

The Cisco Live! logo, featuring the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, script font.

CISCO *Live!*

The text "Let's go" in a large, dark blue, sans-serif font, positioned to the left of a bright, multi-colored sunburst graphic that radiates from the right side of the image.

Let's go

#CiscoLiveAPJC



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 *Live!*

#CiscoLiveAPJC

Cisco Webex App

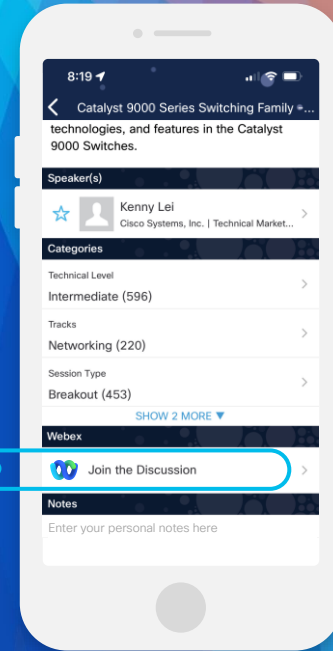
Questions?

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/#BRKSEC-2116>



Your Speaker



Christopher Grabowski
Technical Marketing Engineer
CCIE Security #42466

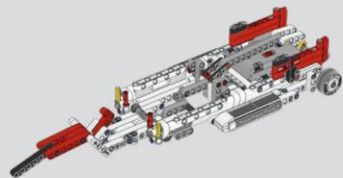
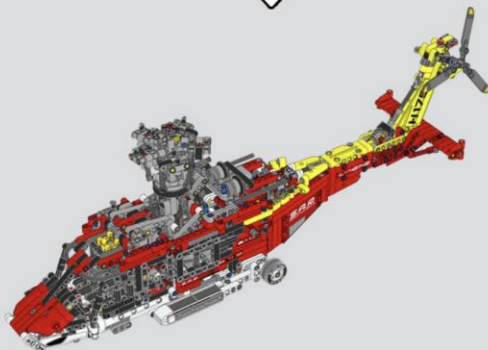
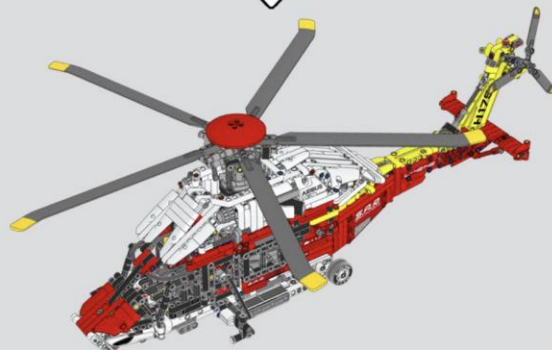
Based in Warsaw, Poland

With Cisco since May 2012

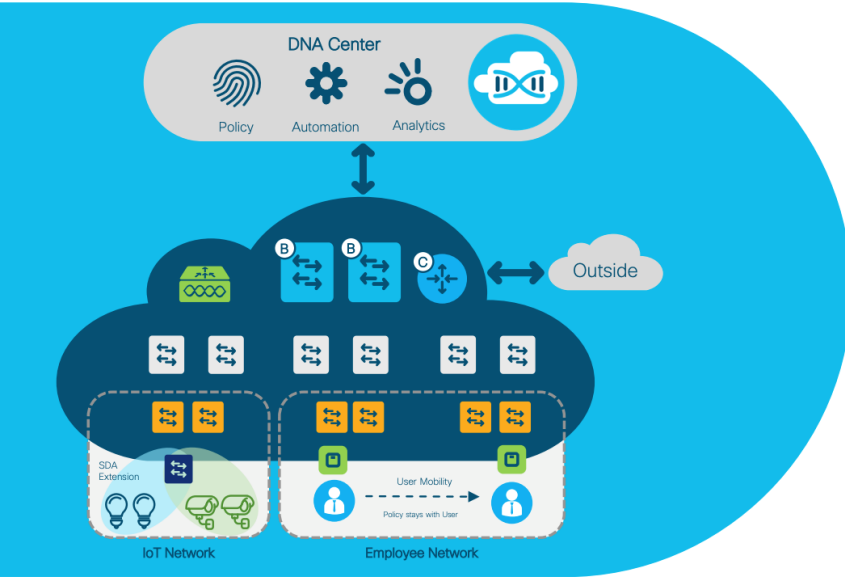
Started with TAC Security, then Advanced Services,
now Technical Marketing Engineer

Focusing on Identity Firewall, SDA/ACI
Integration, TLS Decryption

Enjoys cooking and spending time with the family



Cisco Secure Firewall provides a comprehensive integration with SDA



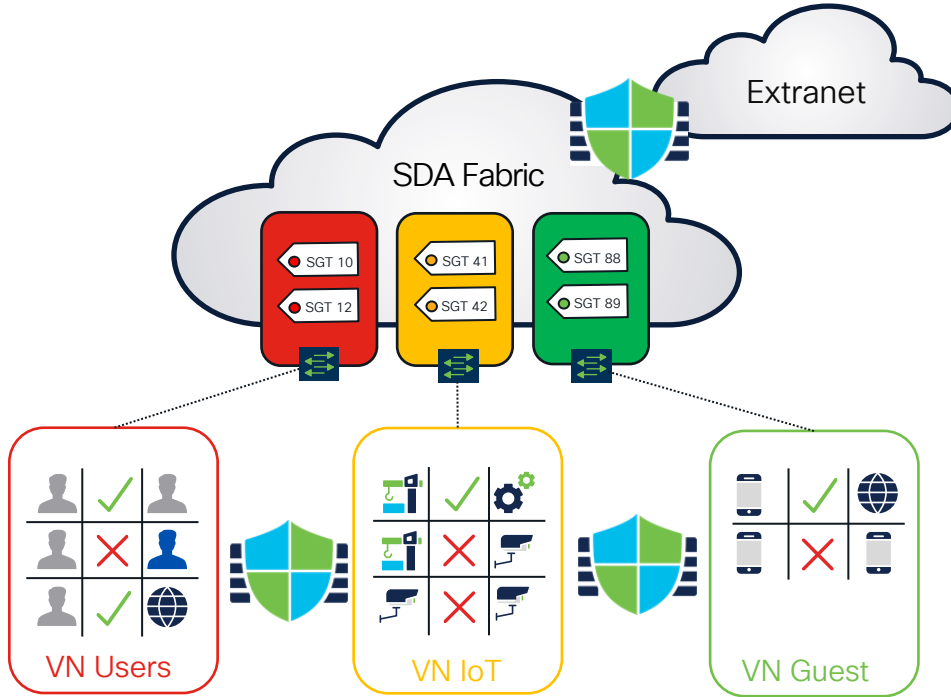
Agenda

- 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



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.

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 enforcement**

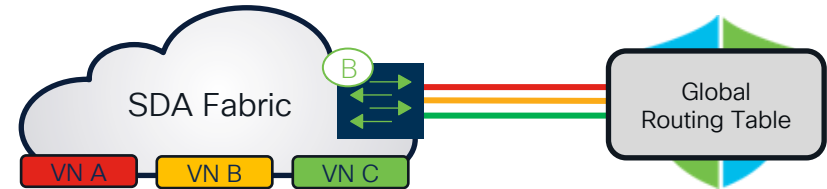


Firewall Deployment Modes and Virtualization Options

Firewall Deployment Modes – VN Separation

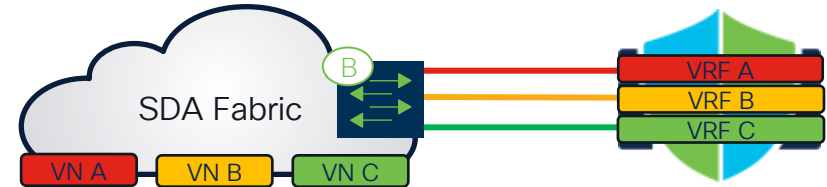
Non-VRF Aware

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



VN to VRF Mapping

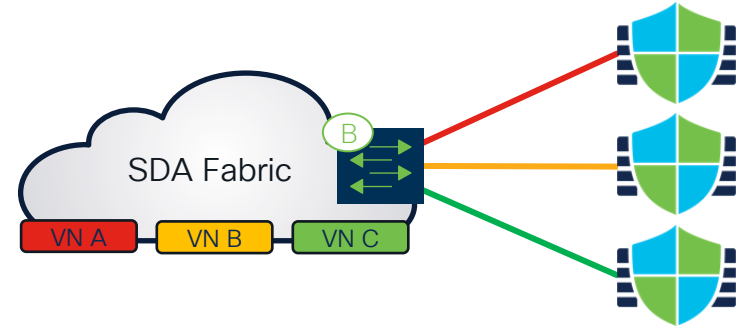
- **VN mapped to VRFs** on the firewall providing routing separation
- **Firewall leaks routes** between VNs, Shared Services and external
- Common firewall policy across VRFs on the firewall, with **VRF aware rules**.



Firewall Deployment Modes – VN Separation

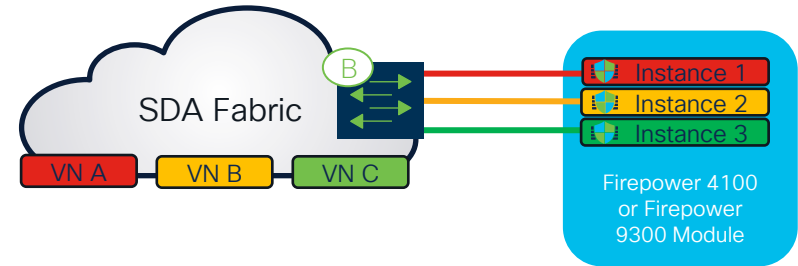
VN to Physical Device mapping

- 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

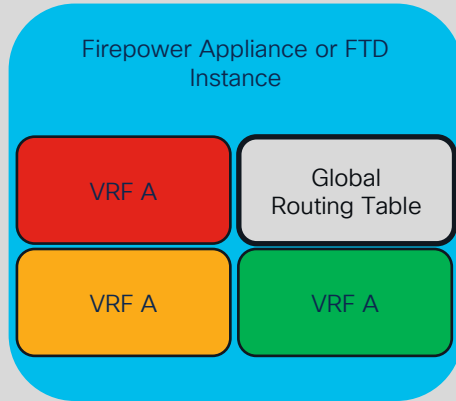
- Supported on Firepower 3100*/4100/9300
- Instantiate multiple logical devices on a single module or appliance
- Physical and logical separation between firewall instances on Supervisor level



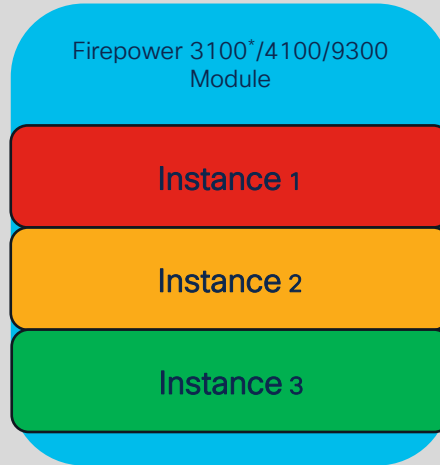
* – Coming in 7.4.1.

Cisco Secure Firewall Virtualization Options

Virtual Routers

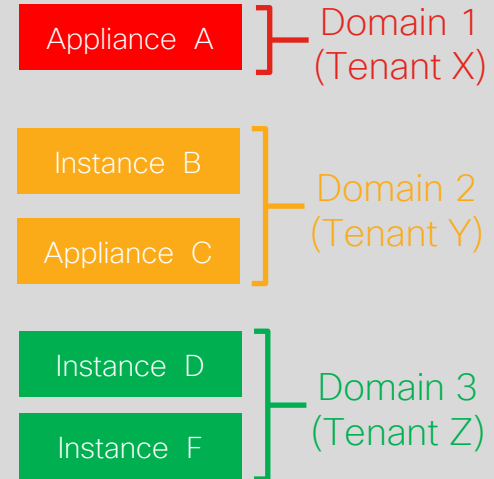


Multi-Instance



* - Coming in 7.4.1.

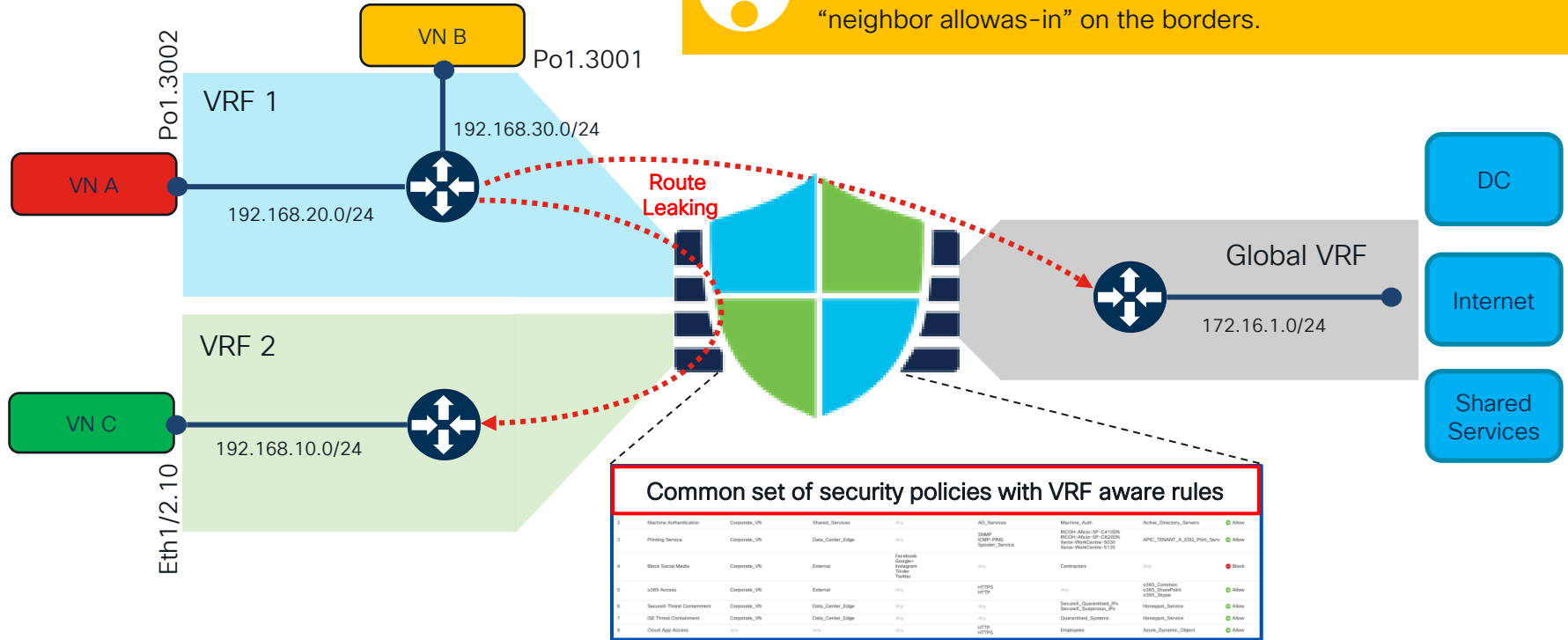
Multi-Domain



Virtual Router Basics

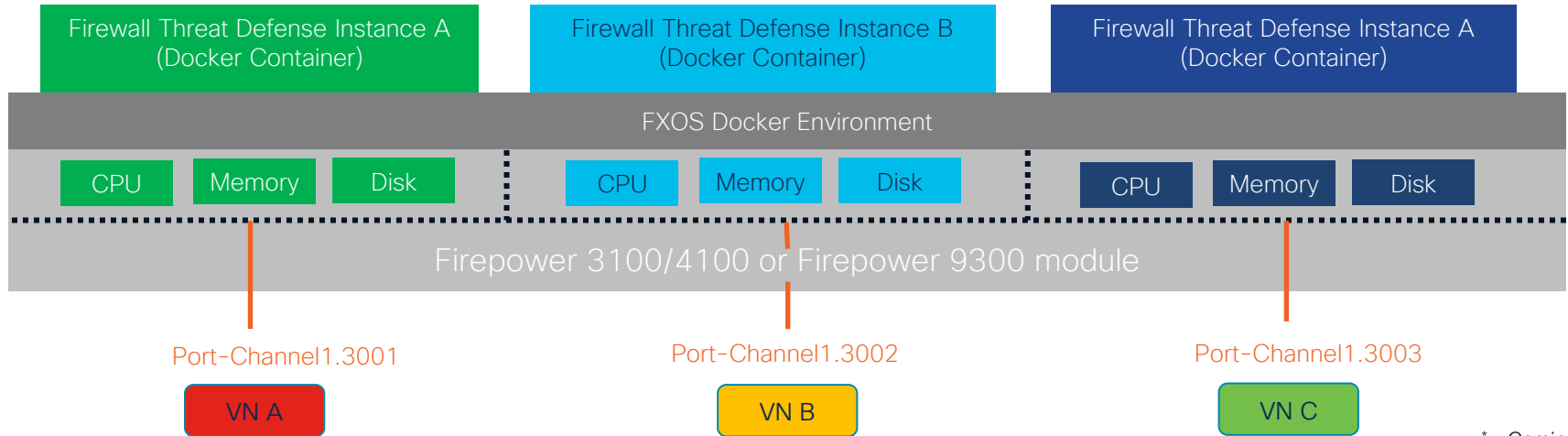


The firewall does not support BGP AS-override. When leaking routes between VNs sharing the same AS number, use “neighbor allowas-in” on the borders.



Firepower 3100/4100/9300 Multi-Instance

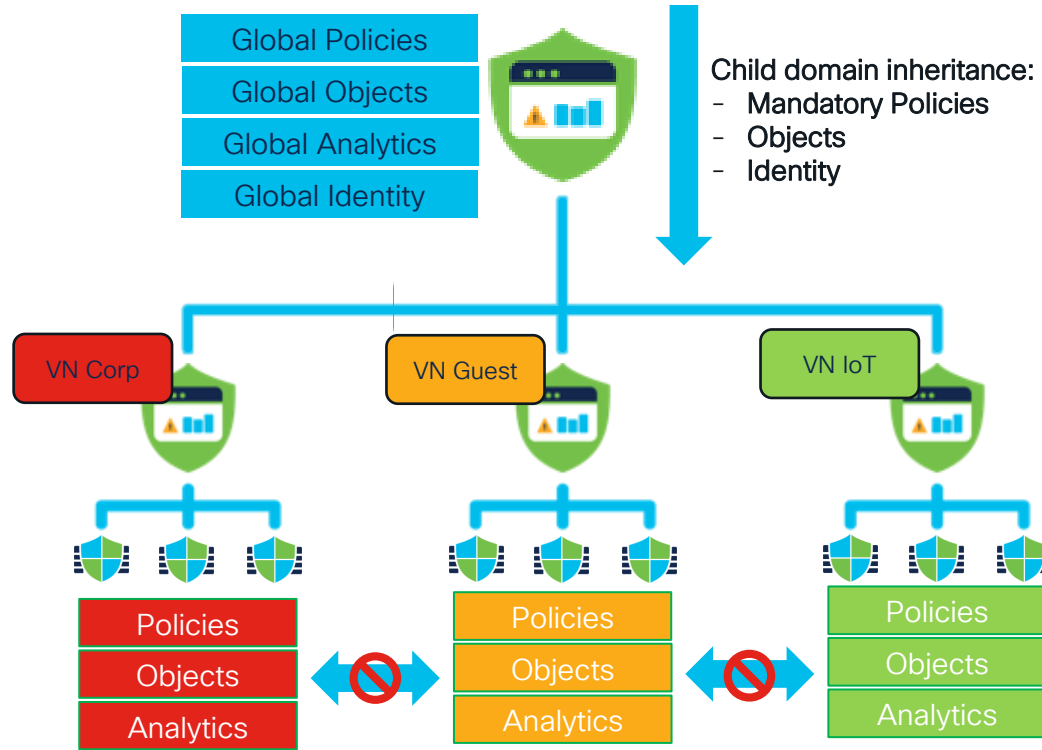
- Supported on Firepower 3100*/4100/9300
- Instantiate **multiple logical devices** on a single module or appliance
- **Complete traffic processing and management isolation** – physical and logical interface and VLAN separation at the Supervisor level



* – Coming in 7.4.1.

Supports up to 100 domains and 3 levels

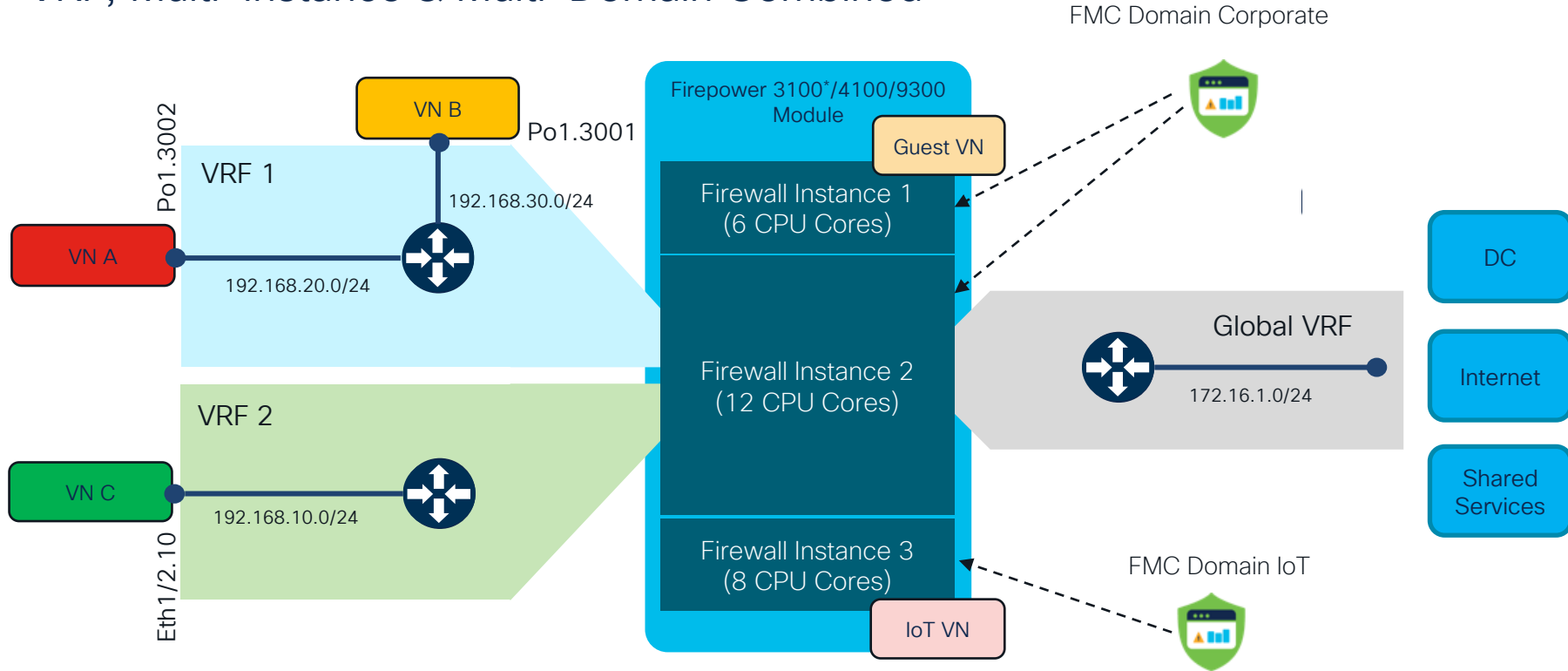
FMC Multi-Domain



Administration, Policy, Object and Eventing isolation

Putting it all together

VRF, Multi-Instance & Multi-Domain Combined

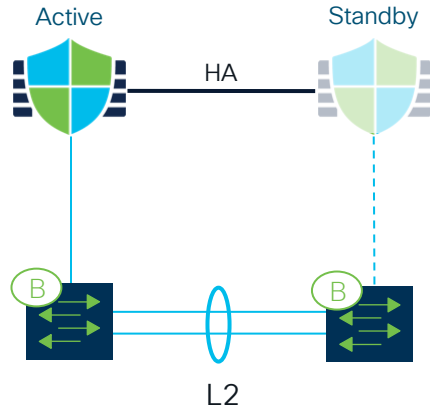
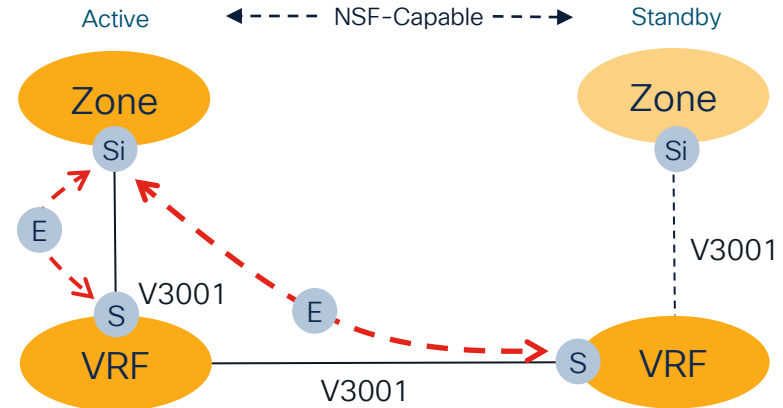


* - Coming in 7.4.1.

Cisco Secure Firewall SDA Attachment Options



Direct FTD Attachment



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

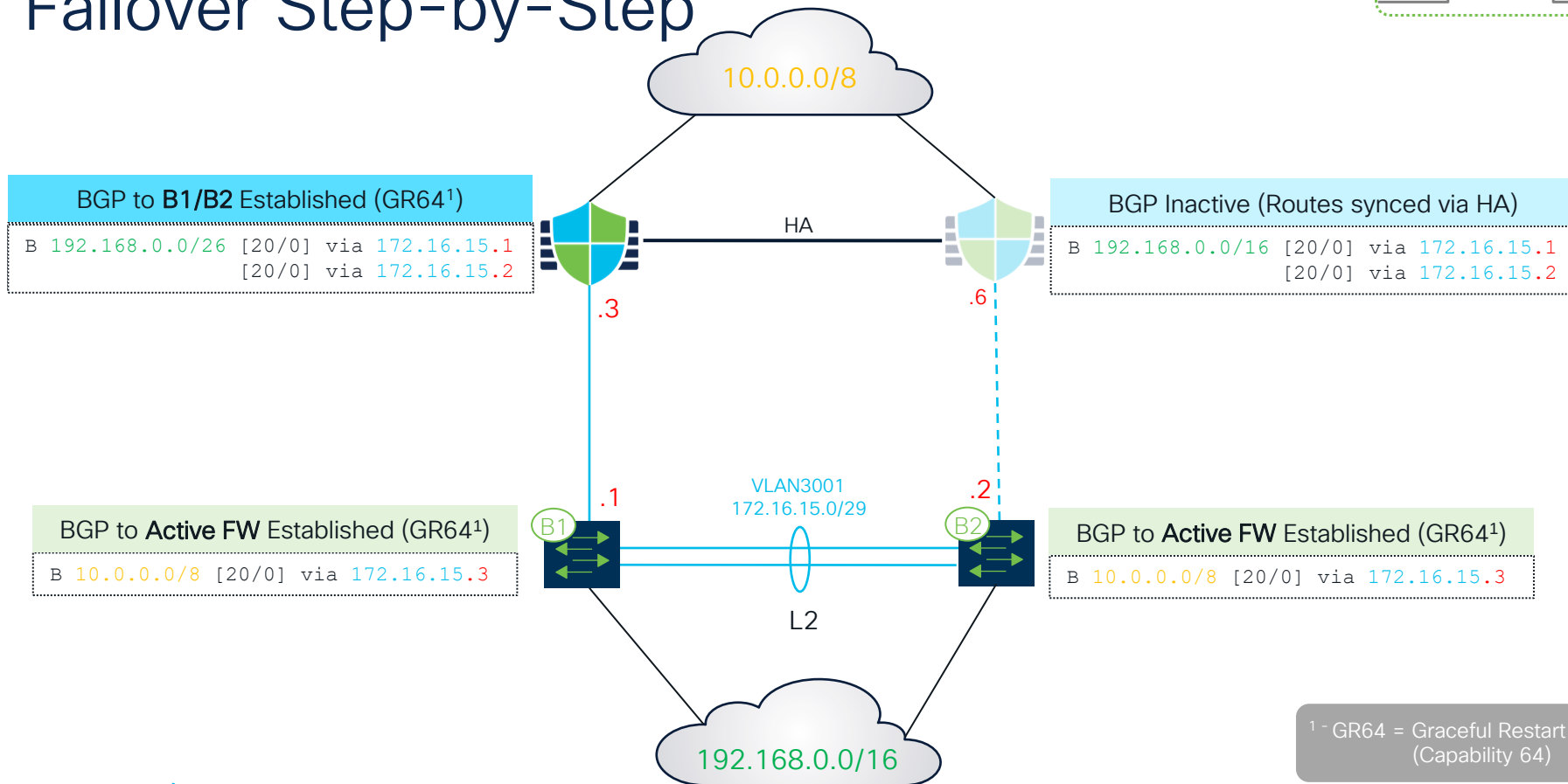
interface **Vlan3001**
vrf forwarding IOT
ip address **172.16.15.2/29**

