

CISCO *Live!*



#CiscoLive



The bridge to possible

Making Cisco Secure Firewall Threat Defense Policy Dynamic with Attribute Based Policy

Christopher Grabowski, Technical Marketing Engineer
BRKSEC-2127

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 June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2127>

Your Speaker



Christopher Grabowski
Technical Marketing Engineer
CCIE Security #42466

Based in Warsaw, Poland

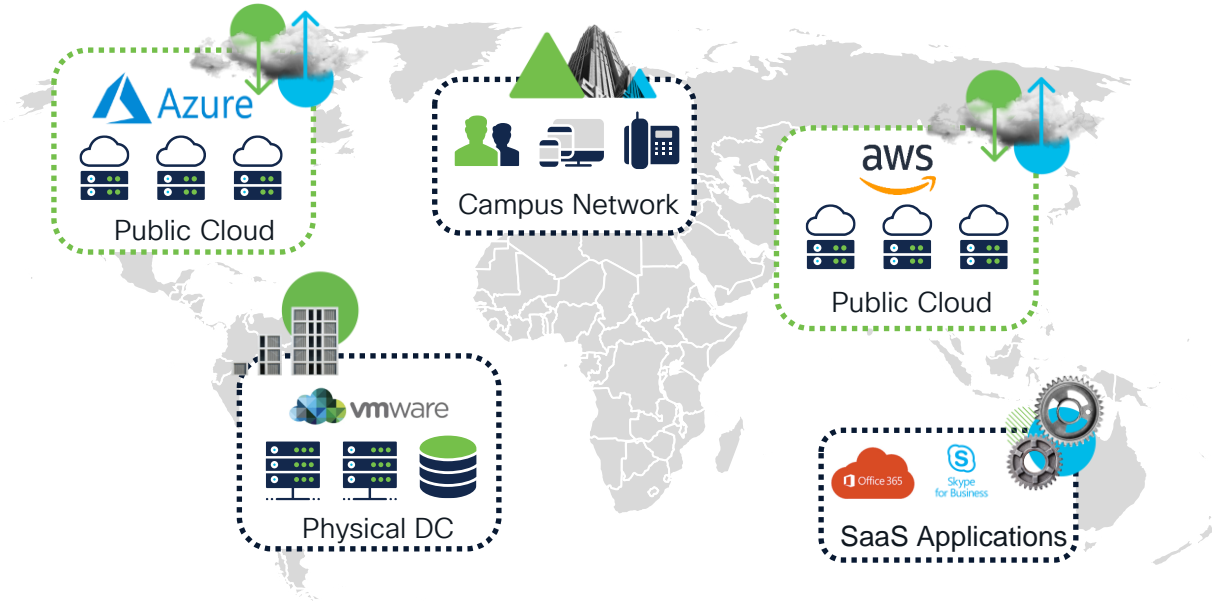
With Cisco since May 2012

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

Focusing on Identity Firewall and SDA/ACI Integration

Enjoys cooking and spending time with the family


Managing Firewall Policy is a Cumbersome Task



PROTECTED ASSET COUNT: 

FIREWALL POLICY SIZE: 

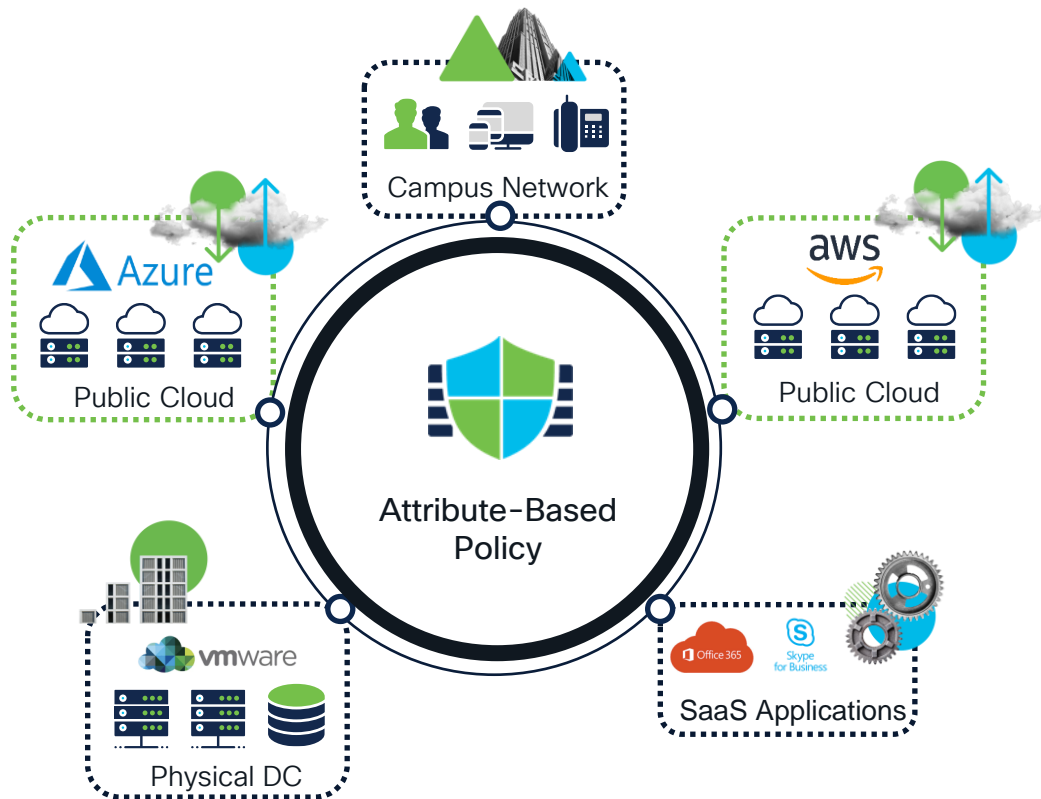
SECOPS TEAM: 



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

Technology Insight for Network Security Policy Management
Gartner

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

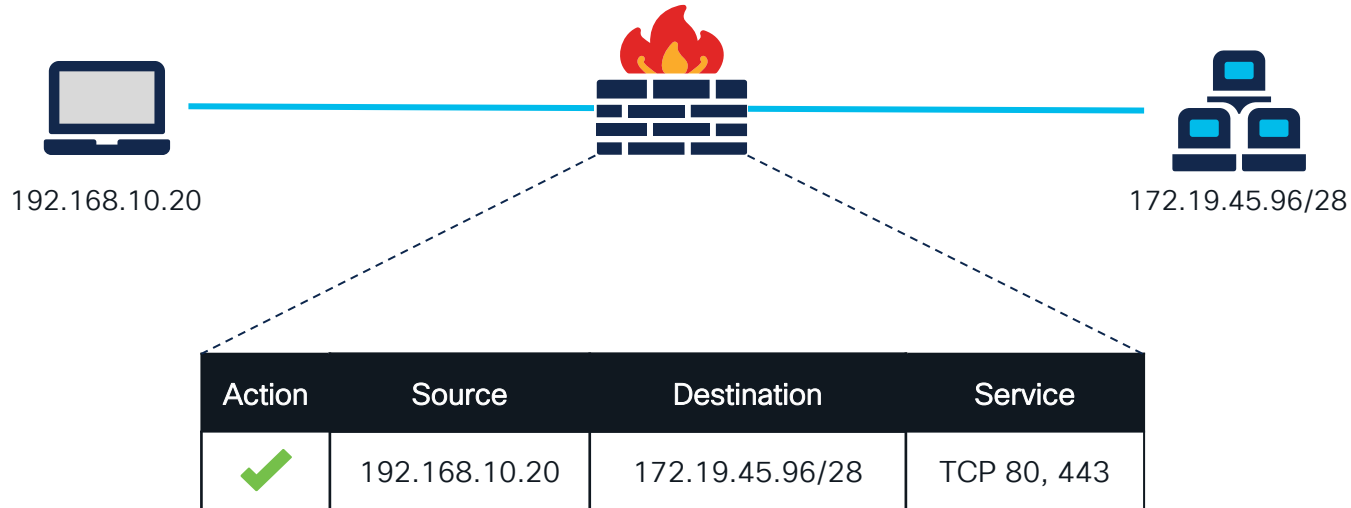


Agenda

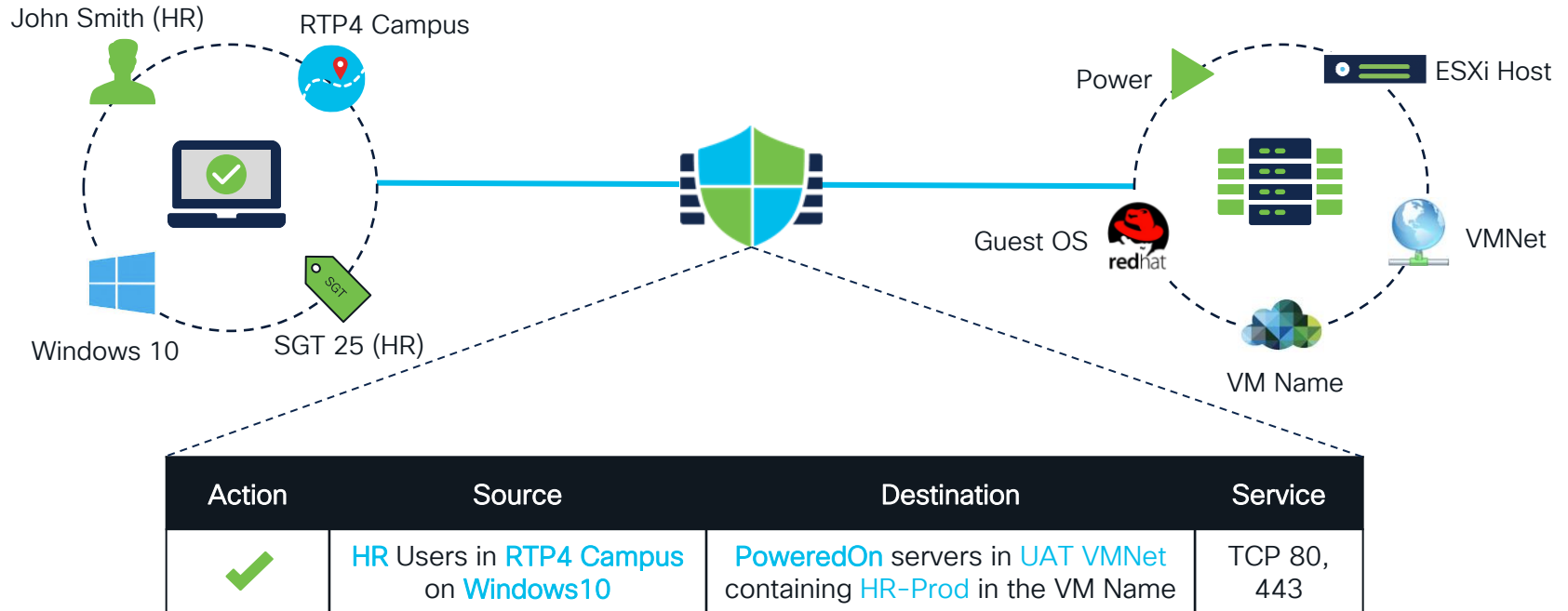
- Introduction
- Inline SGT and ISE Attributes
- Cisco Secure Dynamic Attributes Connector & Demo
- Cisco Secure Workload and ACI Attributes
- SecureX Integration
- Dynamic Objects REST API
- Conclusions

Introduction

Traditional Firewall Policy is not Enough



Shift Towards Intent Based Policy

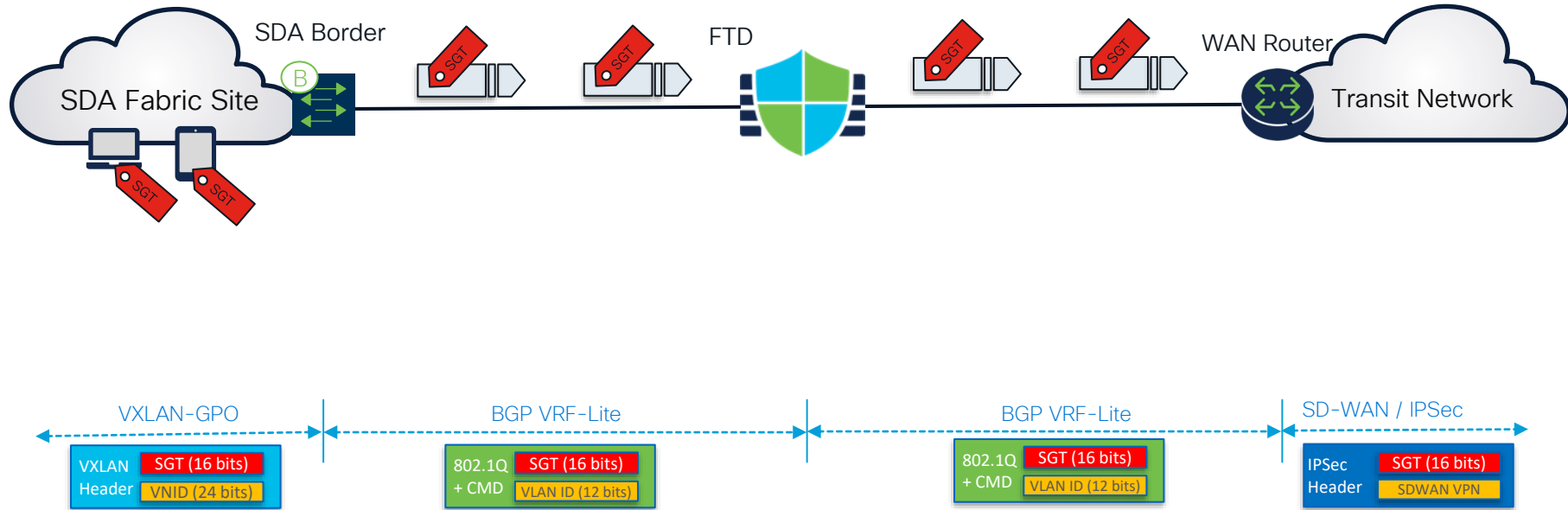


Attribute Based Policy

#	Name	Source Zones	Dest Zones	Users	App. Prot.	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

Attribute-Based Policy Dynamic Attribute Sources

Inline Propagation



Inline Propagation

Add Rule

Name: ☒ Enabled

Insert:

Action:

Time Range:

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

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

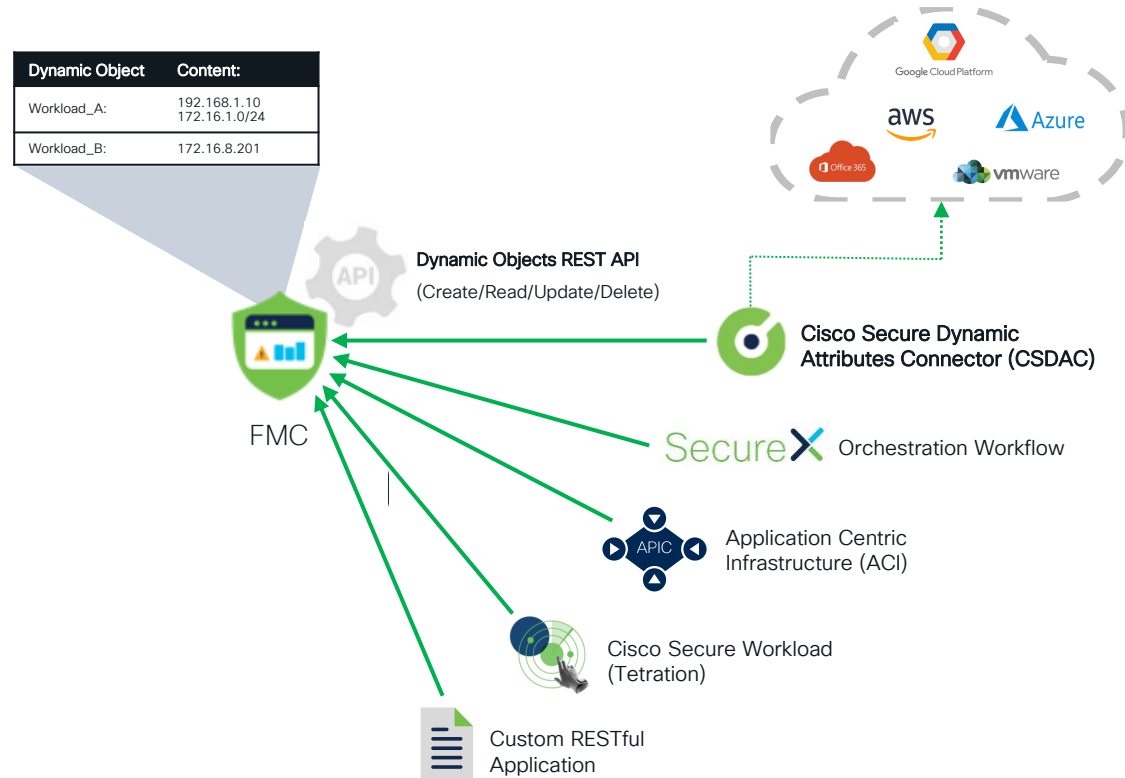
802.1x-Laboratory
any-ipv4
any-ipv6
IPv4-Benchmark-Tests



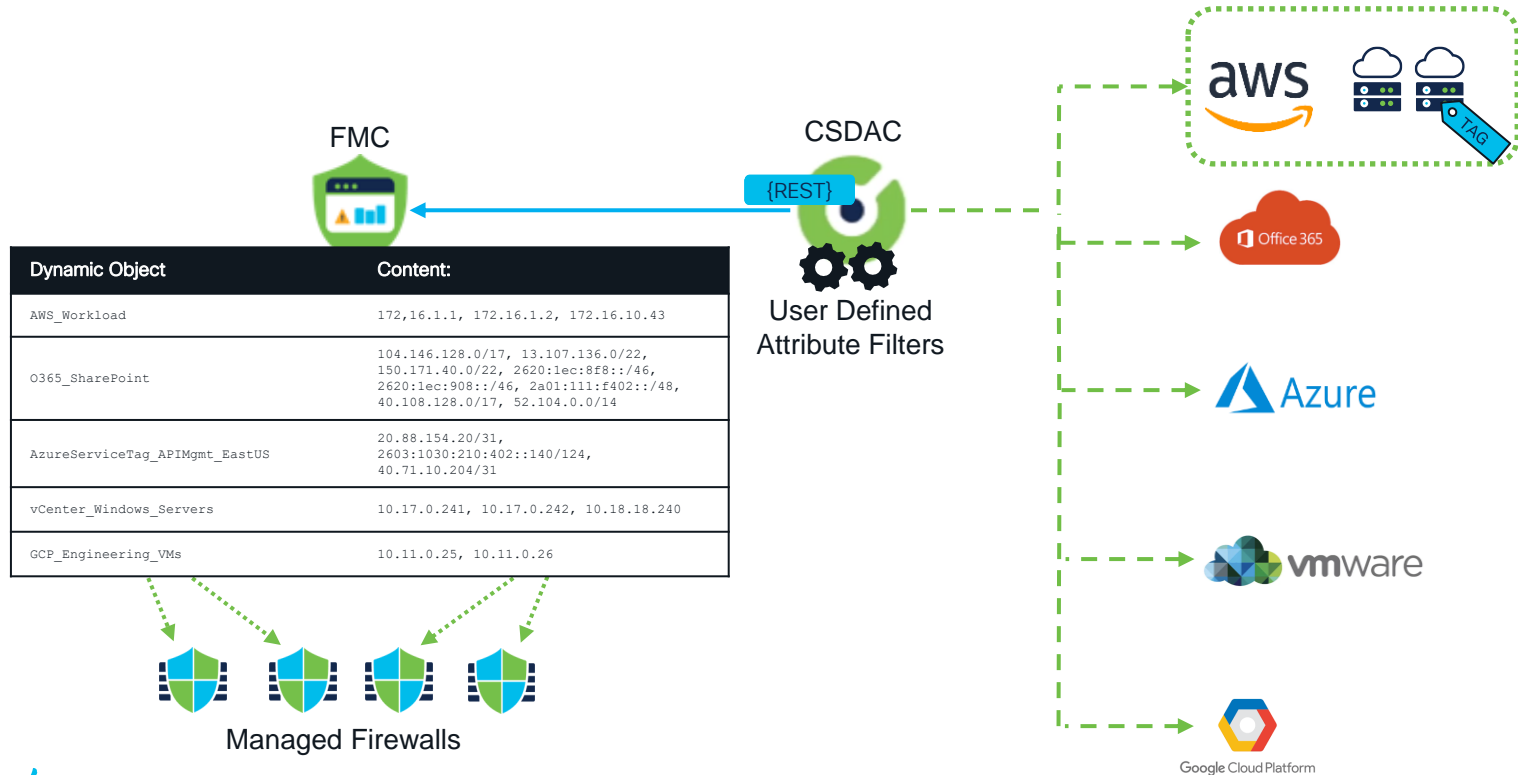
Attribute Based Policy – ISE Context Objects

#	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	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	HoneyPot_Service	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

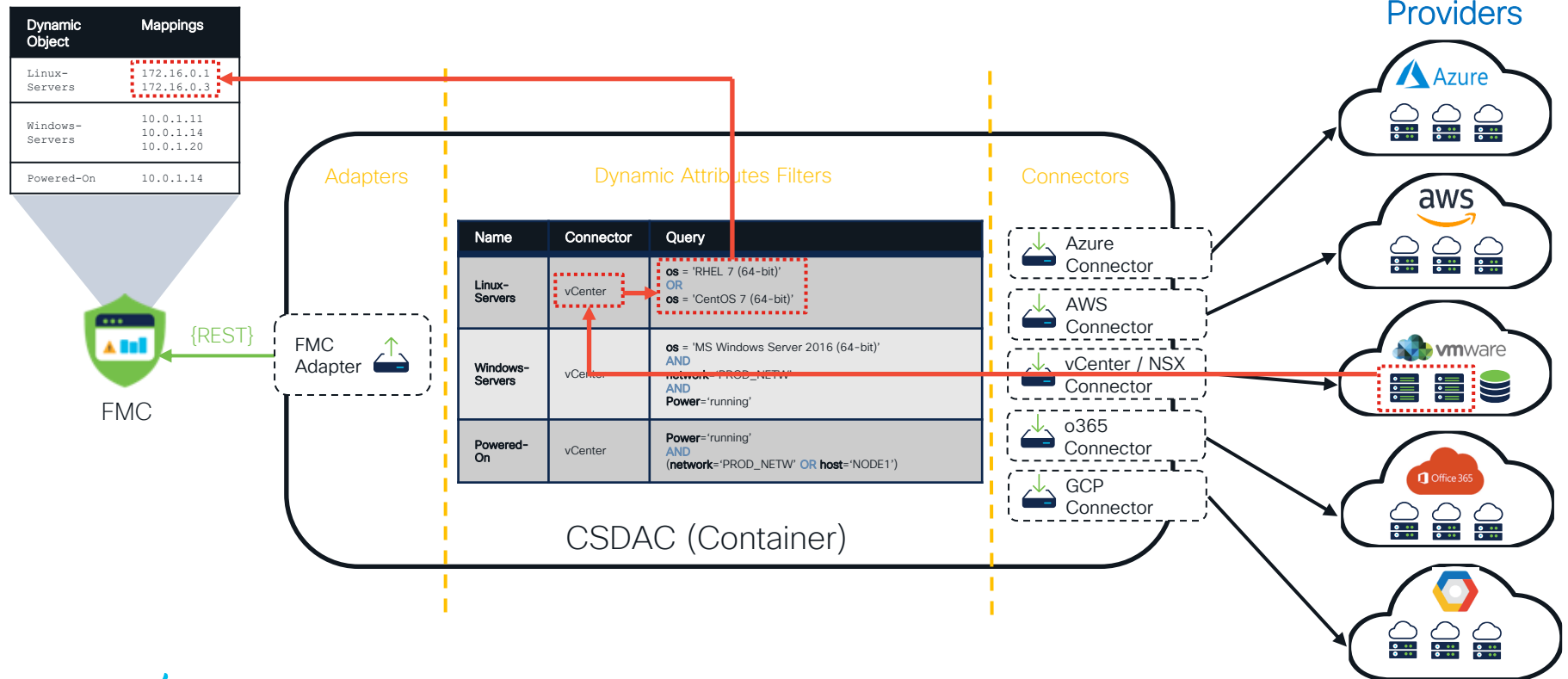
Control Plane Propagation with Dynamic Objects



CSDAC Keeps Track of IP Changes in the Cloud



Architecture of the Dynamic Attributes Connector



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

Workload A

#	Name	Source Networks	Dest Networks	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action	
Mandatory - Secure Policy (1-1)								
1	Workload A	Any	Any	HTTPS	Any	Workload_A	Allow	

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
```

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 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 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	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	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

vCenter / NSX
Dynamic Objects



o365 Public
Feeds



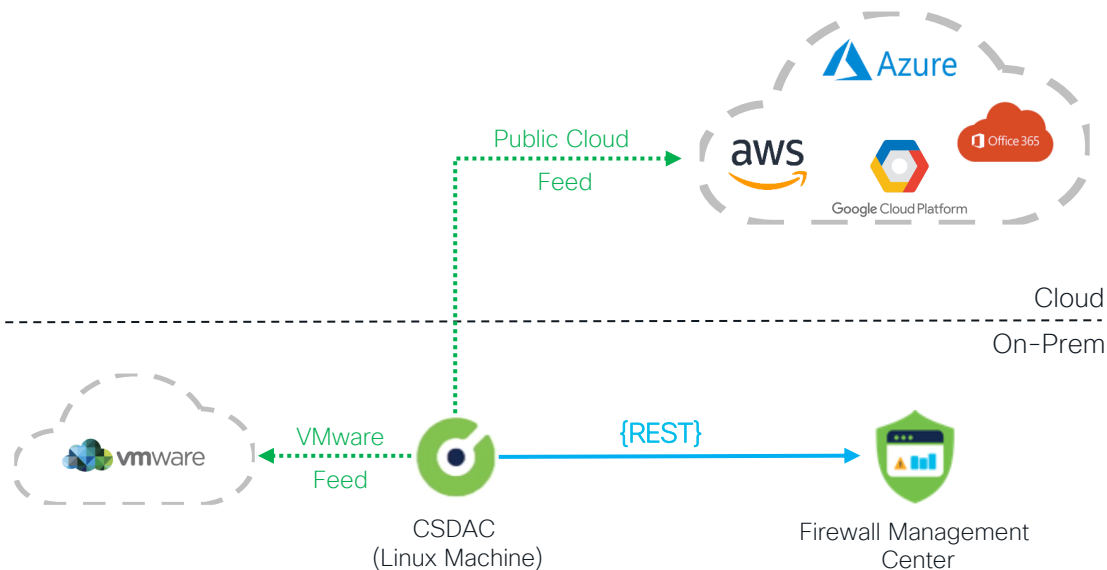
Public Cloud Tags



CSDAC Demo

Cisco Secure Dynamic Attributes Connector On-Prem Deployment

FREE OF CHARGE



CSDAC On-Prem:

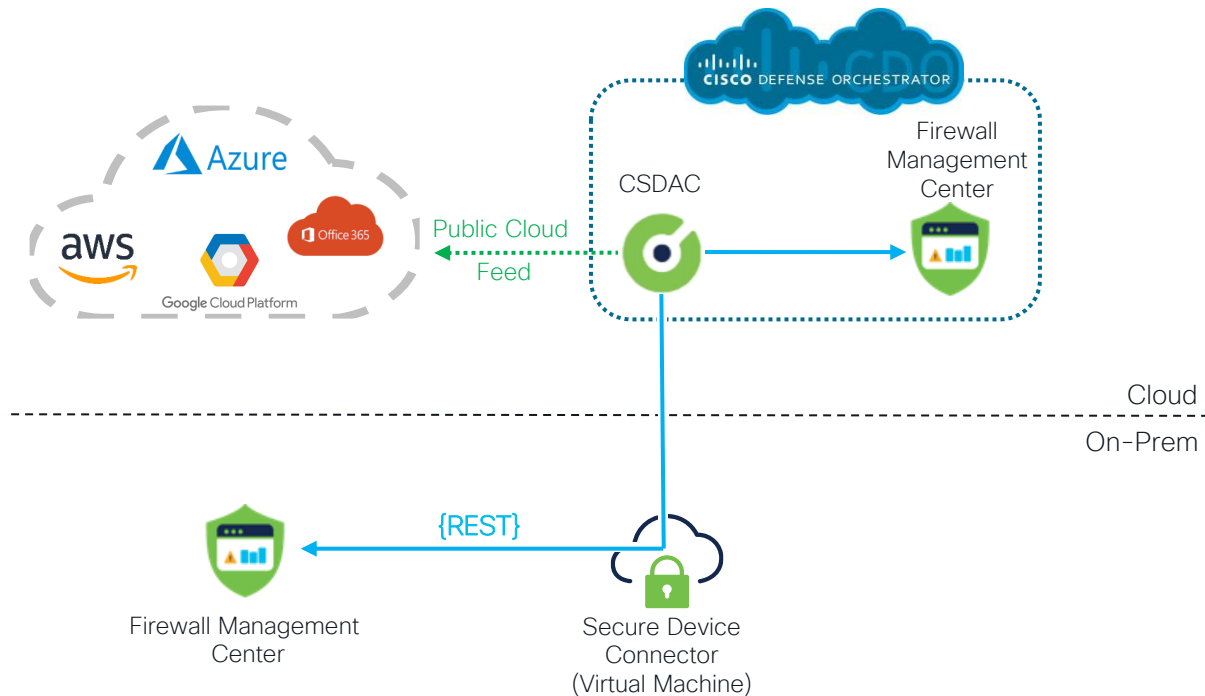
- Supports FMC/FTDs running **7.0 and above**
- **Fully supported** by Cisco TAC with your FMC's contract
- You can download and use it for **free!!!**
- Ansible Galaxy collection installed on Ubuntu/RHEL/CenOS



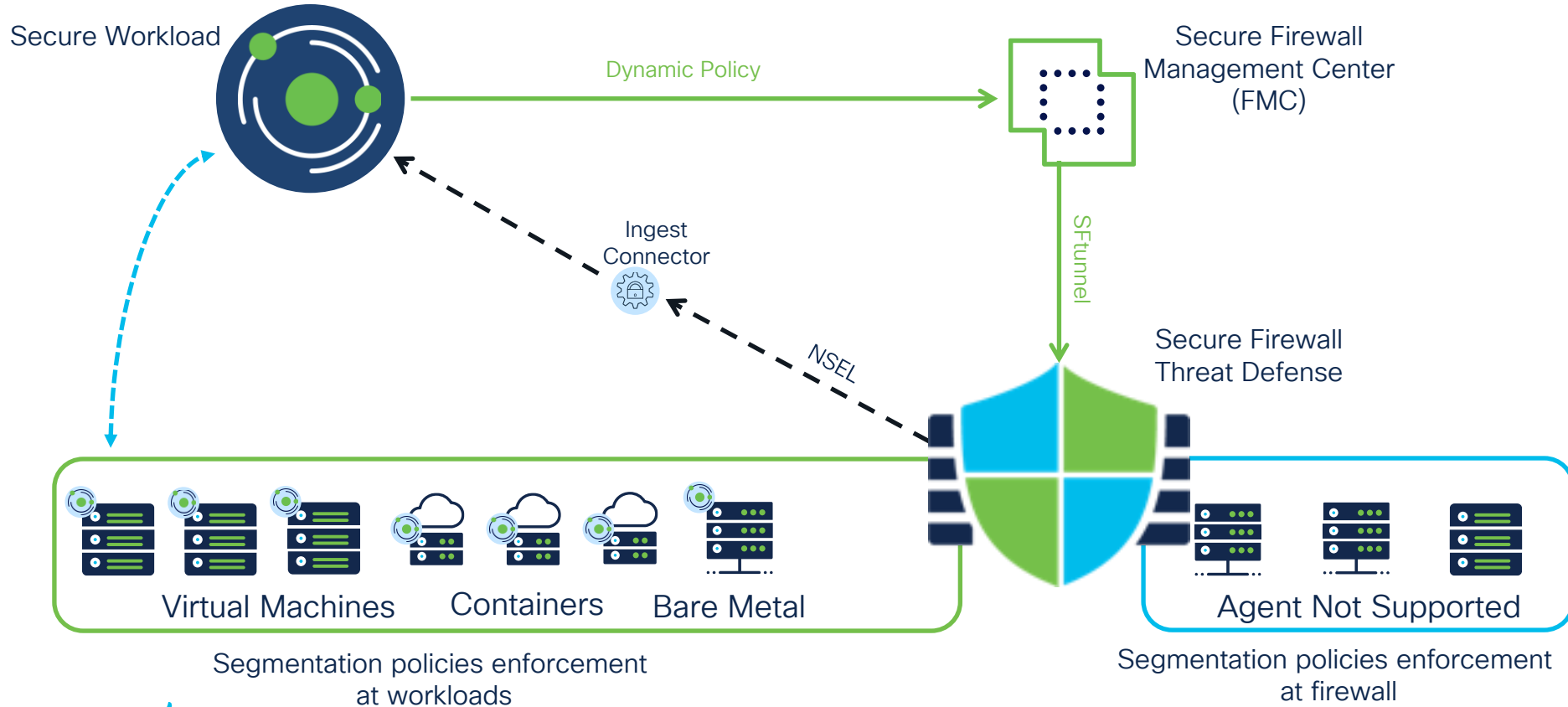
Cloud Delivered Cisco Secure Dynamic Attributes Connector Deployment

Cloud Delivered CSDAC:

- Launched with **Cloud Delivered FMC**
- Supports on-prem FMC running 7.1 and above
- Connects to on-prem FMC over CDO's **Secure Device Connector**
- Supports **Public Cloud Providers**



Cisco Secure Workload Dynamic Policy Push



Accurate and Validated Dynamic Policy

Invoice-App-Firewall PRIMARY

... : DC : DC-1 : Applications : Prod : Invoice-App Version: v1 Last Run: Apr 26, 9:59 PM

Activity Log Matching Inventories 8 Conversations 208 Filters 4 Policies 16 Provided Services Enforcement Status Policy Analysis Enforcement

Switch Application Start ADM Run

1. Generate an accurate micro-segmentation policy based on NSEL firewall flow events with **Application Dependency Mapping**.

2. ADM automatically discovers relationships between services and suggests **Zero Trust** policy.

3. Run **What-If** policy analysis using real-time or historical data for pre-enforcement validation.

16 / 16 policy changes selected for enforcement

Filter Policies ...

Absolute No matching changes

Default Added 15 Removed 0

Priority	Action	Consumer	Provider	Protocols and Ports
100	ALLOW	siwapp-front-end-haproxydb	siwapp-db-tier	TCP : 3306 (MySQL)
100	ALLOW	siwapp-front-end-haproxy	siwapp-app-tier	TCP : 8081
100	ALLOW	siwapp-db-tier	Default : EMEAR	UDP : 53 (DNS)
100	ALLOW	siwapp-db-tier	siwapp-db-tier	TCP : 4567
100	ALLOW	siwapp-db-tier	siwapp-front-end-haproxydb	TCP : 32768-60800

Enforced Policy Version: disabled ?

Enforcement is disabled for this application.
Traffic in, out and within this application's scope may still be enforced by policies from other enforced applications.

Select time range

Apr 27 3:34am - Apr 27 9:34am

18,098,412 total observations
Showing Flow Observations

Enforce Policies

4. Enforce the normalized micro-segmentation on the workloads and the **Cisco Secure Firewall** protected segments.

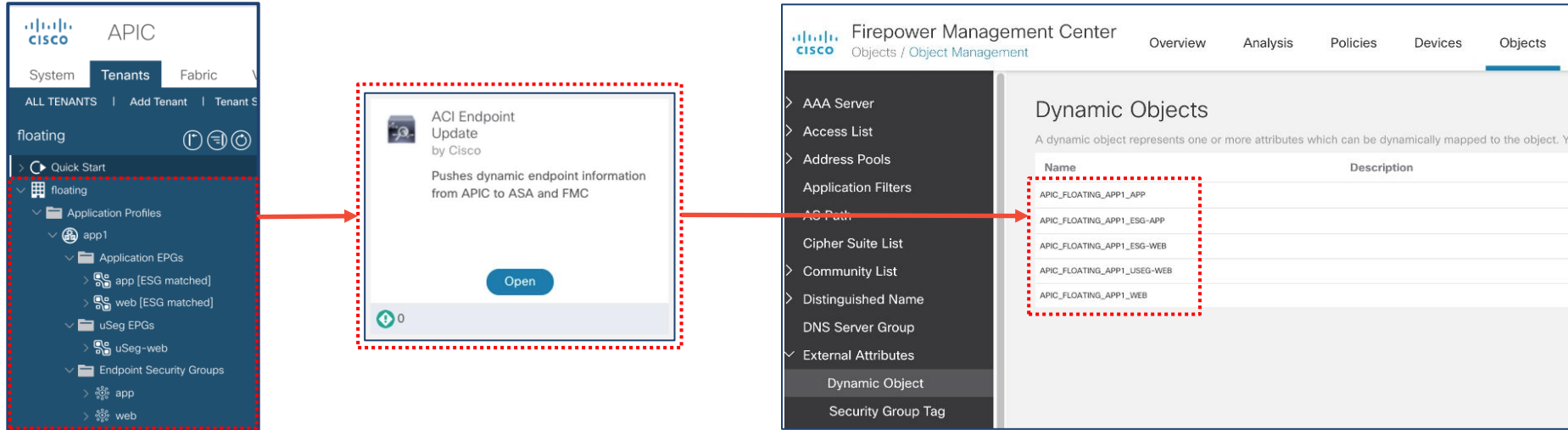
Attribute Based Policy – Cisco Secure Workload Rules and Dynamic Objects

#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic	Destination Dynamic	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	Any	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	Any	Any	Any	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

Cisco Secure Workload pushed
Dynamic Objects

Cisco Secure Workload deployed
Access Control Policy Rule

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	Guaranteed_Systems	Guaranteed_Systems	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Guaranteed_Systems	Guaranteed_Systems	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

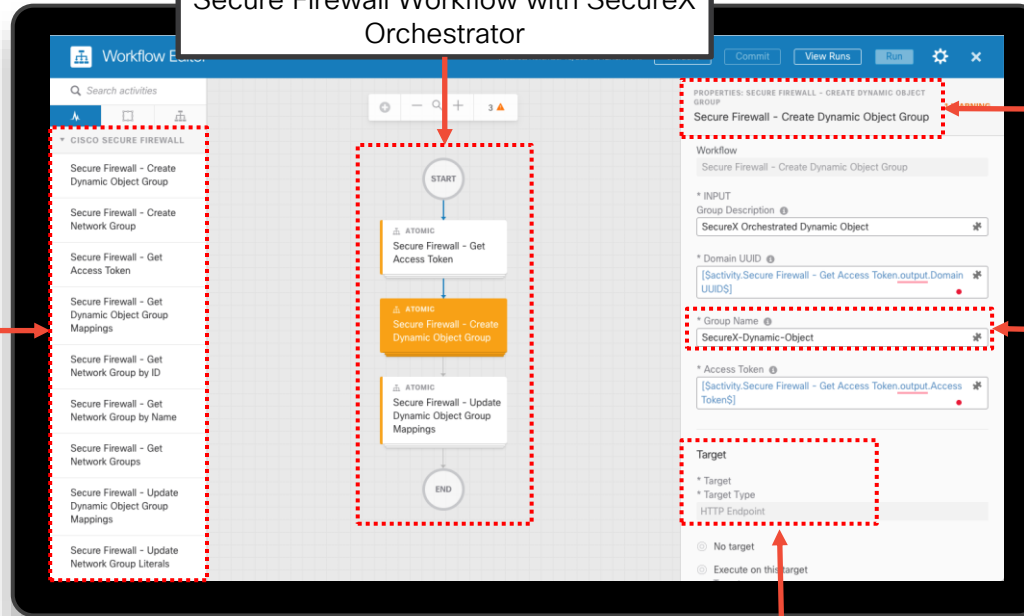
ACI Endpoint Groups (EPG) and
Endpoint Security Group (ESG)



SecureX Orchestration with Dynamic Objects

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

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



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

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.

Attribute Based Policy – SecureX

#	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			Directory	Allow
4	Printing Service	Corporate_VN	Data_Center_Edge	Any	Any	Any	Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	Any	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

SecureX Orchestration remediation workflow Dynamic Objects

SecureX_Quarantined_IPs
SecureX_Suspicious_IPs

Dynamic Objects REST API is Straight Forward

Connect to your FMC at "https://<FMC IP>/api/api-explorer" to browse the REST API documentations

GET /api/fmc_platform/v1/domain/{domainUUID}/object/dynamicobjects

POST /api/fmc_platform/v1/domain/{domainUUID}/object/dynamicobjects

Retrieves the list of all Dynamic Objects or creates a new Dynamic Object.

GET /api/fmc_platform/v1/domain/{domainUUID}/object/dynamicobjects/{objectIdOrName}

PUT /api/fmc_platform/v1/domain/{domainUUID}/object/dynamicobjects/{objectIdOrName}

DELETE /api/fmc_platform/v1/domain/{domainUUID}/object/dynamicobjects/{objectIdOrName}

Retrieves, deletes or modifies an existing Dynamic Object with the specified ID.

GET /api/fmc_platform/v1/domain/{domainUUID}/object/dynamicobjects/{objectIdOrName}/mappings

PUT /api/fmc_platform/v1/domain/{domainUUID}/object/dynamicobjects/{objectIdOrName}/mappings

Retrieves, adds or removes IP addresses mapped to an existing Dynamic Object with the specified ID.

POST /api/fmc_platform/v1/domain/{domainUUID}/object/dynamicobjectmappings

Adds or removes IP addresses mapped to existing Dynamic Objects in bulk.

Configure Dynamic Objects with the REST API



Environment Variables:

X-auth-access-token =
c830333c-614e-44a7-b6ca-dca7b8be605d

Domain UUID =
e276abec-e0f2-11e3-8169-6d9ed49b625f

Workload_A Object ID =
005056AF-6E04-0ed3-0000-021474843199

POST /api/fmc_platform/v1/auth/generatetoken

HEADER Authorization : Basic cnWzdFAcdDovcW86RFFtMU==

Status: 204

HEADER X-auth-access-token : c8303..605d
Domain_UUID : e276abec.b625f

POST /api/fmc_platform/v1/domain/e276abec.b625f/object/dynamicobjects

HEADER X-auth-access-token : c830333c-614e-44a7-b6ca-dca7b8be605d

BODY {
 "name": "Workload_A",
 "type": "DynamicObject",
 "objectType": "IP"
}

Status: 201

BODY
[...]
"id": "005056AF.199",
"name": "Workload_A",
"type": "DynamicObject",
[...]

POST /api/fmc_platform/v1/domain/e276abec.b625f/object/dynamicobjectmappings

HEADER X-auth-access-token : c830333c-614e-44a7-b6ca-dca7b8be605d

BODY {
 "add": [
 {
 "mappings": [
 "172.16.11.100"
],
 "dynamicObject": {
 "id": "005056AF-6E04-0ed3-0000-021474843199"
 }
 }
]
}

Status:
201

FMC



Dynamic Object	Content:
Workload_A	172.16.11.100

REST Allows You to Design your Own Use-Cases

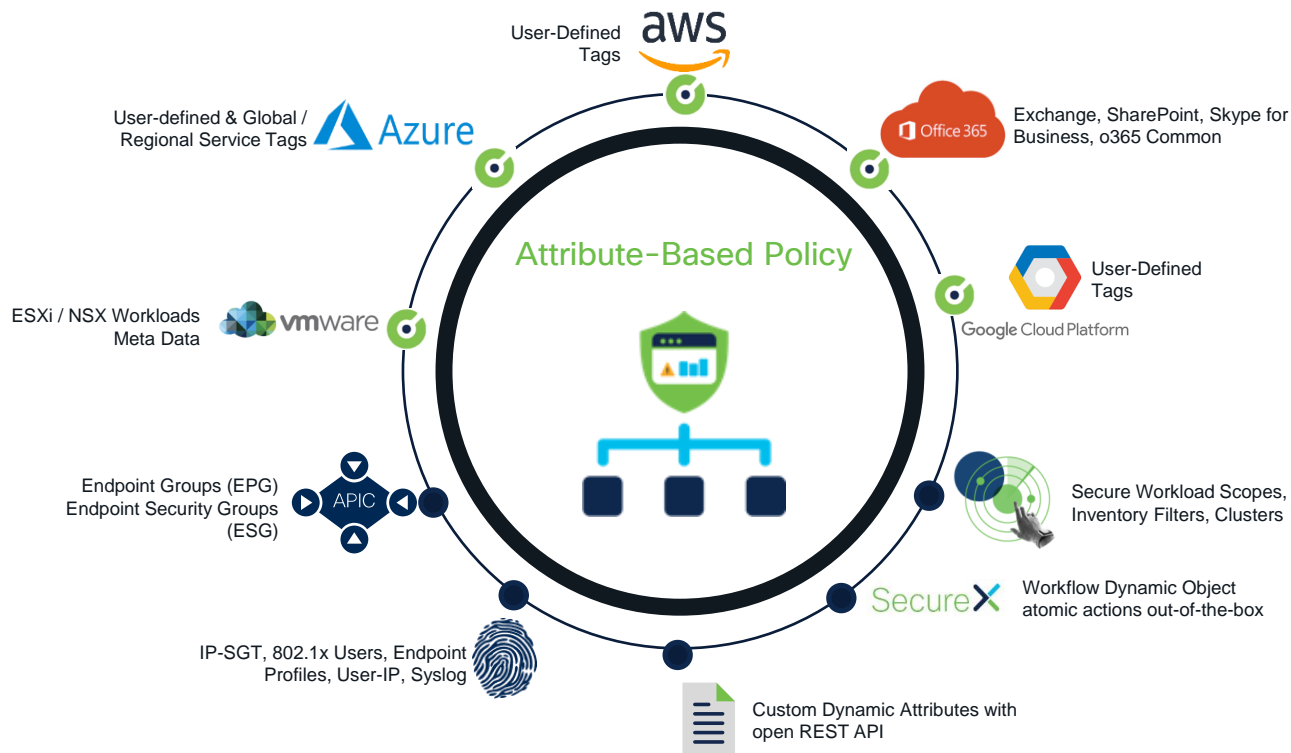
#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)									
√ Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	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	Contructors	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTP HTTPS	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

REST API pushed
Dynamic Object



Conclusions

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



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

- After this session have a look at your traditional firewall policy and try to find some candidates for dynamic attributes.
- Think how you could make your firewall policy dynamic, more secure and easier to manage with Attribute Based Policy and the integrations.
- Set up a CSDAC instance and see how easy it is to get Dynamic Objects into your FMC.

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.



Where to Go Next

- [BRKSEC-2123](#) - Solving the Segmentation Puzzle! Secure Workload and Secure Firewall Integration
- [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
- [BRKSEC-2845](#) - Cisco Secure Firewall and SDA Integration Deep Dive

Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Threat Visibility & Hunting

Security, Orchestration, Automation and Response

Device Insights

Kenna Vuln Mgmt

Incident Response and Remediation Services

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access | Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN
Posture
Telemetry
Threat
Query

ThousandEyes (Visibility)

Device Mgmt
Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

Umbrella/Duo

ZTNA | DNS-layer security | Secure web gateway | L7 firewall + IPS | Cloud access security broker/shadow IT | RAaaS | SSL decryption | Remote browser isolation | Data loss prevention | Cloud malware detection

SDWAN

Cisco Meraki SDWAN | SDWAN by Viptela | Secure Firewall | ThousandEyes | Cloud DDoS, WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge | Cisco Meraki SDWAN | SDWAN by Viptela | Secure Firewall | ThousandEyes

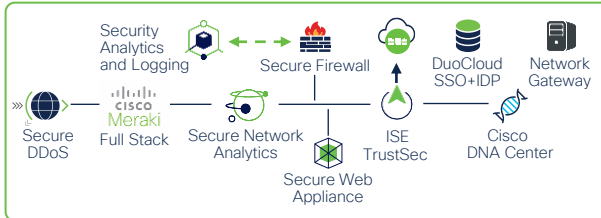
IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

Industrial Router | Industrial Firewall | Industrial Switch/AP | Cyber Vision | ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility



Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

Cloud Native Security | SCN | APIC | Secure Workload | Secure Application by AppDynamics

App Observability | Detection | Response

Hybrid Private | Public Cloud | Secure Cloud Analytics | Secure Firewall | ThousandEyes | Secure DDoS, WAF/Bot

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



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive