

CISCO *Live!*

ALL IN

#CiscoLive



The bridge to possible

Solving the Segmentation Puzzle! Secure Workload and Secure Firewall Integration

Jorge Quintero, Technical Marketing Engineer

BRKSEC-2123

CISCO *Live!*

#CiscoLive

Cisco Webex App

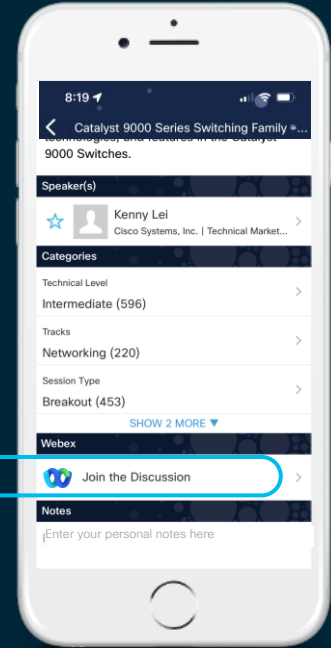
Questions?

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://cicolive.ciscoevents.com/cicolivebot/#BRKSEC-2123>

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



[DEWKS-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](#)

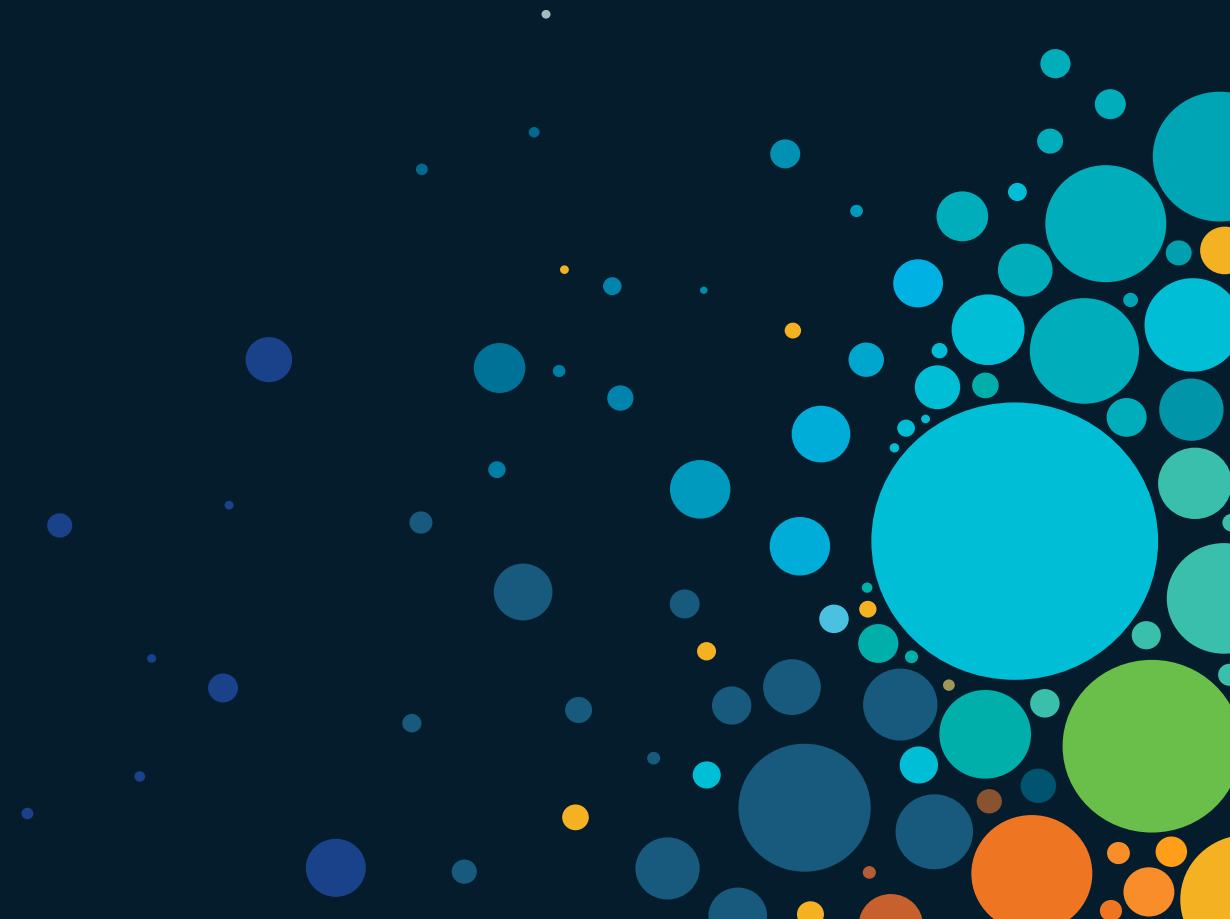
How to Build a Secure Multi-Cloud Environment
with Cisco Secure Workload

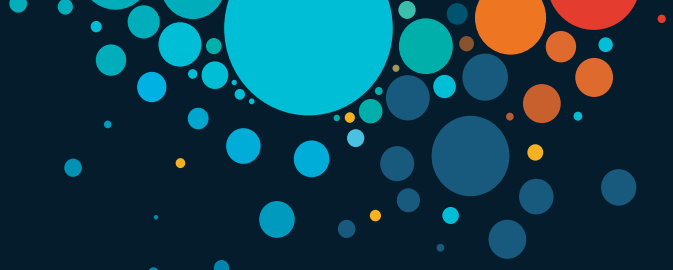


Agenda

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

Introduction





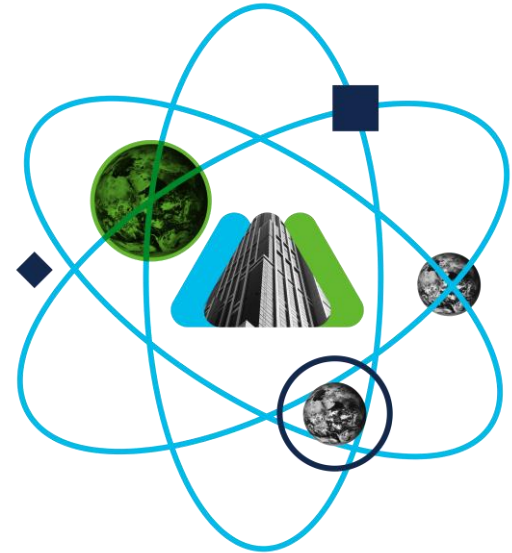
“Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, **least privilege per-request access** decisions in information systems and services in the face of a network viewed as compromised.”

[CISA Zero Trust Maturity Model](#)

CISA

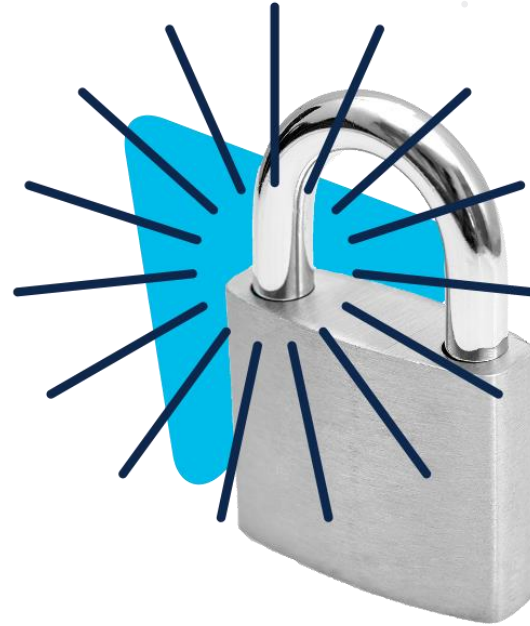
A common theme - Zero Trust..

- 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

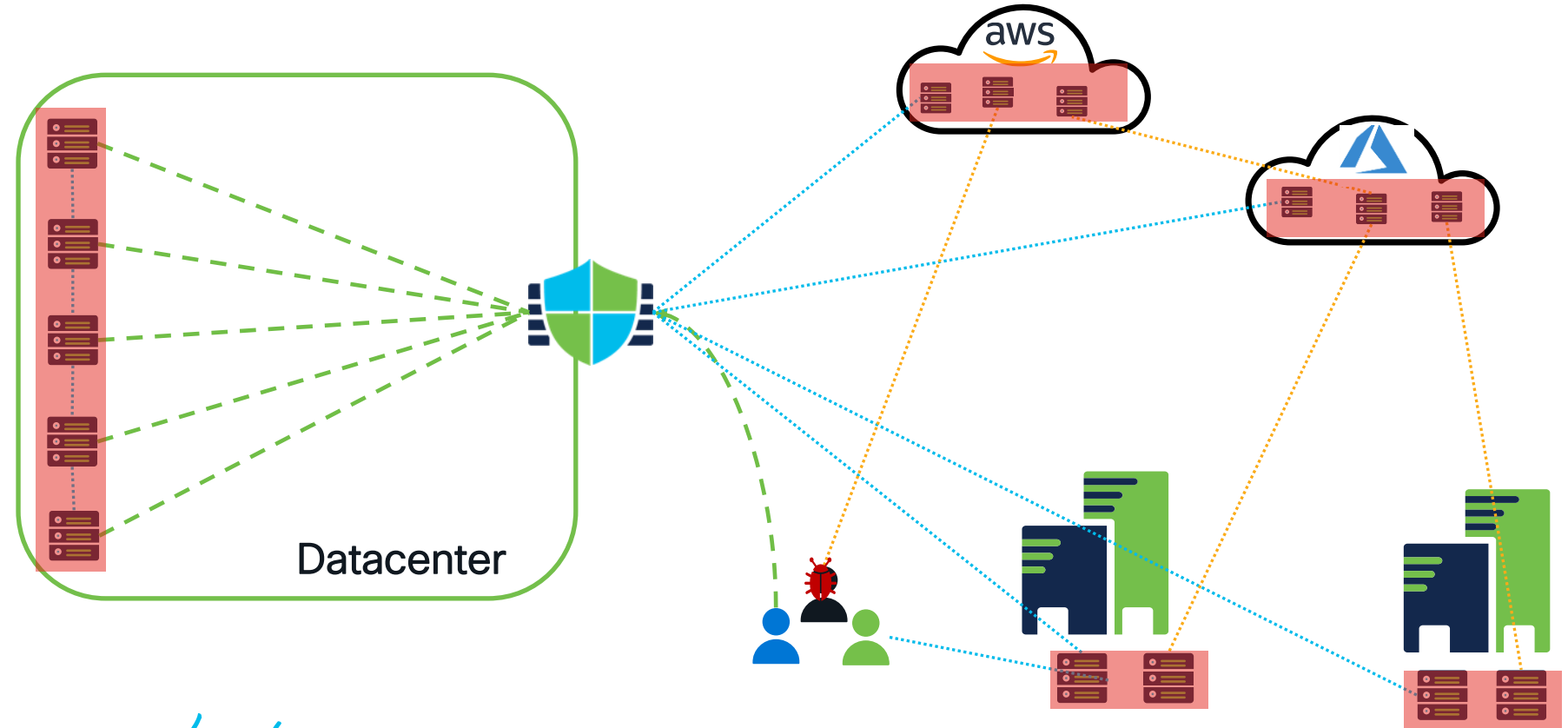


..But all agree segmentation is a critical control

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



Where is the perimeter?



Where can we enforce policy?

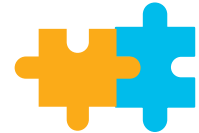
Host-Based



K8s Nodes



Cloud Security Groups



“The Policy Puzzle”



Virtual Desktop



CISCO *Live!*

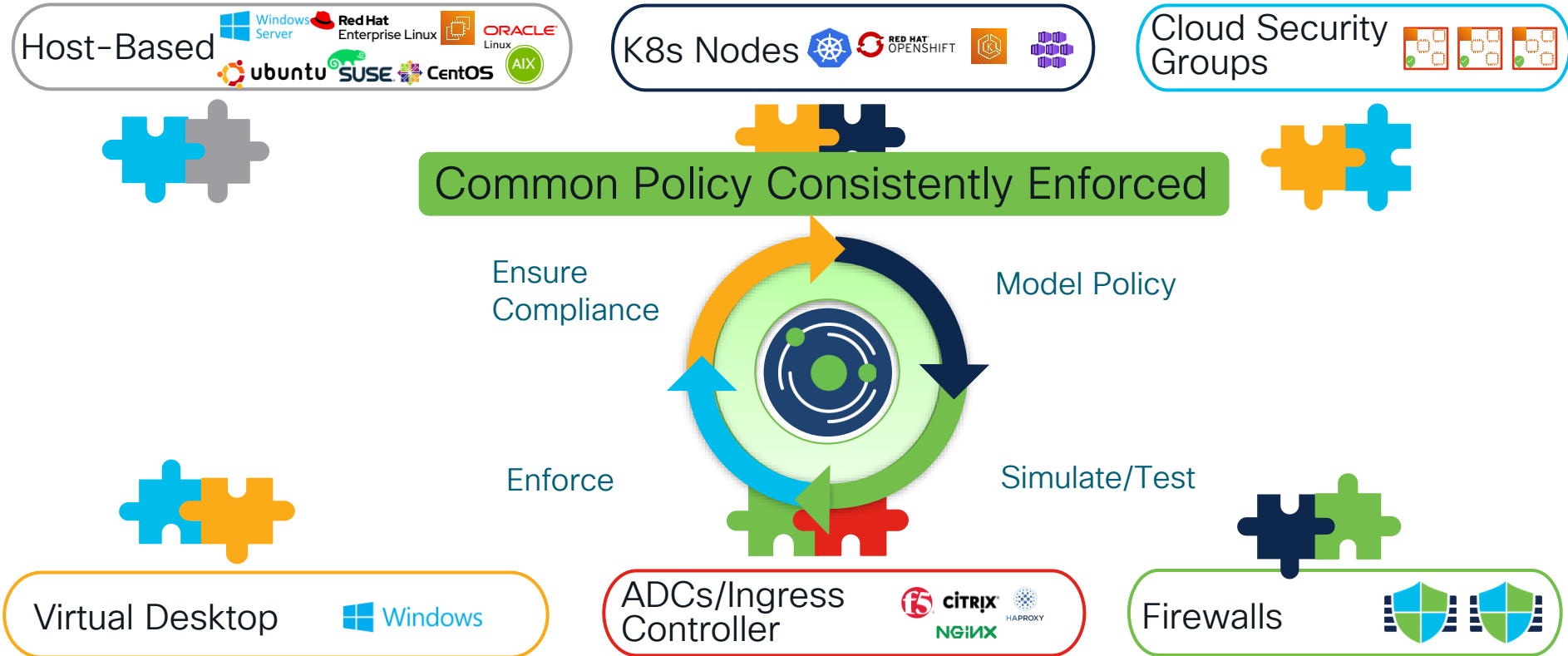
ADCs/Ingress Controller



Firewalls



Solving the puzzle with Secure Workload!



CISCO *Live!*

Solving the puzzle with Secure Workload!

Host-Based



K8s Nodes



Cloud Security Groups



Fitting the pieces together

SecOps

NetOps



AppSec
DevOps

Auditors

Virtual Desktop



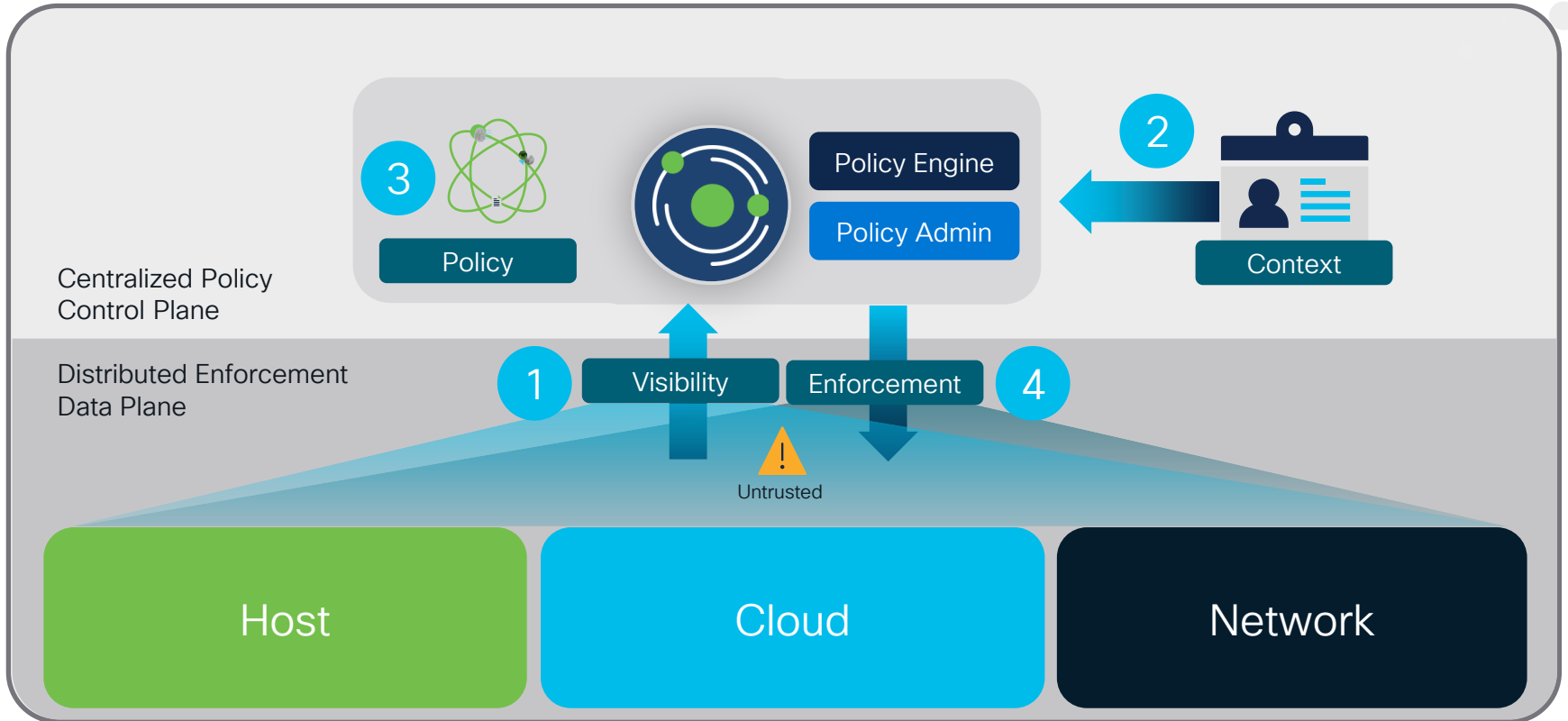
ADCs/Ingress
Controller



Firewalls



Cisco Secure Workload



Integration Overview



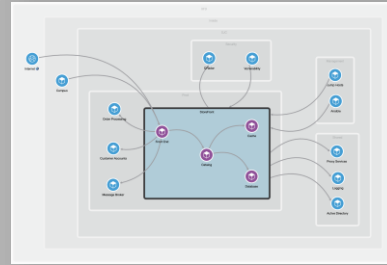
Feature evolution



Integration capabilities

Release 3.6

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



FMC

Access
Control Policy

Dynamic
Objects

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



Broad Visibility

East-West Security with
Secure Firewall and
Secure Workload



Coarse Control

Workload Security with
Secure Workload



Fine-Grained Control

← Closer to application →

Configuration Overview

Supported platforms



Secure Workload

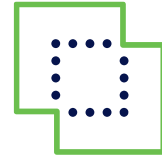


SaaS - Version 3.6

Requires Secure Connector



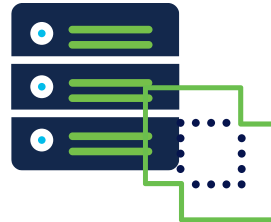
On-Prem - Version 3.6



Secure Firewall Management Center (FMC)

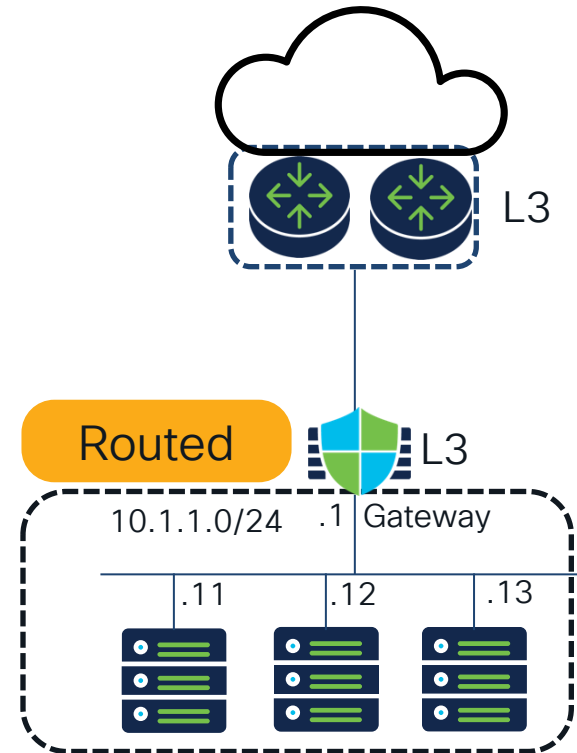
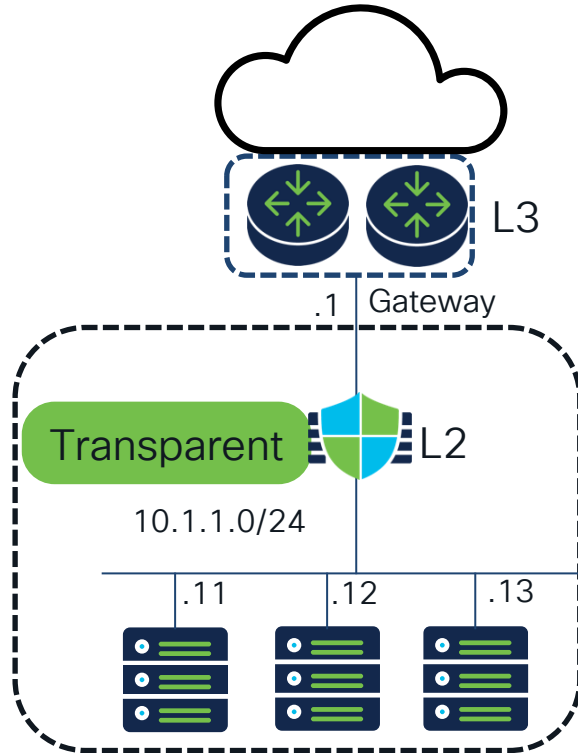


Virtual - Version 7.0.1+

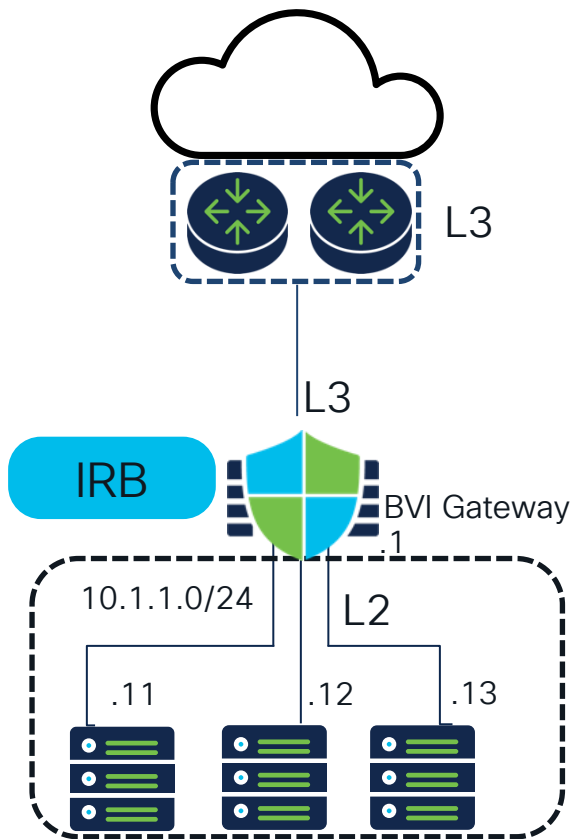


Physical - Version 7.0.1+

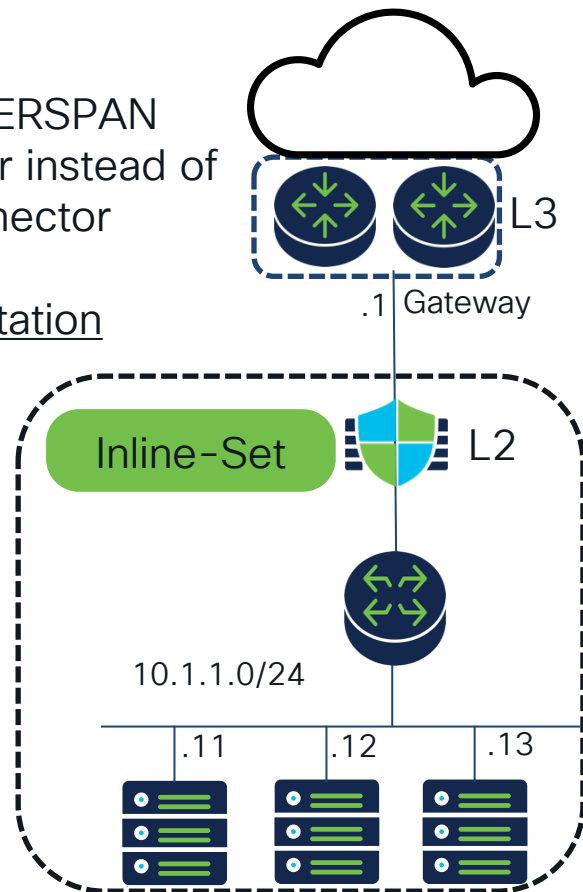
Supported Secure Firewall modes



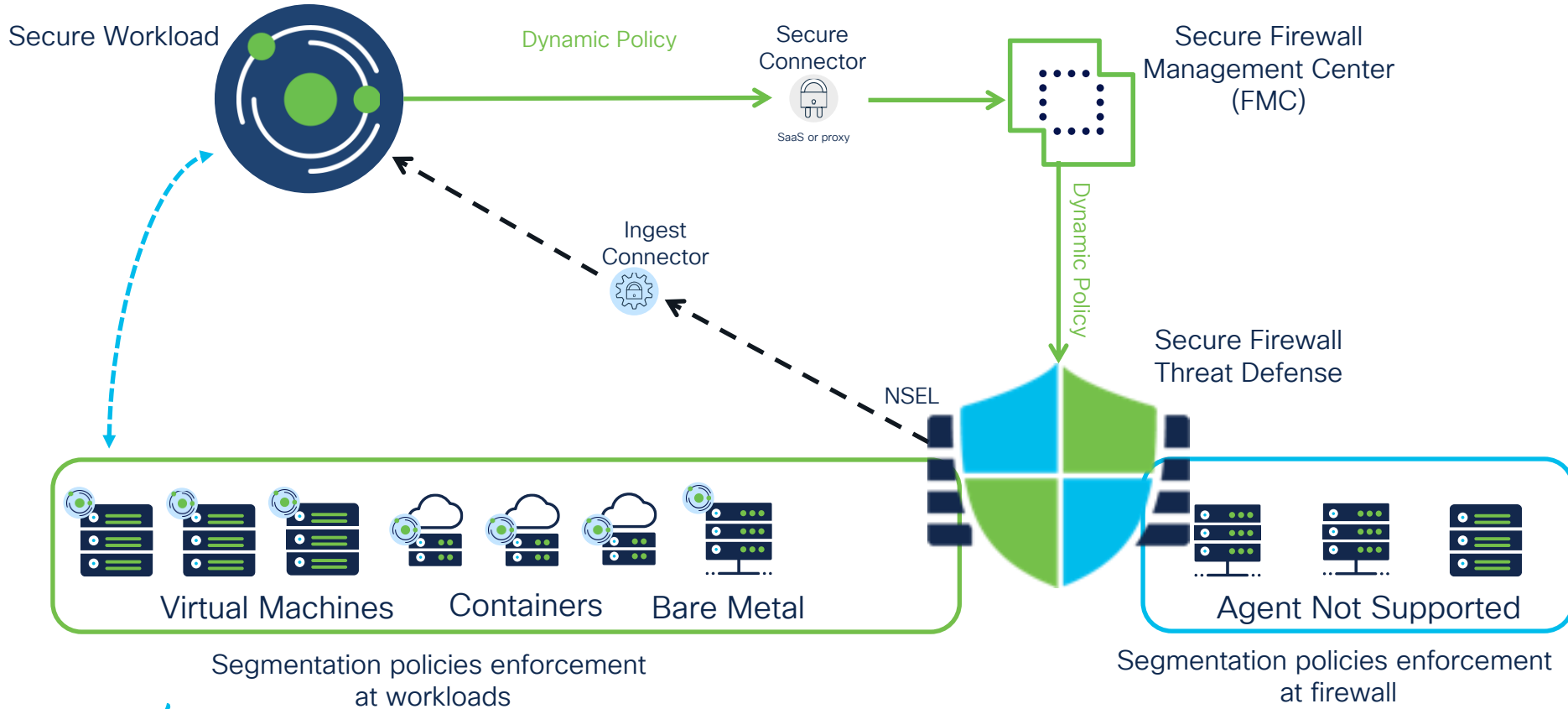
Additional Secure Firewall interface modes



Requires ERSPAN
Connector instead of
ASA Connector
Check
[Documentation](#)



Architecture overview



Configuration overview – steps

Configure Secure Firewall (Enforcement)

Deploy firewalls and assigned them to FMC Domain. Create Access Control Policy

Configure Visibility

Deploy ingest appliance and connector and configure NSEL on firewalls

Configure Enforcement

Configure Secure Workload FMC External Orchestrator and FMC REST API user

Secure Firewall (Enforcement)

Data Ingest Appliance (Visibility)

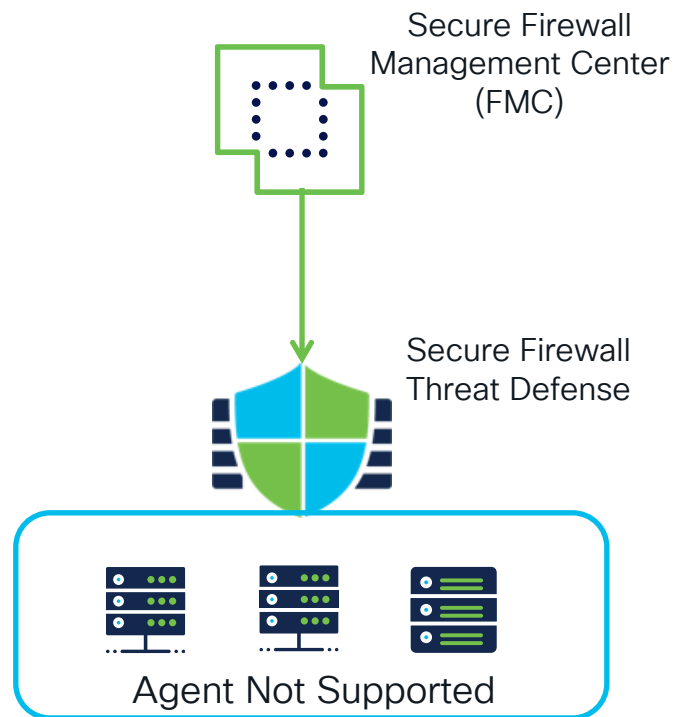


Secure Firewall NSEL (Visibility)

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.

Domain configuration is up to date. Save Cancel Add Domain

Name	Description	Devices	
Global			  
AWS	AWS Firewall	1 Device*	  
Azure	Azure Firewall	1 Device*	  
DC-North-south	DC Firewall Edge	1 Device*	  
Dc-East-West	DC Virtual Firewall	1 Device*	  

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.

User Configuration

User Name **api-workload**

Real Name

Authentication Use External Authentication Method

Password

Confirm Password

Maximum Number of Failed Logins (0 = Unlimited)

Minimum Password Length

Days Until Password Expiration (0 = Unlimited)





Days Before Password Expiration Warning

Force Password Reset on Login

Options Check Password Strength

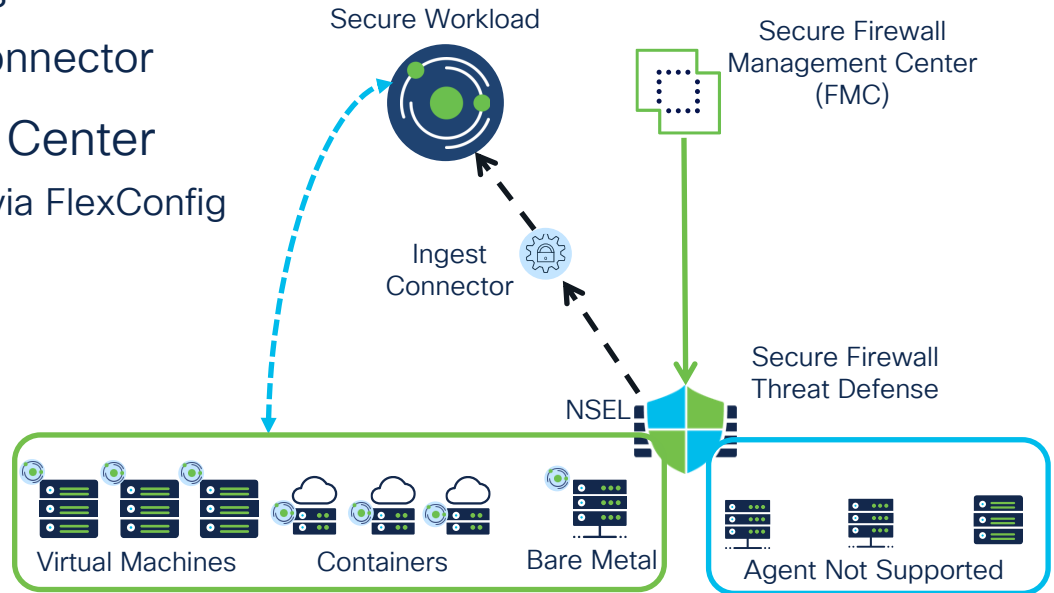
Exempt from Browser Session Timeout

User Role Configuration + Add Domain

Domain	Roles	
Global	Administrator	 
Global \ Dc-East-West	Administrator	 

Configuration overview – visibility

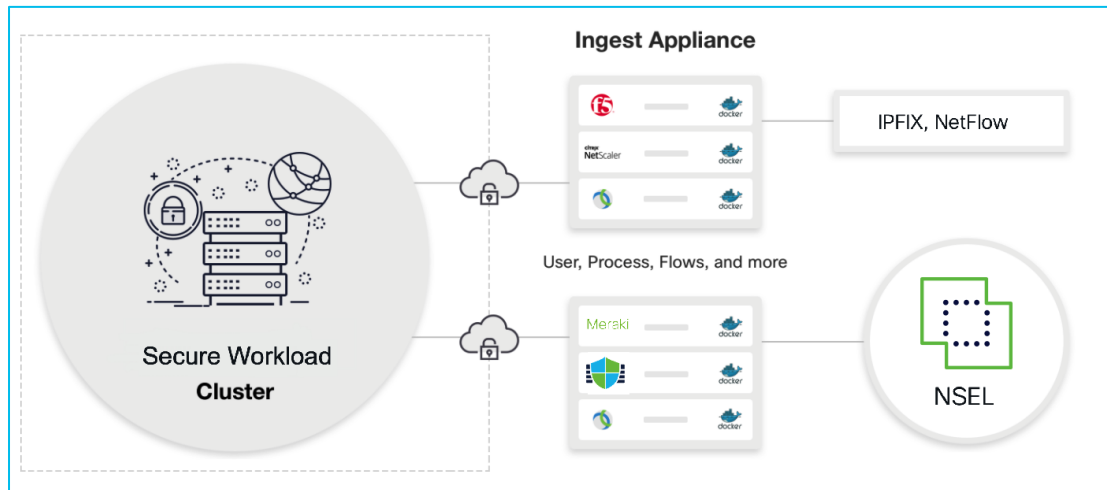
- Secure Workload
 - Deploy Secure Workload agents
 - Deploy Ingest Appliance and Connector
- Secure Firewall Management Center (FMC)
 - Configure NSEL on Secure Firewall via FlexConfig



Data Ingest Appliance and connector

Dedicated lightweight virtual appliance for telemetry ingestion

- OVA available in [cisco.com](https://www.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

The screenshot shows the Cisco Software Download page for Secure Workload G1. The page is titled "Software Download" and includes a breadcrumb trail: Downloads Home / Security / Workload Security / Secure Workload / Secure Workload G1 / Tetration OS- 3.6.1.5. On the left, there is a search bar and a list of releases, with 3.6.1.5 selected. The main content area displays "Secure Workload G1" and "Release 3.6.1.5". Below this, there is a table with columns for "File Information", "Release Date", and "Size". The table contains one entry: "Virtual machine OVA file for running Cisco Secure Workload data ingest sensors such as Cisco Anyconnect, Netflow, F5, Citrix, etc., tetration-data-ingest-3.6.1.5.ova" with a release date of "28-Oct-2021" and a size of "1360.31 MB". A red box highlights the file name, and a red arrow points from a text box on the right to this file name. The page also includes links for "My Notifications", "Related Links and Documentation", "Release Notes for 3.6.1.5", and "Upgrade Guide". The footer of the page includes the URL "hathor-lab.com".

Software Download

Downloads Home / Security / Workload Security / Secure Workload / Secure Workload G1 / Tetration OS- 3.6.1.5

Search...

Expand All Collapse All

Latest Release

3.6.1.21

All Release

3

3.6.1.5

Secure Workload G1

Release 3.6.1.5

My Notifications

Related Links and Documentation

Release Notes for 3.6.1.5

Upgrade Guide

File Information	Release Date	Size
Virtual machine OVA file for running Cisco Secure Workload data ingest sensors such as Cisco Anyconnect, Netflow, F5, Citrix, etc., tetration-data-ingest-3.6.1.5.ova Advisories	28-Oct-2021	1360.31 MB

hathor-lab.com

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

Download OVA 2 VM Configuration 3 Download Configuration Bundle 4 Deploy Virtual Appliance

IP Address (CIDR format) 10.62.159.70/28 x
10.62.159.71/28 x
10.62.159.72/28 +

Gateway IP address 10.62.159.65 x
10.62.159.65 x
10.62.159.65 +

Hostname (optional) tet-ingest.hathor-lab.com

Name Server 10.62.159.50 x
+

Search Domain (optional) hathor-lab.com +

Use proxy server to connect to Tetraton (optional)

HTTP Proxy (optional) http://www.cisco.com:8080

No Proxy (optional) acme.org +

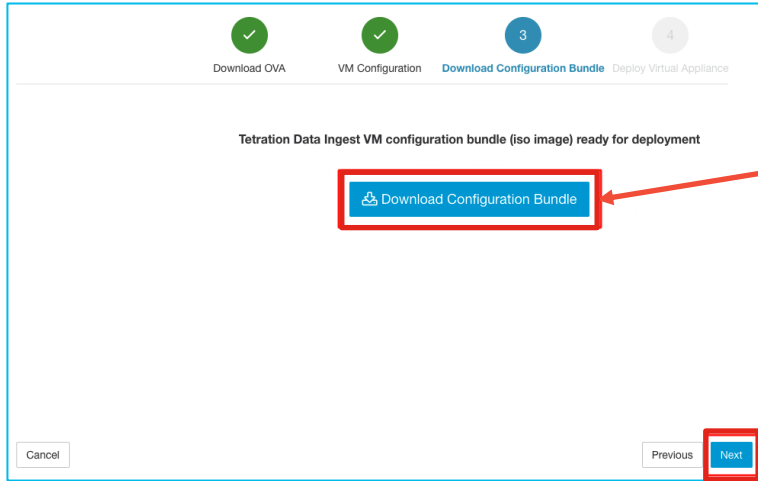
Docker Bridge (CIDR format) (optional) 172.17.0.1/16

Cancel Previous Next

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

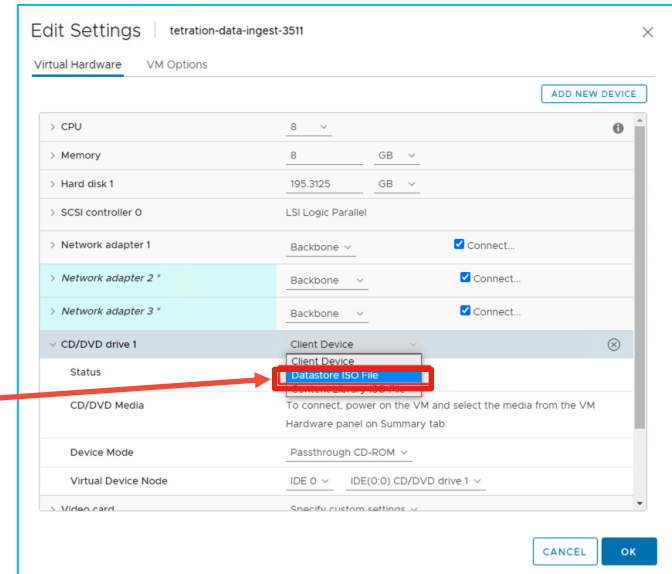
Data Ingest Appliance – config bundle



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

Virtual Appliance

Data Ingest Appliance **ACTIVE** [Commission](#)

Checked In	Registered	Created
Mar 16 2022 08:21:44 pm (CET)	Jan 12 2022 08:29:42 pm (CET)	Jan 12 2022 07:23:59 pm (CET)

Connectors

[Enable Another Connector](#)

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

2. Select ASA Connector

Select a Connector

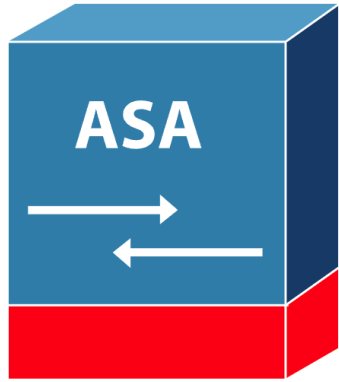
You may choose one of the supported connector for this virtual appliance

Select a connector

- NetFlow
- NetScaler
- F5
- AnyConnect
- ASA**
- Meraki Meraki

Data Ingest Appliance – verify connector

Connector



ASA 

1. Verify that Icon is healthy

Info IP bindings Log Alert Troubleshoot

Listening for

NETFLOW9 on 10.62.159.70 : 4729 / udp

ASA connector NSEL events handling

Flow Event Element ID: 233 Element Name: <i>NF_F_FW_EVENT</i>	Extended Flow Event Element ID: 33002 Element Name: <i>NF_F_FW_EXT_EVENT</i>	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	<i>NF_F_PROTOCOL</i>
Source Address	8	<i>NF_F_SRC_ADDR_IPV4</i>
	27	<i>NF_F_SRC_ADDR_IPV6</i>
Source Port	7	<i>NF_F_SRC_PORT</i>
Destination Address	12	<i>NF_F_DST_ADDR_IPV4</i>
	28	<i>NF_F_DST_ADDR_IPV6</i>
Destination Port	11	<i>NF_F_DST_PORT</i>
Flow Start Time	152	<i>NF_F_FLOW_CREATE_TIME_MSEC</i>
Byte Count	231	<i>NF_F_FWD_FLOW_DELTA_BYTES</i>
Packet Count	298	<i>NF_F_FWD_FLOW_DELTA_PACKETS</i>

Reverse Flow Information

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

ASA connector NSEL NAT-flows

Forward Direction

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

Reverse Direction

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

FMC Netflow extended access list

Firepower Management Center
Objects / Object Management Overview Analysis Policies Devices Objects AMP Intelligence Deploy

AAA Server
Access List
Extended

Object Management
Intrusion Rules

Add Extended Access List

Filter

Extended
An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard identifies traffic based on destination address only. Intrusion Rules identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

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

Edit Extended Access List Object

Name
flow_csw

Entries (1)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application
1	Allow	Any	Any	Any	Any	Any

Allow Overrides

Cancel Save

FMC FlexConfig text objects

Firepower Management Center
Objects / Object Management Overview Analysis Policies Devices Objects AMP Intelligence Deploy

FlexConfig
FlexConfig Object
Text Object

Add Text Object

Text Object

Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

1. Navigate to Objects > FlexConfig 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)

Edit Text Object

Name: csw_event_type

Description:

Variable Type: Single Count: 1

Variable	Count
1 all	1

Allow Overrides

Cancel Save

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

Edit Text Object

Name: csw_nsel_dest

Description:

Variable Type: Multiple Count: 3

Variable	Count
1 App-Out	1
2 10.62.159.70	1
3 4729	1

Allow Overrides

Cancel Save

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

Edit Text Object

Name: netflow_Parameter

Description: This variable provides the global settings for NetFlow export.

Variable Type: Multiple Count: 3

Variable	Count
1 1	1
2 0	1
3 30	1

Allow Overrides

Override (0)

Cancel Save

FMC FlexConfig flow destination

Firepower Management Center
Objects / Object Management Overview Analysis Policies Devices Objects AMP Intelligence Deploy

FlexConfig Object

FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig policies.

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

Add FlexConfig Object

Name: csw_nsel_flow_dest

Description: flow export to CSW connector

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI.

Insert Policy Object > Text Object

Insert System Variable > Network

Insert Secret Key

Security Zones

Standard ACL Object

Extended ACL Object

Route Map

Variables

Name	Dimension	Default Value	Property (Type:Name)
No records to display			

Insert Text Object Variable

Variable Name: nsel

Description:

Available Objects

Search

Selected Object: csw_nsel_dest

Available Objects List:

- csw_event_type
- csw_nsel_dest**
- defaultDNSNameServerList
- defaultDNSParameters
- disableInspectProtocolList
- dnsNameServerList

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

FMC FlexConfig flow destination

Add FlexConfig Object

Name:

Description:

▲ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert

▼ Variables

Name	Dimension	Default Value	Property (Type:N...	Override	Description
nsel	MULTIPLE	App-Out,10.62.159.70,4729	FREE...	false	

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

Add FlexConfig Object

Name:

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert

- Insert Policy Object
- Insert System Variable
- Insert Secret Key
- Text Object
- Network
- Security Zones
- Standard ACL Object
- Extended ACL Object
- Route Map

Variables

Name	Dimension	Default Value	Property (Type:Name)	Overr...	Description
No records to display					

1. A class-map needs to be created to be applied to a policy-map. For this we need to add **3 objects**: 1 **Extended ACL Object** (flow_csw created before) and 2 **text objects** (csw_event_type and csw_nsel_dest)

Insert Extended Access List Object Variable

Variable Name:

Description:

Available Objects

- flow_csw

Selected Object:

Insert Text Object Variable

Variable Name:

Description:

Available Objects

- csw_event_type
- csw_nsel_dest
- defaultDNSNameServerList
- rNameServerList

Selected Object:

Insert Text Object Variable

Variable Name:

Description:

Available Objects

- csw_event_type
- csw_nsel_dest
- defaultDNSNameServerList
- rNameServerList

Selected Object:

FMC FlexConfig class map

Edit FlexConfig Object

Name:

Description:

▲ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert | | Deployment: | Type:

```
class-map flow_csw
match access-list $flow_csw

policy-map global_policy
class flow_csw
flow-export event-type $event destination $nsel.get(1)
```

▼ Variables

Name	Dimension	Default Value	Property (Type:Name)	Overr...	Description
flow_csw	SINGLE	flow_csw	EXD_ACL:flow_csw	false	
event	SINGLE	all	FREEFORM:csw_event_type	false	
nsel	MULTIPLE	[App-Out, 10.62.159.70, 4729]	FREEFORM:csw_nsel_dest	false	

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

FlexConfig Object

Add FlexConfig Object

FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig policies.

Name	Description	
Netflow_Set_Parameters	Set global parameters for NetFlow export.	 


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

Edit FlexConfig Object

Name:

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before

Insert  Deployment: Type:

```
flow-export active refresh-interval $netflow_Parameters.get(0)
flow-export delay flow-create $netflow_Parameters.get(1)
flow-export template timeout-rate $netflow_Parameters.get(2)
```

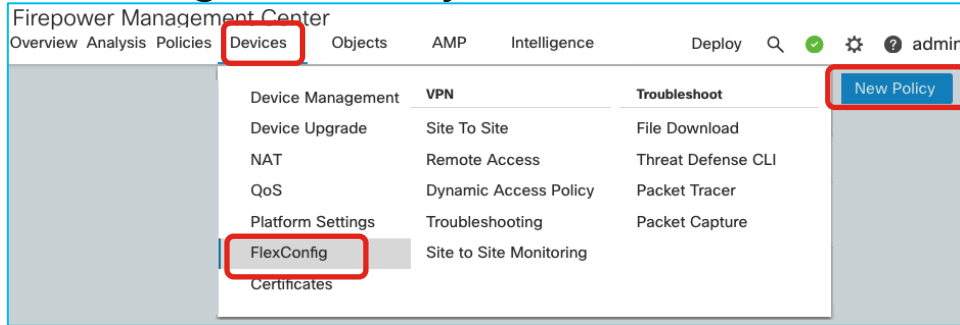
Variables

Name	Dimension	Default Value	Property (Type:Name)	Override	Description
netflow_Parameters	MULTIPLE	[1, 0, 30]	FREEFO...	false	

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**

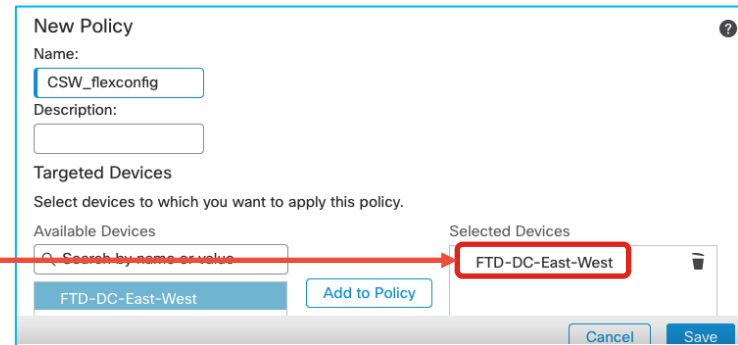
FMC NetFlow export

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

The screenshot shows the configuration page for 'CSW_flexconfig'. Under the 'User Defined' section, three FlexConfig objects are listed and selected with checkboxes: 'csw_nsel_class_map', 'csw_nsel_flow_dest', and 'csw_nsel_parameter'. On the right, the 'Selected Append FlexConfigs' table lists these three objects with their respective descriptions and actions (search and delete icons).

#	Name	Description
1	csw_nsel_class_map	netflow class map for CSW connector
2	csw_nsel_flow_dest	flow export to CSW connector
3	csw_nsel_parameter	Default netflow parameters

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!

Segmentation

Enforced Applications 0 Enforcement Agents 22 Desired Agent Policies 0 / 22

Workspaces Draft Policies Analyzed Policies Enforced Policies Policy Requests 15

12 Workspaces Filter all application workspaces Sort + Create New Workspace

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

Create a New Application Workspace

Name
Invoice-App-Firewall

Description
Enter a description (optional)

Scope
Invoice-App

Cancel Create

ADM workspace (visibility)

Invoice-App-Firewall PRIMARY

... : DC : DC-1 : Applications : Prod : Invoice-App Version: v0

Activity Log Matching Inventories 8 Conversations Filters 4 Policies 1 Provided Services Enforcement Status Policy Analysis

Quick Analysis Filter Policies ...

Absolute policies 0 Default policies 0 Catch All DENY

No Policies defined ?

Network security policies are the building block for many powerful features of Cisco Tetra. A policy represents a relationship between a set of consumer and provider workloads. Allow list, block list, and mixed security models are supported.

The user guide has more details on network security policies.

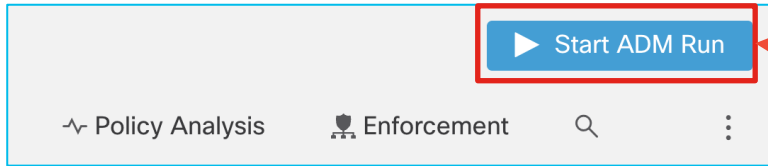
Automatically Discover Policies

or

+ Add a Manual Policy

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-created. 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

Invoice-App-Firewall PRIMARY Switch Application

... : DC : DC-1 : Applications : Prod : Invoice-App Version: v0

Activity Log Matching Inventories 8 Conversations Filters 4 Policies 1 Provided Services Enforcement Status Policy Analysis Enforcement

ADM Run Configuration

Submit ADM Run

ADM discovers security groups and policies for the members of this application using the observations in the selected time range.

Select time range 18,061,527 total observations
 Apr 25 11:00pm - Apr 26 8:00am Showing Flow Observations

Scope: ... : DC : DC-1 : Applications : Prod : Invoice-App **Time Range:** Apr 25 11:00pm - Apr 26 8:00am

Member Workloads: 8 Show

> External Dependencies

> Advanced Configurations

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)

Priority	Action	Consumer	Provider	Protocols And Ports
100	ALLOW	Default : EMEAR : Campus	siwapp-front-end-hapro...	TCP : 1936
100	ALLOW	siwapp-app-tier	siwapp-front-end-hapro...	TCP : 3306 (MySQL)
100	ALLOW	siwapp-db-tier	siwapp-front-end-hapro...	TCP : 32768-60800
100	ALLOW	Sales-Users-VPN	siwapp-front-end-hapro...	TCP : 1936
100	ALLOW	Default : EMEAR : DMZ : I...	siwapp-front-end-hapro...	TCP : 3306 (MySQL)
100	ALLOW	Default : EMEAR : Campus	siwapp-front-end-hapro...	TCP : 80 (HTTP) ...1 more
100	ALLOW	Sales-Users-VPN	siwapp-front-end-hapro...	TCP : 80 (HTTP) ...1 more
100	ALLOW	Default : EMEAR : Campus	siwapp-db-tier	TCP : 3306 (MySQL)

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

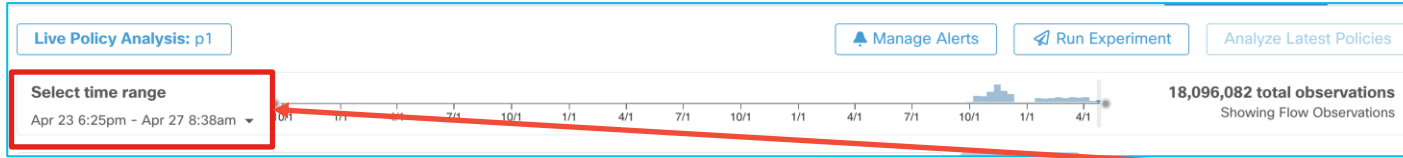
ADM workspace (visibility)

The screenshot displays the ADM workspace interface. At the top left, a status bar indicates "Live Policy Analysis: disabled". To the right, there are two buttons: "Manage Alerts" and "Start Policy Analysis". A red box highlights the "Start Policy Analysis" button, with a red arrow pointing to it from a callout box on the right. Below the status bar, a light blue banner states: "Policy Analysis is disabled for this application. Traffic in, out and within this application's scope is being labeled with policy information from other applications that will impact this application's traffic." In the center, there is a chart showing flow observations over time, with a peak around 10/1. To the right of the chart, it says "18,095,900 total observations" and "Showing Flow Observations". On the left side, a modal window titled "Analyze Latest Policies" is open. It contains a form with the following fields: "Reason for action" (filled with "firewall rules verification"), "Describe the new version:" section with "Name" (filled with "jorguin") and "Description" (filled with "agentless enforcement"). At the bottom of the modal, there are "Cancel" and "Analyze" buttons. A red box highlights the "Analyze" button, with a red arrow pointing to it from a callout box on the right.

1. Enable Policy Analysis

2. Configure the parameters and select Analyze

ADM workspace (visibility)



1. Select a time range to perform the analysis.



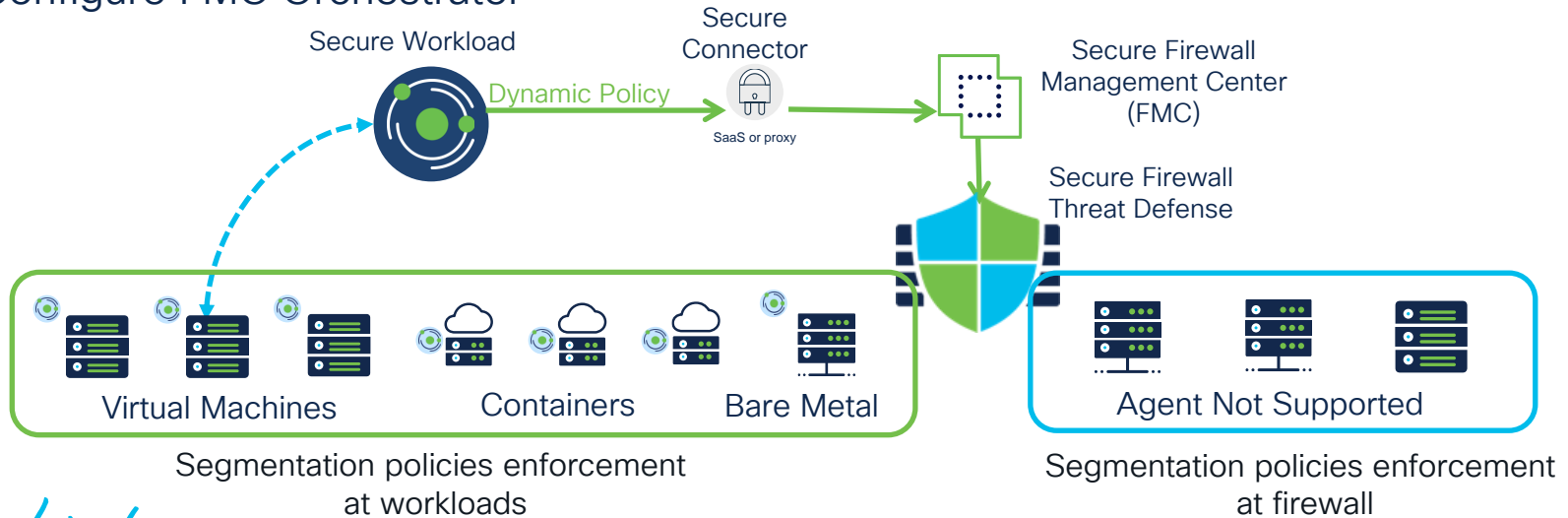
2. Filtering of flows can be done by specifying particular flows or by policy category (Permitted, Rejected, Escaped) and verify the result

Found 34 Flow Observations Show 20

Timestamp	Policy Categories	Consumer Name	Provider Name	Consumer Address	Provider Address	Consumer Port	Provider Port
Apr 26 11:05:00am	PERMITTED	Unknown	Unknown	172.16.16.2	172.16.16.9	3306	33324
Apr 26 11:15:00am	PERMITTED	Unknown	Unknown	172.16.16.2	172.16.16.9	3306	37074

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.

User Configuration

User Name **api-workload**

Real Name

Authentication Use External Authentication Method

Password

Confirm Password

Maximum Number of Failed Logins (0 = Unlimited)

Minimum Password Length

Days Until Password Expiration (0 = Unlimited)





Days Before Password Expiration Warning

Force Password Reset on Login

Options Check Password Strength

Exempt from Browser Session Timeout

User Role Configuration + Add Domain

Domain	Roles	
Global	Administrator	 
Global \ Dc-East-West	Administrator	 

Secure Workload external orchestrator

Edit External Orchestrator Configuration

Basic Config

Hosts List

Domains

Type
FMC BETA

Name
FMC-CL

Description
Description of the i

Full Snapshot Interval (s)
3600

Username
api_csw

Password
Password for the o

Accept Self-signed Cert
 Verbose tsdb Metrics
 Secure Connector Tunnel

Enforcement Mode
Merge

Connection will be tested after the update. [Cancel](#) [Update](#)

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"

Edit External Orchestrator Configuration

Basic Config

Hosts List

Domains

Hosts List +

10.62.159.83	443	×
10.62.159.82	443	×

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

The screenshot displays the 'Edit External Orchestrator Configuration' page. On the left, there is a sidebar with three menu items: 'Basic Config', 'Hosts List', and 'Domains'. The 'Domains' item is highlighted with a red box. The main content area is titled 'Domain(s)' and features a search input field containing 'Global/DC-East-West'. Below the search field is a dropdown menu with four options: 'Global' (highlighted in blue), 'Global/AWS', 'Global/Azure', and 'Global/DC-North-South'. To the right of the dropdown are two buttons: 'Select All' and 'Remove All'. A red box highlights the dropdown menu, and a red arrow points from the 'Domains' menu item to this dropdown. Another red arrow points from the 'Select All' button to the second instruction box.

Secure Workload external orchestrator

FMC-CL FMC May 30 01:43:44 pm (CEST) **Success**

Configuration Details

Id	6294adf0497d4f6faa60df6b
Type	FMC
Name	FMC-CL
Full Snapshot Interval (s)	3600
Username	api_csw
Accept Self-signed Cert	true
Enforcement Mode	merge
Hosts List	<pre>{"host_name": "10.62.159.83", "port_number": 443} {"host_name": "10.62.159.82", "port_number": 443}</pre>
Progress Status	2022-06-02T17:40:12Z completed: 2 managed devices

BRKSEC-2123

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)

Invoice-App-Firewall PRIMARY

Switch Application

Start ADM Run

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

Enforcement

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

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

2. Select “Enforce Policies”

ADM workspace (enforcement)

Update Enforced Policies

1 Review Policy Updates — 2 Impacted Workloads — 3 Impacting Policies — 4 Review & Enforce

Related to: ... : DC : DC-1 : Applications : Prod : Invoice-App

Select the version of policies to enforce.

Version: select a version

p1 jorgquin
Last action: 8:37 AM

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

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

2. Verify the policies to be pushed to the firewall

ADM workspace (enforcement)

Update Enforced Policies

Review Policy Updates — 2 Impacted Workloads — 3 Impacting Policies — 4 Review & Enforce

No workloads will be impacted based on 16 policy updates

Enter attributes... Filter

Showing 0 inventory

Hostname ↑	Address ↓↓	OS ↓↓
No Inventory		

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

ADM workspace (enforcement)

Update Enforced Policies

Review Policy Updates — Impacted Workloads — 3 Impacting Policies — 4 Review & Enforce

Policies from the ancestor applications may have an impact on the workloads in the current application
Please make sure the desired allow policies from ancestor applications are enforced

Scope	Application Workspace (Primary)	Analysis	Enforcement
Default	None		
Default : EMEAR	None		
Default : EMEAR : DC	InfoSec	Version: p7 Policies: Catch-all Action: <input type="radio"/> ALLOW	Disabled
Default : EMEAR : DC : DC-1	None		
Default : EMEAR : DC : DC-1 : Applications	None		
Default : EMEAR : DC : DC-1 : Applications : Prod	None		
... : DC : DC-1 : Applications : Prod : Invoice-App	Invoice-App-Firewall	Version: p1 Policies: 16 Catch-all Action: <input type="radio"/> DENY	Disabled

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)

Update Enforced Policies

Review Policy Updates — Impacted Workloads — Impacting Policies — 4 Review & Enforce

You are about to enforce the following policy changes
New firewall rules may be inserted and any existing rules will be deleted on any of the impacted workloads
The exact list of impacted workloads may change at any time due to dynamic nature of policy intents

Policy Updates	16
Potentially Impacted Workloads	0
Catch-all Action	<input checked="" type="radio"/> DENY

Reason for Enforcement Action (optional)
Cisco Live Demo

Cancel Previous Accept and Enforce

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)

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**

Enforced Policy Version: [p1 - jorgquin] Manage Alerts Stop Policy Enforcement Enforce Policies

Select time range Apr 27 9:34am - Apr 27 11:36am 18,103

Consumer Address = 172.16.16.2 and Provider Address = 172.16.16.9 Filter Flows

Filtered Flow Observations Permitted Rejected Escaped

Top Names contributing to the selected Flow Observations:

Consumer Names	Provider Names
Unknown	Unknown
hathor-win20...	hathor-win20...

Found 3 Flow Observations Show 20

Timestamp	Policy Categories	Outbound Policy Rank	Inbound Policy Rank	Consumer Address	Provider Address	Consumer Port	Provider Port
Apr 27 9:48:00am	PERMITTED	Unknown	Unknown	172.16.16.2	172.16.16.9	3306	6006
Apr 27 10:23:00am	PERMITTED	Default	Default	172.16.16.2	172.16.16.9	3306	
Apr 27 10:40:00am	PERMITTED	Default	Default	172.16.16.2	172.16.16.9	3306	

Found 26 Flow Observations Show 20

Timestamp	Policy Categories	Outbound Policy Rank	Inbound Policy Rank	Consumer Address	Provider Address	Consumer Port	Provider Port
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

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

FMC dynamic objects

Dynamic Objects

Add Dynamic Object

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_615acaf755f026e6f621609	AD-DNS-Internal	1	  
WorkloadObj_615c8055755f020e377c5201	Default:EMEAR: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

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action						
East-West Policy																				
																		Analyze Hit Counts	Save	Cancel
Mandatory - East-West Policy (-)																				
There are no rules in this section. Add Rule or Add Category																				
Default - East-West Policy (1-23)																				
1	Workload_gold	Any	Any	Any	Any	Any	Any	Any	TCP (6):5640	Any	Any	WorkloadObj_	Any	Allow						
2	Workload_gold	Any	Any	Any	Any	Any	Any	Any	Any	TCP (6):5640	Any	Any	WorkloadObj_	Allow						
3	Workload_gold	Any	Any	Any	Any	Any	Any	Any	TCP (6):5660	Any	Any	WorkloadObj_	Any	Allow						
4	Workload_gold	Any	Any	Any	Any	Any	Any	Any	TCP (6):5660	Any	Any	WorkloadObj_	Any	Allow						
5	Workload_gold	Any	Any	Any	Any	Any	Any	Any	TCP (6):443	Any	Any	WorkloadObj_	Any	Allow						
6	Workload_gold	Any	Any	Any	Any	Any	Any	Any	TCP (6):443	Any	Any	WorkloadObj_	Any	Allow						
7	Workload_7	Any	Any	Any	Any	Any	Any	Any	TCP (6):3306	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
8	Workload_8	Any	Any	Any	Any	Any	Any	Any	TCP (6):1936	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
9	Workload_9	Any	Any	Any	Any	Any	Any	Any	UDP (17):53	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
10	Workload_10	Any	Any	Any	Any	Any	Any	Any	TCP (6):32766	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
11	Workload_11	Any	Any	Any	Any	Any	Any	Any	TCP (6):1936	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
12	Workload_12	Any	Any	Any	Any	Any	Any	Any	TCP (6):3306	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
13	Workload_13	Any	Any	Any	Any	Any	Any	Any	TCP (6):3306	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
14	Workload_14	Any	Any	Any	Any	Any	Any	Any	UDP (17):53	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
15	Workload_15	Any	Any	Any	Any	Any	Any	Any	UDP (17):53	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
16	Workload_16	Any	Any	Any	Any	Any	Any	Any	TCP (6):80	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
17	Workload_17	Any	Any	Any	Any	Any	Any	Any	TCP (6):8081	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
18	Workload_18	Any	Any	Any	Any	Any	Any	Any	TCP (6):4567	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
19	Workload_19	Any	Any	Any	Any	Any	Any	Any	TCP (6):3306	Any	Any	WorkloadObj_	WorkloadObj_	Allow						
20	Workload_ca_1	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	WorkloadObj_	Any	Block						
21	Workload_ca_2	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	WorkloadObj_	Any	Block						
22	Transparent-In	inside-transp	inside-transp	outside-transp	outside-transp	Any	Any	Any	Any	Any	Any	Any	Any	Allow						
23	Upstream Rule	inline-set-in	inline-set-out	inline-set-out	inline-set-in	Any	Any	Any	Any	Any	Any	Any	Any	Allow						

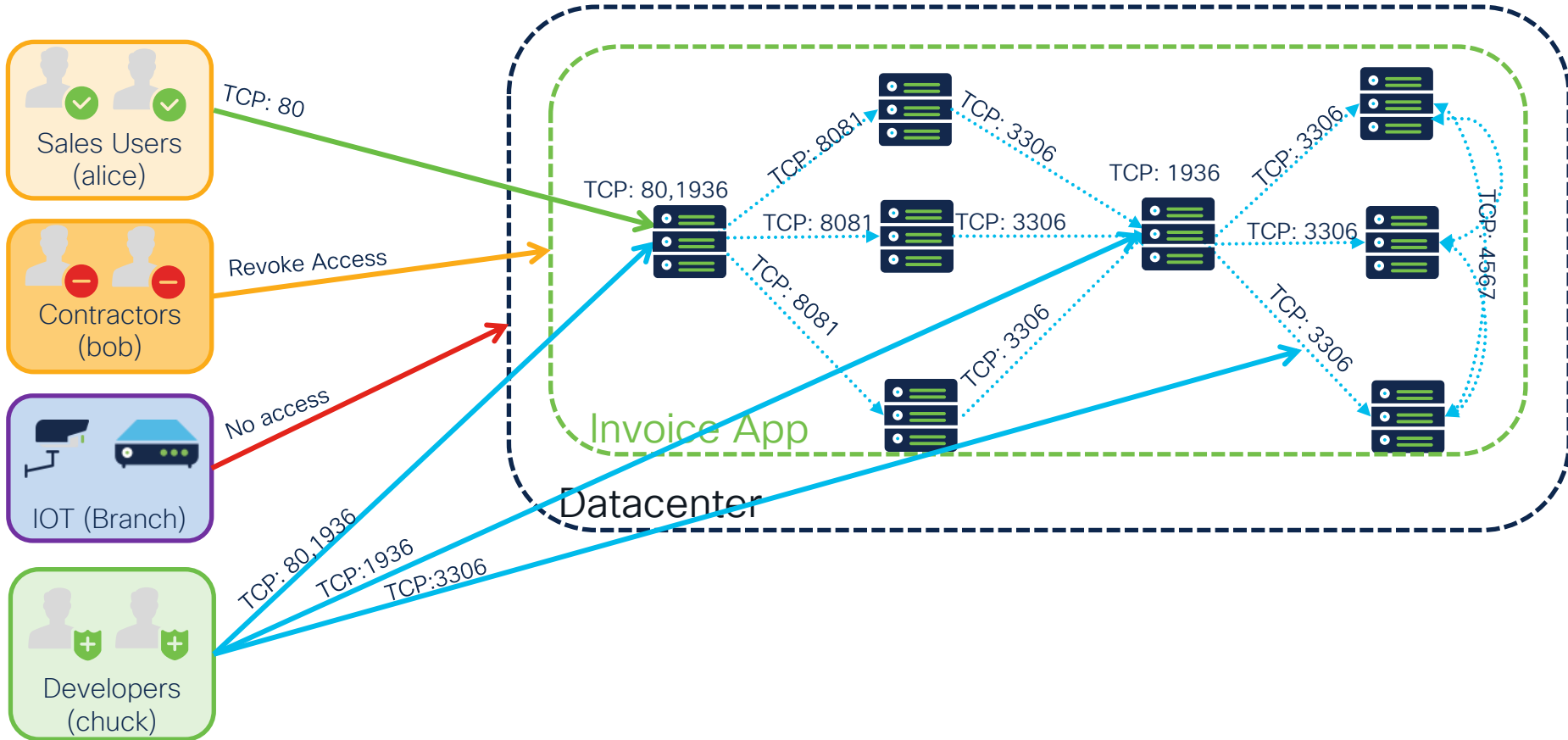
1. Dynamic intent-based policies pushed by Secure Workload!

2. With the “merge” options, Secure Workload honors existing ACLs

Demo

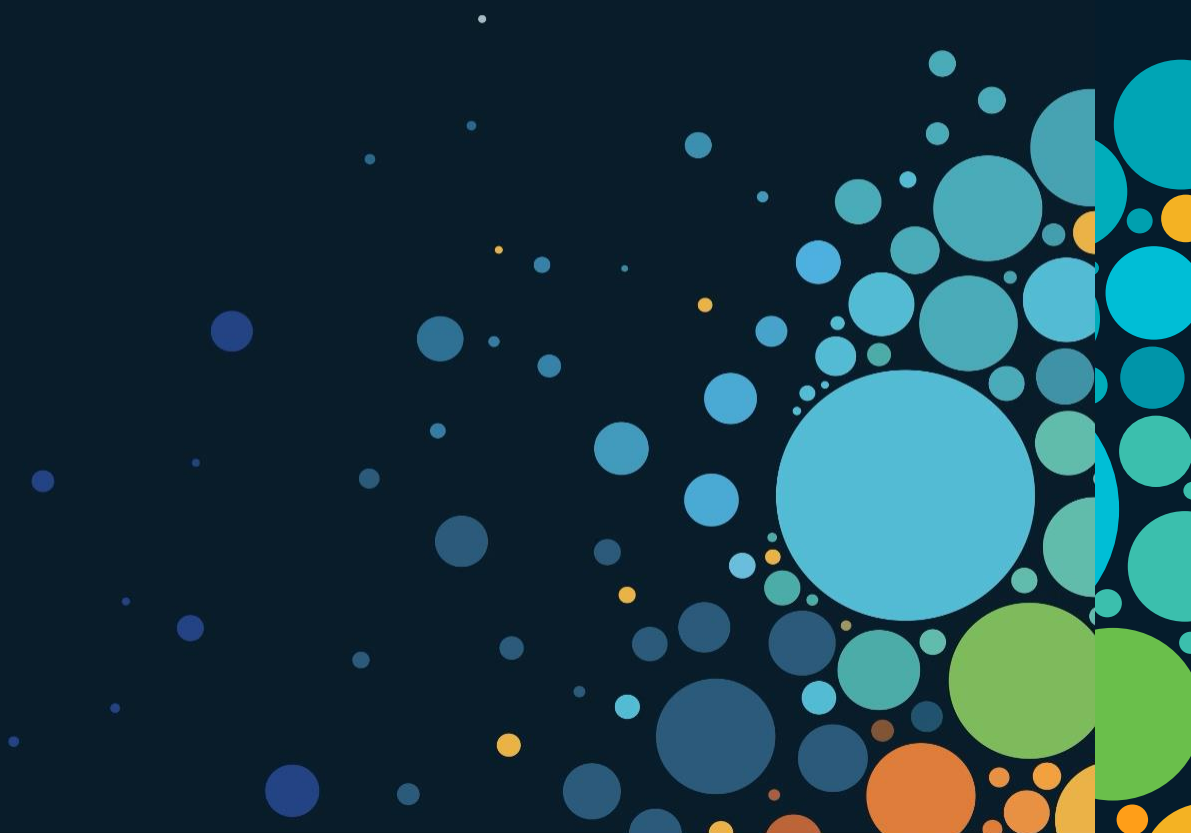


Zero Trust segmentation for Invoice App

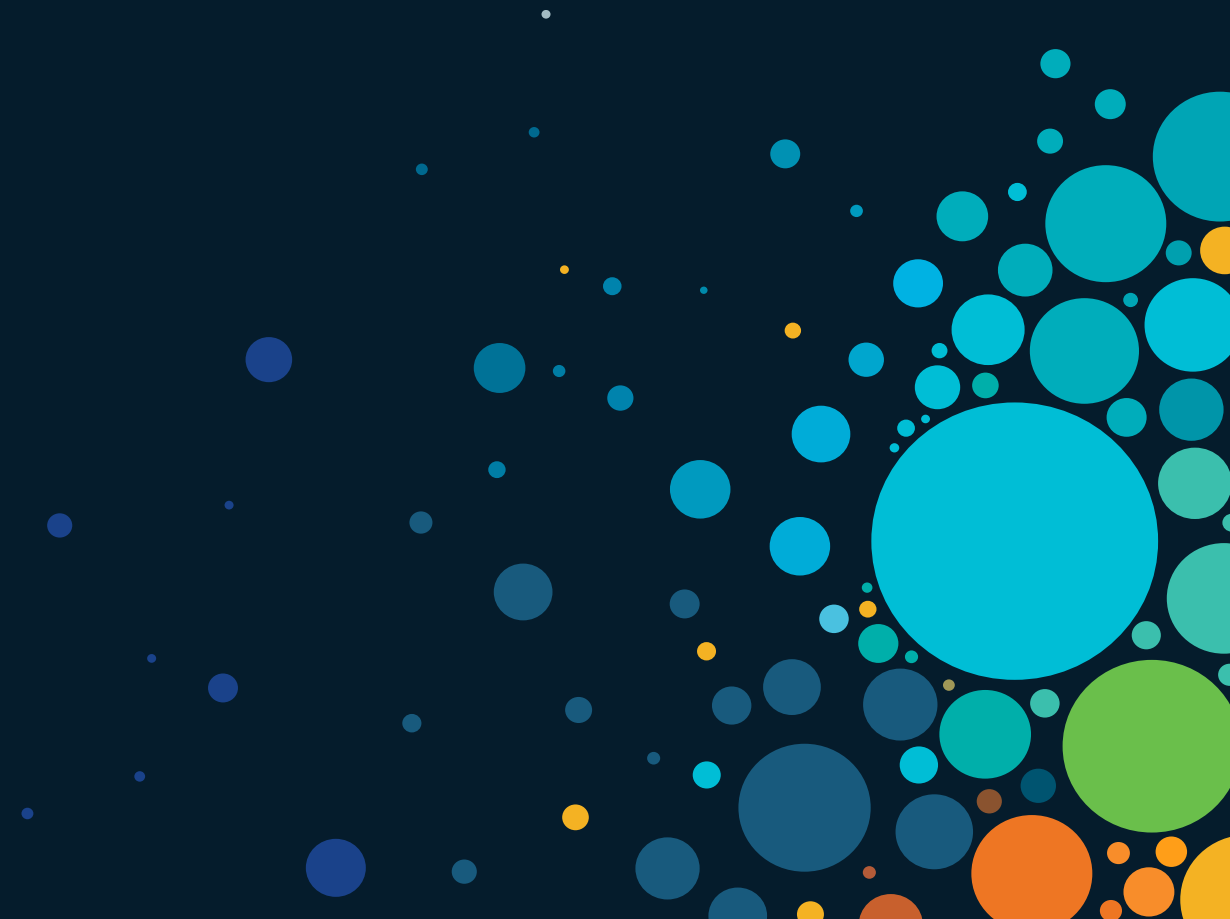


Demo

CISCO *Live!*



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.



Security Operations

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

SECURE X (XDR)

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

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) Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE) **ZERO TRUST** **PRIVATE CLOUD EDGE (MSP or CUSTOMER)**
Threat Protection | Secure Access Control | Managed Remote Access Reliable | Scalable | Flexible

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 **ZERO TRUST**
Scalable | Flexible | Visibility | Comprehensive Security Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

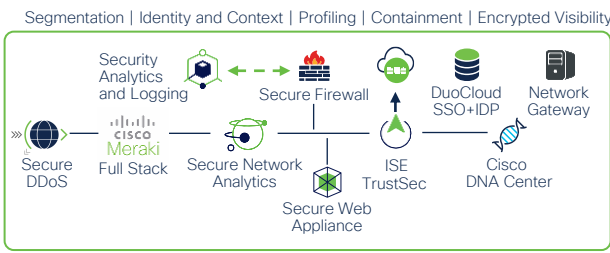
Network Edge

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



Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

Cloud Native Security 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

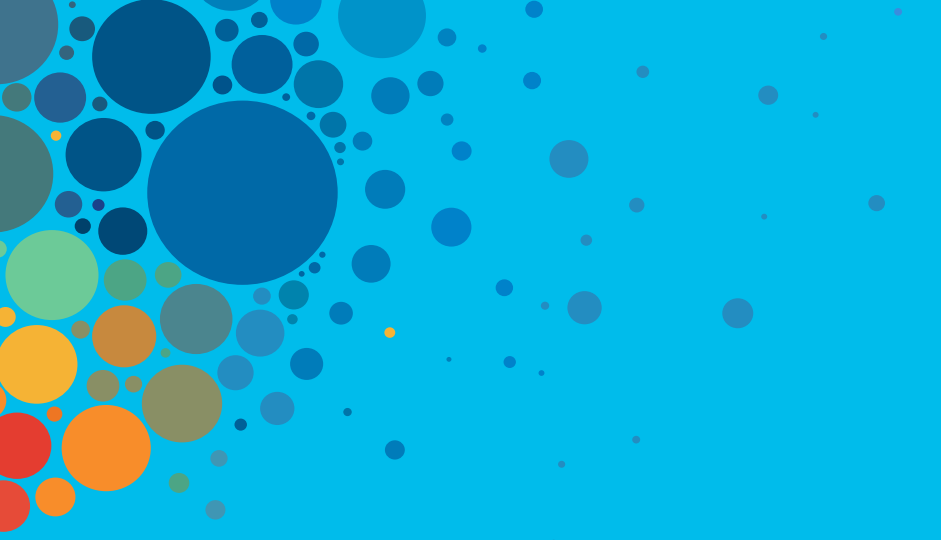
Cisco Guided Study Groups

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

CISCO *Live!*

ALL IN

#CiscoLive