- **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

Failover Step-by-Step

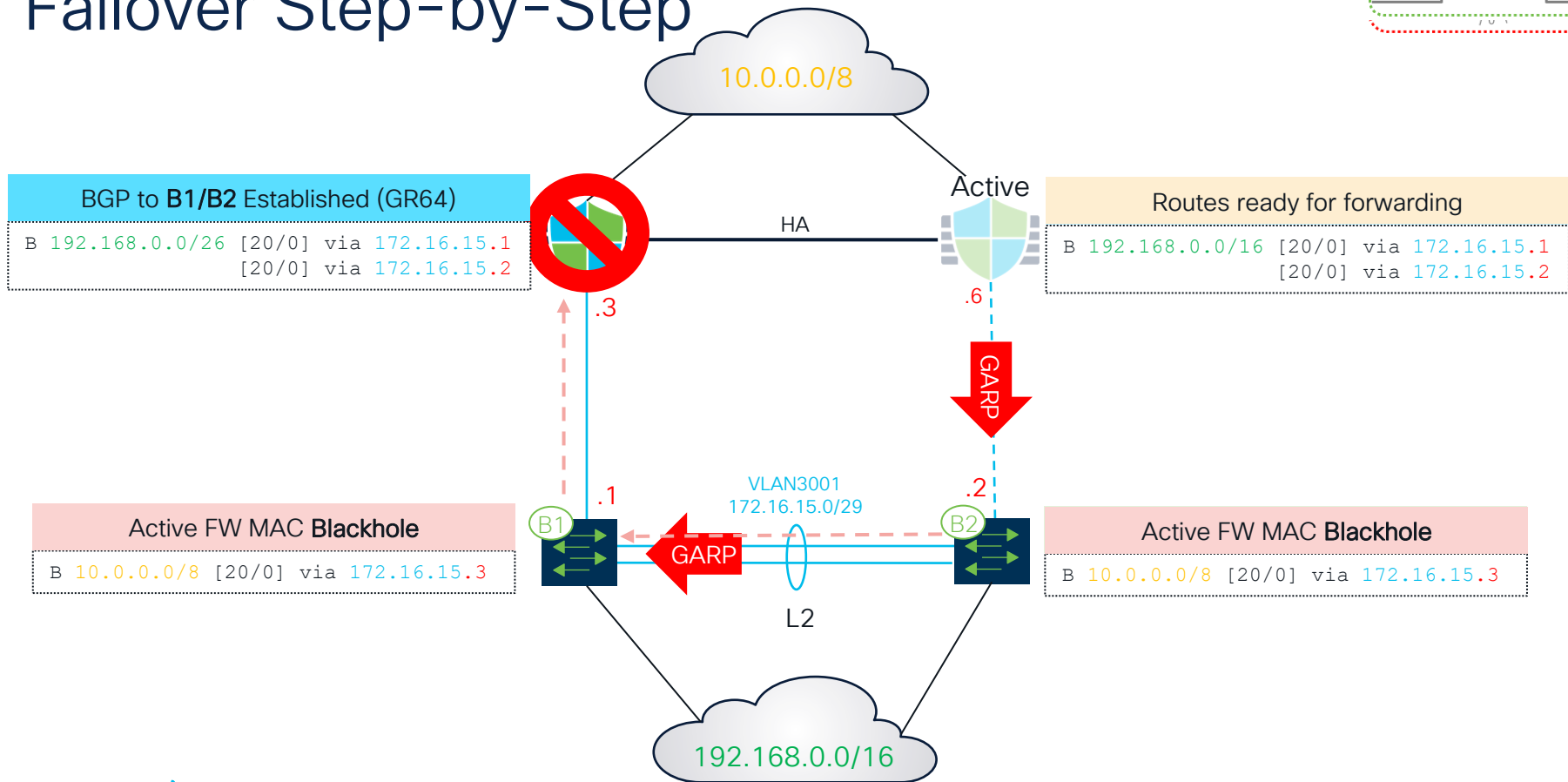
Full connectivity
10101 01101



¹ - GR64 = Graceful Restart
(Capability 64)

Failover Step-by-Step

Full connectivity
10101 01101



Full connectivity

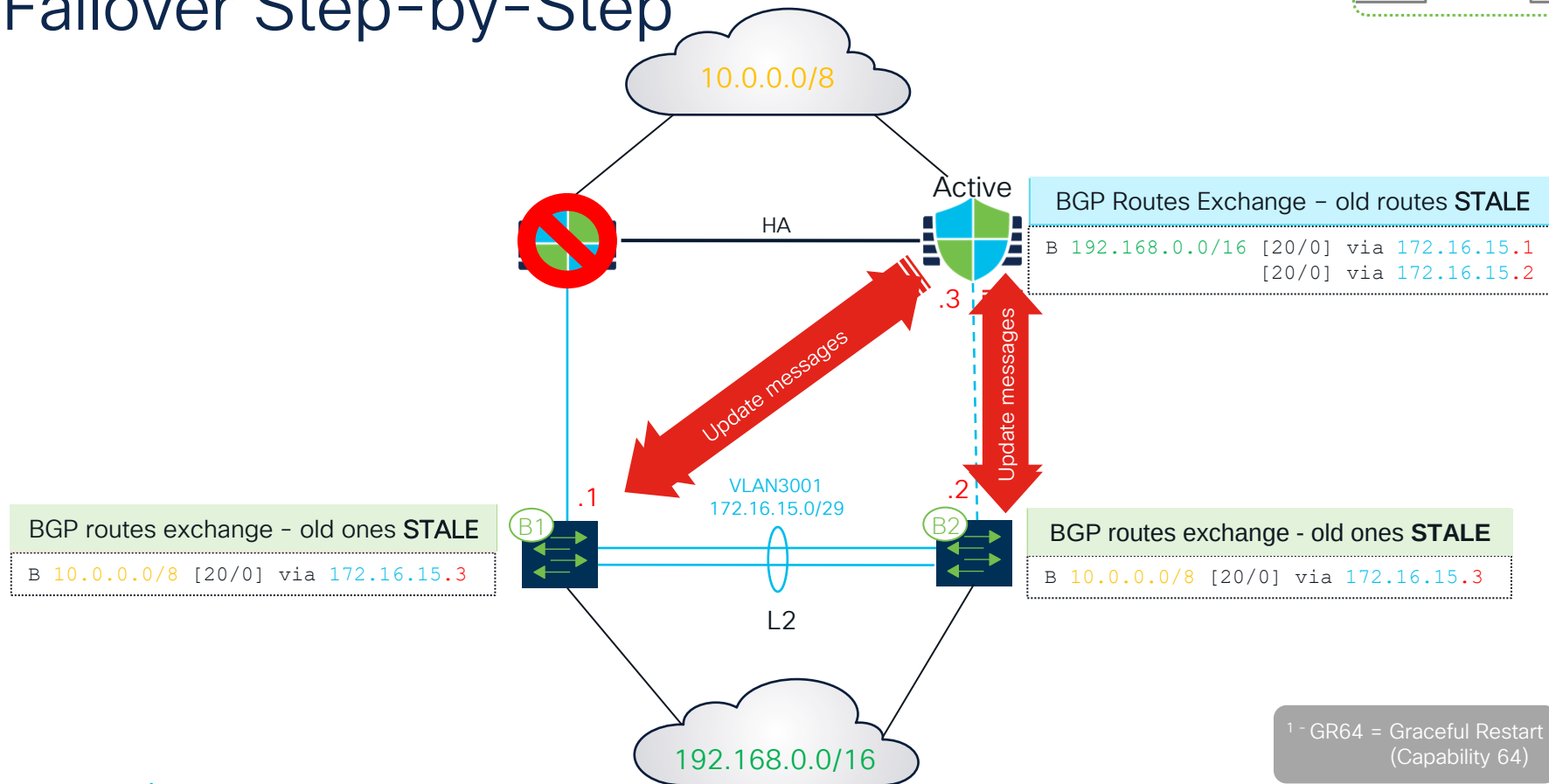
10101 01101

The diagram shows two nodes, each represented by a box containing a 5-bit binary string: '10101' on the left and '01101' on the right. Four horizontal lines connect every bit of the left node to every bit of the right node, illustrating a fully connected mesh topology.



Failover Step-by-Step

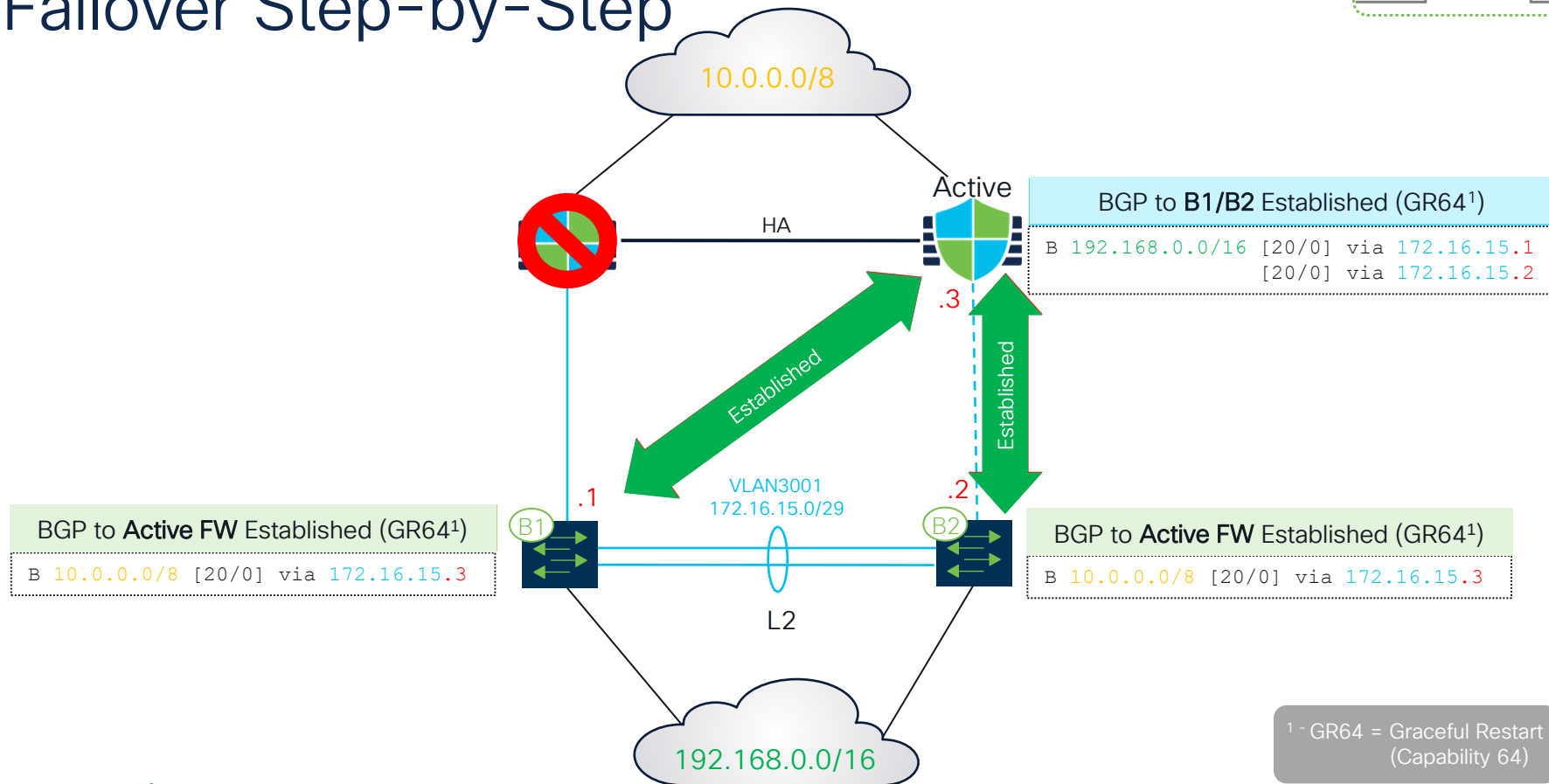
Full connectivity
10101 01101



¹ - GR64 = Graceful Restart
(Capability 64)

Failover Step-by-Step

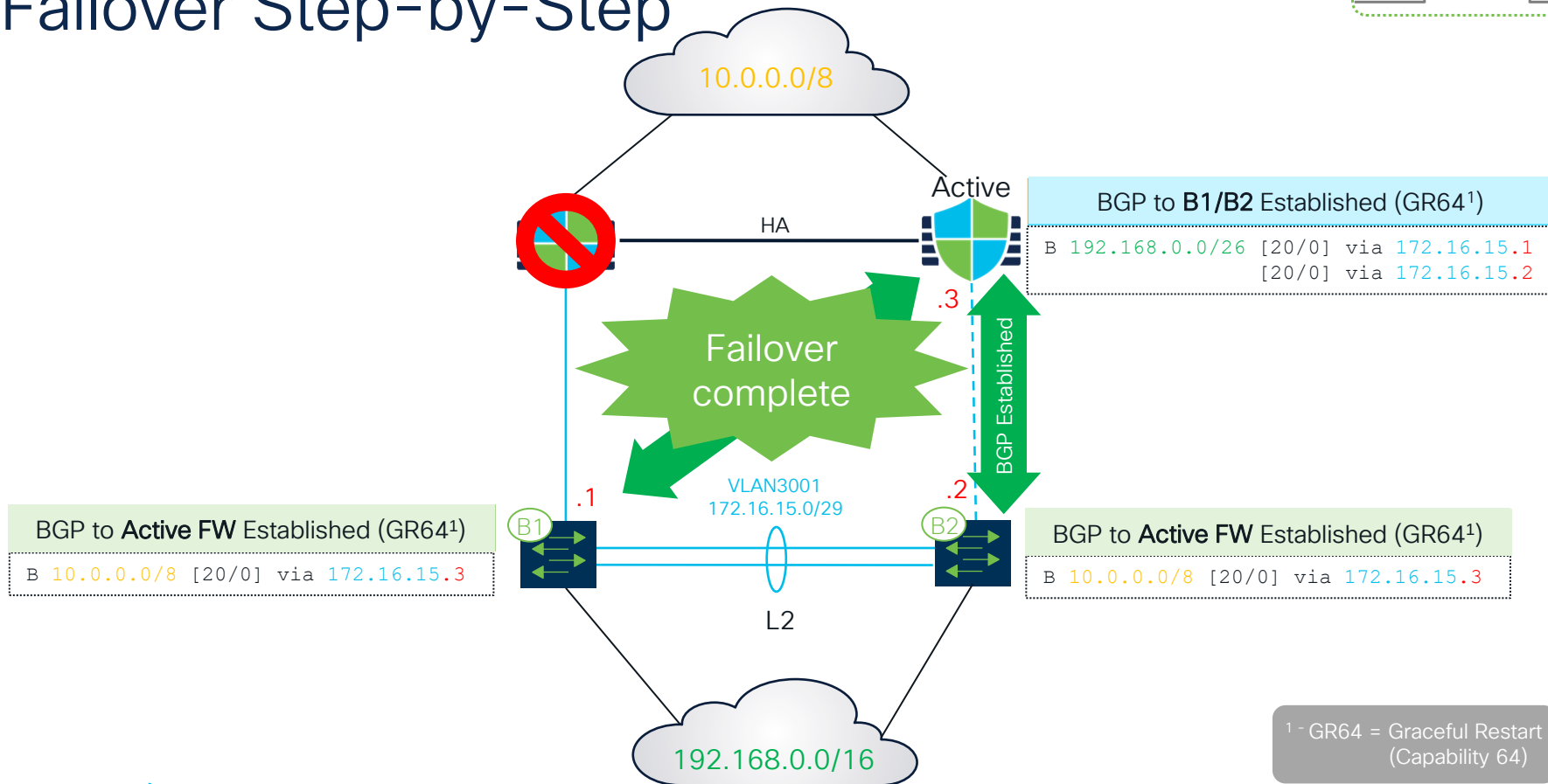
Full connectivity
10101 01101



¹ - GR64 = Graceful Restart
(Capability 64)

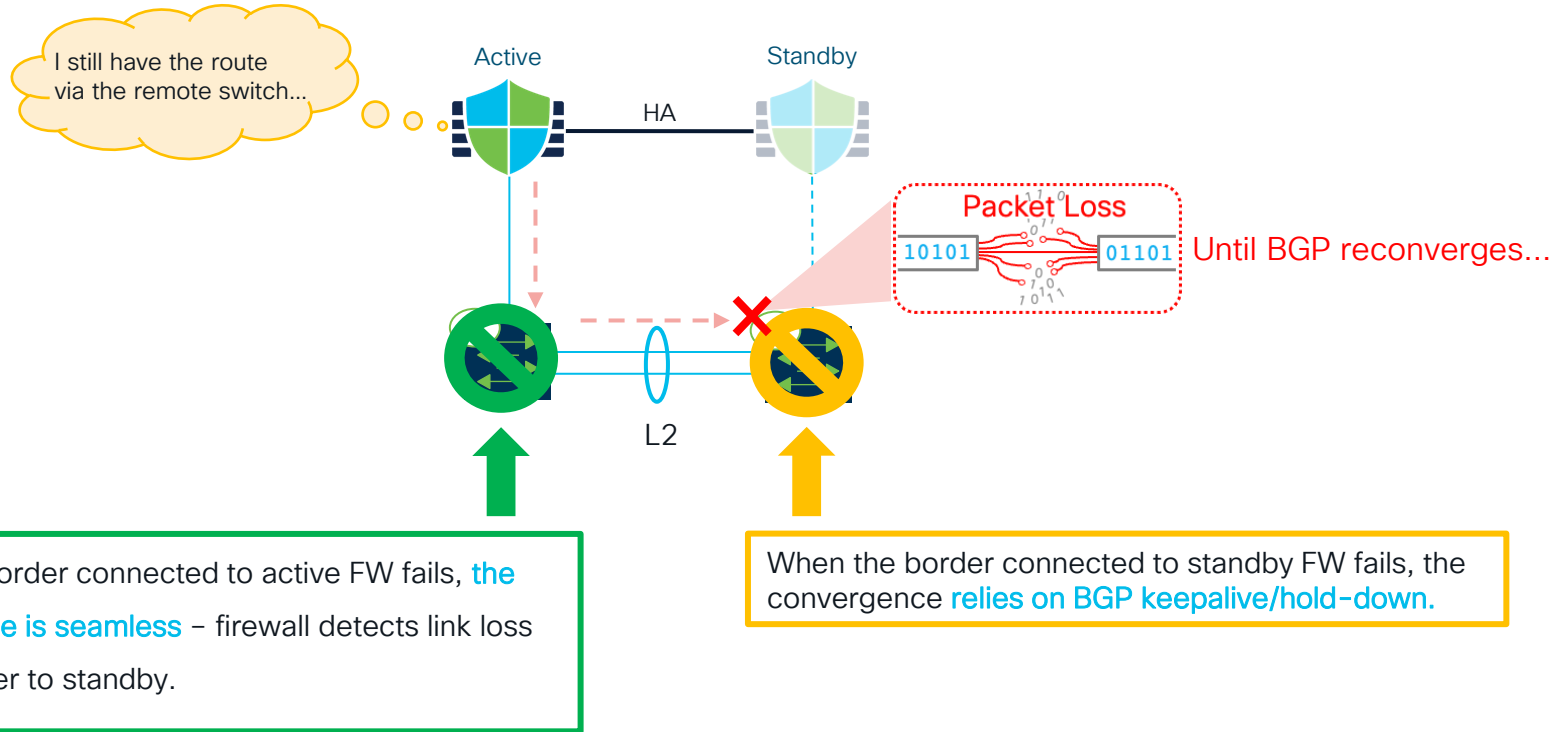
Failover Step-by-Step

Full connectivity
10101 01101

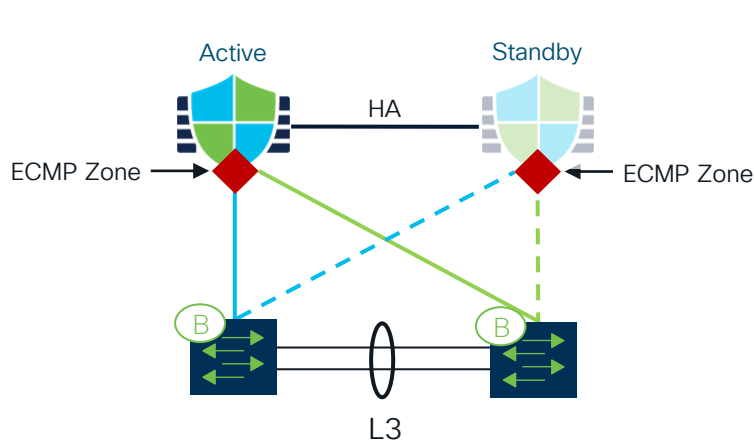
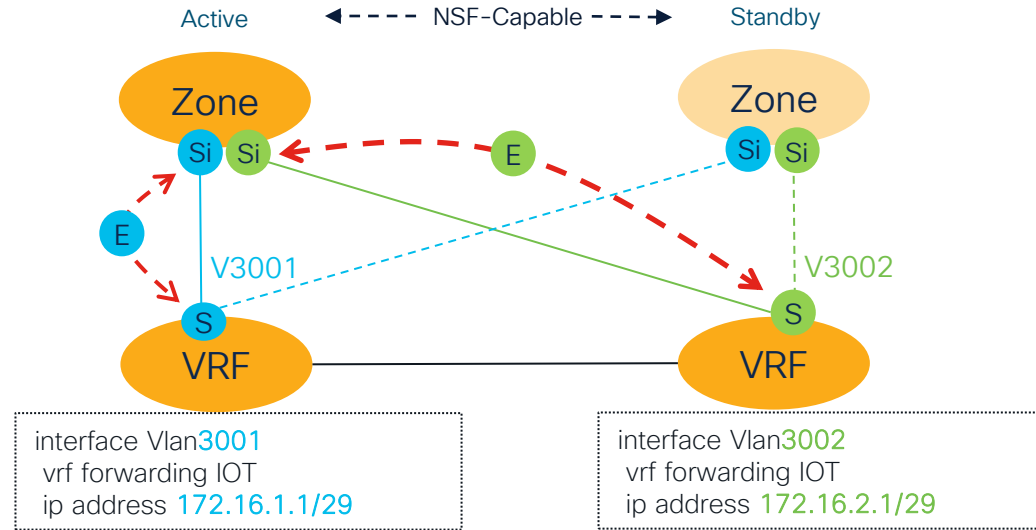


¹ - GR64 = Graceful Restart (Capability 64)

Direct FTD Attachment – Border Failure



Direct FTD Attachment with ECMP



- **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

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

Edit ECMP

Name

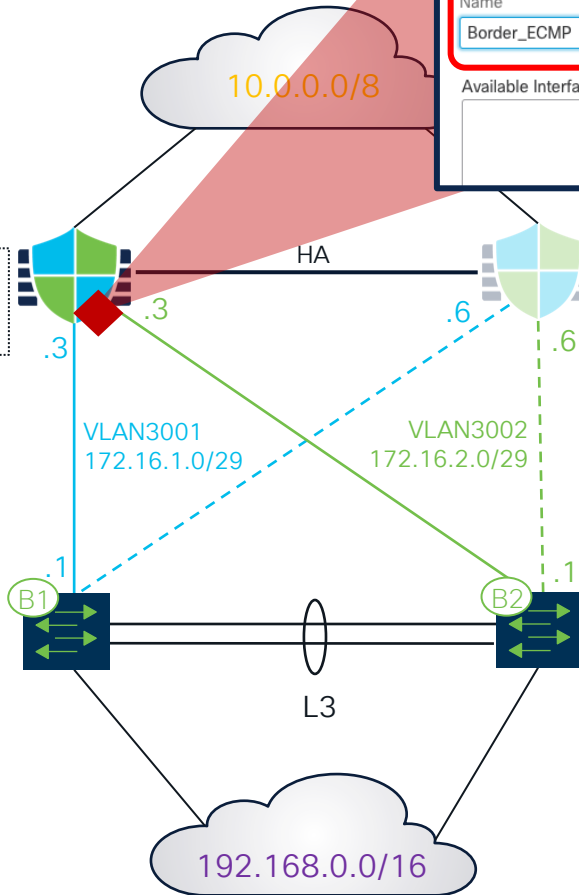
Border_ECMP

Available Interfaces

Selected Interfaces

VLAN3001

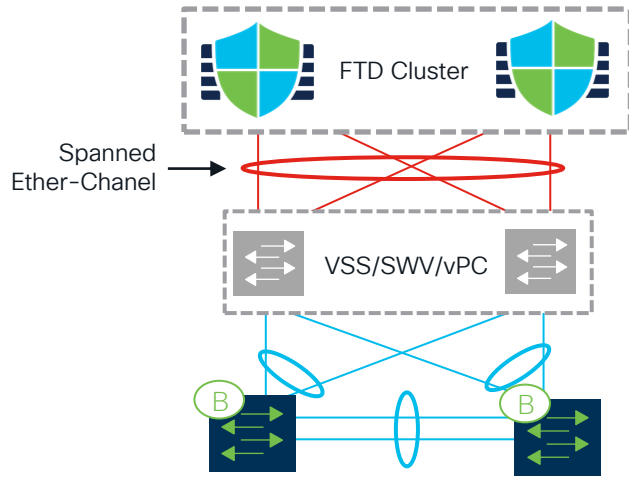
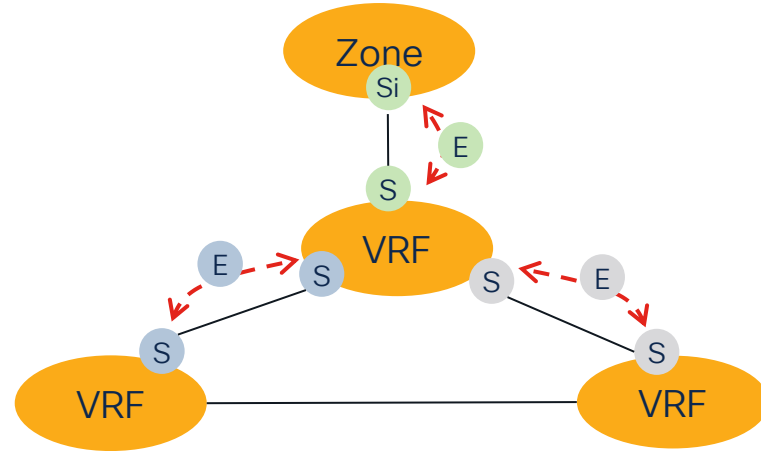
VLAN3002



BGP to **Active** FW Established over
VLAN3002

B 10.0.0.0/8 [20/0] via 172.16.2.3

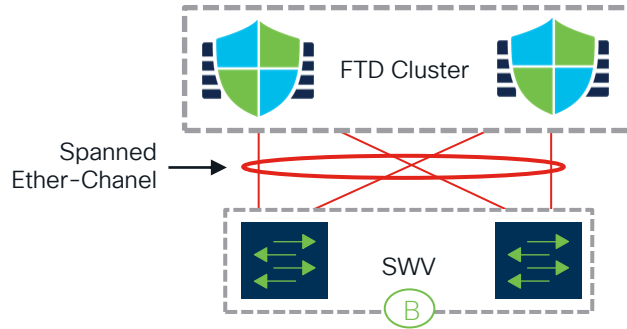
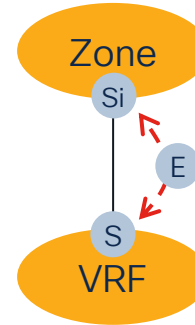
FTD Cluster with Intermediate Switching Layer



- 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

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

DNAC and Firewall Management Center Integration

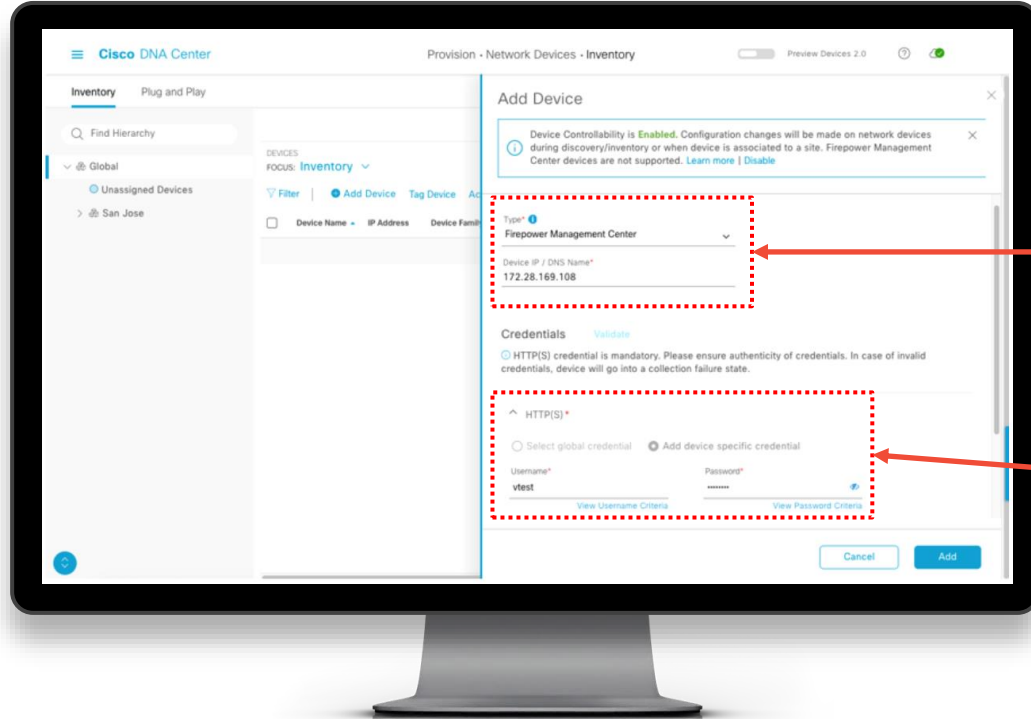


Integrating DNAC with FMC



- **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

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**.

