

The background of the slide is a vibrant, abstract graphic. It features a series of overlapping, wavy bands of color in a rainbow spectrum, transitioning from red and orange on the left to yellow, green, and blue on the right. On the right side, there is a bright, multi-colored sunburst or starburst effect that radiates outwards, creating a sense of energy and excitement.

cisco *Live!*

Let's go

#CiscoLiveAPJC



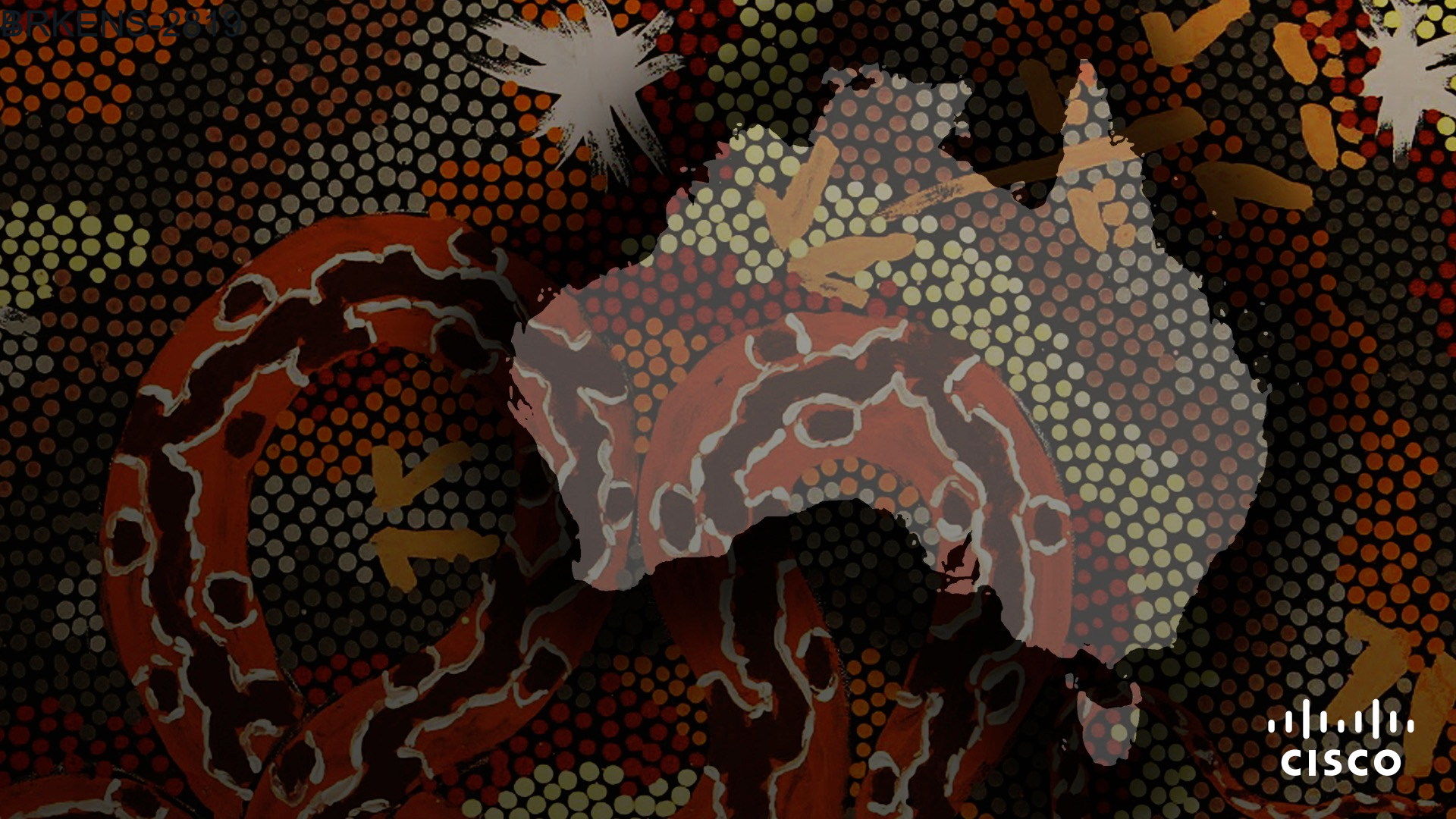
The bridge to possible

Cisco SD-Access and Multi-Domain Segmentation

Jerome Dolphin, Technical Marketing Engineer
CCIE#17805 (R&S, SEC), CCDE#2013::3
BRKENS-2819

CISCO *Live!*

#CiscoLiveAPJC



Cisco Webex App

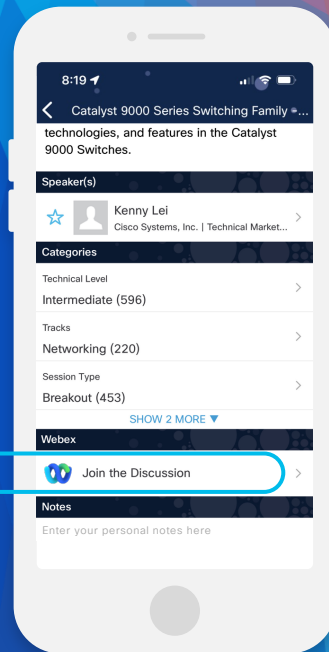
Questions?

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 December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2819>

Agenda

- Introduction
- Lab Network Design and Policy
- Transits and End to End Segmentation
- LAN to DC Segmentation
- Access Privileges with Endpoint Analytics
- Extended Detection and Response
- Conclusion

Introduction

A POC-Inspired Presentation



Why Stay?

- Learn about solutions for end to end connectivity, segmentation and security context across the LAN, WAN, DC and security domains.
- Learn through doing: Configure, integrate and operate real Cisco software defined networking solutions.
- See the functional outcomes.
- Have your questions answered, hopefully.

Why Leave?

- Assumed knowledge due to the scope of topics.
- Not a deep dive on any particular topic.
- Many concepts; the session is recorded.
- Don't like demos.

Disclaimer

- There's many solutions to technical requirements. A wide-reaching presentation cannot cover all combinations.

Disclaimer

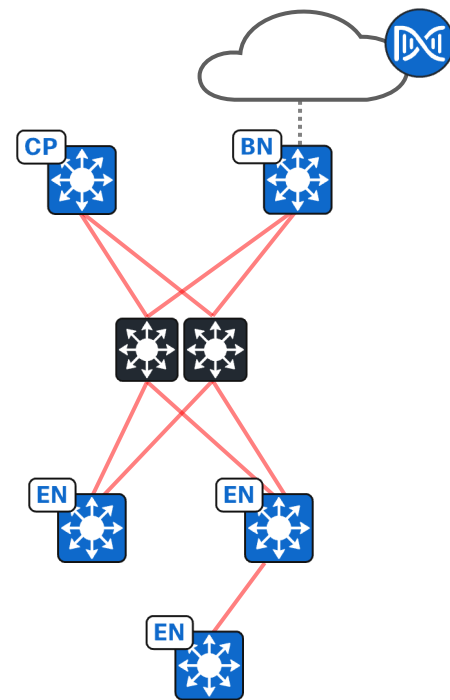
- There's many solutions to technical requirements. A wide-reaching presentation cannot cover all combinations.
- Great places to find help and explore ideas:
 - Cisco partners
 - Cisco CX
 - Cisco sales
 - <https://community.cisco.com>
 - Cisco Live meet the expert
 - www.ciscolive.com

Lab Network Design and Policy

Cisco SD-Access

Mandatory Components

- **Cisco Catalyst Center** – GUI and APIs for intent-based automation of wired and wireless fabric devices.
- **Fabric Border Nodes** – A fabric device that connects external L3 networks to the Cisco SD-Access fabric.
- **Fabric Edge Nodes** – A fabric device that connects wired endpoints to the Cisco SD-Access fabric and optionally enforces micro-segmentation policy.
- **Control Plane Node** – Map System that tracks endpoint to device relationships.



Optional Components

-  **RECAP**



LISP Fabric Deployment Options

- Cisco Catalyst Center automated configuration of a Cisco SD-Access LISP-based fabric which includes Macro and Micro Segmentation
 - Automation Workflows and integrations
 - Best practice standardized configurations
 - SD-Access Assurance

LISP Fabric Deployment Options

- Cisco Catalyst Center automated configuration of a Cisco SD-Access LISP-based fabric which includes Macro and Micro Segmentation
 - Automation Workflows and integrations
 - Best practice standardized configurations
 - SD-Access Assurance

OR

- [CLI](#) Configuration of Cisco LISP VXLAN Fabric which includes Macro and Micro Segmentation
 - Open integration with heterogenous tooling (CLI, [Ansible](#), NSO, etc.)
 - Customization within the parameters of the LISP Fabric validated design
 - Cisco Catalyst Center Device and Client Assurance
 - Subset of features supported compared to what is available with Cisco Catalyst Center.

Lab Topology

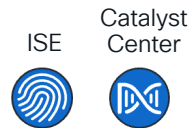
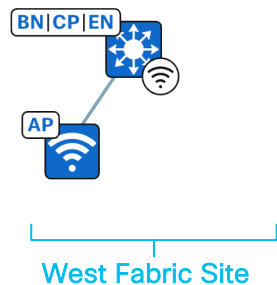
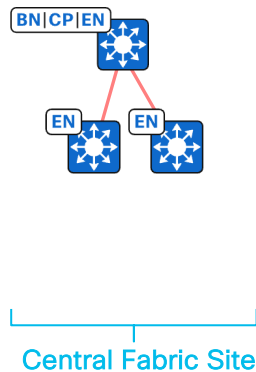
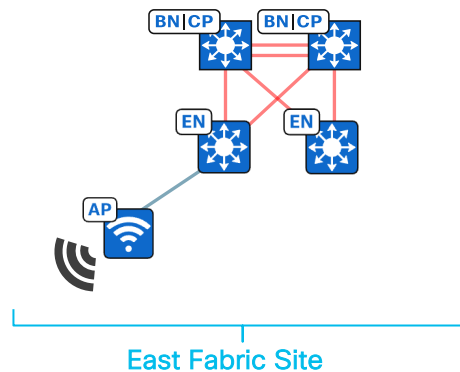


West Fabric Site

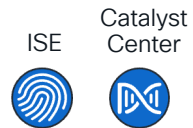
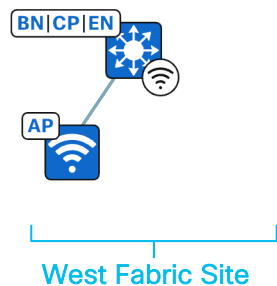
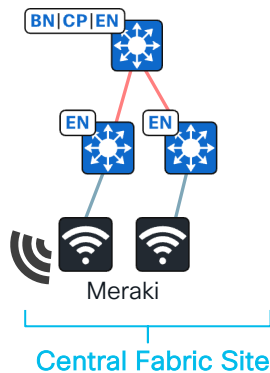
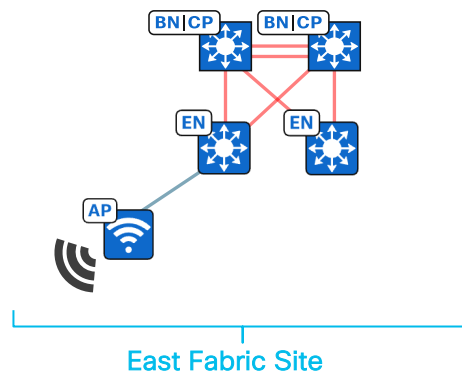
Central Fabric Site

East Fabric Site

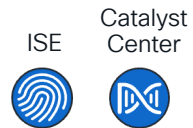
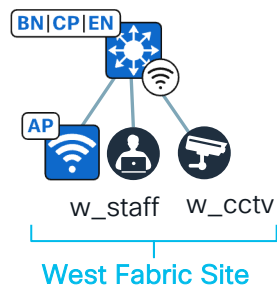
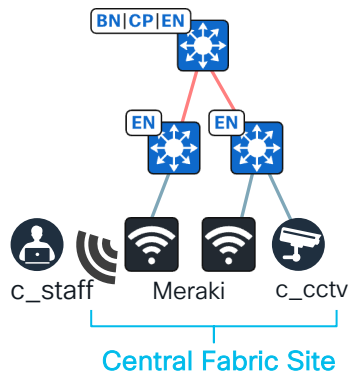
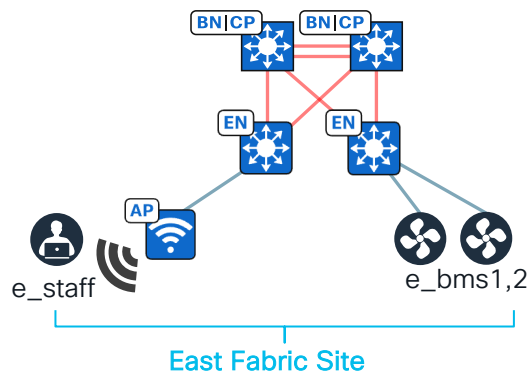
Lab Topology



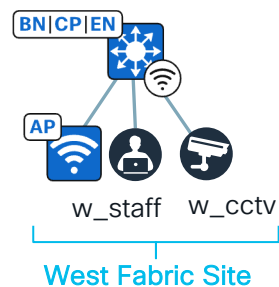
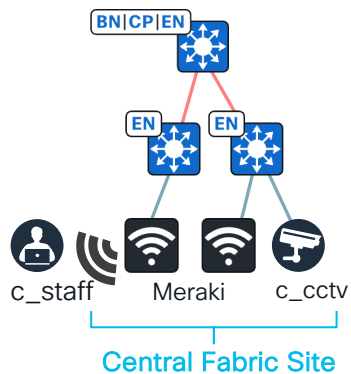
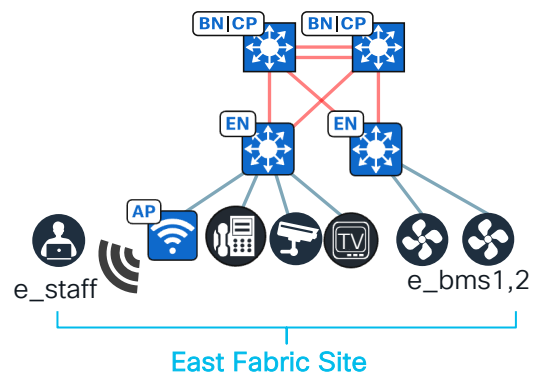
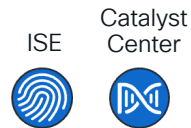
Lab Topology



