Let's go

The bridge to possible

Cisco Secure Firewall Attribute Base Policy and SDA Integration Deep Dive

Christopher Grabowski
Technical Marketing Engineer, Technical Leader

BRKSEC-2116

Cisco Webex App

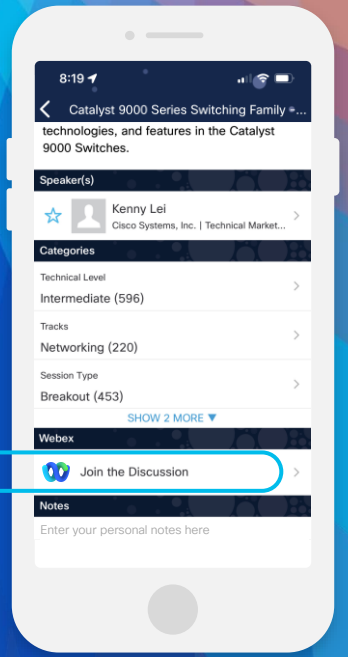
Questions?

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/#BRKSEC-2116

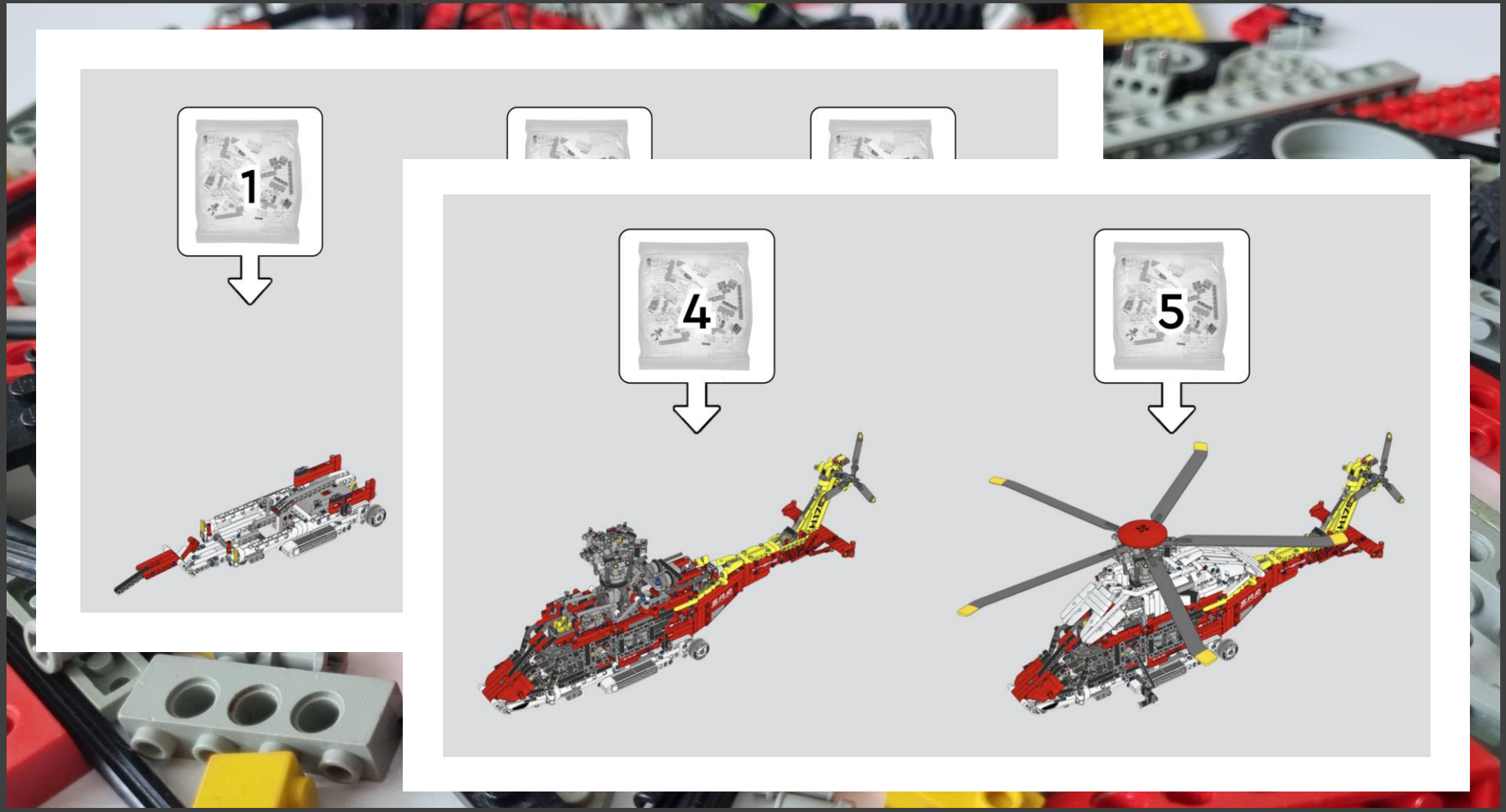
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Your Speaker

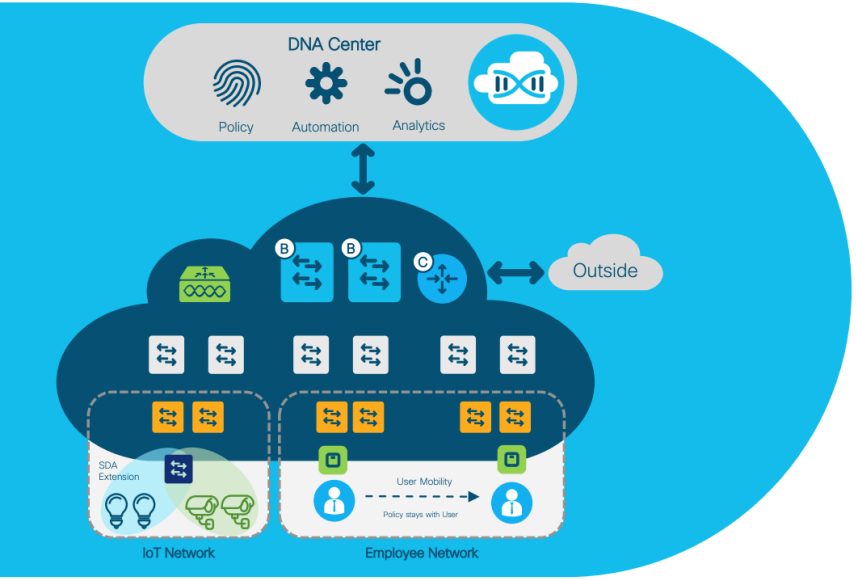
- Based in Warsaw, Poland
- With Cisco since May 2012
- Started with TAC Security, then Advanced Services, now Technical Marketing Engineer
- Focusing on Identity Firewall, SDA/ACI Integration, TLS Decryption
- Enjoys cooking and spending time with the family

Christopher Grabowski
Technical Marketing Engineer
CCIE Security #42466

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


1
4
5

Cisco Secure Firewall provides a comprehensive integration with SDA



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

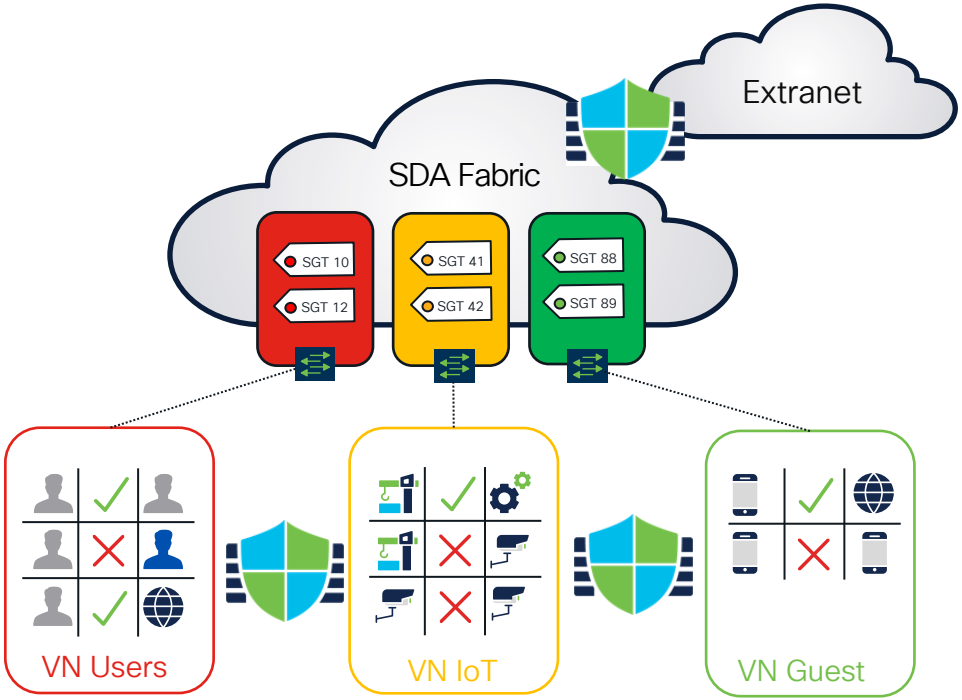
Agenda

- Introduction
- Fusion Firewall Deployment Modes and FTD Virtualization
- Cisco Secure Firewall SDA Attachment Options
- DNAC and Firewall Management Center Integration
- Attribute Based Policy
- Identity Propagation Practical Use-Cases
- Conclusions

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

Introduction

SDA Segmentation Basics



Virtual Network (VN)

First level Segmentation ensures zero communication between forwarding domains unless leaked by routing.

Scalable Group (SG)

Second level Segmentation ensures role-based access control (RBACL) between two groups within a Virtual Network based on contract.

Fusion Firewall (FW)

Stateful enforcement for inter-VN and VN to Extranet segments.

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

Contract Based vs. Firewall Enforcement

Contract based segmentations

- Out-of-the-box functionality
- Managed exclusively by NetOps
- Stateless enforcement
- Limited logging
- Provides Intra-VN enforcement

Firewall enforcement

- Advanced Firewall & IPS
- TLS decryption
- Malware analysis and retrospection
- Attributes Based policy with dynamic objects and identity
- Extensive logging, correlation and Threat Intelligence capabilities
- Requires service insertion design
- NetOps/SecOps collaboration
- Provides Inter-VN enforecement

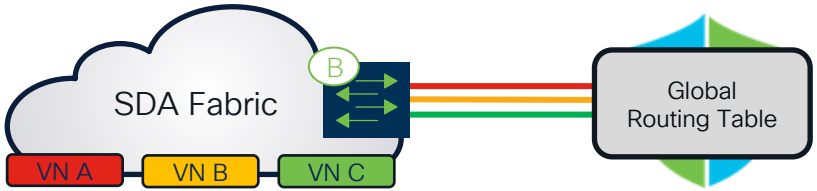
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Firewall Deployment Modes and Virtualization Options

Firewall Deployment Modes – VN Separation

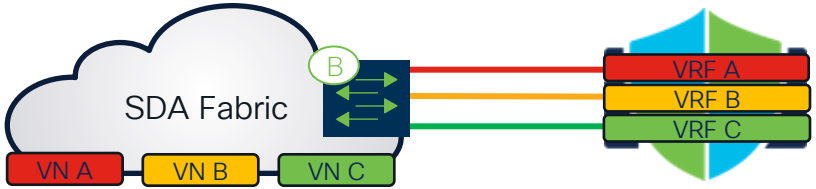
Non-VRF Aware

- Merging VN routing tables in GRT on the firewall
- Single security policy on fireall governing inter-VN and egress traffic



VN to VRF Mapping

- VN mapped to VRFs on the firewall providing routing separation
- Firewall leaks routes between VNs, Shared Services and external
- Common firewall policy across VRFs on the firewall, with VRF aware rules.

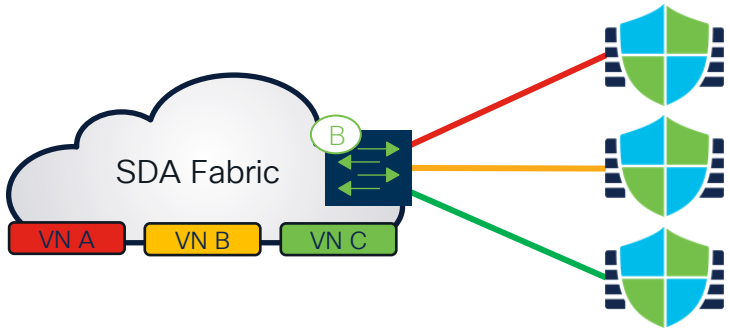


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Firewall Deployment Modes – VN Separation

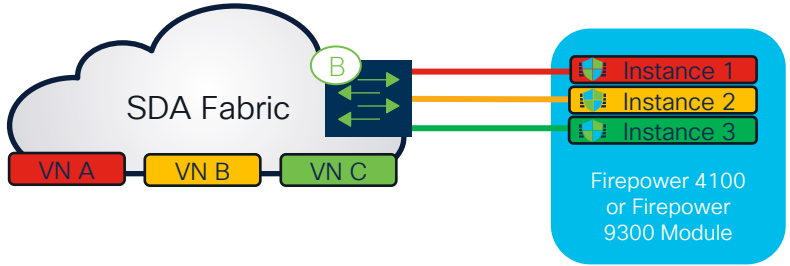
VN to Physical Device mapping

- Full physical separation between VN firewalls
- Individual firewall policies, event stores and management entities
- Multi-Tenancy support – each firewall can be managed by a different entity



VN to Instance mapping

- Supported on Firepower 3100*/4100/9300
- Instantiate multiple logical devices on a single module or appliance
- Physical and logical separation between firewall instances on Supervisor level

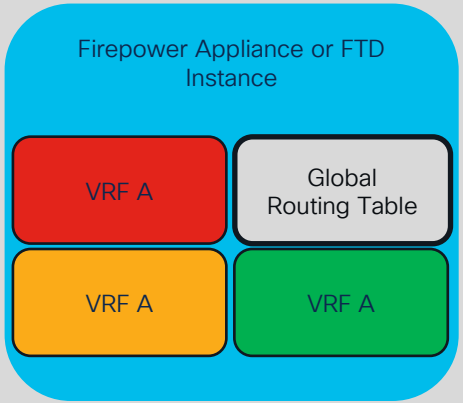


* – Coming in 7.4.1.

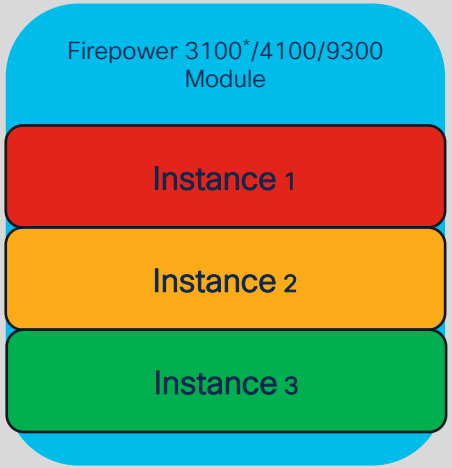
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Firewall Virtualization Options

Virtual Routers

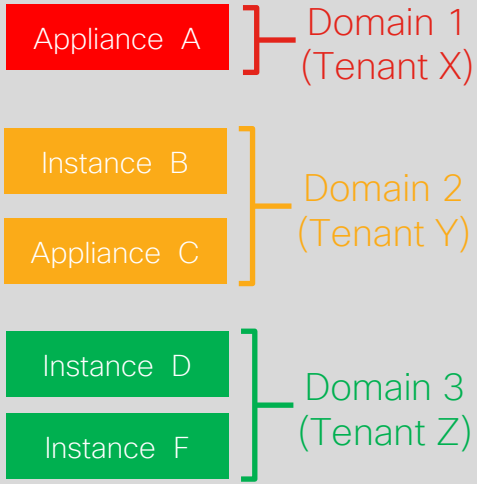


Multi-Instance



* - Coming in 7.4.1.