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**.

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.

Cisco DNA Center Provision - Network Devices - Inventory

Global

DEVICES (4)
FOCUS: Software Images

Device Name	IP Address	Device Family	Site	Reachability	Software Image	Image Version	OS Update Status	Image Needs Update
172.20.97.94	172.20.97.94	Security and VPN	N/A	Reachable	ios-k8-fp2k-rgu-2.3	6.7.0	NA	NA
fpr128	172.20.202.128	Security and VPN	Assign	Reachable	Mark Golden	6.7.0	NA	NA
ftd193	172.20.202.193	Security and VPN	Assign	Reachable	asa9141-1-smp-k8- Upgrade Upgrade	6.6.0	Distribution Pending	OUTDATED
ftdv80								

Image Update Readiness Check

DEVICE DETAILS

Device: ftdv178.cisco.com (172.20.202.178)

Running Image: asa9141-150-smp-k8.bin

Golden Image: Cisco_FTD_Upgrade-6.7.0-65.sh.REL.tar

Reboot Required: Yes

Readiness Checks Results Re-Execute Checks Export As of: Mar 8, 2021 11:32 PM

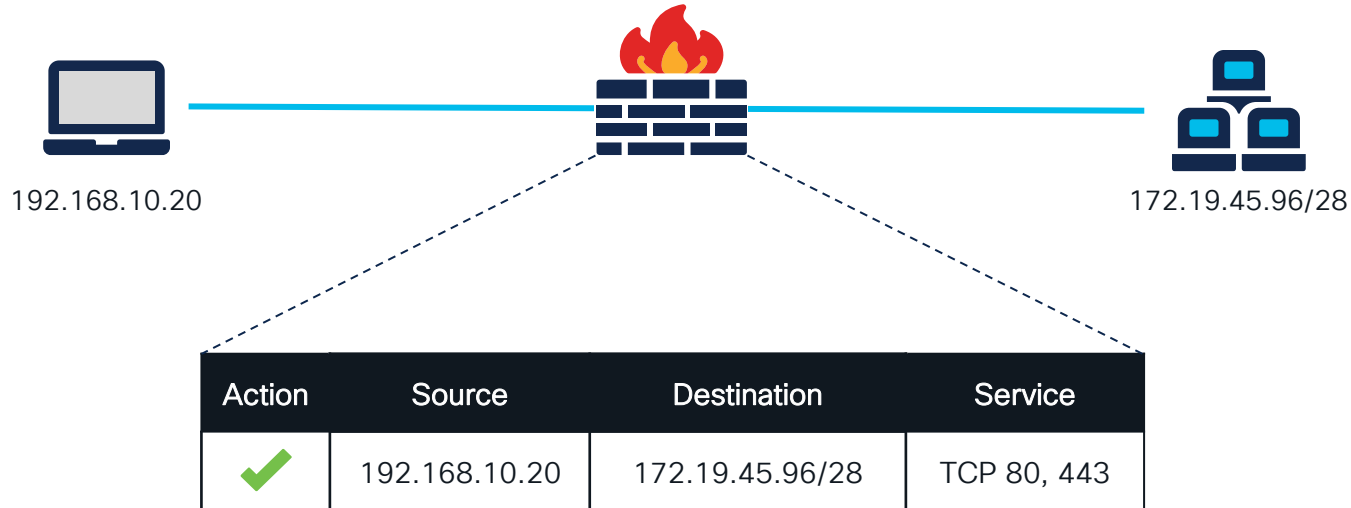
Check Type	Description	Status	Last Checked
FTD Upgrade Readiness Check	FTD Upgrade Readiness Check: SUCCESS	Success	Mon Mar 08 2021 11:31:55 PM

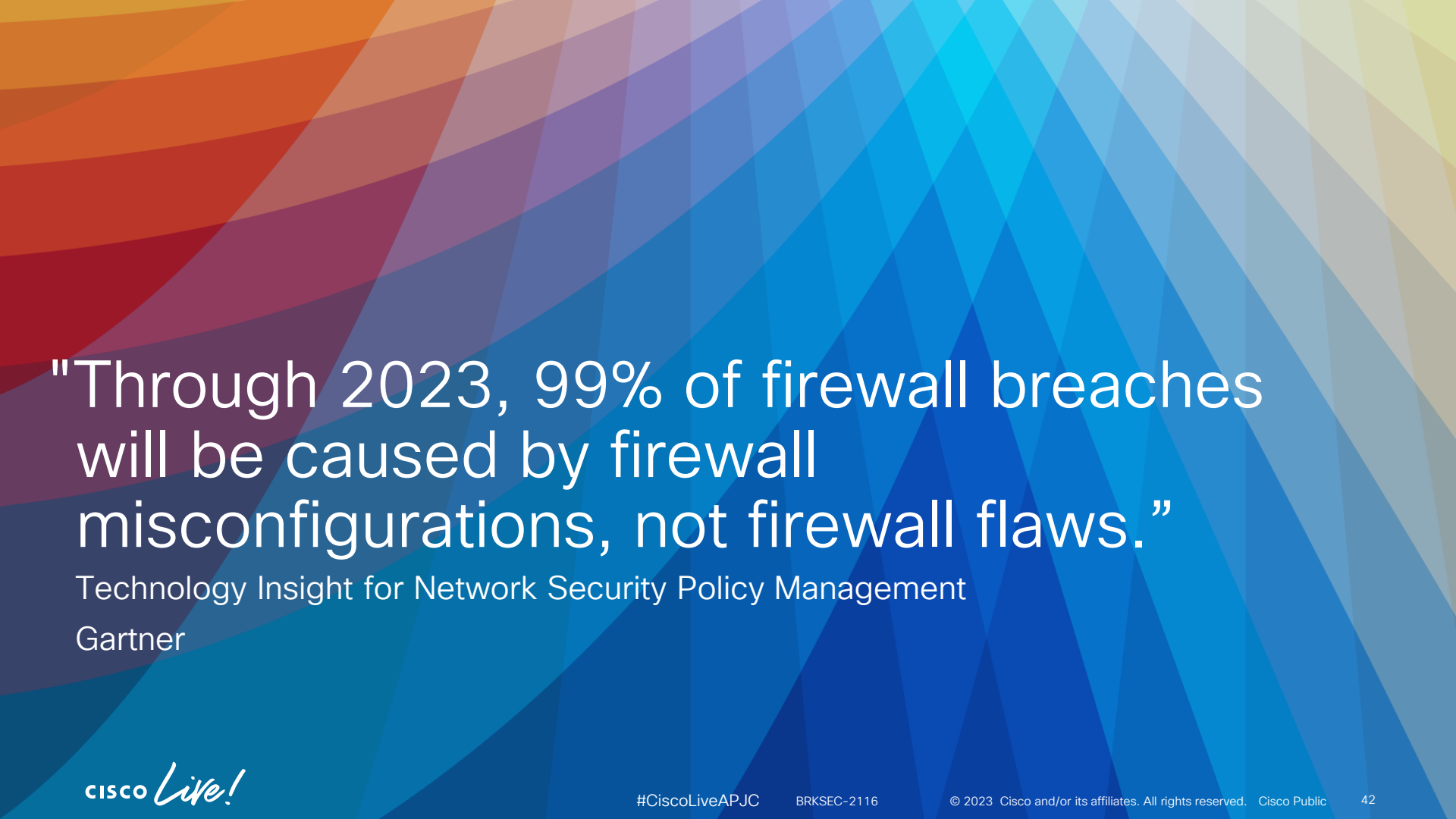
DNAC & FMC Integration Demo

Attribute Based Policy



Traditional Firewall Policy is not Enough



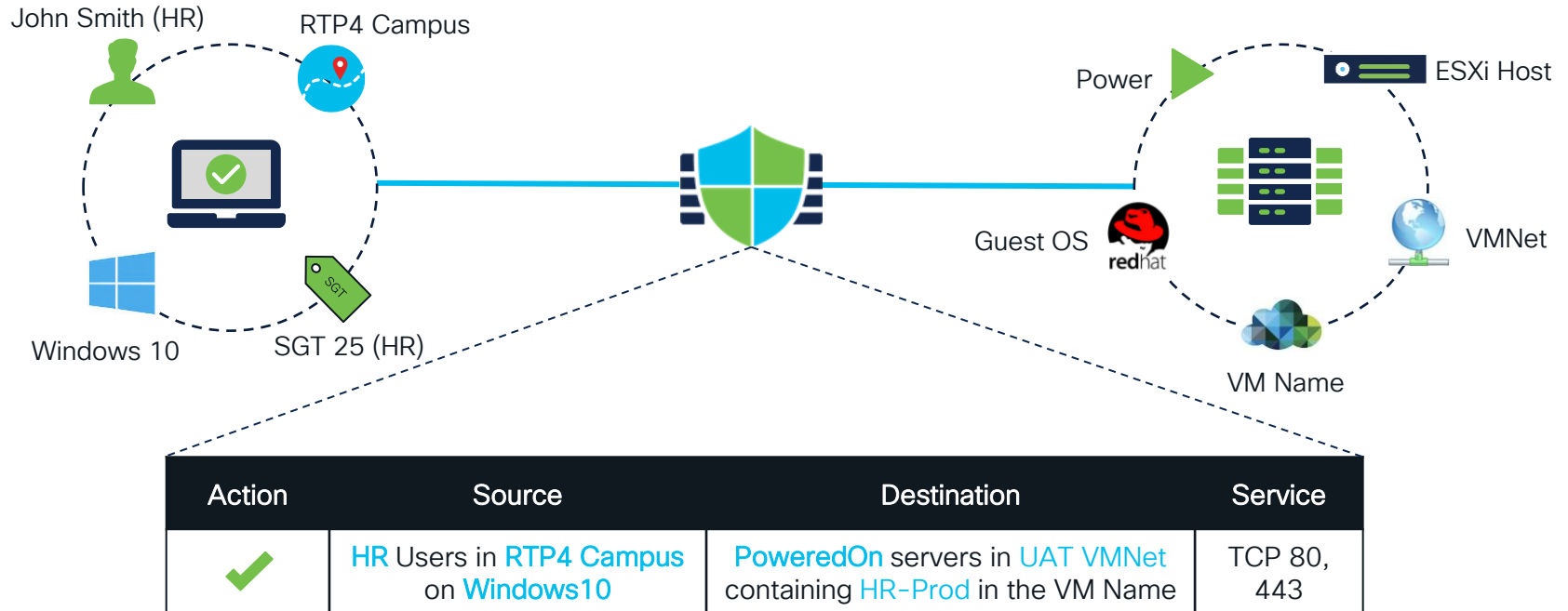


"Through 2023, 99% of firewall breaches
will be caused by firewall
misconfigurations, not firewall flaws."

Technology Insight for Network Security Policy Management

Gartner

Shift Towards Intent Based Policy



Attribute Based Policy

#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	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	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	Print	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Afcio-SP-C410DN RICOH-Afcio-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 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

The diagram illustrates the configuration of attribute-based policies. It features a table of policies with columns for Name, Source Zones, Dest Zones, Users, Applications, Dest Ports, Source Dynamic Attributes, Destination Dynamic Attributes, and Action. Red dashed boxes highlight specific attributes and actions. Red arrows connect these attributes to external icons representing various services and systems:

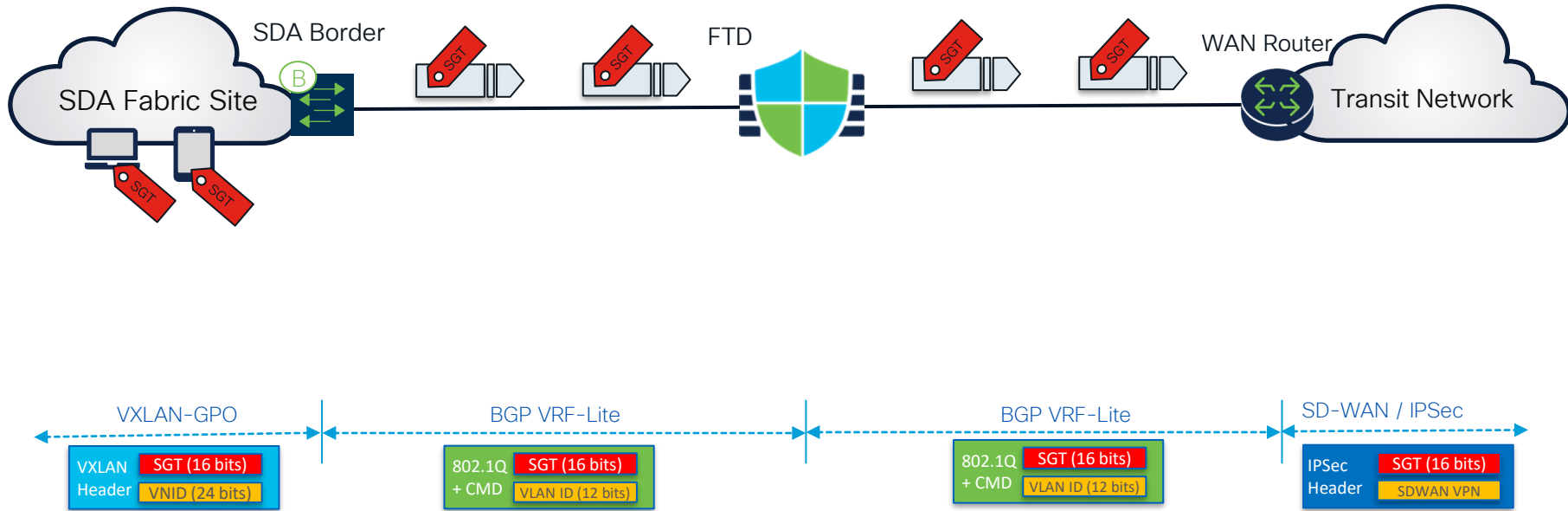
- Workload_1** (Policy 1) is linked to a document icon.
- IoT Support Service** (Policy 2) is linked to a magnifying glass icon.
- Machine Authentication** (Policy 3) is linked to a person icon.
- Print** (Policy 4) is linked to a printer icon.
- Block Social Media** (Policy 5) is linked to a person icon.
- o365 Access** (Policy 6) is linked to a person icon.
- SecureX Threat Containment** (Policy 7) is linked to a person icon.
- ISE Threat Containment** (Policy 8) is linked to a person icon.
- Cloud App Access** (Policy 9) is linked to a person icon.
- WorkloadObj_615c486dc9** (Source Dynamic Attribute for Policy 1) is linked to a document icon.
- WorkloadObj_615c8066483** (Destination Dynamic Attribute for Policy 1) is linked to a document icon.
- IoT_Support** (Source Dynamic Attribute for Policy 2) is linked to a magnifying glass icon.
- IoT** (Destination Dynamic Attribute for Policy 2) is linked to a magnifying glass icon.
- Machine_Auth** (Source Dynamic Attribute for Policy 3) is linked to a person icon.
- VMWare_Active_Directory** (Destination Dynamic Attribute for Policy 3) is linked to a person icon.
- RICOH-Afcio-SP-C410DN** (Source Dynamic Attribute for Policy 4) is linked to a printer icon.
- RICOH-Afcio-SP-C820DN** (Source Dynamic Attribute for Policy 4) is linked to a printer icon.
- Xerox-WorkCentre-5030** (Source Dynamic Attribute for Policy 4) is linked to a printer icon.
- Xerox-WorkCentre-5135** (Source Dynamic Attribute for Policy 4) is linked to a printer icon.
- APIC_A_ESG_Print_Servers** (Destination Dynamic Attribute for Policy 4) is linked to a printer icon.
- Contractors** (Source Dynamic Attribute for Policy 5) is linked to a person icon.
- Branch_Locations** (Source Dynamic Attribute for Policy 5) is linked to a person icon.
- Any** (Destination Dynamic Attribute for Policy 5) is linked to a person icon.
- lab-local/Domain Users** (Source Dynamic Attribute for Policy 6) is linked to a person icon.
- Any** (Source Dynamic Attribute for Policy 6) is linked to a person icon.
- o365_Common** (Destination Dynamic Attribute for Policy 6) is linked to a person icon.
- o365_Exchange** (Destination Dynamic Attribute for Policy 6) is linked to a person icon.
- o365_SharePoint** (Destination Dynamic Attribute for Policy 6) is linked to a person icon.
- SecureX_Quarantined_IPs** (Source Dynamic Attribute for Policy 7) is linked to a person icon.
- SecureX_Suspicious_IPs** (Source Dynamic Attribute for Policy 7) is linked to a person icon.
- Honeypot_Service** (Destination Dynamic Attribute for Policy 7) is linked to a person icon.
- Quarantined_Systems** (Source Dynamic Attribute for Policy 8) is linked to a person icon.
- Honeypot_Service** (Destination Dynamic Attribute for Policy 8) is linked to a person icon.
- Employees** (Source Dynamic Attribute for Policy 9) is linked to a person icon.
- Azure_HR_Workload** (Destination Dynamic Attribute for Policy 9) is linked to a person icon.
- Azure_Intranet_Service** (Destination Dynamic Attribute for Policy 9) is linked to a person icon.

External icons and labels include:

- vmware** (top right)
- APIC** (middle right)
- Office 365** (bottom right)
- SecureX** (bottom center)
- aws** (bottom left)
- Azure** (bottom left)

Attribute-Based Policy Dynamic Attribute Sources

Inline Propagation



Inline Propagation

Add Rule

Name: Source SGT Rule ☒ Enabled

Insert: below rule 2

Action: Allow

Time Range: None

Dynamic Attributes

Available Attributes C

Search by name or value

Security Group Tag

ANY

Auditors

BYOD

Contractors

Developers

Development_Servers

Employees

Guests

Add to Source

Add to Destination

Selected Source Attributes (1)

Security Group Tags

Contractors

Add a Location IP Address

Add

Selected Destination Attributes (0)

any

Attributes of the same type (for example, SGT) match the rule if any attribute is matched. Attributes of different types match the rule only if all attributes are matched. [More info](#)

Cancel Add

Note: Inline SGTs applicable for source criteria only

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 (-)									
v 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	Any	Any	Any	HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_VN	Any	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	Any	Azure_HR_Workload Azure_Intranet_Service	Allow

TrustSec inline propagated
Scalable Group Tags



Note: Inline SGTs applicable for source criteria only

SGT Inline Propagation Through a Firewall Demo

Control Plane Propagation with pxGrid

User:	SGT:	IP:	Source:
-	 10	172.16.0.4	SXP
 Eric	-	172.16.0.22	PassiveID
 Ira	 15	172.19.1.13	RADIUS


Cisco ISE
(PassiveID/RADIUS/SXP)

pxGrid


FMC

Security Group Tag

ANY
Auditors
BYOD
Computers
Contractors
Developers

Available Users

Q Search by name or value

lab.local/*
Group1
Group2
user1
user2

Device type

2Wire-Device
3Com-Device
Aastra-Device
Aastra-IP-Phone
Aerohive-Access-Point
Aerohive-Device
American-Power-Conversion-Device
Android

Location IP

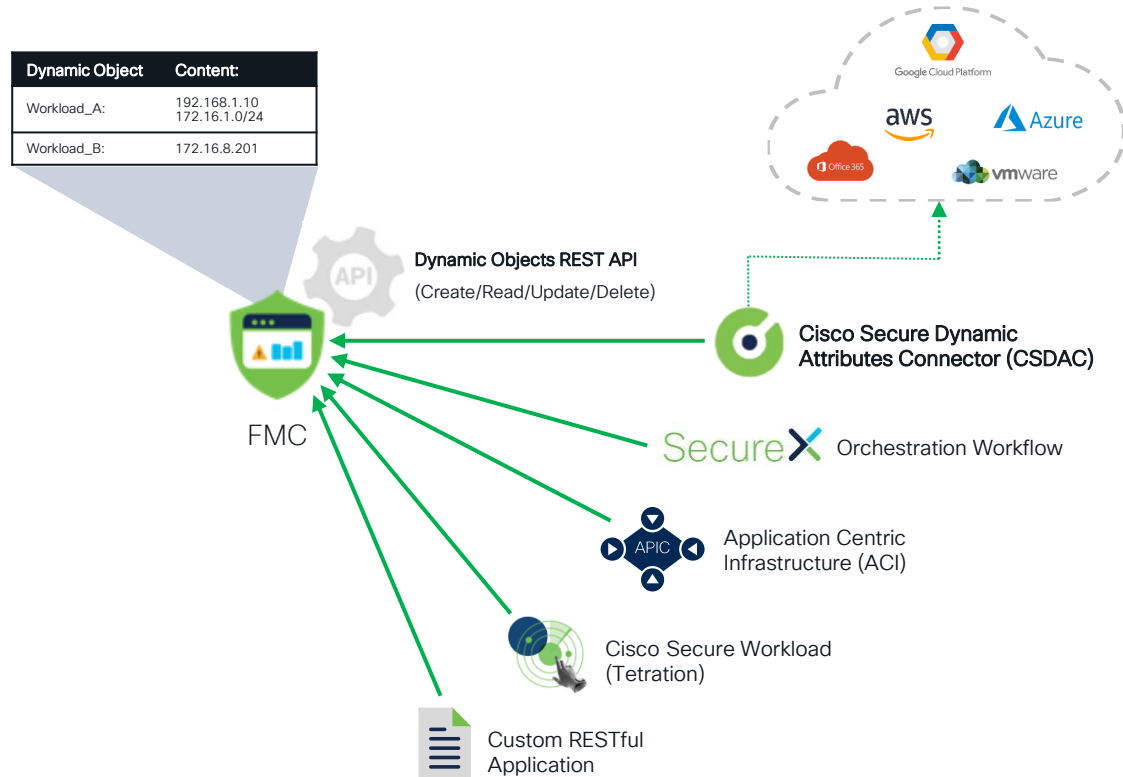
802.1x-Laboratory
any-ipv4
any-ipv6
IPv4-Benchmark-Tests

Entra ID realms
supported in 7.4/7.4.1
(December 2023)

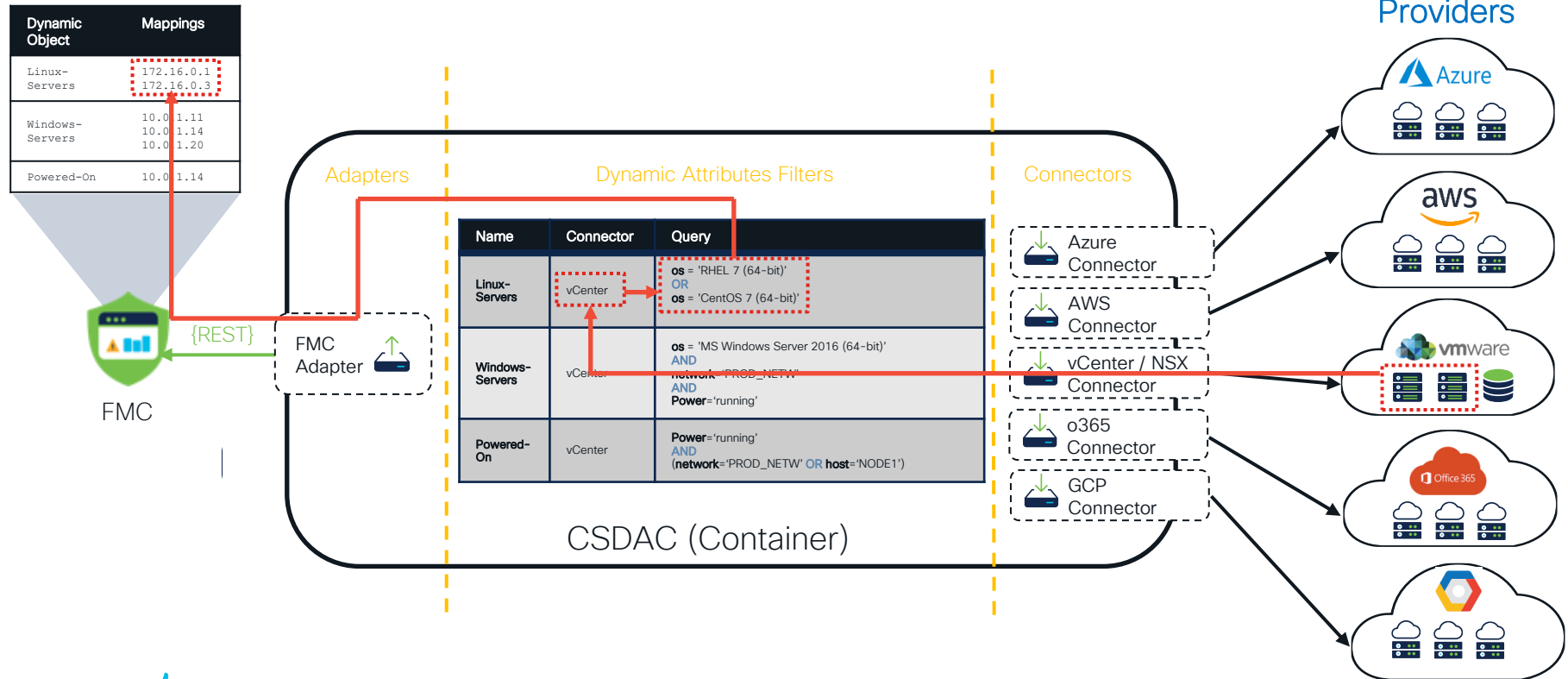
Attribute Based Policy – ISE Context Objects

#	Name	Source Zones	Dest Zones	Users	Application	Identity Services Engine Source & Destination SGTs	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)								
v Default - Attribute-Based Policy (1-9)								
1	Workload_1	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c86dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Printing Service	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	Identity Services Engine AD Users	Corporate_VN	External	Any	Google+ Instagram Tinder Twitter	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	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	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

Control Plane Propagation with Dynamic Objects



Architecture of the Dynamic Attributes Connector



Attribute Based Policy – CSDAC Attributes

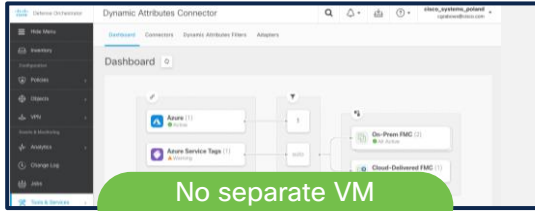
#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)									
v Center / NSX Dynamic Objects									
vmware									
v Center / NSX Dynamic Objects									
vmware									
1	Workload_1	Any	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 ier_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	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

CSDAC Demo

The New Cloud Form Factor



CSDAC in CDO's
Tools & Services



No separate VM
required!!

Cloud Delivered



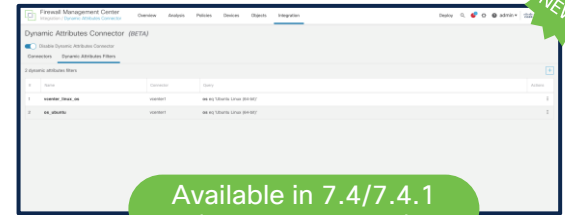
CSDAC
(Linux Machine)



Standalone



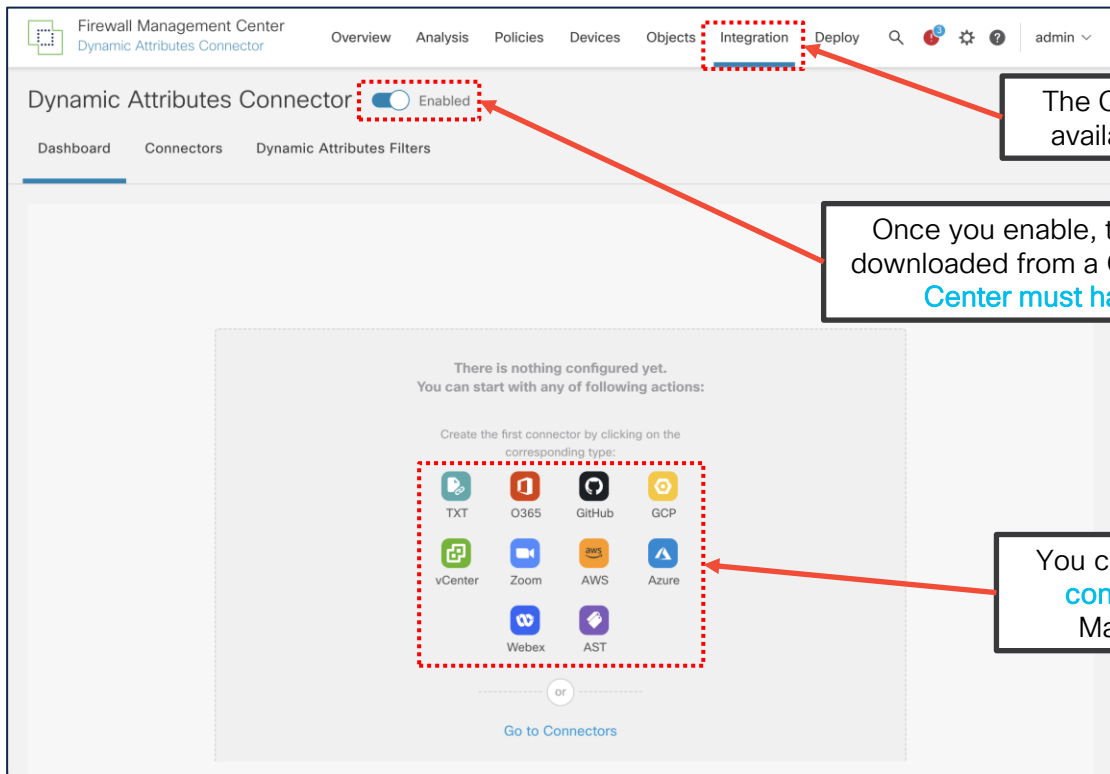
CSDAC in FMC



Available in 7.4/7.4.1
(December 2023)

Built In
(FMC HA Supported)

CSDAC is Now In the Firewall Management Center

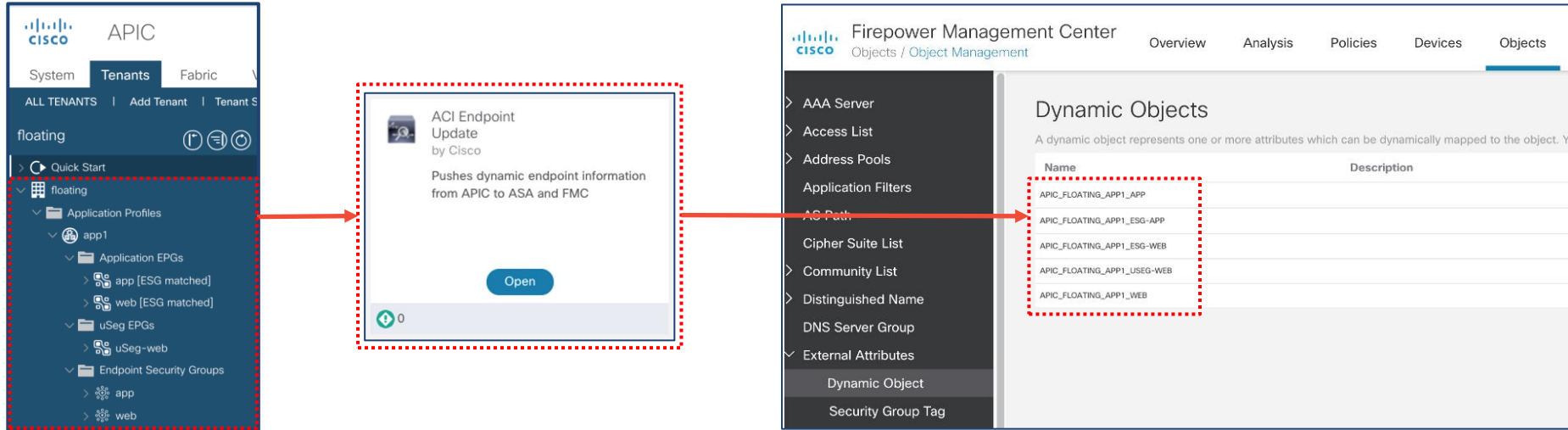


The CSDAC configuration dialog is available under **Integration menu**.

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.

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

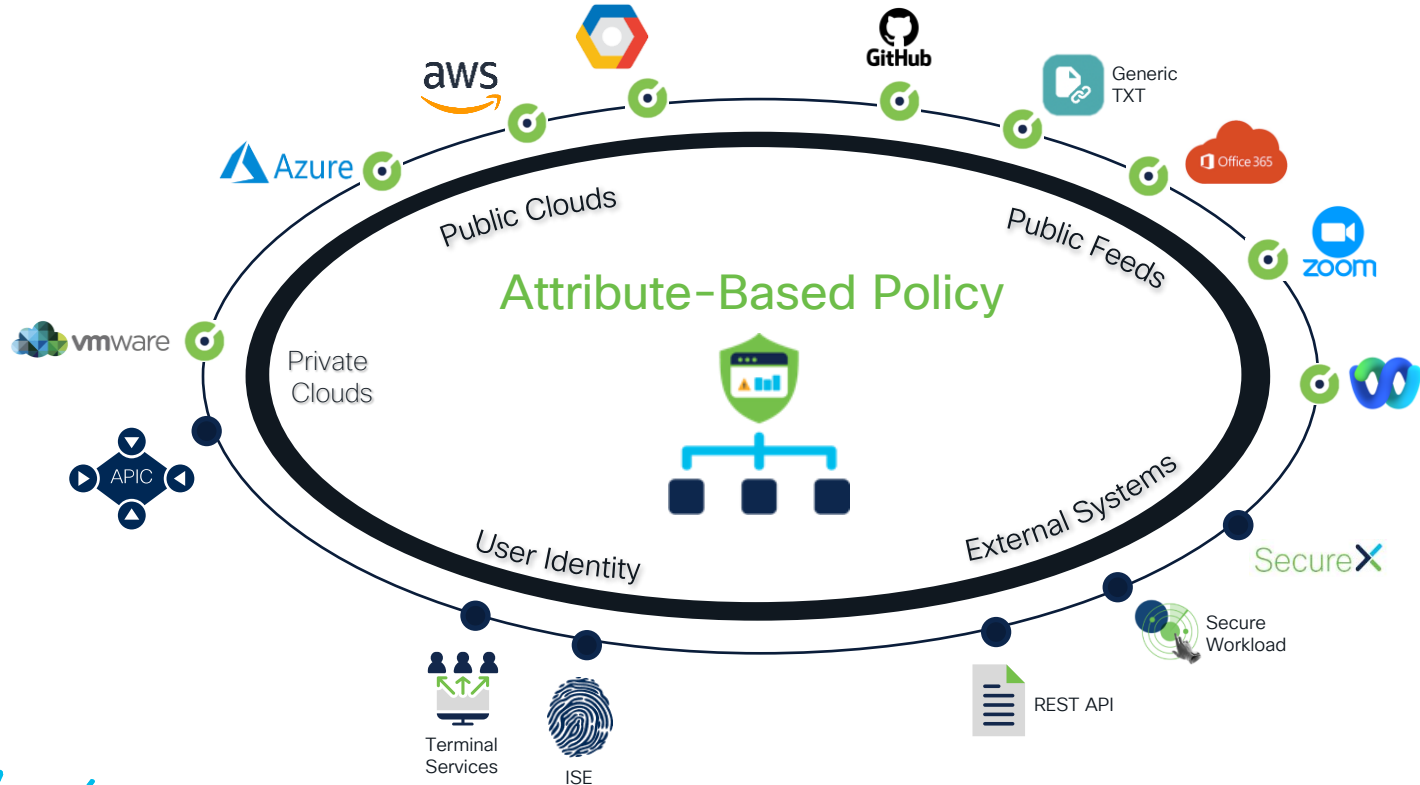
Attribute Based Policy – ACI EPG and ESG

#	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-Exchange o365-Exchange	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Any	Any	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Guaranteed_Systems	Moneyport_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)



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



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

Health Status

2 total 0 critical 1 warning 1 normal 0 disabled

FMC

Devices

Device

> ▲ FMC

▼ ● FTD 7.0

● Reconfiguring Detection

Process is running correctly

● Snort Identity Memory Usage

3.7% of 27.0M used [see less](#)

Total Usage : 3.7%(1.0M / 27.0M)

Memory Usage Detail

Host Cache799.2K

Subnet Cache32B

User Group Mapping Cache208.9K

Binding Detail

Current9 / 64000

Host Binding9

Subnet Binding0

User Group Mapping Detail

User Group Mappings0

Groups Used in Policy0 / 128

Managed Device

CISCO *Live!*

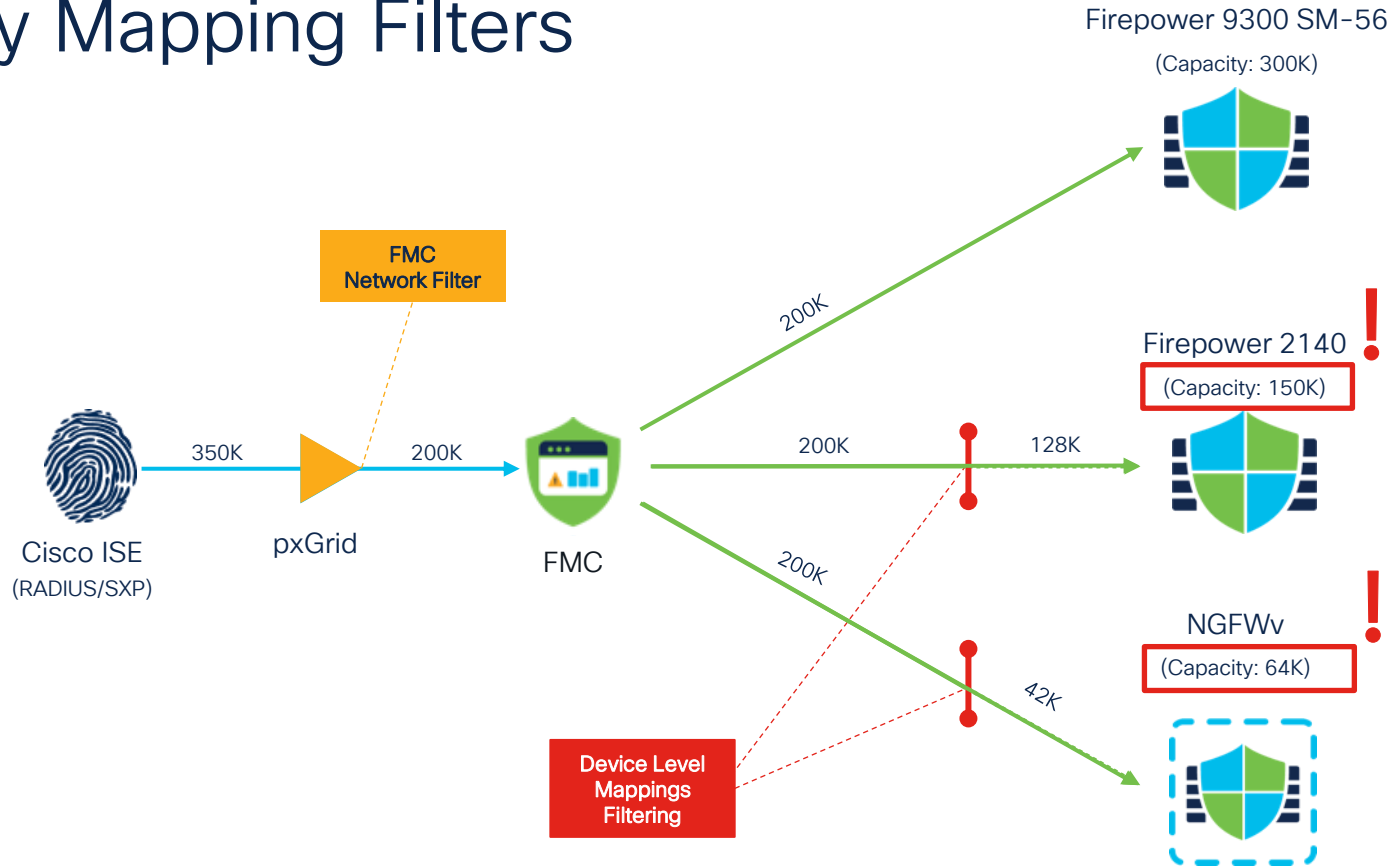
#CiscoLiveAPJC

BRKSEC-2116

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

64

Identity Mapping Filters



Identity Propagation Practical Use- Cases



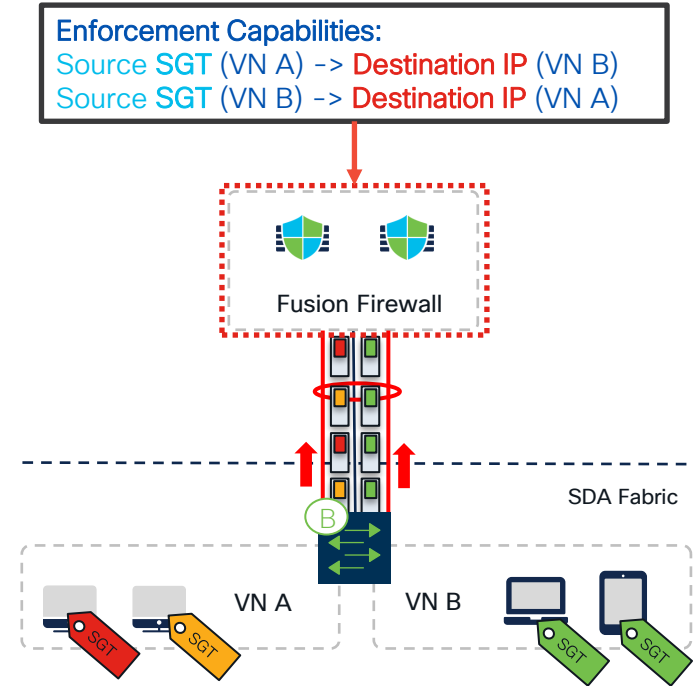
Inter-VN Attribute Based Policy (Inline Tagging)

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



Inter-VN Attribute Based Policy

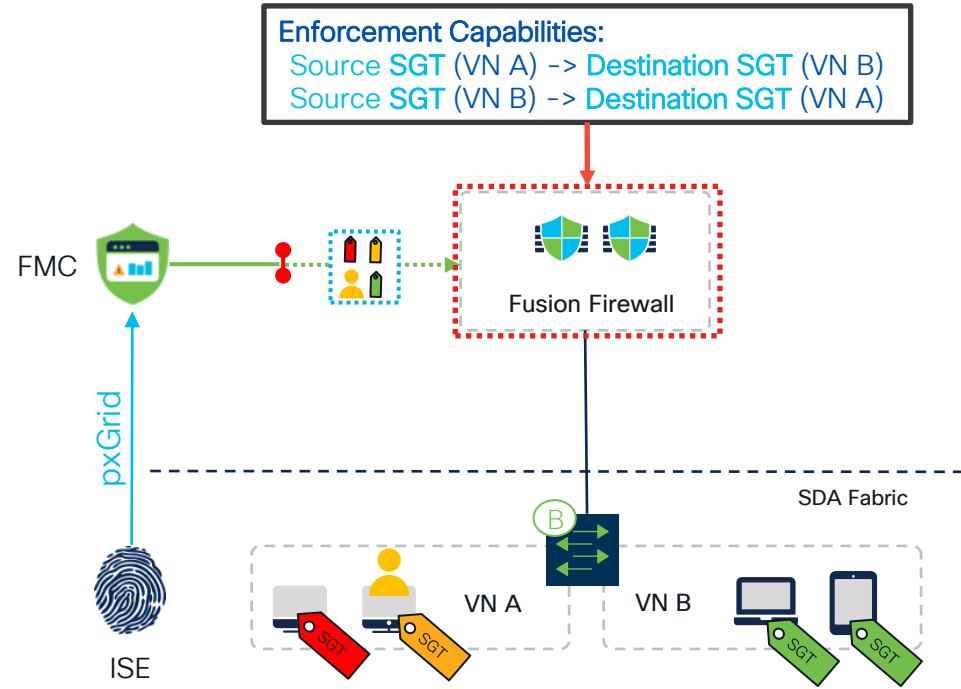
(Control Plane Propagation)

Key Benefits

- **Flexible** Attribute-Based Inter-VN policy
- Identity attributes applicable in **any direction**
- Policy based on 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**



DC/Cloud Access Attribute Based Policy

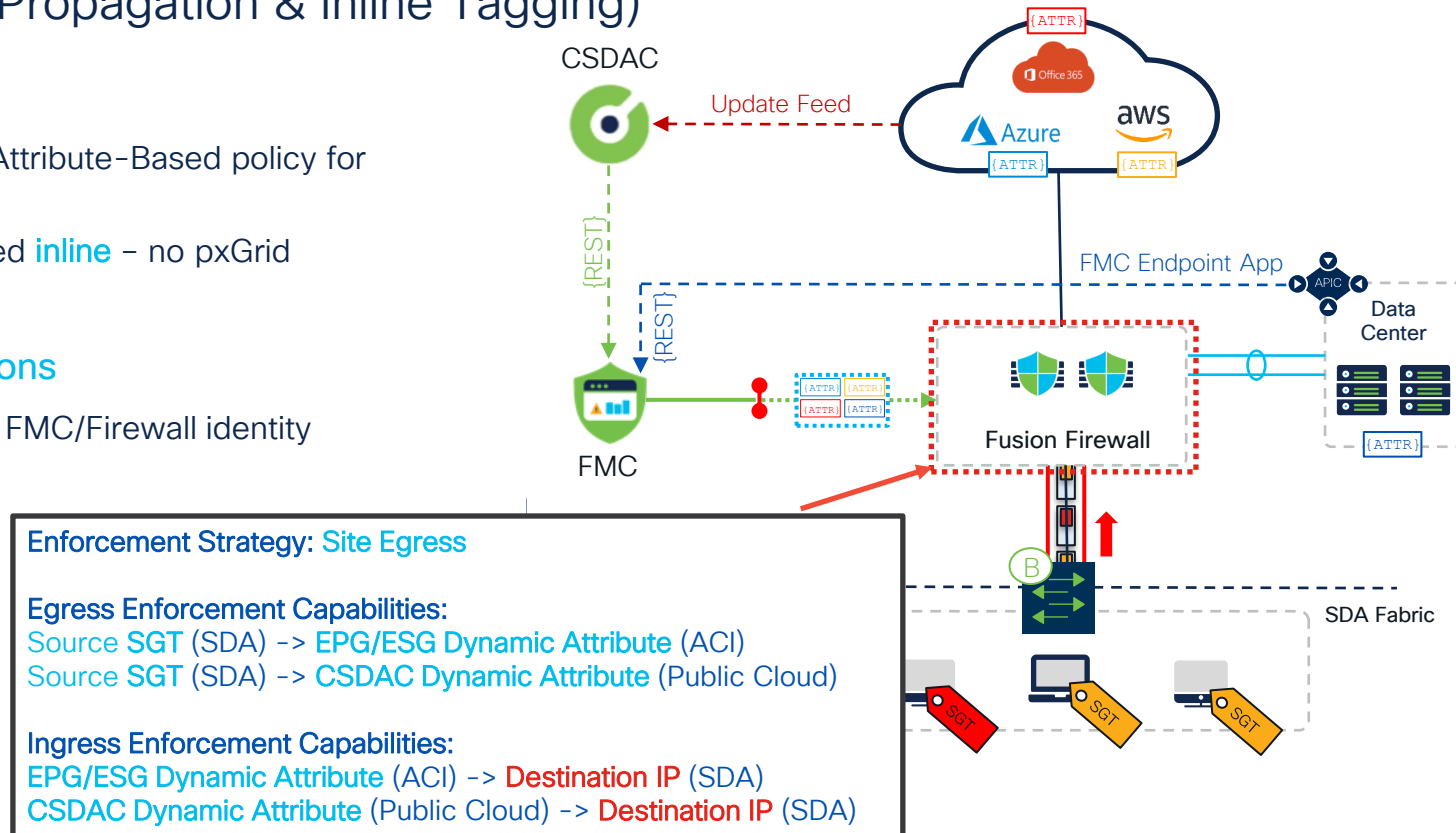
(Control Plane Propagation & Inline Tagging)

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



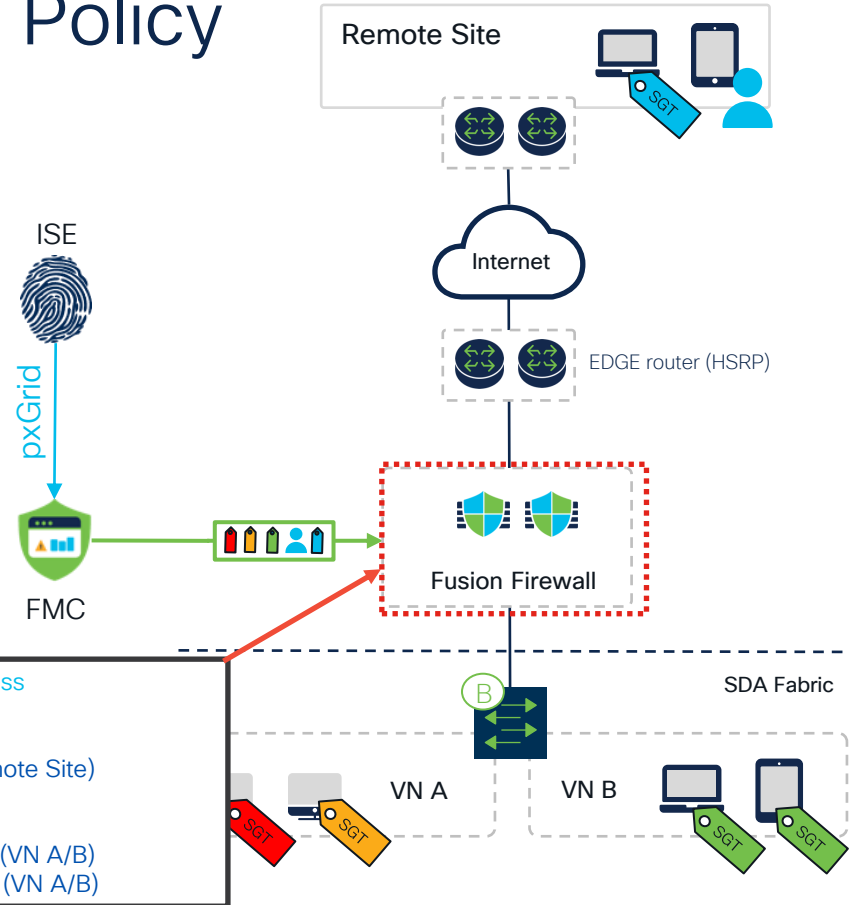
Inter-Site Attribute Based Policy (Control Plane Propagation)

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



Scalable Branch-to-Branch

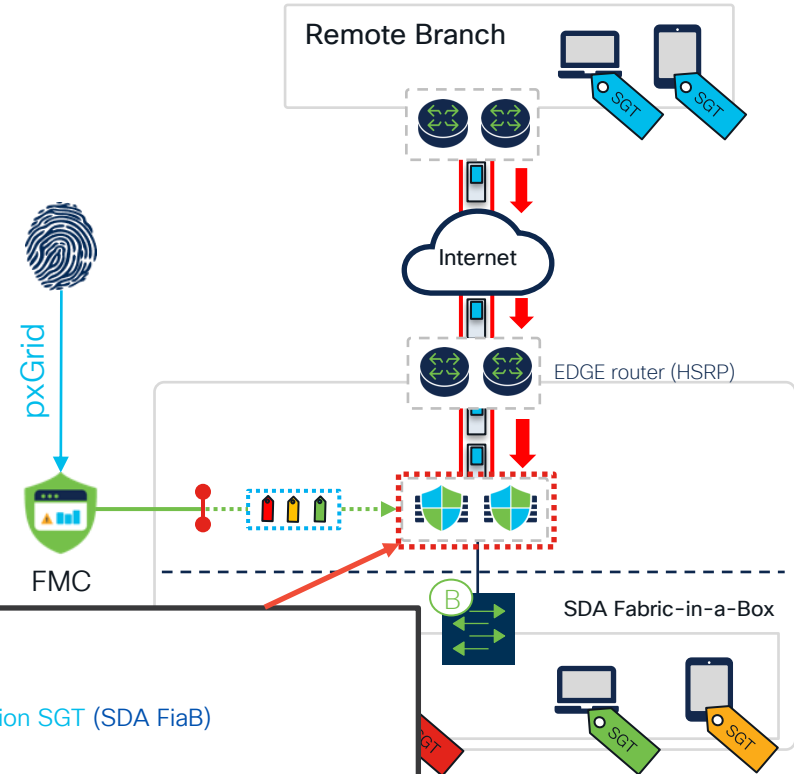
(Control Plane Propagation & Inline Tagging)

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

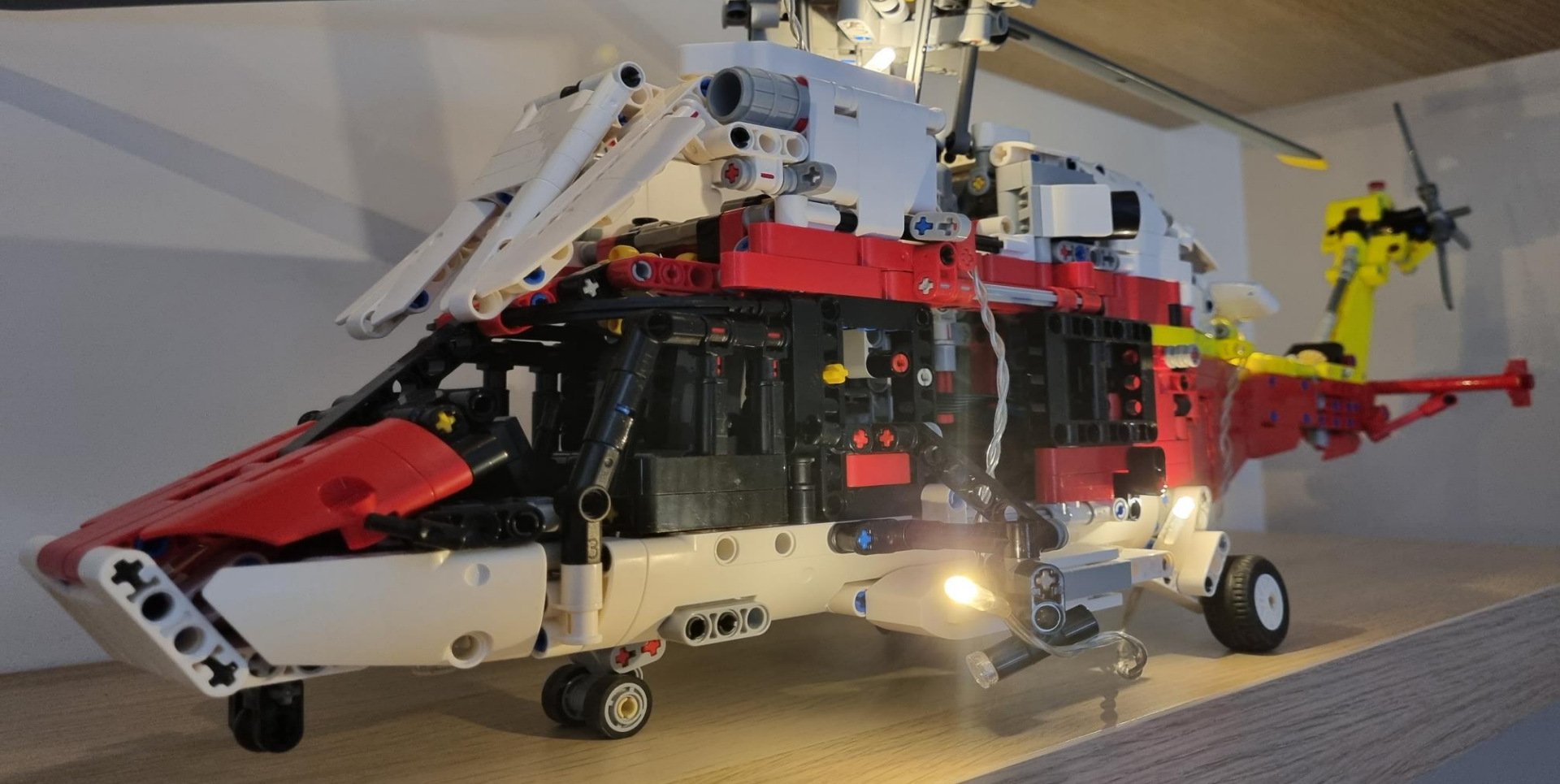
Ingress Enforcement Capabilities:

Source SGT (Remote Branch) -> Destination SGT (SDA FiaB)

Egress Enforcement Capabilities:

Source SGT (SDA FiaB) -> Destination IP (Remote Branch)

Conclusions



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.

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.

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



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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC