
cisco Live!
ALL IN

The bridge to possible

Cisco Secure Firewall and SDA Integration Deep Dive

Christopher Grabowski, Technical Marketing Engineer

BRKSEC-2845

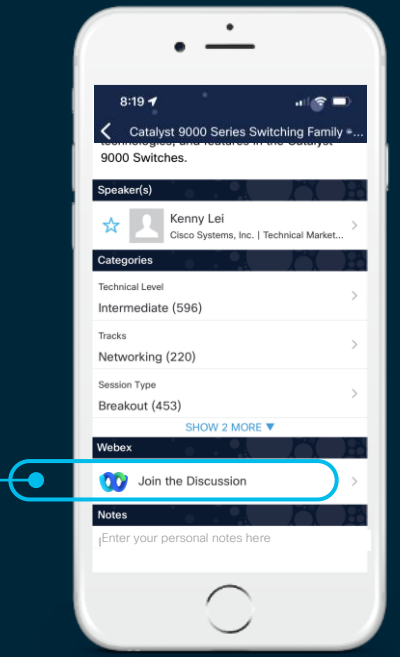
Cisco Webex App

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



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2845

Webex spaces will be moderated by the speaker until June 17, 2022.

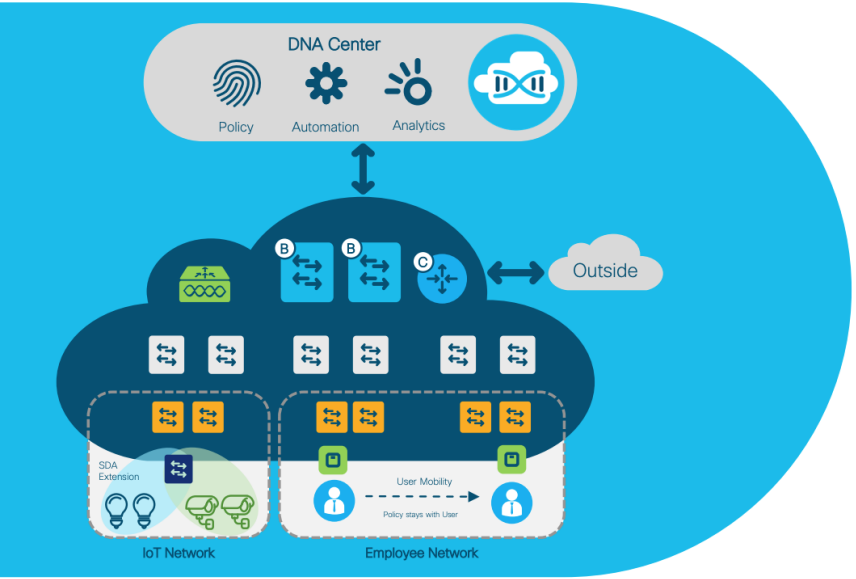
Your Speaker

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

Christopher Grabowski
Technical Marketing Engineer
CCIE Security #42466


MONINI
Classico
OLIO EXTRA VERGINE DI OLIVA
750ml+
33%GRATIS

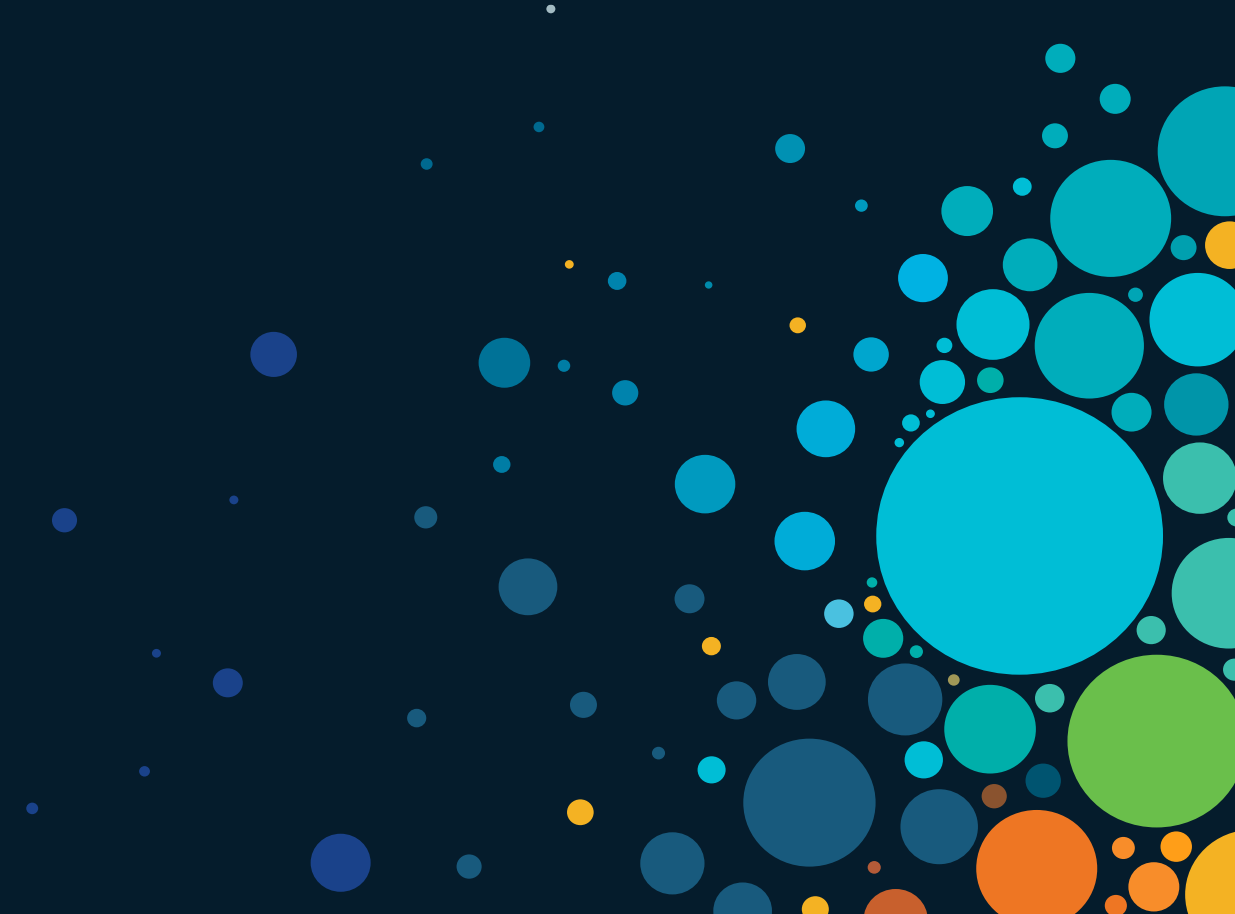
Cisco Secure Firewall provides a comprehensive integration with SDA



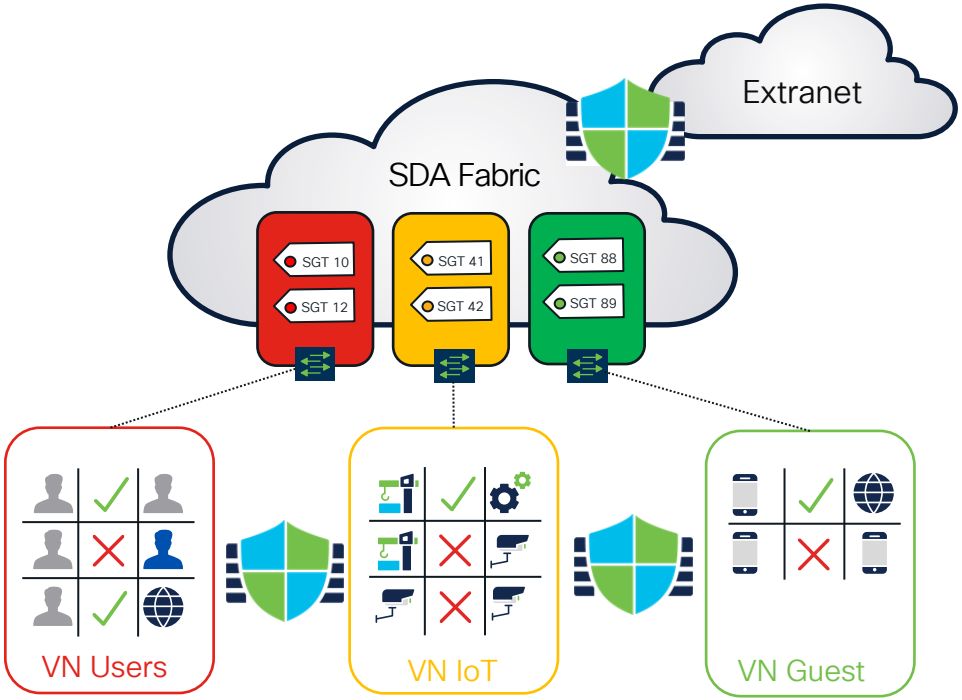
Agenda

- 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

Firewall enforcement

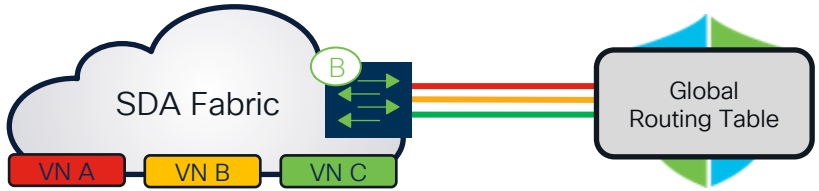
- Next Generation Firewall & IPS
- TLS decryption
- Malware analysis and retrospection
- Attributes Based policy with dynamic objects and identity
- Extensive logging, correlation and Threat Intelligence capabilities
- Requires service insertion design
- NetOps/SecOps collaboration

Firewall Deployment Modes and Virtualization Options

Firewall Deployment Modes – VN Separation

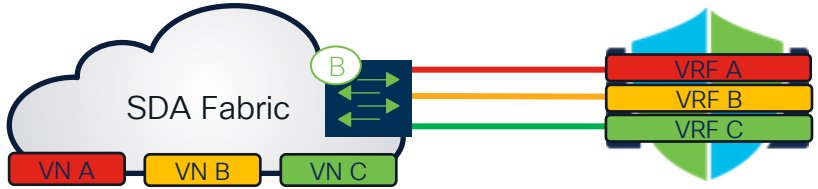
Non-VRF Aware

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



VN to VRF Mapping

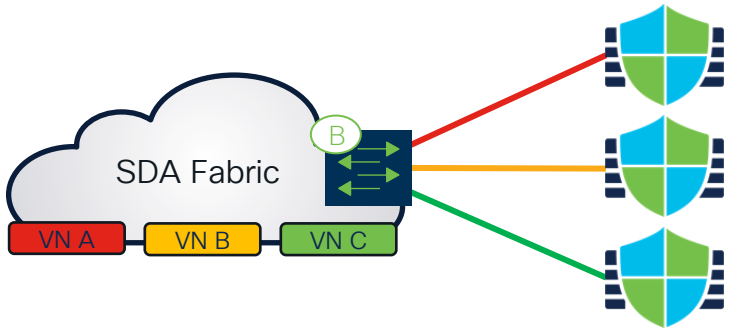
- VN mapped to VRFs on the firewall providing routing separation
- Firewall leaks routes between VNs, Shared Services and external
- Common firewall policy across VRFs on the FTD, with VRF aware rules.



Firewall Deployment Modes – VN Separation

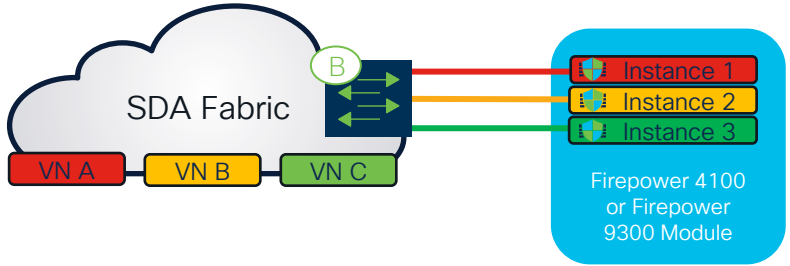
VN to Physical Device mapping

- 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



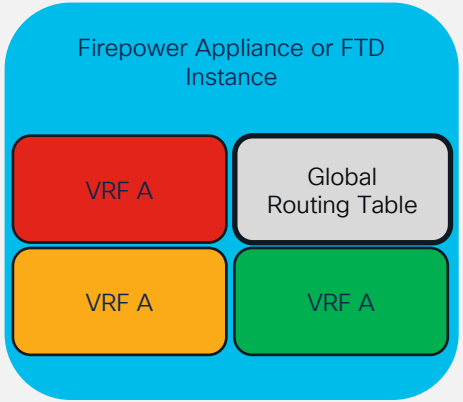
VN to Instance mapping

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

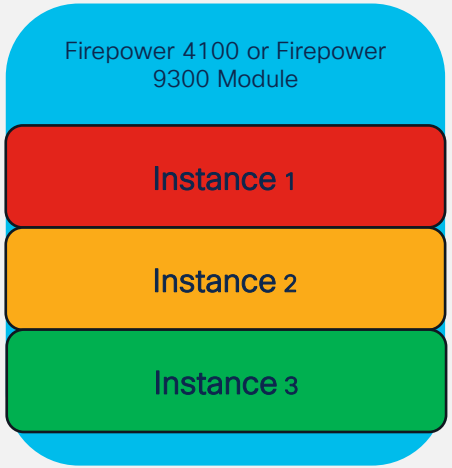


Cisco Secure Firewall Virtualization Options

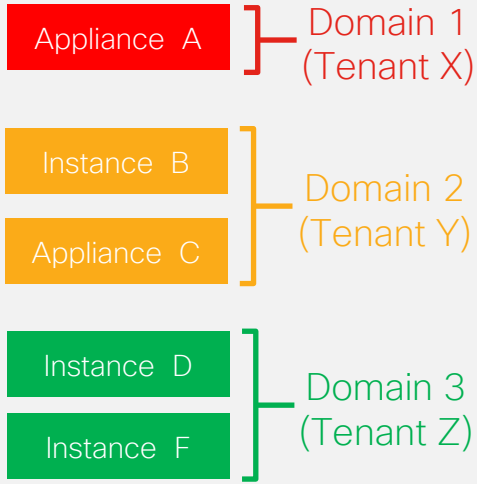
Virtual Routers



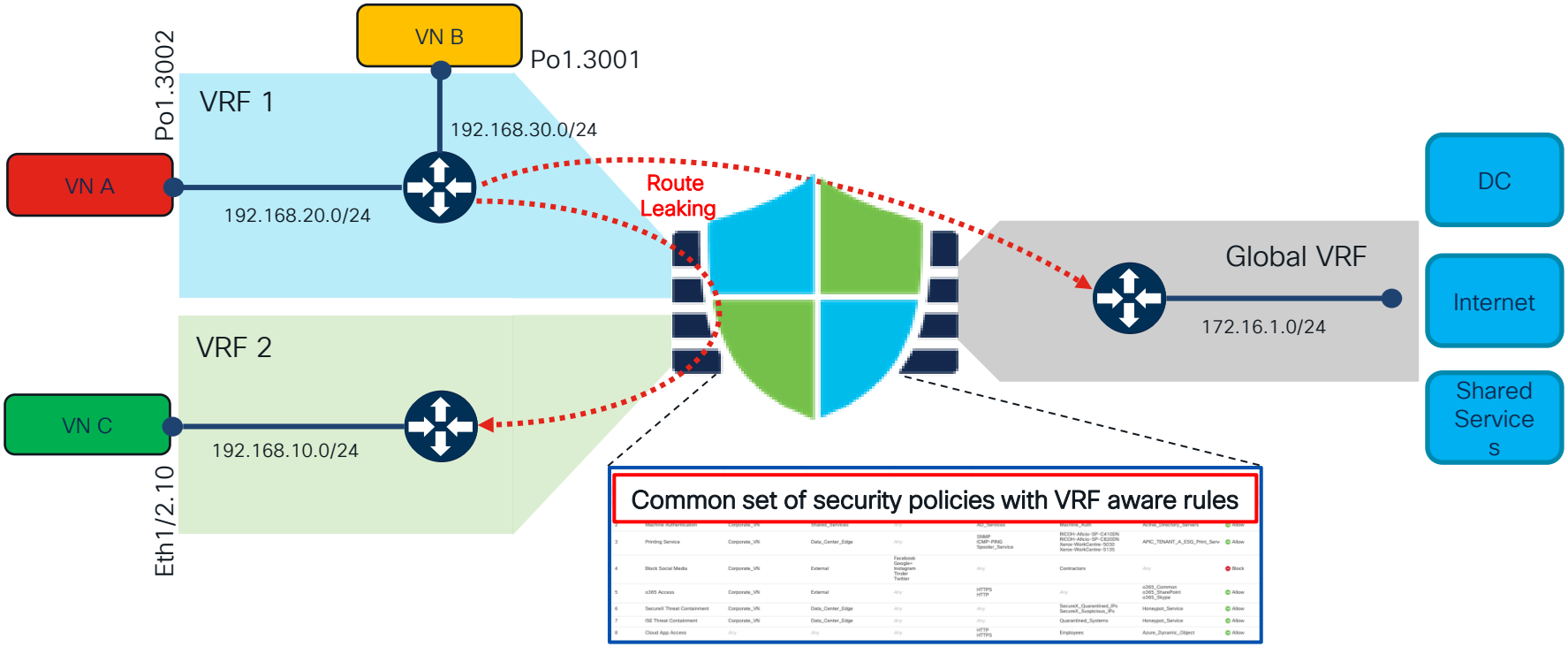
Multi-Instance



Multi-Domain



Virtual Router Basics



VRF Scaling

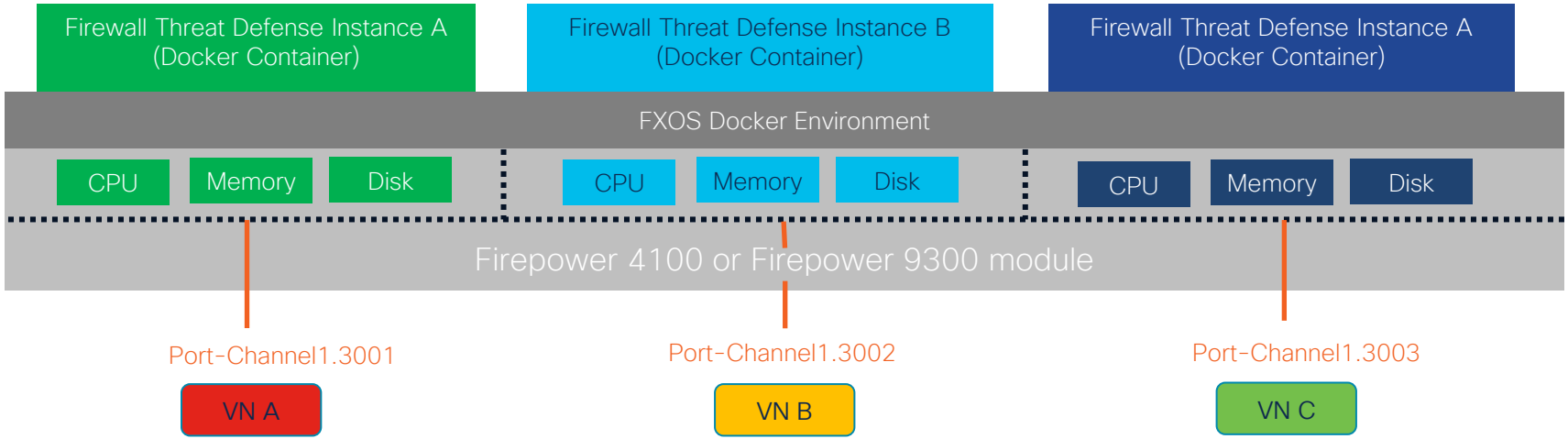
Device Model	Maximum Virtual Routers
Firepower 1010	N/A
Firepower 1120	5
Firepower 1140, 1150, 2110	10
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Firepower 4110, 4112	60
Firepower 4115, 4120	80
Firepower 4125, 4140, 4145, 4150	100
Firepower 9300 appliance, all models	100

Available with the base license on all platforms.

Number of virtual router per instance maps to % of core allocation to the instance.

Firepower 4100/9300 Multi-Instance

- Supported on Firepower 4100 and 9300 only
- 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

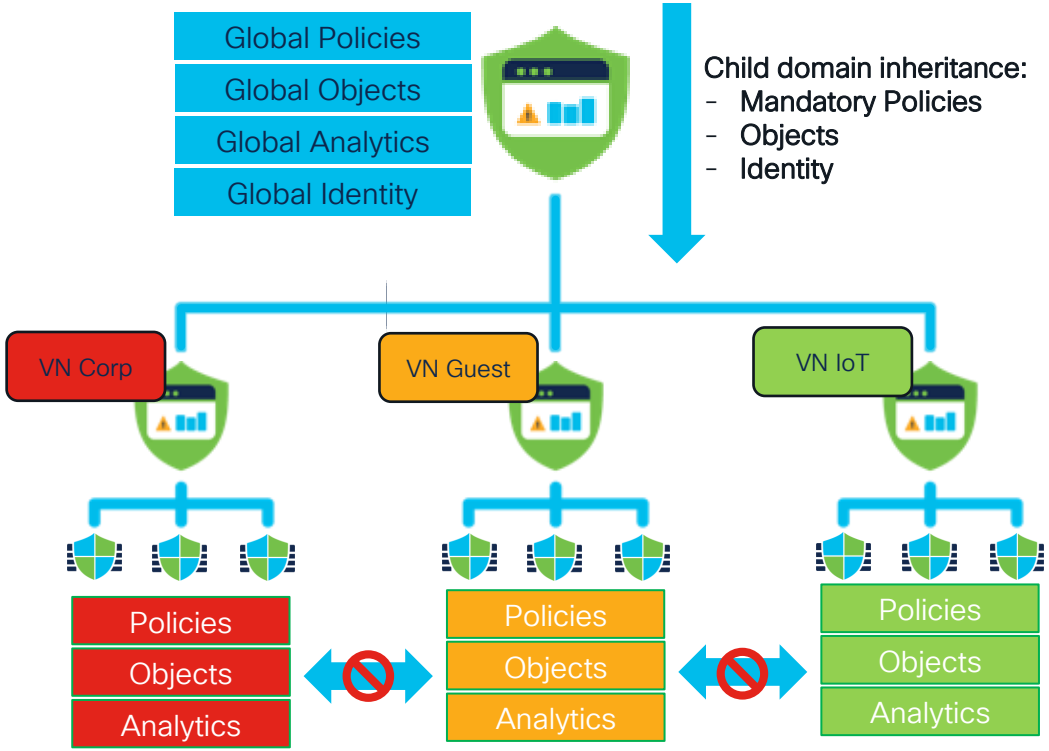


Multi-Instance Scalability

Platform	Total Application CPU Cores	Native CPU Core Allocation (Data Plane/Snort/System)	Total Application Disk	Maximum FTD Instances
Firepower 4115	46	16/28/2	350Gb	7
Firepower 4125	62	24/36/2	750Gb	10
Firepower 4145	86	32/52/2	750Gb	14
Firepower 9300 SM-24	46	20/24/2	750Gb	7
Firepower 9300 SM-36	70	32/36/2	750Gb	11
Firepower 9300 SM-40	78	32/44/2	1.55Tb	13
Firepower 9300 SM-44	86	36/48/2	750Gb	14
Firepower 9300 SM-48	94	40/52/2	1.55TB	15
Firepower 9300 SM-56	110	44/64/2	1.55TB	18

FMC Multi-Domain

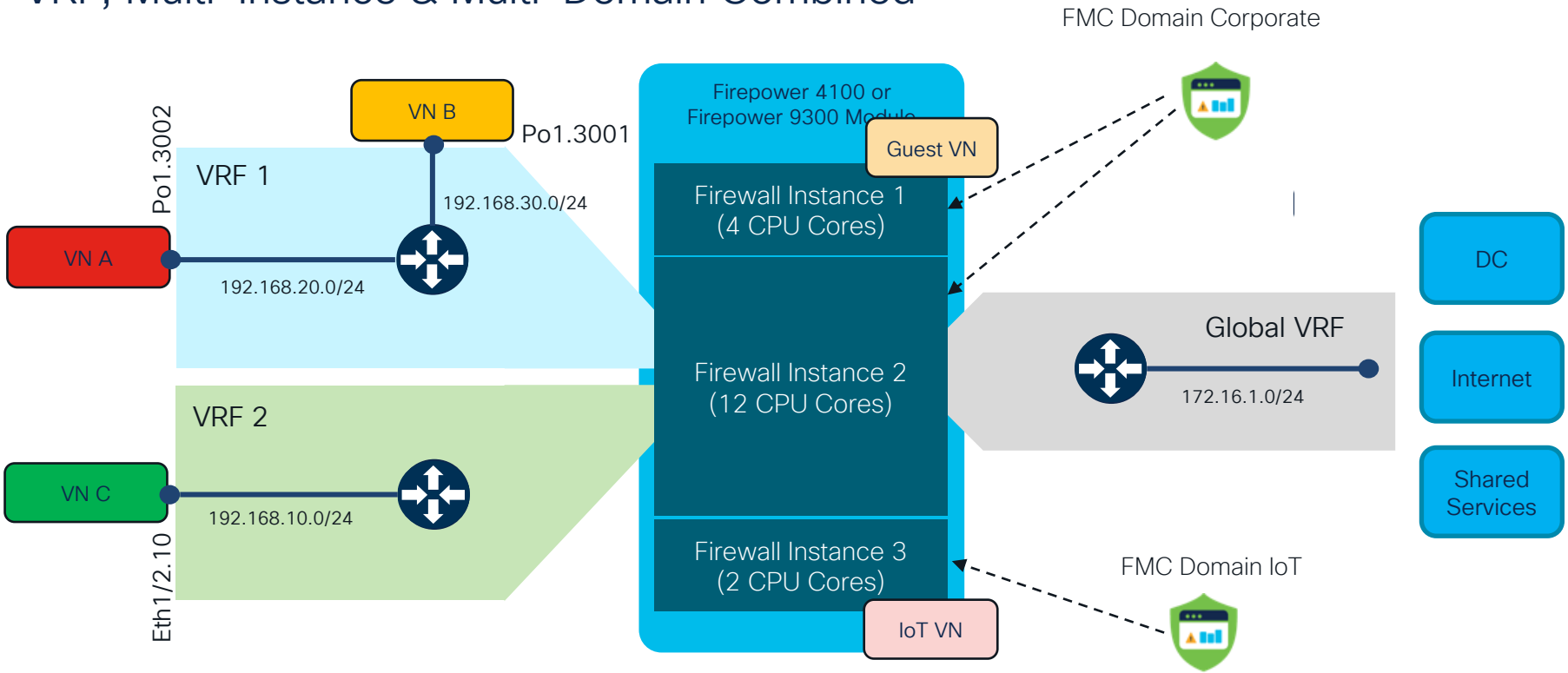
Supports up to 100 domains and 3 levels



Administration, Policy, Object and Eventing isolation

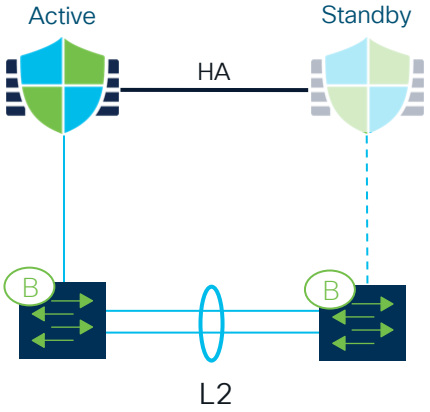
Putting it all together

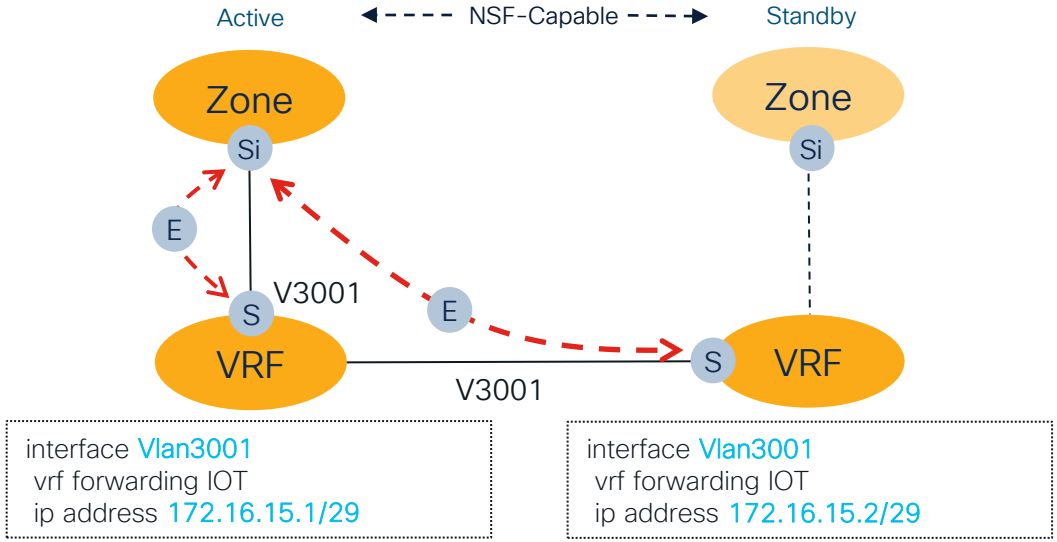
VRF, Multi-Instance & Multi-Domain Combined



Cisco Secure Firewall SDA Attachment Options

Direct FTD Attachment

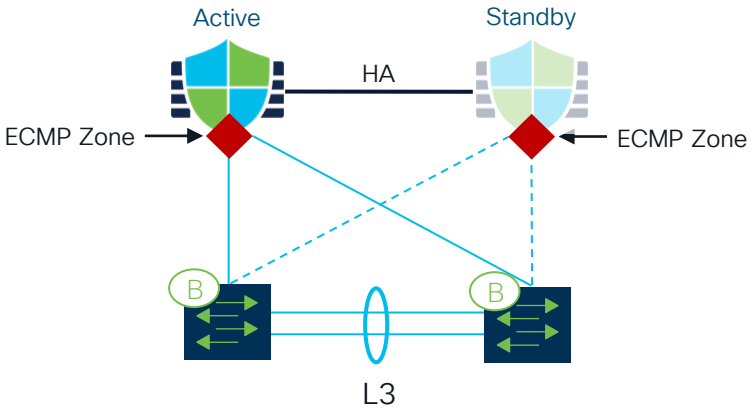


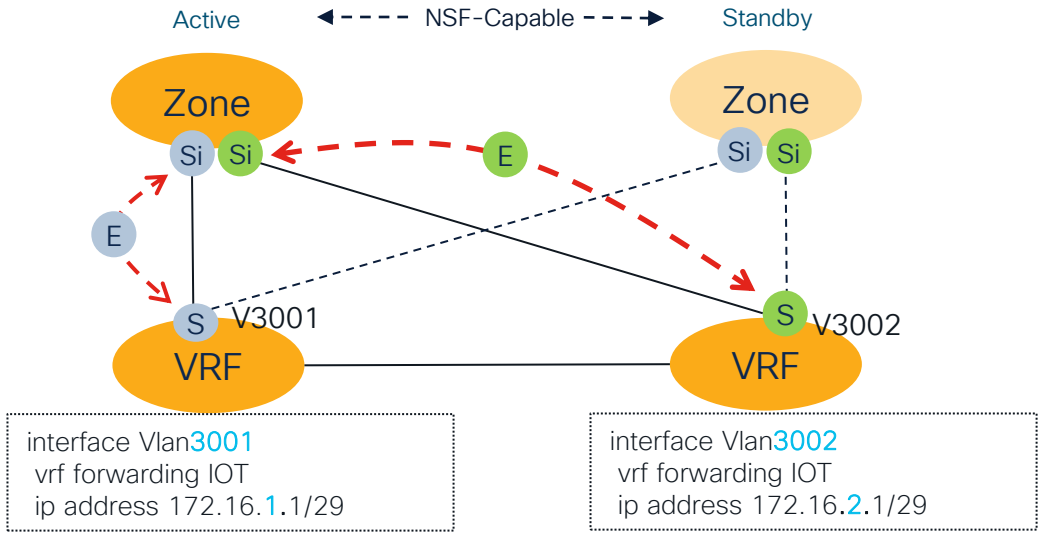


- L2 extension required between Border nodes – consider STP implications
- Active/Standby L2 adjacency with both Borders required
- Firewall Threat Defense supports BGP with NSF

Si sub-int
S SVI
E eBGP

Direct FTD Attachment with ECMP

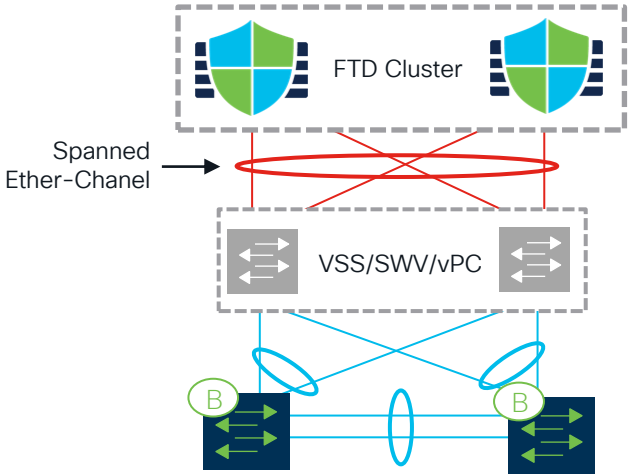


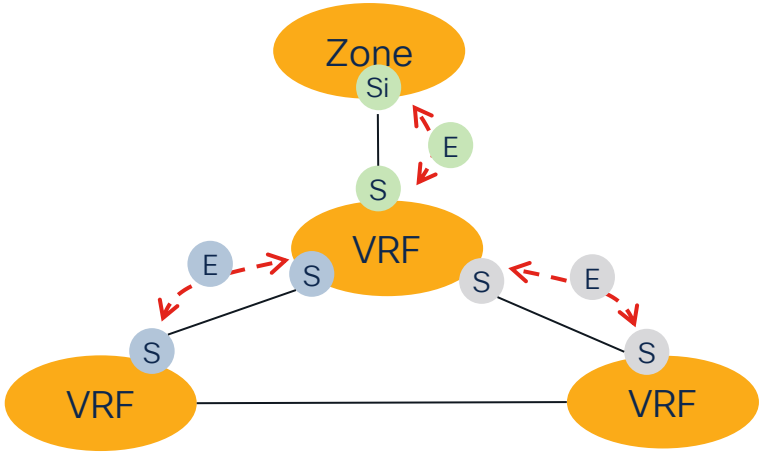


- ECMP Zone clubs together the interfaces and shares common connections table
- You can use both uplinks at the same time and support asymmetric flows across ECMP Zone
- ECMP is supported under global and VRFs on Firewall Threat Defense

Si sub-int
S SVI
E eBGP

FTD Cluster with Intermediate Switching Layer

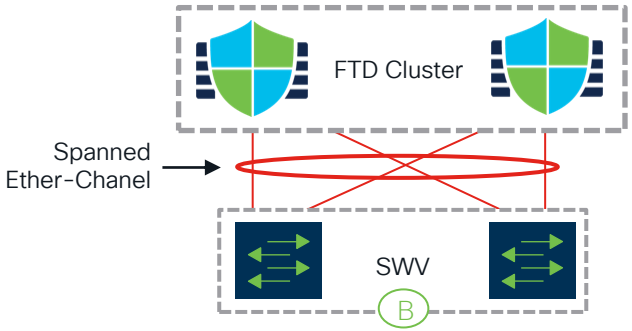


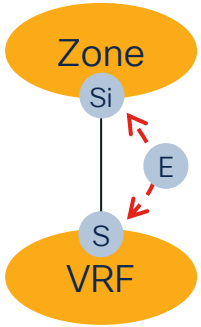


- Firewalls in a cluster symmetrize traffic for stateful NGFW/NGIPS services.
- Intermediate switches load-balance packets to Firewalls in the cluster over spanned Ether-Channel
- VRF and Multi-instance supported with clustering

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

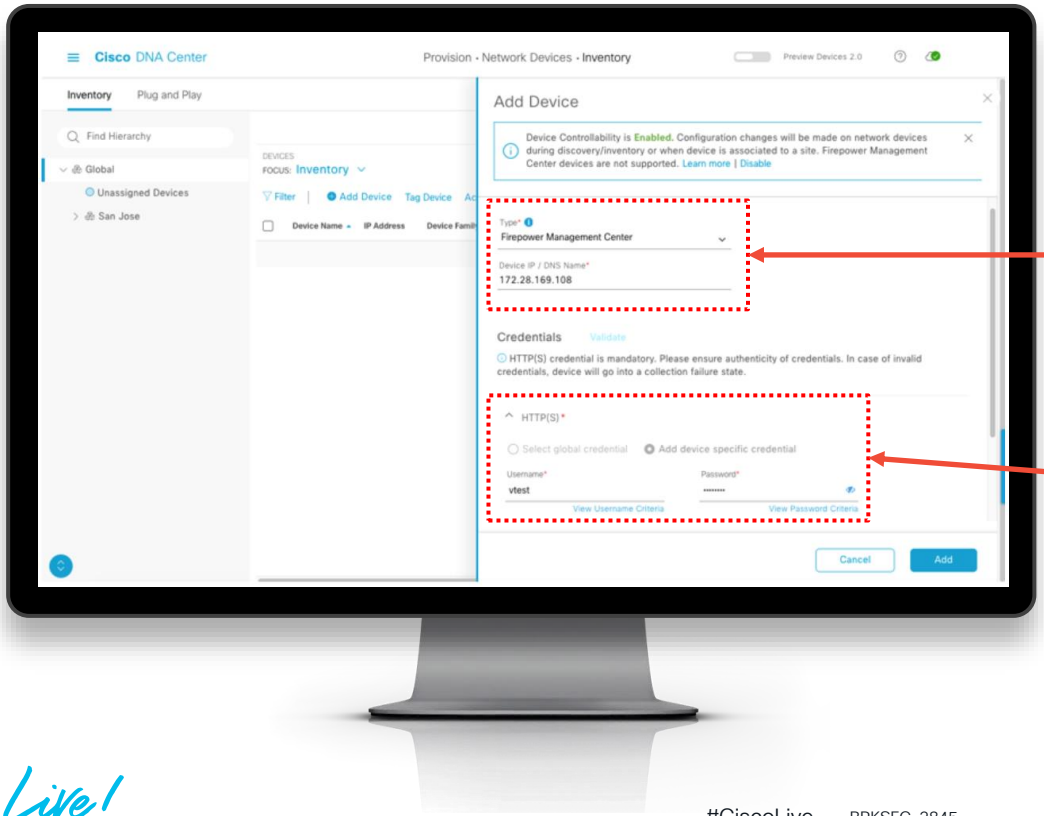
Si sub-int
S SVI
E eBGP

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
- Provisioning – you can assign an FTD to a site and with a Network Profile with basic firewall configuration i.e. mode, interface IP
- 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

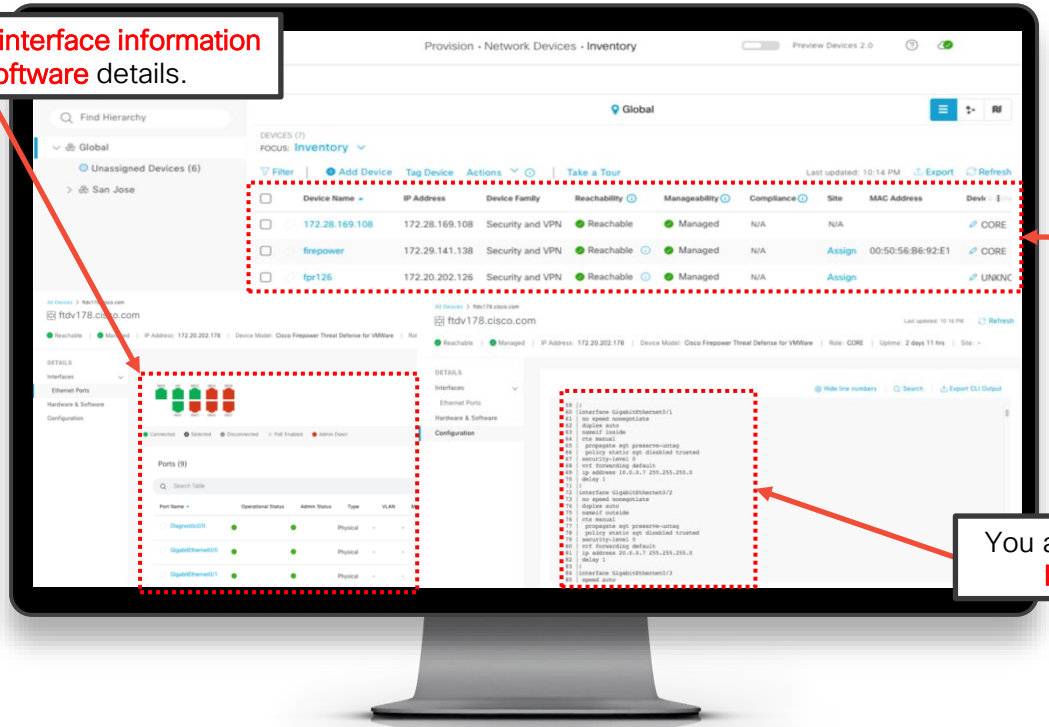


Use Firepower Management Center type and provide an IP Address.

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

Firewall in DNAC's Center Inventory

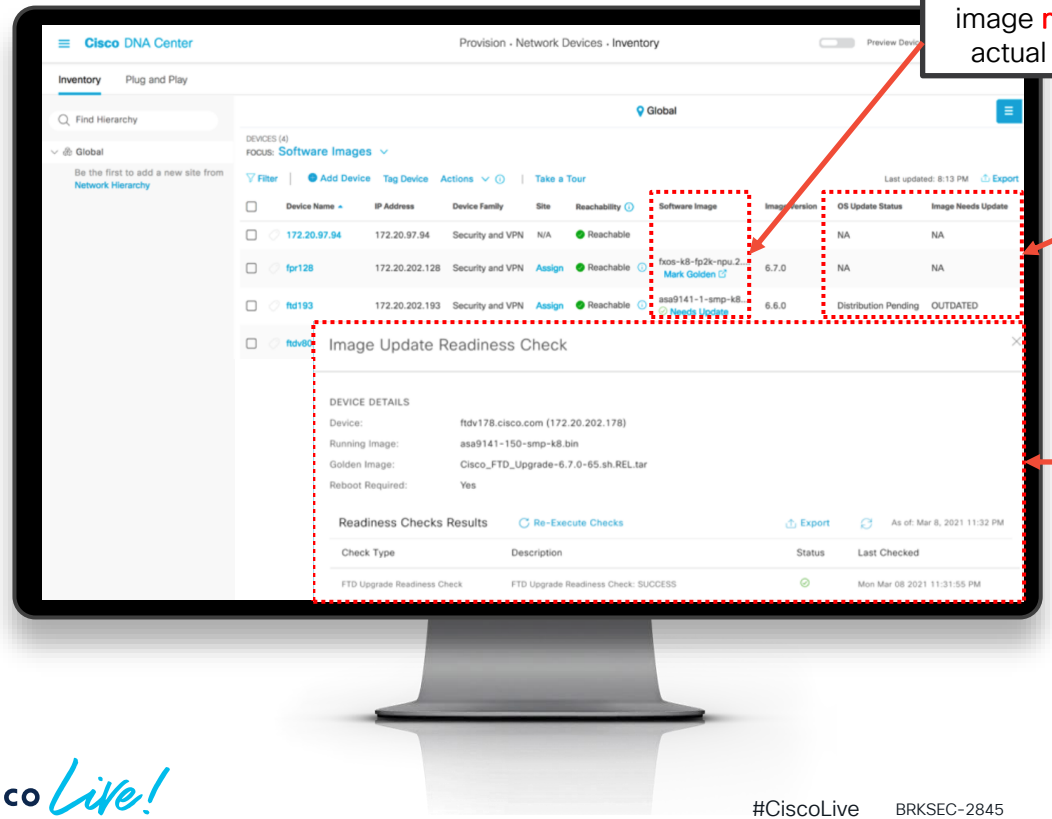
DNAC displays FTD's **interface information** and **hardware/software** details.



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



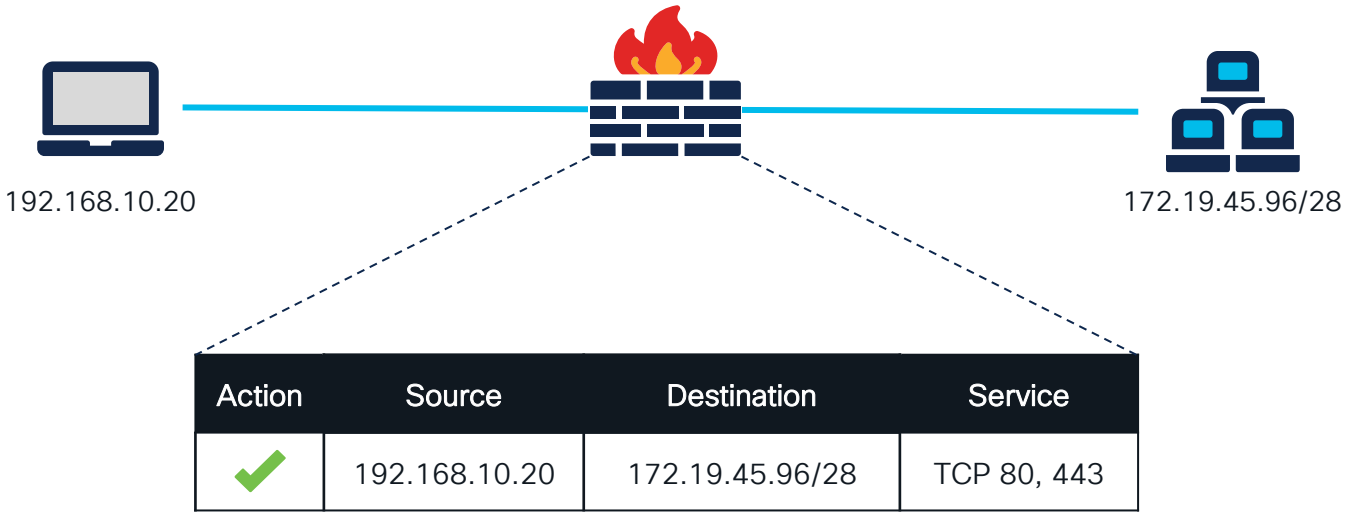
DNAC collects FMC and managed FTD's image **metadata** into image Repository. The actual image files are stored on the FMC.

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.

Attribute Based Policy

Traditional Firewall Policy is not Enough



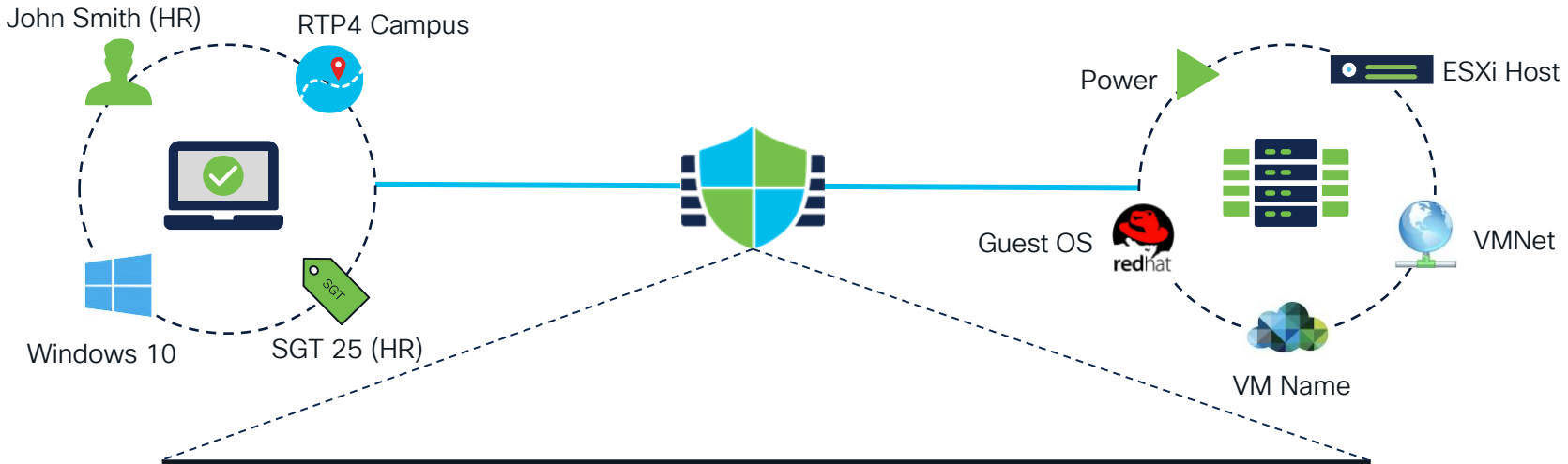
Action	Source	Destination	Service
✔	192.168.10.20	172.19.45.96/28	TCP 80, 443

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

Technology Insight for Network Security Policy Management

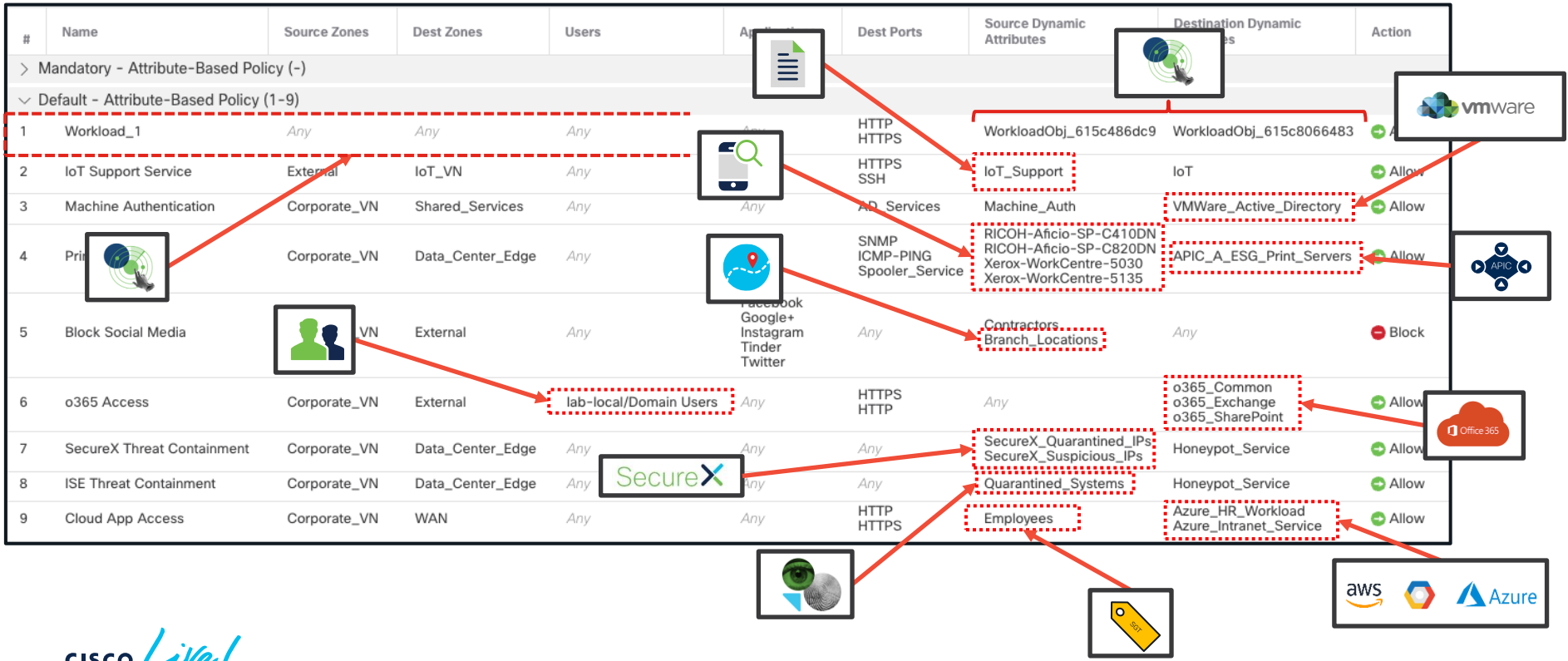
Gartner

Shift Towards Intent Based Policy

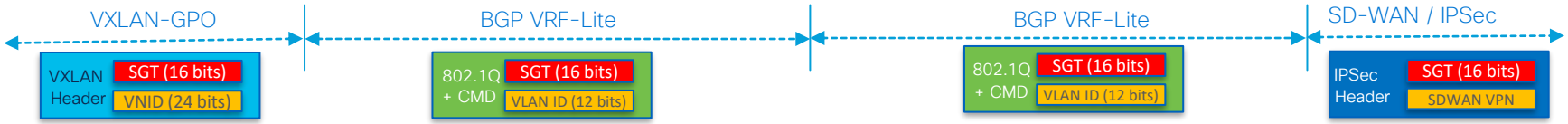


Action	Source	Destination	Service
✔	HR Users in RTP4 Campus on Windows10	PoweredOn servers in UAT VMNet containing HR-Prod in the VM Name	TCP 80, 443

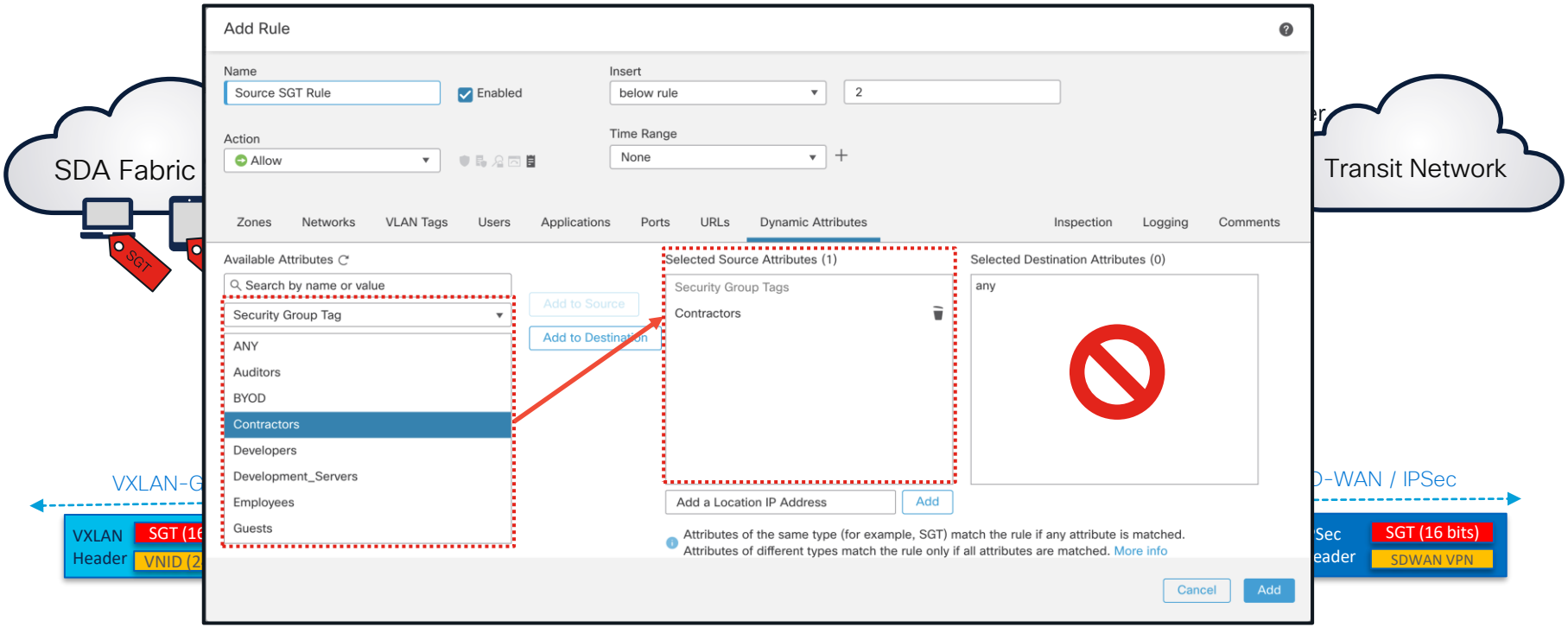
Set your Firewall Policy to adapt in real-time!



Inline Propagation

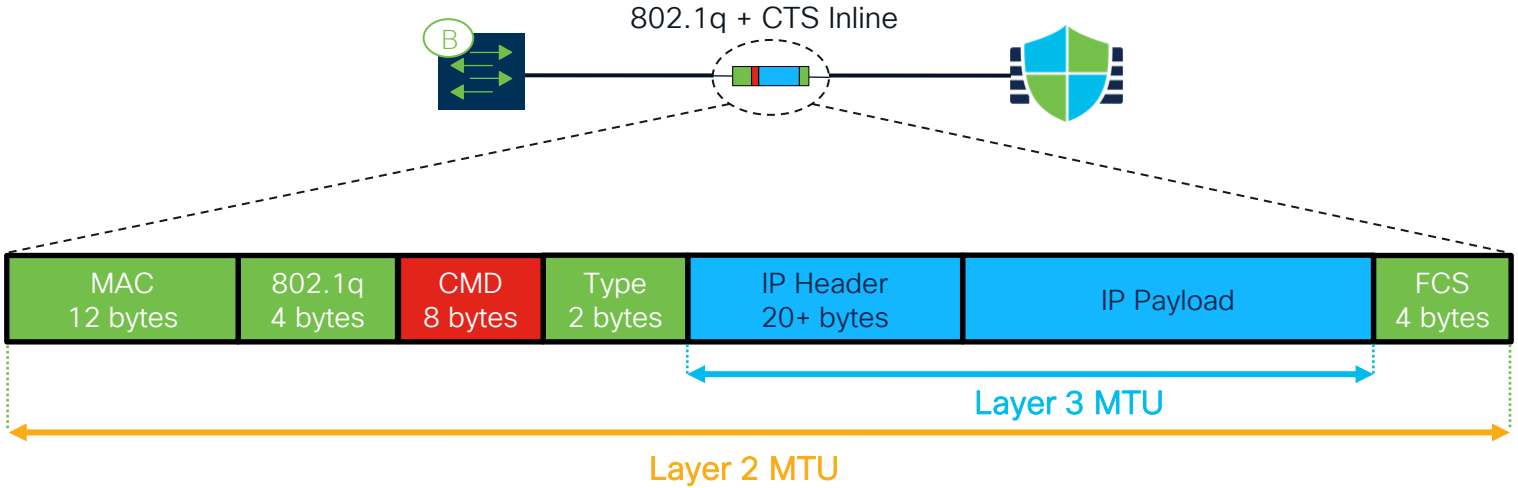


Inline Propagation



Note: Inline SGTs applicable for source criteria only

MTU Considerations

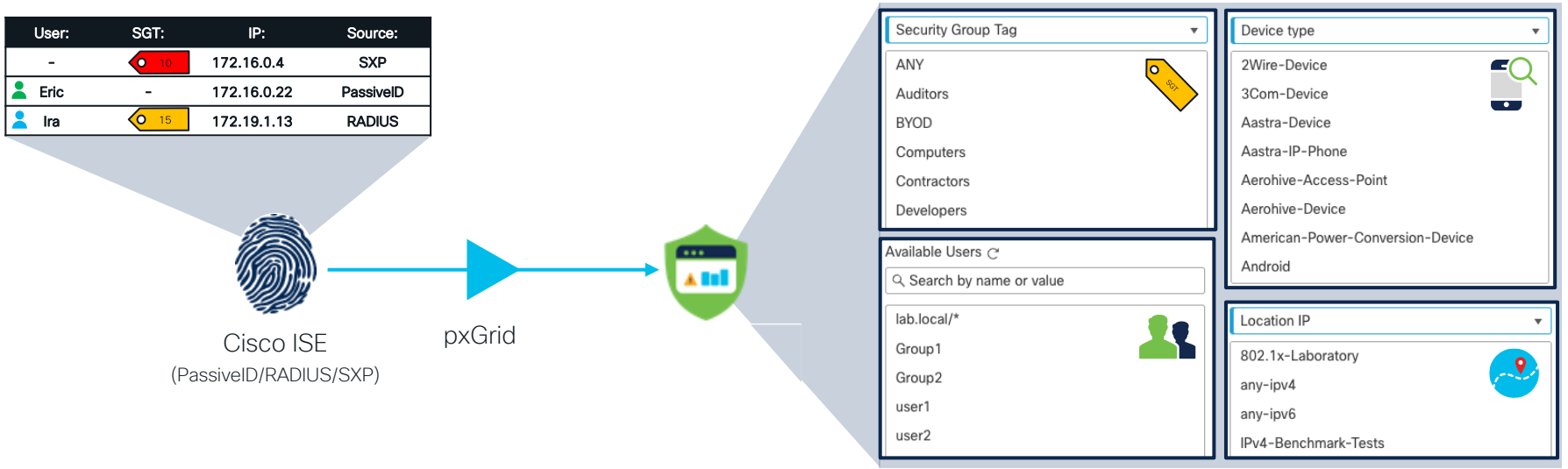


- The MTU on the FTD firewalls the is set up via FMC per interface using Layer 3 MTU.
- For **Firepower 4100/9300** platforms, maximum supported Layer 3 MTU is calculated as follows:

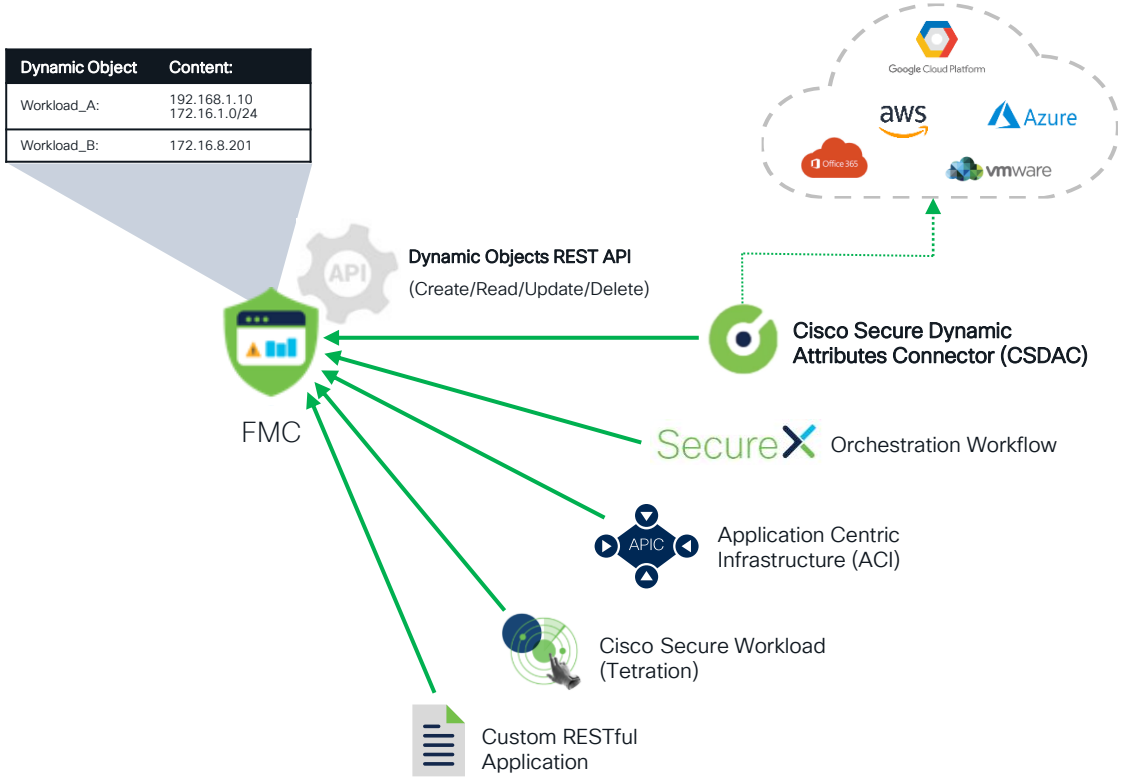
  L3 MTU = 9176 = L2 MTU (9206) – MAC (12B) – 802.1q (4B) – CMD (8B) – Type (2B) – FCS (4B)
- For **Firepower 1100/2100** platforms, maximum supported Layer 3 MTU is calculated as follows:

  L3 MTU = 9186 = L2 MTU (9216) – MAC (12B) – 802.1q (4B) – CMD (8B) – Type (4B) – FCS (4B)

Control Plane Propagation with pxGrid



Control Plane Propagation with Dynamic Objects



Dynamic Objects in Action

Cisco Secure Dynamic Attributes Connector

REST API
(Add 10.0.0.5 to Workload_A)

FMC

SFtunnel Update
(Without policy deployment)

Managed Firewall

Dynamic Object	Content:
Workload_A:	10.0.0.4 10.0.0.5

```
----------------
Host ::ffff:10.0.0.4
----------------
ABP values:  1

----------------
Host ::ffff:10.0.0.5
----------------
ABP values:  1

------------------
ABP NAME-TO-ID MAPPING:
------------------
Workload_A  1
```

Workload A

aws vmware Azure

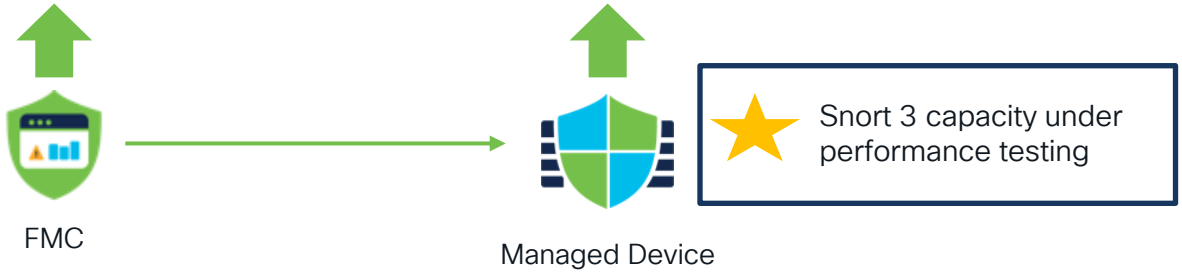
10.0.0.4 10.0.0.5

Dynamic Feed Update

Scaling Firewall Identity Mappings

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

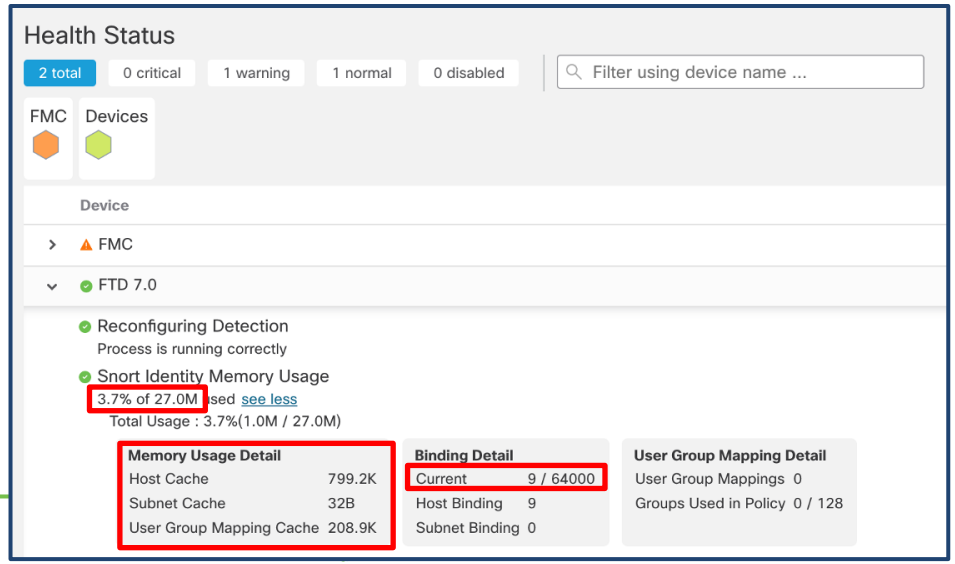
FTD Model	Maximum Concurrent User Logins (Snort2)★
FTDv	64,000
Firepower 1010, 1120, 1140, 1150 Firepower 2110, 2120, 2130, 4110	64,000
Firepower 2140, 4112, 4115, 4120, 4125	150,000
Firepower 4140, 4145, 4150, 9300	300,000



Scaling Firewall Identity Mappings

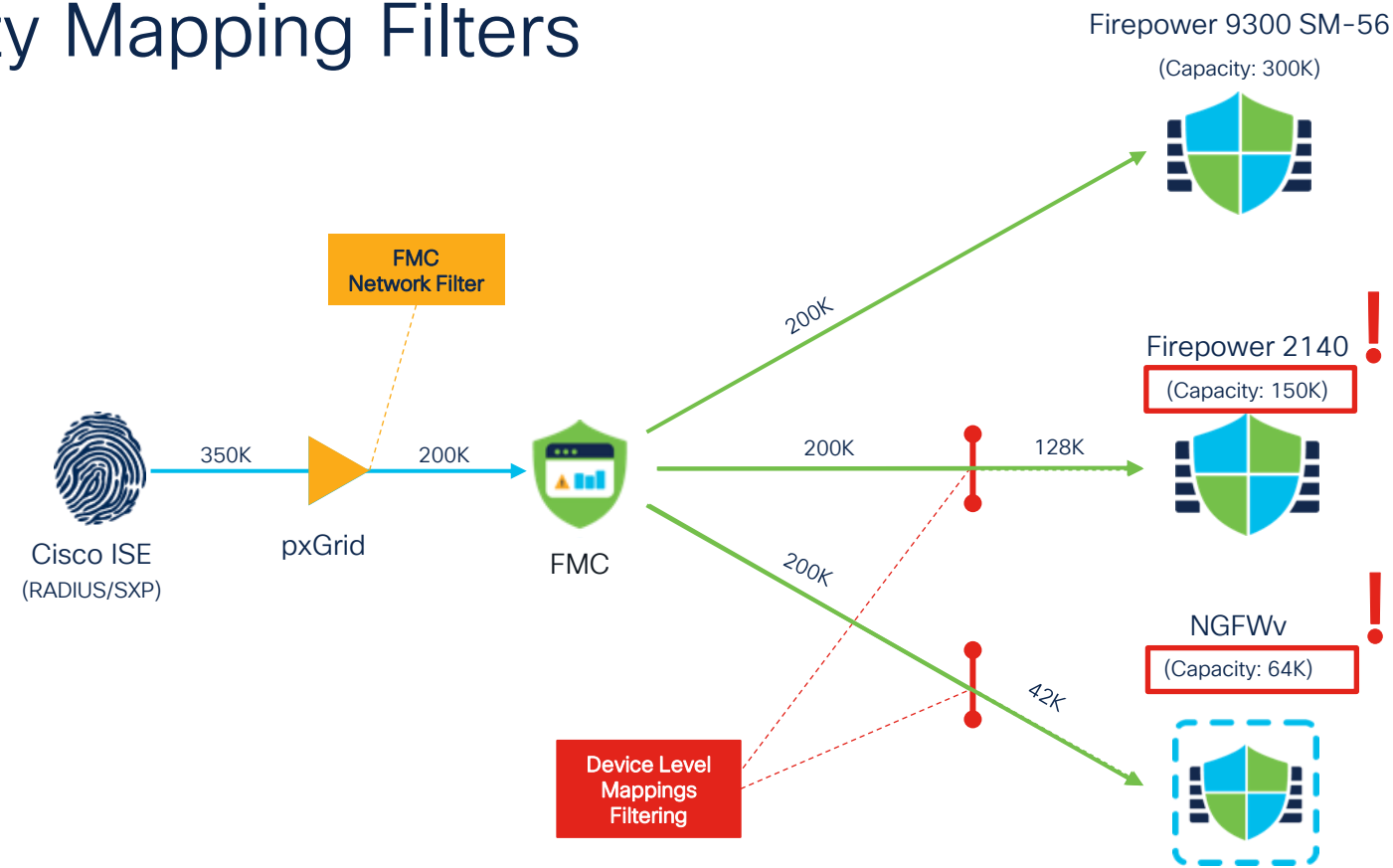
FMC Model	Maximum Downloaded Users (Snort2)★
FMC1000, FMC1600	50,000
FMC2500, FMC2600	150,000
FMC4500, FMC 4600	600,000
FMCv	50,000
FMCv 300	150,000

FMC

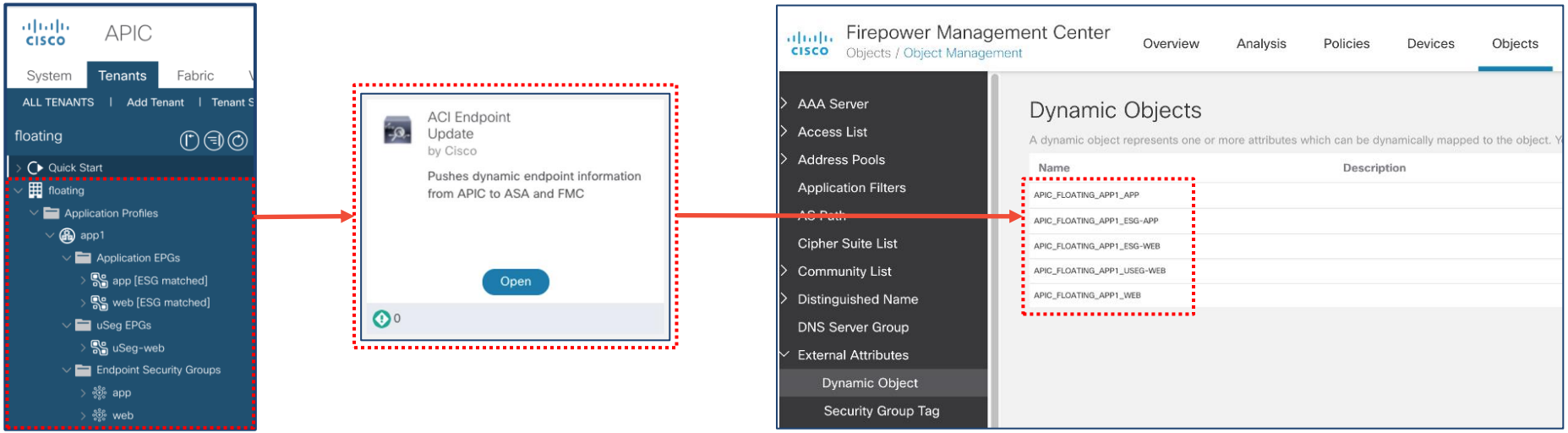


Managed Device

Identity Mapping Filters



ACI Endpoint Update App 2.0

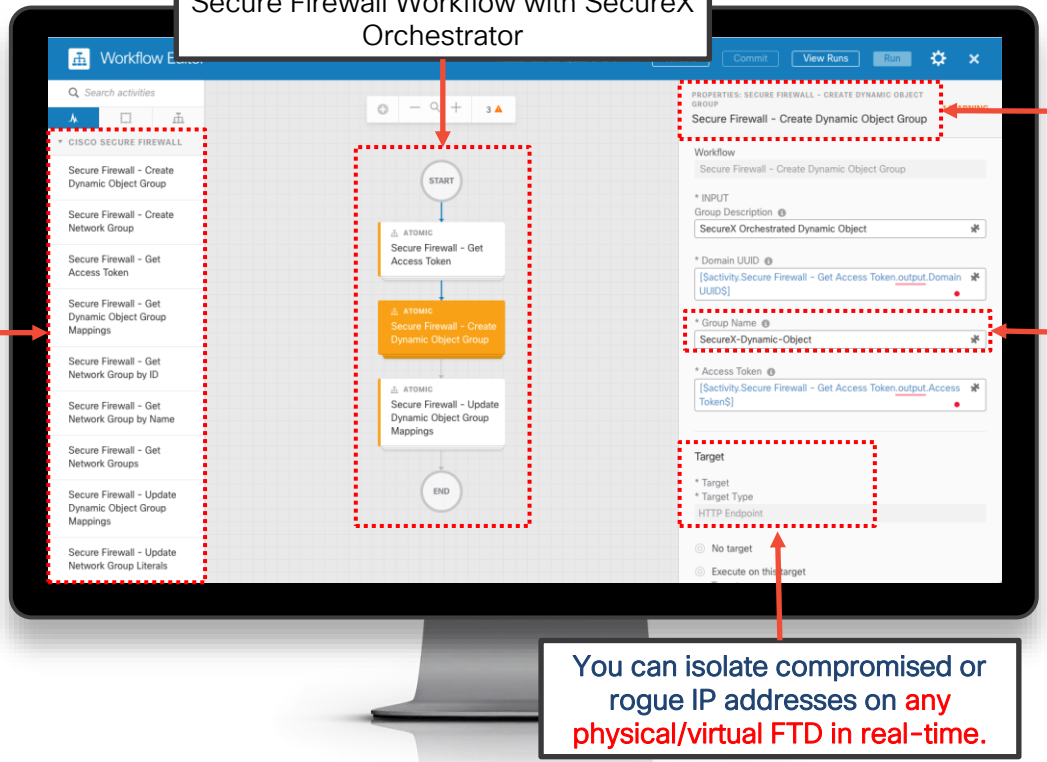


ACI Endpoint Update App is Compatible with FMC 6.7 and above:

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

SecureX Orchestration with Dynamic Objects

Import or create your own Cisco Secure Firewall Workflow with SecureX Orchestrator



Atomic actions to manipulate Dynamic Objects are pre-defined in SecureX.

Cisco Secure Firewall atomic actions section provides a set of common action

Dynamic Objects are often used in Remediation Workflows to block IP addresses.

You can isolate compromised or rogue IP addresses on any physical/virtual FTD in real-time.

Identity Propagation Practical Use-Cases

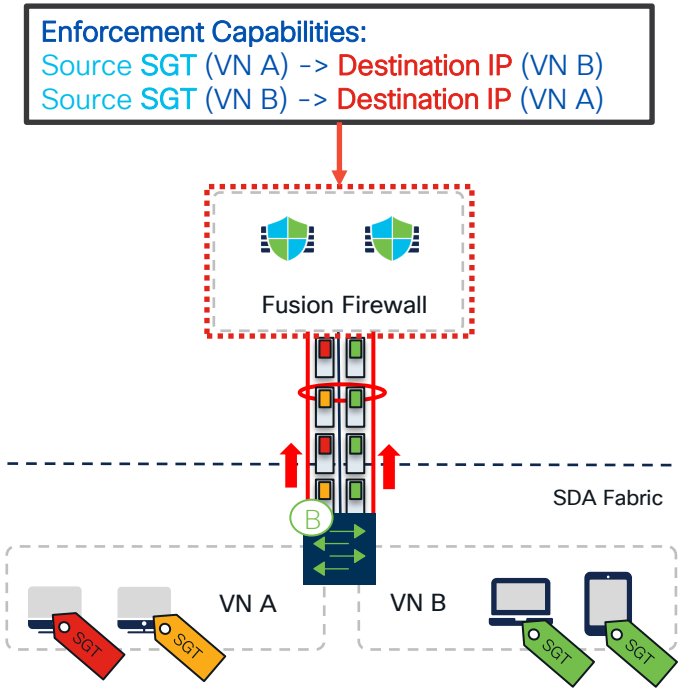
Inter-VN Attribute Based Policy
(Inline Tagging)

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



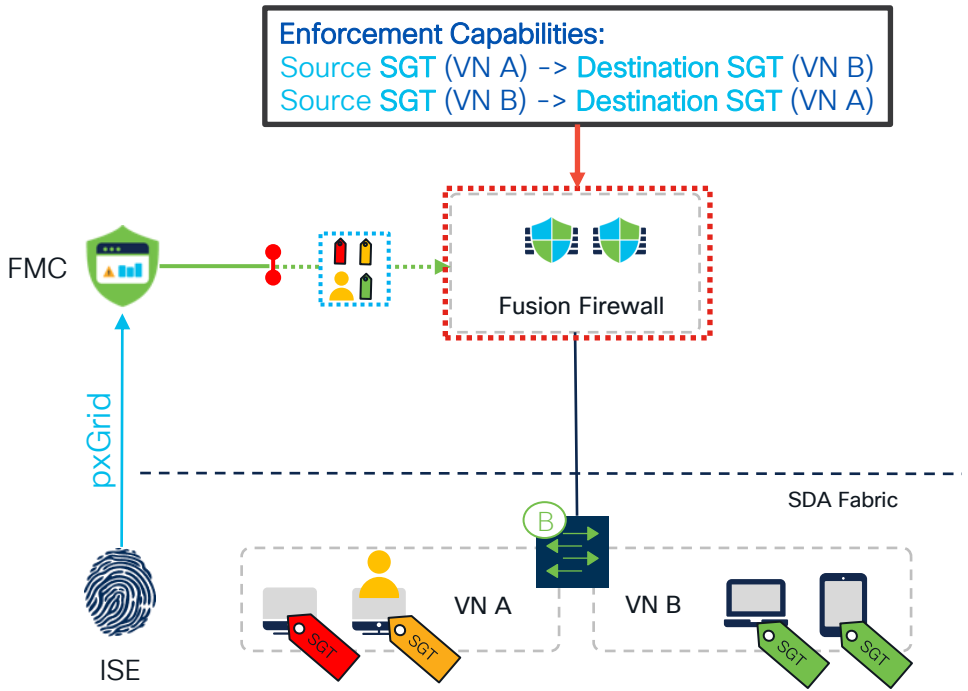
Inter-VN Attribute Based Policy
(Control Plane Propagation)

Key Benefits

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



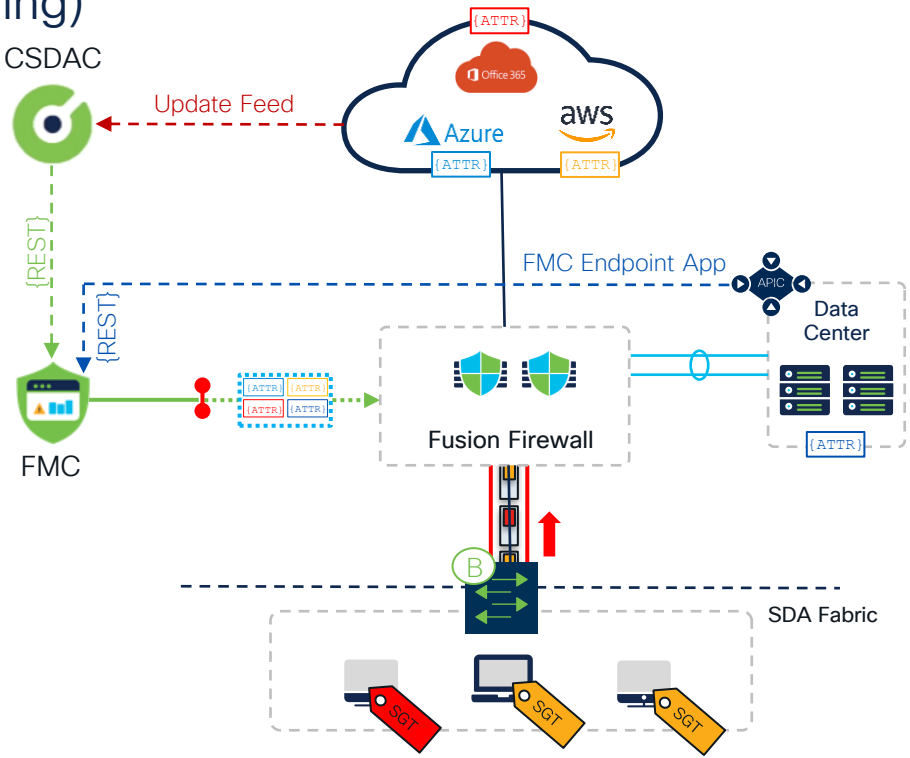
DC/Cloud Access Attribute Based Policy
(Control Plane Propagation & Inline Tagging)

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
- In case of heavy updates via REST API use FMC's bulk update: maximum 1000 entries and less than 2MB in payload per single request



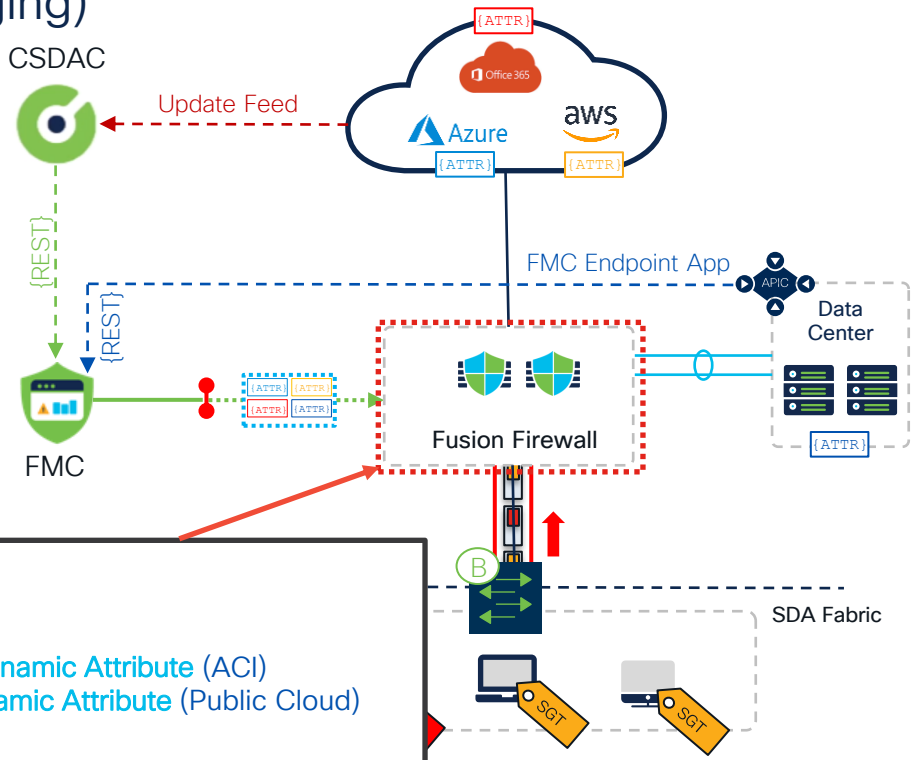
DC/Cloud Access Attribute Based Policy
(Control Plane Propagation & Inline Tagging)

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
- In case of heavy updates via REST API use FMC's bulk update: maxim and less than 2MB in paylo request



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)

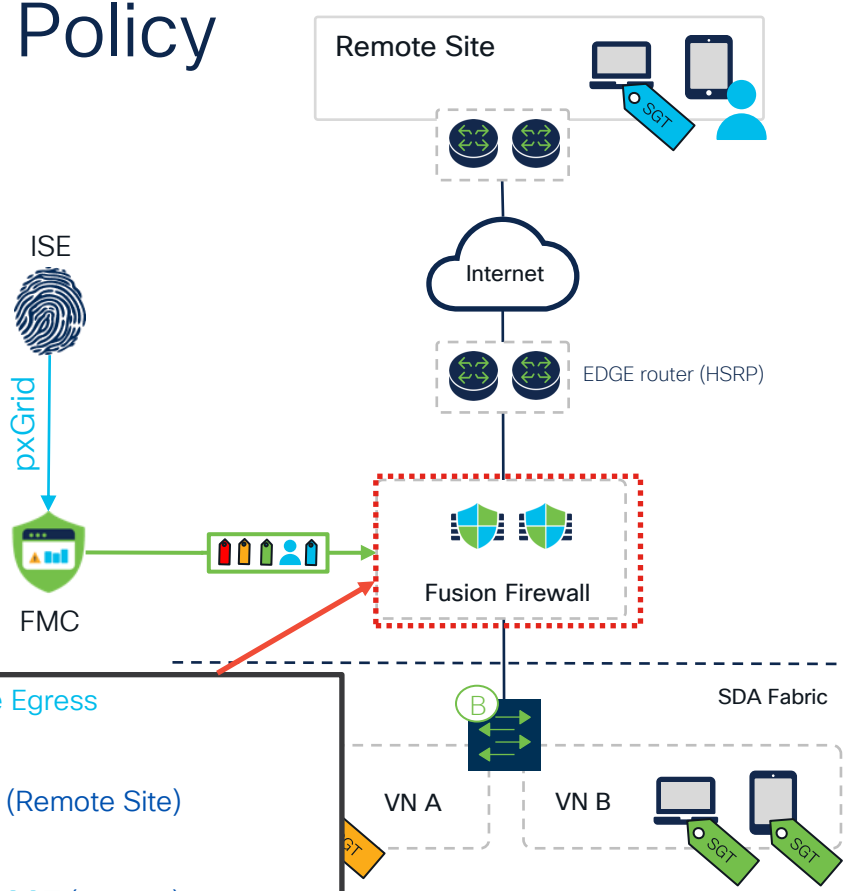
Inter-Site Attribute Based Policy
(Control Plane Propagation)

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)

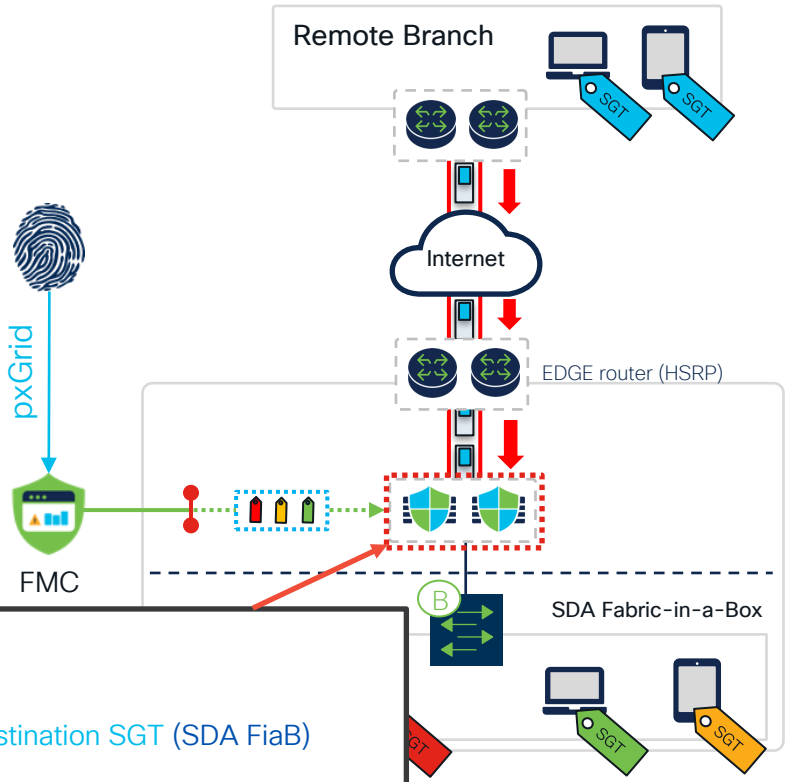
Scalable Branch-to-Branch
(Control Plane Propagation & Inline Tagging)

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

Conclusions

Cisco Secure Firewall provides a comprehensive integration with SDA

- After this session think how you can make your firewall policy dynamic, more secure and easier to manage with CSDAC and Attribute-Based Policy.

- Consider benefits of VRF, Multi-Instance and Multi-Domain firewall virtualization options and choose optimum attachment model.

- Review identity propagation techniques to make the most out of the available dynamic attributes.

Where to Go Next

- BRKSEC-2123 - Solving the Segmentation Puzzle! Secure Workload and Secure Firewall Integration
- BRKSEC-2127 - Making Cisco Secure Firewall Threat Defense Policy Dynamic with Attribute Based Policy
- BRKSEC-2201 - SecureX and Secure Firewall Better Together
- BRKSEC-2236 - Keeping Up on Network Security with Cisco Secure Firewall
- BRKSEC-2709 - Why 1+1 = 3 when using FTD in ACI
- LABSEC-2330 - Bridging the gap between Cloud and On-Prem with SecureX Orchestration Remote

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

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

cisco Live!

Thank you


cisco Live!
ALL IN