Creating a multi-domain architecture using Cisco SD-Access, ISE, ETA, Firepower, ACI and AMP

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

Jeff Lee
Technical Solutions Architect
CCIE#25598 (R&S)

BRKCRS-2819

Virtual Event APJC • 1-2 April 2020

Agenda

- Introduction
- Lab network design and policy
- Cisco SD-Access transits and end to end SGT
- Deploy Cisco SD-Access and ACI integration
- Deploy SGT aware Firepower NG firewall
- Deploy Encrypted Traffic Analytics and Rapid Threat Containment
- AMP for endpoints, TC-NAC and Rapid Threat Containment
- Conclusion

Introduction

You make networking **possible**

About this presentation

POC inspired. Common use cases

Why attend this presentation?

- Learn through doing: Configure, integrate and operate real Cisco software defined networking controllers / orchestrators:
  - Cisco SD-WAN (A glimpse this time, much more next time!)
  - Cisco SD-Access / ISE
  - ACI
  - Firepower NGFW
  - Stealthwatch / ETA
  - AMP cloud
- See the technologies working together
- Better understand end to end connectivity, segmentation and security context across LAN, WAN, DC and security domains

About this presentation

It is:

- End-to-end view of software defined automation, segmentation and complimentary technologies for LAN, WAN, security and data centre
- Demonstrating some in scope topics with screen recordings of real systems

It is not

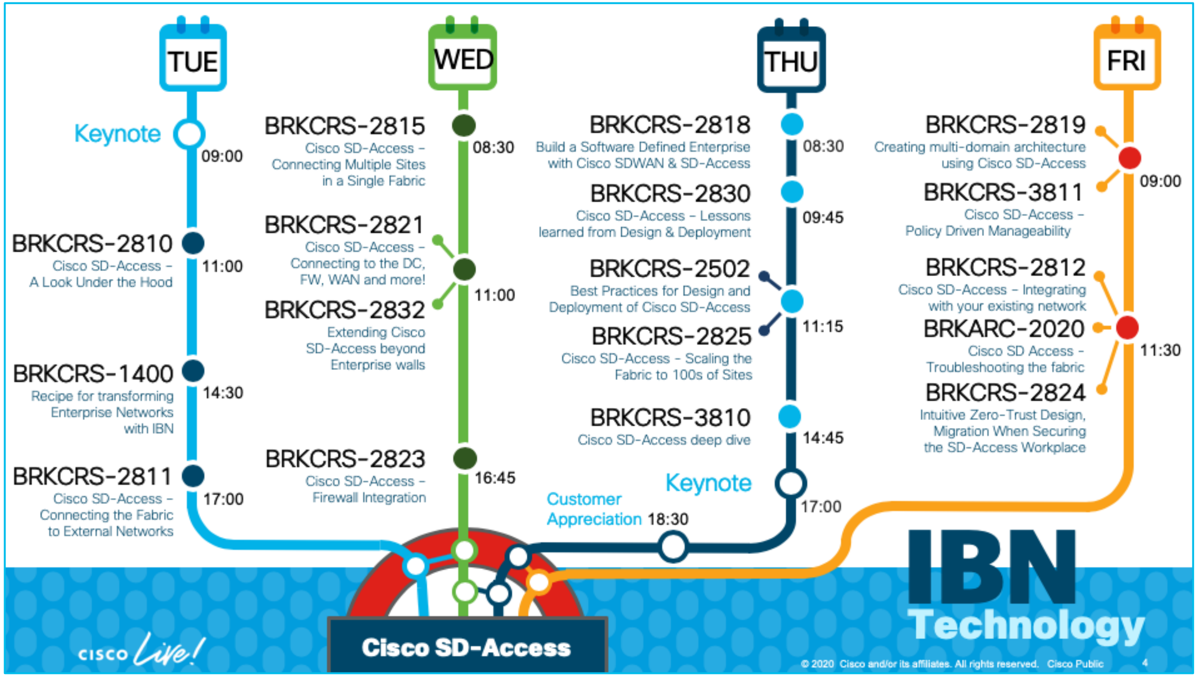
- Level one type of presentation on any topic
- Deep dive into any particular topic

To learn more:

- Regular pointers to other Cisco collateral

Learn more online

- Review all the IBN presentations from Cisco Live Barcelona (January 2020) at www.ciscolive.com



TUE

Keynote 09:00

BRKCRS-2810 11:00
Cisco SD-Access – A Look Under the Hood

BRKCRS-1400 14:30
Recipe for transforming Enterprise Networks with IBN

BRKCRS-2811 17:00
Cisco SD-Access – Connecting the Fabric to External Networks

WED

BRKCRS-2815 08:30
Cisco SD-Access – Connecting Multiple Sites in a Single Fabric

BRKCRS-2821 11:00
Cisco SD-Access – Connecting to the DC, FW, WAN and more!

BRKCRS-2832
Extending Cisco SD-Access beyond Enterprise walls

BRKCRS-2823 16:45
Cisco SD-Access – Firewall Integration

THU

BRKCRS-2818 08:30
Build a Software Defined Enterprise with Cisco SDWAN & SD-Access

BRKCRS-2830 09:45
Cisco SD-Access – Lessons learned from Design & Deployment

BRKCRS-2502 11:15
Best Practices for Design and Deployment of Cisco SD-Access

BRKCRS-2825
Cisco SD-Access – Scaling the Fabric to 100s of Sites

BRKCRS-3810 14:45
Cisco SD-Access deep dive

Keynote 17:00

Customer Appreciation 18:30

FRI

BRKCRS-2819 09:00
Creating multi-domain architecture using Cisco SD-Access

BRKCRS-3811
Cisco SD-Access – Policy Driven Manageability

BRKCRS-2812 11:30
Cisco SD-Access – Integrating with your existing network

BRKARC-2020
Cisco SD Access – Troubleshooting the fabric

BRKCRS-2824
Intuitive Zero-Trust Design, Migration When Securing the SD-Access Workplace

Cisco SD-Access

IBN Technology

cisco Live!

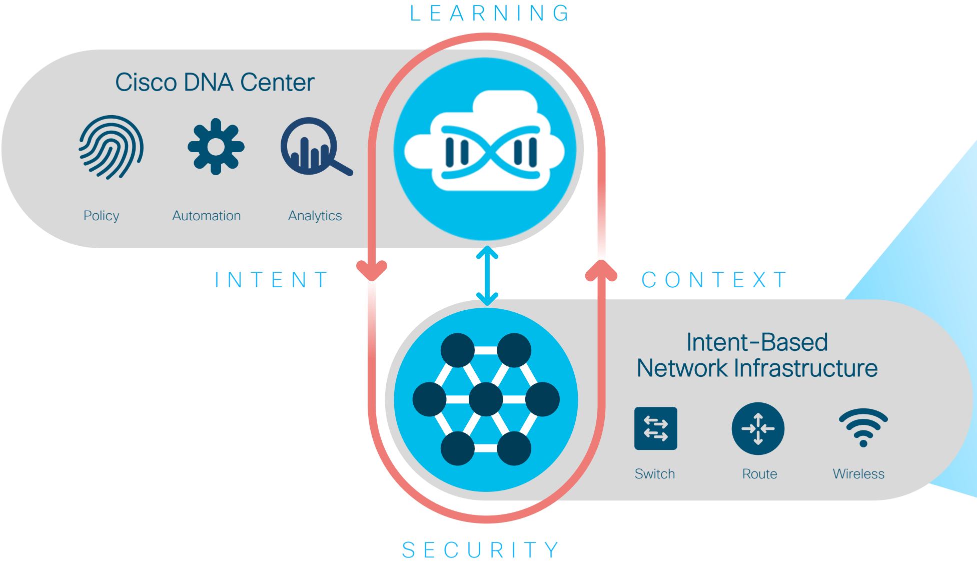
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public 4

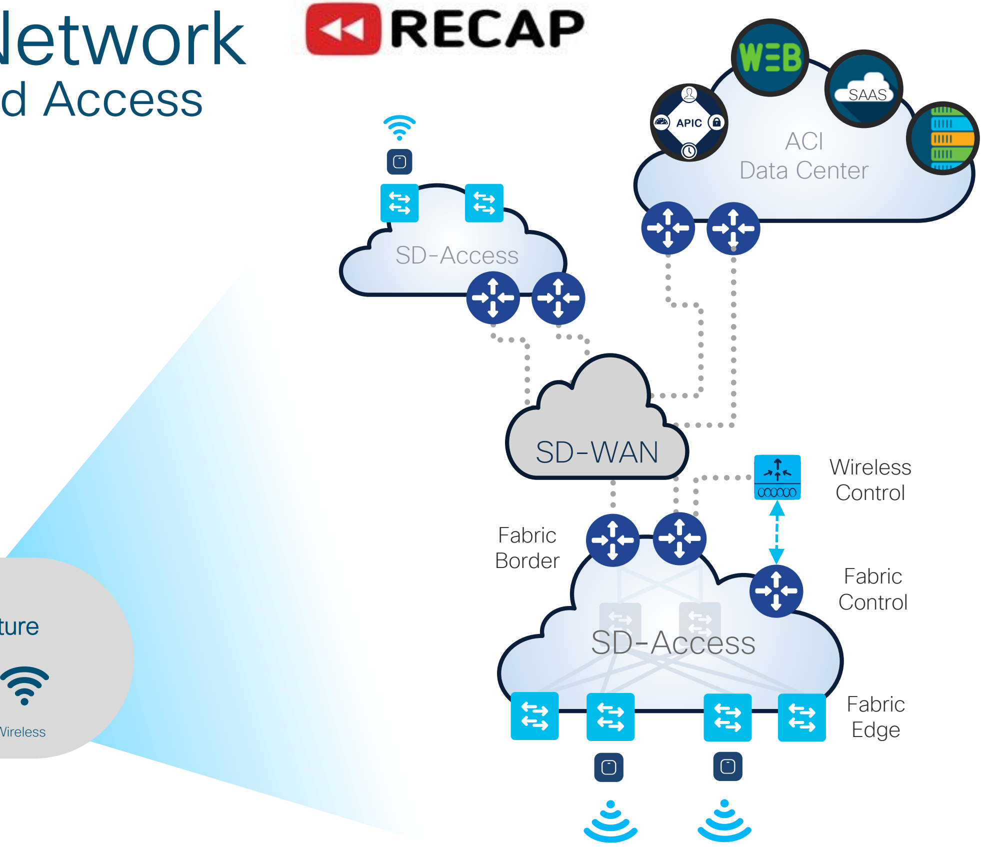
Lab network design and policy

You make security **possible**

Cisco's Intent-Based Network

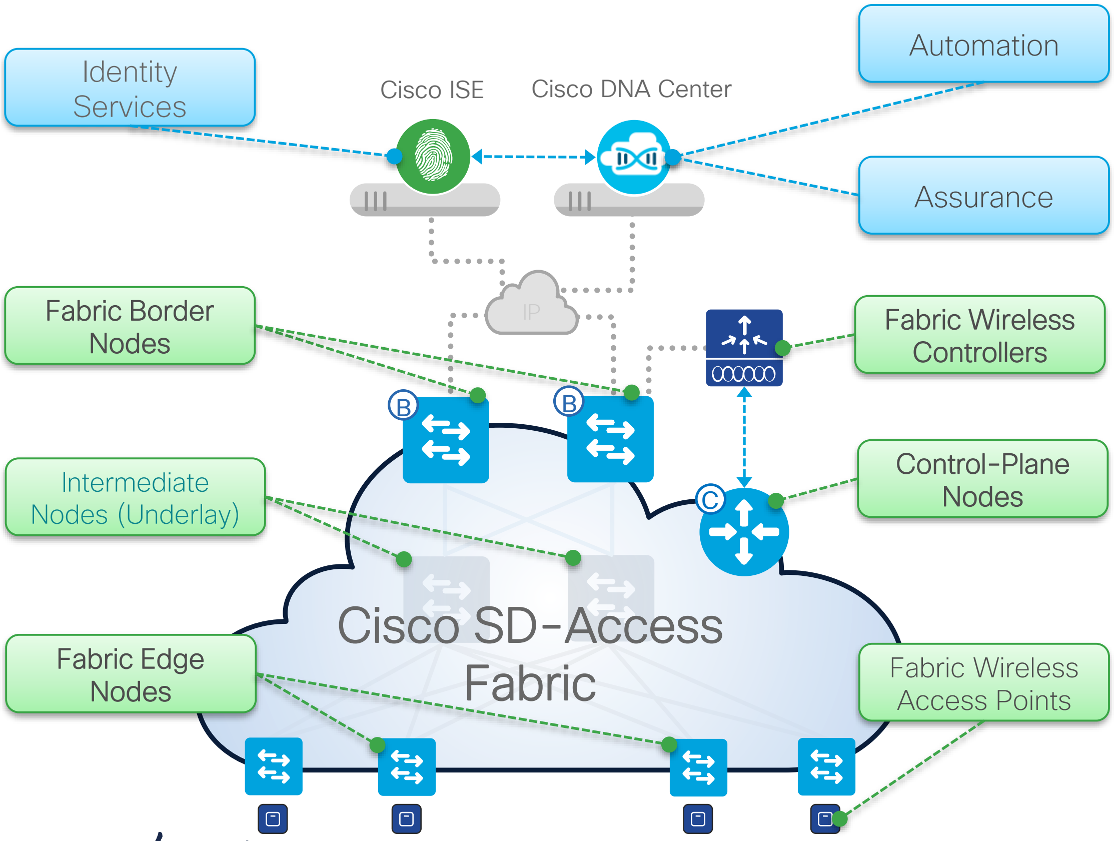
Delivered by Cisco Software Defined Access





Cisco SD-Access
Fabric Roles & Terminology

RECAP

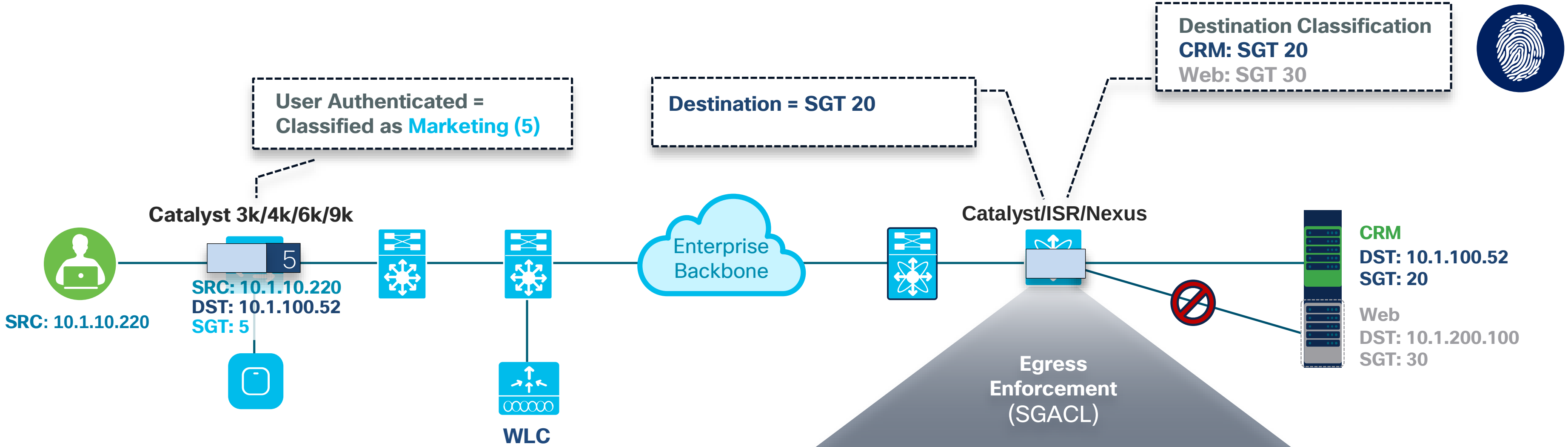


- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric network status
- **Identity Services** – NAC & ID Services (e.g. ISE) for dynamic Endpoint 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

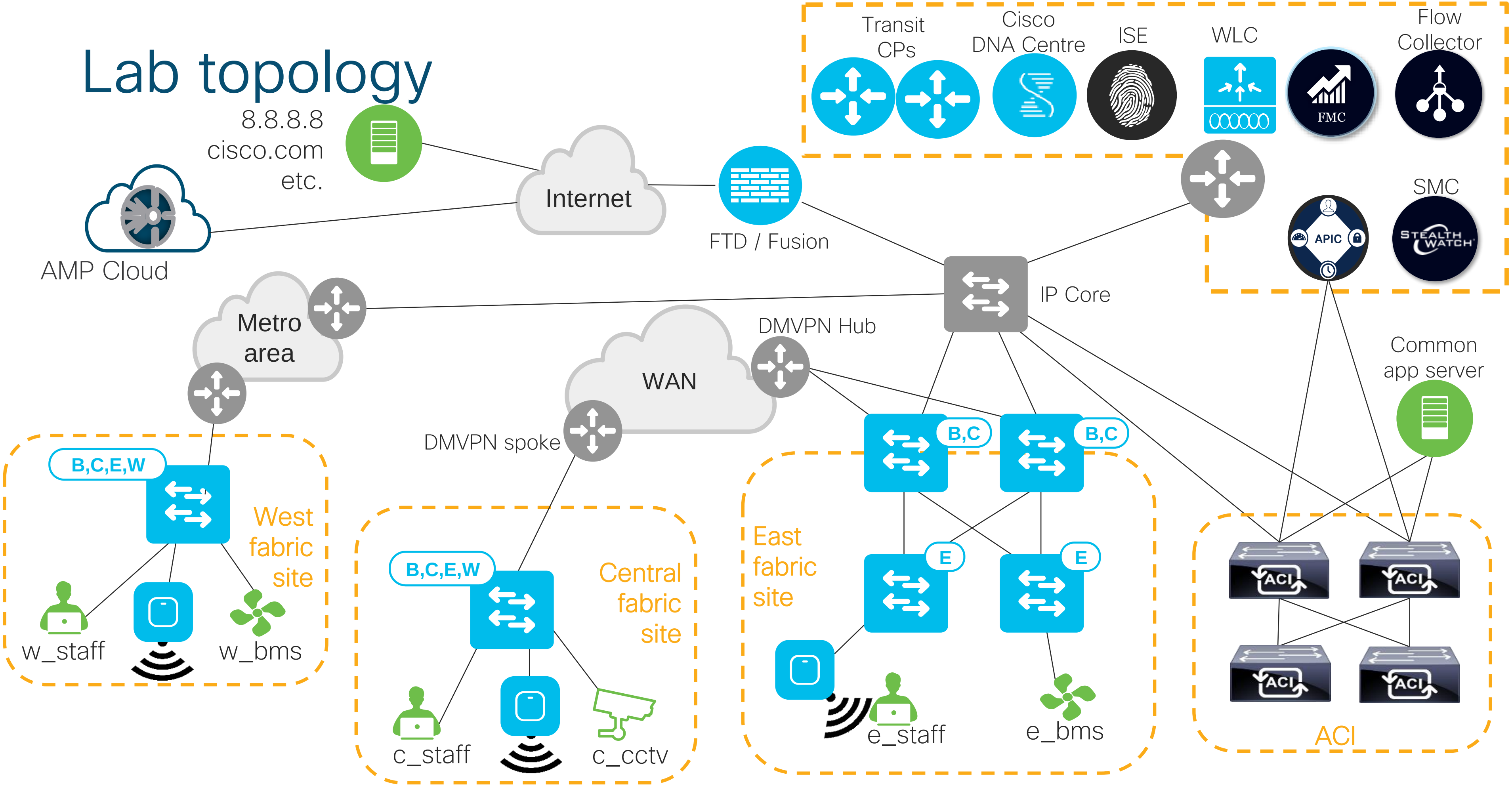
Scalable Group Tag (SGT)

RECAP



DST → ↓ SRC	CRM (20)	Web (30)
Marketing (5)	Permit	Deny
BYOD (7)	Deny	Permit

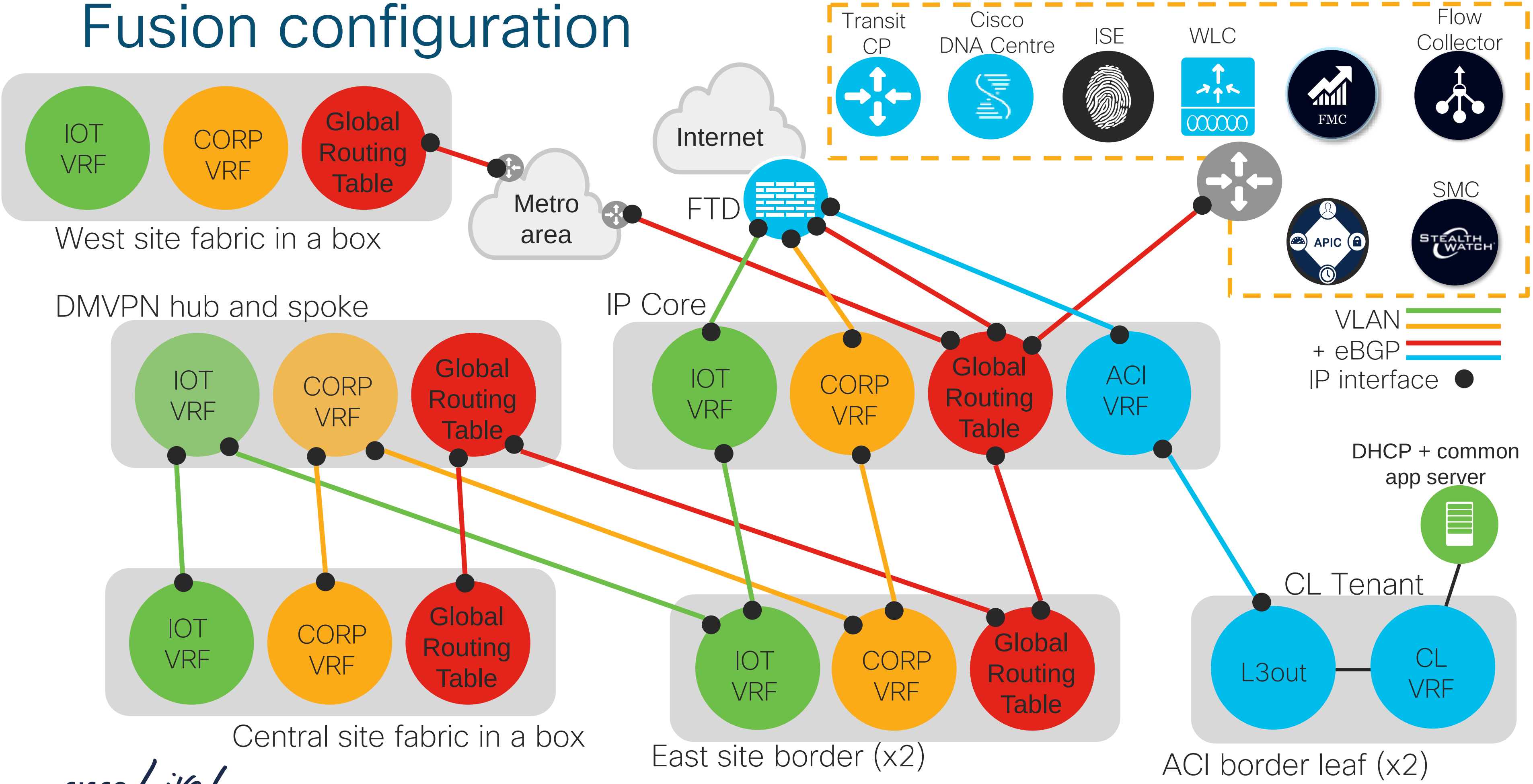
Lab topology



Pre-applied lab configuration

- FTD/Fusion IP interfaces, and eBGP
- Most Cisco SD-Access fabric site configurations
  - BRKEWN-2021 demonstrates how to:
    - Install Cisco DNA Centre, bring up wired and wireless fabric
    - Watch later on ciscolive.com
  - Basic ACI configuration including Tenant, BD, EPG and L3out
  - Basic configuration on everything else in top right box (Stealthwatch, ISE, Firepower)
  - DMVPN hub and spoke in GRT