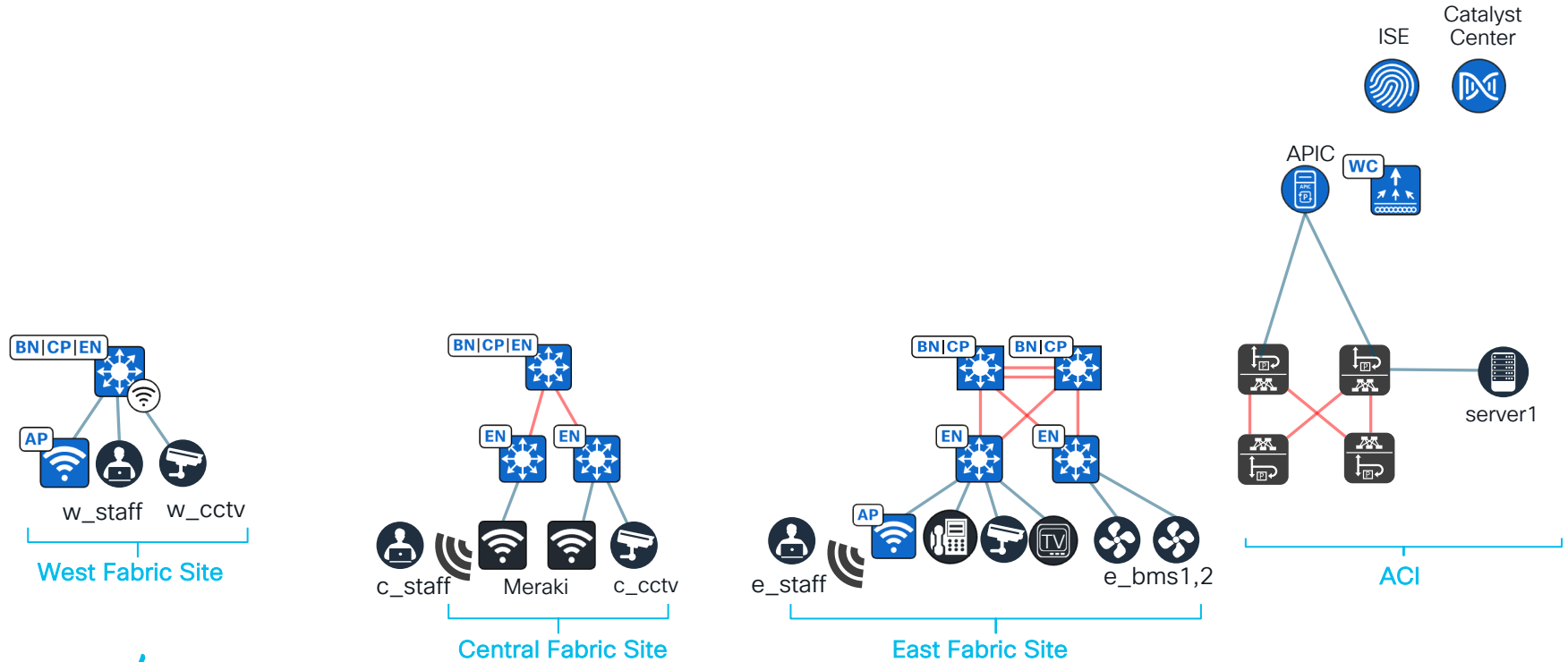
Lab Topology



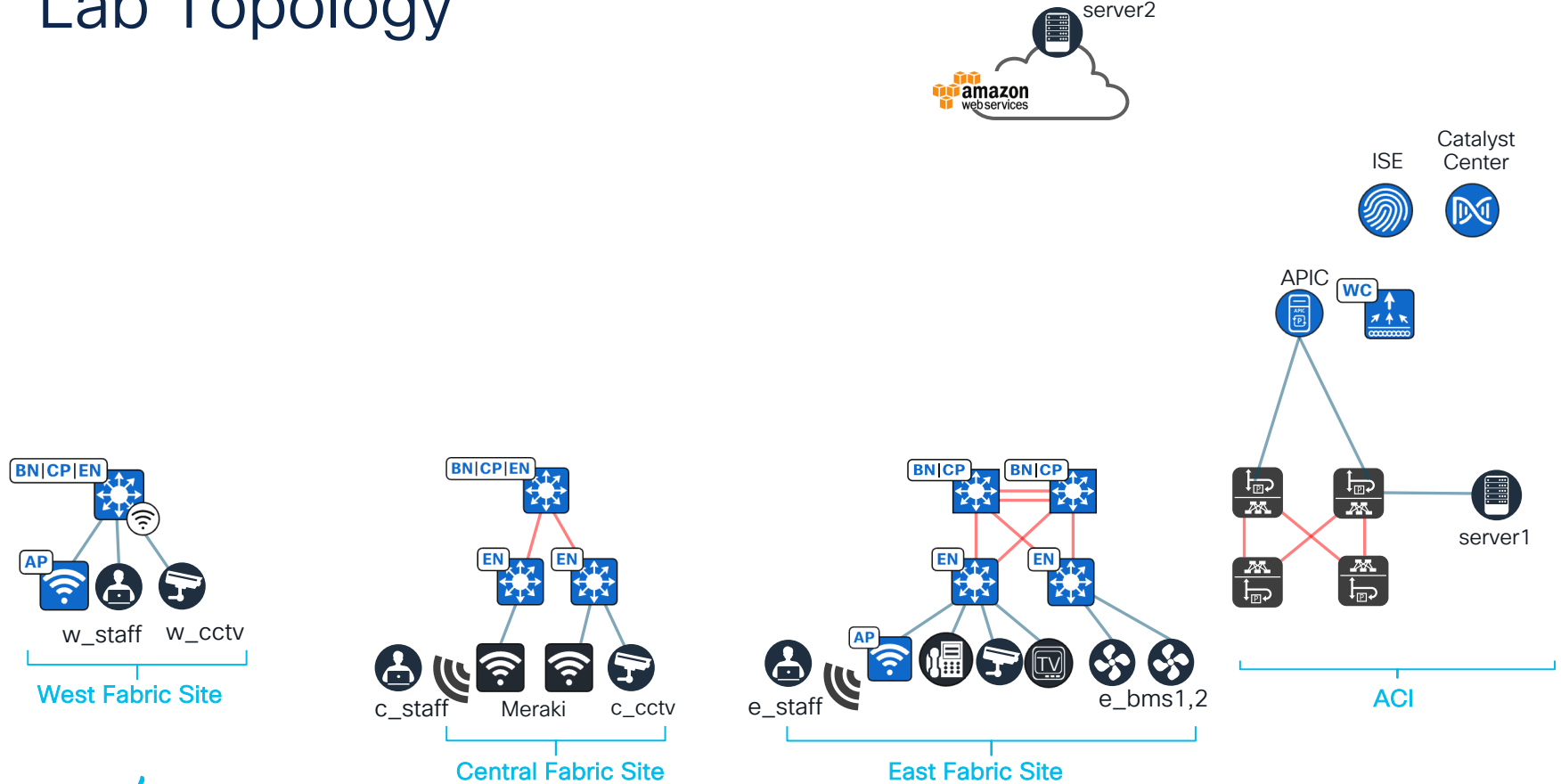
Lab Topology



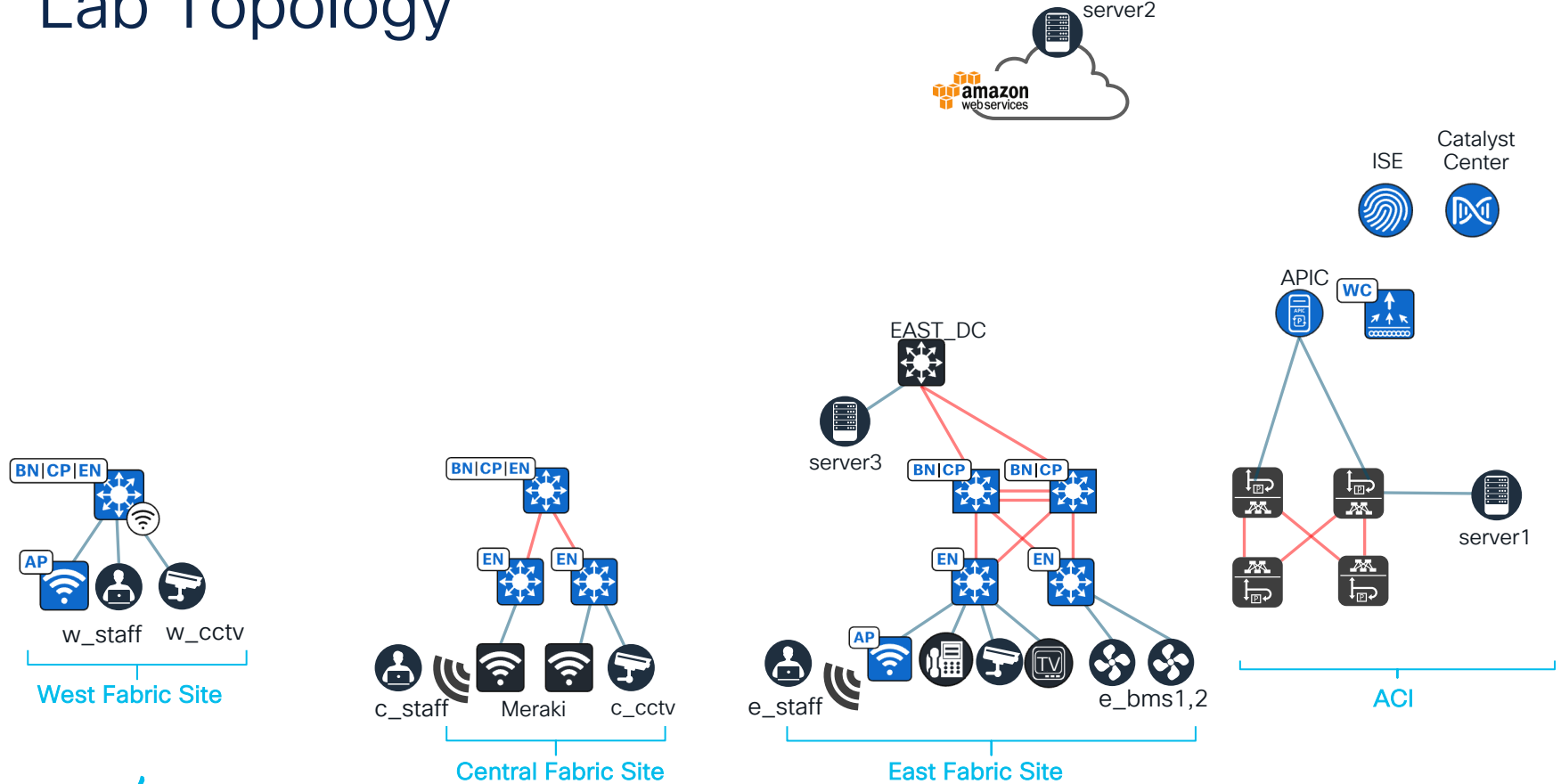
Lab Topology



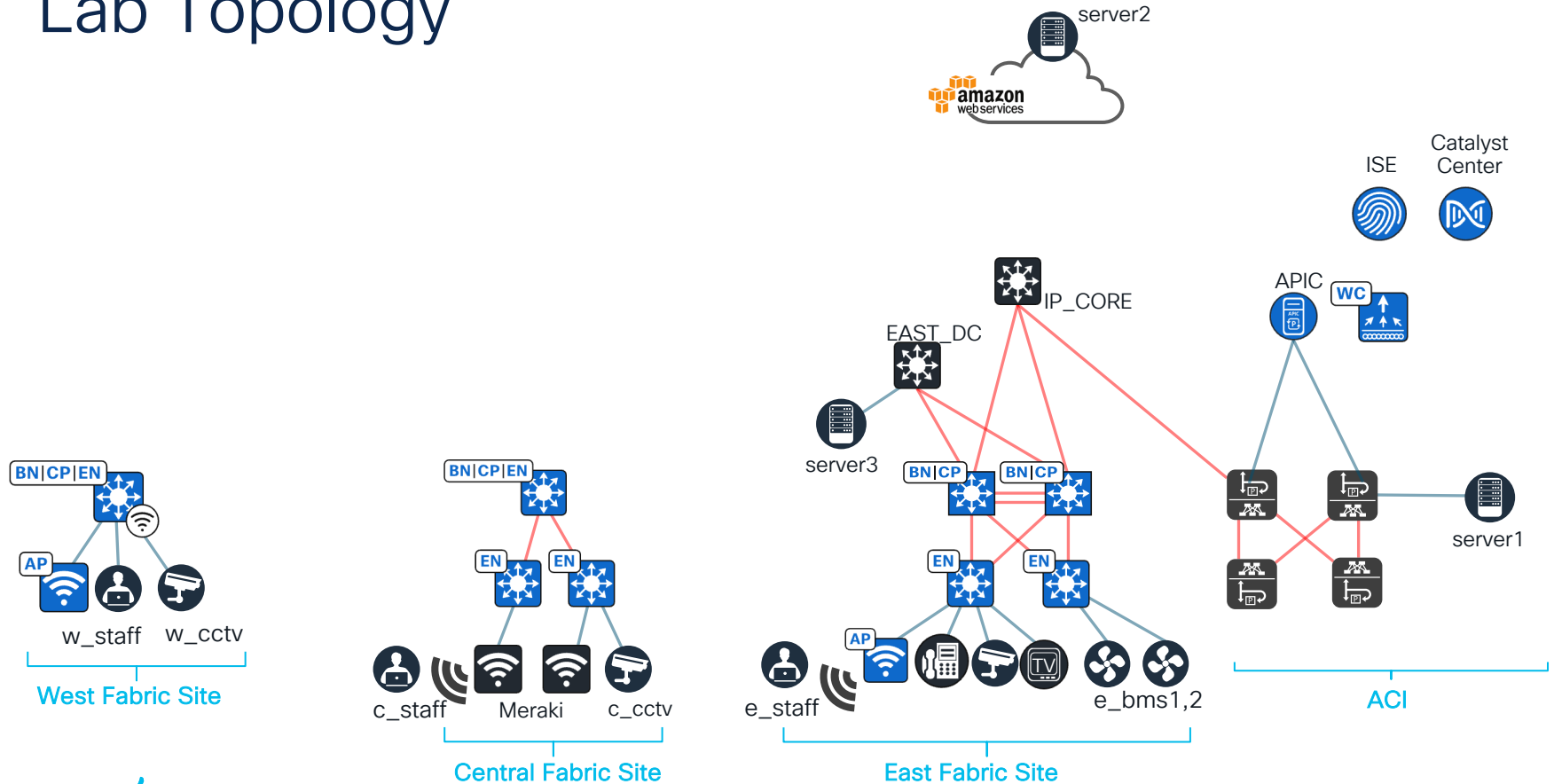
Lab Topology



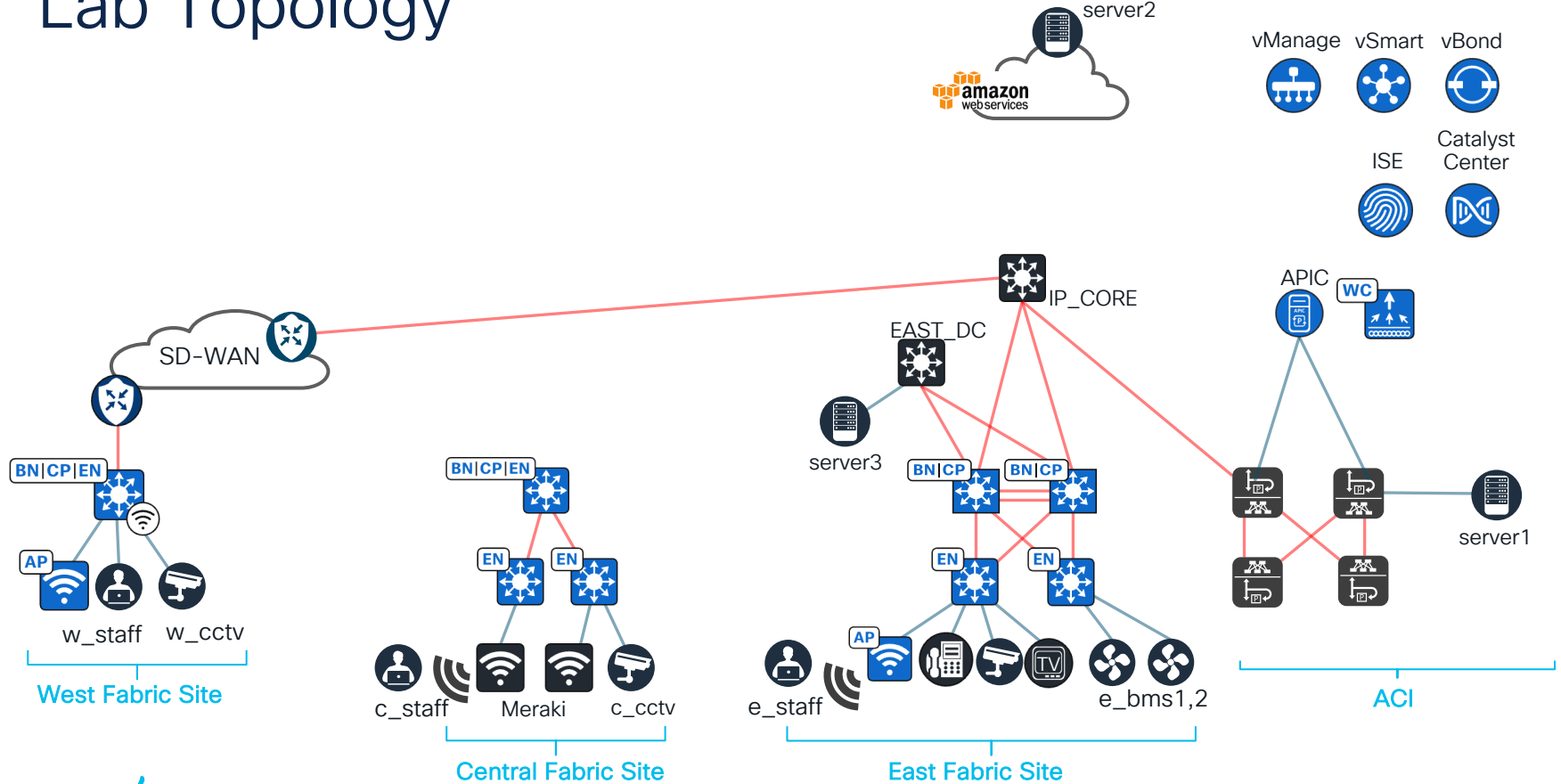
Lab Topology



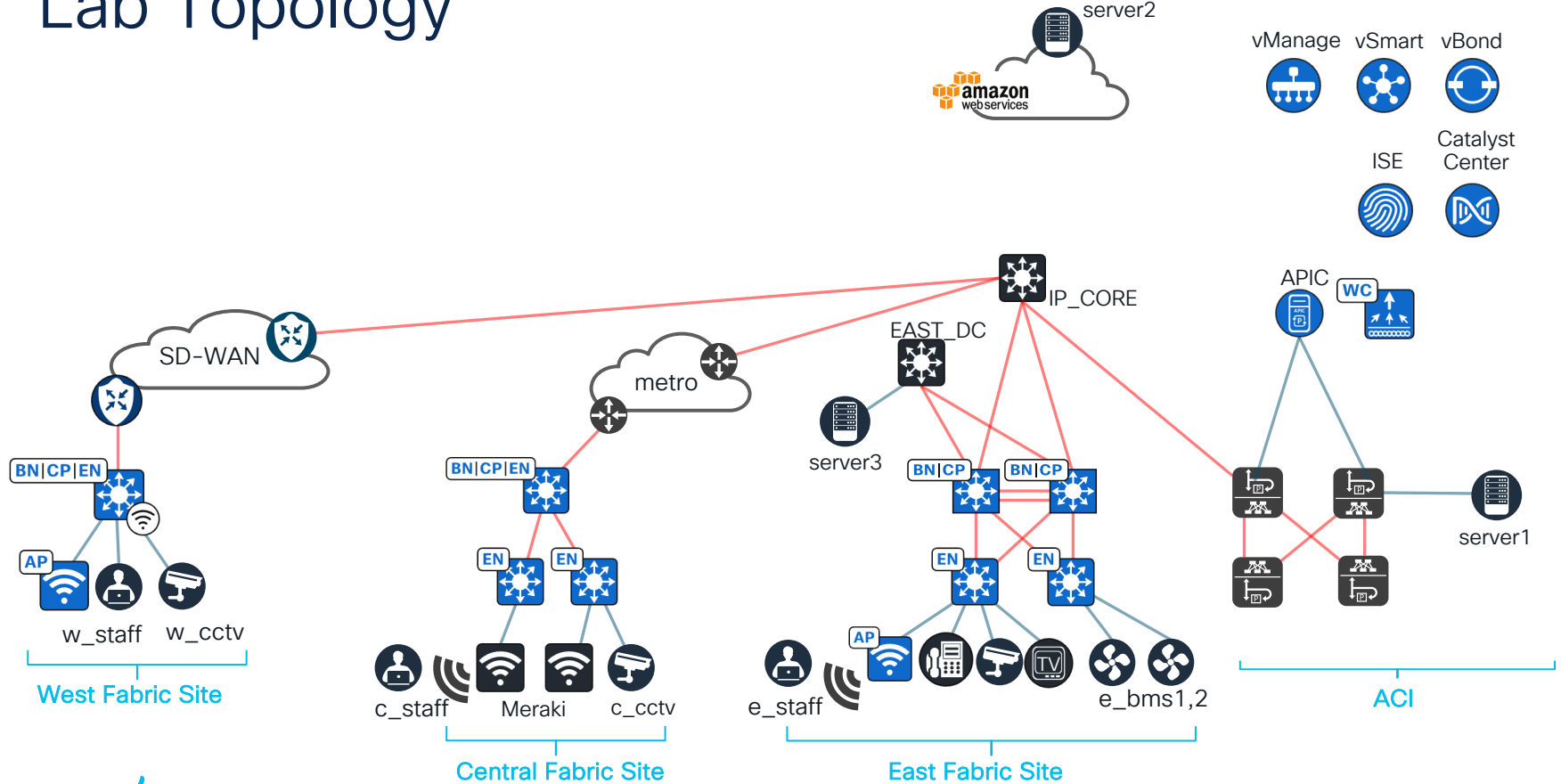
Lab Topology



Lab Topology



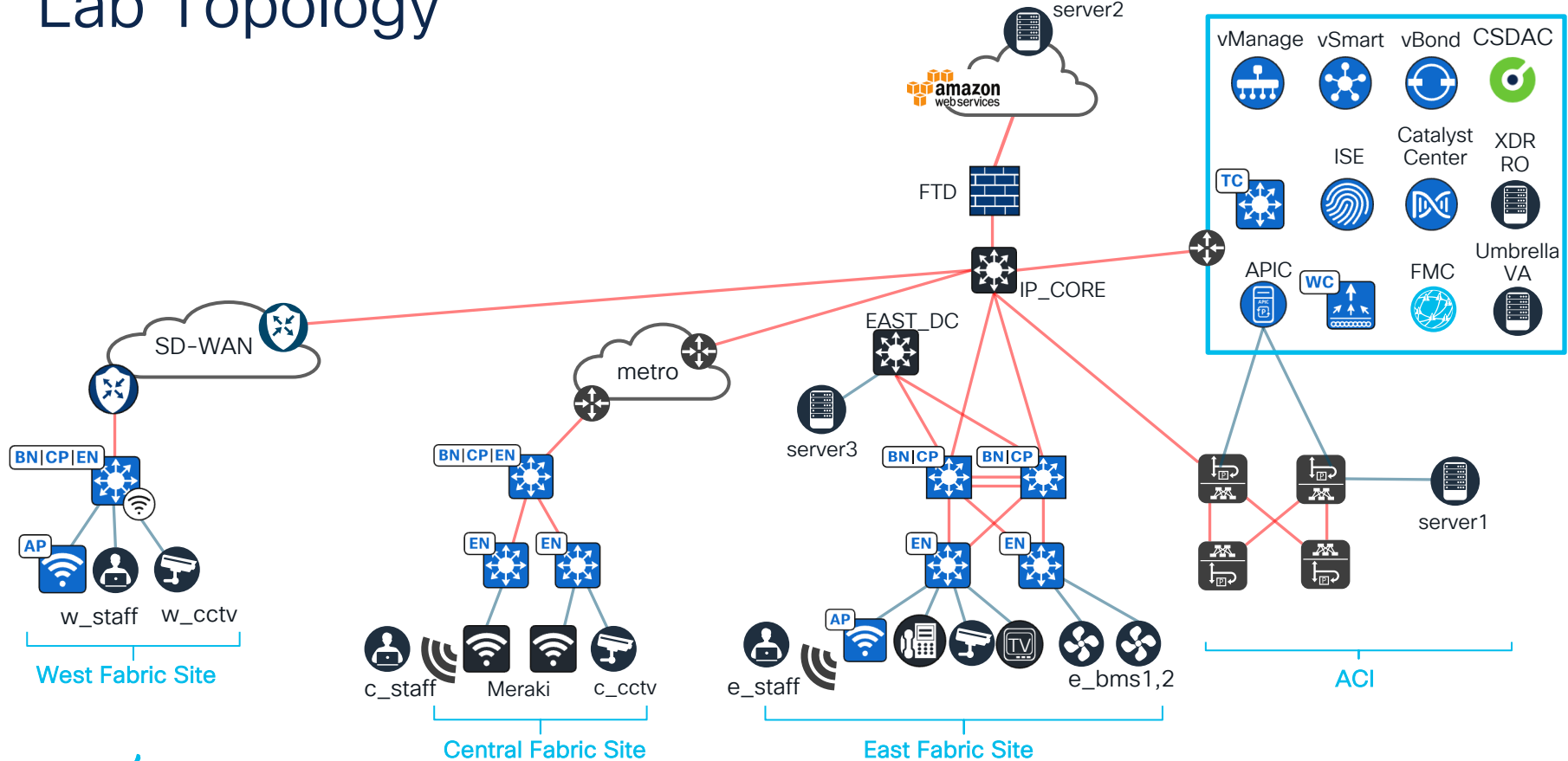
Lab Topology



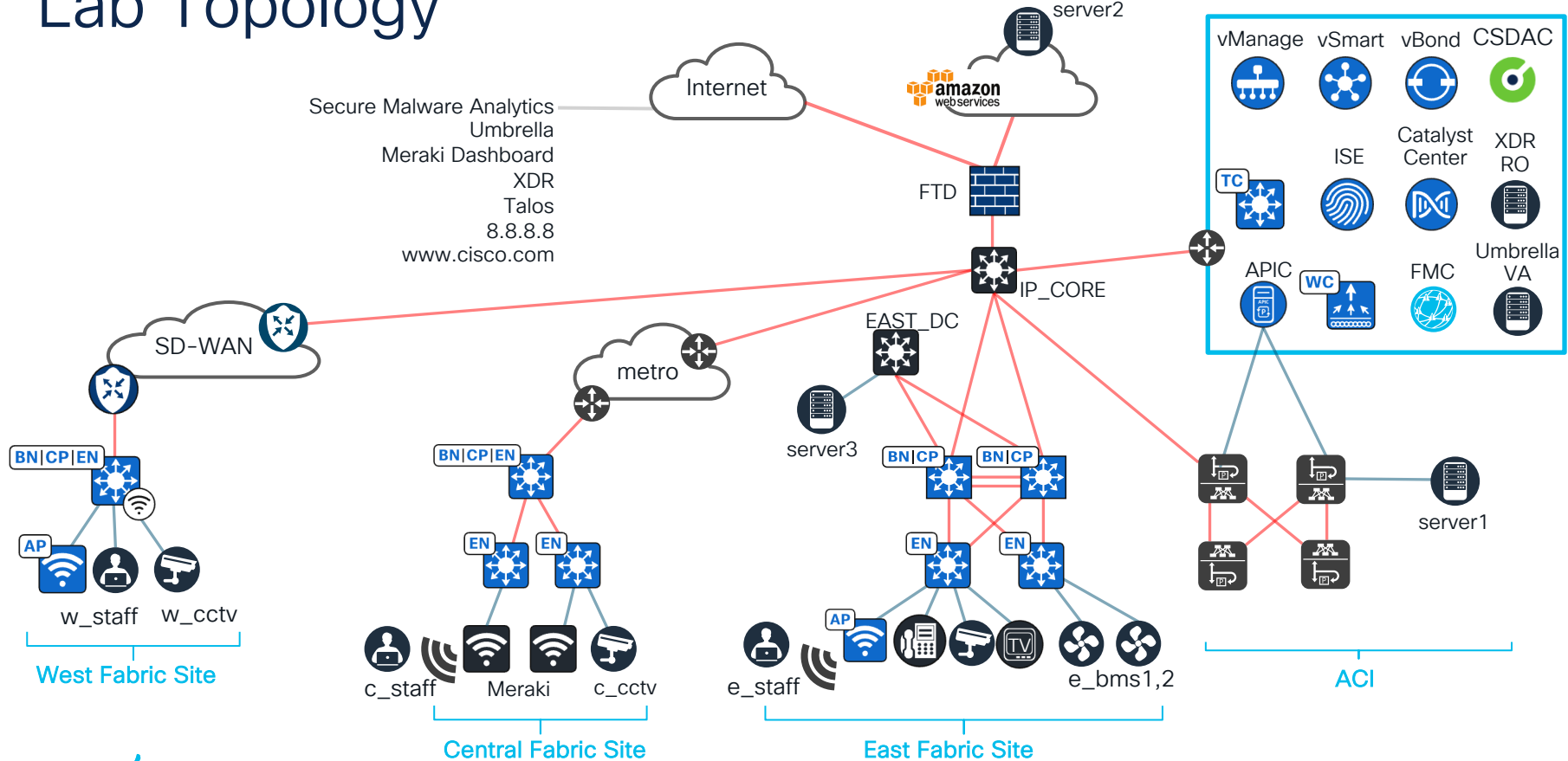
CISCO *Live!*



Lab Topology



Lab Topology



Routing Configuration

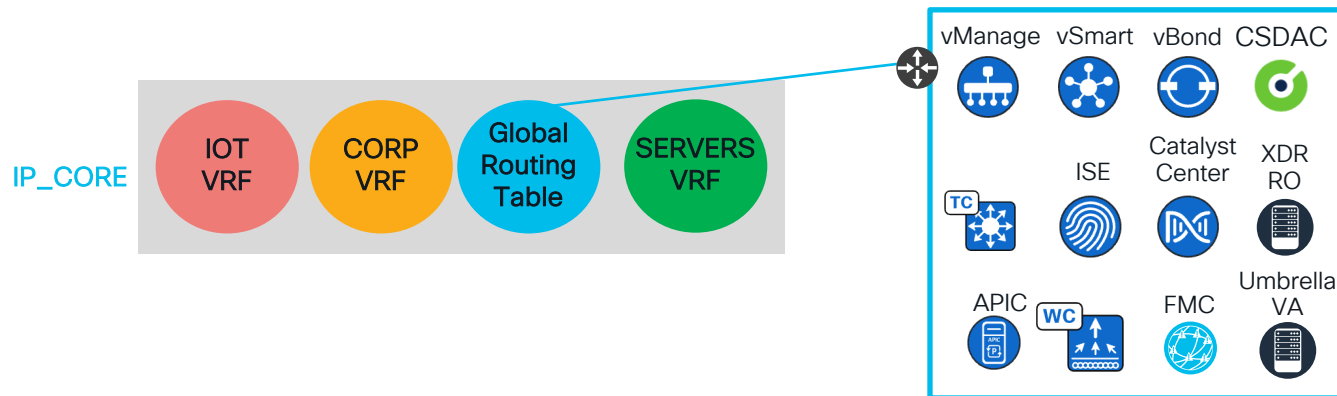


REFERENCE

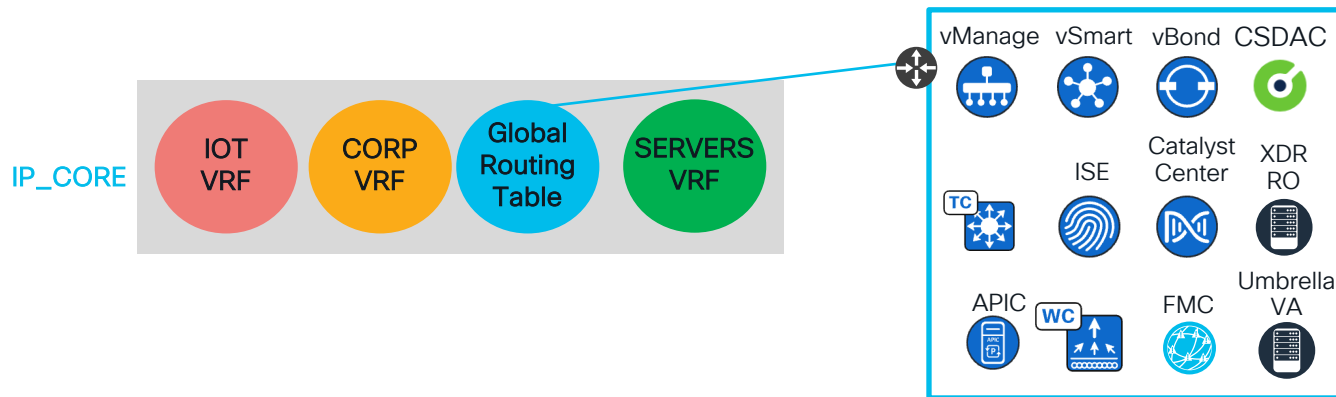
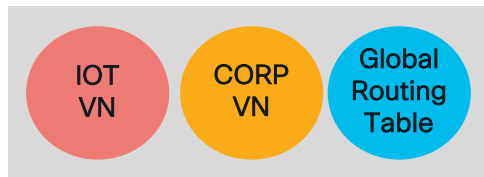
IP_CORE



