentation

Articulating Intent with SGTs

Policy: Physicians have web access to Medical Apps

Traditional Segmentation Policy

```
Switch-1#show ip access-list
```

```
Extended IP access list CorpPolicy
```

```
10 permit tcp 10.1.100.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 80
20 permit tcp 10.1.100.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 443
30 permit tcp 10.2.101.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 80
```

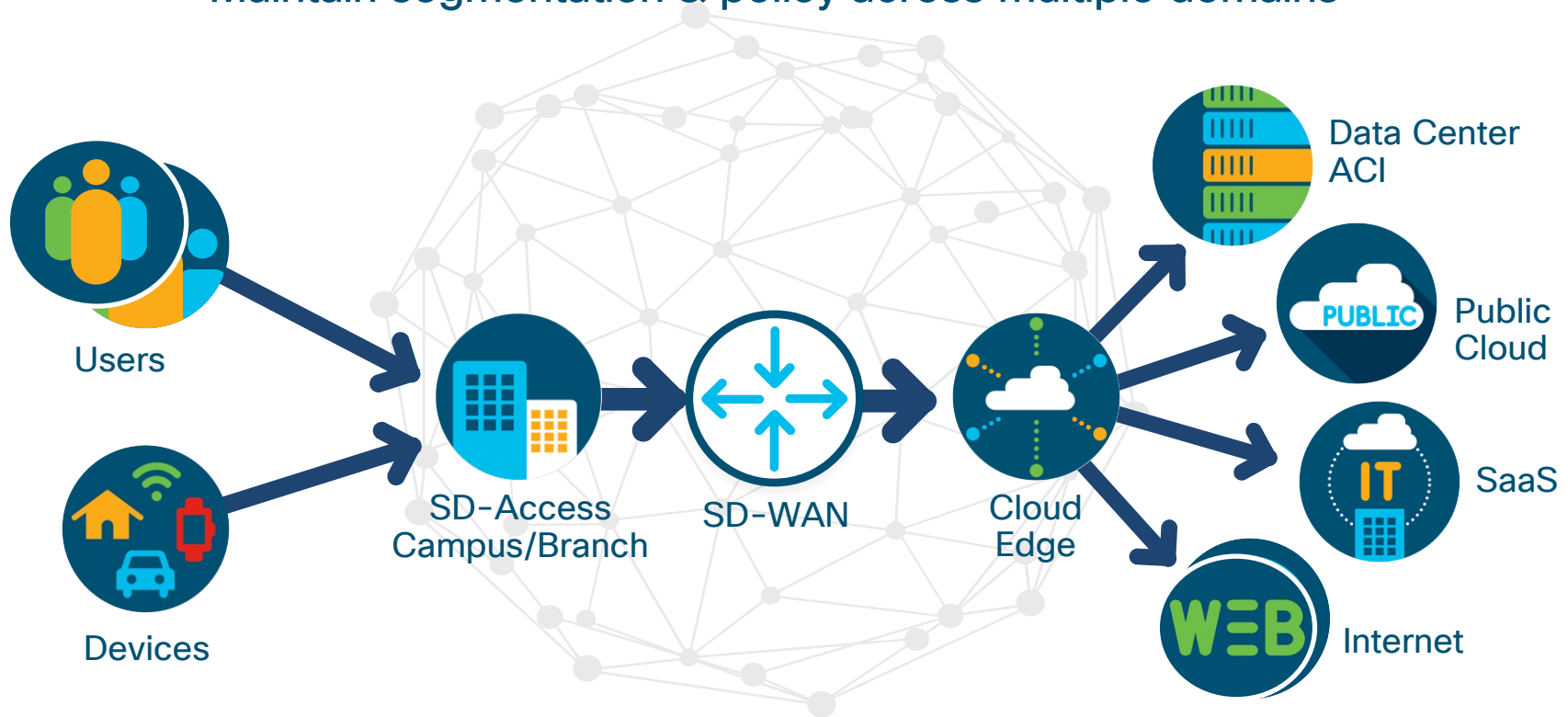
Group-Based Segmentation Policy

```
Switch-1# show cts role-based permissions
```

```
IPv4 Role-based permissions from 10:Physicians to 100:MediApps Web_Only-10
```

Benefits of Intent Based Networking

Maintain segmentation & policy across multiple domains



Consistent Experience for Any User, Any Thing, Anywhere

ACI, DNAC and ISE

Platform and software support

ACI Fabric Hardware	ACI Software	ISE	APIC	DNAC
Nexus 9K*	13.2+	2.4 Patch6	3.2+	1.2.10+

* - Please check release notes for latest recommended information

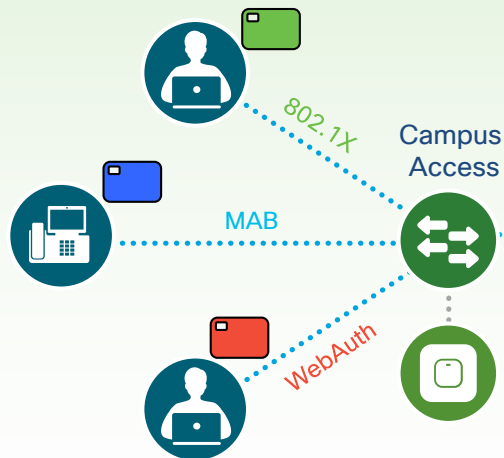
* - (9396PX/TX, 9372PX/TX, 93120TX, 93128TX, 9736PQ LC, 9336PQ, 93108-EX, 93180-EX)

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

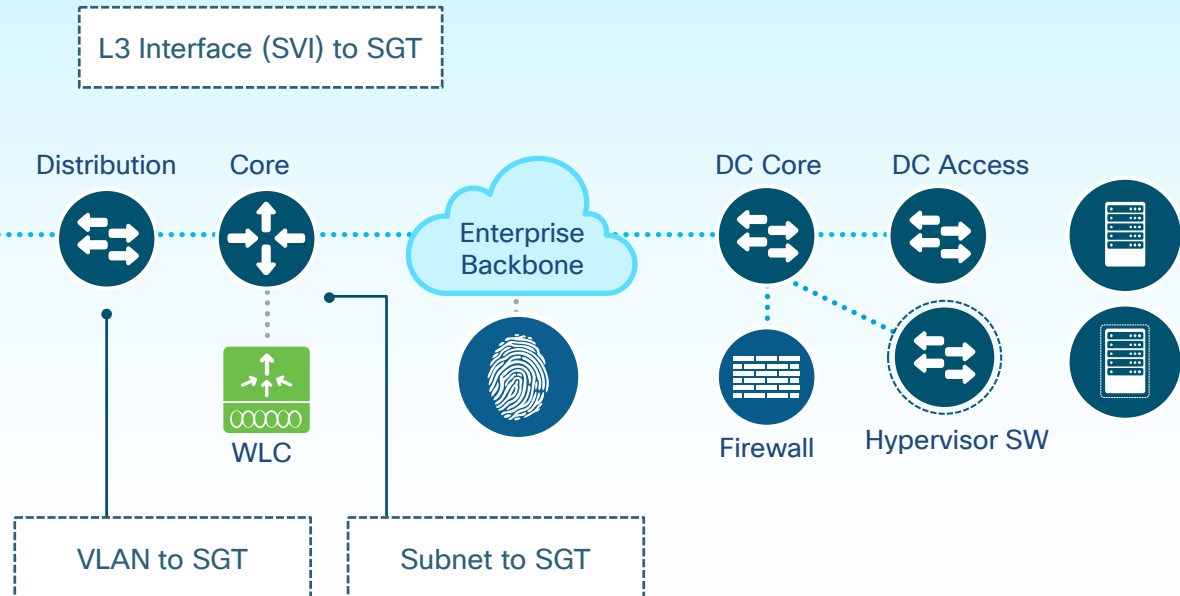
SD-Access Group Assignment – Campus/Branch

Two ways to assign SGT (Scalable Group Tag)

Dynamic Classification

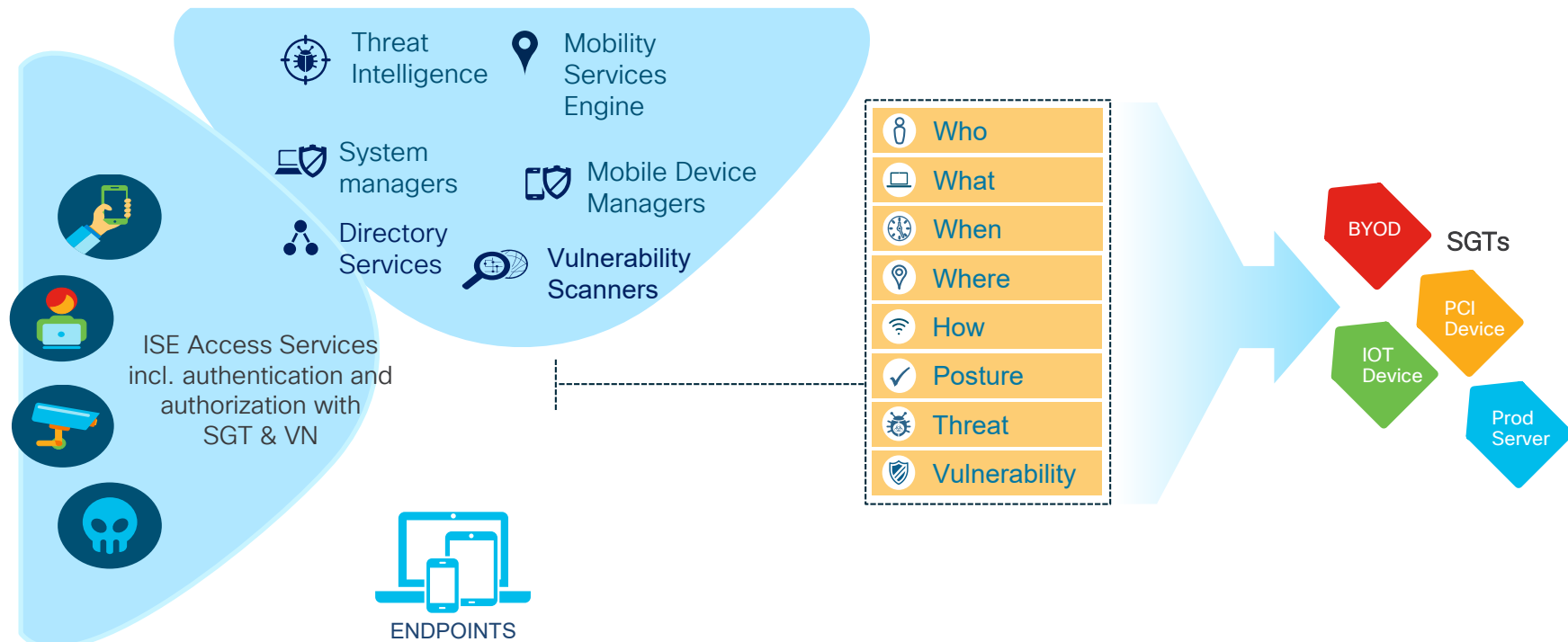


Static Classification



Build Context and Summarize into Scalable Groups

Cisco Identity Services Engine (ISE)



Enabling Consistent Policies Across the Enterprise

Identity Services Engine / Cisco DNA Center



Security

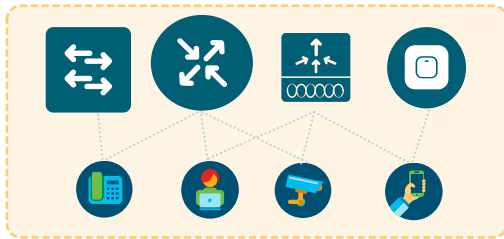


APIC-DC, Controller for ACI

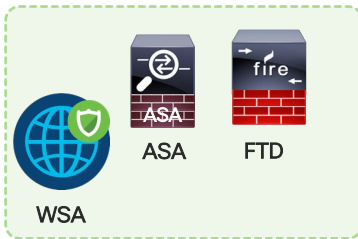


Common Policy Groups

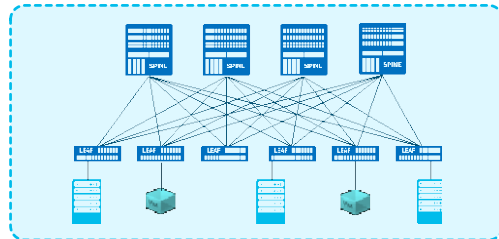
Campus & Branch Networks



Security Apps



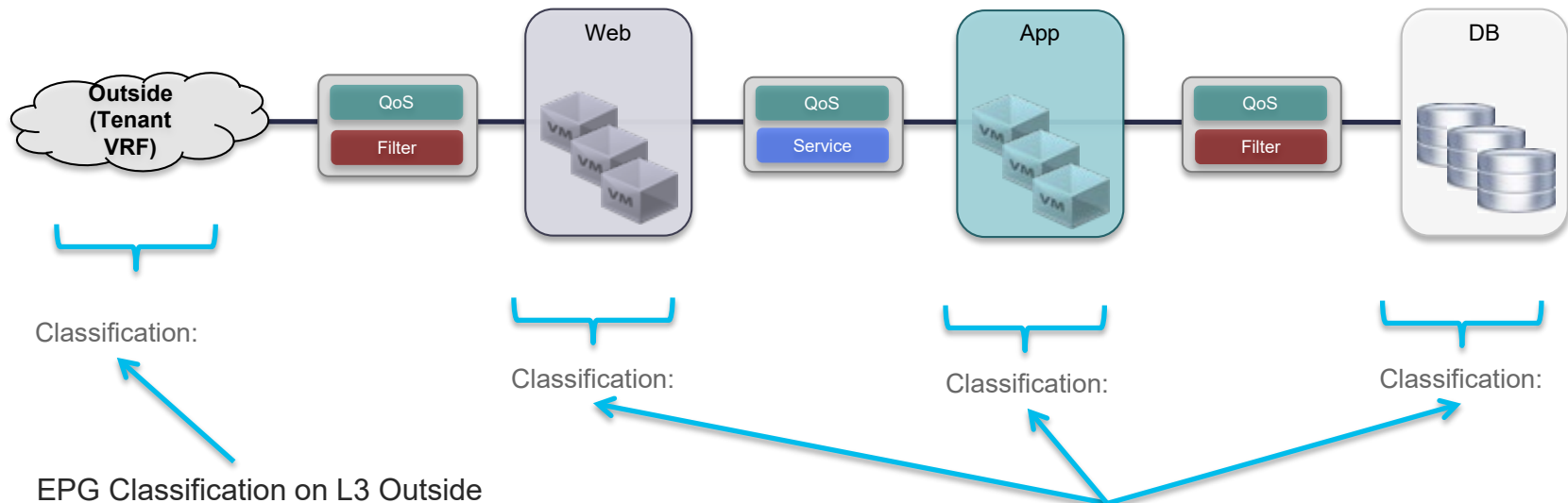
ACI DC/Cloud



Intent-Based Segmentation

Endpoint Classification – Data Center

How to define who is a member of an EPG

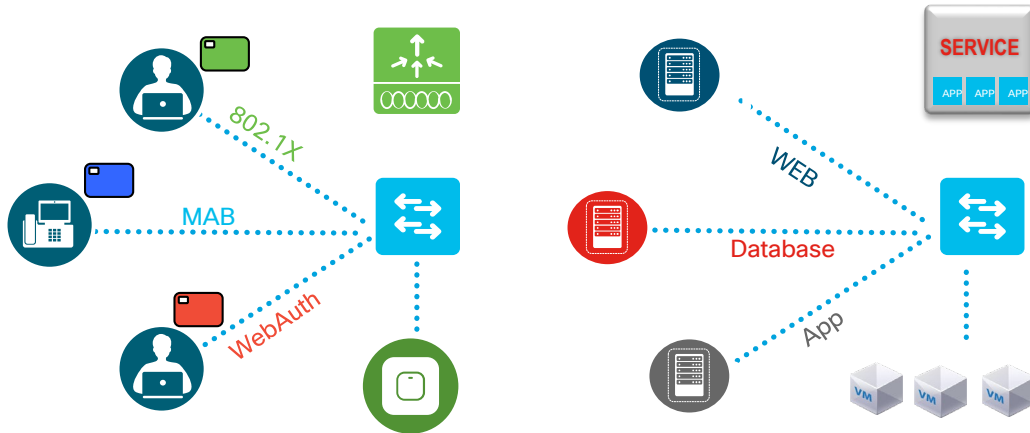


- EPG Classification on L3 Outside is based on IP address, Network/Mask
- TrustSec and SDA identity federation (granular identity from outside the DC)

- EPG Classification on an access/server port is based on different attributes
 - Port + VLAN, Port + VXLAN
 - VM Attributes and Tags
 - IP & MAC Host Address, IP Network/Mask
 - DNS, 802.1x

Disjointed Identity and Policy

Between Campus and Data Center Domains



Focused on User Access
Wireless Integration

Focused on Applications
Compute Integration

Today: No Sharing of
identity?

Goal: Consistent Policies from End to End

Identity Services Engine / DNA Center

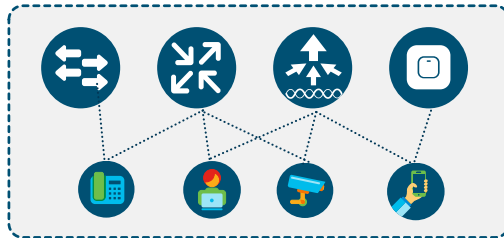


APIC-DC, Controller for ACI

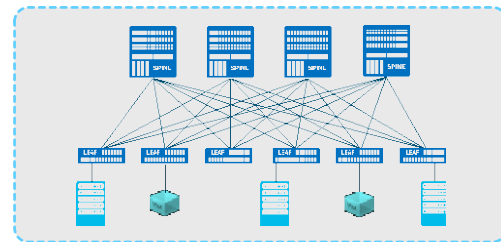


Common Policy Groups

Campus & Branch Networks



ACI DC/Cloud



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

How does integration work?



DNAC, ISE, and APIC Communication



Groups Provisioned from SDA to ACI

The image displays two screenshots from Cisco's network management tools. On the left is the Cisco DNA Center 'Edit Scalable Group' page, and on the right is the Cisco APIC 'Networks' page. A blue callout box with a fingerprint icon and an arrow points from the DNA Center group to the APIC network, indicating the provisioning process.

Cisco DNA Center: Edit Scalable Group

Group-Based Access Control ▾ IP Based A

Scalable Groups (21)

[Enter full screen](#)

Filter Actions ▾ Deploy 0 Select

<input type="checkbox"/>	Name	Tag Value
<input type="checkbox"/>	Auditors	9/0X9
<input type="checkbox"/>	BYOD	15/0XF
<input type="checkbox"/>	Contractors	5/0X5
<input type="checkbox"/>	Developers	8/0X8
<input type="checkbox"/>	Development_Servers	12/0XC
<input type="checkbox"/>	Doctors	18/0X12

Name*
Auditors

Tag Value (decimal)*
9

Description (optional)
Auditor Security Group

Virtual Networks*
User_VN ×

☒ Propagate to ACI

APIC: Networks

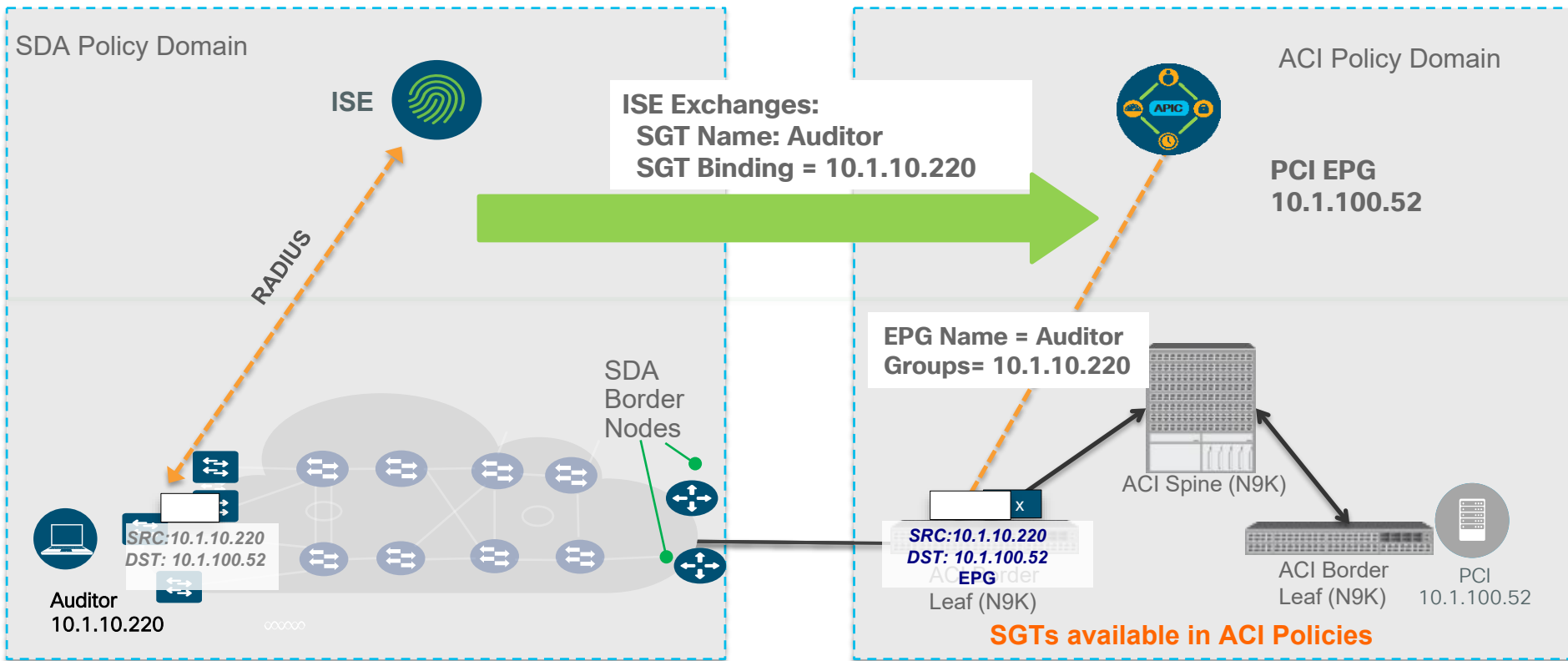
System Tenants Fabric Virtual Networking

ALL TENANTS | Add Tenant | Tenant Search: name or desc

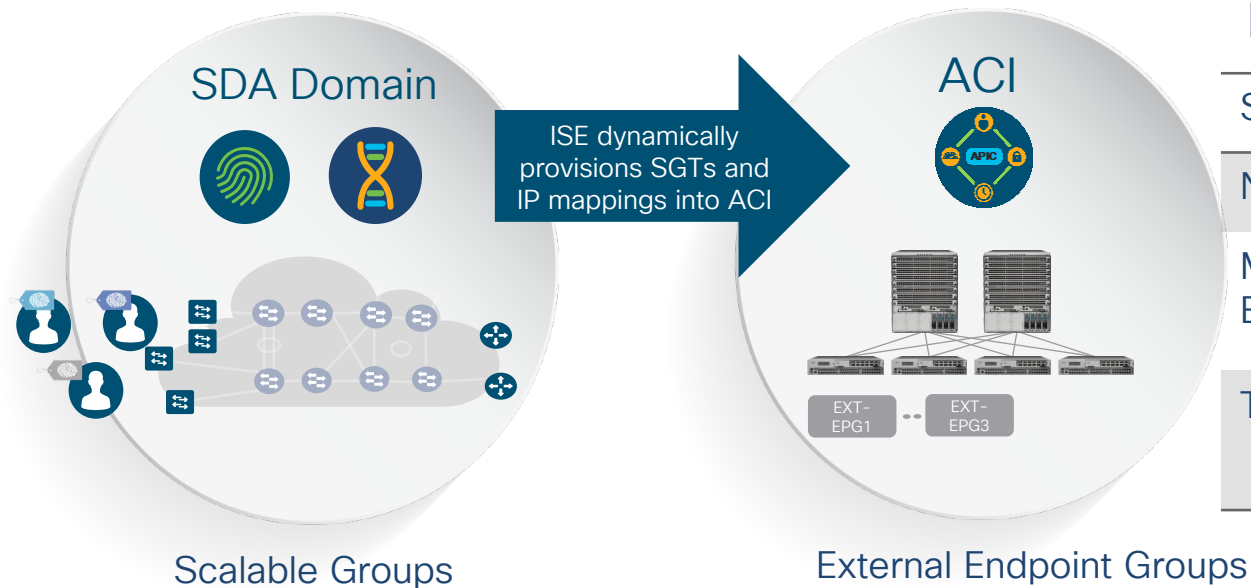
Name
AuditorsSGT
BYODSGT
ContractorsSGT
default
DevelopersSGT
Development_ServersSGT
DoctorsSGT

ISE dynamically provisions EPG and IP mappings into ACI

Details: Groups from SDA Used in ACI



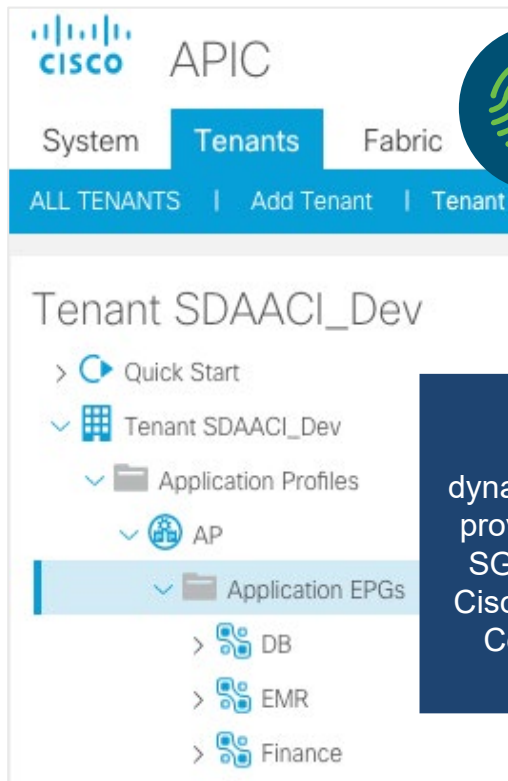
Enforcement Scale in ACI



ACI 3.2 Scale EX, FX and FX2 Hardware

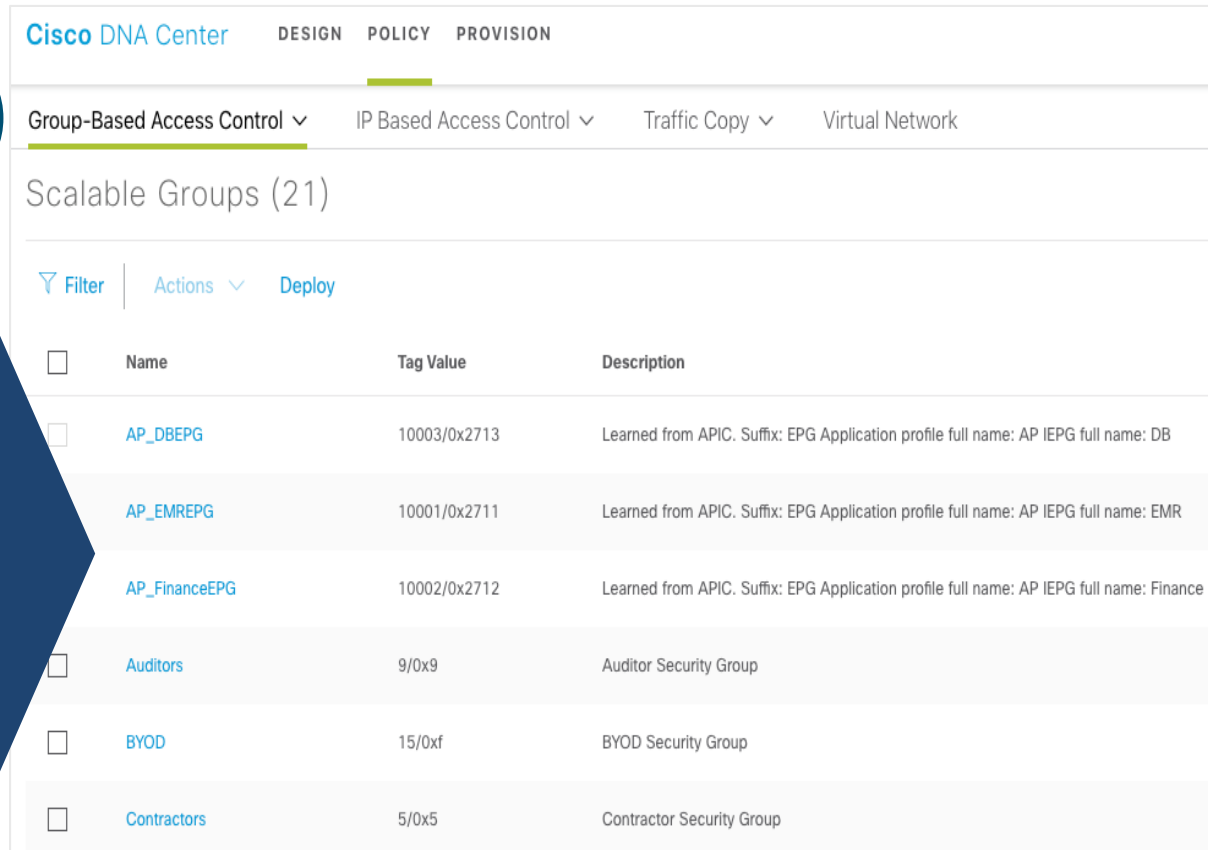
SGT -> External EPG	250
Number of Mappings	64,000
Mappings per External EPG	8000
Transaction rate (target)	100/s

Group from ACI Used in ACI



The screenshot shows the Cisco APIC interface. The top navigation bar includes 'System', 'Tenants', and 'Fabric'. Below this, there are tabs for 'ALL TENANTS', 'Add Tenant', and 'Tenant'. The main content area displays 'Tenant SDAACI_Dev' with a 'Quick Start' button. Under 'Tenant SDAACI_Dev', there is a section for 'Application Profiles' which includes 'AP'. Under 'AP', there is a section for 'Application EPGs' which includes 'DB', 'EMR', and 'Finance'.

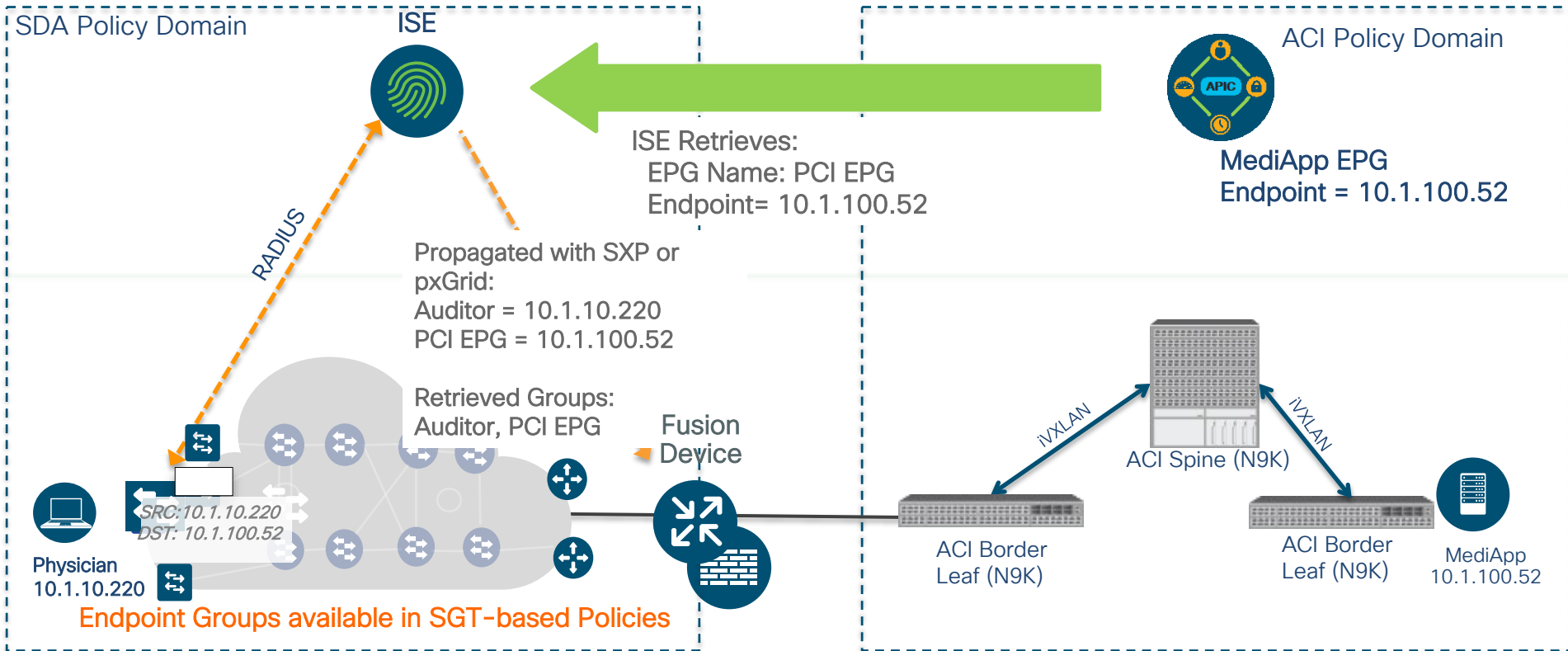
ISE
dynamically
provisions
SGT into
Cisco DNA
Center



The screenshot shows the Cisco DNA Center interface. The top navigation bar includes 'DESIGN', 'POLICY', and 'PROVISION'. Below this, there are tabs for 'Group-Based Access Control', 'IP Based Access Control', 'Traffic Copy', and 'Virtual Network'. The main content area displays 'Scalable Groups (21)' with a 'Filter' button and 'Actions' and 'Deploy' buttons. A table lists the groups:

<input type="checkbox"/>	Name	Tag Value	Description
<input type="checkbox"/>	AP_DBEPG	10003/0x2713	Learned from APIC. Suffix: EPG Application profile full name: AP IEPPG full name: DB
<input type="checkbox"/>	AP_EMREPG	10001/0x2711	Learned from APIC. Suffix: EPG Application profile full name: AP IEPPG full name: EMR
<input type="checkbox"/>	AP_FinanceEPG	10002/0x2712	Learned from APIC. Suffix: EPG Application profile full name: AP IEPPG full name: Finance
<input type="checkbox"/>	Auditors	9/0x9	Auditor Security Group
<input type="checkbox"/>	BYOD	15/0xf	BYOD Security Group
<input type="checkbox"/>	Contractors	5/0x5	Contractor Security Group

Details: ACI Groups Used in SDA (Border or Fusion)



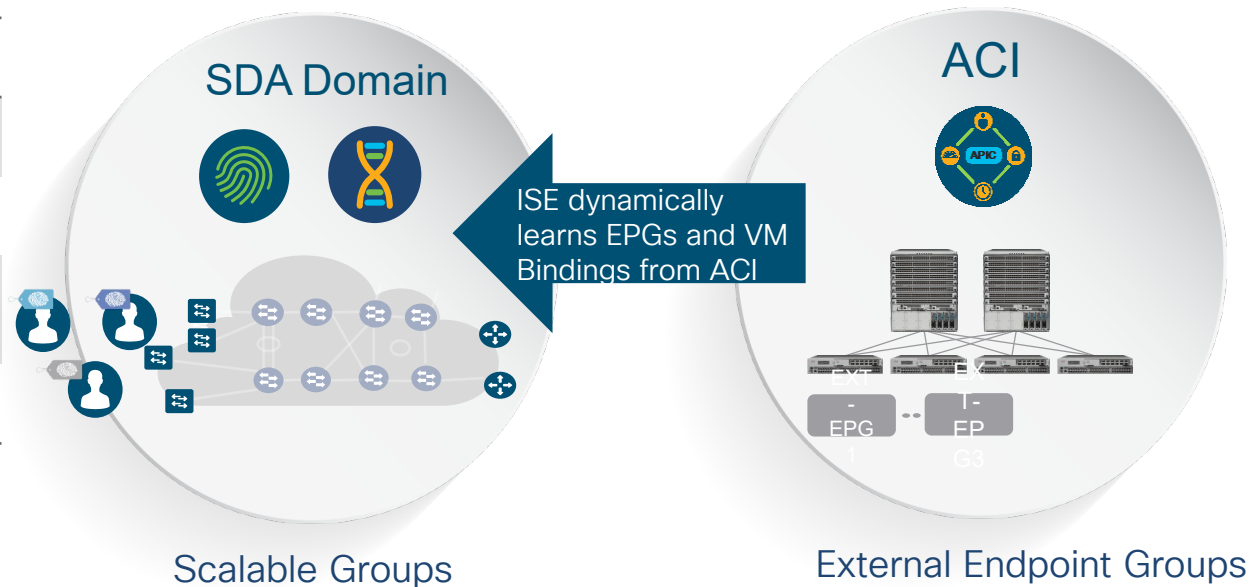
Scaling Enforcement in SDA Environment

ISE/SDA Scale

Numbers of Groups	1000
Number of Mappings*	250k
SXP Peers*	200
pxGrid Peers**	200

*Per pair of ISE SXP Nodes

** Per ISE pxGrid node



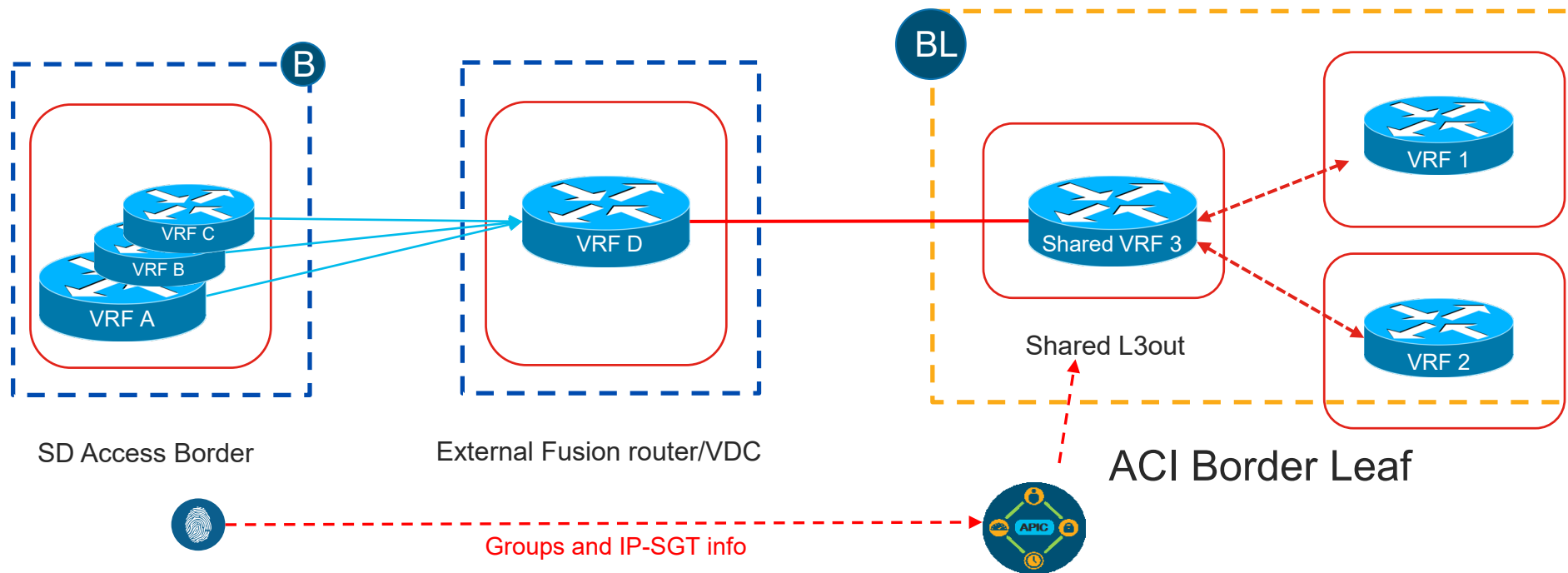
Fusion platforms capable of > 250k Mappings include:
ASR, ISR4k, C6800, ASA and FirePower Appliances

<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/6-5-gbp-system-bulletin.pdf>

How does integration work?

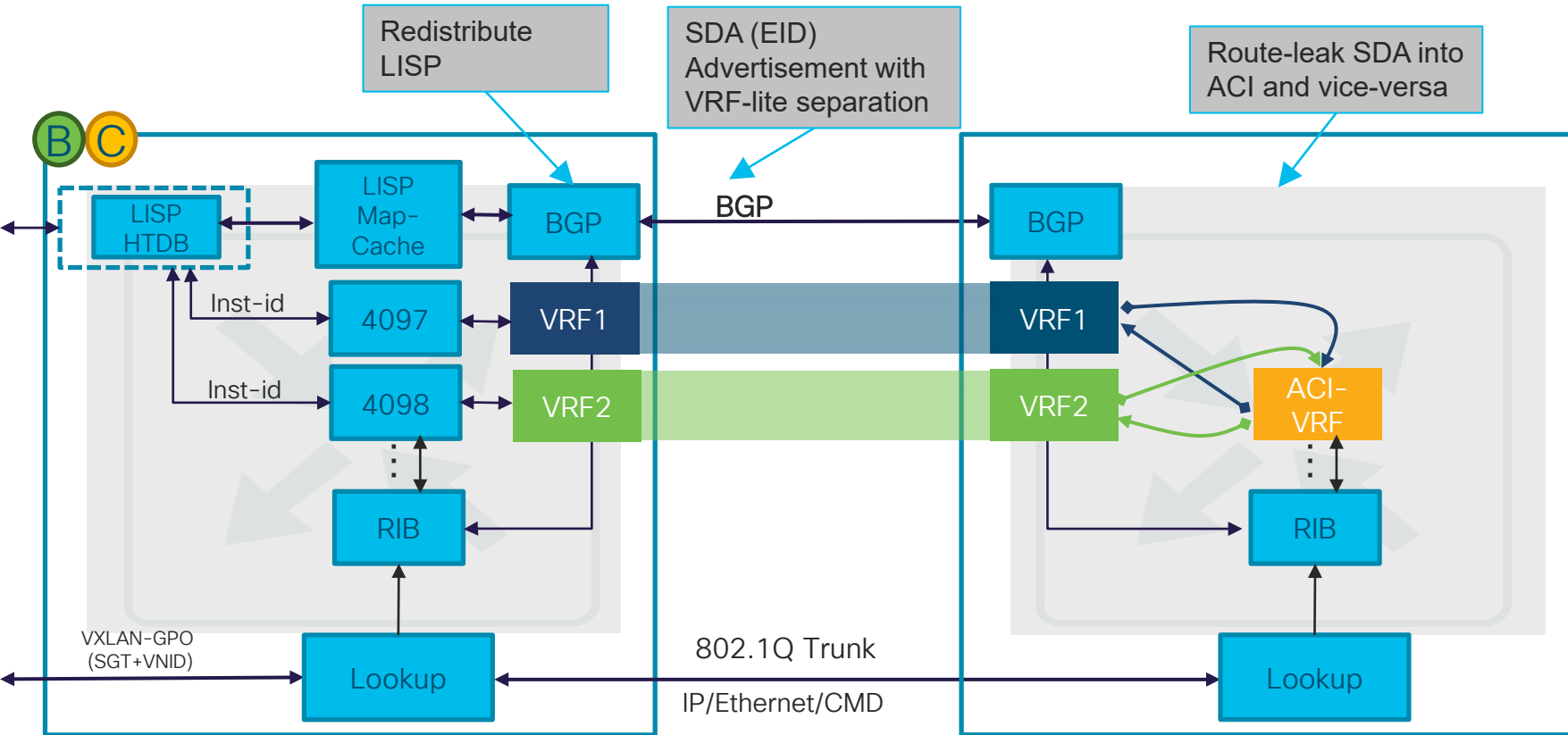


Current Solution: Single VRF, Single Tenant

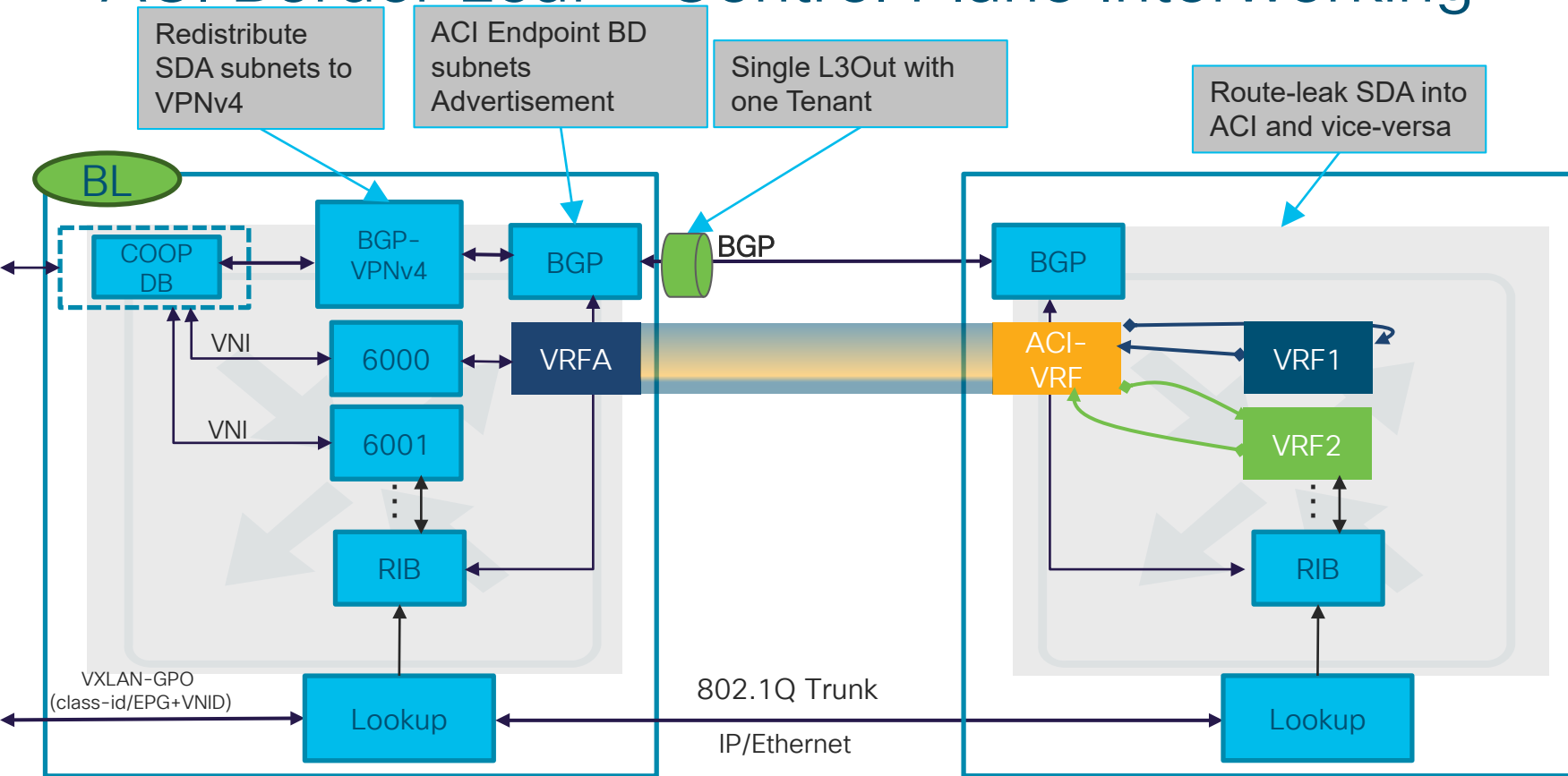


Note: Common tenant can be used for mappings to provide to multiple tenants

SDA Border – Control Plane Interworking



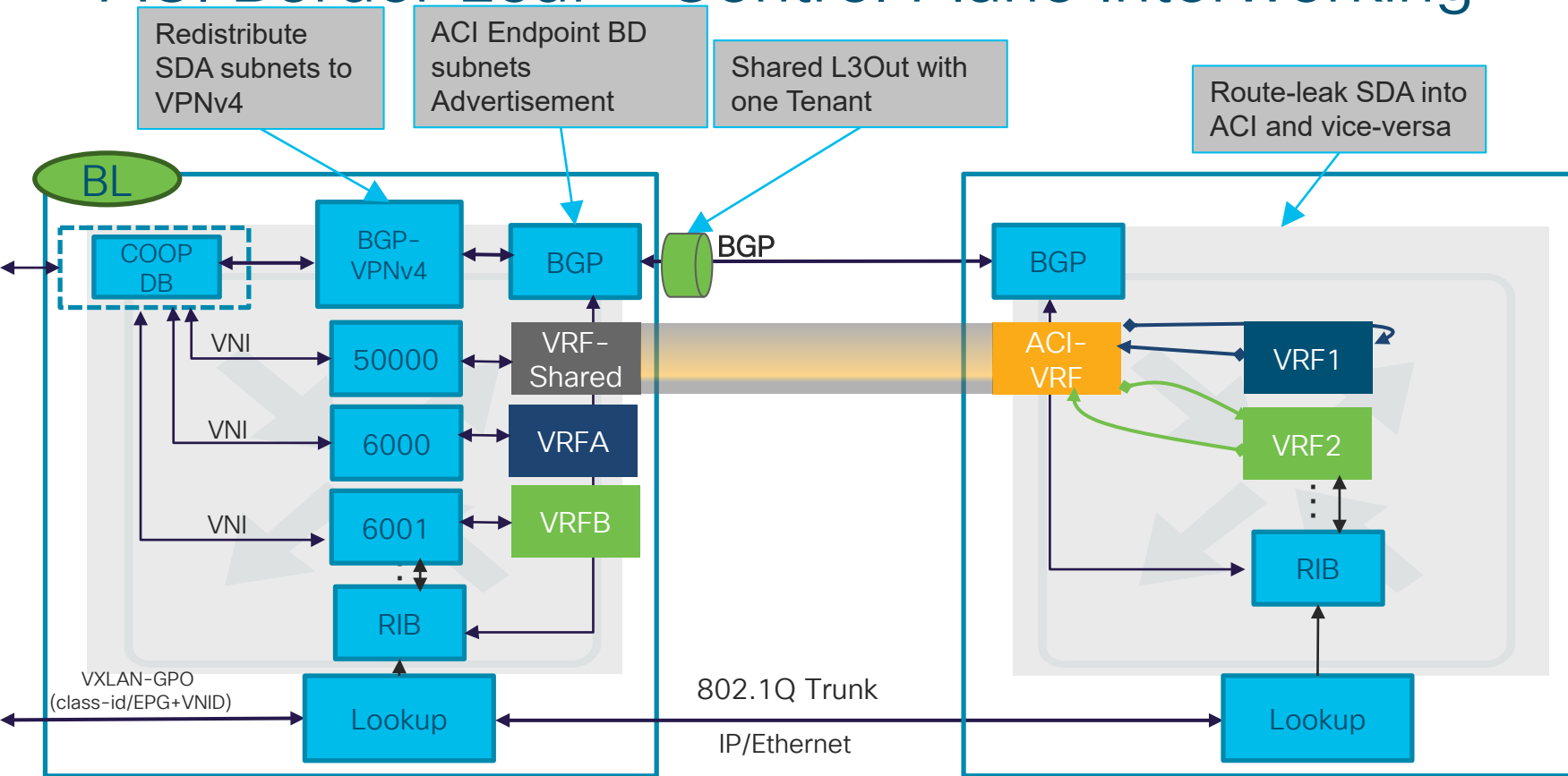
ACI Border Leaf - Control Plane Interworking



cisco Live! ACI-Border Leaf

Fusion

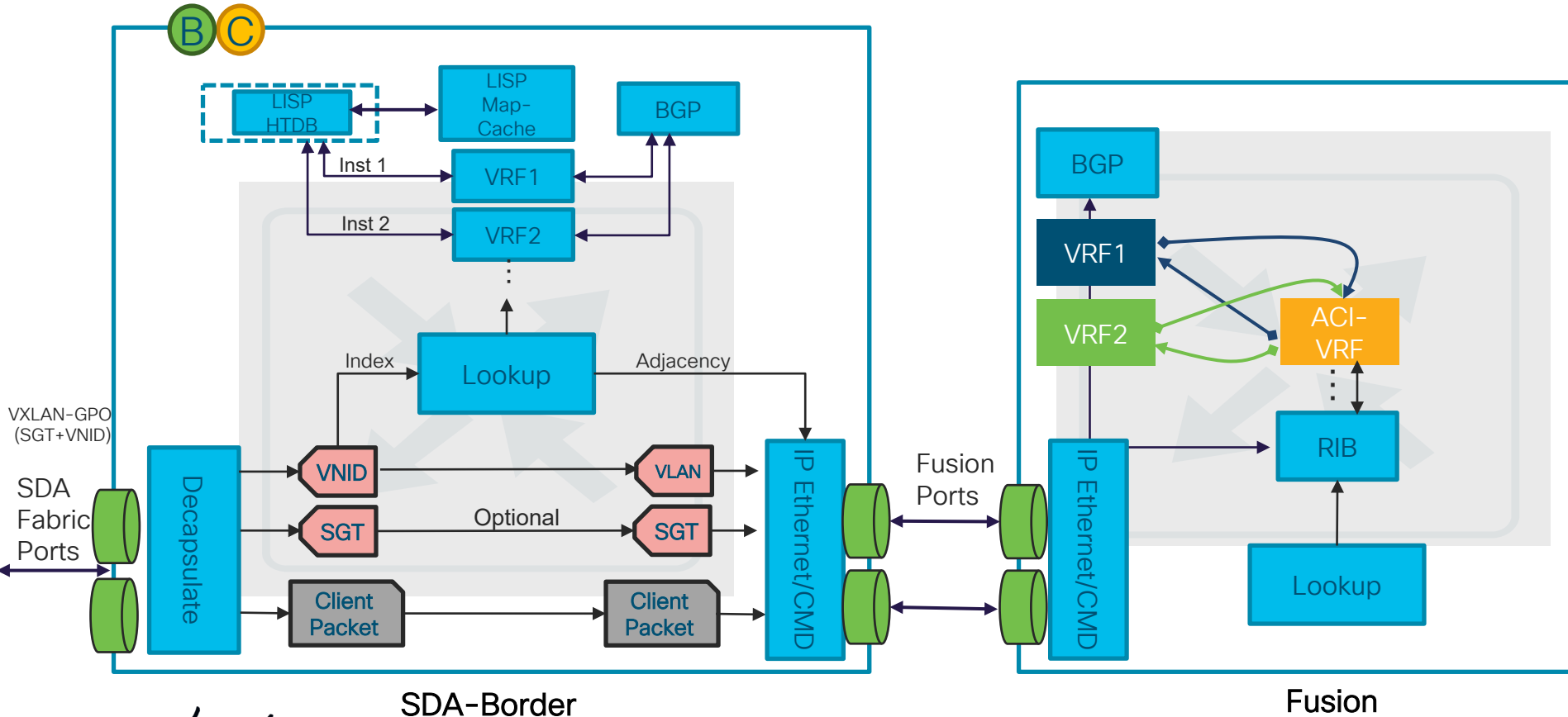
ACI Border Leaf - Control Plane Interworking



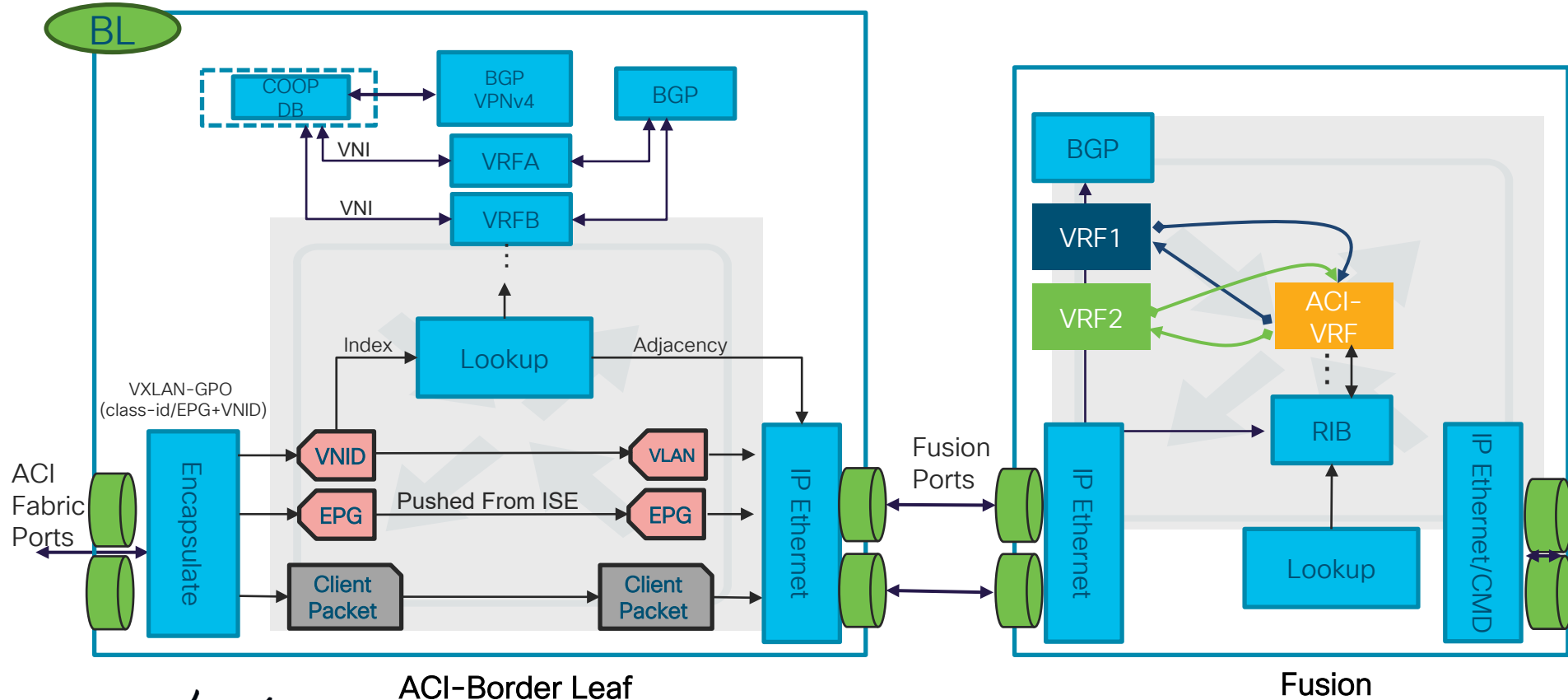
How does integration work?



SDA Border – Data Plane Interworking

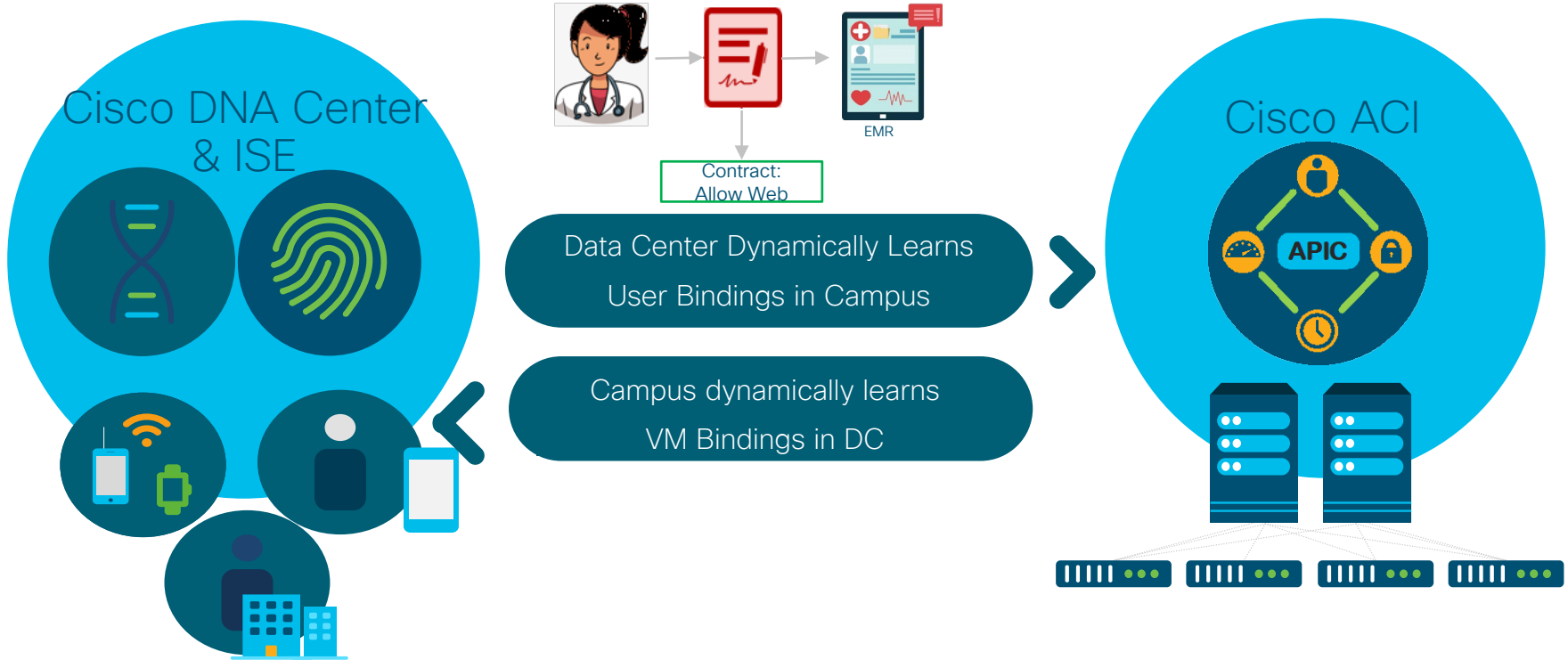


ACI Border Leaf – Data Plane Interworking

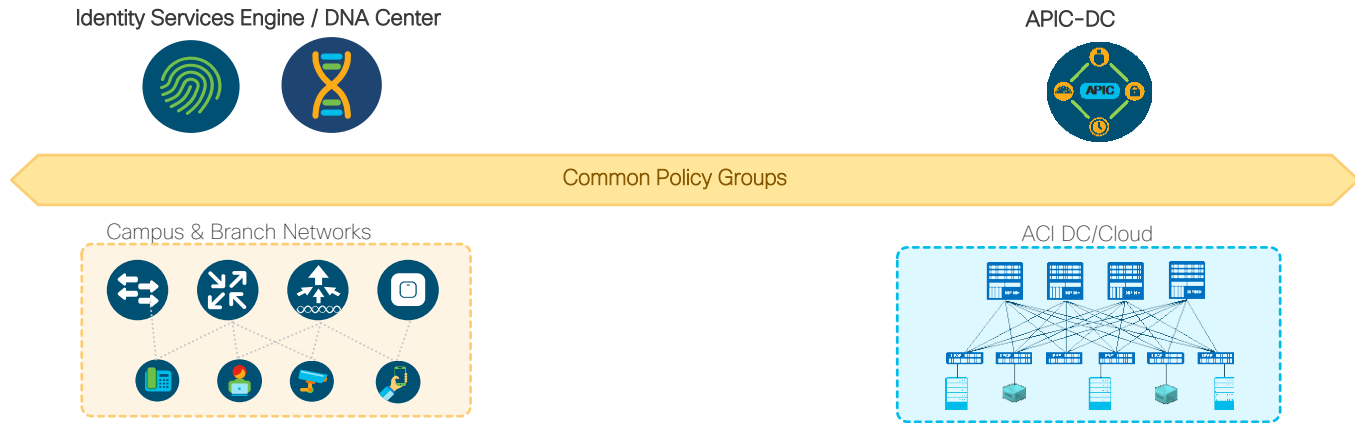


Demo

Demo



SDA-ACI Policy Summary



- Policies automatically take account of endpoint adds/moves changes end to end
Faster policy changes, lower opex, immediate access to new endpoints
- DC app policies aware of users/devices/things, campus policies aware of apps
- Improved visibility of endpoint roles end to end

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



Thank you





You make **possible**