Fusion configuration



Lab endpoints

Hostname / Username	Description	Virtual Network	SGT / EPG	IP Address
w_staff	West site staff user	CORP	Employee	10.4.1.10
c_staff	Central site staff user	CORP	Employee	10.4.2.10
e_staff	East site staff user	CORP	Employee	10.4.3.10
w_bms	West site BMS device	IOT	BMS	10.3.1.10
c_cctv	East site CCTV device	IOT	CCTV	10.3.2.10
e_bms	East site BMS device	IOT	BMS	10.3.3.10
appServer	Common app server	ACI	SHARED_SVR	10.6.4.10

Segmentation policy

Cisco SD-Access TrustSec

Source SGT	Dest SGT	Action
CCTV	BMS	Deny
Quarantine	Quarantine Employee CCTV BMS	Deny

ACI policy

Source SGT	Dest EPG	Action
Employee BMS	SHARED_SVR	Permit

Firepower policy

Source SGT	Destination (IP/URL/SGT)	Action
BMS	Employee (SGT)	Deny
Employee	BMS (SGT)	Permit
Quarantine	8.8.8.8	Permit
Quarantine	Any	Deny

Cisco SD-Access transits and end to end SGT

You make the power of data **possible**

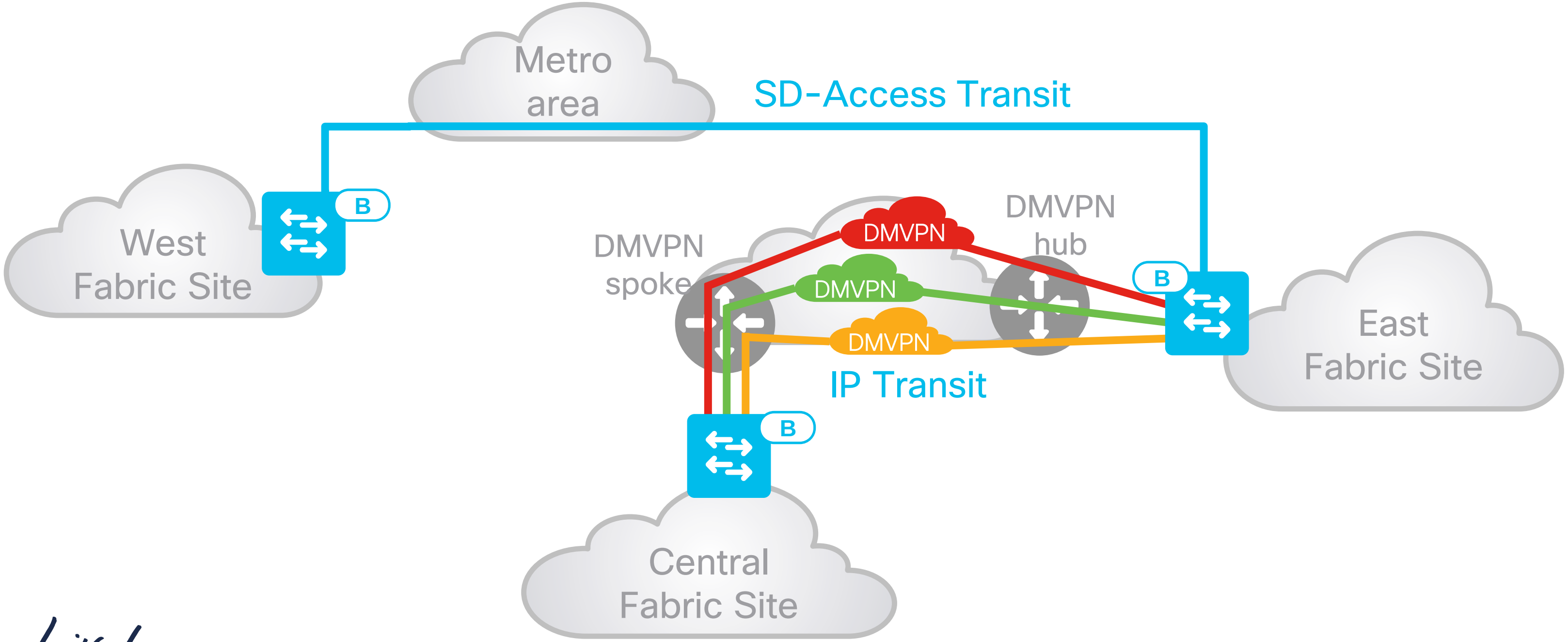
For more information

For your reference

- Watch later at ciscolive.com
  - BRKARC-1004 for an introduction to Cisco SD-WAN on IOS-XE routers
  - BRKCRS-2110 for an introduction to the principles and elements that comprise Cisco SD-WAN
  - BRKCRS-2810 introduces the fundamental concepts and components of Cisco SD-Access
  - BRKCRS-2815 is a deep dive into distributed campus and transits
  - BRKCRS-2821 is a deep dive into connecting Cisco SD-Access fabrics to the outside world
  - BRKCRS-2818 for Cisco SD-Access to SD-WAN integration
- https://community.cisco.com/t5/networking-documents/cisco-sd-access-for-distributed-campus-with-cisco-sd-access-as-a/ta-p/3837269
- https://community.cisco.com/t5/networking-documents/cisco-sd-access-for-distributed-campus-with-ip-as-a-transit/ta-p/3837284

Transits

- **Cisco SD-Access Transit** - Enables a native Cisco SD-Access (LISP,VXLAN,CTS) fabric, with a domain-wide Control Plane node for inter-site communication
- **IP Transit** - Leverages a traditional IP-based (VRF-LITE, MPLS) network, which may require remapping of VRFs and SGTs between sites



SGT preservation is crucial

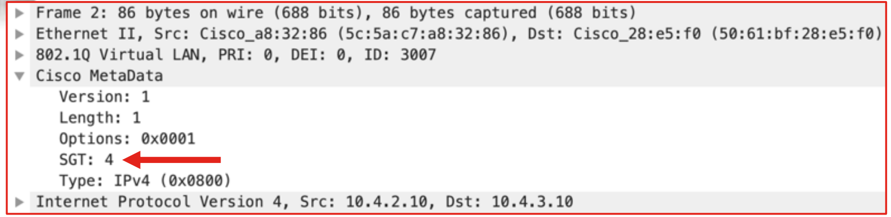
- Source SGT and destination SGT must be known at TrustSec policy enforcement point
- Source SGT can be carried numerous ways:
  - Several options for data plane SGT
  - In control plane via SXP (router, switch, ASA) or pxG (Firepower, Stealthwatch, WSA) or API (ACI)
- Data plane source SGT scales better
- SXP can be harder to design correctly in an SD-Access multisite network
  - Peer SXP per VRF per SD-Access border. SXP peering limits on ISE (max 200) = SXP reflectors
  - Memory limits on SD-Access border switches mean IP:SGT filtering might be required
    - Make sure filtering is right for desired policy outcomes, don’t filter too little or too much
  - Border ISR 4K / ASR 1K has higher IP:SGT scale than border switch

SGT preservation is crucial

- SGT in data plane

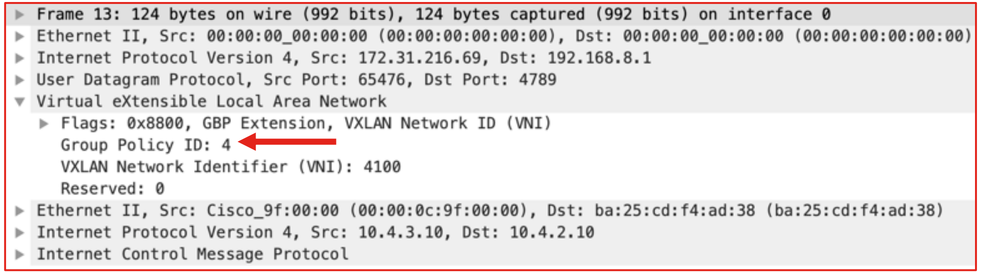
CMD in Ethernet

Note: dropped by non-SGT capable network infrastructure.
Review TrustSec capability matrix and bulletin
https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/solution-overview-listing.html



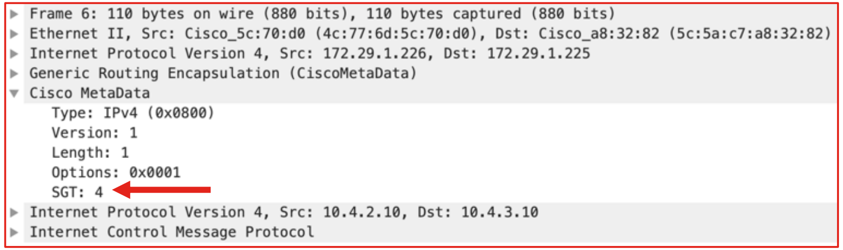
```
▶ Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
▶ Ethernet II, Src: Cisco_a8:32:86 (5c:5a:c7:a8:32:86), Dst: Cisco_28:e5:f0 (50:61:bf:28:e5:f0)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3007
▼ Cisco MetaData
    Version: 1
    Length: 1
    Options: 0x0001
    SGT: 4
    Type: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

VXLAN GPO



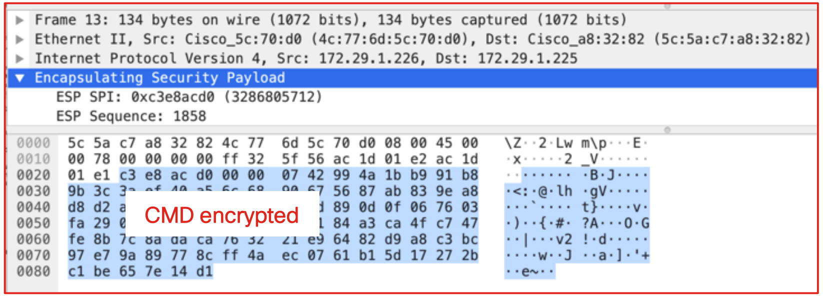
```
▶ Frame 13: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶ Internet Protocol Version 4, Src: 172.31.216.69, Dst: 192.168.8.1
▶ User Datagram Protocol, Src Port: 65476, 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)
▶ 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)
▶ 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 a5 6c 68  90 67 56 87 ab 83 9e a8   ·<:·@·lh ·gV·····
0040  d8 d2 a                    d 89 0d 0f 06 76 03   ···`···· t}····v·
0050  fa 29 0                    1 84 a3 ca 4f c7 47   ·)··{·#· ?A···O·G
0060  fe 8b 7c 8a da ca 76 32  21 e9 64 82 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~··
```

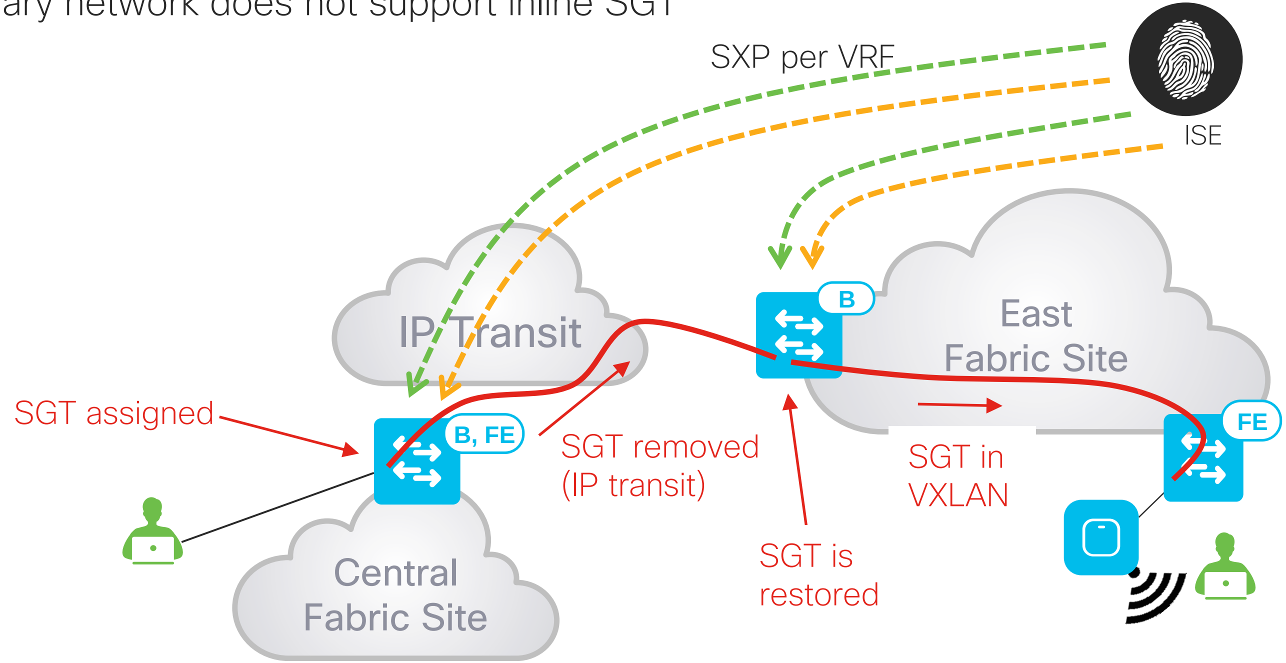
CMD encrypted

If we were doing SXP…

RECAP

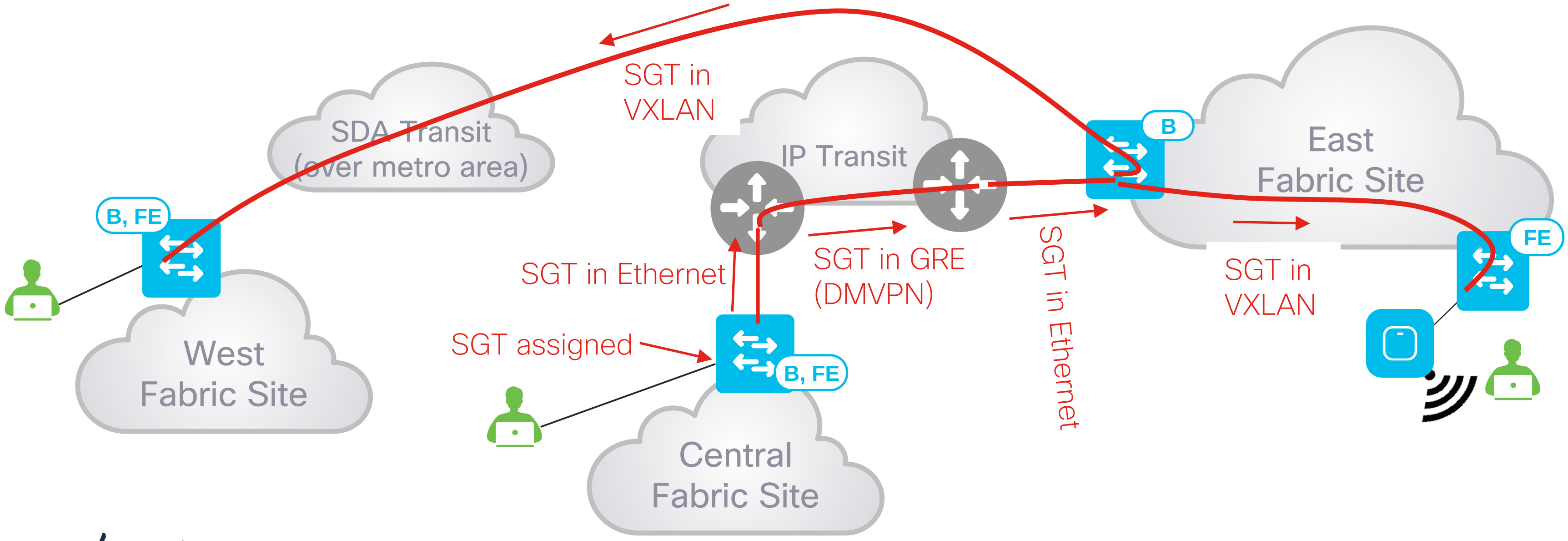
- See BRKCRS-2819 from San Diego 2019 at www.ciscolive.com
- SXP propagates IP:SGT bindings in control plane
- Used when intermediary network does not support inline SGT

IP	SGT
10.4.1.10	STAFF
10.3.1.10	BMS
10.4.2.10	STAFF
10.3.2.10	CCTV
10.4.3.10	STAFF
10.3.3.10	BMS



This time: Inline SGT

- SD-Access Transit between East and West
- IP Transit between East and Central with inline SGT
  - By default border will remove SGT on IP Transit. Can be overridden through configuration



Cisco SD-WAN roles and terminology

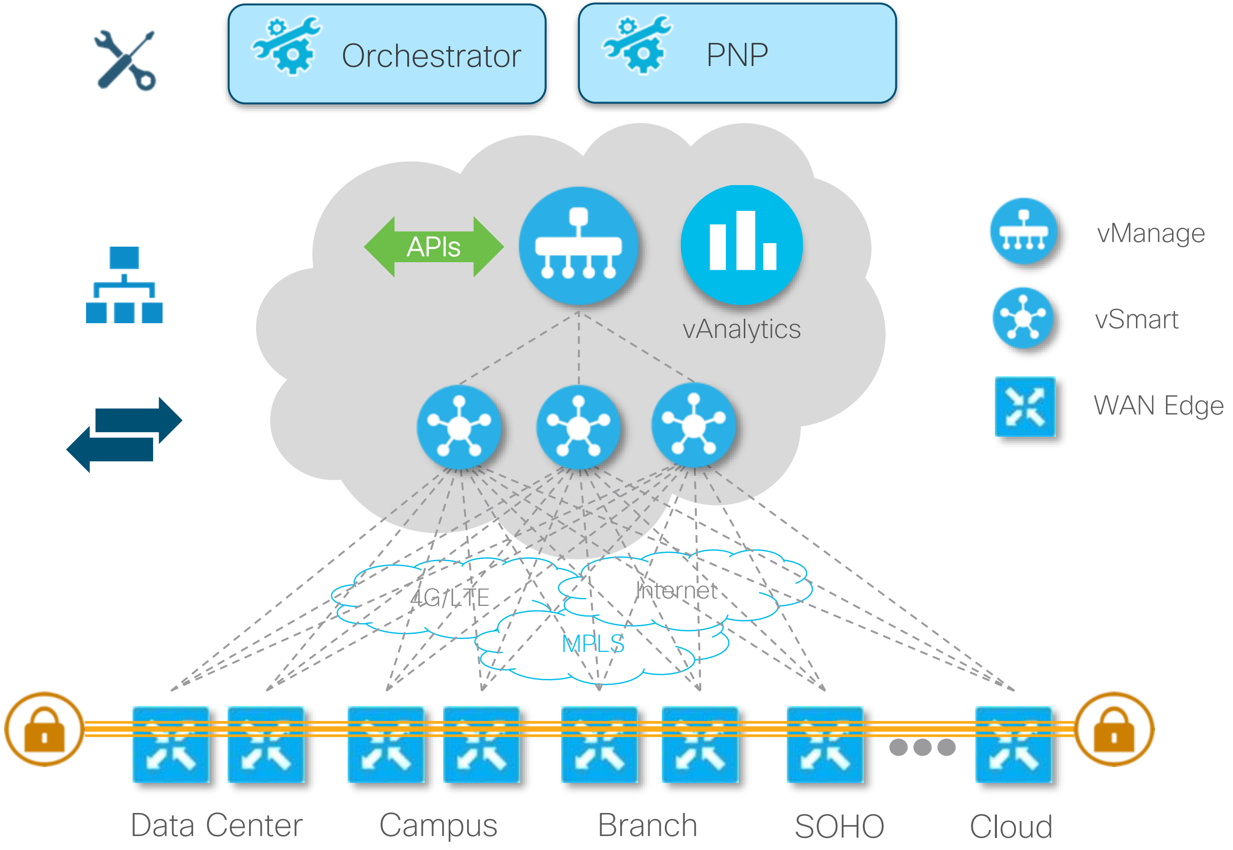
RECAP

Orchestration = vBond