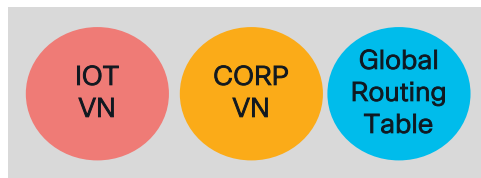
Routing Configuration



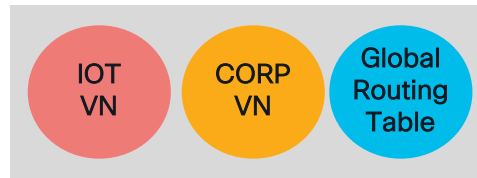
Routing Configuration



West Fabric Site

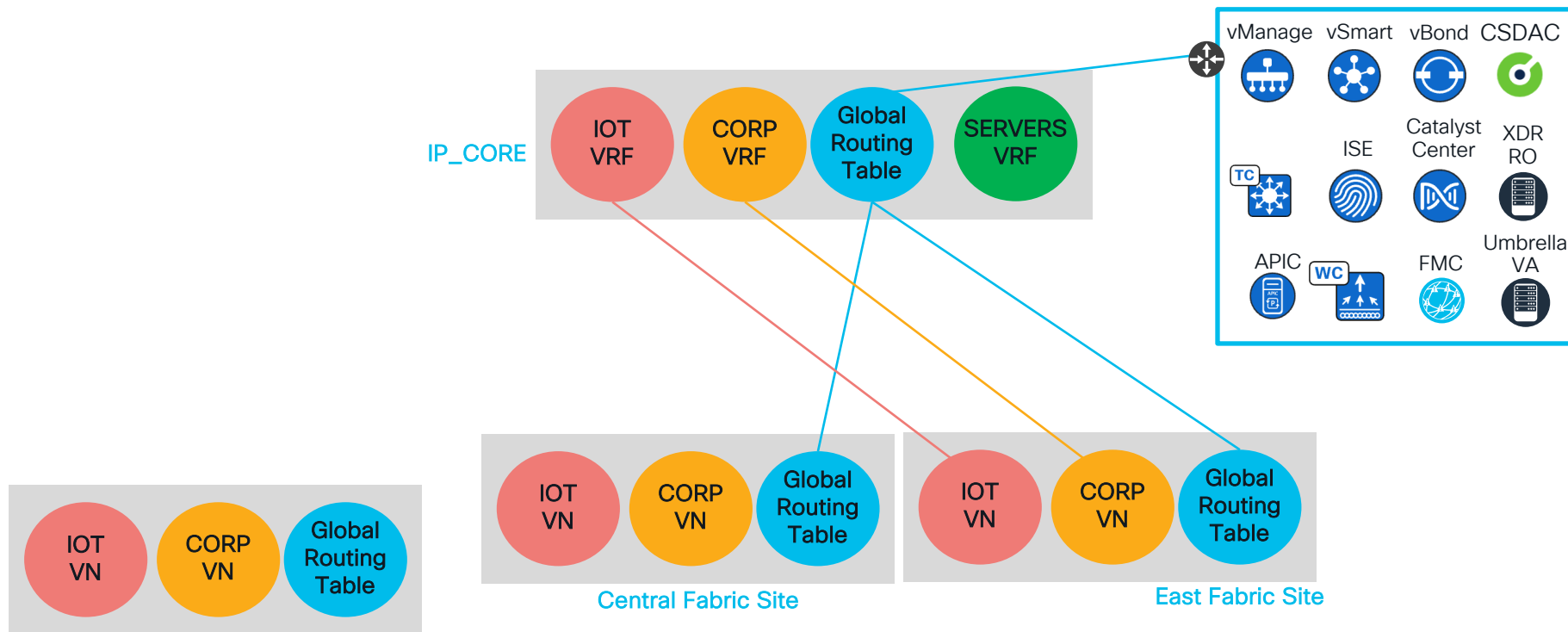


Central Fabric Site

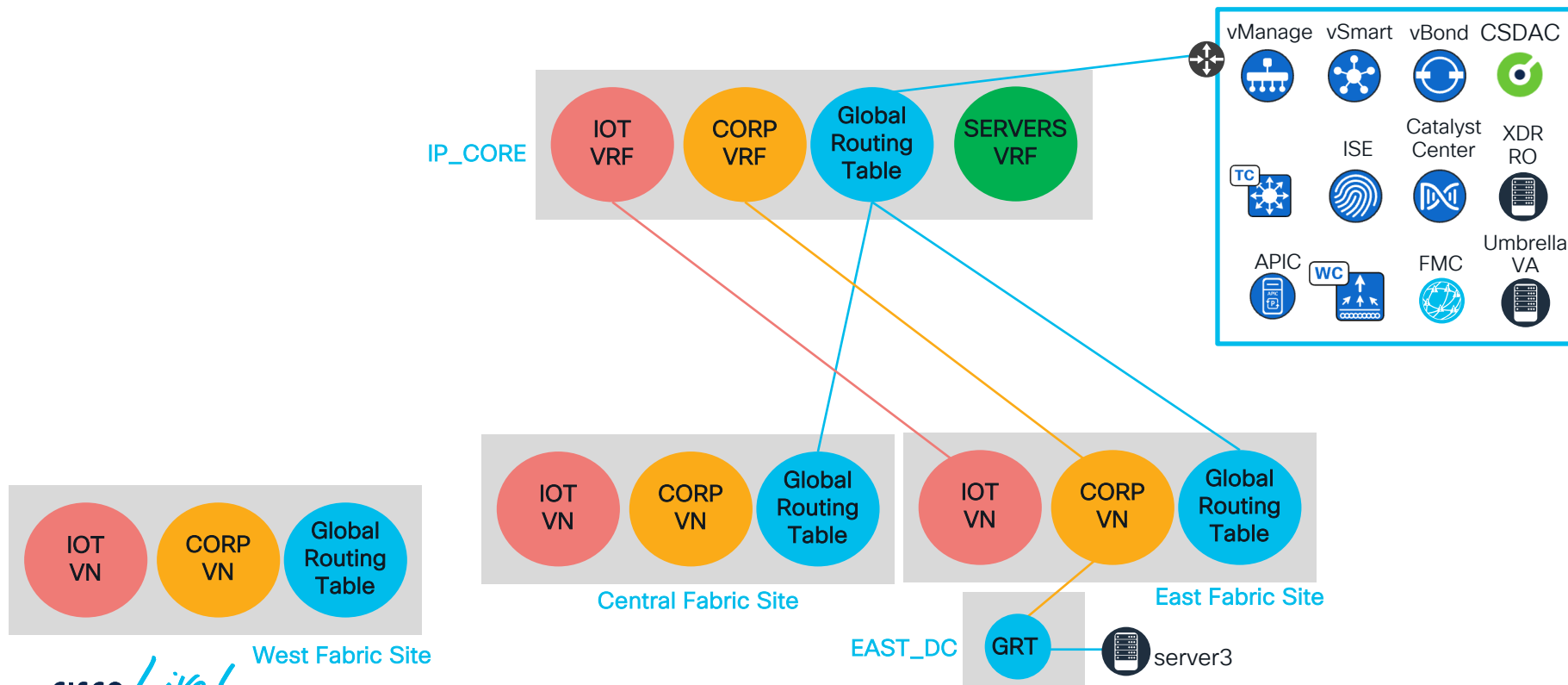


East Fabric Site

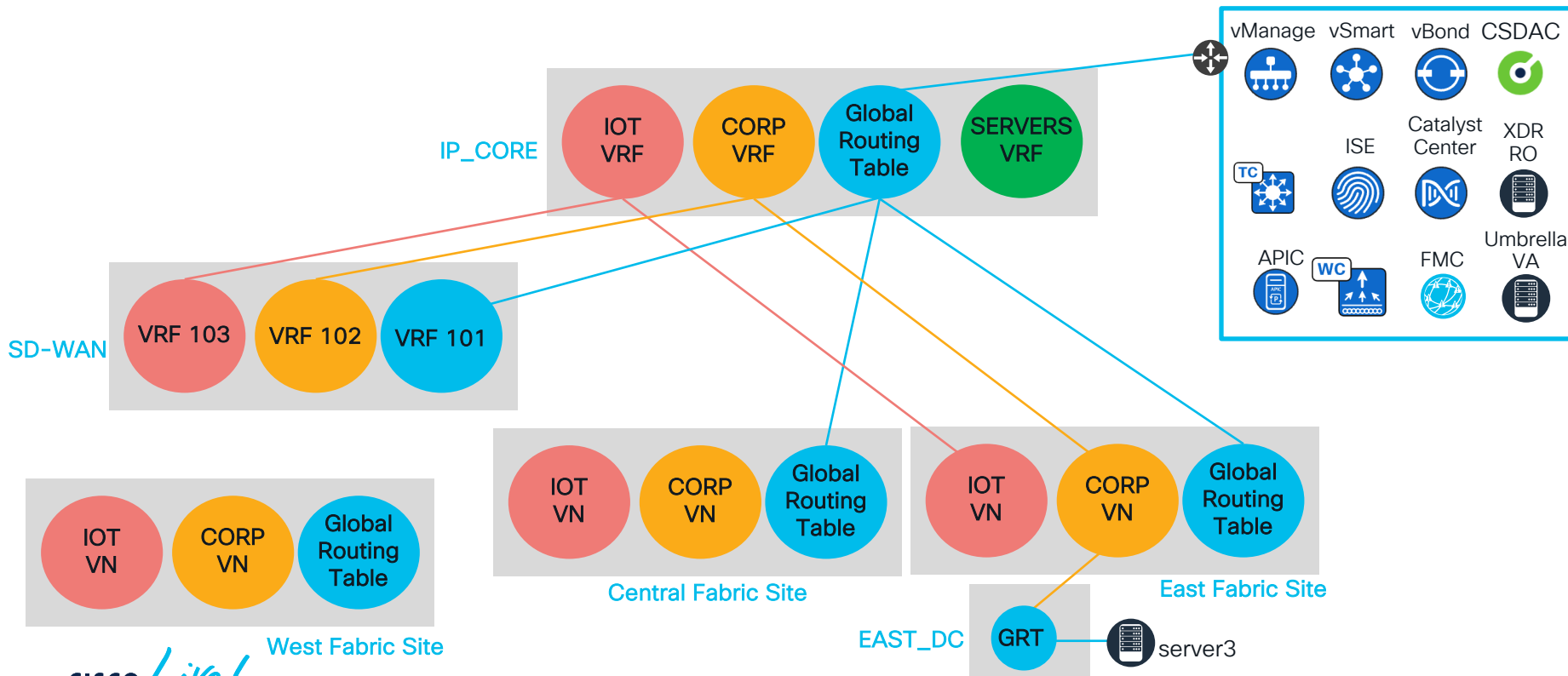
Routing Configuration



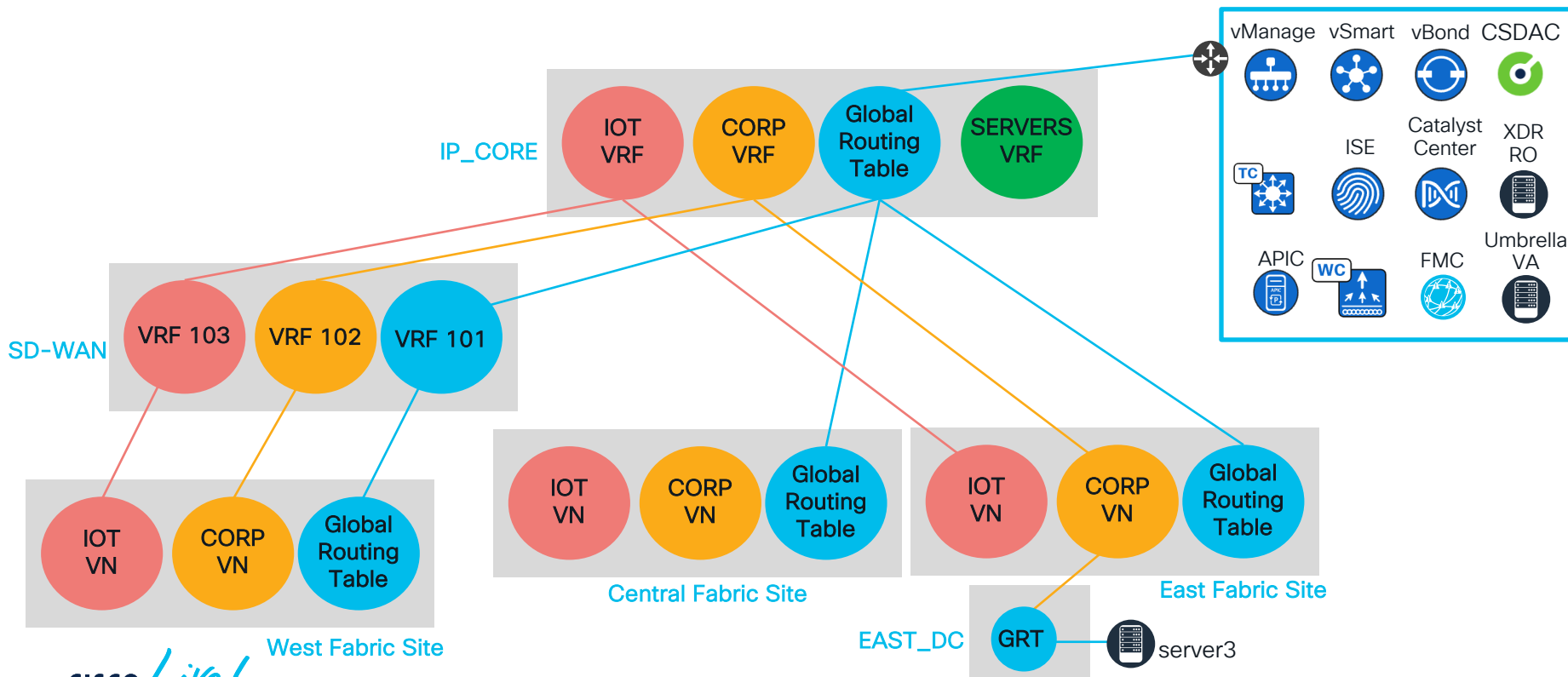
Routing Configuration



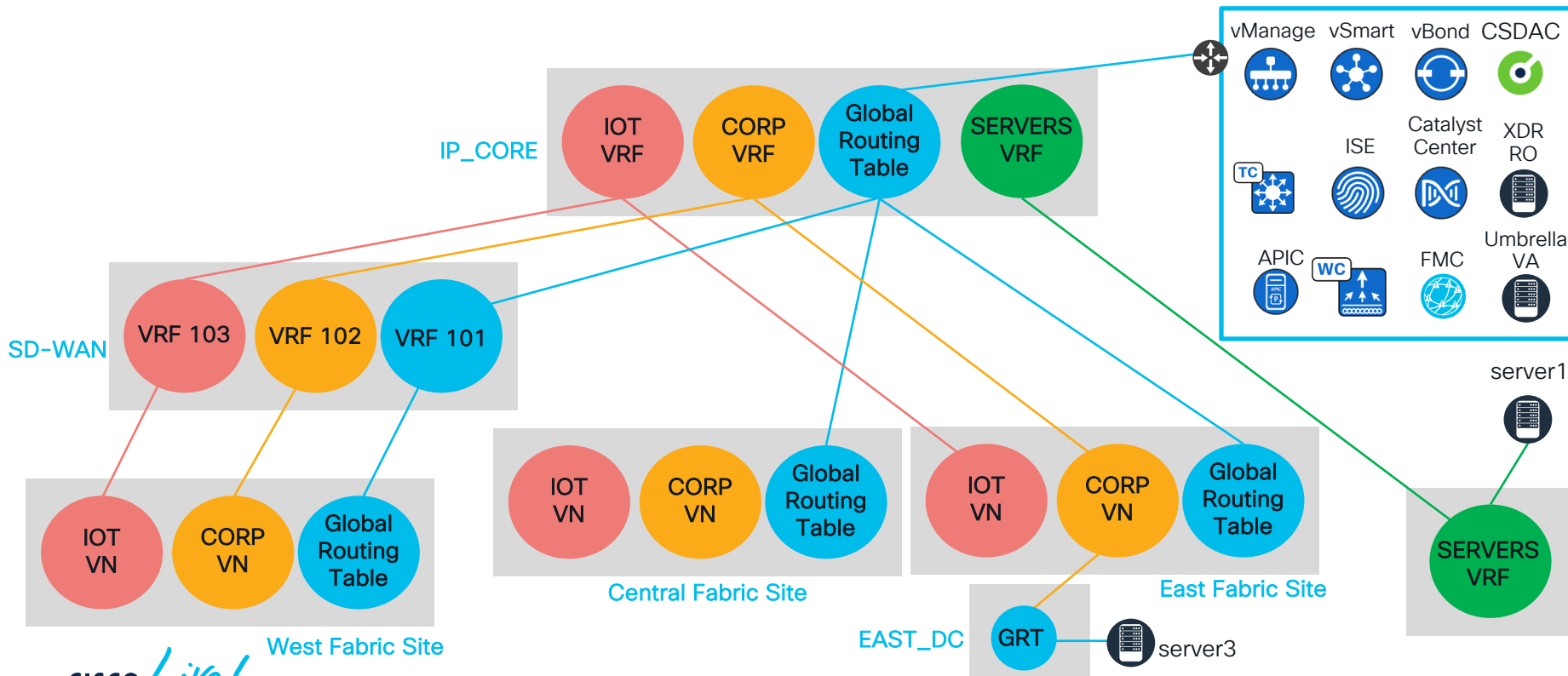
Routing Configuration



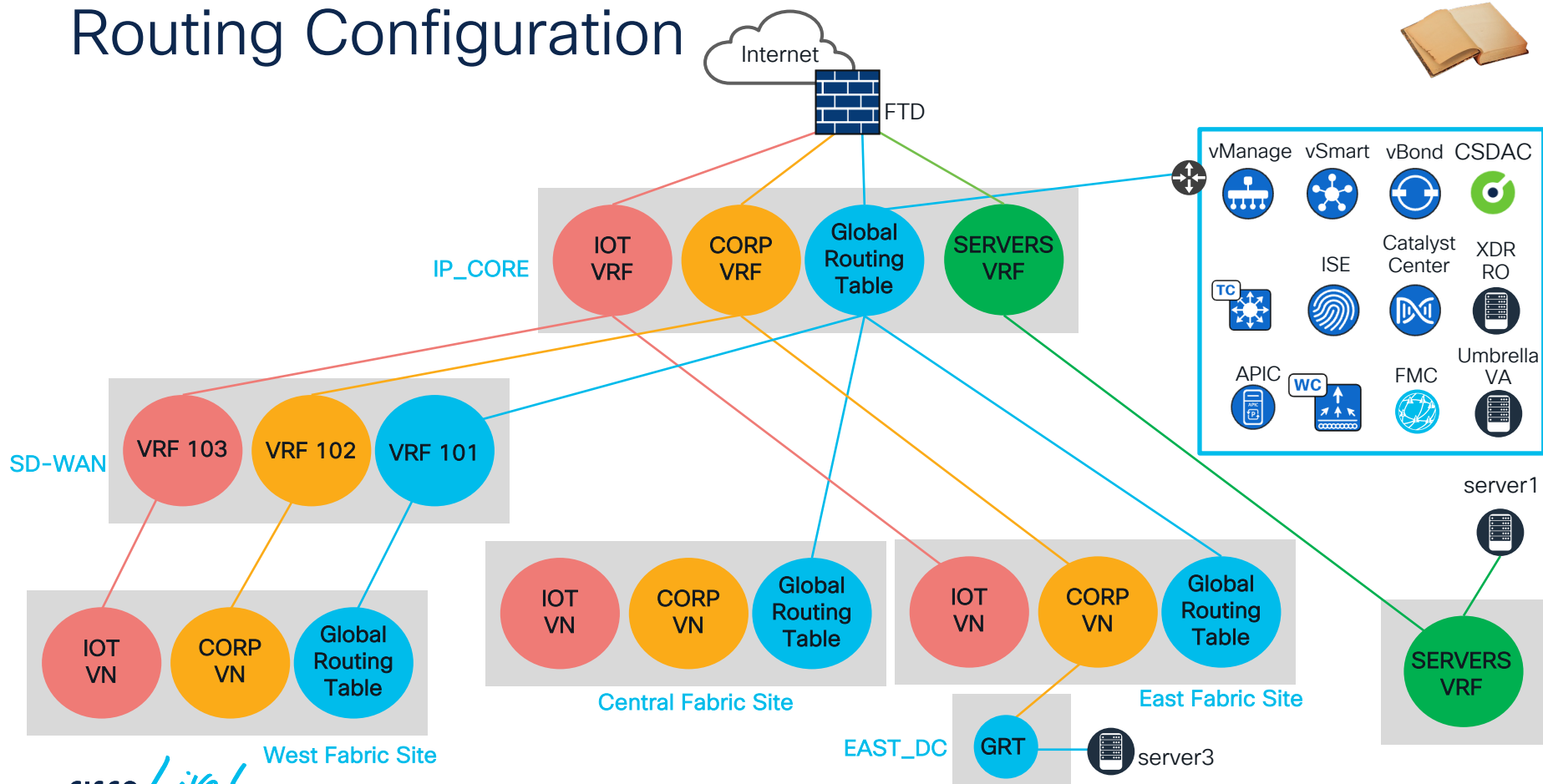
Routing Configuration



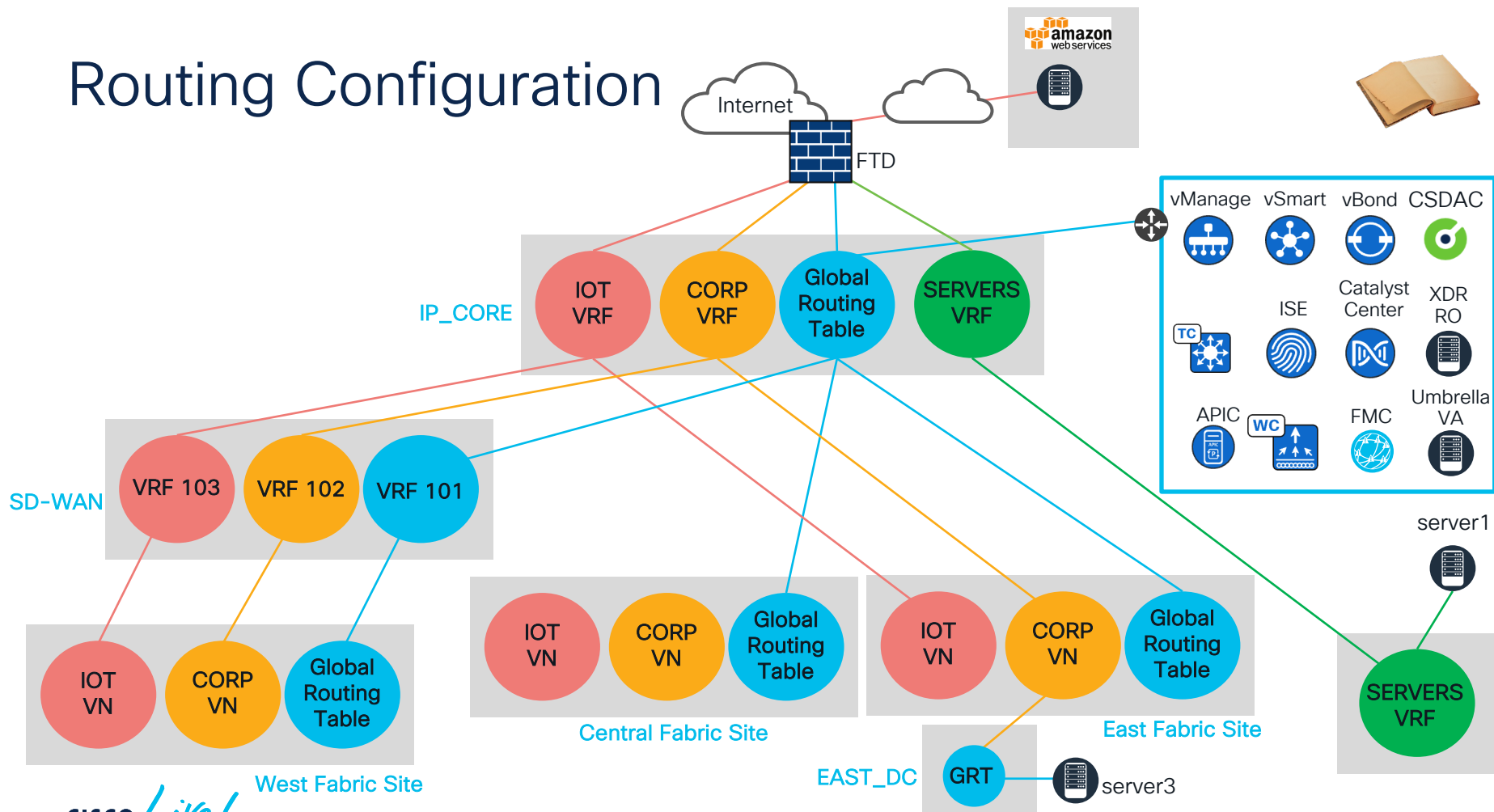
Routing Configuration



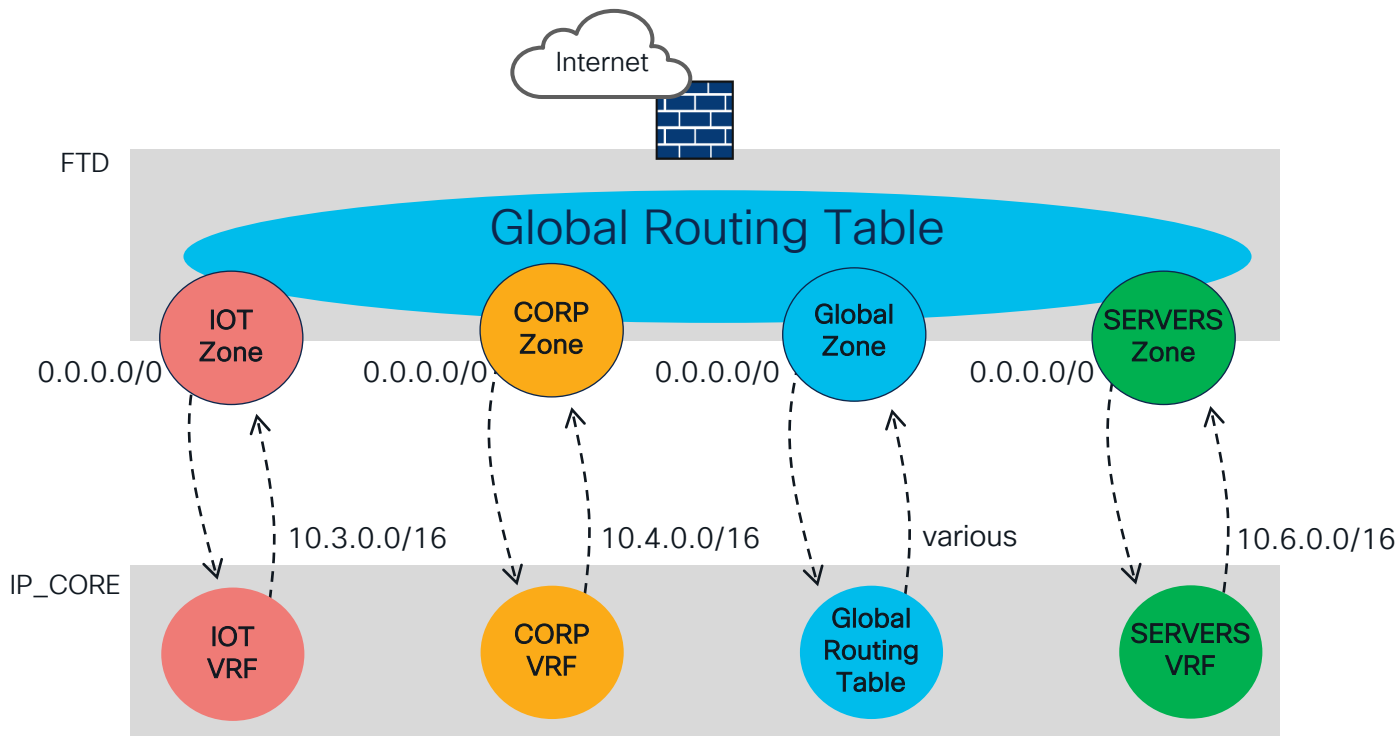
Routing Configuration



Routing Configuration



Inter-VRF Routing Design



Endpoints



Hostname / Username	Description	Virtual Network	SGT / EPG / SG
w_staff	staff endpoint	CORP_VN	Employee
c_staff	staff endpoint	CORP_VN	Employee
e_staff	staff endpoint	CORP_VN	Employee
w_cctv	CCTV device	IOT_VN	CCTV
c_cctv	CCTV device	IOT_VN	CCTV
e_bms1,2	BMS devices	IOT_VN	BMS
server1	ACI connected server	SERVERS VRF	n/a
server2	AWS connected server	n/a	AWS_SERVERS
server3	Traditional switching connected server	CORP_VN	EAST_DC_SERVERS

Endpoints



Hostname / Username	Description	Virtual Network	SGT / EPG
n/a	Apple TV	IOT_VN	TV
n/a	IP Phone 8865	n/a	n/a
n/a	Meraki MV12W	IOT_VN	CCTV

Segmentation Policy



Mechanism	Source	Destination	Action
Group-Based Policy	SGT: CCTV	SGT: BMS	Deny
	SGT: BMS	SGT: CCTV	Deny
	SGT: Quarantine	SGT: Quarantine	Deny
		SGT: Employee	
		SGT:CCTV	
		SGT: BMS	
		SGT: EAST_DC_SERVERS	
	SGT: Employee	SGT: Quarantine	Deny
	SGT: CCTV		
	SGT: BMS		
	SGT: EAST_DC_SERVERS		
	SGT: CCTV	SGT: EAST_DC_SERVERS	Deny
	SGT: BMS		
	SGT: Any	SGT: Any	Permit

Segmentation Policy



Mechanism	Source	Destination	Action
Cisco Secure Firewall	SGT: Employee	SGT: BMS SGT: CCTV	Permit
	SGT: BMS SGT: CCTV	SGT: Employee	Deny
	SGT: Quarantine	www.cisco.com 8.8.8.8	Permit
	SGT: Quarantine	Any	Deny
	SGT: CCTV	EPG: ACI_SERVERS	Permit
	SGT: BMS	EPG: ACI_SERVERS	Deny
	SGT: BMS	Group: AWS_SERVERS	Permit
	SGT: CCTV	Group: AWS_SERVERS	Deny
	Any	Any	Permit

Demo

Transits and End to End Segmentation

For More Information

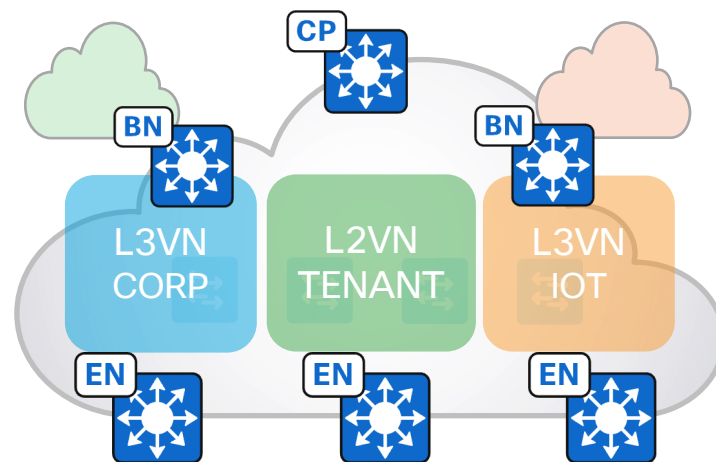
- [Cisco SD-Access CVD](#)
- [Cisco SD-Access | SD-WAN Independent Domain Pairwise Integration](#)
- [Cisco SD-Access Best Practices - Design and Deployment - BRKENS-2502](#)
- [BRKXAR-2001 - Cisco Intent Based Cross and Multidomain Integrations for SDA and SD-WAN](#)
- [Meraki Adaptive Policy Overview](#)
- [How To: Integrate Meraki Networks with ISE](#)
- [Meraki Adaptive Policy Configuration Guide](#)

Cisco SD-Access Fabric

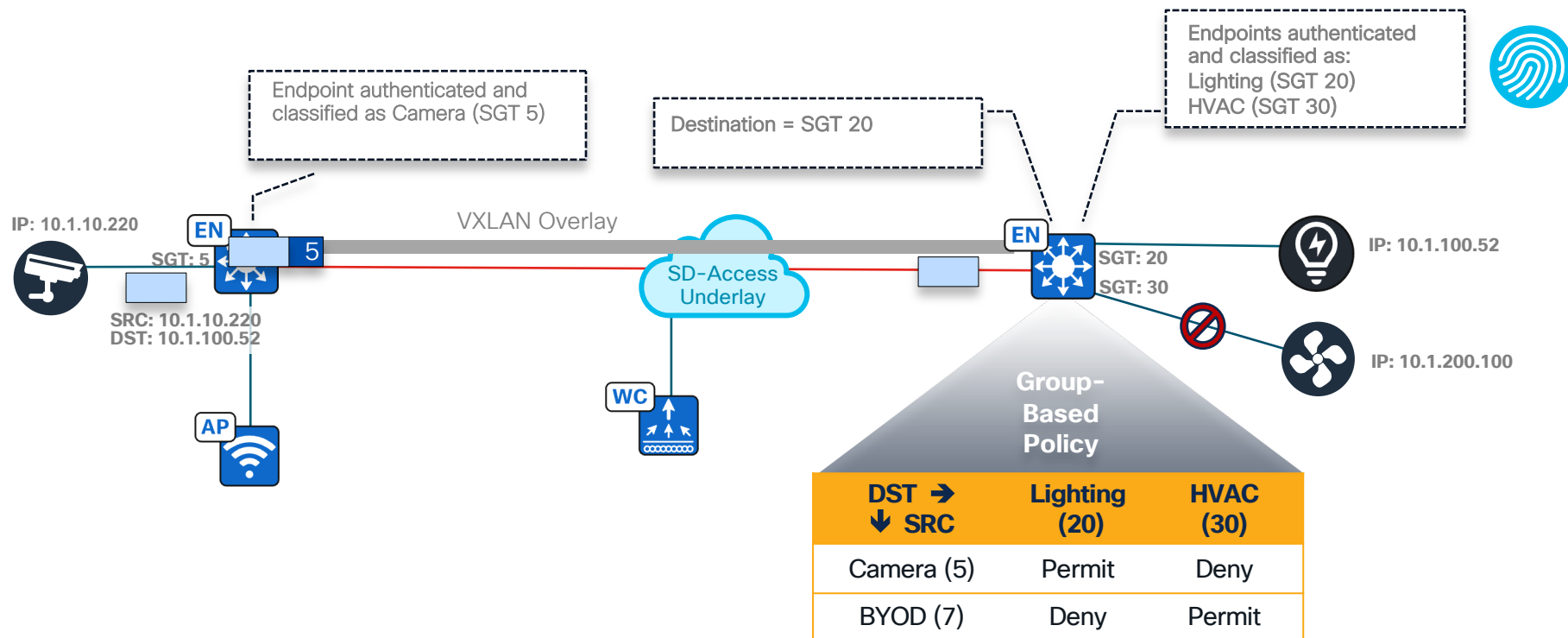
Virtual Networks



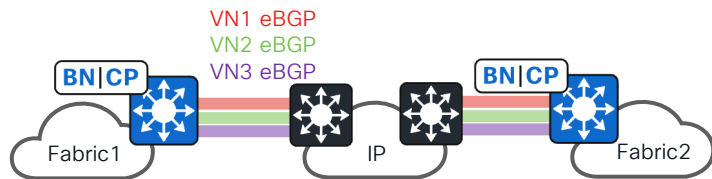
- Layer 3 Virtual Networks use VRFs and LISP Instance IDs to maintain separate routing topologies.
 - Endpoint IDs (IPv4/IPv6 addresses) are routed within an L3VN.
- Layer 2 Virtual Networks use LISP Instance IDs and VLANs to maintain separate switching topologies.
 - Endpoint IDs (MAC addresses) are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



Security Group Tag and Group-Based Policy



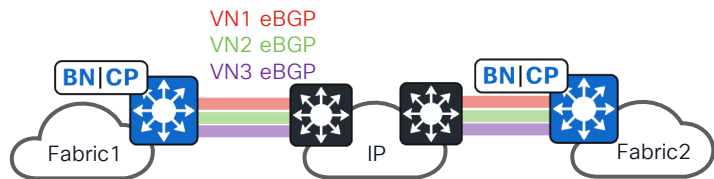
Transits



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 compatible hardware and software.

Transits

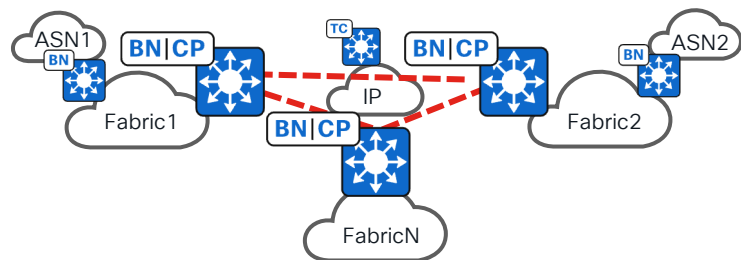


IP-Based Transit

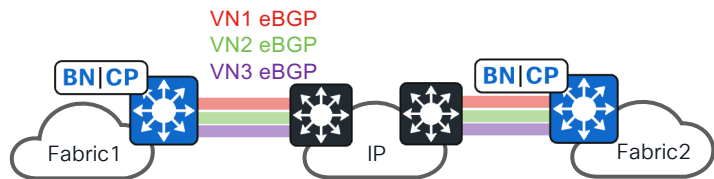
- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires compatible hardware and software.

SD-Access Transit

- SD-Access LISP/VXLAN between Fabric Sites.
- Preserves Layer 3 Virtual Networks and SGTs.
- Fabric as a transit between external routing domains.



Transits



IP-Based Transit

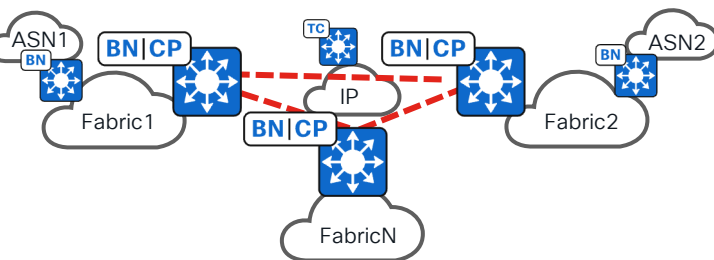
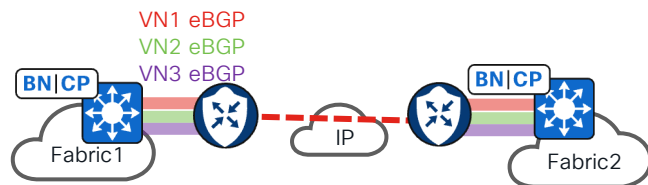
- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires compatible hardware and software.

SD-Access Transit

- SD-Access LISP/VXLAN between Fabric Sites.
- Preserves Layer 3 Virtual Networks and SGTs.
- Fabric as a transit between external routing domains.

SD-WAN Transit

- Cisco SD-WAN between Fabric Sites.
- Border Node connected to SD-WAN Edge.



SGT Preservation is Essential

- Source SGT and destination SGT should be known at policy enforcement point.
- SGT can be transported numerous ways:
 - Source. In data plane.
 - Source and Destination. In control plane via SXP or pxGrid.
- Data plane source SGT scales better.
- SXP can be hard to design correctly in medium to large scale SD-Access networks.
 - Peer SXP per SD-Access Border Node. SXP peering limits on ISE = SXP reflectors.
 - Memory limits on switches can be a bottleneck in larger deployments.
 - SXP does not easily capture static SGTs.

SGT in the Data Plane

CMD in Ethernet

Note: dropped by non-SGT capable network infrastructure.

Review TrustSec capability matrix:

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



```
▶ 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
```

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
```

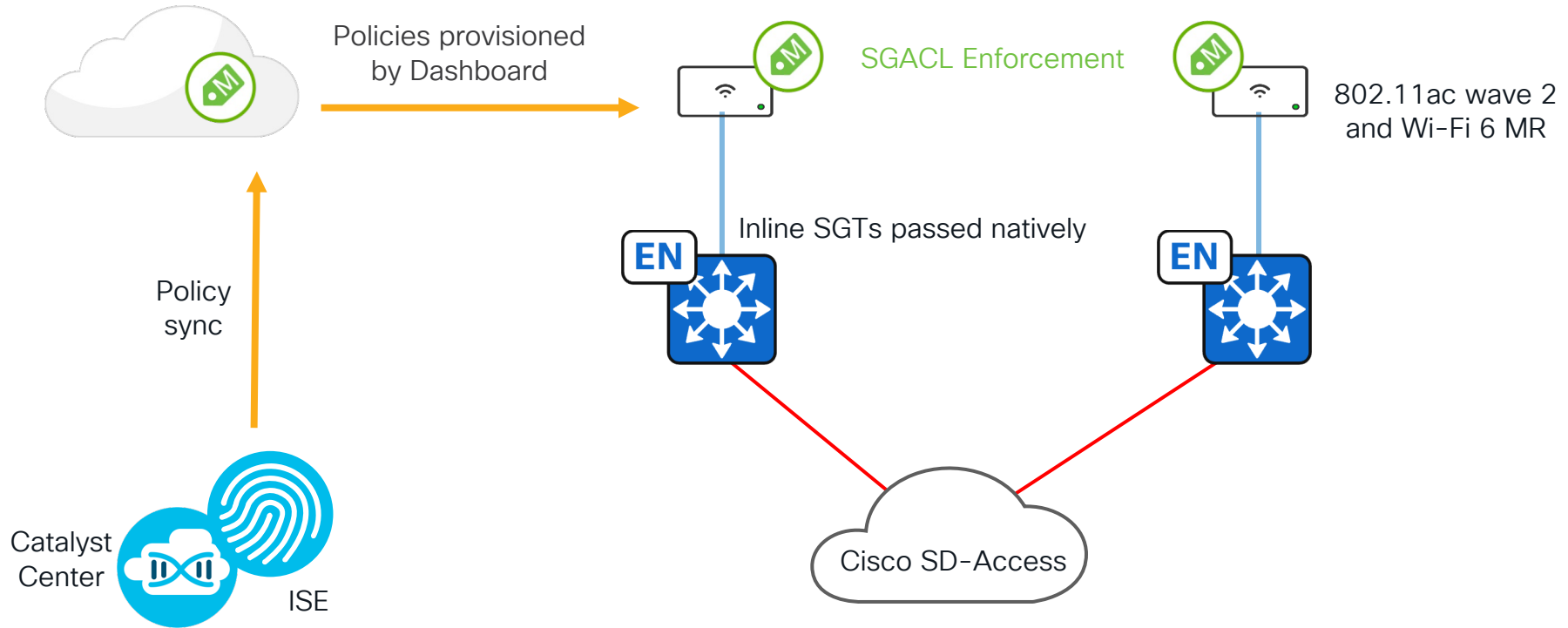
CMD in GRE

```
▶ 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
```

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..2.Lw m\p...E
  0010 00 78 00 00 00 00 ff 32 5f 56 ac 1d 01 e2 ac 1d x.....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 07 42 99 4a 1b b9 91 b8 <.:@.lh .gV....
  0040 d8 d2 a4 60 94 0f 06 76 03 ..:...t}...v...
  0050 fa 29 06 91 7b ca 4f c7 47 ..:...{.#.?A...0-G
  0060 fe 8b 7c 8a da ca 70 32 z1 e9 04 02 d9 a8 c3 bc ..]...v2 !.d....
  0070 97 e7 9a 89 77 8c ff 4a ec 07 61 b1 5d 17 27 2b ...w...J ..a..'+
  0080 c1 be 65 7e 14 d1 ..e...
```

Cisco SD-Access and Meraki Adaptive Policy



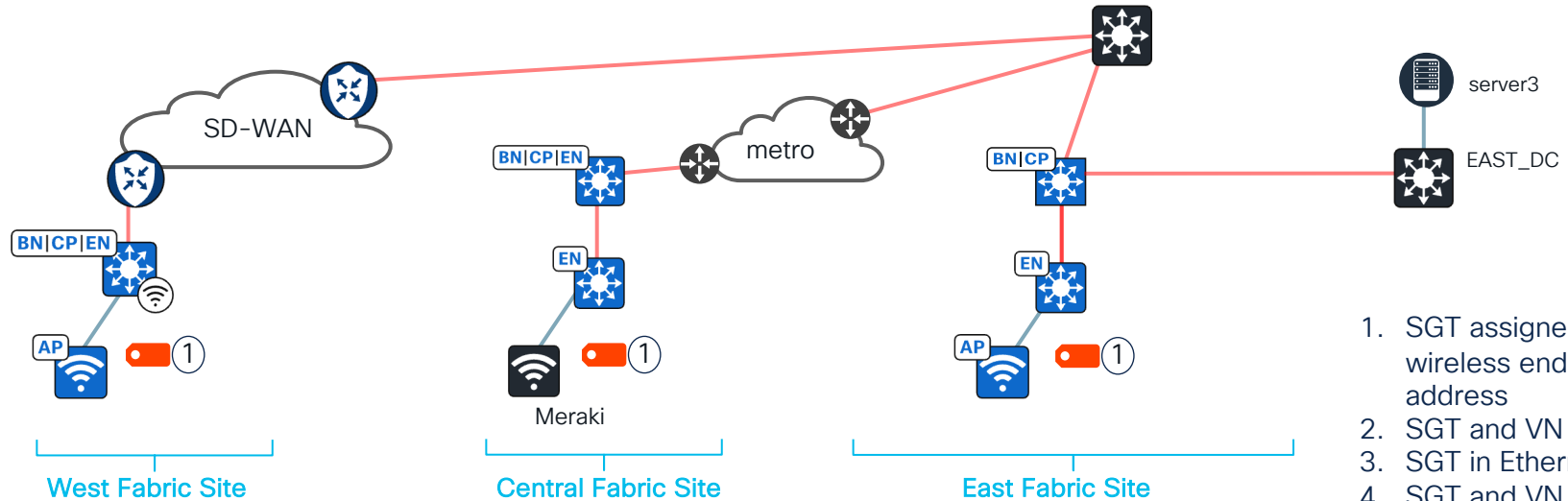
Demo: Transits and End to End Segmentation

- Connect ISE to Meraki Dashboard for Central site Adaptive Policy.
- Connect Central site and East site to Cisco SD-Access Transit.
- Test Central intra-site and inter-site connectivity and segmentation.
- Confirm West site Independent Domains SD-WAN Edge and SD-Access Border Node per-VRF connectivity and SGT propagation.
- Test West intra-site and inter-site connectivity and segmentation.
- Create IP:SGT mappings from EAST_DC server3 and enable policy enforcement towards EAST_DC
- Test segmentation towards EAST_DC server3.

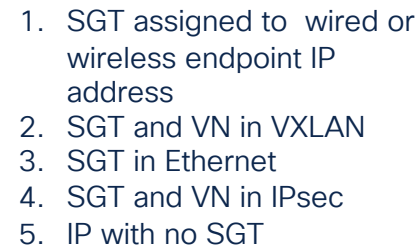
Discussed Previously

- SXP and VRF in [BRKCRS-2819](#) at Cisco Live San Diego 2019.
- SGT and VRF in mGRE (DMVPN) in [BRKCRS-2819](#) at Cisco Live Barcelona 2020.

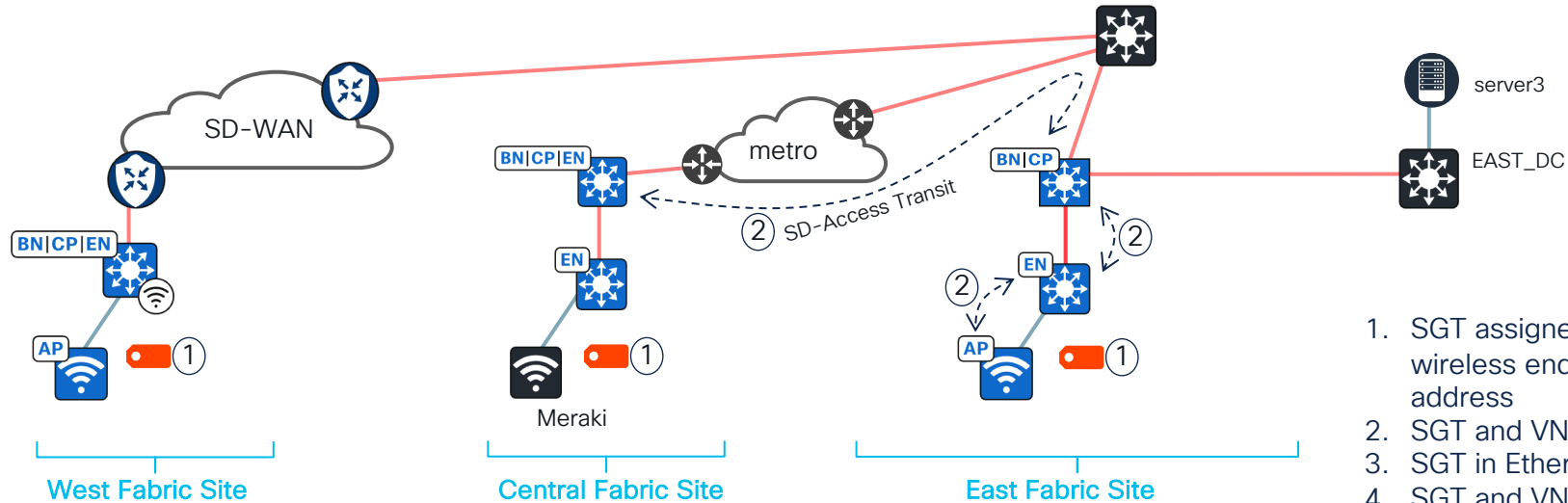
Demo: Transits with End to End Segmentation



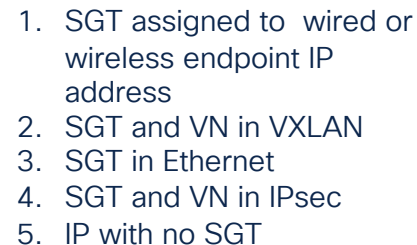
1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT



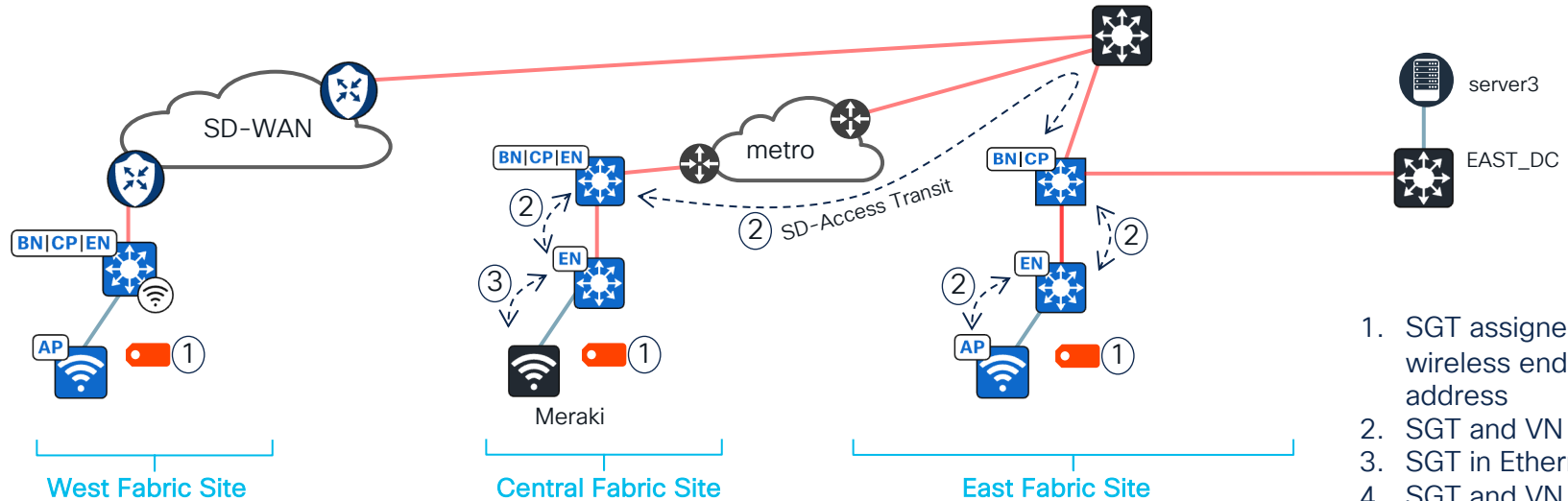
Demo: Transits with End to End Segmentation



1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT

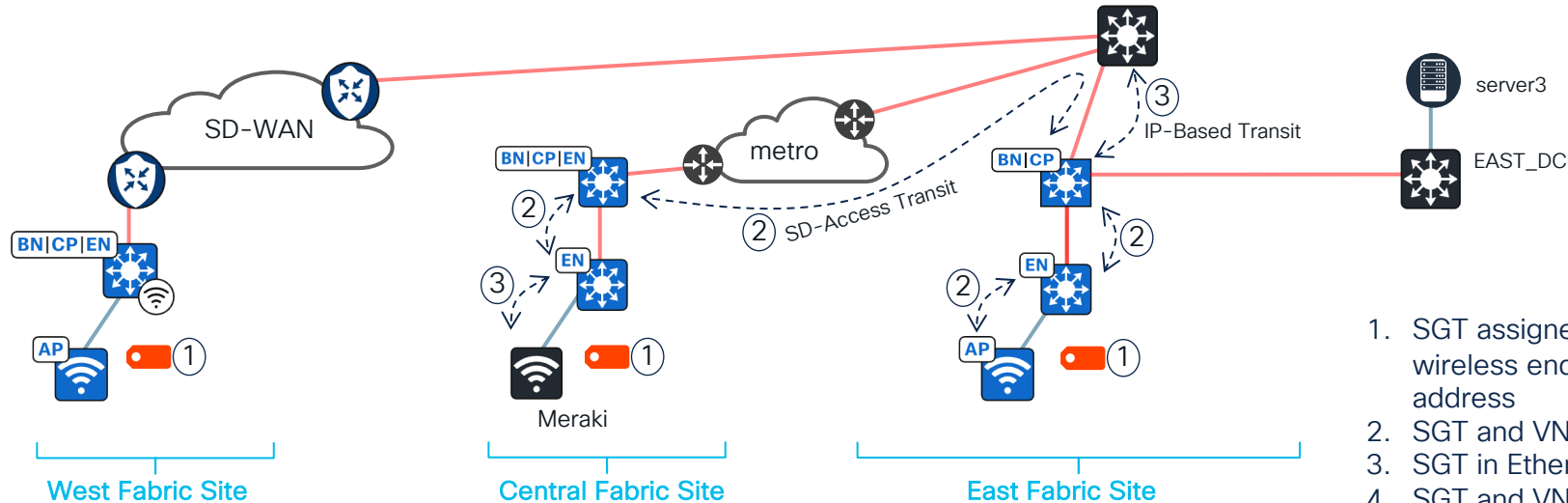


Demo: Transits with End to End Segmentation

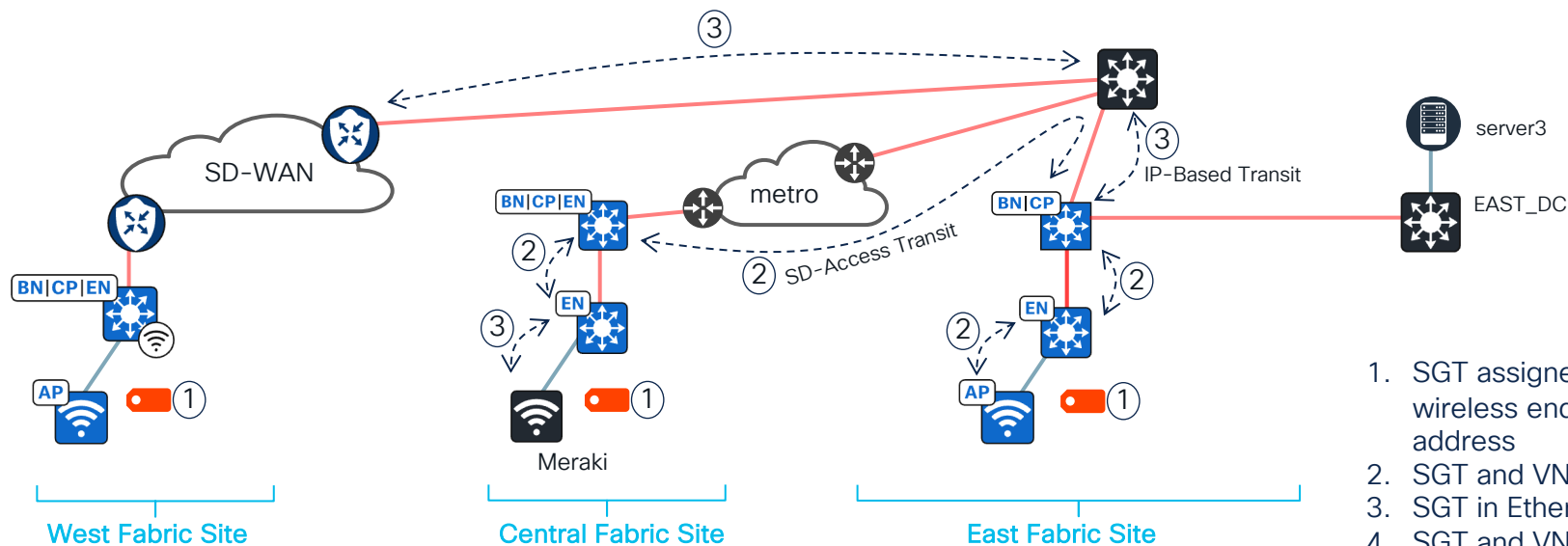


1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT

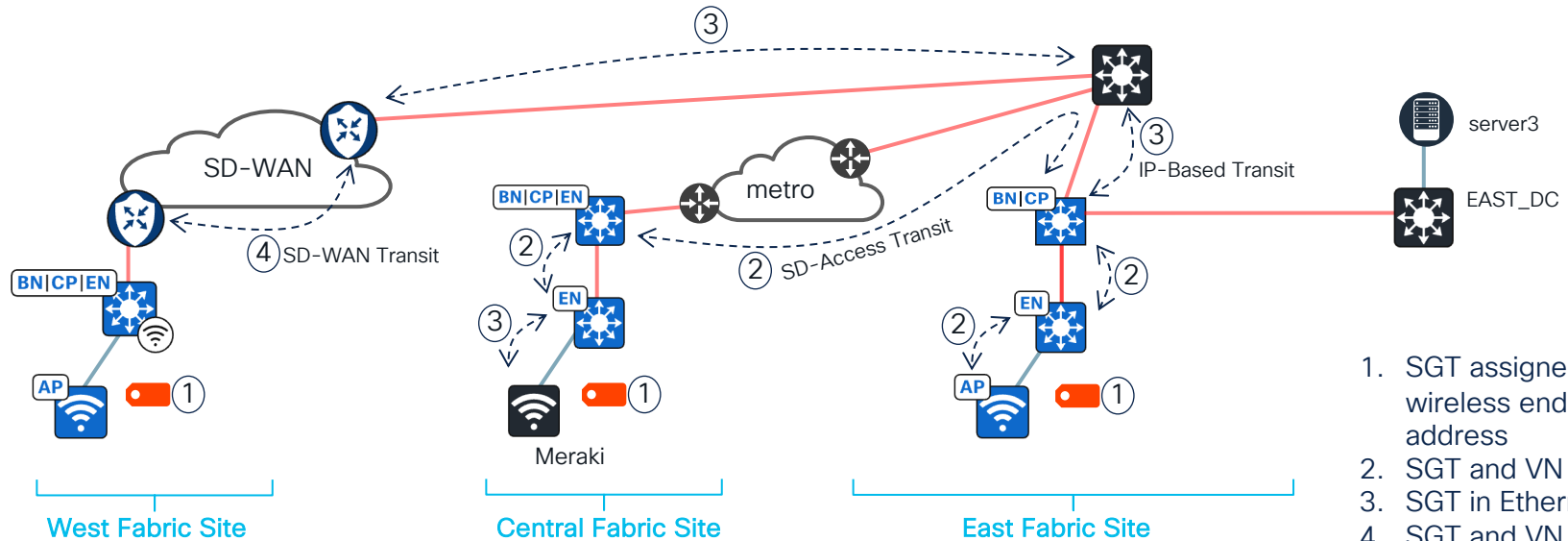
Demo: Transits with End to End Segmentation



