cisco Engage

Text

You make possible

On-line každých 14 dní

Cisco Tech Club Webinář:

Principy řešení SD Access pro podnikové sítě

Přednášející: Jaromír Pilař

Software Defined Access

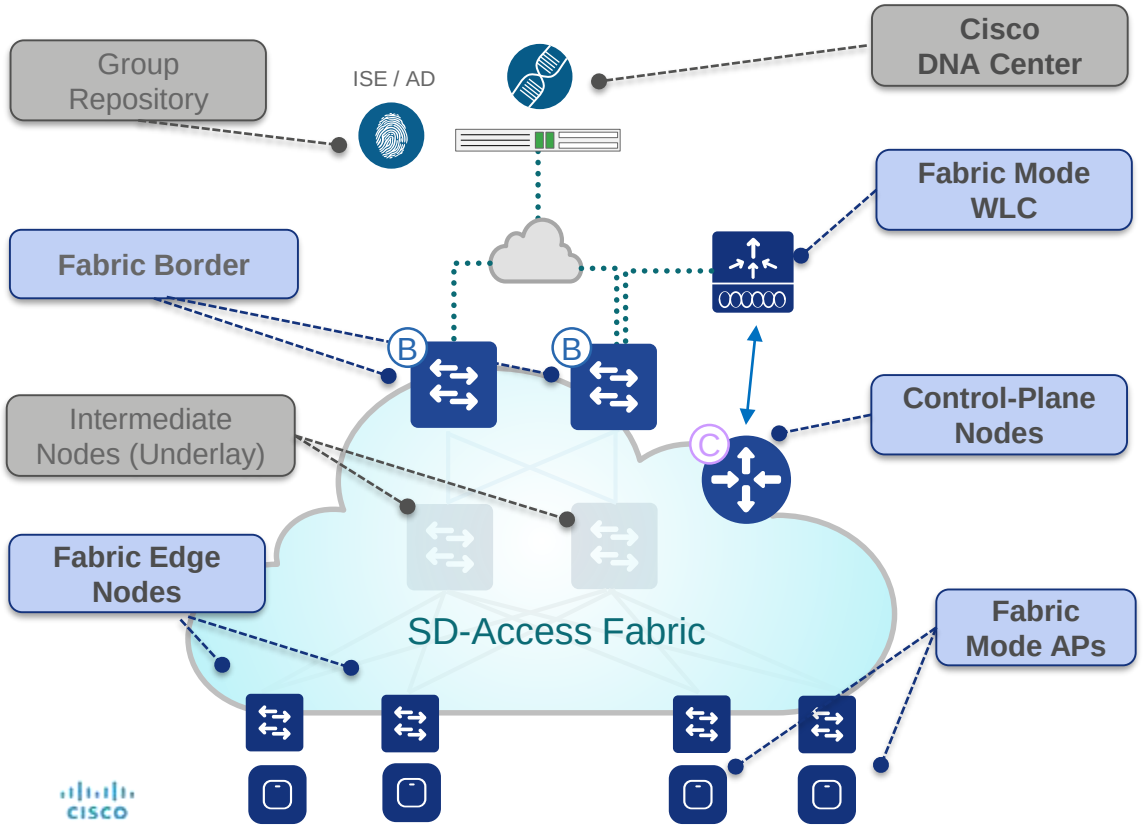
Jaromír Pilař, Consulting System Engineer, CCIE #2910

January 2020

Software Defined Access

Architecture, Technology, Use Cases

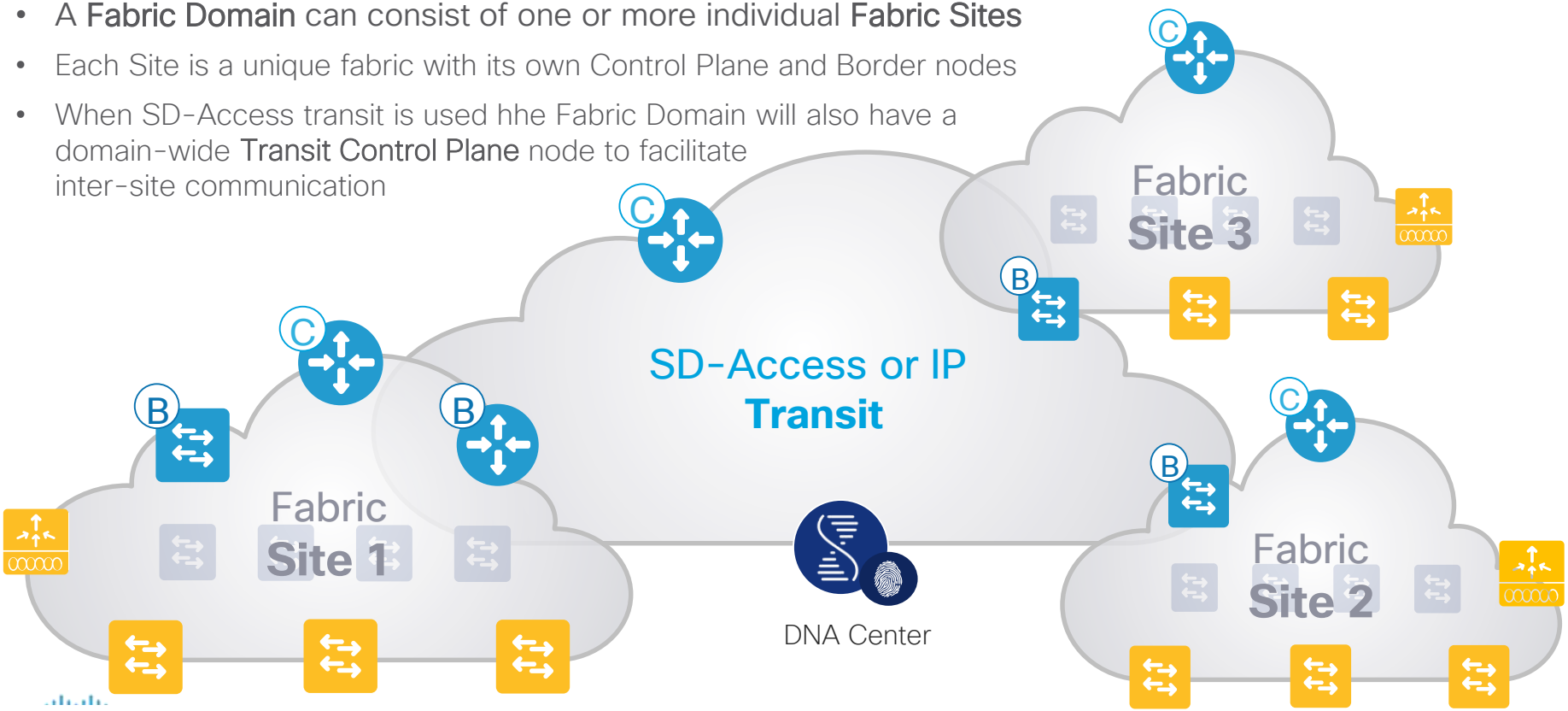
SD-Access Fabric Architecture



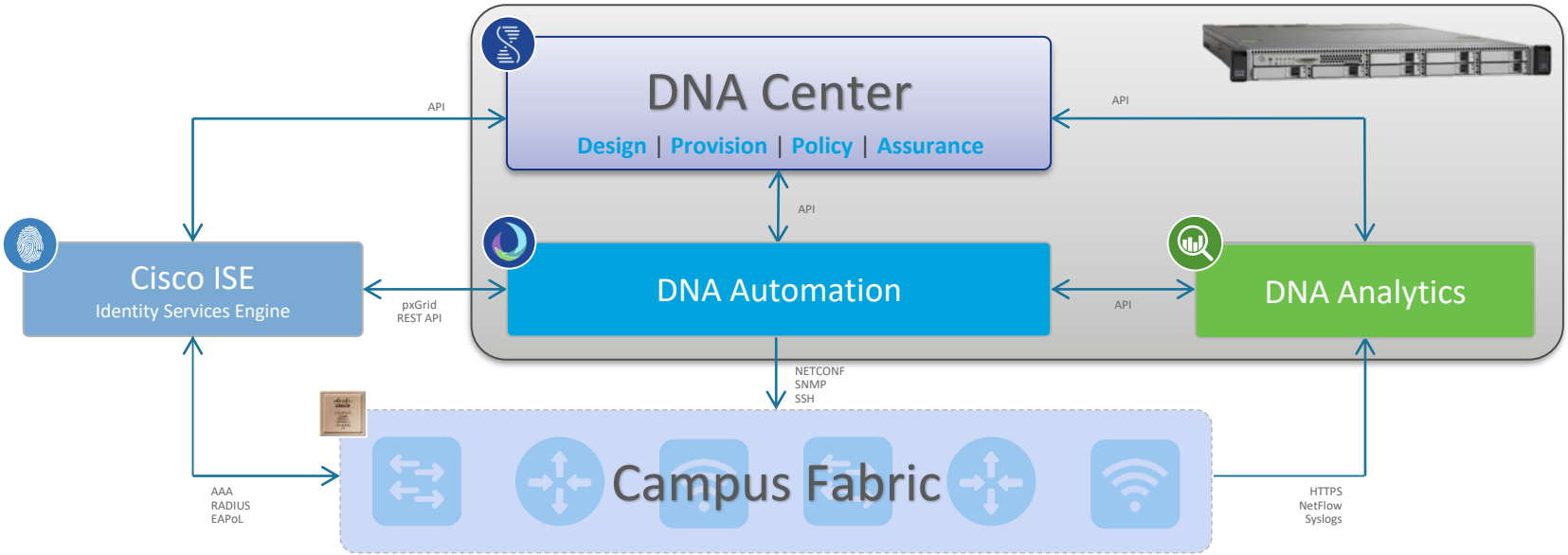
- **DNA Controller** – Enterprise SDN Controller provides GUI management abstraction via multiple Service Apps, which share information
- **Group Repository** – External ID Services (e.g.. ISE) is leveraged for dynamic User or Device to Group mapping and policy definition
- **Control-Plane (CP) Node** – Map System that manages Endpoint ID to Location relationships. Also known as Host Tracking DB (HTDB)
- **Border Nodes** – A Fabric device (e.g.. Core) that connects External L3 network(s) to the SDA Fabric
- **Edge Nodes** – A Fabric device (e.g.. Access or Distribution) that connects wired endpoints to the SDA Fabric
- **Fabric Wireless Controller** – Wireless Controller (WLC) fabric-enabled, participate in LISP control plane
- **Fabric Mode APs** – Access Points that are fabric-enabled. Wireless traffic is VXLAN encapsulated at AP

SD-Access for Distributed Campus

- A **Fabric Domain** can consist of one or more individual **Fabric Sites**
- Each Site is a unique fabric with its own Control Plane and Border nodes
- When SD-Access transit is used hhe Fabric Domain will also have a domain-wide **Transit Control Plane** node to facilitate inter-site communication



DNA Center – Service Components



Cisco Switches | Cisco Routers | Cisco Wireless

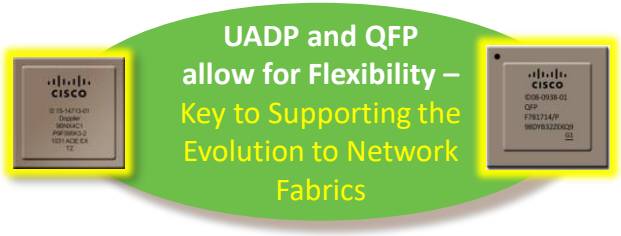
SD Access Fabric – key technologies involved

1. **Control-Plane based on LISP**
2. **Data-Plane based on VXLAN**
3. **Policy-Plane with Cisco TrustSec (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 (No Static)
- No Topology Limitations (Basic IP)

Cisco Hardware and Software innovations



SD-Access Key Component – LISP

1. Control Plane based on LISP

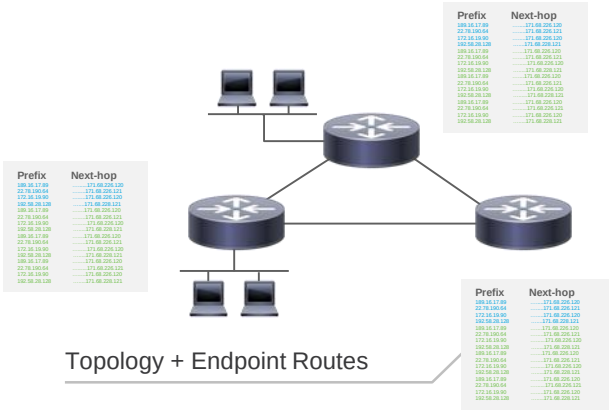
Host Mobility

Routing Protocols = **Big Tables** & **More CPU**
with Local L3 Gateway

LISP DB + Cache = **Small Tables** & **Less CPU**
with Anycast L3 Gateway

BEFORE

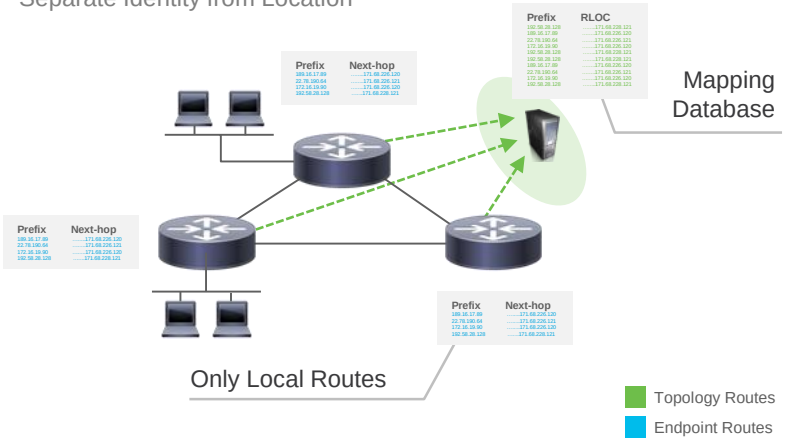
IP Address = Location + Identity



Endpoint Routes are Consolidated to LISP DB

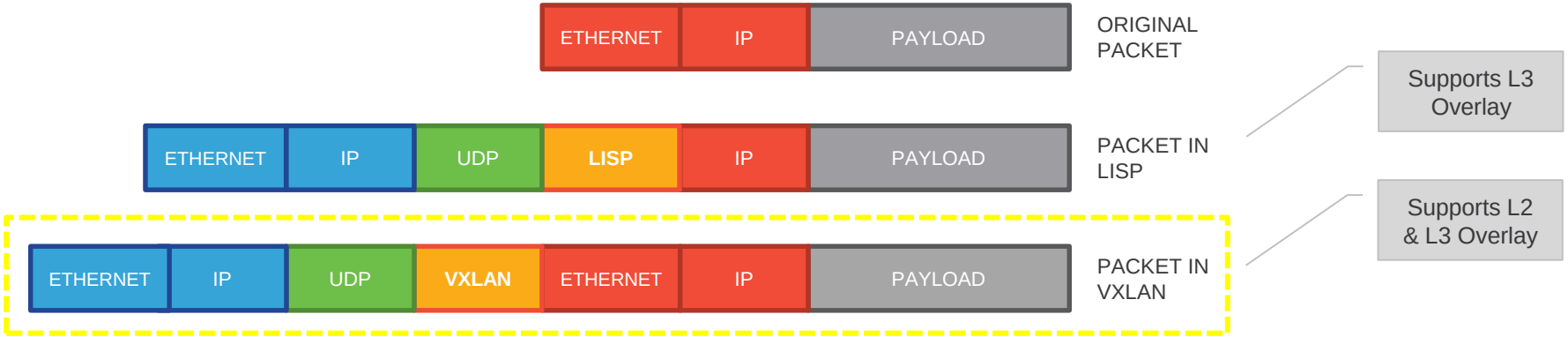
AFTER

Separate Identity from Location



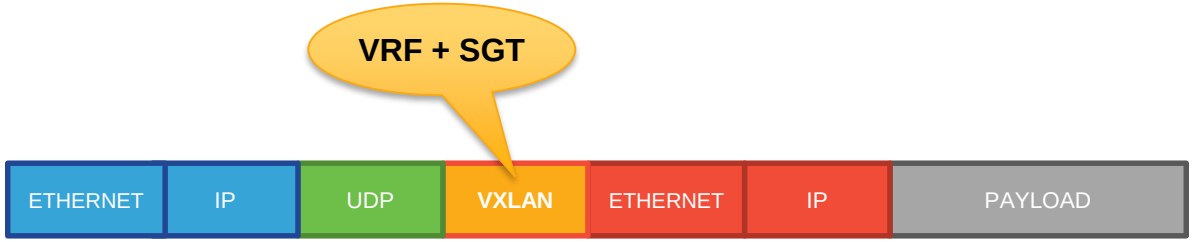
SD-Access Key Components – VXLAN

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



SD-Access Key Components – TrustSec

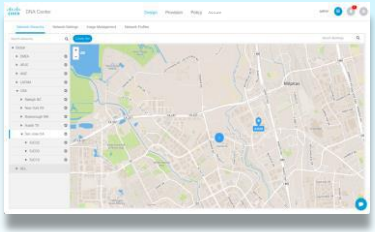
1. **Control Plane based on LISP**
2. **Data-Plane based on VXLAN**
3. **Policy-Plane based on TrustSec**



Virtual Routing & Forwarding
Scalable Group Tagging

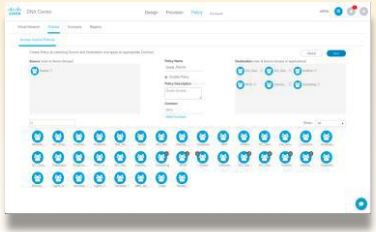
DNA Center Workflow for SD-Access

Design



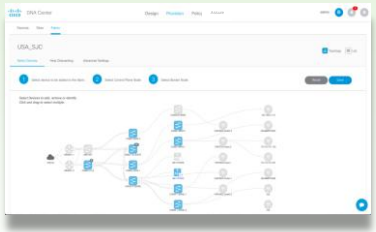
- Global Settings
- Site Profiles
- DDI, SWIM, PNP
- User Access

Policy



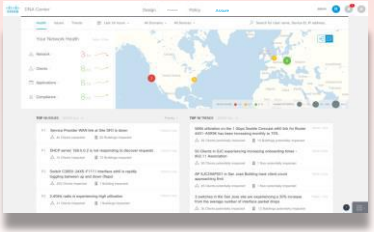
- Virtual Networks
- ISE, AAA, Radius
- Endpoint Groups
- Group Policies

Provision



- Fabric Domains
- CP, Border, Edge
- FEW, OTT WLAN
- External Connect

Assurance



- Health Dashboard
- 360º Views
- FD, Node, Client
- Path Traces

Planning & Preparation

Installation & Integration

SD-Access Use Cases

Use Case	Details	Benefits
Security & Segmentation	• Onboard Users with 802.1x, AD and Static Authentication • Group Users with TrustSec (SGT Tags) • Automate VRF Configuration (line of businesses or departments etc.)	• Reduce time to provision Network Segmentation and User Groups • Provide a foundation to enforce network security policies
User Mobility	• Single point of definition for Wired and Wireless Users • Seamless Roaming between Wired and Wireless	• Management of Wired and Wireless networks and users from Single interface (DNA Center) • Offload Wireless data path to network switches (reduce load on the controller)
Guest Access	• Define specific Groups for Guest Users • Create policy for Guest Users resource access (ex. Internet Access)	• Simplified Policy Provisioning • Time savings when provisioning policies
IoT Integration	• Segment and Group IOT Devices • Define policies for IOT group access and management • Device profiling with flexible authentication options	• Simplify deployment of IOT Devices • Reduce network attack surface with device segmentation
Monitoring Troubleshooting	• Multiple data points on network behavior (syslog, stats etc.) • Contextual data available per User/Device	• Significant reduction in troubleshooting time • Rich context and analytics for decision making
DC Integration	• Policy Management for User to application Access • Full Integration with Cisco Data Center solutions (ACI, PF etc.)	• Administrator can define user to application access policy from a single interface • End to End Policy management for the Enterprise
Branch Integration	• Create Single fabric across multiple regional Branch locations • Leverage Cisco Routers as Fabric Border nodes	• Simplified provisioning and management of branch locations • Enterprise wide policy provisioning and Enforcement

Segmentation and policy

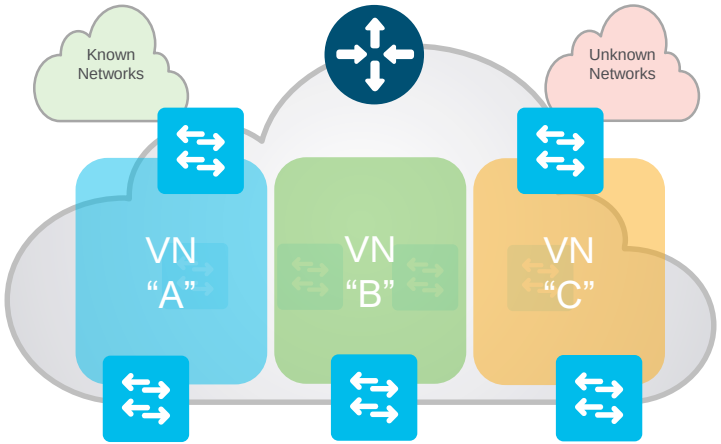
Virtual networks, scalable groups

SD-Access Fabric

Virtual Network– A Closer Look

Virtual Network maintains a separate Routing & Switching instance for each VN

- Control-Plane uses Instance ID to maintain separate VRF topologies (“Default” VRF is Instance ID “4097”)
- Nodes add VNID to the Fabric encapsulation
- Endpoint ID prefixes (Host Pools) are advertised within Virtual Network
- Uses standard “vrf definition” configuration, along with RD & RT for remote advertisement (Border Node)

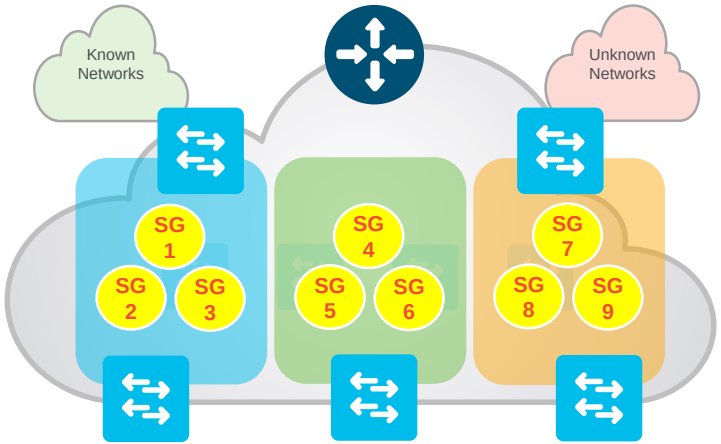


SD-Access Fabric

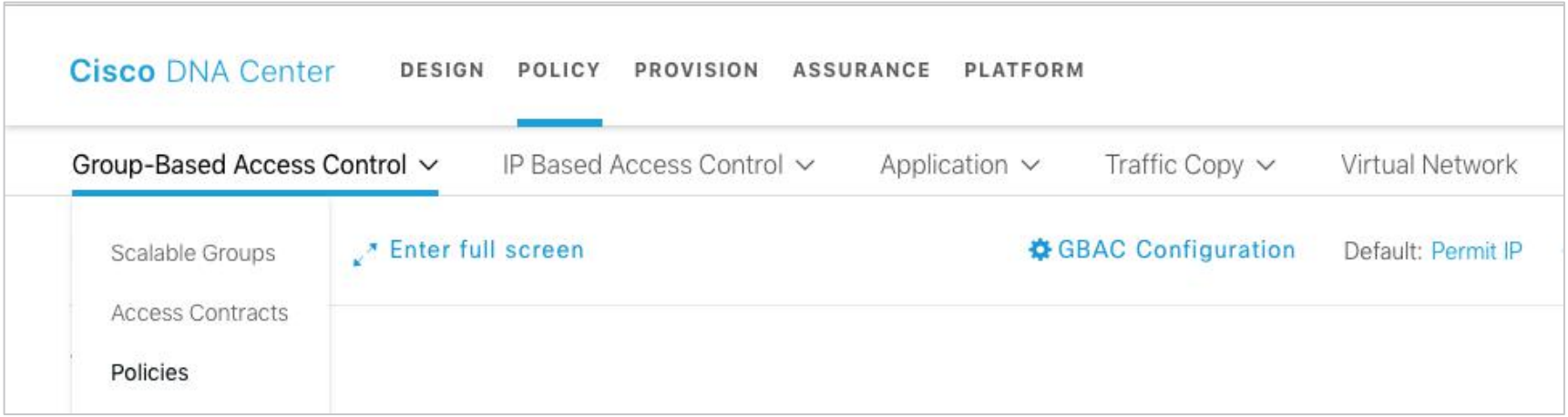
Scalable Groups – A Closer Look

Scalable Group is a logical ID object to “group” Users and/or Devices

- CTS uses “Scalable Groups” to ID and assign a unique Scalable Group Tag (SGT) to Host Pools
- Nodes add SGT to the Fabric encapsulation
- CTS SGTs used to manage address-independent “Group-Based Policies”
- Edge or Border Nodes use SGT to enforce local Scalable Group ACLs (SGACLs)



Enhanced policy capabilities from DNAC 1.3.1



- Group-Based Access Control located under top-level Policy item
- 3 pages: Scalable Groups, Access Contracts, Policies
- Landing page is Policies (Matrix view)
- NOTE: Virtual Network management page is related
  - VN admin can also associate Scalable Groups and VNs

Managing Scalable Groups

Scalable Groups (24)

Filter | Actions | Deploy

Name	Tag Value	Description
AP_EMR_EPG	10004/0x2714	Learned from APIC. Suffix: _EPG Ap
AP_Services_EPG	10003/0x2713	Learned from APIC. Suffix: _EPG Ap
Auditors	9/0x9	Auditor Security Group
BYOD	15/0xf	BYOD Security Group

Policies

The below table shows the access control rules this scalable group is referenced in and which policy it belongs to.

Source Scalable Group	Destination Scalable Group	Contract
Network_Services	Auditors	Permit IP
Quarantined_Systems	Auditors	Deny IP
Auditors	Network_Services	Anti_Malware

Showing 3 of 3

- List of all Scalable Groups
  - Standard DNAC table
  - Learned From shows is learned from ACI
  - Policies shows # of policies using group (link shows detailed list)
- Deploy triggers Environment Data download from ISE to network

Creating/Editing Scalable Groups

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Group-Based Access Control | IP Based Access Control | Application | Traffic Copy | Virtual N

Scalable Groups (55) Last updated: 12:23 PM

Filter | Actions | Deploy

Name	Tag Value	Description	Deployed
A_Division	23/0x17	Business division A	No
Alpha_Partner	33/0x21	Partner Alpha	No
Auditors	9/0x9	Auditor Security Group	Yes
B_Division	24/0x18	Business Group B	Yes
Beta_Partner	34/0x22	Partner Beta	No
BYOD	15/0xf	BYOD Security Group	Yes
C_Division	25/0x19	Business Group C	Yes
Contractors	5/0x5	Contractor Security Group	Yes

Create Scalable Group

Name*
New_Group_1

Tag Value (decimal)*
54

Description (optional)

Virtual Networks*
DEFAULT_VN

Propagate to ACI

Cancel Save

- Scalable Group Name required (format dictated by NAD limitations)
- Tag value generated, may be specified by admin when creating (cannot be edited afterwards)
- Optional description
- SG associated with “Default VN” by default, admin may associate with any other VNs (one or more)
- ”Propagate to ACI” option

Managing Access Contracts

Access Contracts (14)

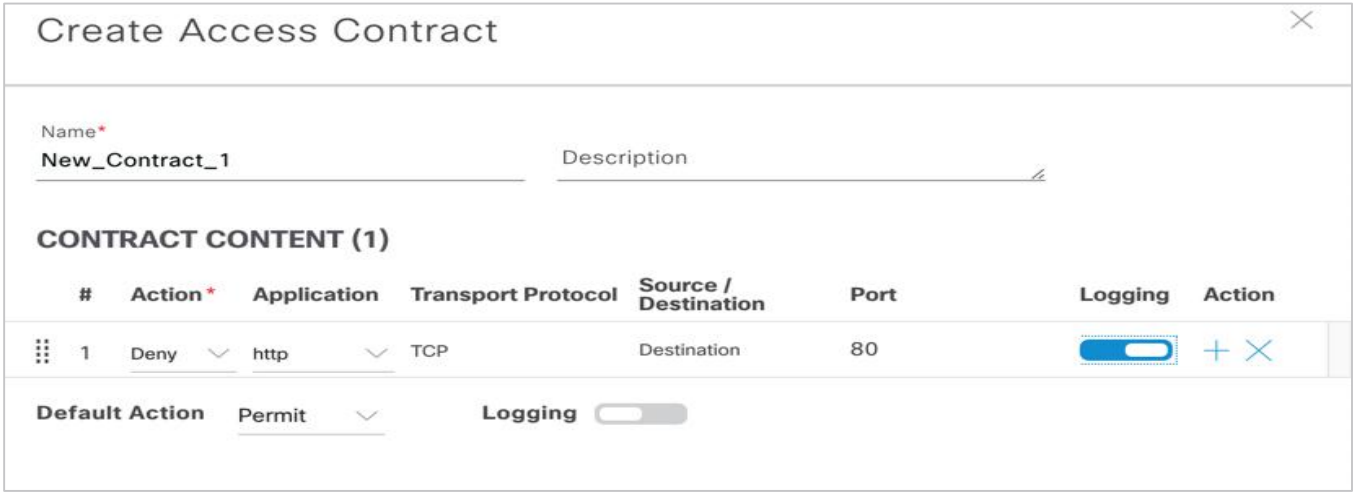
Last updated: 12:59 PM | Refresh | Create Access Contract

Filter | Actions | Deploy | Find

Name	Description	Rules Count	Deployed	Policies
AllowDHCPDNS	Sample contract to allow DHCP and DNS	2	Yes	0
AllowWeb	Sample contract to allow access to Web	2	Yes	0
Allow_Web_Ret	Permit web traffic FROM web servers to clients	2	Yes	0
Anti_Malware	Block services commonly used for horizontal attacks by malware	16	Yes	42

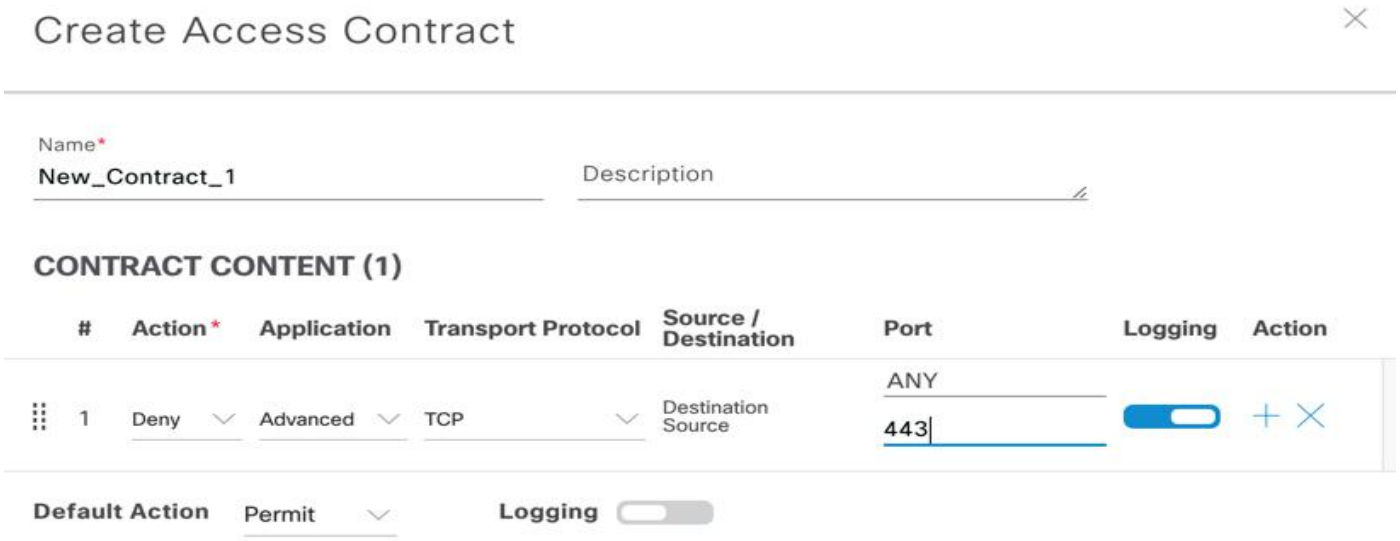
- List of all Access Contracts
  - Standard DNAC table
  - Rules Count shows # of ACE lines
  - Policies shows # of policies using group (link shows detailed list)
- Deploy triggers policy download from ISE to network

Creating/Editing Access Contracts



- Name required (format dictated by NAD limitations), Description opt.
- ACE lines modeled: permit/deny pulldown, Application selection
- Option to add LOG keyword
- ACE lines may be added, inserted, deleted, re-ordered
- Default Action (Catch-All Rule) permit/deny, w optional LOG keyword

Creating/Editing Access Contracts Continued



- Option to select “Advanced” as Application option
- Able to specify Transport Protocol (TCP, UDP, TCP/UDP, ICMP)
- Able to specify Source & Destination ports directly

Cisco SD-Access Group-Based Access Control Policy View (Matrix View)

Cisco DNA Center DESIGN POLICY PROVISION

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

Policies (64) Enter full screen

GBAC Configuration Default: Permit IP Create Policies

Filter Deploy

Permit Deny Custom Default

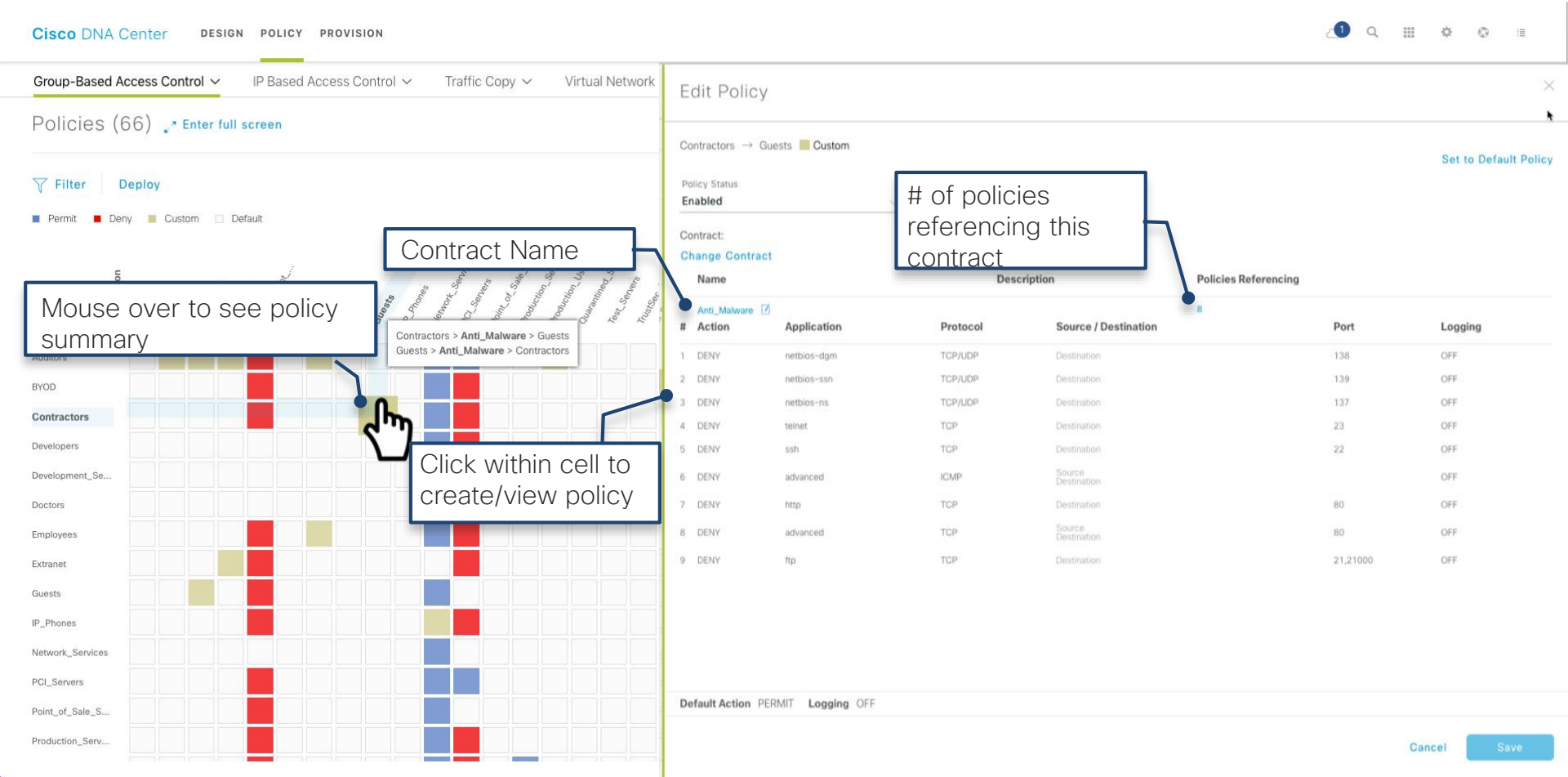
Destination: Auditors, BYOD, Contractors, Developers, Development_..., Doctors, Employees, Extranet, Guests, IP_Phones, Network_Servi..., PCI_Servers, Point_of_Sale_..., Production_Ser..., Production_Us..., Quarantined_S..., Test_Servers, TrustSec_Devic..., Unknown

Source: Auditors, BYOD, Contractors, Developers, Development_Se..., Doctors, Employees, Extranet, Guests, IP_Phones, Network_Services, PCI_Servers, Point_of_Sale_S..., Production_Serv..., Production_Users

Minimap to aid navigation in matrix

Collapse Minimap

Cisco SD-Access Group-Based Access Control Policy View (Matrix View) cont..



Cisco SD-Access Group based access control Policy View (Matrix View) cont..

Cisco DNA Center DESIGN POLICY PROVISION

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

Policies (66) Enter full screen

Filter Deploy

Permit Deny Custom Default

Click to edit contract

Contractors > **Anti_Malware** > Guests
Guests > **Anti_Malware** > Contractors

Destination: Auditors, BYOD, Contractors, Developers, Development_..., Doctors, Employees, Extranet, Guests, IP_Phones, Network_Servi..., PCI_Servers, Point_of_Sale_..., Production_Ser..., Production_Us..., Quarantined_S..., Test_Servers

Source: Auditors, BYOD, Contractors, Developers, Development_Se..., Doctors, Employees, Extranet, Guests, IP_Phones, Network_Services, PCI_Servers, Point_of_Sale_S..., Production_Serv...

Edit Access Contract

Name* Anti_Malware

Description Block ports commonly exploited by

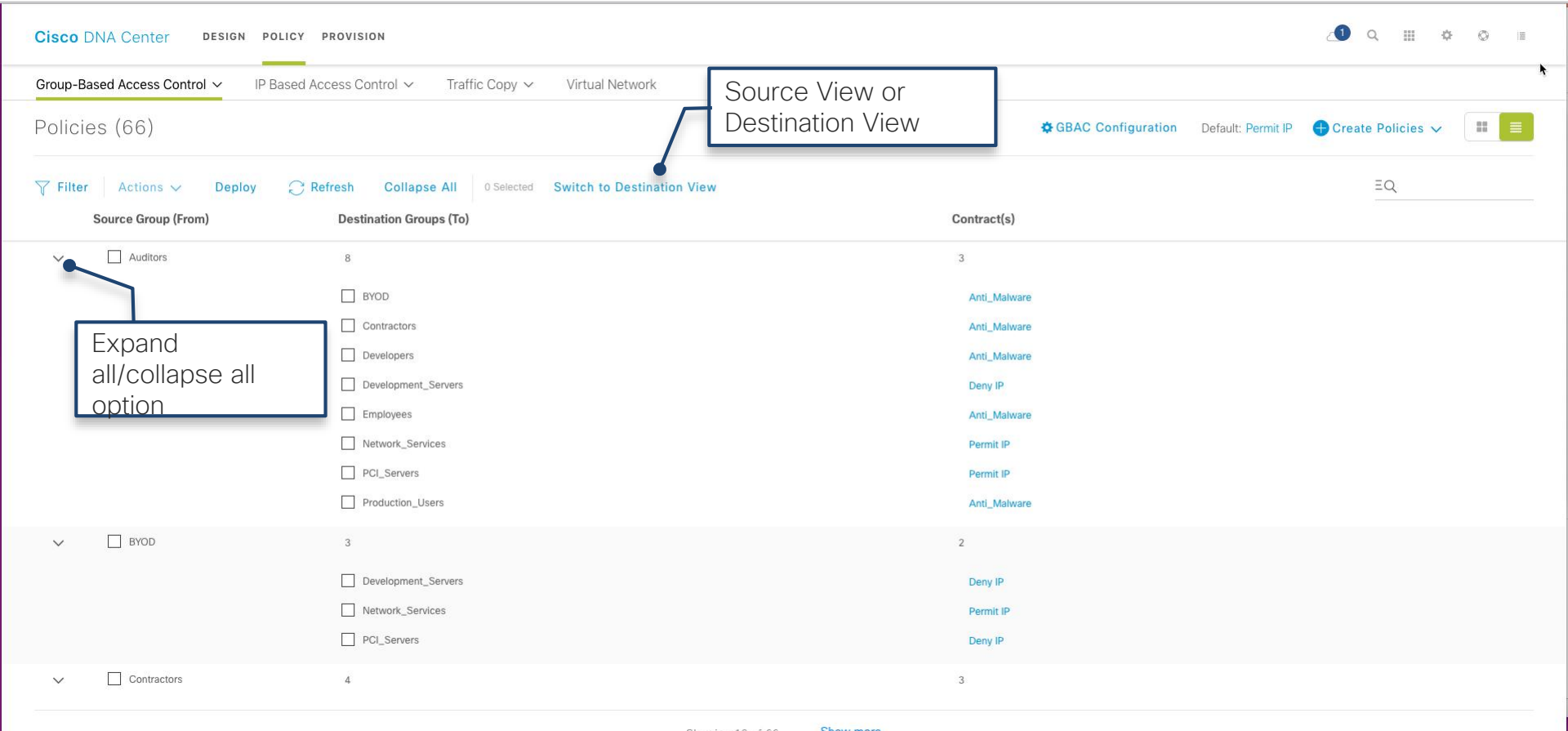
CONTRACT CONTENT (62)

#	Action*	Application	Transport Protocol	Source / Destination	Port	Logging	Action
1	Deny	Advanced	TCP	Destination Source	138 ANY		+ ×
2	Deny	Advanced	TCP	Destination Source	138 ANY		+ ×
3	Deny	Advanced	UDP	Destination Source	138 ANY		+ ×
4	Deny	Advanced	UDP	Destination Source	138 ANY		+ ×
5	Deny	Advanced	TCP	Destination Source	139 ANY		+ ×
6	Deny	Advanced	TCP	Destination Source	139 ANY		+ ×
7	Deny	Advanced	UDP	Destination Source	139 ANY		+ ×
8	Deny	Advanced	UDP	Destination Source	139 ANY		+ ×

Default Action Permit Logging

Cancel Save

Cisco SD-Access Group-Based Access Control Policy View (List View)



Cisco SD-Access Group-Based Access Control Policy View (List View) cont..

Cisco DNA Center DESIGN POLICY PROVISION

Group-Based Access Control IP Based Access Control Traffic Copy Virtual Netw

Policies (66)

Filter Actions Deploy Refresh Collapse All 0 Selected Switch to De

Source Group (From)	Destination Groups (To)
Auditors	8
	BYOD
	Contractors
	Developers
	Development_Servers
	Employees
	Network_Services
	PCI_Servers
	Production_Users
BYOD	3
	Development_Servers
	Network_Services
	PCI_Servers
Contractors	4

View Access Contract

Name
Anti_Malware

Description

CONTRACT CONTENT (9)

#	Act	Application	Transport Protocol	Source / Destination	Port	Logging
1	Den	netbios-dgm	TCP/UDP	Destination	138/138	OFF
2	Den	netbios-ssn	TCP/UDP	Destination	139/139	OFF
3	Deny	netbios-ns	TCP/UDP	Destination	137/137	OFF
4	Deny	tc	TCP	Destination	23	OFF
5	Deny	ssh	TCP	Destination	22	OFF
6	Deny	Advanced	ICMP	–	–	OFF
7	Deny	http	TCP	Destination	80	OFF
8	Deny	Advanced	TCP	Destination Source	ANY 80	OFF
9	Deny	ftp	TCP	Destination	21,21000	OFF

Click to edit contract

Default Action Permit Logging OFF

Cancel Edit

Policy Migration / Sync with ISE

Cisco DNA Center DESIGN POLICY PROVISION

In order to begin using Group Based Access Control, Cisco DNA Center must migrate policy data from the Cisco Identity Services Engine (ISE):

- Any policy features in ISE that currently not supported in Cisco DNA Center will not be migrated, you will a chance to review the migration rule after click
- Any policy information in Cisco DNA Center not already exist in ISE will be copied to ISE to ensure the 2 sources are in sync

Once the data migration is initiated, you cannot use Group Based Access Control in Cisco DNA Center until the operation is complete. Start migration

Start Migration

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

Policies (0) Enter full screen GBAC Configuration Default: Permit IP Create Policies

Filter Deploy

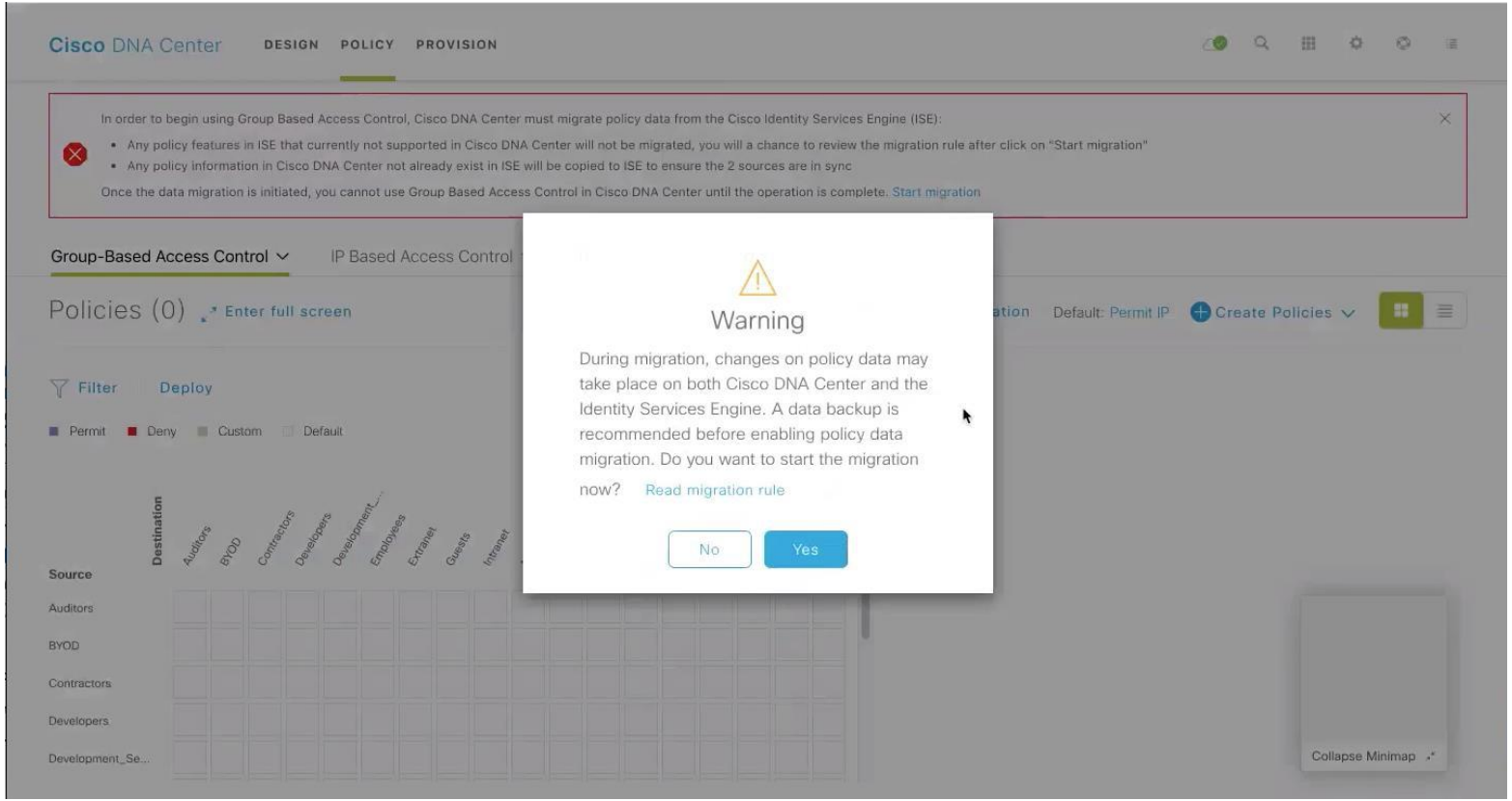
Permit Deny Custom Default

Destination: Auditors, BYOD, Contractors, Developers, Development_..., Employees, Extranet, Guests, Intranet, Network_Servi..., PCI_Servers, Point_of_Sale_..., Production_Ser..., Production_Us..., Quarantined_S..., Test_Servers, TrustSec_Devic..., Unknw...

Source: Auditors, BYOD, Contractors, Developers, Development_Se...

Collapse Minimap

Policy Migration / Sync with ISE



Policy Migration / Sync with ISE

Cisco DNA Center DESIGN POLICY PROVISION

Migration in progress. You cannot interact with Group Based Access Control until the operation is finished. It might take a few mintues to more than an hour.

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

Policies (0) Enter full screen GBAC Configuration Default: Permit IP Create Policies

Filter Deploy

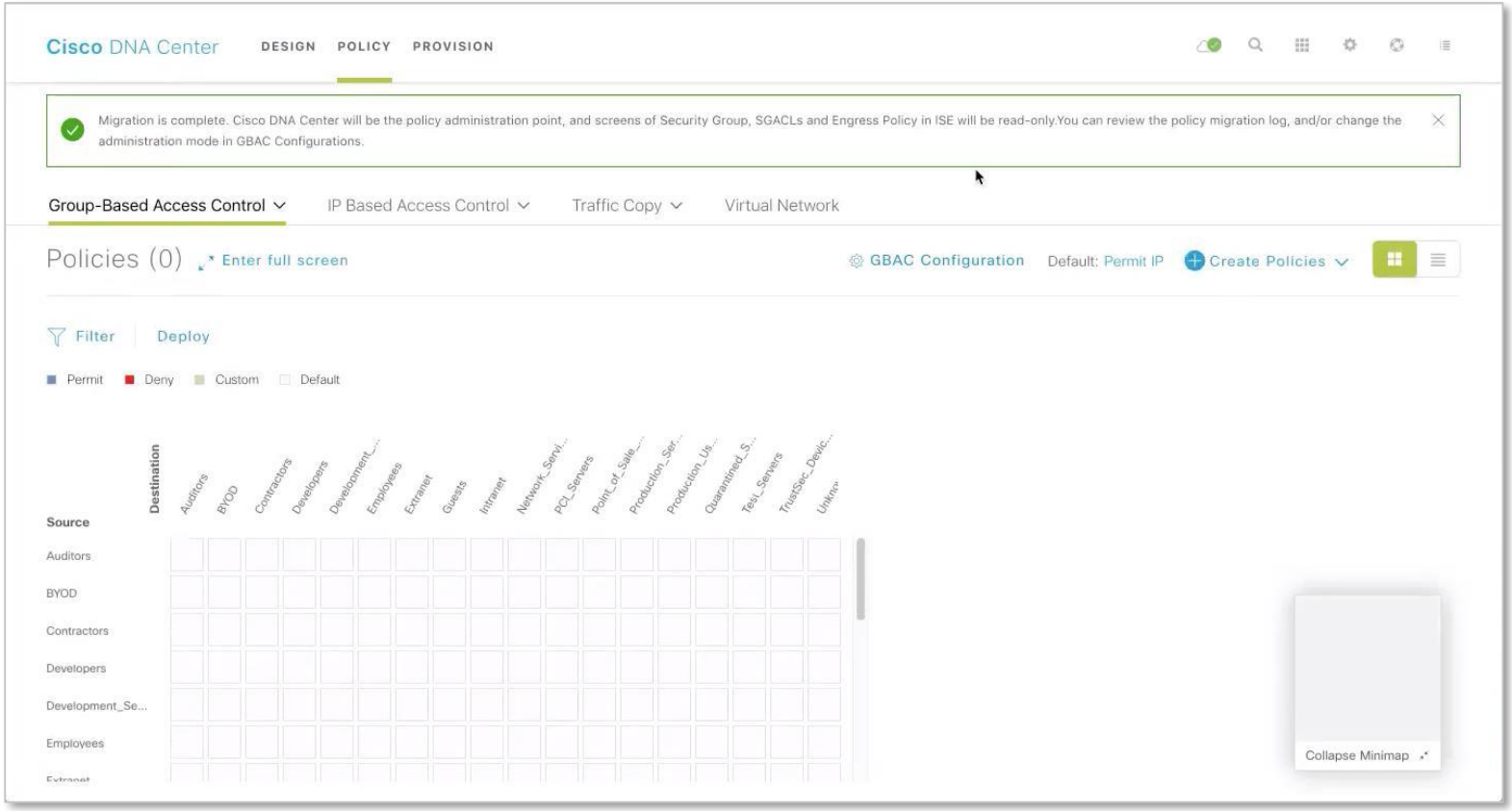
Permit Deny Custom Default

Destination: Auditors, BYOD, Contractors, Developers, Development_..., Employees, Extranet, Guests, Intranet, Network_Servi..., PCI_Servers, Point_of_Sale_..., Production_Sec..., Production_Us..., Quarantined_S..., Test_Servers, TrustSec_Devic..., Unknw

Source: Auditors, BYOD, Contractors, Developers, Development_Se..., Employees, Extranet

Collapse Minimap

Policy Migration / Sync with ISE



ISE: TrustSec UIs READ ONLY (Security Groups, SGACLs, Policy)

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

Network Access | Guest Access | TrustSec | BYOD | Profiler | Posture | Device Administration | PassiveID

Overview | Components | TrustSec Policy | Policy Sets | SXP | Troubleshoot | Reports | Settings

Introduction

Dashboard

TrustSec Overview

Cisco DNA Center is managing TrustSec Security Groups, SGACL's and Egress Policy, those screens are Read Only.

Prepare 1

Plan Security Groups
Identify resources that require different levels of protection

Classify the users or clients that will access those resources

Objective is to identify the minimum required number of Security Groups, as this will simplify management of the matrix

Preliminary Setup
Set up the TrustSec AAA server.

Set up TrustSec network devices.

Check default TrustSec settings to make sure they are acceptable.

If relevant, set up TrustSec-ACI policy group exchange to enable consistent policy across

Define 2

Create Components
Create security groups for resources, user groups and Network Devices as defined in the preparation phase. Also, examine if default SGTs can be used to match the roles defined.

Define the network device authorization policy by assigning SGTs to network devices.

Policy
Define SGACLs to specify egress policy.

Assign SGACLs to cells within the matrix to enforce security.

Exchange Policy
Configure SXP to allow distribution of IP to SGT mappings directly to TrustSec enforcement devices.

Go Live & Monitor 3

Push Policy
Push the matrix policy live.

Push the SGTs, SGACLs and the matrix to the network devices

Real-time Monitoring
Check dashboards to monitor current access.

Auditing
Examine reports to check access and authorization is as intended.

ISE: TS UIs RO!

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration

Network Access | Guest Access | TrustSec | BYOD | Profiler | Posture | Device Administration | Passiv

Overview | Components | TrustSec Policy | Policy Sets | SXP | Troubleshoot | Reports | Settings

- Security Groups
- IP SGT Static Mapping
- Security Group ACLs
- Network Devices
- Trustsec AAA Servers

Security Groups

For Policy Export go to Administration > System > Backup & Restore > Policy Export P

Managed by Cisco DNA Center

Edit | Add | Import | Export | Trash | Pus

Icon	Name	SGT (Dec / Hex)
	Alpha_Partner	33/0021
	Auditors	9/0009
	A_Division	23/0017
	Beta_Partner	34/0022
	BYOD	15/000F
	B_Division	24/0018

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Network Access | Guest Access | TrustSec | BYOD | Profiler | Posture | Device Administration | PassiveID

Overview | Components | TrustSec Policy | Policy Sets | SXP | Troubleshoot | Reports | Settings

- Security Groups
- IP SGT Static Mapping
- Security Group ACLs
- Network Devices
- Trustsec AAA Servers

Security Groups List > Alpha_Partner

Security Groups

* Name

Alpha_Partner

* Icon

Description

Partner Alpha

☑ Propagate to ACI

Security Group Tag (Dec / Hex): 33/0021

Generation Id: 7

Associated Virtual Networks and Subnet/IP Address Pools

Virtual Network Name	Subnet/IP Address Pool Name	Type	Is
Production_VN			fal

Managed by Cisco DNA Center

Save | Reset

ISE TrustSec UI RO Override

FOR EMERGENCY USE ONLY

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | 1 | License Warning

Network Access | Guest Access | TrustSec | BYOD | Profiler | Posture | Device Administration | PassiveID

Overview | Components | TrustSec Policy | Policy Sets | SXP | Troubleshoot | Reports | Settings

- General TrustSec Settings
- TrustSec Matrix Settings
- Work Process Settings
- SXP Settings
- ACI Settings

☐ Auto Create Security Groups When Creating Authorization Rules

☐ SGT Number Range For Auto-Creation - From 5,000 To 5,100

Automatic Naming Options

Select basis for names. (Security Group name will be shortened to 32 characters)

Name Will Include: Rule Name

Optional Additions: ☐ Policy Set Name ☐ Prefix SGT ☐ Suffix SGT

Example Name - *RuleName*

IP SGT static mapping of hostnames

◉ Create mappings for all IP addresses returned by DNS query

○ Create mappings only for the first IPv4 address and the first IPv6 address returned by DNS query

Cisco DNA Center Control of TrustSec Policy

☐ Override Cisco DNA Center Control of TrustSec Policy

Save | Reset

User mobility

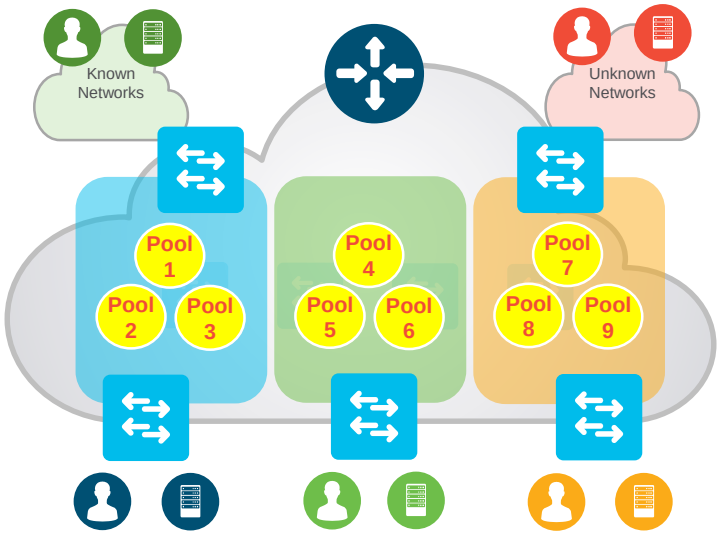
IP pools, anycast gateway, stretched subnets

SD-Access Fabric

Host Pools – A Closer Look

Host Pool provides basic IP functions necessary for attached Endpoints

- Edge Nodes use a Switch Virtual Interface (SVI), with IP Address /Mask, etc. per Host Pool
- Fabric uses Dynamic EID mapping to advertise each Host Pool (per Instance ID)
- Fabric Dynamic EID allows Host-specific (/32, /128, MAC) advertisement and mobility
- Host Pools can be assigned Dynamically (via Host Authentication) and/or Statically (per port)

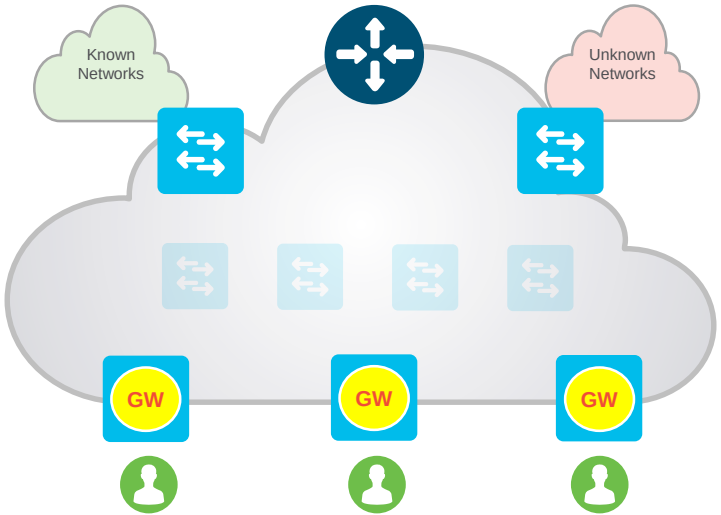


SD-Access Fabric

Virtual Network– A Closer Look

Anycast GW provides a single L3 Default Gateway for IP capable endpoints

- Similar principles and behavior as HSRP / VRRP with a shared Virtual IP and MAC address
- The same Switch Virtual Interface (SVI) is present on EVERY Edge, with the same Virtual IP and MAC
- Control-Plane with Fabric Dynamic EID mapping creates a Host (Endpoint) to Edge relationship
- If (when) a Host moves from Edge 1 to Edge 2, it does not need to change it's IP Default Gateway!

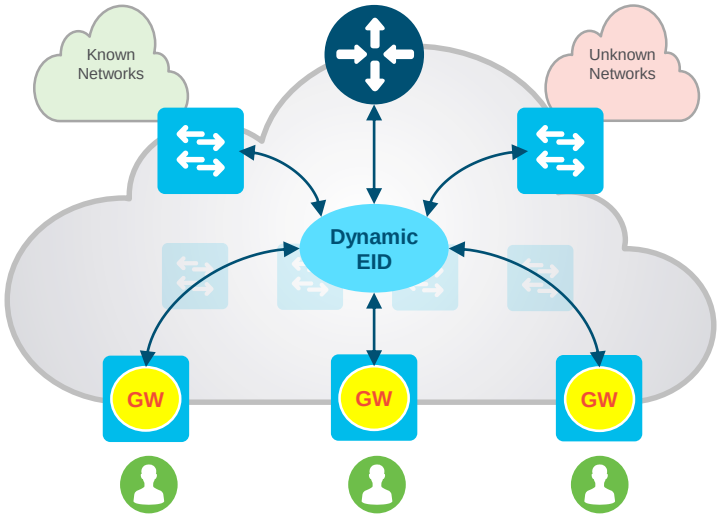


SD-Access Fabric

Endpoint ID Groups – A Closer Look

Stretched Subnets allow an IP subnet to be “stretched” via the overlay

- Host IP based traffic arrives on the local Fabric Edge SVI, and is then transferred by Fabric
- Fabric Dynamic EID mapping allows Host-specific (/32, /128, MAC) advertisement and mobility
- Host 1 connected to Edge A can now use the same IP subnet to communicate with Host 2 on Edge B.
- No longer need a VLAN to connect Host 1 and 2 for IP

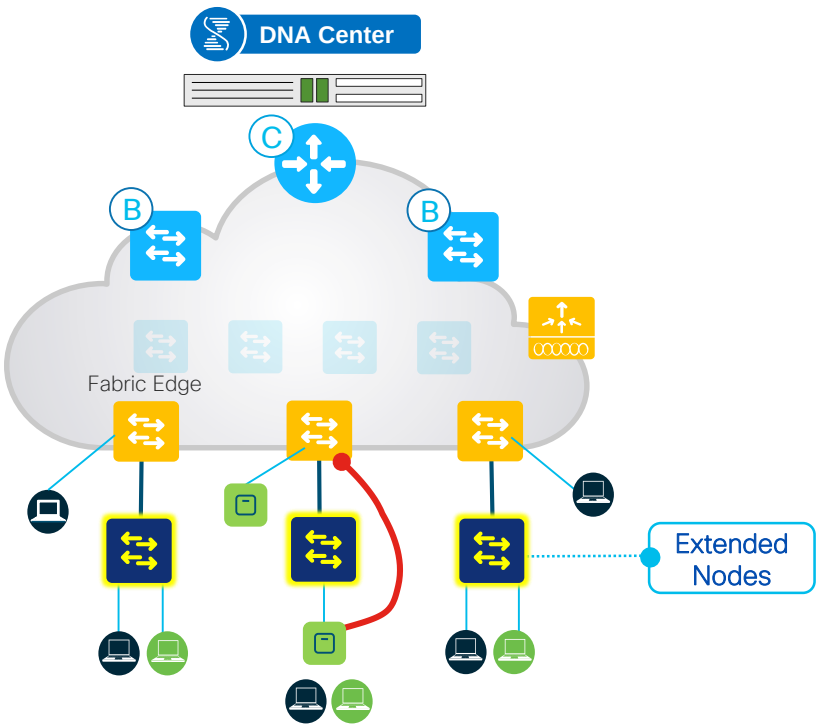


IoT integration

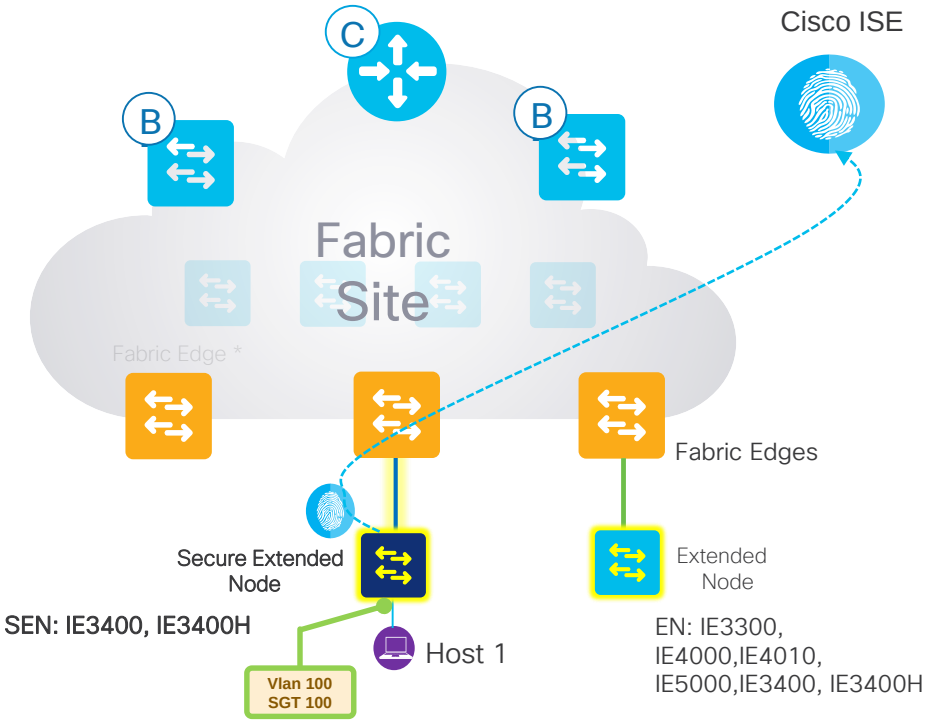
Extended and Secure Extended Node

SD-Access Extended Node

- **Extended node** connects to a single **Edge node** using an **802.1Q Trunk port** (single or multiple VLANs) using static assignment
- Switchports on the Extended node can then be **statically assigned** to an **appropriate IP Pool** (in DNA Center)
- **SGT tagging** (or mapping) is accomplished by **Pool to Group mapping** (in DNA Center) on the connected Edge node
- Traffic **policy enforcement** based on SGTs (SGACLs) is **performed at the Edge node**
- **Supported platforms:** Catalyst 3560-CX, Catalyst Building Switch, IE4000, IE5000



Extended Nodes Enhancements



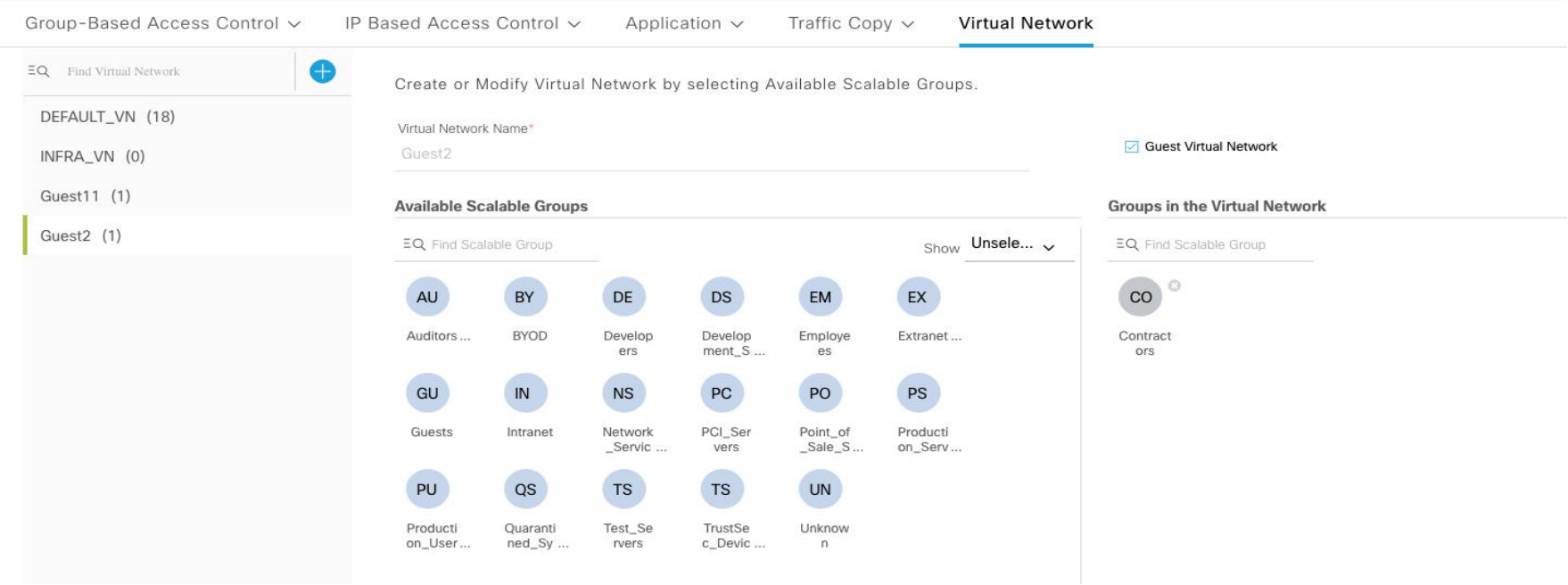
- The ***Secure Extended Node*** will have 802.1x/MAB Authentication enabled to talk to ISE and to download the right vlan and **Secure Group Tag** attributes to the end points.
- The ***Extended Node*** will have 802.1x/MAB Authentication enabled to talk to ISE and to download the right vlan for the end points.
- Secure Extended nodes gets provisioned with SGTs on the port channel interface(s) on which they are connected to Fabric Edge Switches

Guest Access

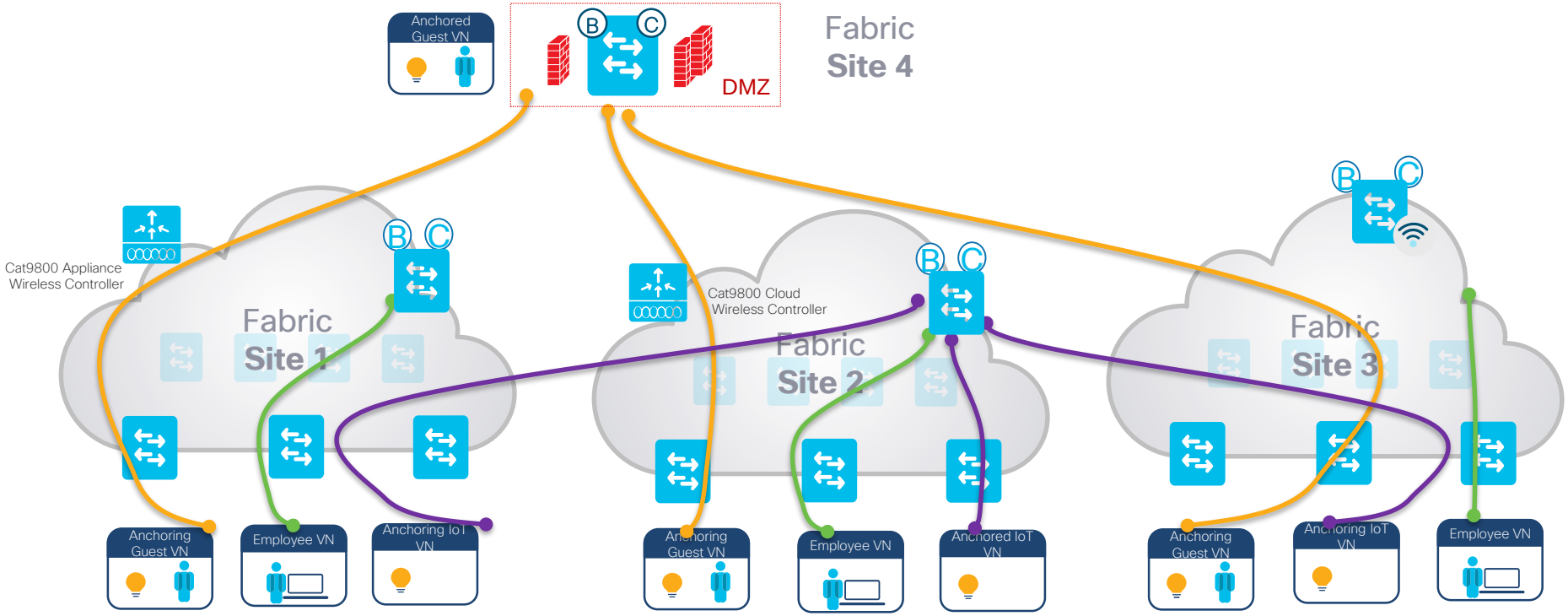
Automatic redirection to guest portal

Cisco SD-Access

Multiple VN for Guest Access in SD-Access



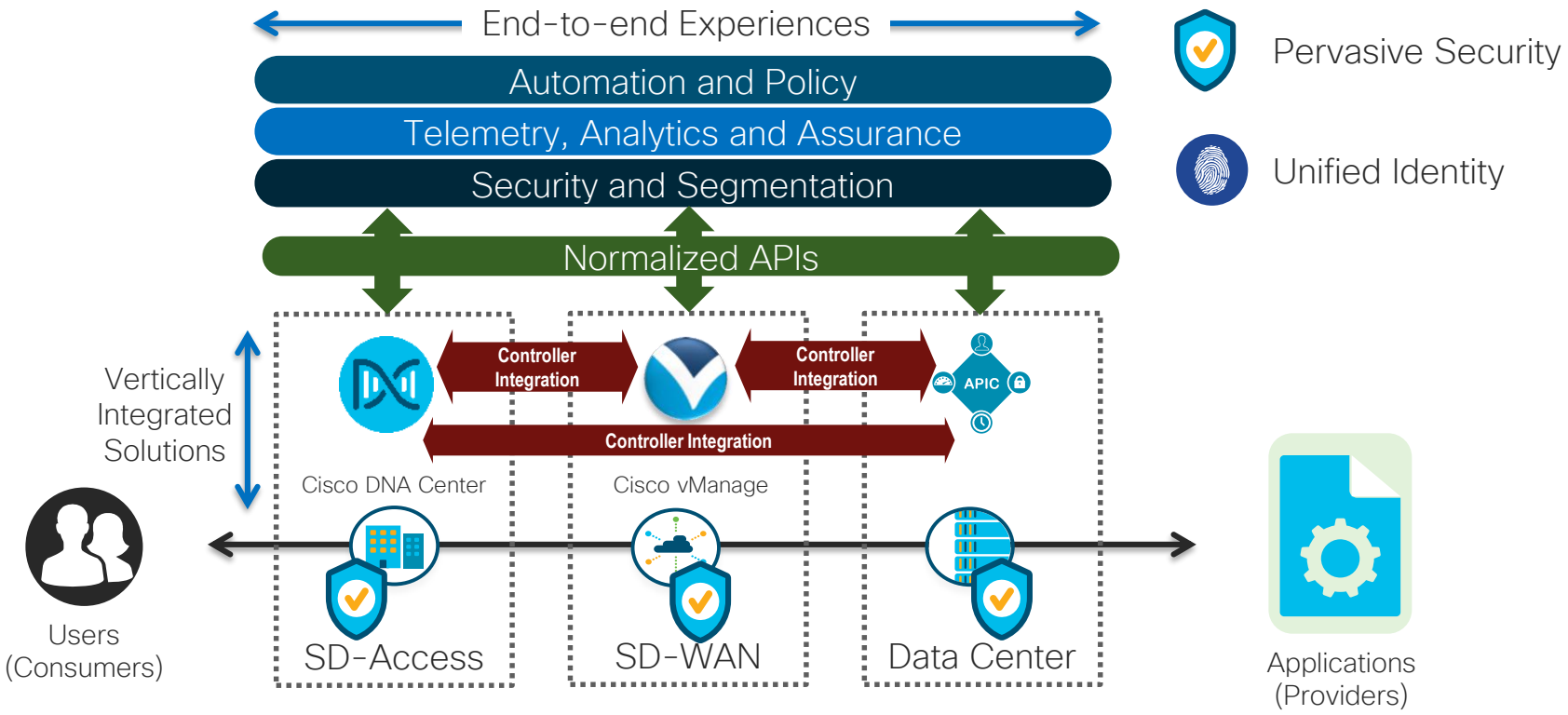
Cisco SD-Access VN Anchoring



Multidomain integration

Campus/DC/Branch network

Interconnecting Multi-Domain Networks



DC integration

Common policy across SDA and ACI domains

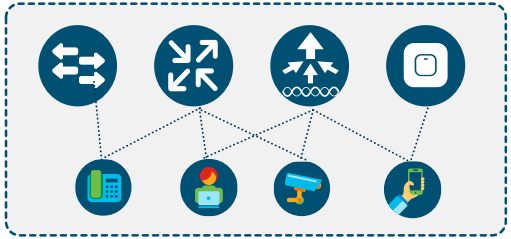
Consistent Policies from End to End

Identity Services Engine / DNA Center

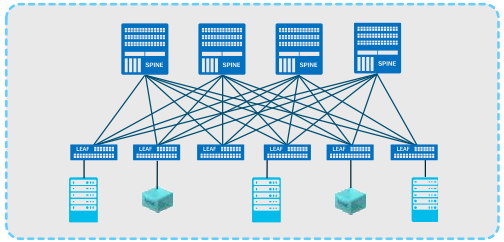
APIC-DC, Controller for ACI

Common Policy Groups

Campus & Branch Networks

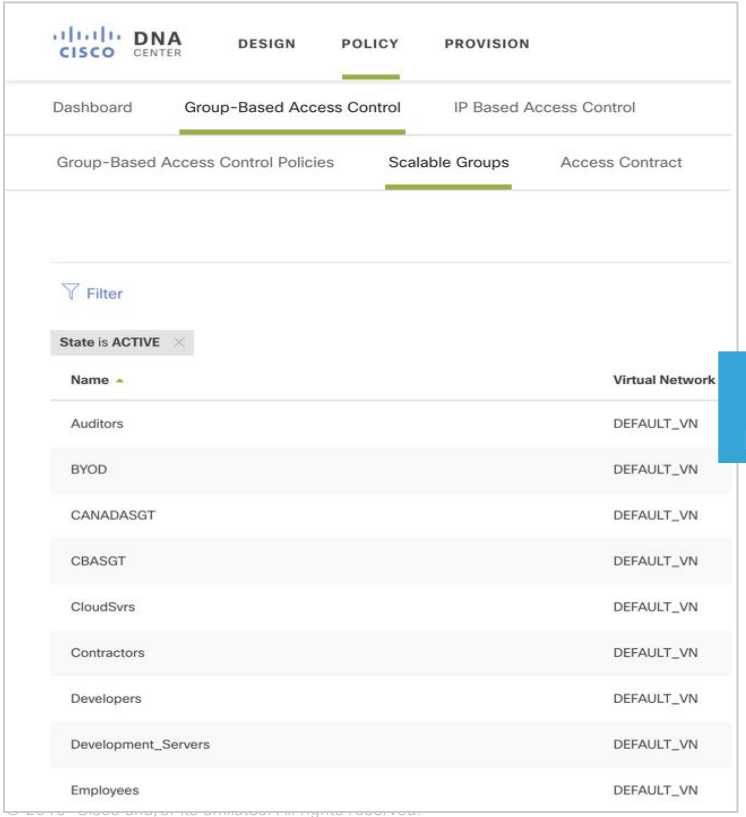


ACI DC/Cloud

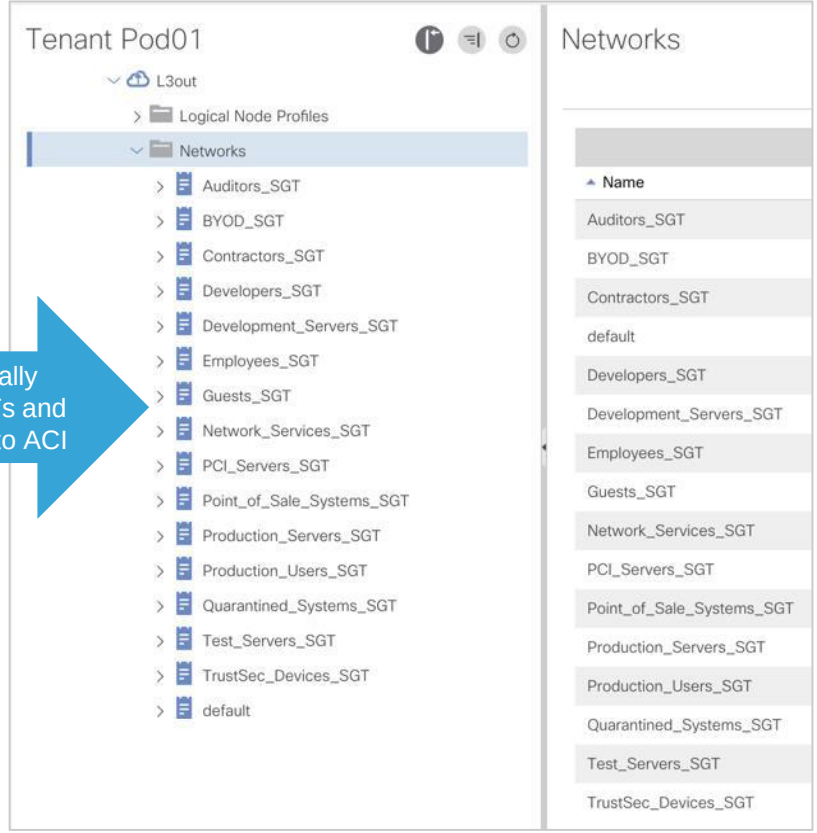


- Consistent Security Policy Groups in SDA and ACI domains
- Groups from SDA used in ACI policies, groups from ACI available in SDA policies

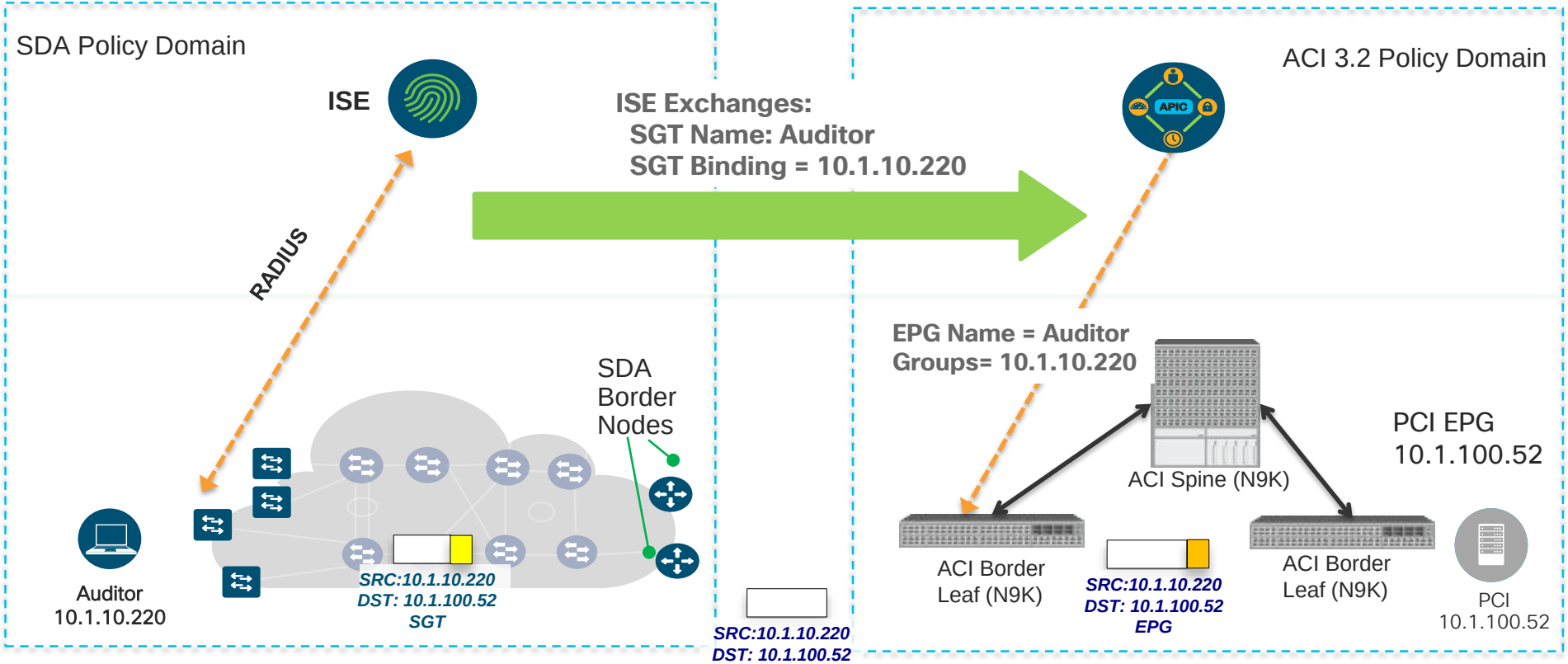
Groups Provisioned from SDA to ACI (by ISE)



ISE dynamically provisions SGTs and IP mappings into ACI

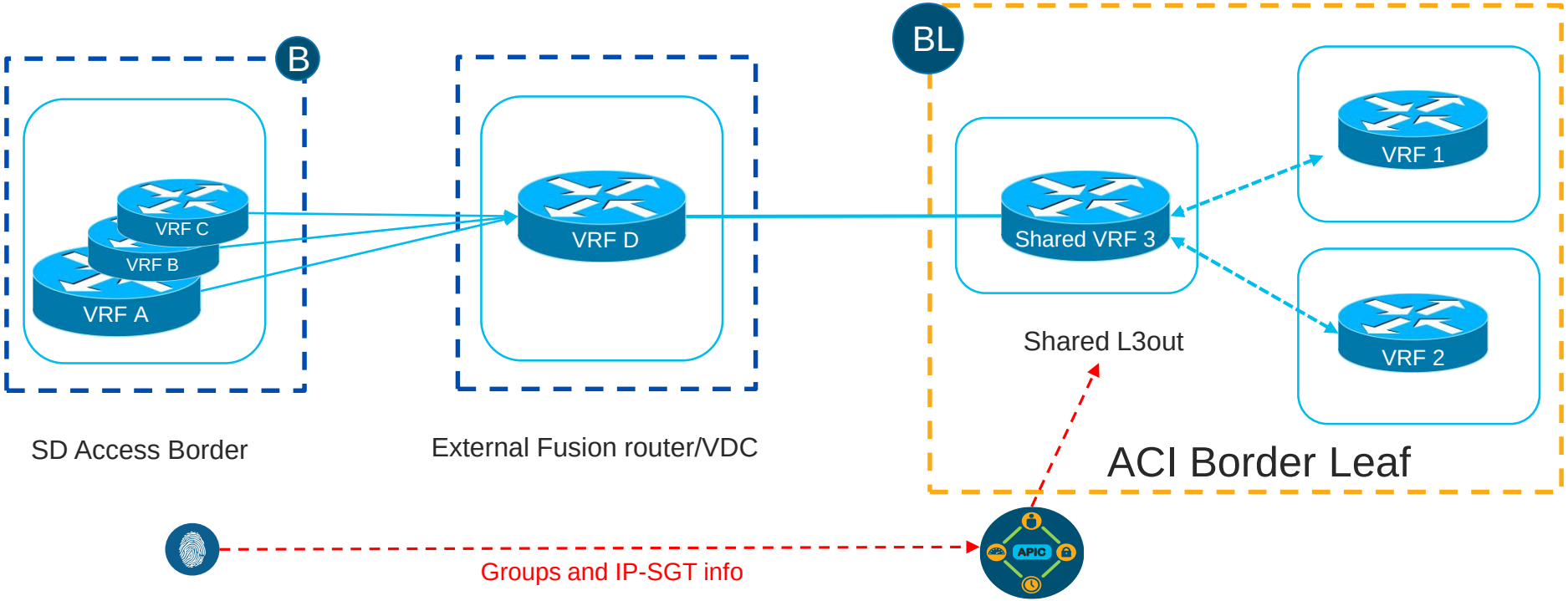


Groups from SDA Used in ACI



SGTs available in ACI Policies

Current Solution: Single VRF, Single Tenant



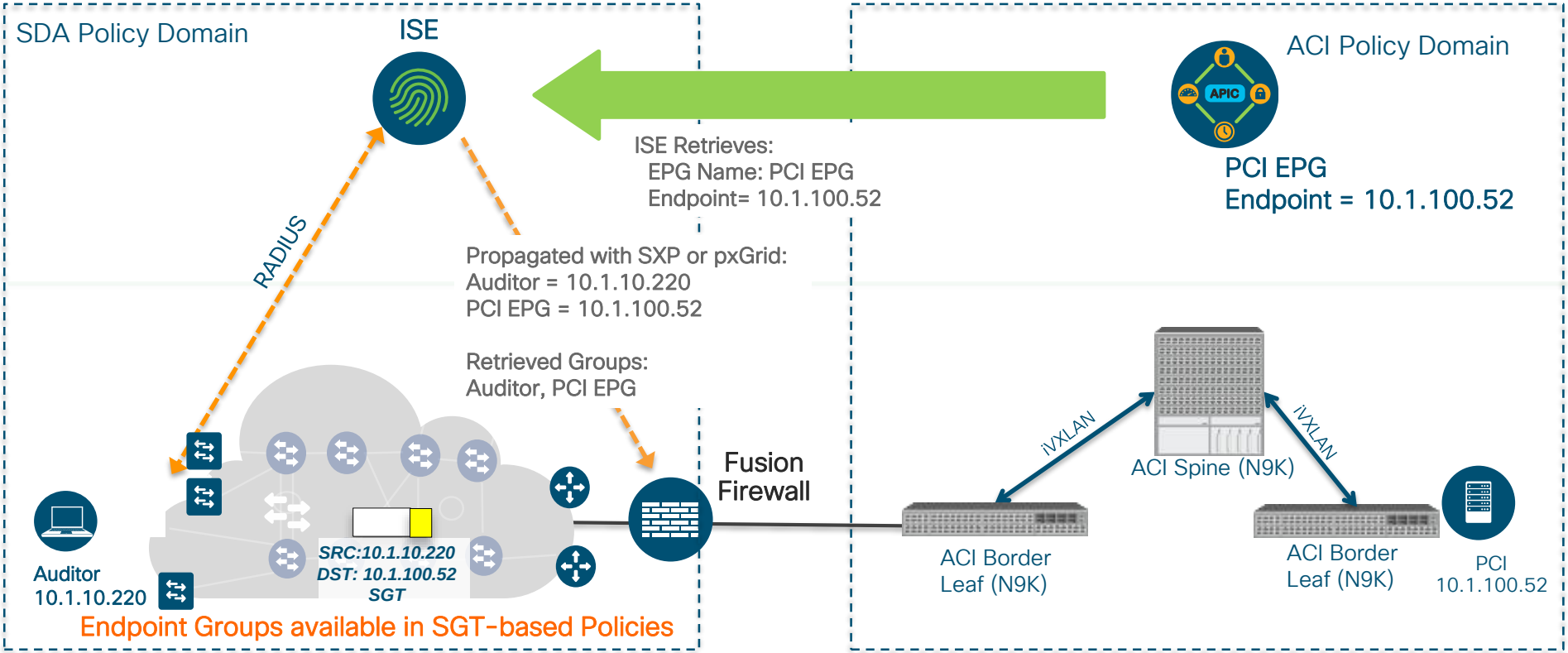
Please Note: Common tenant can be used mappings to provide to multiple tenants

SDA Learning Groups from ACI

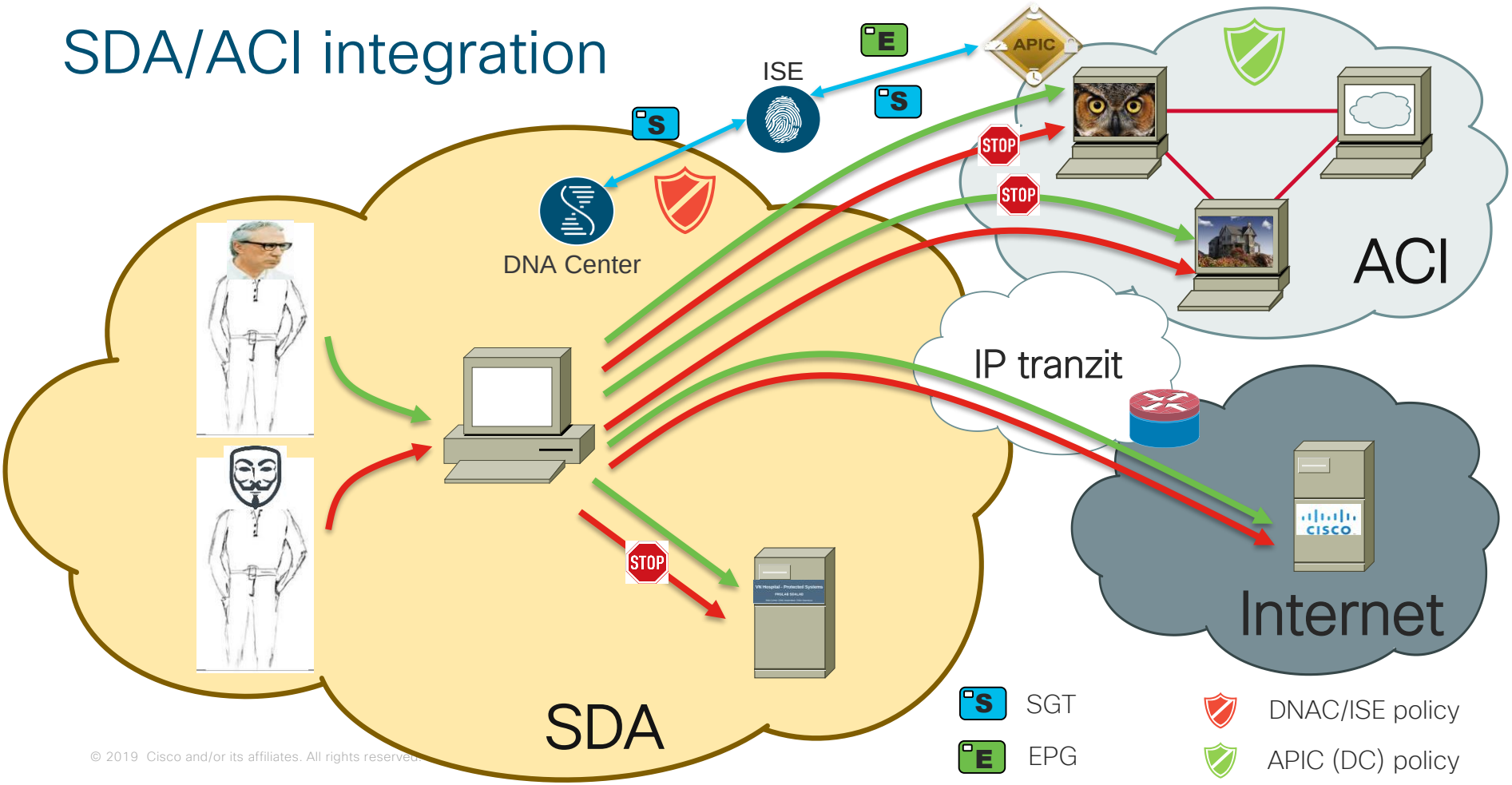
Group-Based Access Control Policies | **Scalable Groups**

Name
AP_DB_EPG
AP_Development_Svr_EPG
AP_HIPAA_Svr_EPG
AP_Medical_Records_EPG
AP_PCI_Svr_EPG
AP_production_app_EPG
AP_production_web_EPG

ACI Groups Used in SDA (Border or Fusion)



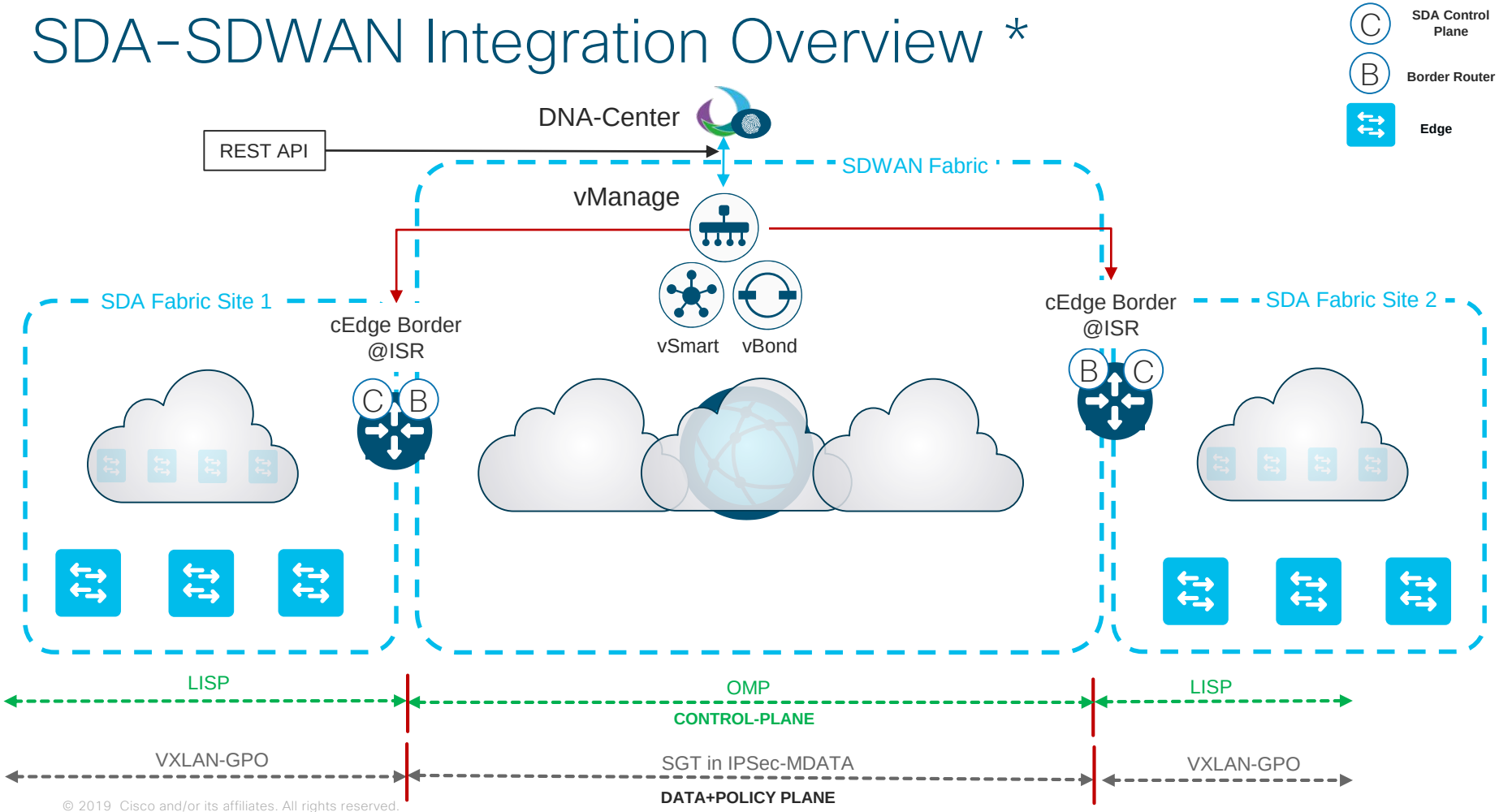
SDA/ACI integration



Branch network integration

Common policy across SDA and SDWAN domains

SDA-SDWAN Integration Overview *



* - roadmap

Software Defined Access

Supported platforms

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

NEW

Catalyst 9200

Catalyst 4500E

Catalyst 6800

Nexus 7700

Catalyst 3650 & 3850

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

AireOS Wave 1 APs*

AireOS Wave 2 APs

Extended

BETA

Cisco Digital Building

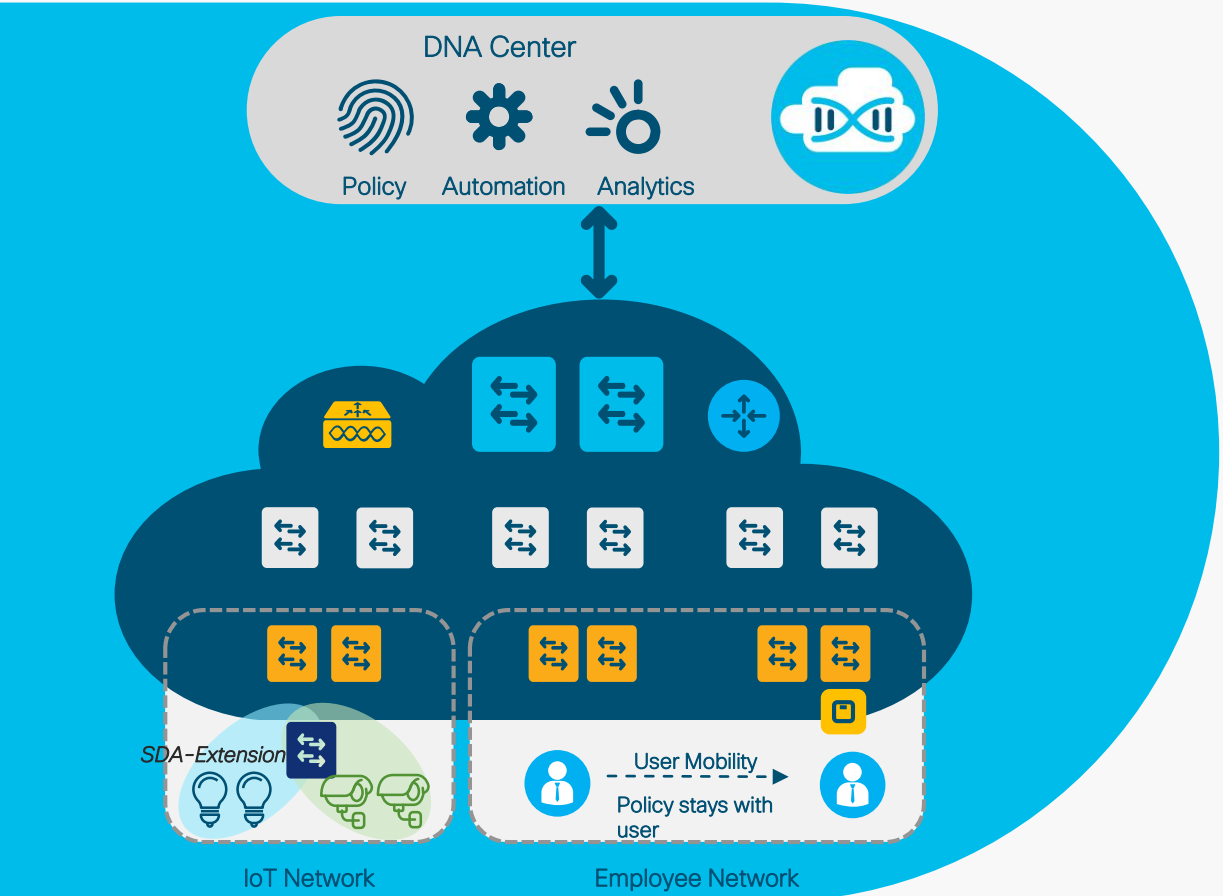
Catalyst 3560-CX

Cisco IE 3300, 3400, 4K/5K

Summary

Software-Defined Access

Networking at the speed of Software!



Identity-based Policy & Segmentation

Decoupled security policy definition from VLAN and IP Address

Automated Network Fabric

Single Fabric for Wired & Wireless with Workflow-based Automation

Insights & Telemetry

Analytics and insights into user and application behavior

Thank you.