Management = vManage
(Multi-tenant or Dedicated)

Control Plane = vSmart
(Containers or VMs)

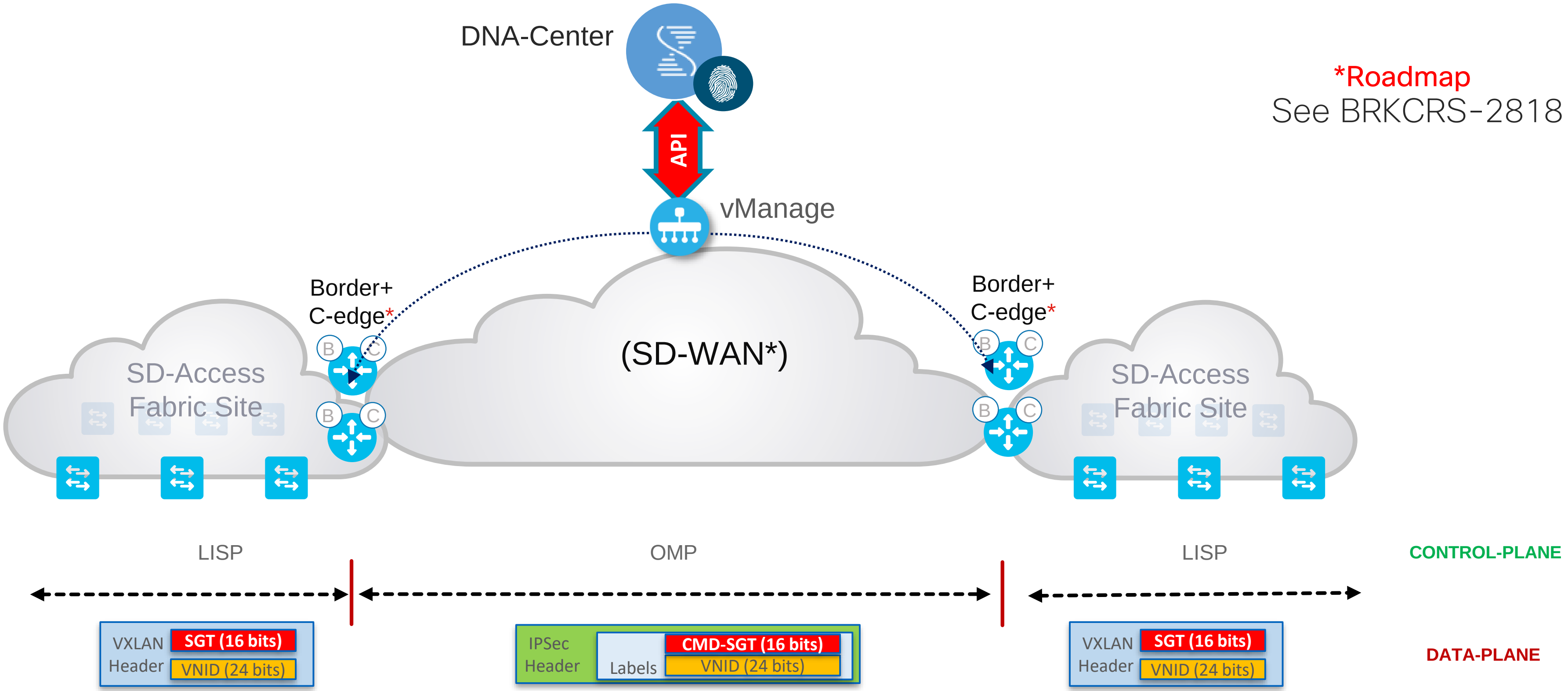
Data Plane = Edge
(vEdge, Cisco ISR/ASR/ENCS, Whitebox)



Cisco SD-WAN Transit

RECAP

*Roadmap
See BRKCRS-2818



Deploy Cisco SD-Access and ACI integration

You make multi-cloud **possible**

For more information

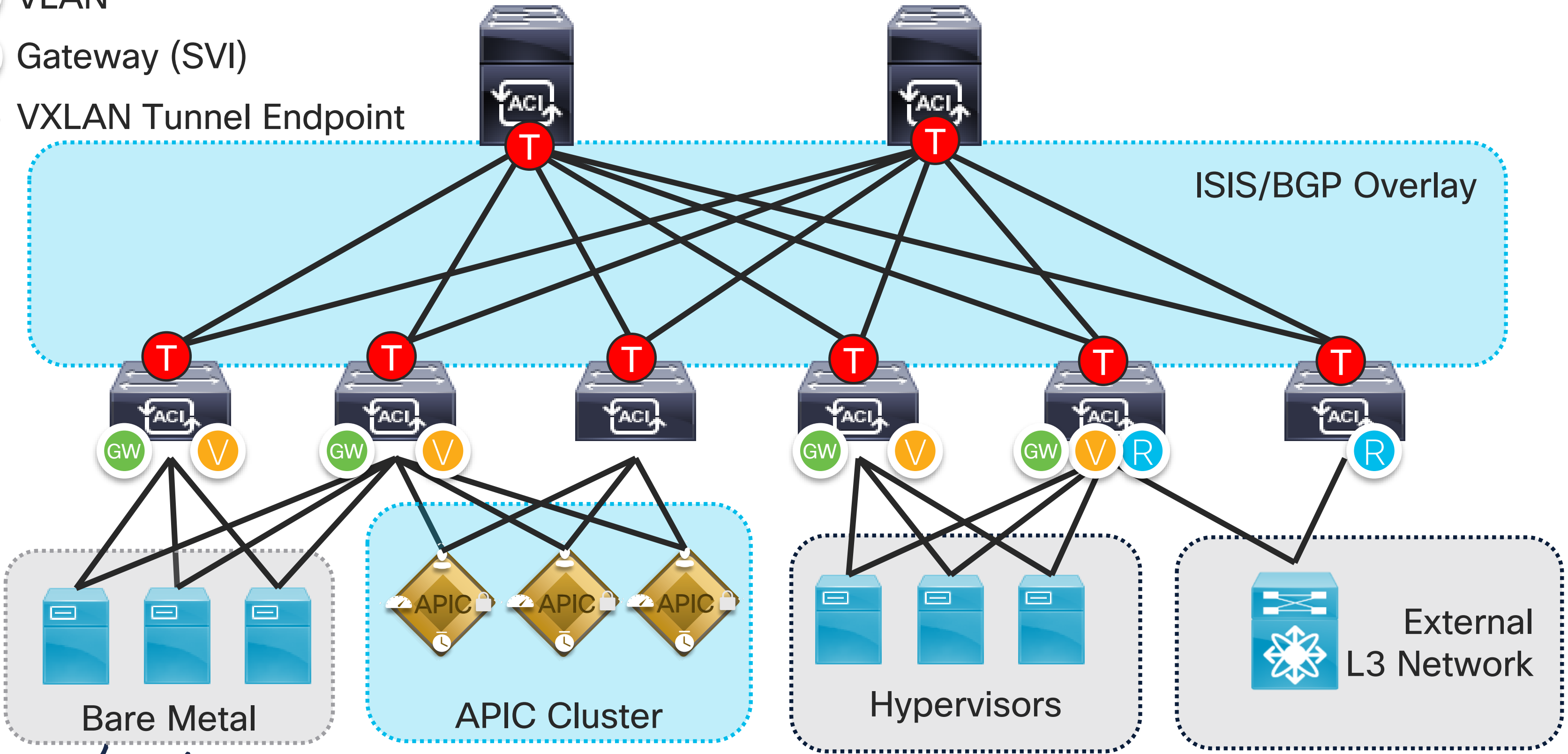
For your reference

- Watch later at ciscolive.com
    - BRKACI-1001 explores configuration options and best practices for people new to ACI
    - BRKACI-2004 builds an ACI fabric from nothing
    - BRKSEC-2048 looks at security options for ACI
    - BRKDCN-2489 looks at how SD-Access integrates with DC architectures, including ACI

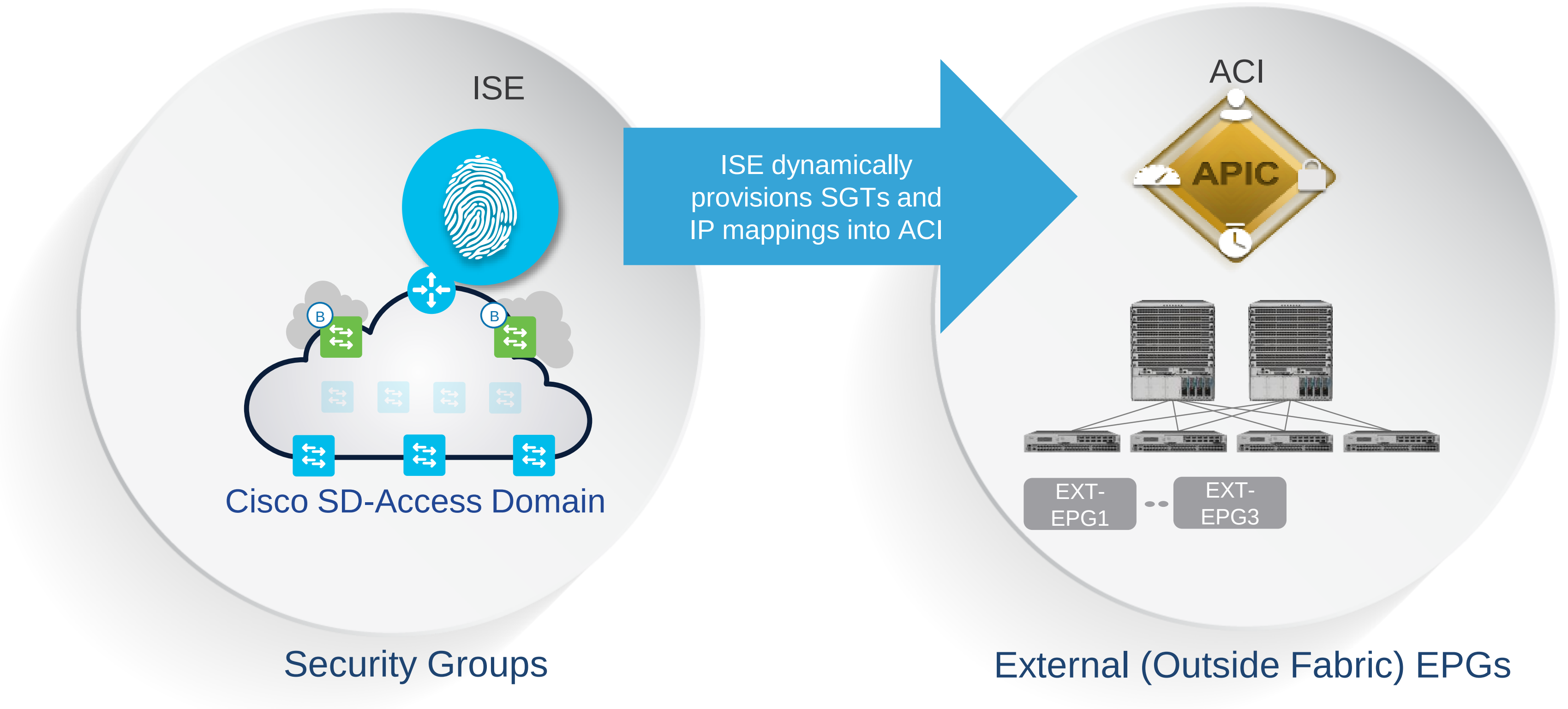
Cisco ACI roles and terminology

RECAP

- R External routing (L3out)
- V VLAN
- GW Gateway (SVI)
- T VXLAN Tunnel Endpoint



Cisco SD-Access SGTs provisioned in ACI



ISE

ISE dynamically provisions SGTs and IP mappings into ACI

ACI

Cisco SD-Access Domain

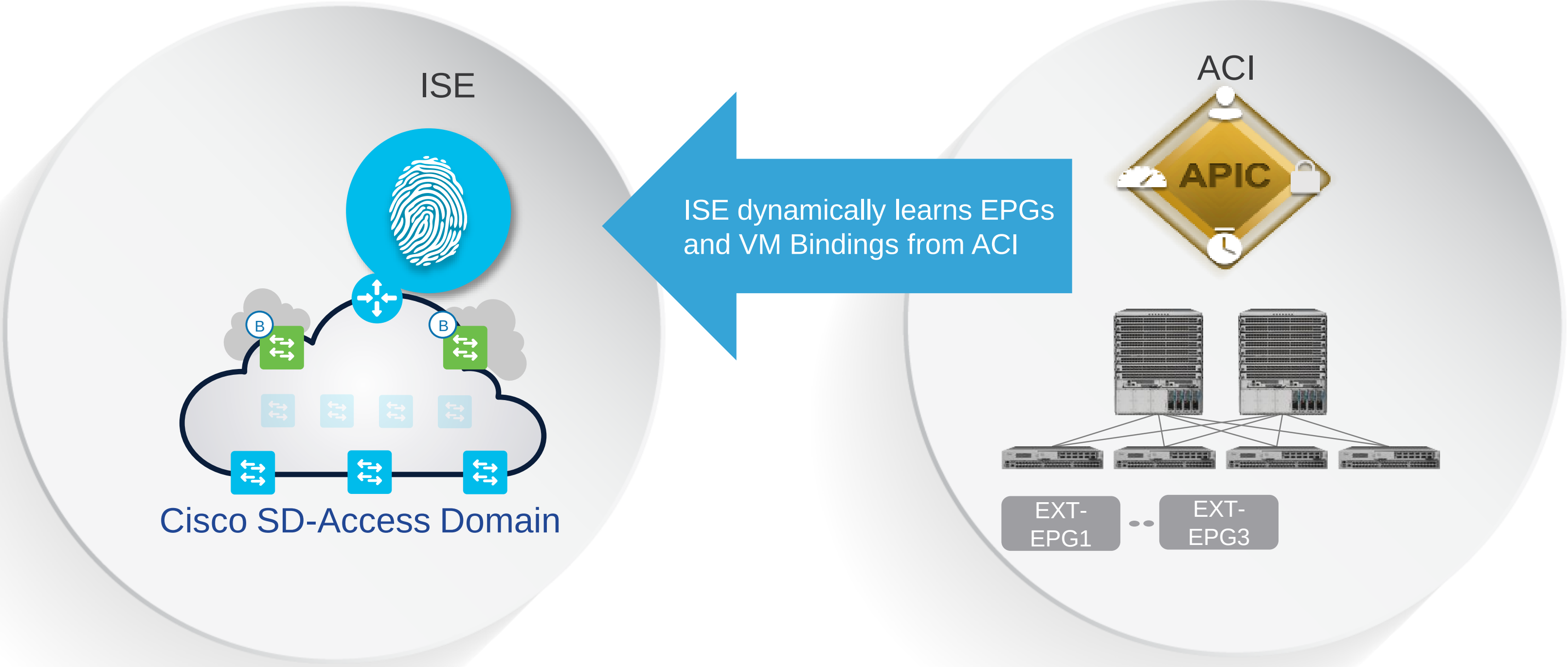
EXT-EPG1

EXT-EPG3

Security Groups

External (Outside Fabric) EPGs

ACI EPGs propagated into Cisco SD-Access



Cisco SD-Access Domain

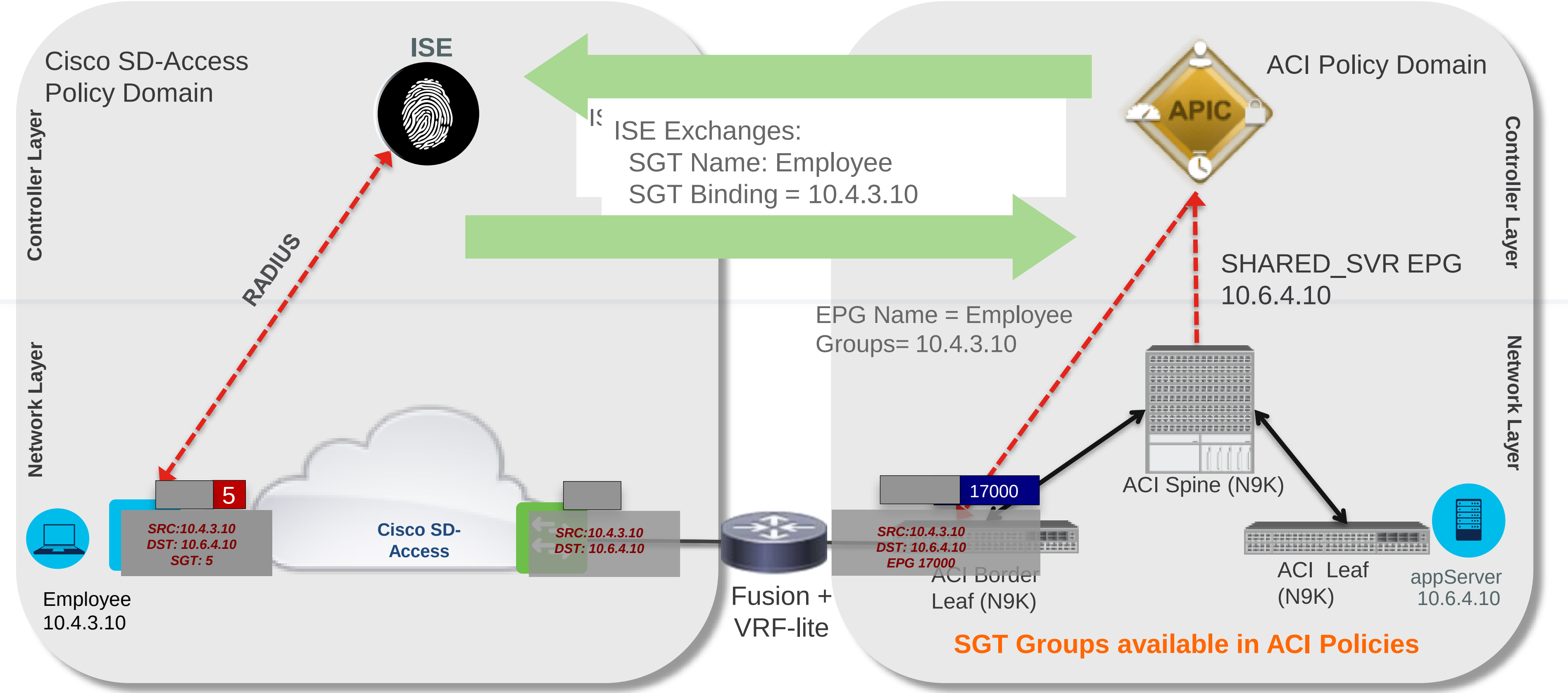
ISE dynamically learns EPGs and VM Bindings from ACI

EXT-EPG1

EXT-EPG3

Security Group from APIC-DC

Internal (Inside Fabric) EPGs



Cisco SD-Access Policy Domain

ISE

ACI Policy Domain

APIC

Controller Layer

Network Layer

RADIUS

IS

ISE Exchanges:
SGT Name: Employee
SGT Binding = 10.4.3.10

SHARED_SVR EPG
10.6.4.10

EPG Name = Employee
Groups= 10.4.3.10

5

SRC:10.4.3.10
DST: 10.6.4.10
SGT: 5

Cisco SD-Access

SRC:10.4.3.10
DST: 10.6.4.10

Employee
10.4.3.10

Fusion +
VRF-lite

17000

SRC:10.4.3.10
DST: 10.6.4.10
EPG 17000

ACI Border
Leaf (N9K)

