

Workload Security: From challenges to Opportunities using Cisco Security

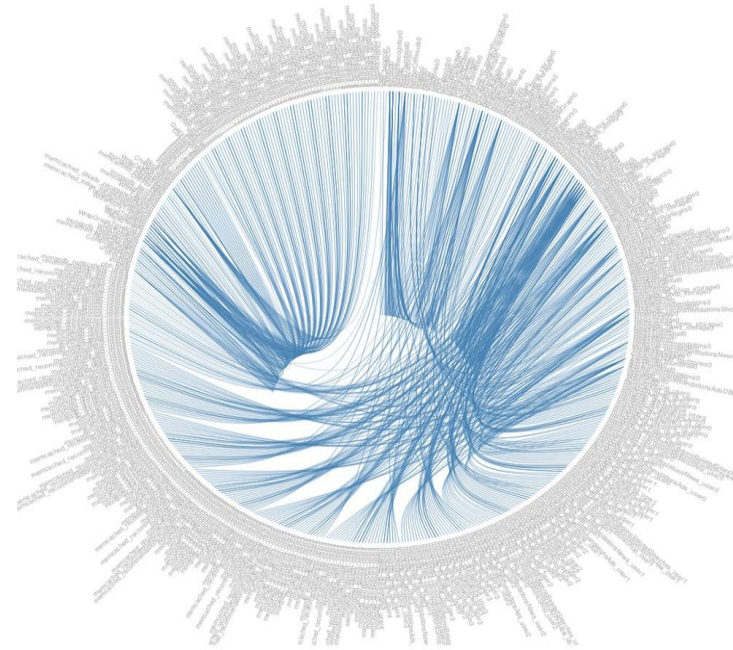
cisco Live !

Fabien Gandola
Senior CyberSecurity TSA

Two obvious but key observations :



Applications are
critical to modern
businesses

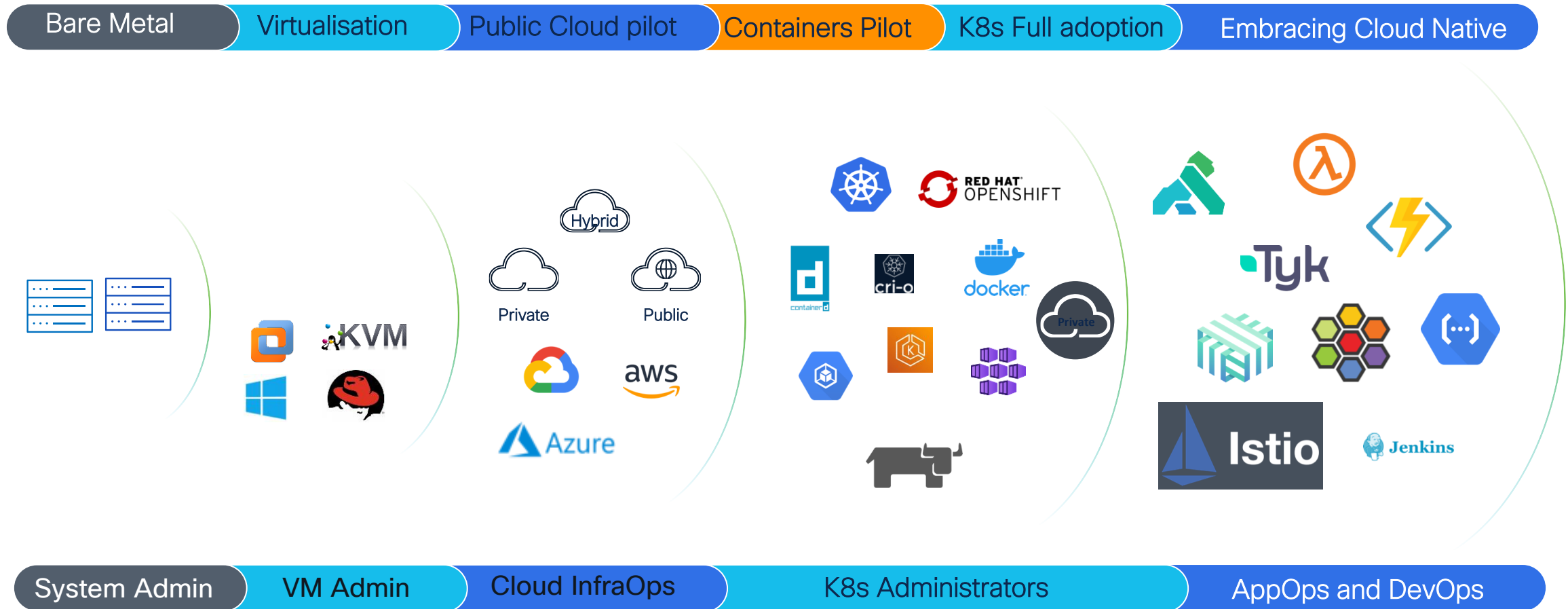


Applications have
dramatically evolved

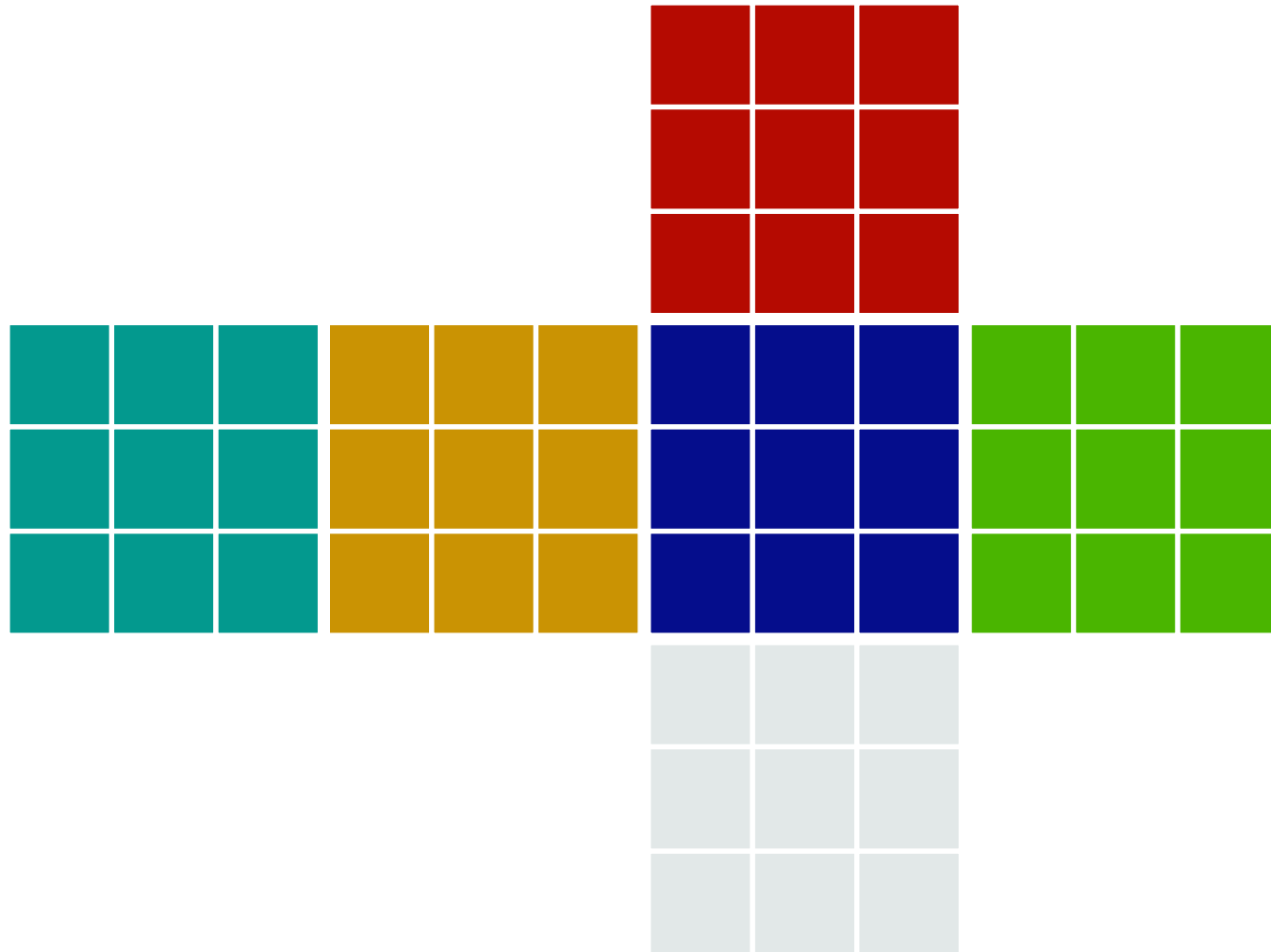
Some of the challenges

- Roles and responsibilities

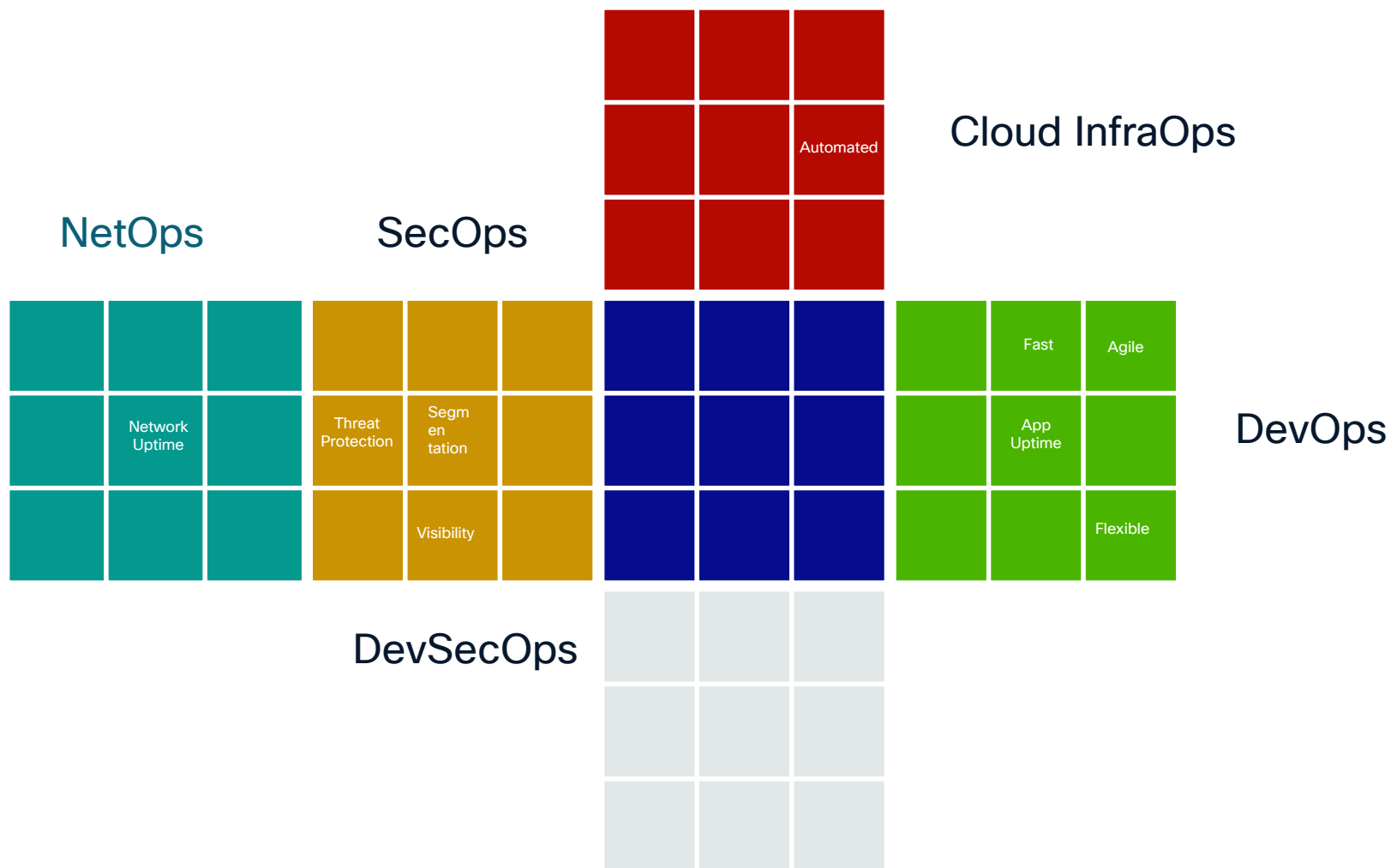
Application workloads evolution



Cloud Security Rubik cube



Cloud Security use cases



Some of the challenges

- Roles and responsibilities
- Understand the Applications behaviour to build a policy
- Different security Domains (groups, objects, labels, Tags...)
- Speed of changes of applications
- Changing policy could break an application
- Several types of enforcement points
- Managing Vulnerabilities
- Dealing with 0 day threats
- ...

Some ideas toward an ideal solution ?

- Automatically discover new applications
- Understand the different way to identify applications
- Automatically map application behaviour to a Zero Trust policy
- Automatically adapt the policy when changes happen
- Test the policy before enforcing it
- Pick the best medium to enforce a policy
- Detect Application with vulnerable components
- Improve protection against 0-Day attacks
- ...

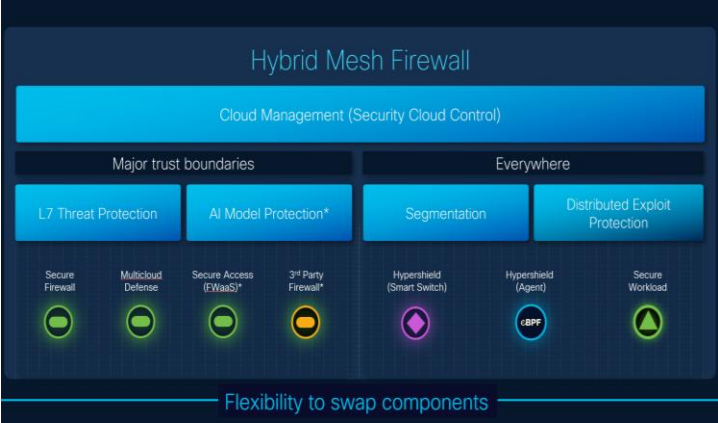
I Have
A
Dream

Our Vision

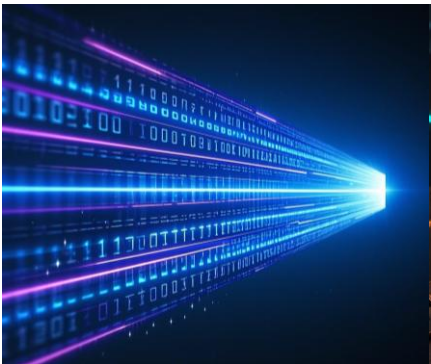
Simplification



Platform



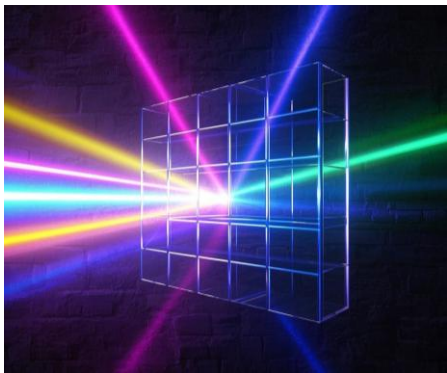
Acceleration



Automation



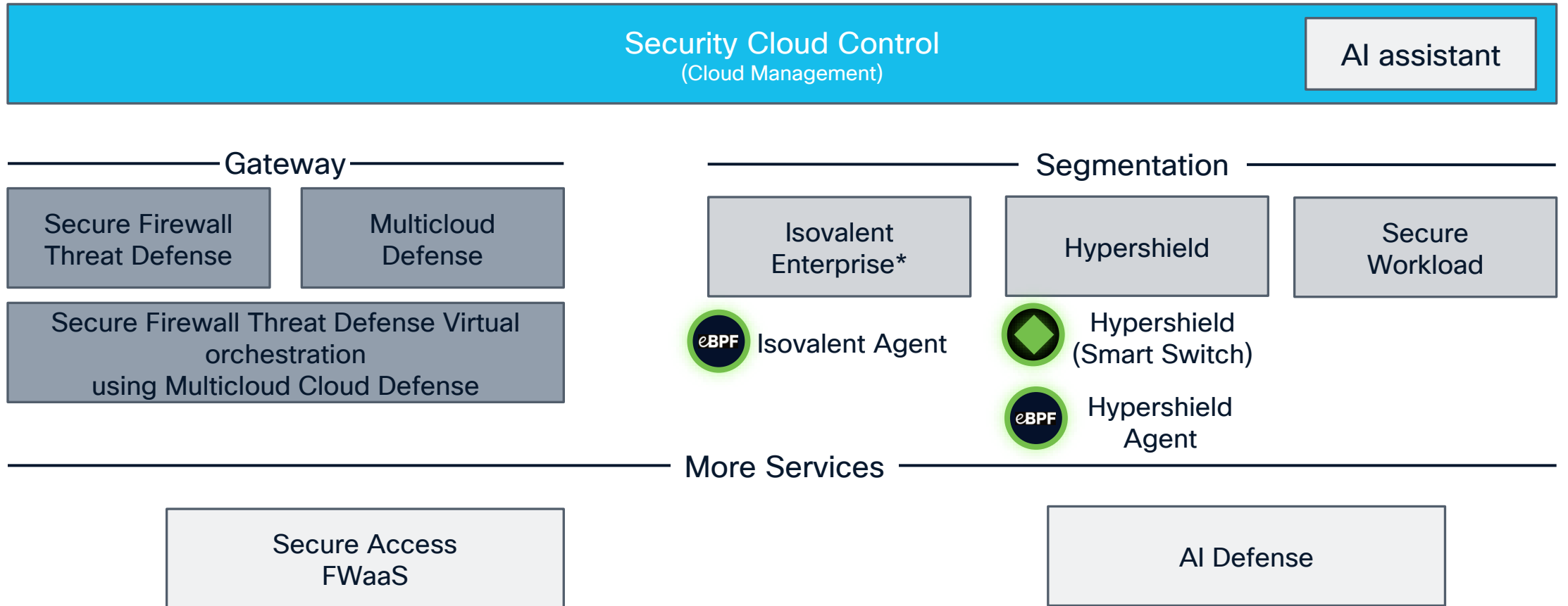
Efficiency



AI



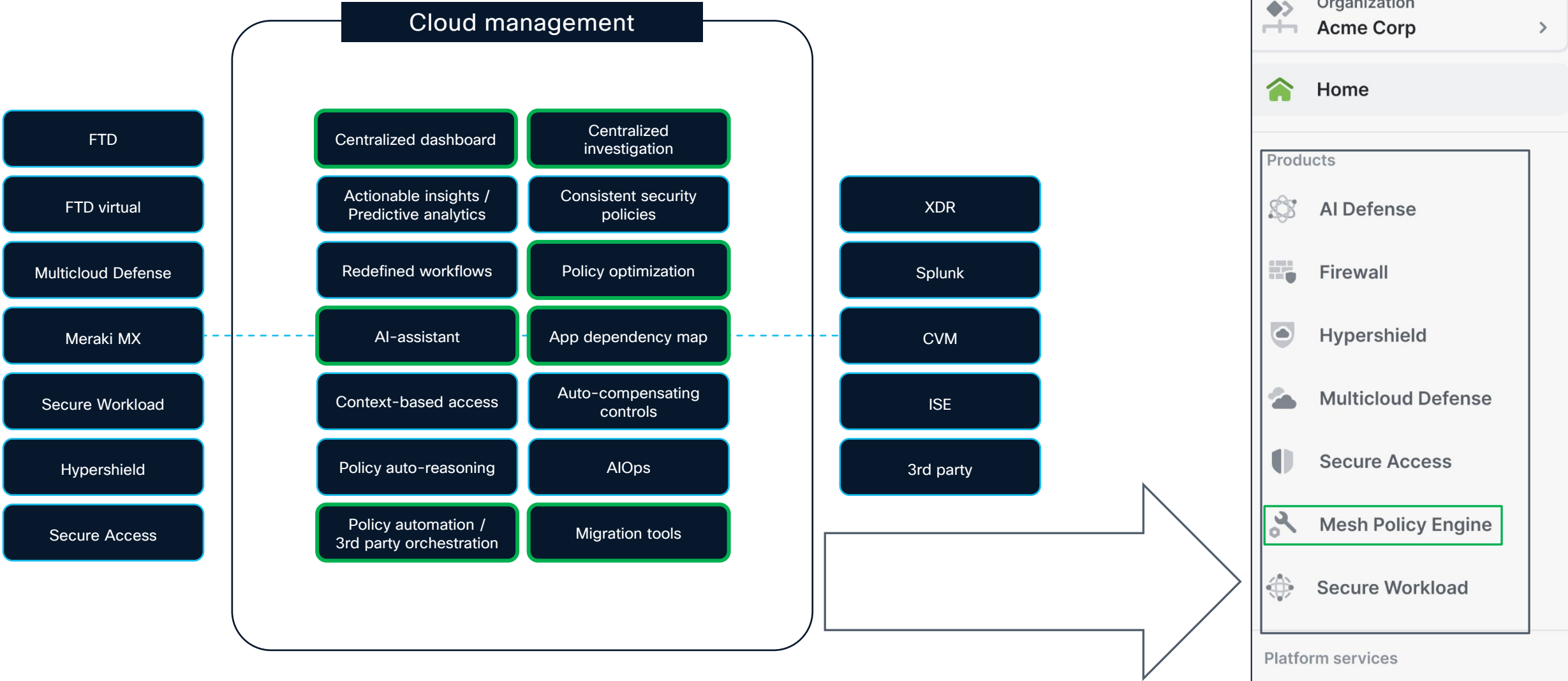
Cisco Cloud Security



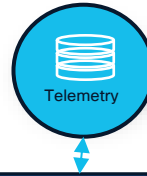
* Currently not included in the Security Cloud Control

Security Cloud Control

Unified Security Platform



Hypershield



Public Cloud | Private Cloud

What should you expect ... and not expect



- No Deep dive
- No Configuration manual
- No Troubleshooting guide
- No AI Defense nor Hypershield



- Introduction to Cisco Vision (short)
- Concrete solutions depending where you are in your Cloud adoption journey addressing your challenges
- Design and best practices

Agenda

- 01 Introduction
- 02 Starting the journey On-prem
- 03 Embracing Cloud Native
- 04 Moving to the Cloud
- 05 Conclusion

About Me



Fabien Gandola

fgandola@cisco.com

TSA Cyber Security EMEA

26 years in Cisco

Cisco Webex App

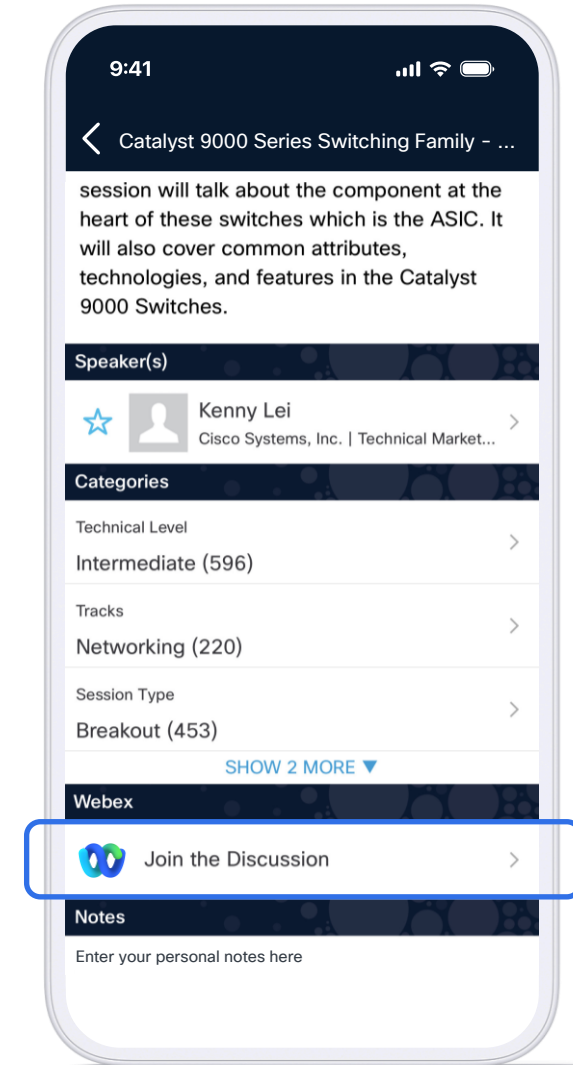
Questions?

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

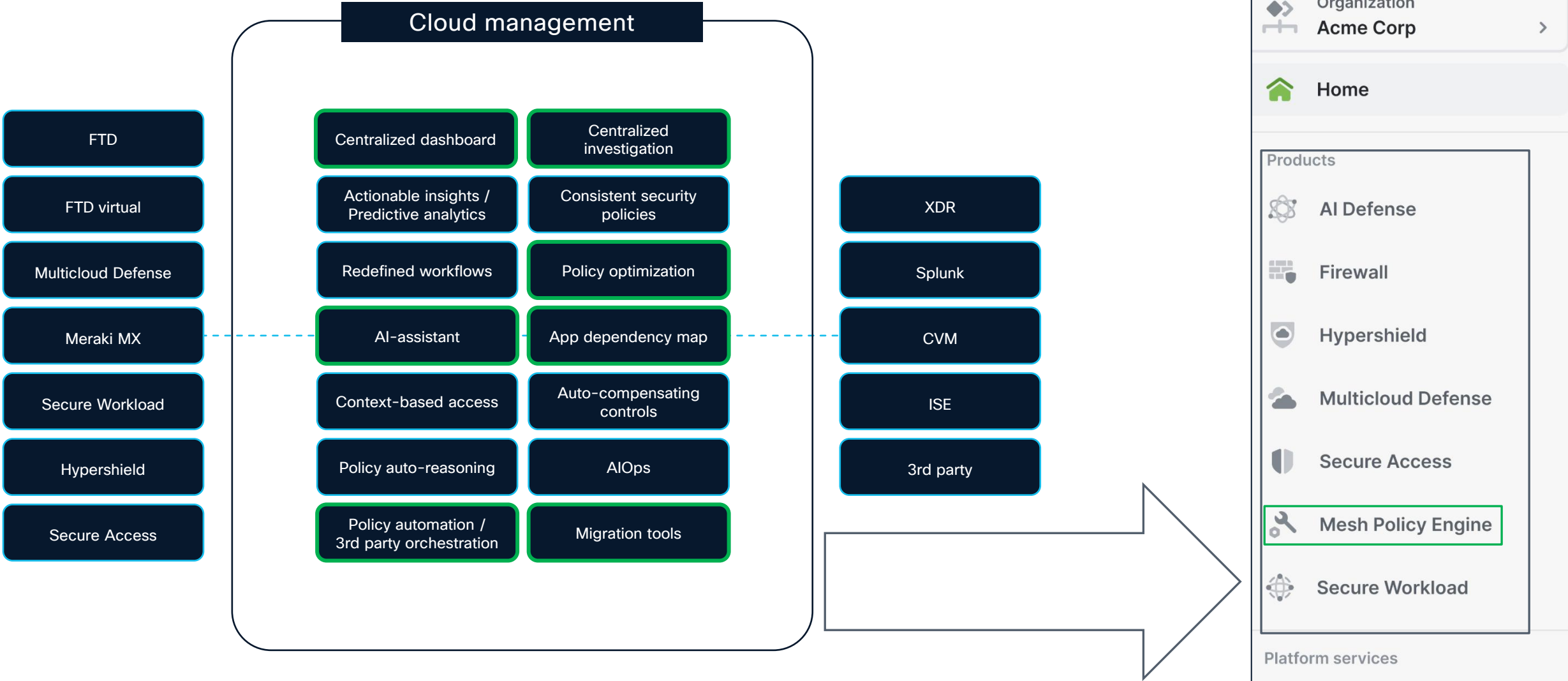
Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2571>

Security Cloud Control

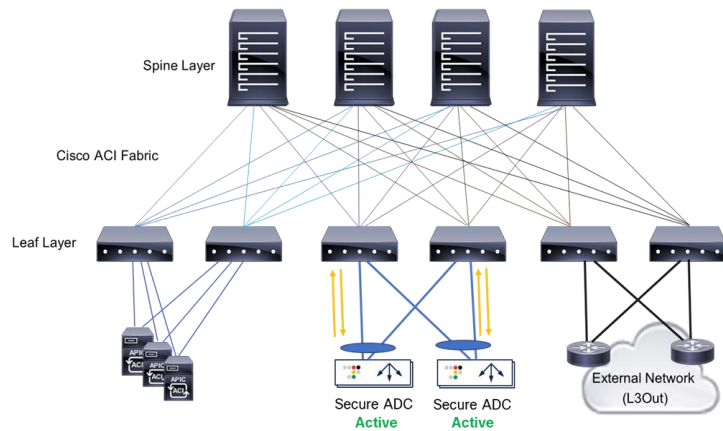
Unified Security Platform





It starts on-prem...

The way we are doing it traditionally...



SDN
Infrastructure
(ACI, NSX,...)



Firewall
(FTD, ASA)



 **SECURE**
Workload

Host based
Firewall

Shortest intro to ACI

Enforce Trust in the DC with Cisco ACI

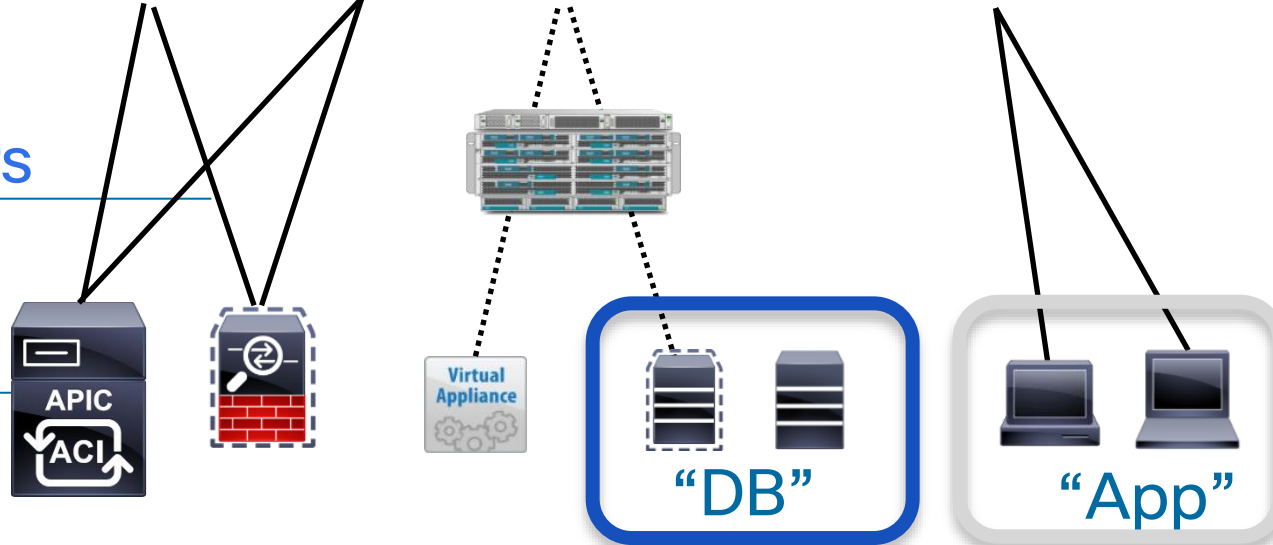
Spine Nodes



Leaf Nodes

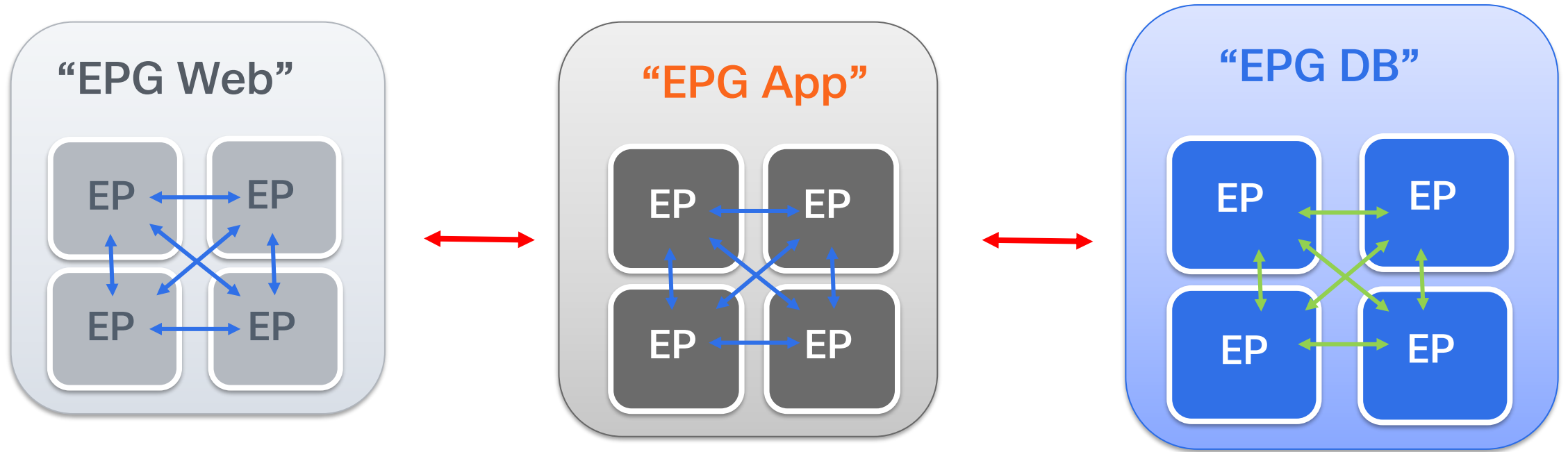


Service Producers



Service Consumers

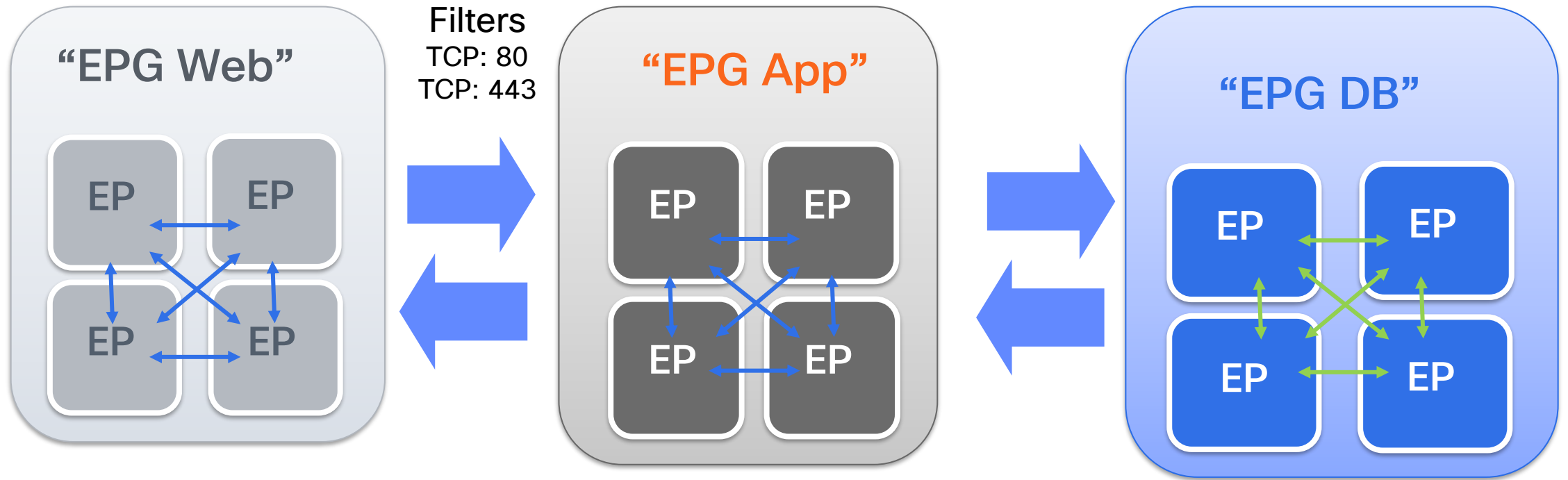
Endpoint Groups Communications



Devices within an Endpoint group can communicate, provided that they have IP reachability (provided by the Bridge Domain/VRF).

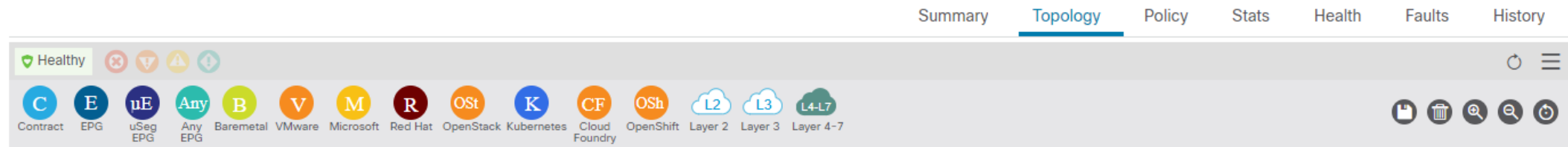
Communication between Endpoint groups is, by default, not permitted.

Contract : Kind of reflexive “Stateless” ACLs



A contract typically refers to one or more ‘filters’ to define specific protocols & ports allowed between EPGs.

Application policy with contract

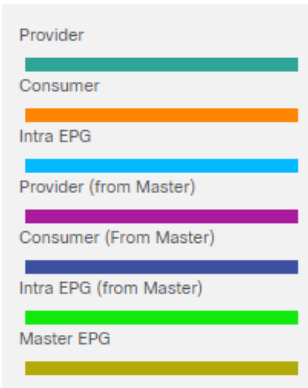


Contracts →

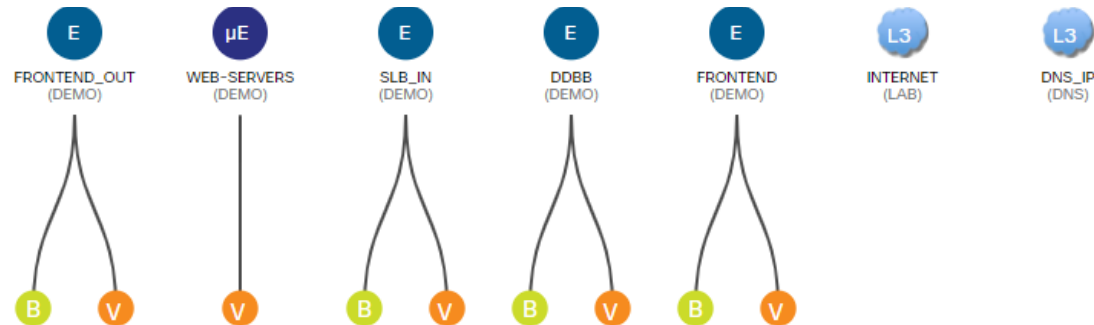
Relation Indicators

Configured ☐ Operational ☐

Show All ☐ On Click ☐



EPG →

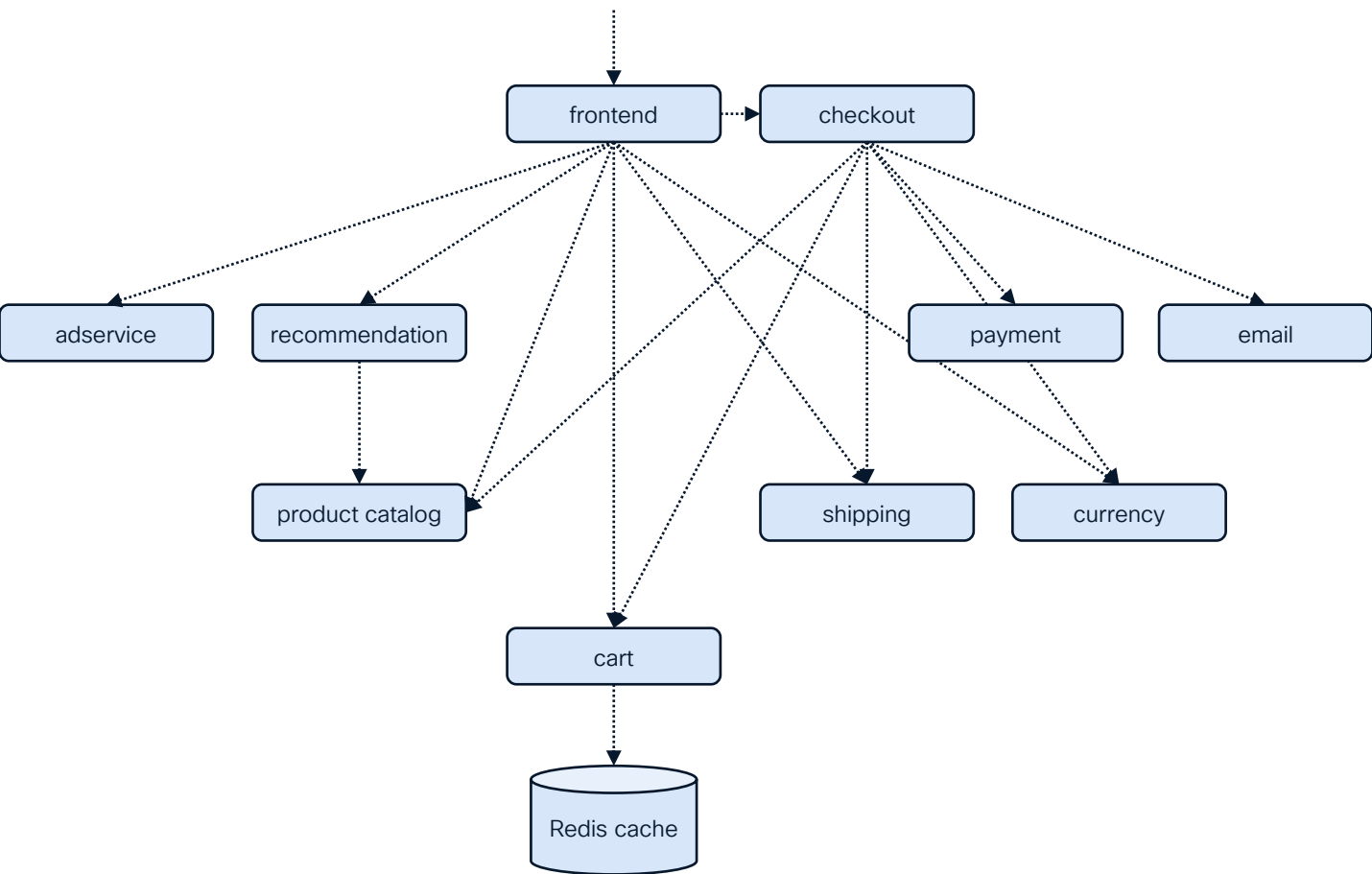


Form Factor →

Cancel Submit

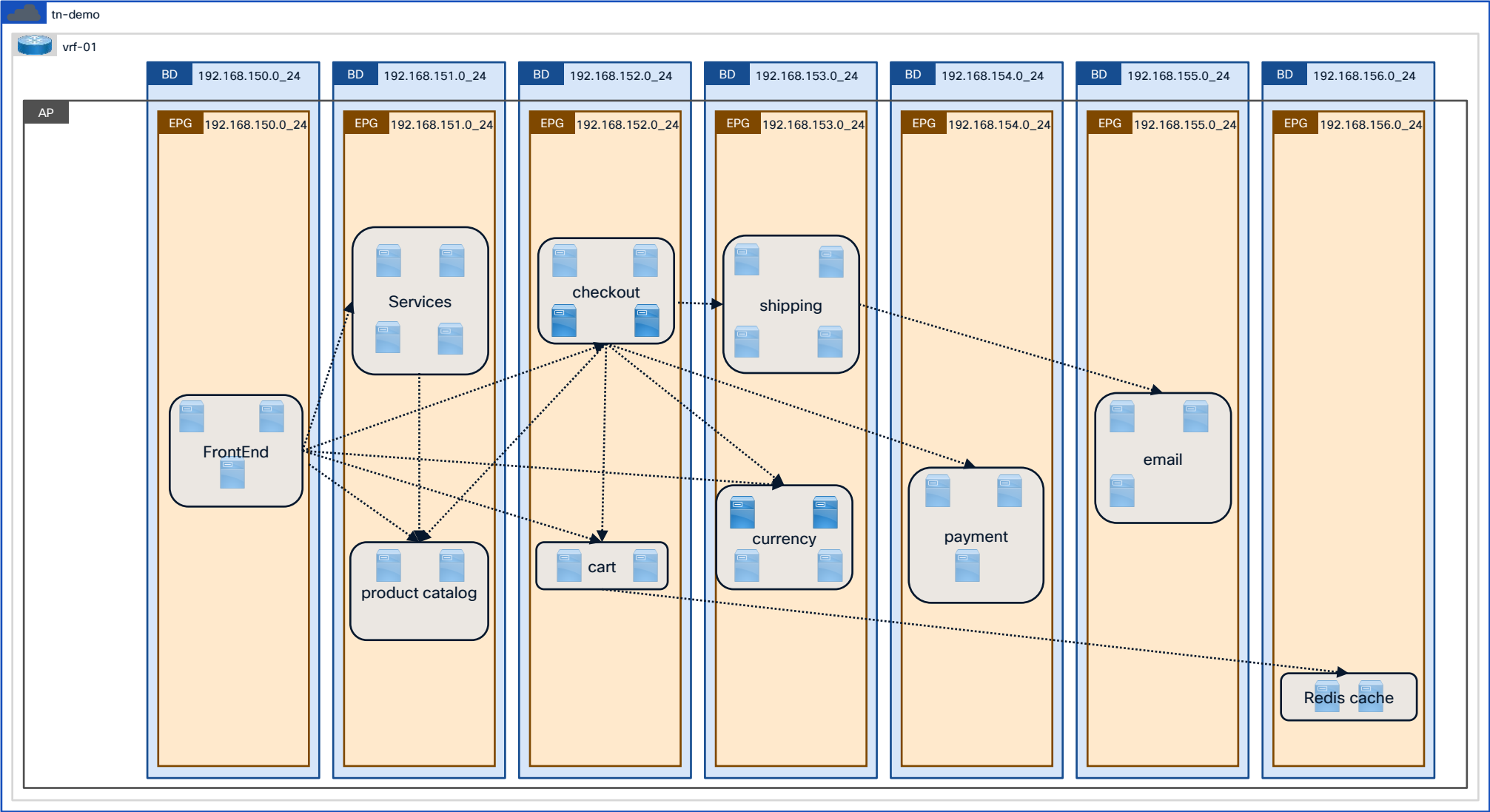
Online Boutique

<https://github.com/GoogleCloudPlatform/microservices-demo>

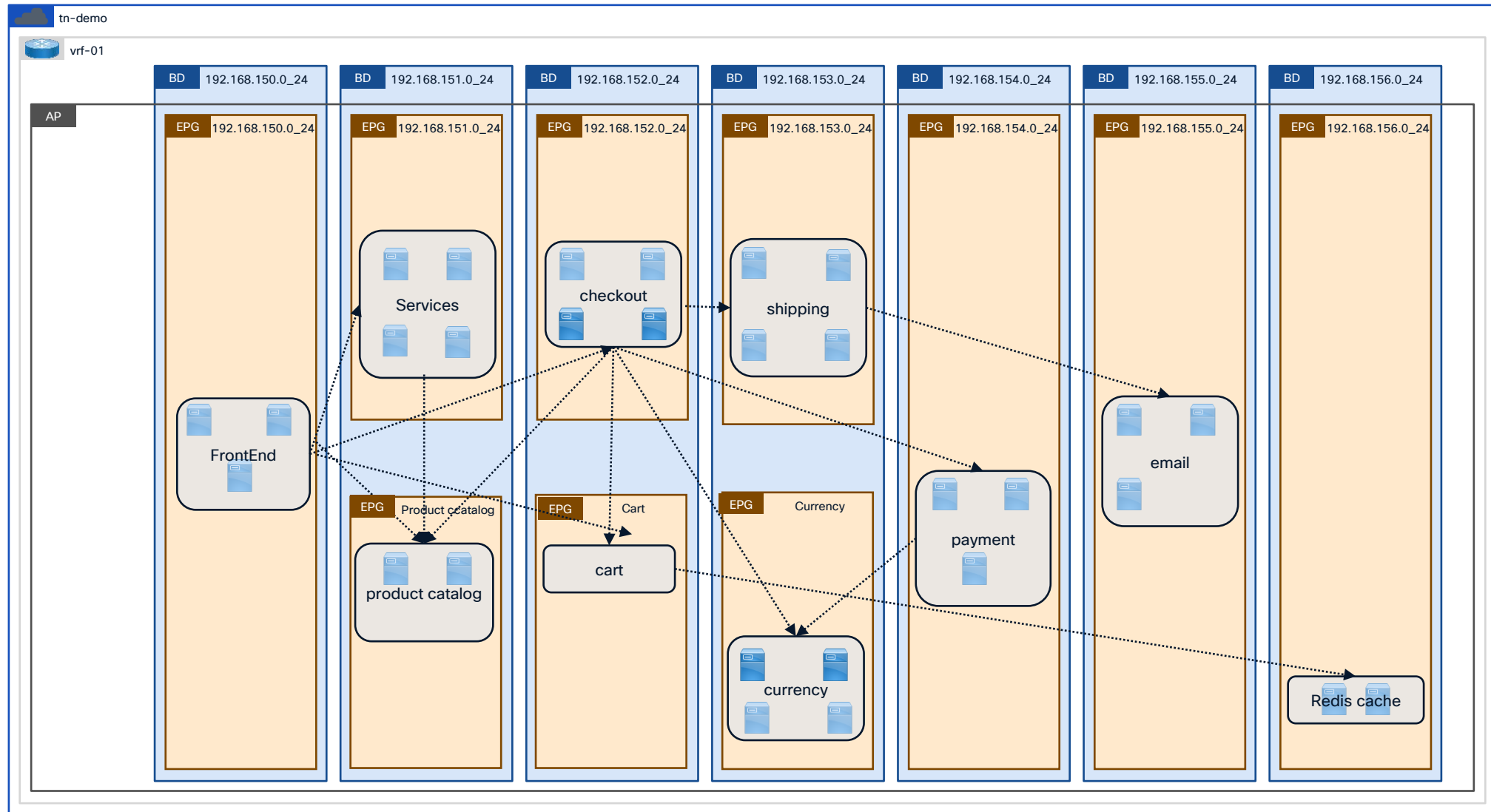


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 8080
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP 3550
	recommendation	TCP 8080
	shipping	TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

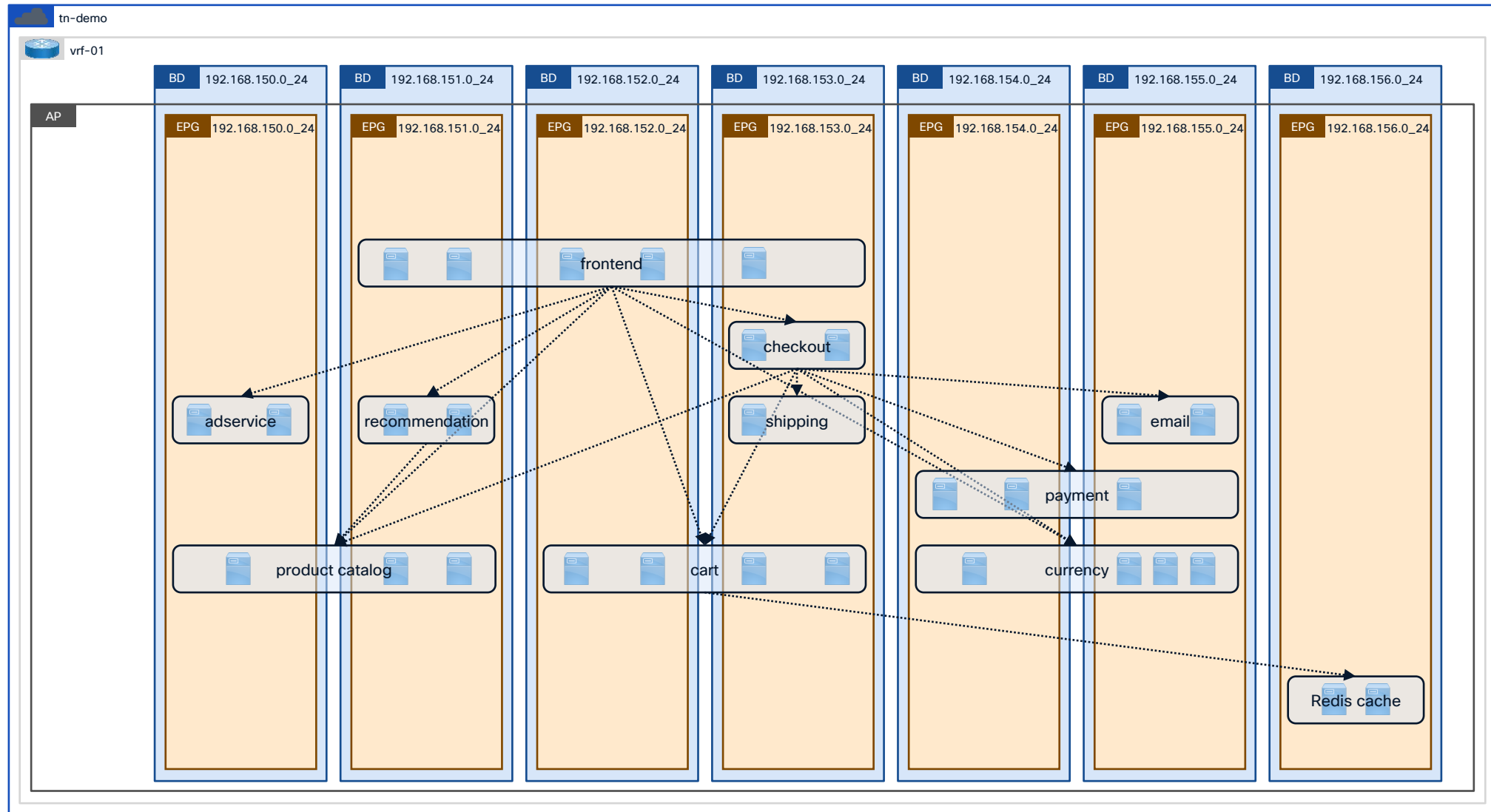
How do we establish trust groups?



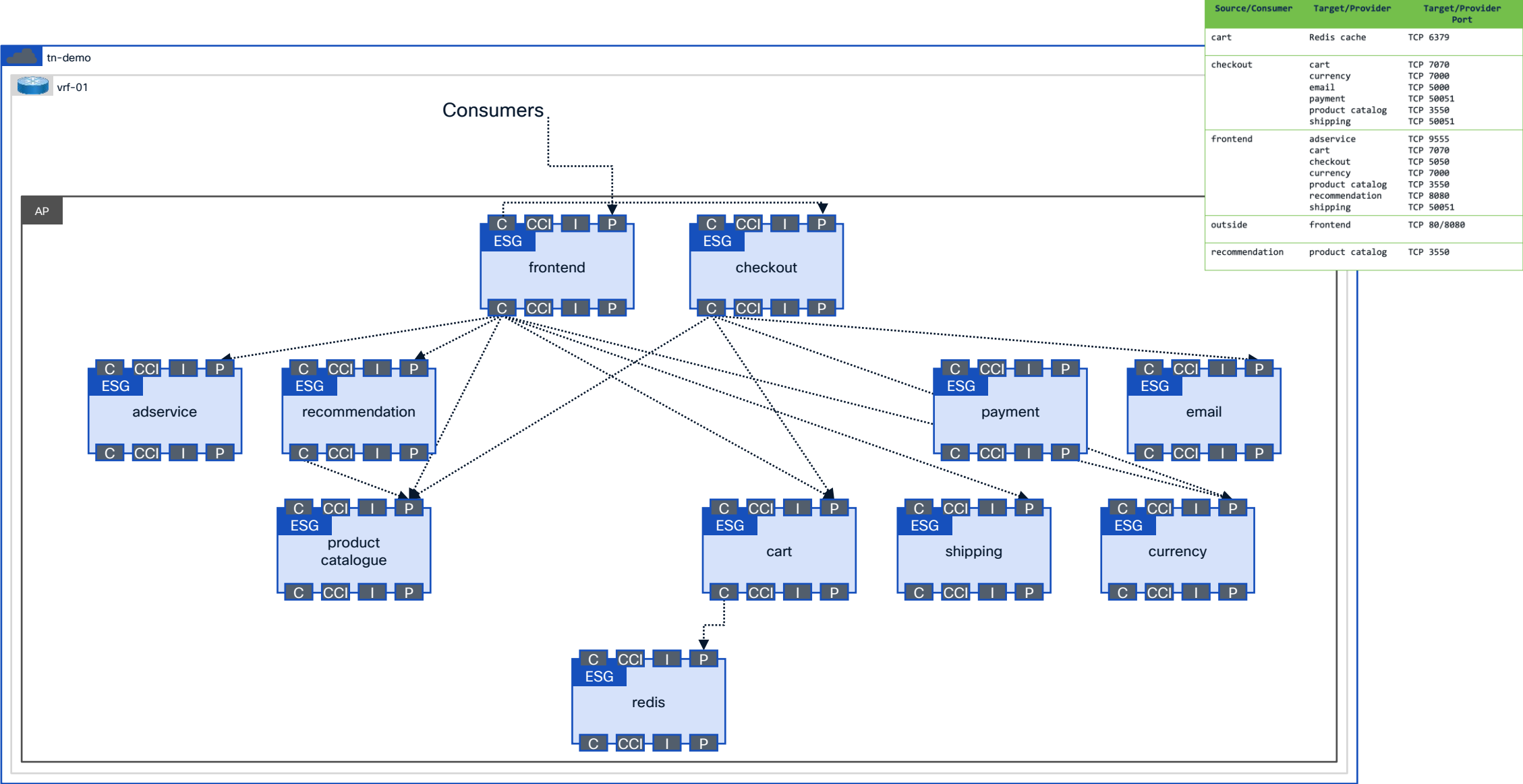
Not so fast – How do we establish trust groups?



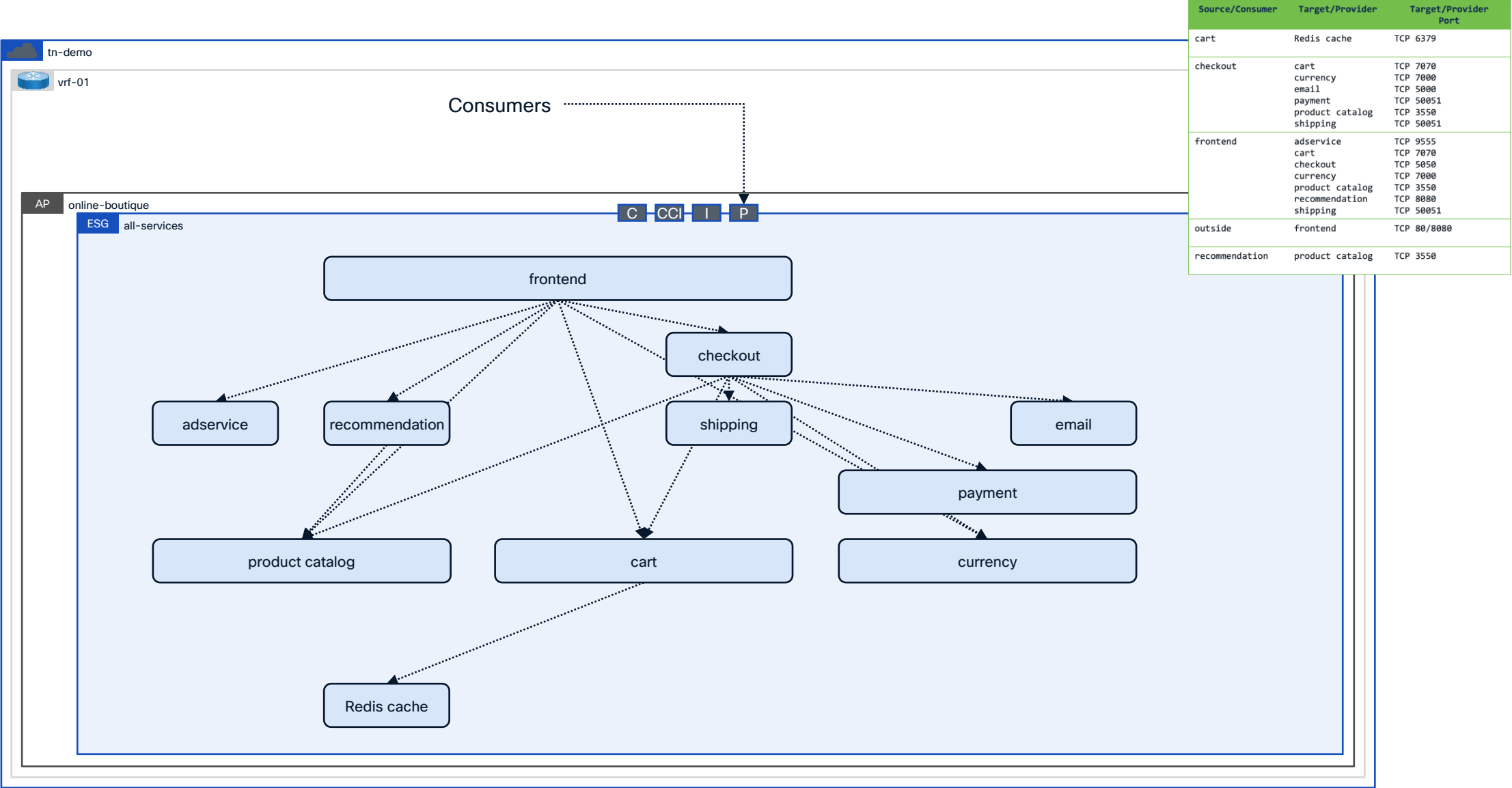
Is subnet the right way to establish trust groups?



Network agnostic endpoint security groups (ESGs)



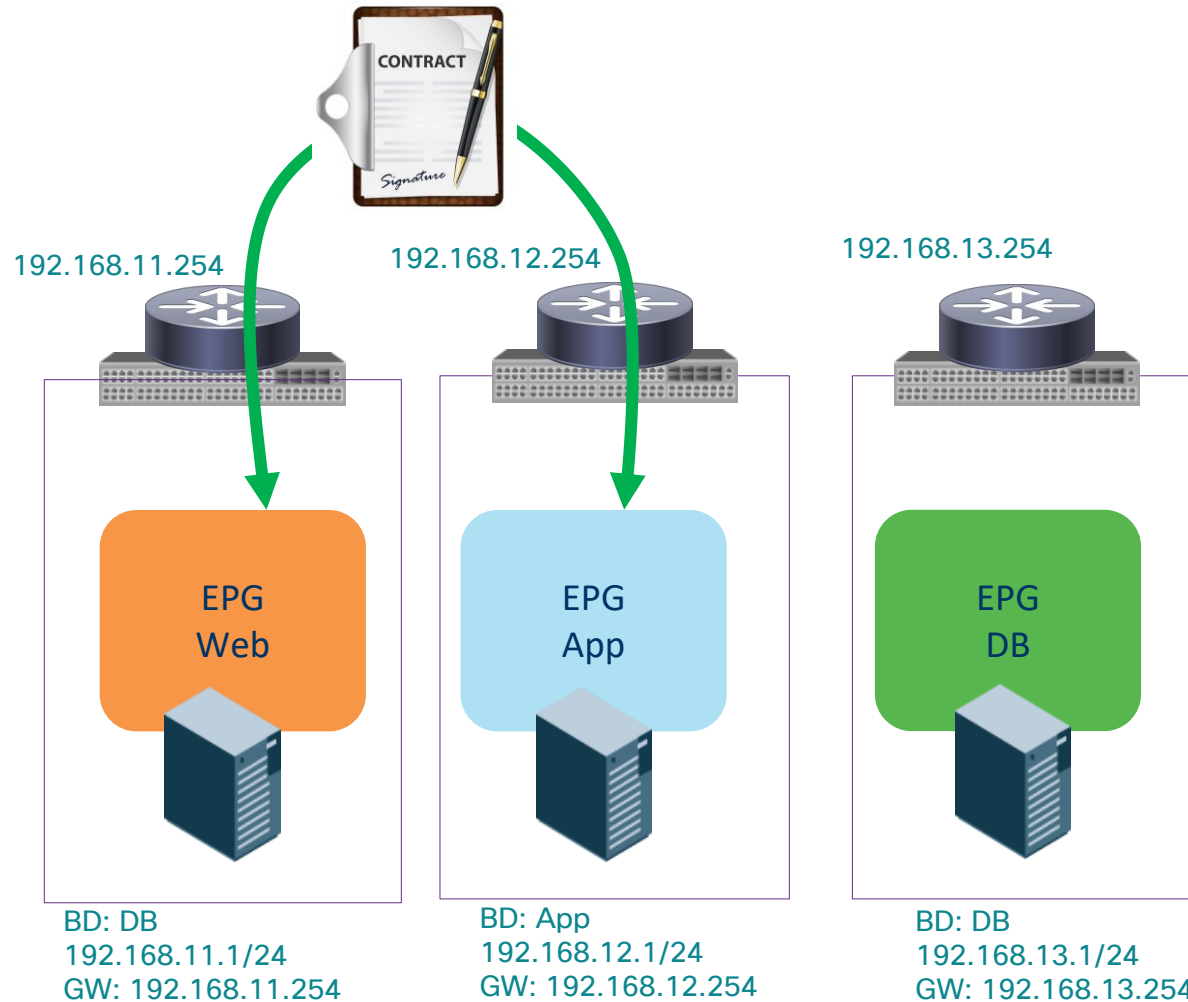
Simpler to start with the DC Edge



How do I Insert a Firewall ?

2 conditions for traffic reaching destination

Before Service graph is deployed

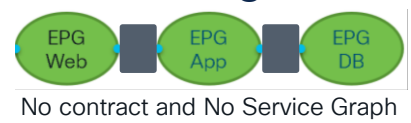
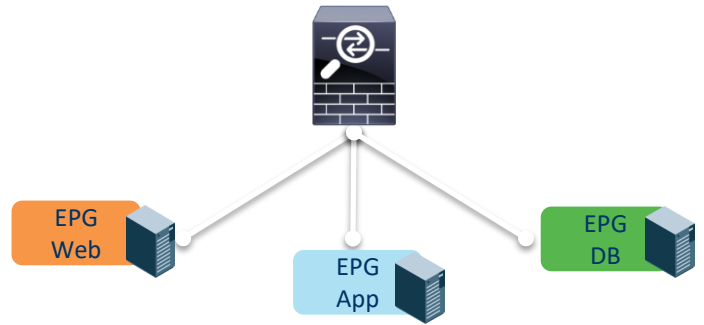


APIC relies on :

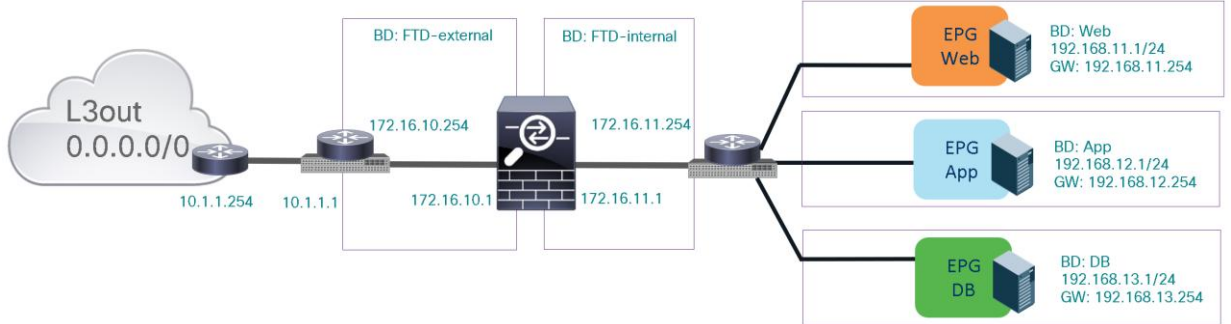
- ✓ **Routing** to forward traffic
- ✓ **Contract** to allow traffic

3 main ways to insert a Firewall in ACI

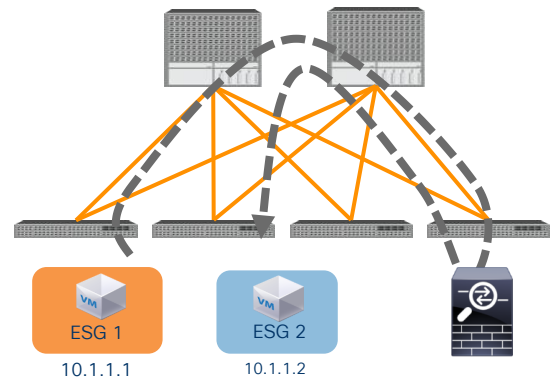
- “Network Stitching” Firewall Insertion



- Traditional Service Graph

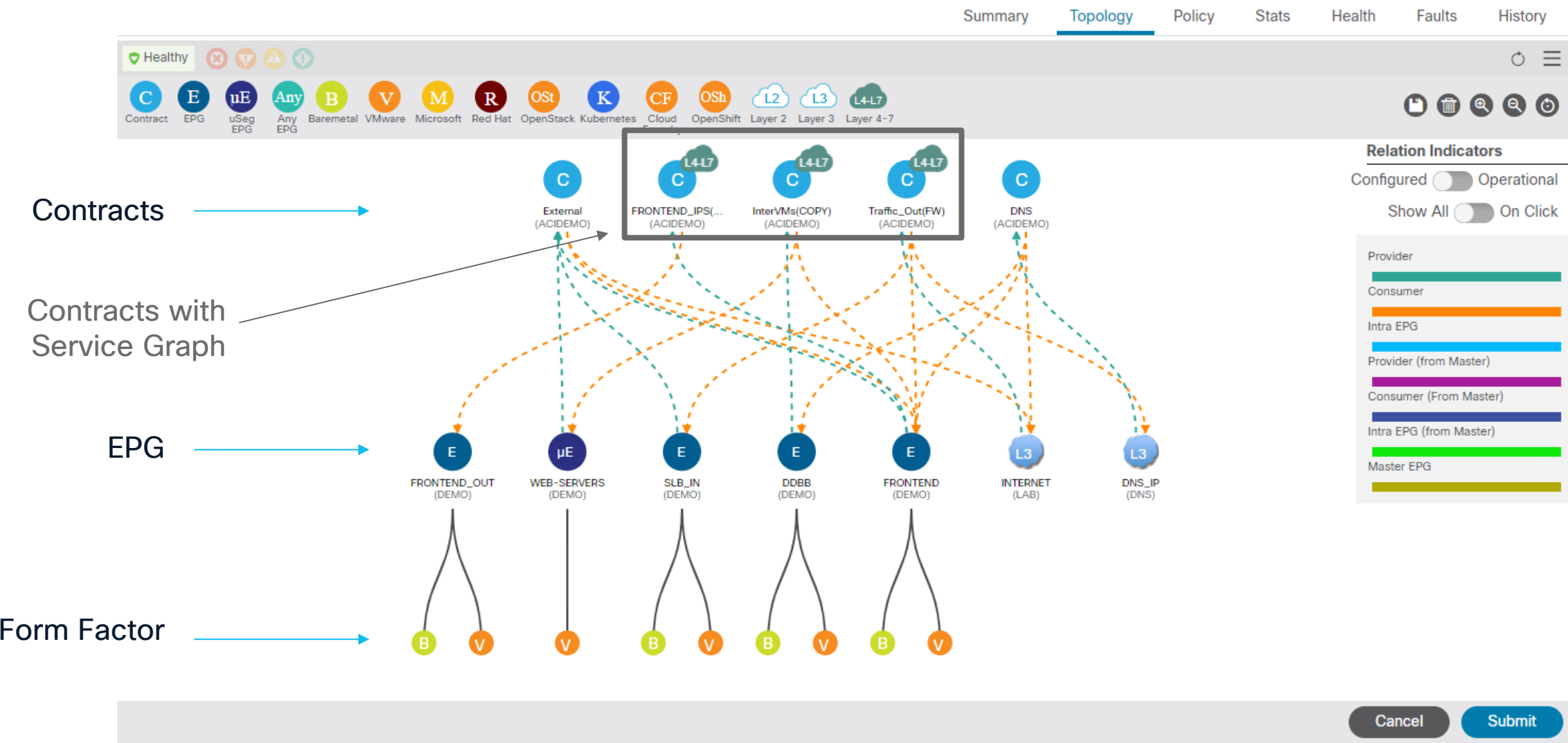


- Service Graph with Policy Based Redirect



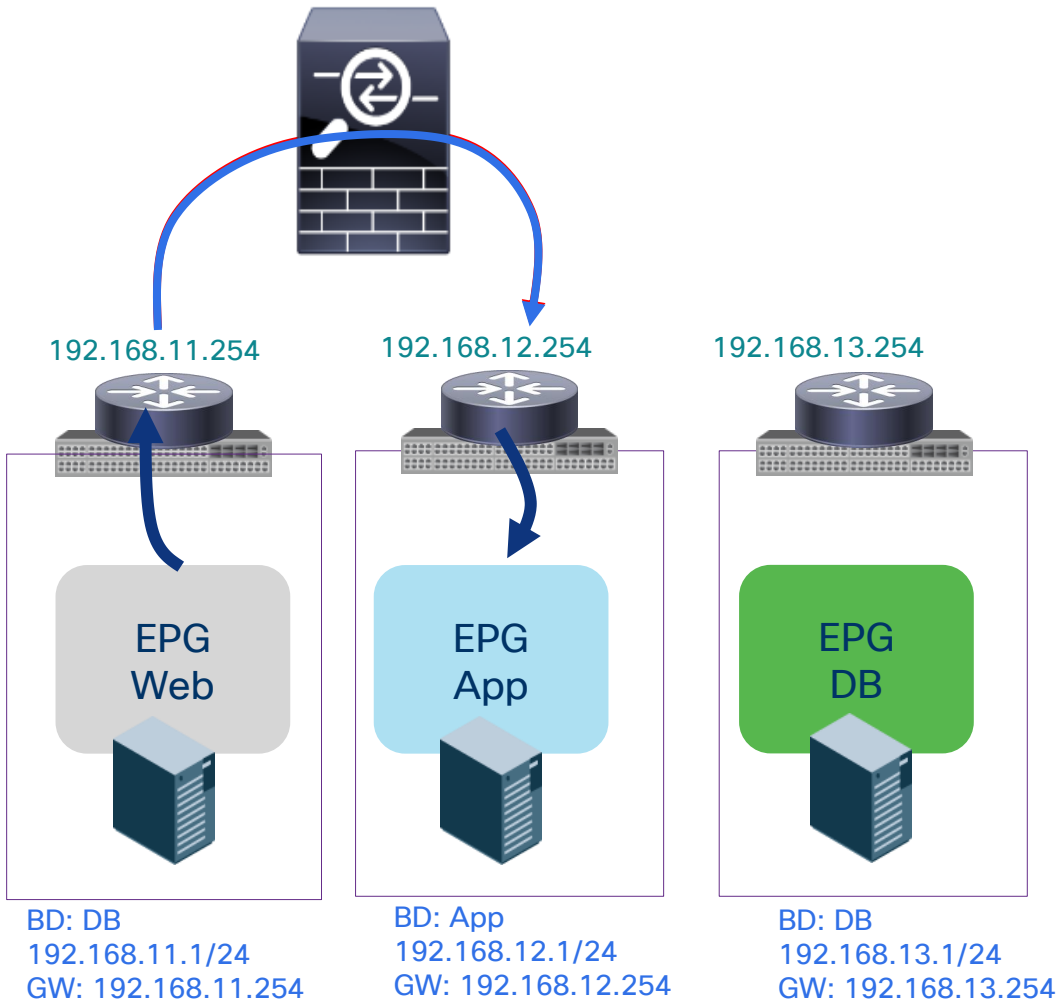
Enforce granular trust at N-S edge and E-W

Attach a Service Graph to a contract

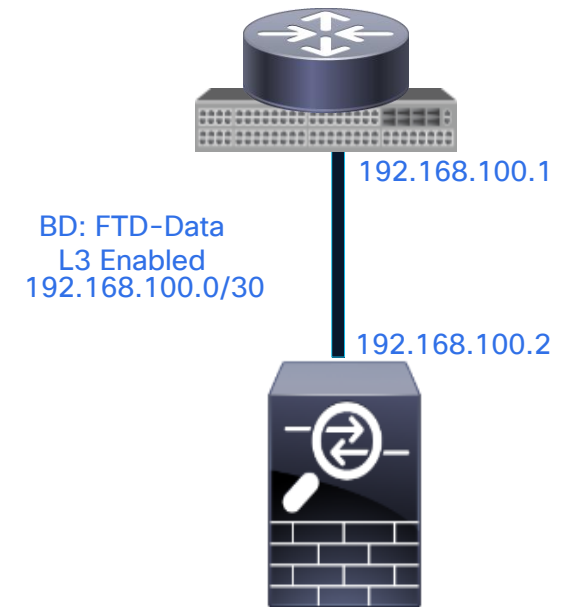


Policy Based Redirect is your Best Friend

With PBR Service Graph



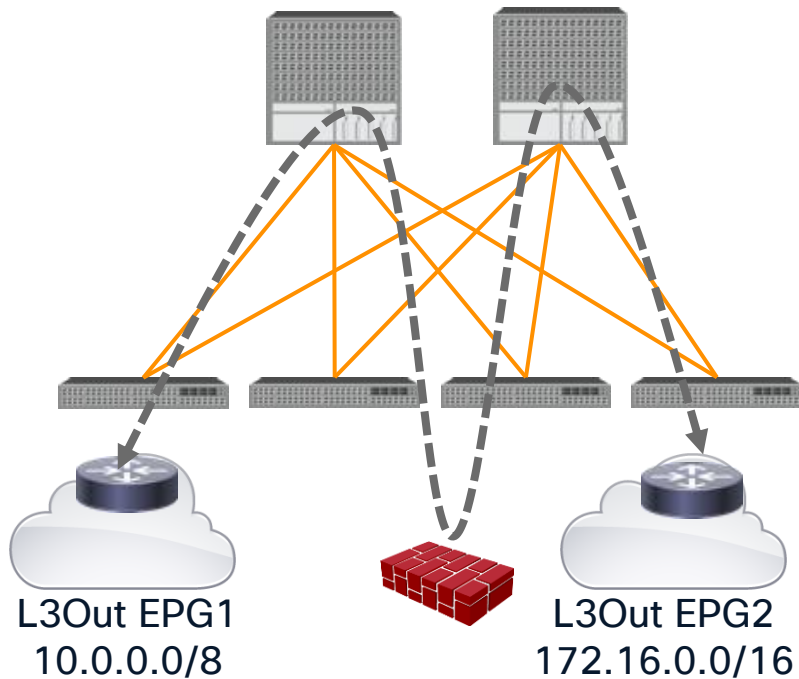
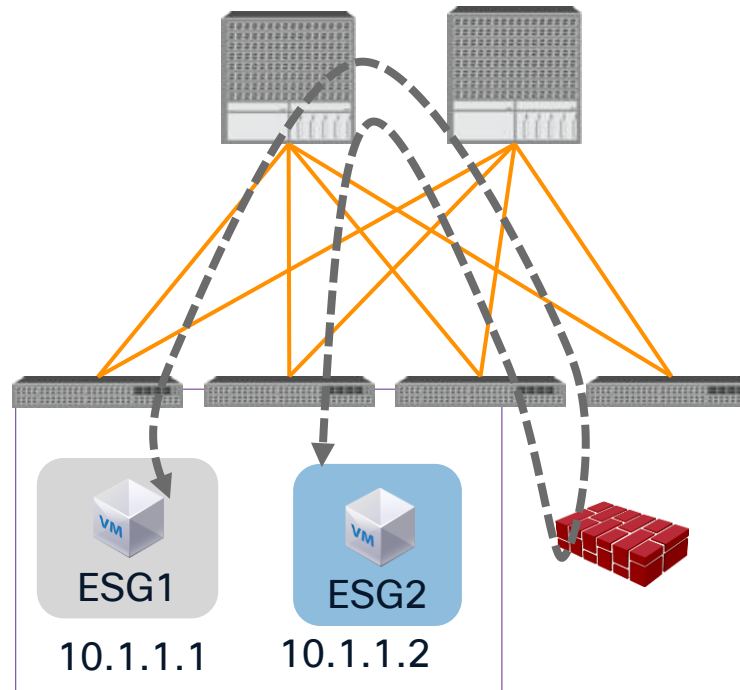
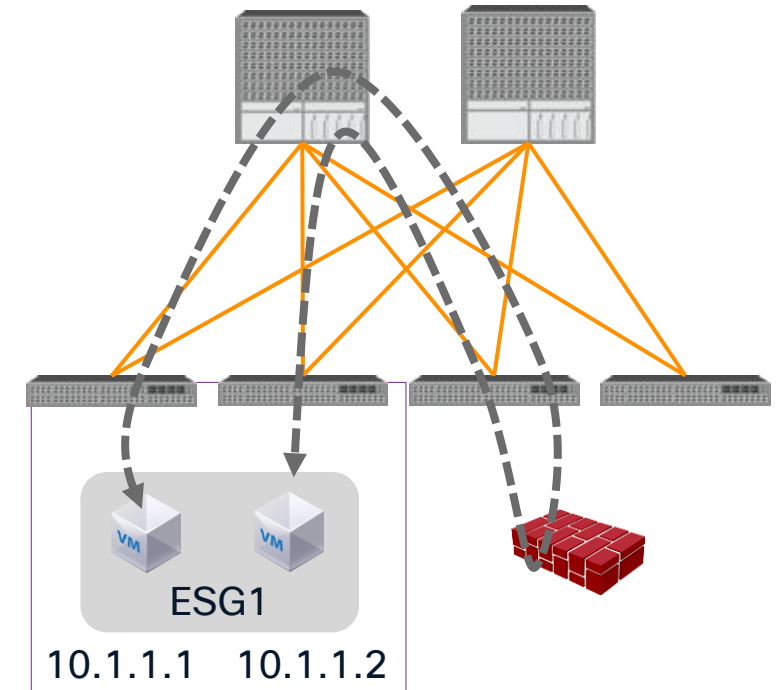
PBR redirects the traffic matching the **contract(s)** to the **Security Service**



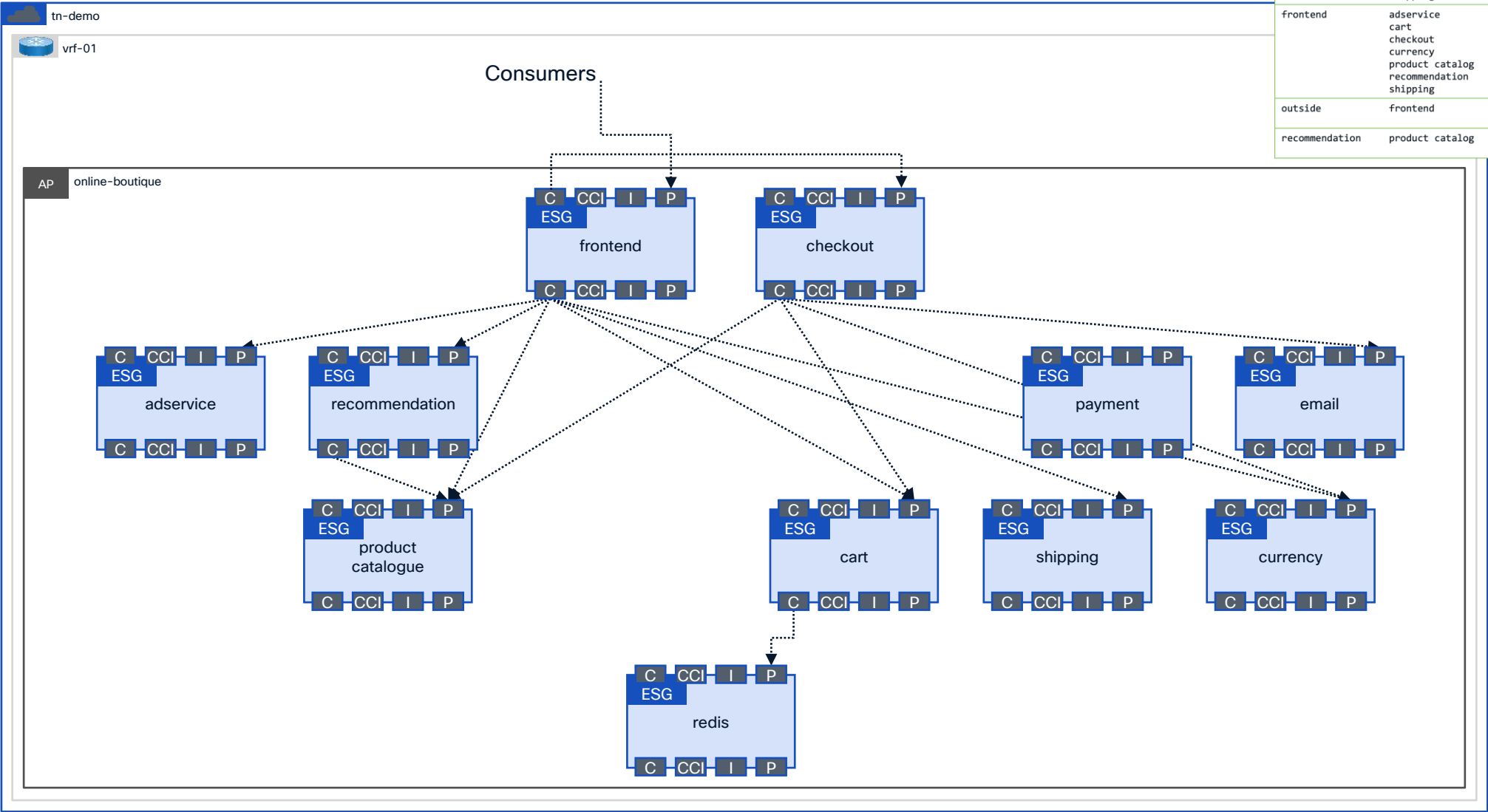
Where can we (re)use PBR?

Wherever contracts can be applied!

- Between EPGs or ESGs.
- Between L3Out EPGs.
- Between EPGs or ESGs in the same subnet.
- Between endpoints in the same EPG or ESG.

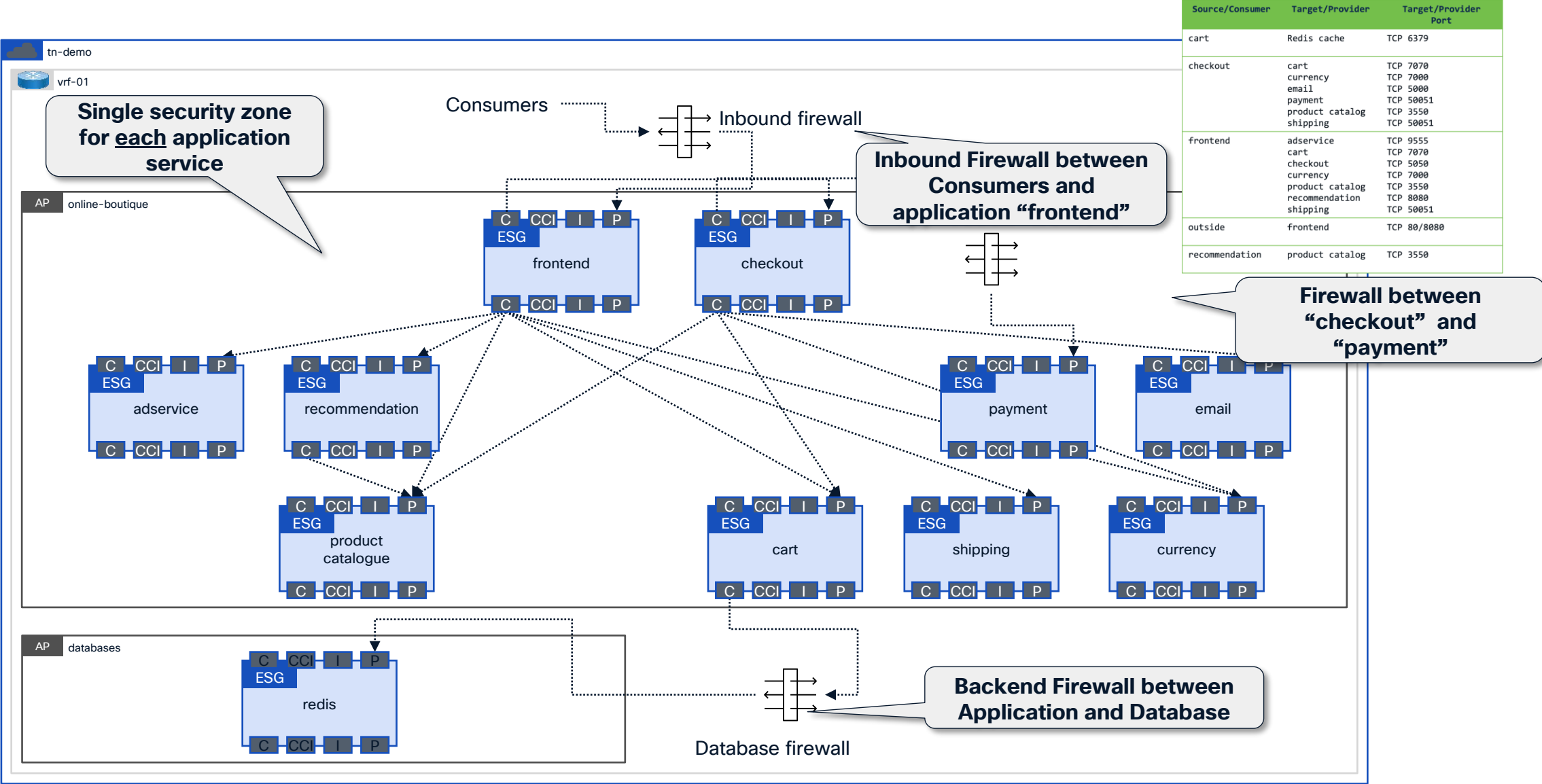


Application tiers across subnets

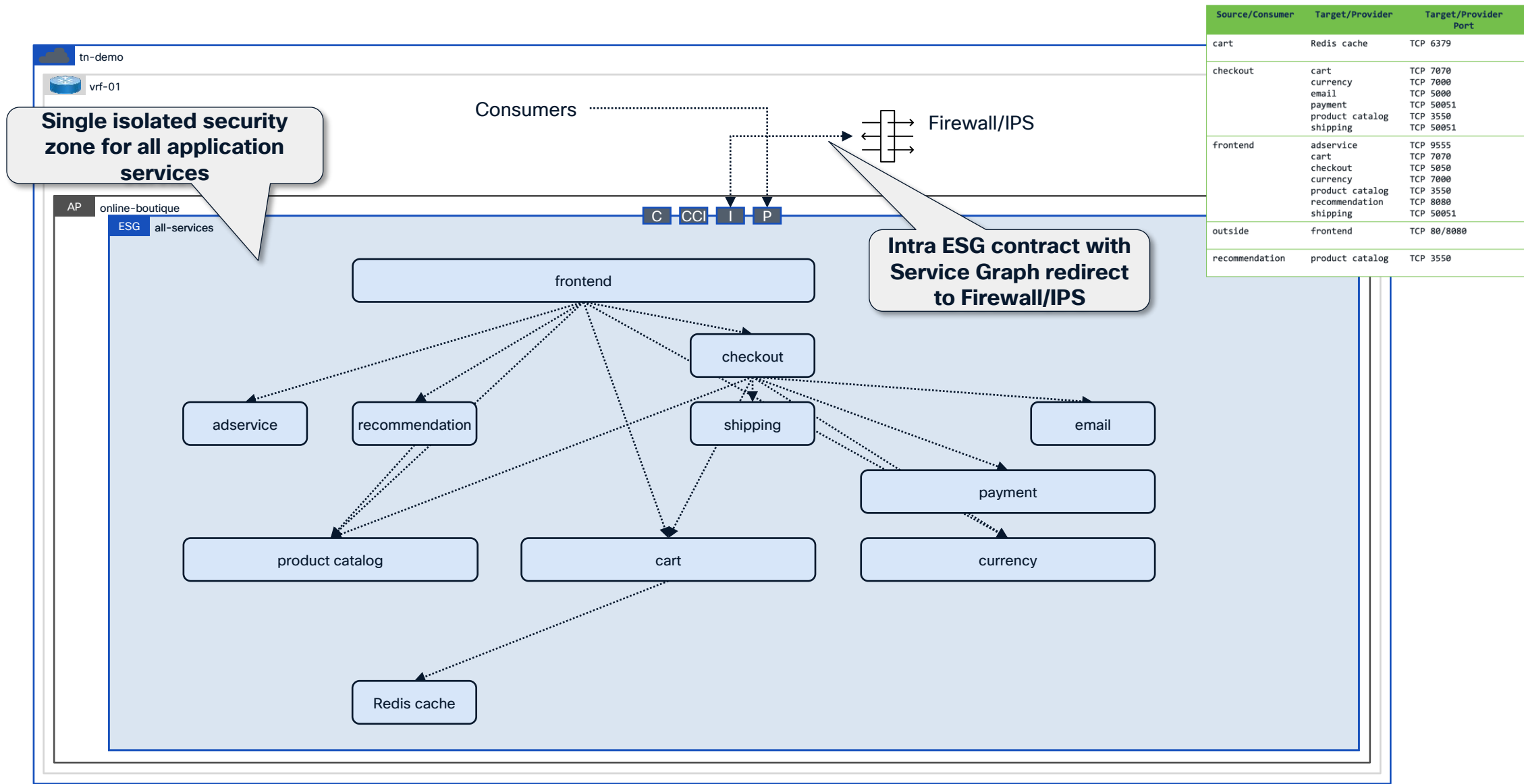


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
frontend	shipping	TCP 50051
	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
recommendation	product catalog	TCP 3550
	recommendation	TCP 8080
	shipping	TCP 50051
outside	frontend	TCP 80/8080

Complement ACI Contracts with Firewalls

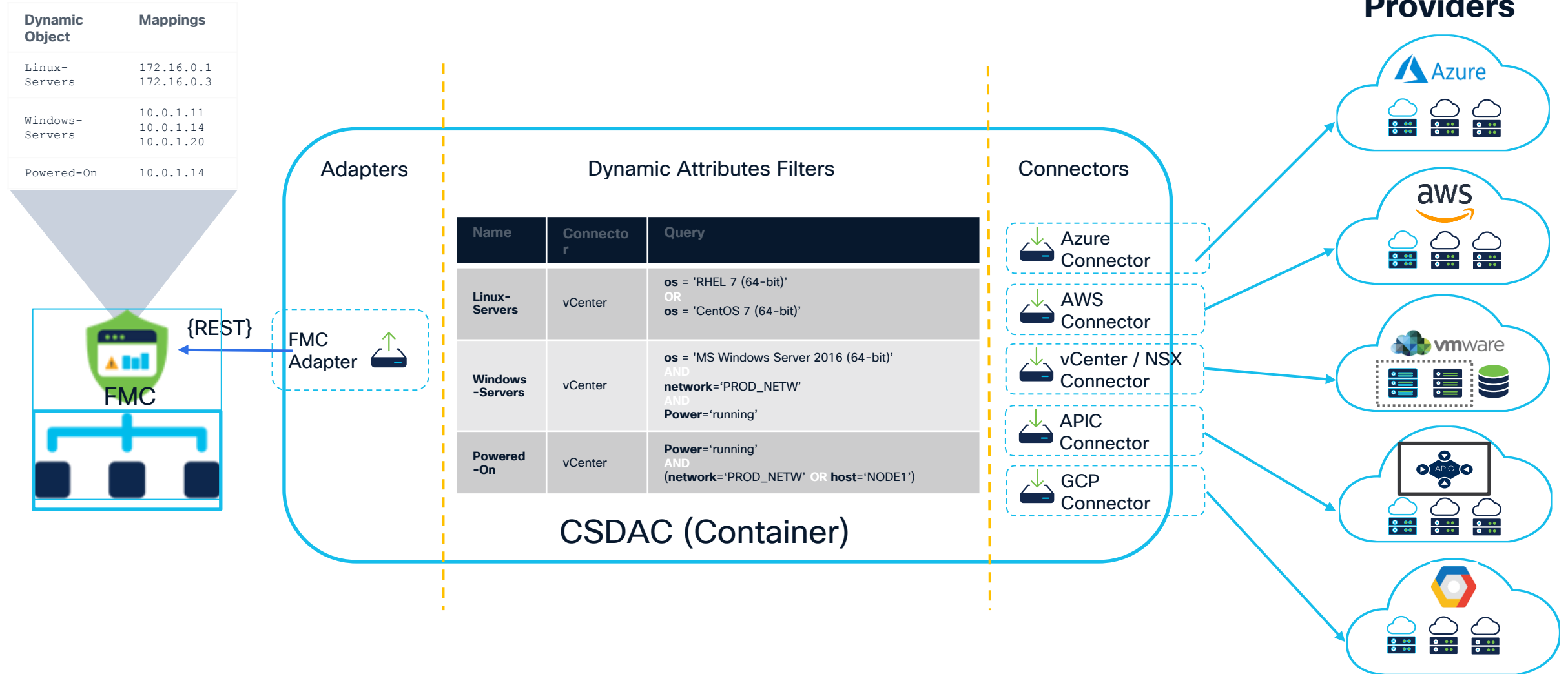


Microsegment with FTD using Intra-ESG SG



**How could I use all those
groups in my Firewall Policy ?**

Doing more with Dynamic Attributes Connector



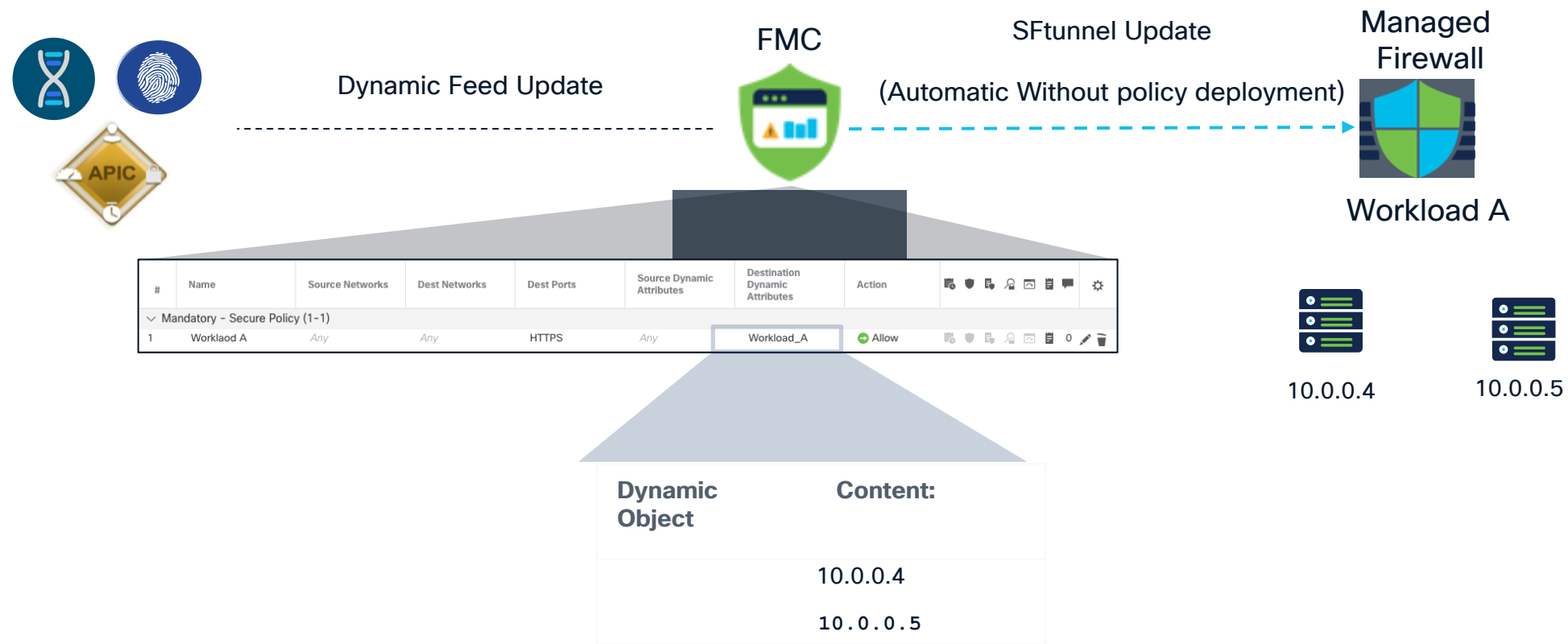
Attribute Based Policy

#	Name	Source Zones	Dest Zones	Users	App	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)									
v Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	→ Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	→ Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	→ Allow
4	Print	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	→ Allow
5	Block Social Media	Corporate_VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	Contractors Branch_Locations	Any	→ Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	→ Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	→ Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	→ Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	→ Allow



Dynamic Objects in Action

Automatic Without policy deployment



Establish Trust – FMC Learns EPGs/ESGs

APIC (aci-dev-01)

System | **Tenants** | Fabric

ALL TENANTS | Add Tenant | Tenant Search: name of

fgandola

Quick Start

fgandola

- Application Profiles
 - applications
 - Application EPGs
 - uSeg EPGs
 - Endpoint Security Groups
 - ALL_EPGs
 - development
 - production
 - firewalls
 - Application EPGs
 - ftd-HA-link
 - ftd-mgmt
 - uSeg EPGs
 - Endpoint Security Groups
 - network-segments
 - Networking
 - Contracts
 - Policies
 - Services
 - Security

Secure Firewall Management Center

Objects / Object Management

Overview | Analysis | Policies | Devices | **Objects** | Integration | Deploy

Dynamic Objects

Name	Description	Number of Mapped IPs
APIC_DEMO_APPLICATIONS_ESG-DEMO-APP		1
APIC_DEMO_NETWORK-SEGMENTS_192.168.150.X_24		1
APIC_FGANDOLA_APPLICATIONS_ESG-ALL_EPGS		2
APIC_FGANDOLA_APPLICATIONS_ESG-DEVELOPMENT		1
APIC_FGANDOLA_APPLICATIONS_ESG-PRODUCTION		1
APIC_FGANDOLA_FIREWALLS_FTD-HA-LINK		1
APIC_FGANDOLA_FIREWALLS_FTD-MGMT		4
APIC_FGANDOLA_NETWORK-SEGMENTS_192.168.151....		1
APIC_FGANDOLA_NETWORK-SEGMENTS_192.168.152....		2
APIC_FGANDOLA_NETWORK-SEGMENTS_192.168.153....		1

APIC_FGANDOLA_FIREWALLS_FTD-MGMT

Mapped IPs

10.237.100.22
10.237.100.23
10.237.100.24
10.237.100.25

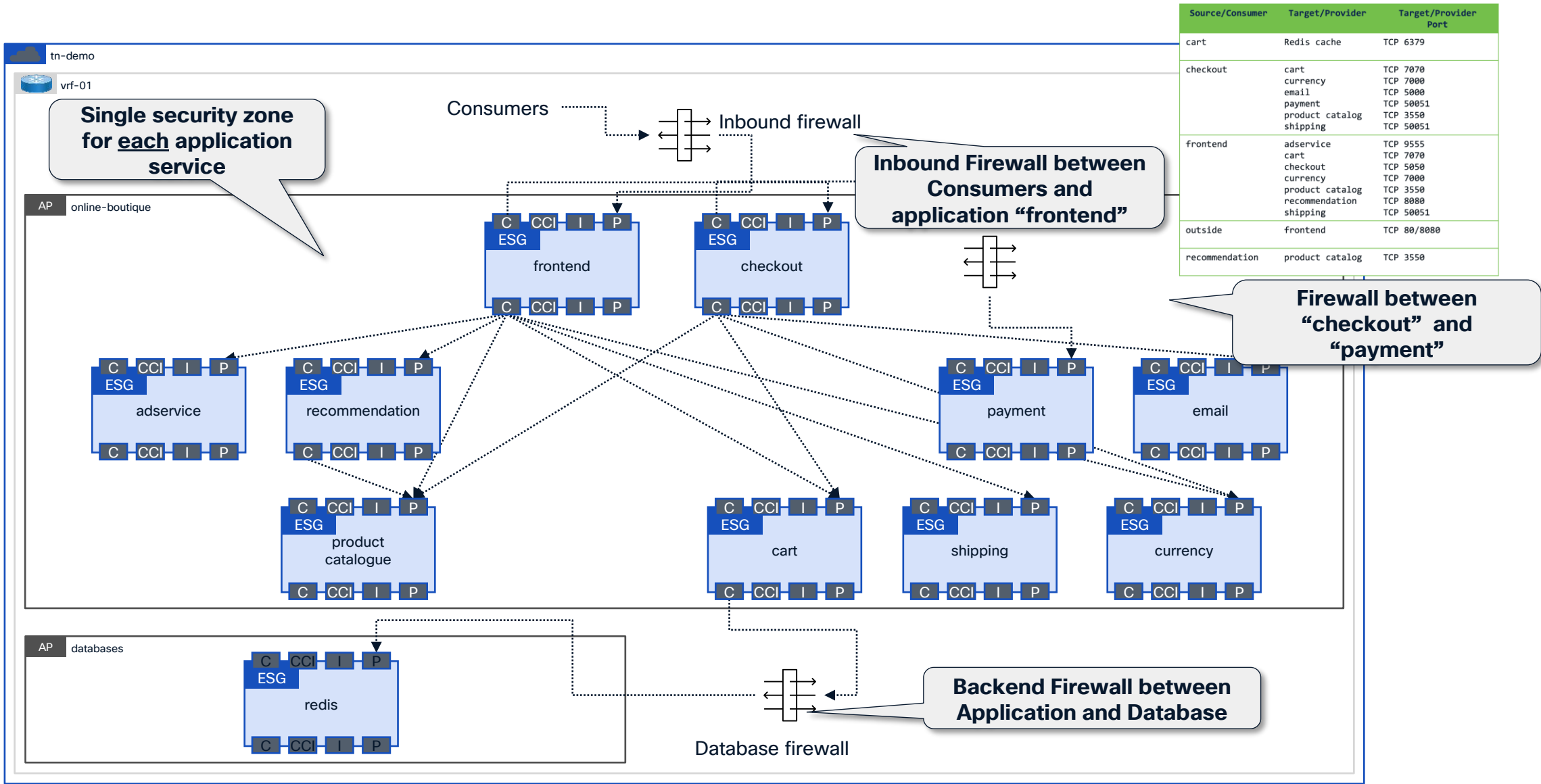
Download OK

© 2025 Cisco and/or its affiliates. All rights reserved.

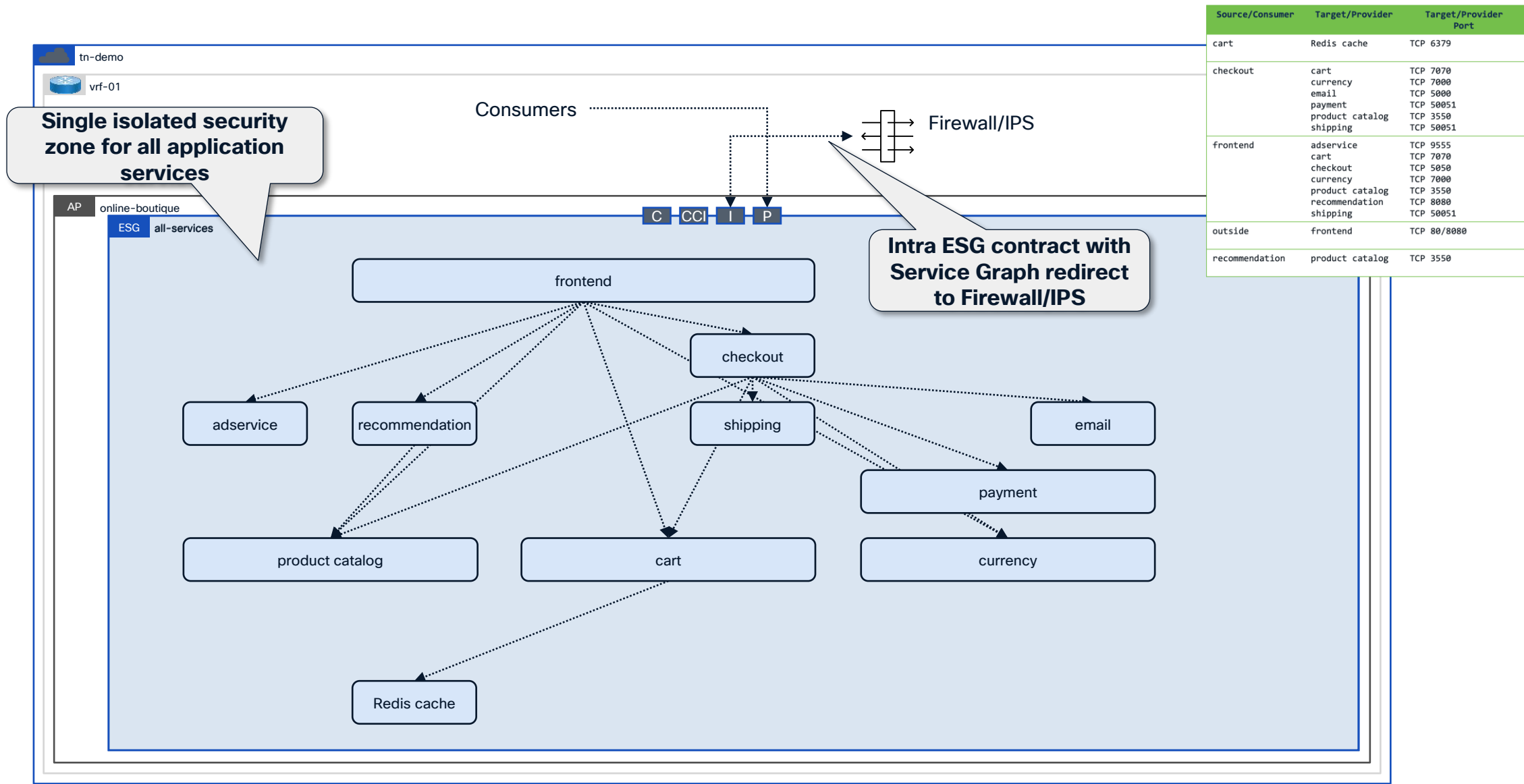
BRKSEC-2571

CISCO

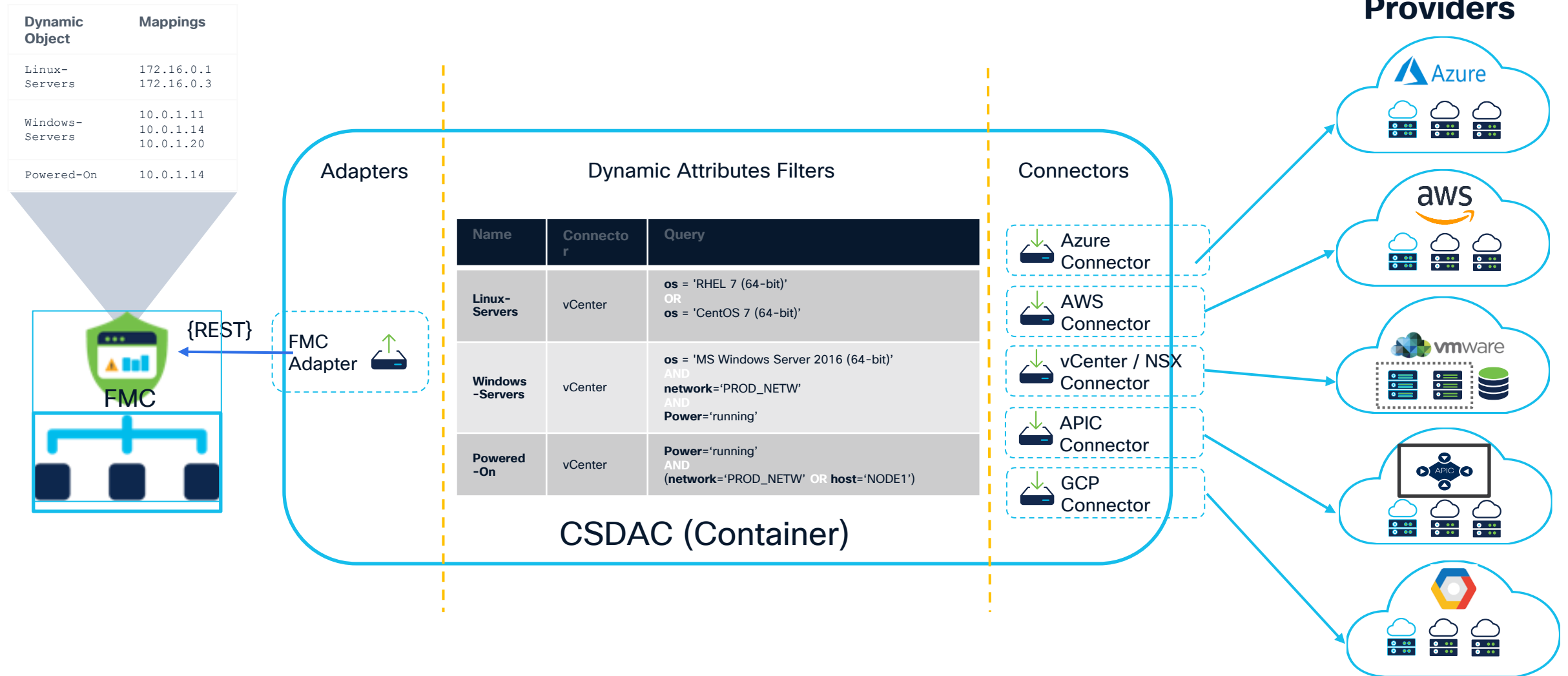
Leverage CSDAC to use EPG and ESG in your FTD policy



Use CSDAC to use Dynamic Group in FTD



Doing more with Dynamic Attributes Connector



Establish Trust – FTD/ASA can leverage SGTs

Action

Block

Time Range

None

Zones

Networks

VLAN Tags

Users

Applications

Ports

URLs

Dynamic Attributes

Inspection

Logging

Comments

Available Attributes

Q Search by name or value

Security Group Tag

Employees

Guests

Network_Services

PCI_Servers

Point_of_Sale_Systems

Production_Servers

Production_Users

Quarantined_Systems

Add to Source

Add to Destination

Selected Source Attributes (1)

Security Group Tags

Developers

Add a Location IP Address

Add

Selected Destination Attributes (2)

Security Group Tags

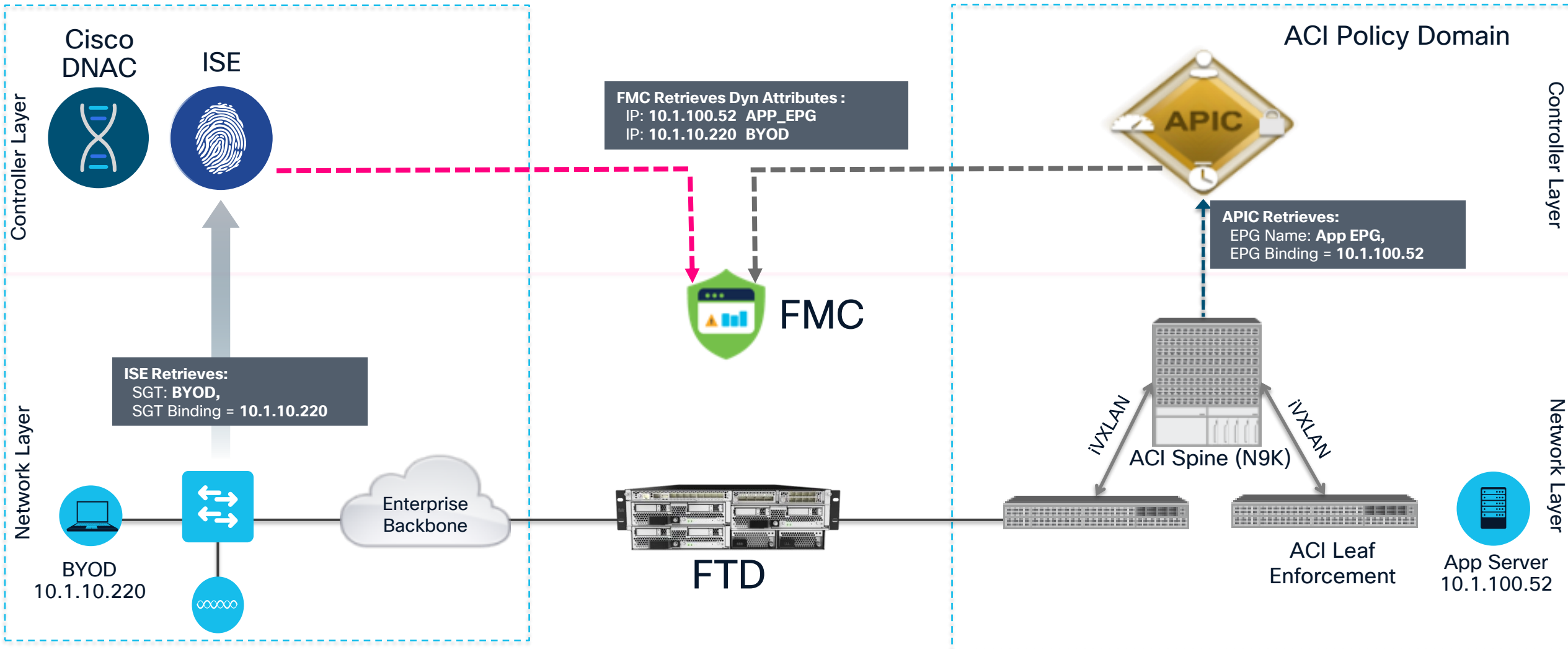
PCI_Servers

Point_of_Sale_Systems

Attributes of the same type (for example, SGT) match the rule if any attribute is matched.

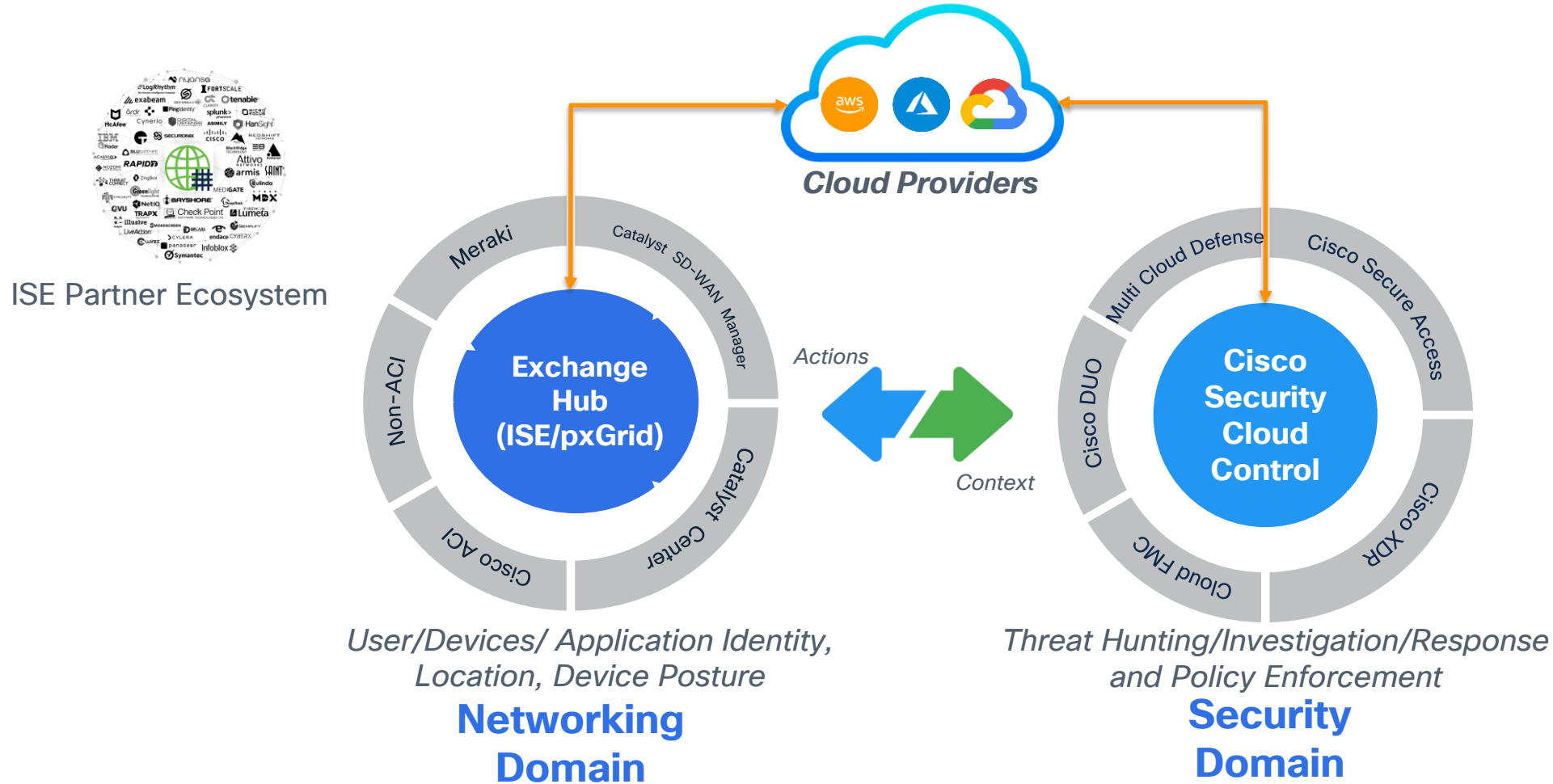
Attributes of different types match the rule only if all attributes are matched. [More info](#)

Use dynamic attributes to enforce trust

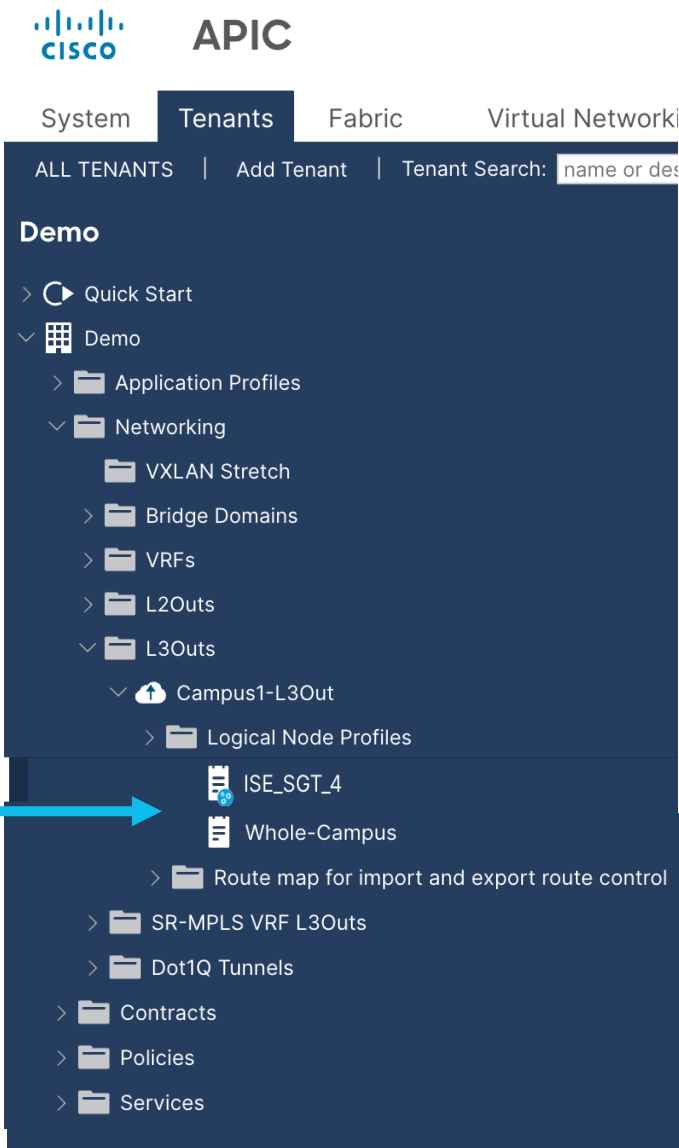


Alternatively establish trust with Cisco ISE

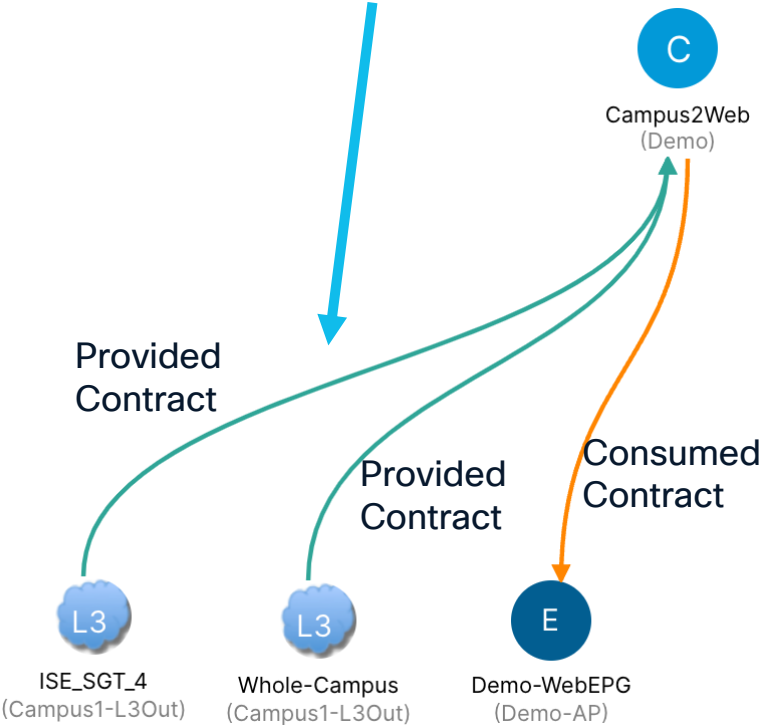
Normalizing and sharing context across domains



Context Sent to ACI



Newly added Group attached to existing Contract in APIC:



Walk before you run...

How do my applications communicate ?

Does the application team know how the application communicate ?



What are the services I must allow for this application to work?

Can I trust the Application team to let me know accurately when application changes impacting communication occurs ?

Dynamically securing the Workload Infrastructure

Profile relationships

Full visibility of all application conversations

Automated policy

Unified policy across for all application workloads

Deploy controls

Fully automated, dynamic attribute-based enforcement

Monitor compliance

Identify communications that violate policy and block if desired



Secure your application workloads:

Learn

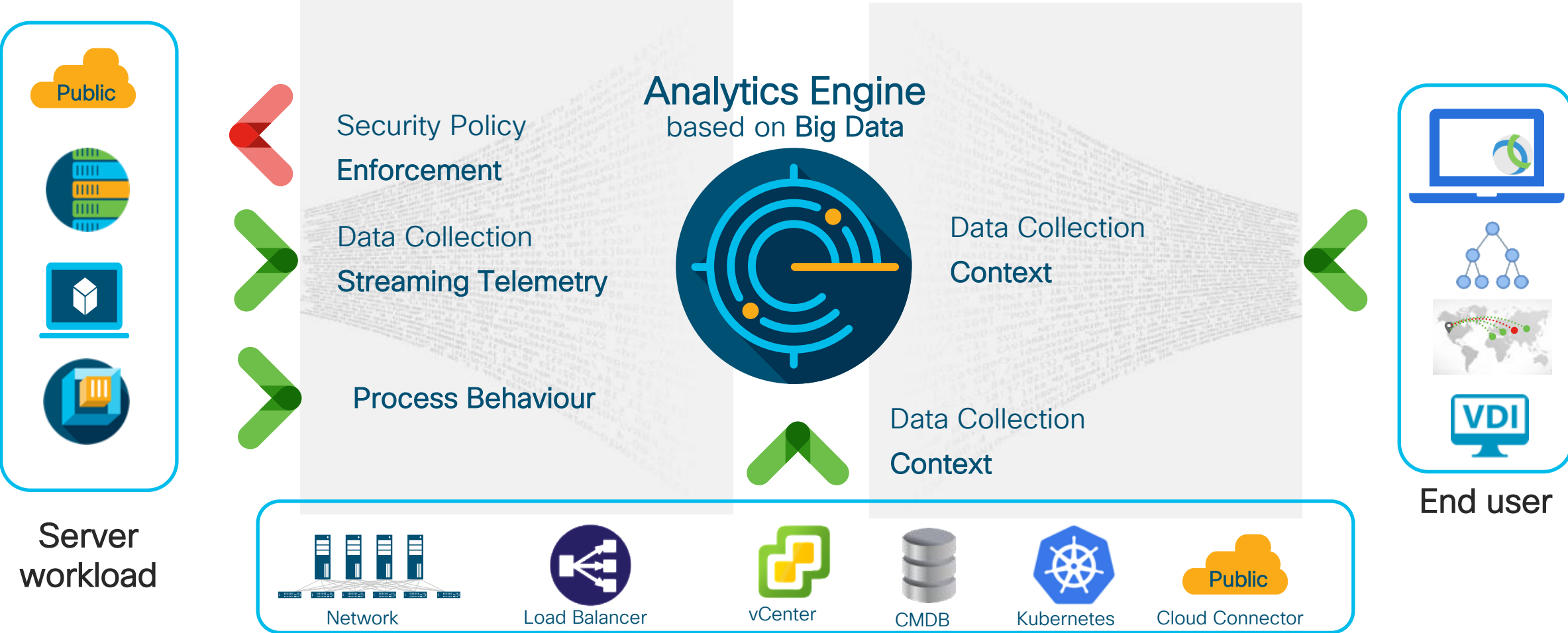
Build

Protect

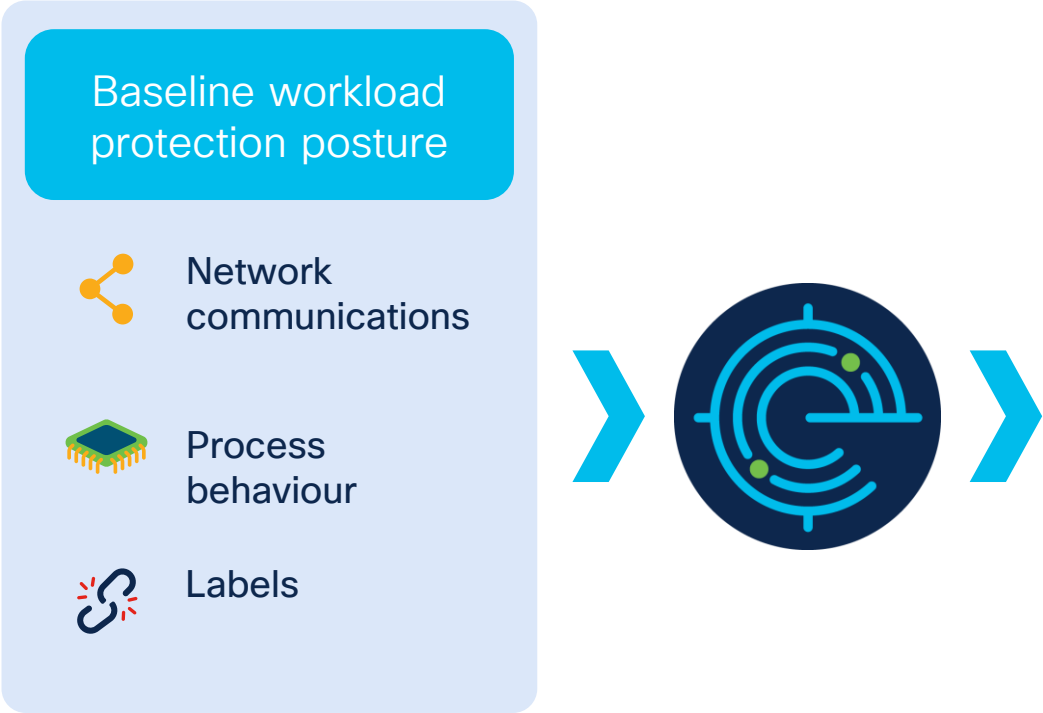
Assure



Secure Workload Architecture



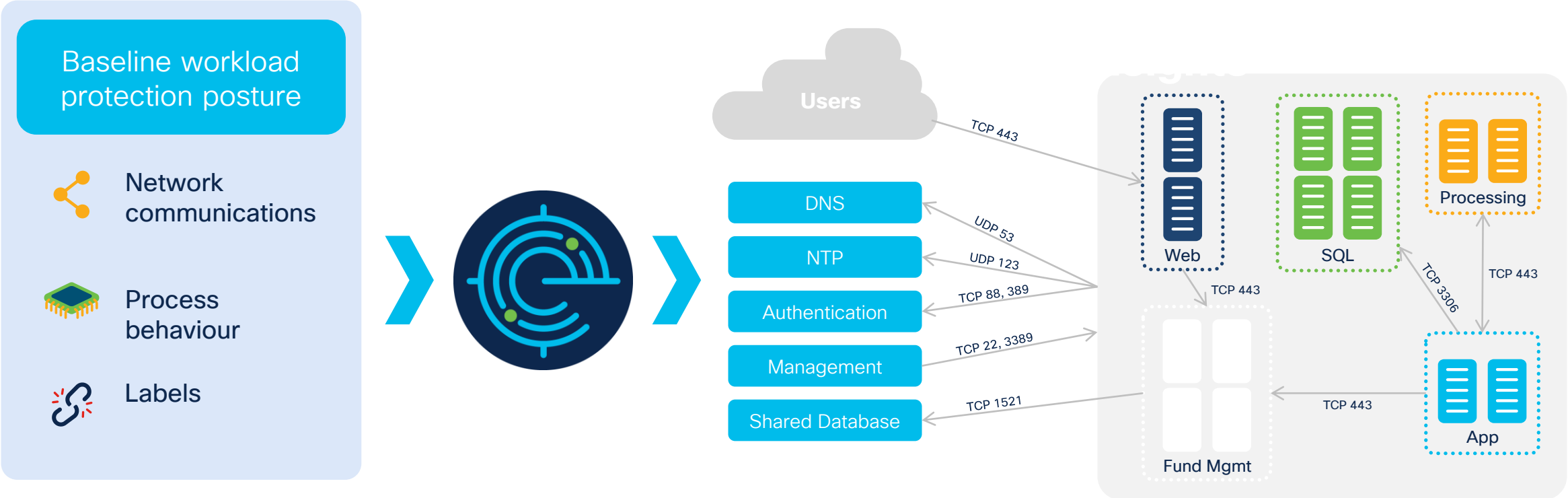
Automated Application Policy Discovery



Automated Application Policy Discovery



Automated Application Policy Discovery



Auto-generated policies

Policy list view

Cisco Secure Workload

Workspaces

DusLab-InvoiceSystem
PRIMARY
...
Version 9
View Version History

Last Run: Feb 6, 2:38 PM

Automatically Discover Policies

Matching Inventories 8
Policies 14
Filters 4
Conversations 271
Provided Services 1
Policy Analysis
Enforcement Status
Enforcement

Filter Policies ...
Run Quick Analysis
Add Policy

Absolute and Default Policies 13
Catch All DENY
Grouped
Ungrouped

	Rank ↑↓	Priority ↑↓	Action ↑↓	Consumer ↓	Provider ↑↓	Protocols And Ports ↑↓	
	Absolute	100	ALLOW	VPN	SLB APP	TCP : 1936	
	Default	100	ALLOW	VPN	SLB APP	TCP : 80 (HTTP)	
	Default	100	ALLOW	SLB DB	DB Tier	TCP : 3306 (MySQL)	
	Default	100	ALLOW	SLB APP	APP Tier	TCP : 8081	
	Default	100	ALLOW	Demo : DusLab : Applications : InvoiceSystem	Demo	UDP : 123 (NTP) ...2 more	
	Default	100	ALLOW	Demo : DusLab : Applications : InvoiceSystem	Demo : DusLab : SharedServices : DNS	UDP : 53 (DNS) ...1 more	
	Default	100	ALLOW	Demo	SLB APP	ICMP ...1 more	
	Default	100	ALLOW	Demo	SLB DB	Inactive	
	Default	100	ALLOW	Demo	APP Tier	Inactive	
	Default	100	ALLOW	DB Tier	DB Tier	TCP : 4567	
	Default	100	ALLOW	APP Tier	SLB DB	TCP : 3306 (MySQL)	

Rows per page 20
Download table data as JSON
Download table data as CSV

Auto-generated policies

- Canvas App view

Workspaces

DusLab-InvoiceSystem

PRIMARY

Version 9

View Version History

Matching Inventories 8

Policies 14

Filters 4

Conversations 271

Provided Services 1

Policy Analysis

Enforcement Status

Enforcement

Last Run: Feb 6, 2:38 PM

Automatically Discover Policies

Filter Policies ...

Run Quick Analysis

+ Policy

Demo

DusLab

Applications

InvoiceSystem

SLB APP

APP Tier

SLB DB

DB Tier

VPN

SharedServices

DNS

Scope InvoiceSystem

Full Name Demo:DusLab:Applications:InvoiceSystem

Primary App DusLab-InvoiceSystem

Query * Scope = invoicesystem

View Scope Details

> Services 0

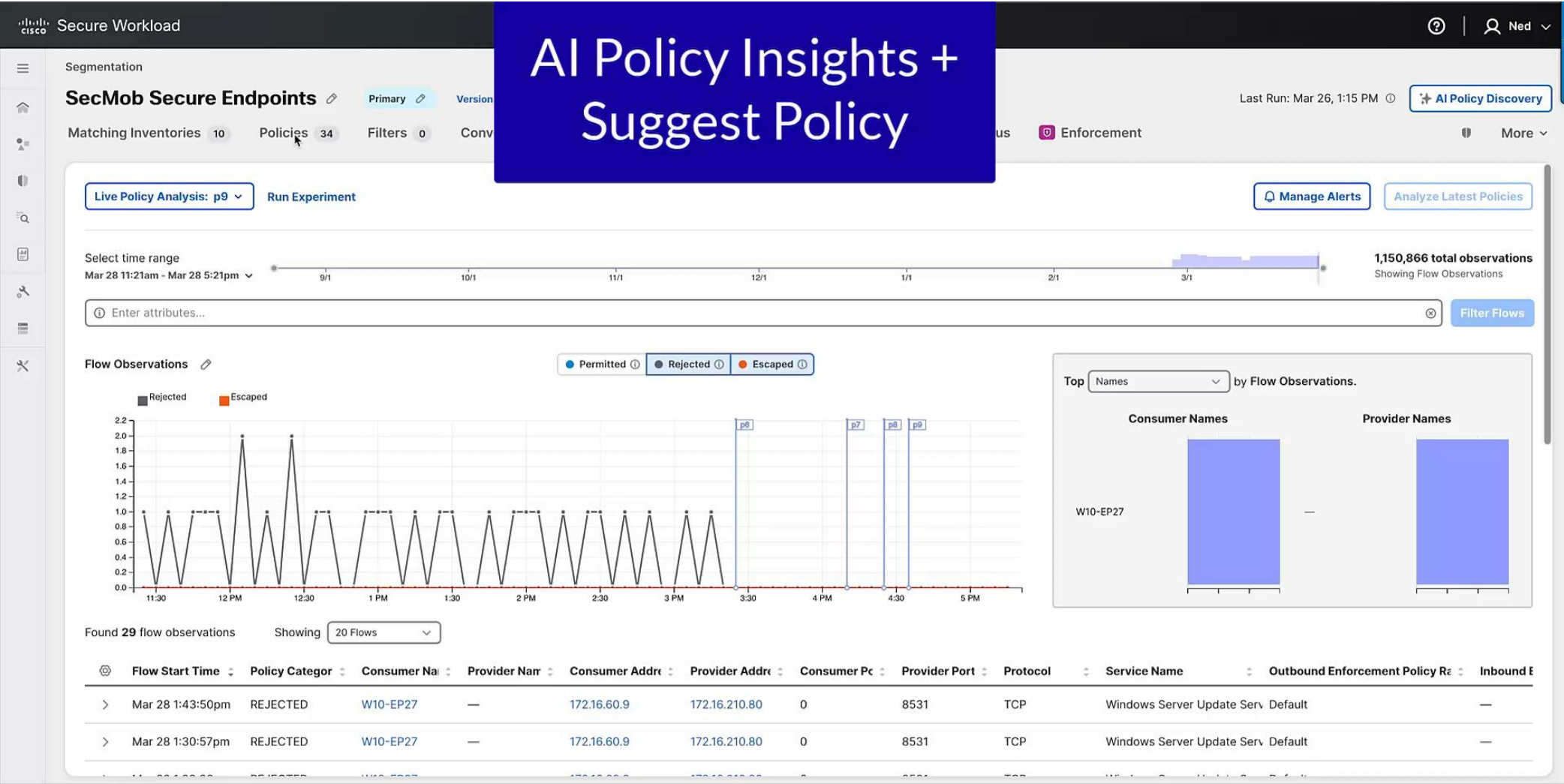
> Pods 0

> Workloads 8

> IP Addresses 0

Policy Lifecycle Mgmt. AI Policy Insights / Suggested Policy

Available Now -3.10.1



AI Suggested Policies

Available Now -3.10.4

Secure Workload

Primary Customer

Segmentation

AI Workspace

Primary

Version: v0

View Version History

Matching Inventories 73

Policies 6

Filters 0

Conversations

Provided Services

Policy Analysis

Enforcement Status

Enforcement

AI Discover Policies

Filter Policies ...

Quick Analysis

Add Policy

AI Suggested Policies 2

Grouped

Ungrouped

Catch All

Deny

Rank	Priority	Action	Consumer	Provider	Protocols and Ports	Actions
Default	100	Allow	Tetration : Workloads : Collector	Tetration	TCP : 8301 ...2 more	
Default	100	Allow	Tetration : Partners	Tetration : Campus	TCP : 1001	
Default	100	Allow	Tetration : Workloads : Adhoc	Tetration : Partners	TCP : 6404	

Rows per page 20

< 1 >

[Download table data as JSON](#)

[Download table data as CSV](#)



**One click away from
enforcement
with CSW**

Policy ready to be enforced

< Workspaces

DusLab-InvoiceSystem

PRIMARY

...

Version 9

View Version History

Last Run: Feb 6, 2:38 PM

Automatically Discover Policies

Matching Inventories 8

Policies 14

Filters 4

Conversations 271

Provided Services 1

Policy Analysis

Enforcement Status

Enforcement

Enforced Policy Version: [p39]

Manage Alerts

Stop Policy Enforcement

Enforce Policies

Select time range

May 16 10:04am - May 16 4:04pm

7/1

10/1

1/1

4/1

7/1

10/1

1/1

4/1

94,539,284 total observations

Showing Flow Observations

Enter attributes...

Filter Flows

Filtered

Flow Observations

Permitted

Rejected

Escaped

Permitted

Rejected

Escaped

800

700

600

500

400

300

200

100

0

10:30

11 AM

11:30

12 PM

12:30

1 PM

1:30

2 PM

2:30

3 PM

3:30

4 PM

Found 46,599 Flow Observations

Show 20

Timestamp

Policy Categories

Outbound Policy Rank

Inbound Policy Rank

Consumer Name

Provider Name

Consumer Address

Provider Address

Consumer Port

Provider Port

Protocol

May 16 10:34:00am

PERMITTED

Default

Default

ciscolabssiwapphaproxy1db

ciscolabssiwappdb2

10.1.96.25

10.1.96.19

47110

3306

TCP

May 16 10:34:00am

PERMITTED

Default

Default

ciscolabssiwapphaproxy1db

ciscolabssiwappdb2

10.1.96.25

10.1.96.19

47134

3306

TCP

May 16 10:34:00am

ESCAPED

Catch All

Catch All

ciscolabssiwappdb2

Unknown

10.1.96.19

10.49.166.11

44458

5640

TCP

May 16 10:34:00am

PERMITTED

Default

Default

ciscolabssiwapphaproxy1db

ciscolabssiwappdb3

10.1.96.25

10.1.96.20

55552

3306

TCP

May 16 10:34:00am

ESCAPED

Catch All

Catch All

ciscolabssiwappdb3

Unknown

10.1.96.20

10.49.166.9

58560

5640

TCP

Top Names

contributing to the selected Flow Observations.

Consumer Names

Provider Names

ciscolabssiw...

ciscolabssiw...

ciscolabssiw...

ciscolabssiw...

ciscolabssiw...

ciscolabssiw...

ciscolabssiw...

ciscolabssiw...

Unknown

ciscolabssiw...

ciscolabssiw...

ciscolabssiw...

ciscolabssiw...

ciscolabssiw...

ciscolabssiw...

ciscolabssiw...

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-2571

Run Policy Experiment

Workspaces

DusLab-InvoiceSystem

Matching Inventories 8

Policies 14

Filters

Live Policy Analysis: p39

Select time range

May 16 10:07am - May 16 4:07pm 7/1

Enter attributes...

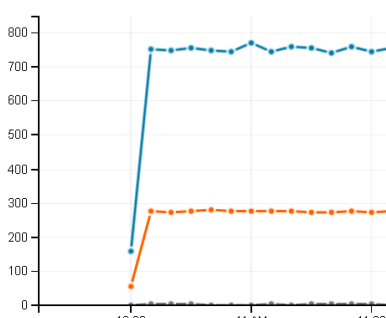
Filtered

Flow Observations

Permitted

Rejected

Escaped



Found 47,211 Flow Observations

Show 20

Timestamp ↑↓	Policy Categories ↑↓
May 16 10:34:00am	PERMITTED
May 16 10:34:00am	PERMITTED
May 16 10:34:00am	ESCAPED

Run Experiment

By running an experiment you can verify the compliance of the past network traffic with respect to current live policies, **version p39**.

Name

CL US23 super screenshot

Start Date

05/14/2023 12:00 PM

End Date

05/15/2023 12:00 PM

Cancel

Run

Run: Feb 6, 2:30

Automatically Discover Policies

Alerts

Run Experiment

Analyze Latest Policies

94,539,896 total observations

Showing Flow Observations

4/1

Provider Names

Unknown	
ciscolabssiw...	
ciscolabssiw...	
ciscolabssiw...	
ciscolabssiw...	
ciscolabssiw...	
ciscolabssiw...	

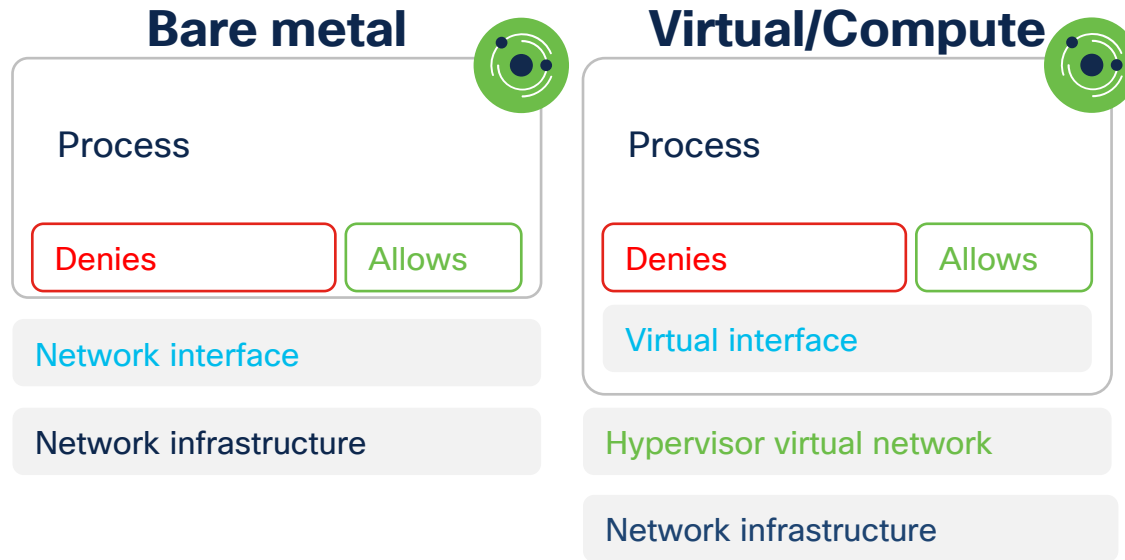
Service Name ↑↓	Inbound Enforcement Policy Ra	Our
MySQL	Default	De
MySQL	Default	De
Secure Workload	Catch All	Ca

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-2571



How does CSW enforce the Policy ?

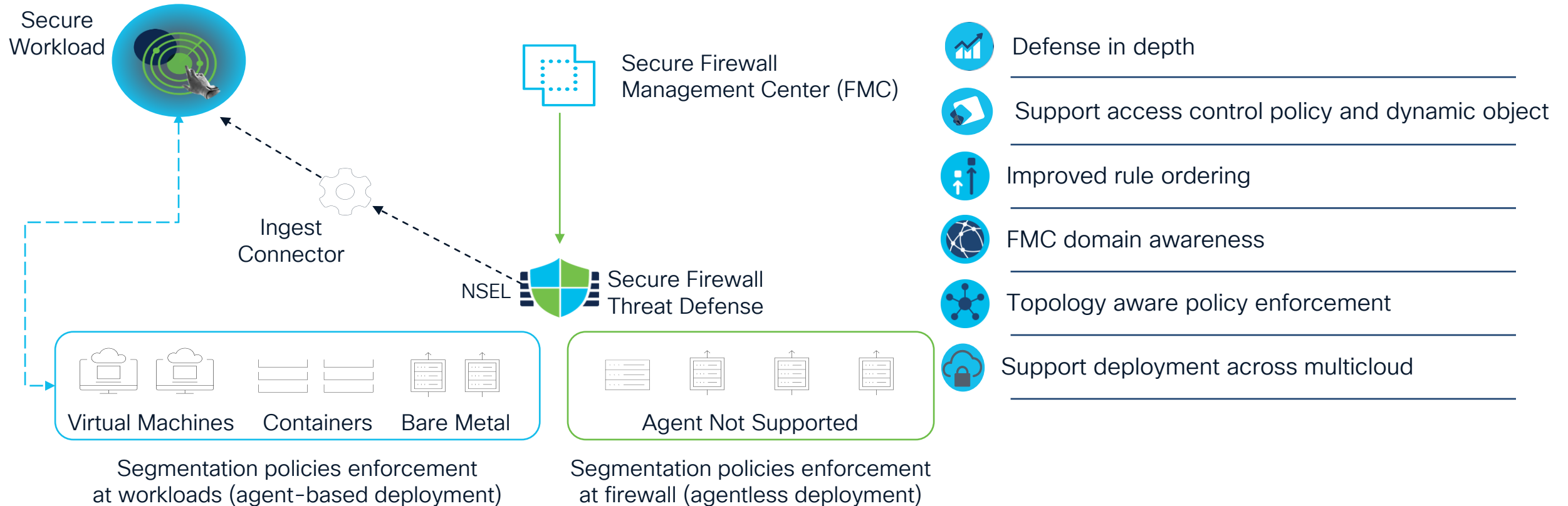


Intent is rendered as security rules in native environment

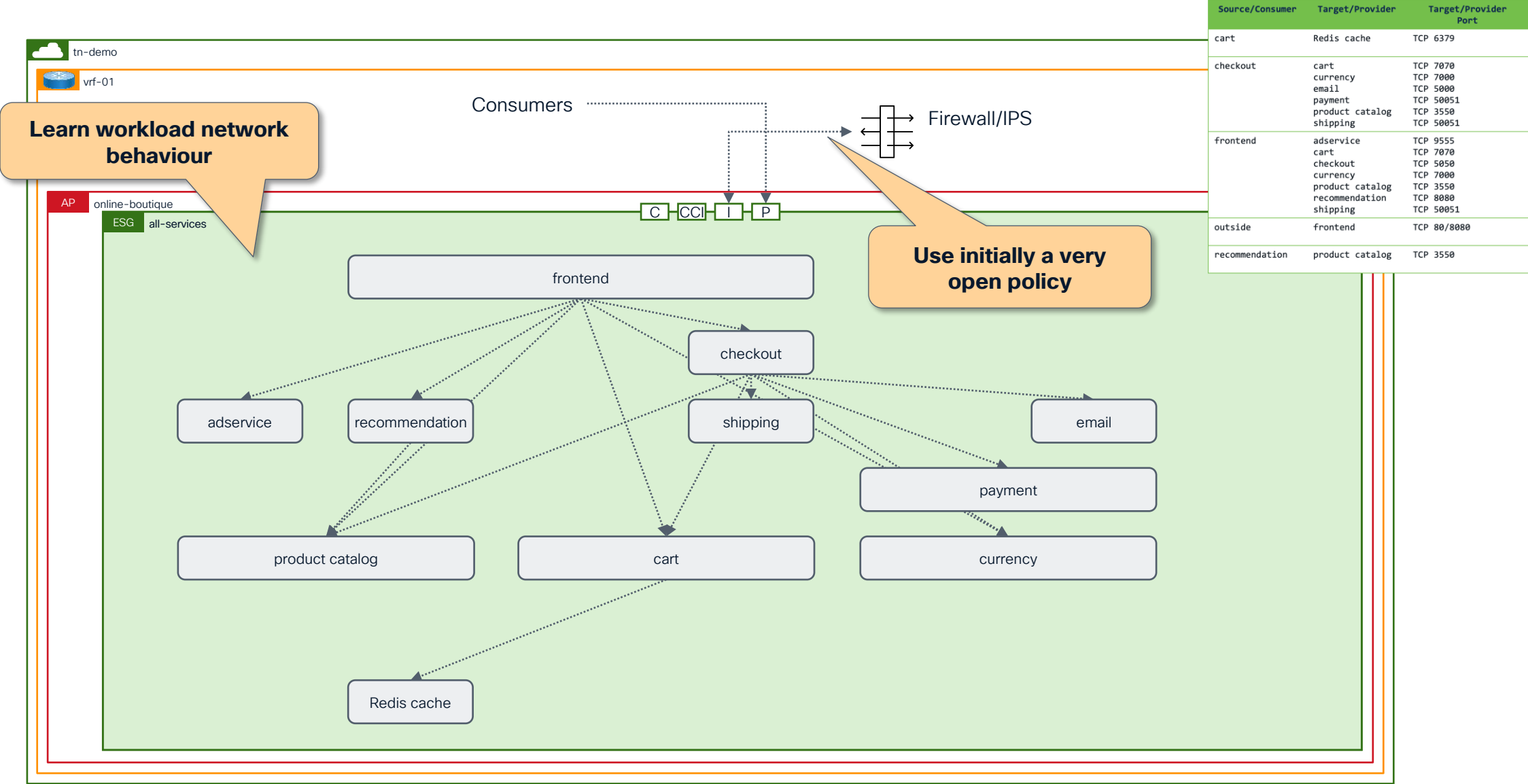
- IP sets on Linux servers
- Windows Advanced Firewall or Windows Filtering Platform on Windows servers

CSW-FMC Integration And Enforcement

Defense-in-depth Use Case

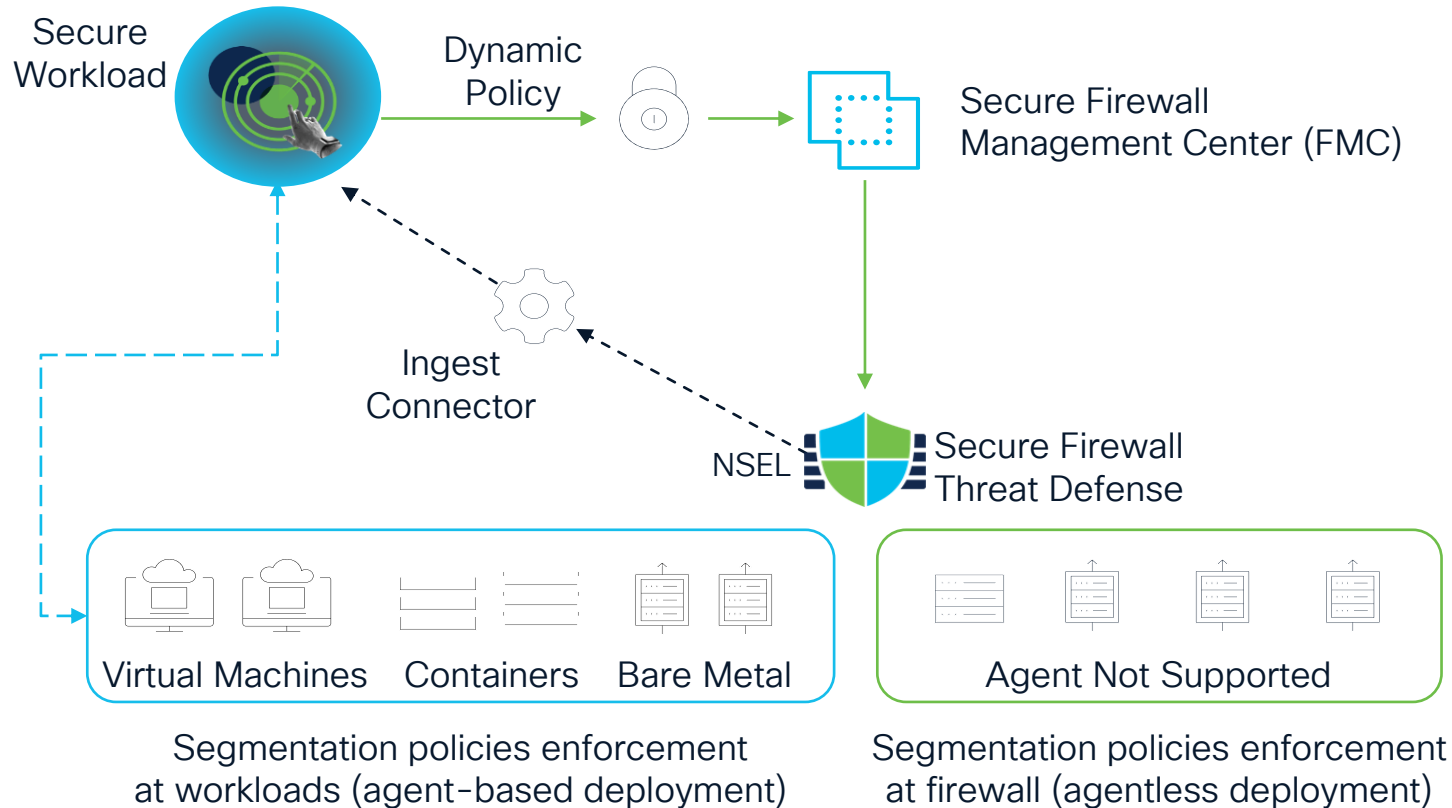


Use FTD to generate Netflow data for CSW



CSW-FMC Integration And Enforcement

Defense-in-depth Use Case



Defense in depth



Support access control policy and dynamic object



Improved rule ordering



FMC domain awareness

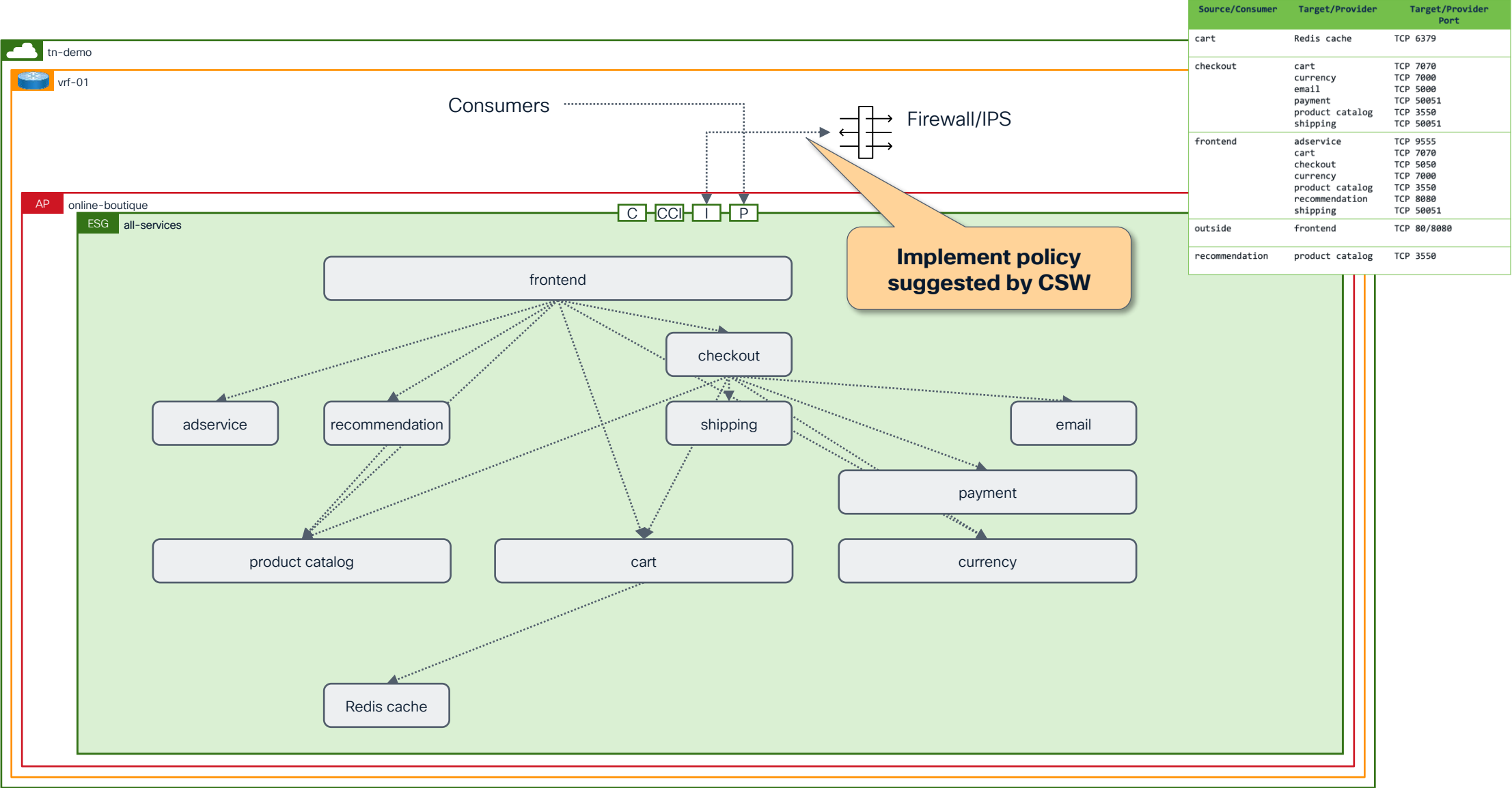


Topology aware policy enforcement

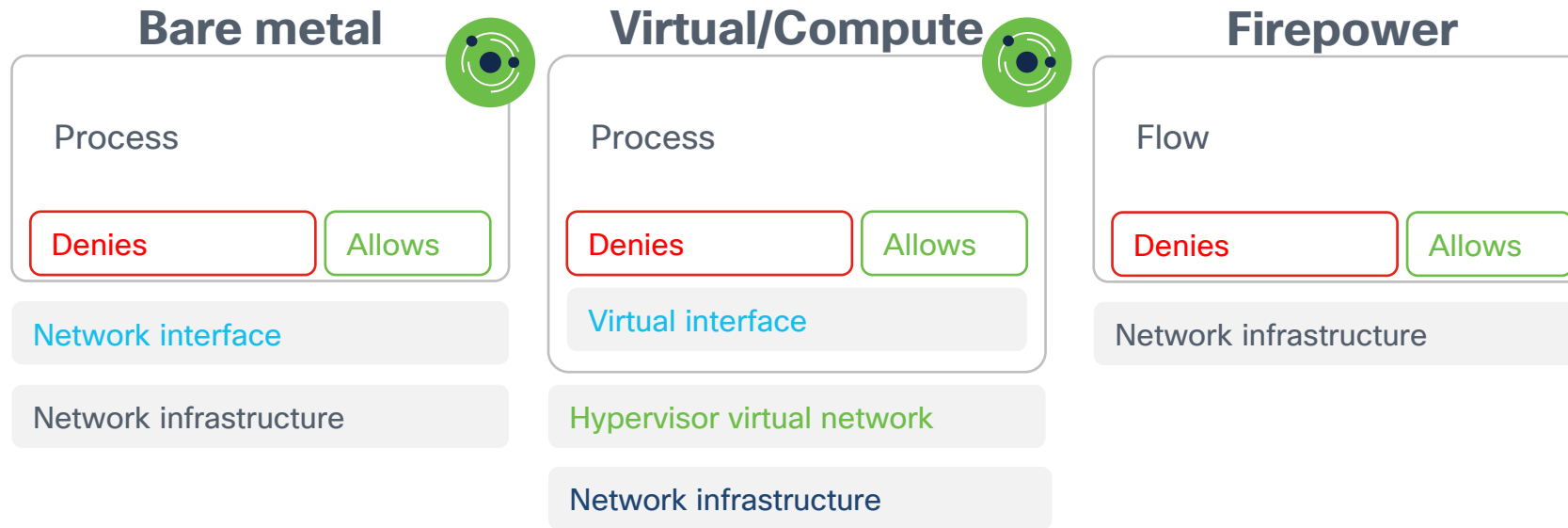


Support deployment across multicloud

Enforce automatically Policy from CSW



How does CSW enforce the Policy ?



Intent is rendered as security rules in native environment

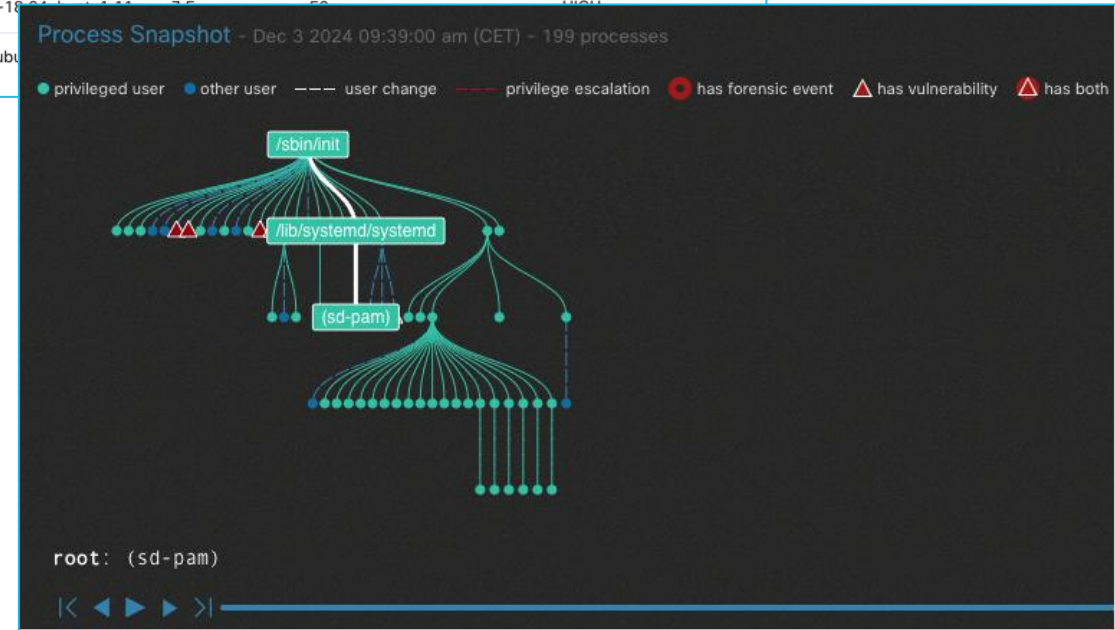
- IP sets on Linux servers
- Windows Advanced Firewall or Windows Filtering Platform on Windows servers
- Access Policies in Firepower Threat Defense

Workload Runtime Observability

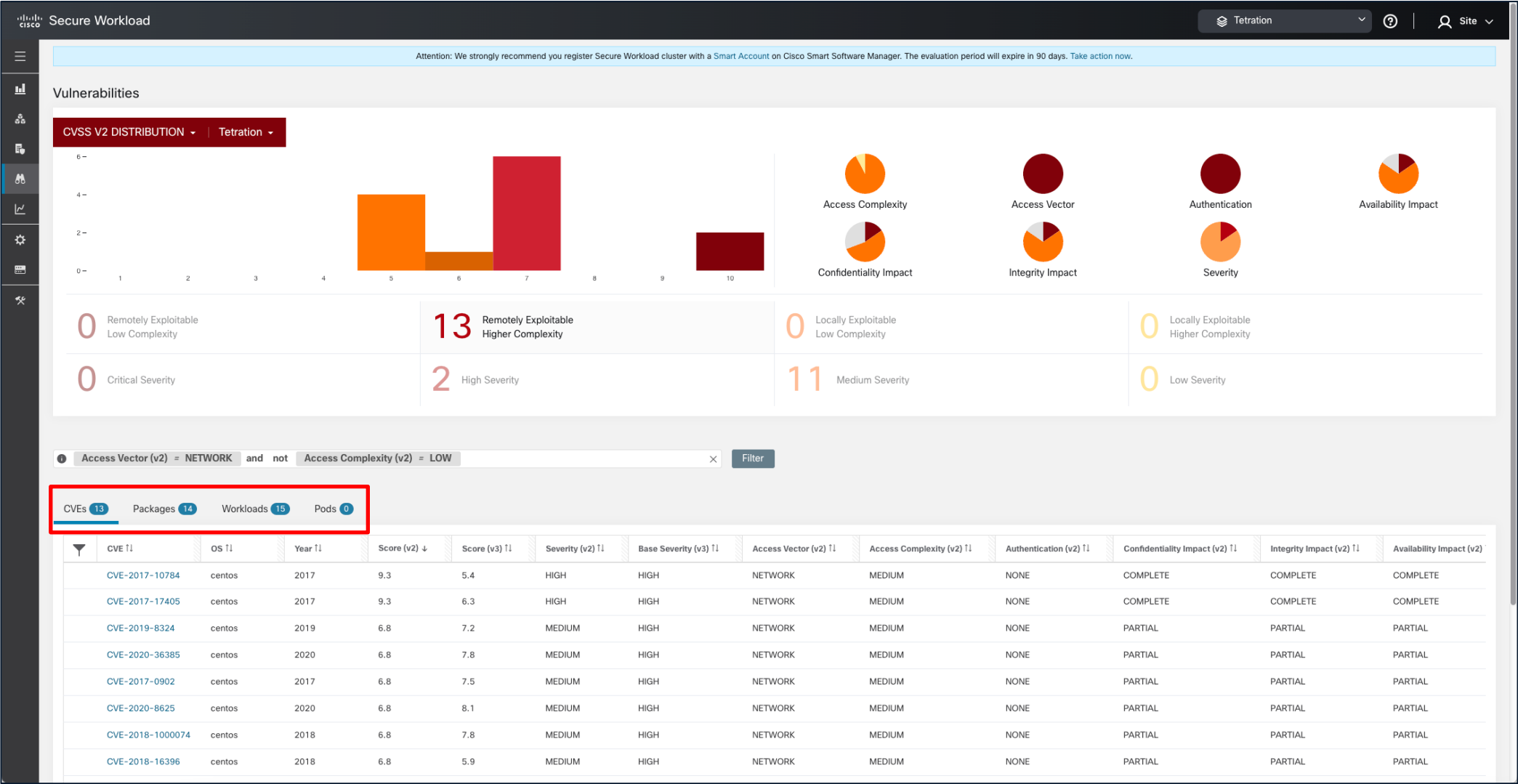
In-Depth Visibility of Workload Estate

- Processes information
 - Resource consumption
 - Malicious processes
- Software packages
 - Vulnerabilities
 - Risk-Based information
- Process-tree and forensics

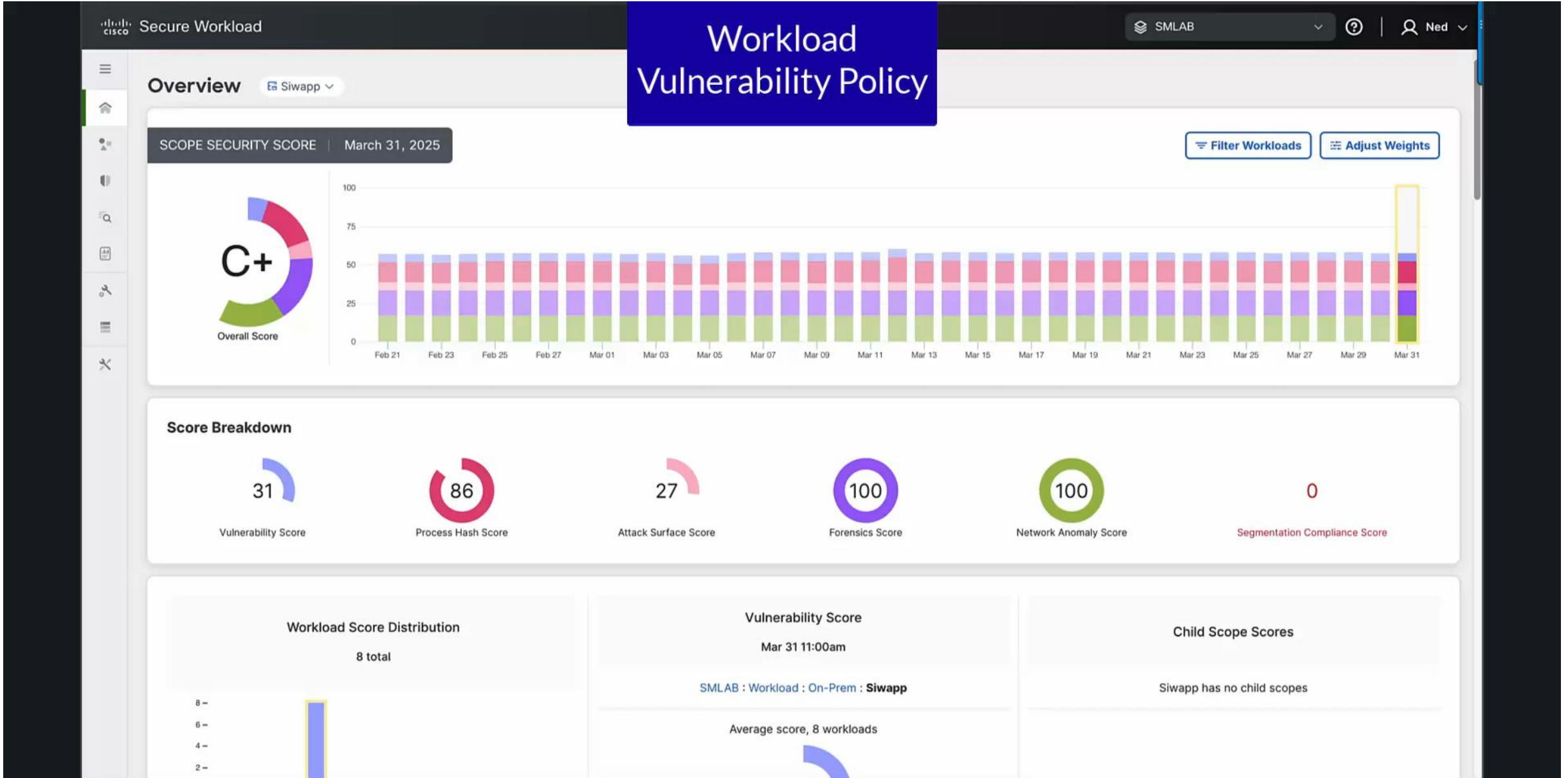
Vulnerabilities						
Enter attributes... × Filter						
Displaying 417 of 417						
▼	CVE ↓	Package Name ↑↓	Package Version ↑↓	Score (V3) ↑↓	Cisco Security Risk Score ↑↓	Base Severity (V3) ↑↓
	CVE-2024-7592	libpython2.7	2.7.17-1-18.04ubuntu1.11	7.5	50	HIGH
	CVE-2024-7592	libpython2.7-minimal	2.7.17-1-18.04ubuntu1.11	7.5	50	HIGH
	CVE-2024-7592	libpython2.7-stdlib	2.7.17-1-18.04ubuntu1.11	7.5	50	HIGH
	CVE-2024-7592	python2.7	2.7.17-1-18.04ubuntu1.11	7.5	50	HIGH
	CVE-2024-7592	python2.7-minimal	2.7.17-1-18.04ubuntu1.11	7.5	50	HIGH
	CVE-2024-7264	curl	7.58.0-2ubuntu1.1	7.5	50	HIGH



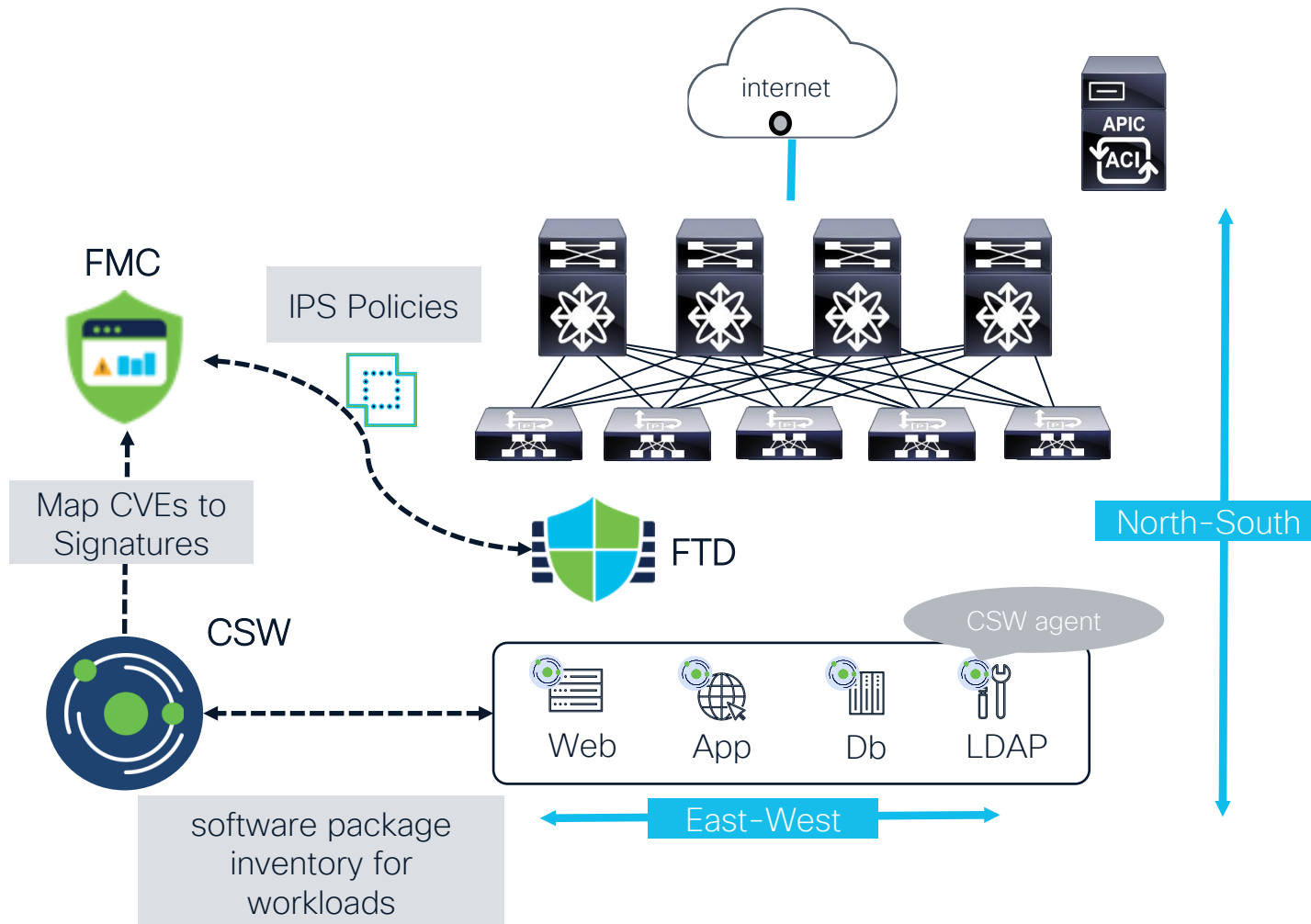
Cisco Secure Workload



Differentiator: Prioritized Vulnerability Policy



Virtual patching - Cisco Secure Firewall



- Secure Workload agents collect CVE data from workloads
- Publish specific CVE data to Firewall Management Center
- Use Firewall recommendations to generate precise IPS policy
- Apply precise IPS policy to protect against CVE exploits

Virtual patching – Cisco Secure Firewall

CSW: Manage > Connector > FMC > Virtual Patching

tme-dc-fmc

SettingsSegmentationVirtual PatchingEvent Log

Rules

Q Search by Rule Name or Description

Filter

Add Rule

	Rule Name	Description	Filter	Query	Created At	Actions
	critical-cves	invoice app	<div>...:Data Centers:Production:Invoice-App</div> <div>critical-cves</div>	<div>CVE Score v3 ≥ 9</div> and <div>Attack Vector (CVSS v3) = NETWORK</div>	May 1 2023 08:18:35 pm (EDT)	<div></div> <div></div>

Virtual patching rule to publish CVEs:
For invoice app workloads, publish CVEs with CVSS score >= 9 and attack vector as network

Workloads with Published CVEs

1 Enter attributes...

Filter

Rules 1, Workloads 7

Rule Name ↕	Workload Name ↕	Exported	
critical-cves	dev-siwapp-db-3	CVEs List	⋮
critical-cves	stage-siwapp-app-3	CVEs List	⋮
critical-cves	stage-siwapp-app-2	CVEs List	⋮
critical-cves	stage-siwapp-haproxy-db	CVEs List	⋮
critical-cves	dev-siwapp-db-2	CVEs List	⋮
critical-cves	stage-siwapp-app-1	CVEs List	⋮
critical-cves	stage-siwapp-haproxy-app	CVEs List	⋮

FMC: Analysis > Hosts > Third party vulnerabilities

	☐	Vulnerability Source ×	Vulnerability ID ×	↓ IP Address ×	Port ×	Bugtraq ID ×	CVE ID ×	SVID ×	Snort ID ×	Title ×	Description ×
▼	☐	CSW d5341dbb-4b4f-31f8-5845-111fb6fbc537 1	2000042	192.168.18.7			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030004Z
▼	☐	CSW d5341dbb-4b4f-31f8-5845-111fb6fbc537 1	2000073	192.168.18.6			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030004Z
▼	☐	CSW d5341dbb-4b4f-31f8-5845-111fb6fbc537 1	2000117	192.168.17.10			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030005Z
▼	☐	CSW d5341dbb-4b4f-31f8-5845-111fb6fbc537 1	2000052	192.168.16.7			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030004Z
▼	☐	CSW d5341dbb-4b4f-31f8-5845-111fb6fbc537 1	2000027	192.168.16.6			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030004Z
▼	☐	CSW d5341dbb-4b4f-31f8-5845-111fb6fbc537 1	2000116	192.168.16.5			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030005Z
▼	☐	CSW d5341dbb-4b4f-31f8-5845-111fb6fbc537 1	2000089	192.168.15.10			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030005Z

ACI Integration

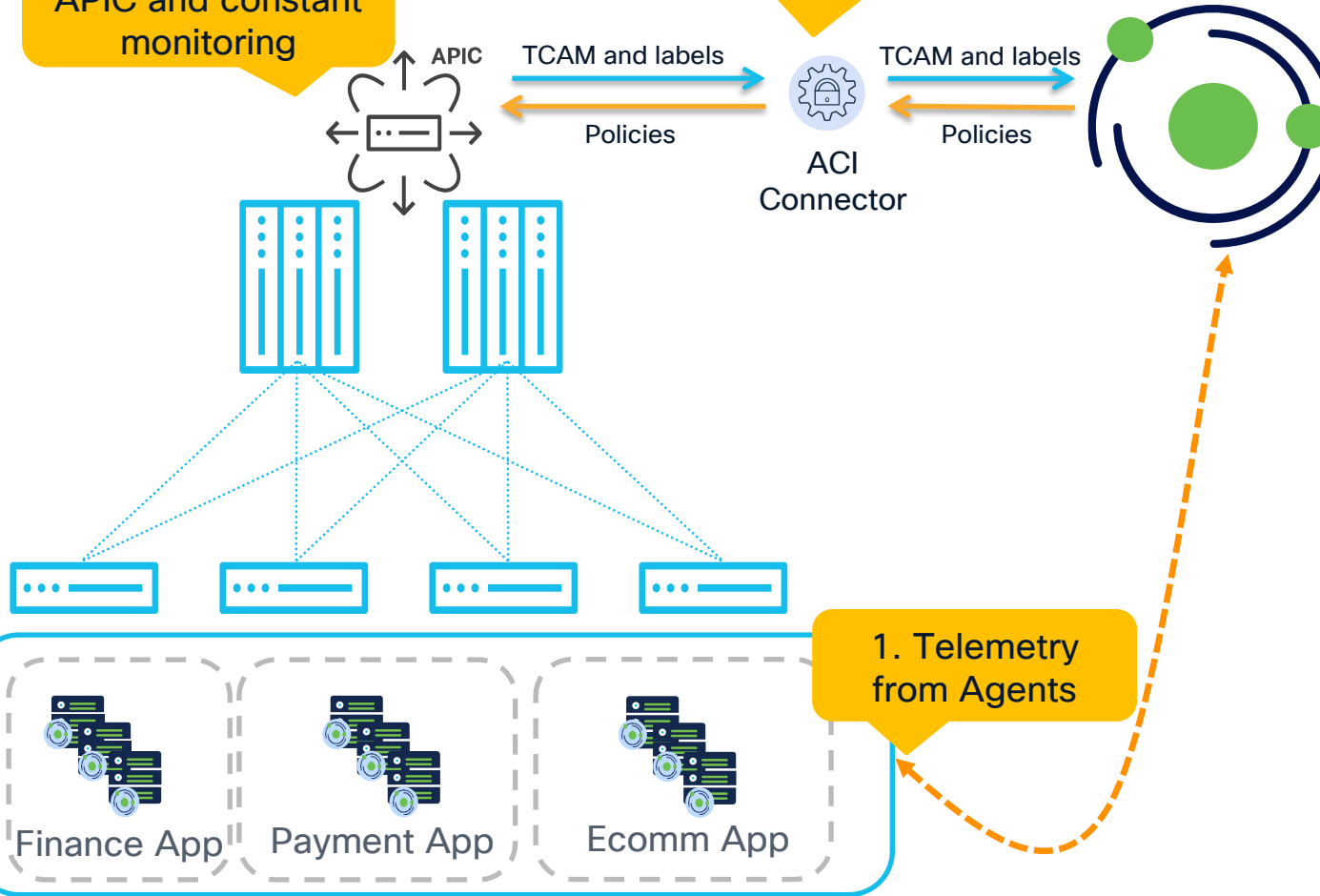
New
4.0

High Level Architecture

3. Enforcement on APIC and constant monitoring

2. Scope to VRF Mapping and Discovery

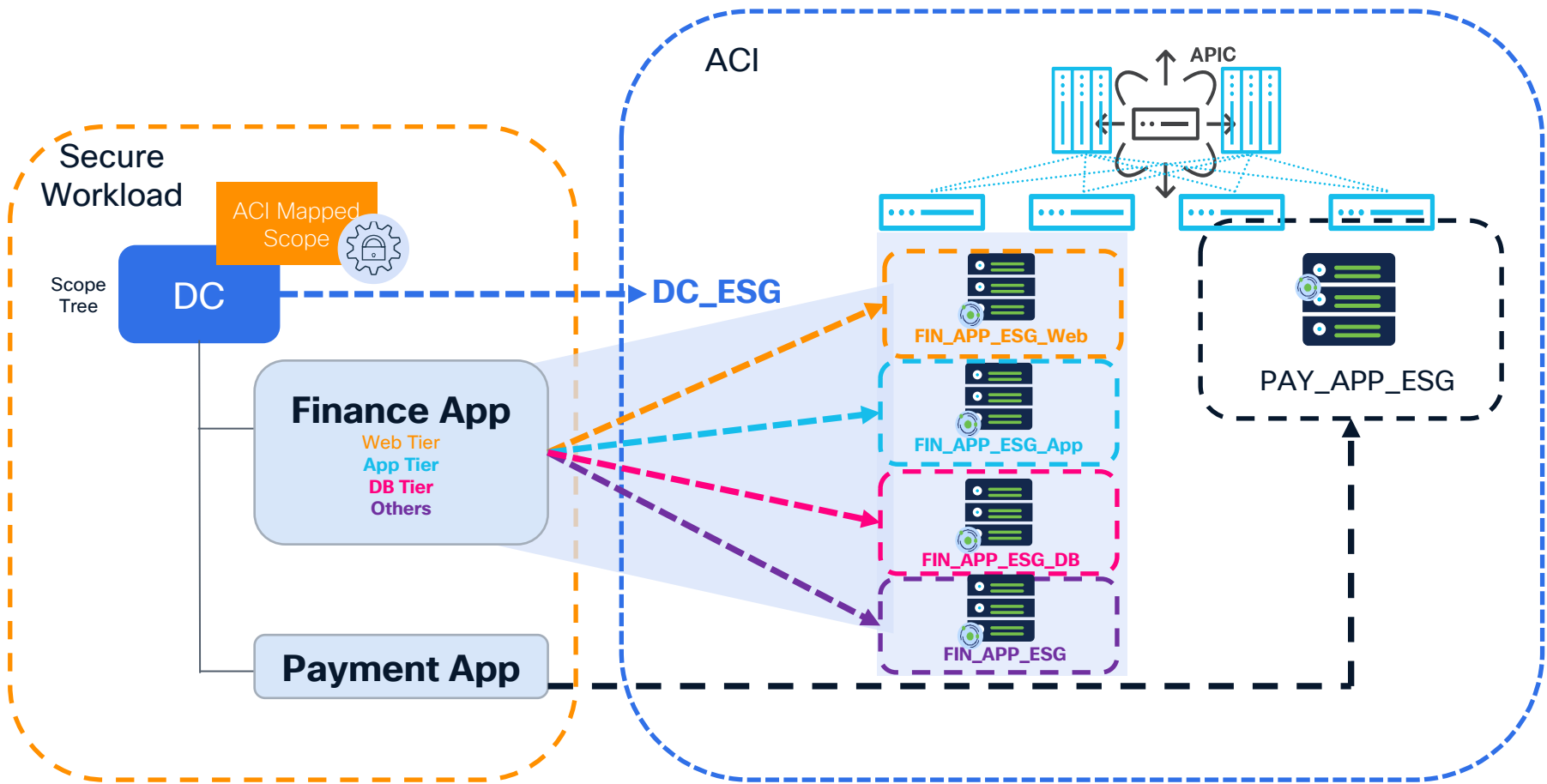
1. Telemetry from Agents



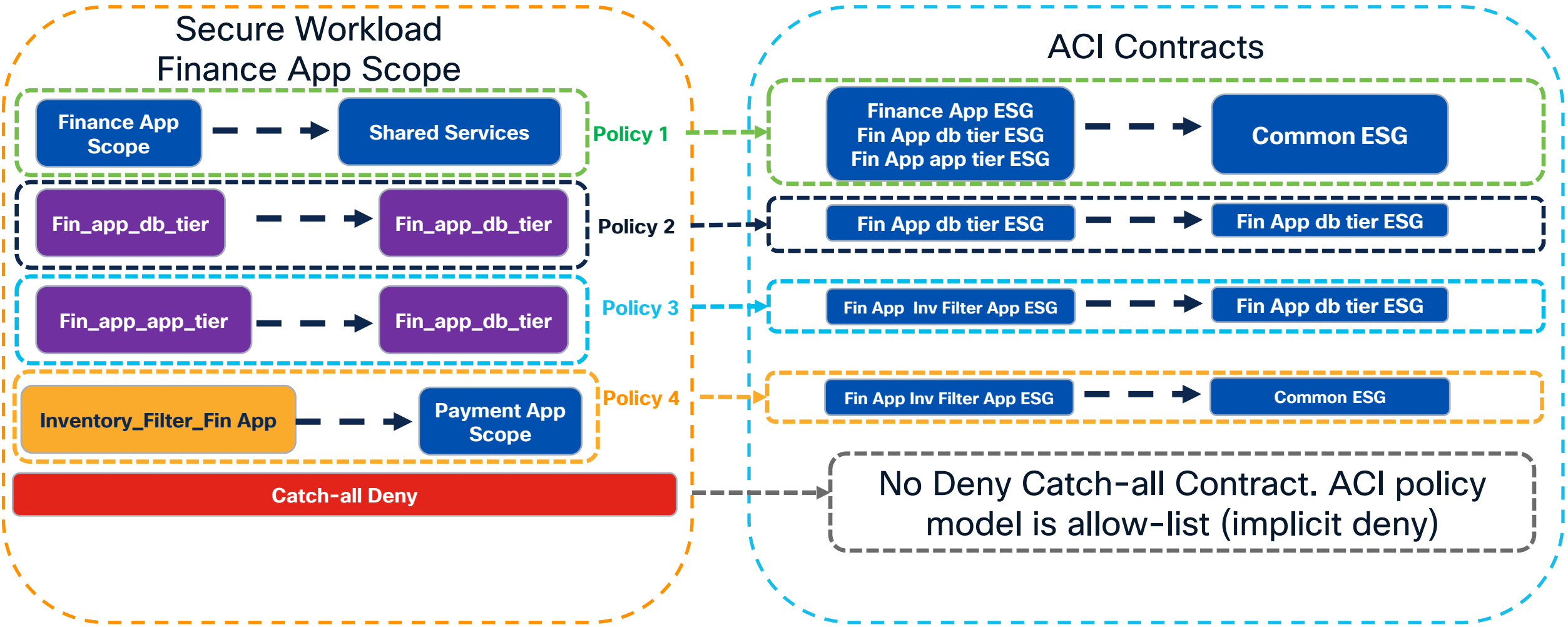
Integration Highlights

- Telemetry via agents installed on workloads
- New ACI Connector (Secure Workload):
 - Workload Discovery
 - Policy optimization and TCAM monitoring
 - Dynamic push ESG contracts on ACI

Secure Workload Objects and Policy Mapping



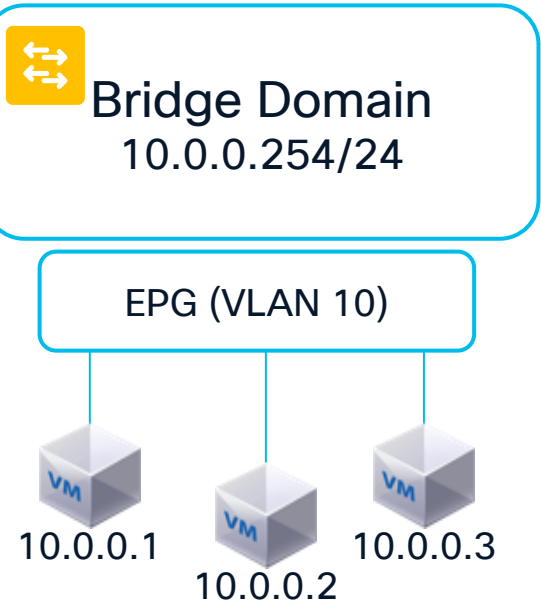
Secure Workload Policies to ACI Contracts



Network Centric & Application Centric Design

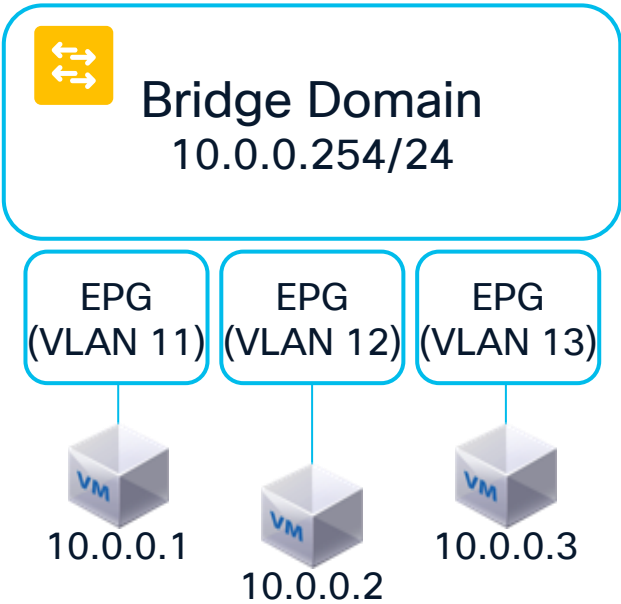
Network Centric

A security group
in 1 subnet



Need more granular
security group

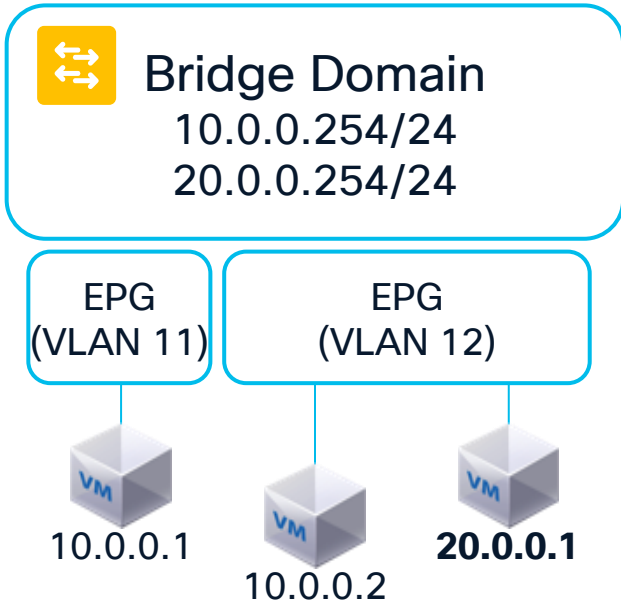
Multiple security groups
in 1 subnet



What if multiple subnets
need to share the same
security rules?

Application Centric

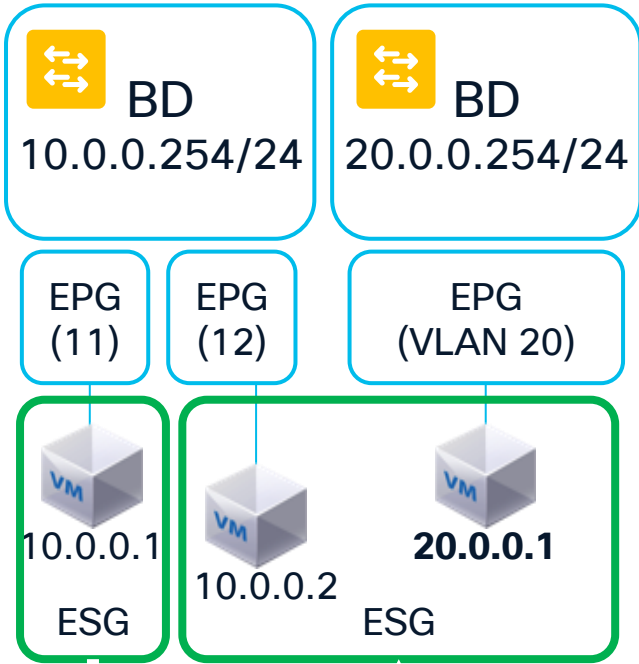
Security groups across
subnets



Sharing a broadcast domain
brings another security
concern

== 5.0 ==
Endpoint Security Group
(ESG)

Security groups **across**
bridge domains



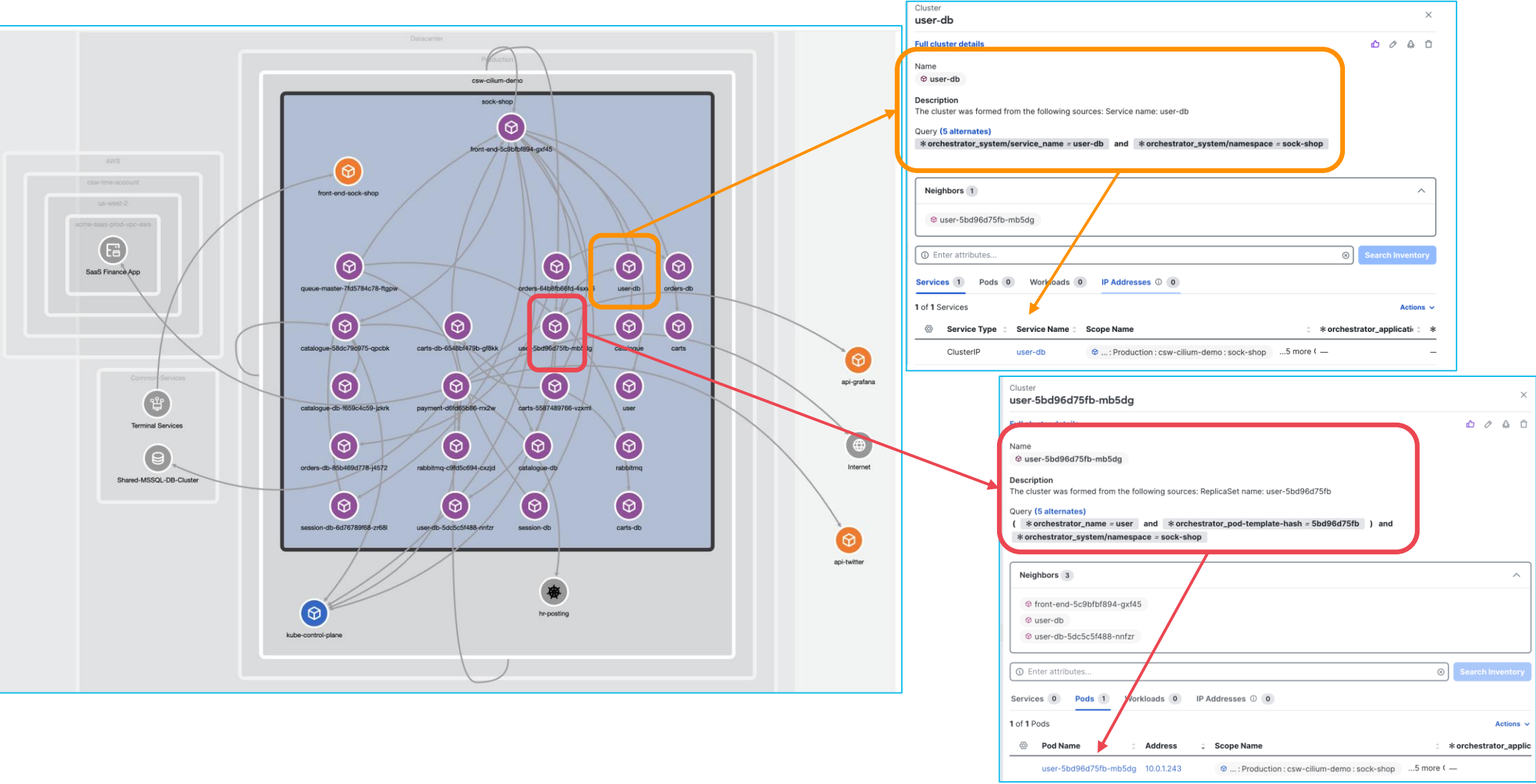
Contract

Flexible security grouping

**Bare Metal...virtual... What
about Containers ???**

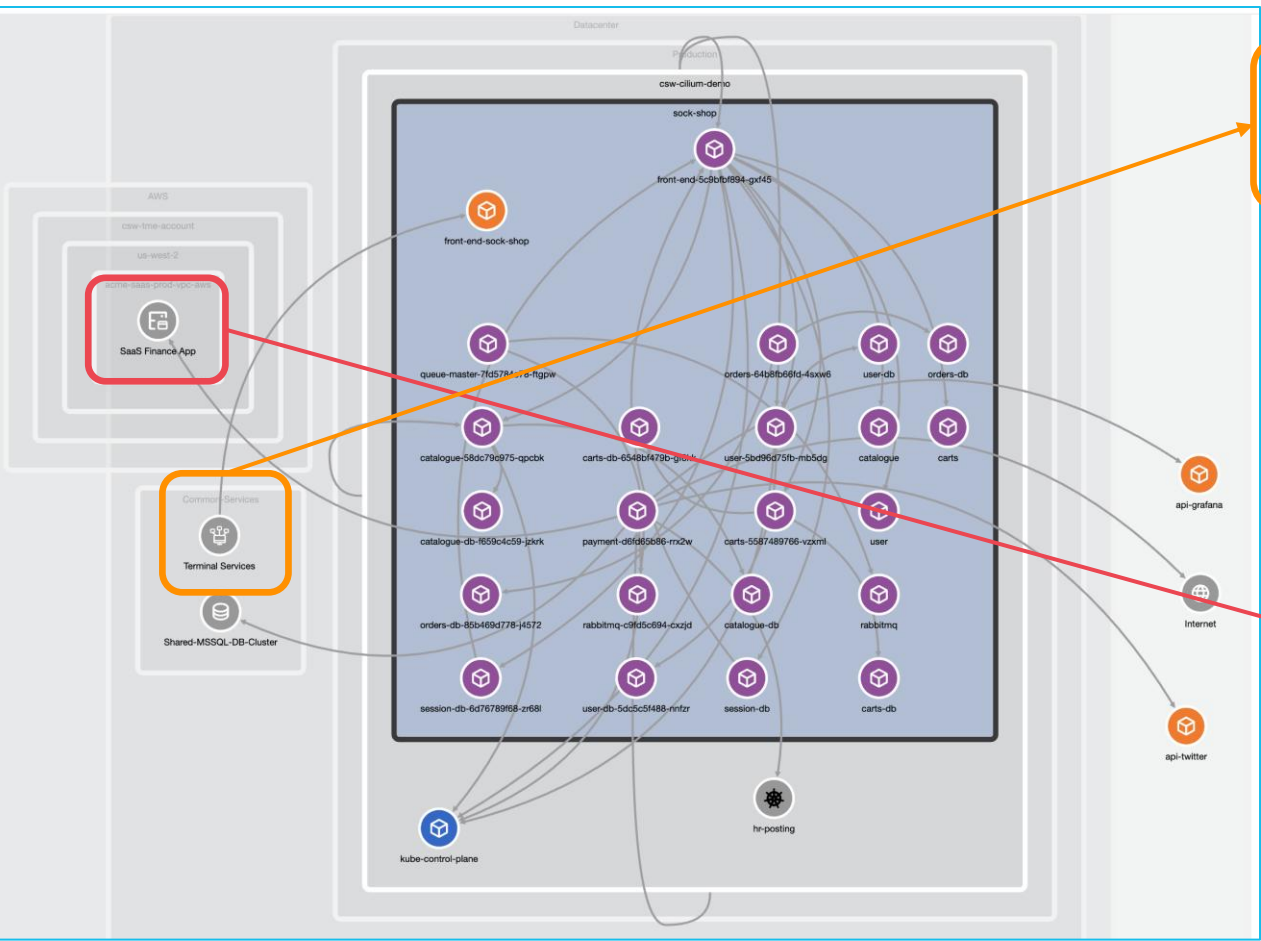
Application Dependency Mapping

Kubernetes Policy Discovery – Pod/Services/Namespaces/Node/Cluster and More!



Application Dependency Mapping

Kubernetes Policy Discovery – End-to-End Discovery



Scope

... : Common-Services : Terminal Services

Full scope details

Name

... : Common-Services : Terminal Services

Primary Workspace

Terminal Services

Query

* application = terminal-service

Enter attributes...

Search Inventory

Services 0 Pods 0 Workloads 5 IP Addresses 1

5 of 5 Workloads

Hostname	Address	* application	* compliance	* compliance_functi	* data_type	* env
h4-dmz-rdshost2	172.20.0.72	terminal-service	nis2	—	—	cor
h4-dmz-rdshost1	172.20.0.71	terminal-service	nis2	—	—	cor

Scope

... : acme-saas-prod-vpc-aws : SaaS Finance App

Full scope details

Name

... : acme-saas-prod-vpc-aws : SaaS Finance App

Primary Workspace

SaaS Finance App

Query

* orchestrator_application = SaaS-Finance or * orchestrator_aws:autoscaling:groupName = SaaS-Finance-App-Tier-Auto-Scale

Enter attributes...

Search Inventory

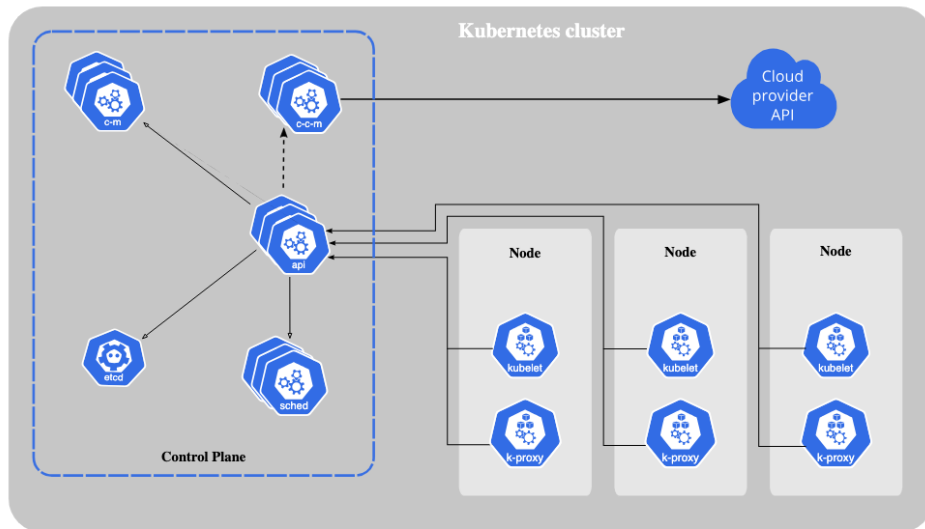
Services 0 Pods 0 Workloads 9 IP Addresses 0

9 of 9 Workloads

Hostname	Address	* application	* compliance	* compliance_functi	* data_type	* env
i-0f7165dbfb0874601	10.255.12.109	—	—	—	—	—
i-0b22ce46f9b273a4d	10.255.12.47	—	—	—	—	—

Moving to cloud Native

Why Do Customers Use Kubernetes?



- **Scalability**

Kubernetes allows applications to scale up or down automatically based on demand, ensuring optimal performance and cost efficiency for both small businesses and large enterprises.

- **High Availability & Reliability**

Kubernetes provides automated failover, self-healing, and load balancing, which help maintain application uptime and stability even during failures or traffic spikes.

- **Automation & Operational Efficiency**

By automating deployment, scaling, updates, and rollbacks, Kubernetes reduces manual intervention and operational overhead, freeing teams to focus on innovation.

- **Cost Optimization**

Kubernetes maximizes resource utilization by efficiently distributing workloads, reducing idle capacity, and helping businesses avoid over-provisioning infrastructure.

- **Faster Time to Market**

Kubernetes supports rapid development and deployment cycles, enabling continuous integration and delivery (CI/CD) practices, which accelerate feature releases and business agility.

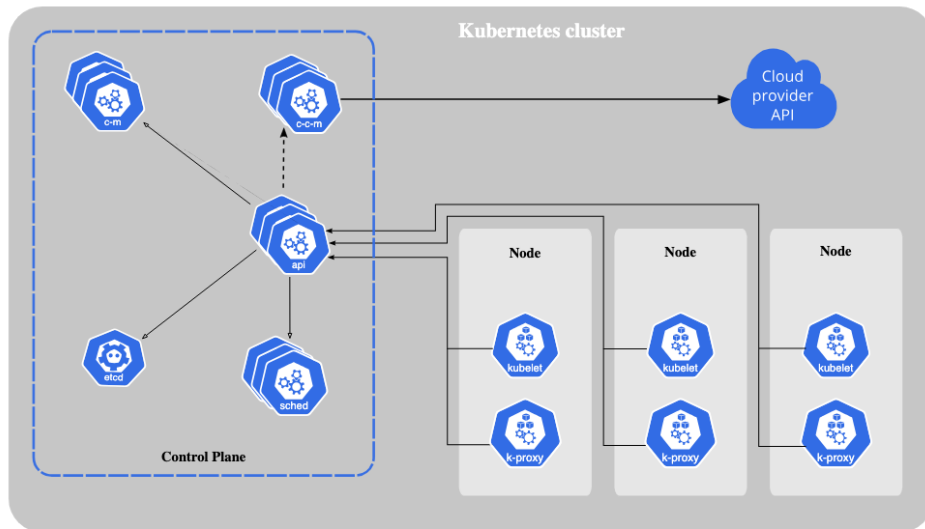
- **Multi-Cloud & Hybrid Flexibility**

Kubernetes enables workloads to run seamlessly across on-premises, public, or hybrid cloud environments, helping organizations avoid vendor lock-in and optimize their cloud strategy.

- **Improved Security & Ecosystem Support**

Kubernetes benefits from a robust open-source ecosystem, with extensive tooling for monitoring, security, and integration, supporting enterprise-grade requirements.

Why Do Customers Use Kubernetes?



- **Scalability**

Kubernetes allows applications to scale up or down automatically based on demand, ensuring optimal performance and cost efficiency for both small businesses and large enterprises.

- **High Availability & Reliability**

Kubernetes provides automated failover, self-healing, and load balancing, which help maintain application uptime and stability even during failures or traffic spikes.

- **Automation & Operational Efficiency**

By automating deployment, scaling, updates, and rollbacks, Kubernetes reduces manual intervention and operational overhead, freeing teams to focus on innovation.

- **Cost Optimization**

Kubernetes maximizes resource utilization by efficiently distributing workloads, reducing idle capacity, and helping businesses avoid over-provisioning infrastructure.

- **Faster Time to Market**

Kubernetes supports rapid development and deployment cycles, enabling continuous integration and delivery (CI/CD) practices, which accelerate feature releases and business agility.

- **Multi-Cloud & Hybrid Flexibility**

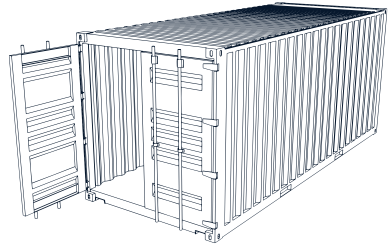
Kubernetes enables workloads to run seamlessly across on-premises, public, or hybrid cloud environments, helping organizations avoid vendor lock-in and optimize their cloud strategy.

- **Improved Security & Ecosystem Support**

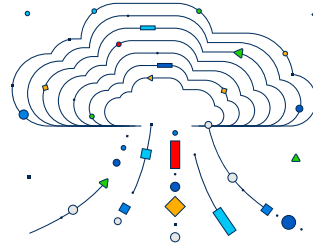
Kubernetes benefits from a robust open-source ecosystem, with extensive tooling for monitoring, security, and integration, supporting enterprise-grade requirements.

Kubernetes - The New Standard To Deploy Applications

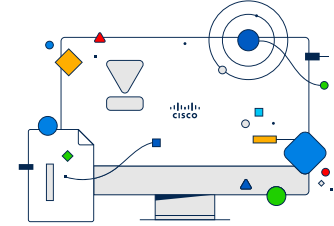
A Hybrid and Multi-Cloud Infrastructure Layer Supporting Both Modern & Legacy Workloads



Containers



AI / ML Workloads



Legacy VM Workloads

Kubernetes



Bare Metal

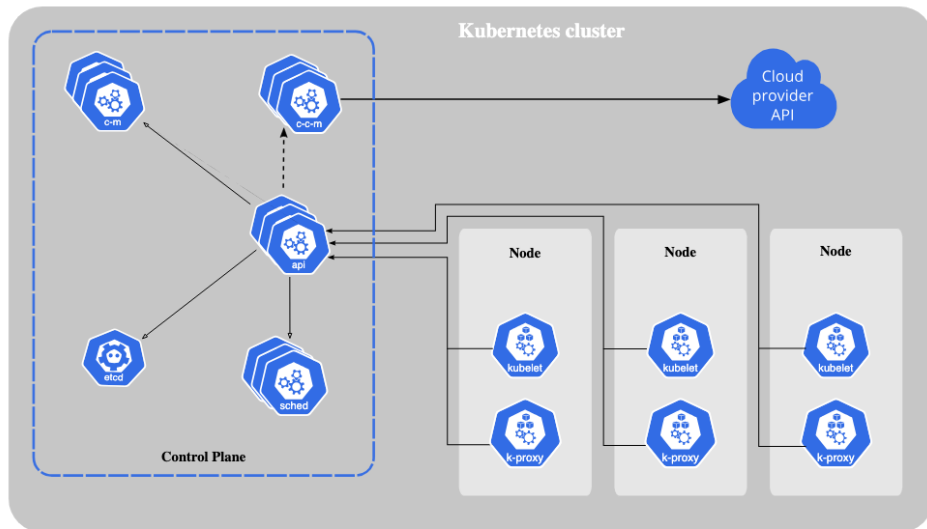
vmware®
by Broadcom

aws

Azure

Google Cloud

Why Do Customers Use Kubernetes?



- **Scalability**

Kubernetes allows applications to scale up or down automatically based on demand, ensuring optimal performance and cost efficiency for both small businesses and large enterprises.

- **High Availability & Reliability**

Kubernetes provides automated failover, self-healing, and load balancing, which help maintain application uptime and stability even during failures or traffic spikes.

- **Automation & Operational Efficiency**

By automating deployment, scaling, updates, and rollbacks, Kubernetes reduces manual intervention and operational overhead, freeing teams to focus on innovation.

- **Cost Optimization**

Kubernetes maximizes resource utilization by efficiently distributing workloads, reducing idle capacity, and helping businesses avoid over-provisioning infrastructure.

- **Faster Time to Market**

Kubernetes supports rapid development and deployment cycles, enabling continuous integration and delivery (CI/CD) practices, which accelerate feature releases and business agility.

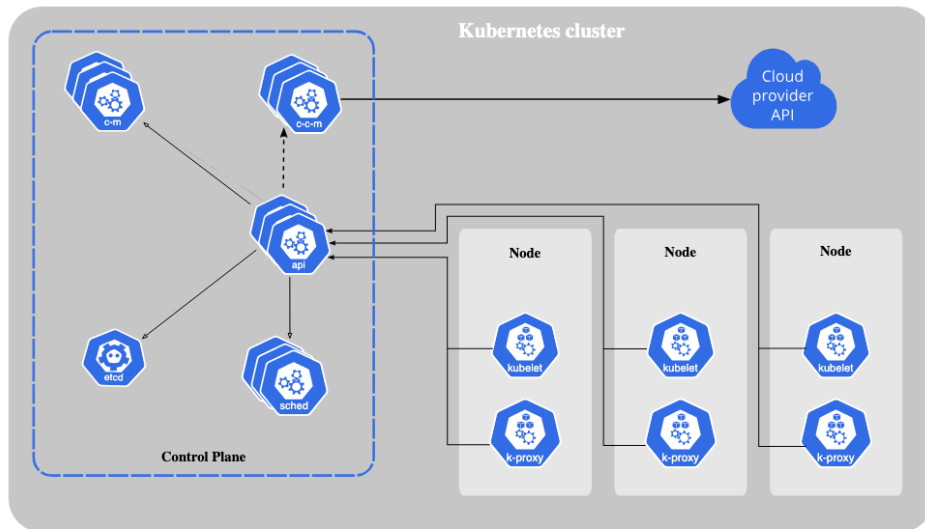
- **Multi-Cloud & Hybrid Flexibility**

Kubernetes enables workloads to run seamlessly across on-premises, public, or hybrid cloud environments, helping organizations avoid vendor lock-in and optimize their cloud strategy.

- **Improved Security & Ecosystem Support**

Kubernetes benefits from a robust open-source ecosystem, with extensive tooling for monitoring, security, and integration, supporting enterprise-grade requirements.

Why Do Customers Use Kubernetes?



- **Scalability**

Kubernetes allows applications to scale up or down automatically based on demand, ensuring optimal performance and cost efficiency for both small businesses and large enterprises.

- **High Availability & Reliability**

Kubernetes provides automated failover, self-healing, and load balancing, which help maintain application uptime and stability even during failures or traffic spikes.

- **Automation & Operational Efficiency**

By automating deployment, scaling, updates, and rollbacks, Kubernetes reduces manual intervention and operational overhead, freeing teams to focus on innovation.

- **Cost Optimization**

Kubernetes maximizes resource utilization by efficiently distributing workloads, reducing idle capacity, and helping businesses avoid over-provisioning infrastructure.

- **Faster Time to Market**

Kubernetes supports rapid development and deployment cycles, enabling continuous integration and delivery (CI/CD) practices, which accelerate feature releases and business agility.

- **Multi-Cloud & Hybrid Flexibility**

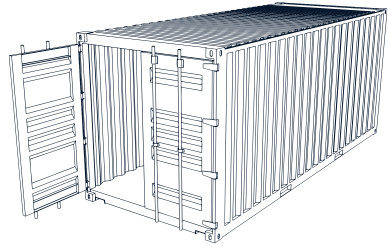
Kubernetes enables workloads to run seamlessly across on-premises, public, or hybrid cloud environments, helping organizations avoid vendor lock-in and optimize their cloud strategy.

- **Improved Security & Ecosystem Support**

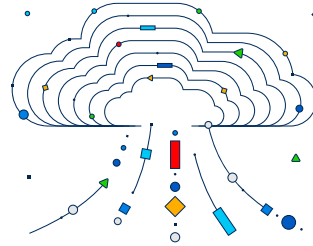
Kubernetes benefits from a robust open-source ecosystem, with extensive tooling for monitoring, security, and integration, supporting enterprise-grade requirements.

Kubernetes - The New Standard To Deploy Applications

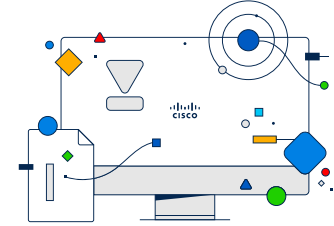
A Hybrid and Multi-Cloud Infrastructure Layer Supporting Both Modern & Legacy Workloads



Containers



AI / ML Workloads



Legacy VM Workloads

Kubernetes



Bare Metal

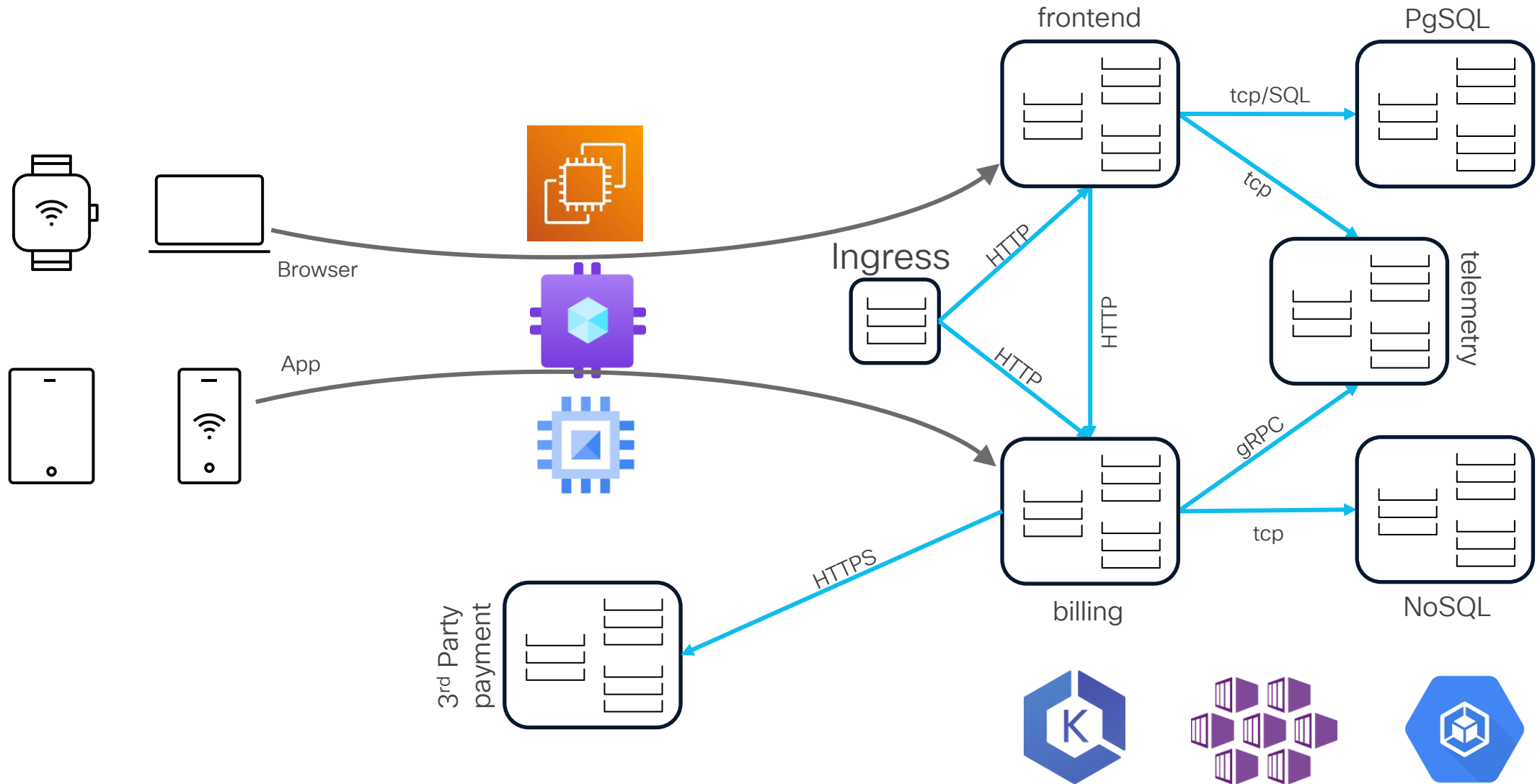
vmware®
by Broadcom

aws

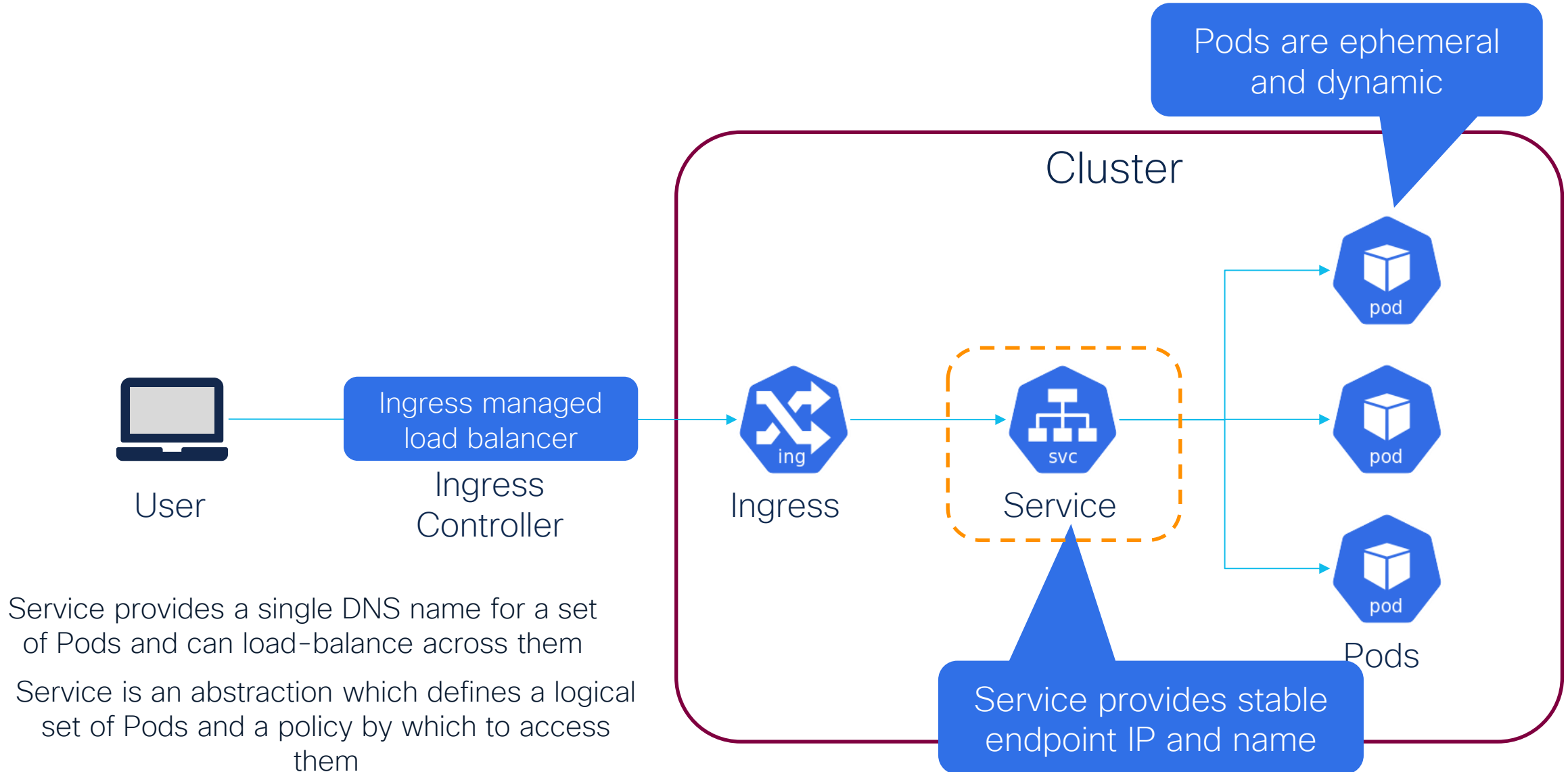
Azure

Google Cloud

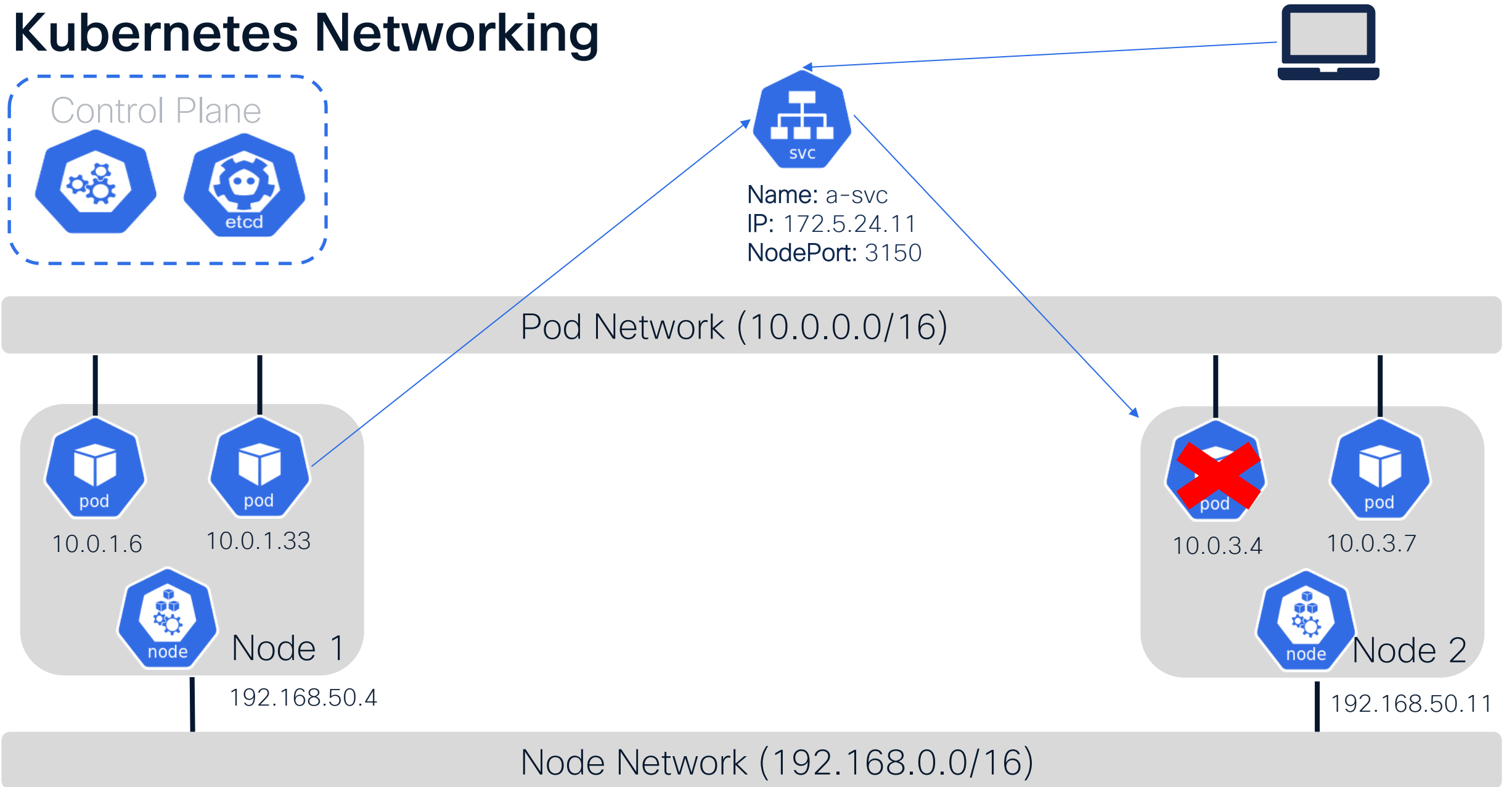
Ok but, where is my network ?



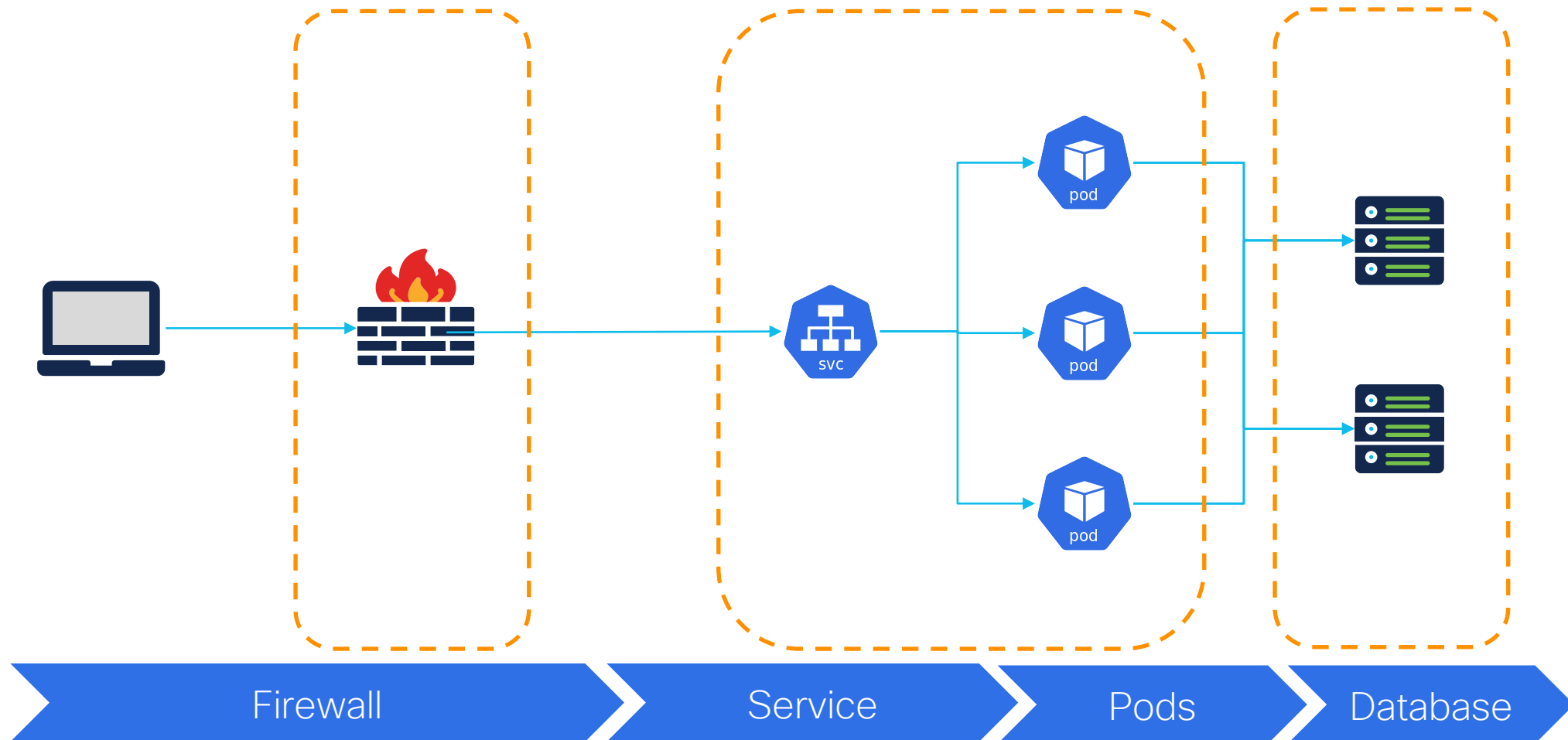
Key K8 Components - Services



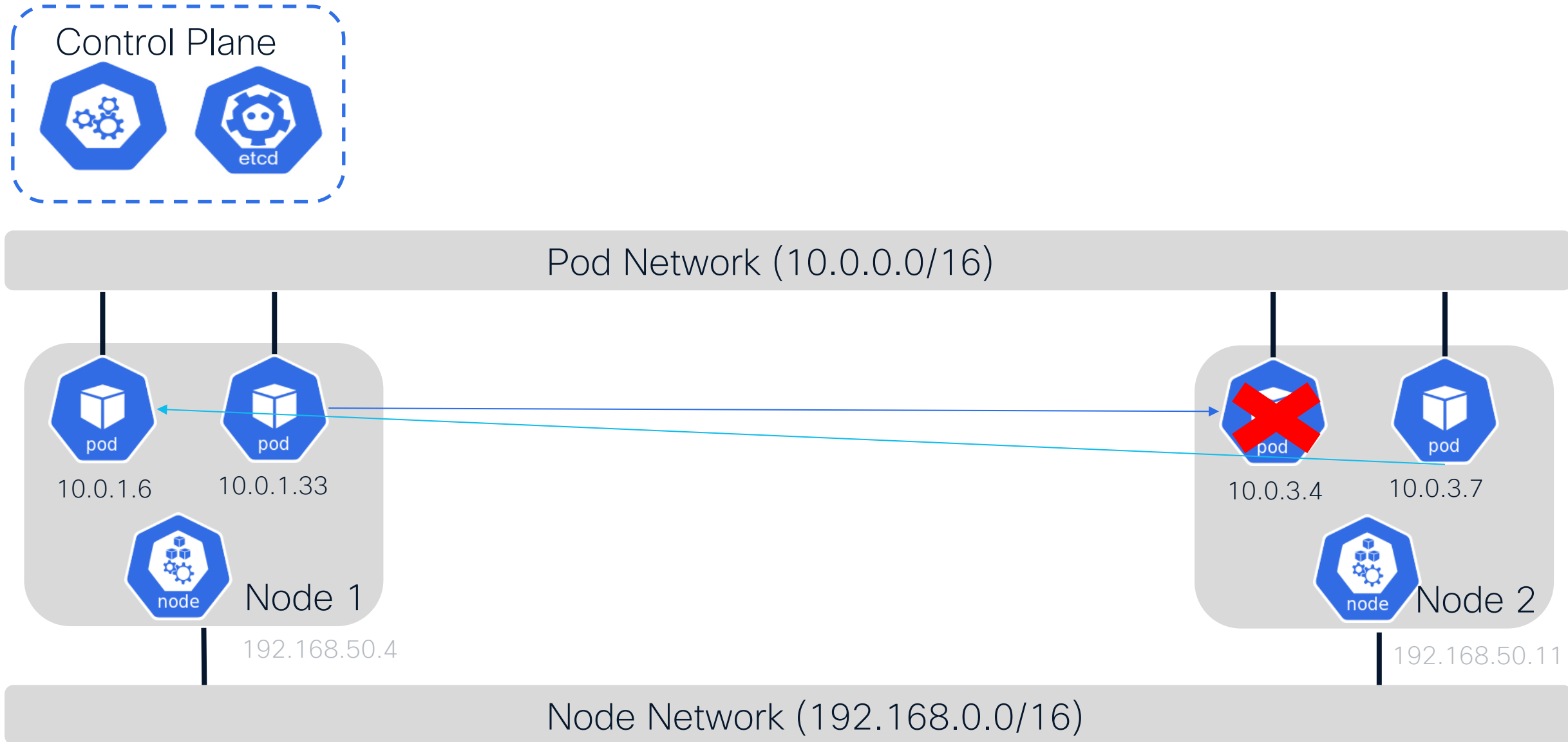
Kubernetes Networking



Complicated Policy Enforcement

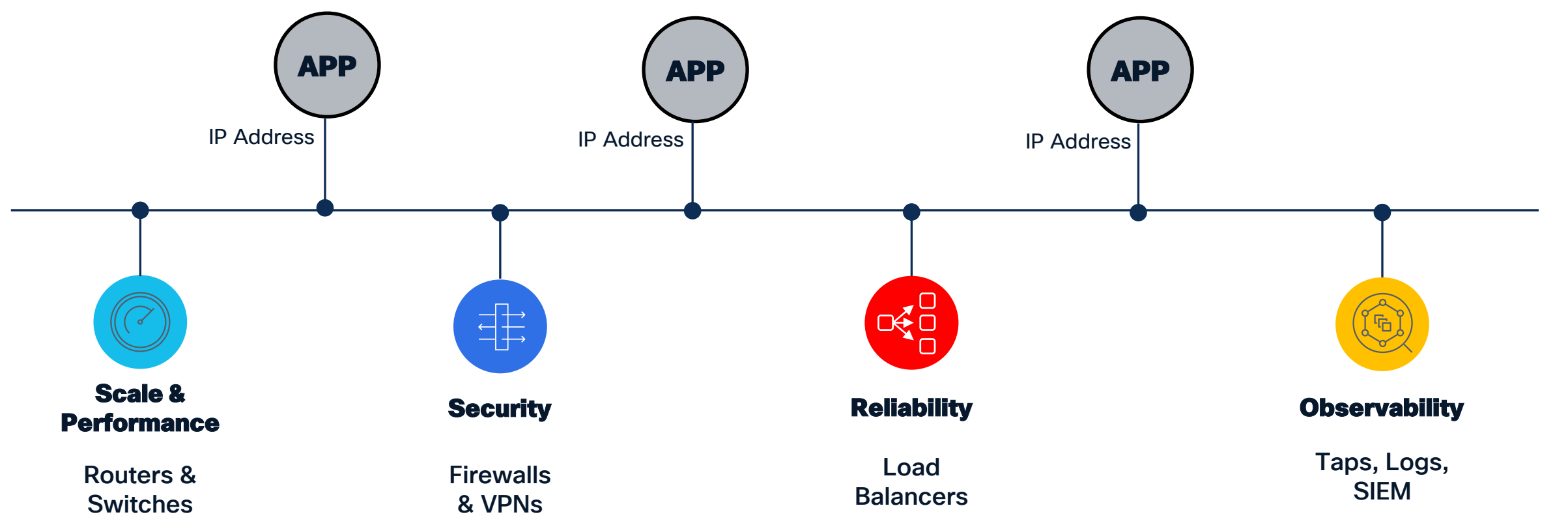


Kubernetes Networking



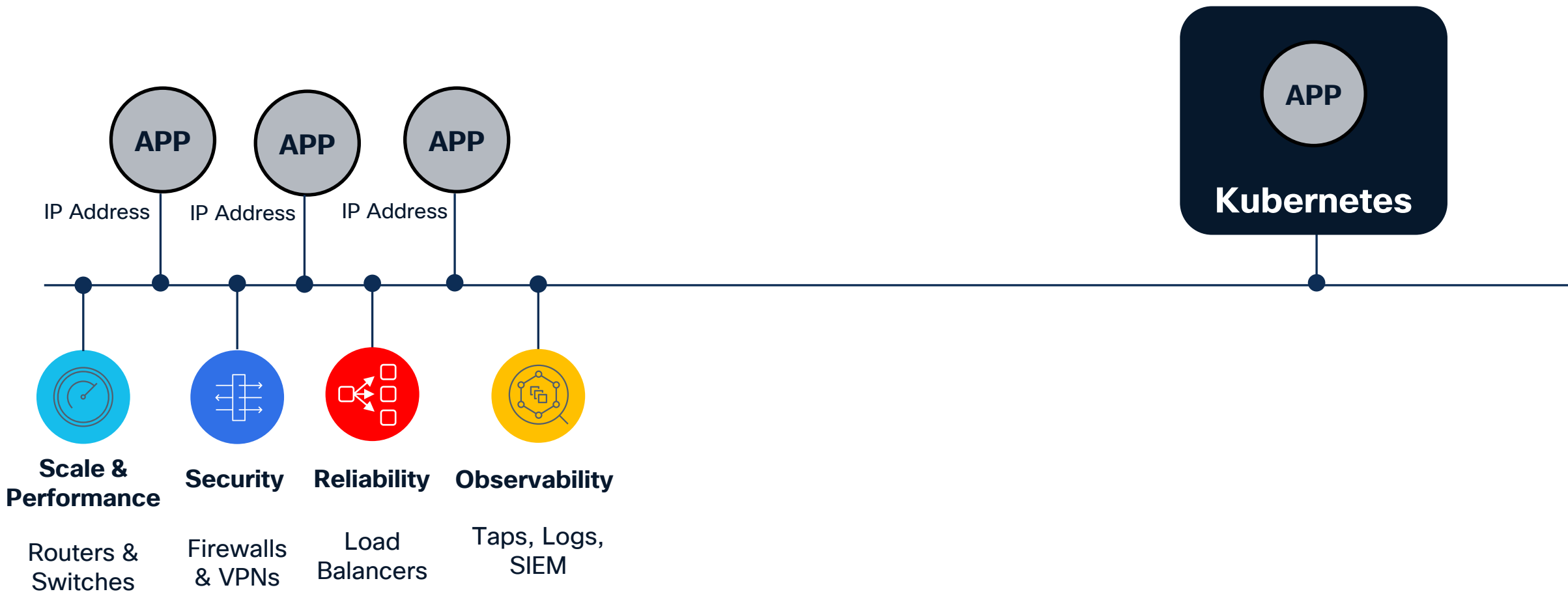
The Network has Always Been Essential to Applications

But Kubernetes Environments Are Challenging for Enterprise Infrastructure Teams



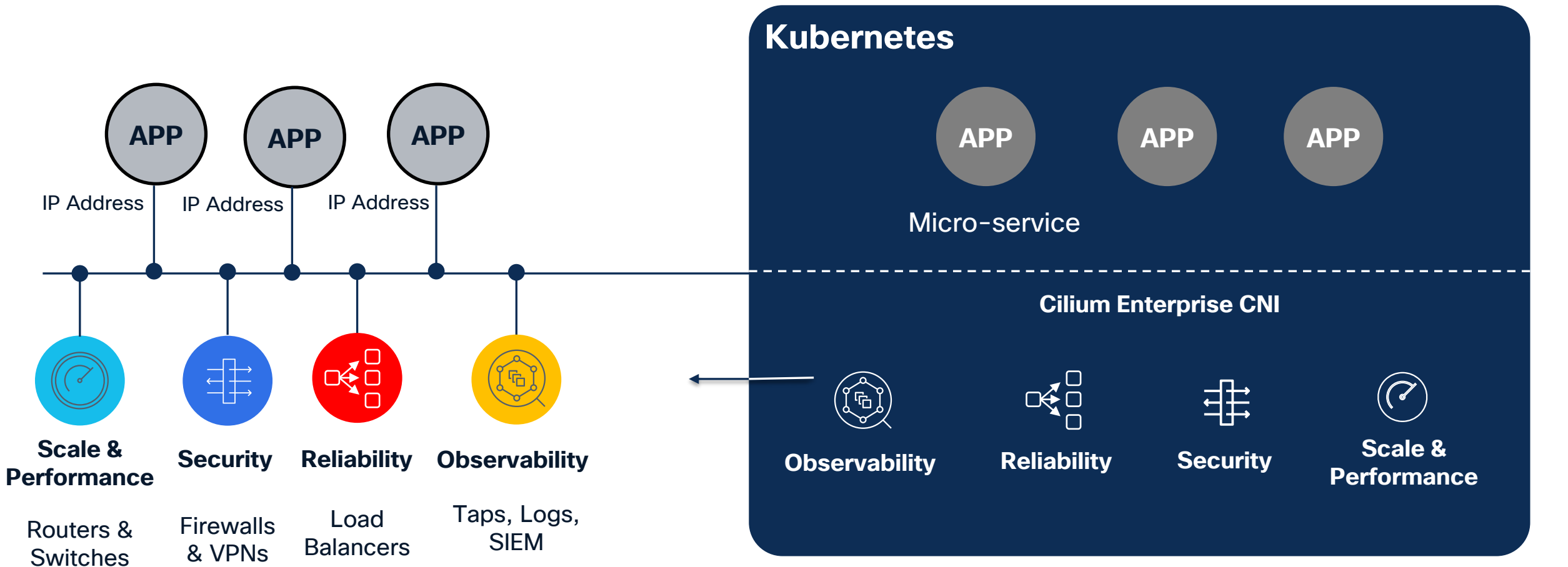
The Network has Always Been Essential to Applications

But Kubernetes Environments Are Challenging for Enterprise Infrastructure Teams



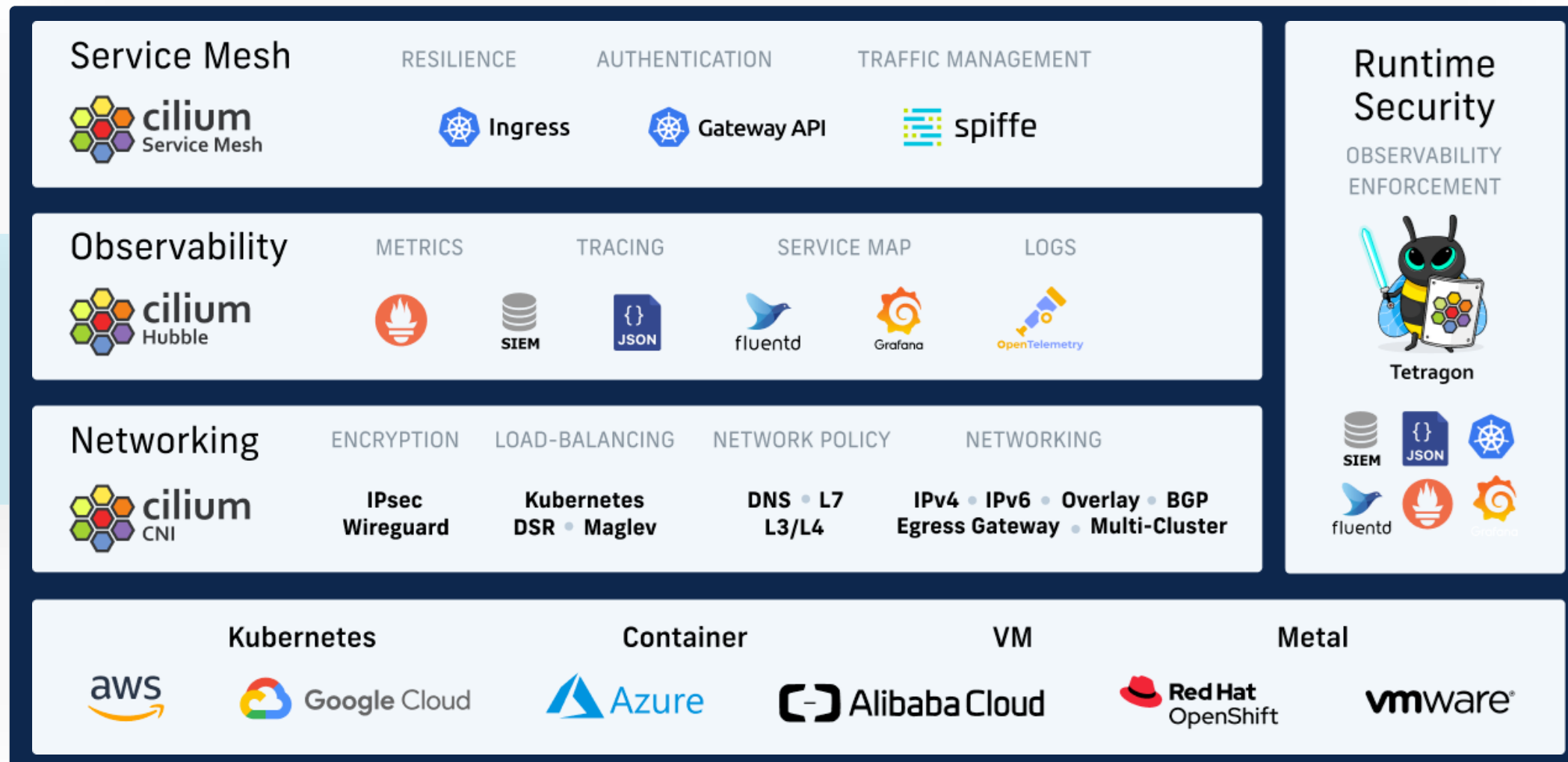
The Network has Always Been Essential to Applications

But Kubernetes Environments Are Challenging for Enterprise Infrastructure Teams



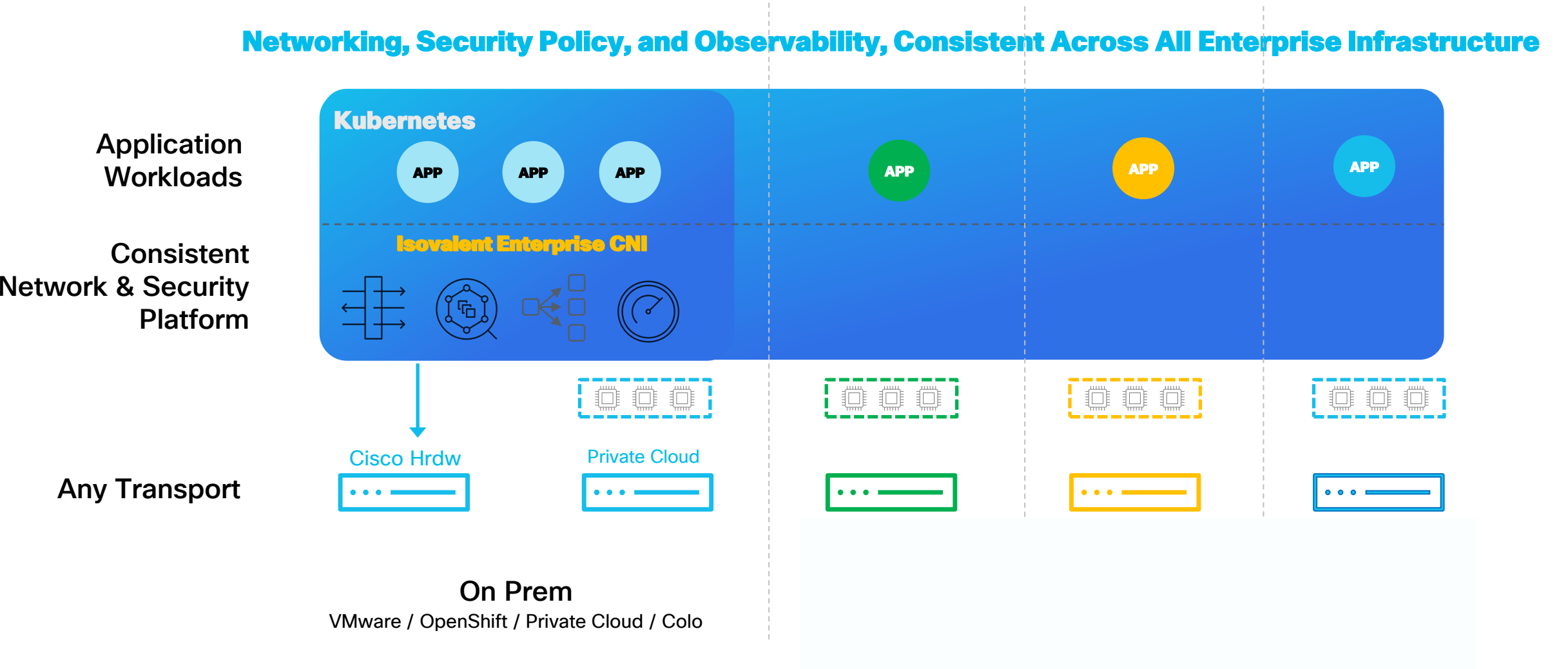
powers many things

Capabilities For Your Cloud Native Journey



This is Why Cisco Acquired Isovalent.

It's the Technology Foundation for Cisco's Hybrid & Multi-Cloud Networking & Security Strategy



Where is my interface and network cabling

Kubernetes CNI Explained

Concepts of Kubernetes Container Network Interface (CNI)

CNI (Container Network Interface)

A framework for configuring network interfaces in Linux containers.

Plugins

Responsible for setting up networking for pods. Examples include Calico, Flannel, and Weave

Network Namespace

Isolates network resources like IP addresses and interfaces for each pod.

IPAM (IP Address Management)

Allocates and manages IP addresses for pod interfaces.

Benefits

Provides modularity, flexibility, and ensures interoperability between different networking so

Kubernetes Service Mesh Explained

Concepts of a Kubernetes Service Mesh

Service Mesh

A dedicated infrastructure layer for managing service-to-service communication.

Data Plane

Handles the communication between services by proxying requests.

Control Plane

Manages the configuration and policy enforcement for the data plane.

Sidecar Proxy

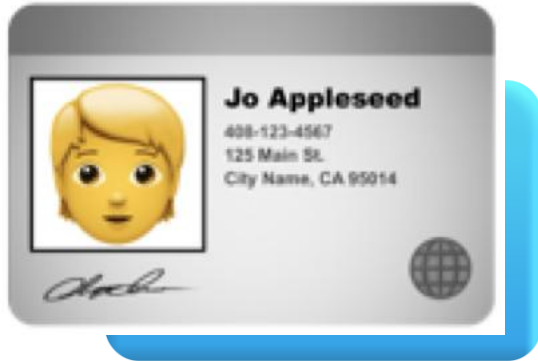
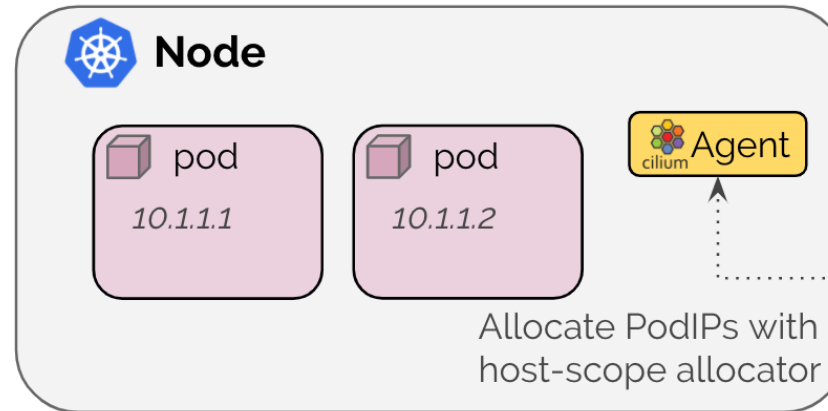
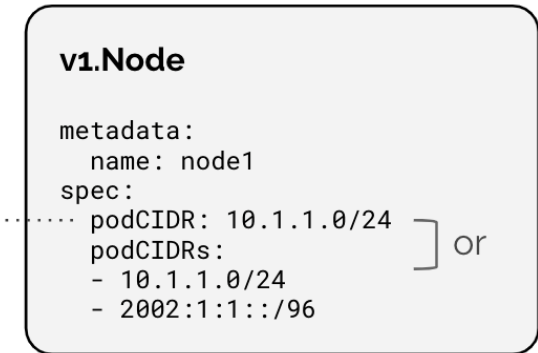
A proxy deployed alongside each service instance, intercepting and managing network traffic.

Benefits

Provides observability, security, and traffic management without altering application code.

Key Functions of a CNI Plugin

IP Address Management (IPAM)



CNI plugins are responsible for assigning IP addresses to pods, ensuring that each pod has a unique IP address within the cluster.

<https://isovalent.com/labs/cilium-ipam/>



Key Functions of a CNI Plugin

Network Isolation



CNIs can implement network policies to control the traffic flow between pods. This helps in ensuring security and compliance by isolating workloads as needed.

Network Isolation in Kubernetes

[Namespace: dev]

[Namespace: prod]

[Namespace: test]

[Pods]

[Pods]

[Pods]

<---- Default: All pods can talk to each other ---->

[NetworkPolicy applied to prod namespace]

- Some arrows between pods/namespaces are blocked

- Only allowed traffic passes (e.g., API -> DB)

Example Policy:

kind: NetworkPolicy

spec:

podSelector: { app: db }

ingress:

- from: { app: api }

Key Functions:

- Namespace-based logical isolation

- Fine-grained traffic control

- Enforced by CNI plugin

- Supports security & compliance

<https://isovalent.com/labs/tetragon-getting-started/>

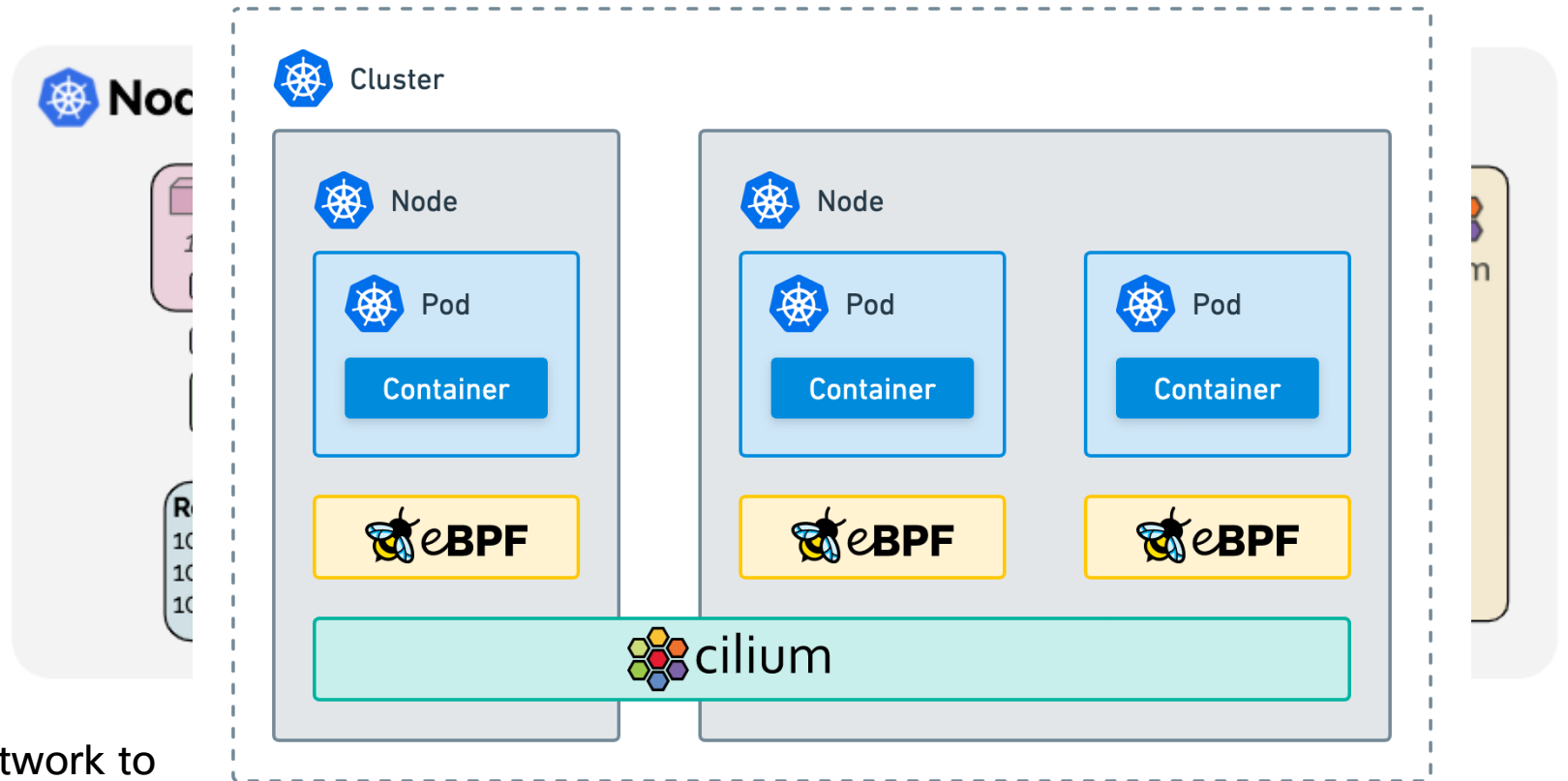


Key Functions of a CNI Plugin

Routing and Connectivity



A CNI plugin configures the underlying network to ensure that pods can communicate with each other, regardless of the node they are running on. This involves setting up appropriate routing rules and network bridges.



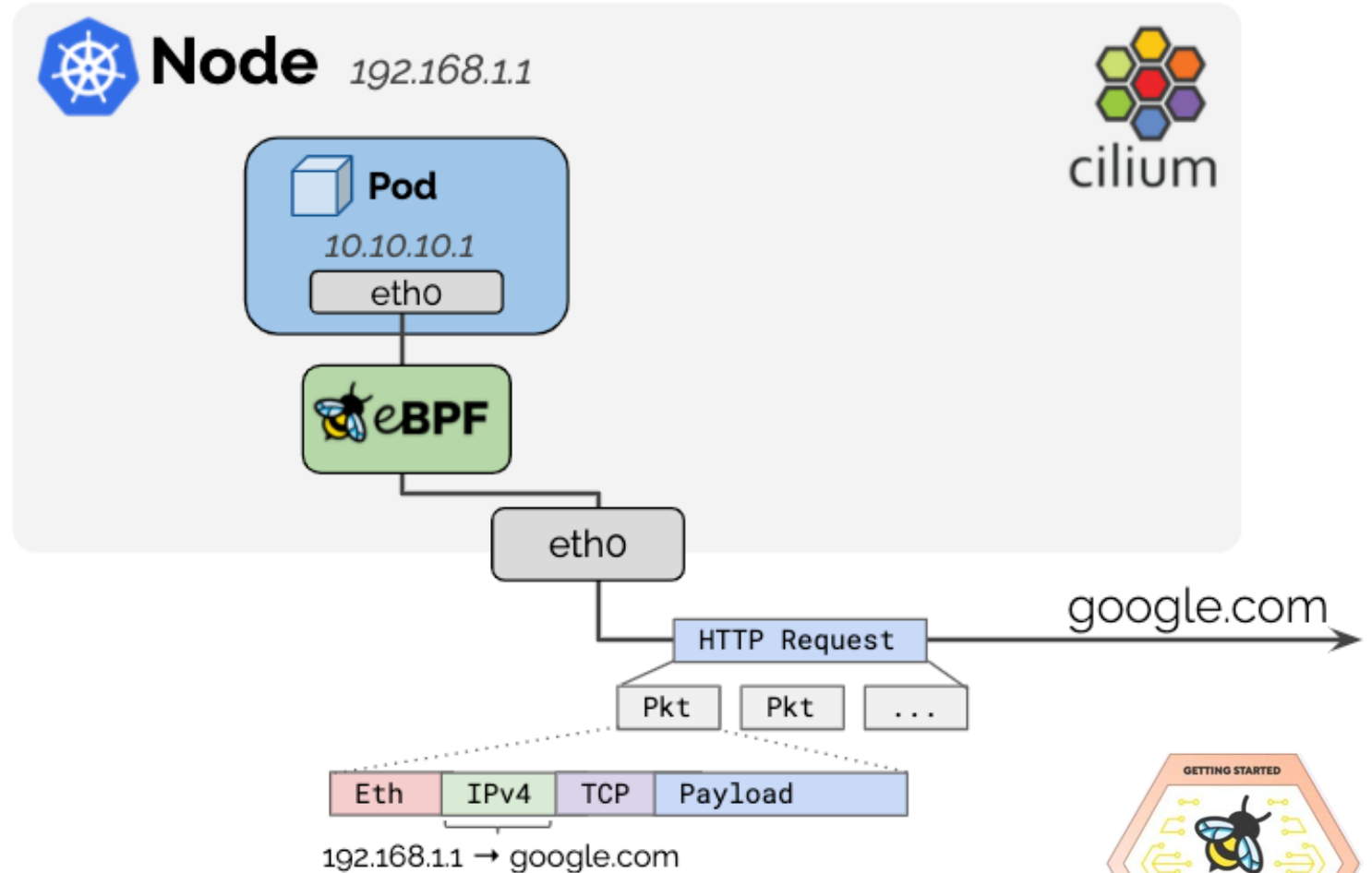
<https://isovalent.com/labs/cilium-lb-ipam-l2-announcements>

Key Functions of a CNI Plugin

Integration with Host Networking



CNI plugins manage the integration between the container network and the host network. This includes setting up network interfaces and ensuring correct routing of traffic to and from the pods.

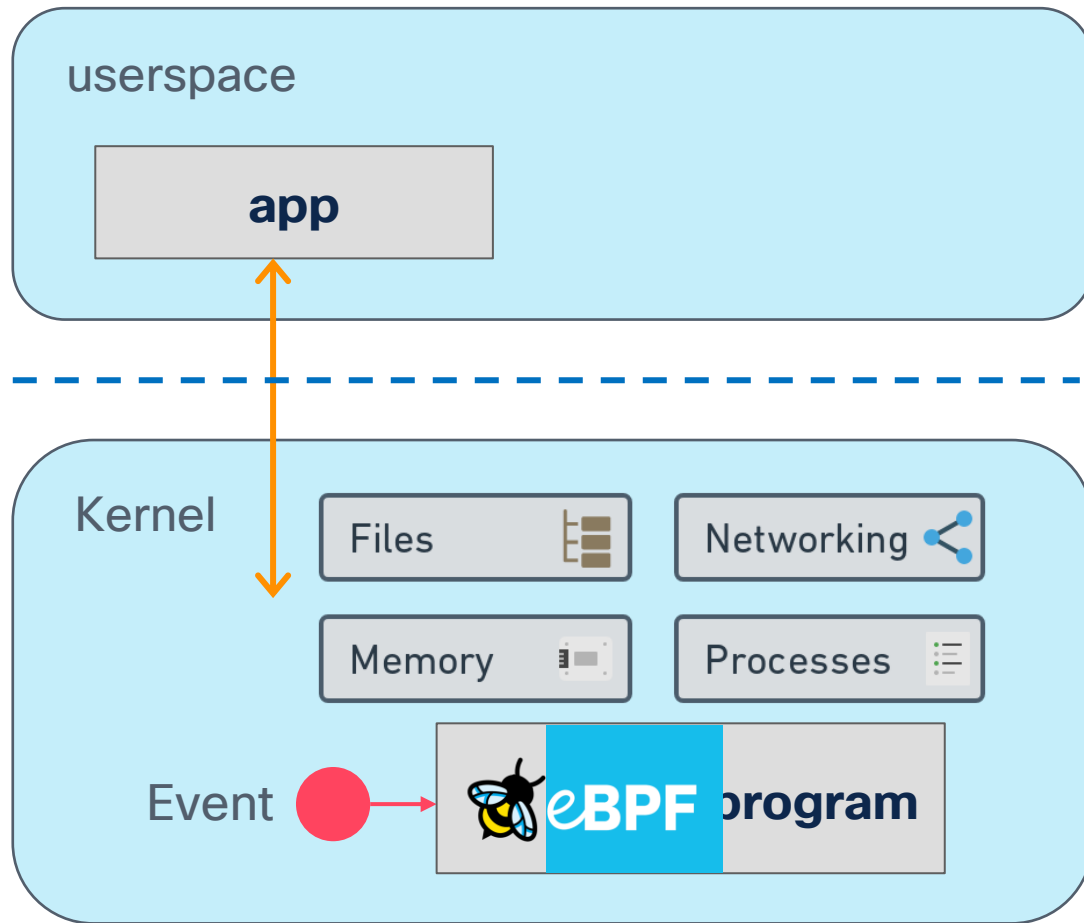
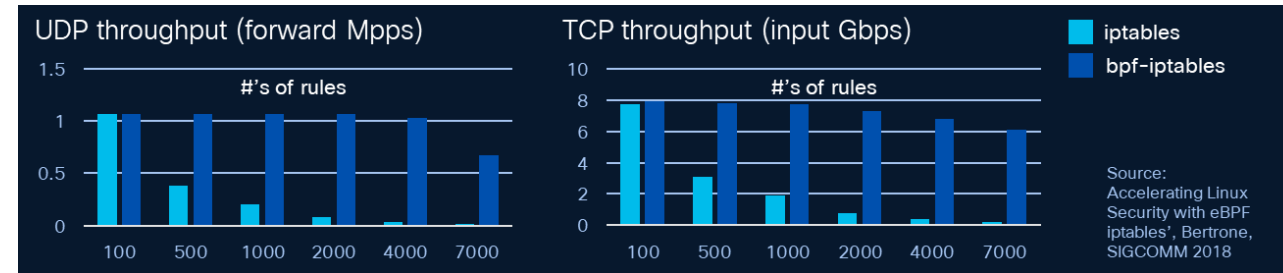


<https://isovalent.com/labs/ebpf-getting-started/>



eBPF – Extended Berkely Packet Filter

Makes the kernel programmable in a secure and efficient way

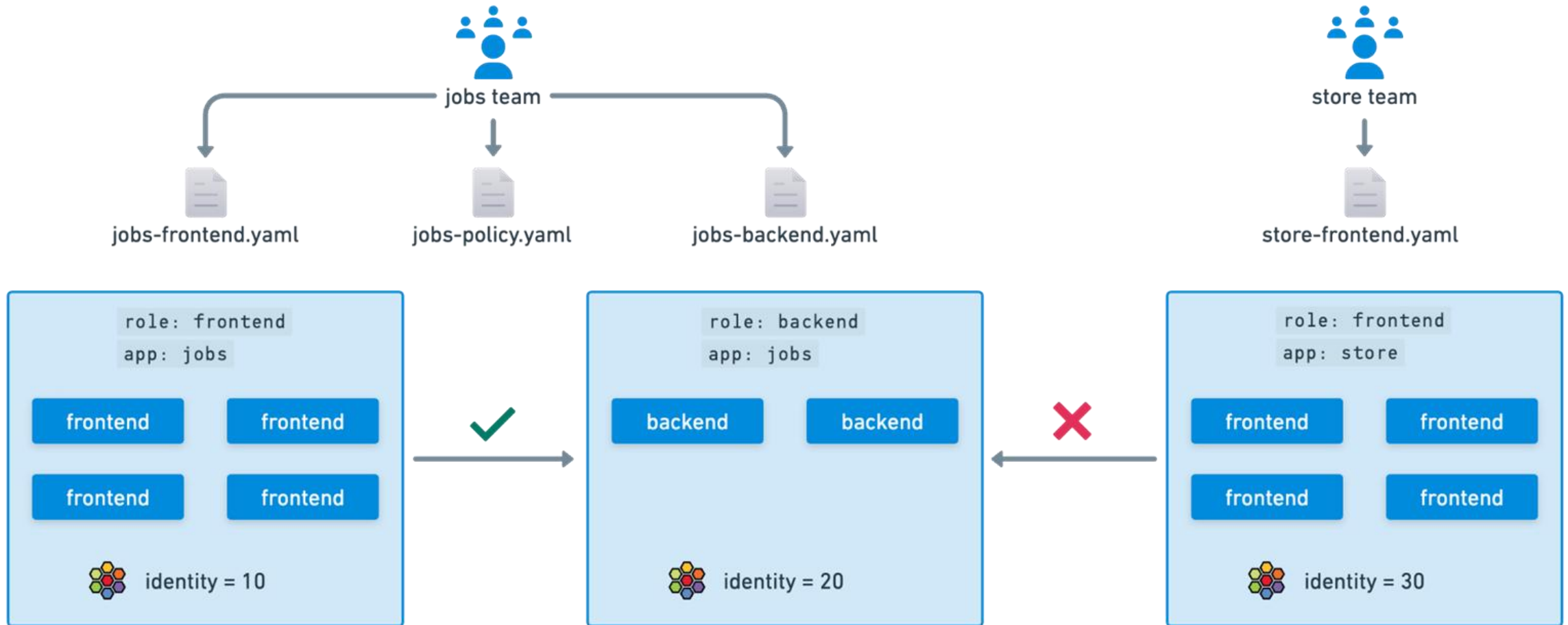


System calls

- eBPF runs in a restricted execution environment
- Before eBPF script is compiled:
 - Verifier ensures things such as memory safety
 - Hardening process (program execution protection, mitigation against spectre, constant blinding, ...)
- eBPF can only access pre-approved kernel functions and data structures

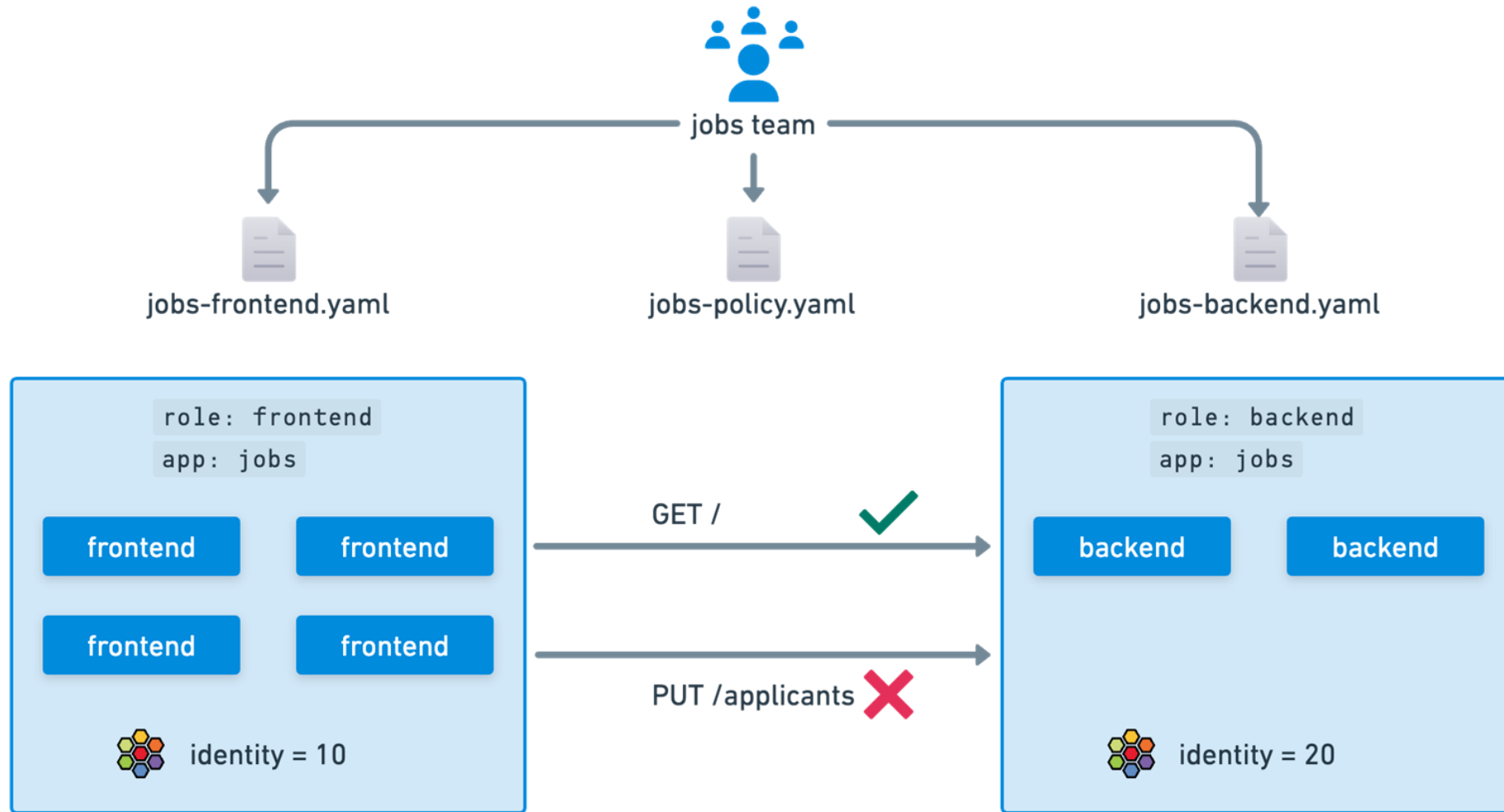
Micro-Segmentation

Label based East-West Application or Multi-tenet Security Enforcement

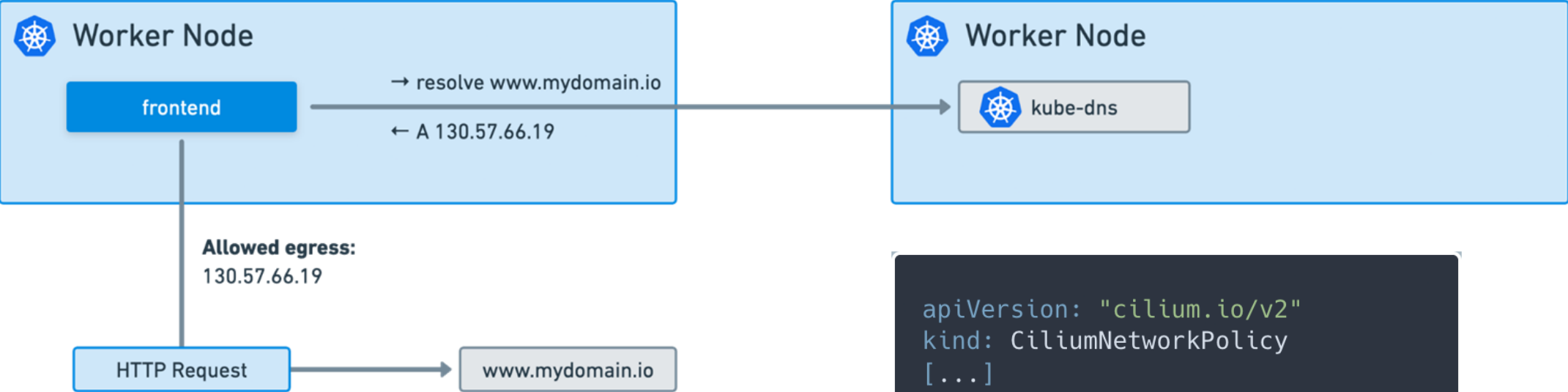


API-Aware Security

Safely Secure API Endpoints by filtering Protocols, Methods and Paths

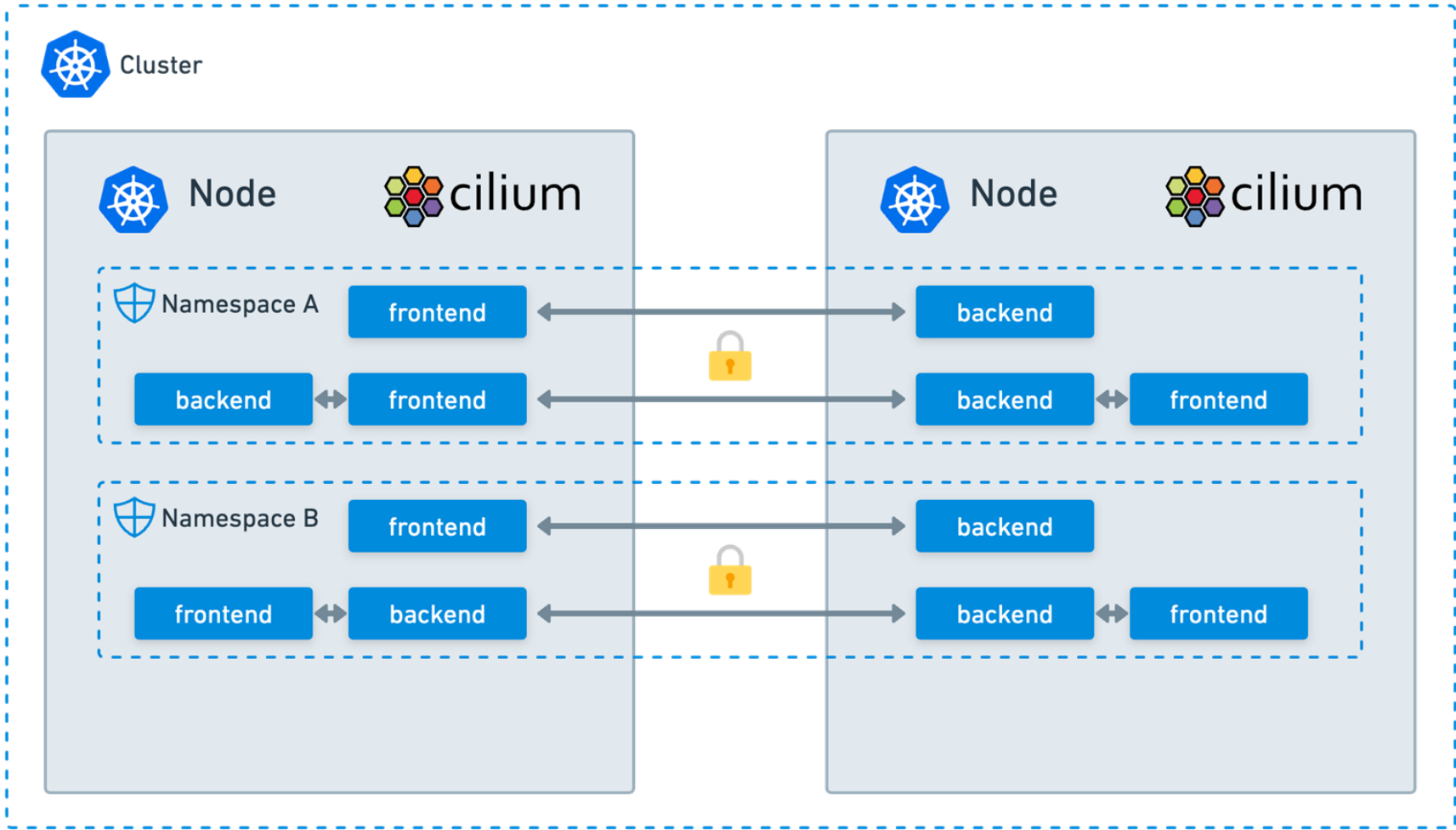


DNS-aware Cilium Network Policy



```
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
[...]
specs:
- endpointSelector:
  matchLabels:
    app: frontend
  egress:
  - toFQDNs:
    - matchName: "*.mydomain.io"
    toPorts:
    - ports:
      - port: "443"
        protocol: TCP
```

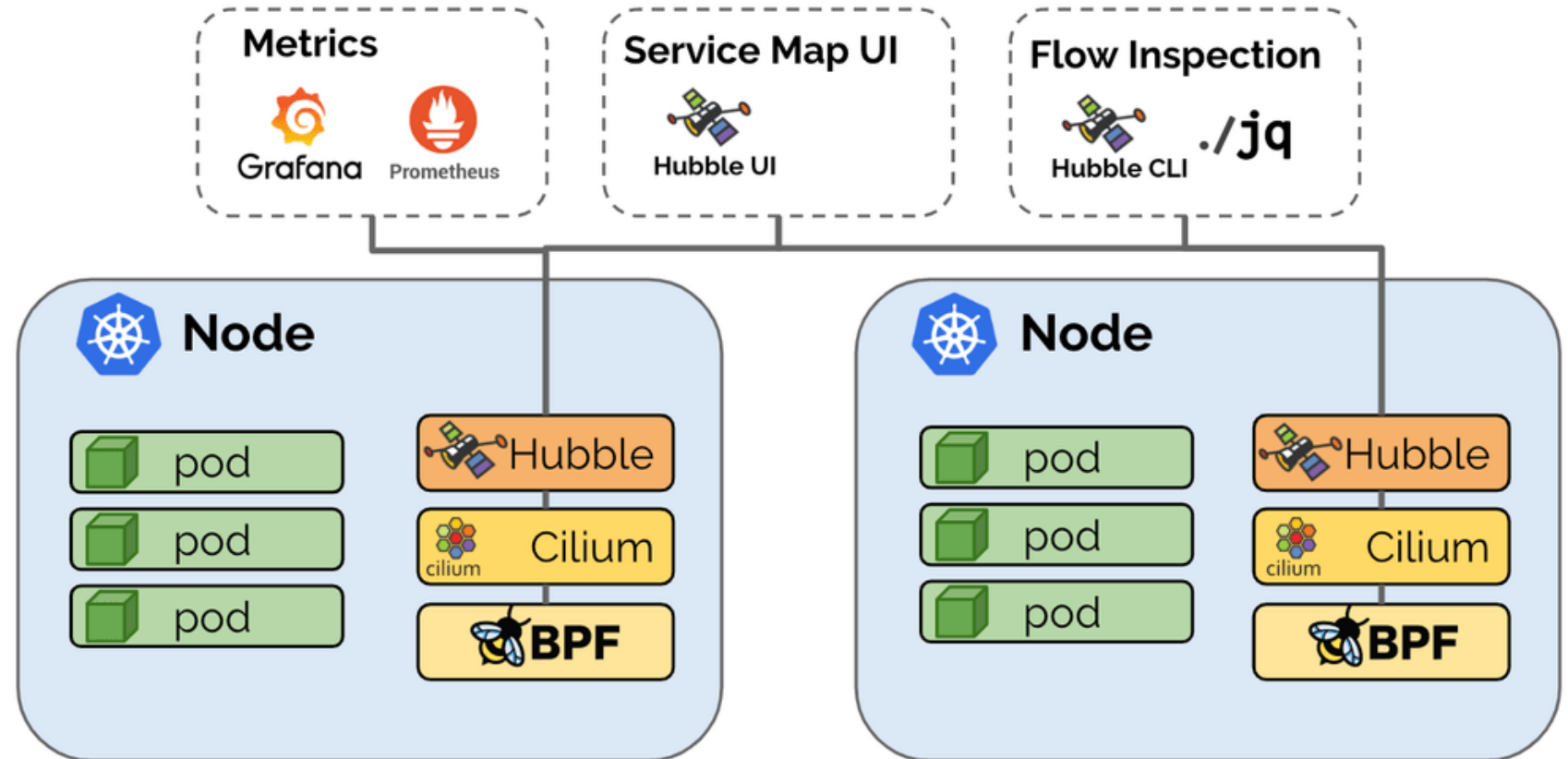
Transparent Data Encryption



Hubble CLI



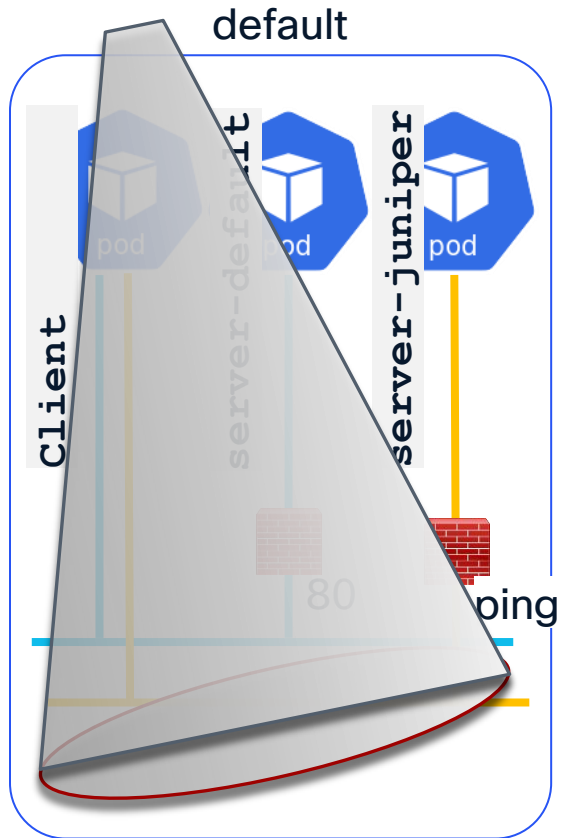
Hubble is a fully distributed networking and security observability platform for cloud native workloads. Hubble is open source software and built on top of Cilium and eBPF to enable deep visibility into the communication and behaviour of services as well as the networking infrastructure in a completely transparent manner.



Basic Lab Deployment – Netpolicy – validate



hubble



```
root@server:~# hubble observe --pod client --protocol icmp
```

```
..~ client (ID:12606) -> server-default (ID:3255) to-stack FORWARDED (ICMPv4 EchoRequest)
..~ client (ID:12606) <> server-default (ID:3255) policy-verdict:none INGRESS DENIED (ICMPv4 EchoRequest)
..~ client (ID:12606) <> server-default (ID:3255) Policy denied DROPPED (ICMPv4 EchoRequest)
..~ client (ID:61243) -> server-jupiter (ID:31088) policy-verdict:L4-Only EGRESS ALLOWED (ICMPv4 EchoRequest)
..~ client (ID:61243) -> server-jupiter (ID:31088) to-stack FORWARDED (ICMPv4 EchoRequest)
..~ client (ID:61243) -> server-jupiter (ID:31088) to-endpoint FORWARDED (ICMPv4 EchoRequest)
..~ client (ID:61243) <- server-jupiter (ID:31088) to-stack FORWARDED (ICMPv4 EchoReply)
..~ client (ID:61243) <- server-jupiter (ID:31088) to-endpoint FORWARDED (ICMPv4 EchoReply)
```

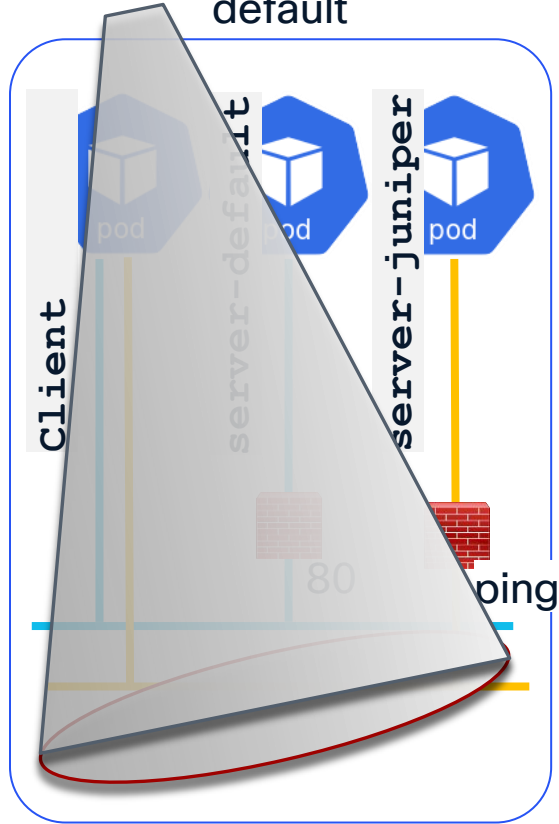
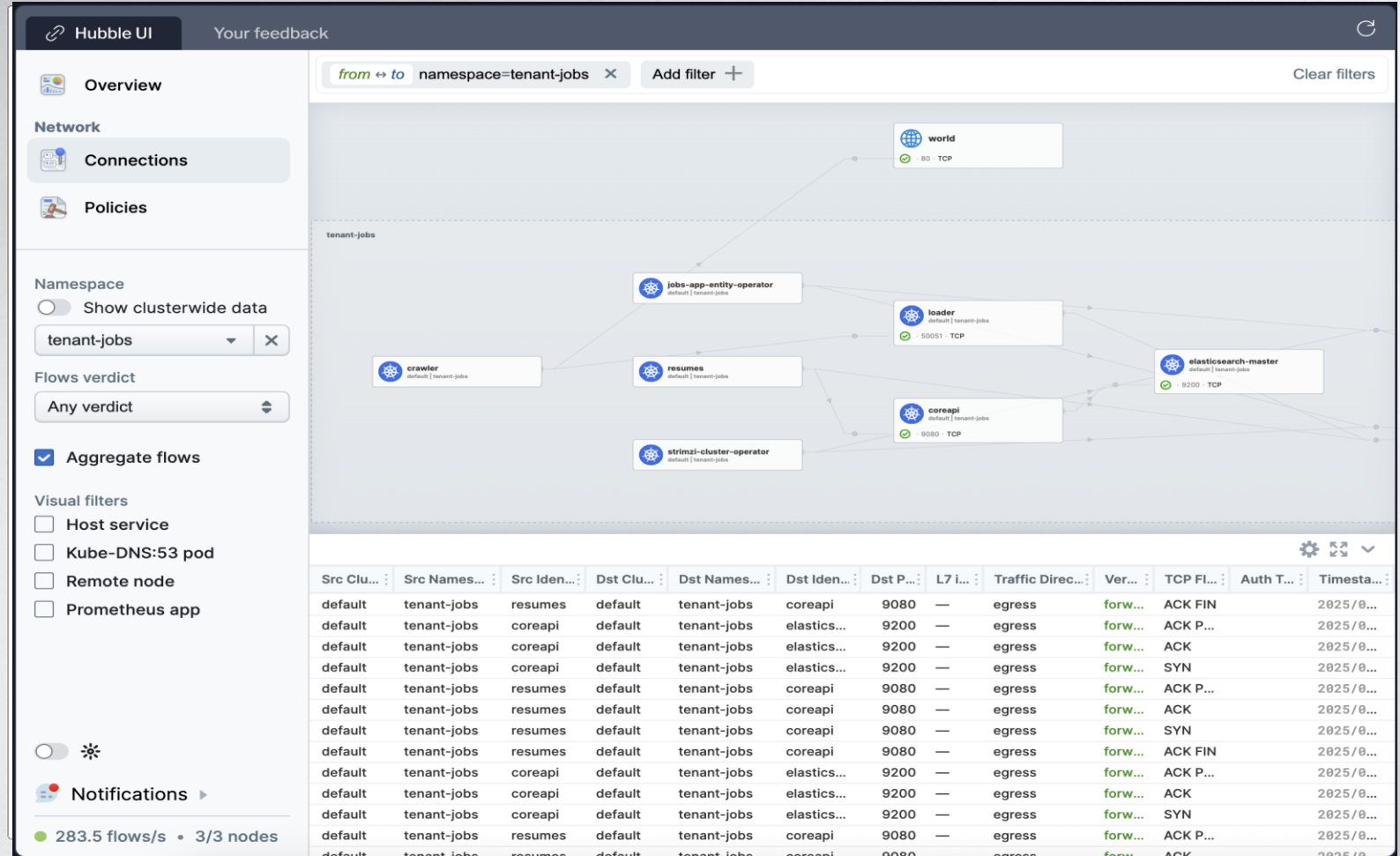
```
root@server:~# hubble observe --pod client --protocol icmp --last
```

```
50 --verdict=DROPPED
```

```
..~ client (ID:12606) <> server-default (ID:3255) policy-verdict:none INGRESS DENIED (ICMPv4 EchoRequest)
..~ client (ID:12606) <> server-default (ID:3255) Policy denied DROPPED (ICMPv4 EchoRequest)
```

MacBook Air

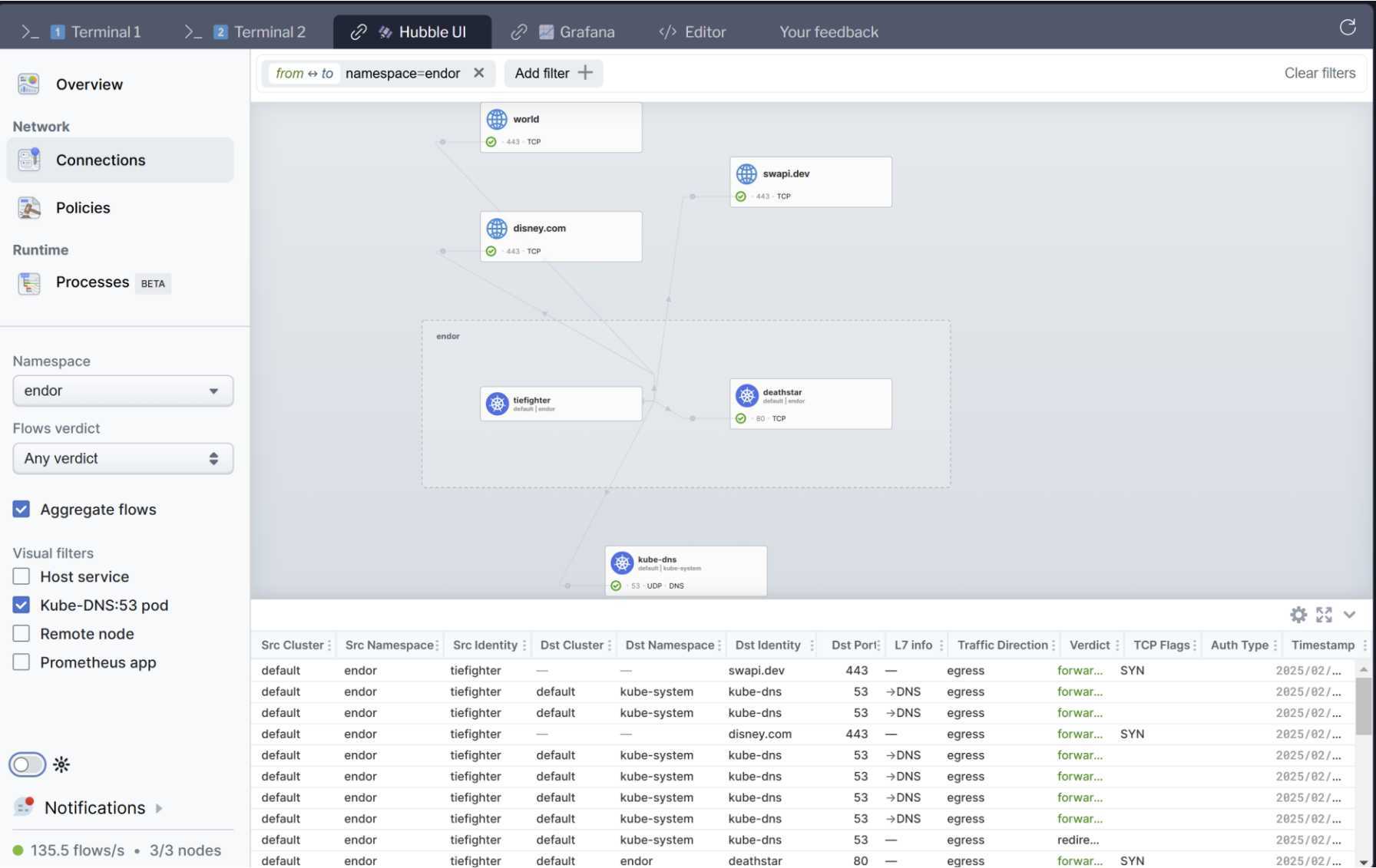
default



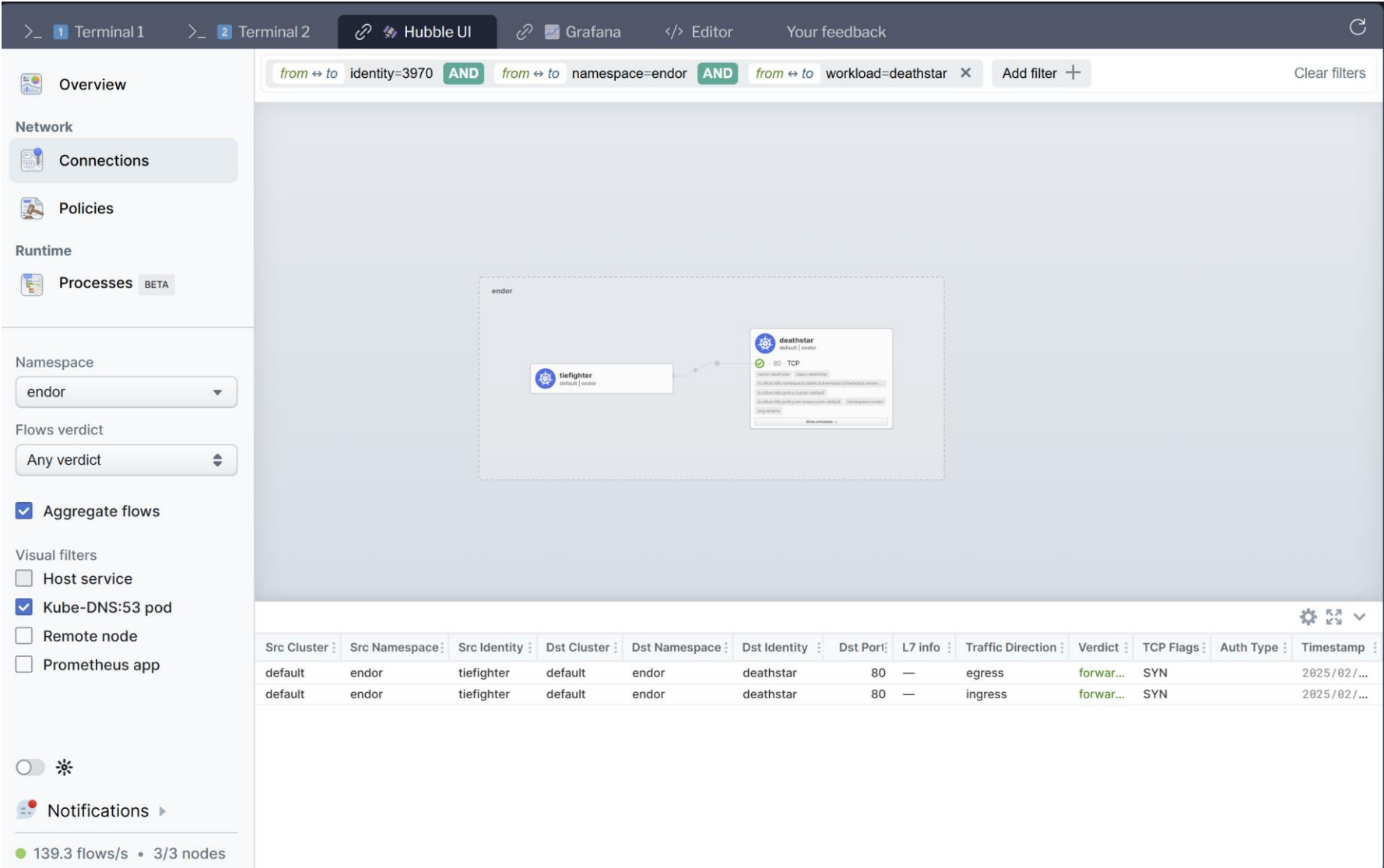
The background of the slide is an abstract composition of numerous thin, flowing lines in shades of blue, yellow, orange, and purple, creating a sense of motion and depth. A large, semi-transparent white rectangle is positioned on the left side of the slide, serving as a backdrop for the main text.

Is there a GUI?

Start with App Dependency Map & DNS visibility



Explore microservice interactions



Visualize policy

Terminal 1

Terminal 2

Hubble UI

Grafana

Editor

Your feedback

Overview

Network

Connections

Policies

Runtime

Processes BETA

Namespace

end

Flows verdict

Any verdict

☒ Aggregate flows

Network policies

Filters applied

Visualize all

Selected policy visualized on map

allow-all

deathstar

☒ *

Notifications

143.2 flows/s • 3/3 nodes

from ↔ to identity=3970 AND from ↔ to namespace=endor AND from ↔ to workload=deathstar

Add filter

Clear filters

Outside Cluster

Any endpoint

In Namespace

end

Any pod

In Cluster

Everything in the cluster

In Namespace

end

Any pod

In Cluster

Everything in the cluster

Kubernetes DNS

1 apiVersion: cilium.io/v2

2 kind: CiliumNetworkPolicy

3 metadata:

4 name: deathstar

5 namespace: endor

6 spec:

7 endpointSelector:

8 matchLabels:

9 org: empire

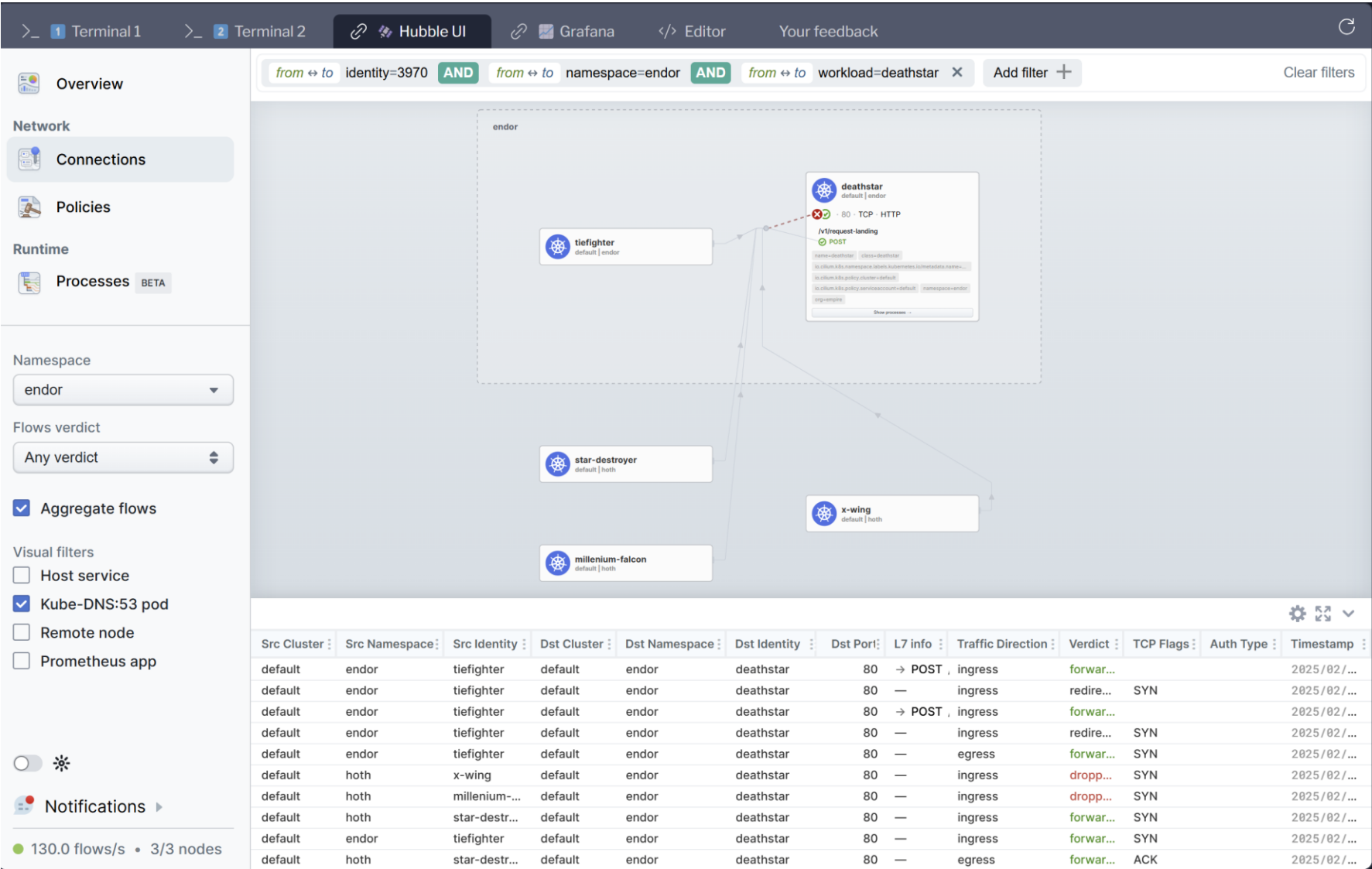
10 class: deathstar

11

Preferences

Src Identity	Dst Identity	Traffic Direction	Verdict
tiefighter	deathstar	egress	forwarded
tiefighter	deathstar	egress	forwarded
tiefighter	deathstar	ingress	forwarded
tiefighter	deathstar	ingress	forwarded

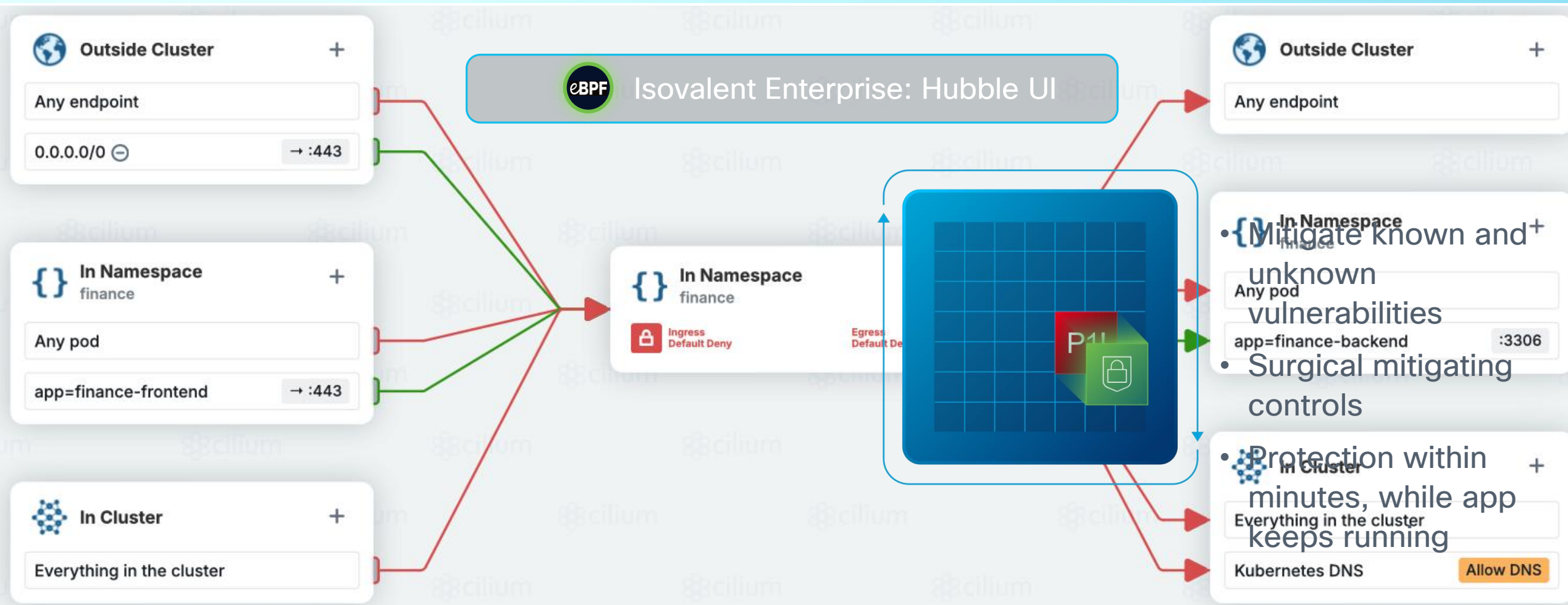
Add layer 7 visibility and enforcement



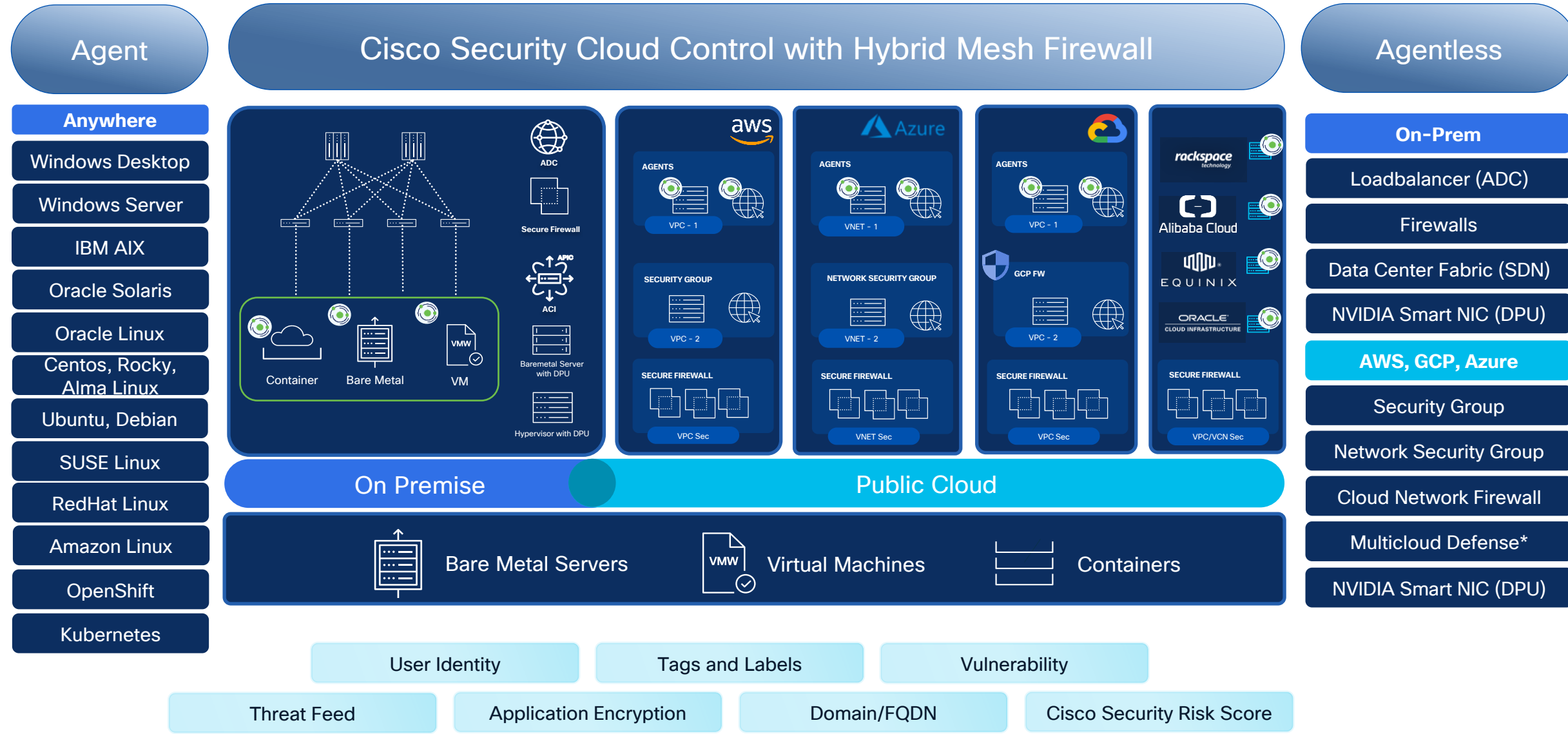
Manual

Innovations from Isovalent Automated by Hypershield

Autonomous

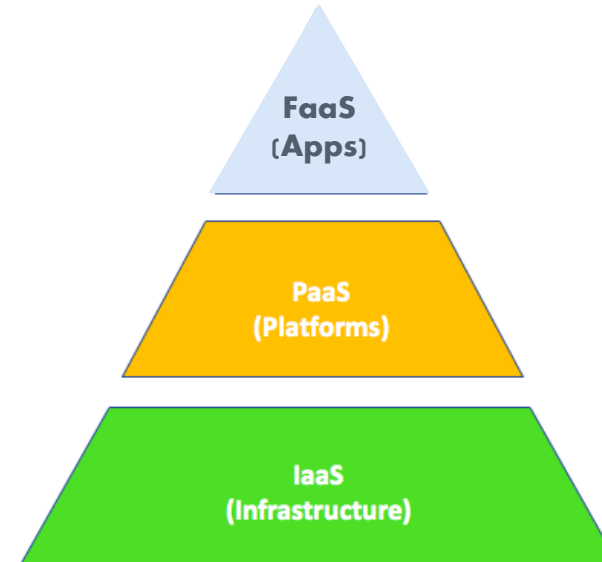


Zero Trust coverage for apps from on-premises to cloud



Moving to the Cloud...

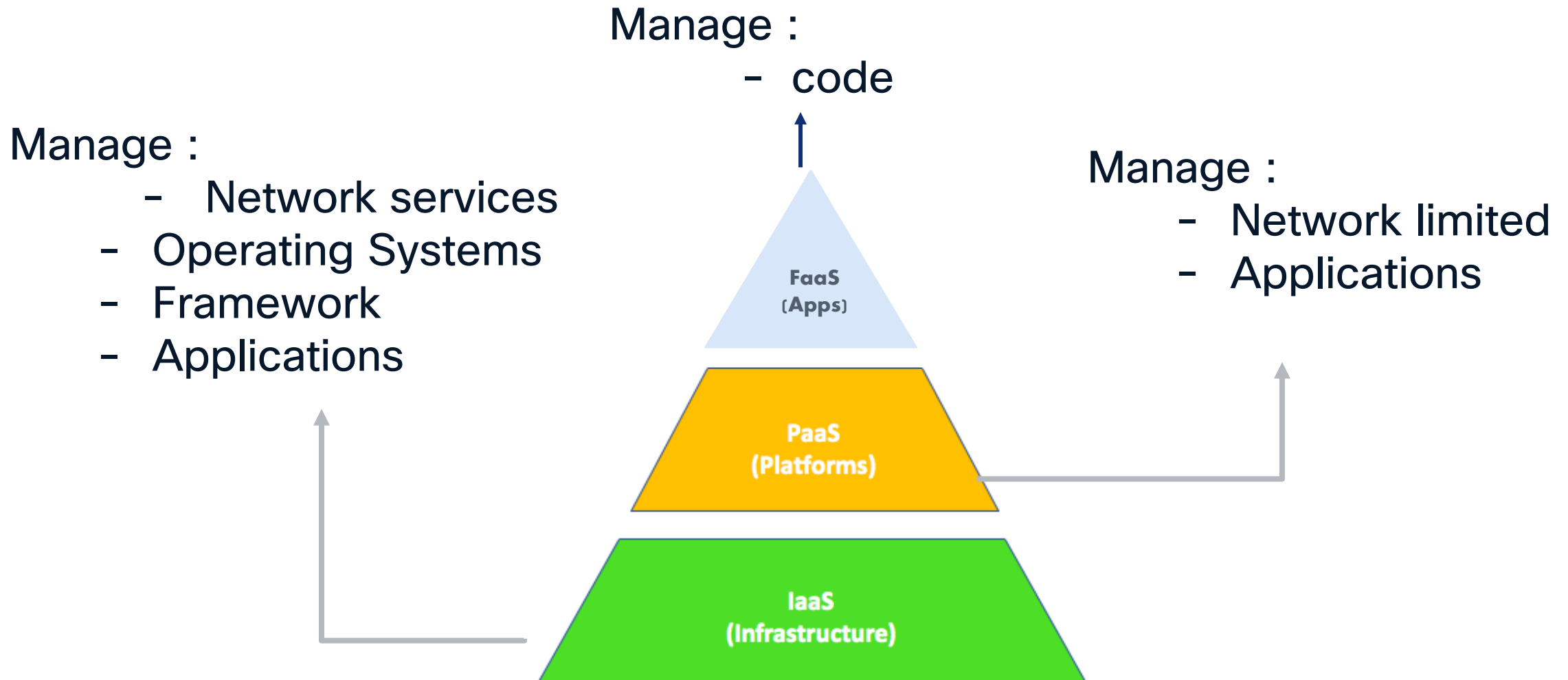
Two new parameters to consider in Cloud



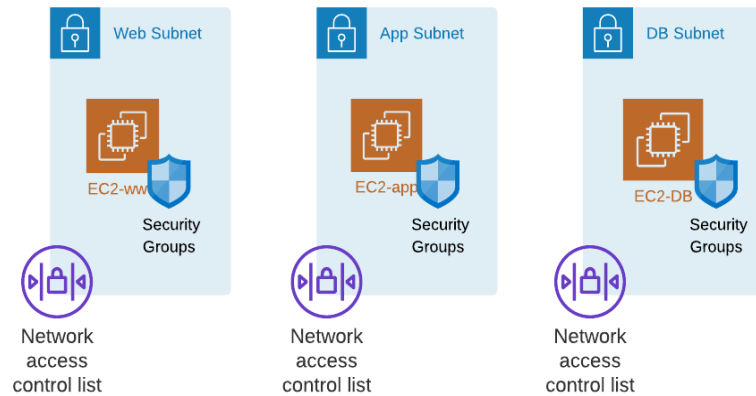
New Infrastructure skills for each Service
Cloud Providers

Public Cloud Service Model

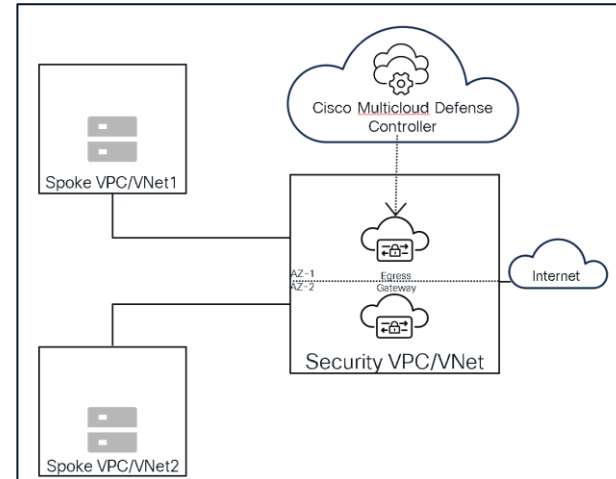
IaaS compared to PaaS Compared to FaaS



The way we do it in the Cloud...



Public Cloud
Infrastructure



Firewall
(Multicloud Defense, FTDv)

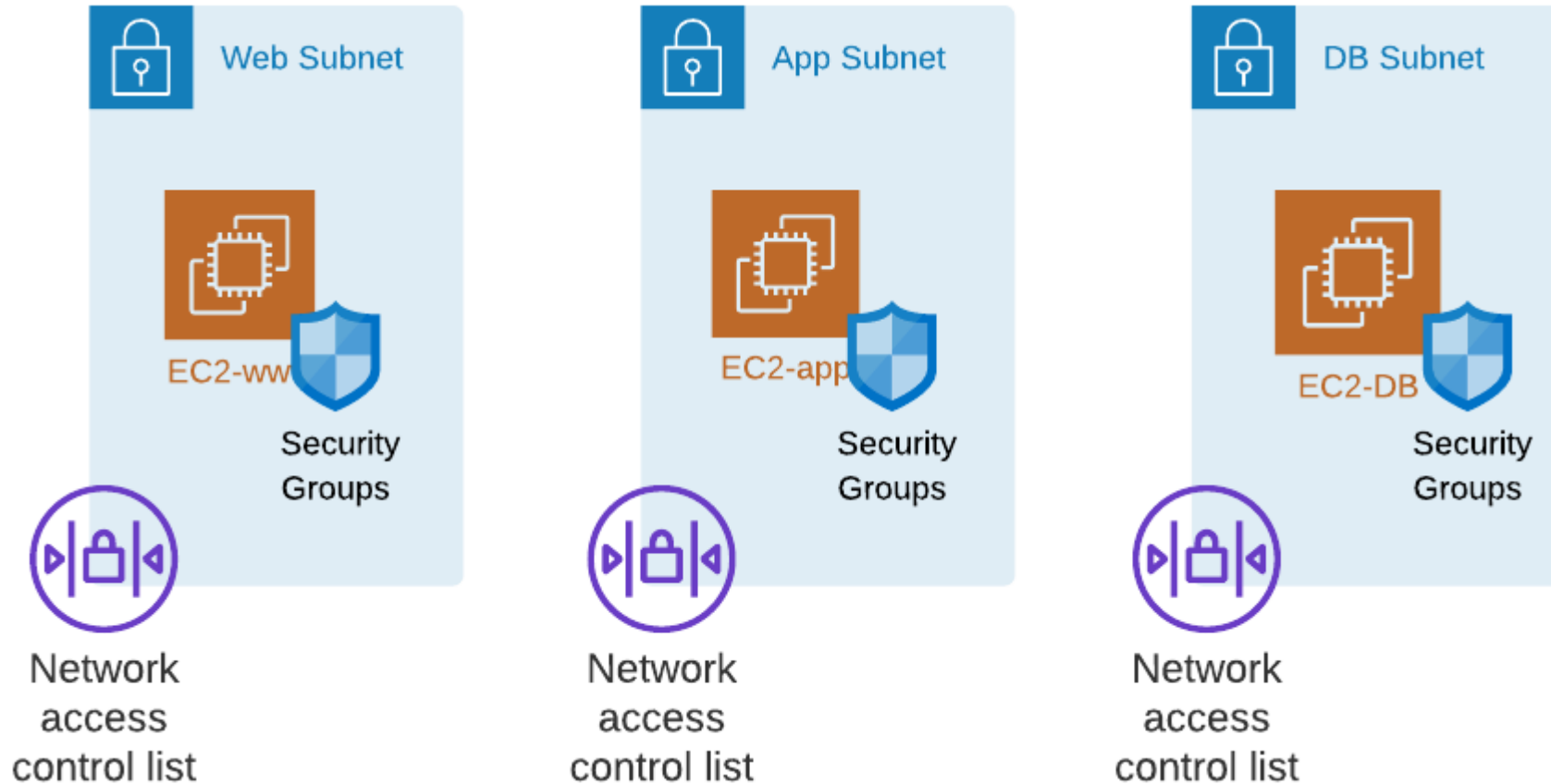


CISCO **SECURE**
Workload

Host based
Firewall

Macrosegmentation in the Cloud

Security Groups and Network Access list

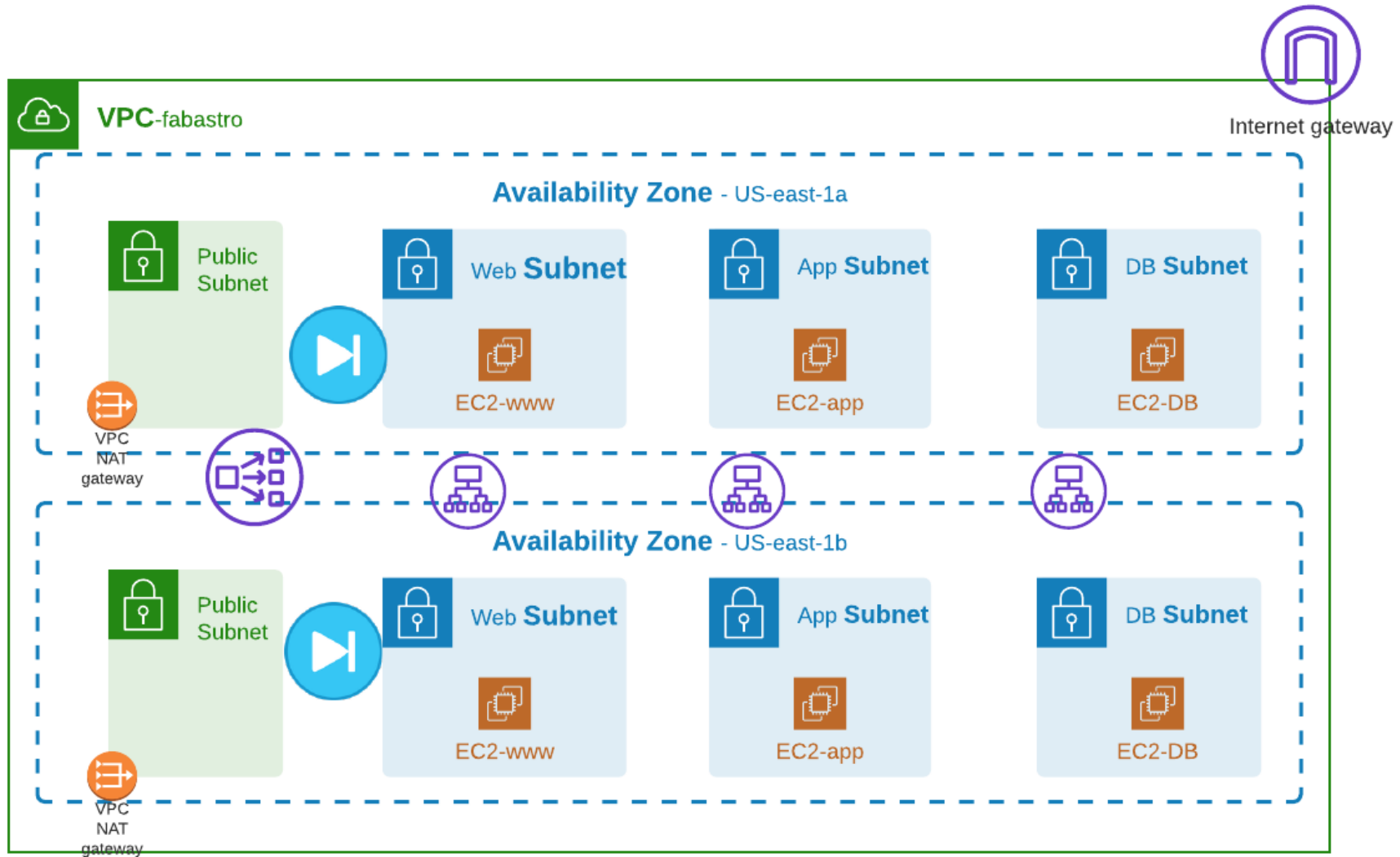


Use security group as Source within VPC

Inbound rules Info						
Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
sgr-0e10062e4544d68b7	SSH ▼	TCP	22	Custom ▼	<div><input type="text" value="93.6.40.55/32"/></div>	<div><input type="text"/></div> <div>Delete</div>
-	All ICMP - IPv4 ▼	ICMP	All	Custom ▼	<div><input type="text" value="sg-0348c8d389e1ad1bd"/></div>	<div><input type="text"/></div> <div>Delete</div>

Back to Network security with Firewall

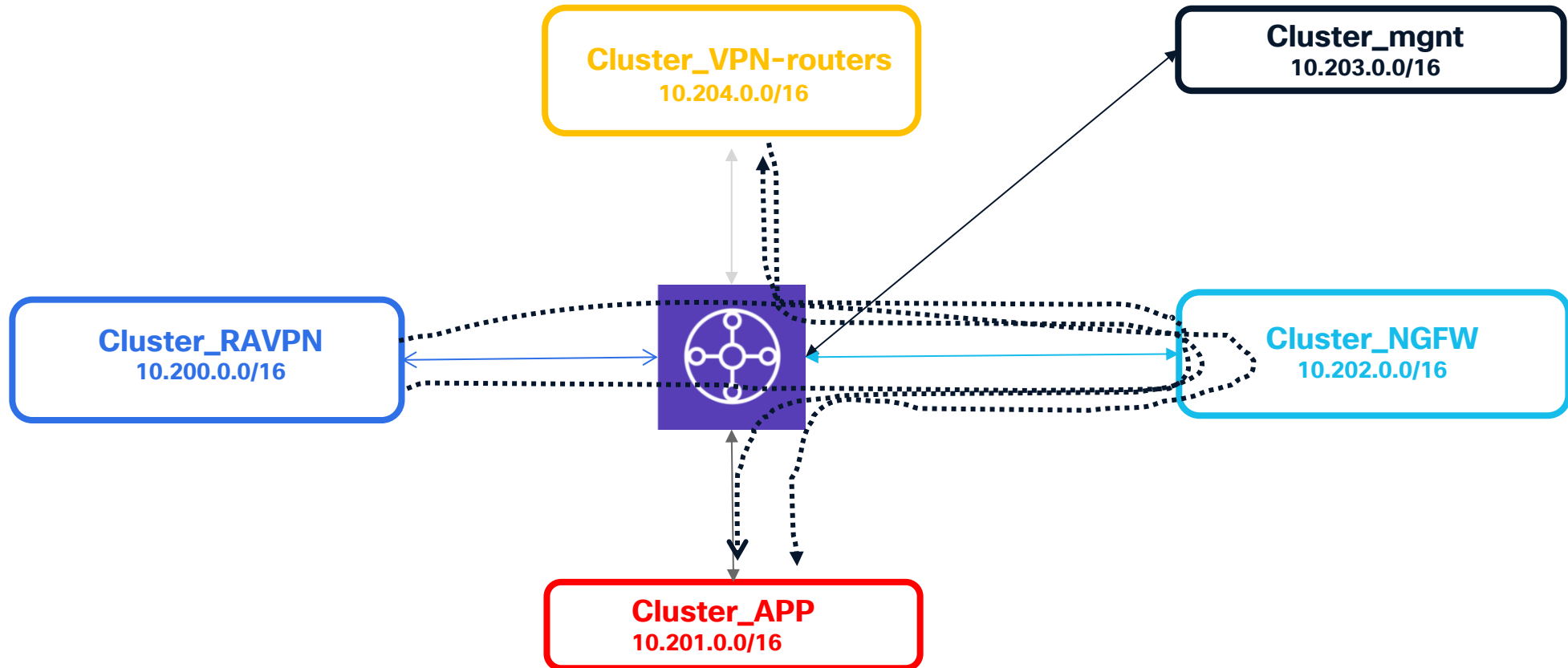
FTD insertion with HA

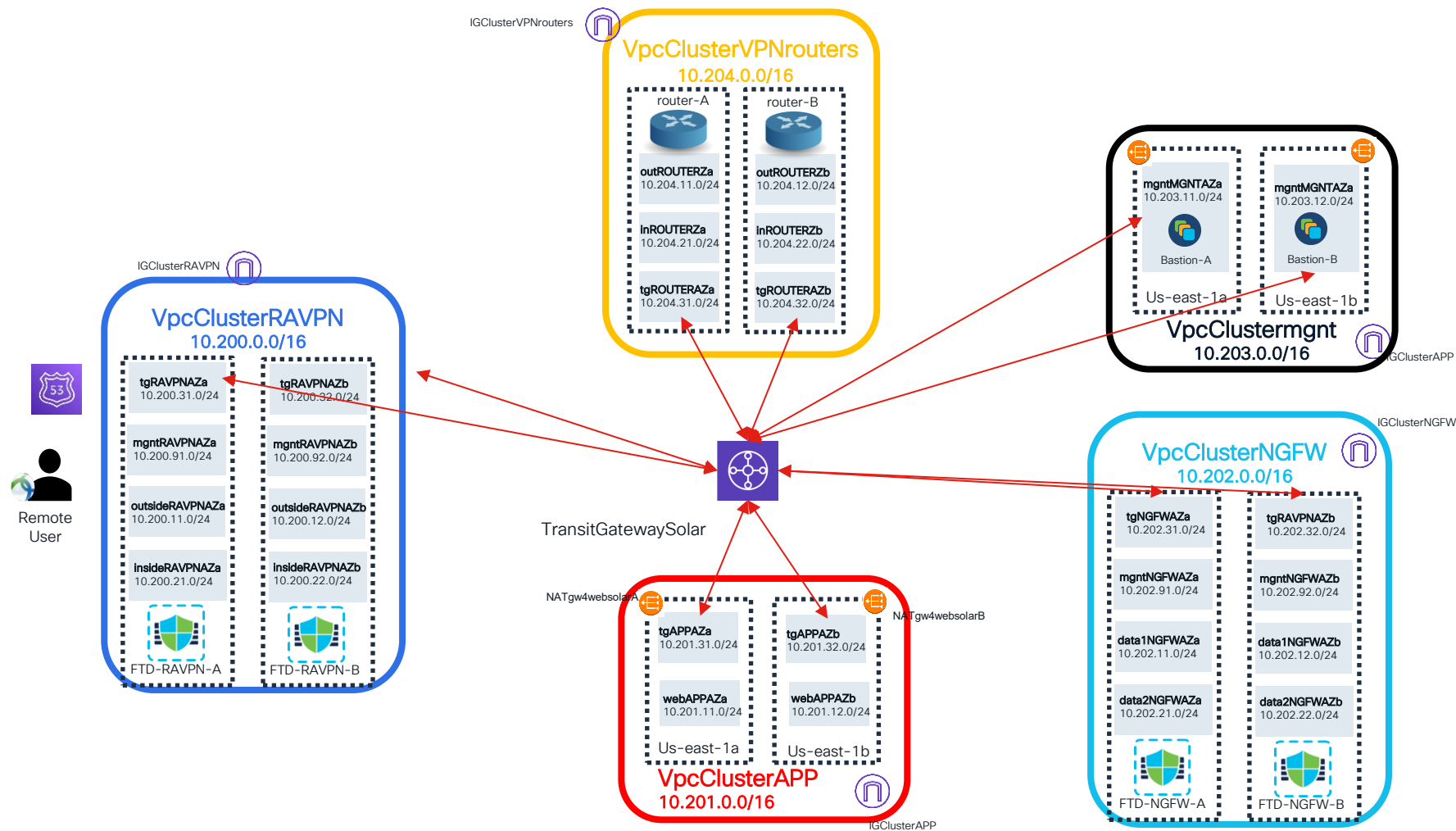


Limits of this design



Security Insertion with Service VPC





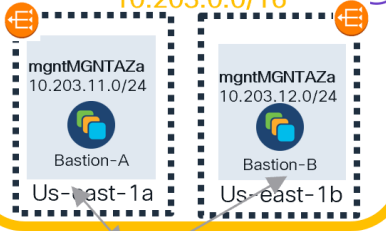
mgntTableMGNT

10.201.0.0/16 → mgnytgtVPCattachment
10.202.0.0/16 → mgnytgtVPCattachment
10.204.0.0/16 → mgnytgtVPCattachment
10.200.0.0/16 → mgnytgtVPCattachment
0.0.0.0/0 → IGClusterAPP

Cluster_mgnt

vpc-0884c73ab1840747e
10.203.0.0/16

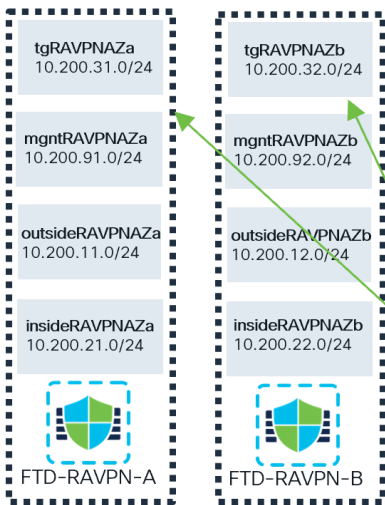
IGClusterAPP



IGClusterRAVPN

Cluster_RAVPN

vpc-0bb0e7dc4edfa6848
10.200.0.0/16



TGW rt MGNT

10.202.0.0/16 → ngfwtgtVPCattachment
10.200.0.0/16 → ravpntgtVPCattachment
10.201.0.0/16 → apptgtVPCattachment
10.204.0.0/16 → vpnroutertgtVPCattachment



TransitGateway
Solar

TGW rt Inspection

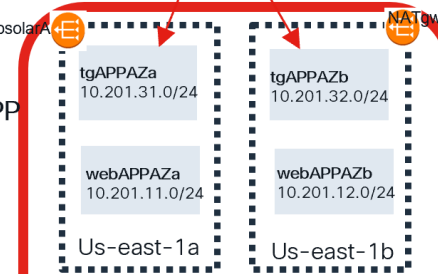
10.199.0.0/16 → ravpntgtVPCattachment
10.200.0.0/16 → ravpntgtVPCattachment
10.201.0.0/16 → apptgtVPCattachment
10.203.0.0/16 → mgnytgtVPCattachment

ngfwtgtVPCattachment

TGW rt SPOKE

0.0.0.0/0 → ngfwtgtVPCattachment
10.203.0.0/16 → mgnytgtVPCattachment

apptgtVPCattachment



Cluster_APP

vpc-03970f4882f78640d
10.201.0.0/16

IGClusterAPP

IGClusterNGFW

Cluster_NGFW

vpc-031a746e4abb1b2ed
10.202.0.0/16



egwlbendpointRouteNGFW

10.202.101.0/24 → LOCAL
0.0.0.0 → ngfwtgtVPCattachment

tgAZa RouteNGFW

10.202.0.0/16 → LOCAL
0.0.0.0 → egwlbNGFWendpoints
10.203.0.0/16 → ngfwtgtVPCattachment

tgAZb RouteNGFW

10.202.0.0/16 → LOCAL
0.0.0.0 → egwlbNGFWendpoints
10.203.0.0/16 → ngfwtgtVPCattachment

mgntTableNGFW

10.203.0.0/16 → mgnytgtVPCattachment
0.0.0.0/0 → IGClusterAPP

tgwrouteRAVPN

10.199.1.0/24 → insideRAVPNENIA
10.199.2.0/24 → insideRAVPNENIB
0.0.0.0/0 → ravpntgtVPCattachment

insARouteTableRAVPN

10.201.0.0/16 → TGW-attach-VPC-ravpn
10.204.0.0/16 → TGW-attach-VPC-ravpn

insBRouteTableRAVPN

10.201.0.0/16 → TGW-attach-VPC-ravpn
10.204.0.0/16 → TGW-attach-VPC-ravpn

mgntRouteTableRAVPN

0.0.0.0/0 → IGClusterRAVPN
10.203.0.0/16 → TGW-attach-VPC-ravpn

outsideAZa TableRAVPN

0.0.0.0/0 → IGClusterRAVPN

tgAPPAZaRouteTableAPP

0.0.0.0 → IGClusterAPP

APP rt web Aza

10.199.0.0/16 → TGW-attach-VPC-APP
10.200.0.0/16 → TGW-attach-VPC-APP
10.201.0.0/16 → LOCAL
10.203.0.0/16 → TGW-attach-VPC-APP
10.204.0.0/16 → TGW-attach-VPC-APP
0.0.0.0/0 → NATgw4websolarA

APP rt web Azb

10.199.0.0/16 → TGW-attach-VPC-APP
10.200.0.0/16 → TGW-attach-VPC-APP
10.201.0.0/16 → LOCAL
10.203.0.0/16 → TGW-attach-VPC-APP
10.204.0.0/16 → TGW-attach-VPC-APP
0.0.0.0/0 → NATgw4websolarB

Multi-Cloud Security configuration complexity

What do we need to
configure?

Security VPCs

VPC and DNS Flow Log capture

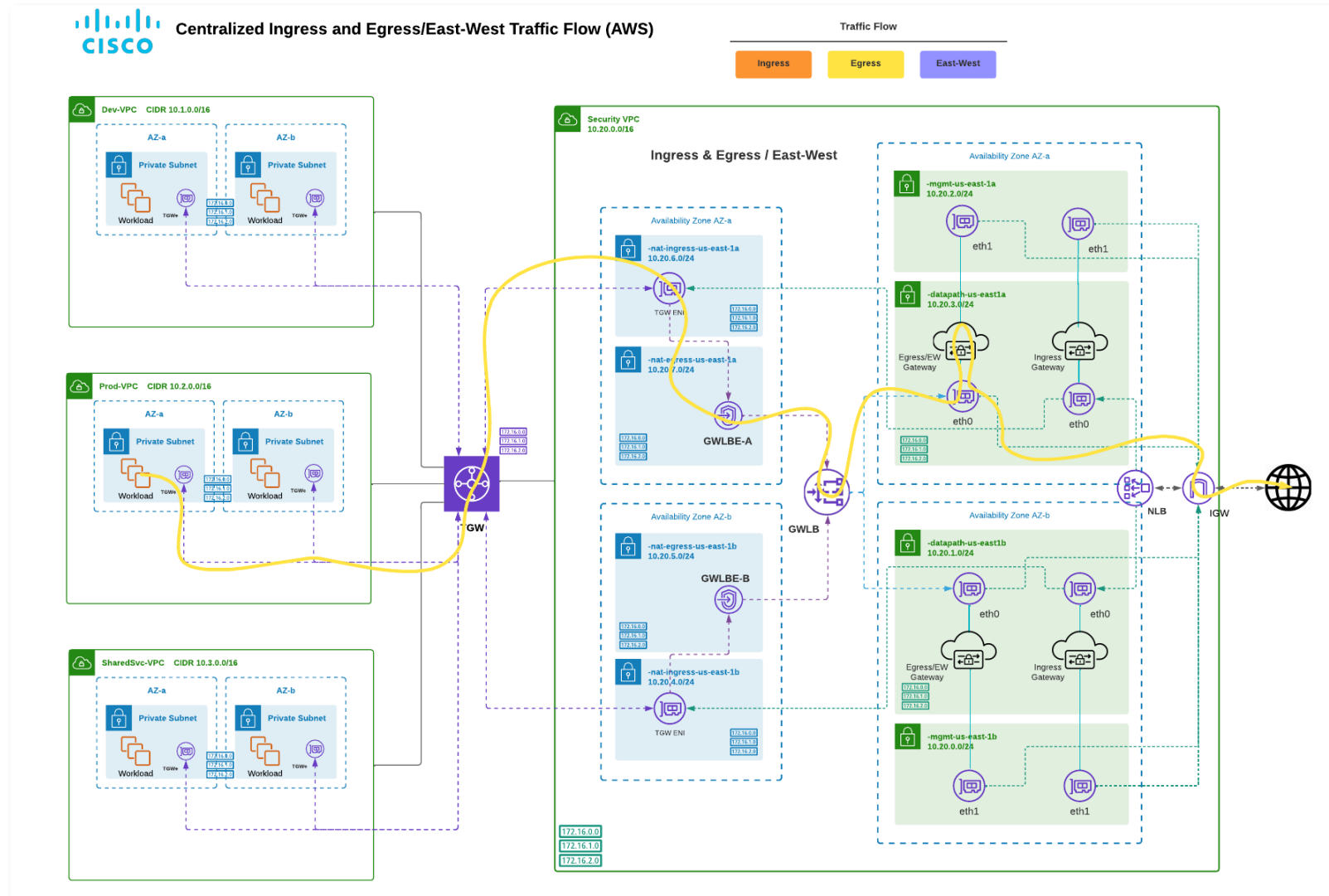
Network Load Balancer

Gateway Load Balancers

Multicloud Defense Gateways
(Deployment, Insertion, Autoscaling)

AWS Transit Gateways
(New or existing, TGW attachment)

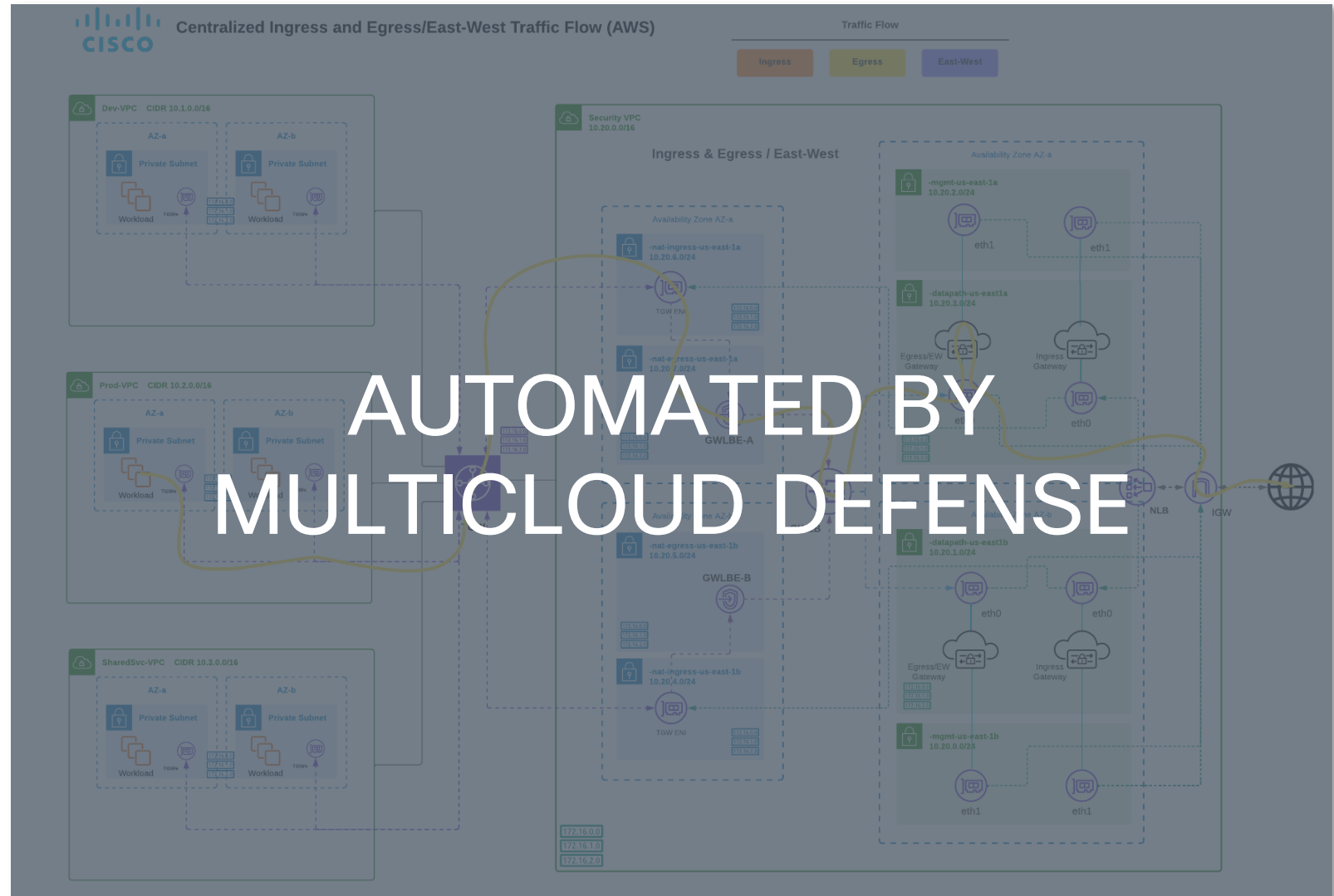
VPC subnet routing to TGW



Cisco Multicloud Defense automates orchestration

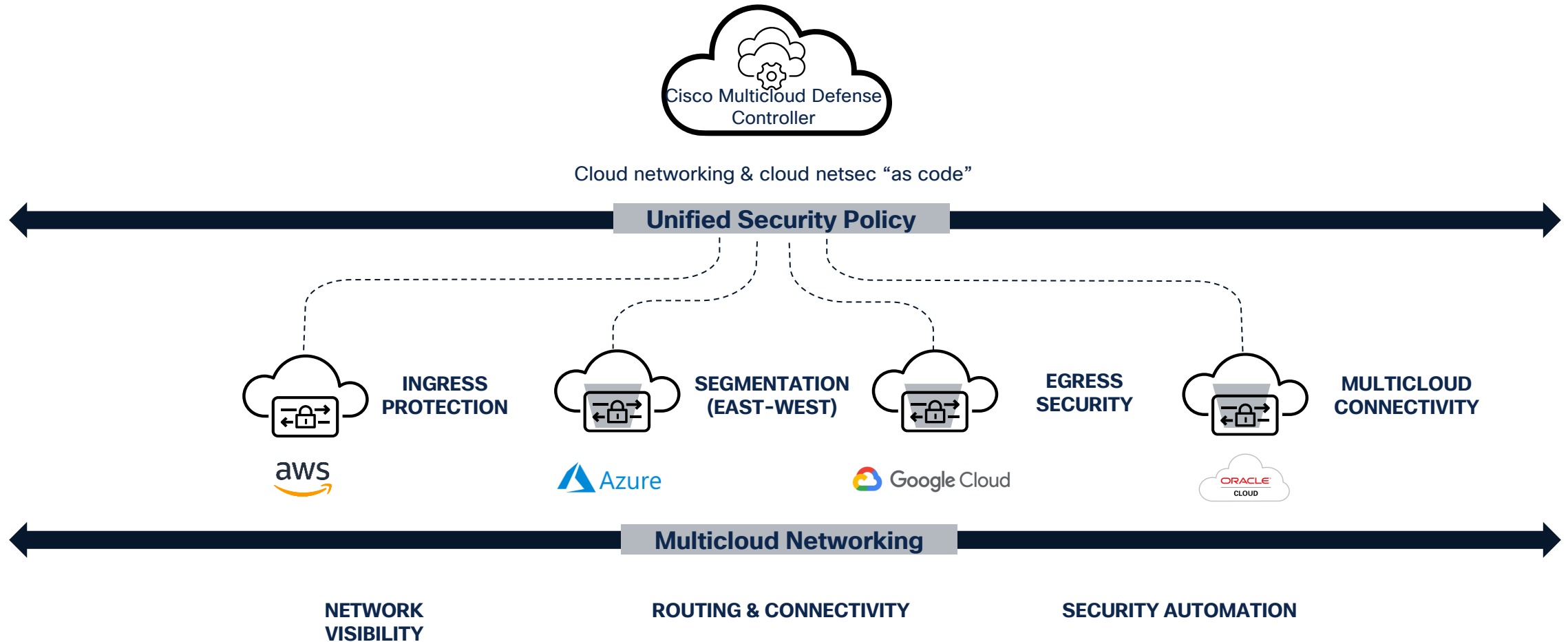
What do we need to
configure?

AUTOMATED
BY
MULTICLOUD
DEFENSE



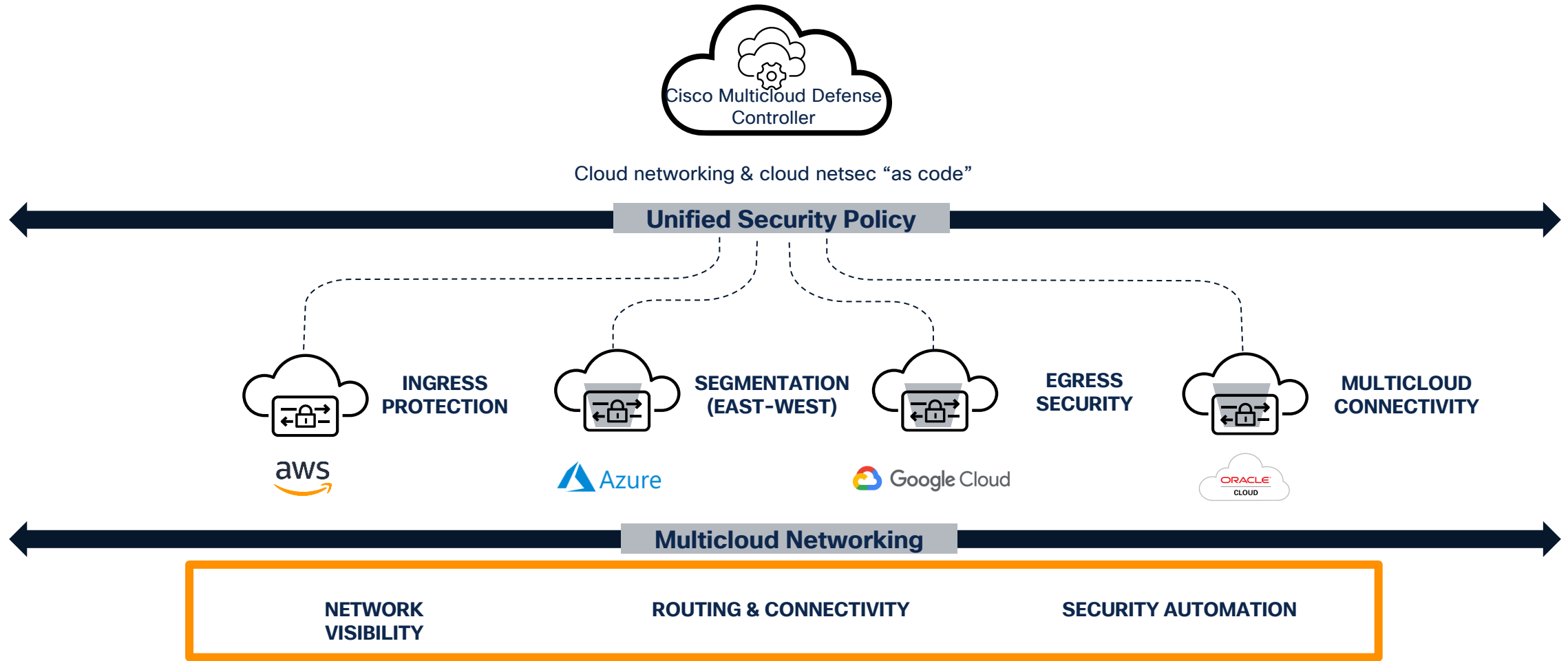
Cisco Multicloud Defense

Combining multicloud networking, automation, and cloud-native network security controls



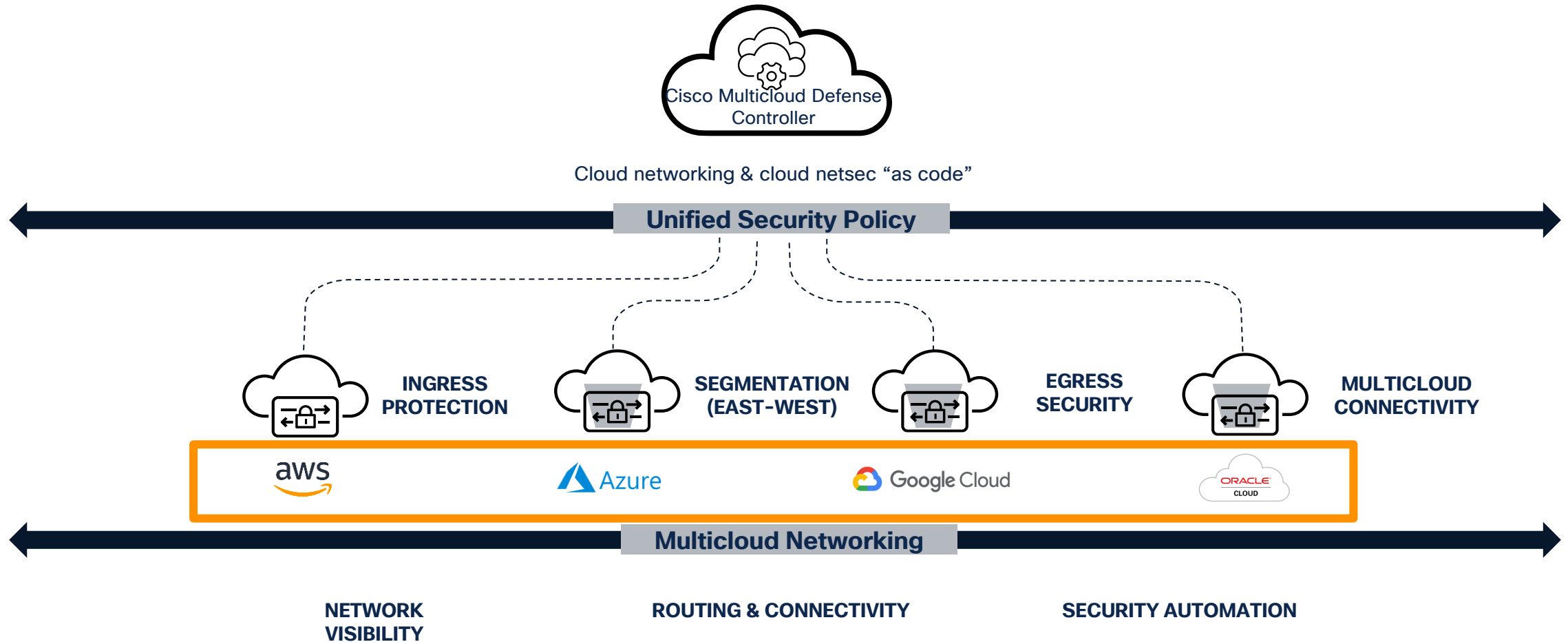
Cisco Multicloud Defense

Combining multicloud networking, automation, and cloud-native network security controls



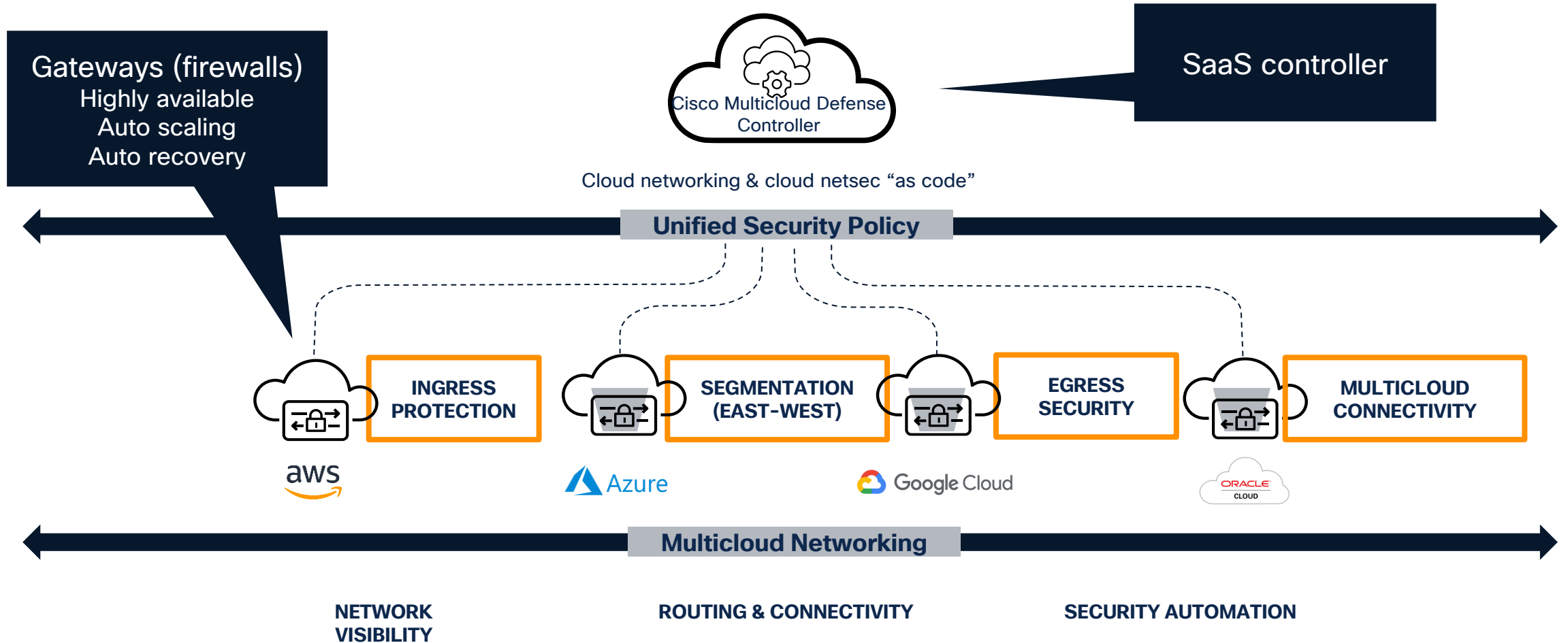
Cisco Multicloud Defense

Combining multicloud networking, automation, and cloud-native network security controls



Cisco Multicloud Defense

Combining multicloud networking, automation, and cloud-native network security controls



Fully Orchestrated



{ **REST:API** }

A screenshot of a code editor with a dark theme. The left sidebar shows an 'EXPLORER' view with a file tree for 'CISCOMCD-DEPLOY'. The main editor area shows the 'ciscomcd_gateway.tf' file, which contains Terraform configuration for an AWS ingress gateway. The code includes comments and variable assignments for various parameters like account name, gateway image, instance type, and settings. The cursor is positioned at the end of a resource block definition.

```
1 # Cisco MCD Terraform Documentation
2 # https://registry.terraform.io/providers/ciscomcd-security/ciscomcd/latest/docs
3 # AWS Terraform Documentation
4 # https://registry.terraform.io/providers/hashicorp/aws/latest/docs
5
6 # Create a new Cisco MCD Ingress Gateway Stack
7 # If the desire is to destroy the Gateway Stack, comment out the resource block
8 # If the desire is to create the Gateway Stack, uncomment out the resource block
9 resource "ciscomcd_gateway" "ingress_gateway" {
10   name = var.ciscomcd_ingress_gateway_name
11   csp_account_name = var.ciscomcd_aws_account_name
12   gateway_image = var.ciscomcd_ingress_gateway_version
13   instance_type = var.ciscomcd_ingress_gateway_instance_type
14   mode = "HUB"
15   security_type = var.ciscomcd_ingress_gateway_security_type
16   policy_rule_set_id = ciscomcd_policy_rule_set.ingress_policy.rule_set_id
17   #policy_rule_set_id = data.ciscomcd_policy_rule_set.ingress_policy.rule_set_id
18   ssh_key_pair = var.ciscomcd_ingress_gateway_ssh_key_pair
19   aws_iam_role_firewall = var.ciscomcd_firewall_role_name
20   region = var.aws_account_region
21   vpc_id = ciscomcd_service_vpc.service_vpc.id
22   min_instances = var.ciscomcd_ingress_gateway_autoscale_min
23   max_instances = var.ciscomcd_ingress_gateway_autoscale_max
24   gateway_state = var.ciscomcd_ingress_gateway_status
25   # settings {
26   #   name = "controller.use_internal_lb"
27   #   value = var.ciscomcd_ingress_gateway_internal_lb
28   # }
29
30 }
```

A screenshot of an API client interface with a dark theme. The left sidebar shows a tree view of API endpoints under 'Cisco MCD - Sample API'. The main area shows a 'POST' request to '((baseUrl))/api/v1/gateway/run...'. The 'Body' tab is selected, displaying a JSON payload for creating a gateway. The payload includes fields for account name, source, client version, gateway name, csp account name, name, description, mode, type, min/max instances, health check port, policy rule set ID, flags, and settings.

```
1 {
2   "common": {
3     "acctName": "{{acctName}}",
4     "source": "RESTAPI",
5     "clientVersion": "CiscoMCD-2022"
6   },
7   "gateway": {
8     "cspAcctName": "AWS-Account3",
9     "name": "aws-egress-gw",
10    "description": "AWS EDGE Gateway",
11    "mode": "EDGE",
12    "type": "CLUSTER",
13    "minInstances": 1,
14    "maxInstances": 1,
15    "healthCheckPort": 65534,
16    "policyRuleSetId": 20,
17    "flags": [
18      "GATEWAY_FLAGS_EGRESS_FIREWALL",
19      "GATEWAY_FLAGS_AWS_GATEWAY_LB"
20    ]
21  },
22  "settings": [
23    {
24      "name": "gateway.aws.ebs.encryption.key.default"
25    },
26    {
27      "name": "controller.gateway.assign_public_ip",
28      "value": "true"
29    },
30    {
31      "name": "gateway.fqdn_ip_cache.entry_ttl",
32      "value": "300"
33    }
34  ]
35 }
```

Secure multicloud infrastructure in mins with Cisco Multicloud Defense

Step 1

Connect Account



Connect a cloud account with the Multicloud Defense Controller

Connect Account

Securely onboard Cloud accounts

Step 2

Enable Traffic Visibility



Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account

Enable Visibility

Enable DNS query & VPC/NSG flow logs

Step 3

Secure Your Account

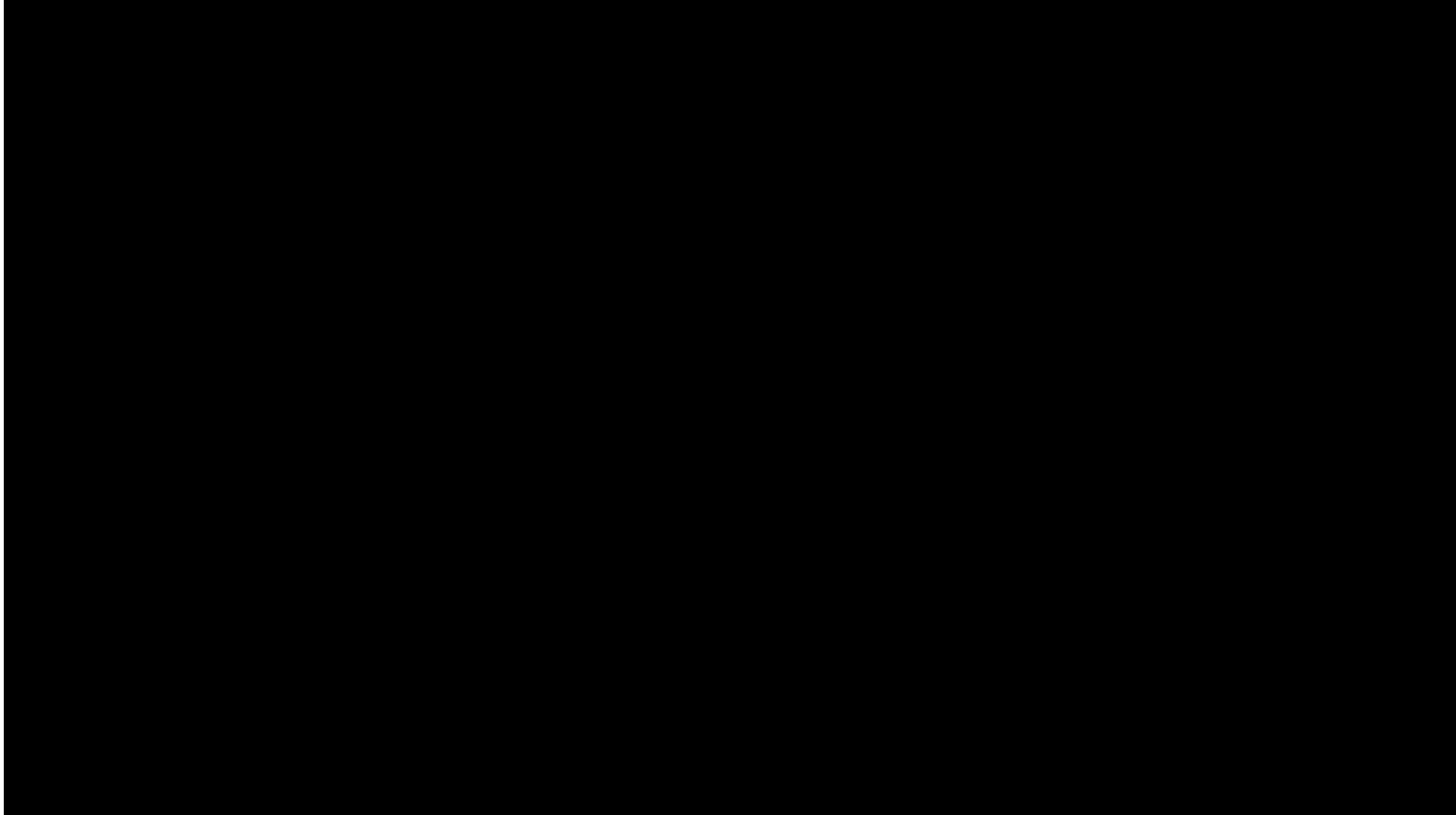


Setup a Service VPC and Multicloud Defense Gateway to secure your Account

Secure Account

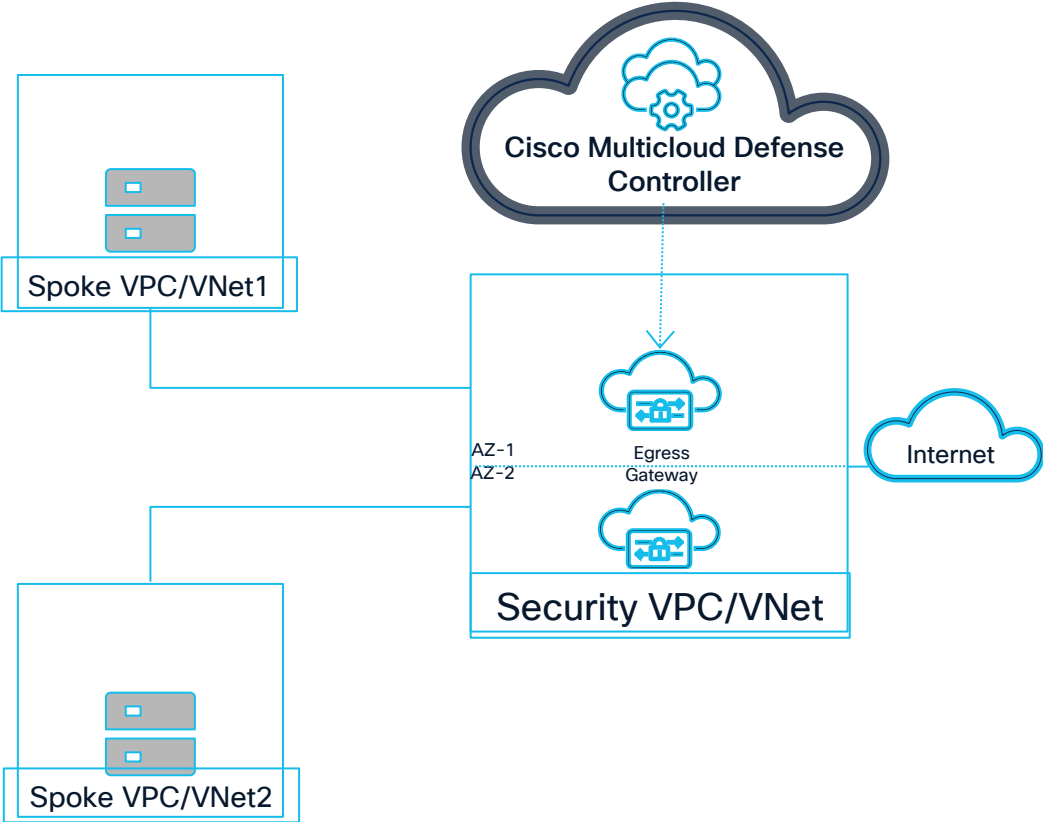
Orchestration and Automation

Multicloud Defense Demo

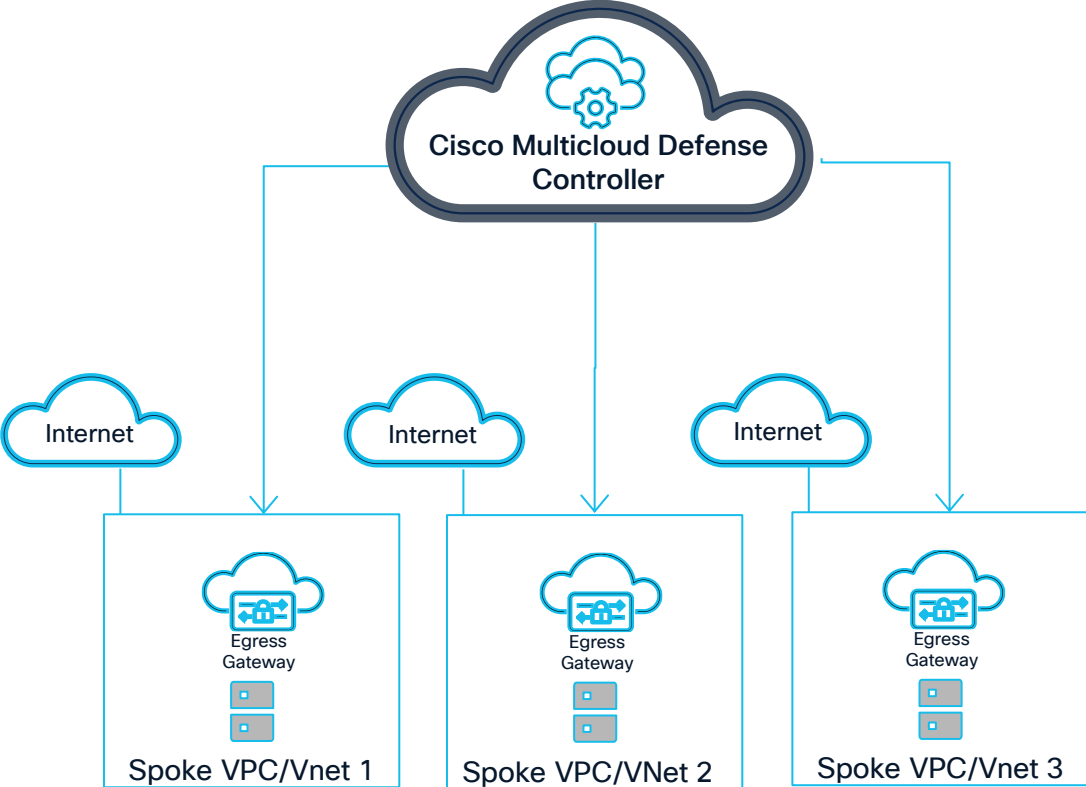


Deployment Models

Centralized Security Model



Distributed Security Model



Centralized Security Model

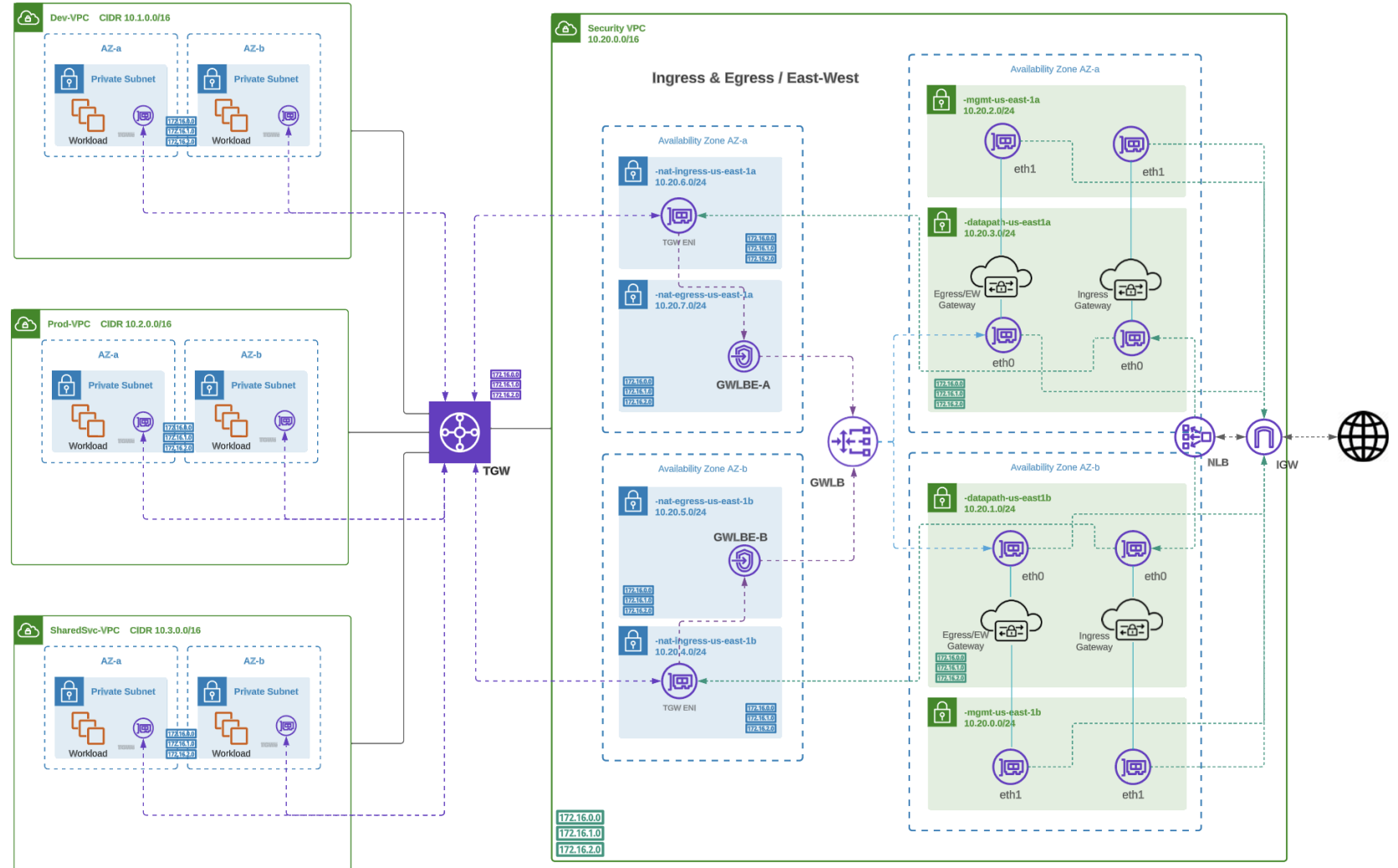
Amazon Web Services

Orchestration

Security VPC
Network Load Balancer
Gateway Load Balancer
Transit Gateway and attachments
Autoscale and auto heal
Traffic Engineering – Route Table

Lifecycle management

Ingress and Egress Gateway



Centralized Security Model – Egress Traffic

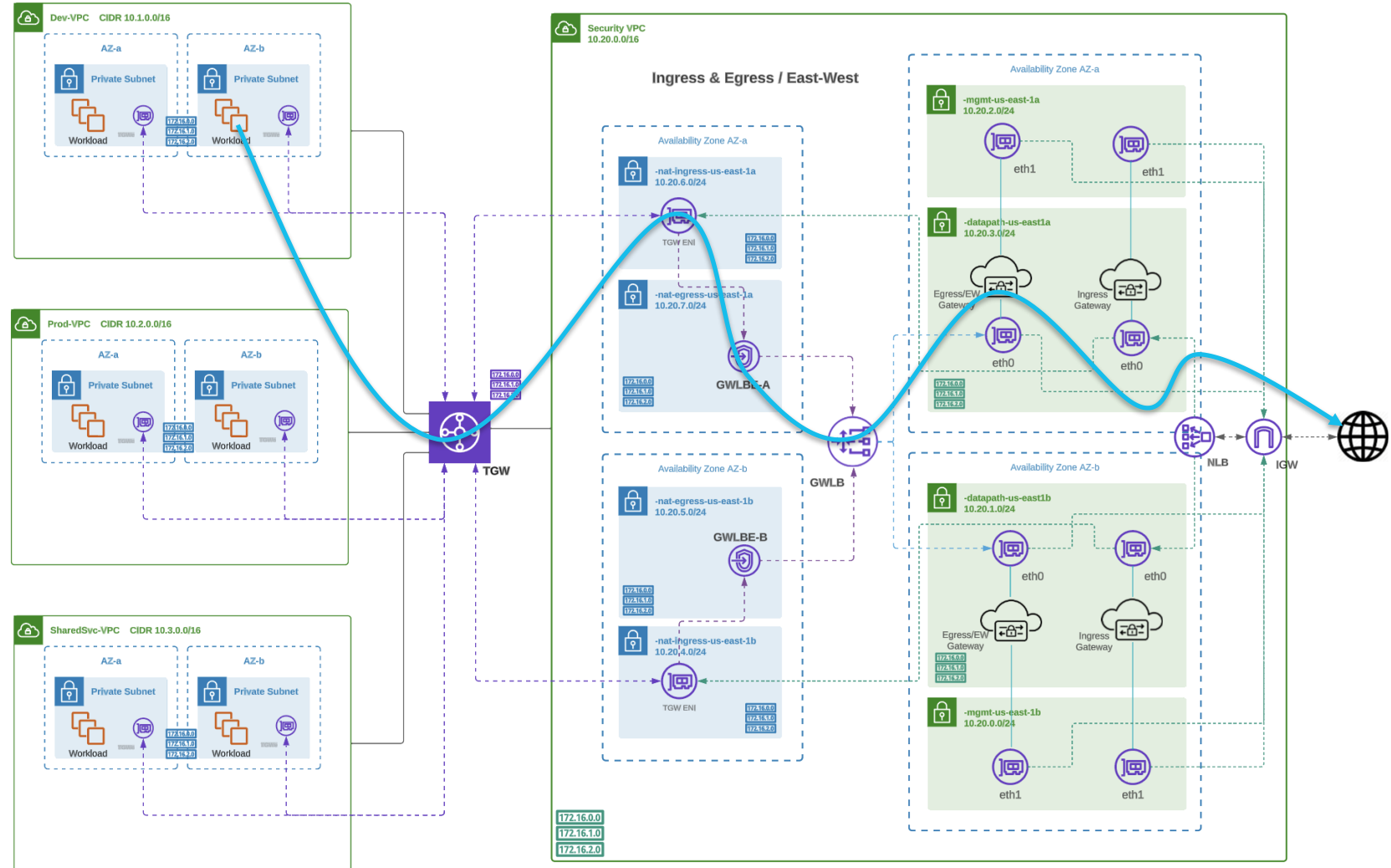
Amazon Web Services

Orchestration

Security VPC
Network Load Balancer
Gateway Load Balancer
Transit Gateway and attachments
Autoscale and auto heal
Traffic Engineering – Route Table

Lifecycle management

Ingress and Egress Gateway



Centralized Security Model – Ingress Traffic

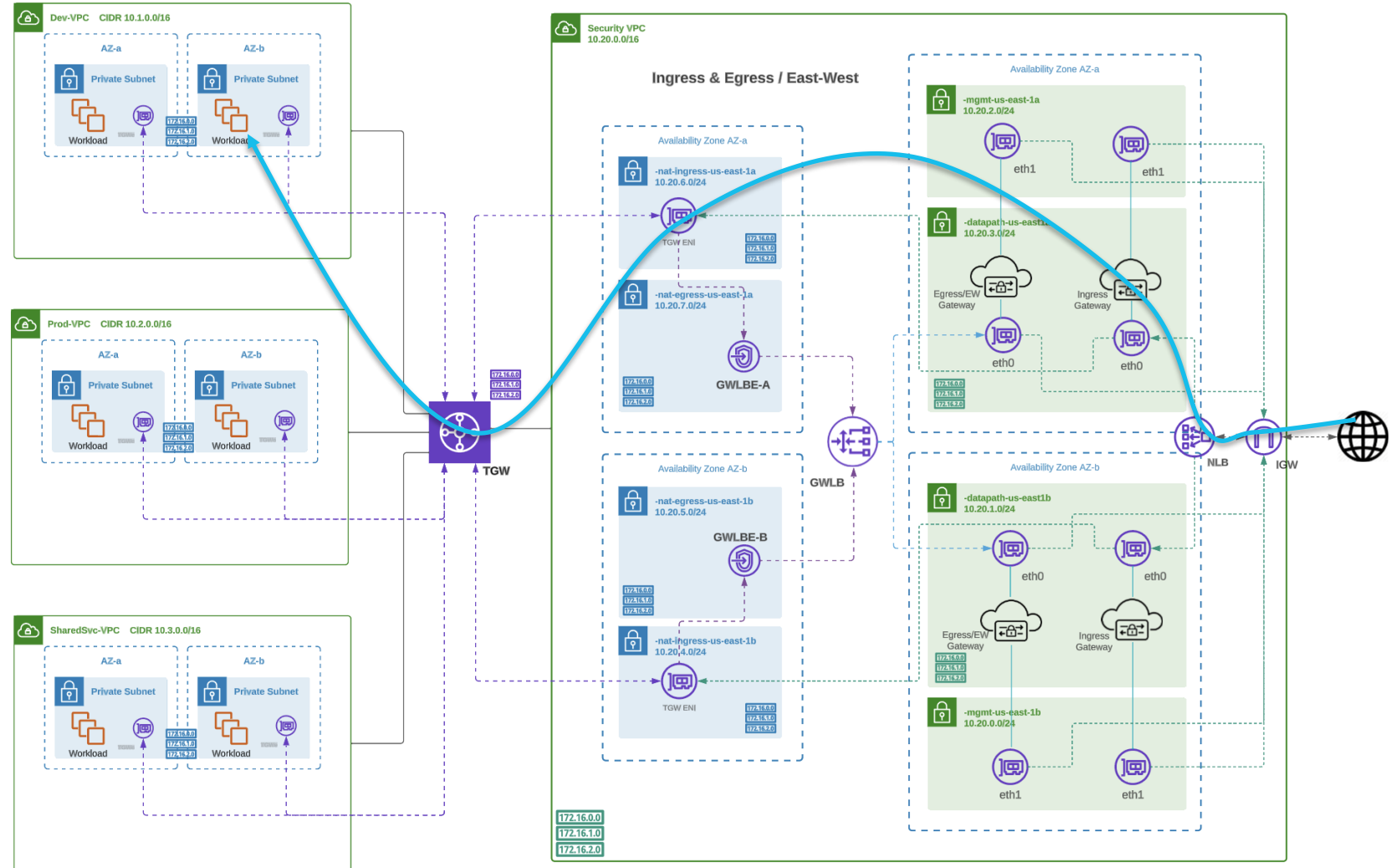
Amazon Web Services

Orchestration

Security VPC
Network Load Balancer
Gateway Load Balancer
Transit Gateway and attachments
Autoscale and auto heal
Traffic Engineering – Route Table

Lifecycle management

Ingress and Egress Gateway



Centralized Security Model _ East/West Segmentation

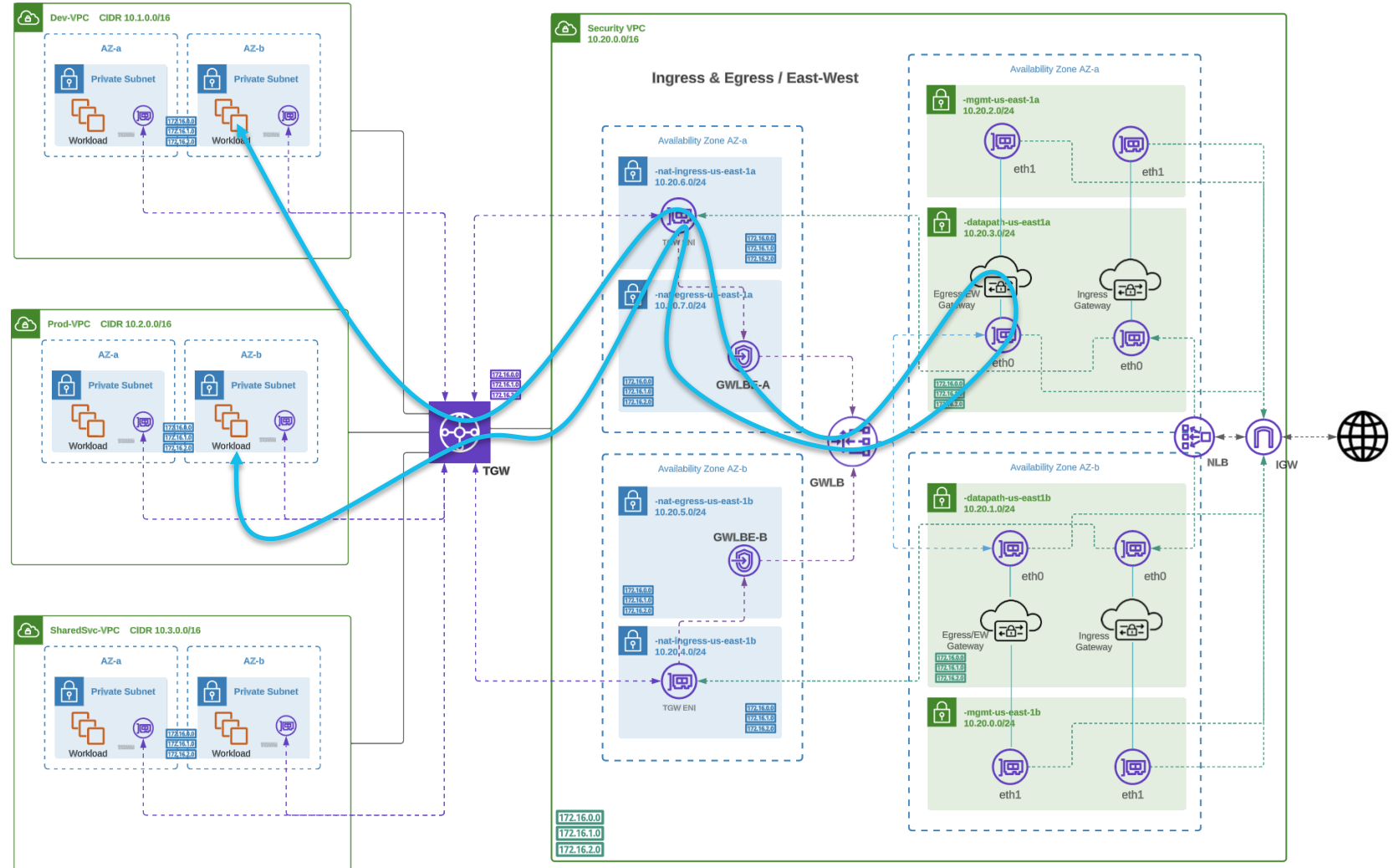
Amazon Web Services

Orchestration

Security VPC
Network Load Balancer
Gateway Load Balancer
Transit Gateway and attachments
Autoscale and auto heal
Traffic Engineering - Route Table

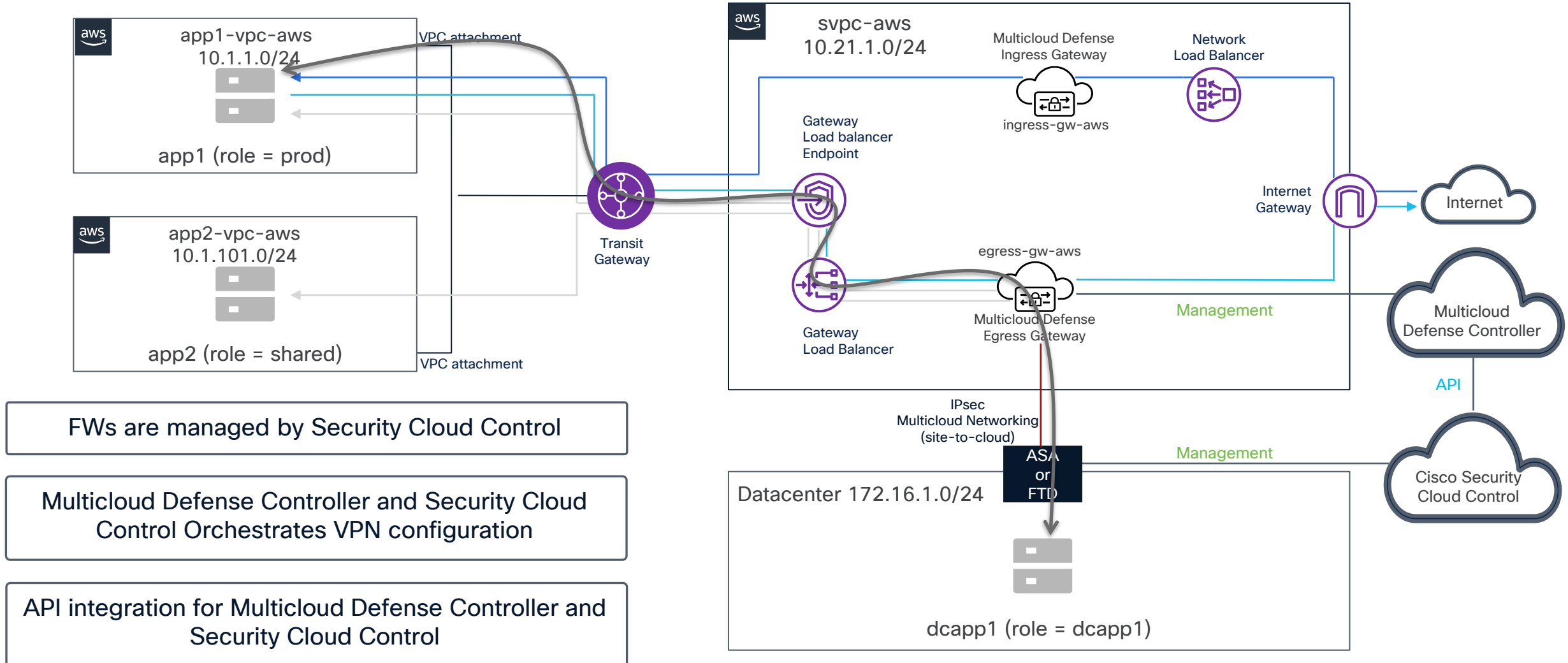
Lifecycle management

Ingress and Egress Gateway



Multicloud Networking

Site-to-cloud connectivity: Centralized Security Model



But I use FTD on Prem...

Secure Firewall Threat Defense Virtual

Private Cloud



Public Cloud



Gov/IC Cloud



Virtual firewall performance-based licensing from 100Mbps up to 16 Gbps

FTDv5 (100Mbps), FTDv10 (1 Gbps), FTDv20 (3 Gbps), FTDv30 (5 Gbps), FTDv50 (10 Gbps), and FTDv100 (16 Gbps)

Cloud Leadership

Clustering & Auto Scaling

Integration with cloud native services & infrastructure

Accelerated Networking

Smart & Tiered Licensing

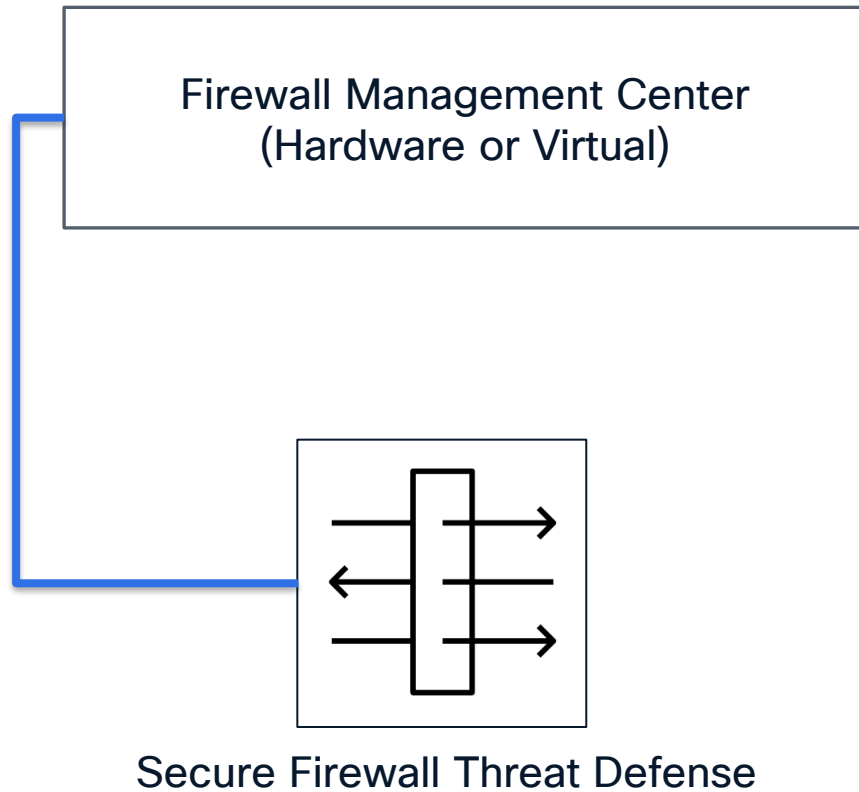
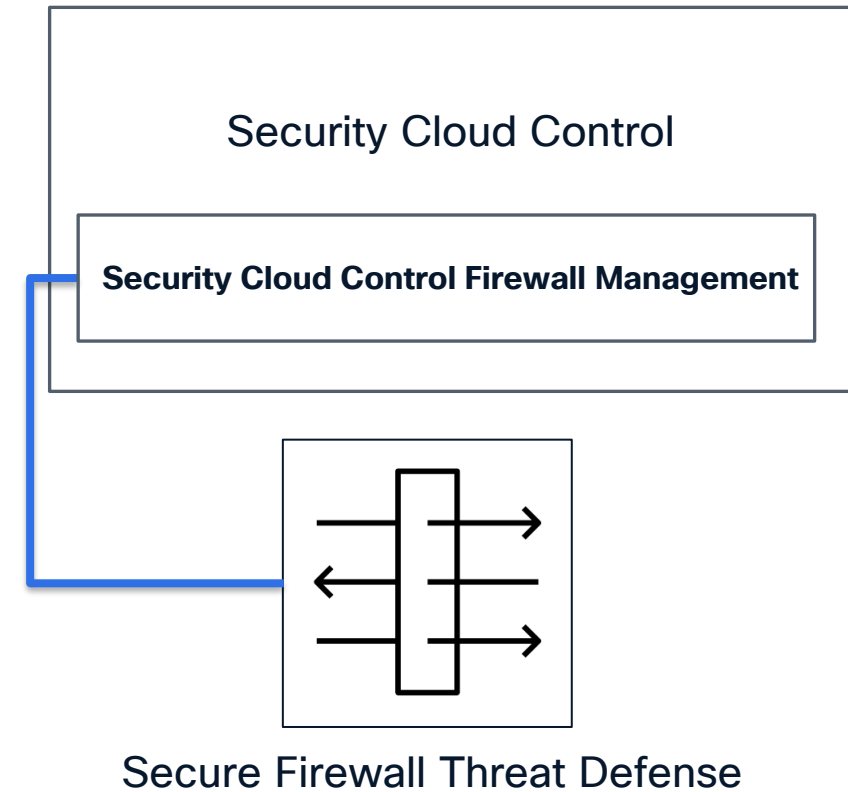
Dynamic Policy

Quickstarts, Infrastructure as Code and Automation

Gateway Load balancer integration

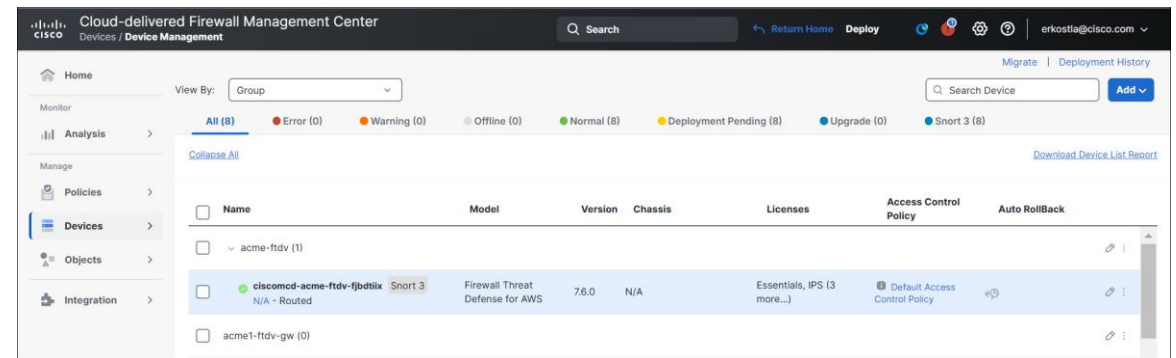
Snapshots

Firewall Management



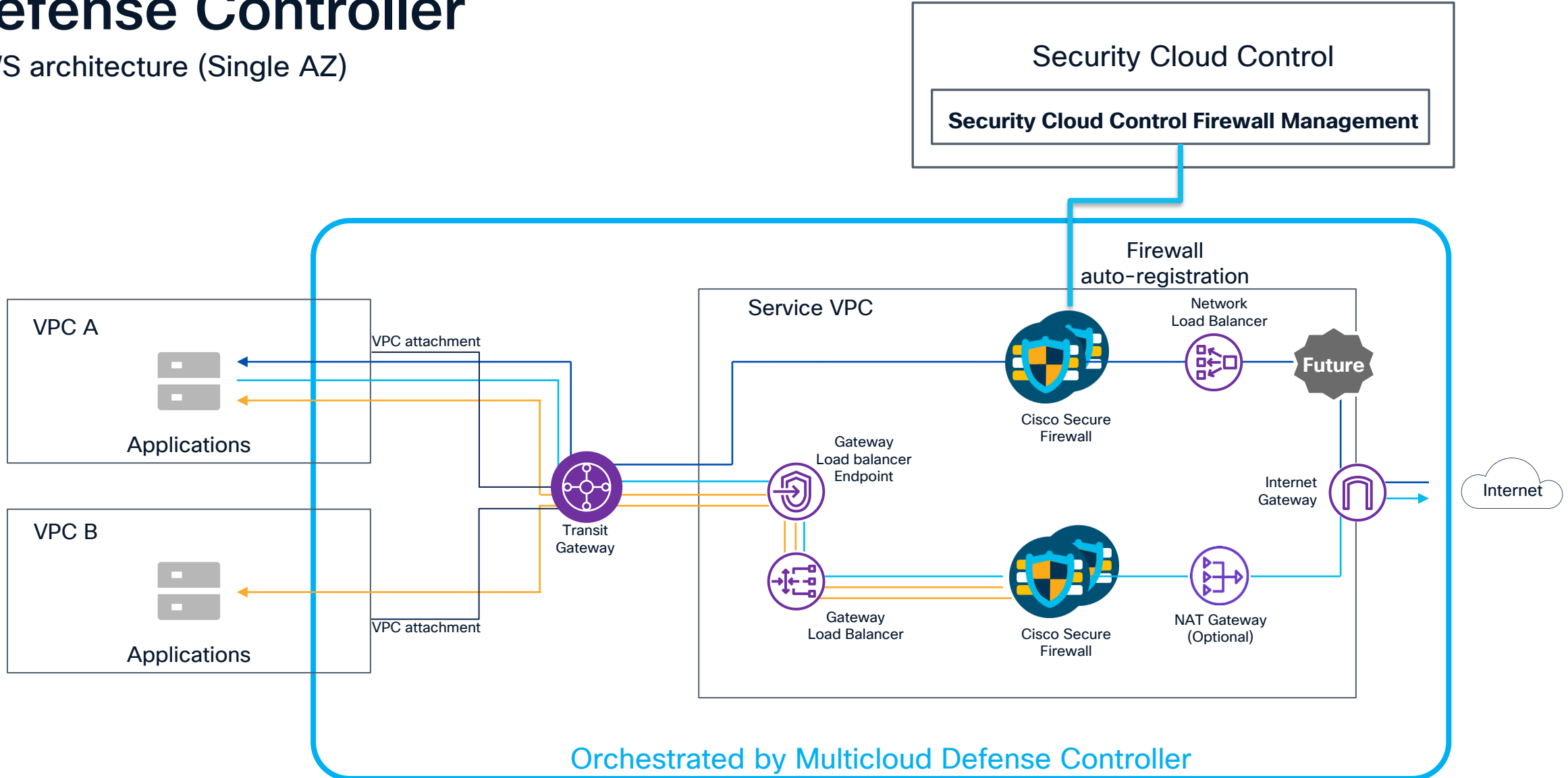
Secure Firewall Threat Defense Virtual orchestrated by Multicloud Defense Controller

- Simplifies Secure Firewall (FTDv) deployment
 - Deploy one or more firewalls, along with load balancers
 - Configures all necessary routing
 - Identical workflow for all public cloud providers
- Simplifies Secure Firewall (FTDv) operations
 - Automatically scales in or out FTDv's to adjust to load
 - Monitors health of each FTD and replace unhealthy unit
- Performs registration and license management
- Bootstraps FTDv
 - Configure interfaces, device group, platform settings, NAT, and routing
 - Creates all objects on the FMC that are needed for FTDv deployment
- For policy consistency, any existing ACP can be utilized



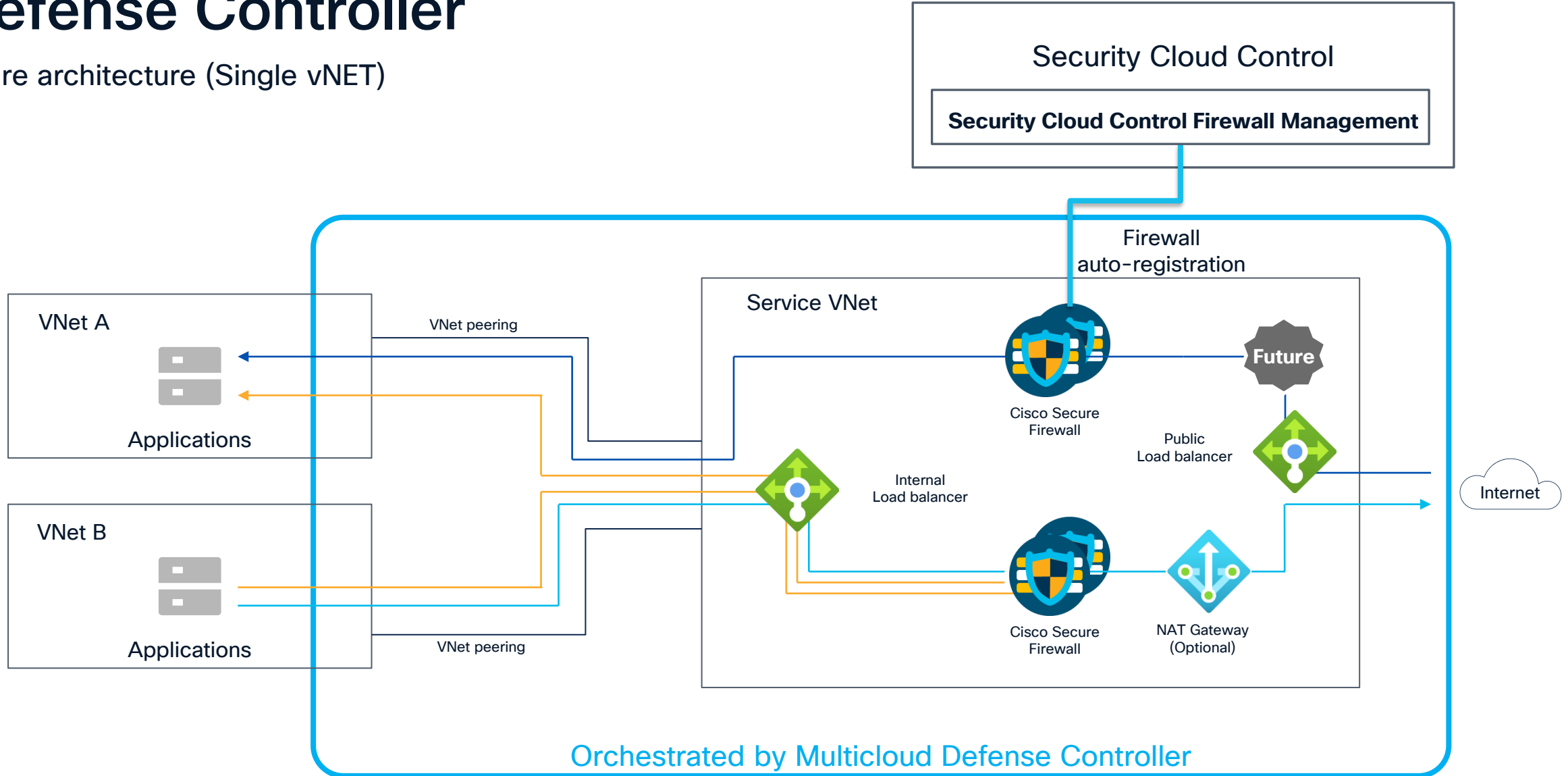
Cisco Secure Firewall Virtual Orchestrated by Multicloud Defense Controller

AWS architecture (Single AZ)



Cisco Secure Firewall Virtual Orchestrated by Multicloud Defense Controller

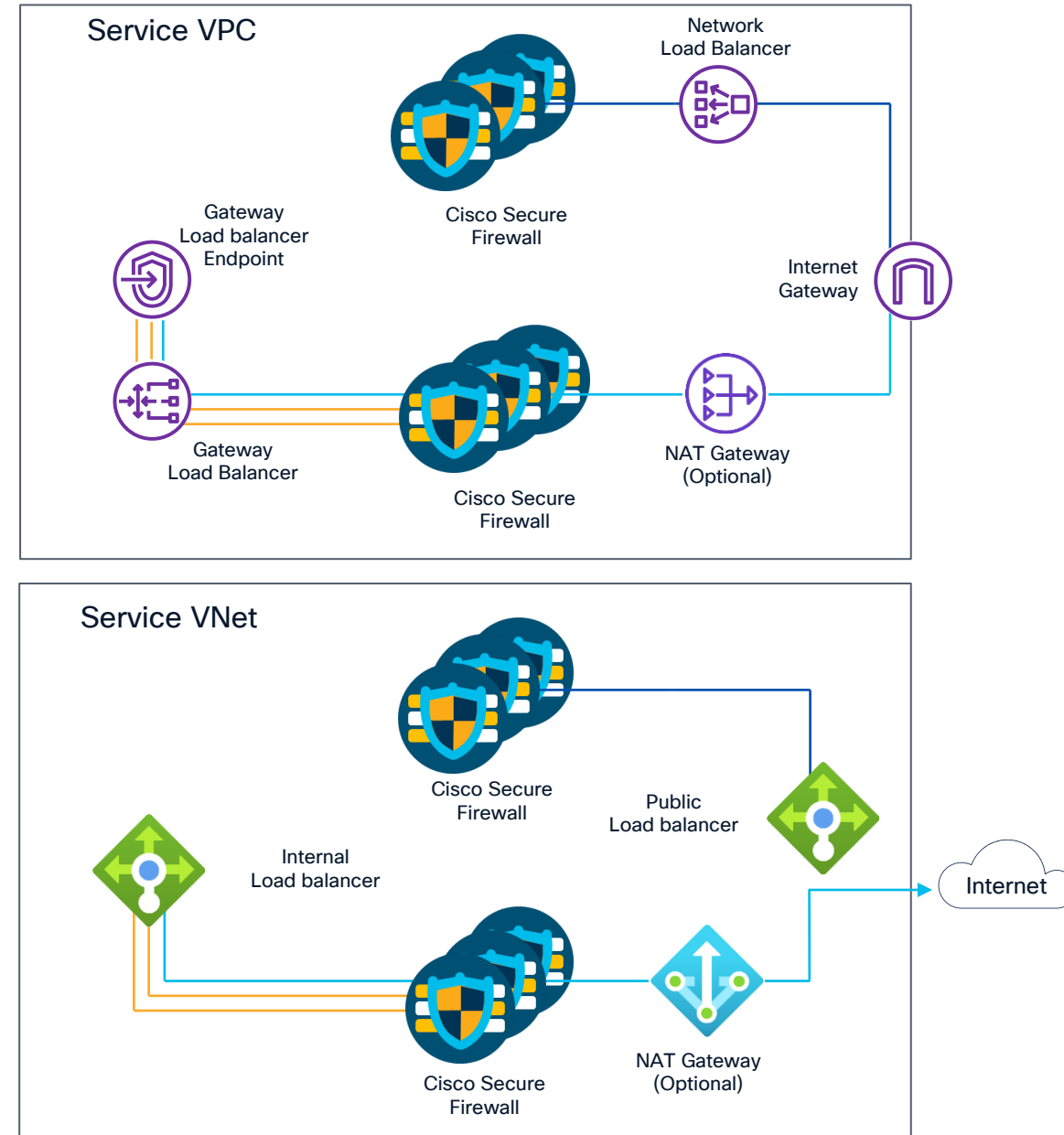
Azure architecture (Single vNET)



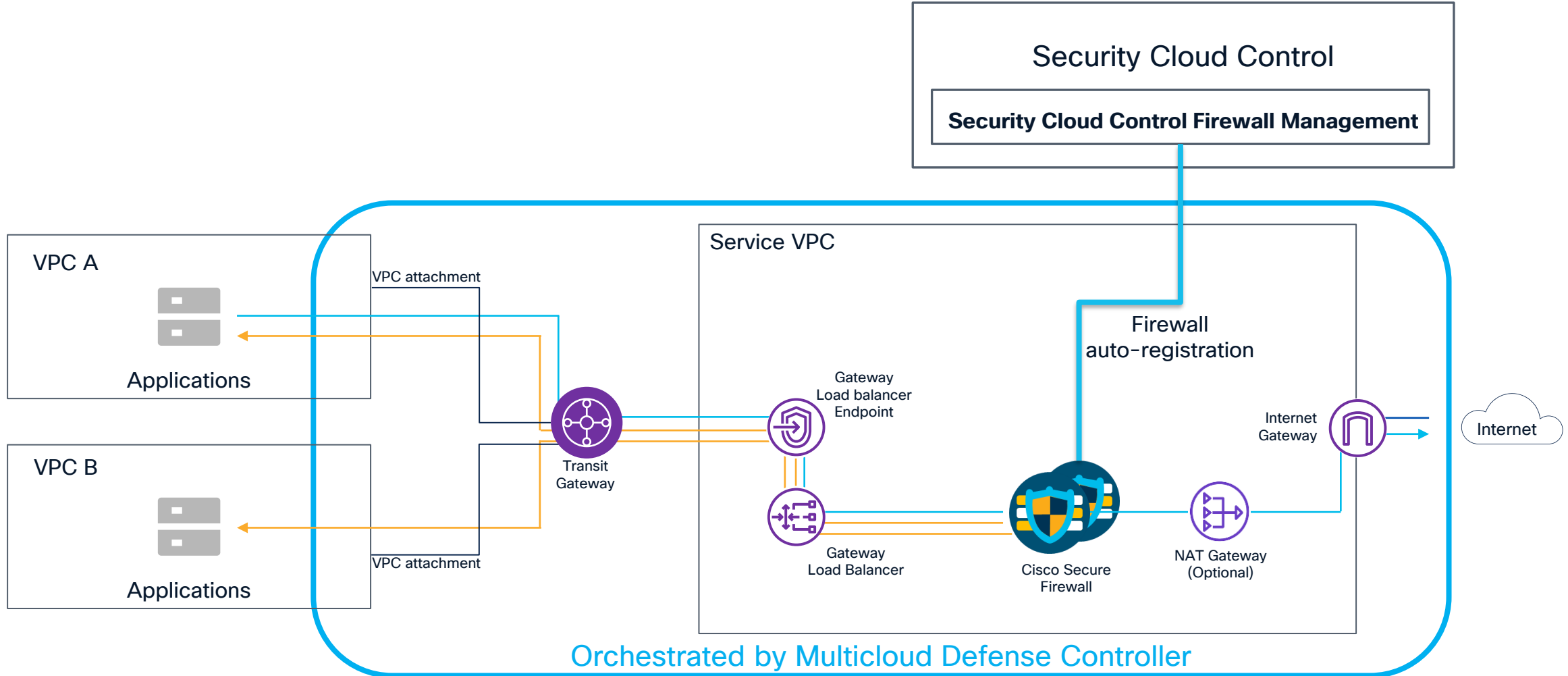
Autoscaling

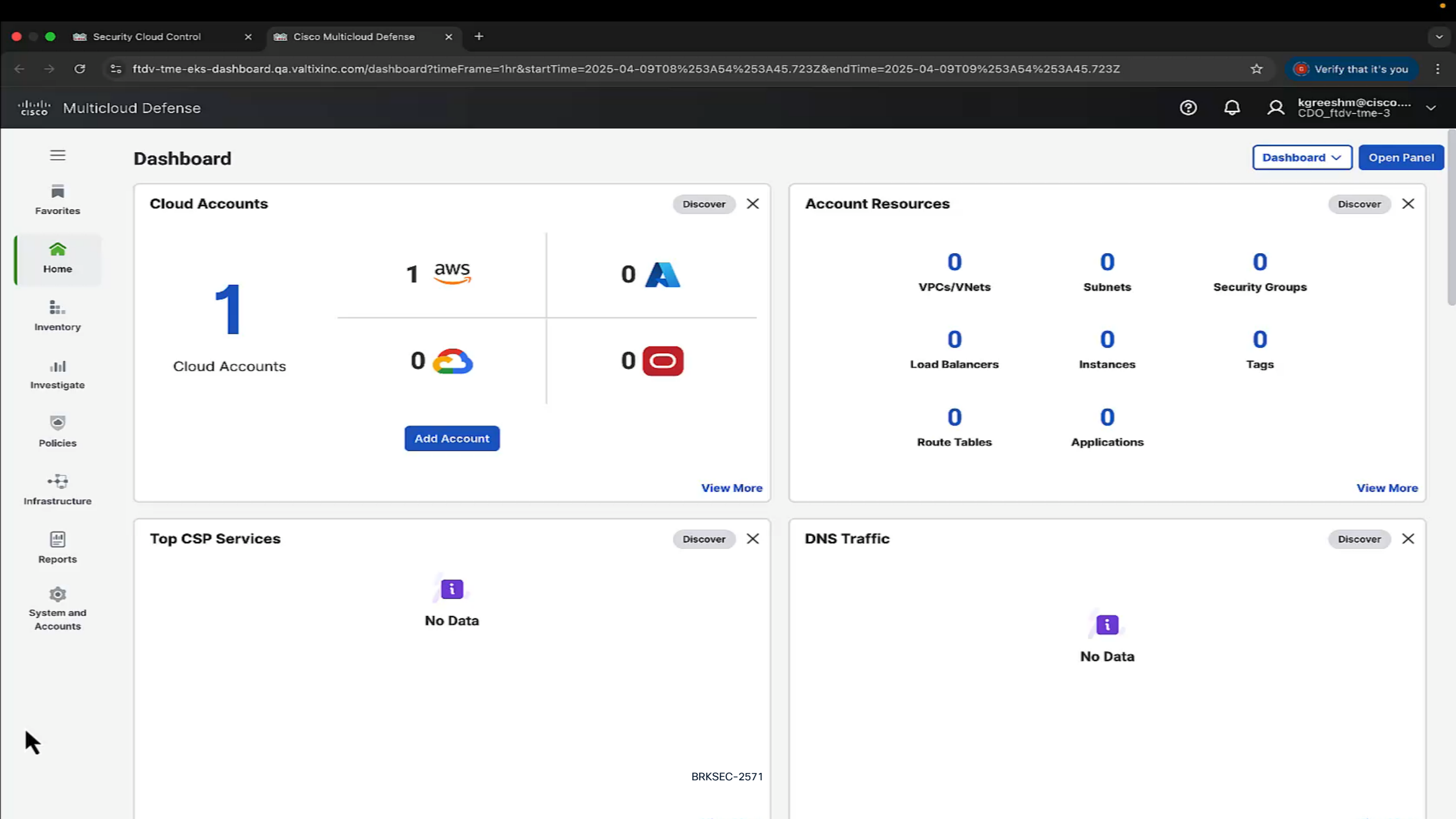
Multicloud Defense controller handles autoscaling of FTDv

- Monitor metrics – **CPU usage and Memory**
- **No Cloud Formation or ARM templates needed** – Autoscaling is natively handled by the Multicloud Defense Controller
- Auto-scaled firewalls are automatically added to the Security Cloud Controller Firewall Manager
- Auto-scaled firewalls are automatically added to the load balancer
- Lifecycle managed of firewalls is handled by the controller
 - Health status monitoring
 - Auto healing
 - Traffic engineering
- **No Manual configuration is needed**



Secure Firewall Orchestration by Multicloud Defense Demo





Dashboard Dashboard Open Panel

Cloud Accounts

Discover

1 aws

0

0

0

Cloud Accounts

Add Account

View More

Account Resources

Discover

0 VPCs/VNets

0 Subnets

0 Security Groups

0 Load Balancers

0 Instances

0 Tags

0 Route Tables

0 Applications

View More

Top CSP Services

Discover

No Data

BRKSEC-2571

DNS Traffic

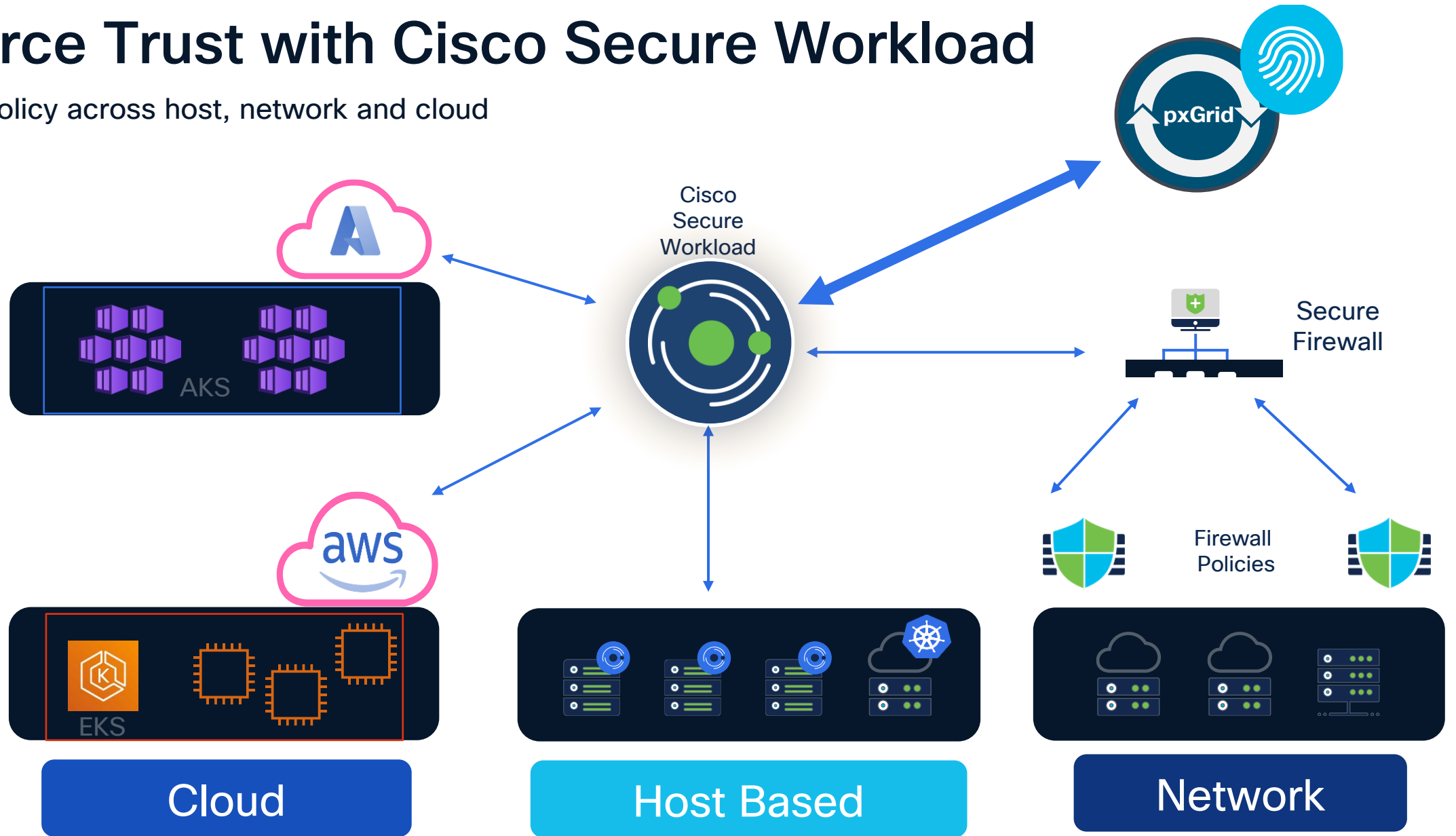
Discover

No Data

**Could I benefit from visibility,
ADM and enforcement from
CSW in public cloud ?**

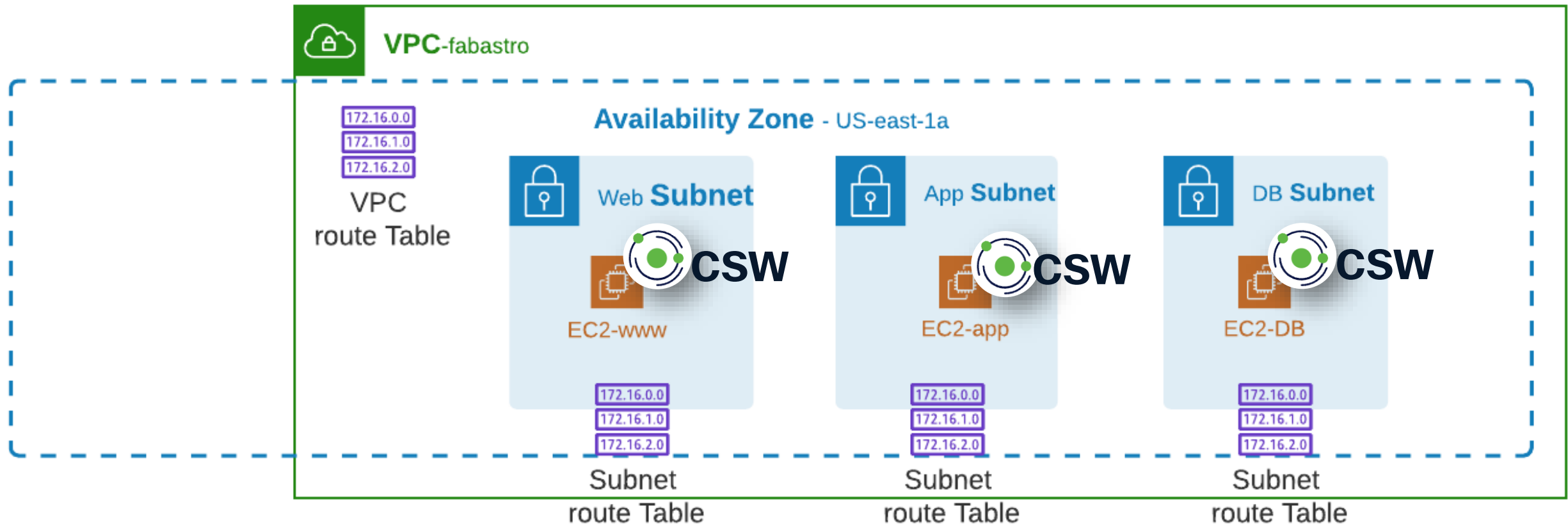
Enforce Trust with Cisco Secure Workload

Unified policy across host, network and cloud



Improving Security in IaaS Model

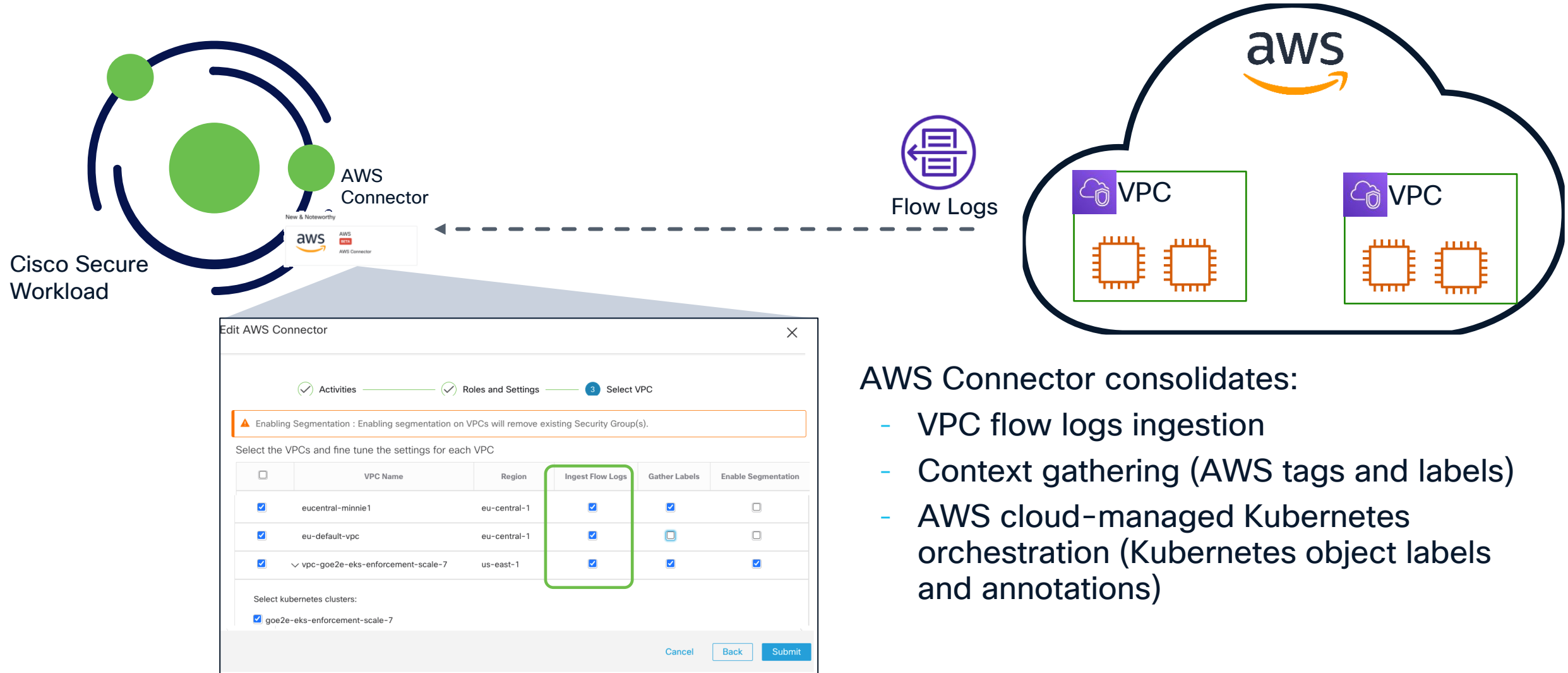
Leveraging Cisco Secure Workload to segment within a VPC or a subnet





**No big fan
of using agents ?**

Cisco Secure Workload Cloud-Based Sources

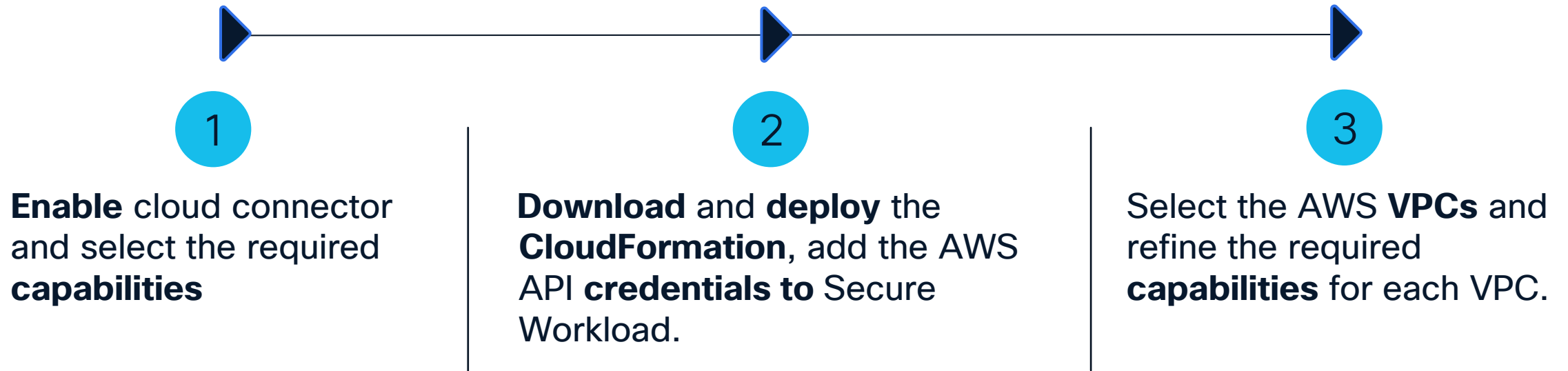


AWS Connector consolidates:

- VPC flow logs ingestion
- Context gathering (AWS tags and labels)
- AWS cloud-managed Kubernetes orchestration (Kubernetes object labels and annotations)

AWS Connector

Ingesting cloud telemetry – VPC flow logs and AWS tags/labels



AWS Connector – Select Capabilities



1

Enable and configure the connector capabilities

Connector

Enable

Capabilities

Flow Visibility

Segmentation

Managed K8s

Inventory Enrichment



Edit AWS Connector

X

1 Activities

2 Roles and Settings

3 Select VPC

4 View Groups

Name of the connector

AWS

Select Activities to be performed with Cisco Secure Workload on your AWS Resources

☒ Gather Labels ⓘ

☒ Ingest Flow Logs ⓘ

☒ Segmentation ⓘ

☐ Managed kubernetes services ⓘ

The recommended AWS (IAM) roles and permissions depend on the selections you make above.

Cancel

Back

Next

AWS Connector - IAM

Secure Workload automatically generates a CloudFormation template with the required IAM policy

Users can download and deploy the CloudFormation template.

Proxy and AWS Security Groups limits can be configured

2

✓ Activities

2 Roles and Settings

3 Select VPC

Cisco Secure Workload requires relevant permissions to access and read flow logs settings and perform policy enforcement.

Based on the capability selections, the following CloudFormation template has been auto-generated. Use this to apply the relevant permissions to the desired user:

```
{
  "Resources": {
    "ManagedPolicy": {
      "Type": "AWS::IAM::Policy",
      "Properties": {
        "PolicyName": {
          "Ref": "PolicyName"
        },
        "PolicyDocument": {
          "Version": "2012-10-17",
          "Statement": [
            {
              "Effect": "Allow",
              "Action": [
                "ec2:DescribeVpcs"
              ]
            }
          ]
        }
      }
    }
  }
}
```

Additional Help

[Create a Cloud Formation Stack](#)

[Create a New User](#)

[Example Commands](#)

Access Key

Secret Key

Does your network require HTTP Proxy to reach AWS?

YesNo

Please provide your proxy URL:

Full Scan Interval

3600seconds

Delta Scan Interval

60seconds

AWS Limits

Security Groups Per Region

2500

Security Groups Per Network Interface

5

Rules per Security Group

60



AWS Connector – Select VPCs



3

- Multiple VPCs can be selected
- Capabilities can be customized and refined for each VPC individually

Edit AWS Connector						X
☐	default	ap-northeast-1	☐	☐	☐	
☐	test-vpc	ap-northeast-1	☐	☐	☐	
☐	lab-vpc	ap-northeast-1	☐	☐	☐	
☐	vpc-e6ecd481	sa-east-1	☐	☐	☐	
☐	vpc-967901fe	ca-central-1	☐	☐	☐	
☐	vpc-06686161	ap-southeast-1	☐	☐	☐	
☐	vpc-20fcc147	ap-southeast-2	☐	☐	☐	
☐	vpc-cfcd36a5	eu-central-1	☐	☐	☐	
☐	SecureVPC	us-east-1	☐	☐	☐	
☒	csw-vpc	us-east-1	☒	☒	☒	

Zoning & (Macro/Micro)Segmentation Demo

Chrome

File Edit View History Bookmarks Profiles Tab Window Help

us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances:instanceState=running

Services Search for services, features, blogs, docs, and more [Option+S]

Resource Groups & Tag Editor

New EC2 Experience Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances New

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances New

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs New

AMI Catalog

Elastic Block Store

Volumes New

Snapshots New

Lifecycle Manager New

Network & Security

Security Groups

Instances (9) Info

Search

Instance state = running

Clear filters

Connect

Instance state

Actions

Launch instances

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
☐	dev-storage-1	i-0fc7b1de63344f911	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	-
☐	dev-sql-1	i-0b063fd1cbeb0914d	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	-
☐	dev-web-1	i-0aa5be3edb1ef3226	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	-
☐	dev-storage-2	i-050e049948215bbd5	Running	t2.micro	2/2 checks passed	No alarms	us-west-2b	ec2-34-213-2
☐	dev-sql-2	i-04201f6c2fecfe88c	Running	t2.micro	2/2 checks passed	No alarms	us-west-2b	ec2-35-163-1
☐	dev-web-2	i-0fd95bc88828304f1	Running	t2.micro	2/2 checks passed	No alarms	us-west-2b	ec2-34-209-1
☐	aws-sapphire-prod-sql	i-0eee56c4a4238156f	Running	t2.micro	2/2 checks passed	No alarms	us-west-2a	-
☐	aws-sapphire-prod-web	i-07cf51cb82e99cf9b	Running	t2.micro	2/2 checks passed	No alarms	us-west-2a	-
☐	aws-sapphire-prod-nfs	i-05f7cda90d27d276f	Running	t2.micro	2/2 checks passed	No alarms	us-west-2a	-

Select an instance

Feedback

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Conclusion

Zero Trust for Applications Everywhere

Hybrid Mesh Platform

Cloud Management (Security Cloud Control)

App to App (Hybrid Mesh Firewall)

Segmentation

Distributed Exploit Protection

Firewalling

Secure Workload

Isovalent Enterprise

Hypershield future



Flexibility to choose your journey

The right capability agent or agentless for the right use case
Going beyond security with CNI, service mesh and observability

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

