

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Software-Defined Segmentation

Live Case Study Deep Dive

Amit Singh, TME – Cisco Validated
BRKENS-2823

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

Questions?

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

How

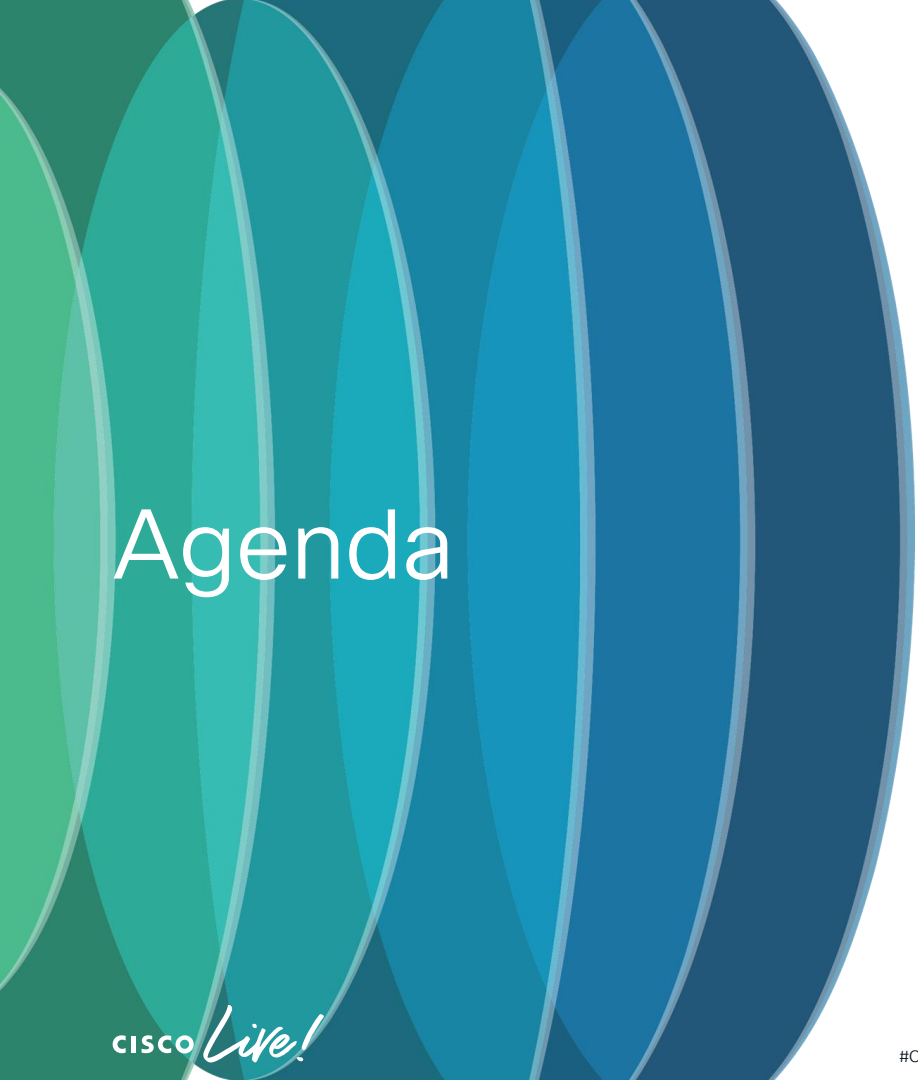
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2823>

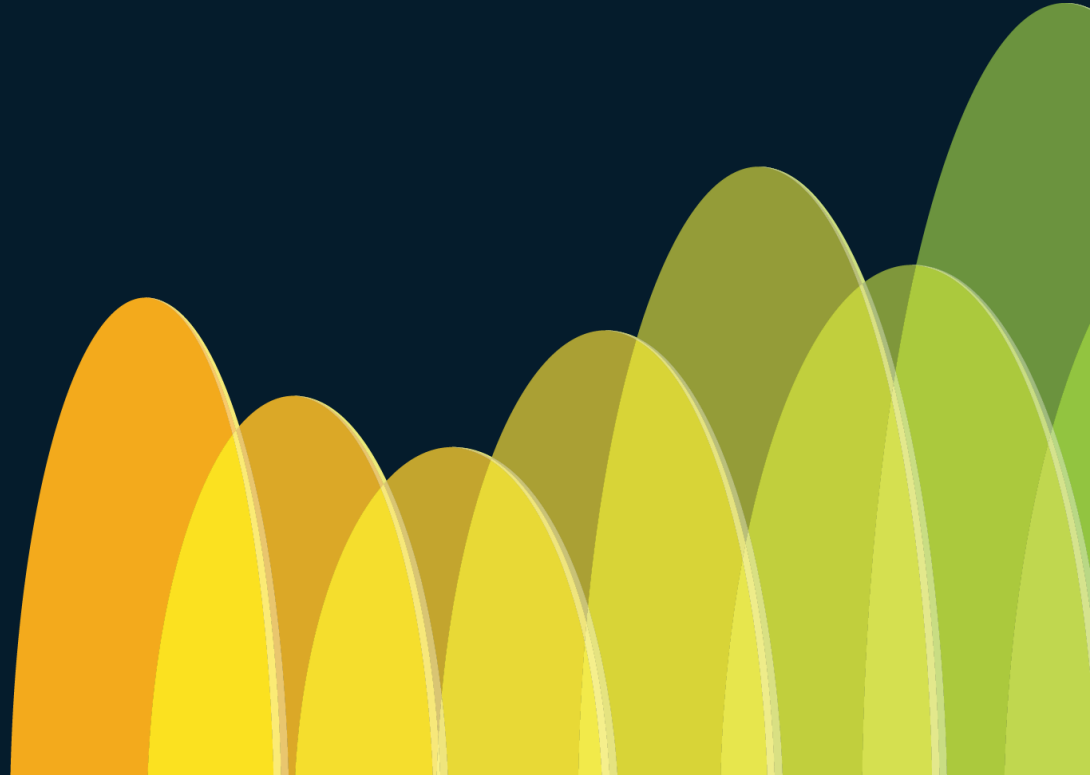




Agenda

- Introduction
- Case Study Environment
- Identity Service Engine (ISE)
- Catalyst Center SDA
- Meraki Adaptive Policy
- Catalyst SD-WAN TrustSec
- End-to-End Segmentation in multi-domain environment – Demo

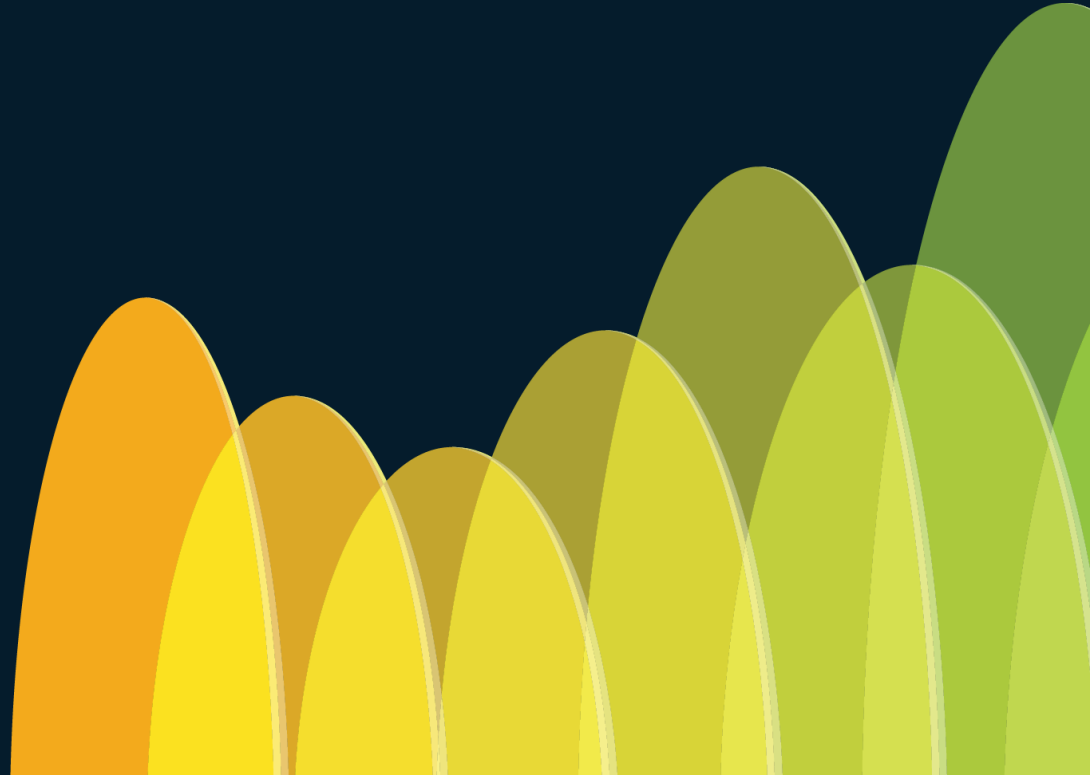
Introduction



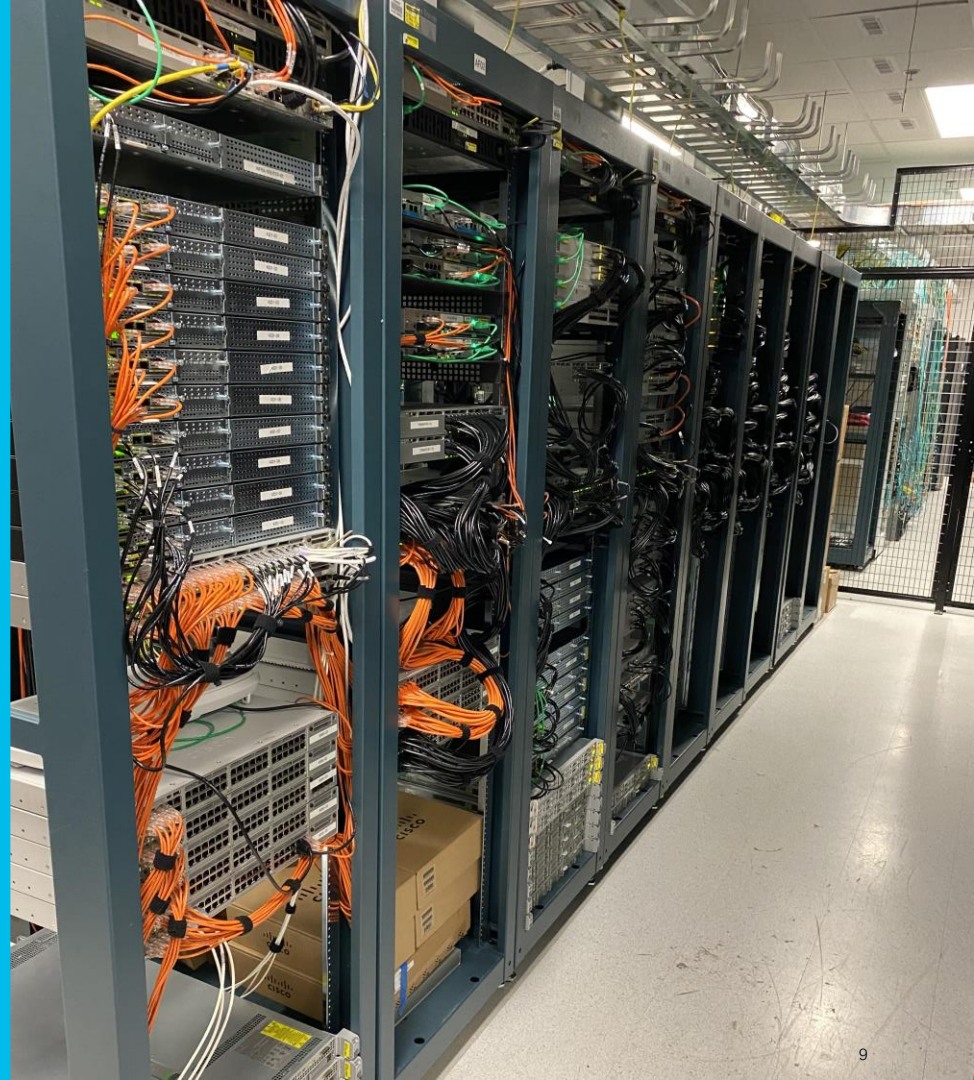
About this session

- This session is a case study on using software-defined segmentation to secure a hybrid network environment with Cisco Catalyst and Meraki devices, managed by a common Cisco Identity Service Engine (ISE) for centralized identity and security policy.
- We will examine how ISE can set VLANs, ACLs, and SGTs on various device types, how these SGTs are distributed across the LAN and WAN, and ultimately how they can be utilized to enforce a consistent security policy in a multi domain network environment.

Case Study Environment



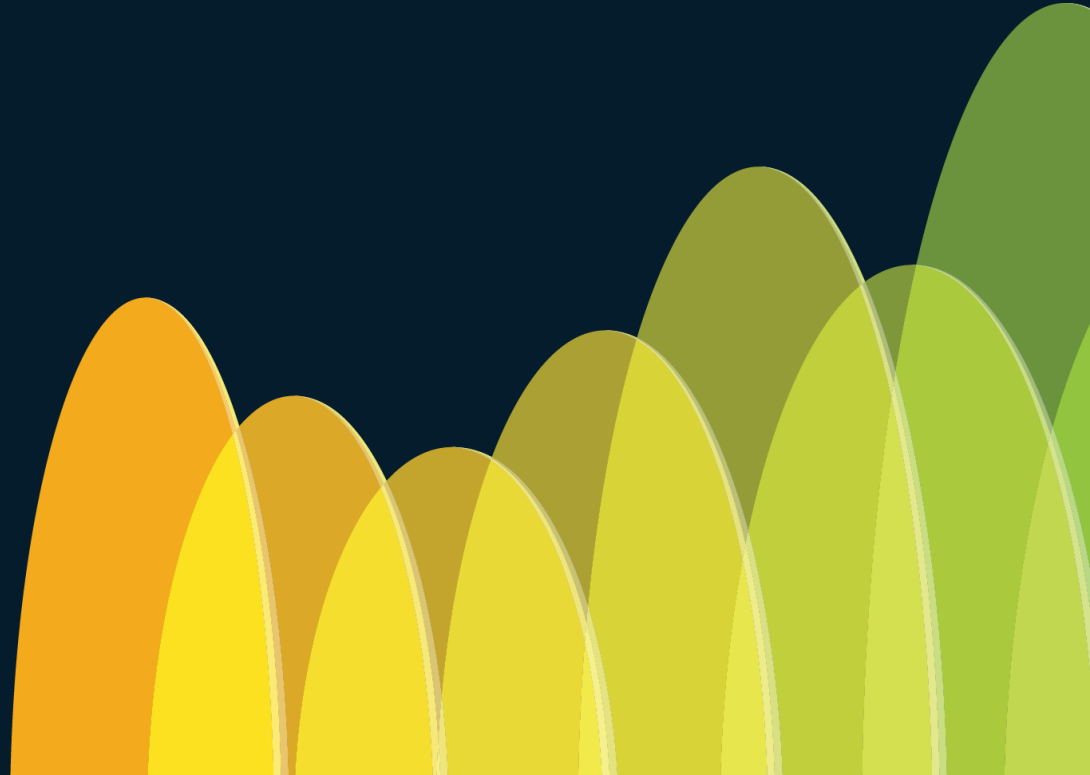
Cisco Validated Master Case Study



Hardware and software

- Catalyst platforms: Cat 9Ks, Cat 8ks, ISR 4Ks, WLCs/APs
- Meraki platforms: MS, MR, MX, etc.
- Cisco ISE release: 3.x
- Catalyst Center release 2.3.7.x
- Catalyst SD-WAN release 20.12
- Meraki release 18.x
- Catalyst platform release 17.12.02

Identity Service Engine (ISE)

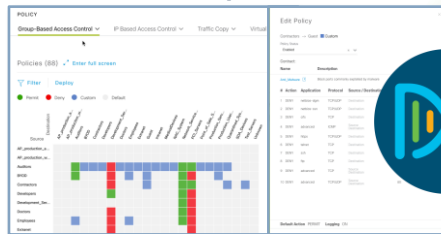
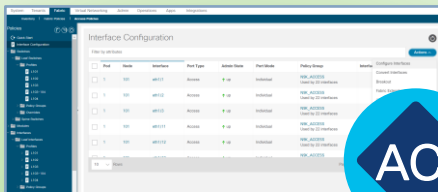
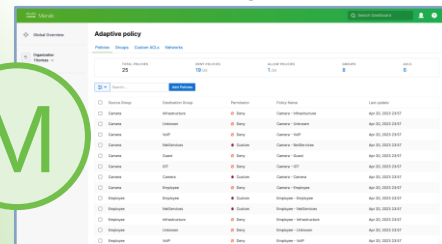


ISE is the core of Cisco's multi-domain policy

Data Center

Campus

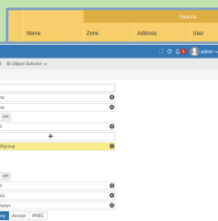
Campus



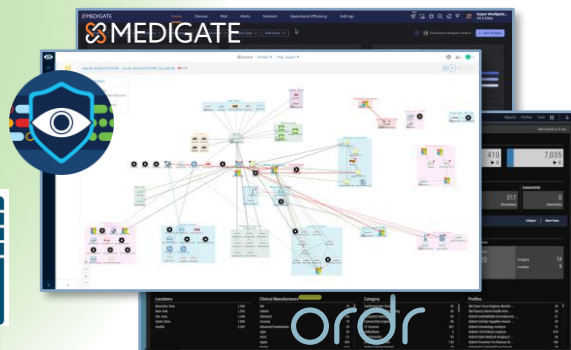
Security



3rd Parties



IoT



cisco *Live!*

Why ISE at the Core?



Hybrid Deployments: Maintain integrity of network security through deploying hybrid networks.



Redundancy: Mitigate the need to perform an extra step of replicating policies across multiple platforms.

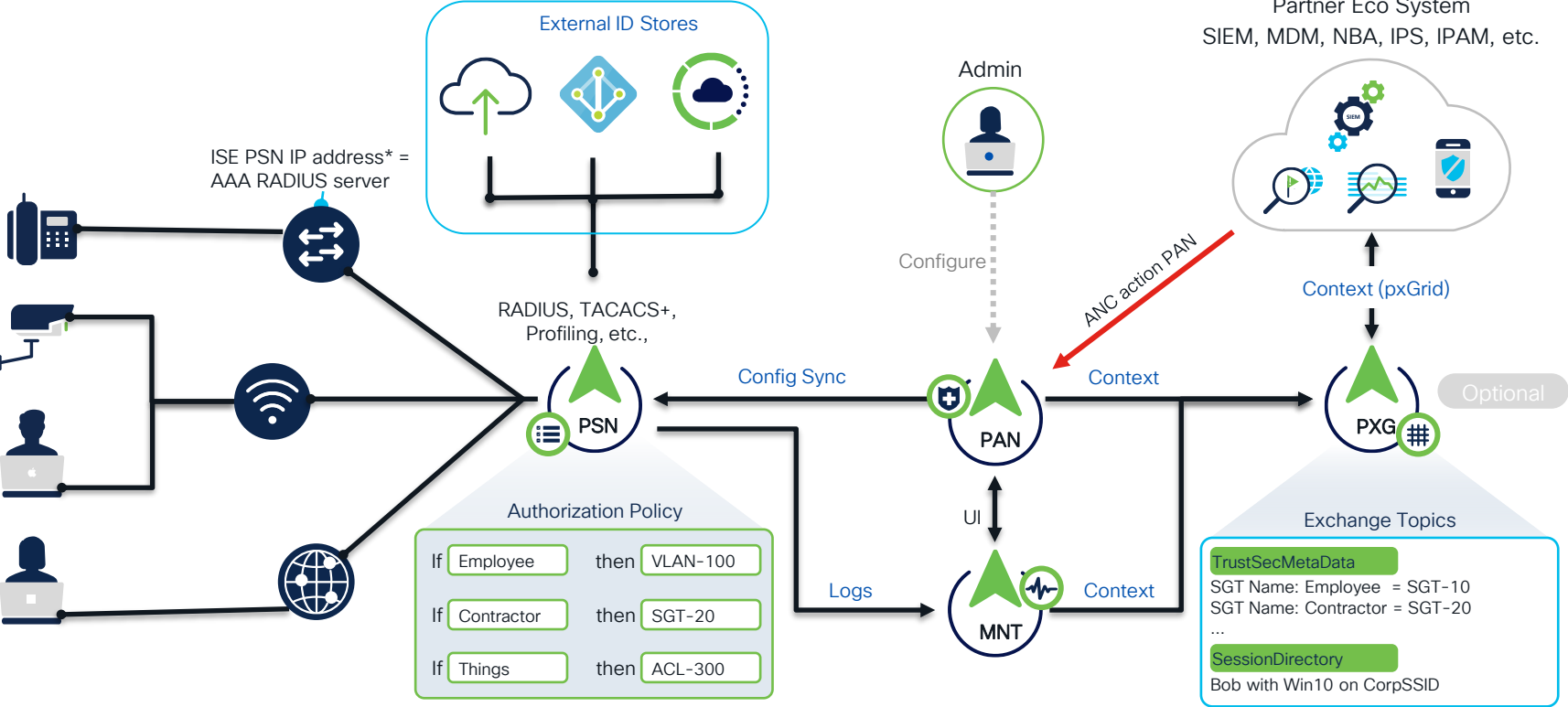


Potential Errors: Reduce the possibility of errors in policies that will affect the user experience.



Simplified Experience: Allows ISE to be the single source of truth and interface for policy management.

ISE Distributed Deployment



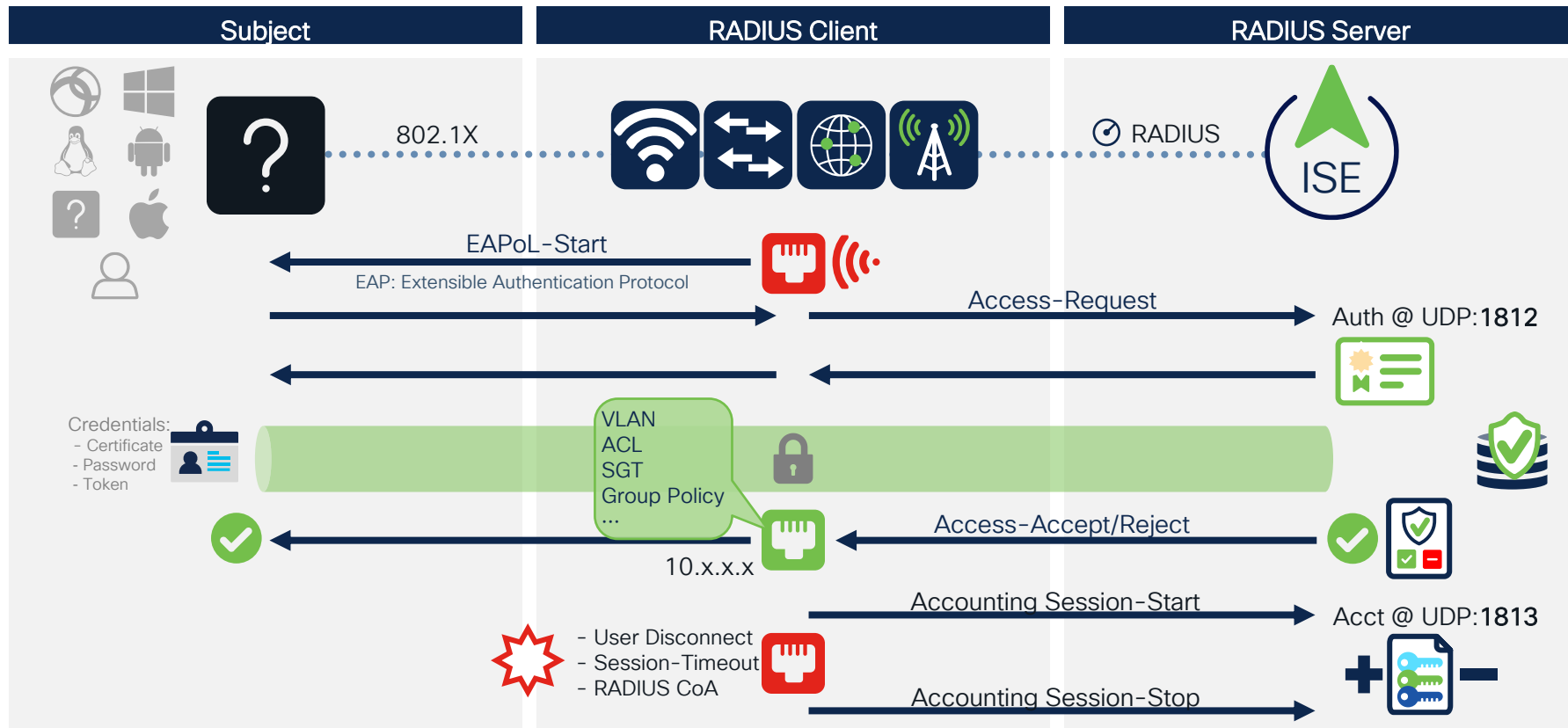
*PSNs can optionally be behind a load-balancer and can be accessed via Load Balancer Virtual IP address (VIPs)

RADIUS : 802.1X



RFC2865 : RADIUS
RFC2866 : Accounting

RFC3579 : EAP Support
RFC5176 : CoA Support



Radius Result

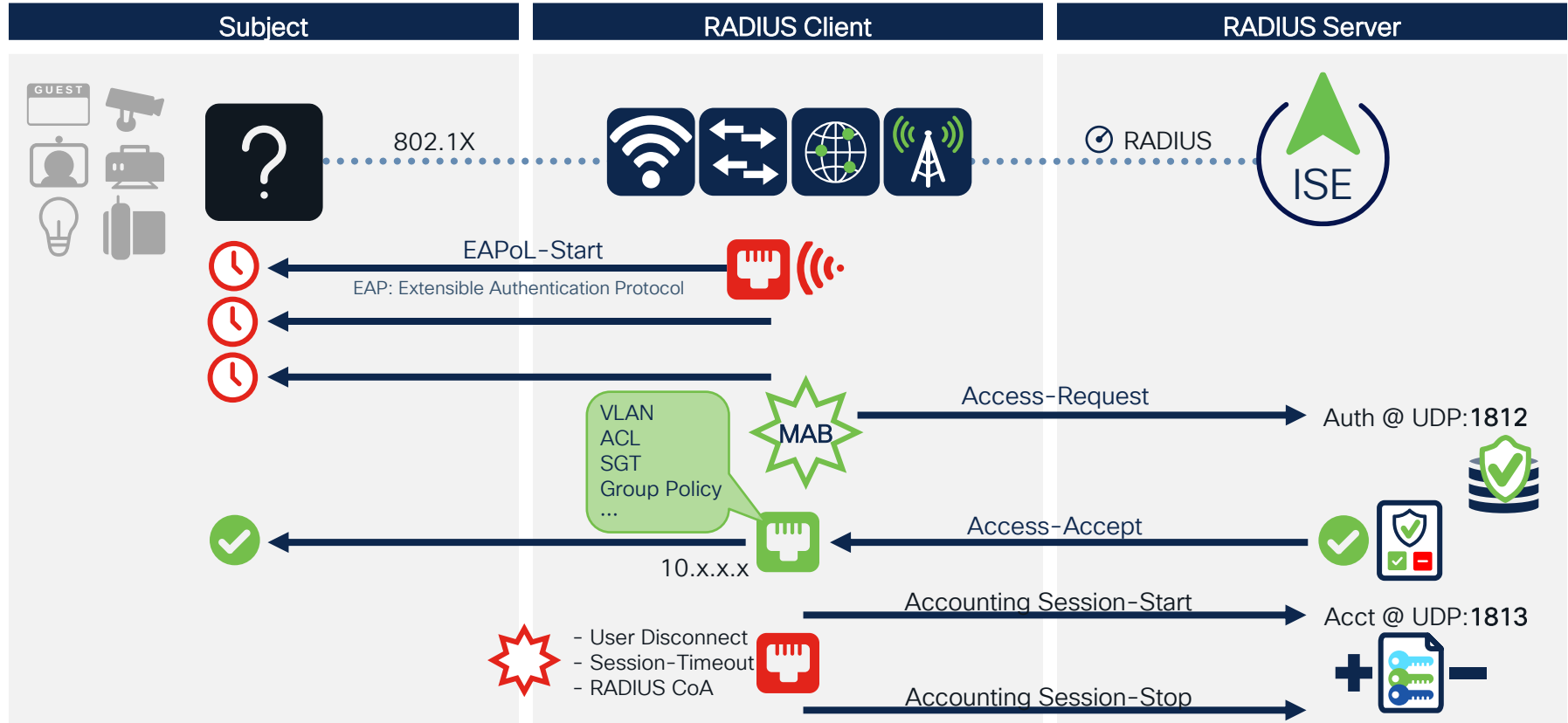
Overview

Event	5200 Authentication succeeded
Username	nnj202-client21
Endpoint Id	A0:CE:C8:76:14:04 ⓘ
Endpoint Profile	Workstation
Authentication Policy	Default >> Dot1X
Authorization Policy	Default >> dot1x-wired-NNJ-SDA-DACL-Employee_Campus_VN
Authorization Result	dot1x-wired-employee-sda

Result

Class	CACS:4E3FCA0A0000002AAB87DF7D:NYC-ISE-01/505935695/4810
Session-Timeout	1800 seconds
Termination-Action	RADIUS-Request
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) SDA-Employee
EAP-Key-Name	19:66:52:8f:c7:c3:ab:1a:93:fb:37:e5:4d:d4:c0:00:7a:75:c4:8f:e7:f3:6d:4e:32:3f:b2:e6:2a:7a:f8:c4:42:b7:5b:16:33:67:ff:95:2c:06:5e:f7:13:88:56:ea:a1:af:9d:27:ab:09:45:cf:ed:8a:80:4b:78:cf:f2:8c:09
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-employee-acl-01-654d3da0
cisco-av-pair	cts:security-group-tag=0004-40
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Essential license consumed.

RADIUS : MAC authentication bypass (MAB)

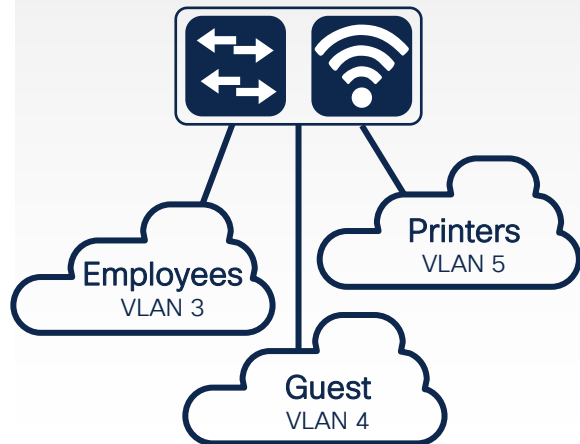


ISE segmentation options

Beyond RADIUS access-accept / access-reject

VLANs

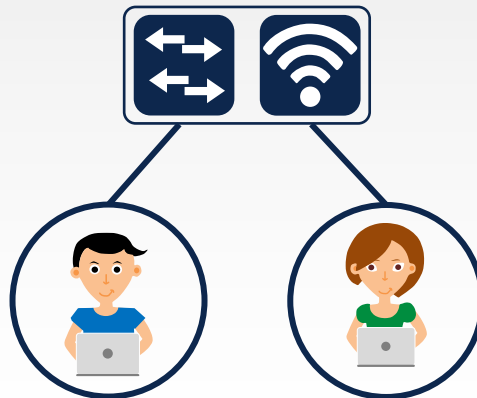
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

Downloadable ACL (Wired) or
Named ACL (Wired + Wireless) or
Meraki Filter-list



Employee

permit ip any any

Contractor

deny ip host <critical>
permit ip any any

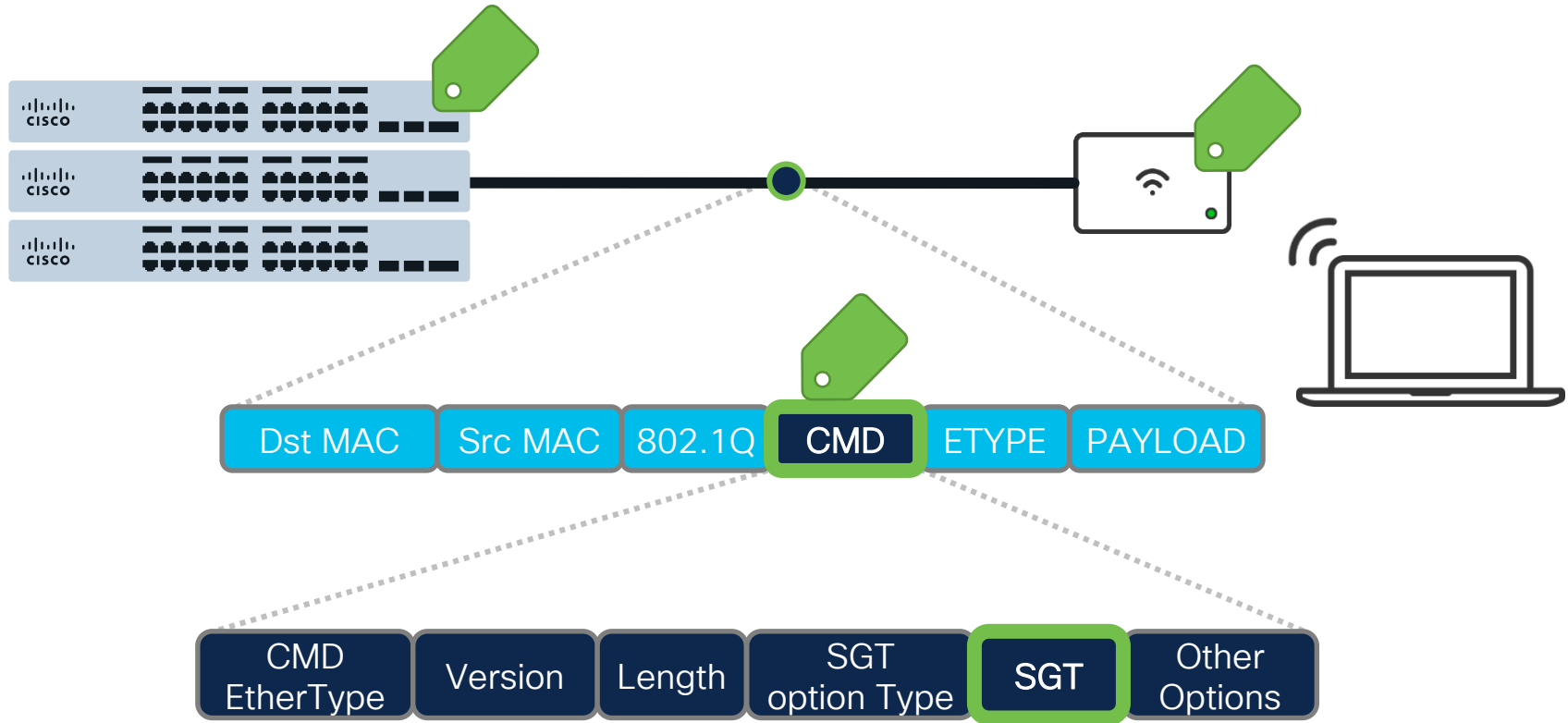
Security Group Tags

Cisco Group-Based Policy



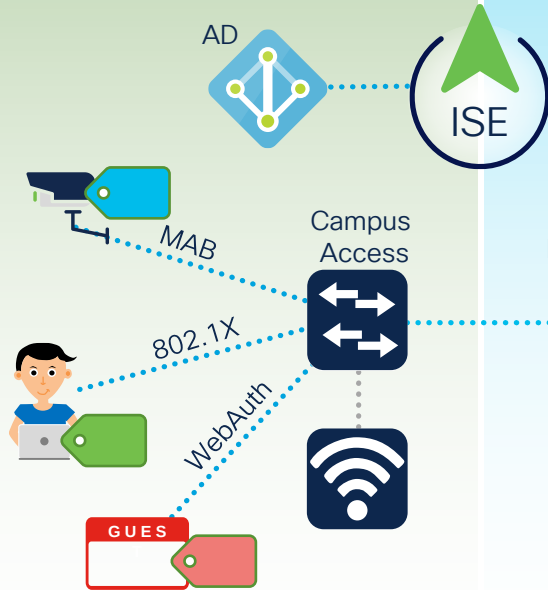
16-bit SGT assignment and
SGT based Access Control

What are security group tags (SGTs)?

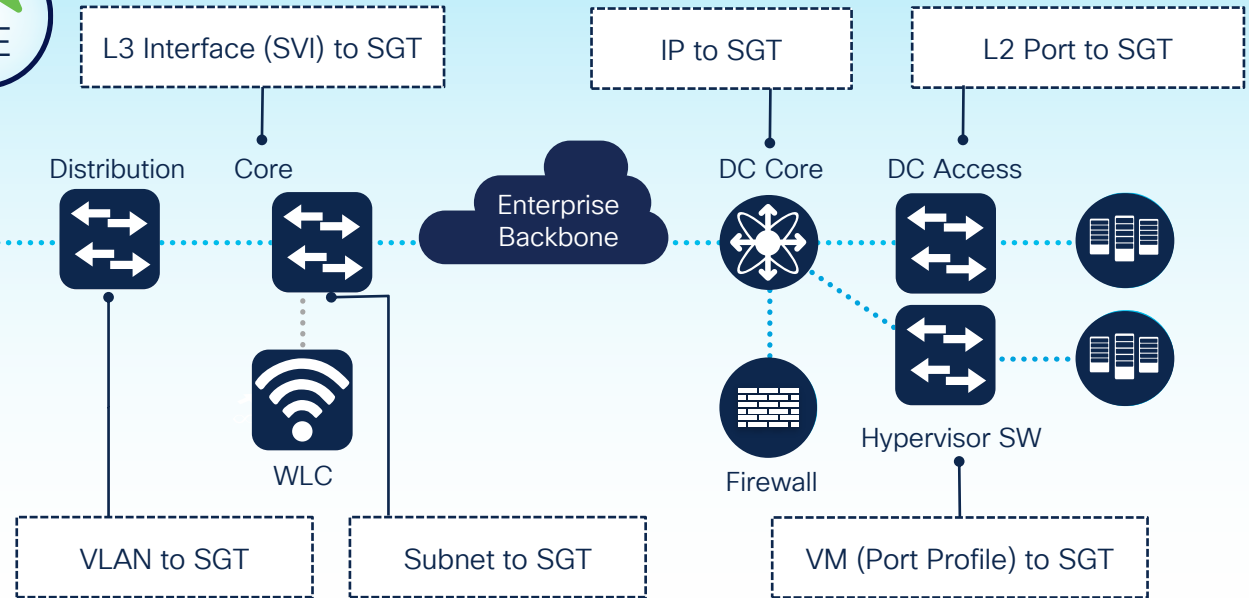


Classification Mechanisms

Dynamic Classification

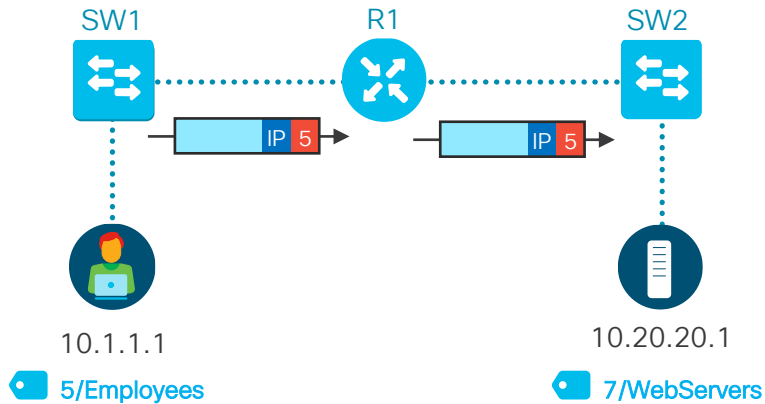


Static Classification



TrustSec Propagation Options

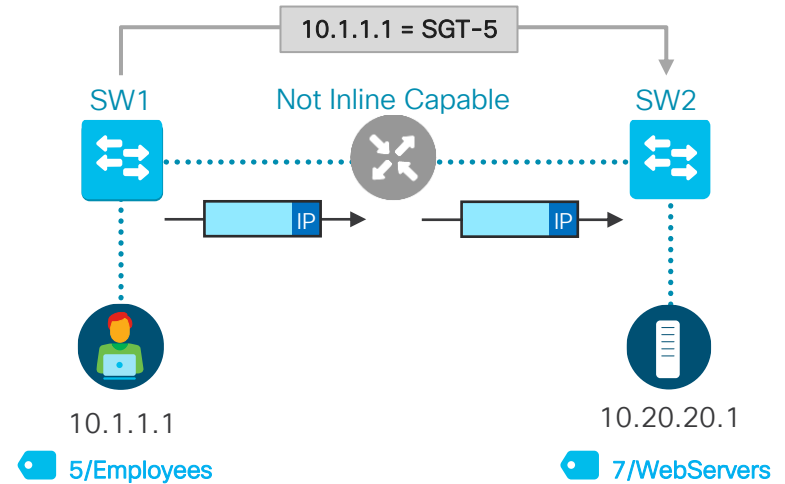
DATA PLANE PROPOGATION (INLINE TAGGING)



SGT carried inline in the data traffic. Methods include, SGT over:



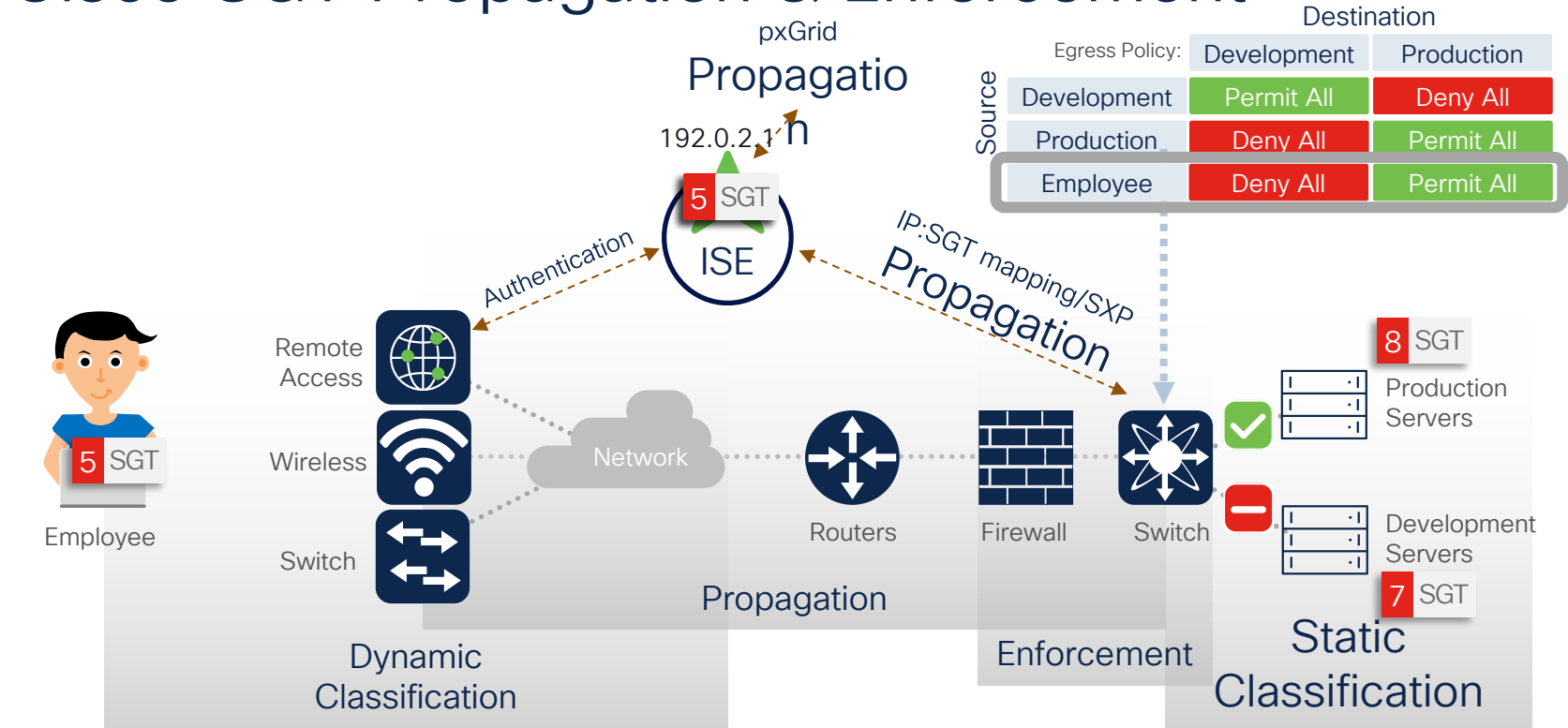
CONTROL PLANE PROPOGATION (SXP)



IP-to-SGT data shared over control protocol. No SGT in the data plane. Methods include, IP-to-SGT exchange over:



Cisco SGT Propagation & Enforcement



SGT in the Data Plane

CMD in Ethernet

```
▶ Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
▶ Ethernet II, Src: Cisco_a8:32:86 (5c:5a:c7:a8:32:86), Dst: Cisco_28:e5:f0 (50:61:bf:28:e5:f0)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3007
▼ Cisco MetaData
  Version: 1
  Length: 1
  Options: 0x0001
  SGT: 4
  Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.4.2.10, Dst: 10.4.3.10
```

CMD in GRE

```
▶ Frame 6: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
▶ Ethernet II, Src: Cisco_5c:70:d0 (4c:77:6d:5c:70:d0), Dst: Cisco_a8:32:82 (5c:5a:c7:a8:32:82)
▶ Internet Protocol Version 4, Src: 172.29.1.226, Dst: 172.29.1.225
▶ Generic Routing Encapsulation (CiscoMetaData)
▼ Cisco MetaData
  Type: IPv4 (0x0800)
  Version: 1
  Length: 1
  Options: 0x0001
  SGT: 4
▶ Internet Protocol Version 4, Src: 10.4.2.10, Dst: 10.4.3.10
▶ Internet Control Message Protocol
```

VXLAN GPO

```
▶ Frame 13: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶ Internet Protocol Version 4, Src: 172.31.216.69, Dst: 192.168.8.1
▶ User Datagram Protocol, Src Port: 65476, Dst Port: 4789
▼ Virtual eXtensible Local Area Network
  Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
  Group Policy ID: 4
  VXLAN Network Identifier (VNI): 4100
  Reserved: 0
▶ Ethernet II, Src: Cisco_9f:00:00 (00:00:0c:9f:00:00), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
▶ Internet Protocol Version 4, Src: 10.4.3.10, Dst: 10.4.2.10
▶ Internet Control Message Protocol
```

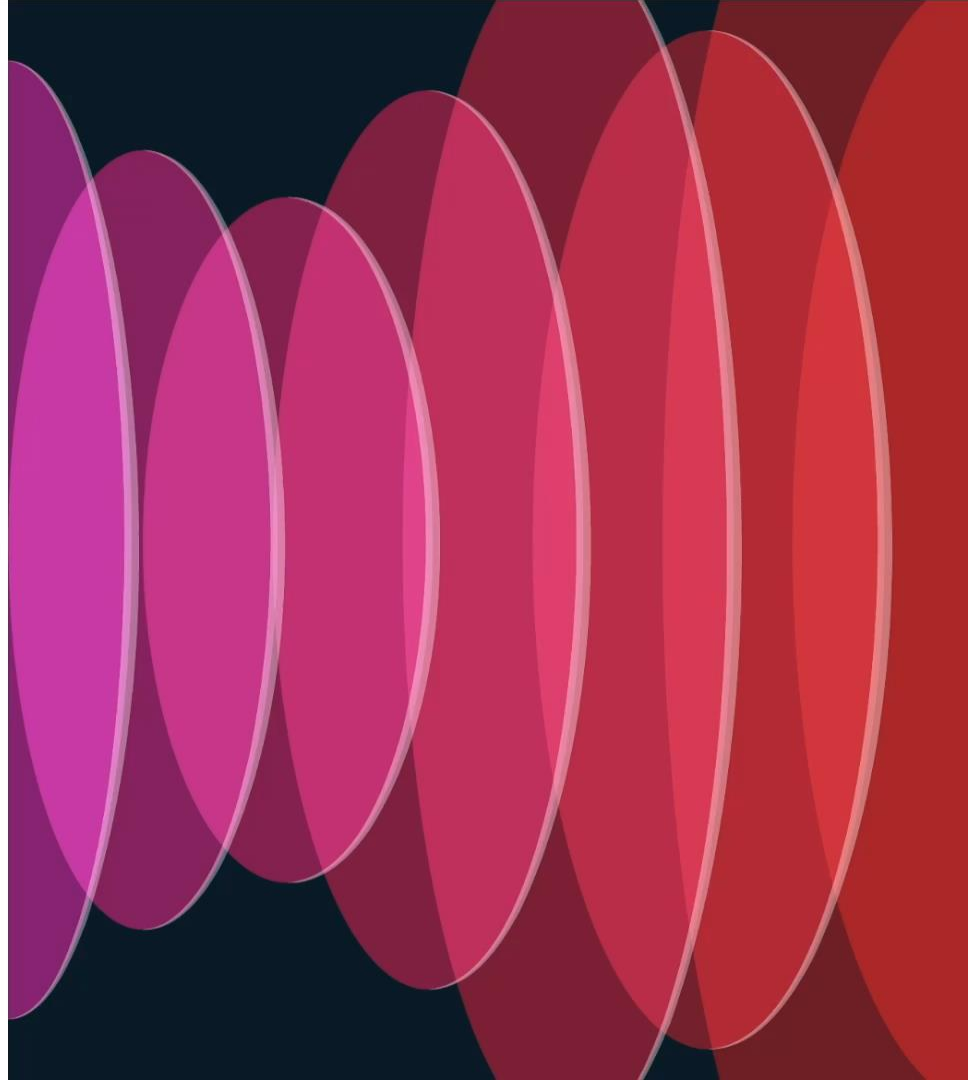
CMD in IPsec

```
▶ Frame 13: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
▶ Ethernet II, Src: Cisco_5c:70:d0 (4c:77:6d:5c:70:d0), Dst: Cisco_a8:32:82 (5c:5a:c7:a8:32:82)
▶ Internet Protocol Version 4, Src: 172.29.1.226, Dst: 172.29.1.225
▼ Encapsulating Security Payload
  ESP SPI: 0xc3e8acd0 (3286805712)
  ESP Sequence: 1858
  0000 5c 5a c7 a8 32 82 4c 77 6d 5c 70 d0 08 00 45 00 \Z~2Lw m\p...E
  0010 00 78 00 00 00 00 ff 32 5f 56 ac 1d 01 e2 ac 1d .....2_V.....
  0020 01 e1 c3 e8 ac d0 00 00 07 42 99 4a 1b b9 91 b8 .....B.J....
  0030 9b 3c 3a ef 40 00 00 00 00 00 00 00 00 00 00 00 <: @.lh .gV....
  0040 d8 d2 a4 60 94 0f 06 76 03 0f 06 76 03 ..{.#. ?A...0-G
  0050 fa 29 06 91 7b 00 00 00 00 00 00 00 00 00 00 ..]...v2 !d....
  0060 fe 8b 7c 8a da ca 7b 32 z1 e9 04 02 d9 a8 c3 bc ...w..J ..a..'+
  0070 97 e7 9a 89 77 8c ff 4a ec 07 61 b1 5d 17 27 2b ..e...
  0080 c1 be 65 7e 14 d1
```

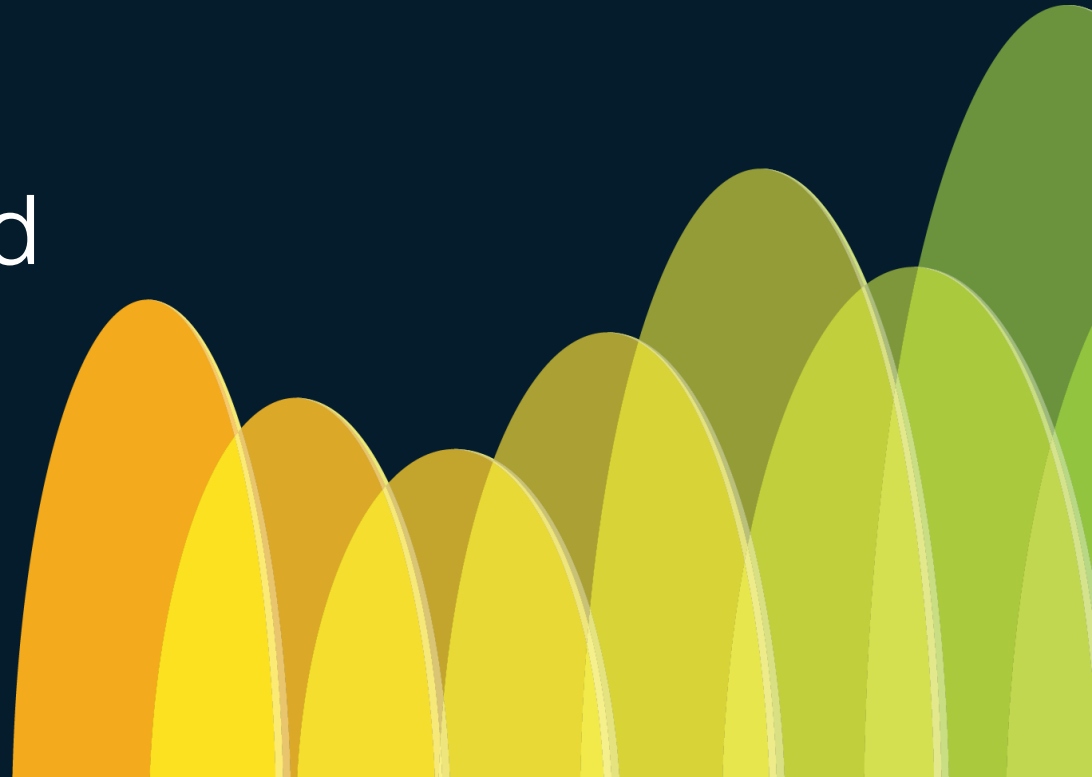
Review TrustSec capability matrix:

<https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/solution-overview-listing.html>

ISE TrustSec Demo

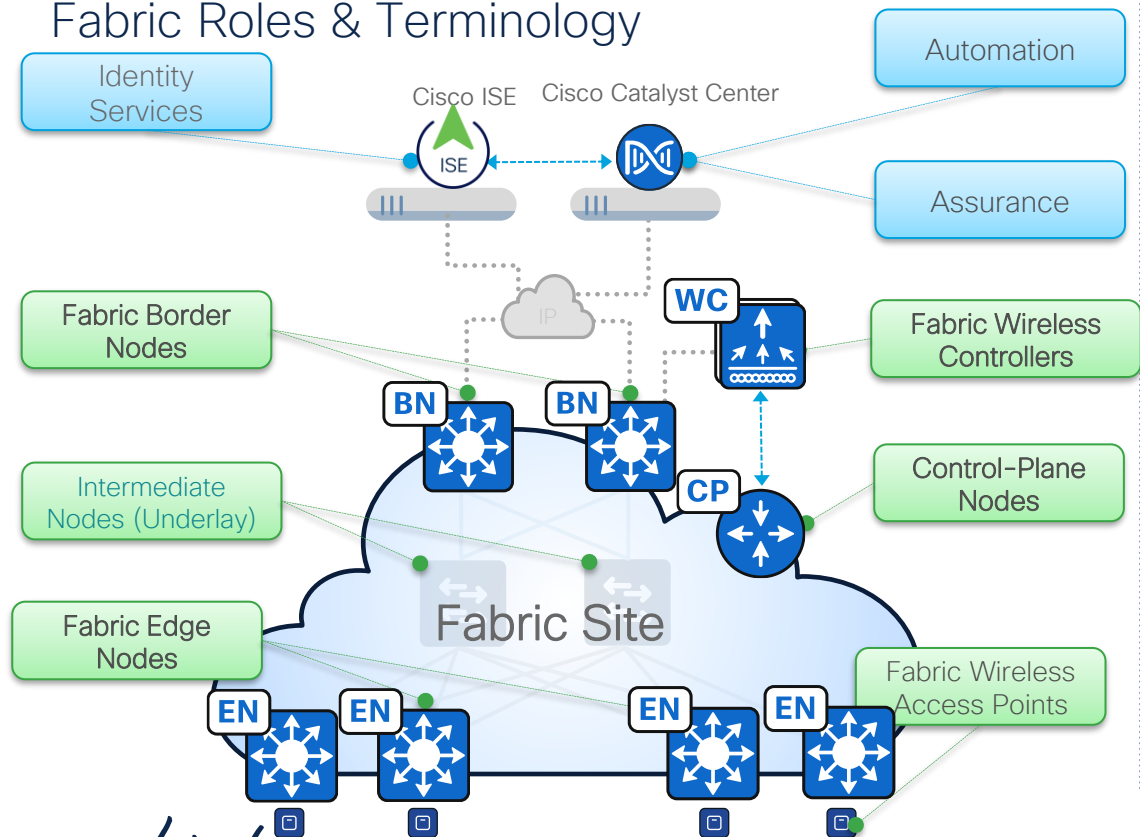


Catalyst Center Software Defined Access



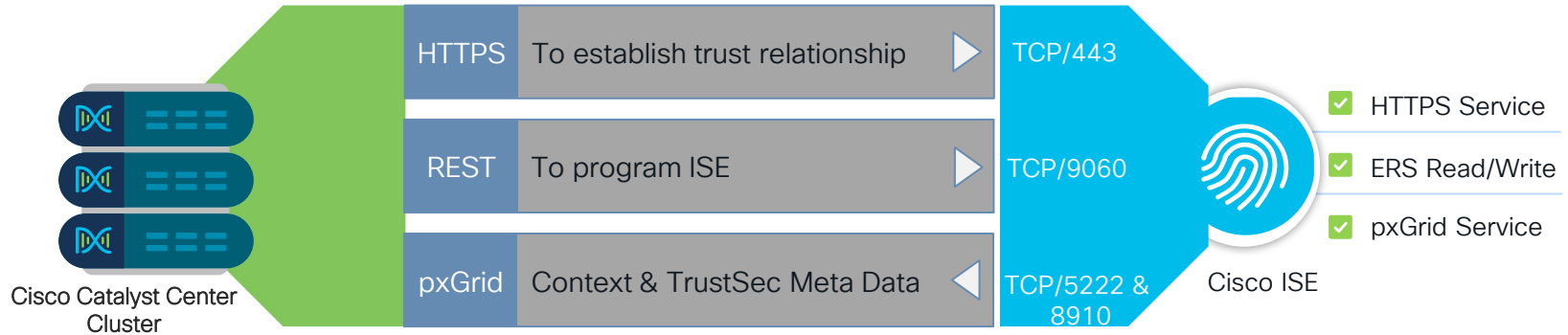
Cisco SD-Access

Fabric Roles & Terminology



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

Cisco Catalyst Center & ISE Communication



Cisco ISE: Enable below ISE Services

Administration > System > Deployment > Select ISE Host Name

Enable pxGrid Services

Administration > Settings > ERS Settings

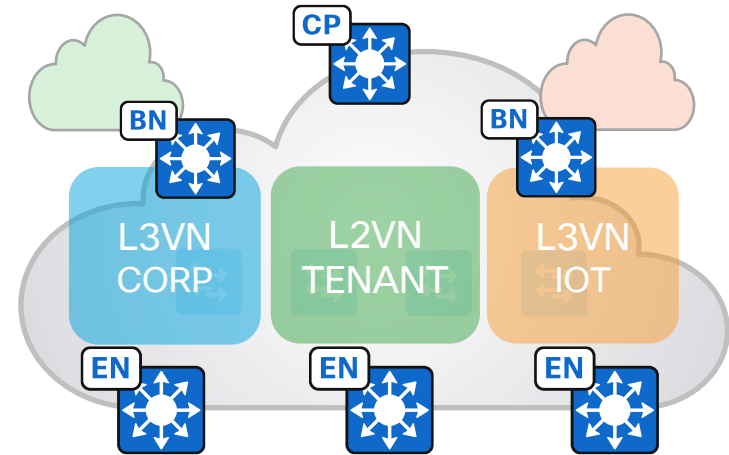
Enable *ERS for Read/Write on PAN*

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

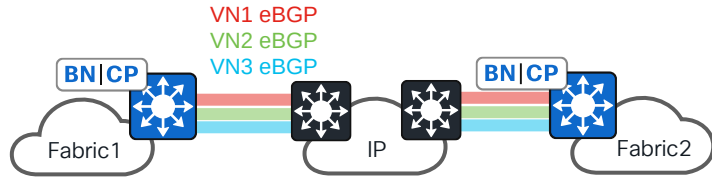
Cisco SD-Access Fabric

Virtual Networks

- Layer 3 Virtual Networks use VRFs and LISP Instance IDs to maintain separate routing topologies.
 - Endpoint IDs (IPv4/IPv6 addresses) are routed within an L3VN.
- Layer 2 Virtual Networks use LISP Instance IDs and VLANs to maintain separate switching topologies.
 - Endpoint IDs (MAC addresses) are switched within an L2VN.
- Edge Nodes, Border Nodes and Fabric APs add and remove the Virtual Network assignments.

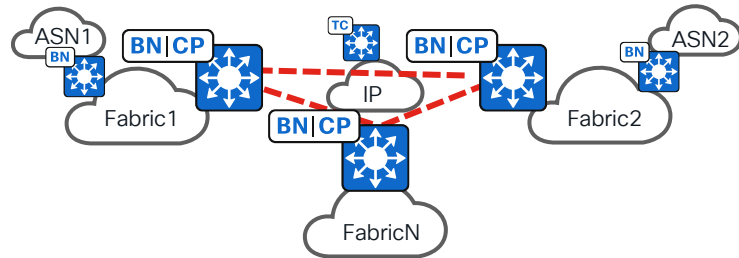


Connect to outside world using Transits



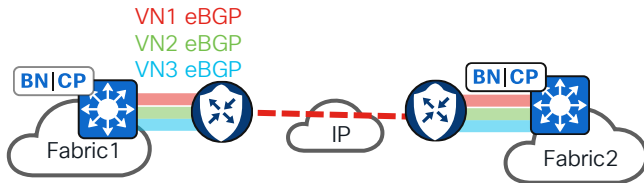
IP-Based Transit

- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.



SD-Access Transit

- SD-Access LISP/VXLAN between Fabric Sites.
- Natively preserves Layer 3 Virtual Networks and SGTs.
- Capable of fabric as a transit between external routing domains.

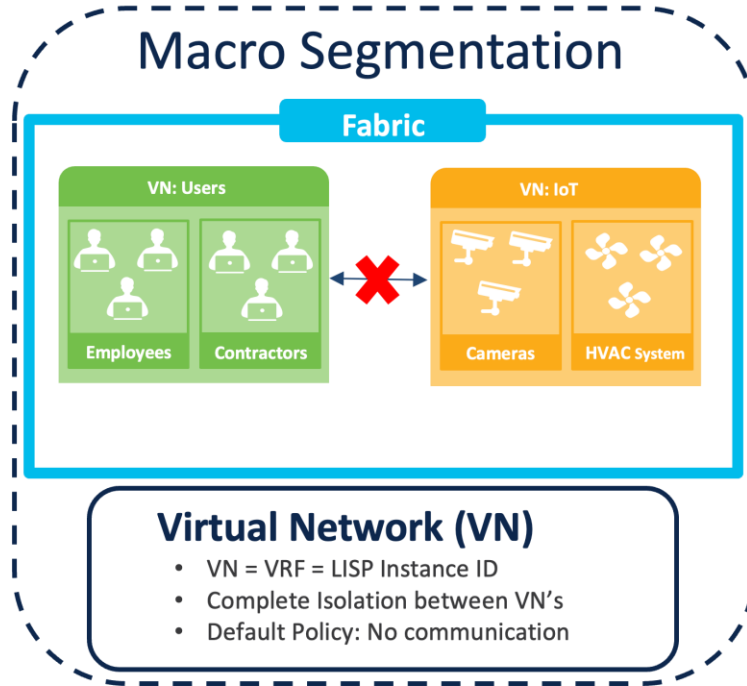
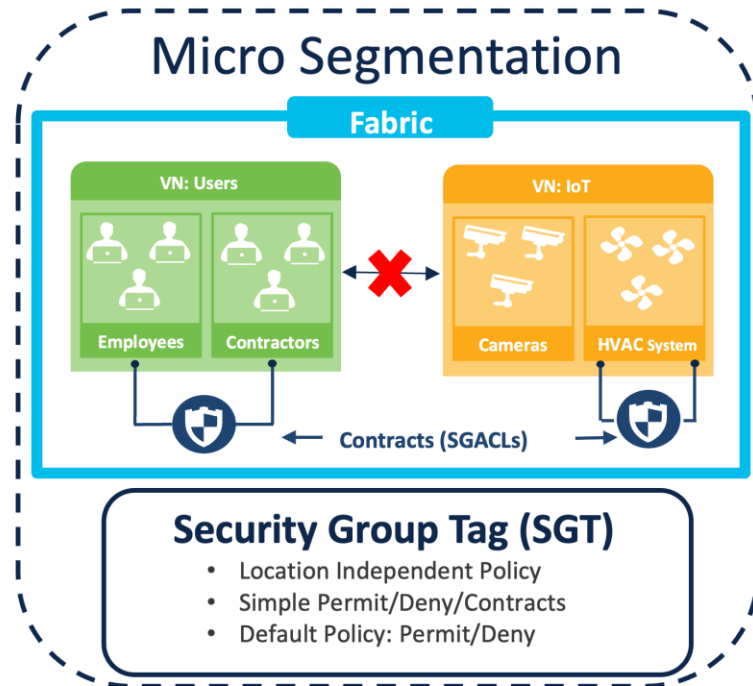


SD-WAN Transit

- Cisco SD-WAN between Fabric Sites.
- Capable of preserving Layer 3 Virtual Networks and SGTs.
- Dedicated SD-WAN Edge for design flexibility. See [Independent Domains PDG](#).

Cisco SD-Access Policy

Segmentation Strategies



Data Plane Propagation - VXLAN



User Datagram Protocol, Src Port: 65476, Dst Port: 4789

Source Port: 65476

Destination Port: 4789

Length: 90

[Checksum: [missing]]

[Checksum Status: Not present]

[Stream index: 0]

[Timestamps]

[Time since first frame: 0.000000000 seconds]

[Time since previous frame: 0.000000000 seconds]

Virtual eXtensible Local Area Network

Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)

1... .. = GBP Extension: Defined

.... ..0... .. = Don't Learn: False

.... 1... .. = VXLAN Network ID (VNI): True

.... .. 0... = Policy Applied: False

.000 .000 0.00 .000 = Reserved(R): 0x0000

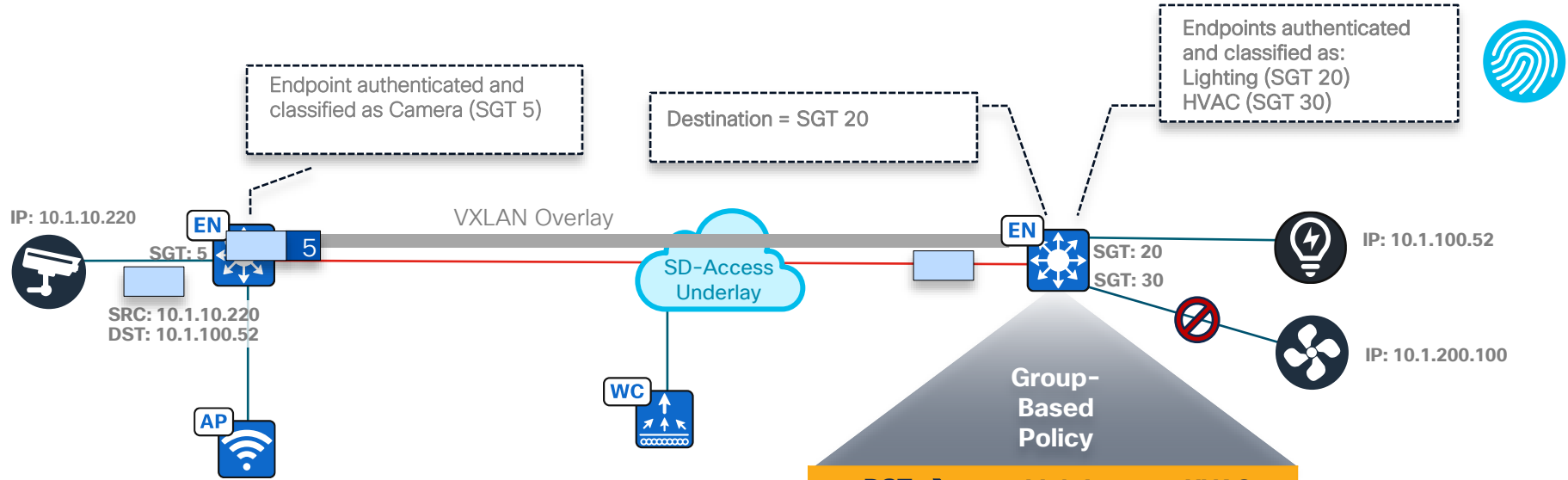
Group Policy ID: 4

VXLAN Network Identifier (VNI): 4100

Reserved: 0

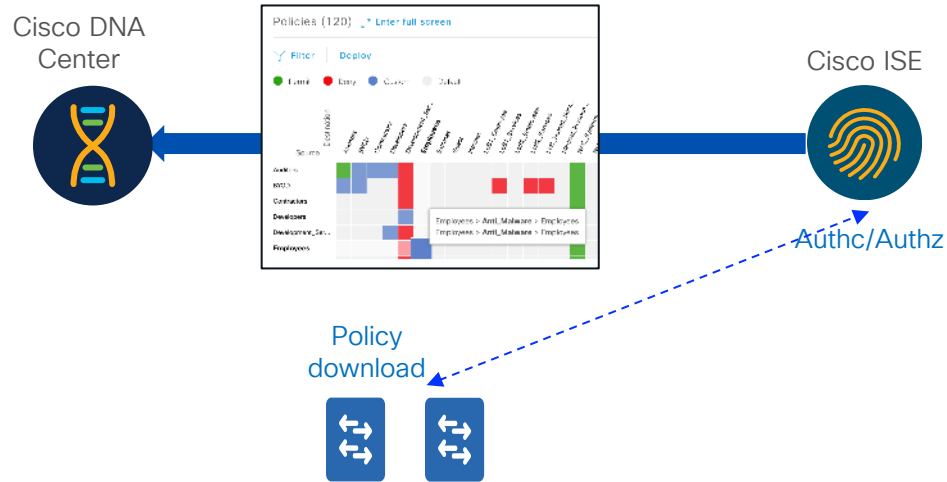
VRF + SGT

Segmentation Operation in SD-Access Fabric



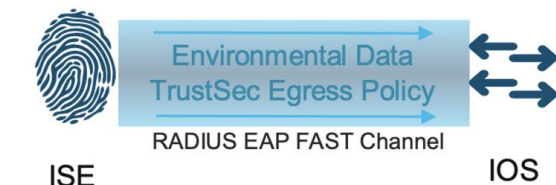
- Classification: Dynamic/ISE
- Propagation: SGT in VXLAN
- Enforcement: Egress Fabric Edge

SGACL



```
NNJ202-Edge1-FL01#sh cts role-based permissions
IPv4 Role-based permissions default:
    Permit IP-00
IPv4 Role-based permissions from group 16:HR_users to group 4:Employees:
    Block_ICMP-01
IPv4 Role-based permissions from group 18:DC_Web_Services_Employe to group 4:Employees:
    Web_Only-15
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

ISE and 'Network Devices' Secure communication using PAC Keys



Switch authenticates with Cisco ISE for Secure EAP FAST Channel

```
Switch# cts credential id C6800-001 password cisco
```

RADIUS PAC keys pushed by ISE. Switch uses this to talk to ISE securely*

```
Switch# show cts pacs
```

```
AID: 3E465B9E3F4E012E6AD3159B403B5004
```

```
PAC-Info:
```

```
PAC-type = Cisco Trustsec
```

```
AID: 3E465B9E3F4E012E6AD3159B403B5004
```

```
I-ID: C6800-0001
```

```
A-ID-Info: Identity Services Engine
```

```
Credential Lifetime: 13:12:04 UTC Jan 12 2016
```

```
PAC-Opaque:
```

```
000200B800030001000400103E465B9E3F4E012E6AD3159B403B50040006009C  
000301008C3B32A200B23EF4A53D9DF79A6E4B2600000013555D348600093A80  
8273497B5BB779165C75E75DDF4619CB3D4AD755949603F5488C5904CA27F13C  
6FB45F333209915DCCED288FF304F8517663FD49D2D2D3EBF664300E3FD66925  
A7DEB8C93570913A369280EB251091D92D90FEDA7BBD1148C7CCA8D018011F00  
9A5548286430573F854DD3C9231476EE32E47B7AB7075372051BB3FD  
Refresh timer is set for 12w4d
```

Use Device ID for TrustSec ☒

Identification

Device Id

* Password

Device SGT

```
NNJ202-Edge1-FL01#sh cts environment-data
```

```
CTS Environment Data
```

```
=====
```

```
Current state = COMPLETE
```

```
Last status = Successful
```

```
Service Info Table:
```

```
Local Device SGT:
```

```
SGT tag = 2-04:TrustSec_Devices
```

```
Server List Info:
```

```
Installed list: CTSServerList1-0001, 1 server(s):
```

```
*Server: 10.100.0.10, port 1812, A-ID BDE53477C033F78480308A28B25F2C10
```

```
Status = ALIVE
```

```
auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
```

```
Security Group Name Table:
```

```
0-20:Unknown
```

```
2-04:TrustSec Devices
```

```
3-00:test
```

```
4-40:Employees
```

```
5-01:IoT
```

Environmental Data



Security Groups

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Icon	Name	SGT (Dec / Hex)
☐	Unknown	0/0000
☐	Employee_FullAccess	10/000A
☐	PCI_Devices	100/0064
☐	Web_Servers	110/006E
☐	Mail_Servers	120/0078
☐	TrustSec_Infra_SGT	2/0002
☐	Employee_BYOD	20/0014
☐	Unregist_Dev_SGT	255/00FF
☐	Contractors	30/001E

Switch# **show cts environment-data**

CTS Environment Data

=====

Current state = COMPLETE

Last status = Successful

Local Device SGT:

SGT tag = 2-00:TrustSec_Infra_SGT

Server List Info:

Installed list: CTSServerList1-0001, 1 server(s):

*Server: 10.1.1.222, port 1812, A-ID 3E465B9E3F4E012E6AD3159B403B5004

Status = DEAD

auto-test = TRUE, keywrap-e

= 20 secs

Multicast Group SGT Table:

Security Group Name Table:

0-00:Unknown

2-00:TrustSec_Infra_SGT

10-00:Employee_FullAccess

20-00:Employee_BYOD

30-00:Contractors

100-00:PCI_Devices

110-00:Web_Servers

120-00:Mail_Servers

255-00:Unregist_Dev_SGT

Environment Data Lifetime = 86400 secs

Last update time = 21:57:24 UTC Thu Feb 4 2016

Env-data expires in 0:23:58:00 (dd:hr:mm:sec)

Env-data refreshes in 0:23:58:00 (dd:hr:mm:sec)

Cache data applied = NONE

State Machine is running

Security Group Name Table:

0-00:Unknown

2-00:TrustSec_Infra_SGT

10-00:Employee_FullAccess

20-00:Employee_BYOD

30-00:Contractors

100-00:PCI_Devices

110-00:Web_Servers

120-00:Mail_Servers

255-00:Unregist_Dev_SGT

IP Transit – Manual SGT or SXP

```
NNJ-Core1#sh run | b sxp
cts sxp enable
cts sxp default source-ip 10.200.255.11
cts sxp default password Cisc012345
cts sxp connection peer 10.100.0.10 password default mode local listener hold-time 0 0
cts sxp log binding-changes
cts sxp node-id IPv4 10.200.255.11
```

SXP

```
NNJ202-CP-Border1#sh run int g1/0/3
Building configuration...
```

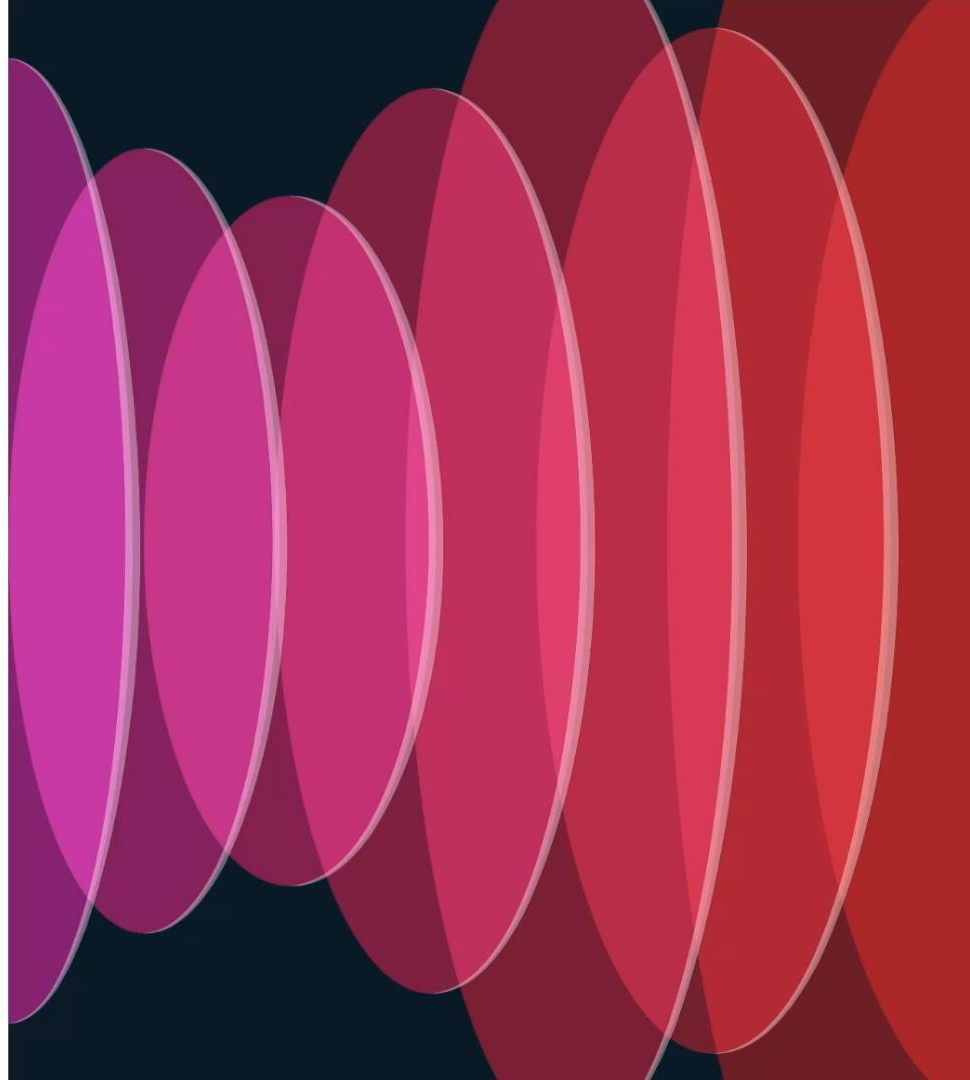
Inline

```
Current configuration : 177 bytes
!
interface GigabitEthernet1/0/3
 description Trunk to NNJ-Core1
 switchport mode trunk
 cts manual
  policy static sgt 2 trusted
 bfd interval 100 min_rx 100 multiplier 3
end
```

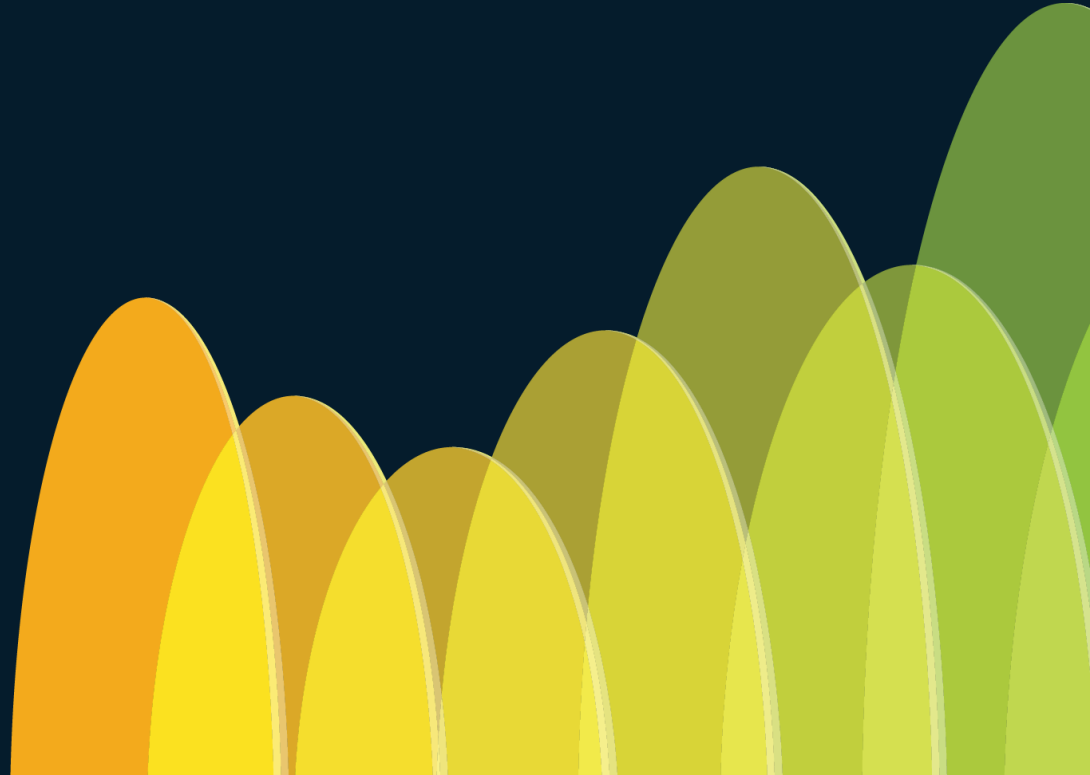
```
NNJ-Core1#sh cts sxp sgt-map brief
SXP Node ID(configured):0x0AC8FF0B(10.200.255.11)
IP-SGT Mappings as follows:
IPv4,SGT: <10.6.120.100 , 4:Employees>
IPv4,SGT: <10.7.120.100 , 4:Employees>
IPv4,SGT: <10.53.180.5 , 5:IoT>
IPv4,SGT: <10.58.120.11 , 4:Employees>
IPv4,SGT: <10.58.120.14 , 4:Employees>
IPv4,SGT: <10.60.120.20 , 4:Employees>
IPv4,SGT: <10.63.0.6 , 4:Employees>
IPv4,SGT: <10.100.0.60 , 18:DC_Web_Services_Employe>
```

SXP

Catalyst Center Demo



Meraki Adaptive Policy



Meraki adaptive policy



Organization-Wide intent-based policy



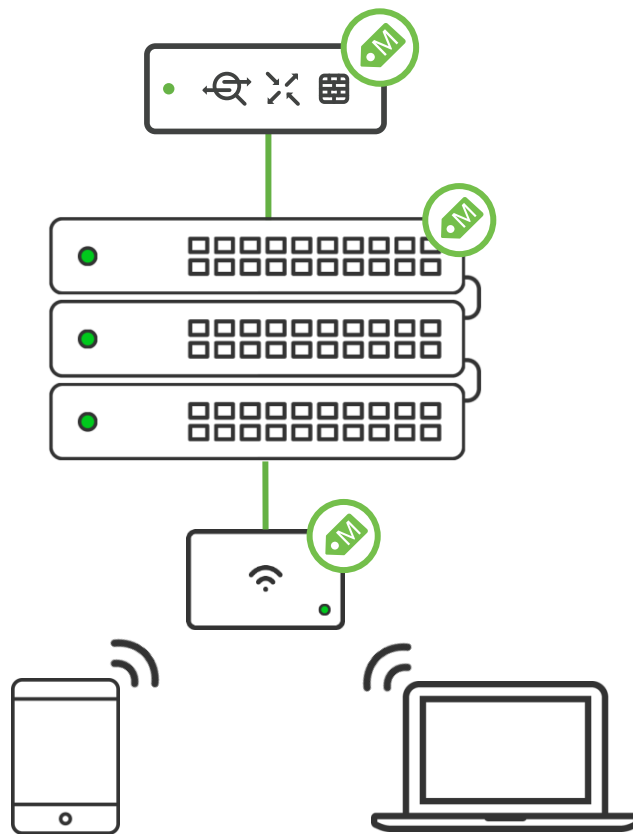
Utilizes inline Security Group Tags (SGTs)



Context shared over the data-plane

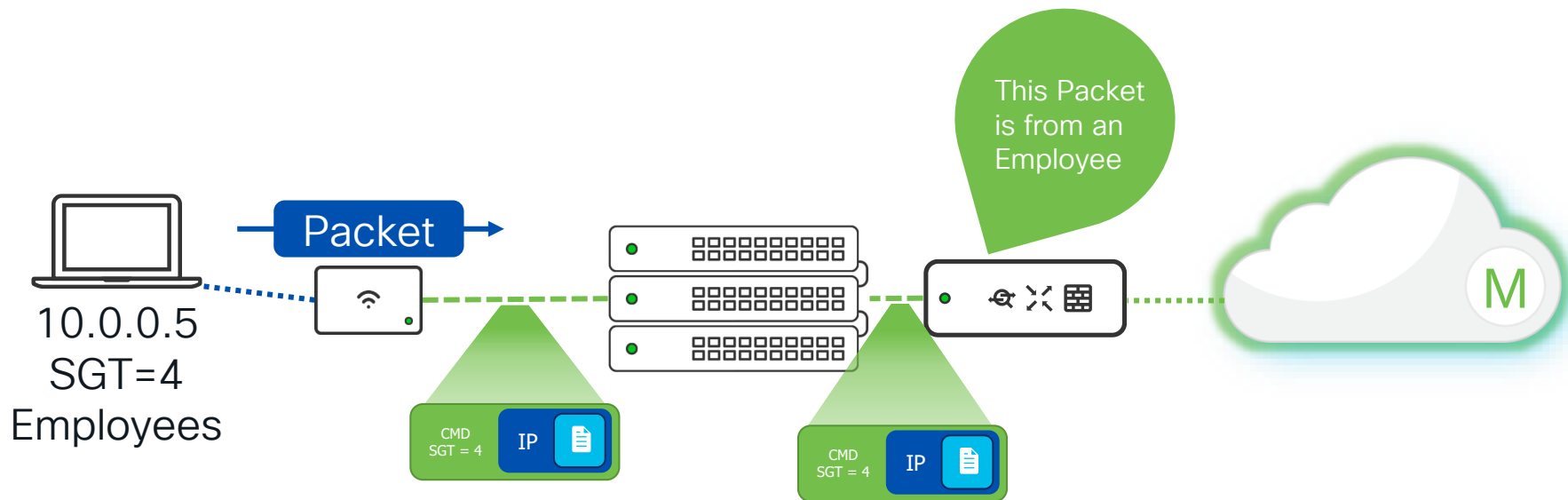


IP and topology agnostic security providing consistent policy for wired and wireless access



Scalable Identity and Context

Sharing information over the dataplane, in every packet



ISE and Meraki together



Dashboard > Organization > Setting > RADIUS Servers

Network
CVF-53-APX

Network-wide

Security & SD-WAN

Switching

Insight

Organization

Access policies

Name

Radius_Auth

Authentication method

my RADIUS server

RADIUS Servers

#	Name	Host	Port	Secret	Actions
1	MCS ISE	10.100.0.10	1812	*****	Show

Select RADIUS

+ Add a server

☒ RADIUS Server Testing

☒ RADIUS CoA support

☒ Enable RADIUS accounting servers

RADIUS Accounting Servers

#	Name	Host	Port	Secret	Actions
1	MCS ISE	10.100.0.10	1813	*****	Show

Select RADIUS

+ Add a server

RADIUS attribute specifying group policy name

Filter-Id

Host Mode

Single-Host

Access policy type

Hybrid authentication

Increase access speed

☒ Enabling this option will make switches execute 802.1X and MAC-bypass authentication simultaneously so that clients authenticate faster. However, it will increase load on your RADIUS servers.

802.1X Control Direction

inbound-only

Scaling considerations



60x SGTs



3600 Policies



113 ACEs Per Policy



8000 IP to SGT Maps



**Limited by standard hardware endpoint scaling e.g. CAM tables*

Group Policy on MS and MR



Per-session 802.1X inbound ACL enforcement



Named ACL orchestration



On-the-fly ACL update (no CoA required)

Name

Schedule

Bandwidth unlimited [details](#)

Hostname visibility

Firewall and traffic shaping

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Allow	TCP	10.10.1.4	1883	MQTT-1883	⚙️ ✕
2	Allow	TCP	10.10.1.4	1884	MQTT-1884	⚙️ ✕
3	Deny	Any	10.0.0.0/8	Any	Block 10-8	⚙️ ✕
4	Deny	Any	172.16.0.0/12	Any	Block 172-12	⚙️ ✕
5	Deny	Any	192.168.0.0/16	Any	Block 192-16	⚙️ ✕
	Allow	Any	Any	Any	Default rule	

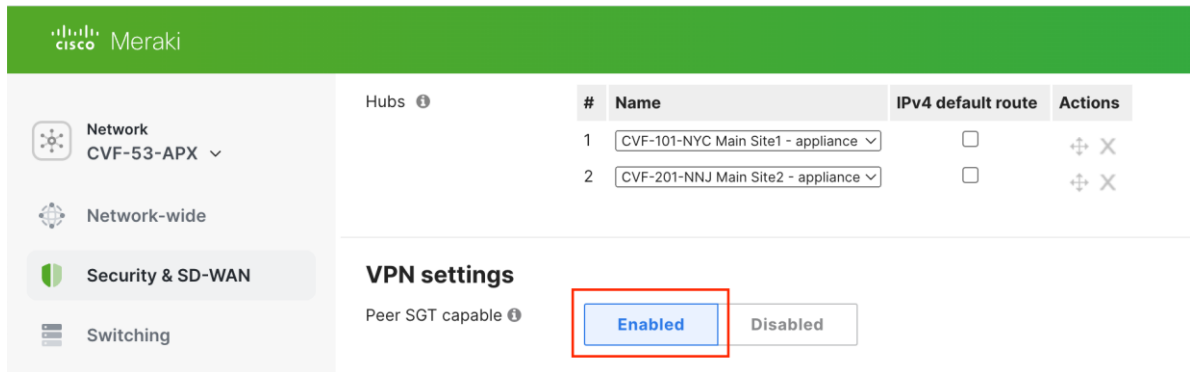
[Add a firewall rule](#)



Filter-ID → Dashboard
Group-Policy



AutoVPN SGT Propagation



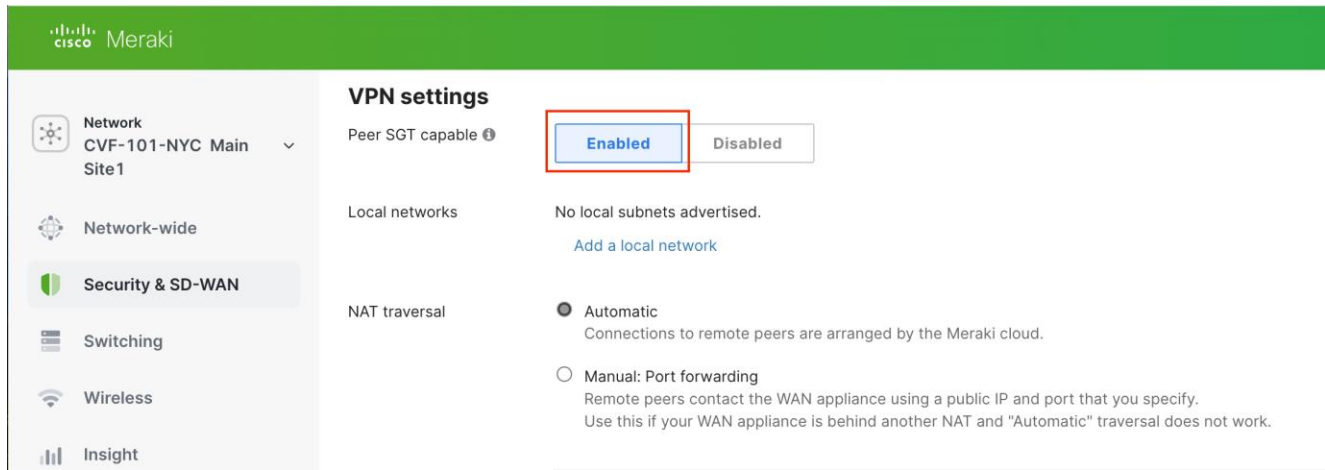
The screenshot shows the Cisco Meraki dashboard. On the left, the navigation menu includes Network, Network-wide, Security & SD-WAN, and Switching. The main content area is titled 'Hubs' and contains a table with two entries:

#	Name	IPv4 default route	Actions
1	CVF-101-NYC Main Site1 - appliance	☐	+ X
2	CVF-201-NNJ Main Site2 - appliance	☐	+ X

Below the table, the 'VPN settings' section shows 'Peer SGT capable' with a red box around the 'Enabled' button and a 'Disabled' button.

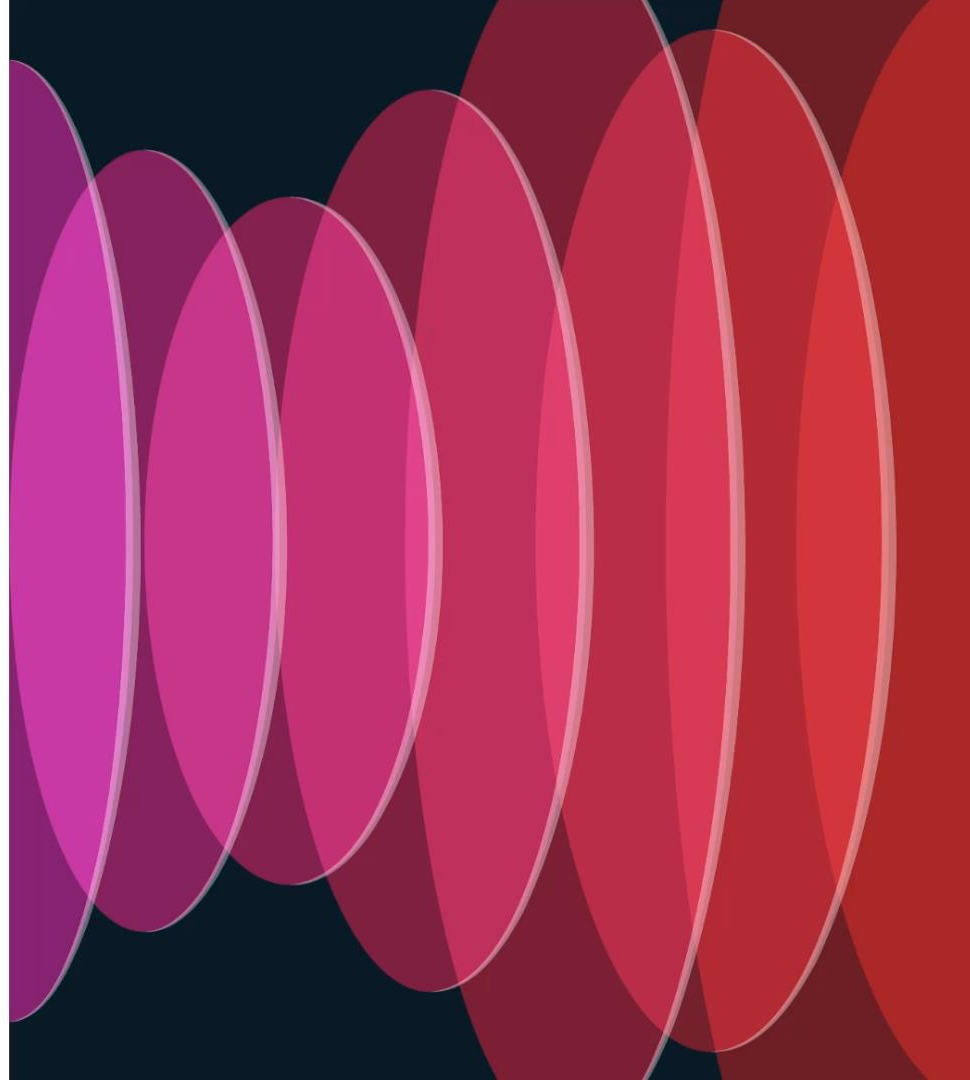
← Hub

Spoke →

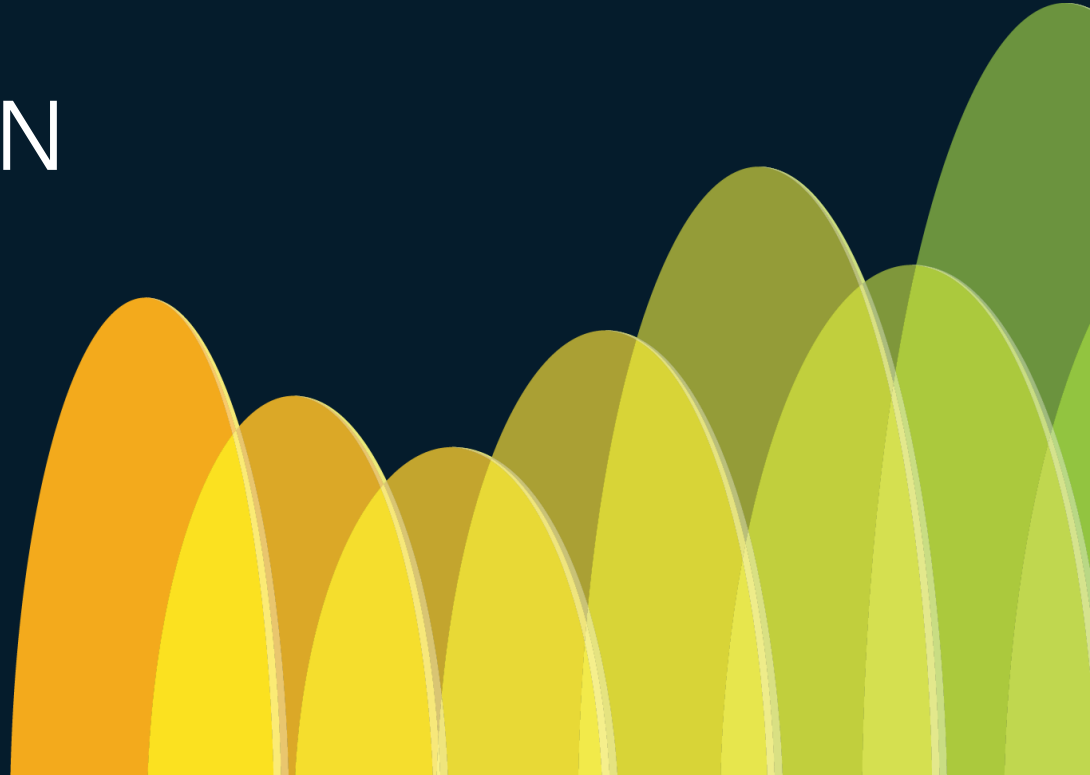


The screenshot shows the Cisco Meraki dashboard for a specific network. The left navigation menu is the same as the previous screenshot. The main content area is titled 'VPN settings' and shows 'Peer SGT capable' with a red box around the 'Enabled' button and a 'Disabled' button. Below this, the 'Local networks' section states 'No local subnets advertised.' with a link 'Add a local network'. The 'NAT traversal' section has two options: 'Automatic' (selected) and 'Manual: Port forwarding'.

Meraki Adaptive Policy Demo

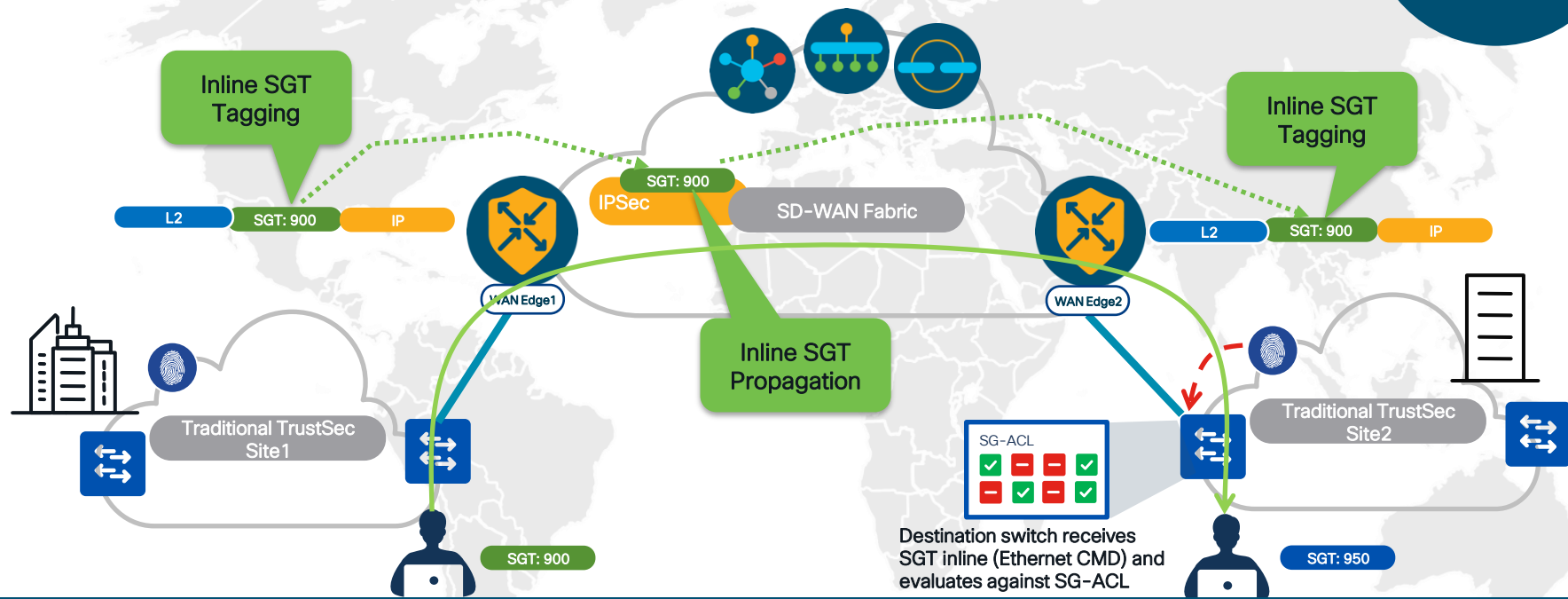


Catalyst SD-WAN Manager – Data Plane tagging



SGT inline tagging and propagation

SD-WAN transparently connects user groups across campus and branches



SGT-based Policy for Traffic between TrustSec/SDA and TrustSec/SDA sites

Catalyst SD-WAN Manager configuration - LAN

Device Templates

Feature Templates

Feature Template > Cisco VPN Interface Ethernet > BR-LAN-Sub-IF-100-CTS_v1

Device Type

ISR4331,C8300-1N1S-6T,C8200-1N-4T

Template Name*

BR-LAN-Sub-IF-100-CTS_v1

Description*

BR LAN Sub Interface 100 Template with CTS enabled v1

Basic Configuration

Tunnel

NAT

VRRP

ACL/QoS

ARP

TrustSec

Advanced

TrustSec

Default is Off

Enable SGT Propagation

On

Off

Propagate

On

Off

Security Group Tag

2

Trusted

On

Off

Enable Enforcement

On

Off

Enforcement Security Group Tag

Catalyst SD-WAN Manager configuration – WAN

Device Templates

Feature Templates

Feature Template > Cisco VPN Interface Ethernet > BR-WAN-MPLS-IF-1-CTS_v1

Device Type

ISR4331,C11111X-8P,C1121-8PLTEPW*,C8000v,C8300-1N1S-6T,C8200-1N-4T

Template Name*

BR-WAN-MPLS-IF-1-CTS_v1

Description*

BR WAN MPLS Interface Template with CTS v1 - Baseline

Basic Configuration

Tunnel

NAT

VRRP

ACL/QoS

ARP

TrustSec

Advanced

✓ TUNNEL

Tunnel Interface

🌐

☒ On

☐ Off

Per-tunnel Qos

✓

☐ On

☒ Off

Color

🌐

mpls

▼

CTS SGT Propagation

🌐

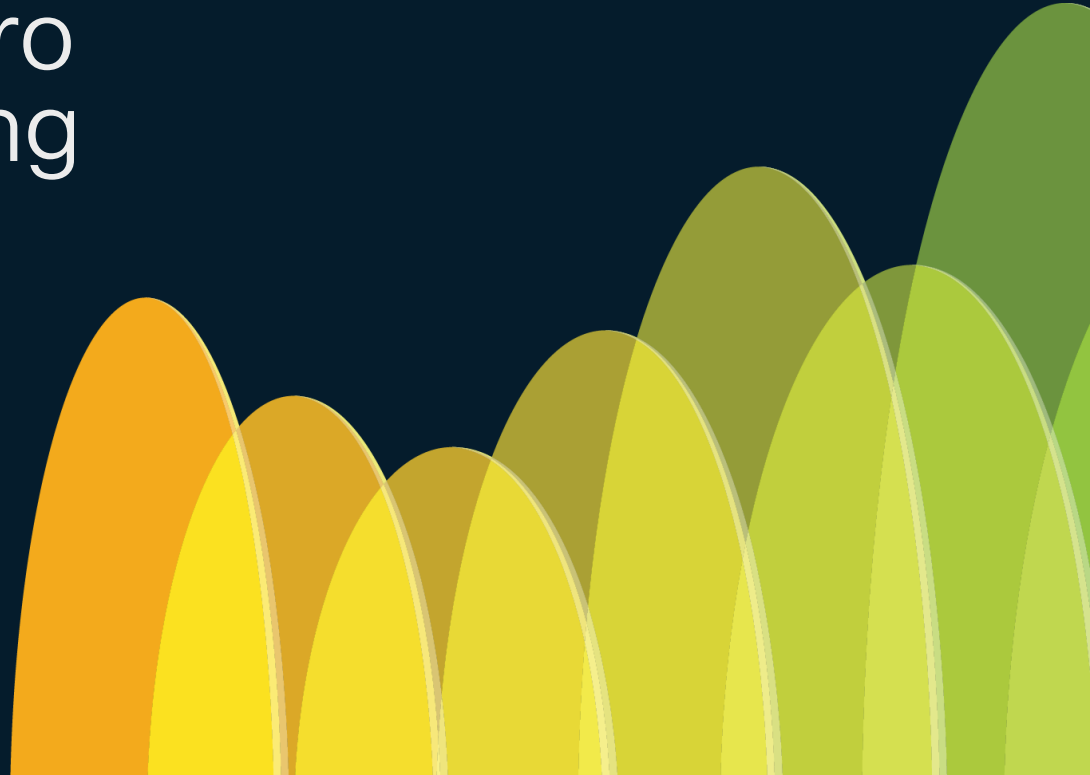
☒ On

☐ Off

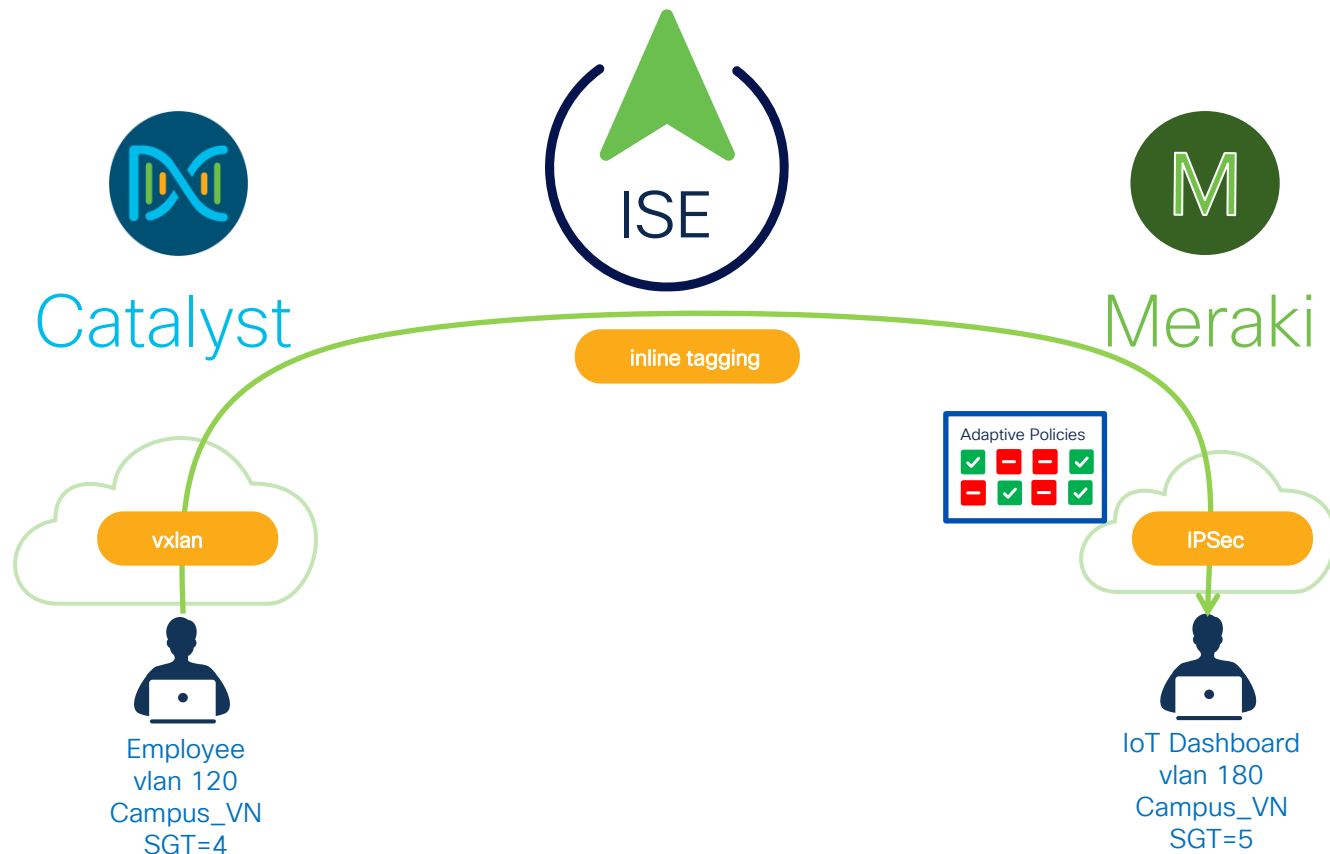
?

Default is Off

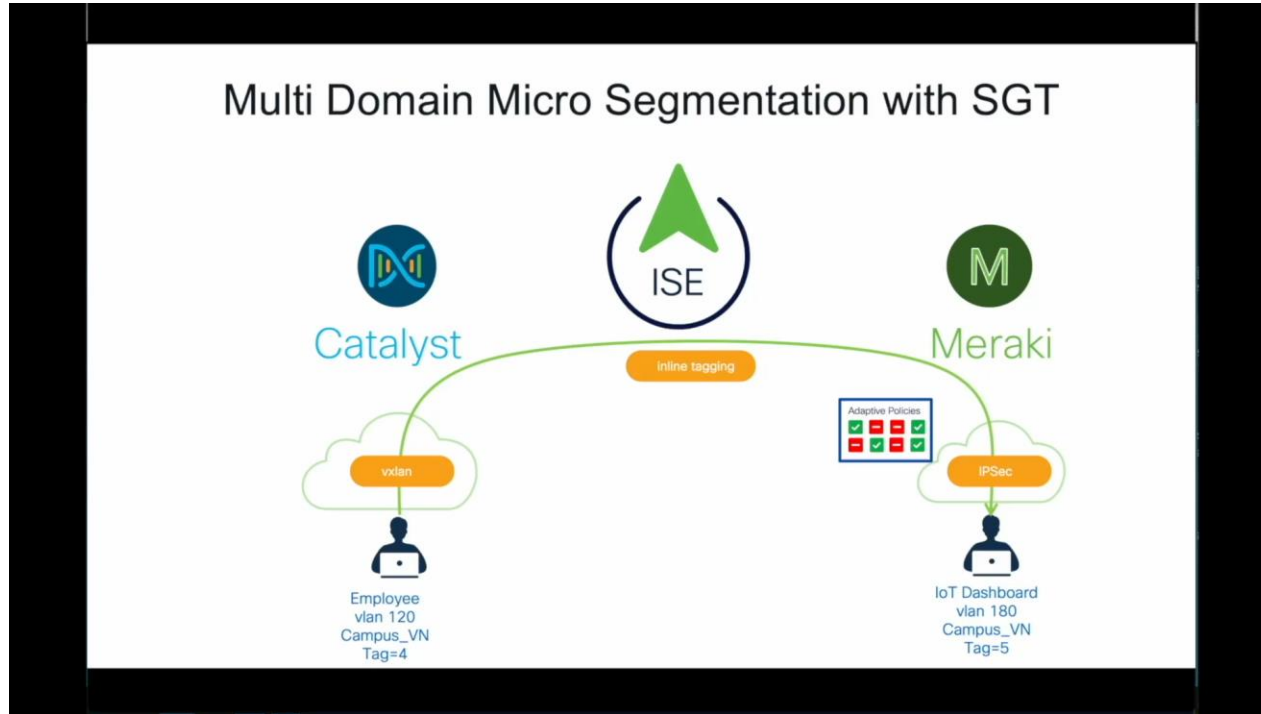
Multi-Domain Micro Segmentation using SGTs - Demo



Multi Domain Micro Segmentation with SGT



Catalyst and Meraki End-to-End Segmentation Demo



Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand
- Visit [cisco validated communities](#) for more content

Contact me at: Amitsi4@cisco.com



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC