
cisco Live!
ALL IN

The bridge to possible

Solving the Segmentation Puzzle! Secure Workload and Secure Firewall Integration

Jorge Quintero, Technical Marketing Engineer

BRKSEC-2123

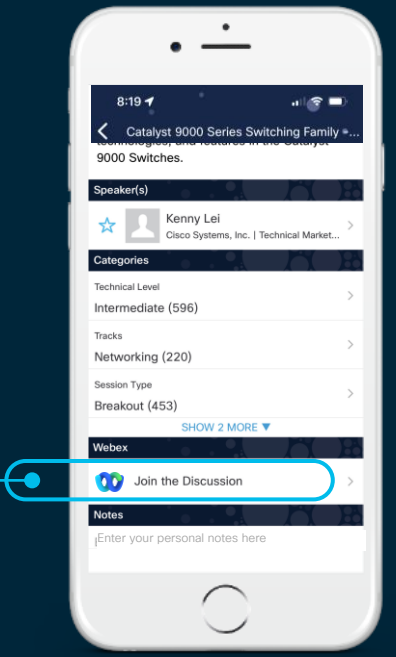
Cisco Webex App

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-2123

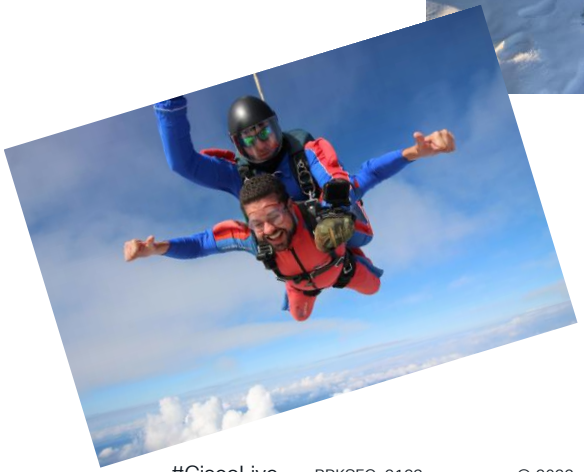
Webex spaces will be moderated by the speaker until June 17, 2022.

Session abstract

In a world of application workloads deployed anywhere, at any time, and with multi-cloud solutions, traditional security segmentation approaches have proven to be inefficient, not scalable, error-prone, and complex. With all of these constraints, there is no wonder why it often leads to security gaps, enough to say that segmentation is the cornerstone of every Zero-Trust architecture. Secure Workload has been solving this problem—however, installing software agents in every workload is not always feasible. This session will show participants the Secure Workload and Secure Firewall integration for unified segmentation and use-cases. The session also covers a walk-through of the integration and demos.

About your speaker

- Name
  - Jorge Quintero
  - Technical Marketing Engineer
  - Cisco employee since 2016
  - 10+ years in IT industry
- Free Time
  - Traveling
  - Anything outdoors



Learning Map

Building Zero Trust Security with Secure Workload

You are here!

TECSEC-2007
Find Your Zen with
Zero Trust Microsegmentation

BRKSEC-2250
Decoding Kubernetes Networking and Policy as Code Using Cisco Secure Workload

BRKSEC-2123
Solving the Segmentation Puzzle!
Secure Workload and Secure Firewall Integration

DEVWKS-2160
Exploring Cisco Secure Workload Programmability with Real-world Use Cases

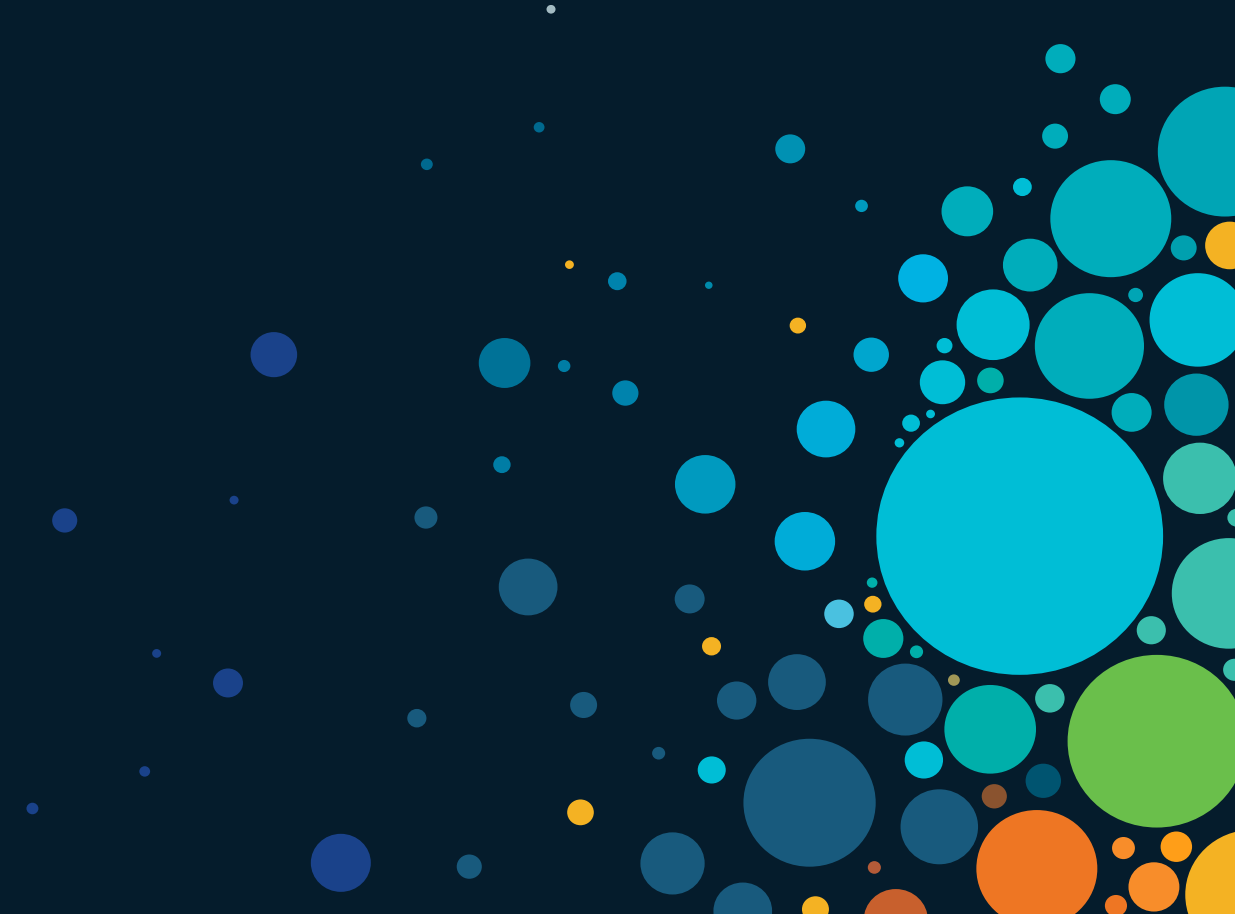
BRKSEC-2126
Brace Yourself! Take a Proactive Approach to Defend Your Application Workloads

BRKSEC-1773
How to Build a Secure Multi-Cloud Environment with Cisco Secure Workload

Agenda

- Introduction
- Integration Overview
- Configuration Overview
- Demo
- Summary

Introduction



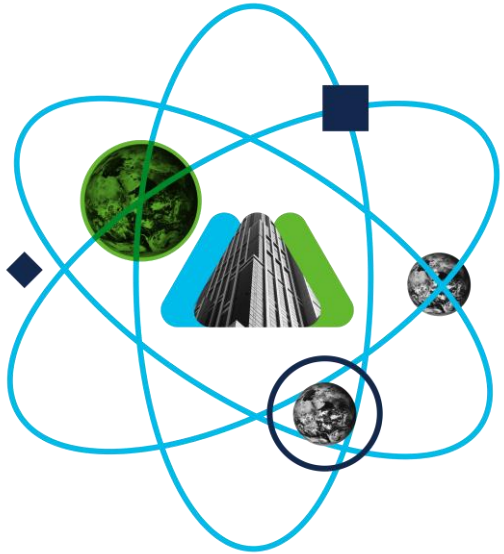
"Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised."

CISA Zero Trust Maturity Model

CISA

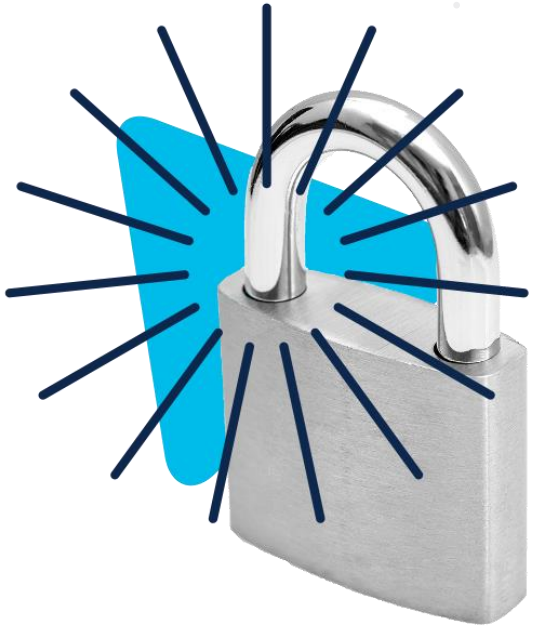
A common theme - Zero Trust..

- Zero Trust Frameworks, Models, Guidance and Architectures
  - NIST 800-207
  - Forrester Zero Trust eXtended
  - Gartner CARTA
  - CISA Zero Trust Maturity
  - ACSC Essential Eight
  - NCSC Zero Trust Design Principles
  - Vendor Specific Architectures

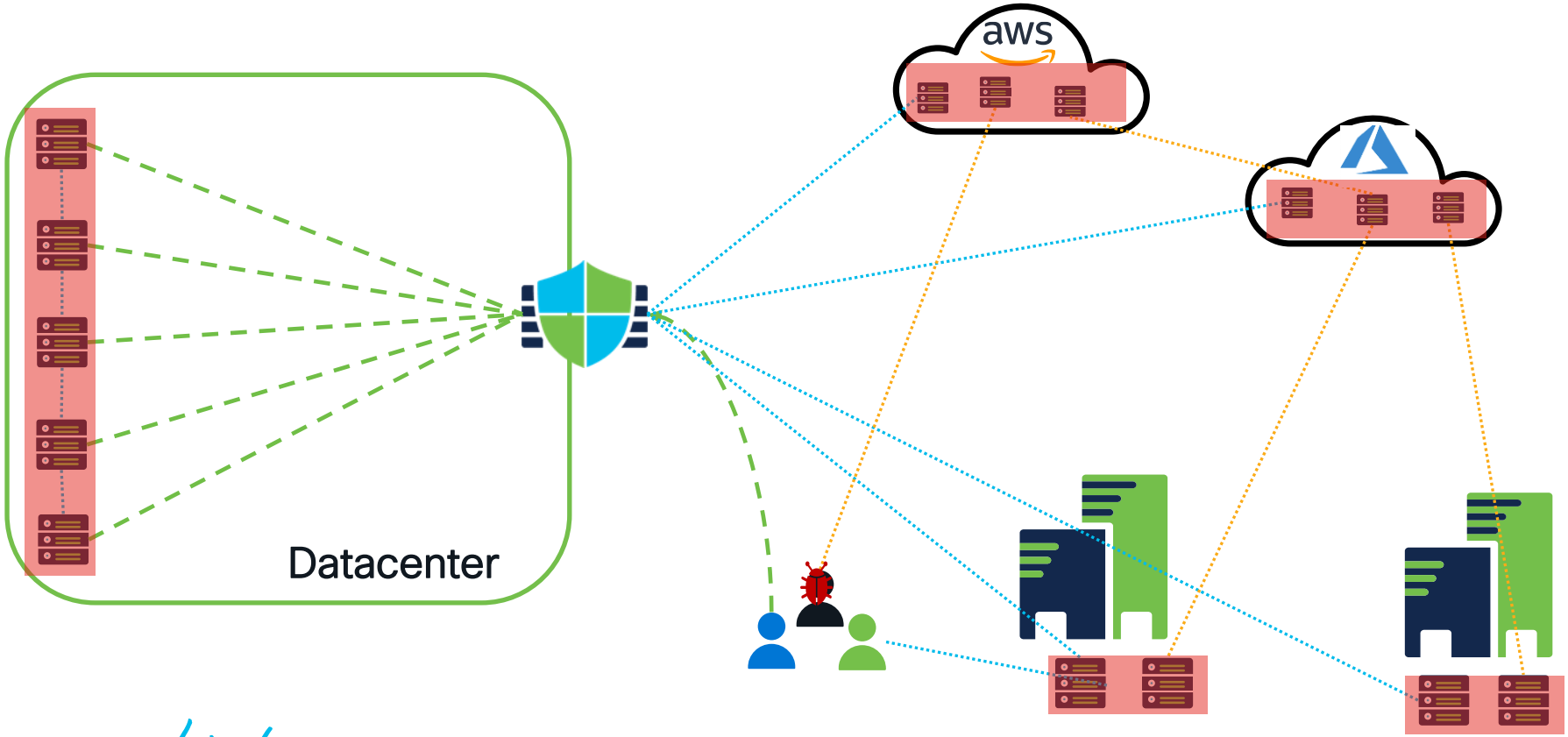


..But all agree segmentation is a critical control

- Zero trust segmentation
- Access control enforcement
- Restrict access to commonly exploited protocols



Where is the perimeter?



Where can we enforce policy?

Host-Based

K8s Nodes

Cloud Security Groups

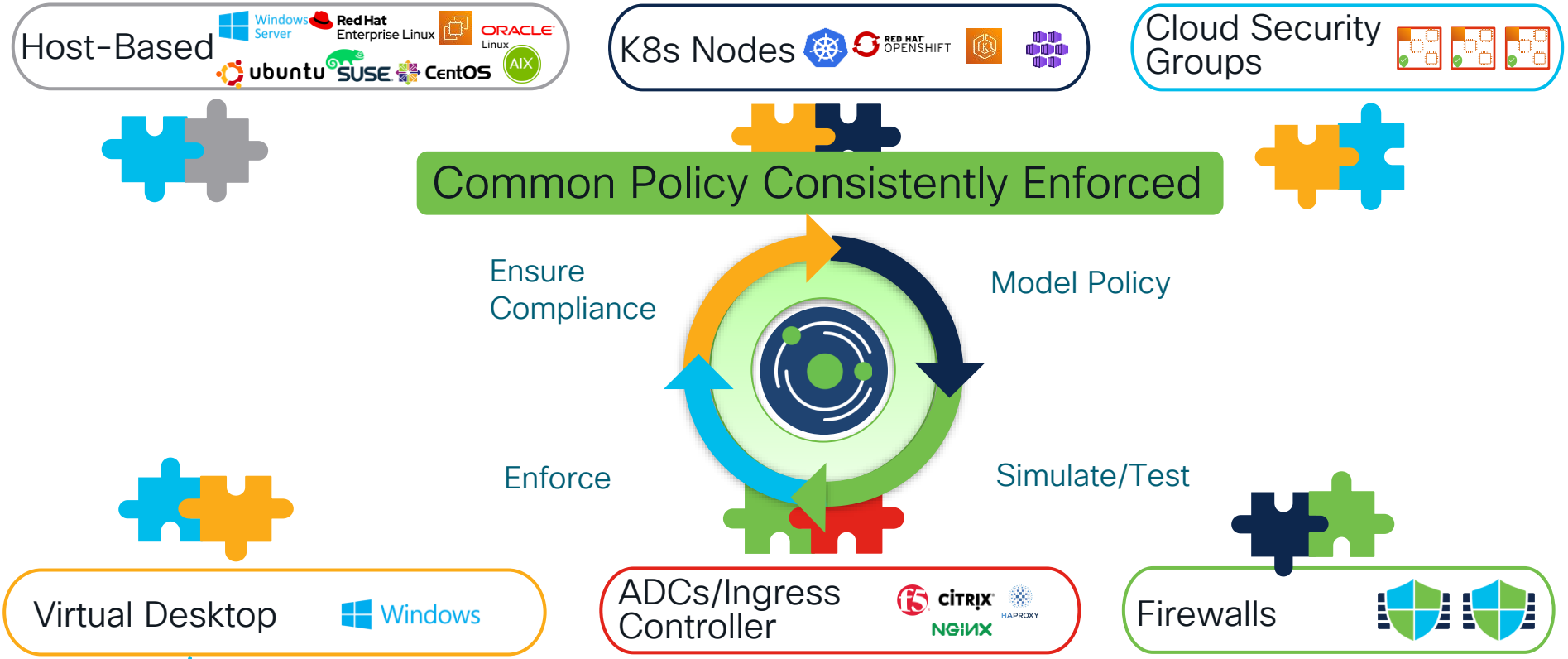
"The Policy Puzzle"

Virtual Desktop

ADCs/Ingress Controller

Firewalls

Solving the puzzle with Secure Workload!



Solving the puzzle with Secure Workload!

Host-Based

K8s Nodes

Cloud Security Groups

Fitting the pieces together

SecOps

NetOps

AppSec DevOps

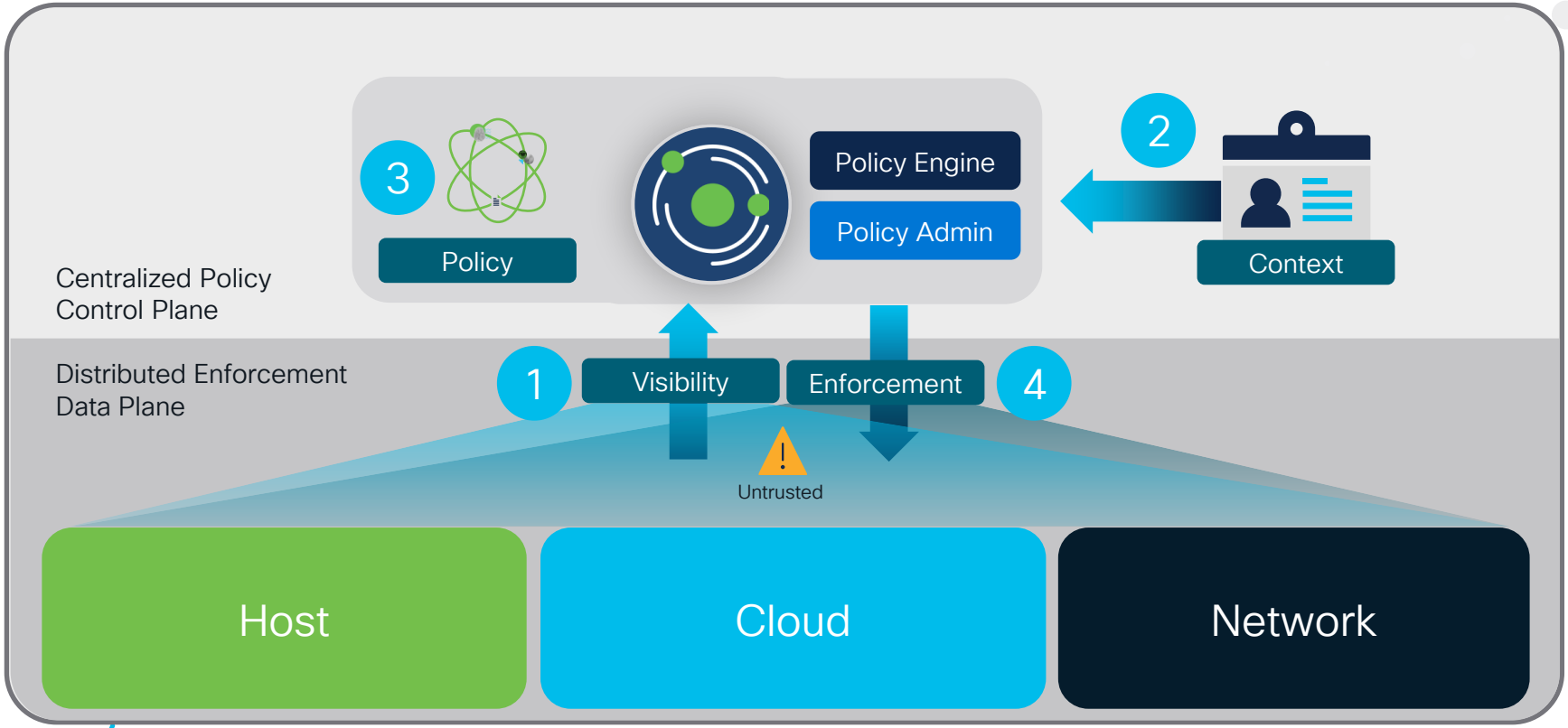
Auditors

Virtual Desktop

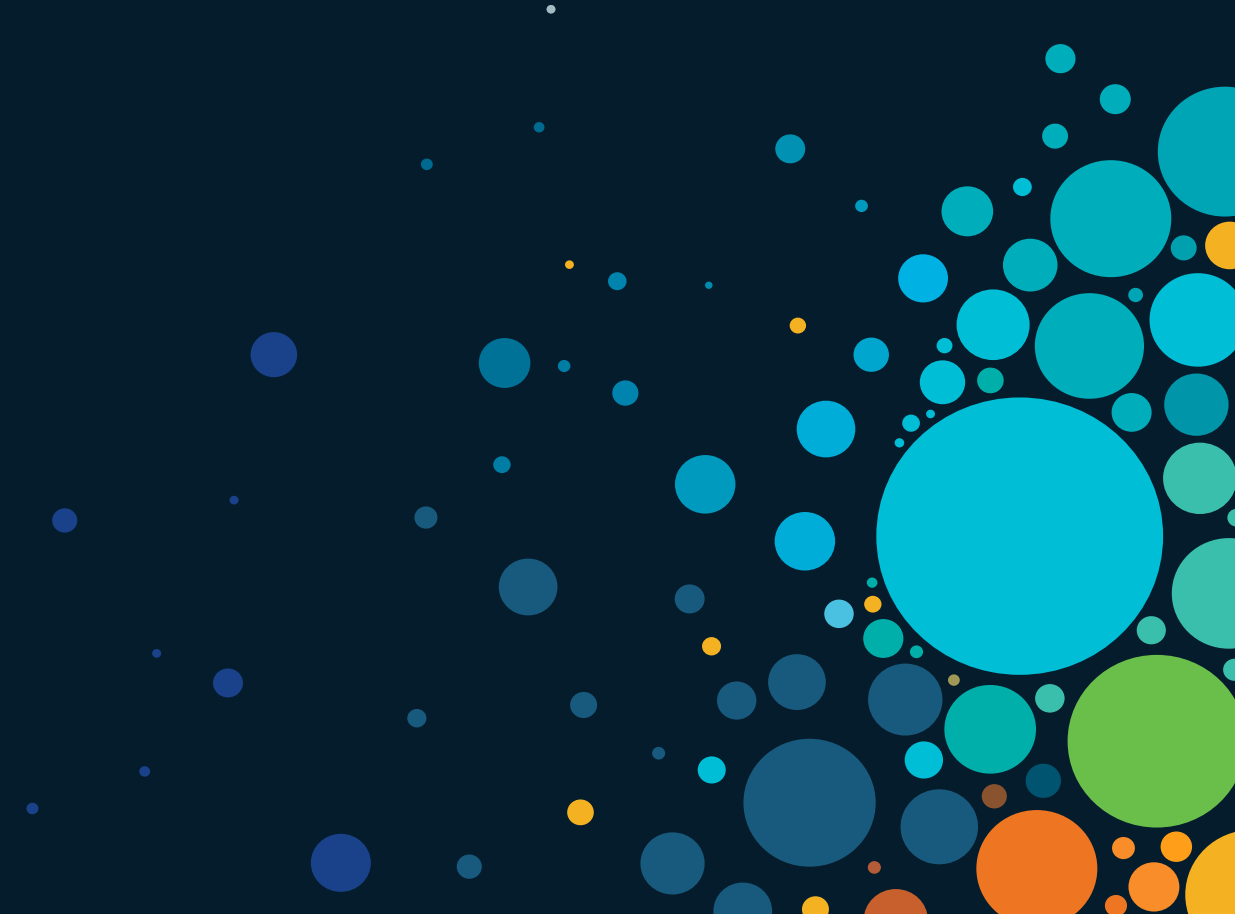
ADCs/Ingress Controller

Firewalls

Cisco Secure Workload



Integration Overview

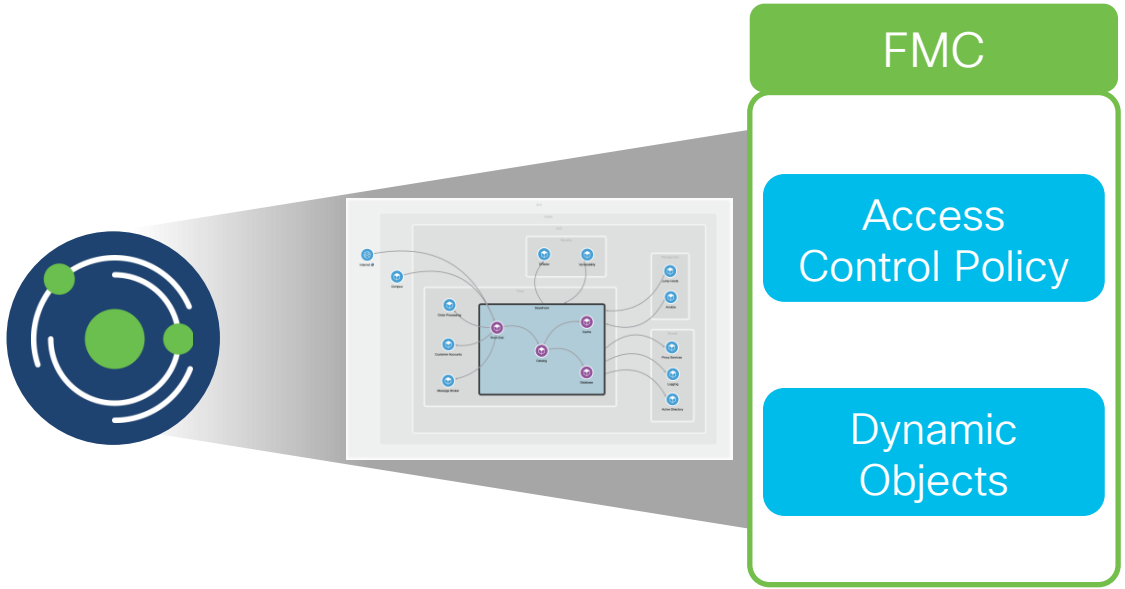


Feature evolution

Integration capabilities

Release 3.6

- Native Integration
- Dynamic Objects
- Access Control Policy
- NSEL Records for ADM policy
- Domain Awareness (patch 3)



Use-cases

Visibility

- Generate policies for agent and agentless workloads across multi-cloud environment
- Workload attribute import with integrations such as IPAM, CMDB, AWS, and more
- User and endpoint context with ISE and AnyConnect integration
- Verify and analyze flows for policy compliance

Enforcement

- Defense In-Depth
  - Attribute-Based enforcement using hierarchical policies for agent and agentless workloads
  - Rapid Threat Containment for agent and agentless workloads with FMC Remediation Module
- Policy Lifecycle automation
- Enforce segmentation policies to applications where agent installation is not feasible

End-to-End protection

North-South Security with Secure Firewall

East-West Security with Secure Firewall and Secure Workload

Workload Security with Secure Workload

Broad Visibility

Coarse Control

Fine-Grained Control

Closer to application

Configuration Overview

Supported platforms

Secure Workload

SaaS - Version 3.6

Requires Secure Connector

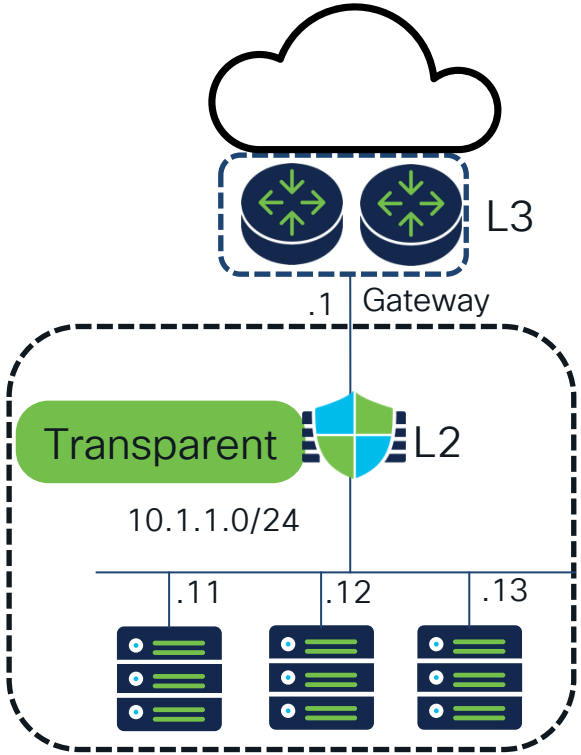
On-Prem - Version 3.6

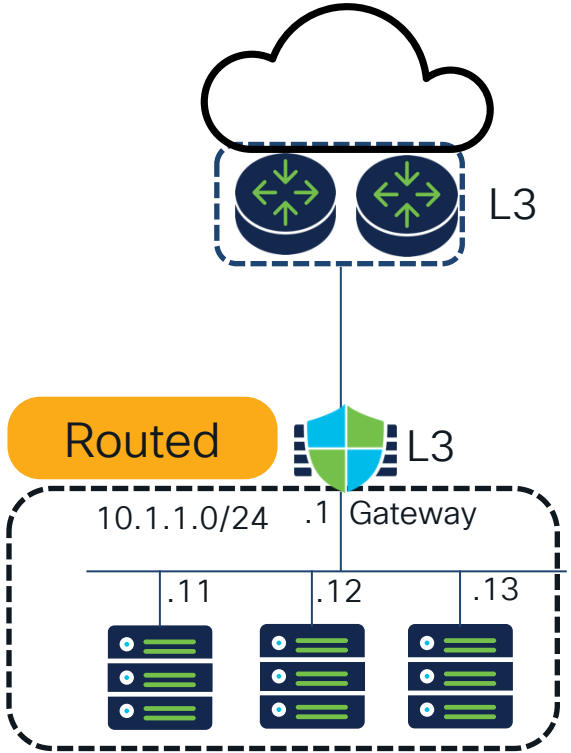
Secure Firewall Management Center (FMC)

Virtual - Version 7.0.1+

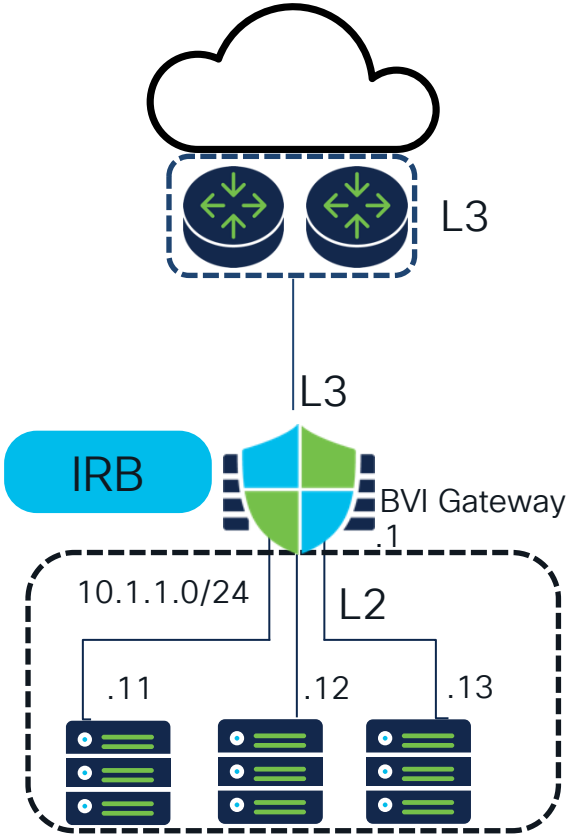
Physical - Version 7.0.1+

Supported Secure Firewall modes

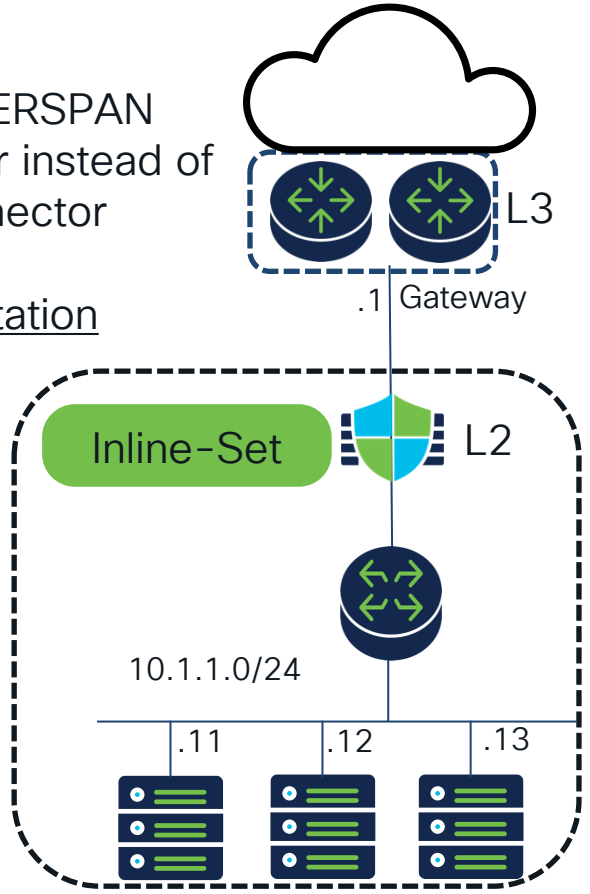




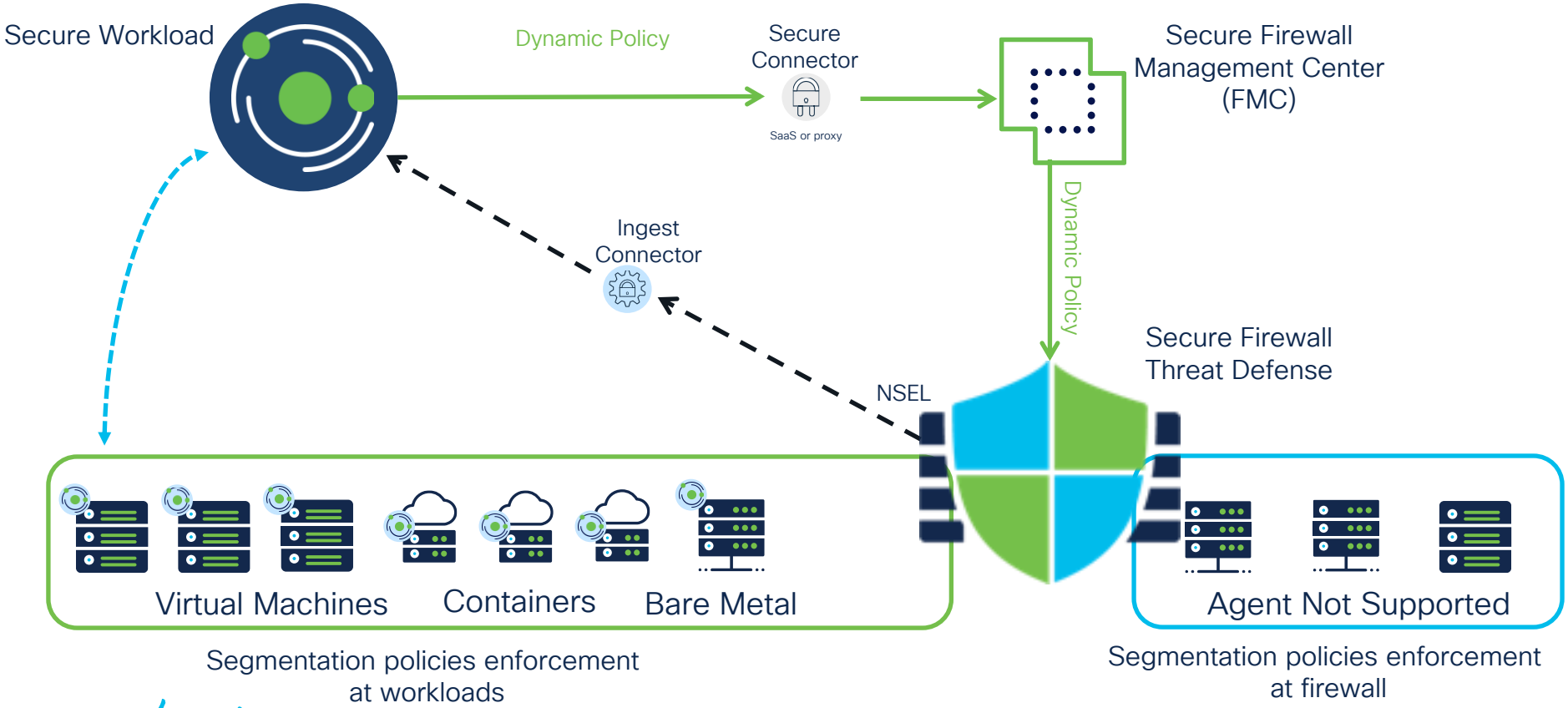
Additional Secure Firewall interface modes



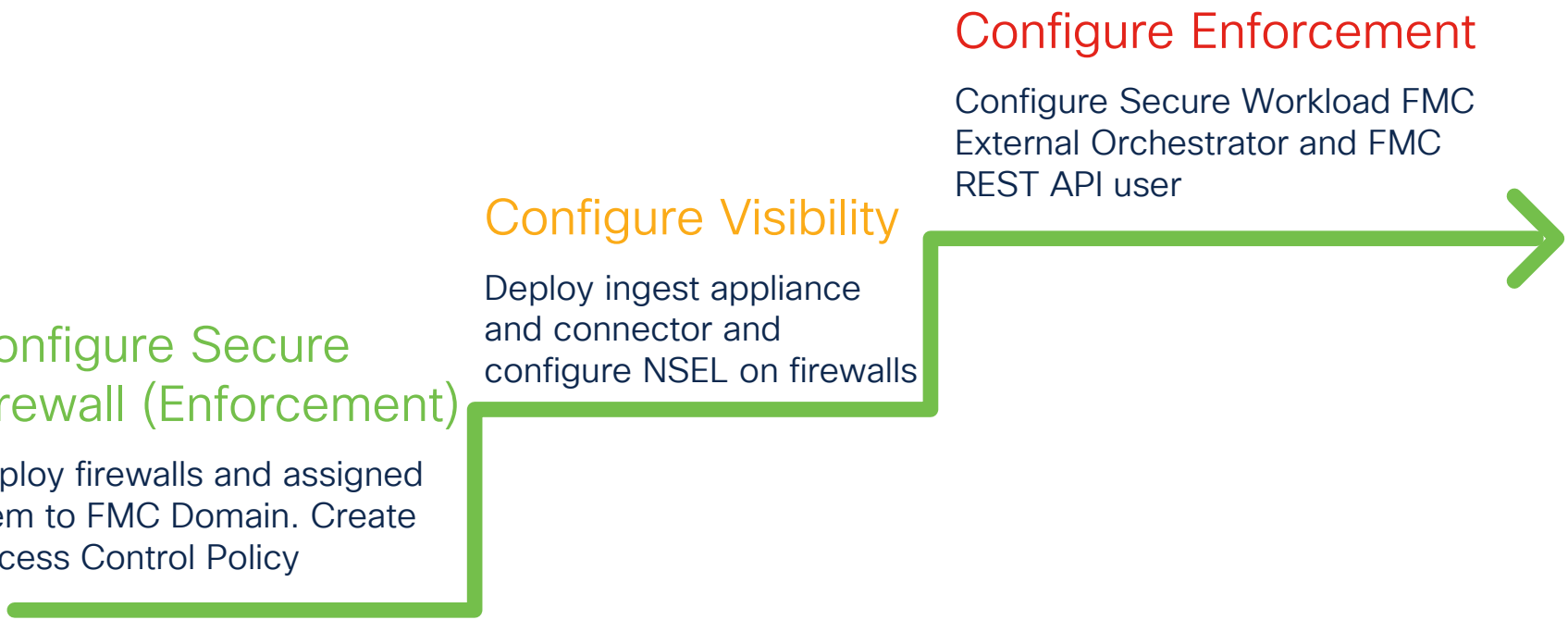
Requires ERSPAN Connector instead of ASA Connector Check Documentation



Architecture overview



Configuration overview – steps



Secure Firewall (Enforcement)

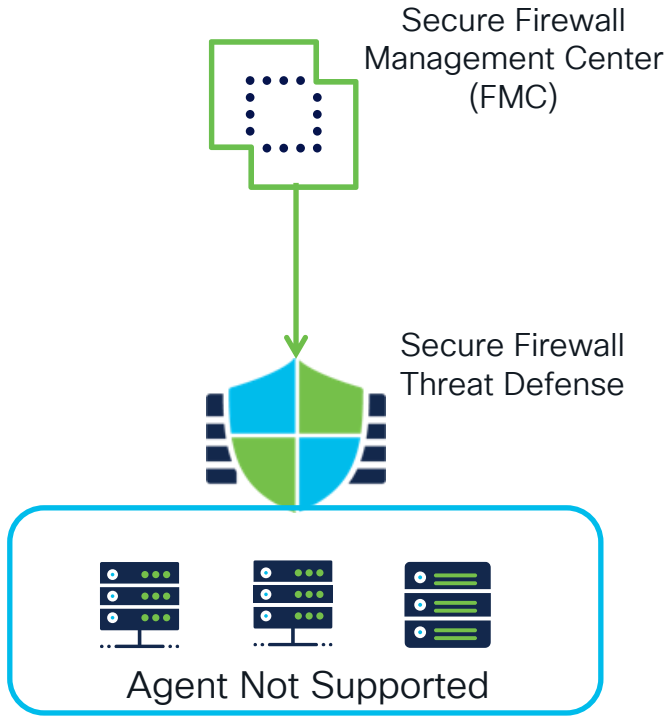
Data Ingest Appliance (Visibility)

Secure Firewall NSEL (Visibility)

Secure Workload Orchestrator (Enforcement)

Configuration overview – Secure Firewall

- Deploy Secure Firewalls
  - Transparent or Routed
  - IRB supported
  - ERSPAN for inline-sets
- Create FMC Domain
  - Create Access Control Policy

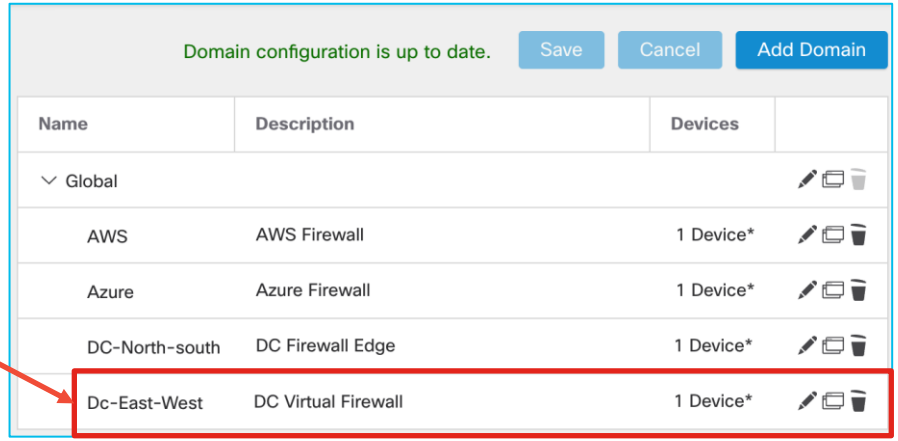


FMC domains

Mapping locations and firewalls for unified segmentation!

1. Create domains and assign firewalls to each domain depending on their location. The objective is to separate “Administrator Managed” firewalls from “Secure Workload Managed Firewalls”.

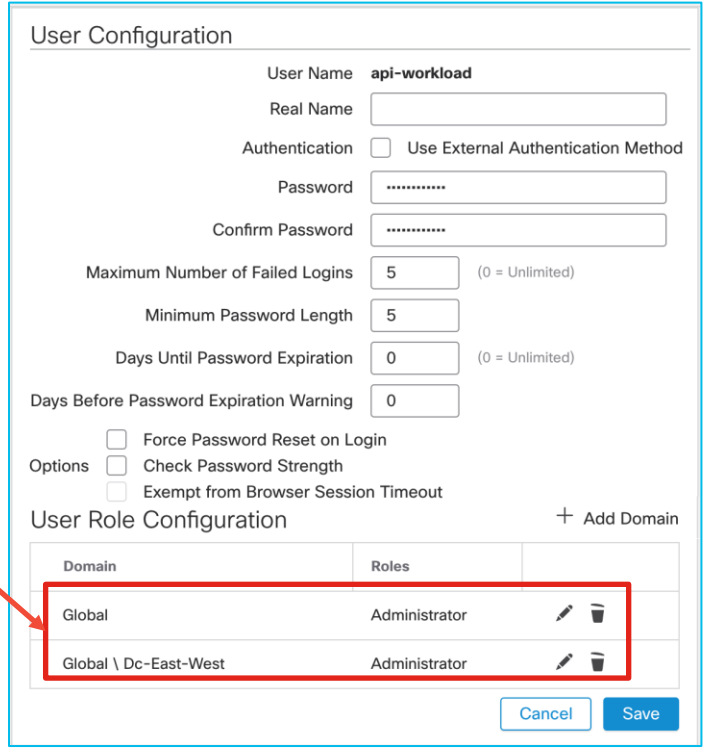
Note: Our current recommendations and guidance is to deploy the integration in **new** Secure Firewall and Firewall Management Center **deployments**.



FMC REST API user

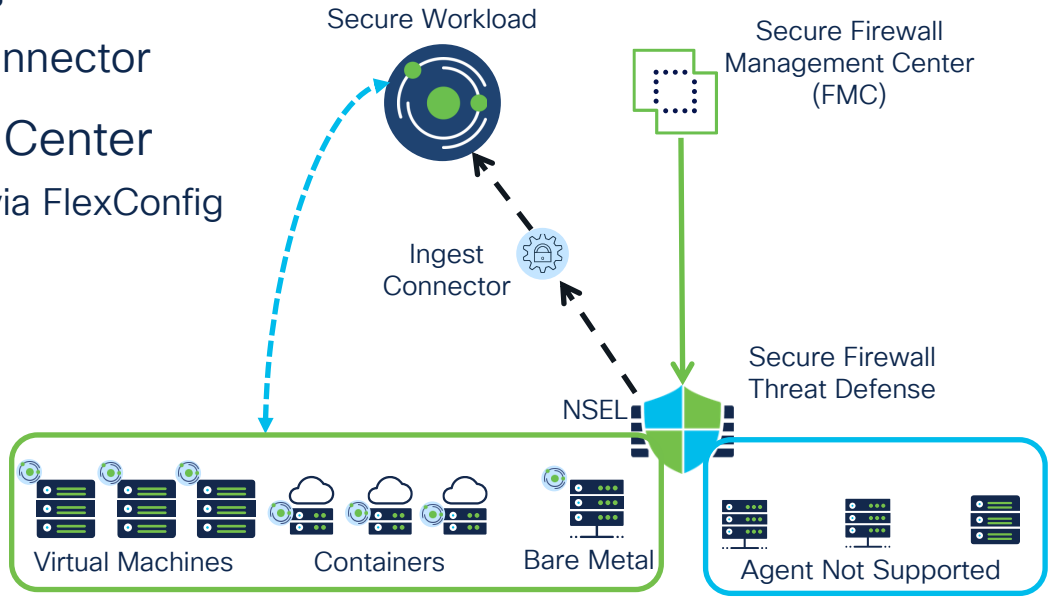
Automating policy deployment to Secure Firewalls

1. Configure REST API user. User must have access to the **global domain** and the **domain** where the **controlled firewall** is located and must have administrator rights.



Configuration overview – visibility

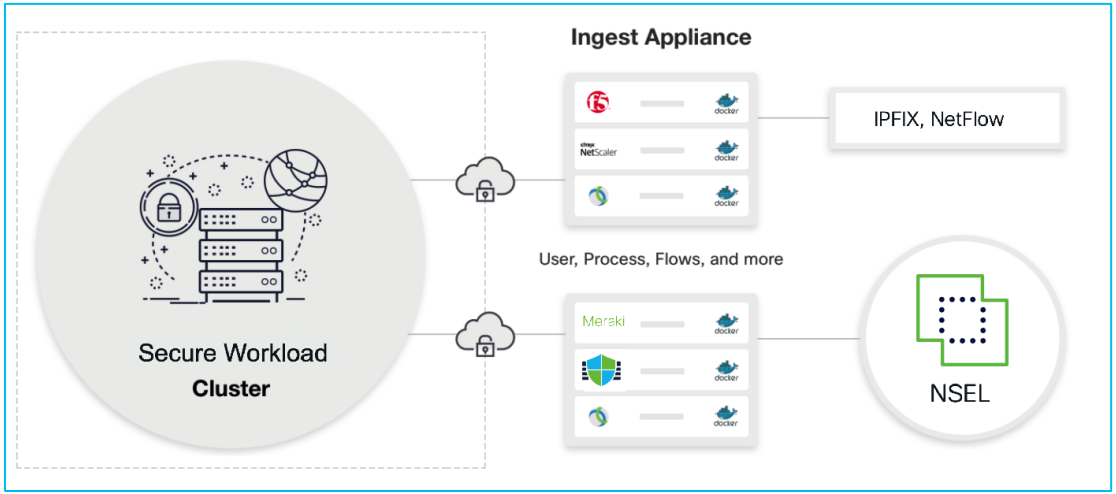
- Secure Workload
  - Deploy Secure Workload agents
  - Deploy Ingest Appliance and Connector
- Secure Firewall Management Center
  - Configure NSEL on Secure Firewall via FlexConfig



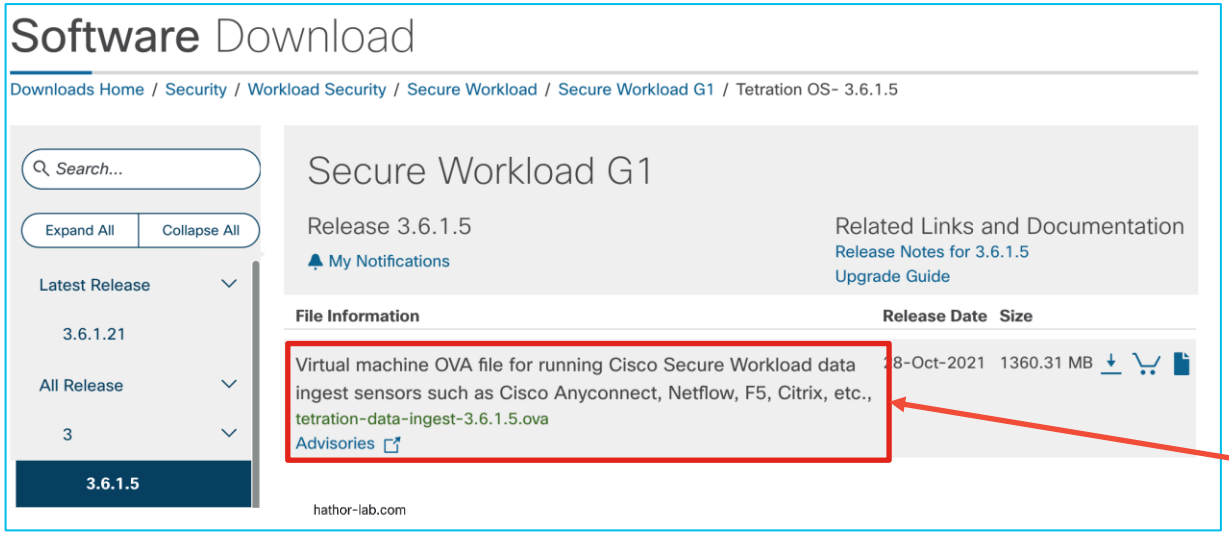
Data Ingest Appliance and connector

Dedicated lightweight virtual appliance for telemetry ingestion

- OVA available in cisco.com
- VMware support (KVM coming soon!)
- Supports IPFIX, NetFlow and NSEL
- Up to 3 connectors per appliance
  - Secure Firewall (ASA) Connector
  - F5
  - NetScaler
  - AnyConnect
  - Meraki



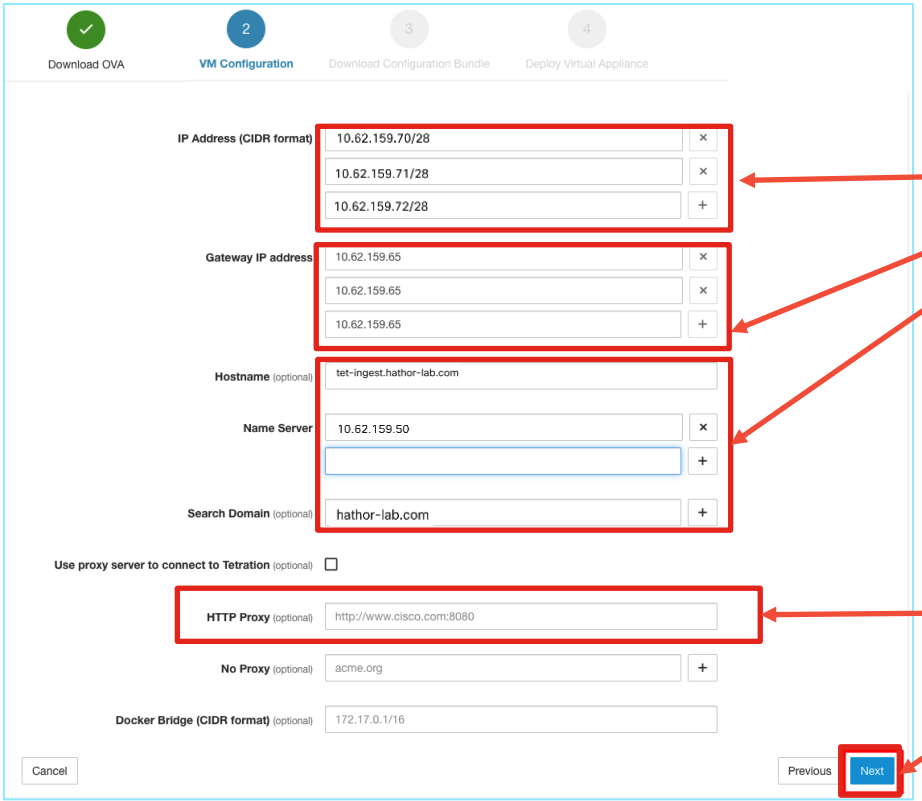
Data Ingest Appliance – download OVA



1. Download the Virtual Machine OVA. It is in the first release of each new version.

NOTE: Deploy the OVA in ESXi but do not turn it on.

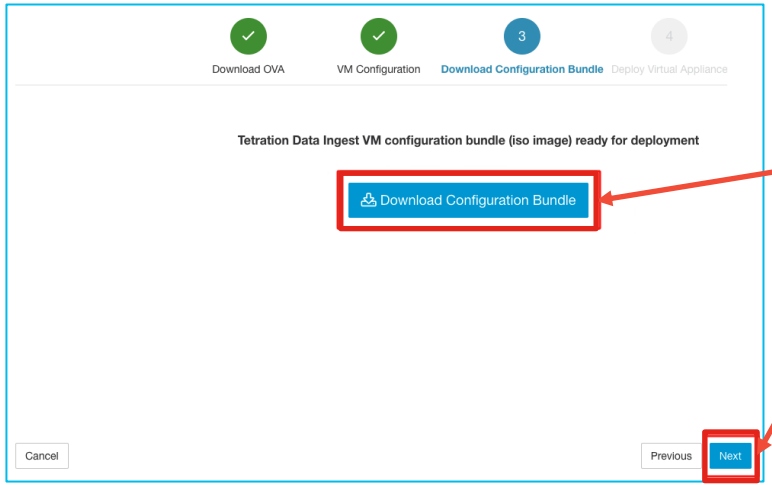
Data Ingest Appliance – OVA configuration



1. Configure the VM appliance IP Address settings. Each VM appliance supports up to 3 connectors.

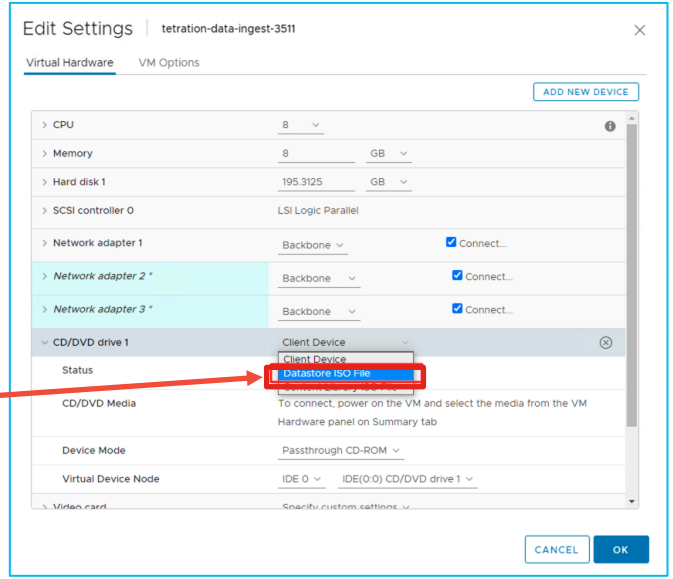
2. Optional: Configure proxy settings if a proxy device is in the environment. Select next

Data Ingest Appliance – config bundle



1. Download the configuration bundle and select next.

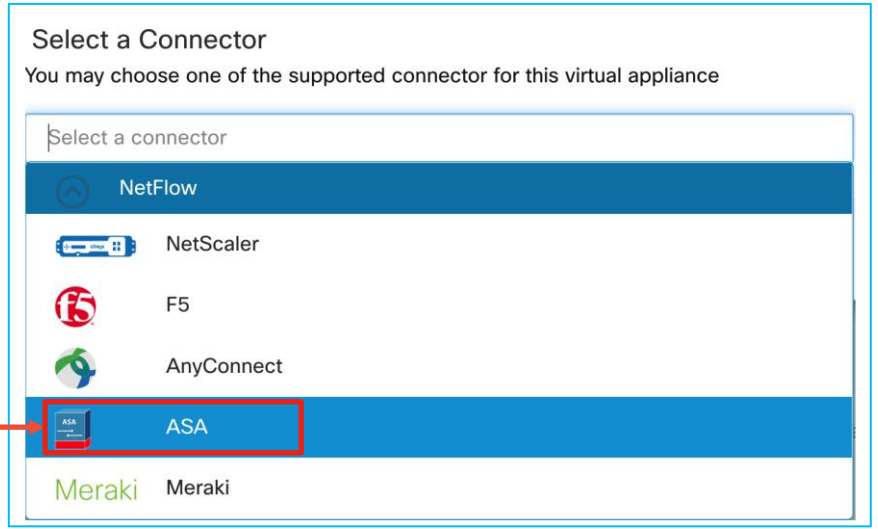
NOTE: Do not turn the VM appliance yet



2. Upload the configuration bundle iso to ESXi datastore and select the VM appliance CD/DVD drive to load it from datastore and **Turn on VM Appliance**

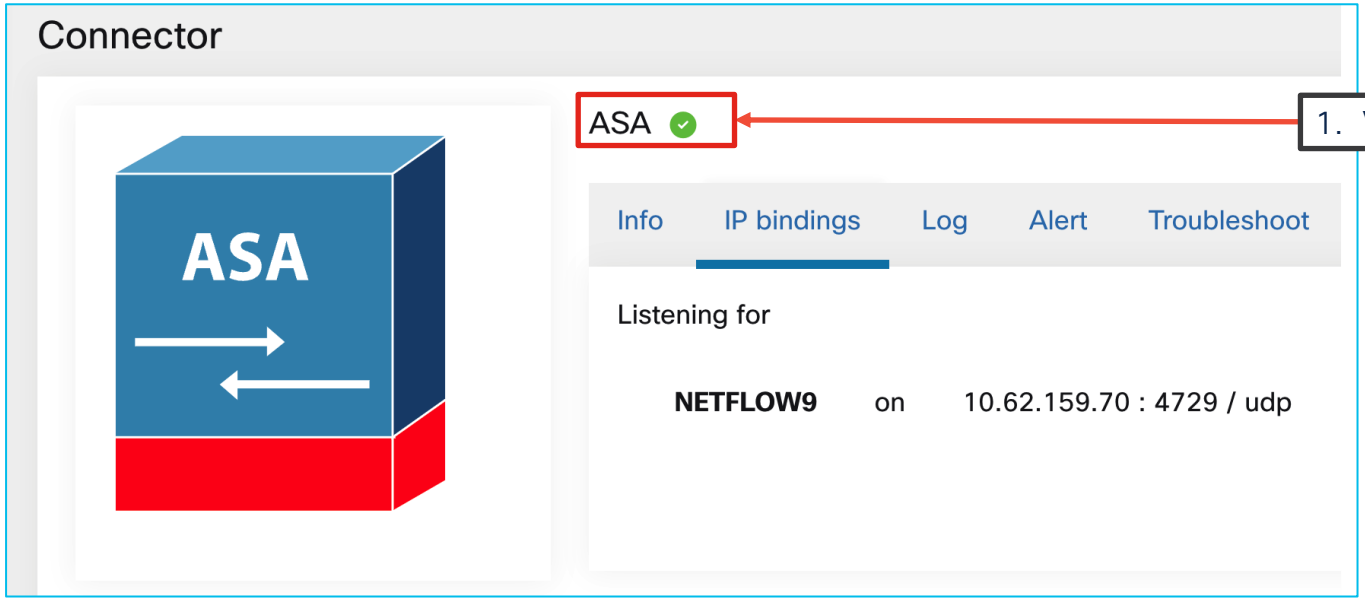
Data Ingest Appliance – enable connector

1. Verify that state is active after deploy and click ”Enable Another Connector”



2. Select ASA Connector

Data Ingest Appliance – verify connector



ASA connector NSEL events handling

Flow Event **Element ID: 233** **Element Name:** ***NF_F_FW_EVENT***	**Extended Flow Event** **Element ID: 33002** **Element Name:** ***NF_F_FW_EXT_EVENT***	**Action on ASA connector**
0 (default, ignore this value)	Don't care	No op
1 (Flow created)	Don't care	Send flow to Secure Workload
2 (Flow deleted)	> 2000 (indicates the termination reason)	Send flow to Secure Workload
3 (Flow denied)	1001 (denied by ingress ACL)	Send flow with disposition marked as rejected to Secure Workload
	1002 (denied by egress ACL)	
	1003 (denied connection by ASA interface or denied ICMP(v6) to device)	
	1004 (first packet on TCP is not SYN)	
4 (Flow alert)	Don't care	No op
5 (Flow updated)	Don't care	Send flow to Secure Workload

ASA connector NSEL flow observations

Forward Flow observation

Field	NSEL Element ID	NSEL Element Name
Protocol	4	*NF_F_PROTOCOL*
Source Address	8	*NF_F_SRC_ADDR_IPV4*
	27	*NF_F_SRC_ADDR_IPV6*
Source Port	7	*NF_F_SRC_PORT*
Destination Address	12	*NF_F_DST_ADDR_IPV4*
	28	*NF_F_DST_ADDR_IPV6*
Destination Port	11	*NF_F_DST_PORT*
Flow Start Time	152	*NF_F_FLOW_CREATE_TIME_MSEC*
Byte Count	231	*NF_F_FWD_FLOW_DELTA_BYTES*
Packet Count	298	*NF_F_FWD_FLOW_DELTA_PACKETS*

Reverse Flow Information

Field	NSEL Element ID	NSEL Element Name
Protocol	4	*NF_F_PROTOCOL*
Source Address	12	*NF_F_DST_ADDR_IPV4*
	28	*NF_F_DST_ADDR_IPV6*
Source Port	11	*NF_F_DST_PORT*
Destination Address	8	*NF_F_SRC_ADDR_IPV4*
	27	*NF_F_SRC_ADDR_IPV6*
Destination Port	7	*NF_F_SRC_PORT*
Flow Start Time	152	*NF_F_FLOW_CREATE_TIME_MSEC*
Byte Count	232	*NF_F_REV_FLOW_DELTA_BYTES*
Packet Count	299	*NF_F_REV_FLOW_DELTA_PACKETS*

ASA connector NSEL NAT-flows

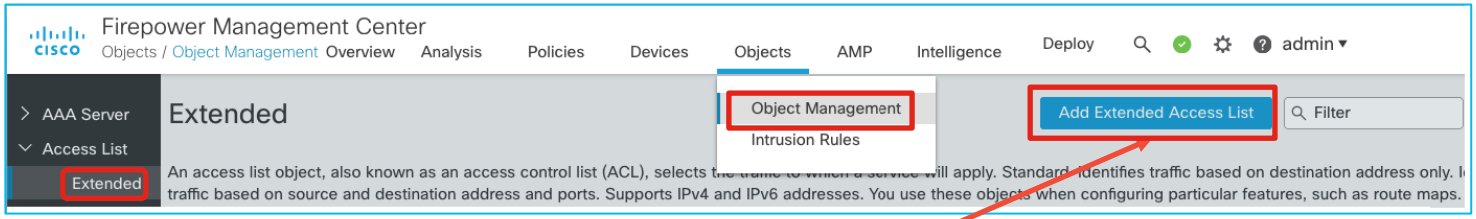
Forward Direction

Field	NSEL Element ID	NSEL Element Name
Protocol	4	*NF_F_PROTOCOL*
Source Address	225	*NF_F_XLATE_SRC_ADDR_IPV4*
	281	*NF_F_XLATE_SRC_ADDR_IPV6*
Source Port	227	*NF_F_XLATE_SRC_PORT*
Destination Address	226	*NF_F_XLATE_DST_ADDR_IPV4*
	282	*NF_F_XLATE_DST_ADDR_IPV6*
Destination Port	228	*NF_F_XLATE_DST_PORT*
Flow Start Time	152	*NF_F_FLOW_CREATE_TIME_MSEC*
Byte Count	231	*NF_F_FWD_FLOW_DELTA_BYTES*
Packet Count	298	*NF_F_FWD_FLOW_DELTA_PACKETS*

Reverse Direction

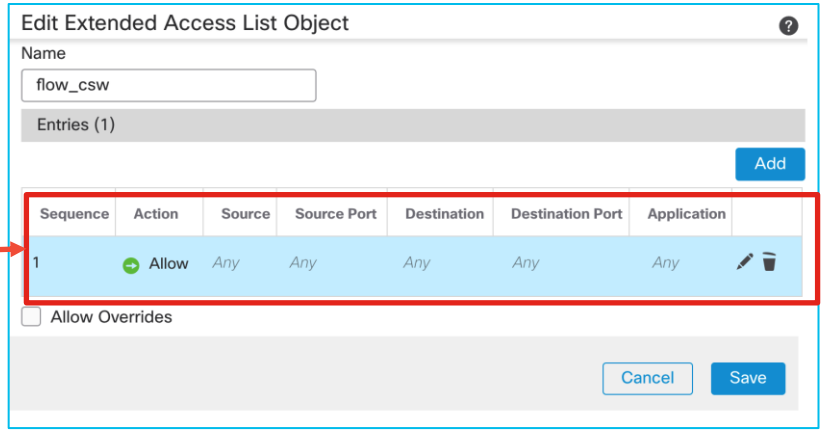
Field	NSEL Element ID	NSEL Element Name
Protocol	4	*NF_F_PROTOCOL*
Source Address	226	*NF_F_XLATE_DST_ADDR_IPV4*
	282	*NF_F_XLATE_DST_ADDR_IPV6*
Source Port	228	*NF_F_XLATE_DST_PORT*
Destination Address	225	*NF_F_XLATE_SRC_ADDR_IPV4*
	281	*NF_F_XLATE_SRC_ADDR_IPV6*
Destination Port	227	*NF_F_XLATE_SRC_PORT*
Flow Start Time	152	*NF_F_FLOW_CREATE_TIME_MSEC*
Byte Count	232	*NF_F_REV_FLOW_DELTA_BYTES*
Packet Count	299	*NF_F_REV_FLOW_DELTA_PACKETS*

FMC Netflow extended access list

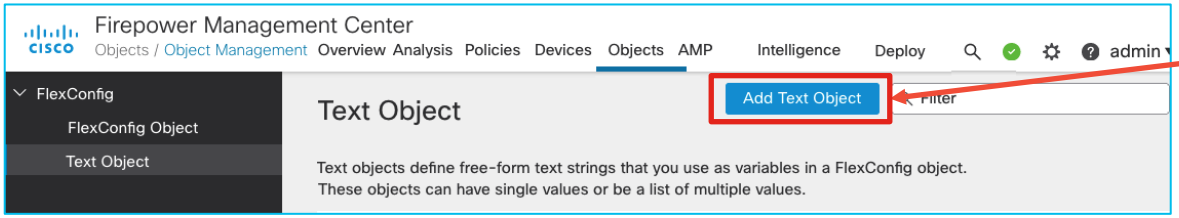


1. Navigate to Objects > Access List > Extended > Add Extended Access List

2. Name the ACL and specify the interested flow information to export NSEL information

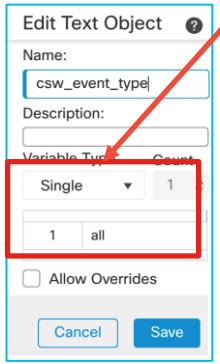


FMC FlexConfig text objects



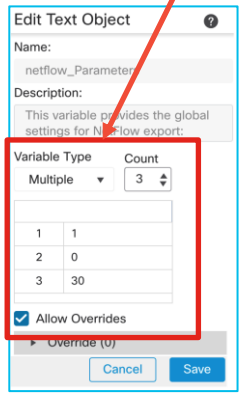
1. Navigate to Objects > FlexConfing Object > Text Object and Add 2 Text Objects

2. The first object is **single variable** for **netflow event type**. In this example we are using all (check Secure Workload user guide for more specifics event types)



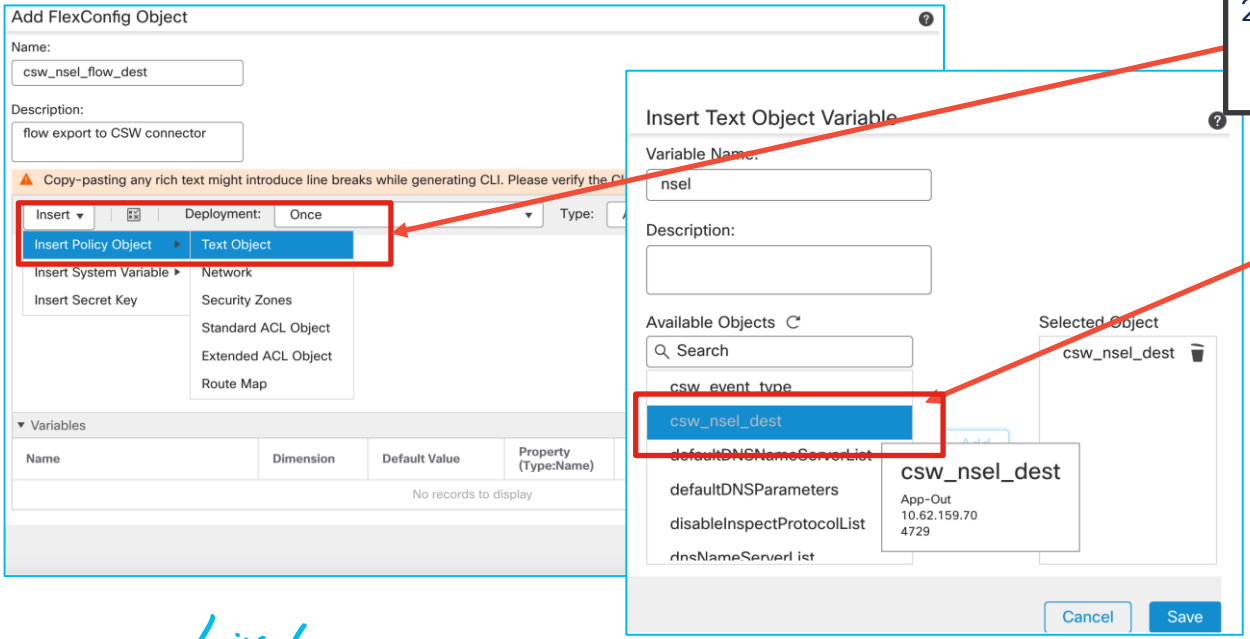
3. The second object is **multiple variable** for **netflow destination**. Syntax is *interface name, netflow destination IP, destination port*

4. Last one is the netflow parameters. You can use the default ones or create a new one (default one shown below).



FMC FlexConfig flow destination

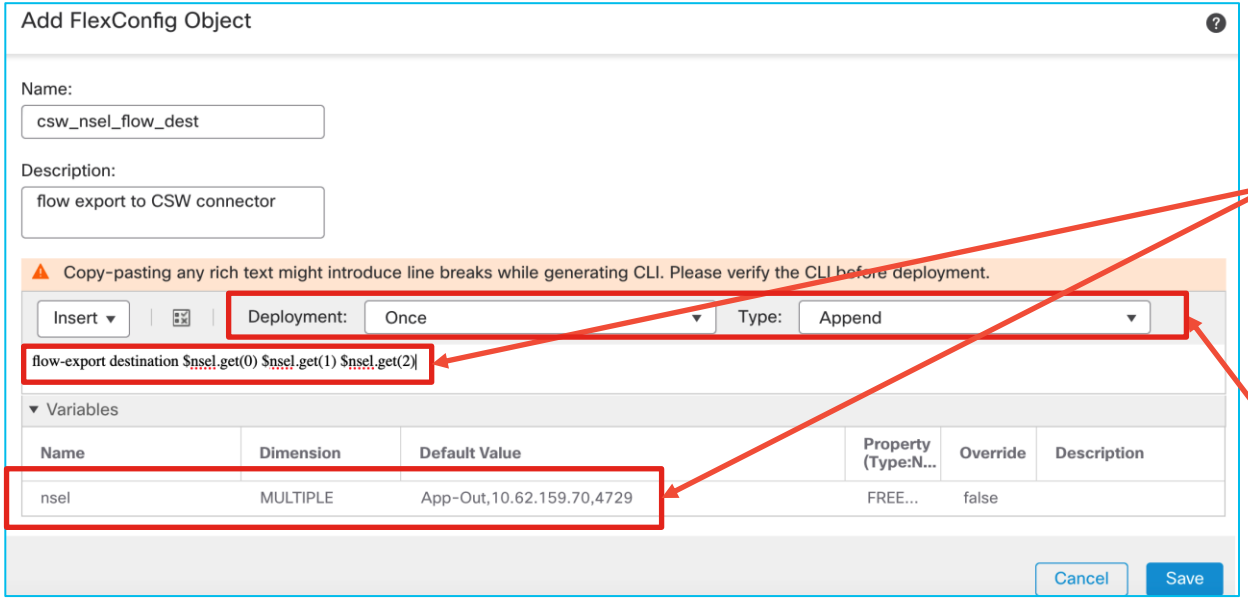
1. Navigate to FlexConfig > FlexConfig Object and Add **three** new Flexconfig Object



2. Name the FlexConfig object and select Insert **Policy Object > Text Object**

3. Name the variable and add the **"csw_nsel_dest"** object created before

FMC FlexConfig flow destination



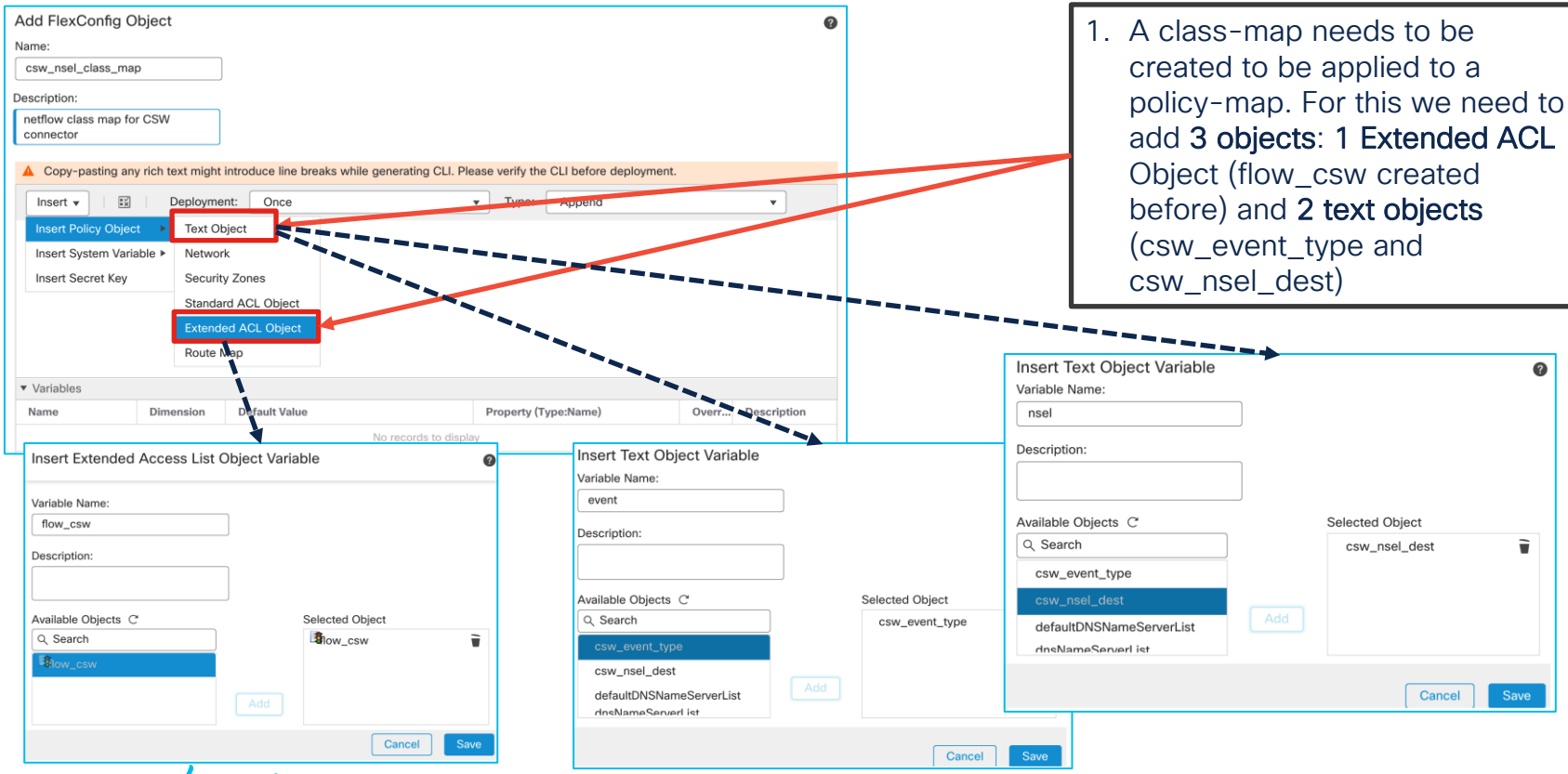
4. Use CLI syntax "**flow export destination *<interface variable name> <address variable> <port variable>*"** where variable values are imported from the objects

To get the variable values, you need to call the variable by appending **symbol $** to the variable name ($nsel) followed by a "dot"get and the variable location (e.g 0, 1, 2)

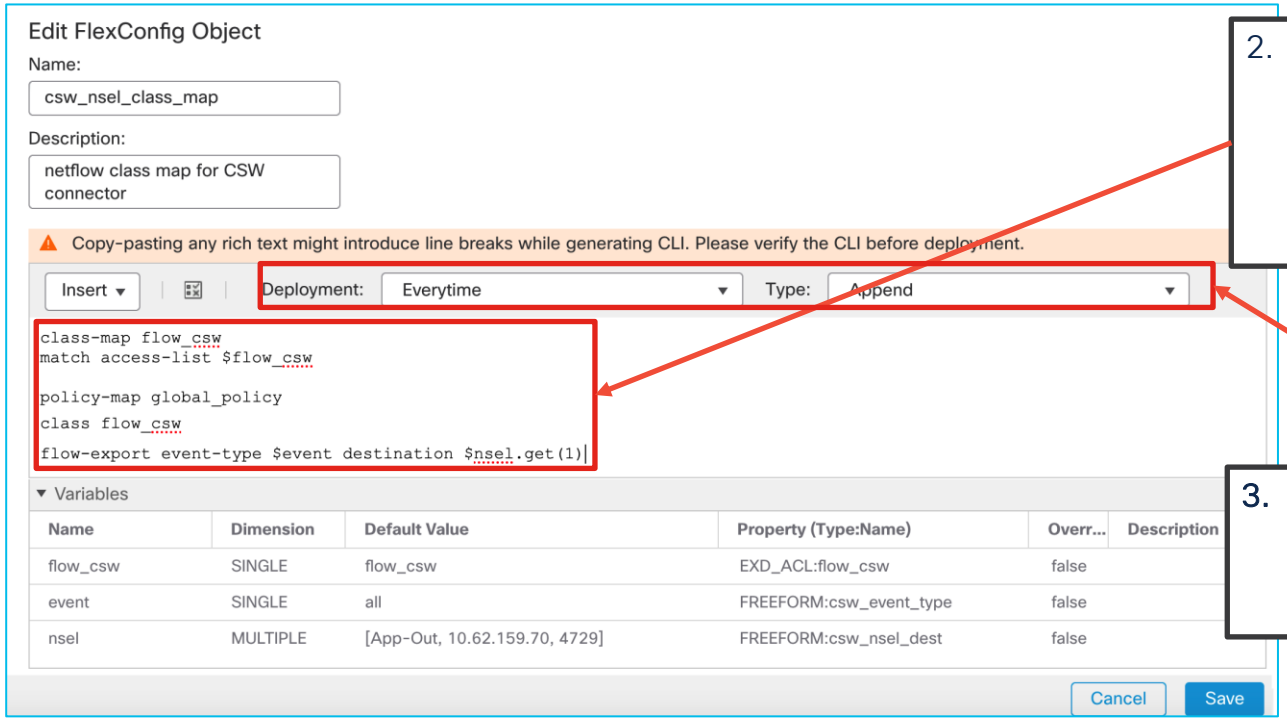
flow-export destination $nsel.get(0) $nsel.get(1) $nsel.get(2)

5. **Deployment** for this FlexConfig Object must be **Once** and **type Append**

FMC FlexConfig class map



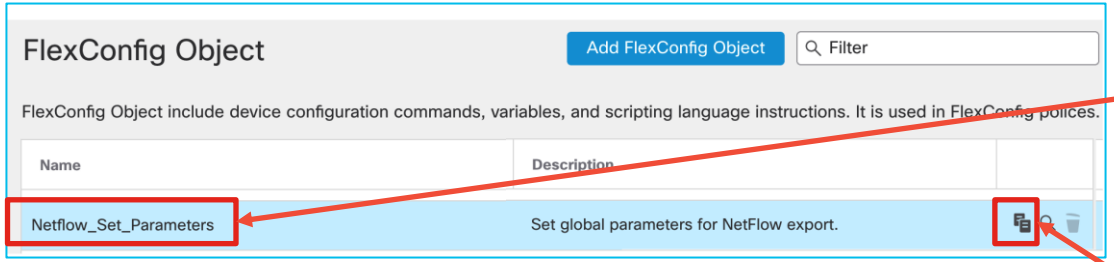
FMC FlexConfig class map



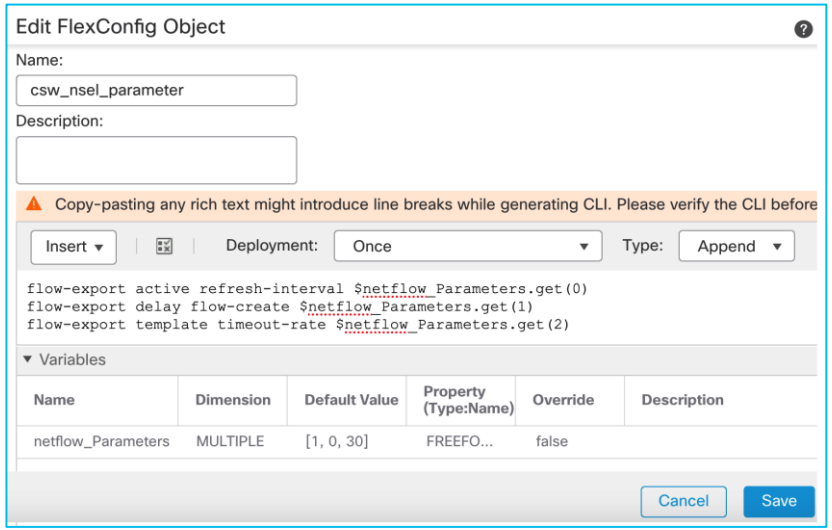
2. Apply the same principle as with the Flow Destination FlexConfig Object. Use CLI syntax to map a class-map to the extended access-list and apply the class-map to the policy-map

3. **Extremely Important!.** Deployment type for this FlexConfig Object **MUST be Everytime** and type **Append.**

FMC FlexConfig NSEL parameters



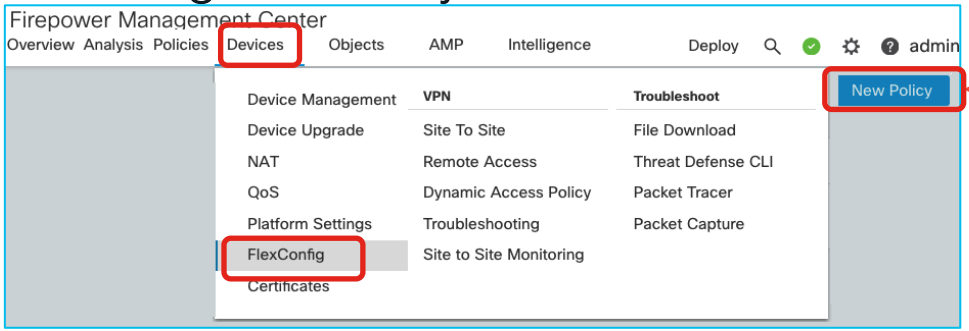
1. NSEL parameter is optional (if not specified, default values will be used).



2. In this example we create a new FlexConfig Object by copying the default FlexConfig Object. All values used are default. Deployment is set to **Once** and type **Append**

FMC NetFlow export

Sending telemetry data to Secure Workload!



1. Navigate to Devices > FlexConfig > create New Policy

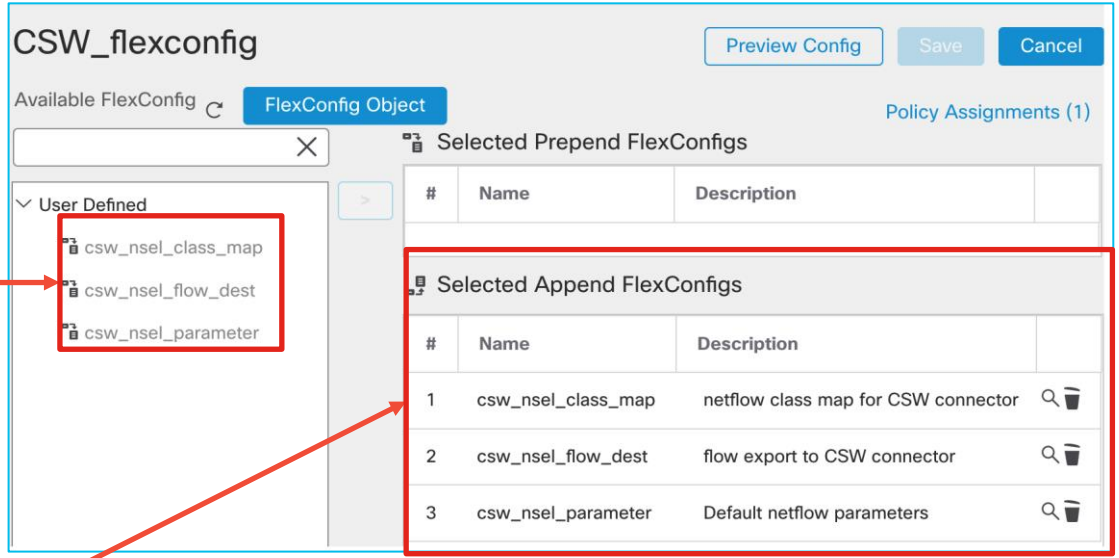
2. Create a new FlexConfig Policy and assign the Secure Firewall sending telemetry

FMC NetFlow export

Sending telemetry data to Secure Workload!

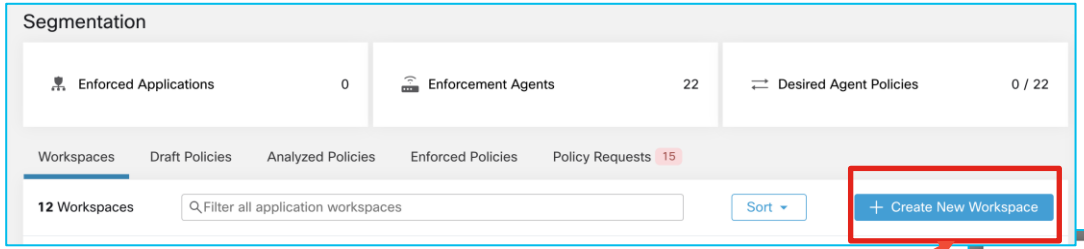
3. Select all FlexConfigs NSEL Objects created

4. Verify the FlexConfigs Objects are appended and Save. Once done you can proceed to deploy



ADM workspace (visibility)

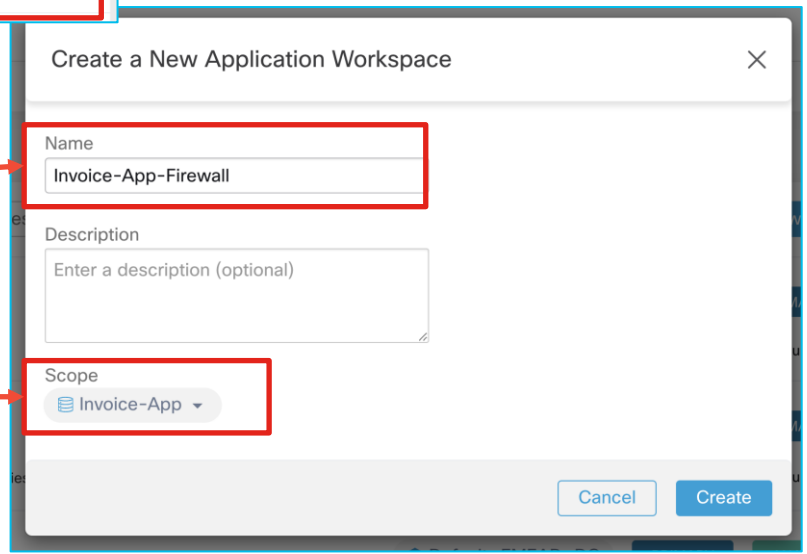
Get Visibility of manual and automated generated policies!



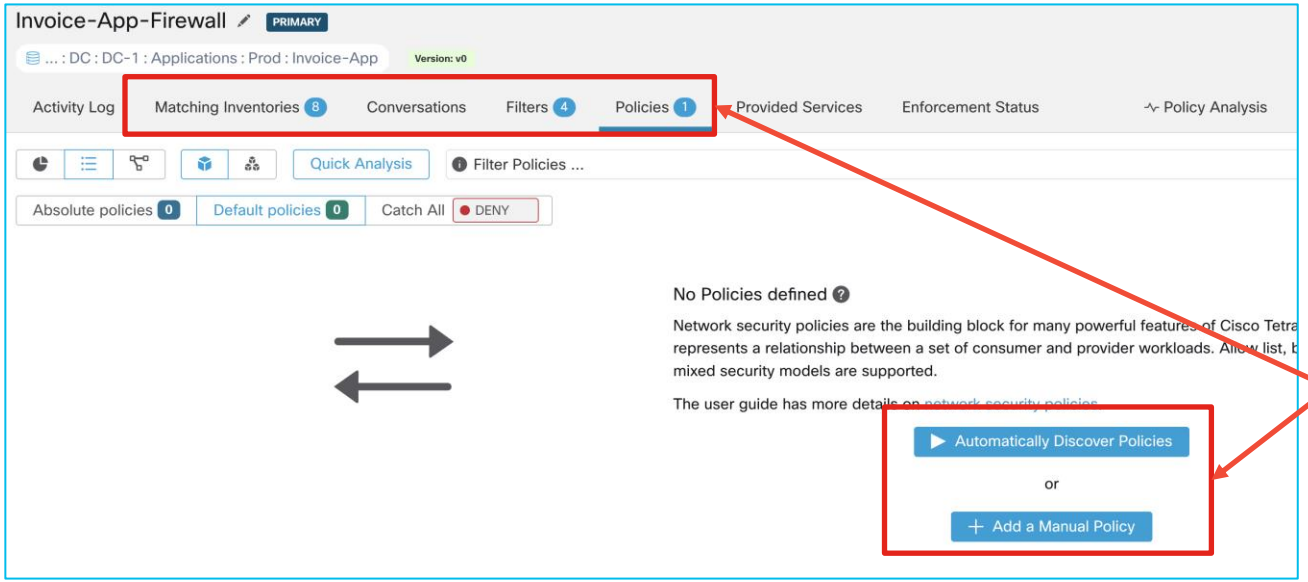
1. Navigate to Defend > Segmentation and create a new application workspace

NOTE: In this case we are this workspace is for an agentless application

2. Select the appropriate scope

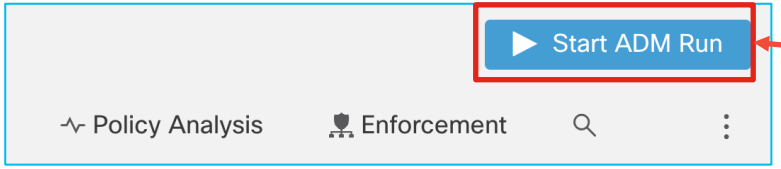


ADM workspace (visibility)

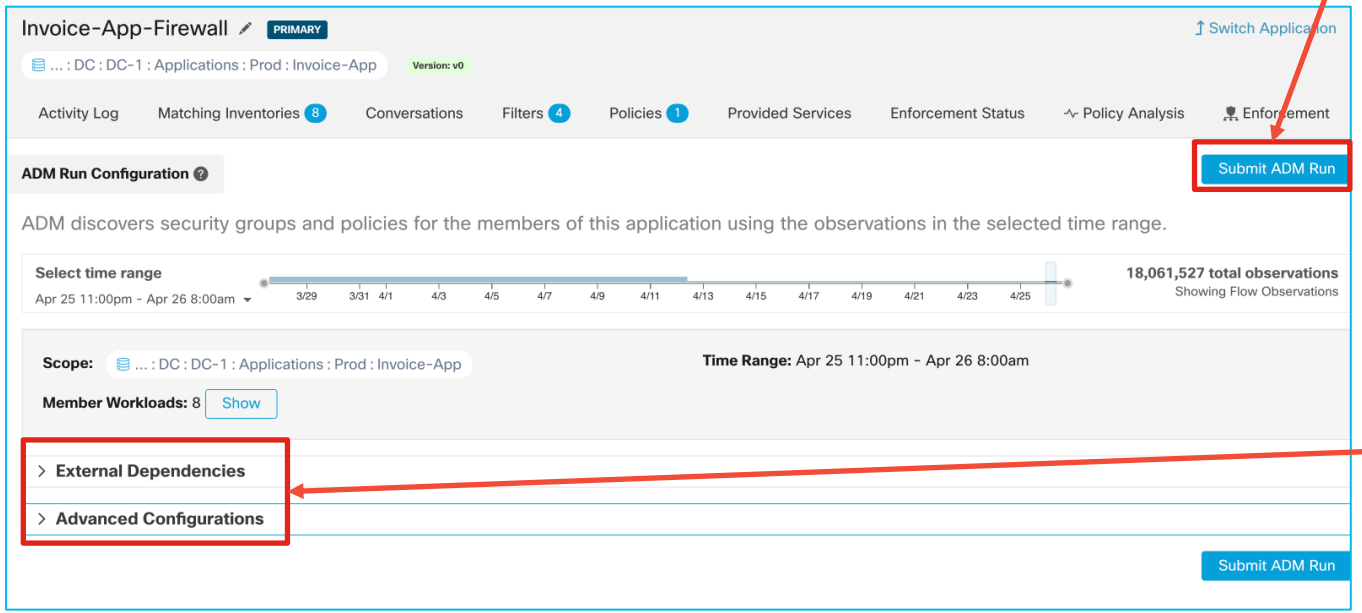


1. Currently no policies are defined. You can create manual policies, run ADM to discover policies or both!
2. Exploring other tabs, you can observe that there are **8** matching inventories (8 workloads) that are part of this application
3. Also, you can check that there are 4 filters already pre-cared. Leverage the knowledge of this workloads to pre-create inventory filters and promote clusters discovered by ADM.
4. Finally, only one policy is present (DENY CATCH ALL)

ADM workspace (visibility)

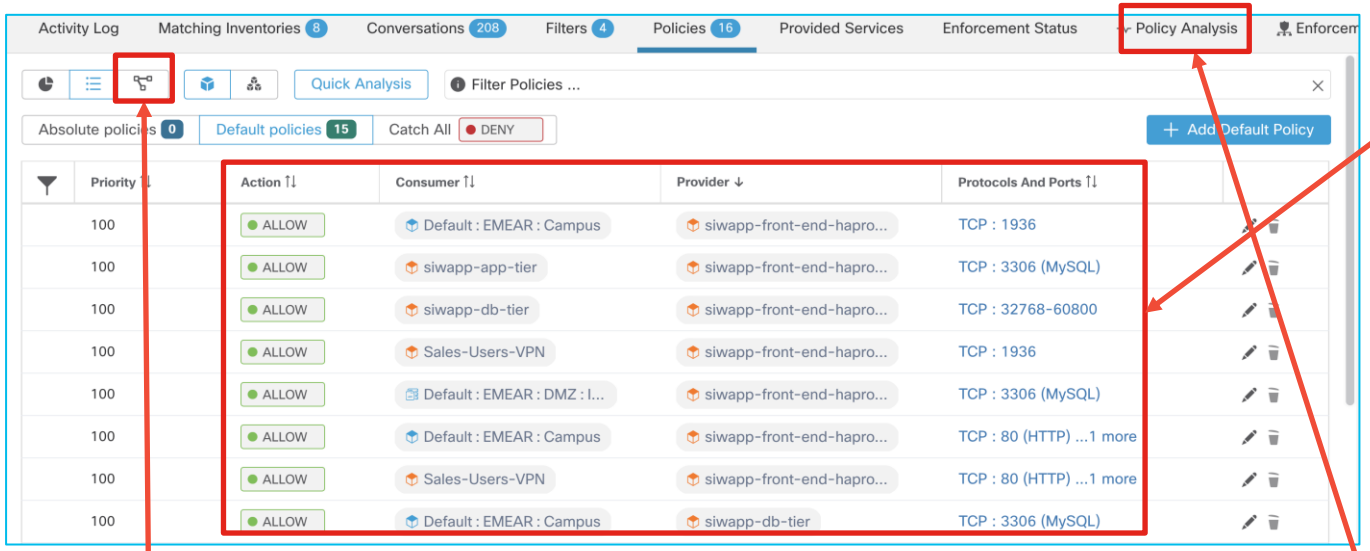


1. Select a time-range to run ADM and submit ADM Run



2. It is also possible to tune ADM with additional parameters such as external dependencies (to match inventory filters instead of full scopes) and advance configurations for ADM granularity.

ADM workspace (visibility)

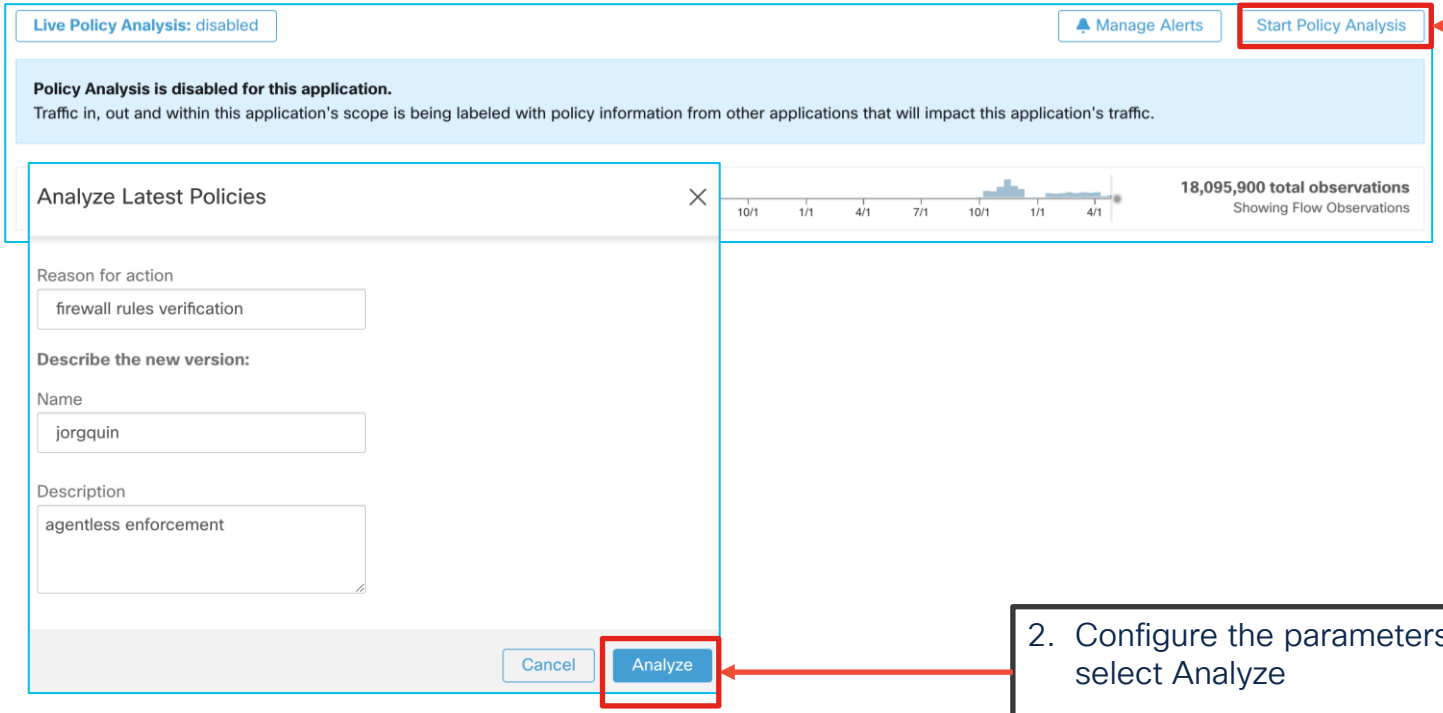


1. ADM has automatically suggested 14 allow-list zero trust policies (15 is catch all deny).

2. For further analysis, Policy Analysis can be enabled to verify with real operation traffic flows how the policies will filter traffic

3. There is another view to the policy list, which is call “Policy Canvas”, detailing in a graphical way how the policies look like

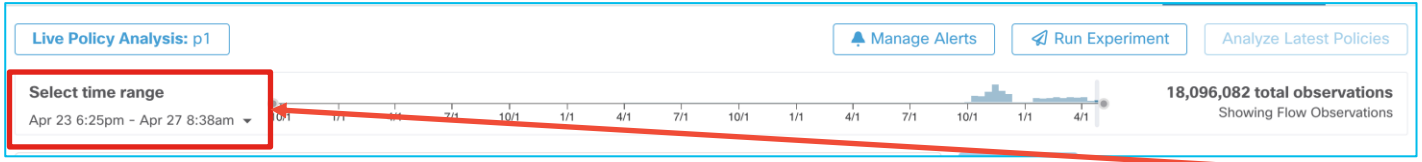
ADM workspace (visibility)



1. Enable Policy Analysis

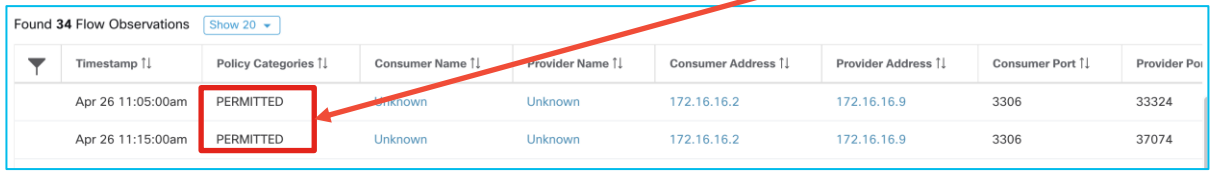
2. Configure the parameters and select Analyze

ADM workspace (visibility)



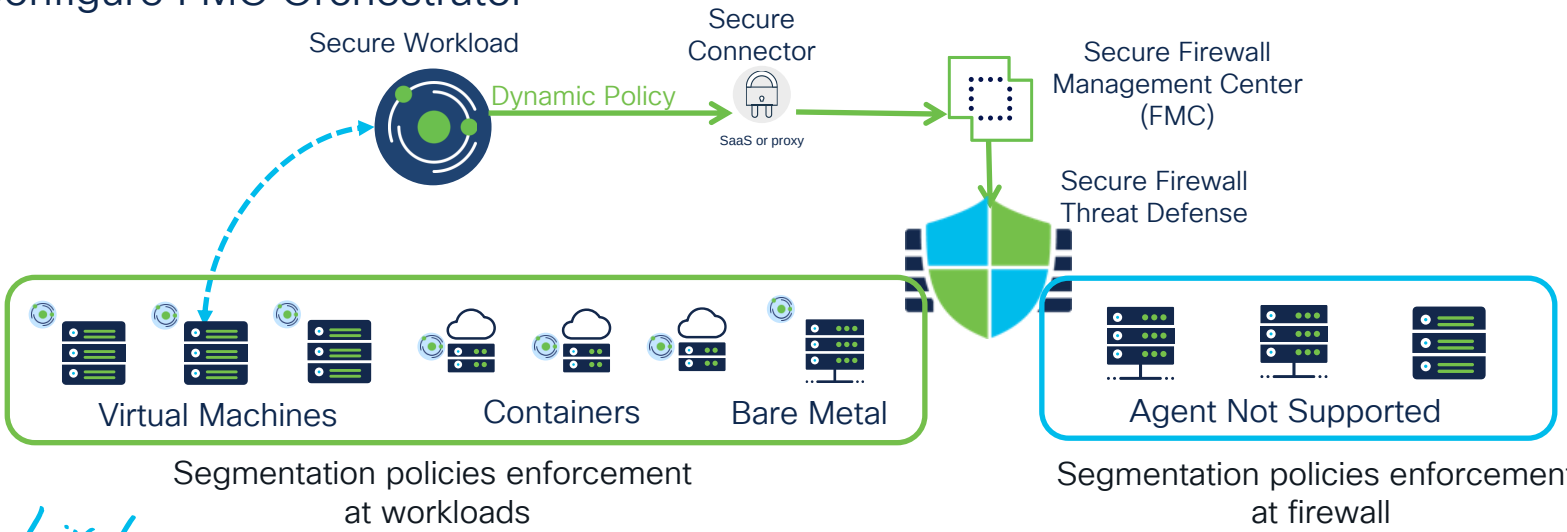
1. Select a time range to perform the analysis.

2. Filtering of flows can be done by specifying particular flows or by policy category (Permitted, Rejected, Escaped) and verify the result



Configuration overview – enforcement

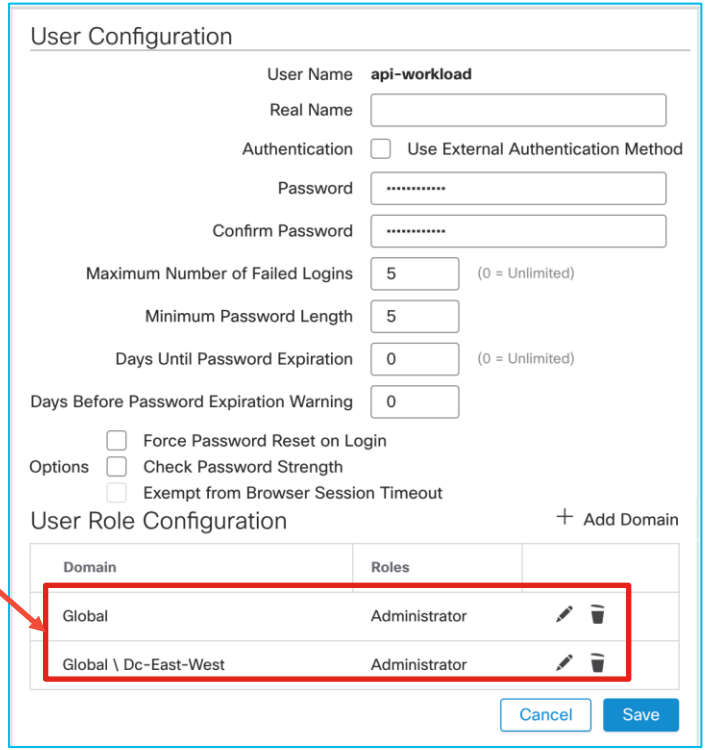
- Secure Workload
  - Deploy Secure Connector (if required)
  - Create REST API admin user in FMC
  - Configure FMC Orchestrator



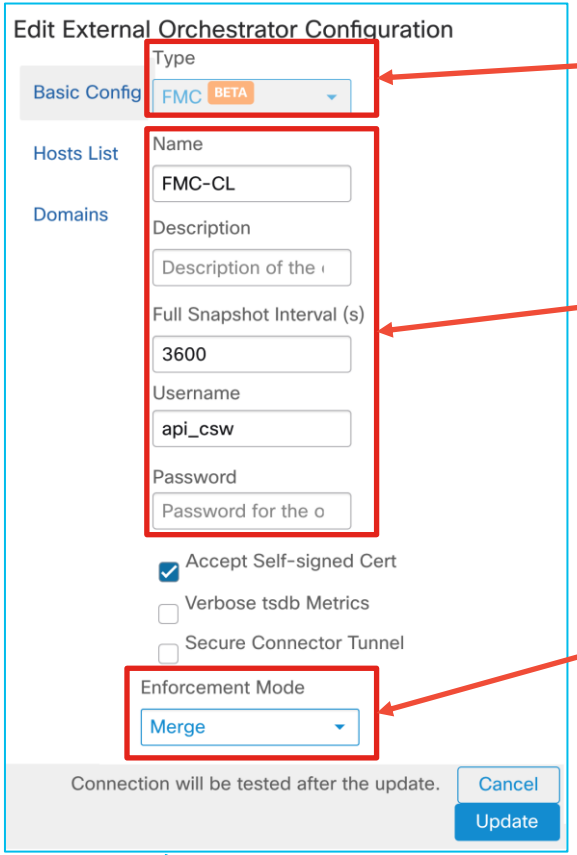
FMC REST API user

Automating policy deployment to Secure Firewalls

1. Configure REST API user. User must have access to the **global domain** and the **domain** where the **controlled firewall** is located and must have administrator rights.



Secure Workload external orchestrator



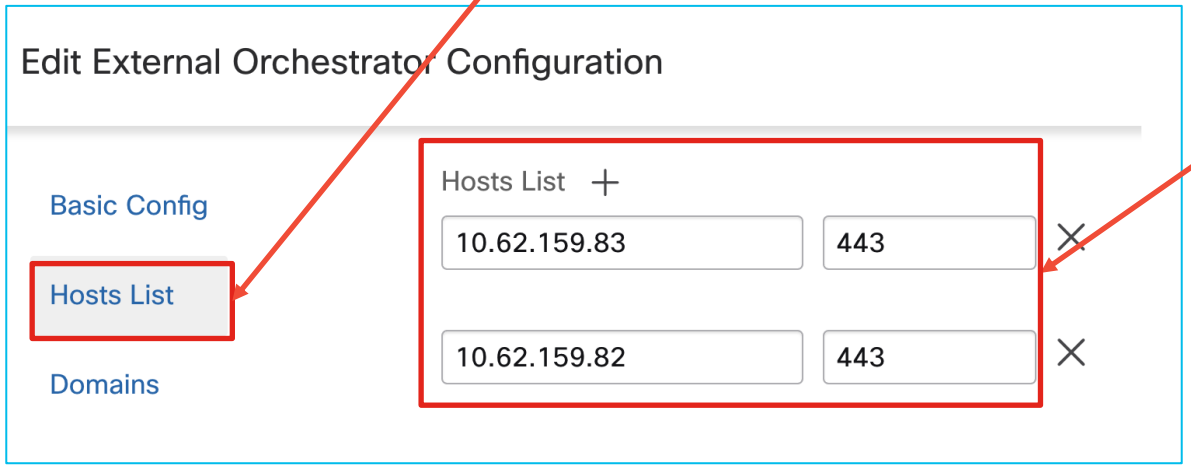
1. Select under Type “FMC”

2. Configure name, description, api username and password. If FMC is behind a proxy, you will need to enable Secure Connector Tunnel.

3. For enforcement, configure **“Merge”** if you want to still keep existing rules in FMC ACP or **“Override”** to only have Secure Workload rules.

Secure Workload external orchestrator

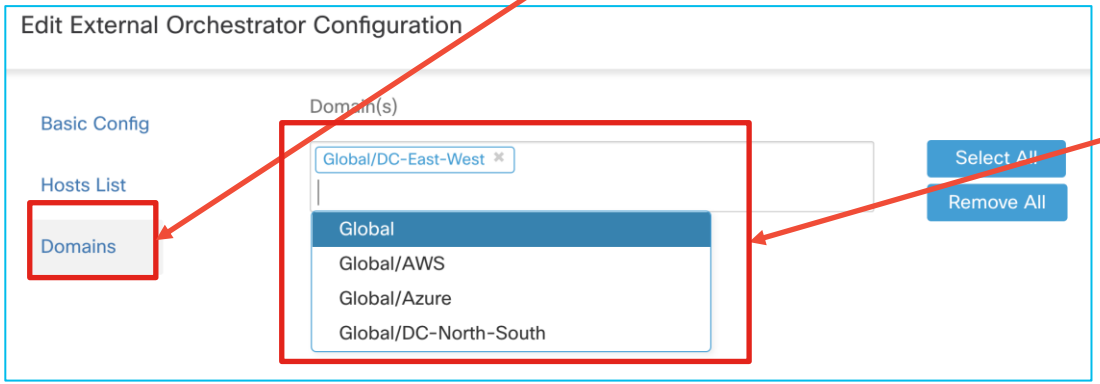
1. Select “Hosts List”



2. Configure the FMC IP address of Primary and port. Optionally Secondary FMC

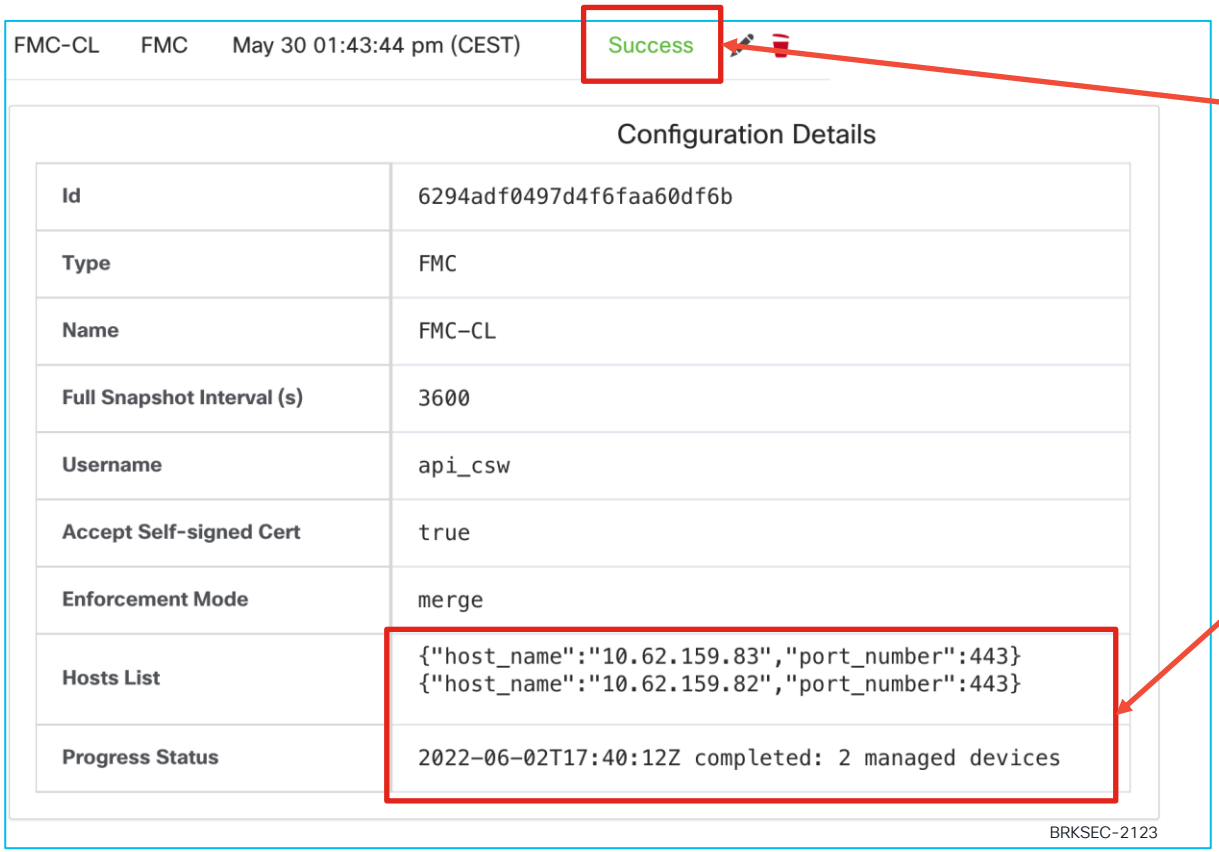
Secure Workload external orchestrator

1. Select “Domains”



2. Select the domain or domains for enforcement

Secure Workload external orchestrator

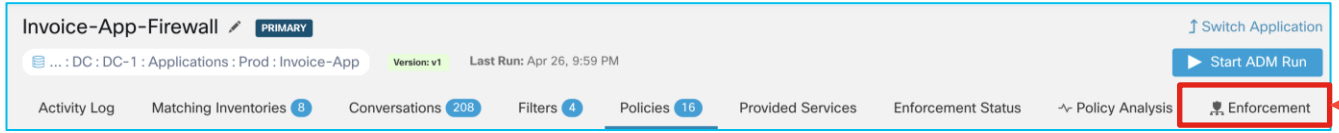


1. Verify that the connection status is success.

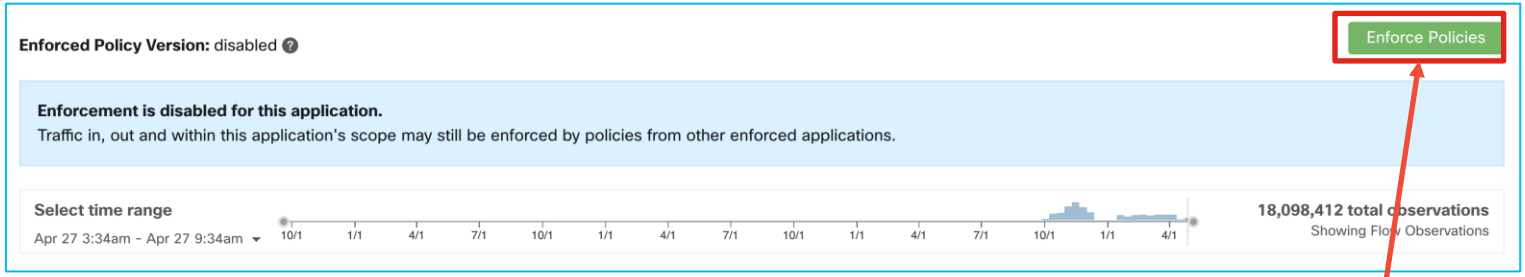
Note: It will fail at the very first try and afterwards (if everything is correct) will change to success.

2. By clicking on the External Orchestrator, you will get additional information (e.g how many managed devices were detected or the reason of failure)

ADM workspace (enforcement)

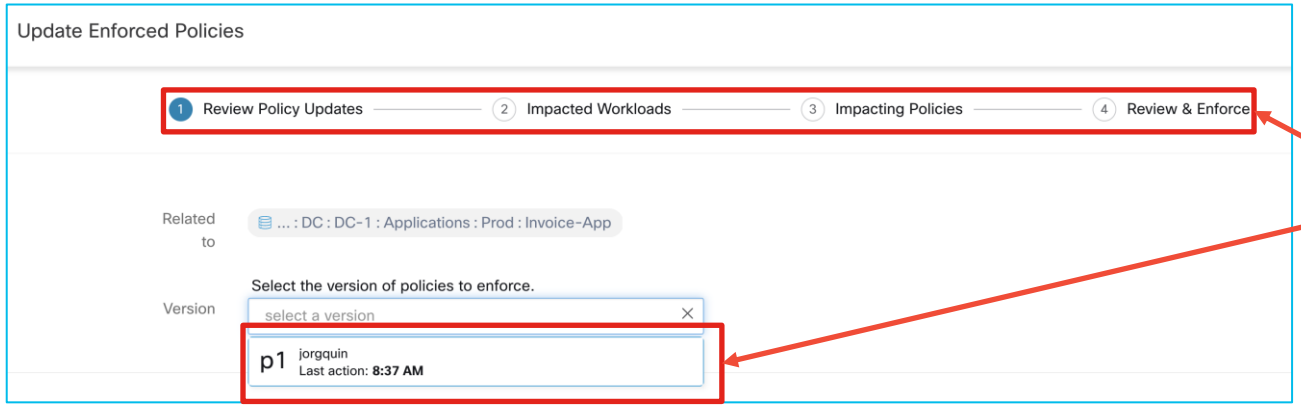


1. Navigate back to the ADM workspace and select “Enforcement”

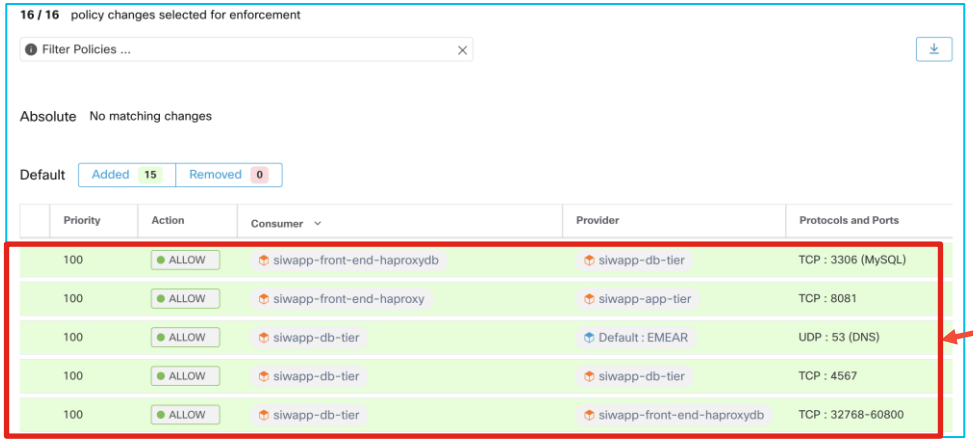


2. Select “Enforce Policies”

ADM workspace (enforcement)

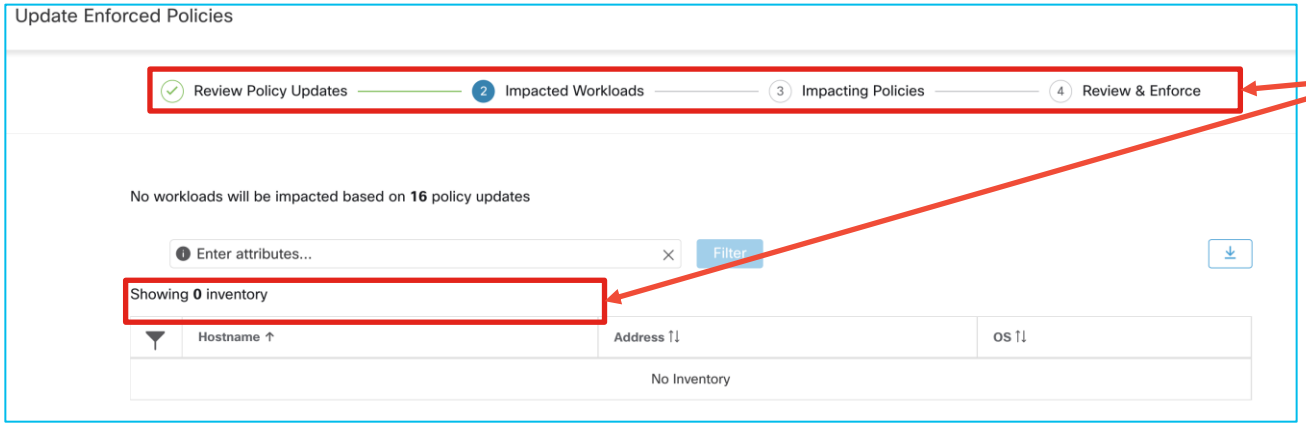


1. A Wizard will pop-up and guide you through the enforcement process. Select the policy version



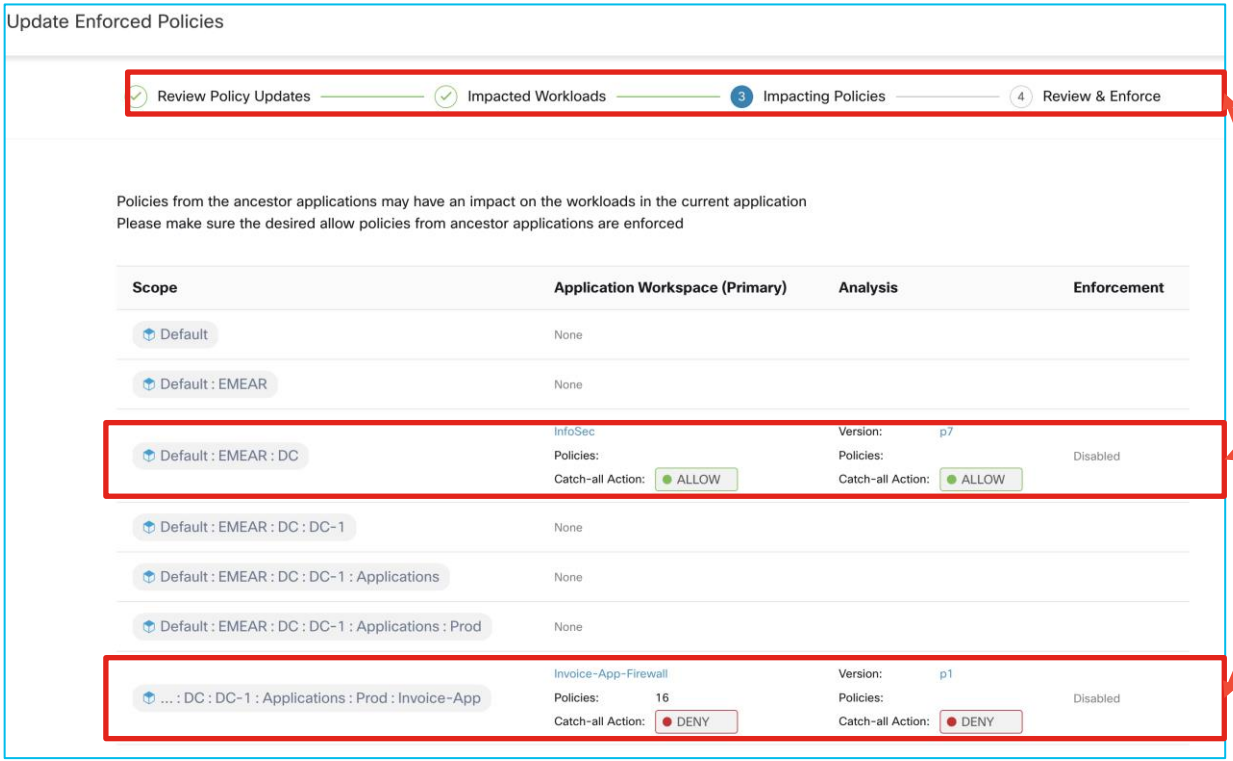
2. Verify the policies to be pushed to the firewall

ADM workspace (enforcement)



1. Because we are enforcing an agentless application, no host will be shown.

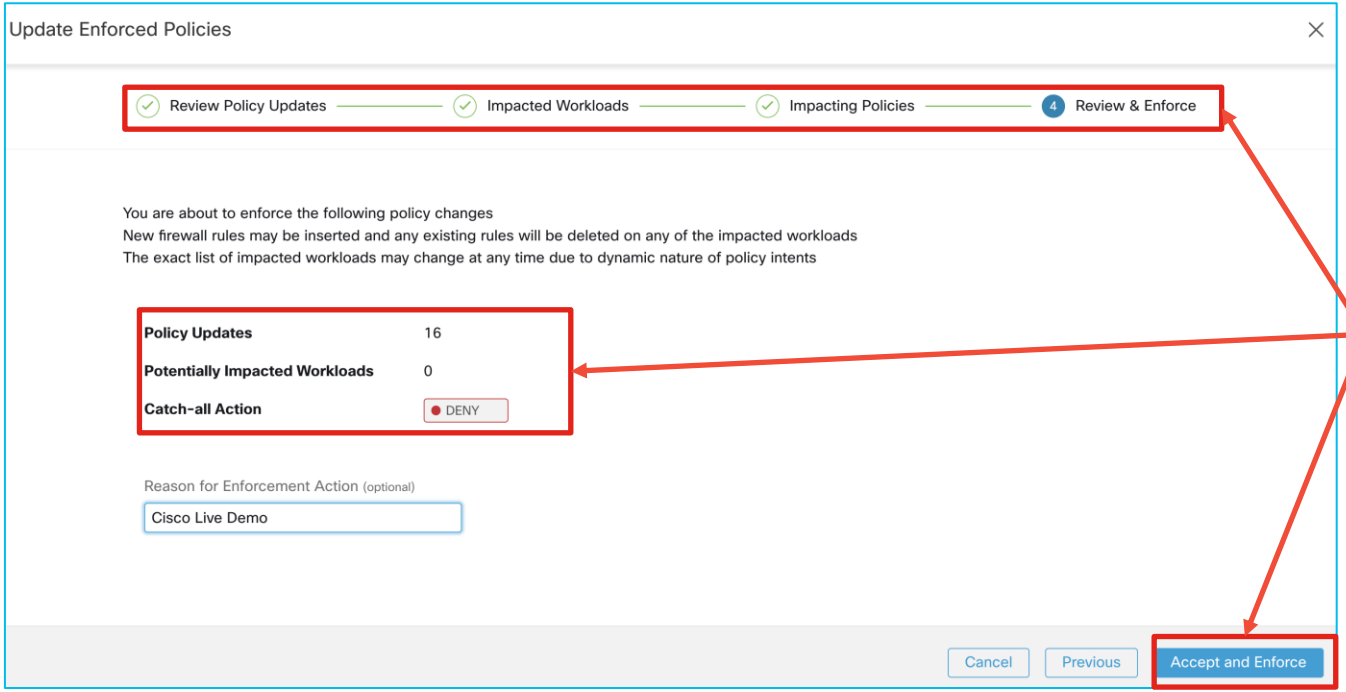
ADM workspace (enforcement)



1. Secure Workload will flatten the hierarchical policies. This means that policies created on upper scopes (e.g Compliance or Regulatory) will take precedence, and lastly the application specific policies.

In this example, we can see that the InfoSec compliance rules are allowing the traffic and at the bottom we have the Application specific rules, with the default catch-all action

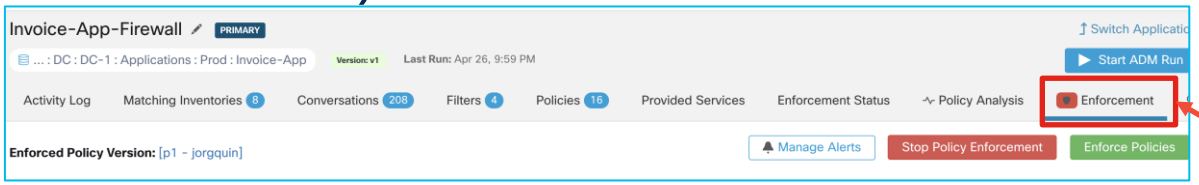
ADM workspace (enforcement)



1. Before enforcement, please make sure to understand the requirements of the integration. We **only** recommend to enforce on new deployments.

While possible to integrate with existing deployments, we strongly discourage it at the moment. It may result in undesirable outcomes

ADM workspace (enforcement – add policy decision)



1. Verify that the policy enforcement is allowing the require flows and rejecting (filtering) traffic that is not in the policy

2. You can also see the reason of the rejected flows. In this case is the Catch-All Deny rule

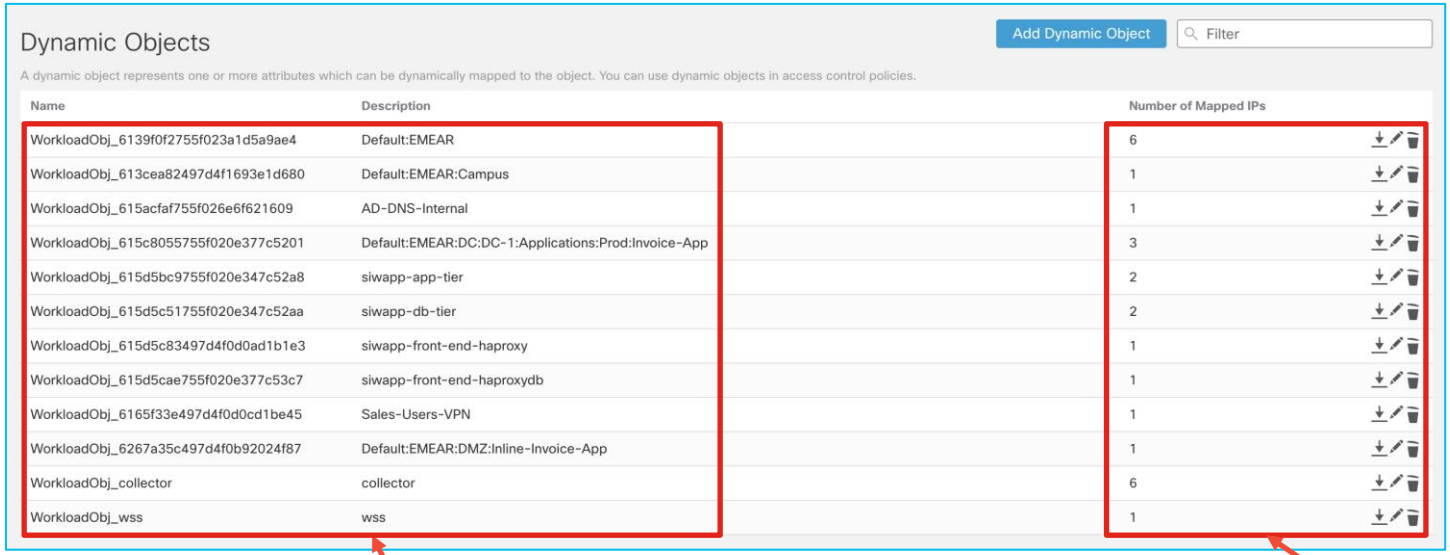
Found **3** Flow Observations Show 20

Timestamp	Policy Categories	Outbound Policy Rank	Inbound Policy Rank	Consumer Address	Provider Address	Consumer Port	Provider Po
Apr 27 9:48:00am	PERMITTED	Unknown	Unknown	172.16.16.2	172.16.16.9	3306	60006
Apr 27 10:23:00am	PERMITTED	Default	Default	172.16.16.2	172.16.16.9	3306	44664
Apr 27 10:40:00am	PERMITTED	Default	Default	172.16.16.2	172.16.16.9	3306	44664

Found **26** Flow Observations Show 20

Timestamp	Policy Categories	Outbound Policy Rank	Inbound Policy Rank	Consumer Address	Provider Address	Consumer Port	Provider Po
Apr 27 9:53:00am	REJECTED	Catch All	Unknown	172.16.16.6	185.141.27.108	51151	123
Apr 27 9:53:00am	REJECTED	Unknown	Catch All	10.63.42.243	172.16.16.6	0	51137
Apr 27 9:53:00am	REJECTED	Catch All	Unknown	172.16.16.6	116.203.52.212	51137	123

FMC dynamic objects



Dynamic Objects

Add Dynamic Object | Filter

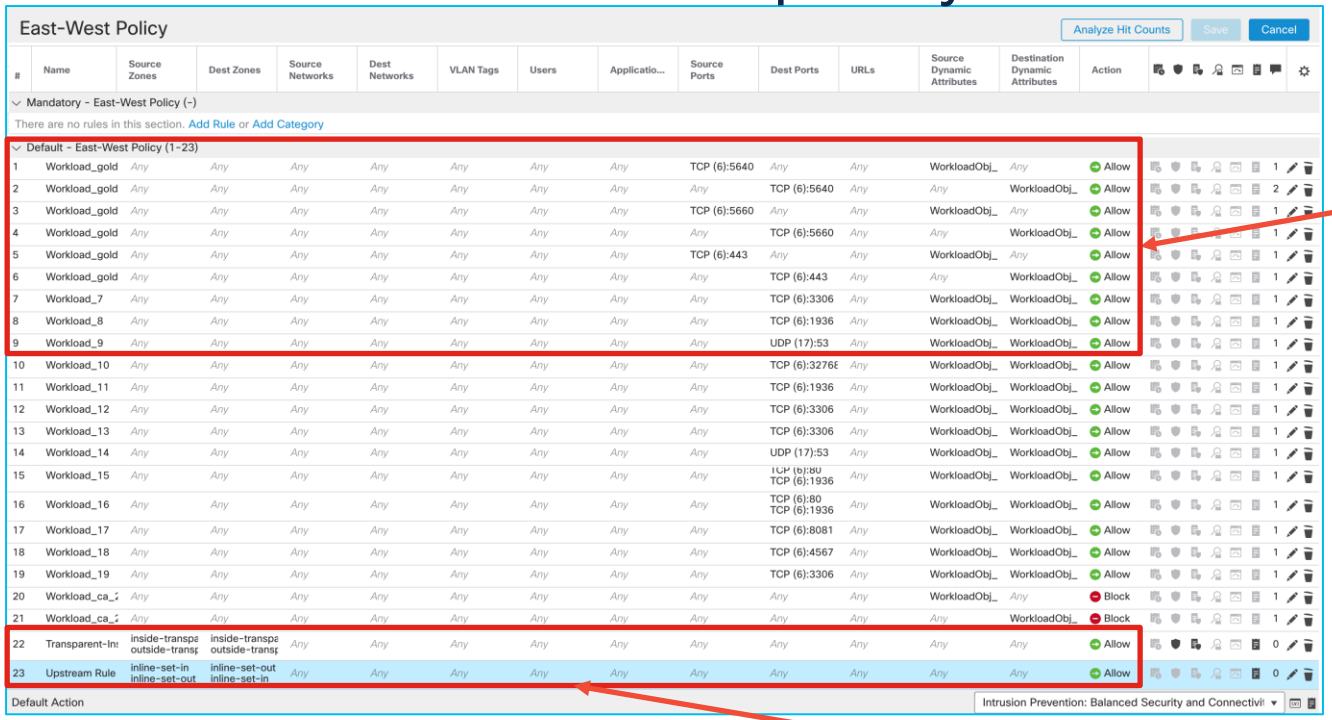
A dynamic object represents one or more attributes which can be dynamically mapped to the object. You can use dynamic objects in access control policies.

Name	Description	Number of Mapped IPs
WorkloadObj_6139f0f2755f023a1d5a9ae4	Default:EMEAR	6
WorkloadObj_613cea82497d4f1693e1d680	Default:EMEAR:Campus	1
WorkloadObj_615acfaf755f026e6f621609	AD-DNS-Internal	1
WorkloadObj_615c8055755f020e377c5201	Default:EMEAR:DC:DC-1:Applications:Prod:Invoice-App	3
WorkloadObj_615d5bc9755f020e347c52a8	siwapp-app-tier	2
WorkloadObj_615d5c51755f020e347c52aa	siwapp-db-tier	2
WorkloadObj_615d5c83497d4f0d0ad1b1e3	siwapp-front-end-haproxy	1
WorkloadObj_615d5cae755f020e377c53c7	siwapp-front-end-haproxydb	1
WorkloadObj_6165f33e497d4f0d0cd1be45	Sales-Users-VPN	1
WorkloadObj_6267a35c497d4f0b92024f87	Default:EMEAR:DMZ:Inline-Invoice-App	1
WorkloadObj_collector	collector	6
WorkloadObj_wss	wss	1

1. Navigate to Objects > Object Management > External Attributes > Dynamic Objects. Here Secure Workload pushes dynamic objects.

2. Each object will have a specific number of IP mapped. There is the option to download and verify the objects

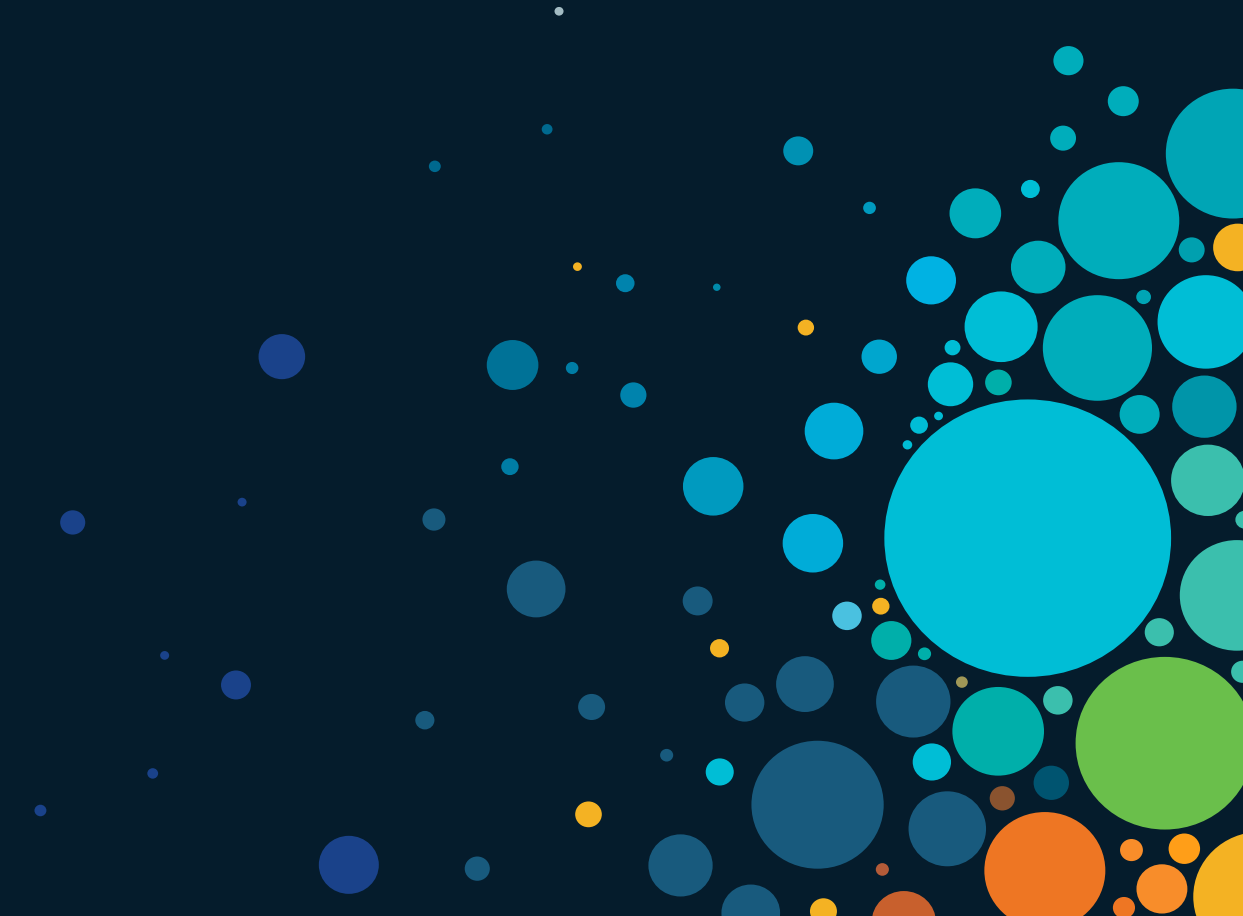
FMC access control policy



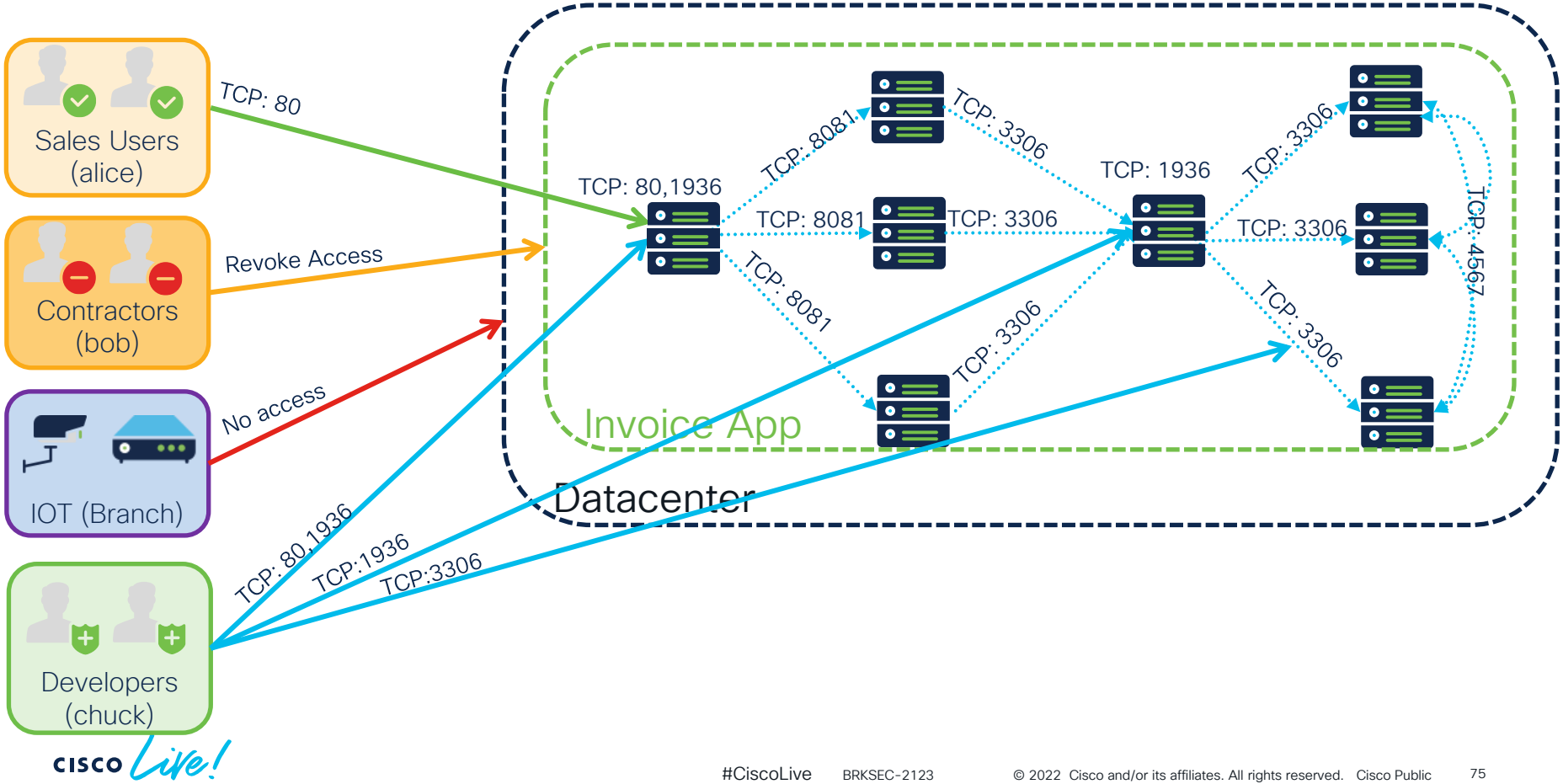
1. Dynamic intent-based policies pushed by Secure Workload!

2. With the **"merge"** options, Secure Workload honors existing ACLs

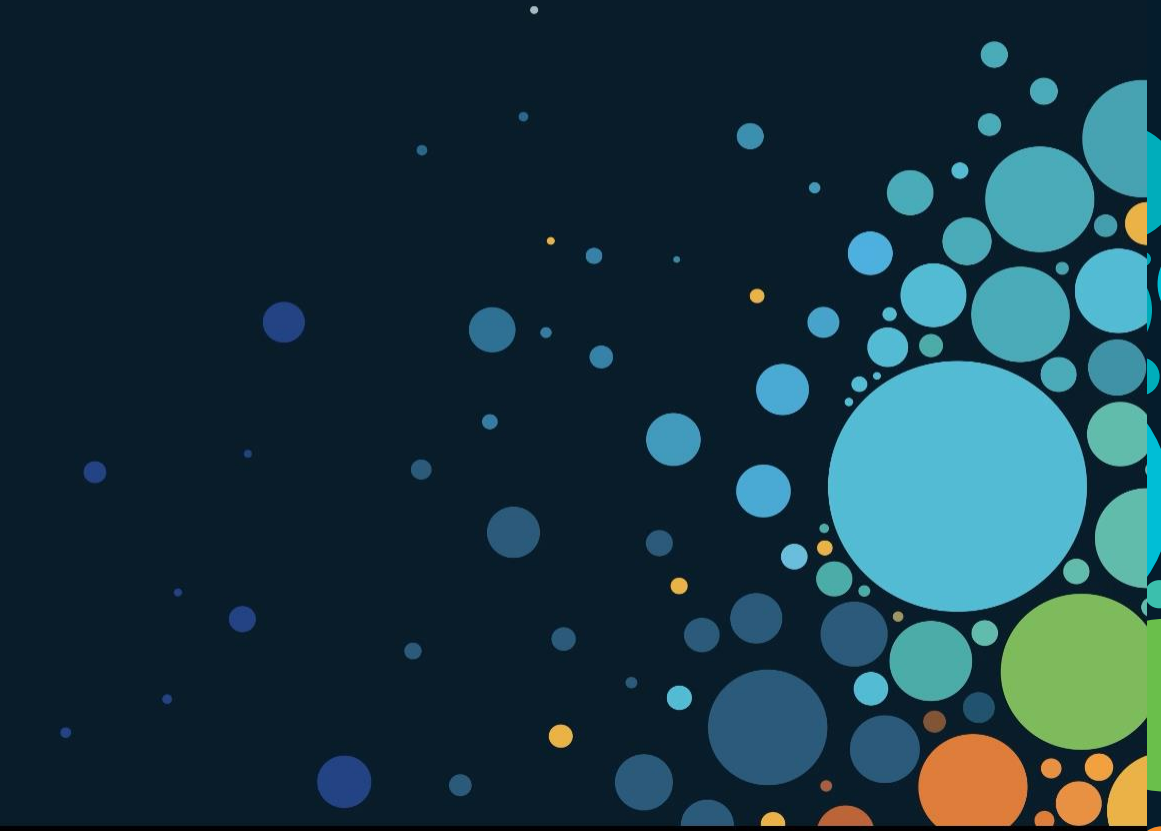
Demo



Zero Trust segmentation for Invoice App



Demo



Summary

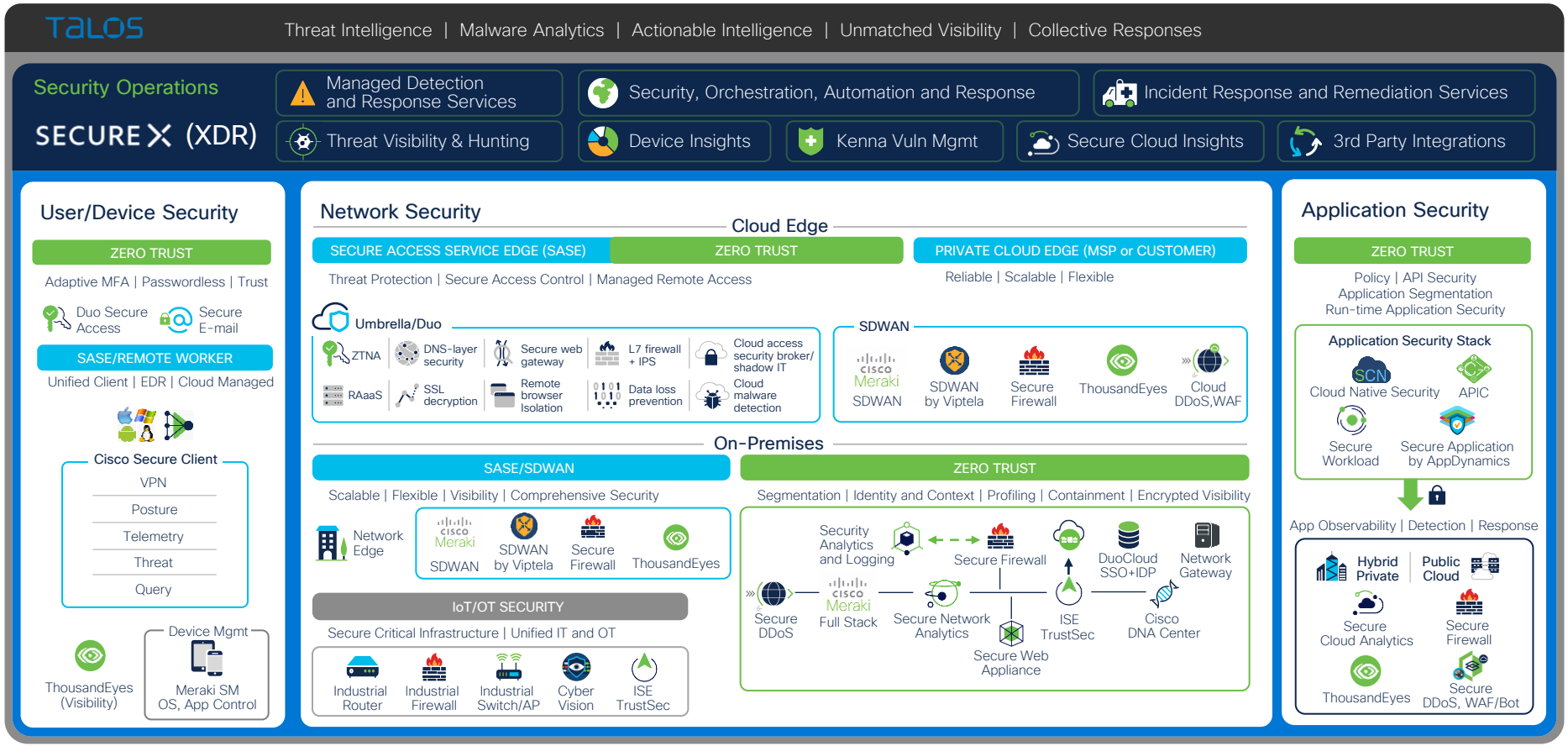
Key takeaways

- Get in-depth visibility of your workloads!
  - Secure Workload + Secure Firewall NSEL
  - Can be deployed in any environment (existing deployments and new deployments)
- For Zero Trust Segmentation Enforcement
  - Recommendation and guidance is only for new deployments
- Enhance your policies with additional integrations!
  - Enrich workload and user identity with integrations such as IPAMs, CMDBs, ISE, AnyConnect and more
  - Threat Containment with FMC Remediation Module

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 Secure | Security Reference Architecture



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