ACI Spine (N9K)

ACI Leaf
(N9K)

appServer
10.6.4.10

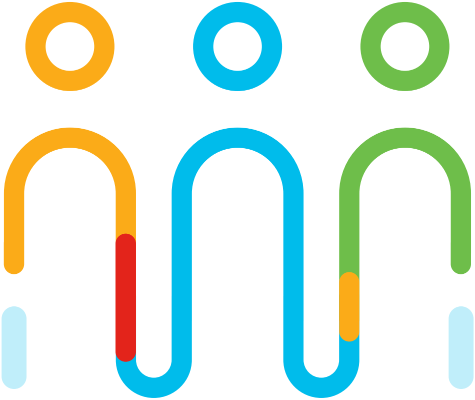
SGT Groups available in ACI Policies

Demo: SD-Access and ACI integration

- Integrate ISE to APIC
- Configure policy on APIC to:
  - Allow Employee SGT and BMS SGT to access SHARED_SERVER EPG
- Test and confirm

Demo

Deploy SGT aware Firepower NG firewall



You make customer experience **possible**

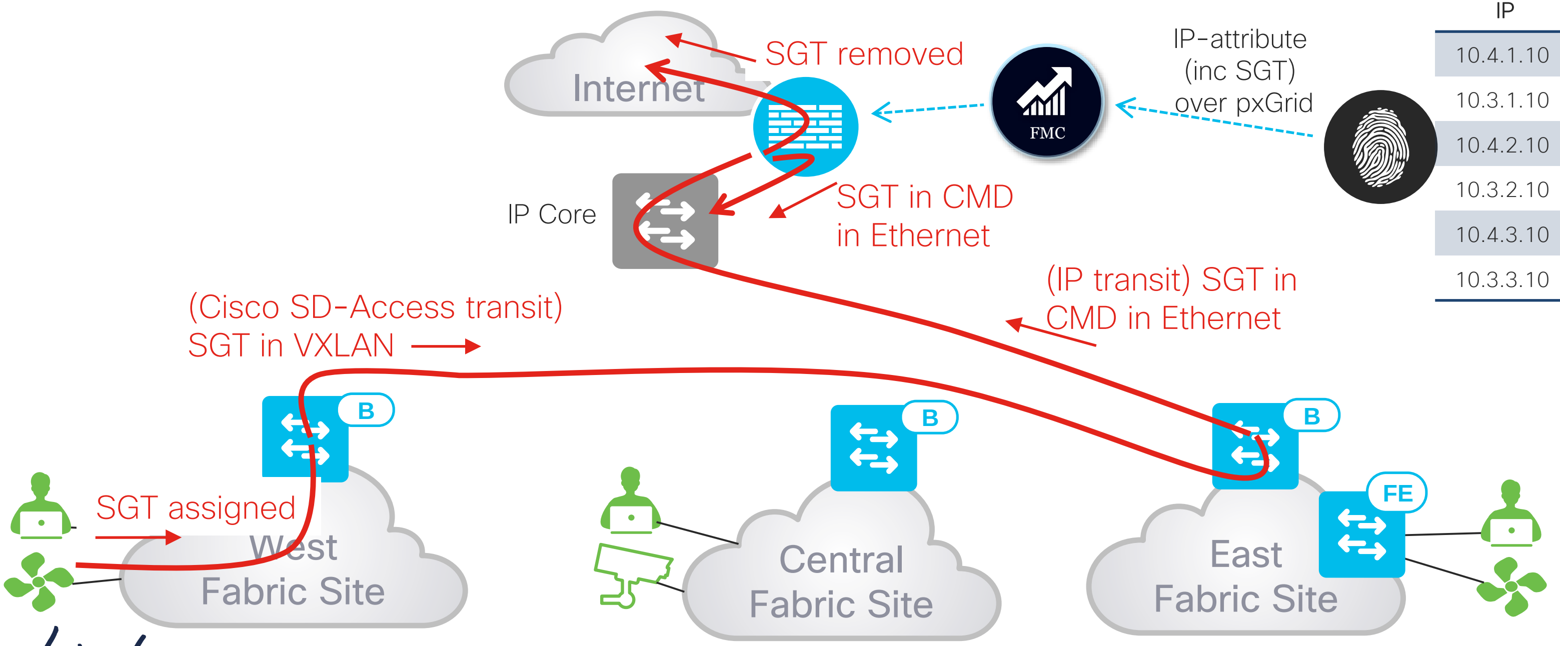
For more information

For your reference

- Watch later at ciscolive.com
  - BRKRST-2100 End to end group (SGT) based segmentation, including Firepower NGFW and pxGrid
  - BRKSEC-3690 TrustSec deep dive
- Integrate Firepower 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/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html

SGT preservation and matching

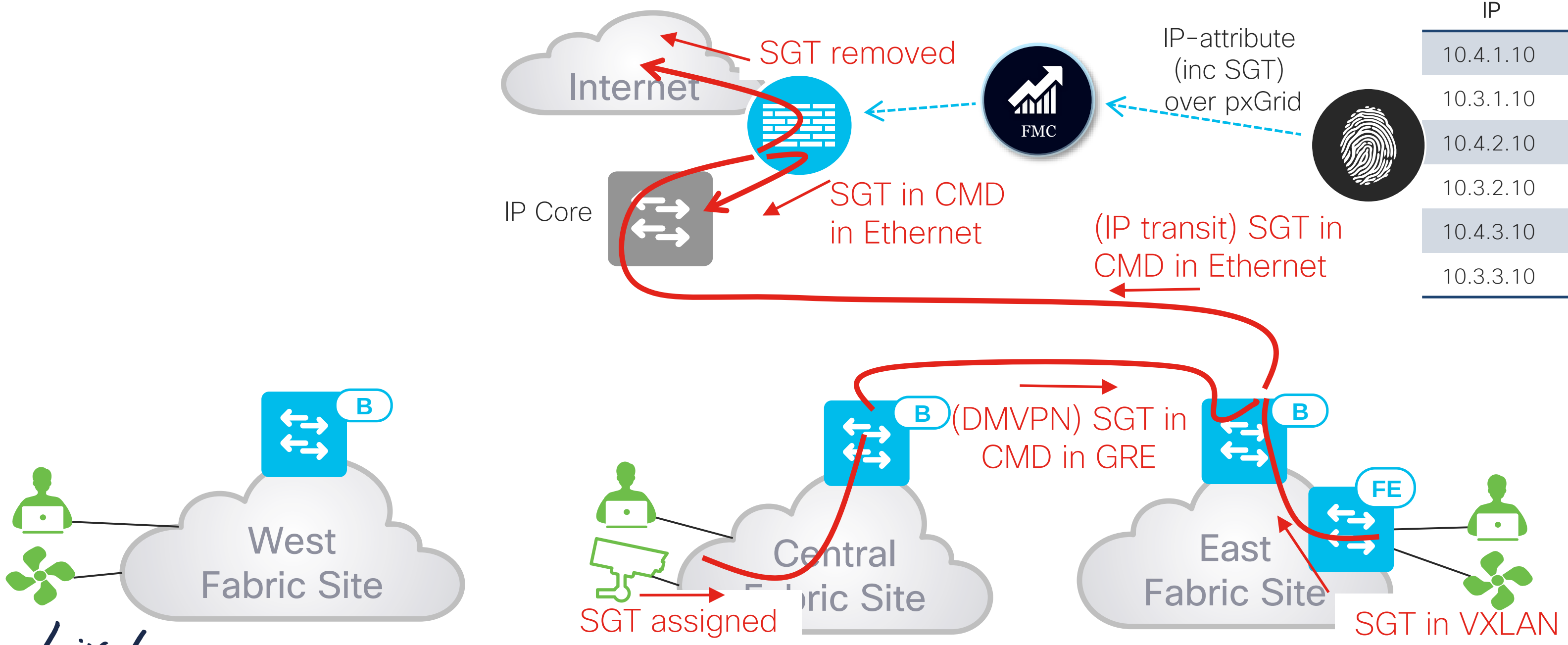
- West to Internet or inter-VN
  - ISE is aware of IP:SGT
  - Firepower downloads IP-attributes over pxGrid
  - East site border configured to propagate SGT towards FTD via manual override of default SDA behavior



IP	SGT
10.4.1.10	STAFF
10.3.1.10	BMS
10.4.2.10	STAFF
10.3.2.10	CCTV
10.4.3.10	STAFF
10.3.3.10	BMS

SGT preservation and matching

- Central and East to Internet or inter-VN
  - East site border configured to propagate SGT towards DMVPN via manual override of default SDA behavior
  - Central site border configured to propagate SGT towards DMVPN via manual override of default SDA behavior



IP	SGT
10.4.1.10	STAFF
10.3.1.10	BMS
10.4.2.10	STAFF
10.3.2.10	CCTV
10.4.3.10	STAFF
10.3.3.10	BMS

Demo: Firepower SGT policy

- Block Quarantine SGT access to everything, except
  - 8.8.8.8
- Block BMS SGT to Employee SGT
- Permit Employee SGT to BMS SGT
- Test and confirm

Demo

Deploy Encrypted Traffic Analytics and Rapid Threat Containment

You make the power of data **possible**

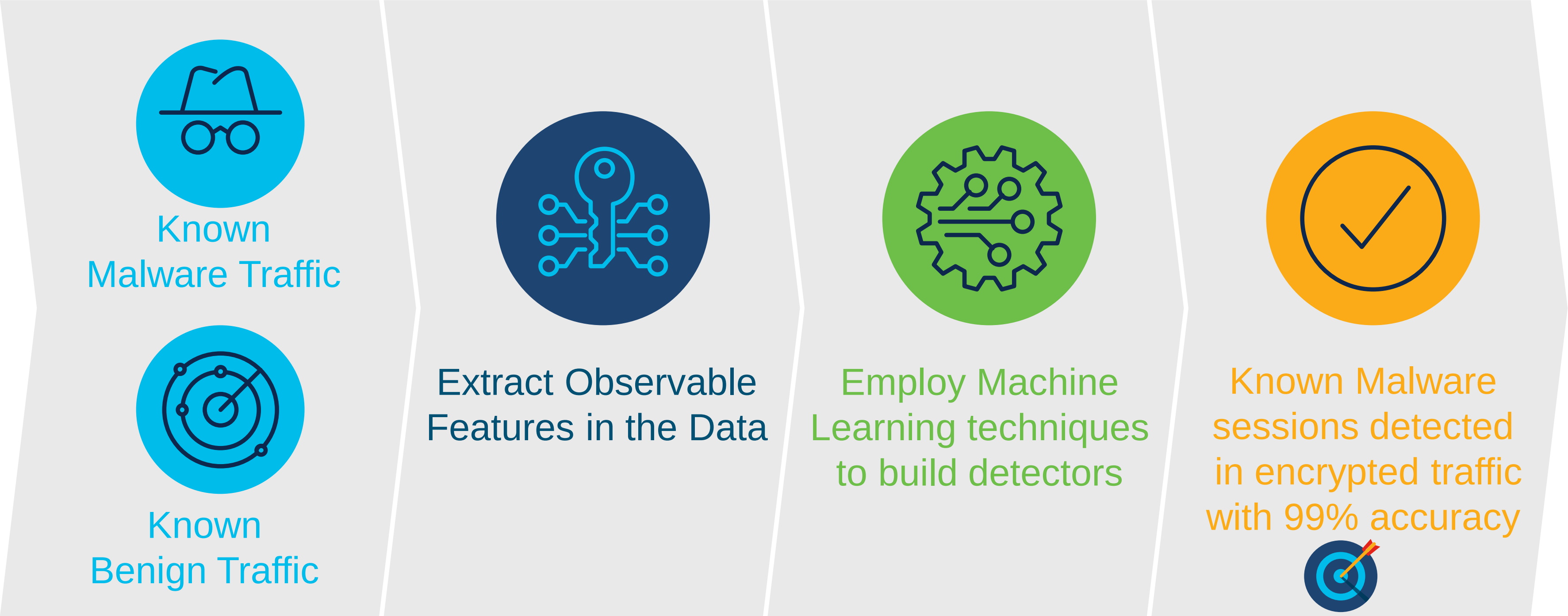
For more information

For your reference

- Watch later at ciscolive.com
  - BRKSEC-1000 Introduces Encrypted Traffic Analytics (ETA)
  - BRKCRS-1449 introduces the fundamentals of ISE, AMP and Stealthwatch
  - BRKSEC-3557 is a deep dive, including Rapid Threat Containment
- www.cisco.com/go/rtc
- Integrate Stealthwatch and ISE:
  - https://community.cisco.com/t5/security-documents/deploying-cisco-stealthwatch-7-0-with-cisco-ise-2-4-using-pxgrid/ta-p/3793357
- ETA in Cisco SD-Access design and deployment guides
  - https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/eta-design-guide-2019oct.pdf
  - https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/eta-sda-fabric-deployment-guide-2019sep.pdf

Encrypted Traffic Analytics

RECAP



Known Malware Traffic

Known Benign Traffic

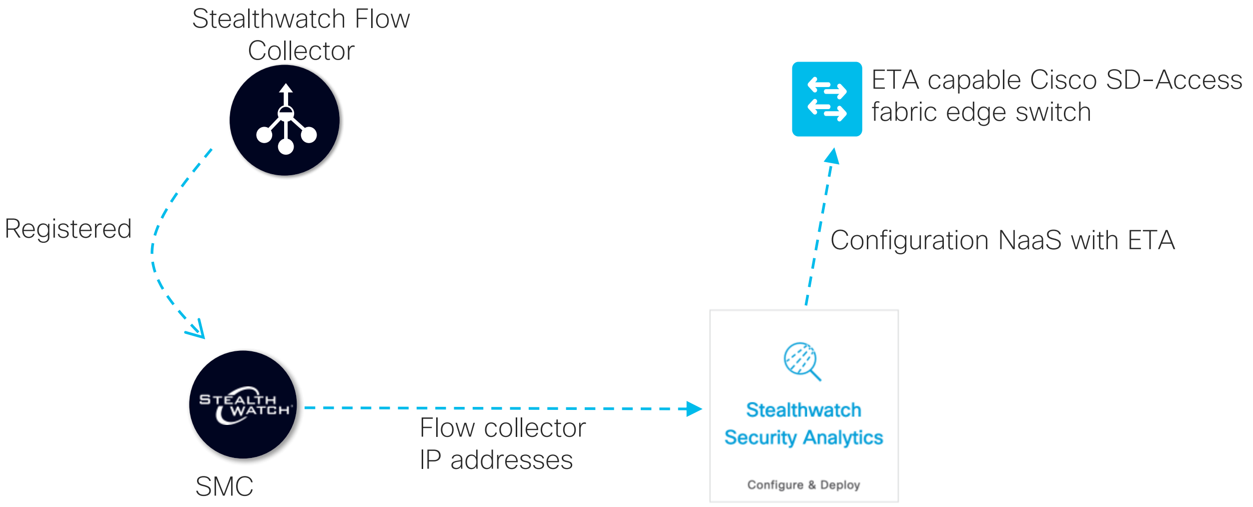
Extract Observable Features in the Data

Employ Machine Learning techniques to build detectors

Known Malware sessions detected in encrypted traffic with 99% accuracy

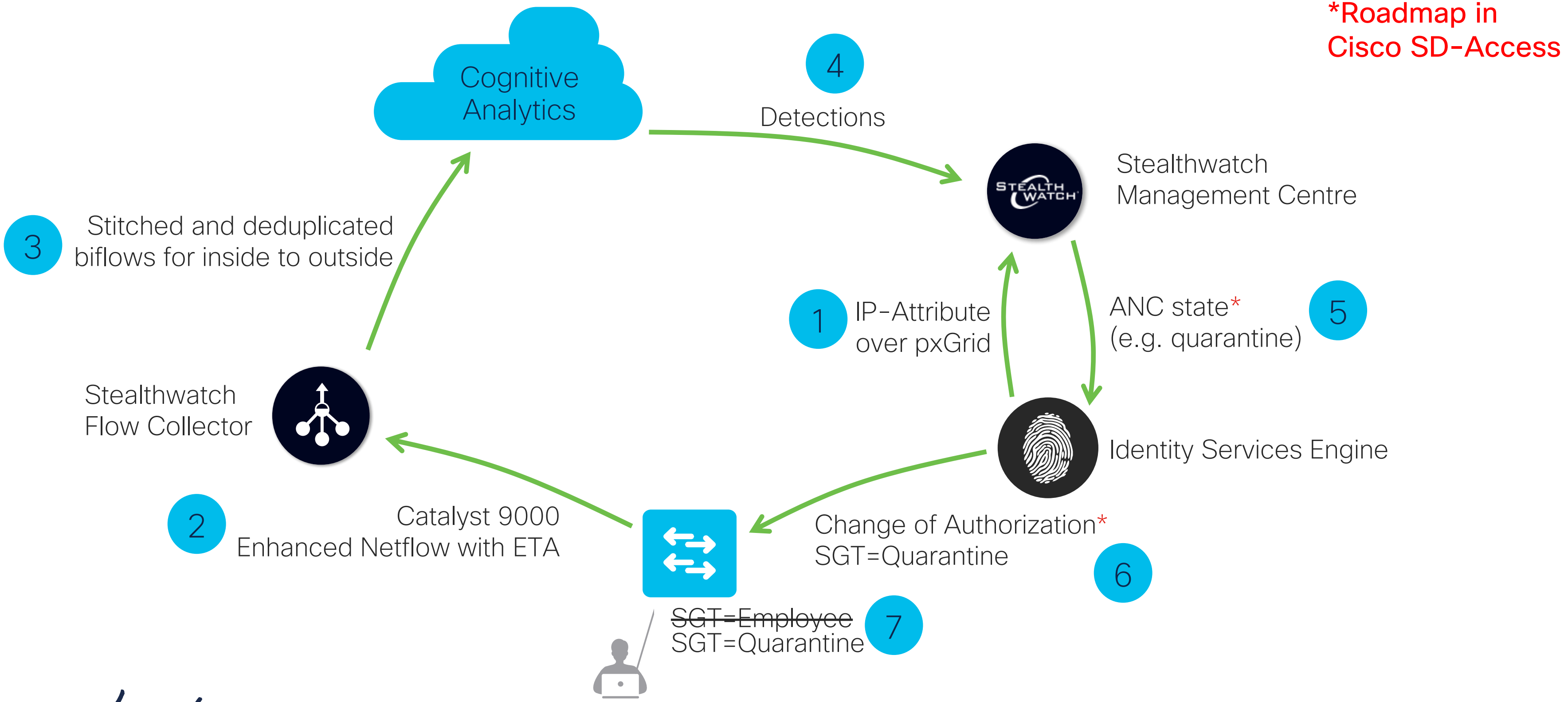
SSA with Cisco SD-Access

- Stealthwatch Security Analytics is an application within Cisco DNA Centre
- Reads Flow Collector IP addresses from Stealthwatch Management Centre
- Provisions NaaS with ETA into Catalyst 9000 Cisco SD-Access fabric edge devices


Stealthwatch Flow Collector
Registered
STEALTH WATCH
SMC
Flow collector IP addresses
Stealthwatch Security Analytics
Configure & Deploy
Configuration NaaS with ETA
ETA capable Cisco SD-Access fabric edge switch

ETA and RTC in Cisco SD-Access

*Roadmap in Cisco SD-Access



Demo: ETA and RTC

- Use Stealthwatch Security Analytics to enable ETA on East fabric site Cat 9300 fabric edge switch
- Trigger ETA detection from e_staff Windows 7 workstation
- Quarantine Windows 7 workstation
- Confirm SGT changed from Employee to Quarantine and network access is restricted accordingly

Demo

Advanced Malware Protection, TC-NAC and Rapid Threat Containment

You make multi-cloud **possible**

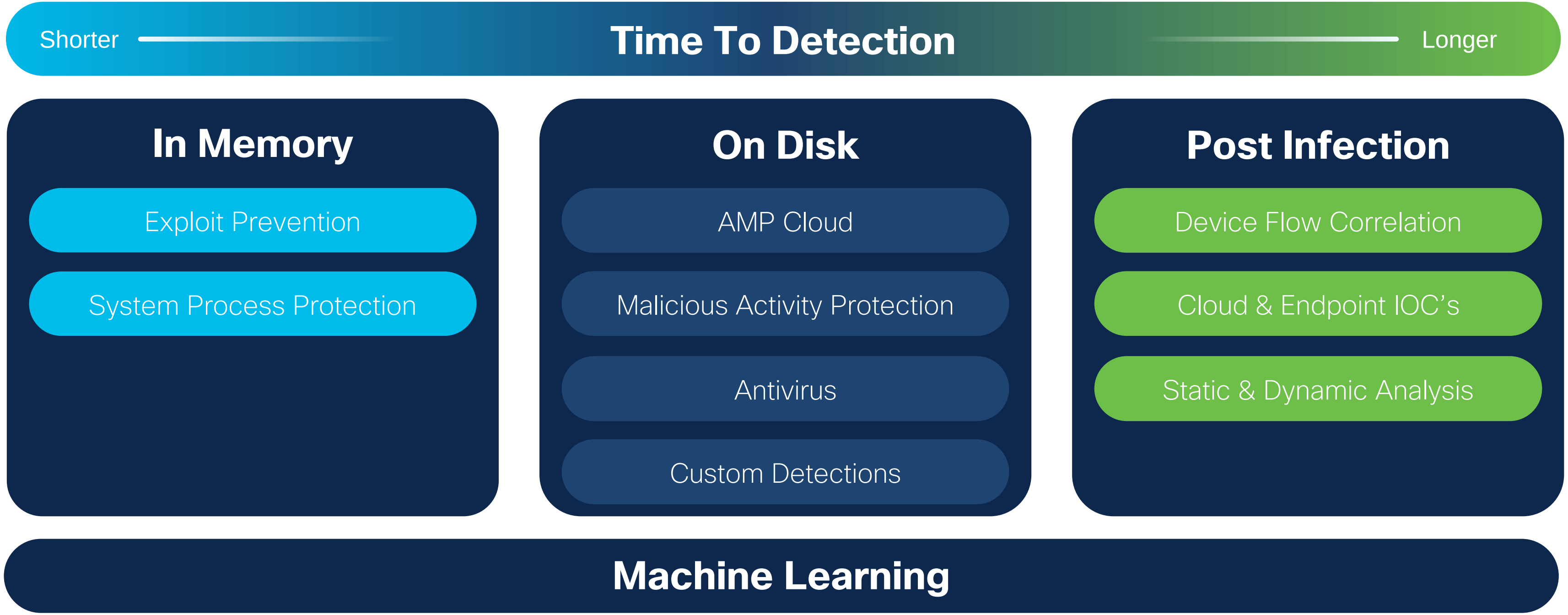
For more information

For your reference

- Watch later at ciscolive.com
  - BRKCRS-1449 introduces the fundamentals of ISE, AMP and Stealthwatch
  - BRKSEC-2890 covers AMP integrations
  - BRKSEC-3557 is a deep dive, including Rapid Threat Containment
- www.cisco.com/go/amp

AMP for endpoints

RECAP



Shorter — Time To Detection — Longer

In Memory

- Exploit Prevention
- System Process Protection

On Disk

- AMP Cloud
- Malicious Activity Protection
- Antivirus
- Custom Detections

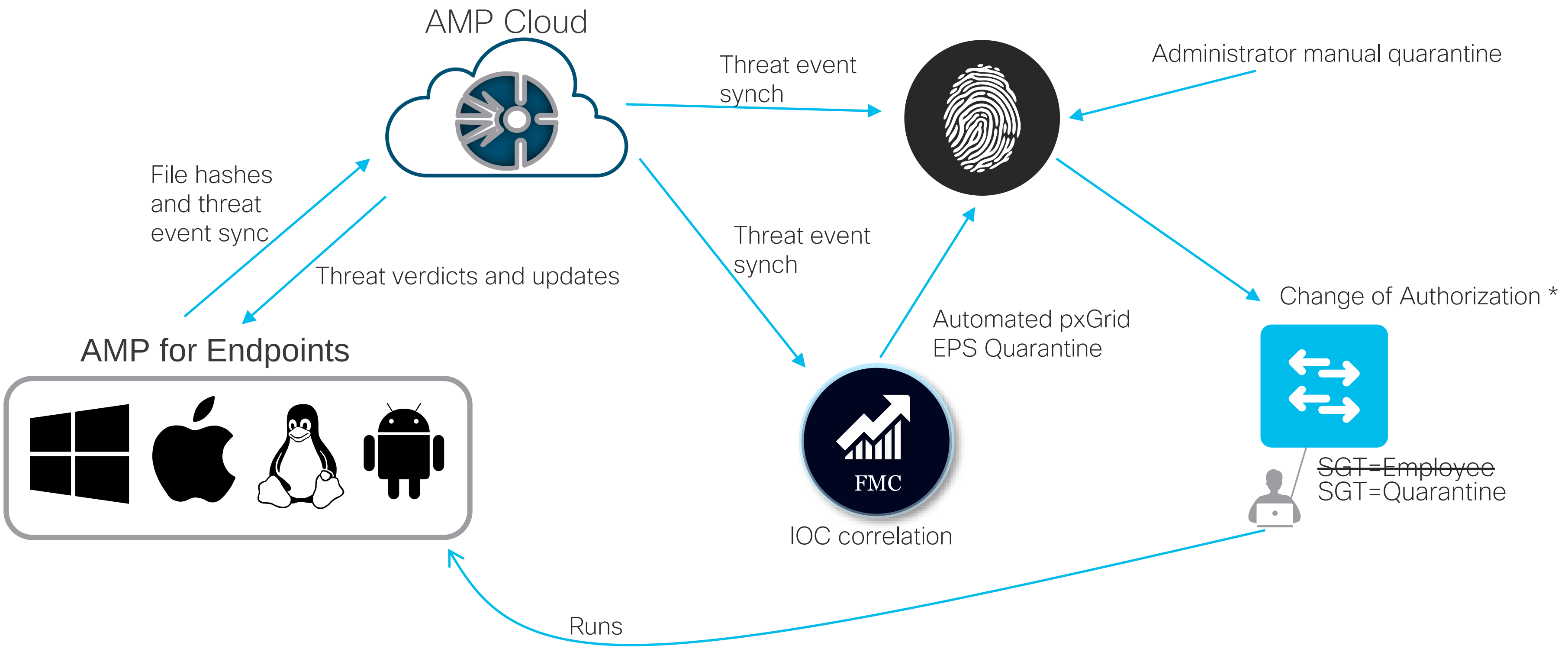
Post Infection

- Device Flow Correlation
- Cloud & Endpoint IOC's
- Static & Dynamic Analysis

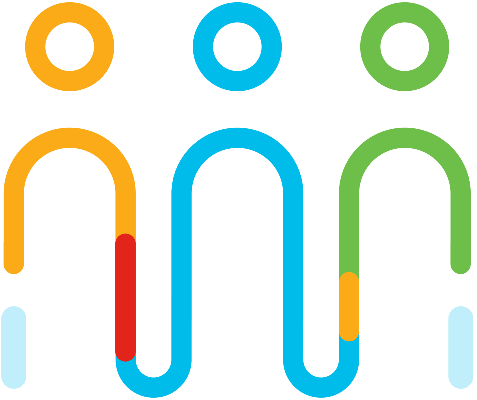
Machine Learning

AMP, TC-NAC and Rapid Threat Containment

*Roadmap in Cisco SD-Access


AMP Cloud
Threat event synch
Administrator manual quarantine
File hashes and threat event sync
Threat verdicts and updates
Threat event synch
Automated pxGrid EPS Quarantine
Change of Authorization *
AMP for Endpoints
FMC
IOC correlation
~~SGT=Employee~~
SGT=Quarantine
Runs

Conclusion



You make customer experience **possible**

Conclusion

- ✓ Discussed and demonstrated multi-domain integrations spanning WAN, LAN, DC and security
  - ✓ Cisco SD-WAN (A glimpse this time, more next time)
  - ✓ Cisco SD-Access / ISE and SGT preservation between sites
  - ✓ ACI
  - ✓ Firepower NGFW
  - ✓ Stealthwatch, ETA and RTC
  - ✓ AMP for endpoints, TC-NAC and RTC
- ✓ Proven integration of Cisco software defined solutions
- ✓ Greater integrations and automations to come!

Thank you