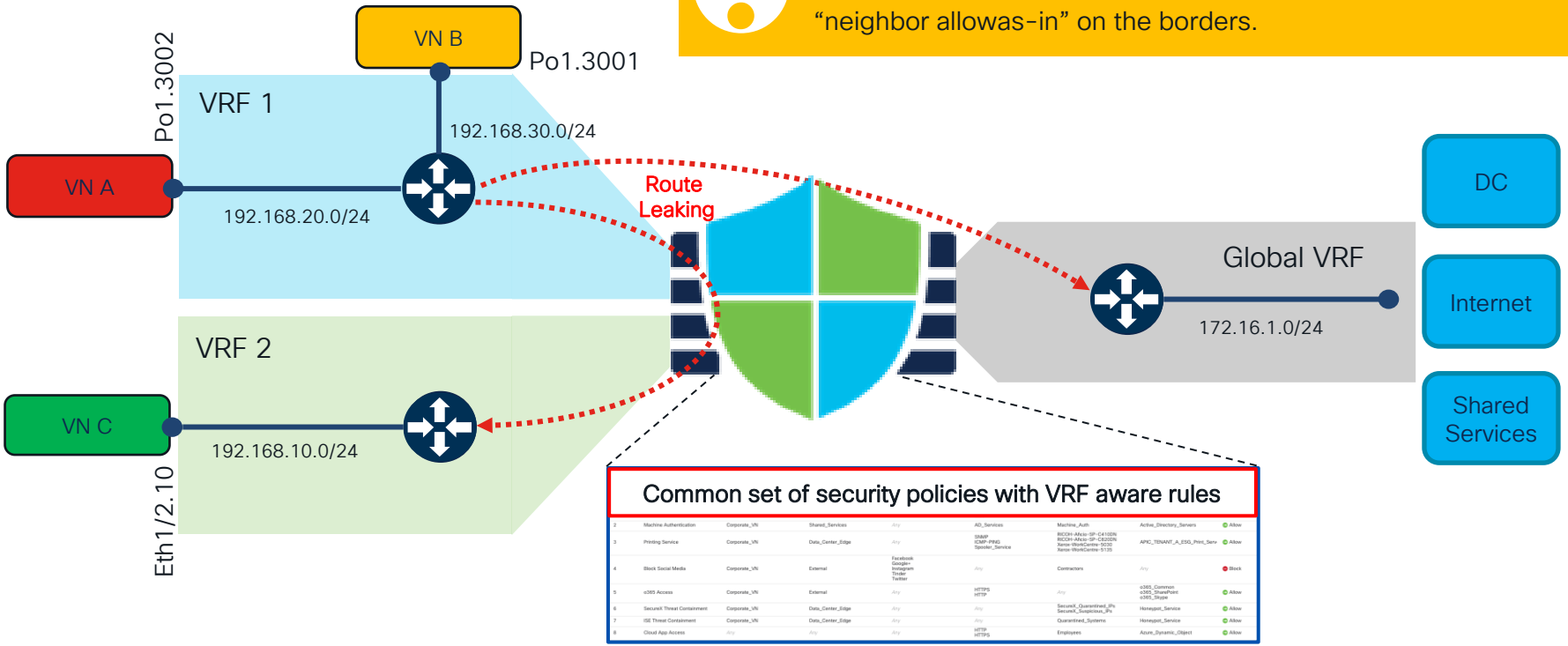
Multi-Domain



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

Virtual Router Basics

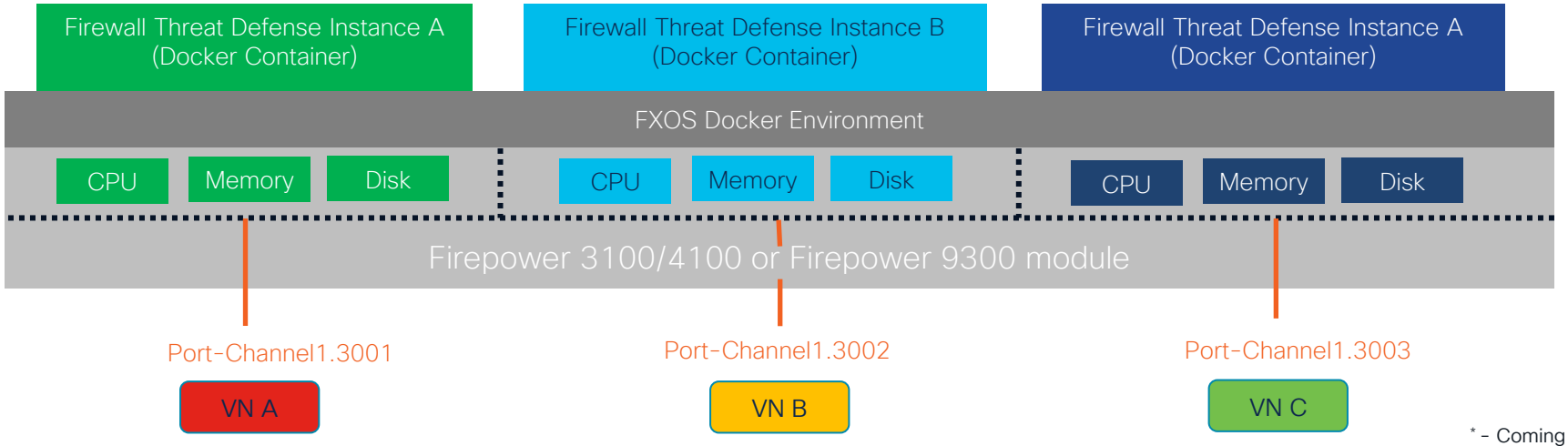
The firewall does not support BGP AS-override. When leaking routes between VNs sharing the same AS number, use "neighbor allowas-in" on the borders.



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

Firepower 3100/4100/9300 Multi-Instance

- Supported on Firepower 3100*/4100/9300
- Instantiate multiple logical devices on a single module or appliance
- Complete traffic processing and management isolation – physical and logical interface and VLAN separation at the Supervisor level

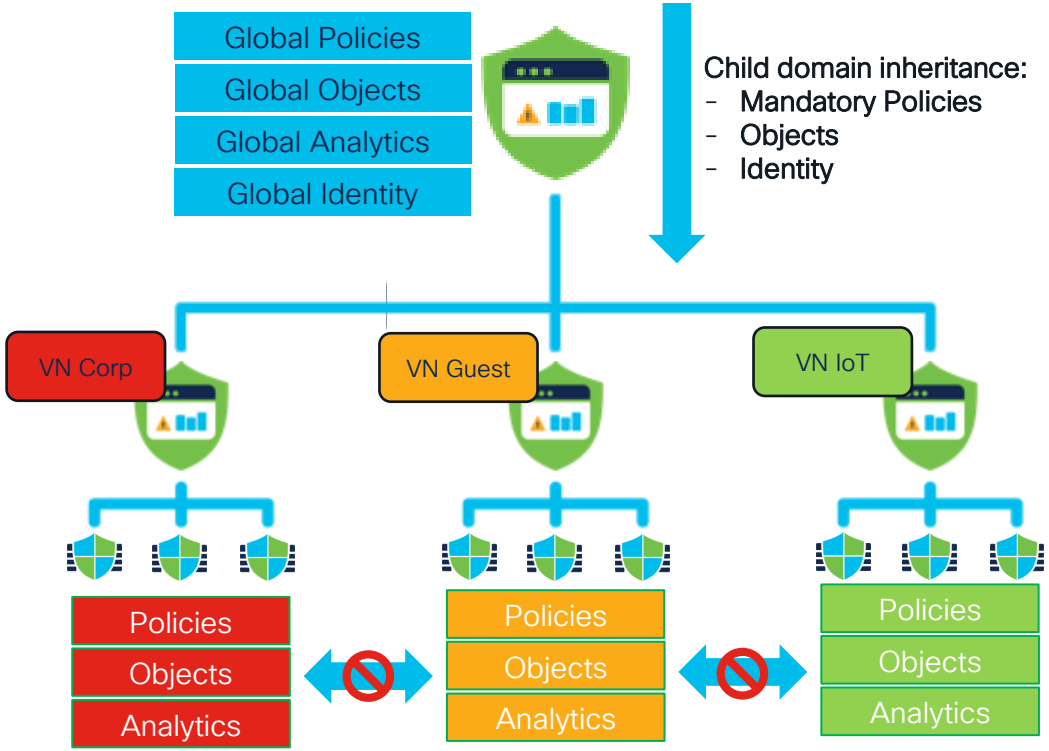


* – Coming in 7.4.1.

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

FMC Multi-Domain

Supports up to 100 domains and 3 levels

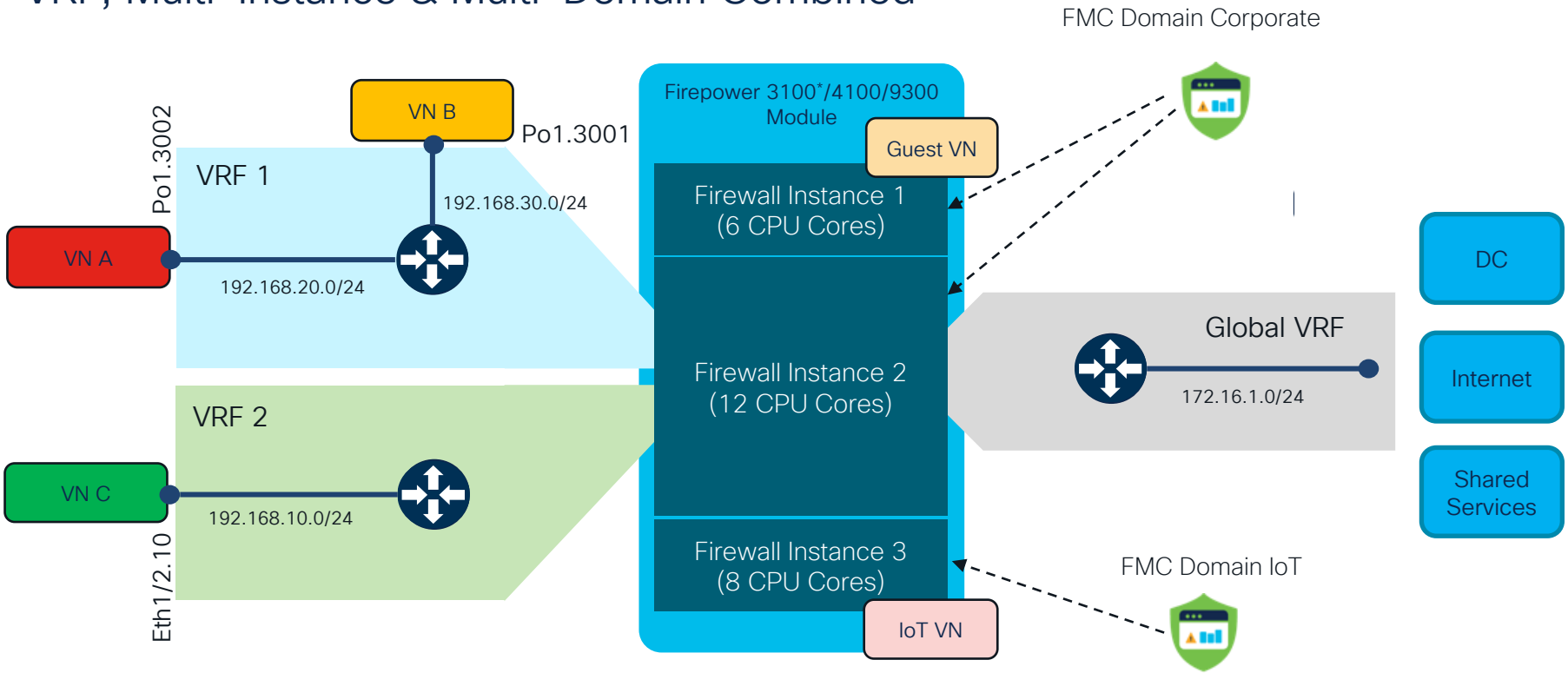


Administration, Policy, Object and Eventing isolation

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

Putting it all together

VRF, Multi-Instance & Multi-Domain Combined

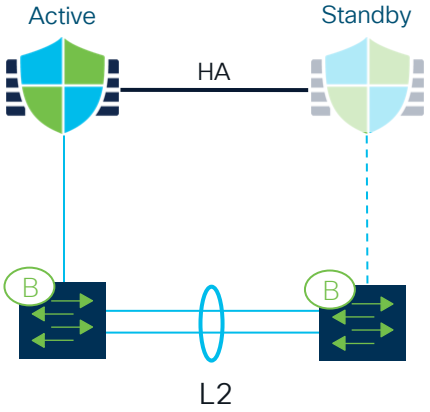


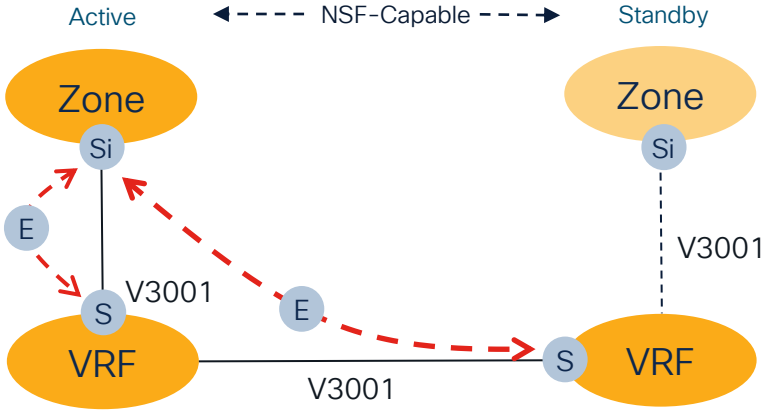
* - Coming in 7.4.1.

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

Cisco Secure Firewall SDA Attachment Options

Direct FTD Attachment






```
interface Vlan3001
 vrf forwarding IOT
 ip address 172.16.15.1/29
```

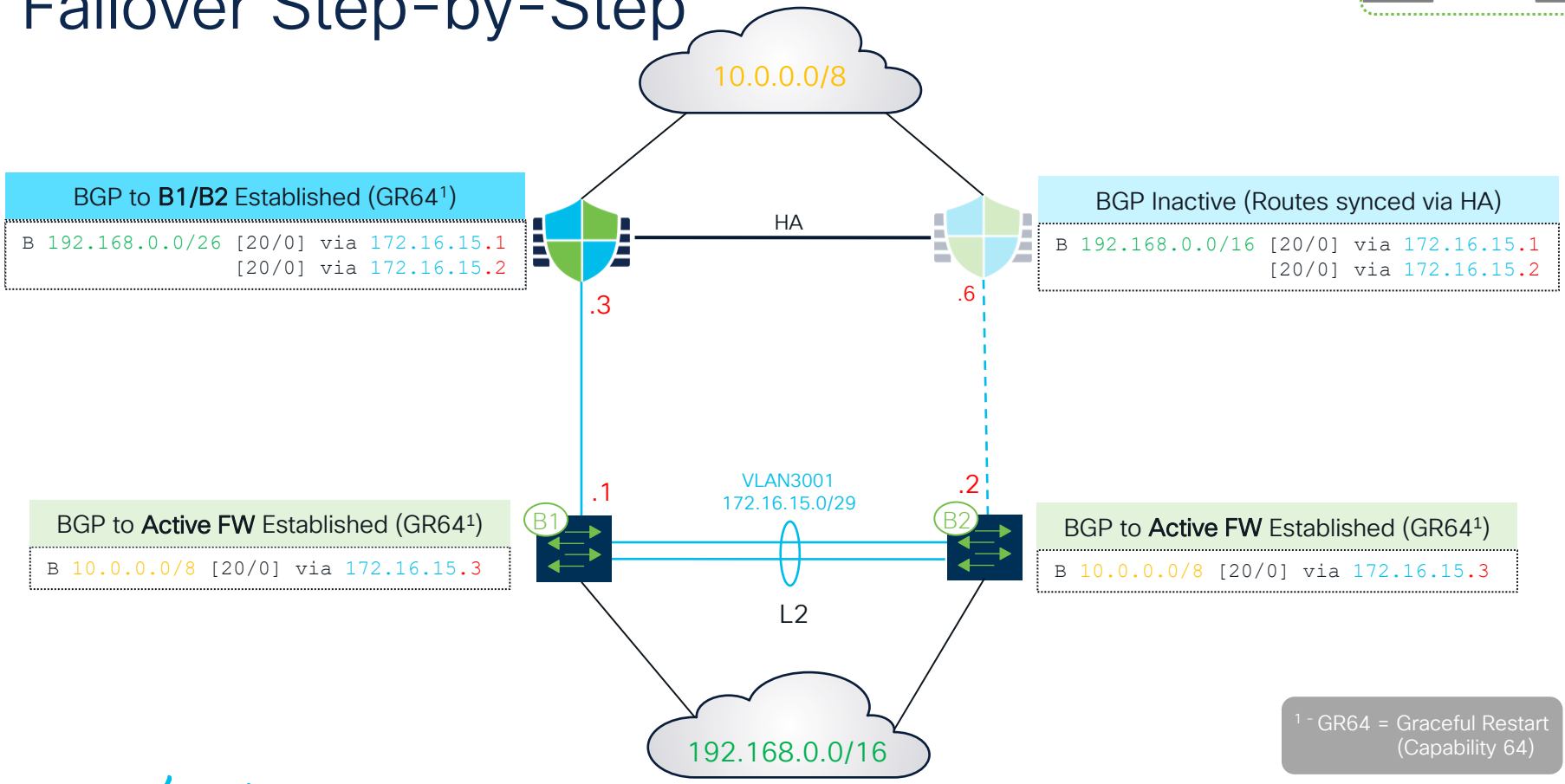
```
interface Vlan3001
 vrf forwarding IOT
 ip address 172.16.15.2/29
```

- L2 extension required between Border nodes – consider STP implications
- Active/Standby L2 adjacency with both Borders required (on the
- Firewall Threat Defense supports BGP with NSF (BFD and NSF are mutually exclusive)

Si sub-int
S SVI
E eBGP

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

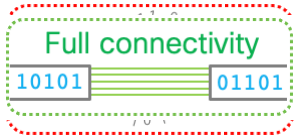
Failover Step-by-Step

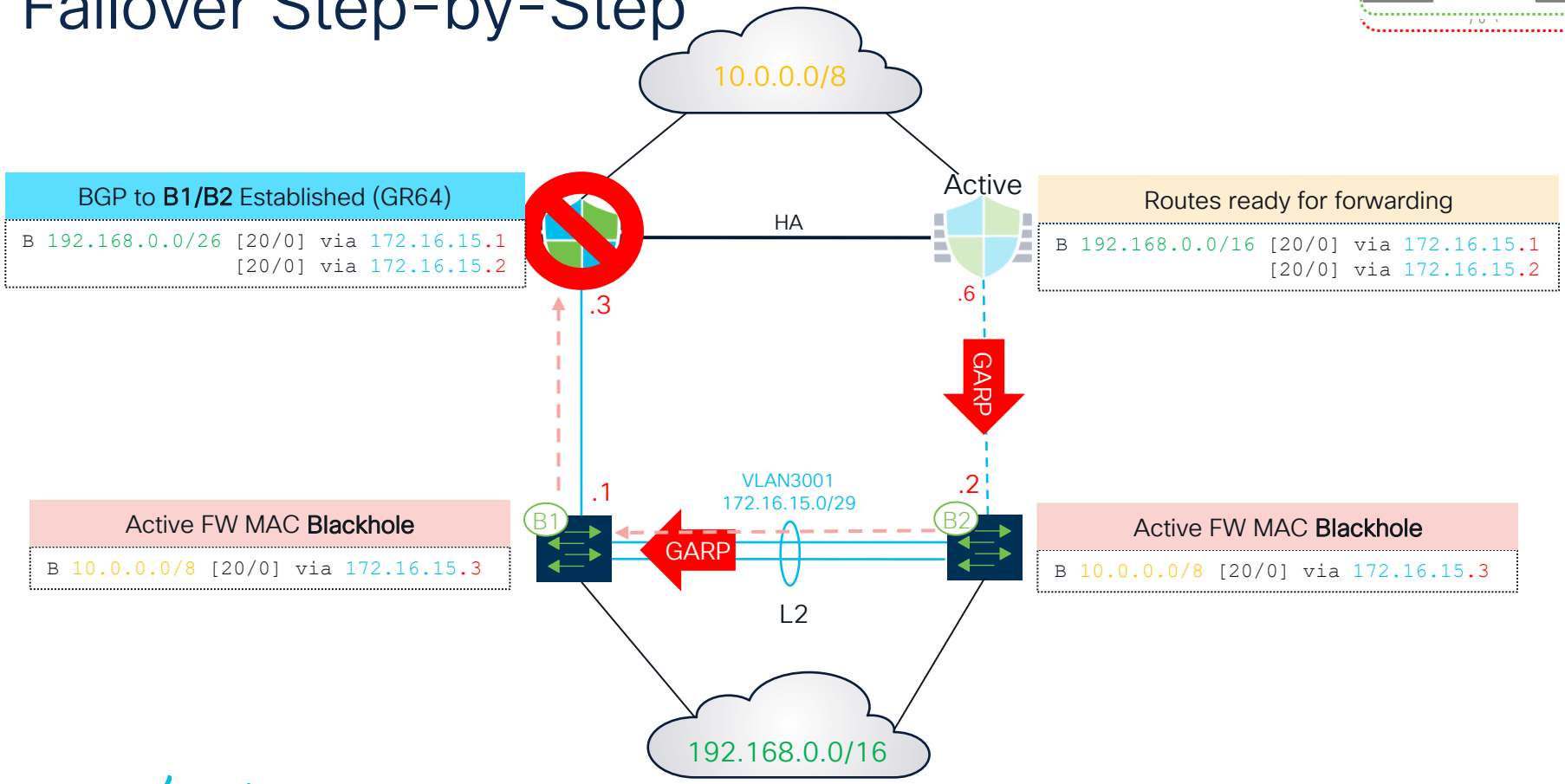


[1] - GR64 = Graceful Restart (Capability 64)

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

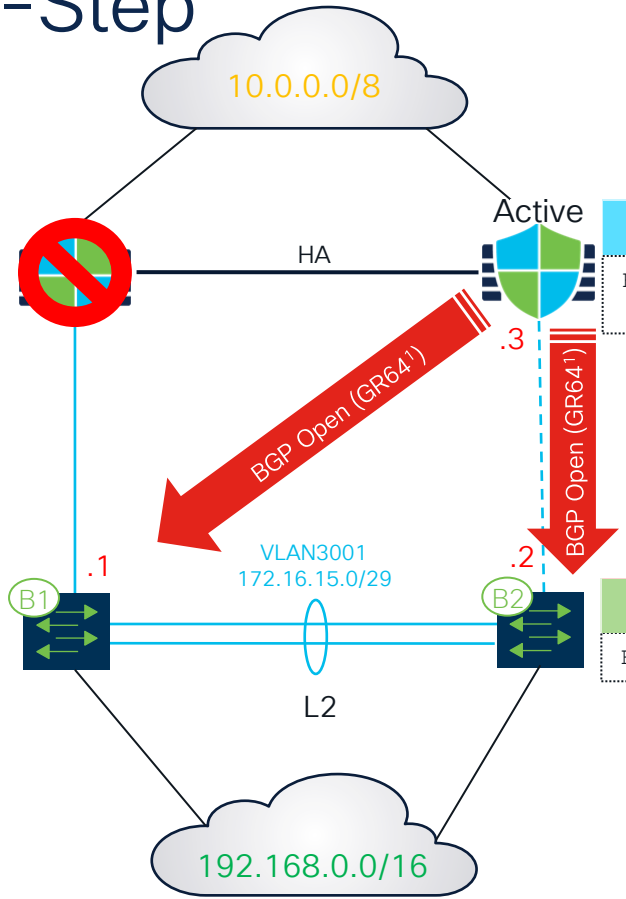
Failover Step-by-Step





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

Failover Step-by-Step



Full connectivity

10101 — 01101

Gracefully re-establishing BGP peering

```
B 192.168.0.0/16 [20/0] via 172.16.15.1
                 [20/0] via 172.16.15.2
```

Gracefully re-establishing BGP peering

```
B 10.0.0.0/8 [20/0] via 172.16.15.3
```

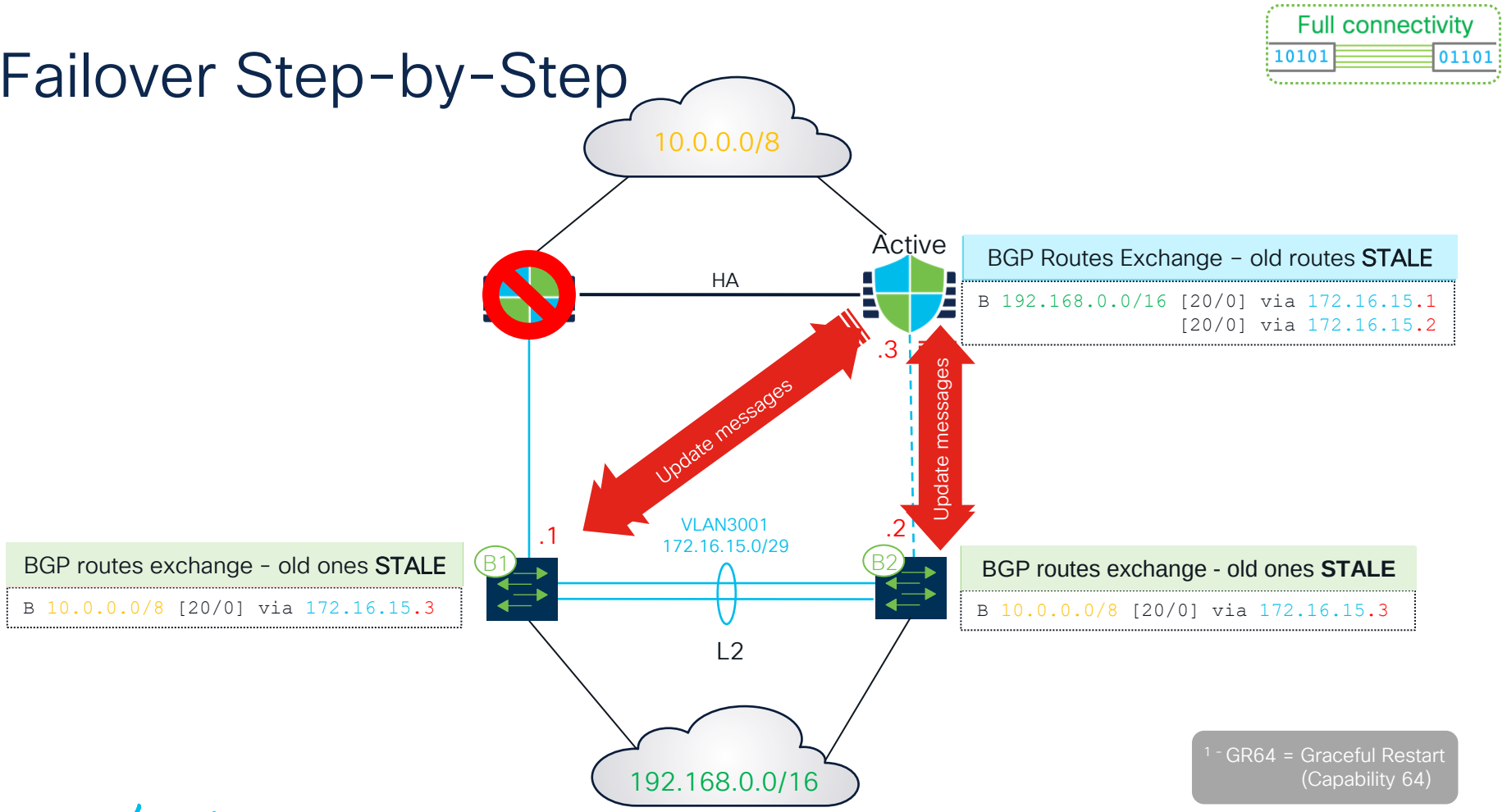
Gracefully re-establishing BGP peering

```
B 10.0.0.0/8 [20/0] via 172.16.15.3
```

[1] - GR64 = Graceful Restart (Capability 64)

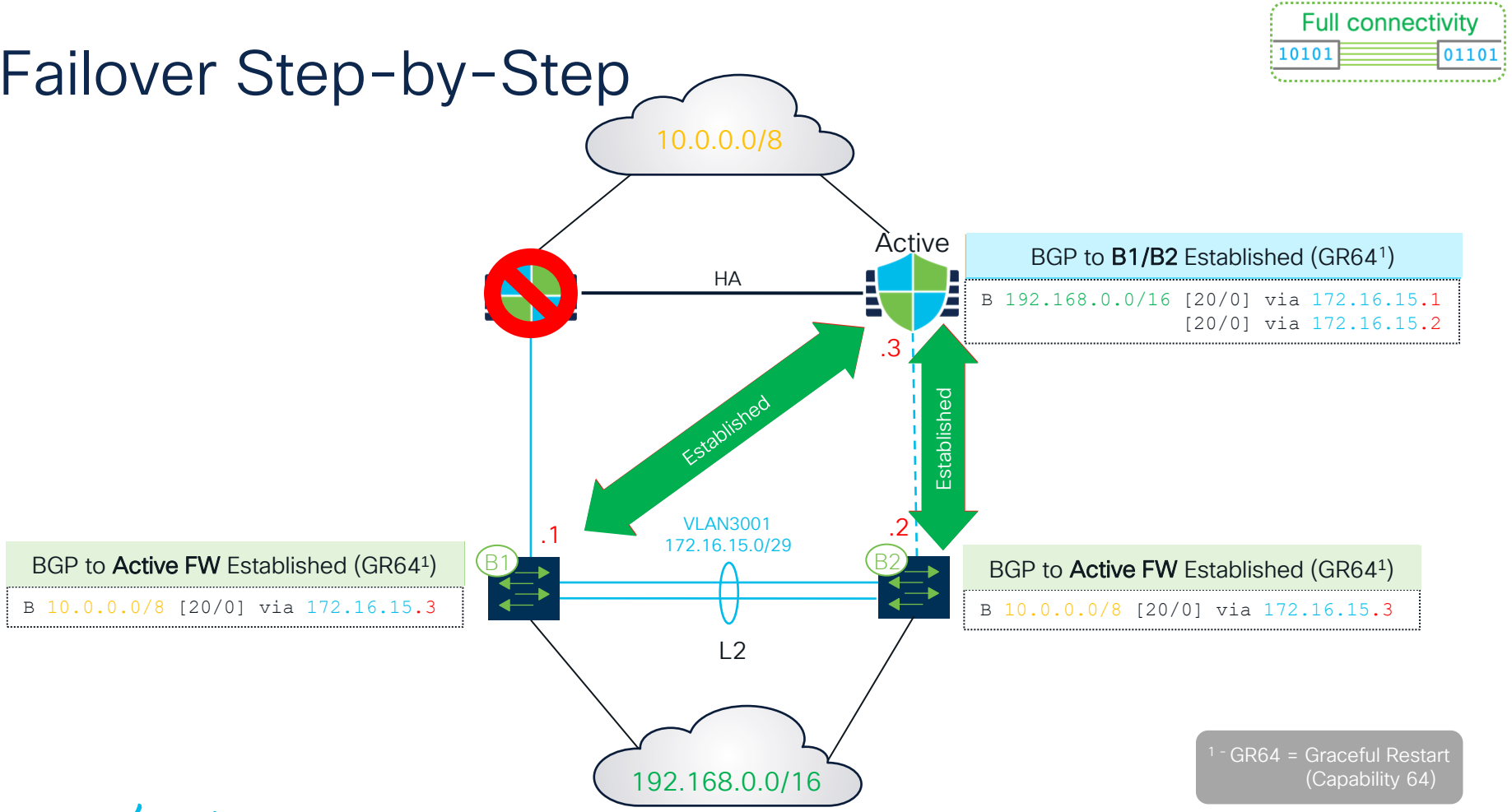
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Failover Step-by-Step



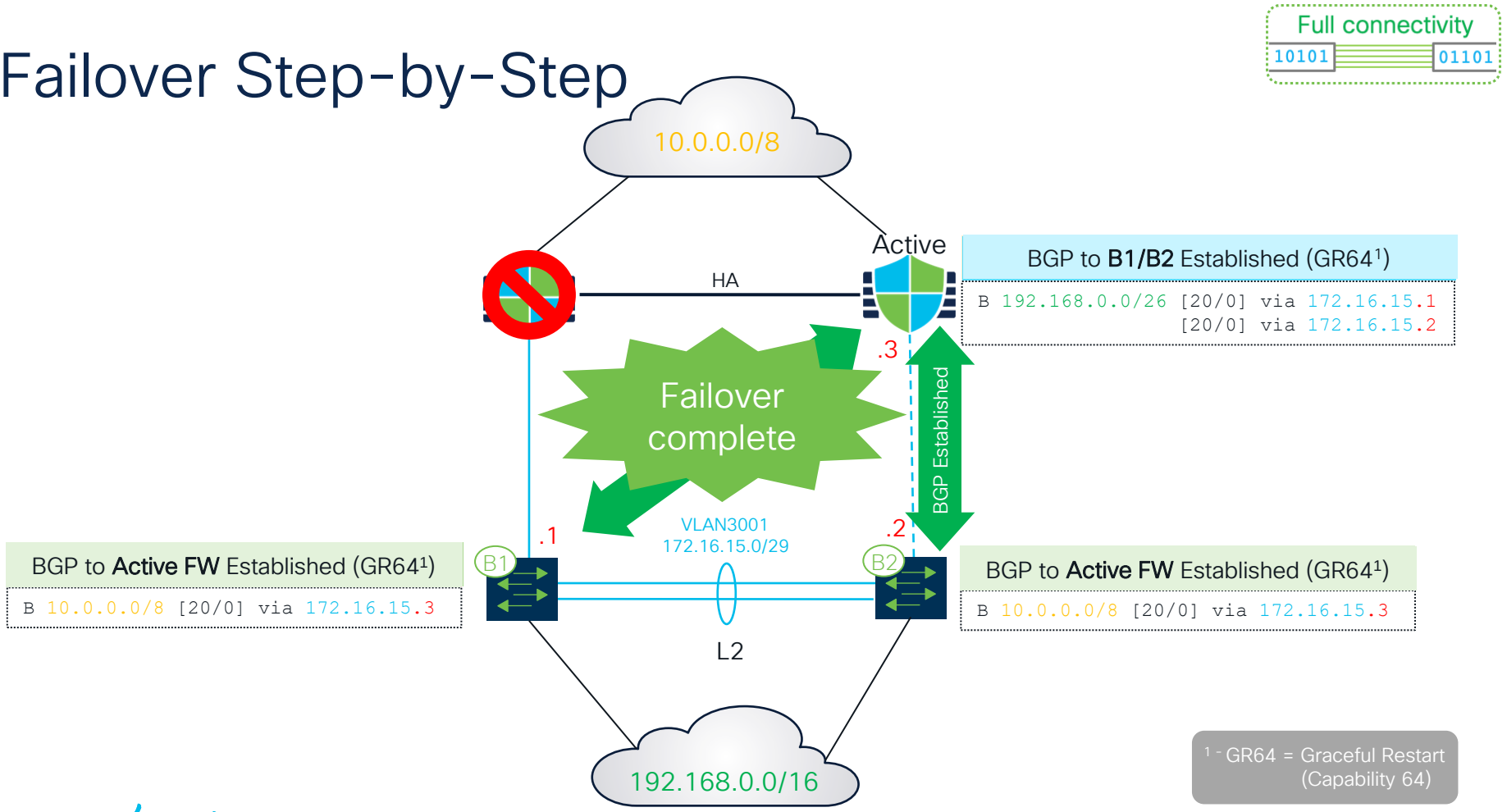
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Failover Step-by-Step