Demo: Transits with End to End Segmentation

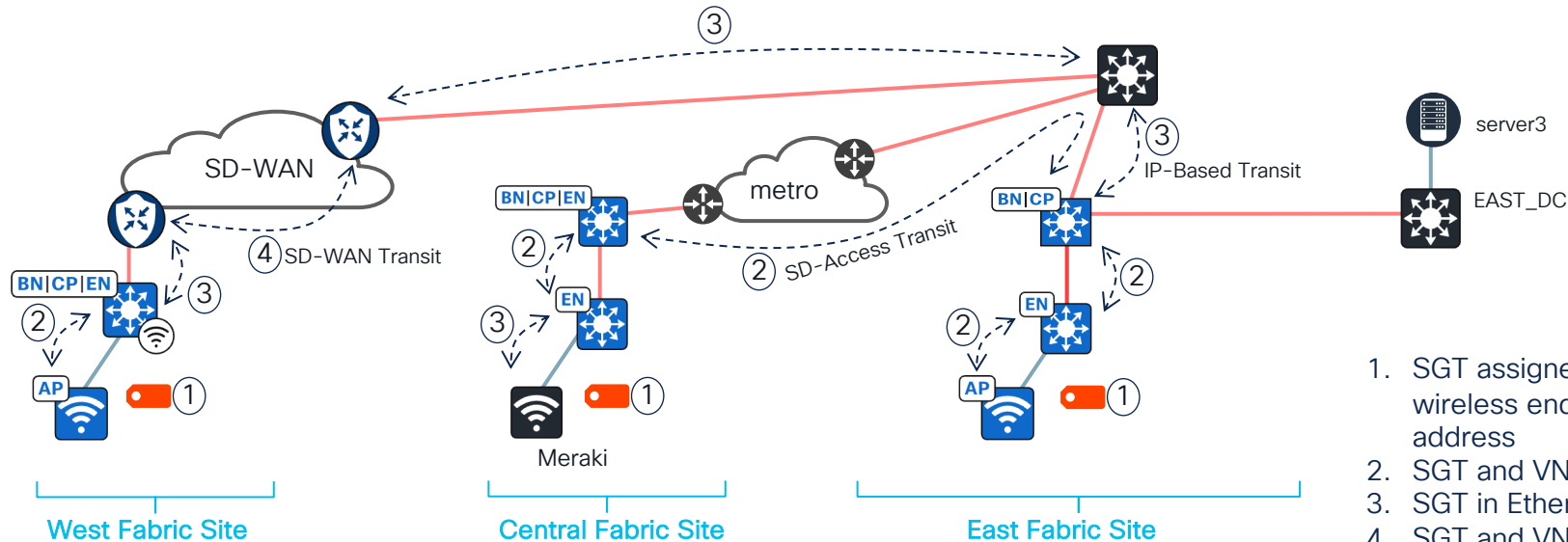


Demo: Transits with End to End Segmentation

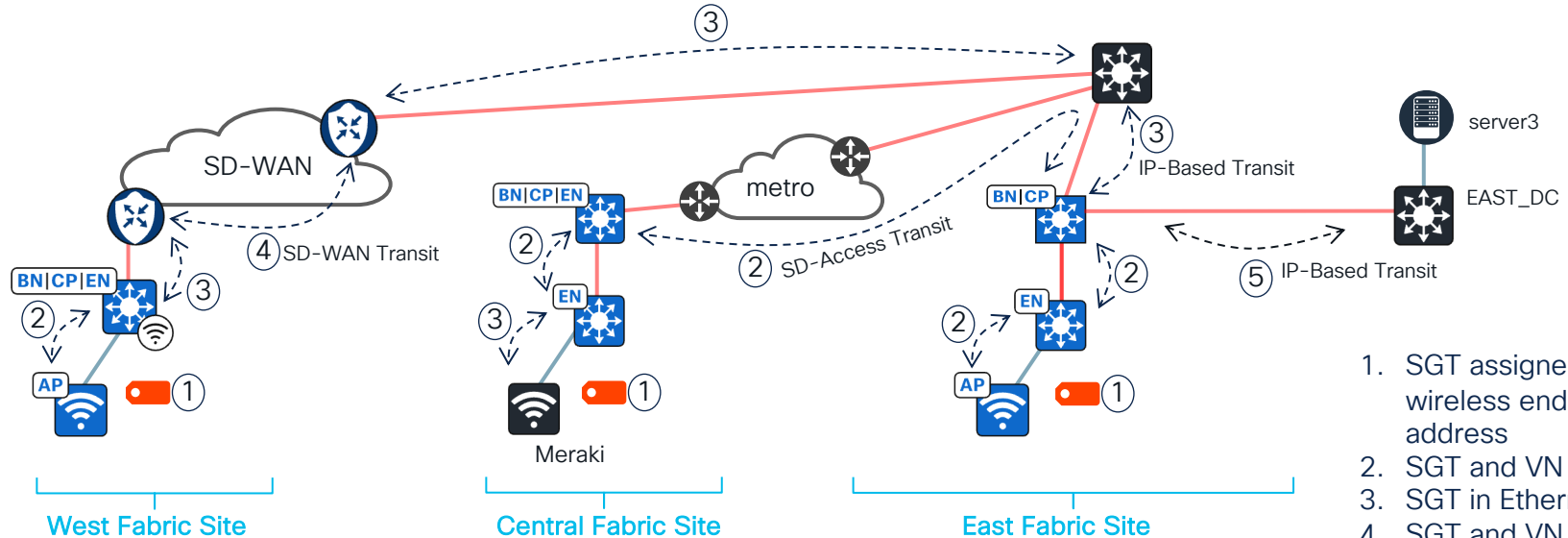


1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT

Demo: Transits with End to End Segmentation

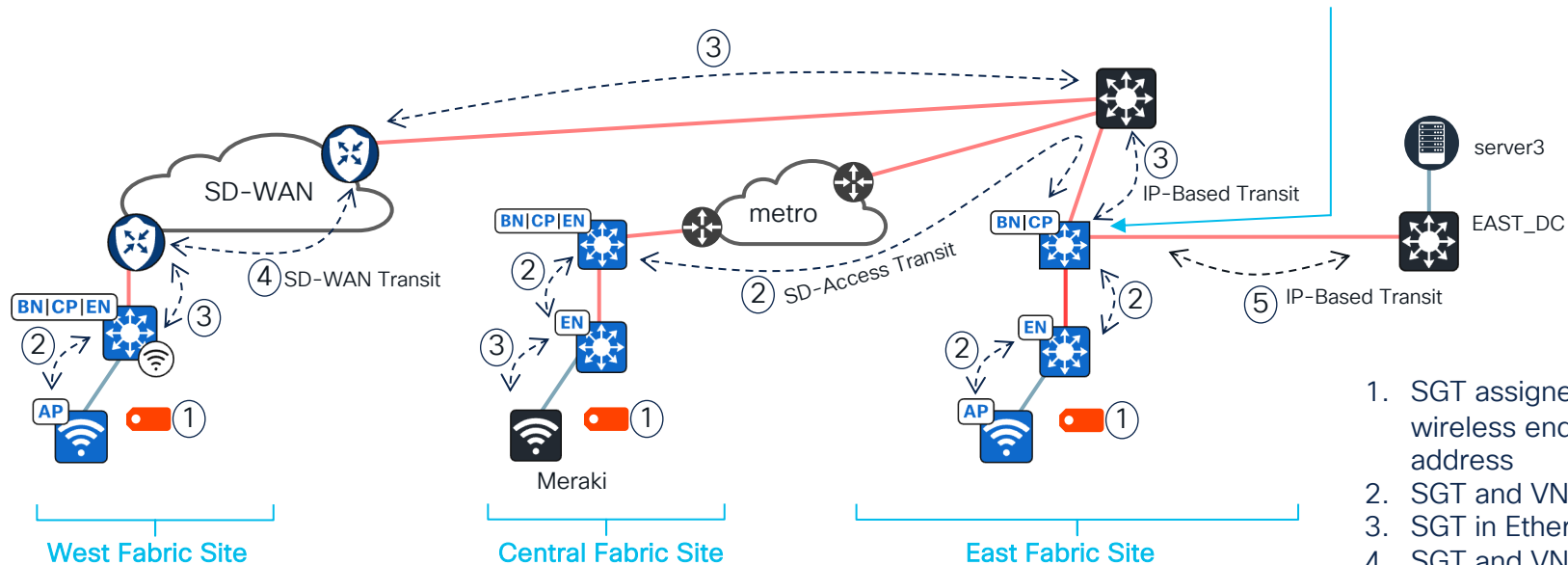


Demo: Transits with End to End Segmentation



Demo: Transits with End to End Segmentation

```
!BN L3VN Static IP-SGT mappings for external assets
cts role-based sgt-map vrf CORP_VN 10.4.255.0/24 sgt 9
!
!SGT policy enforcement on L3 handoff VLAN towards EAST DC
cts role-based enforcement vlan-list 2222
```



Wireless Design Options



Fabric-Enabled Wireless

- **Single** Management platform for Wired/Wireless
 - Centralized Control Plane for Wireless
 - Distributed Data Plane for Wireless
 - No broadcast needed on the AP pool
- Consistent Access Policy definition for Wired/Wireless
 - **Consistent Policy Enforcement** Point for Wired/Wireless
- Wireless Control Plane integration with Fabric Control Plane – **Performance** for onboarding and roaming of wireless endpoints **at massive scale**
- Policy for East-West traffic is enforced at Fabric Edge Security **policies enforced by switch in hardware (e.g. SGACLs)** – no performance impact

Cloud / MR Locally Switched Wireless

- Separate Management platform for Wired/Wireless
 - Centralized Cloud Control Plane for Wireless
 - Distributed Data Plane for Wireless
 - Broadcast needed on the AP pool (Meraki)
- Consistent Access Policy definition for Wired/Wireless
 - Separate Policy Enforcement Points
 - (AP for Wireless, Switch for Wired)
- No integration between Wireless Control Plane and Fabric Control Plane – Performance and scale for onboarding and roaming depends on broadcast flooding capacity of the wired network
- Policy for East-West traffic is enforced at AP
 - Security policies enforced by AP in software – potential performance impact



Non-Fabric Wireless Local Switching

- Cisco SD-Access Anycast Gateways serving non-Fabric locally switched APs should have Intra-Subnet Routing enabled for fast wireless endpoint roaming, but there are tradeoffs:
 - No IPv6 on ISR Anycast Gateways.
 - No optional Layer 2 flooding over VXLAN for ISR Anycast Gateways.
 - For fast wireless client roaming the non-Fabric locally switched APs should patch to SD-Access Edge Nodes, not Policy Extended Nodes.
- Non-Fabric locally switched wireless and Layer 2 flooding:
 - Meraki AP management VLAN must have Layer 2 Flooding enabled for key distribution.
 - No Layer 2 Flooding is required to service the Cisco Catalyst FlexConnect wireless.
 - For non-Cisco locally switched wireless, the vendor may require Layer 2 Flooding in client VLANs, it depends on the vendor.



Non-Fabric Wireless Local Switching

- In this demo Meraki APs are authenticated by closed authentication Edge Node ports. ISE sends an interface template AV pair that calls an Interface Template on the Edge Node.

- ISE Authorization Profile

```
Access Type = ACCESS_ACCEPT  
cisco-av-pair = interface-template-name=MERAKI_FLEX_AP_TEMPLATE
```

- Corresponding IOS XE Interface Template

```
template MERAKI_FLEX_AP_TEMPLATE  
  cts manual  
  policy static sgt 2 trusted  
  no cts role-based enforcement  
  switchport trunk native vlan 1021  
  switchport trunk allowed vlan 1021,1023  
  switchport mode trunk  
  access-session host-mode multi-host peer
```

Demo

LAN to DC Segmentation

For More Information

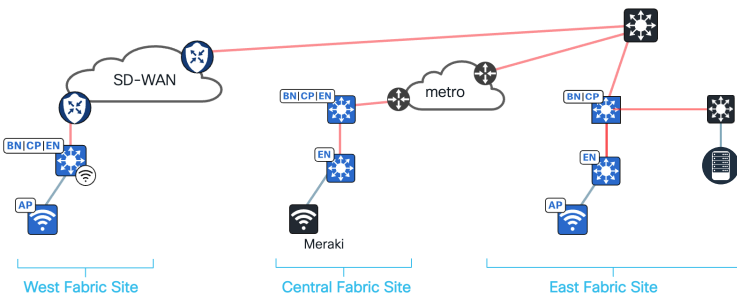
- Watch later at ciscolive.com:
 - [BRKSEC-2845 Cisco Secure Firewall and SD-Access Integration Deep Dive](#)
- Integrate Cisco Secure Firewall Management Centre with ISE pxGrid:
 - <https://community.cisco.com/t5/security-documents/how-to-configure-pxgrid-in-ise-production-environments/ta-p/3646330?attachment-id=145871>
 - https://www.cisco.com/c/en/us/td/docs/security/firepower/630/fdm/fptd-fdm-config-guide-630/fptd-fdm-identity-sources.html#id_71786
- [Cisco Secure Dynamic Attributes Connector Configuration Guide](#)

Demo: Firewall Segmentation with SGT and DC Attributes

- Integrate FMC with ISE.
- Use CSDAC to load AWS SG:IP pairs into Cisco Secure Firewall Management Centre (FMC).
- Use APIC FMC Endpoint Update application to load EPG attributes into Cisco Secure Firewall Management Centre (FMC).
- Load server3 static IP:SGT pair into ISE, so it's propagated to Cisco Secure Firewall Management Centre (FMC).
- Build required FMC policies incorporating SGT, ACI and AWS attributes.
- Test and prove connectivity outcomes.

Demo: Firewall Segmentation with SGT and DC Attributes

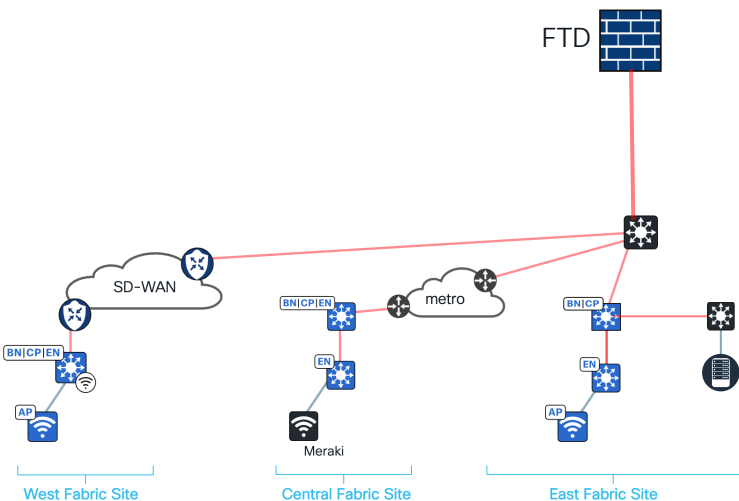
IP	SGT
10.4.1.10	Employee
10.3.1.10	BMS
10.3.1.10	CCTV
	etc...



CISCO *Live!*

1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT

Demo: Firewall Segmentation with SGT and DC Attributes



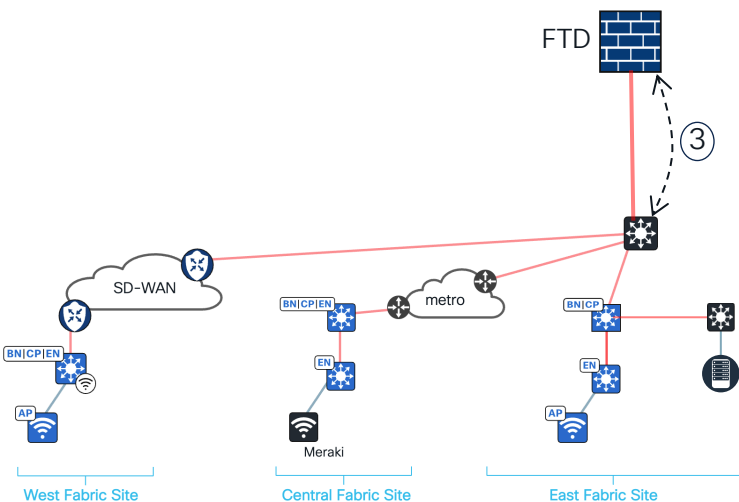
IP	SGT
10.4.1.10	Employee
10.3.1.10	BMS
10.3.1.10	CCTV
	etc...



Cisco Secure Firewall
Management Center

1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT

Demo: Firewall Segmentation with SGT and DC Attributes



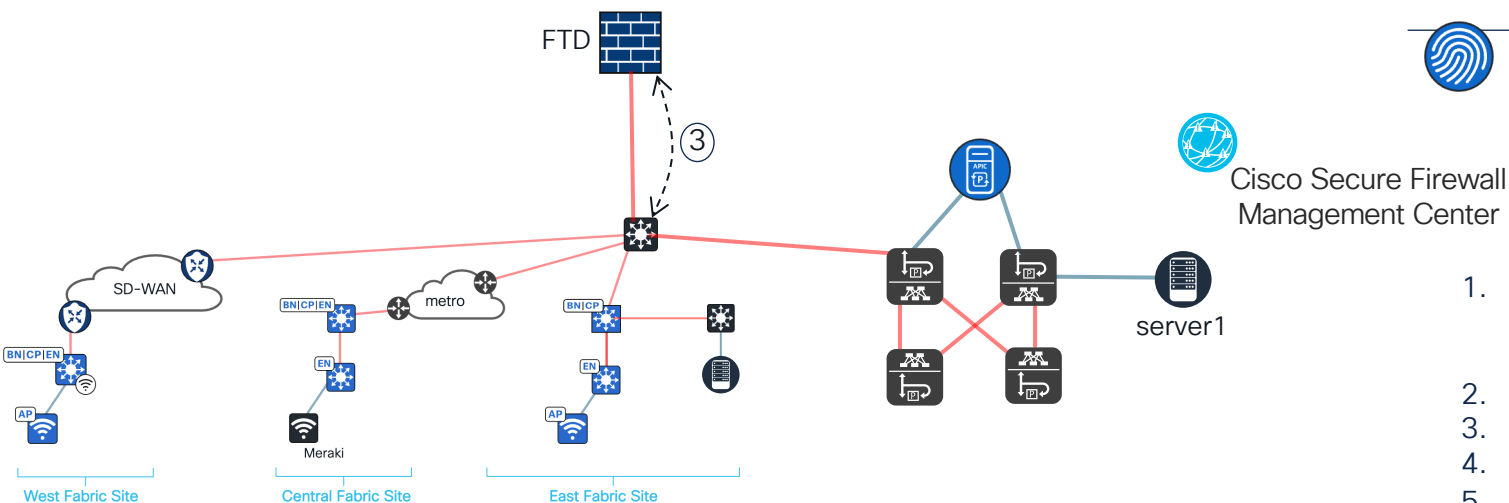
IP	SGT
10.4.1.10	Employee
10.3.1.10	BMS
10.3.1.10	CCTV
	etc...



Cisco Secure Firewall
Management Center

1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT

Demo: Firewall Segmentation with SGT and DC Attributes



IP	SGT
10.4.1.10	Employee
10.3.1.10	BMS
10.3.1.10	CCTV
	etc...

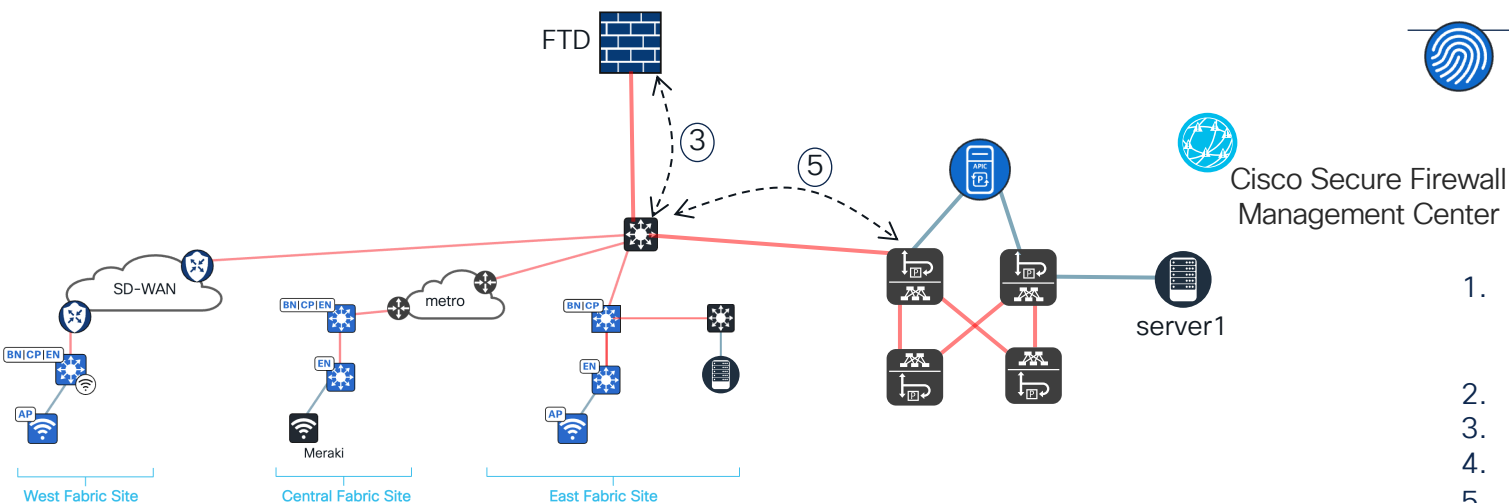


Cisco Secure Firewall
Management Center



1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT

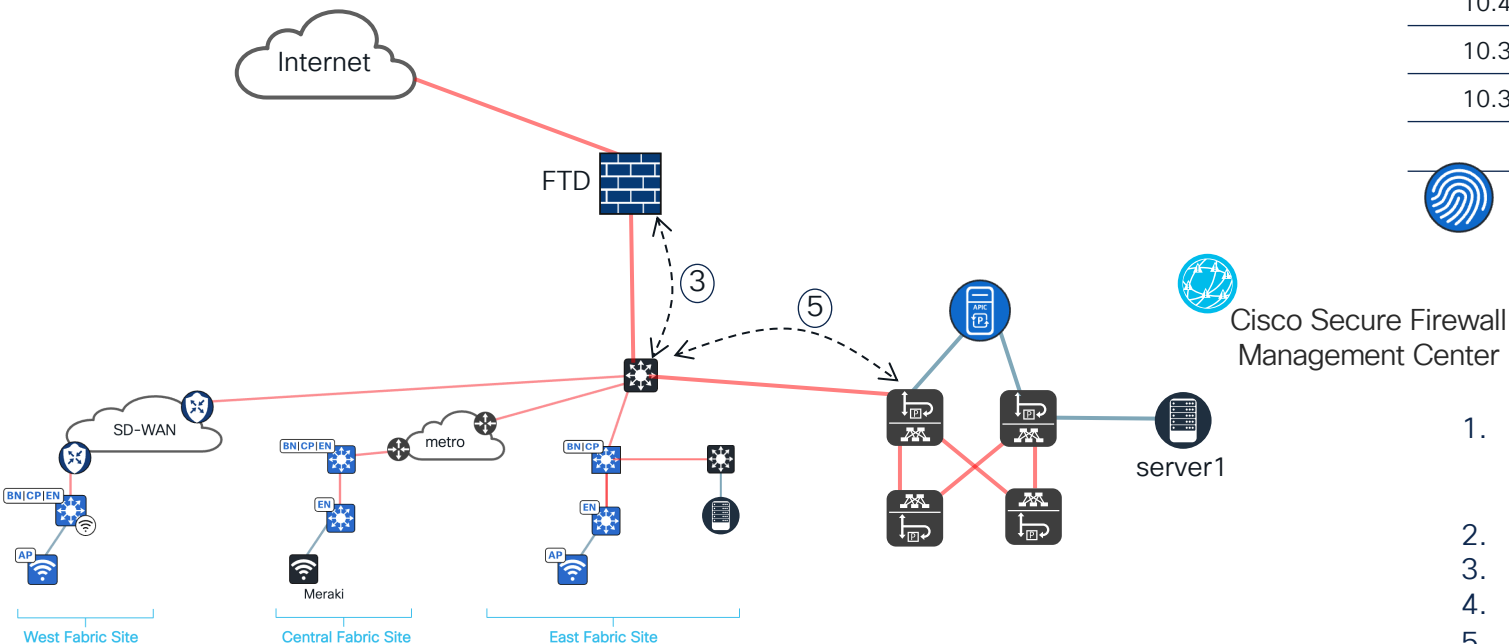
Demo: Firewall Segmentation with SGT and DC Attributes



IP	SGT
10.4.1.10	Employee
10.3.1.10	BMS
10.3.1.10	CCTV
	etc...



Demo: Firewall Segmentation with SGT and DC Attributes

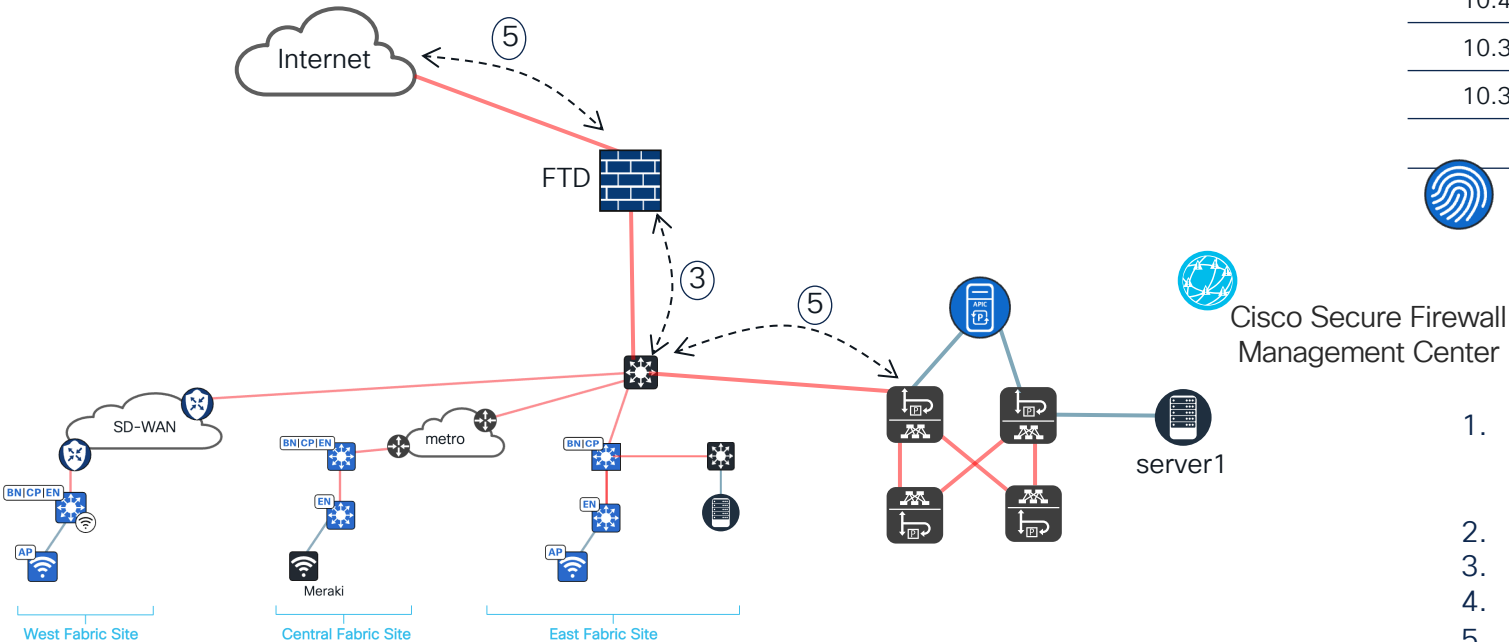


IP	SGT
10.4.1.10	Employee
10.3.1.10	BMS
10.3.1.10	CCTV
	etc...



1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT

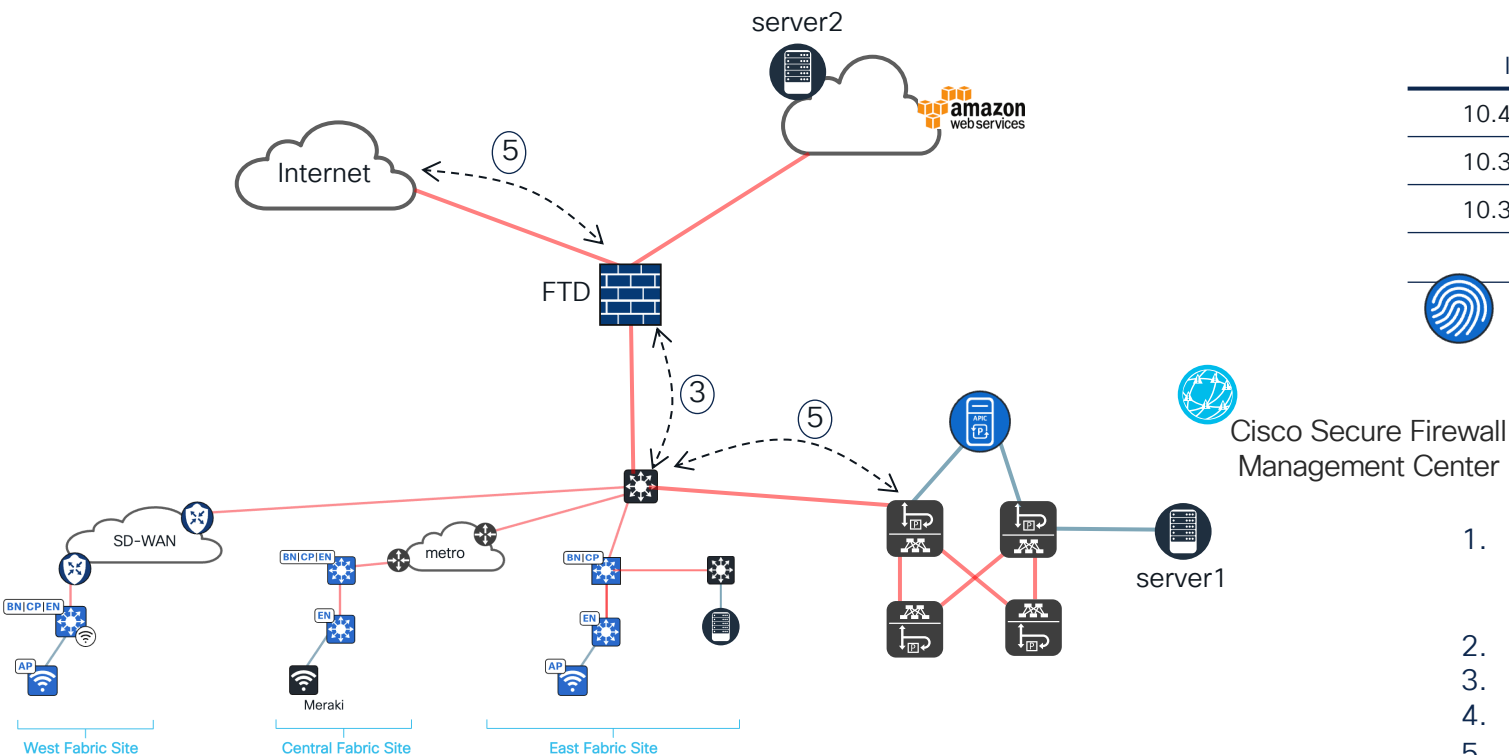
Demo: Firewall Segmentation with SGT and DC Attributes



IP	SGT
10.4.1.10	Employee
10.3.1.10	BMS
10.3.1.10	CCTV
	etc...



Demo: Firewall Segmentation with SGT and DC Attributes



IP	SGT
10.4.1.10	Employee
10.3.1.10	BMS
10.3.1.10	CCTV
	etc...



Cisco Secure Firewall Management Center

1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT

CISCO *Live!*



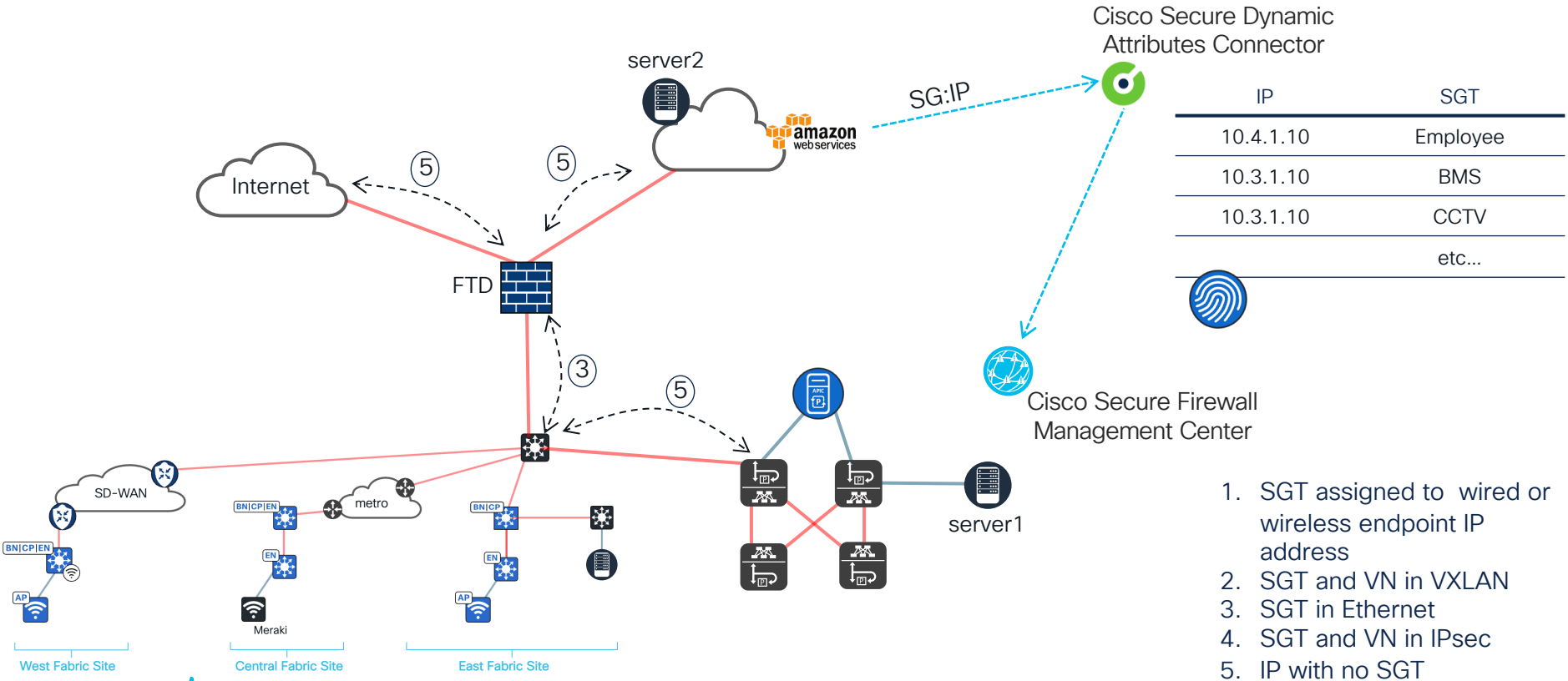
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

86

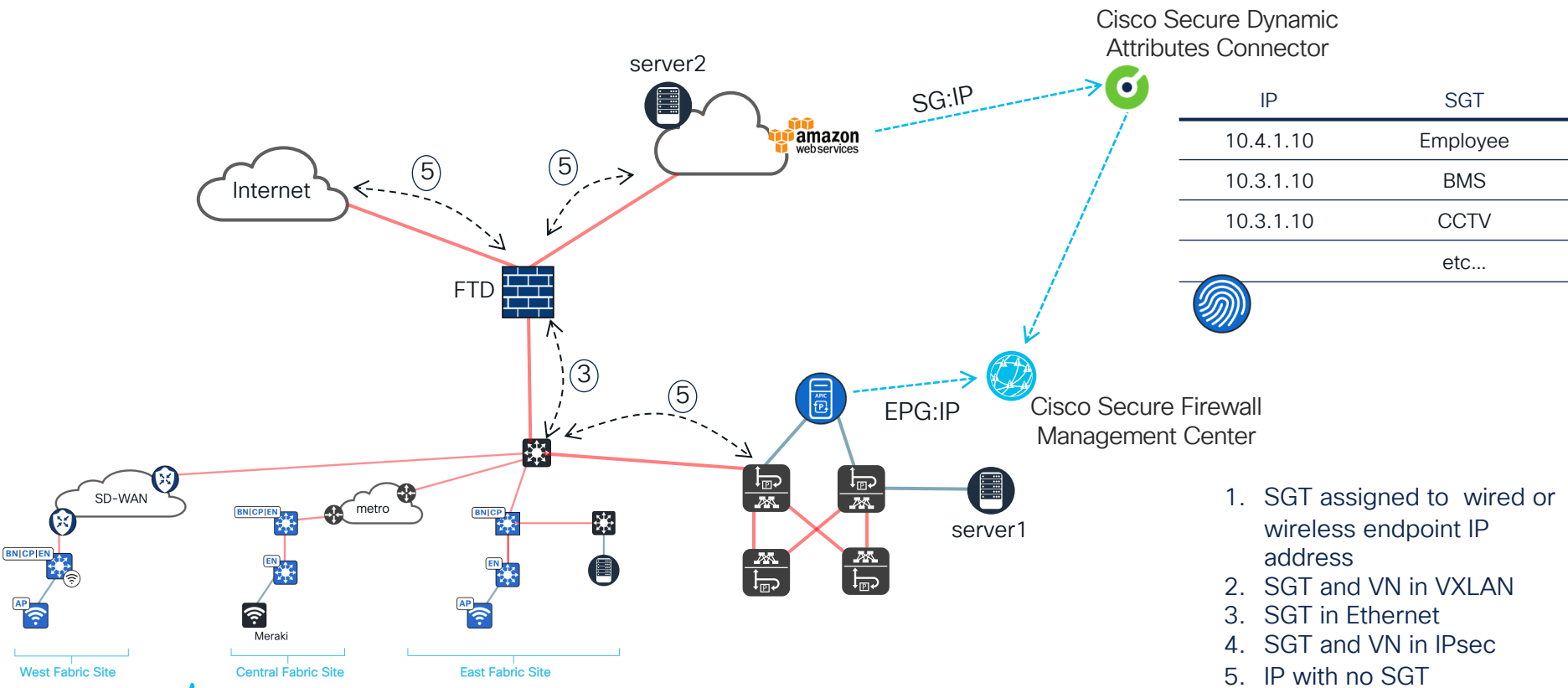


1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT

Demo: Firewall Segmentation with SGT and DC Attributes



Demo: Firewall Segmentation with SGT and DC Attributes



CISCO *Live!*



1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT

CISCO *Live!*



1. SGT assigned to wired or wireless endpoint IP address
2. SGT and VN in VXLAN
3. SGT in Ethernet
4. SGT and VN in IPsec
5. IP with no SGT

CISCO *Live!*





Demo

cisco *Live!*

#CiscoLifeAPJC

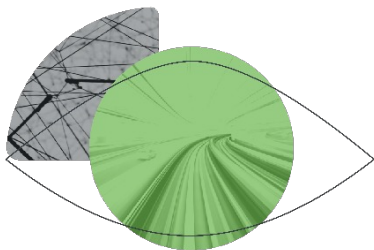
Access Privileges with Endpoint Analytics

For More Information

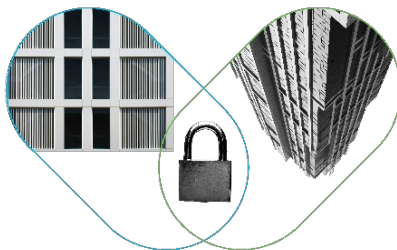
- Watch later at ciscolive.com:
 - [BRKENS-2850 What is Your First Step in Protecting Endpoints and Reducing the Attack Surface?](#)
 - [BRKENS-2851 Identify Suspicious Behavior, Limit Attack Exposure on Endpoints Using Trust Analytics](#)
- Cisco AI Endpoint Analytics Deployment Guide:
 - <https://community.cisco.com/t5/networking-knowledge-base/cisco-ai-endpoint-analytics-deployment-guide/ta-p/4266702>

Cisco Zero Trust – Network and Cloud

Visibility



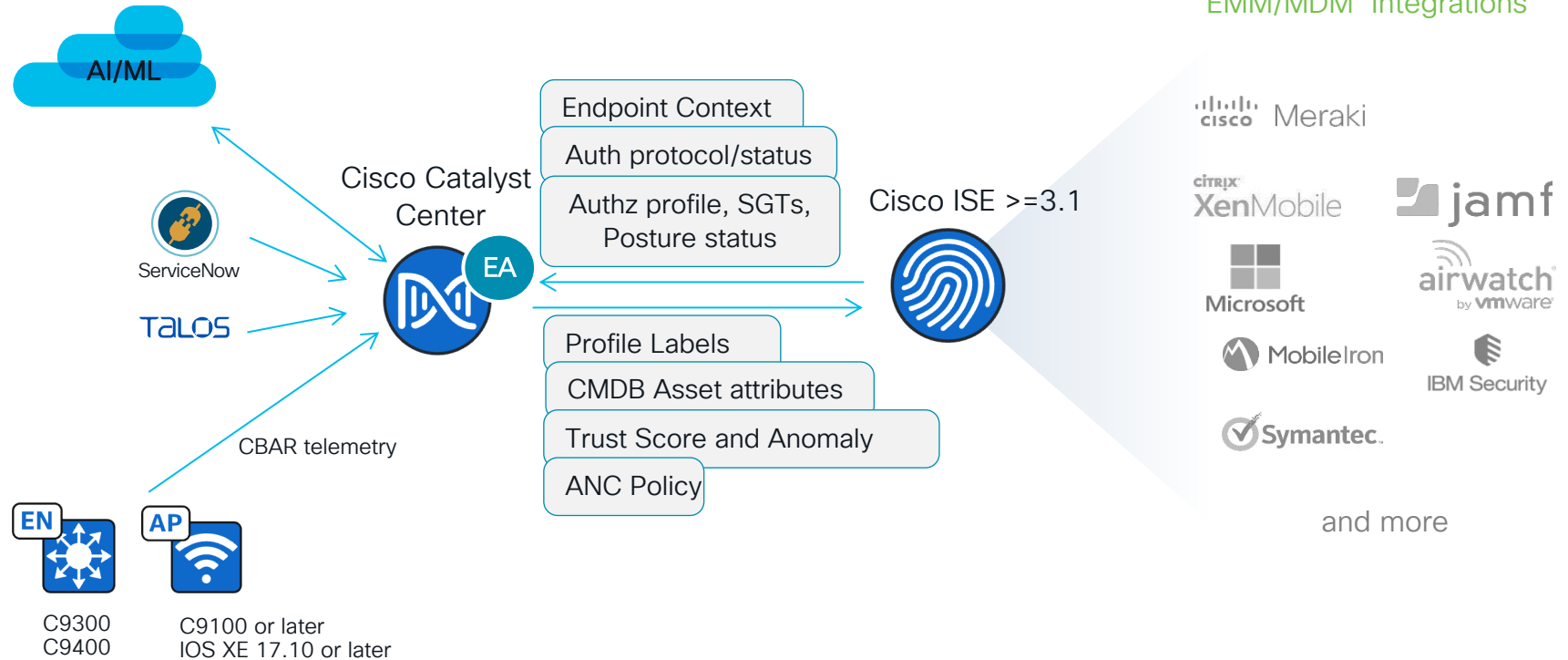
Segmentation



Containment



Endpoint Analytics and Trust Analytics Architecture





Compatibility Matrix

Catalyst Center	EA Capability	Cat9K Needed?	Min Cat9k Version	Wired CAT9k		Wireless CAT9800 ⁵		Traffic Telemetry Appliance (TTA)	ISE Needed?	
				Fabric	Non-Fabric	Local	Flex		For Endpoint Visibility in EA	For Policy Enforcement ⁶
2.1.2.x	DPI Based Profiling	Yes	17.3.1+	✓	✓	✓	✓	✓	No	Yes
	AI Smart Grouping	Optional ¹	17.3.1+	✓	✓	✓	✓	✓	Optional ¹	Yes
	ISE Asset topic integration	No	NA	NA	NA	NA	NA	NA	No	Yes
2.2.2.x	AI Spoofing Detection ³	Optional ¹	17.3.1+	✓	✓	✓	✓	✓	Optional ¹	Yes
2.2.3.x	Changed profile labels	Yes	17.6.1+	✓	✓	✓	✓	✓	No	Yes
	NAT Detection	Yes	17.6.1+	✓	✓	✓	✓	✓	No	Yes
	Concurrent MAC Detection	Yes	17.6.1+	✓	✓	✓ ²	✓ ²	✗	No	Yes
	ISE Auth method visibility	No	NA	NA	NA	NA	NA	NA	Yes (3.1+)	NA
	ISE Posture visibility	No	NA	NA	NA	NA	NA	NA	Yes (3.1+)	NA
	ISE Enhanced Authz Integration	No	NA	NA	NA	NA	NA	NA	NA	Yes (3.1+)
2.3.2.x (CA)	Open Port Scan ⁴	Yes	17.7.1+	✓	✓	✗	✗	✗	No	Yes
	Weak Credential Scan ⁴	Yes	17.7.1+	✓	✓	✗	✗	✗	No	Yes
2.3.3.x	Talos Low Reputation ³ IP	No	NA	NA	NA	NA	NA	NA	No	Yes

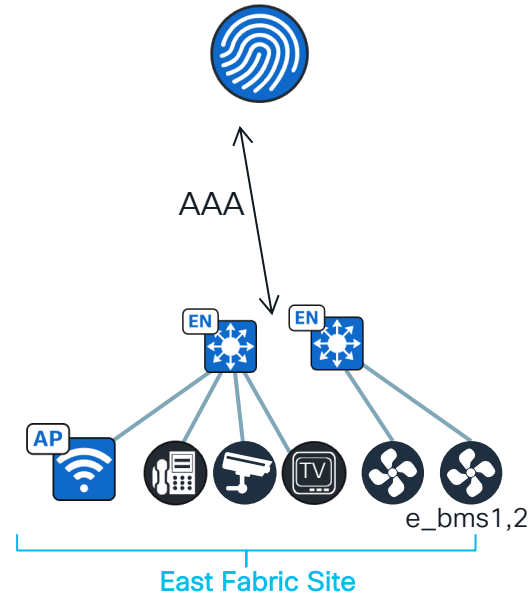
Demo: Analytics-Based Access Privileges

- Profile some real endpoints with Endpoint Analytics. Use results to assign network access privileges.
- Test and prove connectivity outcomes.

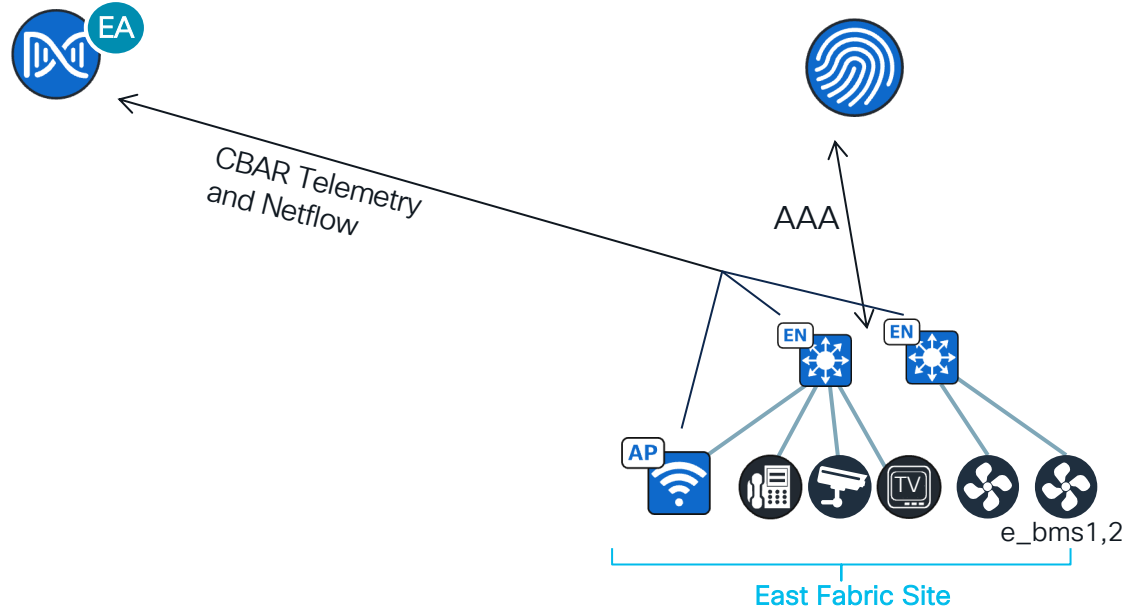
Discussed Previously

- Cisco Secure Network Analytics (Stealthwatch) and Encrypted Traffic Analytics (ETA) in [BRKCRS-2819](#) at Cisco Live Barcelona 2020.
- Cisco Trust Analytics [BRKENS-2819](#) at Cisco Live Las Vegas 2023

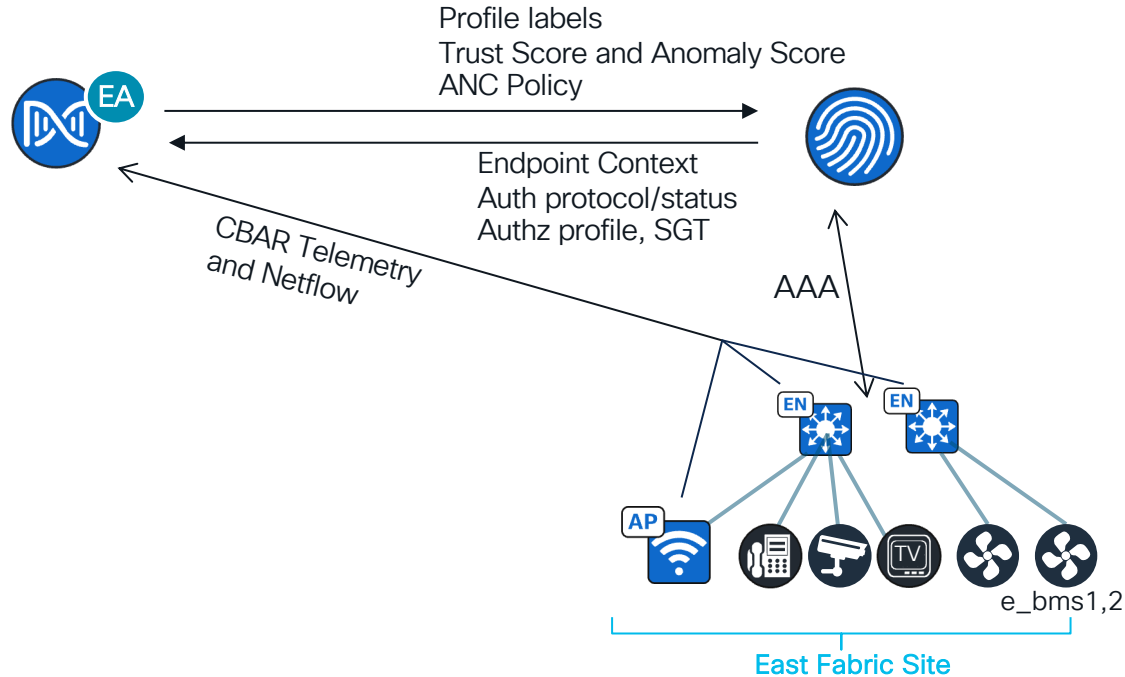
Demo: Analytics-Based Access Privileges



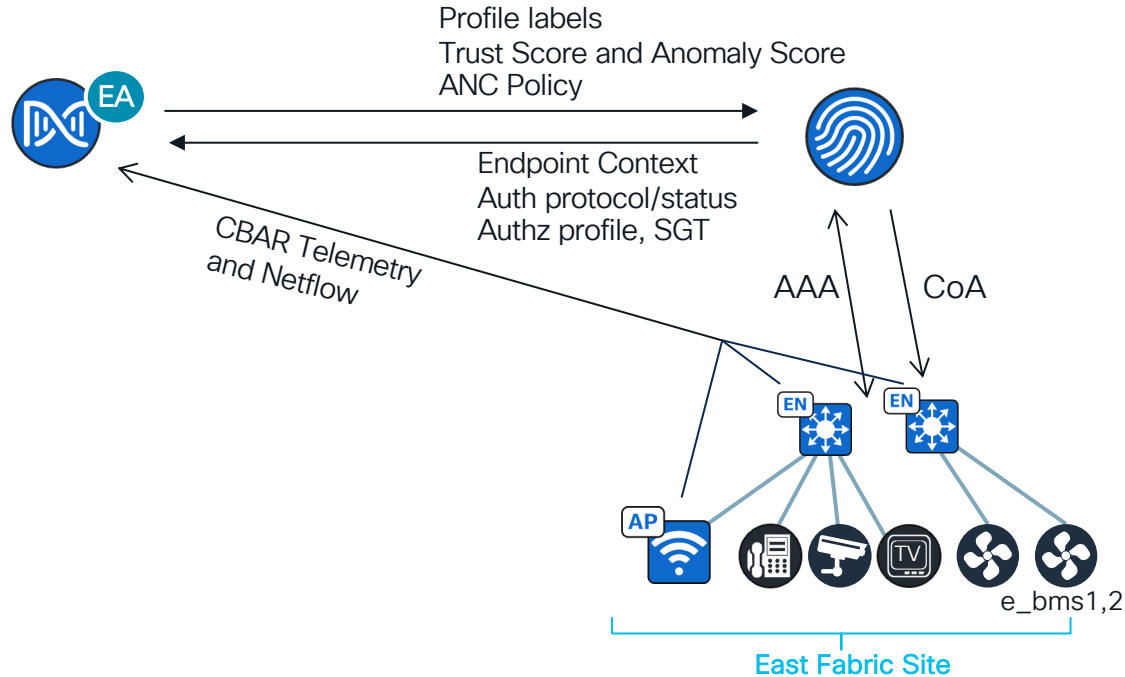
Demo: Analytics-Based Access Privileges



Demo: Analytics-Based Access Privileges



Demo: Analytics-Based Access Privileges



Extended Detection and Response

For More Information

- [Cisco XDR landing page](#)
- [Cisco Endpoint Security landing page](#)
- [Cisco Umbrella landing page](#)
- [Cisco Secure Cloud Analytics landing page](#)

Cisco XDR



Demo: Extended Detection and Response

- Configure XDR to consume Umbrella and Cisco Secure Endpoint events.
- Define an XDR incident response automation, in this case apply Quarantine SGT to the offending endpoint.
- From e_staff, access malware file. Confirm detection and manually quarantine the endpoint via SGT change from BMS to Quarantine.
- From e_bms2, access a malware URL and confirm automatic quarantine of the endpoint via SGT change from BMS to Quarantine.

Demo: Secure Endpoint and Rapid Threat Containment

Secure Malware Analytics

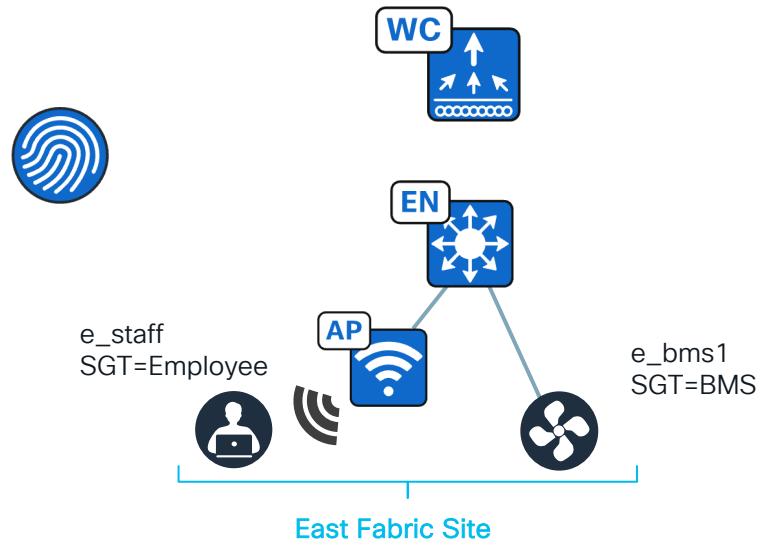


XDR



Umbrella

Internet SaaS



Demo: Secure Endpoint and Rapid Threat Containment

Secure Malware Analytics



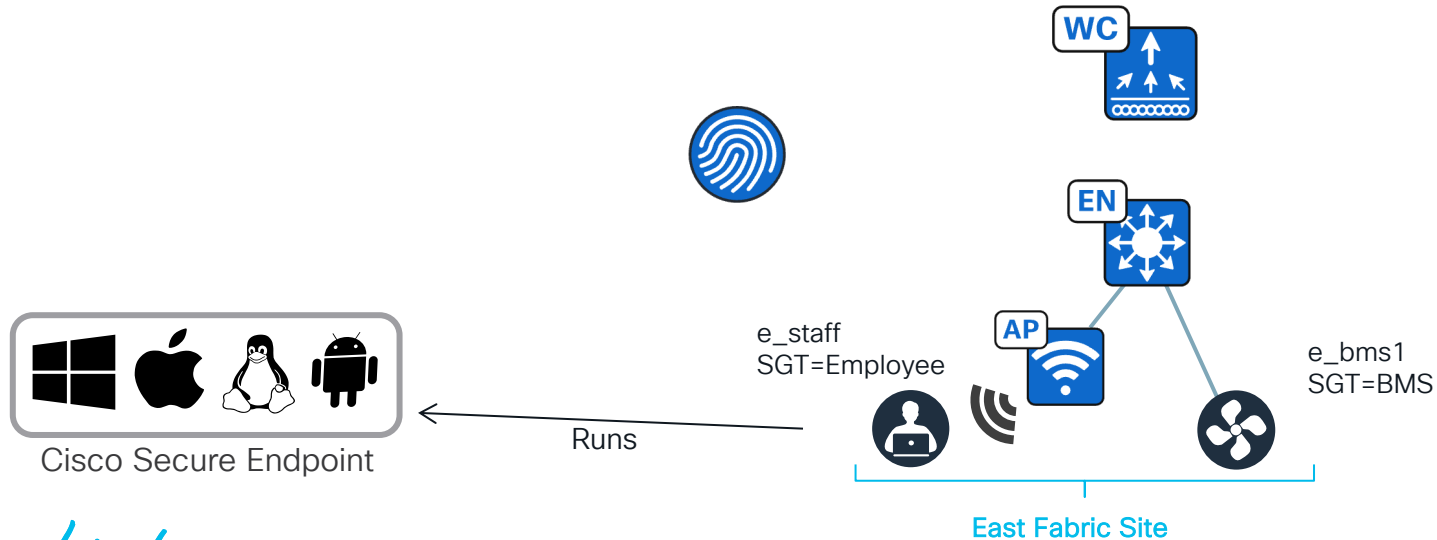
XDR



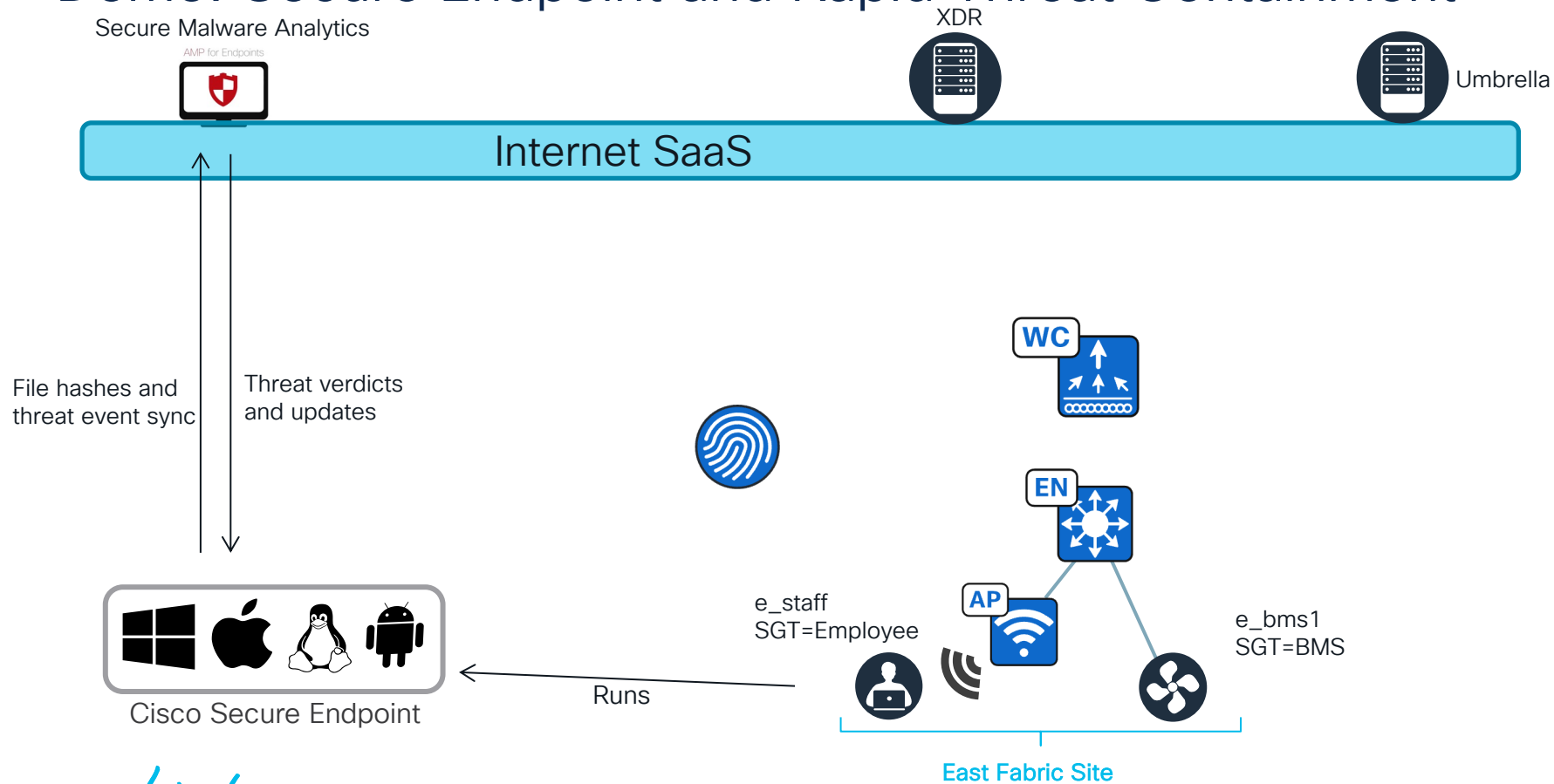
Umbrella



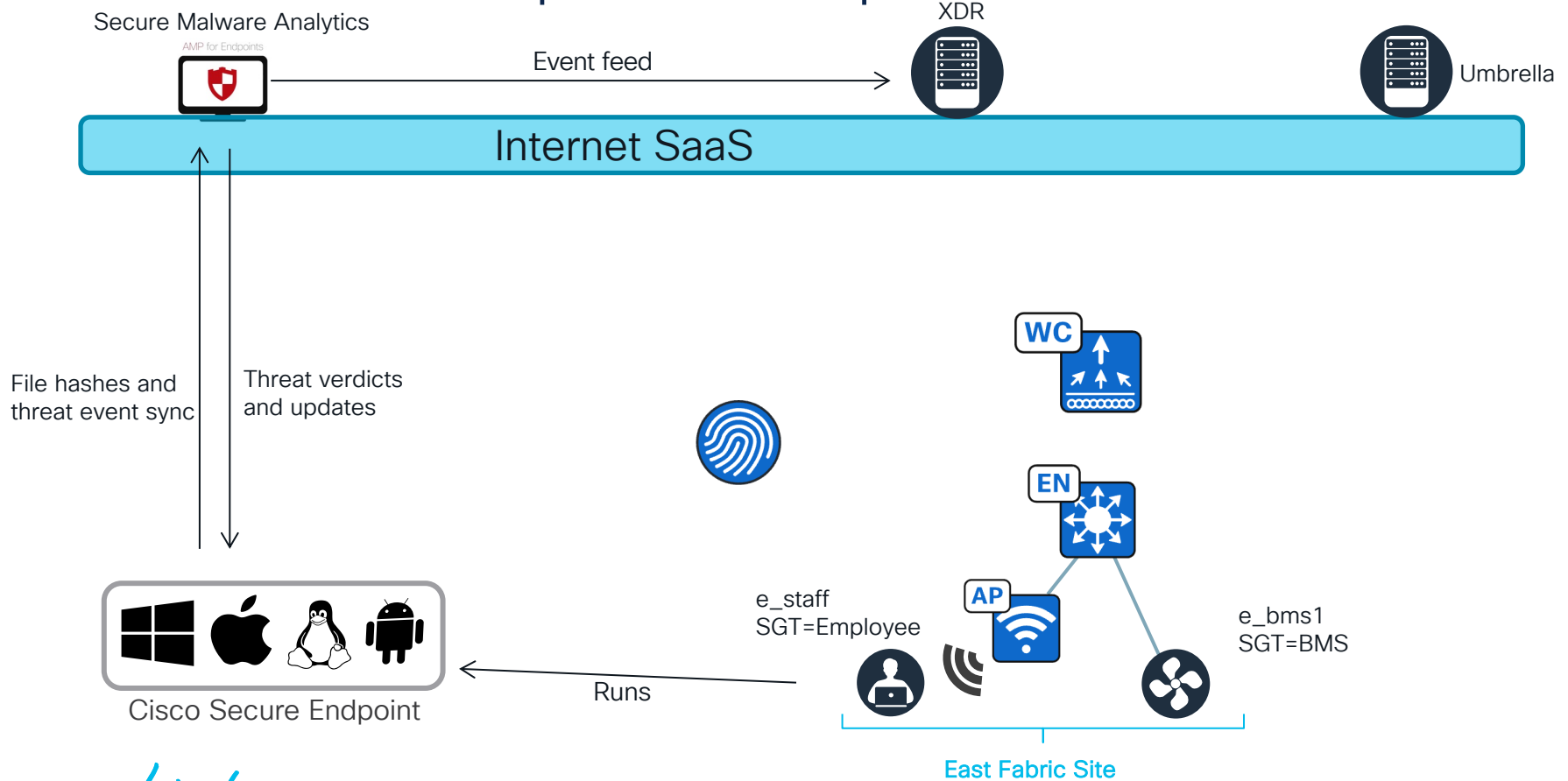
Internet SaaS



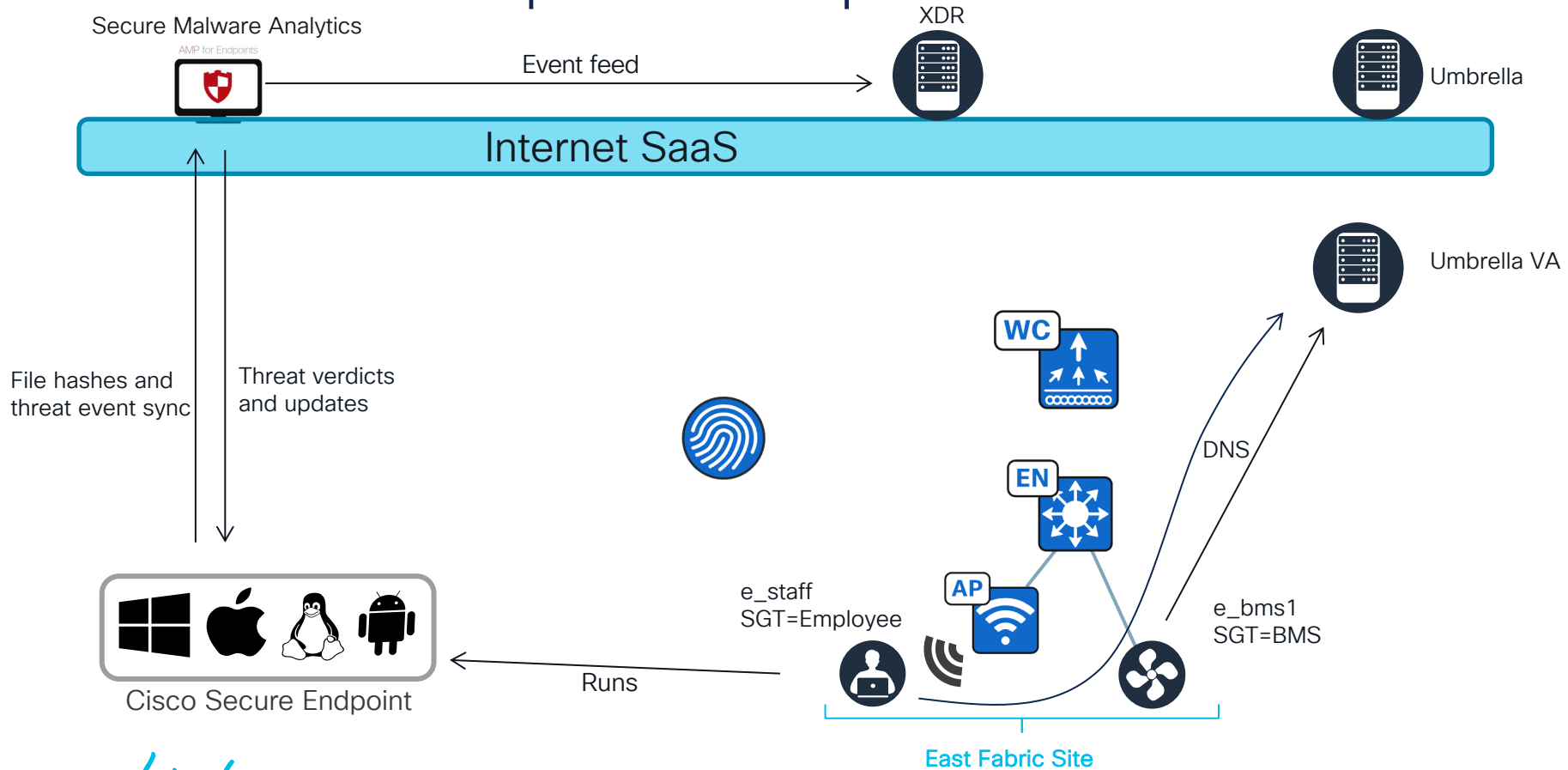
Demo: Secure Endpoint and Rapid Threat Containment



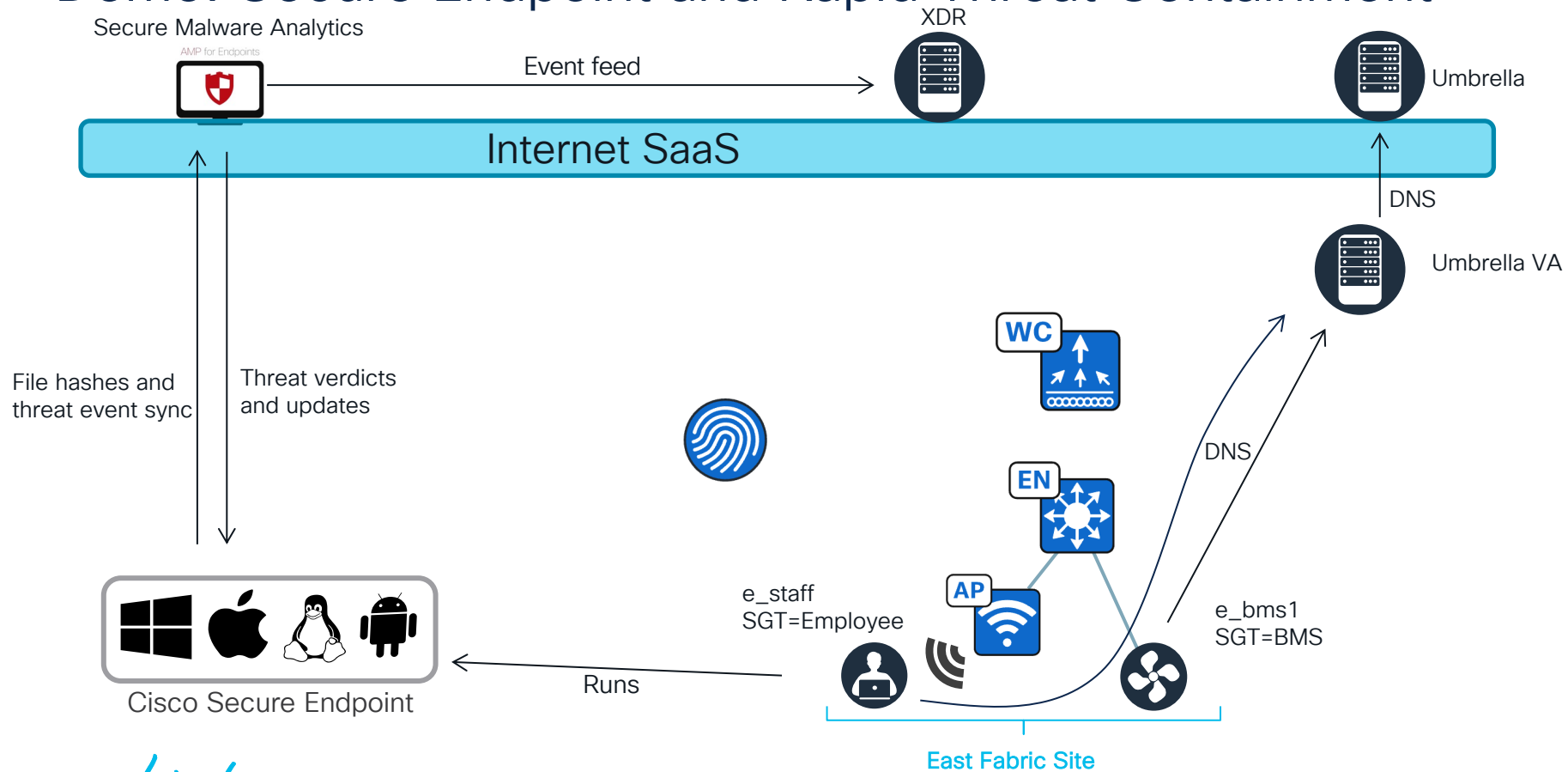
Demo: Secure Endpoint and Rapid Threat Containment



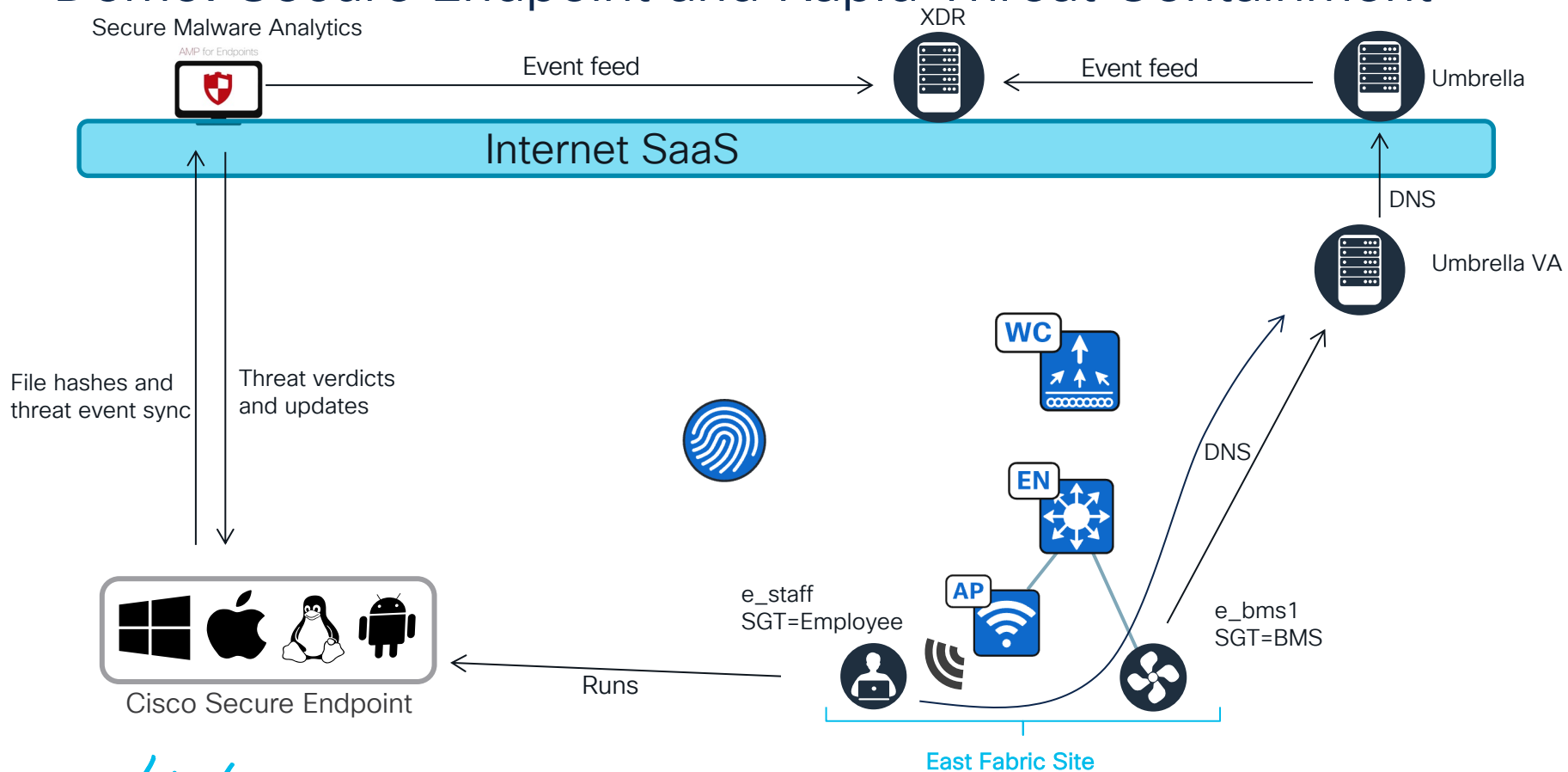
Demo: Secure Endpoint and Rapid Threat Containment



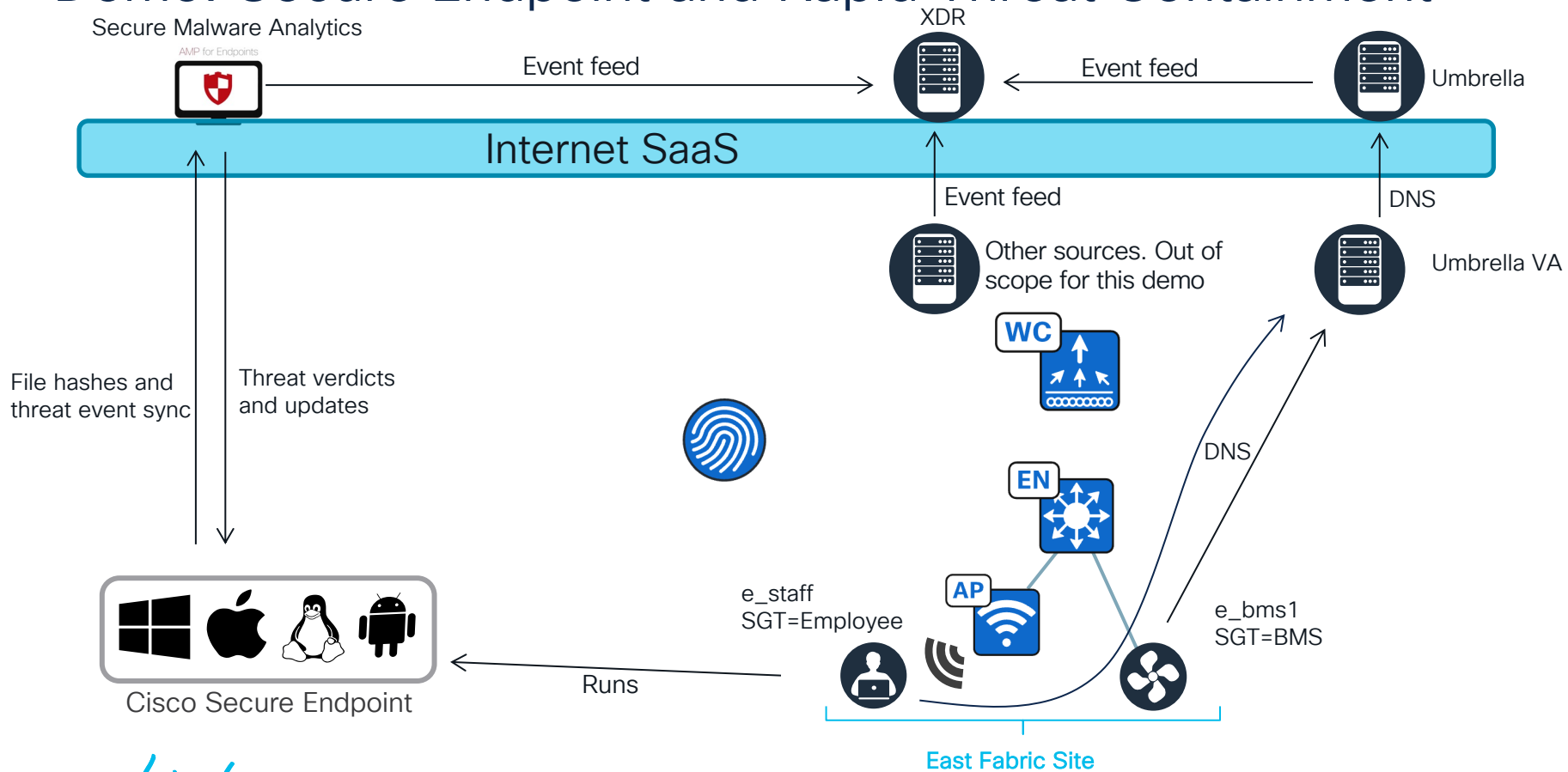
Demo: Secure Endpoint and Rapid Threat Containment



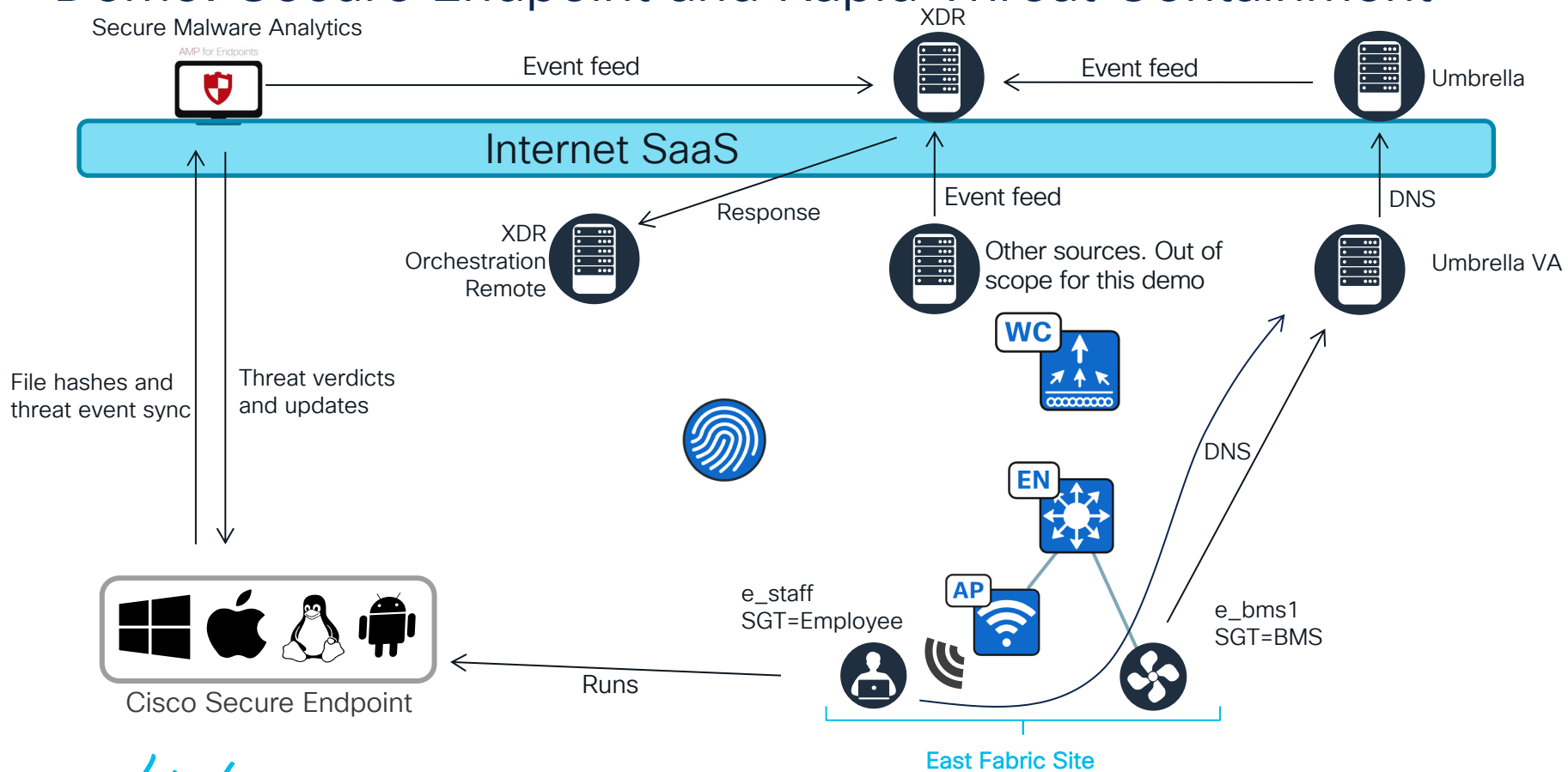
Demo: Secure Endpoint and Rapid Threat Containment



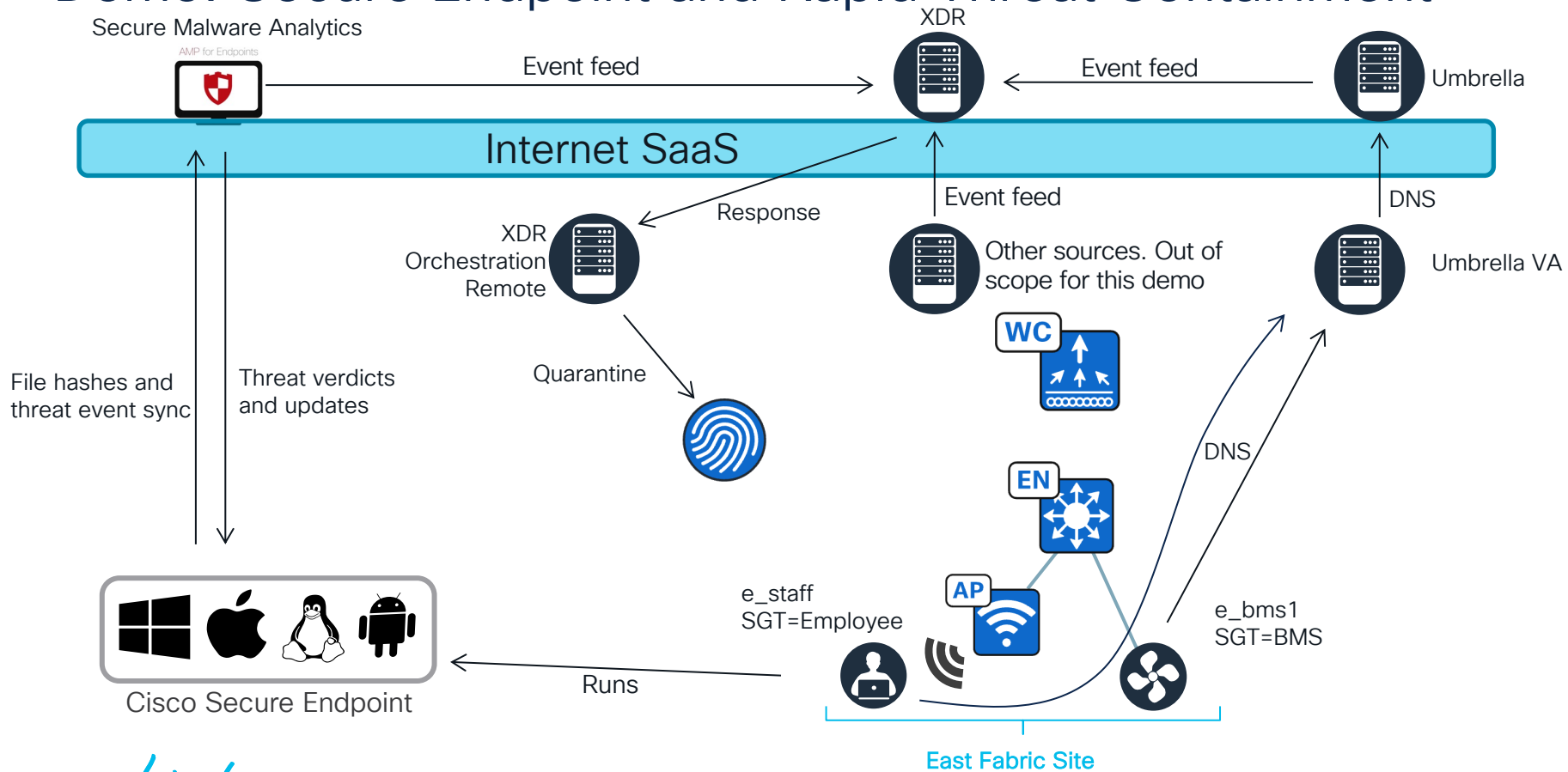
Demo: Secure Endpoint and Rapid Threat Containment



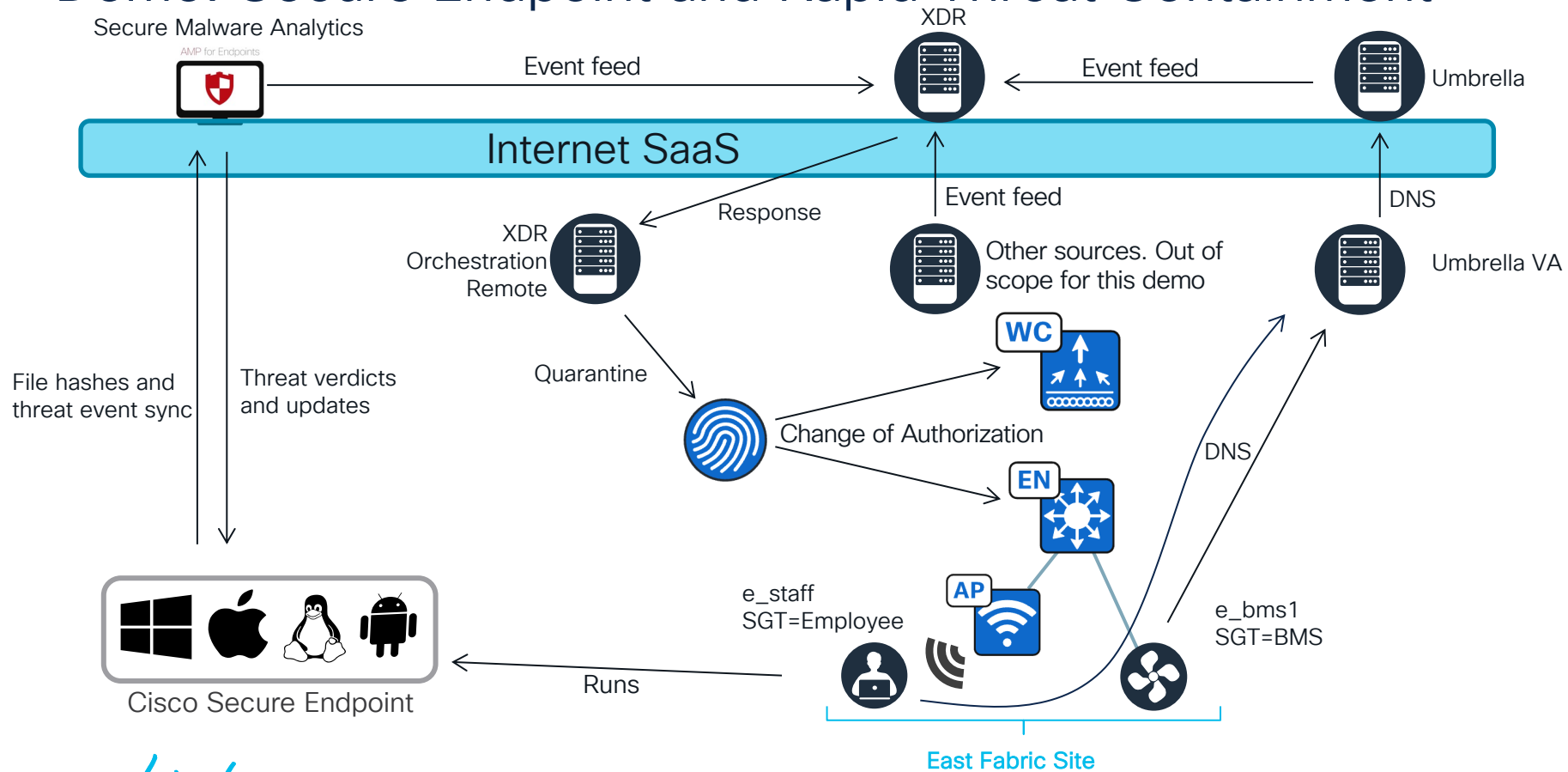
Demo: Secure Endpoint and Rapid Threat Containment



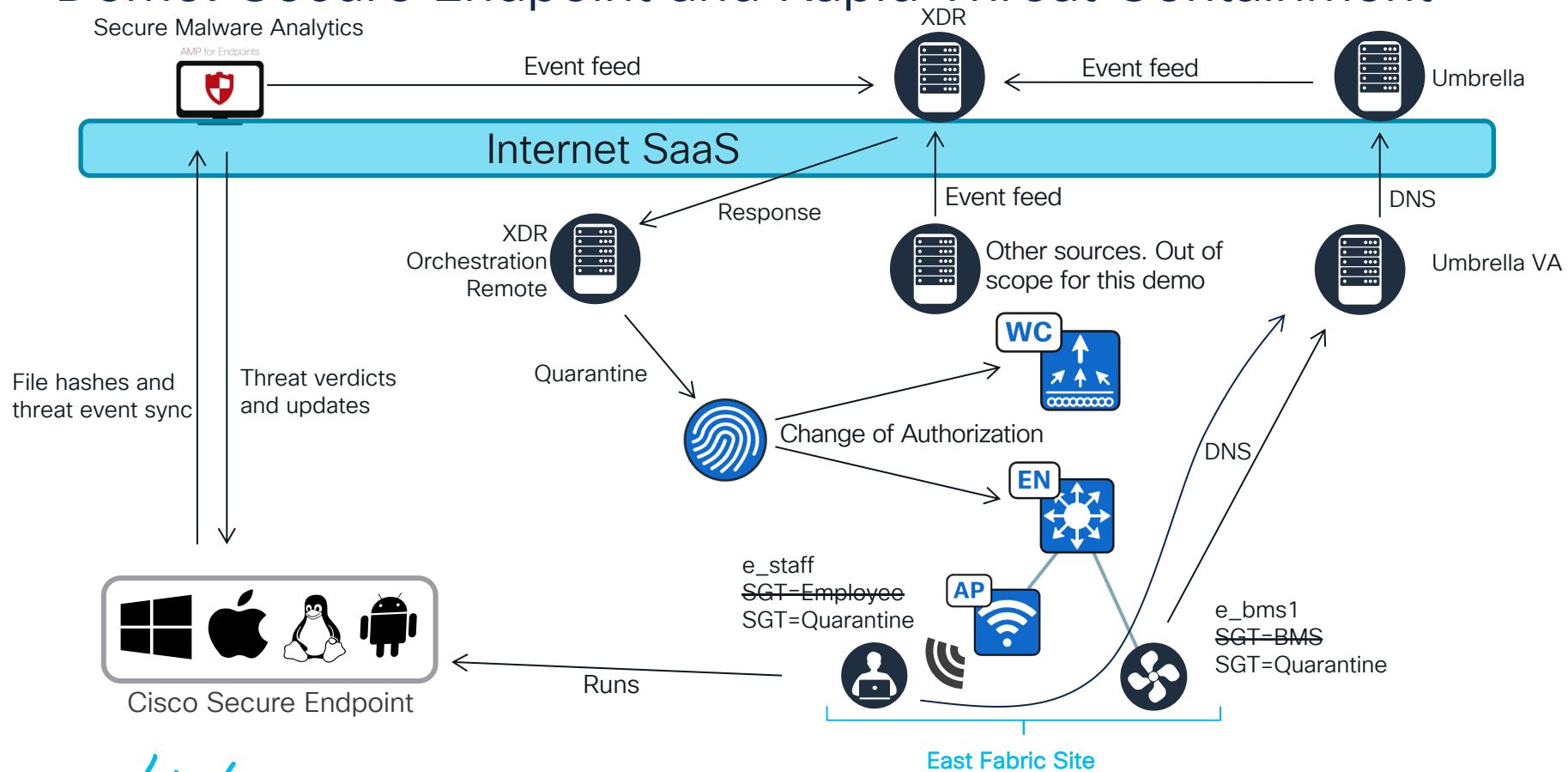
Demo: Secure Endpoint and Rapid Threat Containment



Demo: Secure Endpoint and Rapid Threat Containment



Demo: Secure Endpoint and Rapid Threat Containment

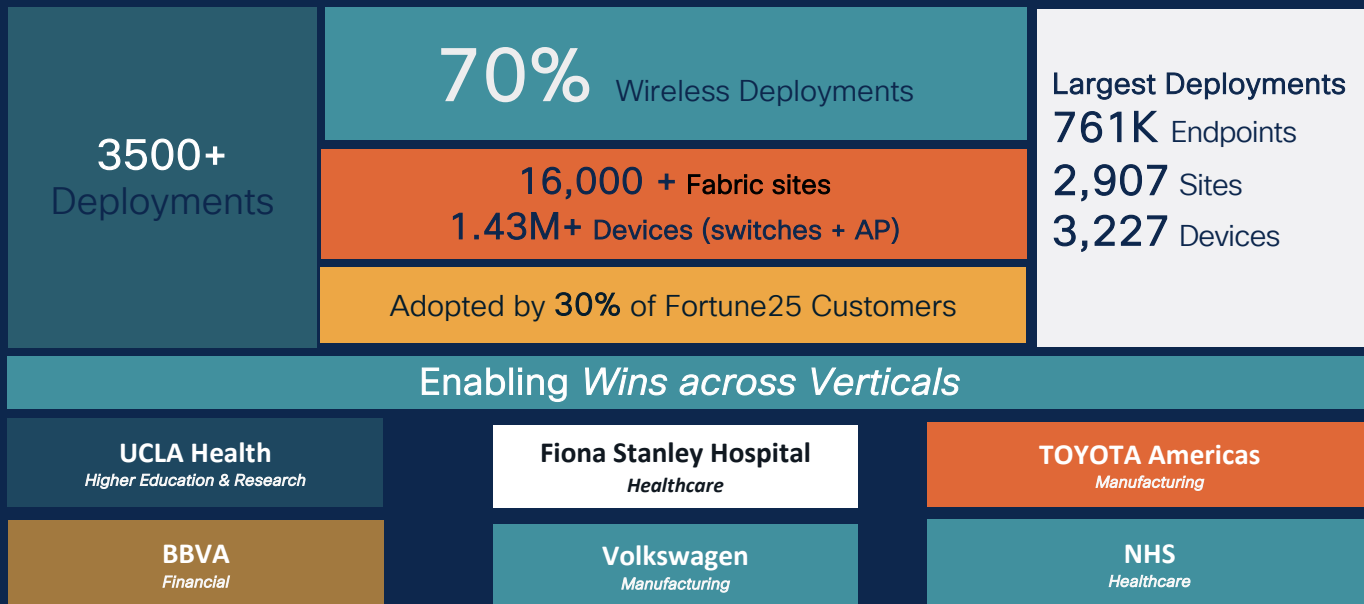


Demo

Conclusion

SD-Access LISP VXLAN Fabric

Industry Leading Campus Architecture



Modern, Open and Scalable Fabrics

IETF Standard based Protocols

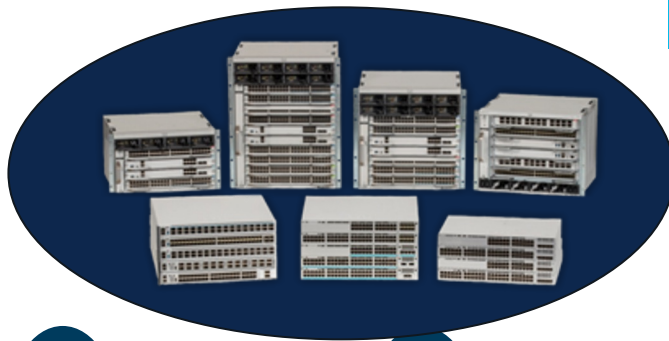
Cisco Catalyst Center

Cisco SD-Access

LISP VXLAN Fabric*

Cisco Catalyst 9000

BGP EVPN VXLAN Fabric



Enterprise



Healthcare



Education



Financial



Public Sector



Manufacturing



Hospitality



Media



Transportation



Retail

CISCO *Live!*

*Cisco's Lead Motion

#CiscoLiveAPJC

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Flexible Fabric Options Tailored to *Customer Outcomes*!

SD-Access with LISP Control Plane VxLAN Data Plane

Network Simplification

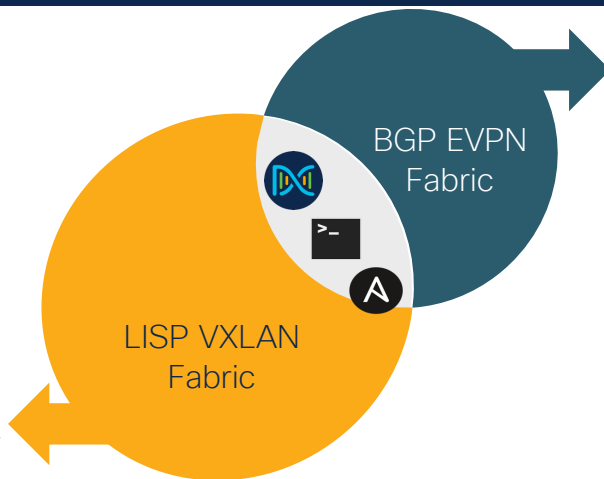
Lightweight, extensible, massive scale with rapid convergence. Single overlay for wired/wireless

Mobility First Requirement

Fabric Integrated Wireless, L2 Mobility, Enhanced wireless performance

Segmentation

Zero-Trust Architecture with Unified Wired + Wireless Policy



SD-Access with BGP EVPN Control Plane VxLAN Data Plane

One Fabric Architecture (Campus & DC)

Operational ease with a single familiar protocol

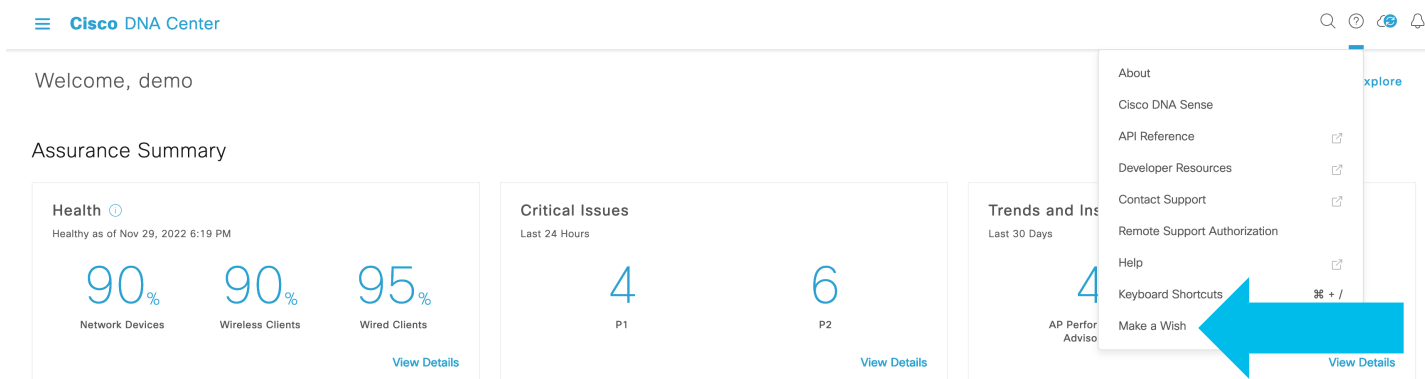
Multi-vendor interoperability

Vendor-agnostic solution with unique Cisco differentiators

One Infrastructure | Single Data plane | Consistent Zero-Trust Experience

Conclusion

- We value your Cisco SD-Access feedback. Please keep it coming!
- If something is missing then in the Make a Wish UI, briefly describe the use case and business value.



- It couldn't be done without you.

Conclusion

- Discussed and demonstrated:
 - Transits and End to End Segmentation
 - LAN to DC Segmentation
 - Access Privileges with Endpoint Analytics
 - Extended Detection and Response
- We've just scratched the surface, there's many more permutations.
 - Talk to a partner, CX, SE and AM representative to explore all the options.



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase 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



The bridge to possible

Thank you



#CiscoLiveAPJC

