



The bridge to possible

Segmentation with Cisco Catalyst SD-WAN and ISE

Steve Penland – Solutions Engineer
BRKENT-2166

CISCO *Live!*

#CiscoLive

Cisco Webex App

Questions?

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

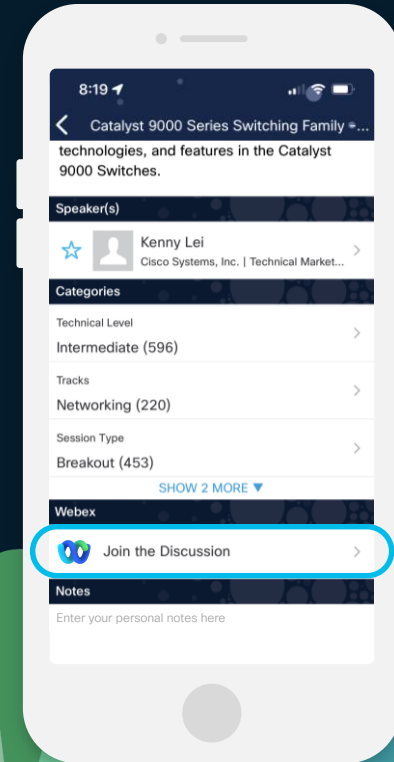
How

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

Webex spaces will be moderated by the speaker until June 7, 2024.

CISCO *Live!*

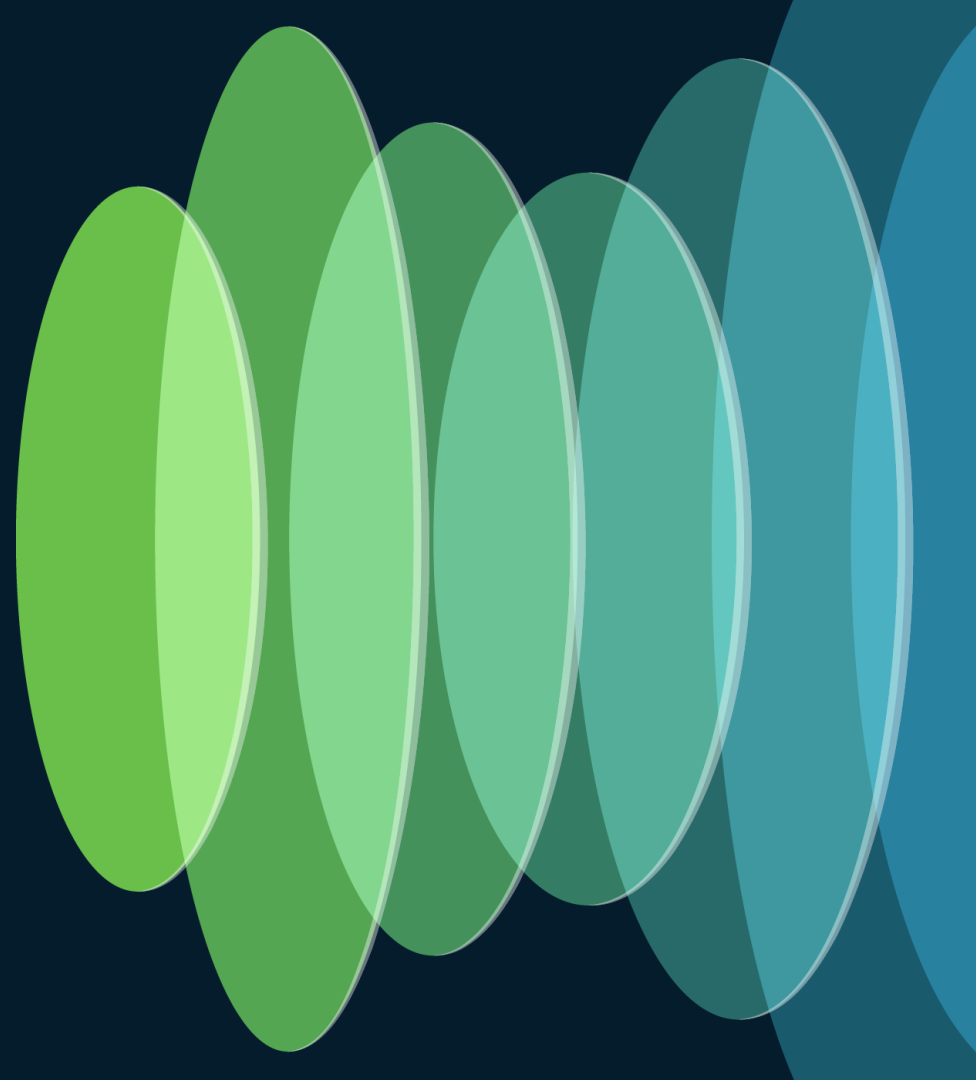
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2166>



Agenda

- Introduction
- Macrosegmentation
- Microsegmentation
- Demo
- Identity Based FW Rules
- Conclusion

Introduction



Why is network segmentation important?



National Security Agency | Cybersecurity Information Sheet

Advancing Zero Trust Maturity Throughout the Network and Environment Pillar

Executive summary

After gaining access to an organization's network, one of the most common techniques malicious cyber actors use is lateral movement through the network, gaining access to more sensitive data and critical systems. The Zero Trust network and environment pillar curtails adversarial lateral movement by employing controls and capabilities to logically and physically segment, isolate, and control access (on-premises and off-premises) through granular policy restrictions.

<https://media.defense.gov/2024/Mar/05/2003405462/-1/-1/0/CSI-ZERO-TRUST-NETWORK-ENVIRONMENT-PILLAR.PDF>

The fundamentals of segmentation

- Identify device/user and determine access to network
 - Is the user trusted and on a managed device?
 - If unmanaged is the device allowed on the network?
 - Is the device patched and in compliance?
- Assign to segment
 - VLAN, VRF, SGT
- Create and enforce policy
 - Which segments are allowed to communicate with each other and over what protocols?

Challenges of creating end to end segmentation

- VLANs and ACLs
 - Traditionally static and managed per device
 - IP based
- VRF
 - Multi VRF over private transport can be expensive
 - Multi VRF over internet requires an overlay with complex configuration
- SGTs
 - Maintaining SGT markings end to end can be challenging
 - IP to SGT binding scale

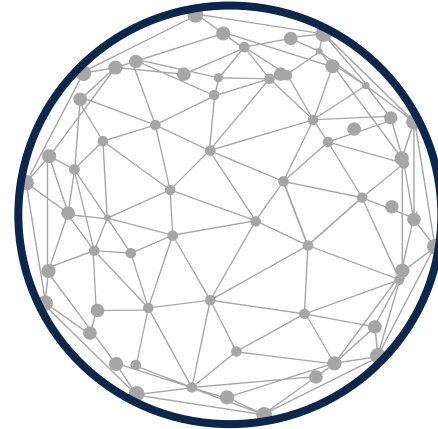
ISE and SD-WAN enable segmentation



Policy engine



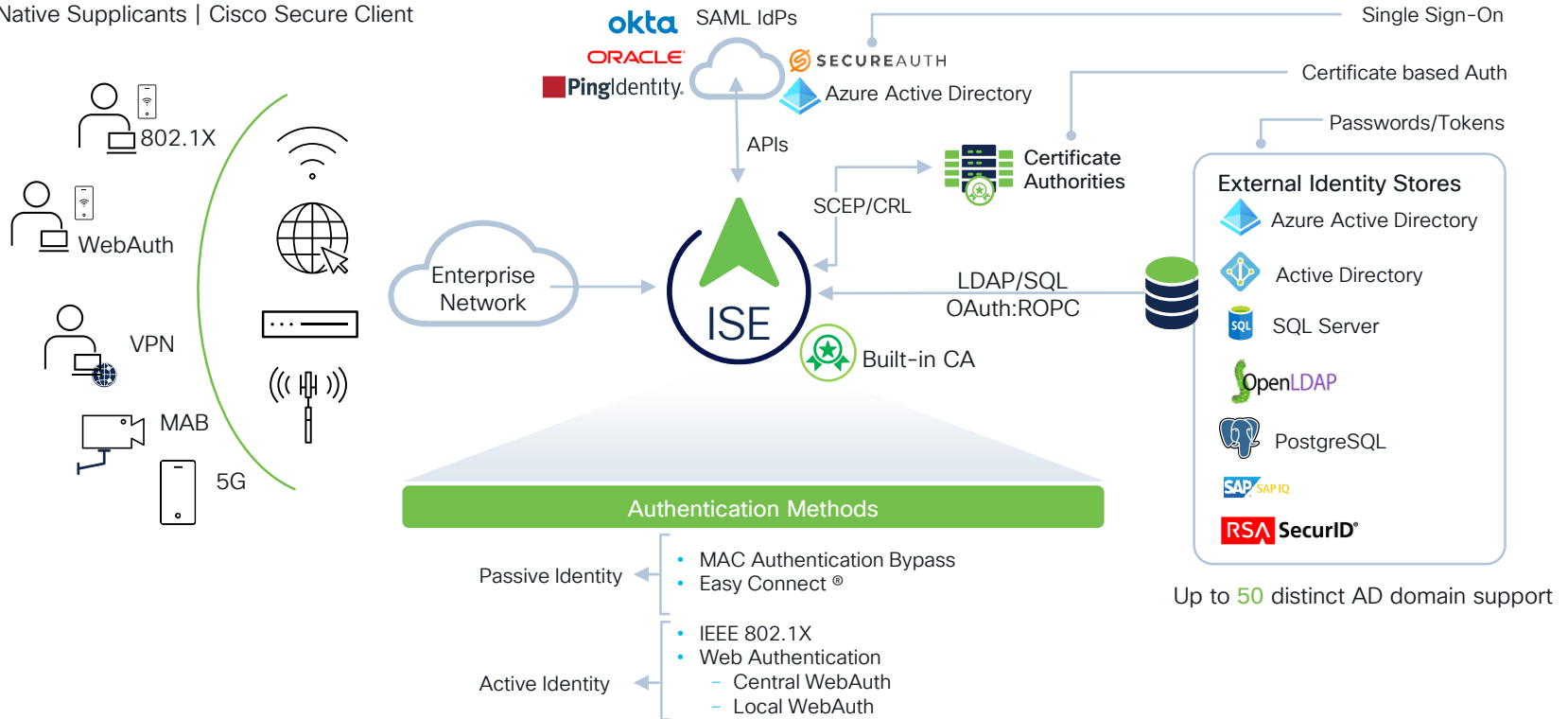
Catalyst SD-WAN



Transport and enforcement

ISE Secure Access Control Options

Native Applicants | Cisco Secure Client



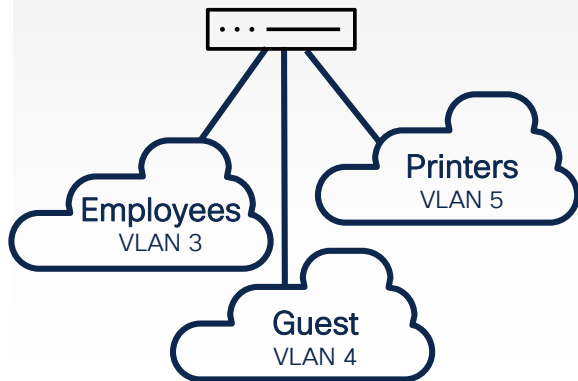
Up to 50 distinct AD domain support

Authorization Enforcement Options

Beyond RADIUS Access-Accept / Access-Reject

VLANs

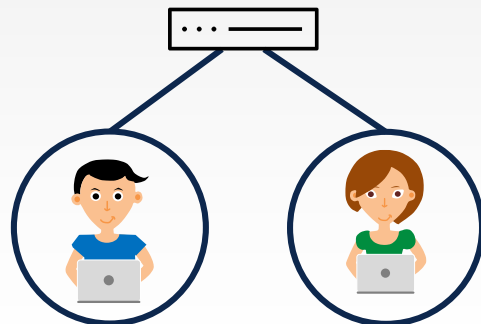
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

Downloadable ACL (Wired) or
Named ACL (Wired + Wireless)



Employee
permit ip any any

Contractor
deny ip host <critical>
permit ip any any

Security Group Tags

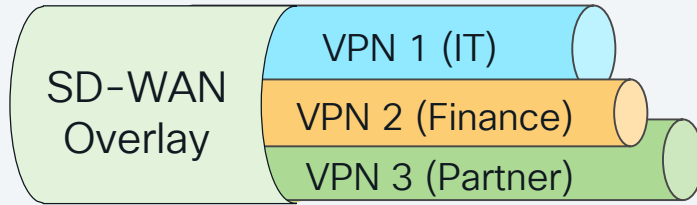
Cisco Group-Based Policy



16-bit SGT assignment and
SGT based Access Control

Segmentation is built into SD-WAN

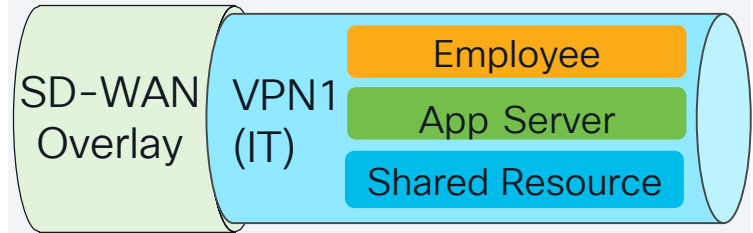
Macro Segmentation



VPN Level Segmentation

- IT VPN
- Finance VPN
- Partner VPN

Micro Segmentation

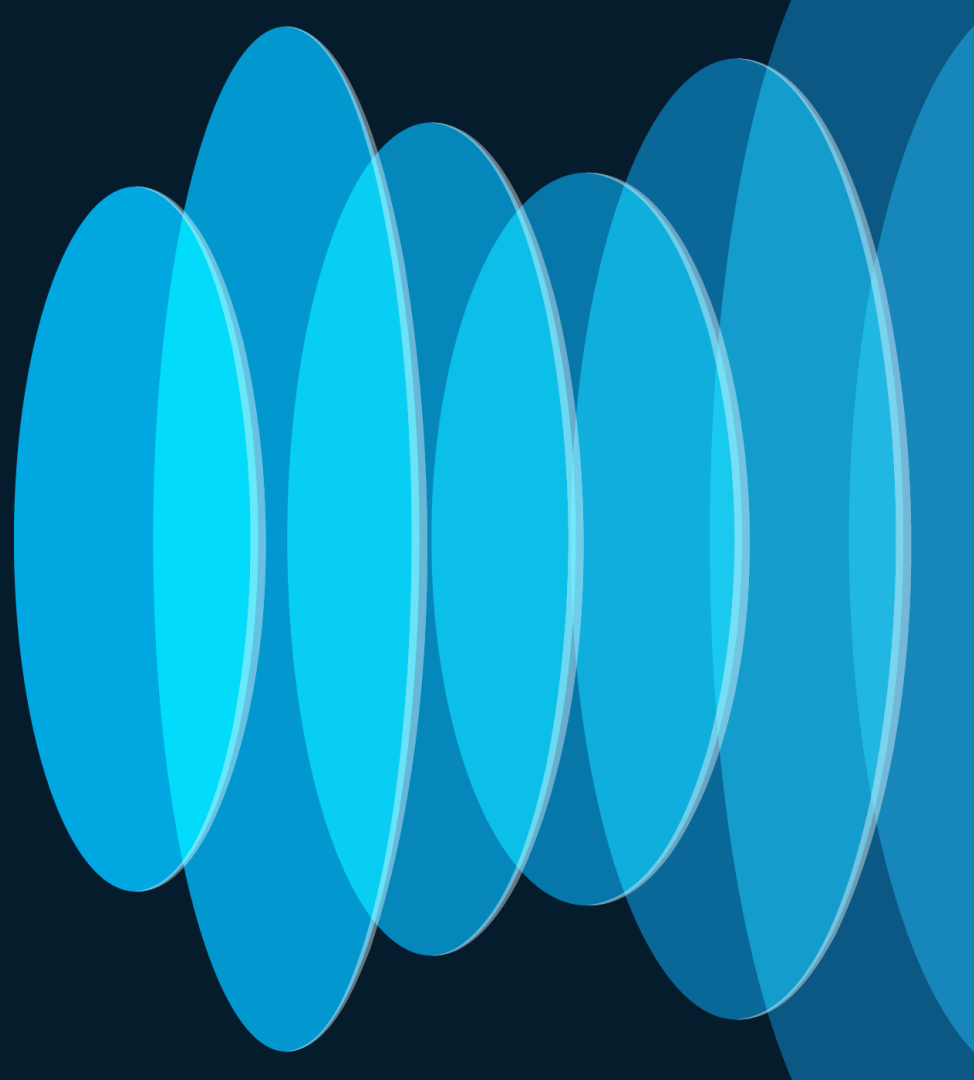


Group Level Segmentation

Example: IT VPN

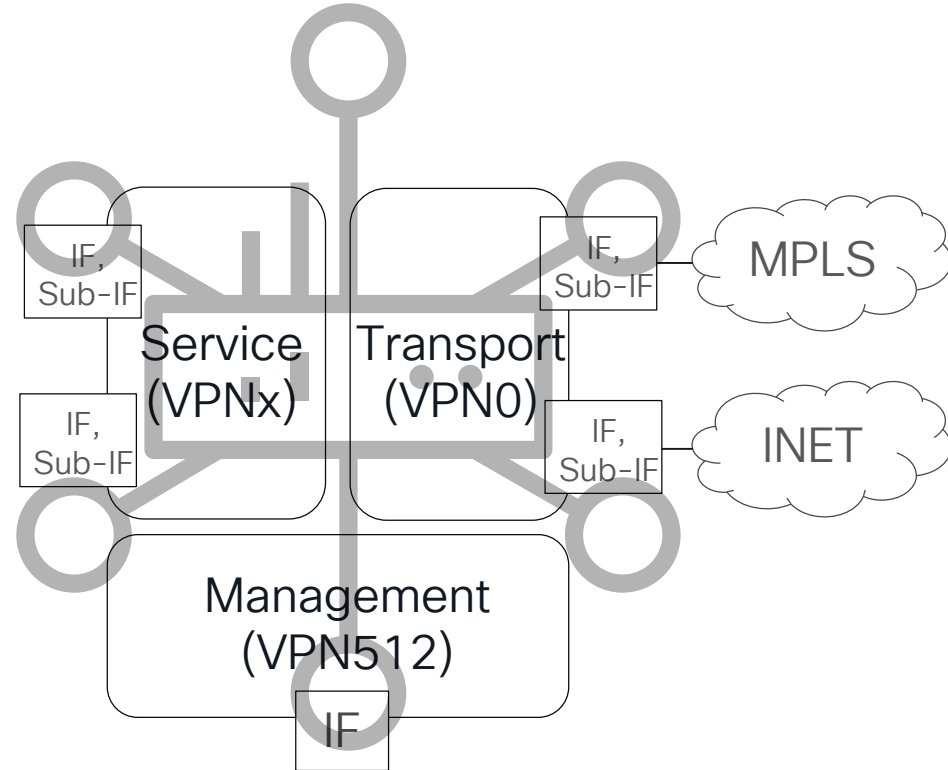
- Employee
- App Server
- Shared Resource

Macro Segmentation



What is a VRF or VPN?

- VRF and VPN both refer to the same thing.
 - Traditionally Cisco has used VRF
 - Catalyst SD-WAN uses the term VPN
- Separate routing domains
- By default, a device in one VPN cannot talk to a device in another VPN.

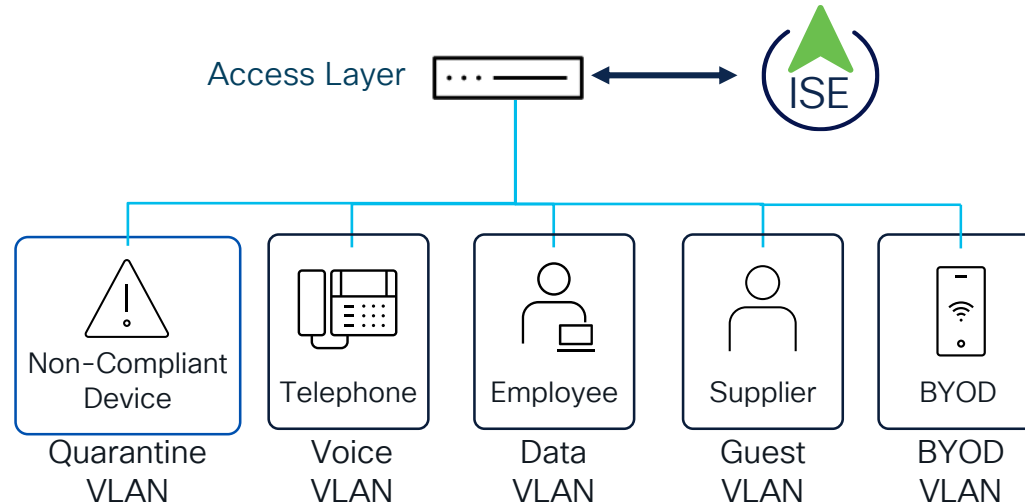


Common Uses

- Segmenting devices that should have very limited (controlled) needs to communicate outside their VPN.
 - Employees
 - Guest Users
 - IOT Devices
- Compliance – PCI DSS, HIPPA, NERC CIP, etc...
- Mergers and acquisitions

How are users/devices placed into the correct VPN

- Endpoint is attached to the network access device (NAD).
- NAD communicates with ISE (RADIUS) to authenticate the device.
- If authentication is successful ISE provides the NAD the dynamic VLAN assignment and dynamic ACL.



ISE Default Authentication Policy

The screenshot displays the Cisco Identity Services Engine (ISE) interface for managing authentication policies. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Policy / Policy Sets'. A sidebar on the left contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy (highlighted), Administration, Work Centers, and Interactive Features. The main content area shows a list of authentication policies under the heading 'Authentication Policy(3)'. The table has columns for Status, Rule Name, Conditions, Use, Hits, and Actions. Three policies are listed: MAB, Dot1X, and Default. The MAB and Dot1X policies are grouped under 'Default Conditions' by a blue box and arrow. The Default policy is expanded to show 'Identity Stores' under the 'Options' section, also highlighted by a blue box and arrow.

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB			
✓	Dot1X	OR Wired_802.1X Wireless_802.1X			
✓	Default				

Default Conditions

Identity Stores

ISE Default Authentication Policy

External Identity Sources

- > Certificate Authentica...
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

Internal Endpoints

Options

- If Auth fail: REJECT
- If User not found: CONTINUE
- If Process fail: DROP

All_User_ID_Stores

Options

- If Auth fail: REJECT
- If User not found: REJECT
- If Process fail: DROP

MAB

DOT1X

ISE Default Authorization Policy

Authorization Policy(12)

Status	Rule Name	Conditions	Results
✓	Wireless Block List Default	AND Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blocked List	Block_Wireless_Access
✓	Profiled Cisco IP Phones	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones
✗	Unknown_Compliance_Redirect	AND Network_Access_Authentication_Passed Compliance_Unknown_Devices	Cisco_Temporal_Onboard

If

Then

ISE Authorization Profile

* Access Type **ACCESS_ACCEPT** ▼

Network Device Profile  Cisco ▼ 

Service Template

Track Movement 

Agentless Posture 

Passive Identity Tracking 

▼ Common Tasks

ACL IPv6 (Filter-ID)

Security Group 

VLAN

Tag ID **1**

[Edit Tag](#)

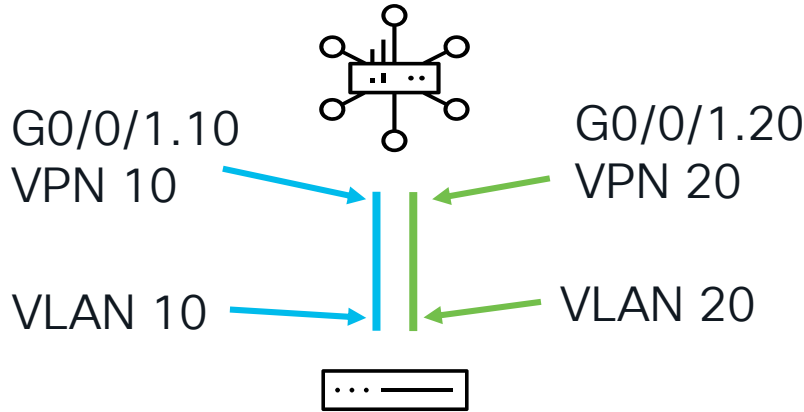
ID/Name **VLAN10** ▼

Assign
VLAN

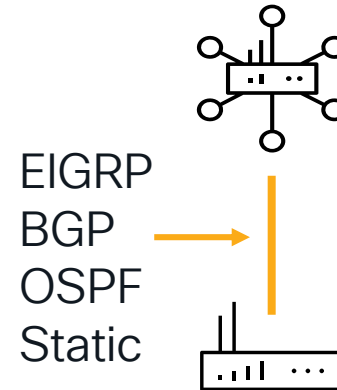


Connecting the LAN to the WAN

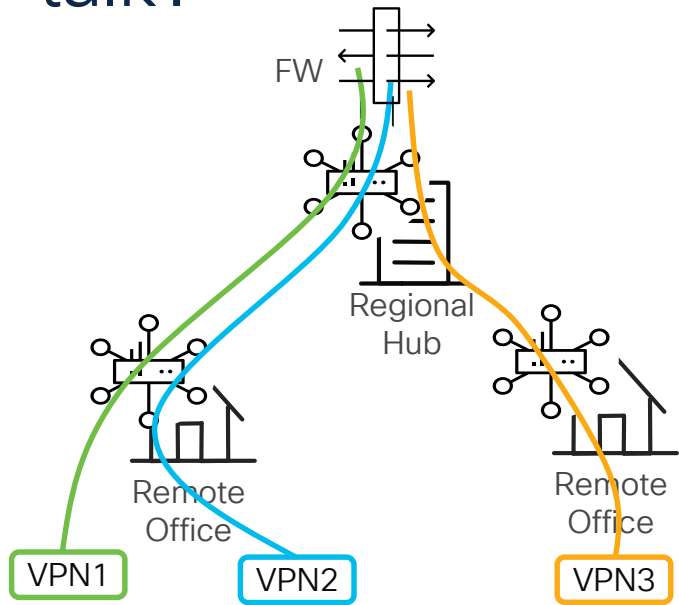
L2 trunk from LAN to WAN
with router sub interfaces in
different VPNs



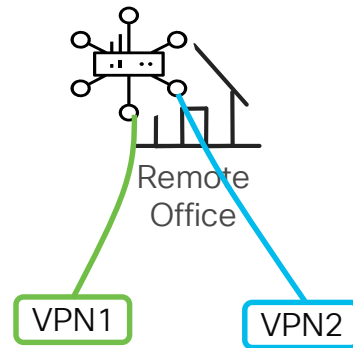
VRF aware routing protocol
between LAN and WAN.



What if devices in two different VPNs need to talk?

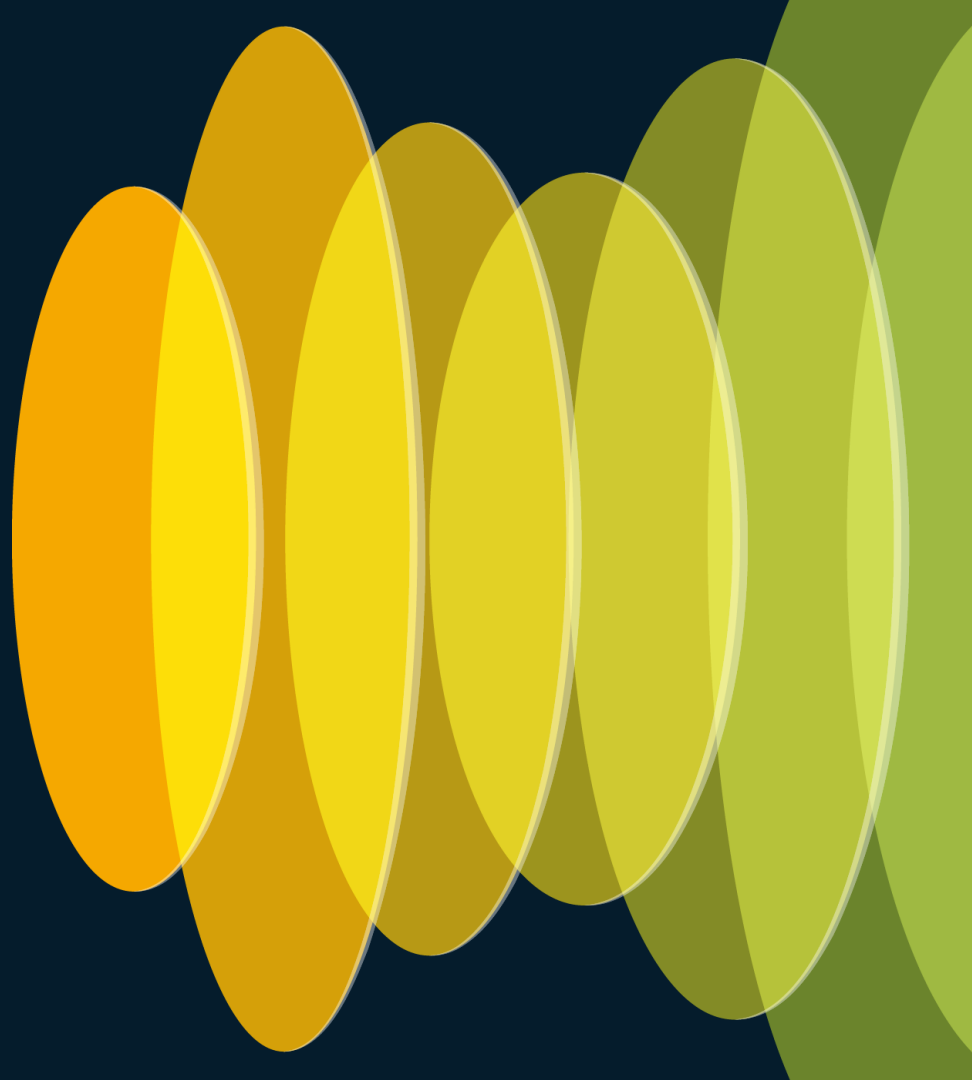


Route through aggregation point.



Local VPN leaking with built in NGFW capabilities.