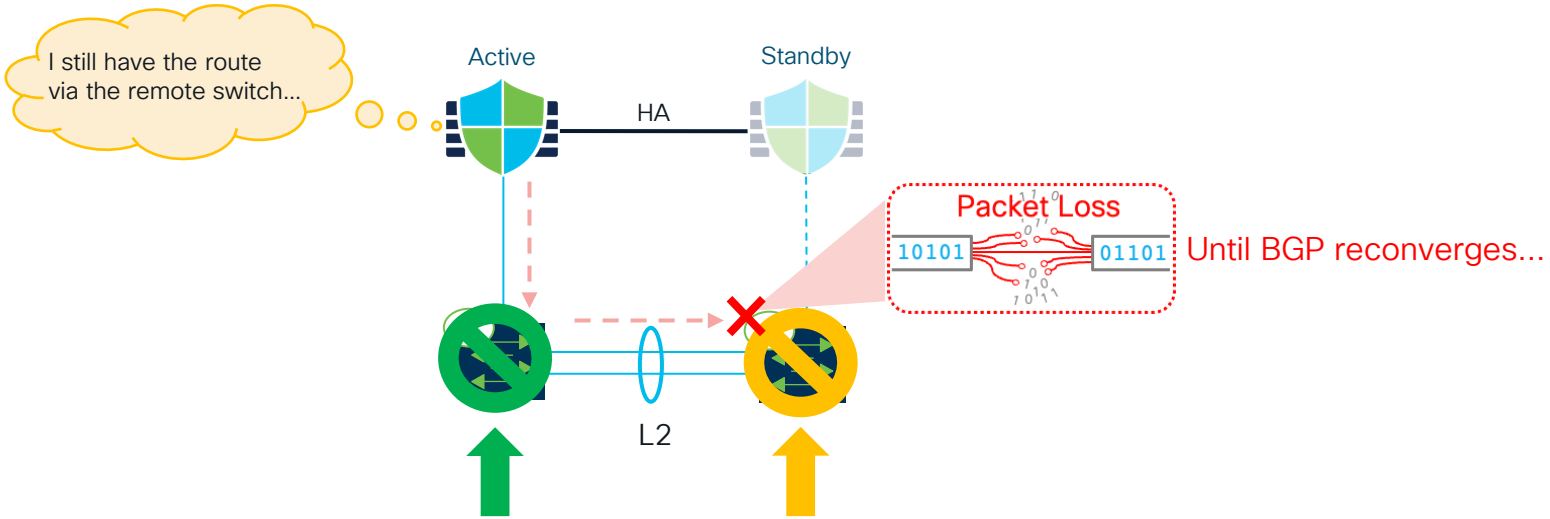
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Failover Step-by-Step



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

Direct FTD Attachment – Border Failure

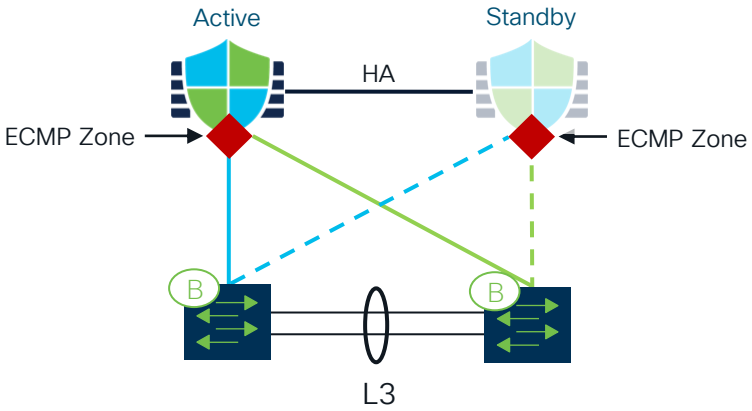


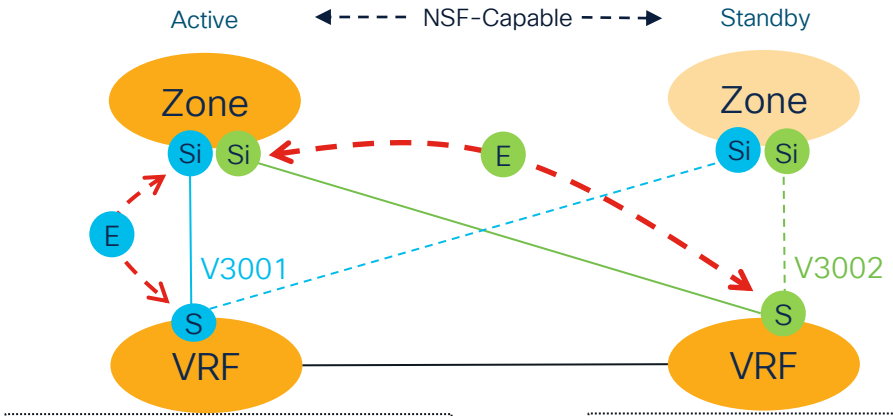
When the border connected to active FW fails, the convergence is seamless – firewall detects link loss and fails over to standby.

When the border connected to standby FW fails, the convergence relies on BGP keepalive/hold-down.

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

Direct FTD Attachment with ECMP






```
interface Vlan3001
 vrf forwarding IOT
 ip address 172.16.1.1/29
```

```
interface Vlan3002
 vrf forwarding IOT
 ip address 172.16.2.1/29
```

- ECMP Zone clubs together the interfaces and shares common connections table
- You can use both uplinks at the same time and support asymmetric flows across ECMP Zone
- Multicast routing IP PIM is not supported on ECMP Zone

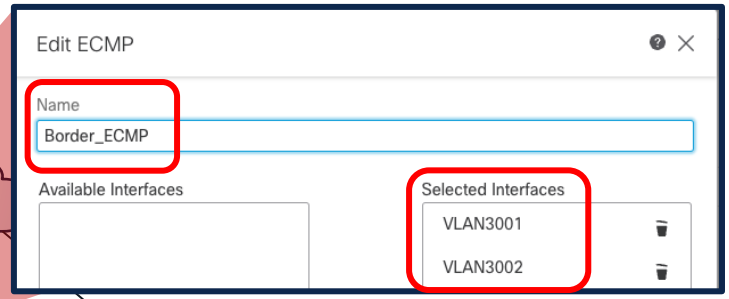
Si sub-int
S SVI
E eBGP

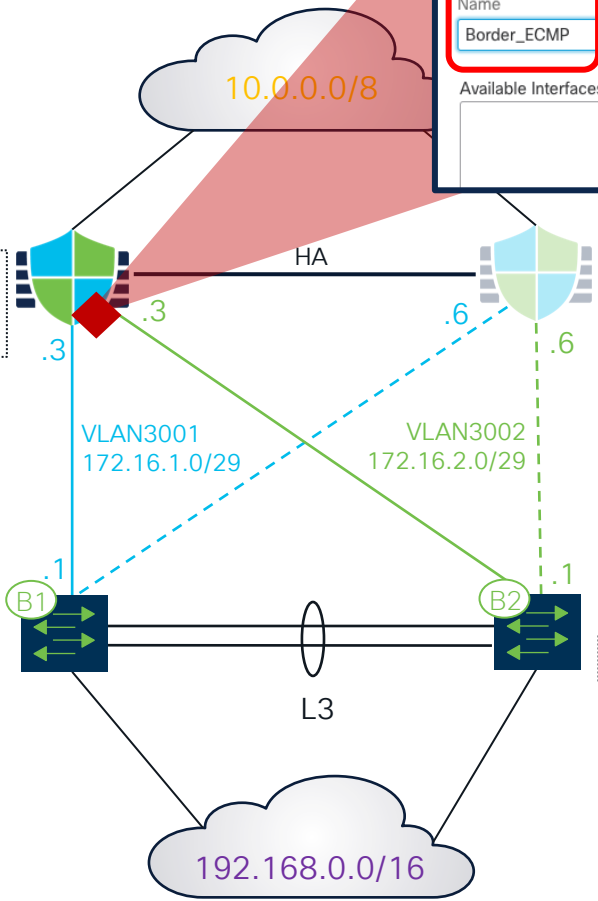
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Logical Diagram

BGP established:
- to **B1** over VLAN3001 (via 172.16.1.1)

```
B 192.168.0.0/16
    [20/0] via 172.16.1.1, VLAN3001, BORDER_ECMP
```





BGP to **Active FW** Established over VLAN3001

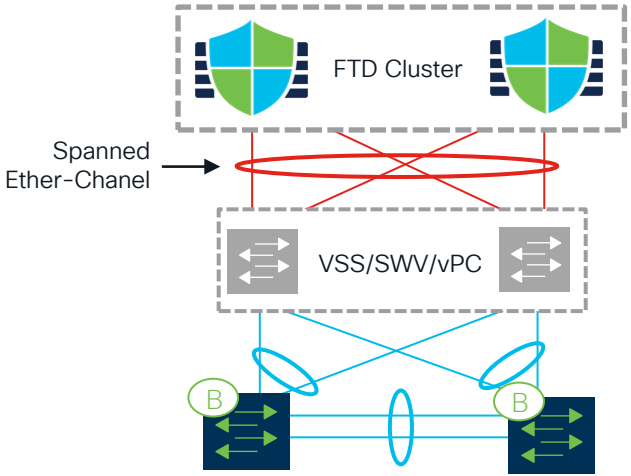
```
B 10.0.0.0/8 [20/0] via 172.16.1.3
```

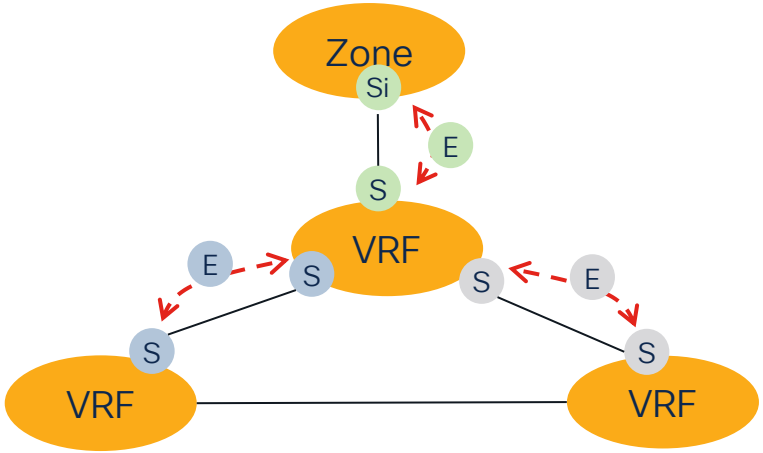
BGP to **Active FW** Established over VLAN3002

```
B 10.0.0.0/8 [20/0] via 172.16.2.3
```


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

FTD Cluster with Intermediate Switching Layer



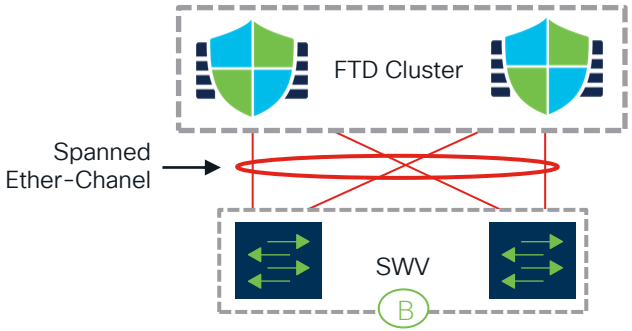


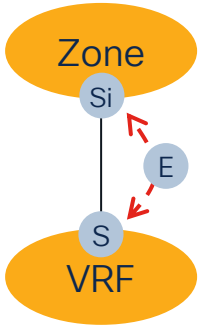
- Firewalls in a cluster symmetrize traffic for stateful NGFW/NGIPS services.
- Intermediate switches load-balance packets to Firewalls in the cluster over spanned Ether-Channel
- VRF and Multi-instance supported with clustering

Si sub-int
S SVI
E eBGP

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

FTD Cluster with Stacked Borders





- Straight-forward routing design at the cost of somewhat reduced redundancy
- Spanned Ether-Channel set directly between firewall cluster and stacked border nodes
- VRF and Multi-instance supported with clustering

Si sub-int
S SVI
E eBGP

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

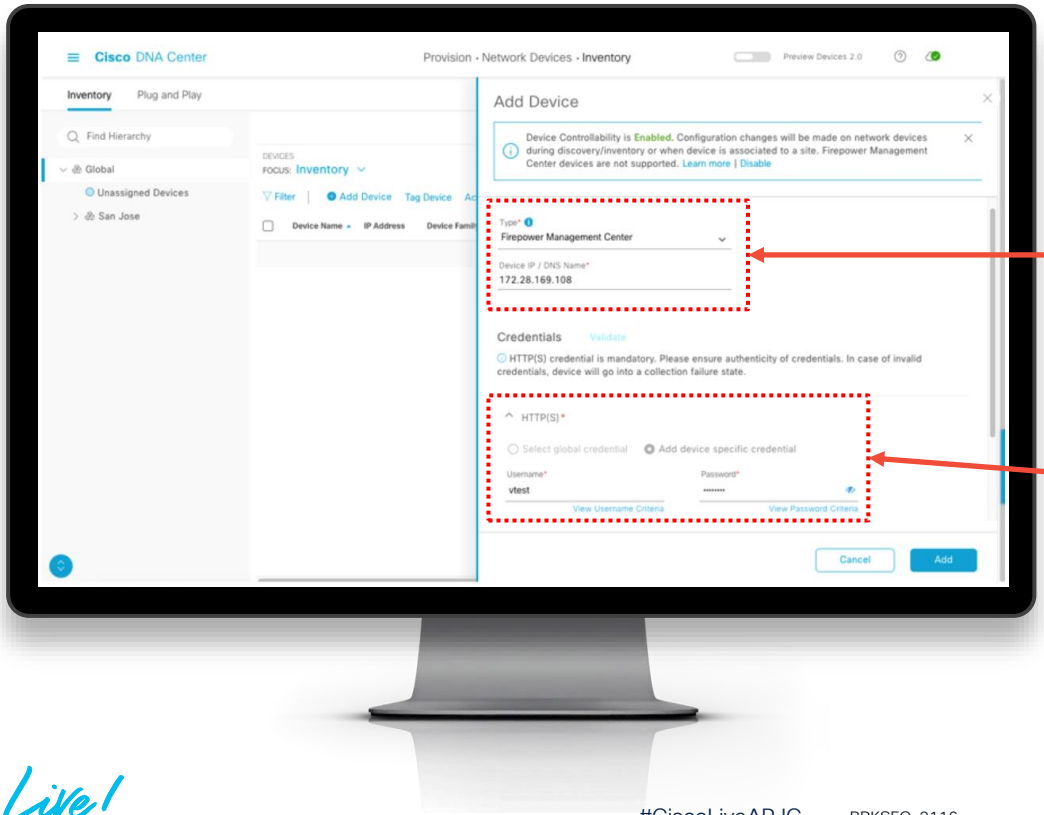
DNAC and Firewall Management Center Integration

Integrating DNAC with FMC

- REST based integration – DNAC calls FMC's API resources
- Inventory collection – DNAC adds FMC and managed FTD devices to the inventory
- Software Image Management – DNAC collects FMC/FTD images metadata into Image Repository; you can trigger readiness/upgrade job on FMC from DNAC

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

Adding FMC Device to DNAC Center



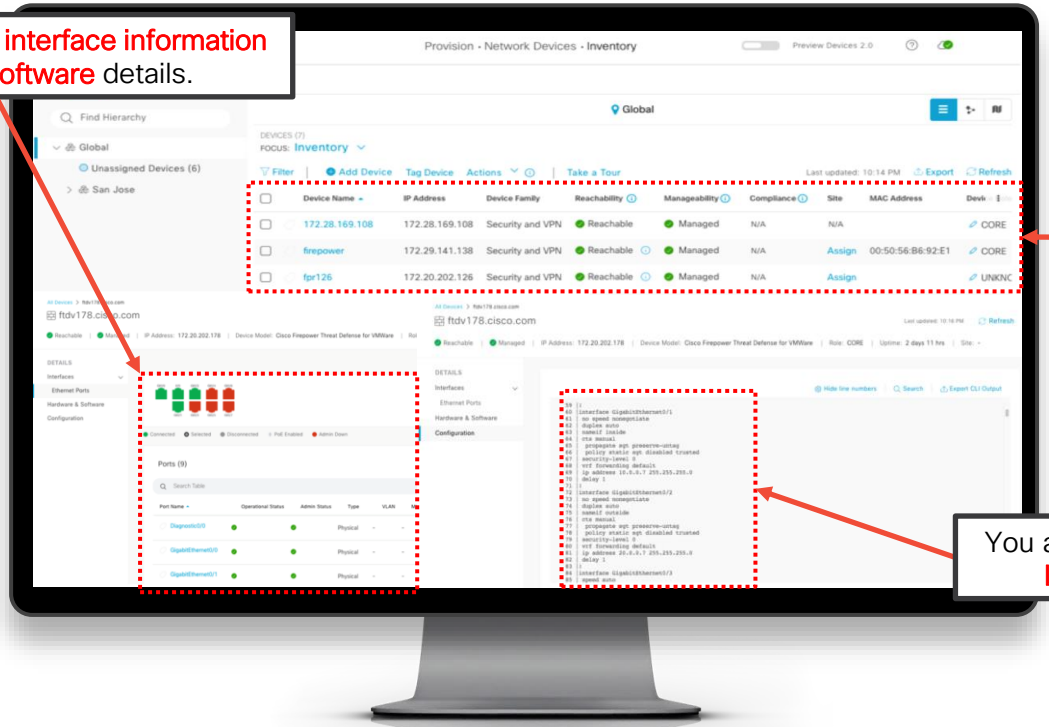
Use Firepower Management Center type and provide an IP Address.

Provide username and password for REST API access. Ensure these credentials are used exclusively by DNAC.

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

Firewall in DNAC's Center Inventory

DNAC displays FTD's **interface information** and **hardware/software** details.

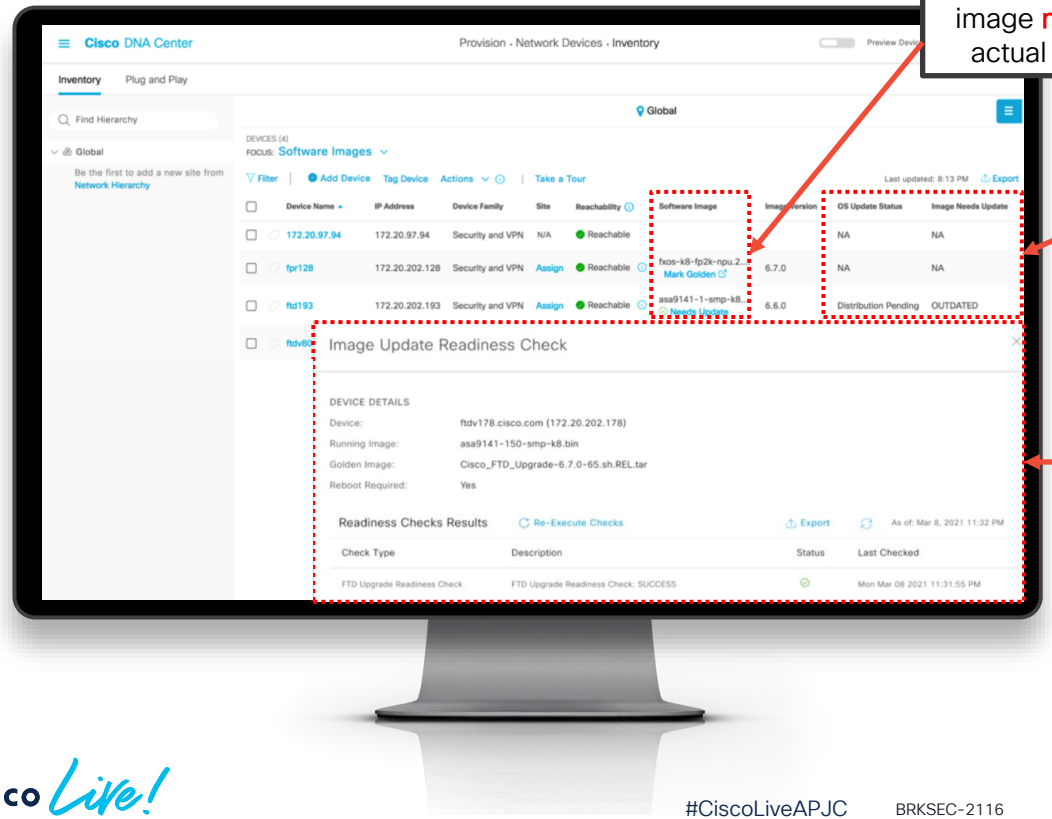


DNAC imports **all FTD firewalls managed by the FMC** into the Inventory.

You also can review the running **LINA configuration file**.

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

Cisco Secure Firewall Upgrade Workflow



DNAC collects FMC and managed FTD's image **metadata** into image Repository. The actual image files are stored on the FMC.

DNAC provides **upgrade status**, as reported by FMC and performs a **re-sync of FTD firewalls** after an upgrade job.

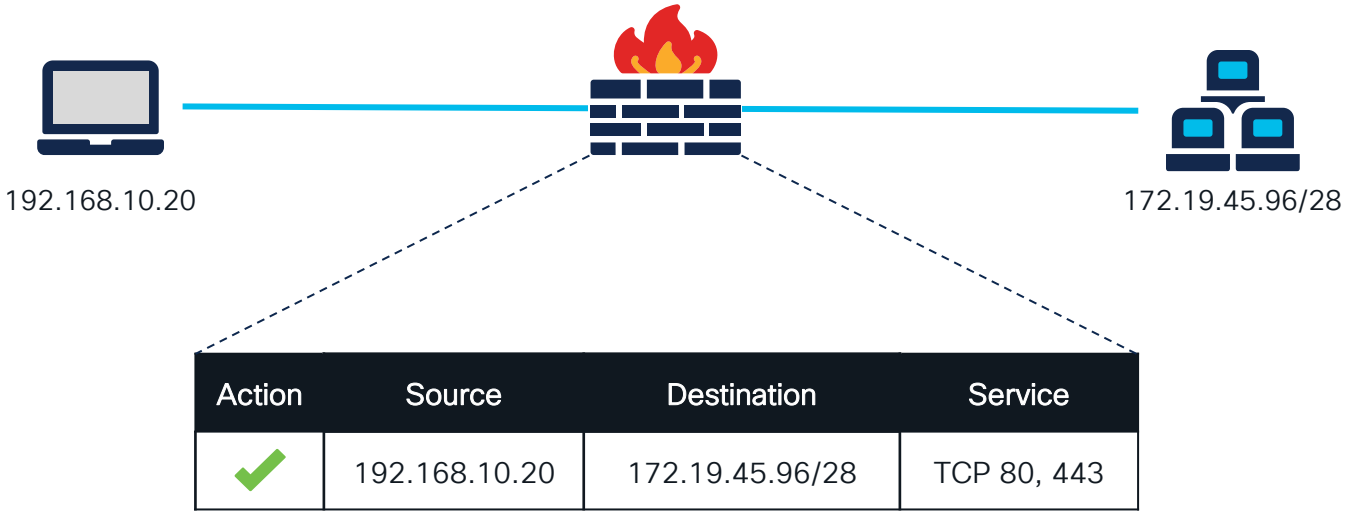
DNAC triggers API calls to FMC to run **upgrade readiness** and **upgrade workflows** on selected FTD images.

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

DNAC & FMC Integration Demo

Attribute Based Policy

Traditional Firewall Policy is not Enough



Action	Source	Destination	Service
✔	192.168.10.20	172.19.45.96/28	TCP 80, 443

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

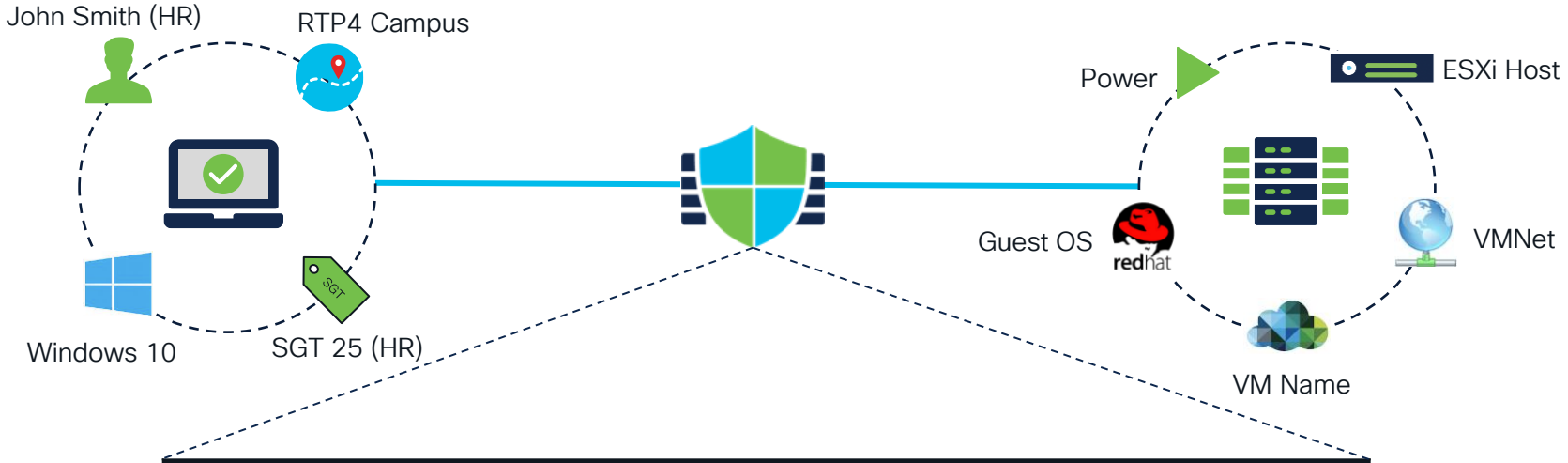
"Through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws."

Technology Insight for Network Security Policy Management

Gartner

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

Shift Towards Intent Based Policy

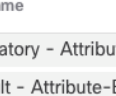


Action	Source	Destination	Service
✔	HR Users in RTP4 Campus on Windows10	PoweredOn servers in UAT VMNet containing HR-Prod in the VM Name	TCP 80, 443

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

Attribute Based Policy

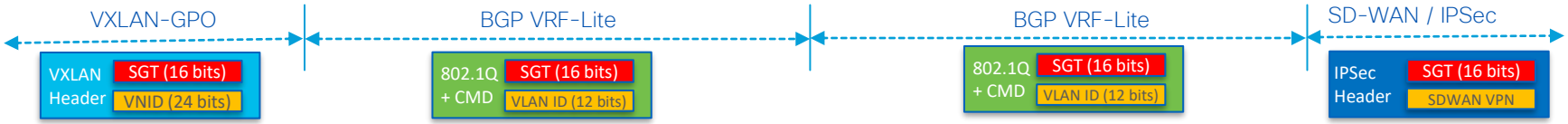
#	Name	Source Zones	Dest Zones	Users	Ap...	Dest Ports	Source Dynamic Attributes	Destination Dynamic ...es	Action
>	Mandatory - Attribute-Based Policy (-)								
v	Default - Attribute-Based Policy (1-9)								
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	A...
2	IoT Support Service	External	IoT_VN	Any		HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Pri...	Corporate_VN	Data_Center_Edge	Any		SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	...VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow



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

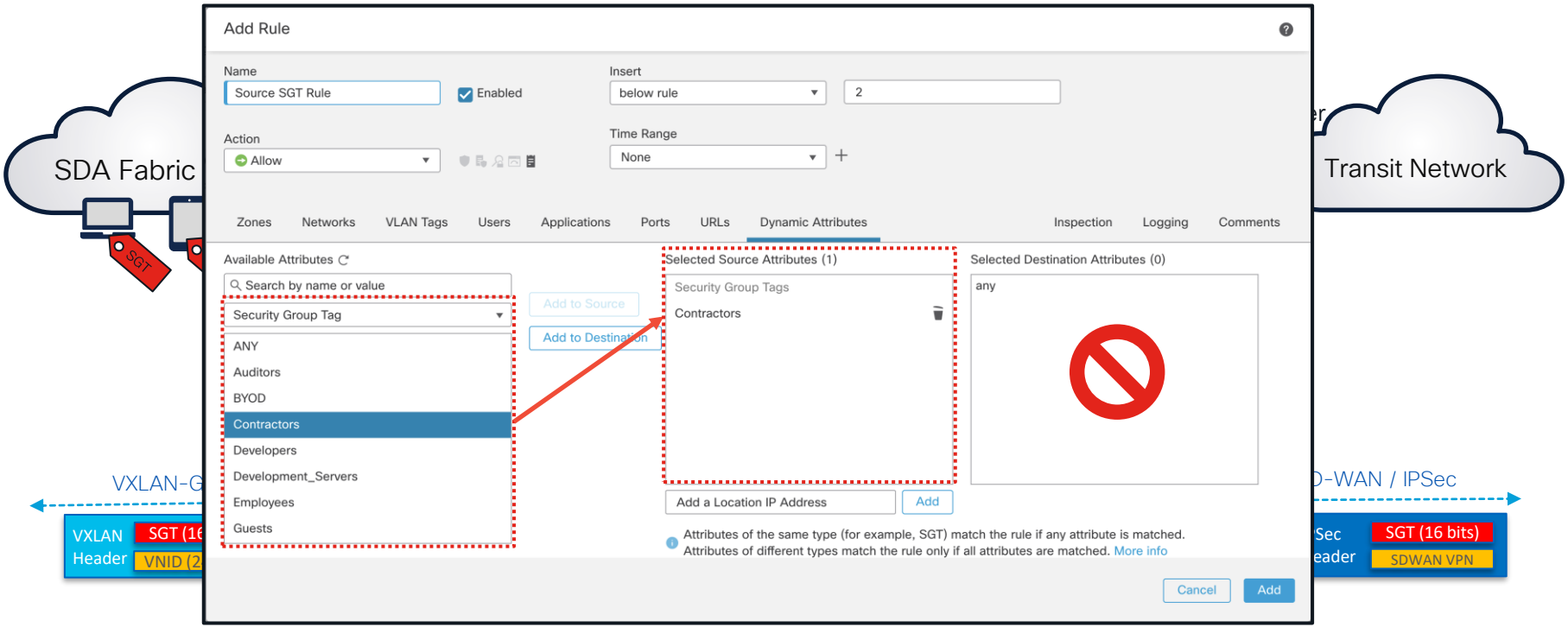
Attribute-Based Policy Dynamic Attribute Sources

Inline Propagation



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

Inline Propagation



Note: Inline SGTs applicable for source criteria only

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

Attribute Based Policy – Inline SGTs

#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)									
⌄ Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Printing Service	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	Corporate_VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_				HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_				Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

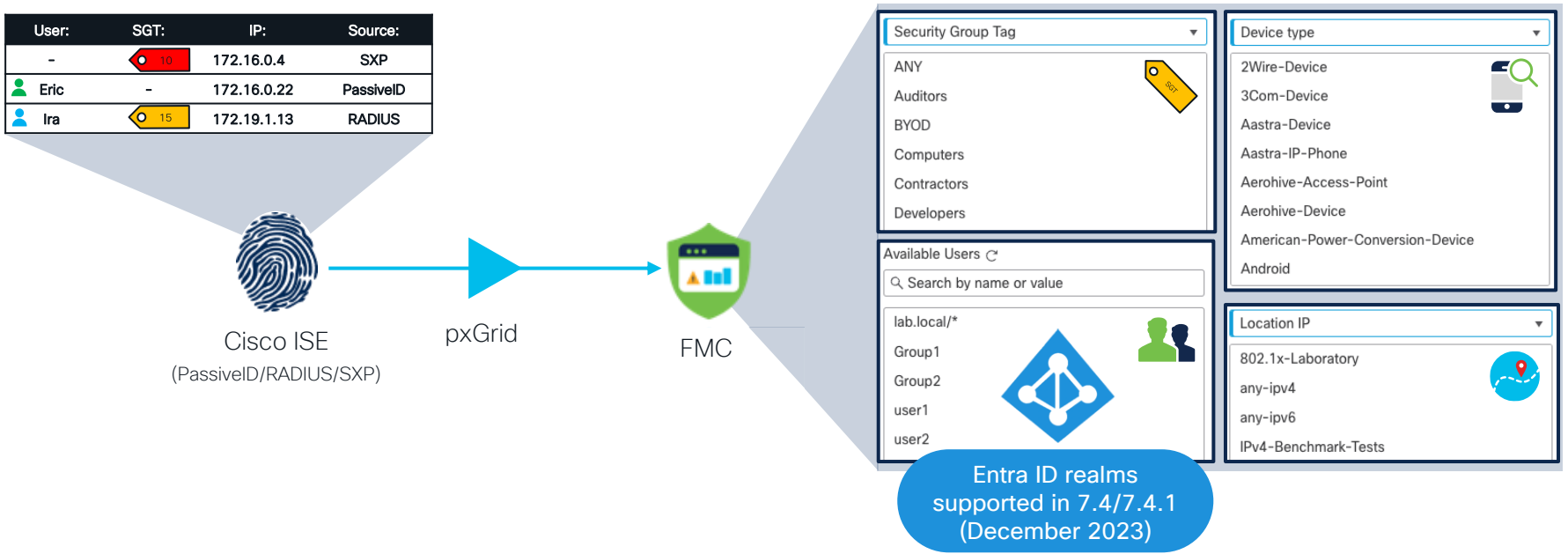
TrustSec inline propagated
Scalable Group Tags

Note: Inline SGTs applicable for source criteria only

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

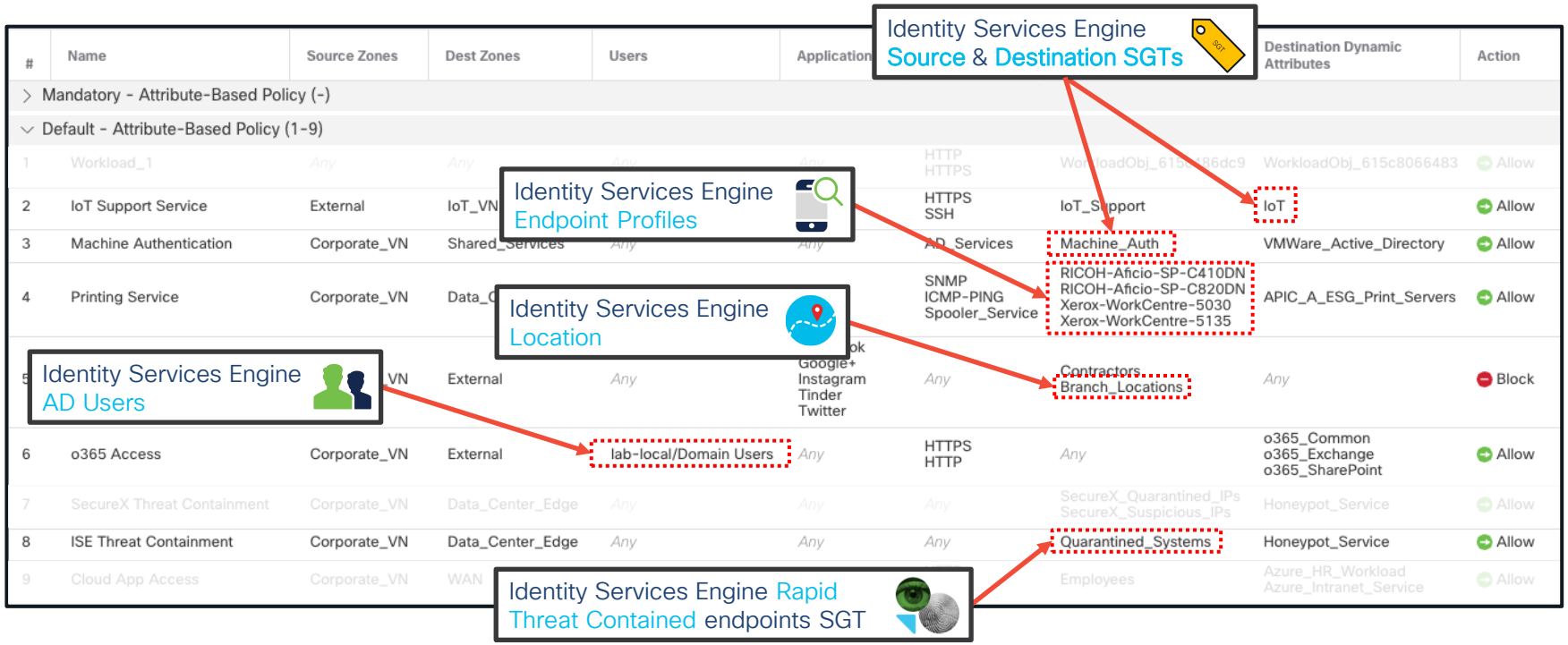
SGT Inline Propagation Through a Firewall Demo

Control Plane Propagation with pxGrid



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

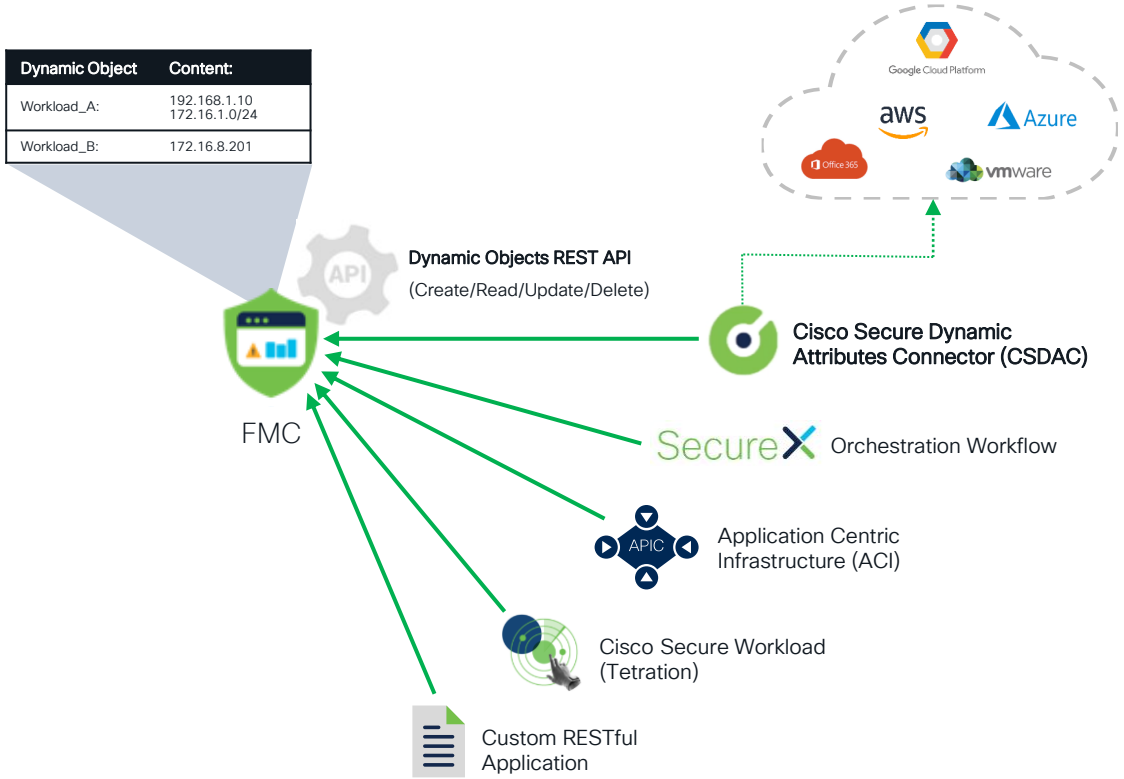
Attribute Based Policy – ISE Context Objects



#	Name	Source Zones	Dest Zones	Users	Application	Service	Destination Dynamic Attributes	Action
Mandatory - Attribute-Based Policy (-)								
Default - Attribute-Based Policy (1-9)								
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Printing Service	Corporate_VN	Data_C	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5		VN	External	Any	ok Google+ Instagram Tinder Twitter	Any	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN				Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

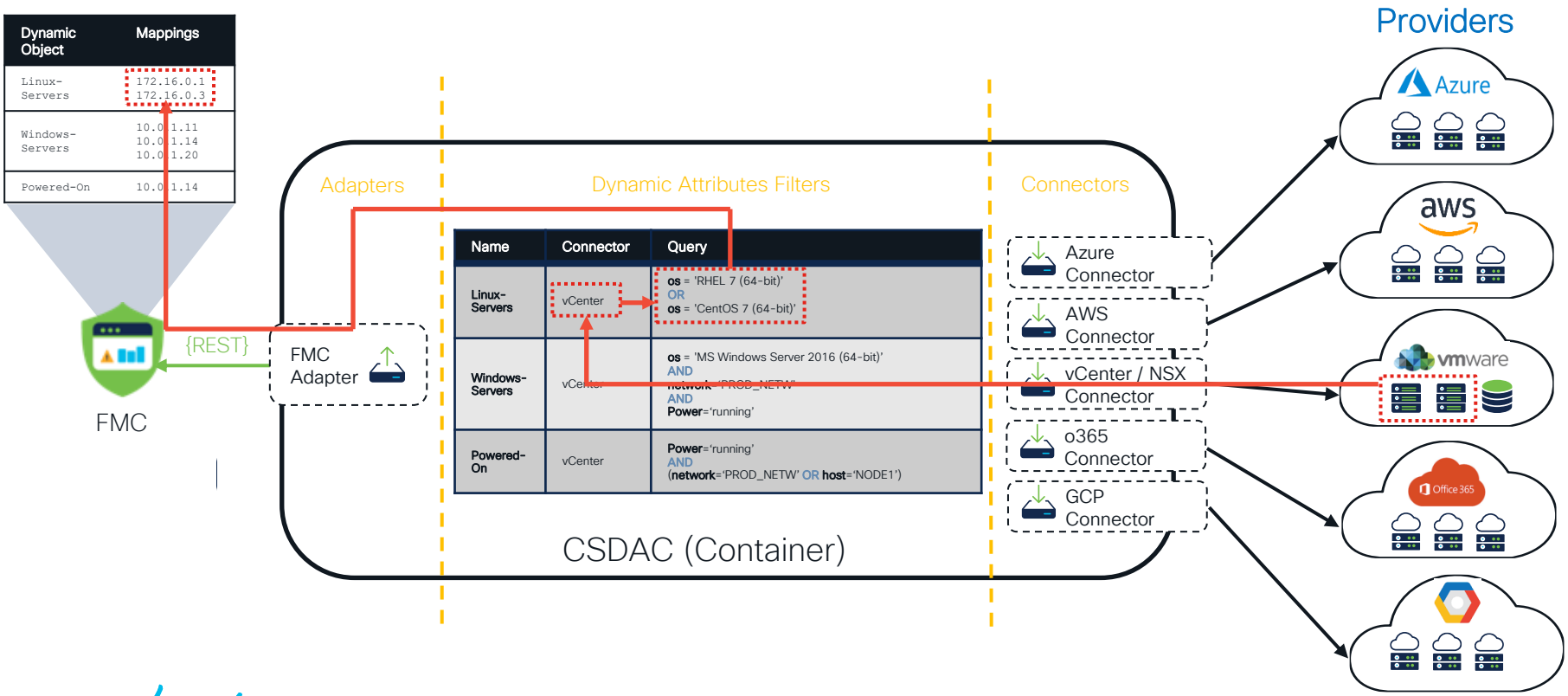
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Plane Propagation with Dynamic Objects



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

Architecture of the Dynamic Attributes Connector



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

Attribute Based Policy – CSDAC Attributes

#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)									
⌄ Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Printing Service	Corporate_VN	Data_Center_Edge	Any	Any	SNMP -PING ler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	Corporate_VN	External	Any	Any Instagram Tinder Twitter		Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any		SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any		Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

vCenter / NSX Dynamic Objects

o365 Public Feeds

Public Cloud Tags

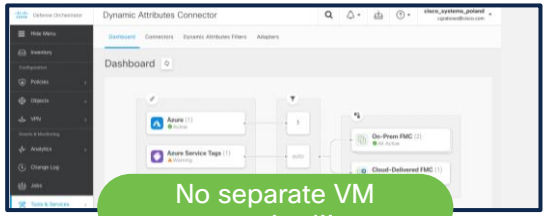
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

CSDAC Demo

The New Cloud Form Factor

CDO

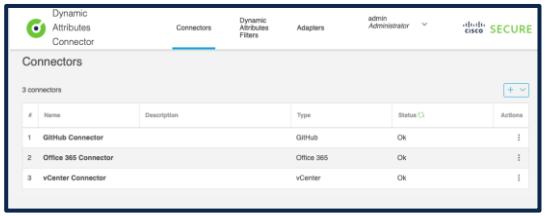
CSDAC in CDO's Tools & Services



No separate VM required!!

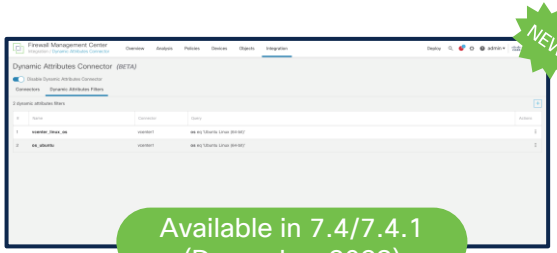
Cloud Delivered

CSDAC (Linux Machine)



Standalone

CSDAC in FMC



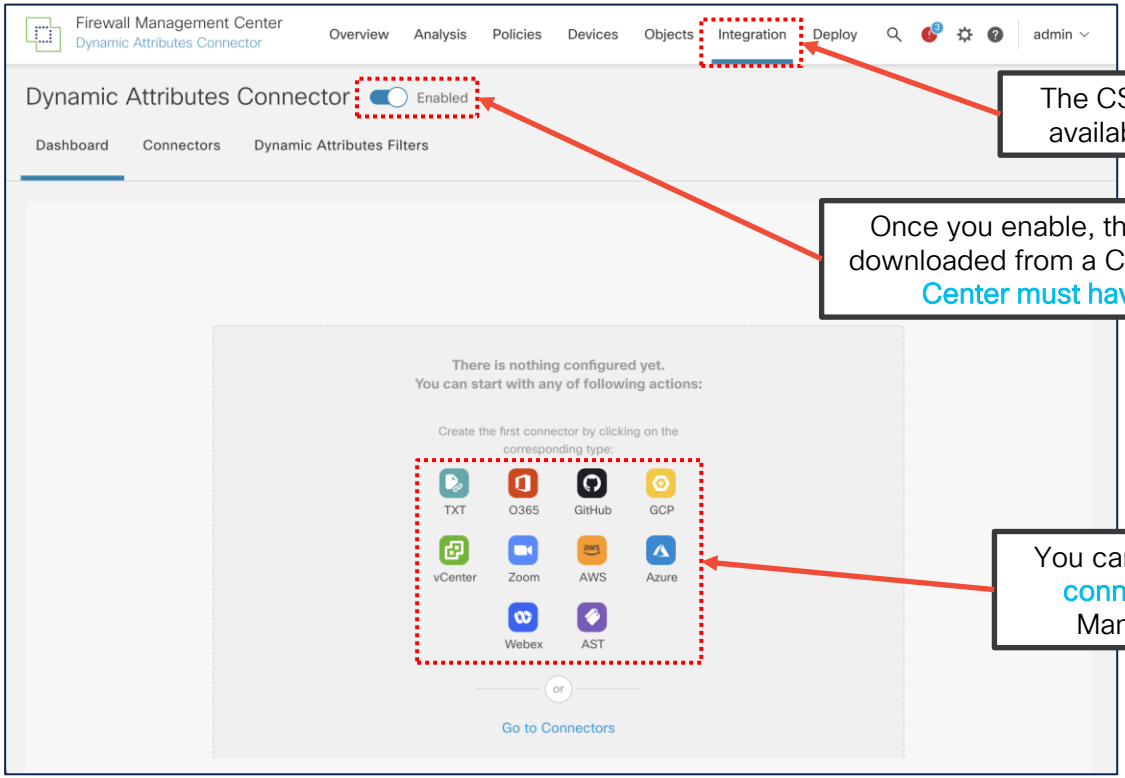
Available in 7.4/7.4.1 (December 2023)

Built In

(FMC HA Supported)

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

CSDAC is Now In the Firewall Management Center



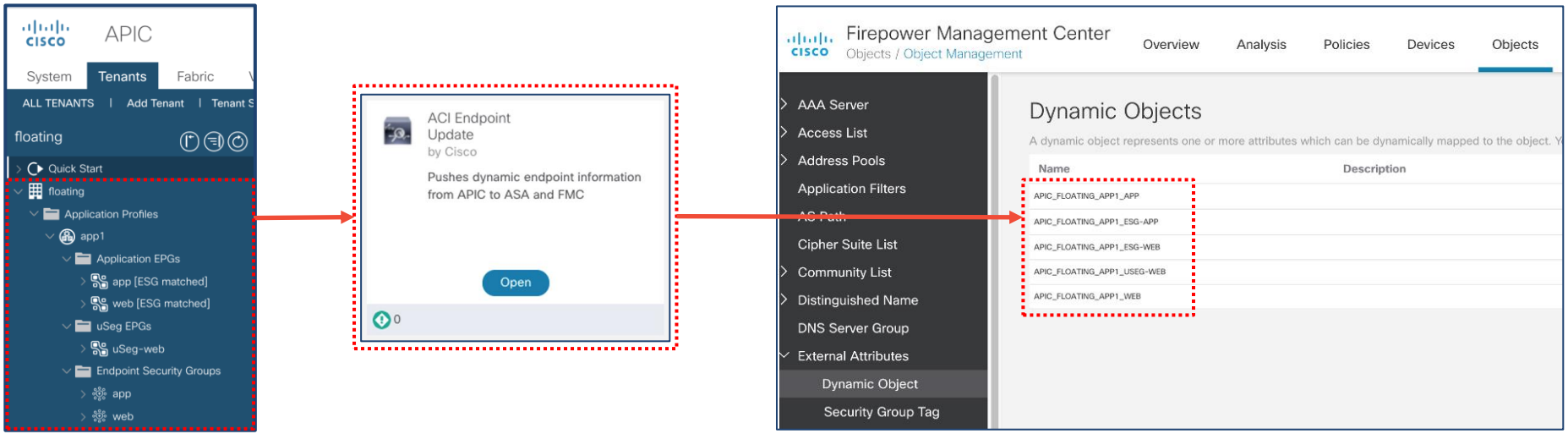
The CSDAC configuration dialog is available under Integration menu.

Once you enable, the latest CSDAC images are downloaded from a Cisco repository. Management Center must have Internet connectivity.

You can configure between 10-30 connectors, depending on the Management Center model.

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

ACI Endpoint Update App 2.0



ACI Endpoint Update App is Compatible with FMC 6.7 and above:

- With FP 7.0+, use Dynamic Objects – no Deployment Needed
- With FP 6.7, use Network Group Objects – Deployment Required

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

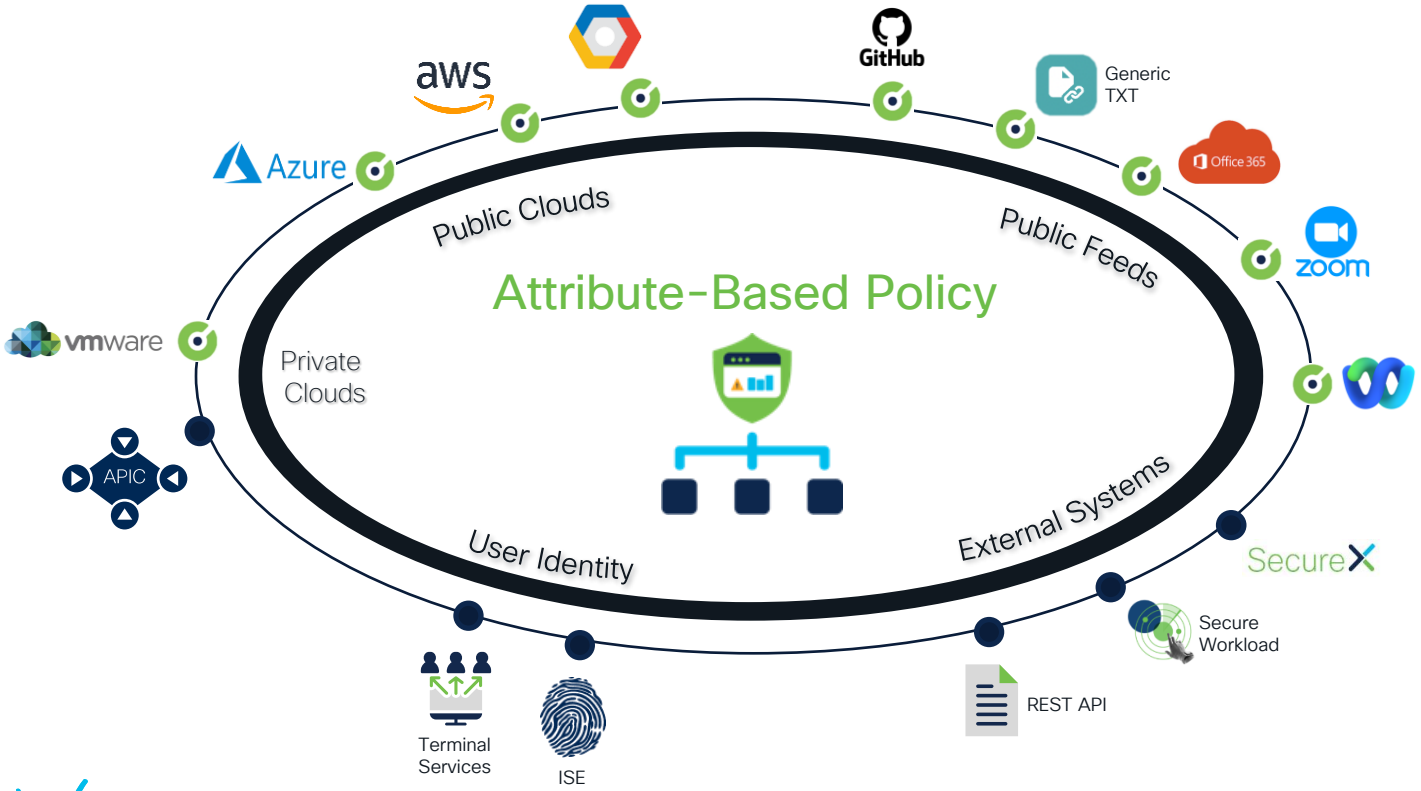
Attribute Based Policy – ACI EPG and ESG

#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)									
⌄ Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Printing Service	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	Corporate_VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_common o365_exchange	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any			
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	HoneyPot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

ACI Endpoint Groups (EPG) and Endpoint Security Group (ESG)

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

Attribute-Base Policy makes your firewall rules dynamic, more secure and easier to manage

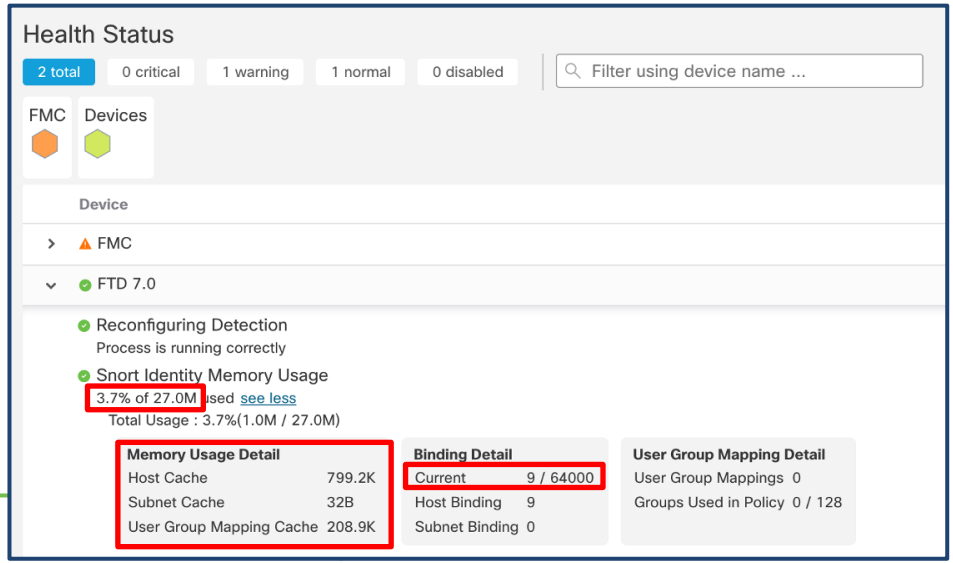


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling Firewall Identity Mappings

FMC Model	Maximum Recommended Users (Snort2) ★
FMC1000, FMC1600	50,000
FMC2500, FMC2600	150,000
FMC4500, FMC 4600	600,000
FMCv	50,000
FMCv 300	150,000

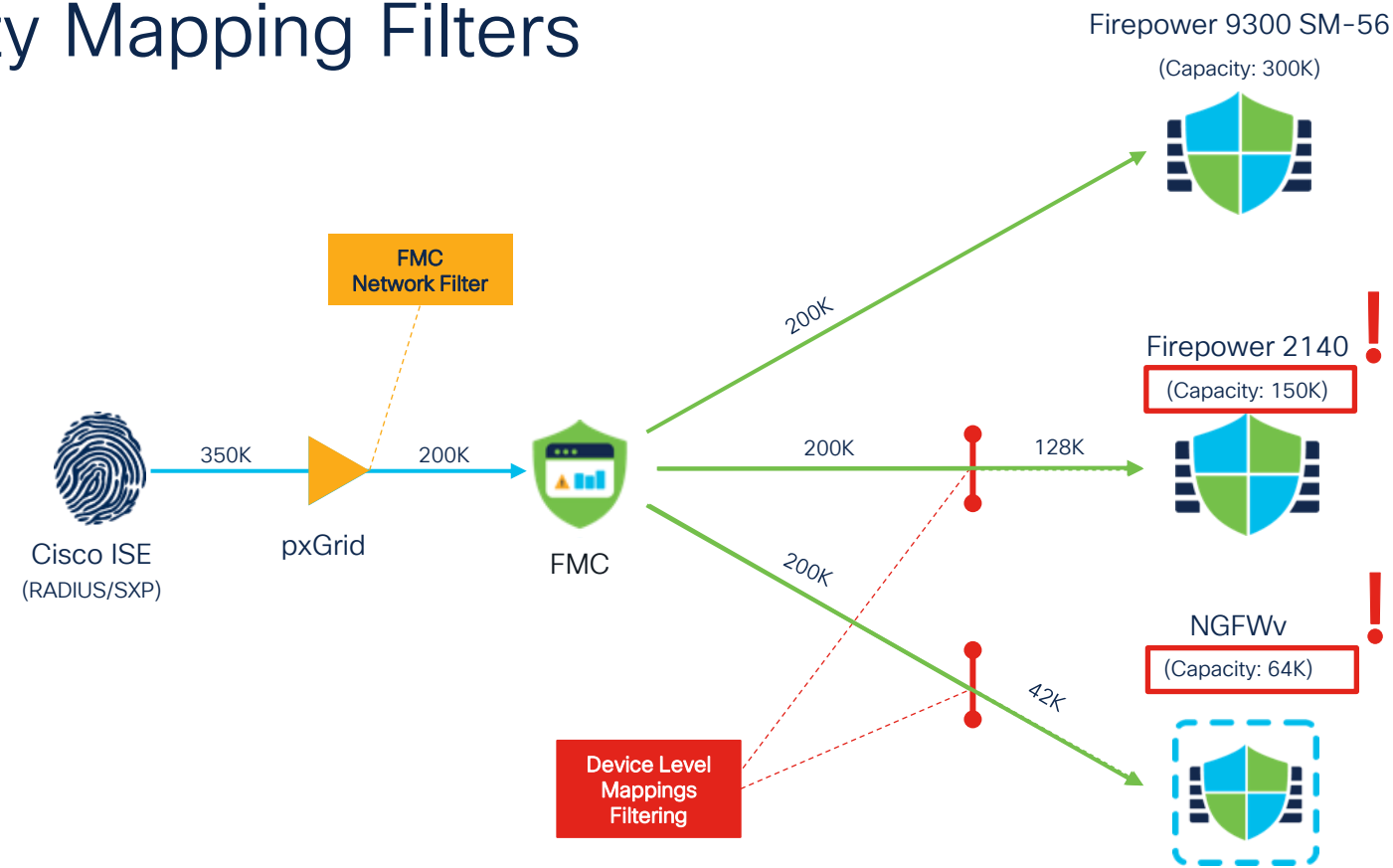
FMC



Managed Device

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

Identity Mapping Filters



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

Identity Propagation Practical Use-Cases

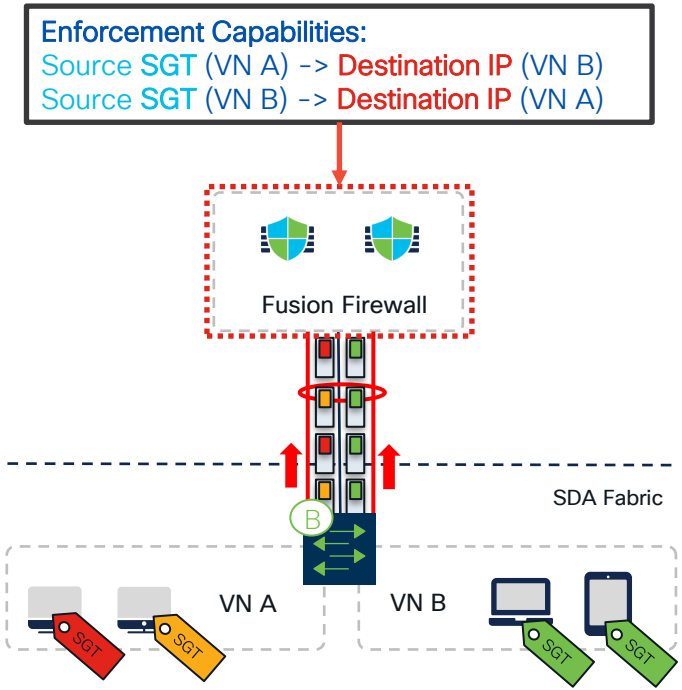
Inter-VN Attribute Based Policy
(Inline Tagging)

Key Benefits

- Scalable Inter-VN policies with source SGT criteria only
- pxGrid integration not mandatory
- Straight forward design with firewall as an SDA fusion device

Scaling Considerations

- SGT information provided inline – no Identity Memory utilization
- Endpoint count unbounded by FMC/Firewall capacity



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

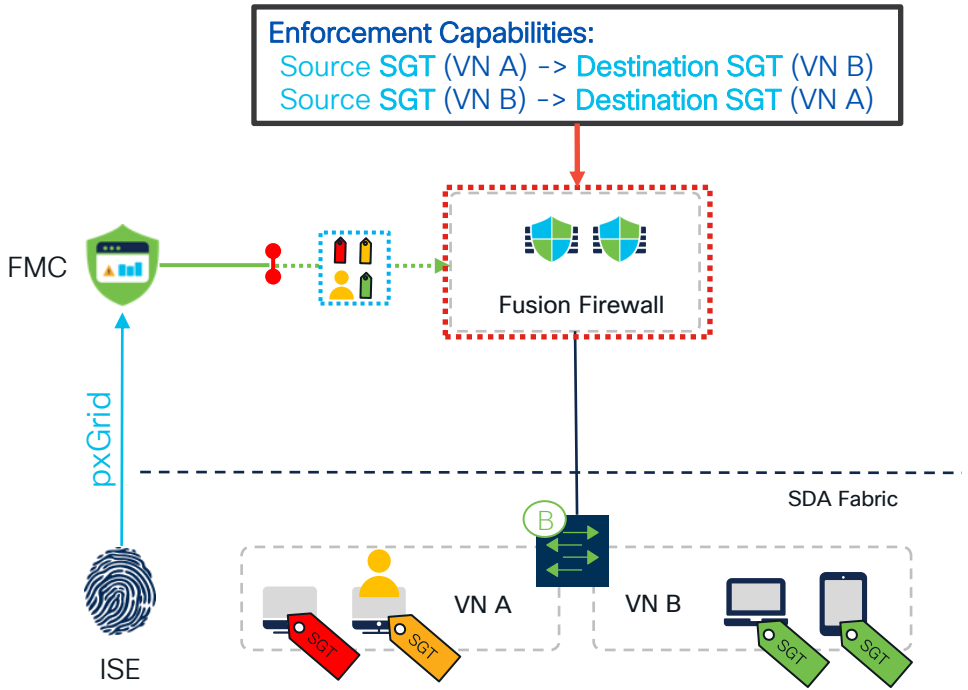
Inter-VN Attribute Based Policy
(Control Plane Propagation)

Key Benefits

- Flexible Attribute-Based Inter-VN policy
- Identity attributes applicable in any direction
- Policy based of any combination of source/destination SGTs, User Groups and Dynamic Attributes

Scaling Considerations

- Management Center must support cumulative endpoint binding for the entire network
- Use Device Level Filters to filter out remote endpoint bindings with Mapping Filters if not used in the firewall policy
- Firewalls must support endpoint binding count in each site



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

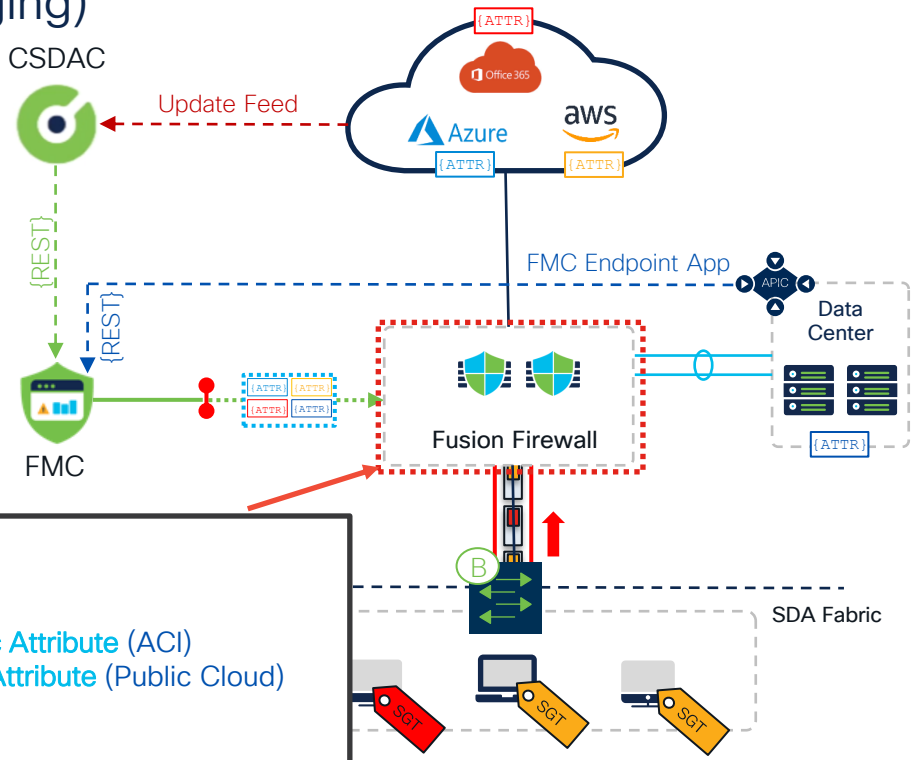
DC/Cloud Access Attribute Based Policy
(Control Plane Propagation & Inline Tagging)

Key Benefits

- Extremely scalable Attribute-Based policy for user to DC/Cloud
- User identity provided inline – no pxGrid integration

Scaling Considerations

- Minimal utilization of FMC/Firewall identity memory



Enforcement Strategy: Site Egress

Egress Enforcement Capabilities:
Source SGT (SDA) -> EPG/ESG Dynamic Attribute (ACI)
Source SGT (SDA) -> CSDAC Dynamic Attribute (Public Cloud)

Ingress Enforcement Capabilities:
EPG/ESG Dynamic Attribute (ACI) -> Destination IP (SDA)
CSDAC Dynamic Attribute (Public Cloud) -> Destination IP (SDA)

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

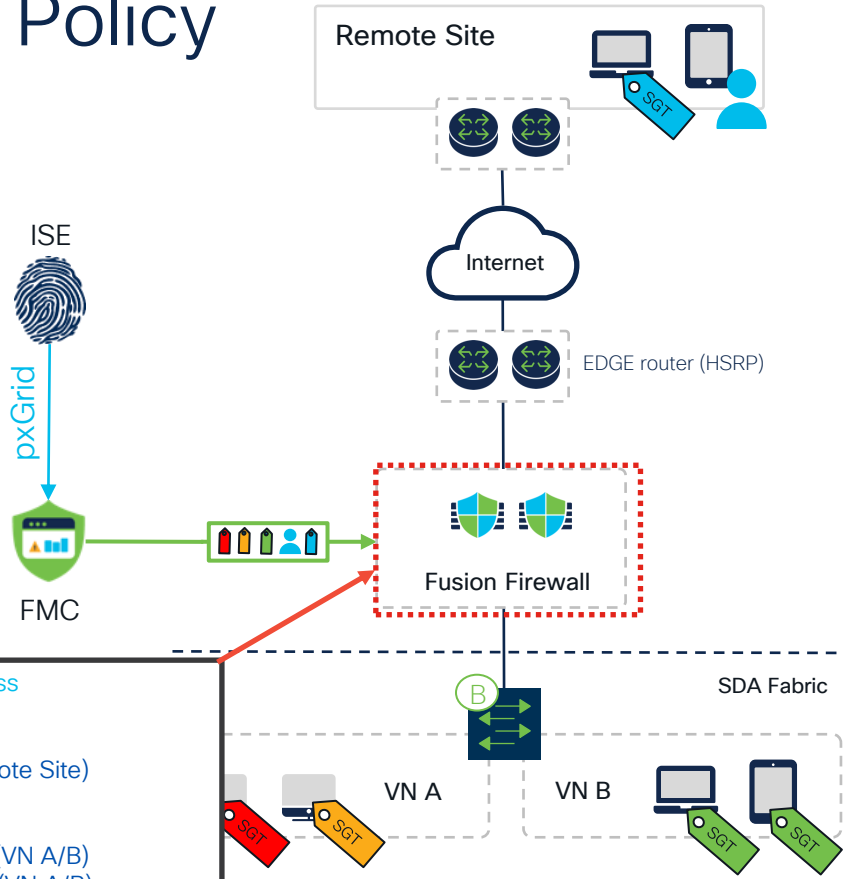
Inter-Site Attribute Based Policy
(Control Plane Propagation)

Key Benefits

- Identity attributes applicable in any direction
- No inline propagation dependencies – flexible firewall insertion design

Scaling Considerations

- Firewall learns bindings of all endpoints in the network
- Consider FMC/Firewall with capacity supporting cumulative global endpoint count and dynamic attributes



Enforcement Strategy: Site Ingress or Site Egress

Egress Enforcement Capabilities:
Source SGT (VN A/B) -> Destination SGT (Remote Site)

Ingress Enforcement Capabilities:
Source SGT (Remote Site) -> Destination SGT (VN A/B)
Source User (Remote Site) -> Destination SGT (VN A/B)

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

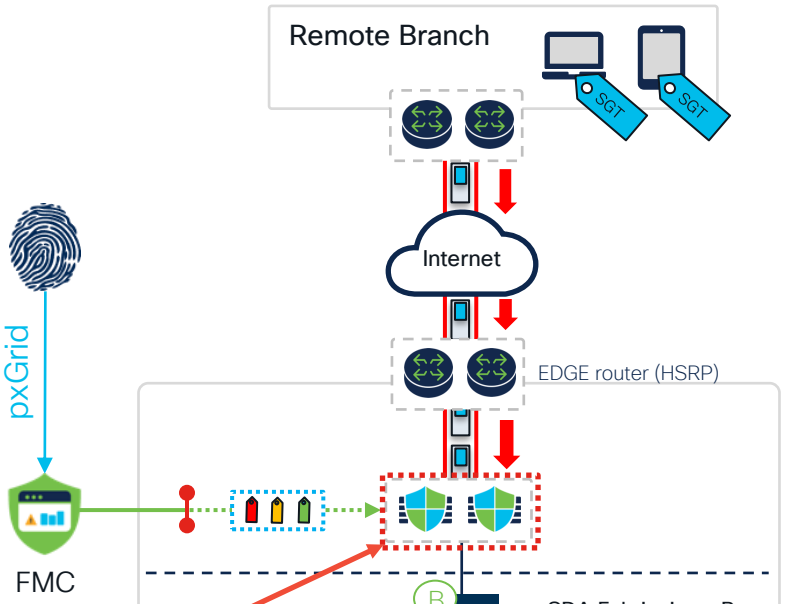
Scalable Branch-to-Branch
(Control Plane Propagation & Inline Tagging)

Key Benefits

- Scalable branch Attribute-Based policy design
- Security policy enforced in the destination site

Scaling Considerations

- Firewalls learn bindings of endpoints in their local sites only
- Filter out non-local bindings with Mapping Filters
- Remote bindings provided inline – SGT propagation over WAN/IPSec required
- FMC must support global endpoint count



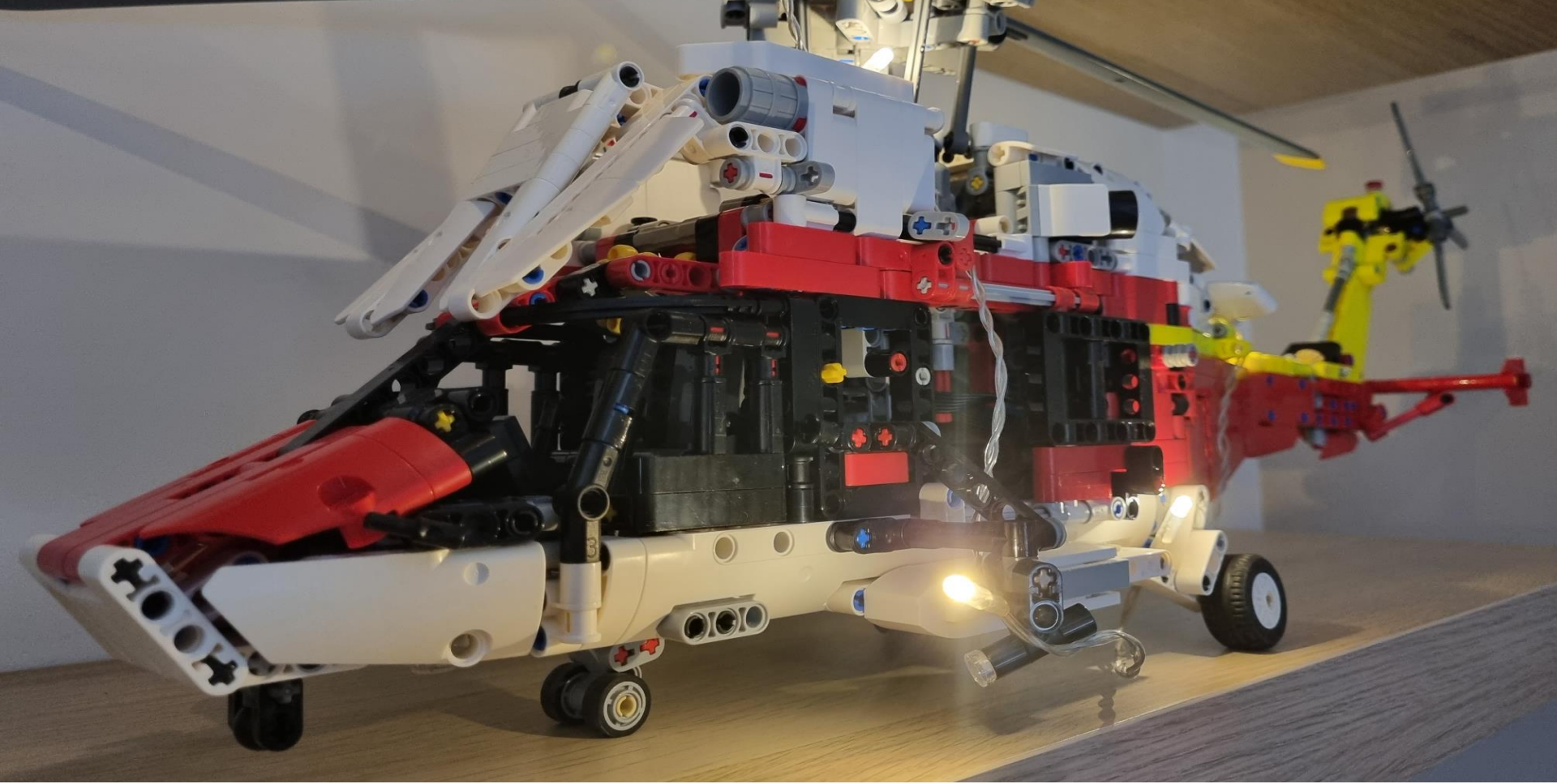
Enforcement Strategy: Site Ingress

Ingress Enforcement Capabilities:
Source SGT (Remote Branch) -> Destination SGT (SDA FiaB)

Egress Enforcement Capabilities:
Source SGT (SDA FiaB) -> Destination IP (Remote Branch)

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

Conclusions



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

Cisco Secure Firewall provides a comprehensive integration with SDA

- Consider benefits of VRF, Multi-Instance and Multi-Domain firewall virtualization options and choose optimum attachment model.
- Add your Firewall Management Center to the DNAC's inventory – it's super easy!
- After this session think how you can make your firewall policy dynamic, more secure and easier to manage with CSDAC and Attribute-Based Policy.
- Review identity propagation techniques to make the most out of the available dynamic attributes.

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

Session Surveys

Please share your feedback on this session!

It is very important to me personally...

...and helps me build better content for you next time.

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

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

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

cisco Live!

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.

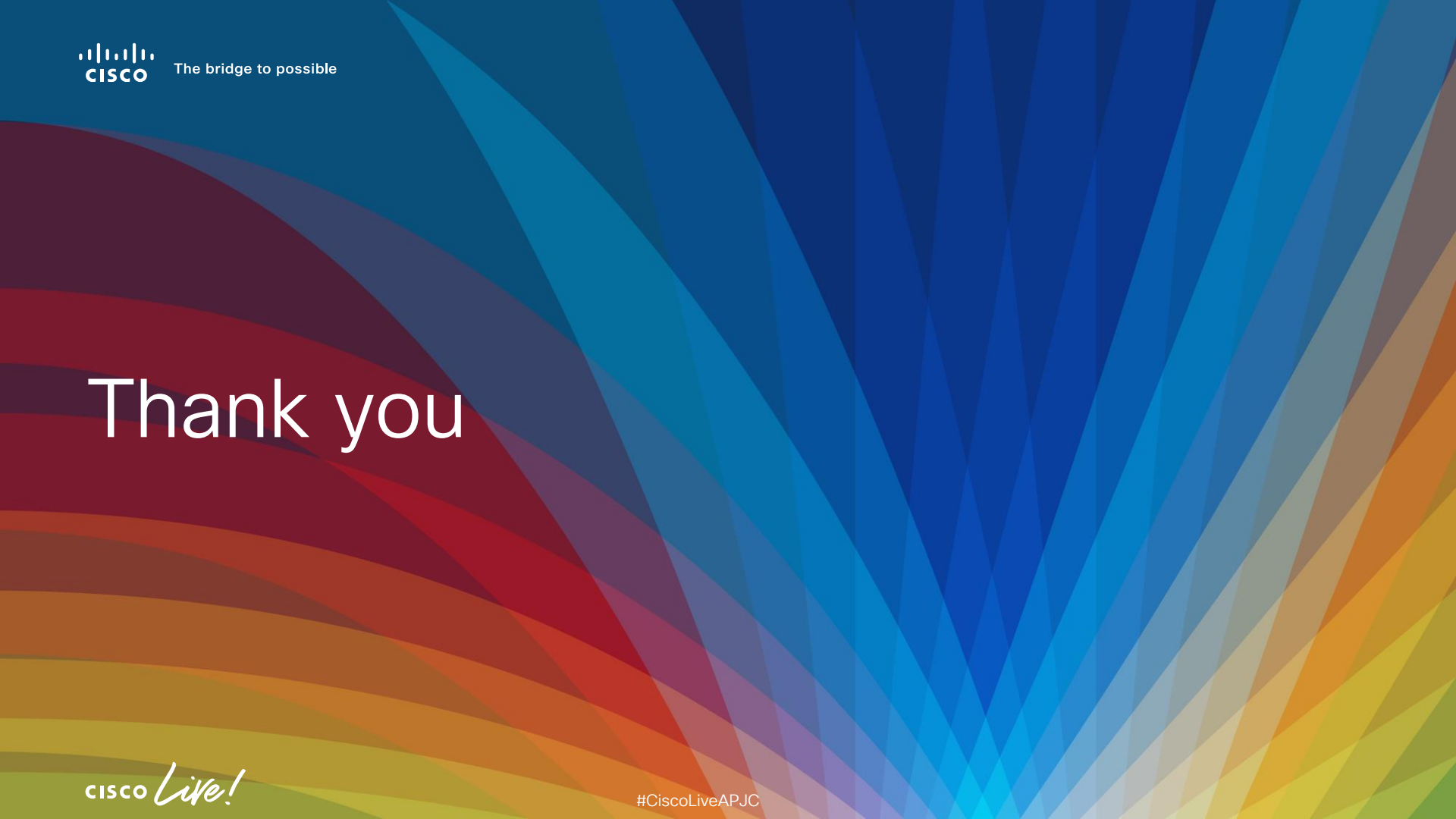
Meet the Expert Opening Hours:

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

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

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


cisco
The bridge to possible
Thank you
cisco Live!
#CiscoLiveAPJC

cisco Live!

Let's go

#CiscoLiveAPJC