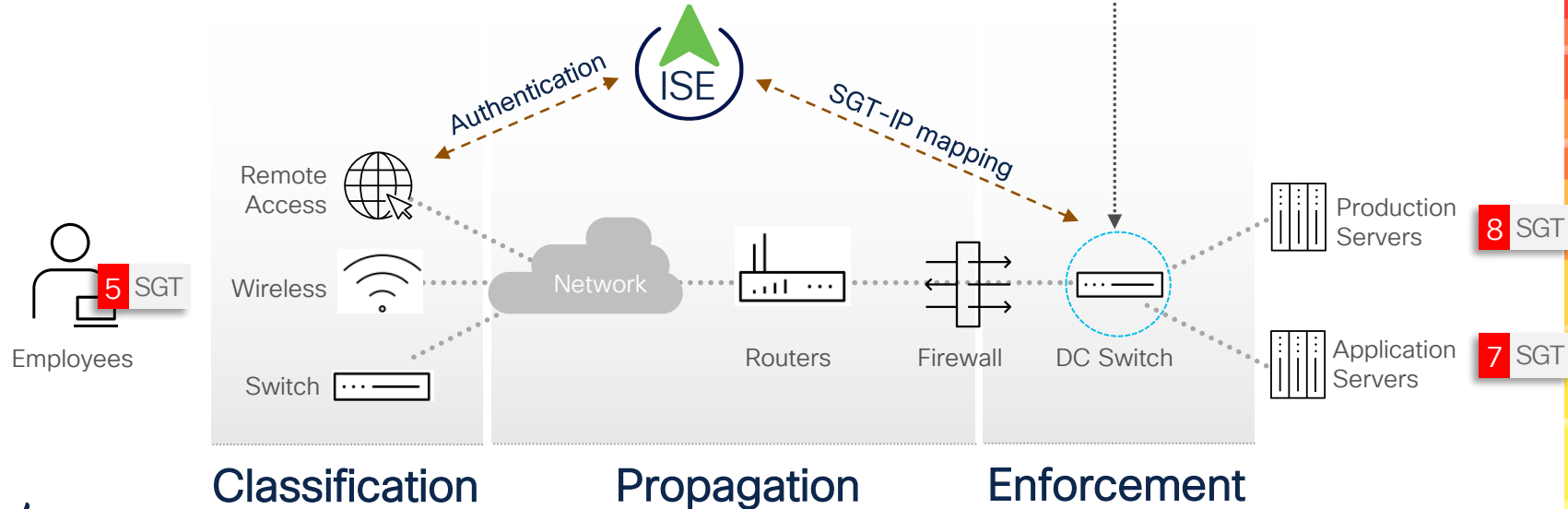
Microsegmentation with SGTs



Cisco TrustSec overview

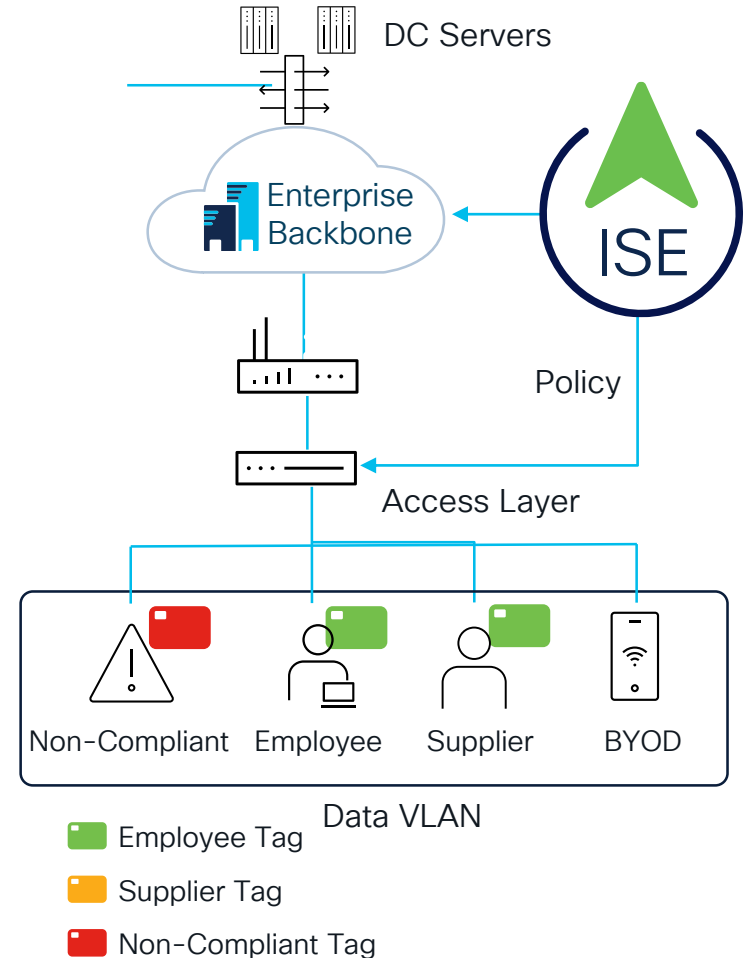
Segmenting with Security Group Tags (SGTs)

		Destination	
Egress Policy		App_Serv	Prod_Serv
Source	Employee	Permit All	Deny All
	App_Serv	Permit All	Deny All
	Prod_Serv	Deny All	Permit All



SGT Classification

- SGTs are assigned to devices as they are authenticated onto the network.
 - 802.1x
 - MAB
 - Web Portal
- No VLAN change
- No topology change
- Packets are marked on ingress.



SGT Authorization Policy

Authorization Policy(12)

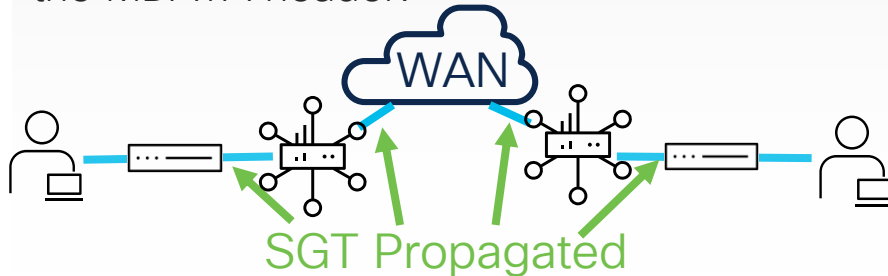
				Results
Status	Rule Name	Conditions	Profiles	Security Groups
⊕	Search			
⊗	NonCompliant_Devices_Redirect	AND Network_Access_Authentication_Passed Non_Compliant_Devices	Cisco_Temporal_Onboard	Quarantined_Systems
⊗	Compliant_Devices_Access	AND Network_Access_Authentication_Passed Compliant_Devices	PermitAccess	Employees
⊗	Employee_EAP-TLS	AND Wireless_802.1X BYOD_is_Registered EAP-TLS MAC_in_SAN	PermitAccess	BYOD
⊗	Employee_Onboarding	AND Wireless_802.1X EAP-MSCHAPv2	NSP_Onboard	BYOD
⊗	Wi-Fi_Guest_Access	AND Guest_Flow Wireless_MAB	PermitAccess	Guests

Propagation Methods

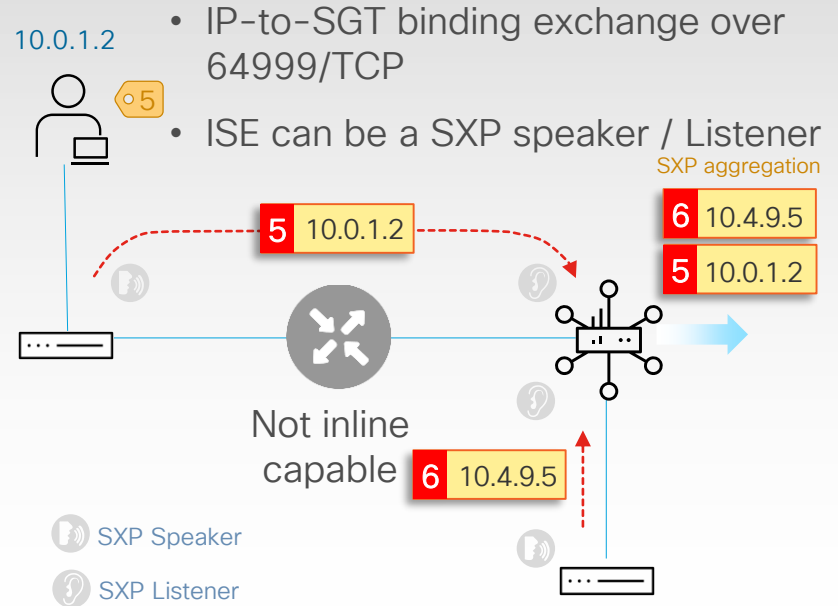
Inline Methods

Ethernet Inline Tagging:
(EtherType:0x8909) 16-Bit SGT encapsulated within Cisco Meta Data (CMD) payload.

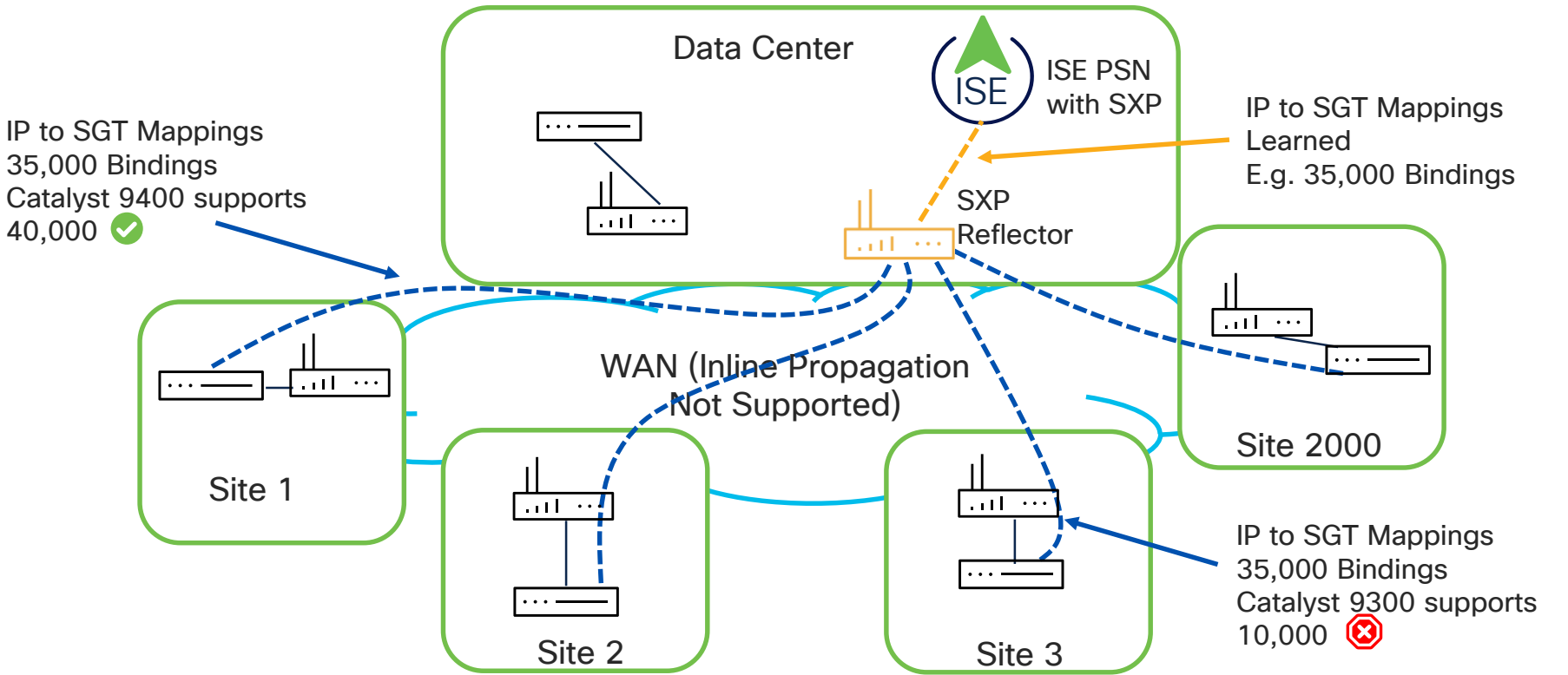
SD-WAN: Edge router picks up the SGT from the Ethernet frame and encodes it into the MDATA header.



SGT Exchange Protocol (SXP)



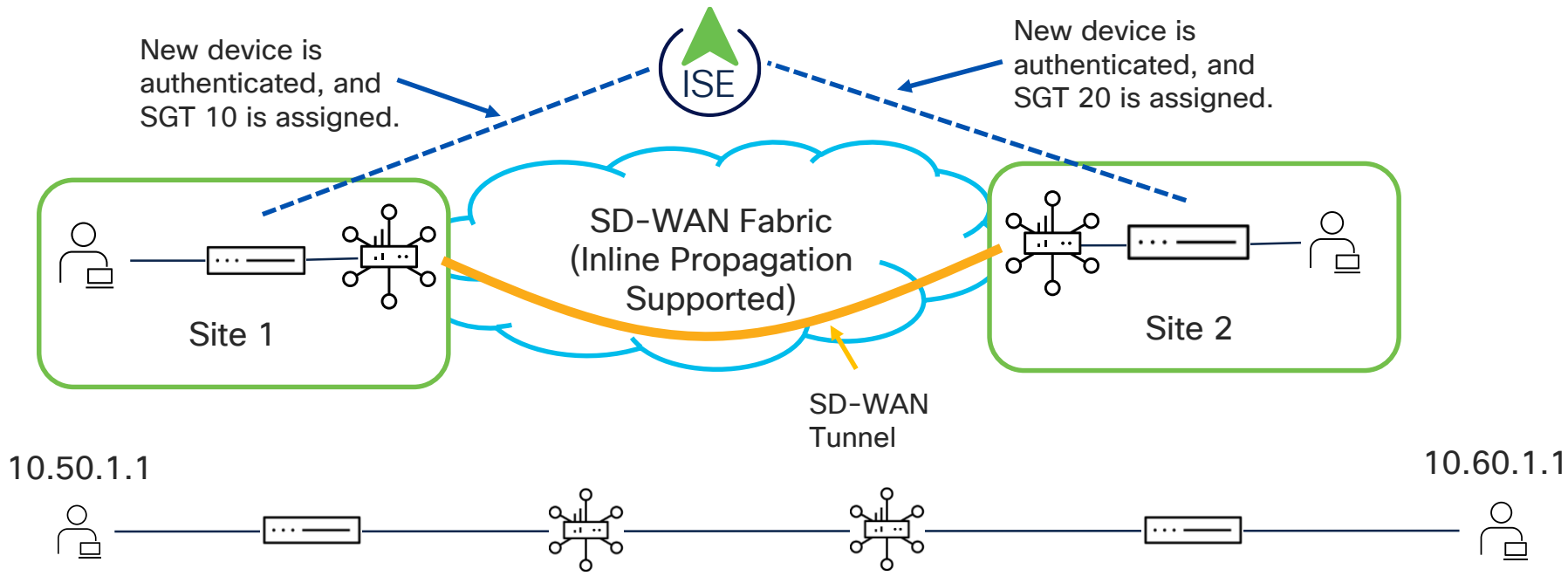
SXP Propagation Challenge



<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/policy-platform-capability-matrix.pdf>
https://www.cisco.com/c/en/us/td/docs/security/ise/performance_and_scalability/b_ise_perf_and_scale.html



SD-WAN inline propagation solves this problem.



Enable SGT propagation in SD-WAN

- WAN Interface
 - Enable CTS SGT Propagation for the tunnel.
 - No other changes to the WAN interface.

CTS SGT Propagation



```
interface Tunnel1
  no shutdown
  ip unnumbered GigabitEthernet1
  no ip redirects
  cts manual
  exit
  tunnel source GigabitEthernet1
  tunnel mode sdwan
```

Enables CTS SGT Propagation (will momentarily flap the interface).

Enable SGT propagation in SD-WAN

- LAN (Service Side) Interface
 - Enable CTS SGT Propagation
 - Only L3 interfaces supported
 - Set SGT value to be assigned to untagged packets
 - Mark the interface trusted.

TrustSec

Enable SGT Propagation	<input type="text" value="🌐"/>	<input checked="" type="radio"/> On <input type="radio"/> Off
Propagate	<input type="text" value="🌐"/>	<input checked="" type="radio"/> On <input type="radio"/> Off
Security Group Tag	<input type="text" value="🌐"/>	<input type="text" value="2"/>
Trusted	<input type="text" value="🌐"/>	<input checked="" type="radio"/> On <input type="radio"/> Off
Enable Enforcement	<input type="text" value="✔"/>	<input type="radio"/> On <input type="radio"/> Off
Enforcement Security Group Tag	<input type="text" value="✔"/>	<input type="text" value=""/>

Enable SGT propagation in SD-WAN

LAN (Service Side) Interface Configuration

Enables interface for SGTs
(will flap the interface and
also increase the MTU by 8
bytes)

Trust SGTs received on the
interface. If packet is
received without SGT
assign a source SGT of 2.

```
interface GigabitEthernet2
no shutdown
arp timeout 1200
vrf forwarding 10
ip address 10.10.10.1 255.255.255.252
no ip redirects
ip mtu 1500
load-interval 30
cts manual
policy static sgt 2 trusted
exit
```

TrustSec Policy

Production Matrix

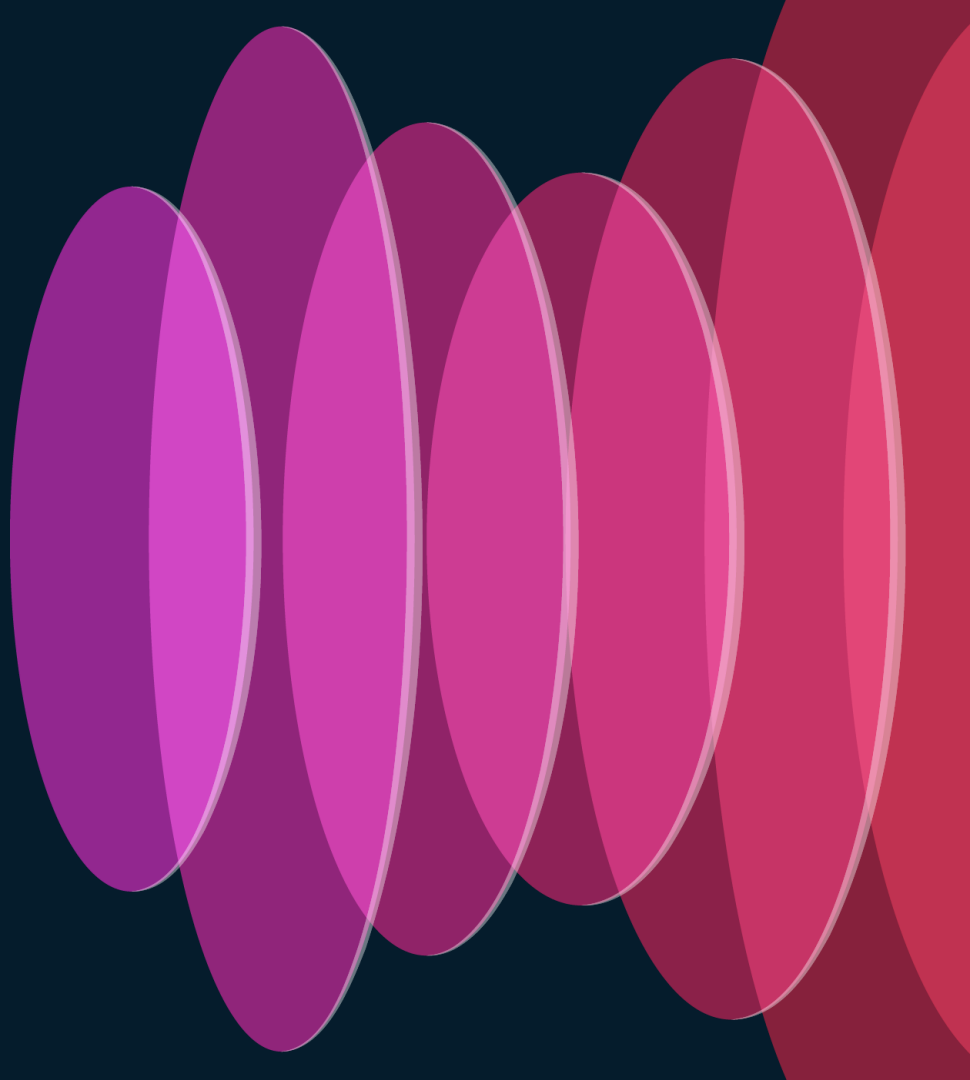
Populated cells: 53

Refresh

Edit Add Clear Deploy Verify Deploy Monitor All - Off Import Export View All

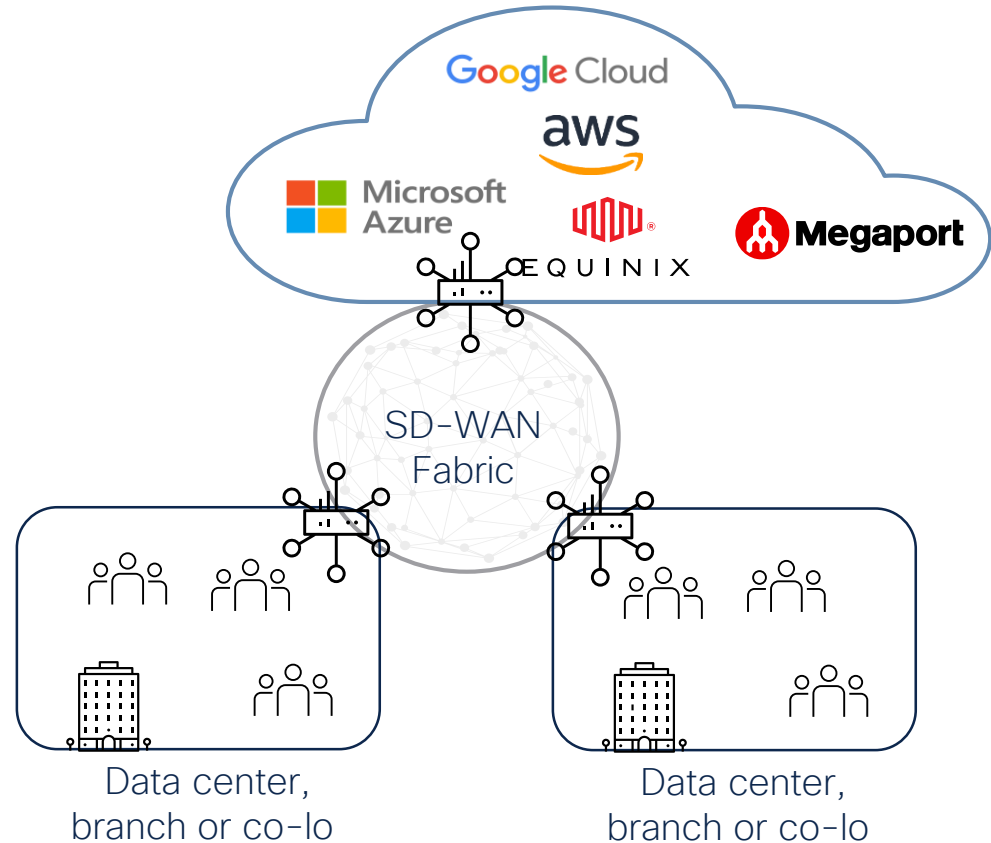
Destination ▶	BYOD 15/000F	Contractors 5/0005	Developers 8/0008	Development_Ser... 12/000C	Employees 4/0004	Guests 6/0006	Production_Serv... 11/000B	Quarantined_Sys... 255/00FF	TrustSec_Device... 2/0002	Unknown
Source ▼										
BYOD 15/000F		Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	permit_https	Deny IP		
Contractors 5/0005	Deny IP		Deny IP	Deny IP	Deny IP	Deny IP	permit_https	Deny IP	Deny IP	
Developers 8/0008						Deny IP		Deny IP		
Development_Ser... 12/000C						Deny IP		Deny IP		
Employees 4/0004				Deny IP			permit_https	Deny IP	permit_ssh	
Guests 6/0006	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP		Deny IP	Deny IP	Deny IP	
Production_Serv... 11/000B				Deny IP		Deny IP		Deny IP		
Quarantined_Sys... 255/00FF	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	

Microsegmentation with SD-WAN Enforcement



SD-WAN Router SGT Enforcement

- Site uses access switches which are not capable of inline tagging or enforcement.
- Small site without switch.
- SGT enforcement in the cloud / SDCI.



SD-WAN Router Setup

To allow SGACL download to the router RADIUS must be configured.

Start by creating one or more RADIUS servers.

Update Radius Server

Address	<input type="text" value="198.18.10.150"/>
Authentication Port	<input type="text" value="1812"/>
Accounting Port	<input type="text" value="1813"/>
Timeout	<input type="text" value="5"/>
Retransmit Count	<input type="text" value="3"/>
Key Type	<input type="radio"/> Key <input checked="" type="radio"/> PAC Key
Key	<input type="text" value="....."/>

SD-WAN Router Setup Continued

Create RADIUS group and configure CTS

VPN and Source Interface used for router to reach ISE

RADIUS server and RADIUS group created in previous step.

Update Radius Group

VPN ID	<input type="text" value="10"/>
Source Interface	<input type="text" value="Loopback10"/>
Radius Server	<input type="text" value="198.18.10.150 ✖"/>
CTS Authorization List	<input type="text" value="cts_lisst"/>
RADIUS group	<input type="text" value="radius-10"/>

SD-WAN Router Setup Continued

Configure SXP

Must match values in ISE

Device SGT

Credentials ID [trustsec_credentials_id]

Credentials Password [trustsec_credentials_pwd]

Enable Enforcement On Off

Enable SXP On Off

Source IP [sxp_source_ip]

Password

Node ID Type IP Interface Name 8 Char Hex String

Node ID [sxp_default_node_id]

SD-WAN Router Setup Continued

Configure SXP Peer

Peer IP	<input type="text" value="198.18.10.150"/>
Source IP	<input type="text" value=""/> <small>[sxp-connection_source-ip]</small>
Preshared Key	<input checked="" type="radio"/> Password <input type="radio"/> Key Chain <input type="radio"/> None
Mode	<input checked="" type="radio"/> Local <input type="radio"/> Peer
Mode Type	<input checked="" type="radio"/> Listener <input type="radio"/> Speaker <input type="radio"/> Both
Minimum Hold Time	<input type="text" value="0"/>
Maximum Hold Time	<input type="text" value="0"/>
VPN ID	<input type="text" value="10"/>

SGT Enforcement Verification

Network Wide Path Insights (NWPI) captures flow SGT information as well as SGACL enforcement.

The screenshot displays a network device interface with the following details:

- Hostname: AWS-USW-RTR1
- Event List: FIRST_PACKET
- Version: 17.12.03.0.3740, Input: GigabitEthernet2, Output: Tunnel100513
- Expand All Features (button)

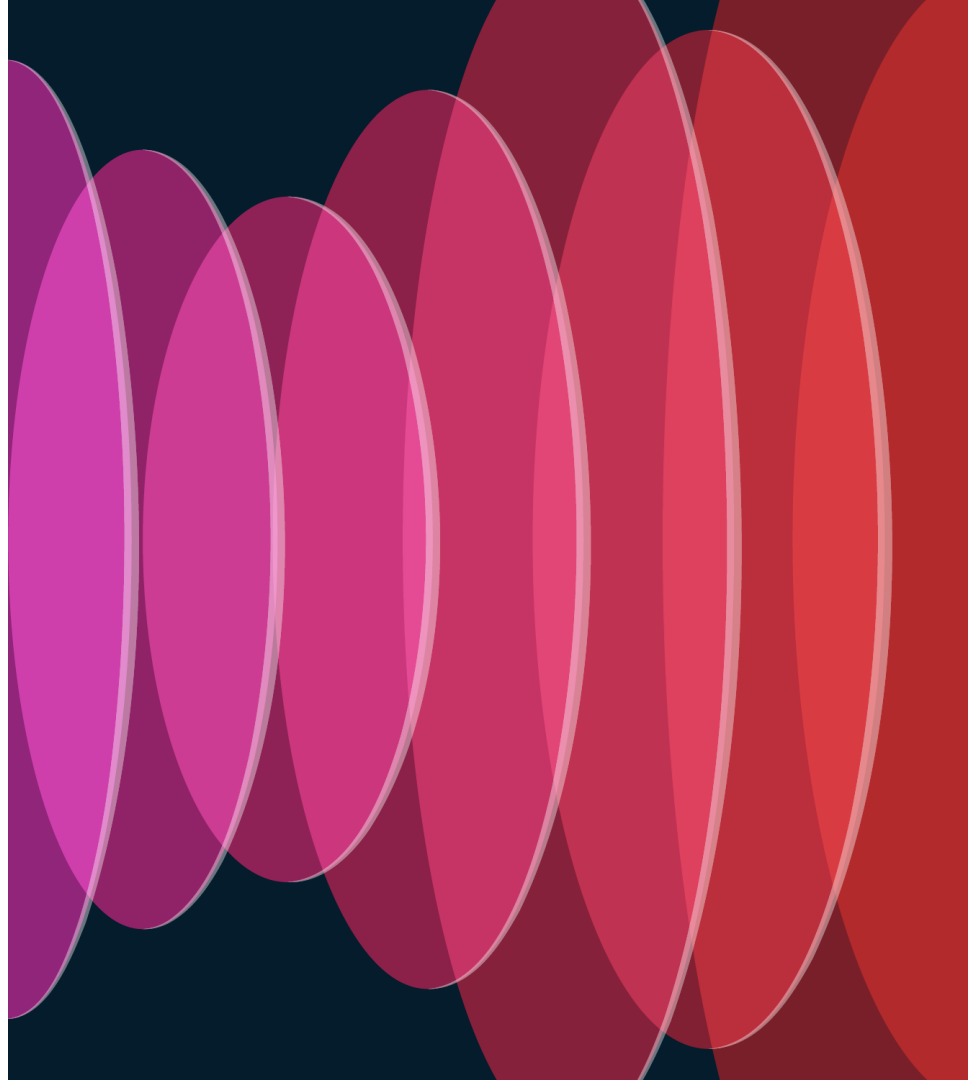
Ingress Feature	Egress Feature
<p>SDWAN Forwarding</p> <p>SDWAN lookup OCE: Input : GigabitEthernet2 Hash Value : 0 Encap : ipsec SLA : 0 SDWAN VPN : 1 SDWAN Proto : MDATA In Label : 1003 Local Color : public-internet Remote Color : public-internet FTM Tun ID : 5 SDWAN Session Info SRC IP : 10.30.1.152 SRC Port : 12347 DST IP : 128.107.219.49 DST Port : 12366 Remote System IP : 1.1.20.1 Lookup Type : TUN_DEMUX Service Type : NONE MDATA ver : 0x2 MDATA next proto : IPV4(0x1) MDATA num : 2 MDATA type : SGT_TYPE(0x1) MDATA SGT : 10 MDATA type : NWPI_TYPE(0x2)</p>	<p>CTS_OUTPUT_SGACL</p> <p>Input : Tunnel2 Output : Tunnel100513 Action : SGACL_DENY Source SGT : 10 Destination SGT : 20 SGACL ID : 0x5 ACE ID : 0x1</p> <p>DROP_REPORT</p> <p>Drop Cause : Ipv4Ac1 Input : Tunnel2 Output : Tunnel100513</p>

Useful Monitoring Commands

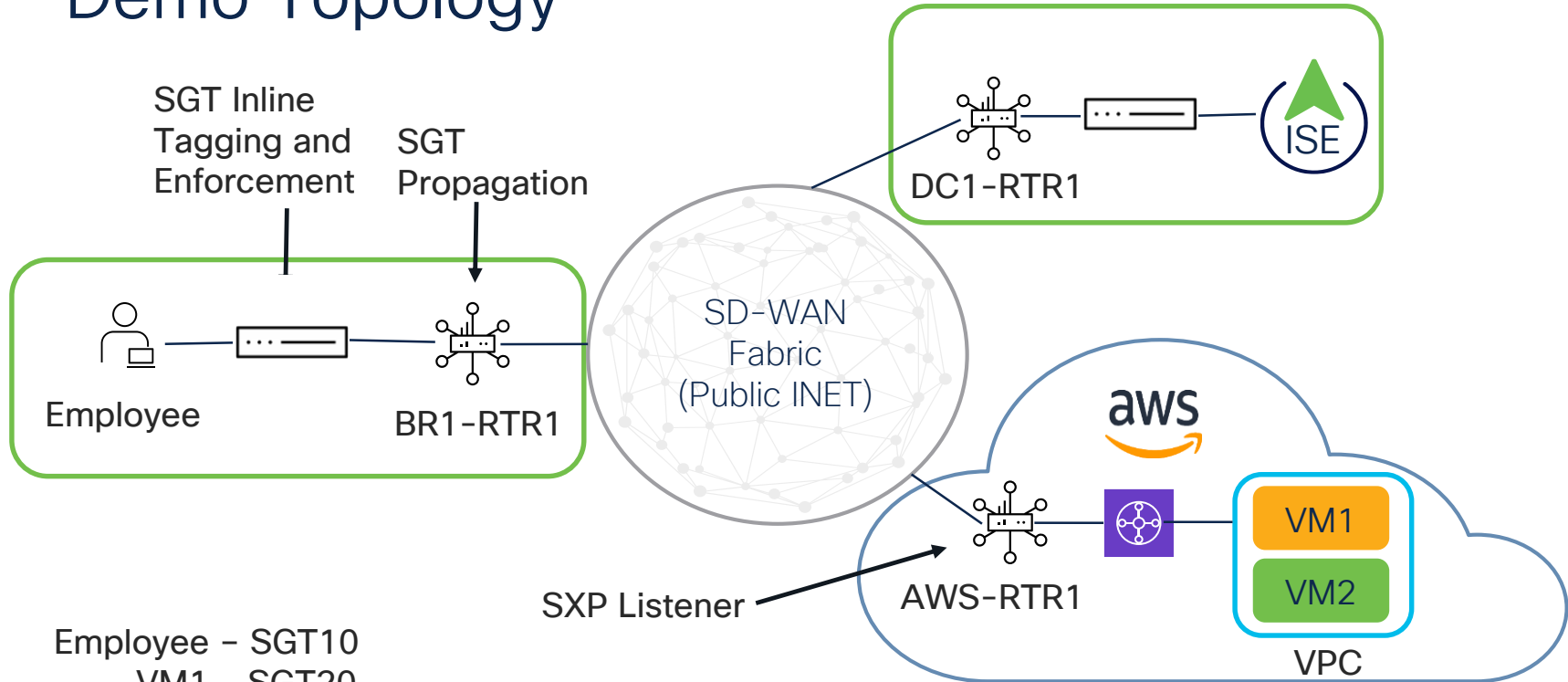
- show cts pac – *verify RADIUS*
- show cts environment-data – *verify CTS SGT download*
- show cts role-based sgt-map – *verify IP to SGT bindings*
- show cts sxp connections – *verify connection to SXP server*
- show cts role-based permissions – *verify SGACLs*
- show cts role-based counters – *verify SGACL enforcement*

Demo

CISCO *Live!*

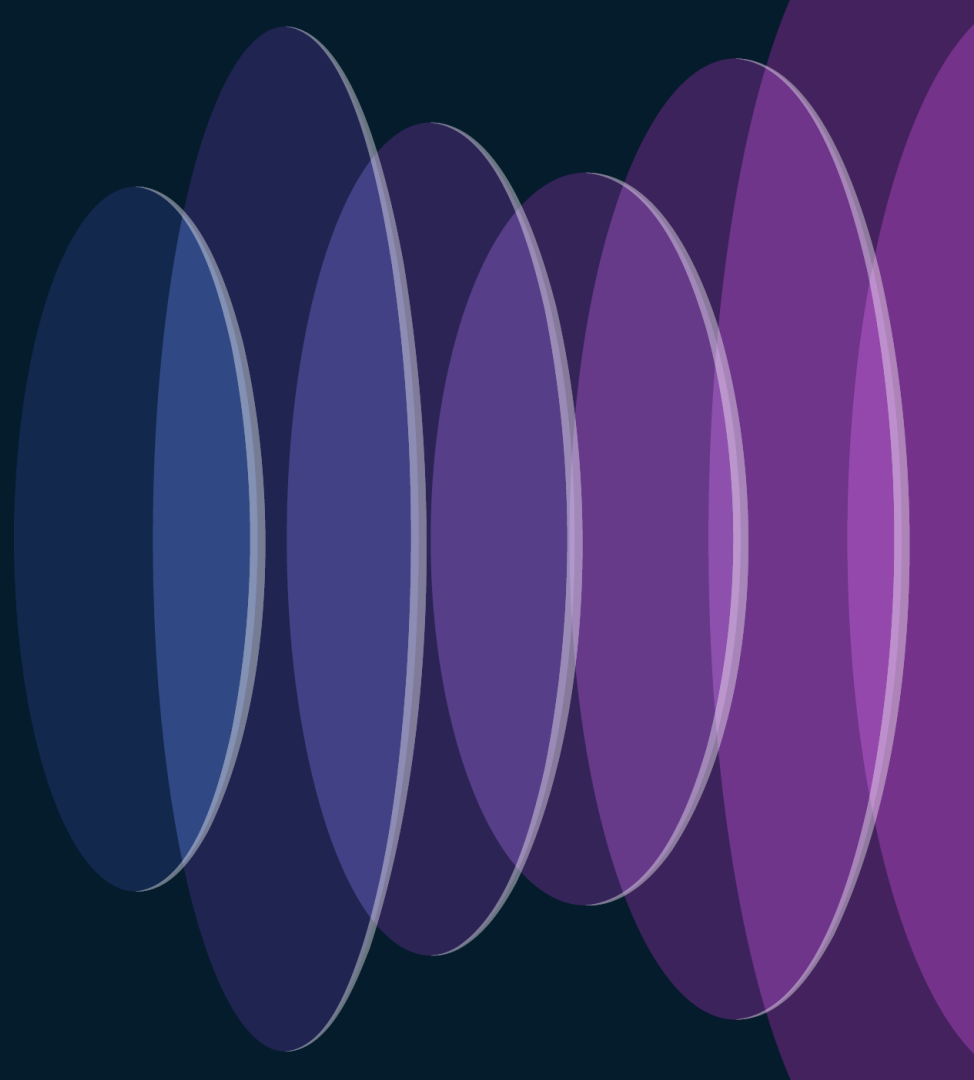


Demo Topology



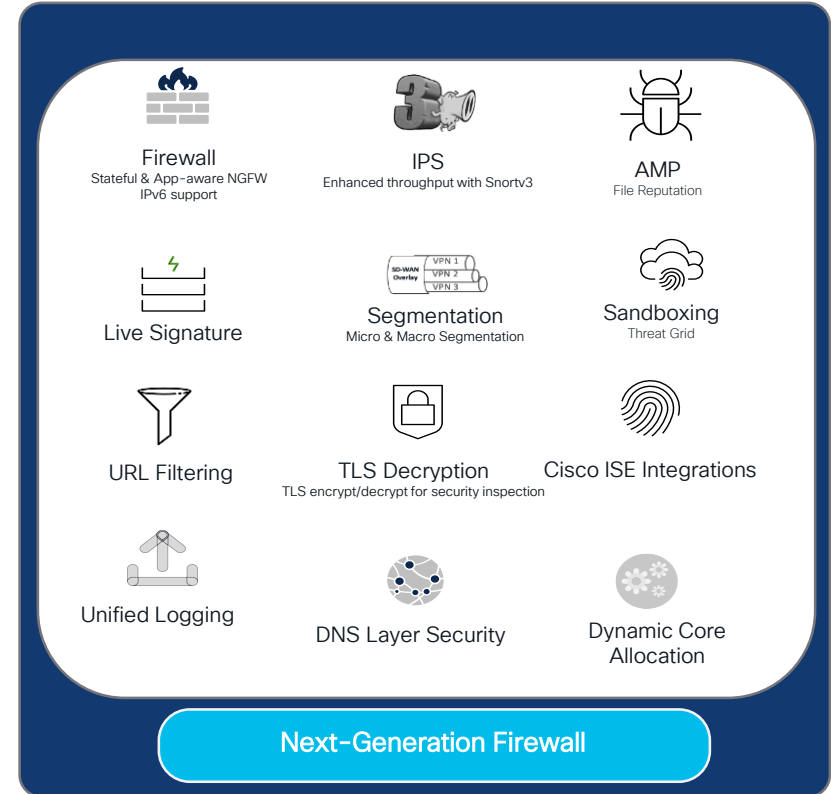
Employee - SGT10
VM1 - SGT20
VM2 - SGT30

SD-WAN Identity based FW

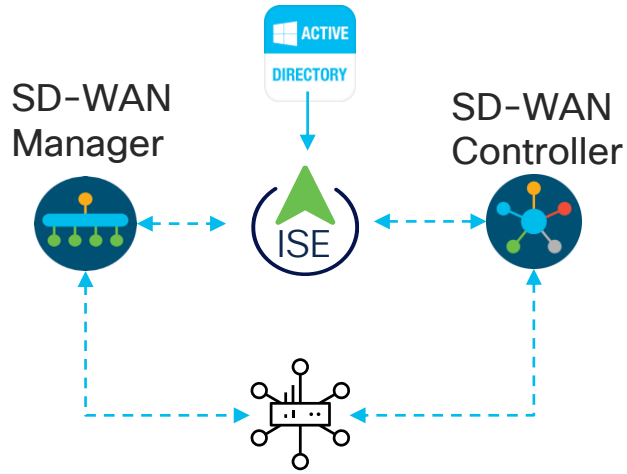


Cisco SD-WAN NGFW Capabilities

- Built into the SD-WAN solution is a NGFW feature set.
- Managed centrally from SD-WAN Manager
- Build on Cisco Talos Threat Intelligence Group



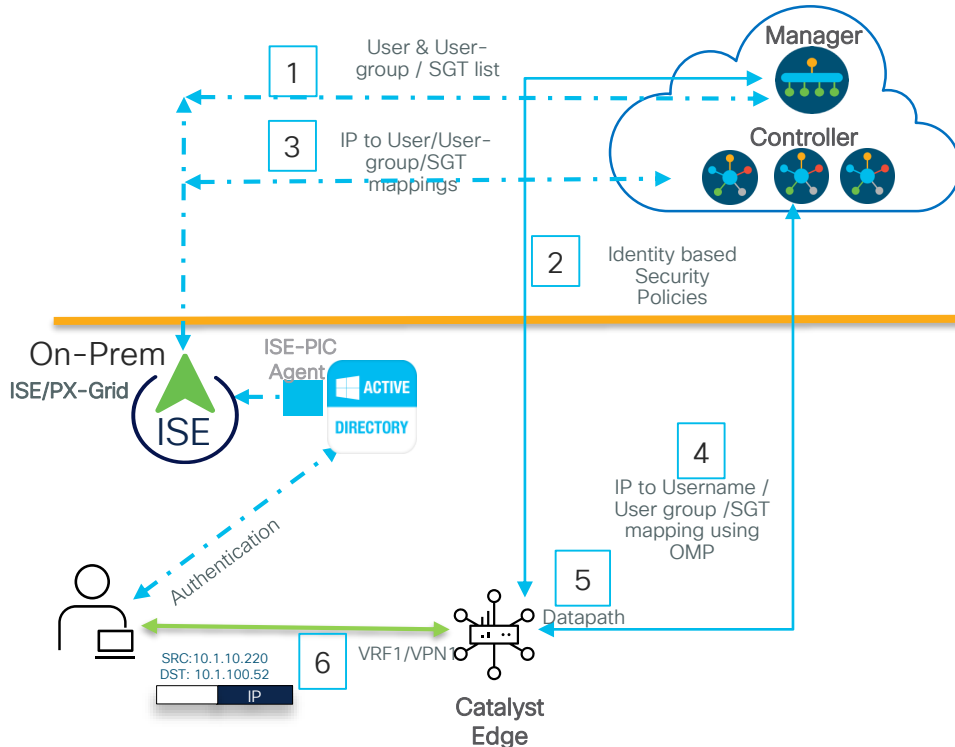
ISE/AD Integration for Identity based FW rules



- It is easier for any organization to define the Security policy based on Identities rather using IP addresses which provides the granular control over the users, groups, devices and applications.
- With Cisco ISE and AD Integration, Identity based Firewall rules can be defined under Security Policy. The Identity can be a User/User Group or Security Group tag (SGT)
- To support the Identity based Firewall rules, SD-WAN Controller and Manager works with ISE/pxGrid and Active Directory Services

Source	Destination	Application	Action
IP-Subnet1	Any	Any	Inspect
188.1.12.0/24	Geo-EU	Banking	Drop
Employees	Prod_SVR	Video Streaming	Inspect
SGT 12	Any	Video Streaming	Drop
Any	FQDN-1	Any	Inspect

ISE/AD Integration – Hi-Level Architecture



- Management Plane
 - (1) Manager obtains the User/User-group information from ISE/PxGrid
 - (2) Admin authors security policies using Username/User-group. vManage sends policies to the device
- Controller Distribution
 - (3) Controller obtains IP to Username / User to User-group mappings from ISE/PxGrid when a user logs in (ie., a session is created).
 - (4) Controller pushes the IP to Username / User to User-group mappings to device (These IP-user bindings are for the active users)
- Device - Control and Data-plane
 - (2) Catalyst Firewall rules with username / user-group provisioned via Manager and pushed to device
 - (4) Edge Device learns IP to username / user to user-group mappings.
 - (5) IP-User-group received from Controller and programmed in data path
 - (6) Edge Device receives flows and enforces the configured username/user-group based policies
- Logging and Reporting
 - Device includes identity information in show commands
 - Manager connection events include User information as applicable.

SD-WAN Manager / ISE Integration Setup

In Administration >
Integration
Management, add
ISE server

Feature Subscription*

Select the feature you would like to retrieve the metadata information from ISE

User/User Groups



Join Point*

Enter the Join Point

AD Domain*

Enter the location of your AD Domain

Security Group Tag (SGT)

Add ISE Server

ISE Server IP Address*

10.50.10.150

Username*

admin

Password*

••••••••

VPN*

0



ISE Server CA

PXGrid Server CA

SD-WAN Manager / ISE Integration Setup

- Once integration is configured you can view the Users and User Groups.
- Firewall rules can then be built using these as source and/or destinations.

View Users / User Groups ➤

Users User Groups

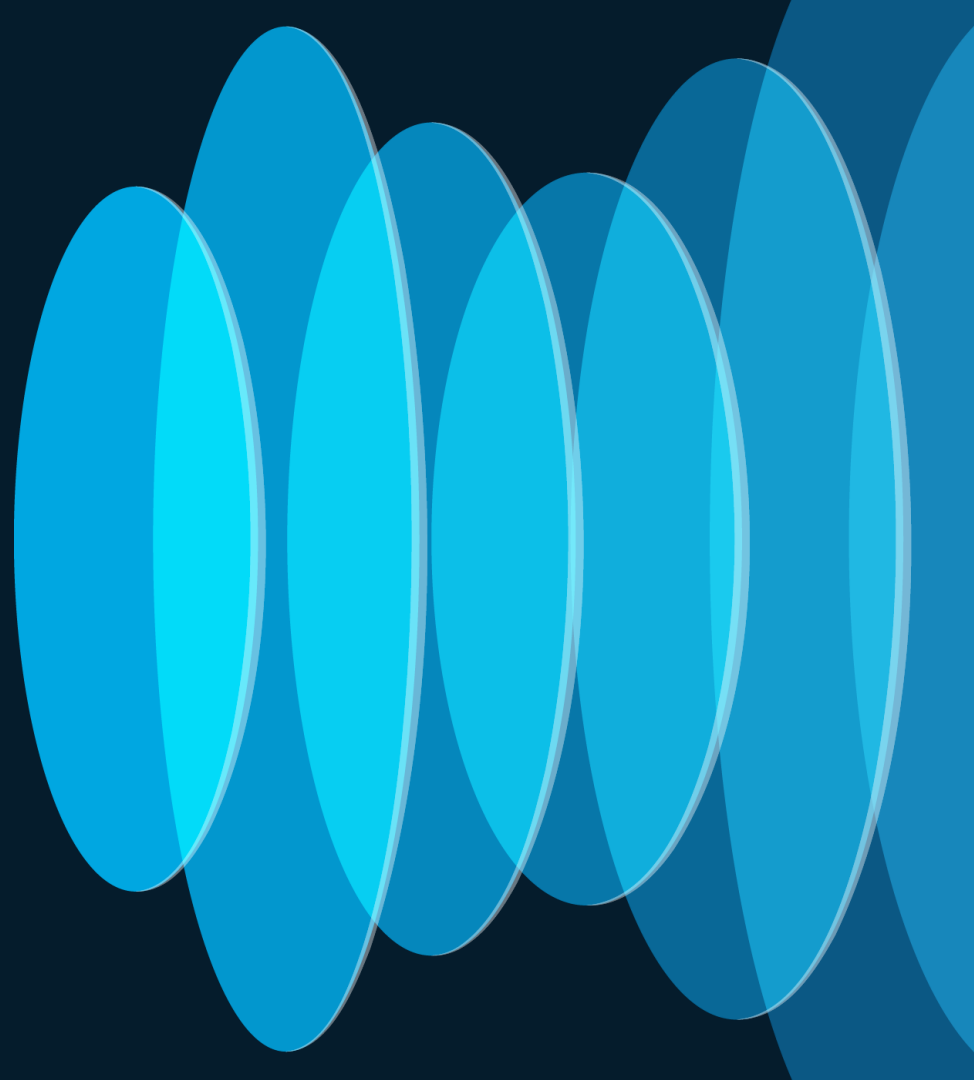
Users (27) ⚙️

🔍 Search Table ⏮

As of: Jun 08, 2022 04:52 PM 🔄

Name	Source
administrator	AD3DOMAIN.COM
guest	AD3DOMAIN.COM
defaultaccount	AD3DOMAIN.COM
krbtgt	AD3DOMAIN.COM
fwusertest1	AD3DOMAIN.COM
testuser1	AD3DOMAIN.COM
testuser2	AD3DOMAIN.COM

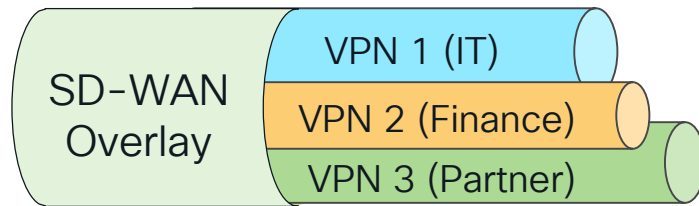
Conclusion



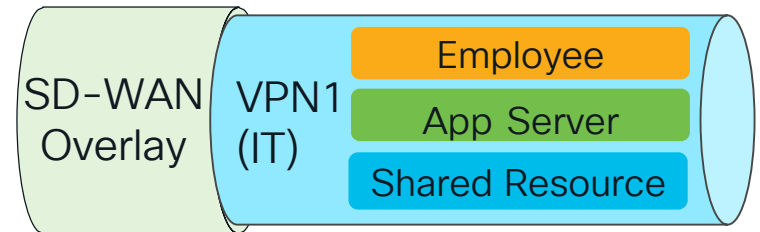
Closing Thoughts

- As network attacks continue to become more sophisticated, segmentation continues to grow in importance.
- ISE and SD-WAN provide the tools to help achieve network segmentation.
- Different options for different use cases. Understand your needs.

Macro Segmentation



Micro Segmentation



Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn **exclusive prizes!**



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

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: spenland@cisco.com



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive