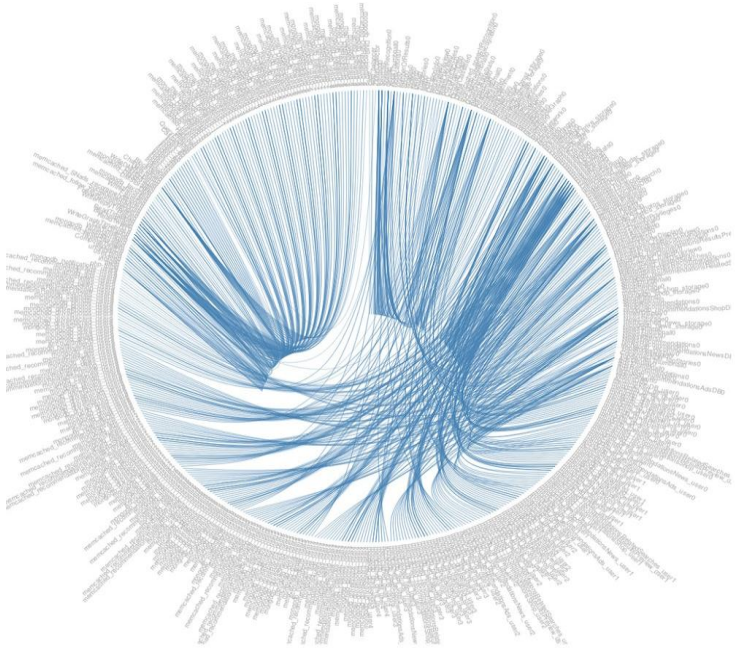
Workload Security: From challenges to Opportunities using Cisco Security

Fabien Gandola
Senior CyberSecurity TSA

Two obvious but key observations :

Applications are critical to modern businesses



Applications have dramatically evolved

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

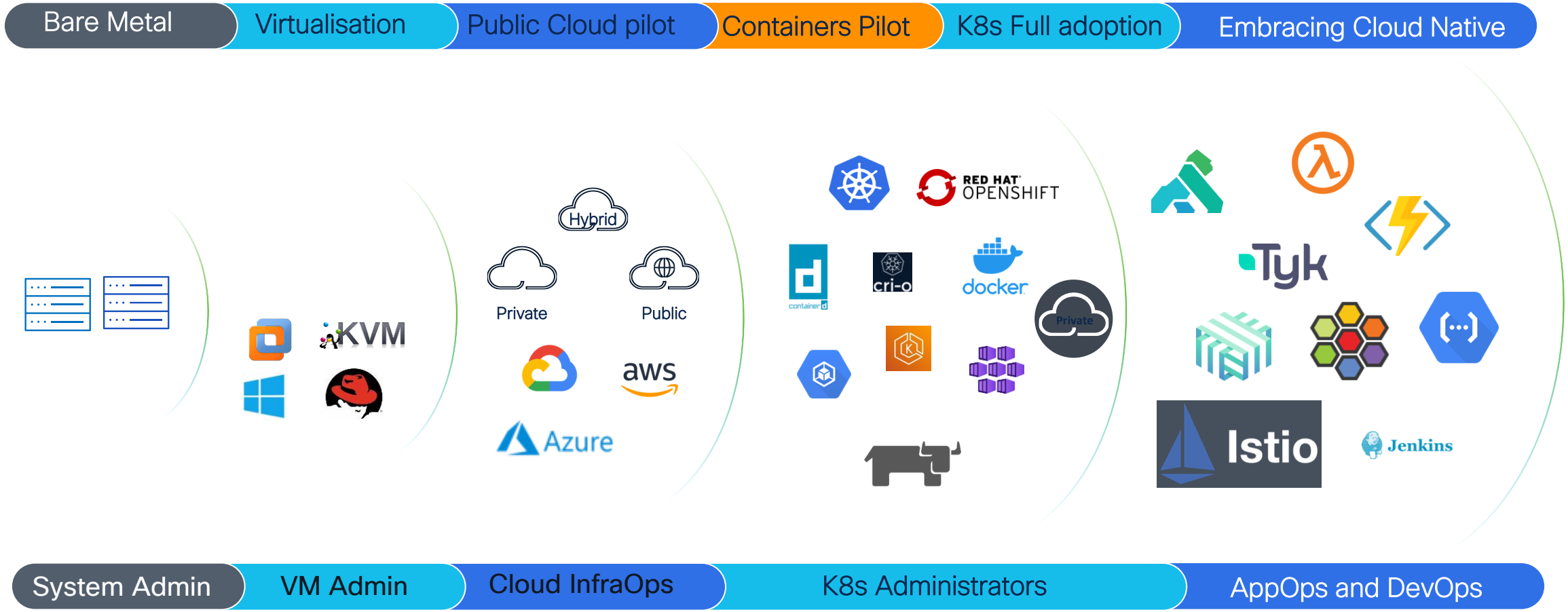
cisco

Some of the challenges

- Roles and responsabilities

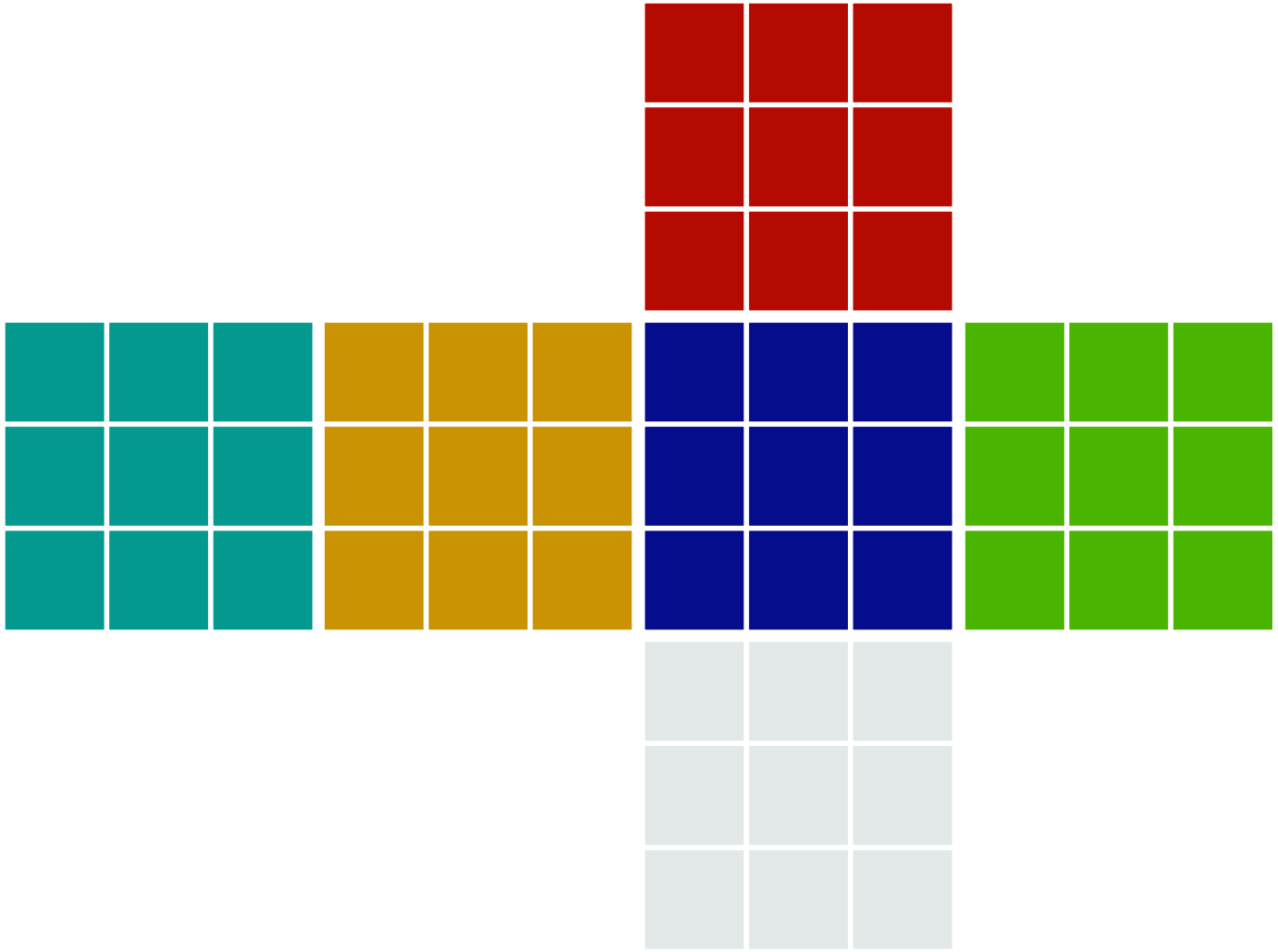
© 2025 Cisco and/or its affiliates. All rights reserved.

Application **workloads** evolution



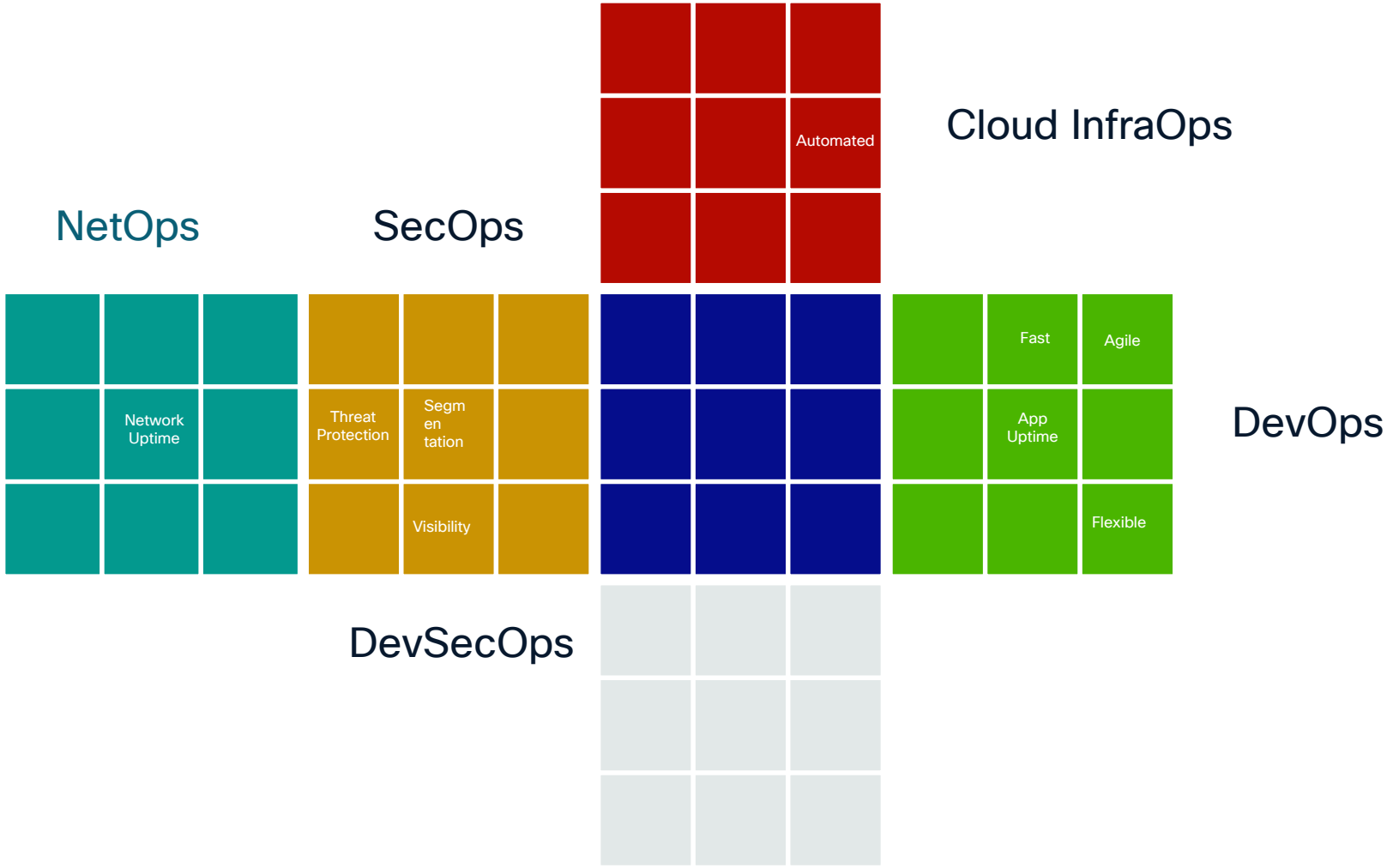
© 2025 Cisco and/or its affiliates. All rights reserved.

Cloud Security Rubik cube



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

Cloud Security use cases



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

Some of the challenges

- Roles and responsabilities
- 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
- ...

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

cisco

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
- ...

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

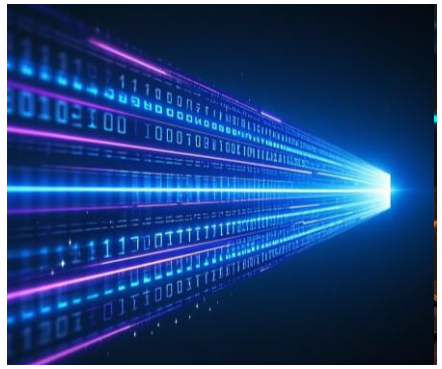
cisco

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

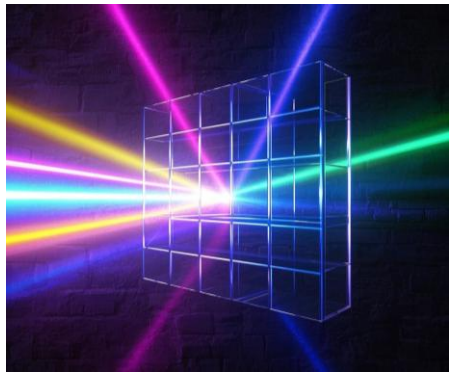
Our Vision

Simplification

Acceleration



Efficiency



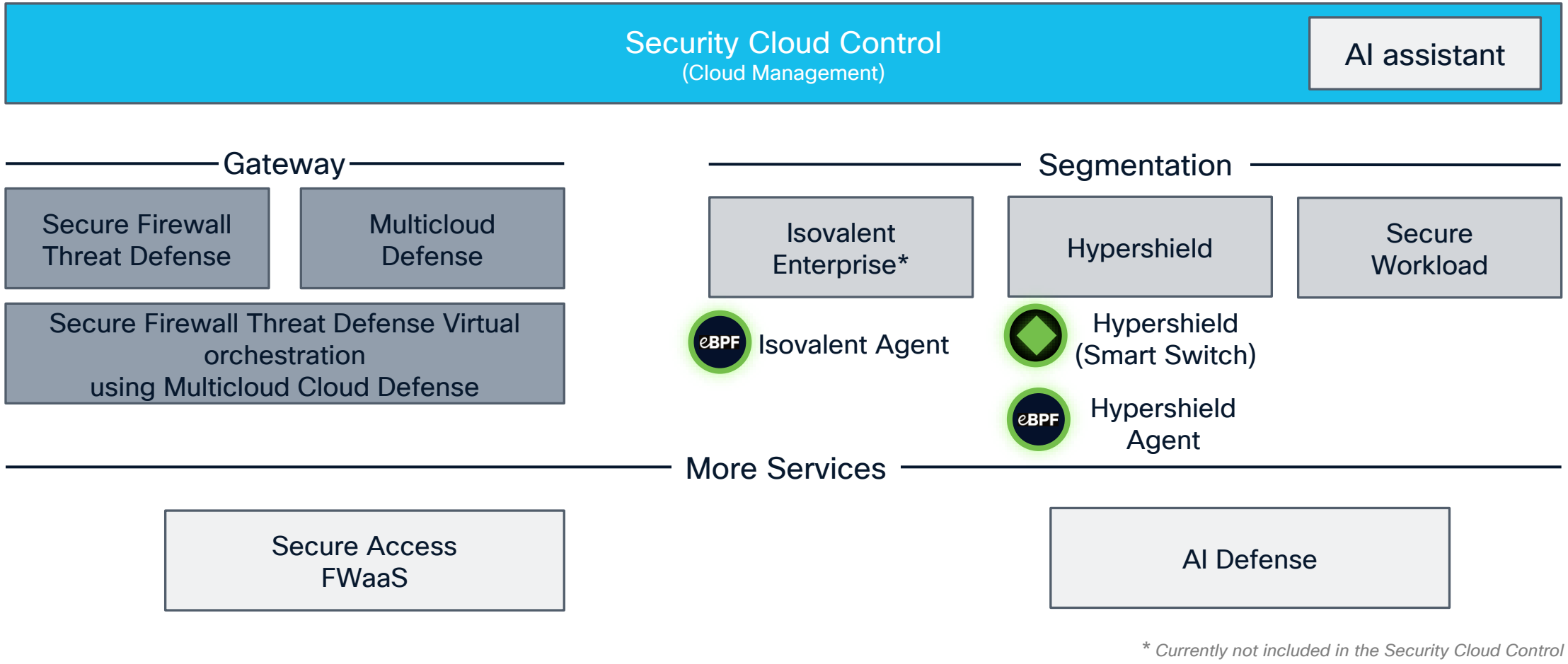
Platform

Automation

AI

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

Cisco Cloud Security

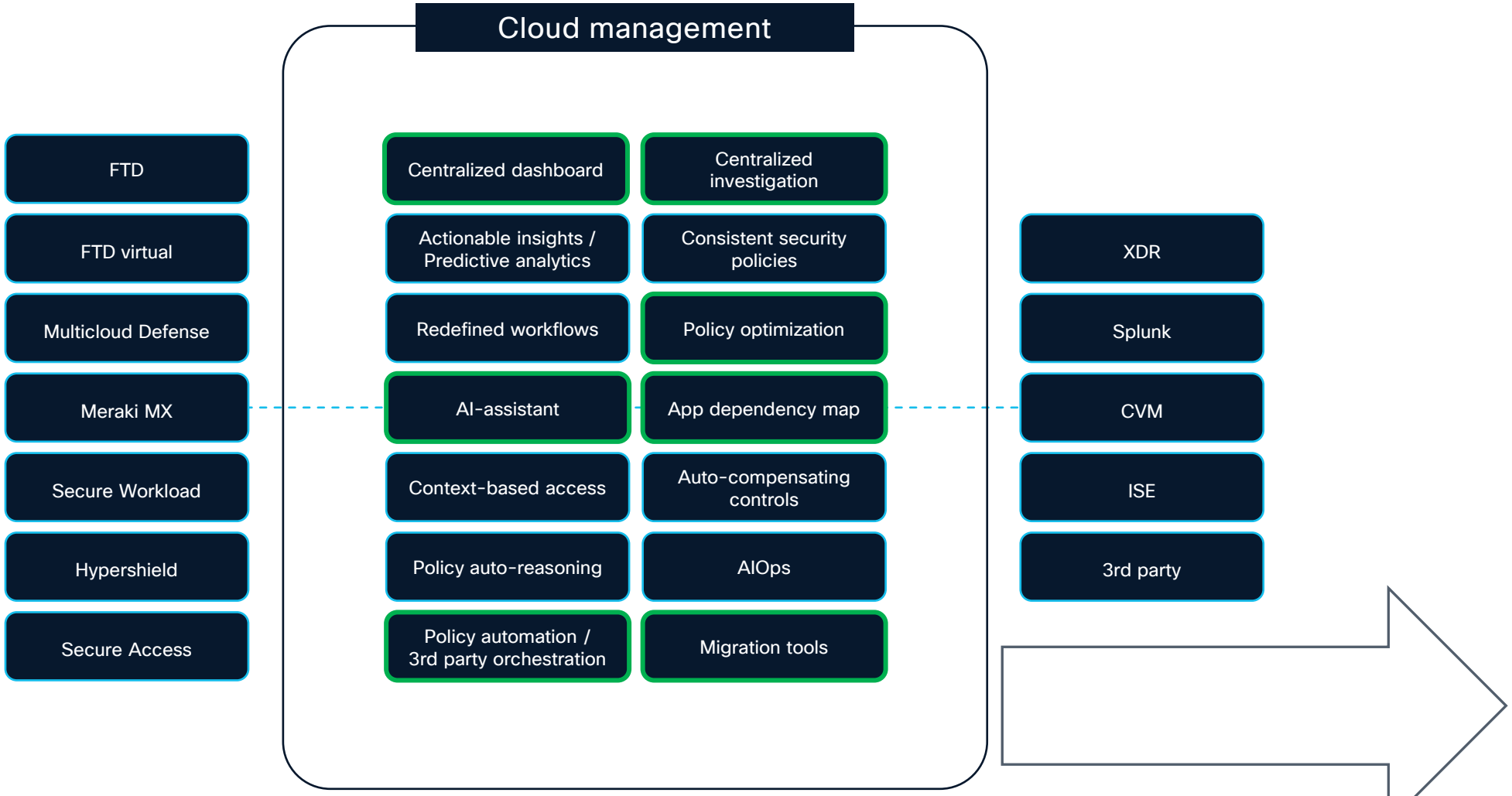


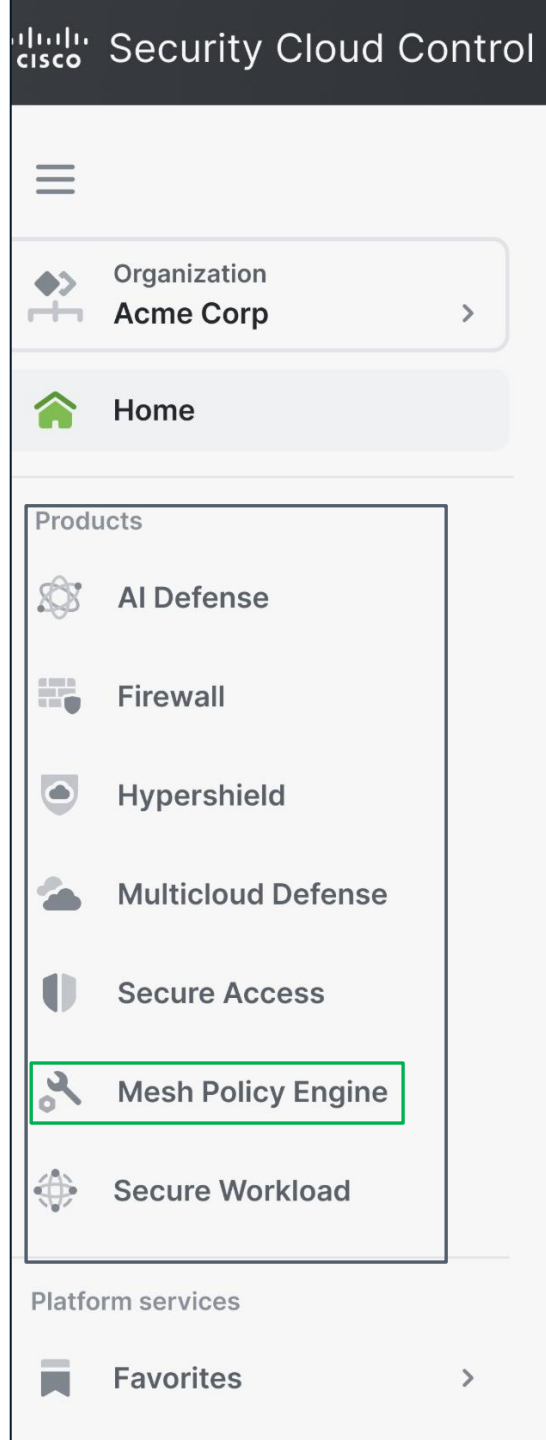
* *Currently not included in the Security Cloud Control*

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

Security Cloud Control

Unified Security Platform

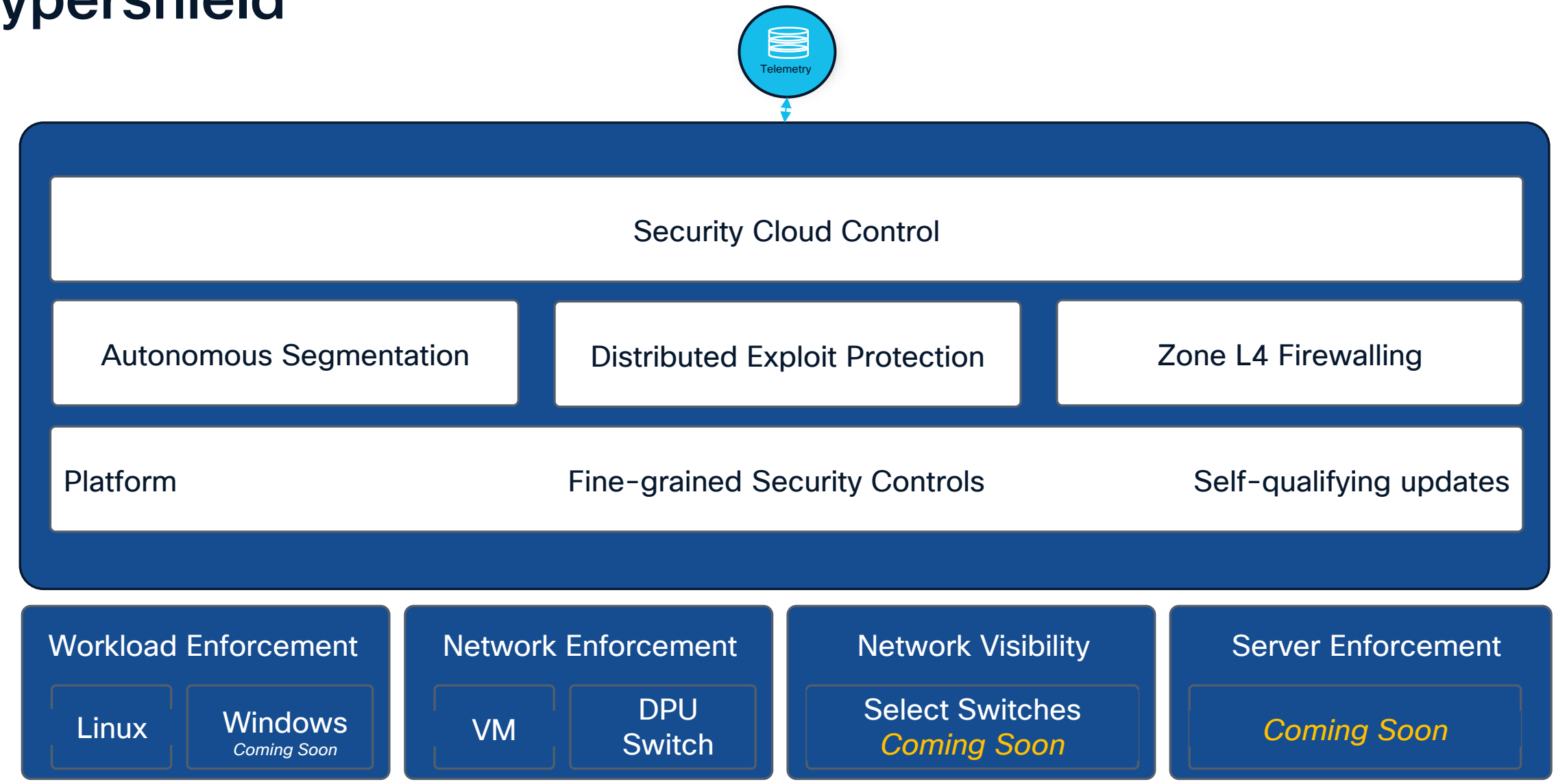




© 2025 Cisco and/or its affiliates. All rights reserved.

Sign-up:
security.cisco.com

Hypershield



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

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

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

Agenda

01 Introduction

02 Starting the journey On-prem

03 Embracing Cloud Native

04 Moving to the Cloud

05 Conclusion

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

About Me

Fabien Gandola
fgandola@cisco.com

TSA Cyber Security EMEA

26 years in Cisco

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

Cisco Webex App

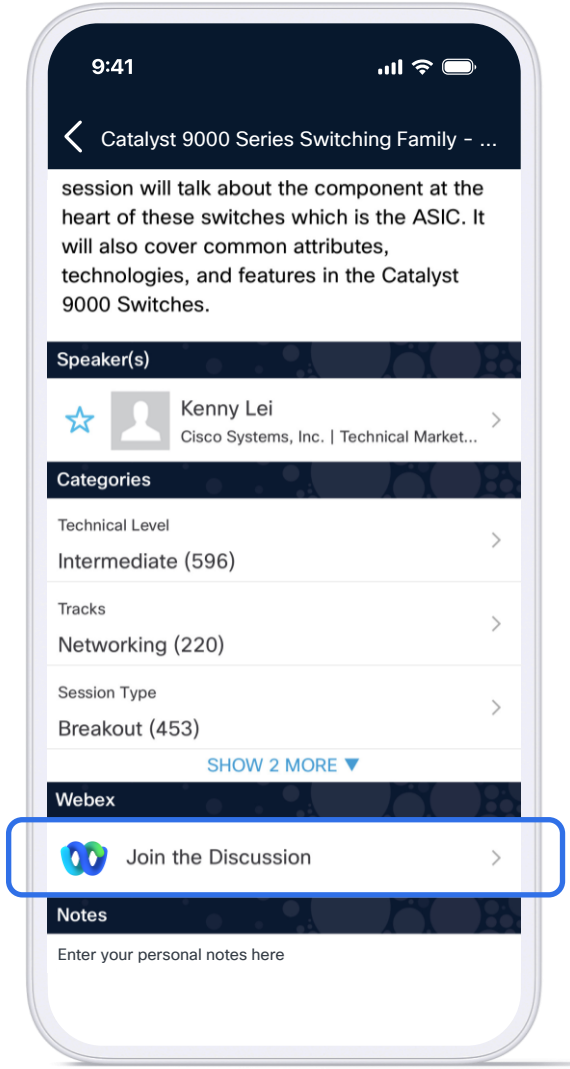
Questions?

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.

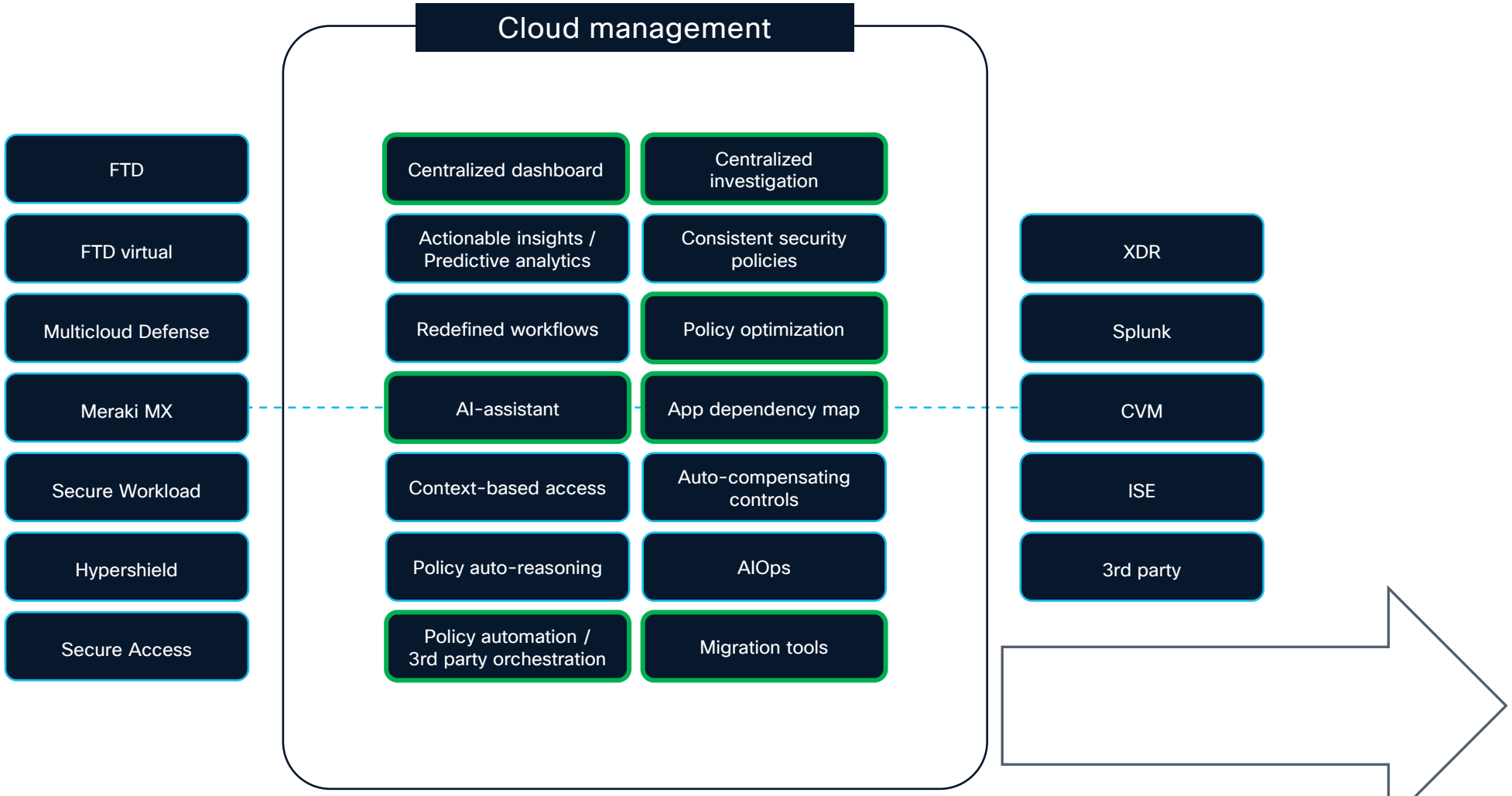


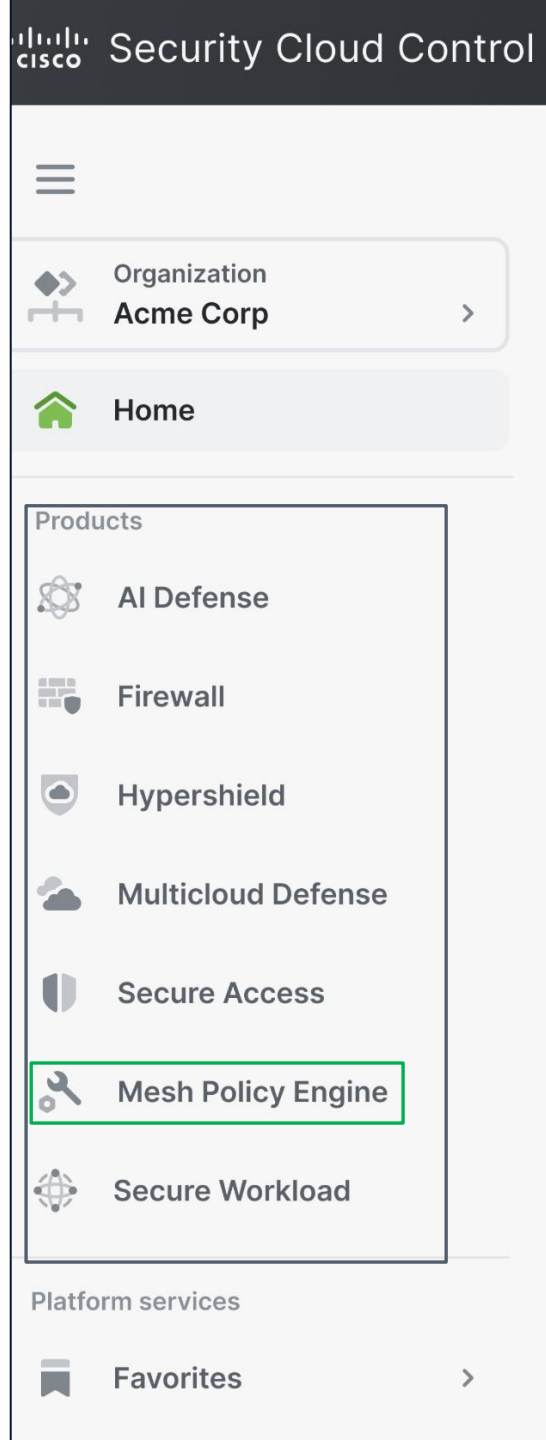
https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKSEC-2571**

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

Security Cloud Control

Unified Security Platform



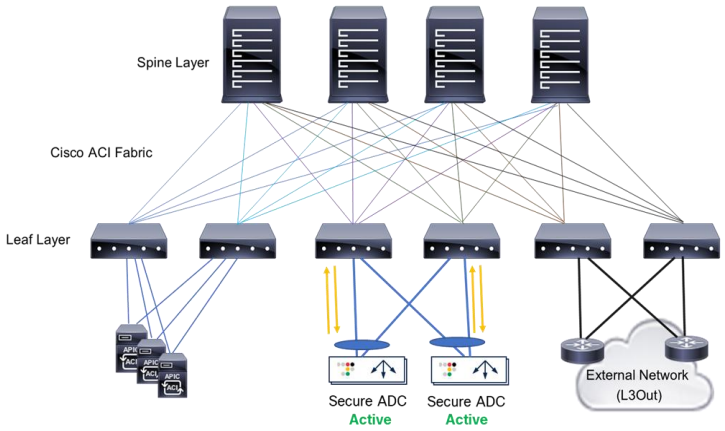


© 2025 Cisco and/or its affiliates. All rights reserved.

Sign-up:
security.cisco.com

It starts on-prem...

The way we are doing it traditionally...



SDN Infrastructure (ACI, NSX,...)

Firewall (FTD, ASA)

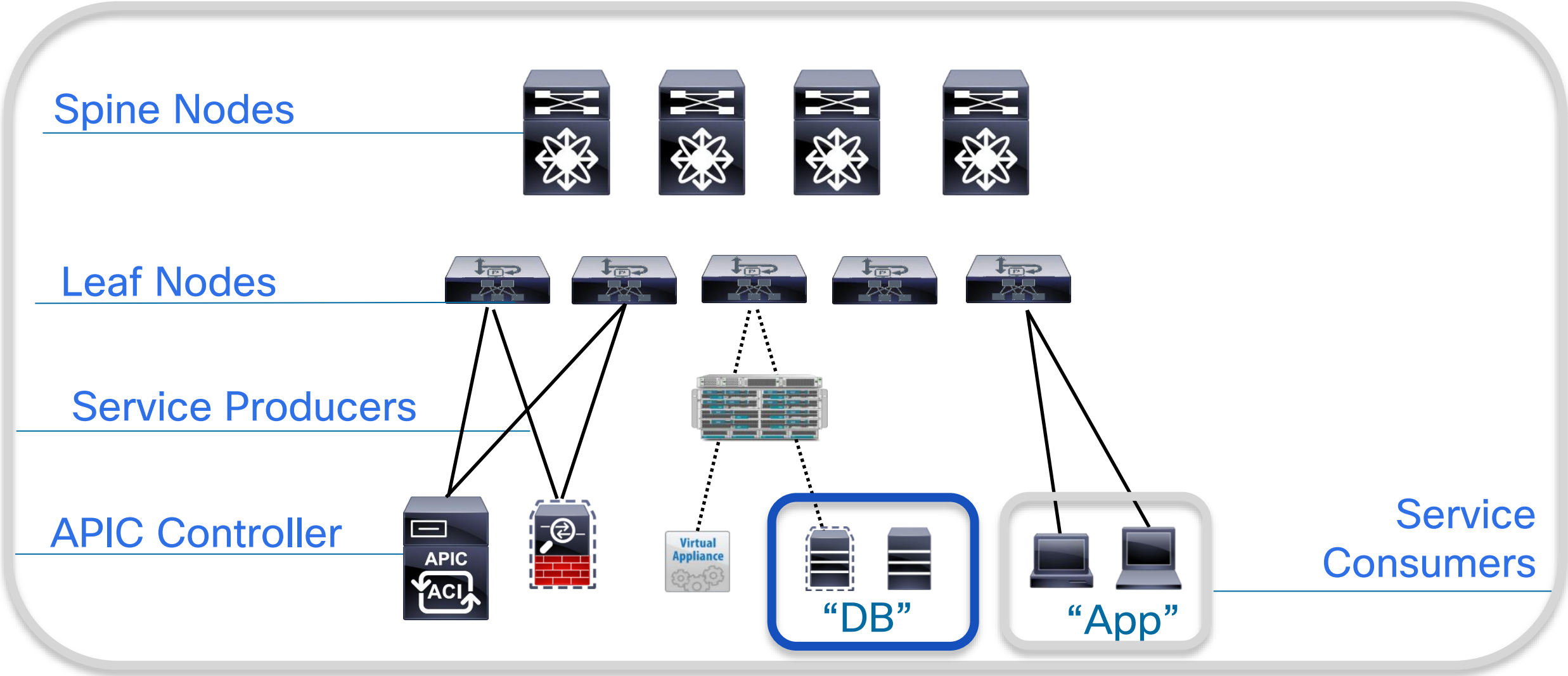
cisco SECURE Workload

Host based Firewall

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

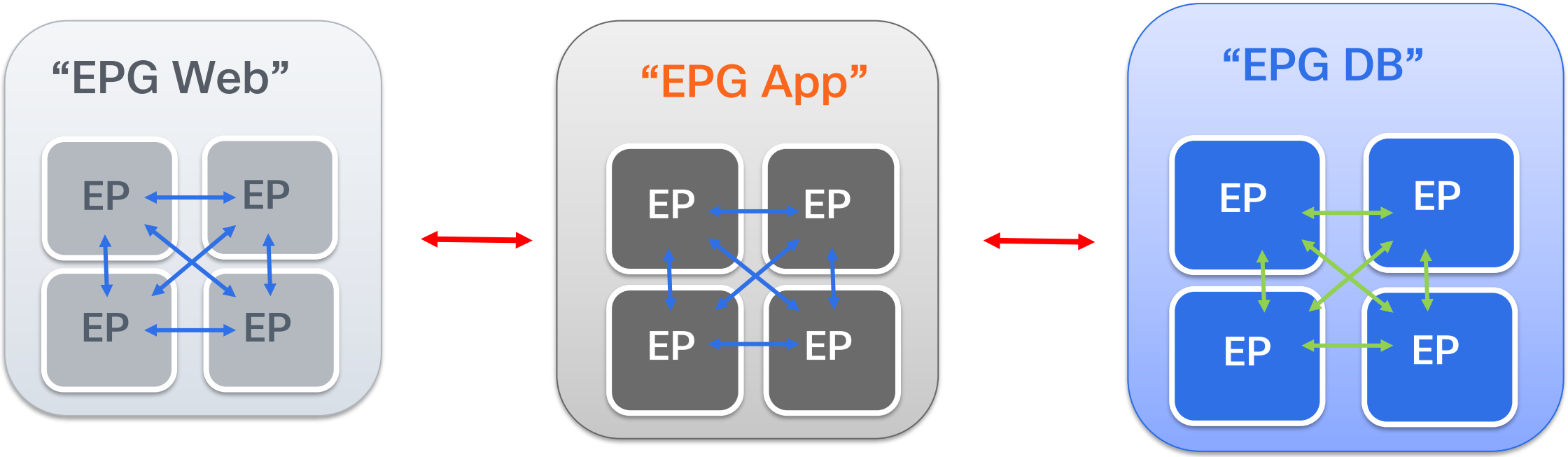
Shortest intro to ACI

Enforce Trust in the DC with Cisco ACI



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

Endpoint Groups Communications

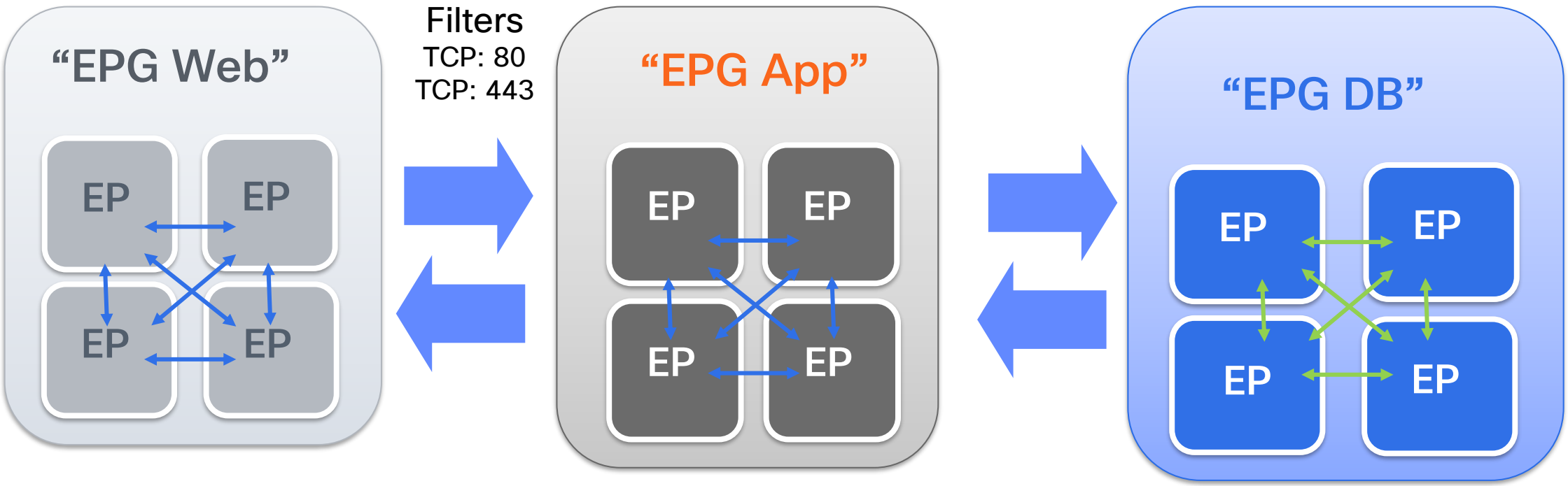


Devices within an Endpoint group can communicate, provided that they have IP reachability (provided by the Bridge Domain/VRF).

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

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

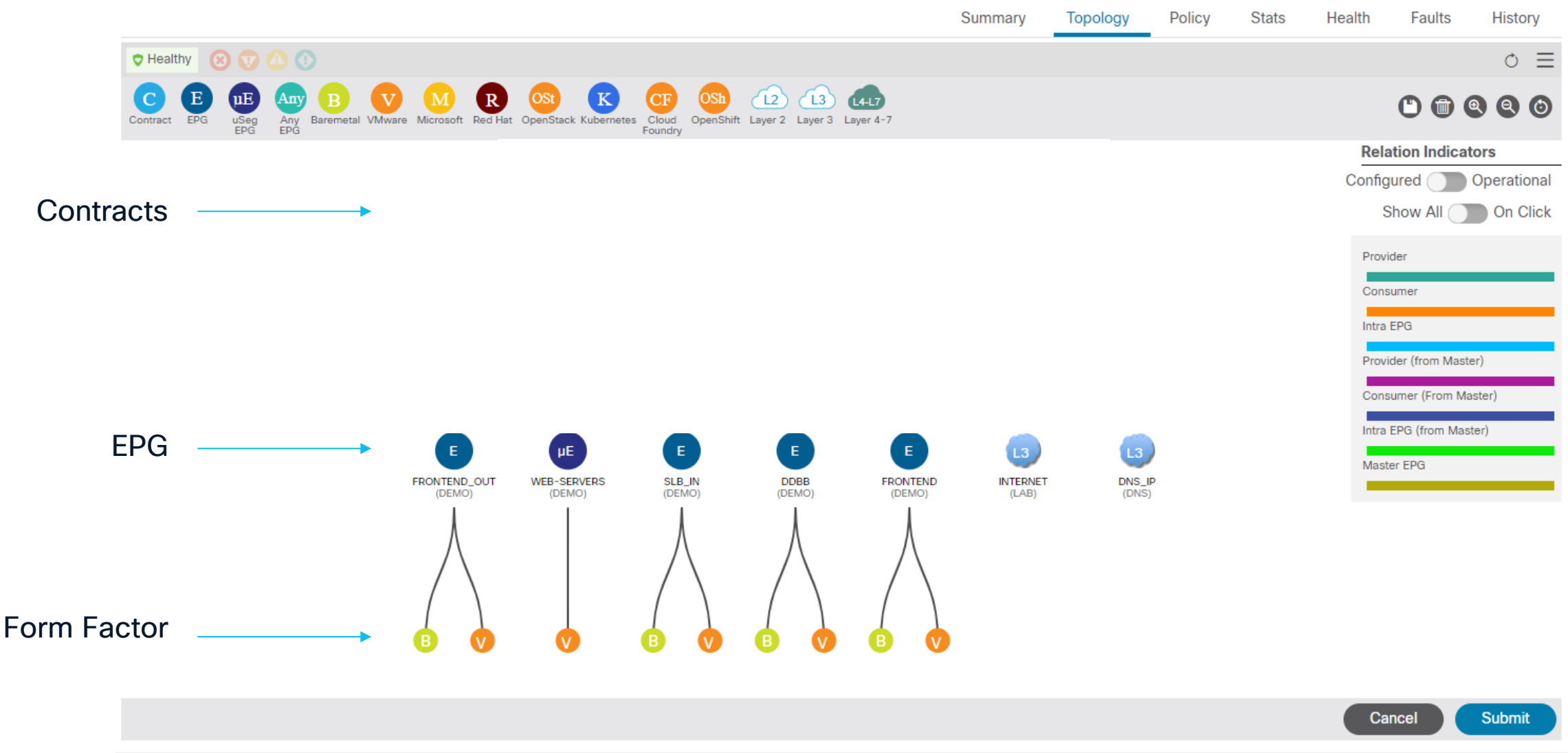
Contract : Kind of reflexive “Stateless” ACLs



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

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

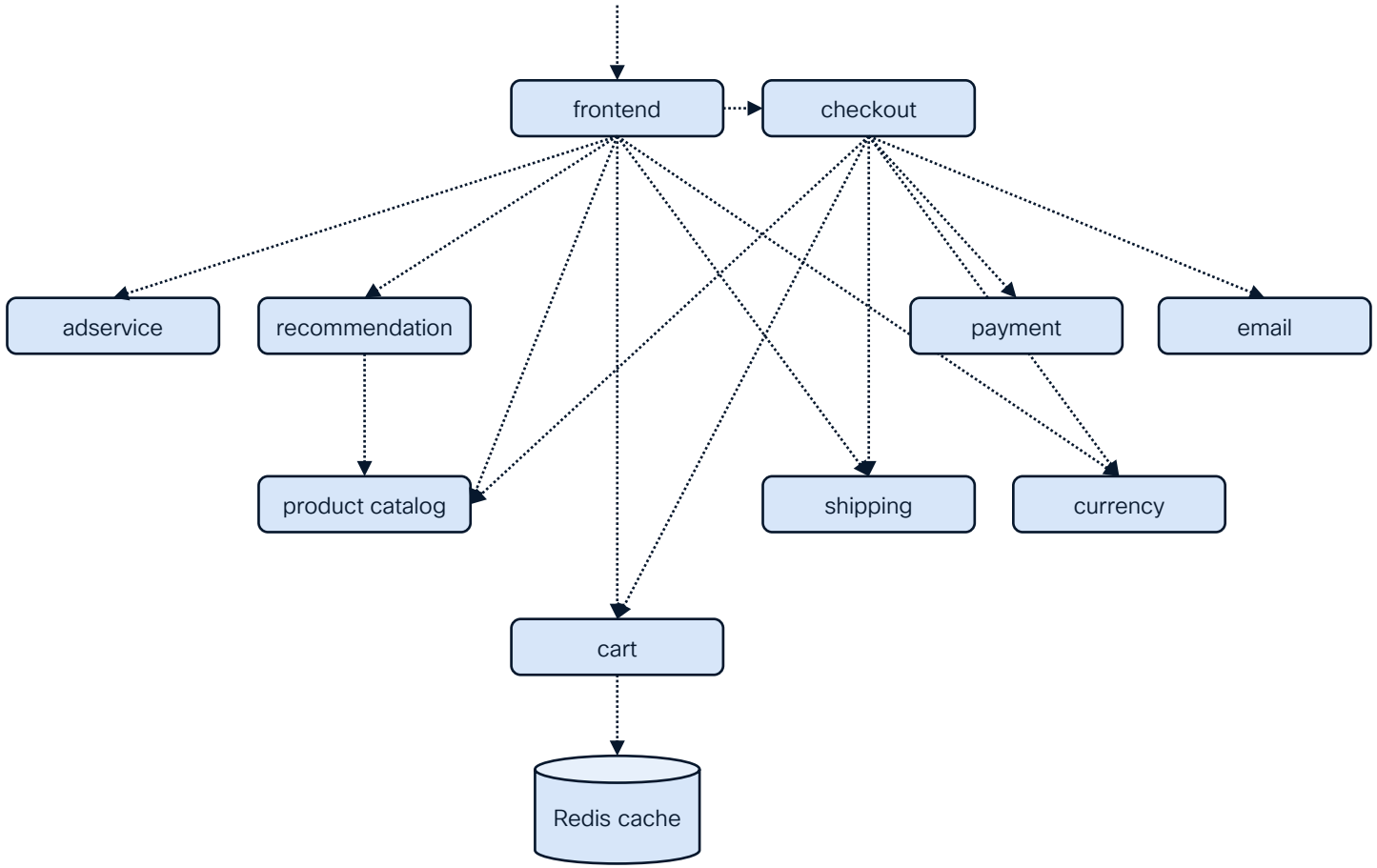
Application policy with contract



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

Online Boutique

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

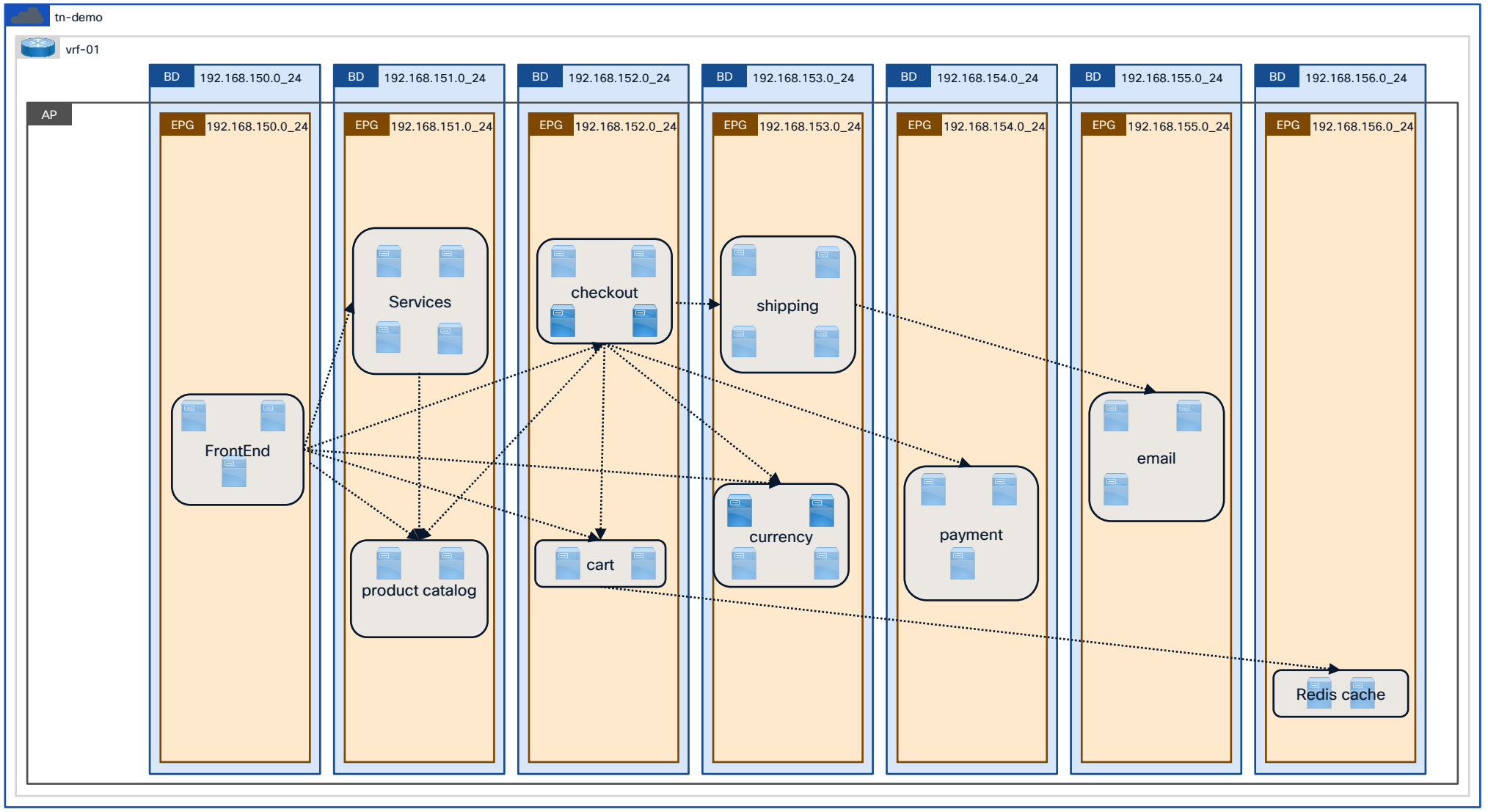


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart currency email payment product catalog shipping	TCP 7070 TCP 7000 TCP 8080 TCP 50051 TCP 3550 TCP 50051
frontend	adservice cart checkout currency product catalog recommendation shipping	TCP 9555 TCP 7070 TCP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

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

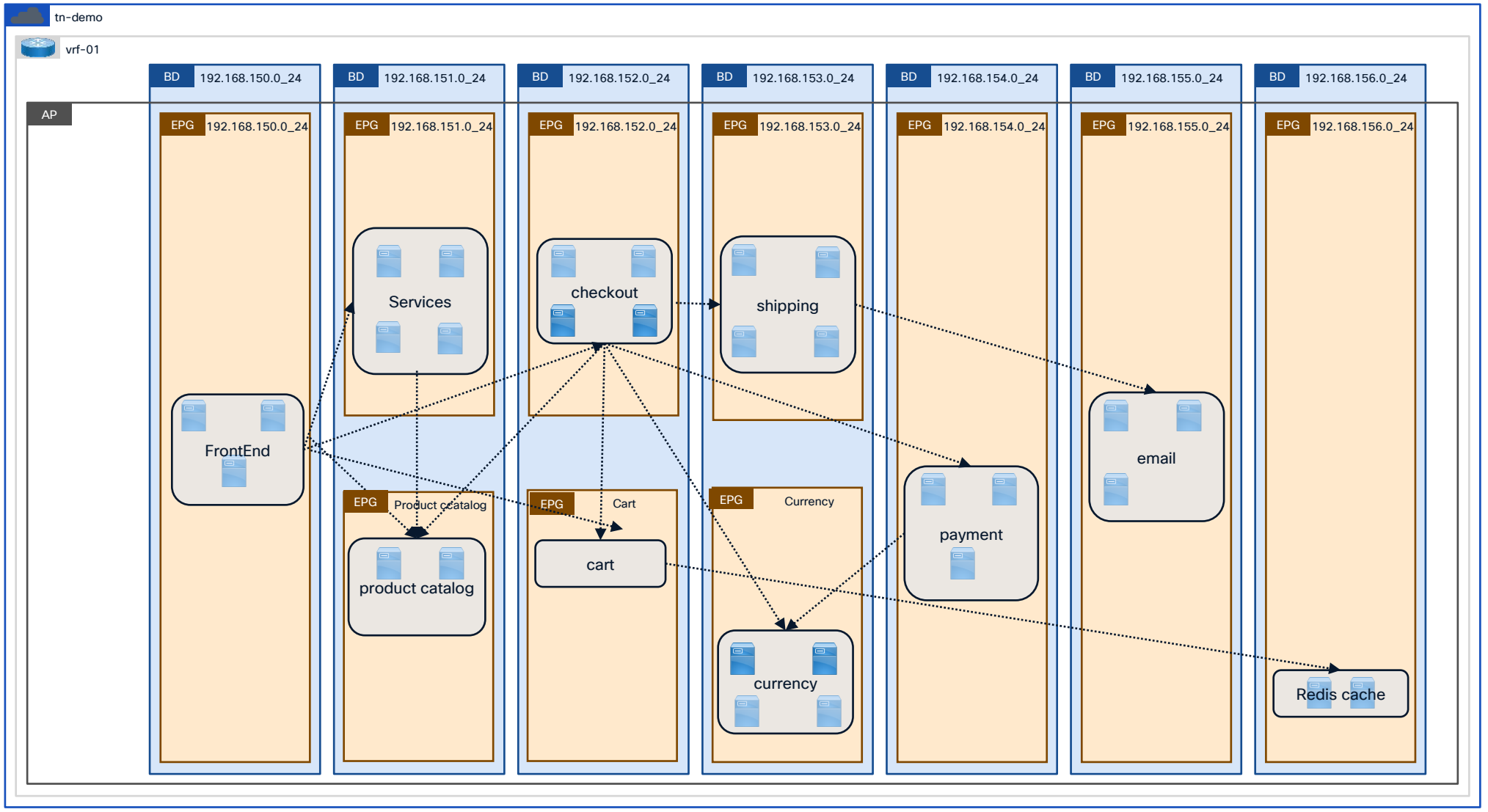
cisco

How do we establish trust groups?



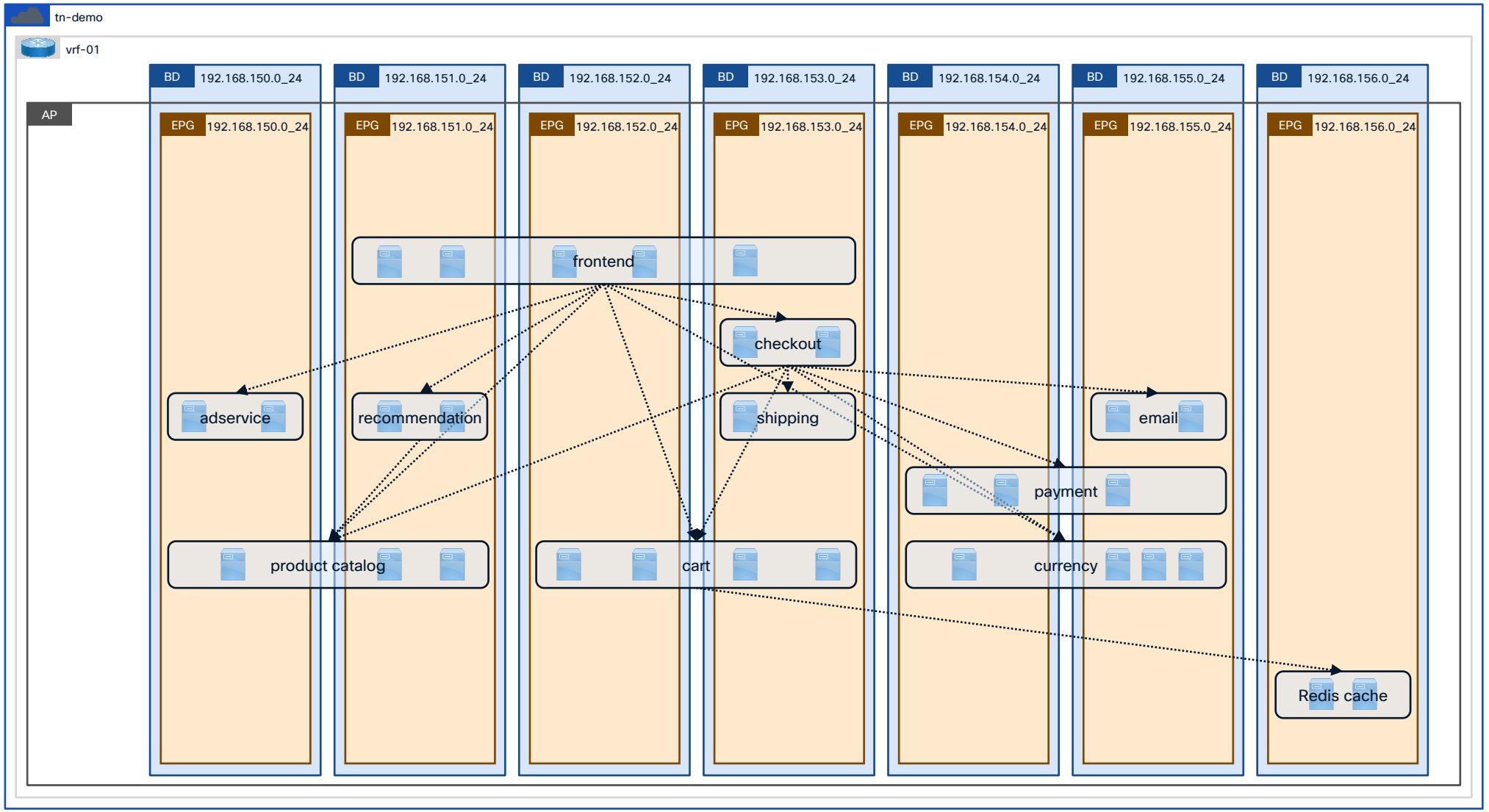
© 2025 Cisco and/or its affiliates. All rights reserved.

Not so fast – How do we establish trust groups?



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

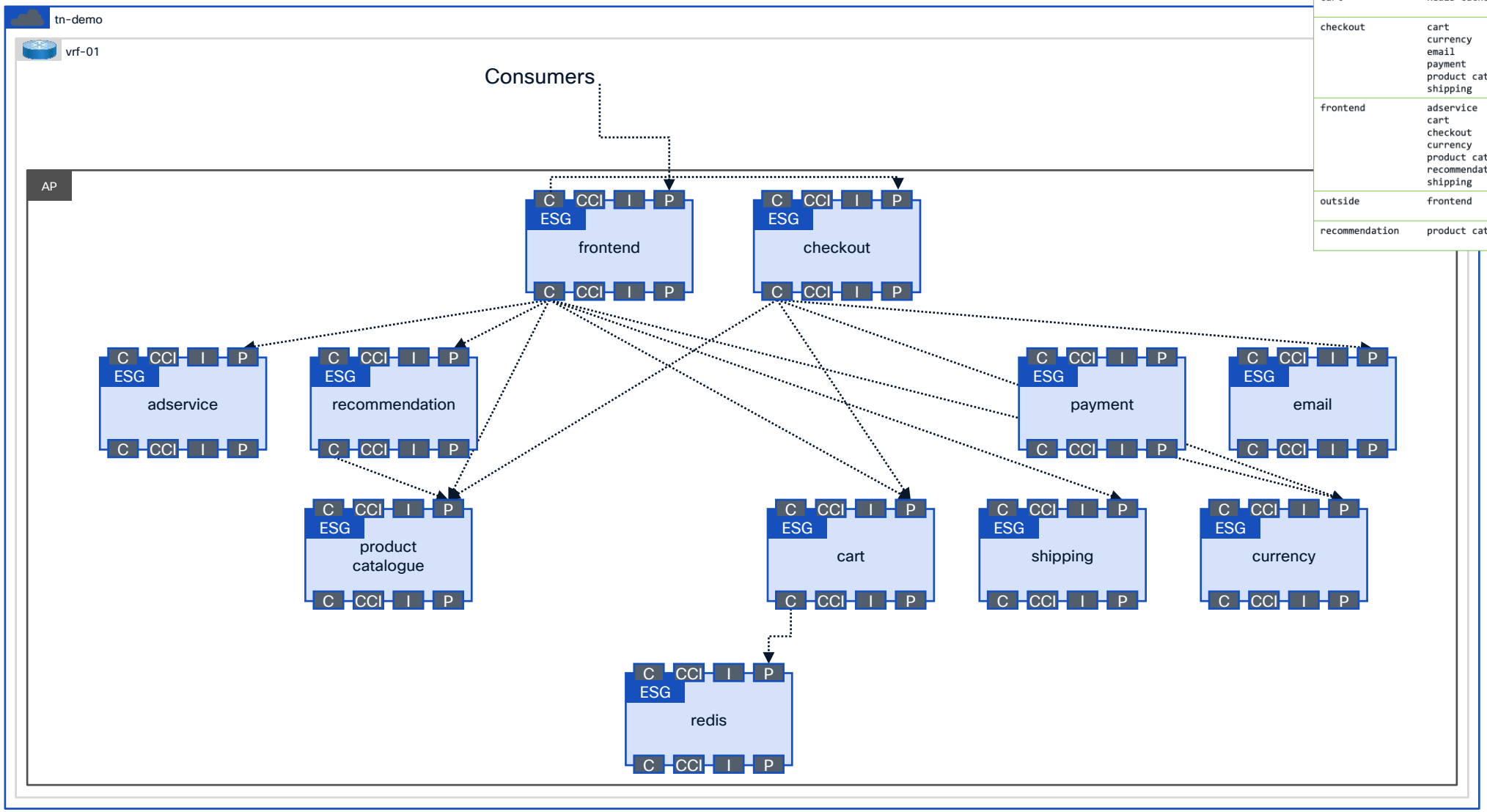
Is subnet the right way to establish trust groups?



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

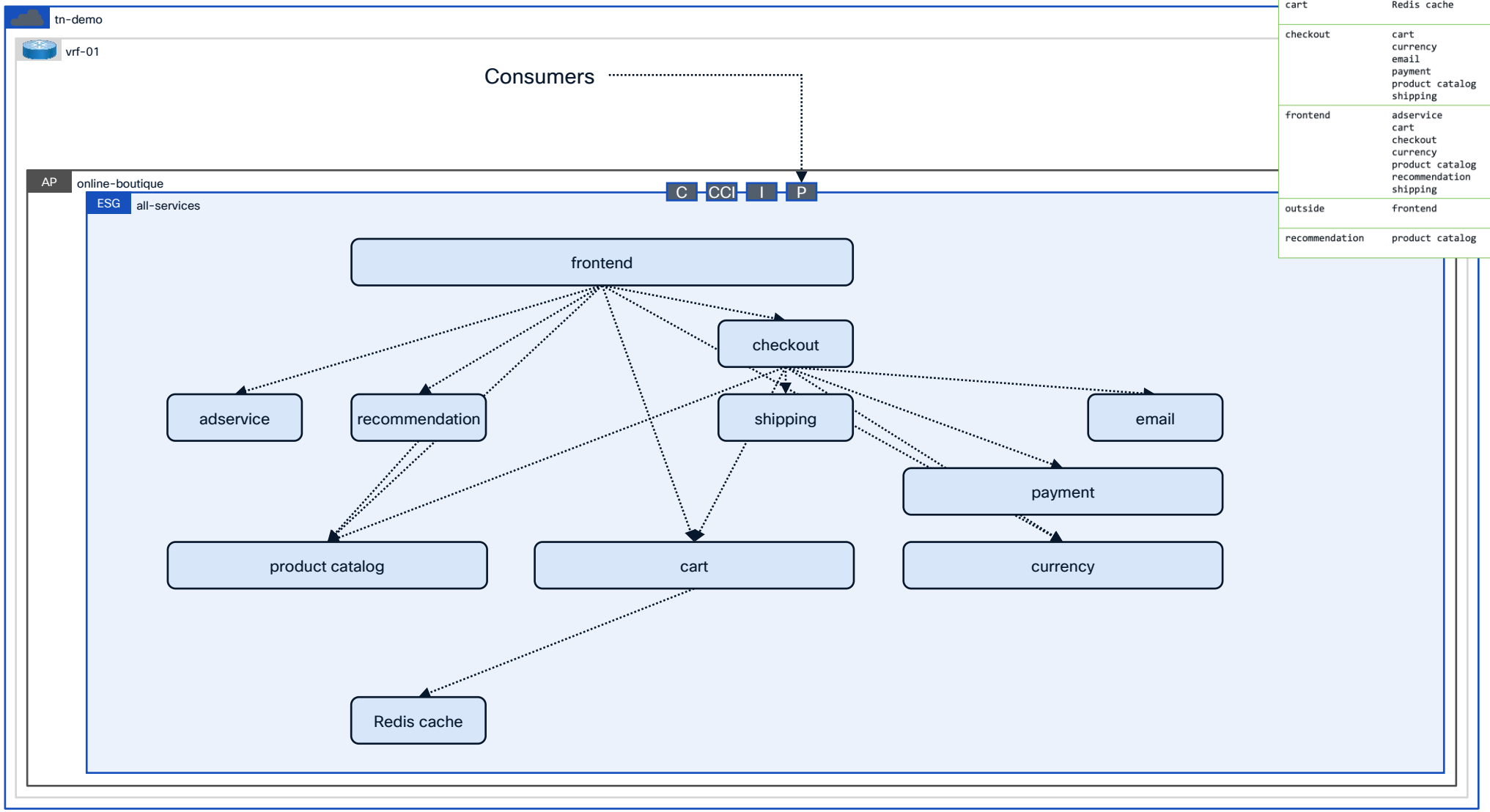
Network agnostic endpoint security groups (ESGs)

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
	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



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

Simpler to start with the DC Edge



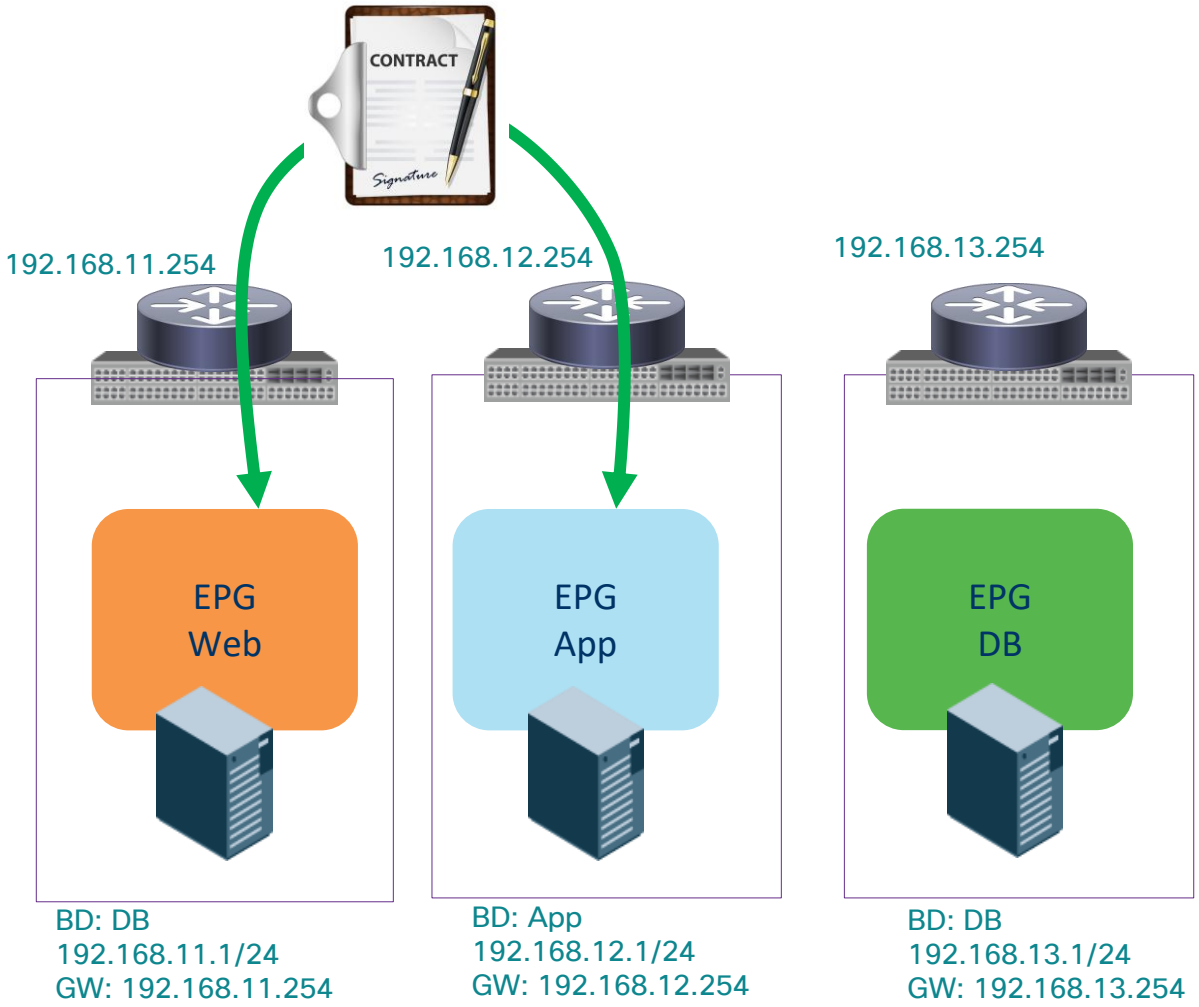
Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

How do I Insert a Firewall ?

2 conditions for traffic reaching destination

Before Service graph is deployed



APIC relies on :

✓ **Routing** to forward traffic

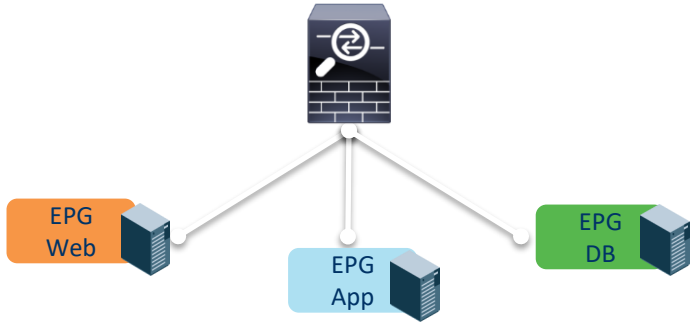
✓ **Contract** to allow traffic

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

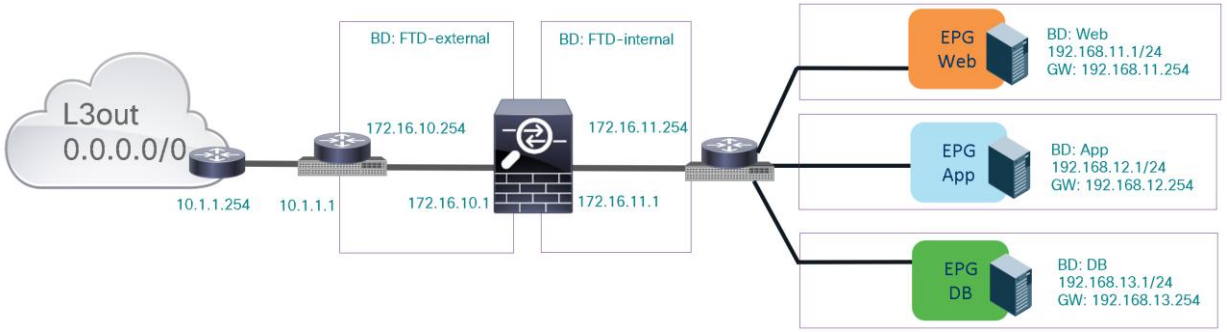
3 main ways to insert a Firewall in ACI

- “Network Stitching” Firewall Insertion

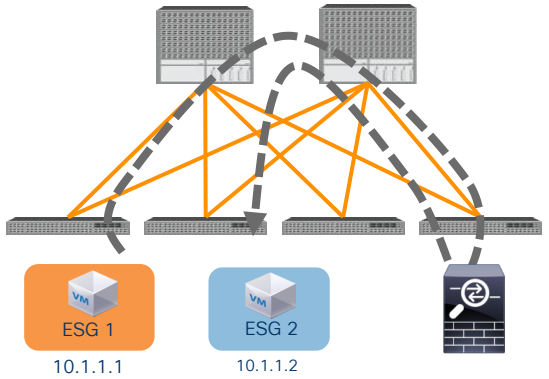
No contract and No Service Graph



- Traditional Service Graph



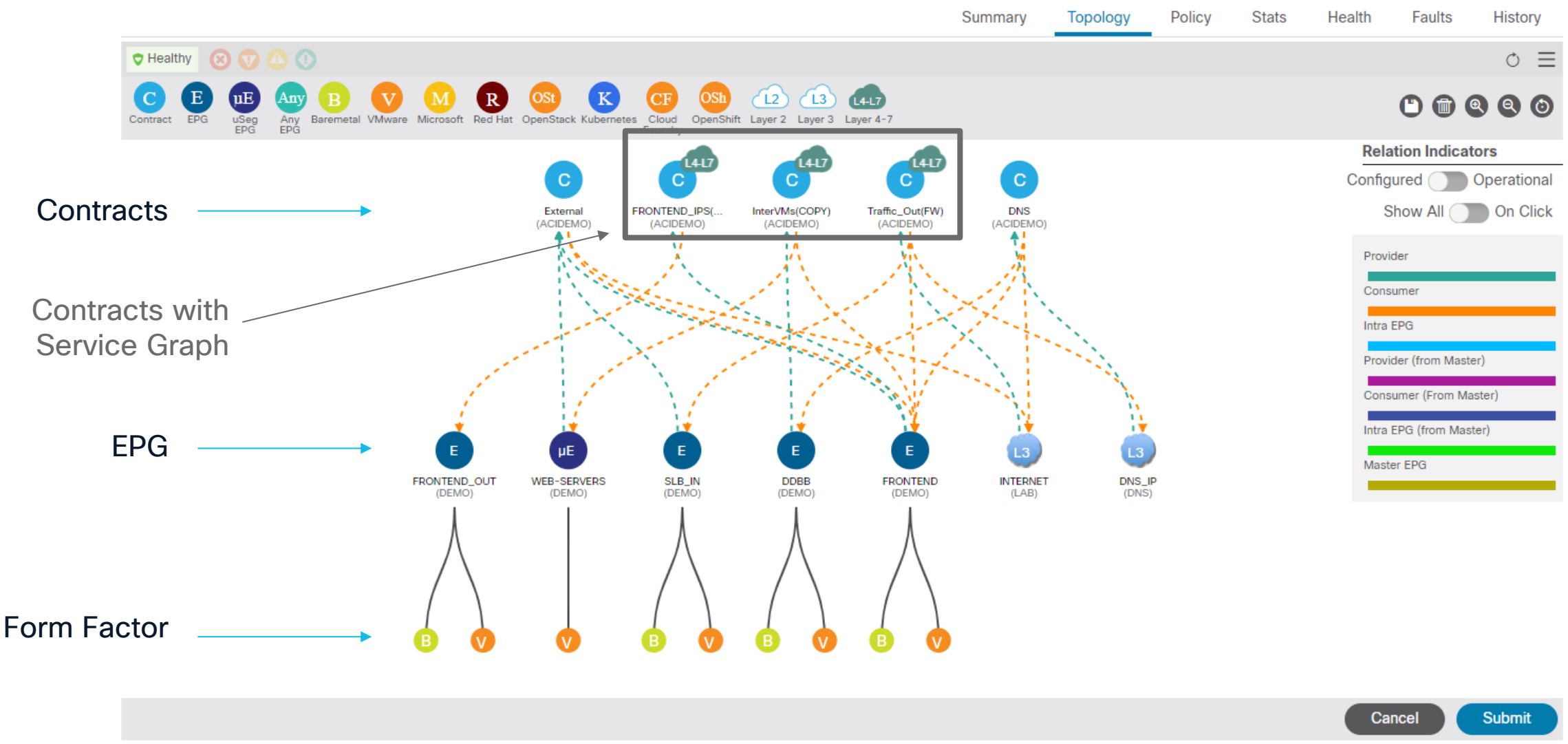
- Service Graph with Policy Based Redirect



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

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

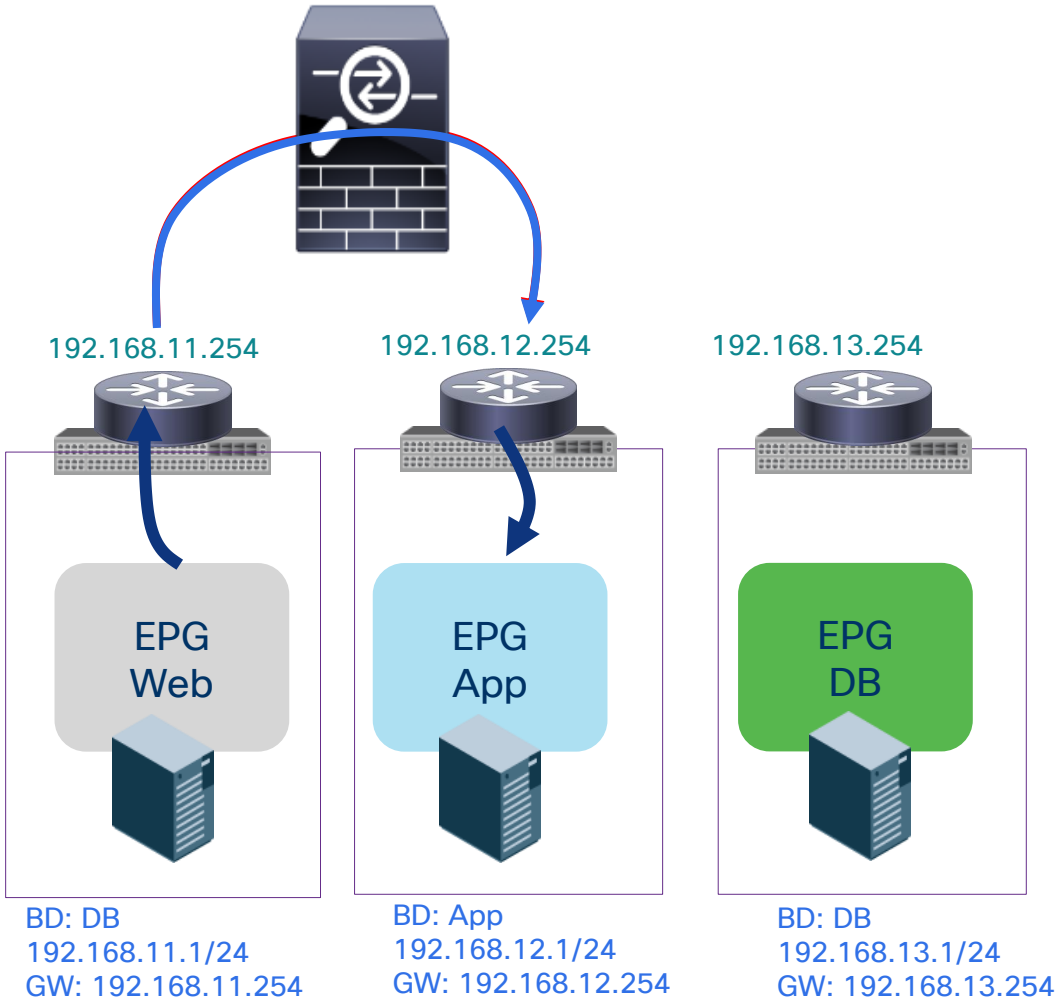
Attach a Service Graph to a contract



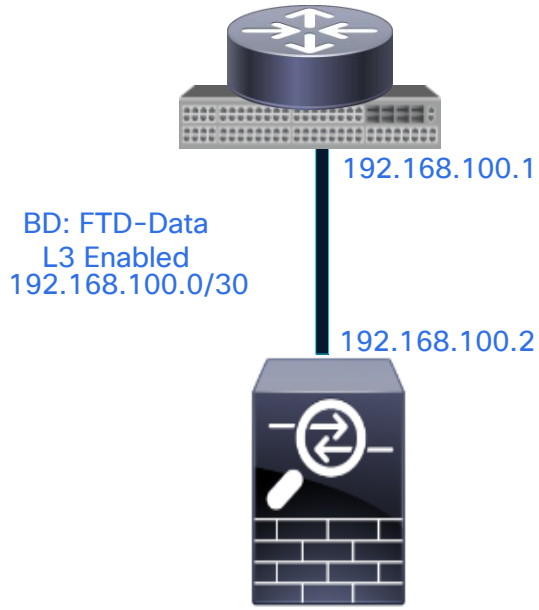
© 2025 Cisco and/or its affiliates. All rights reserved.

Policy Based Redirect is your Best Friend

With PBR Service Graph



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

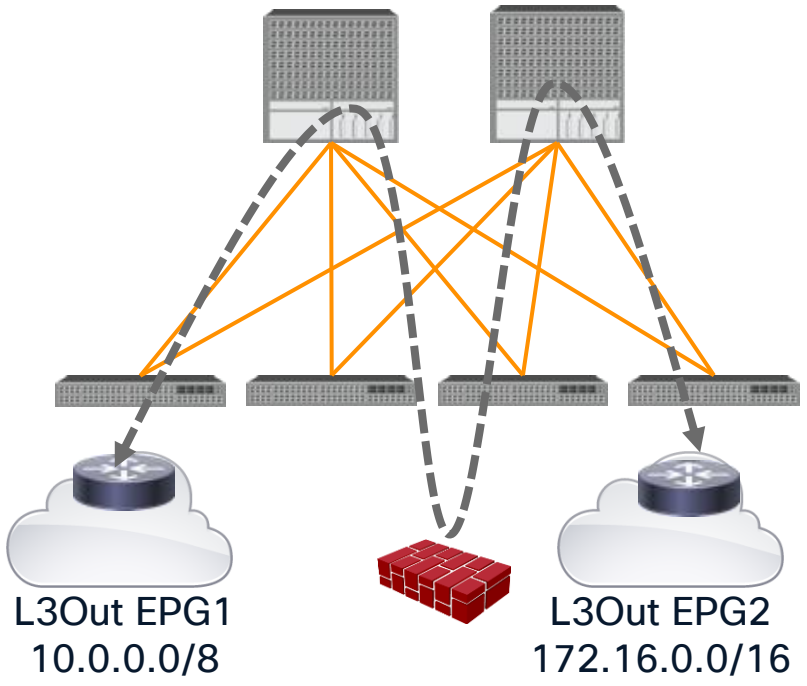


© 2025 Cisco and/or its affiliates. All rights reserved.

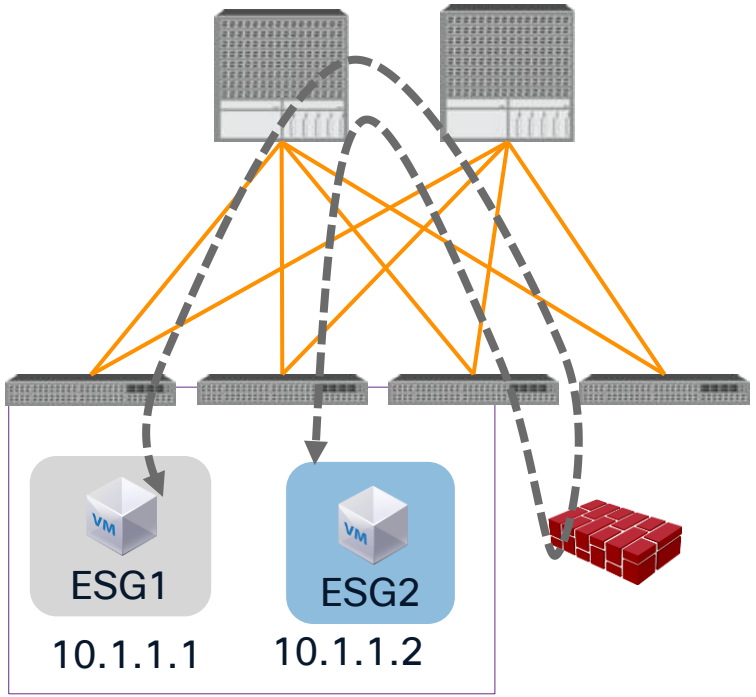
Where can we (re)use PBR?

Wherever contracts can be applied!

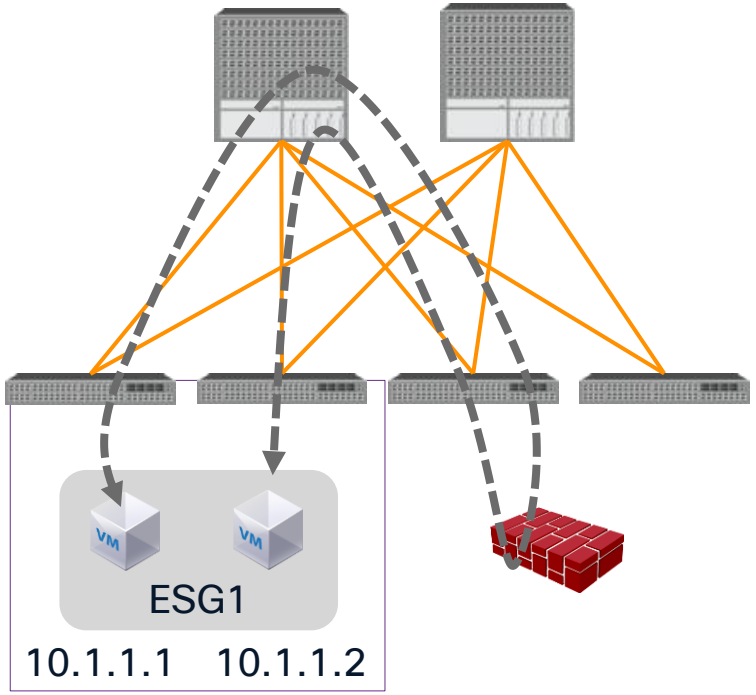
- Between EPGs or ESGs.
- Between L3Out EPGs.



- Between EPGs or ESGs in the same subnet.



- Between endpoints in the same EPG or ESG.

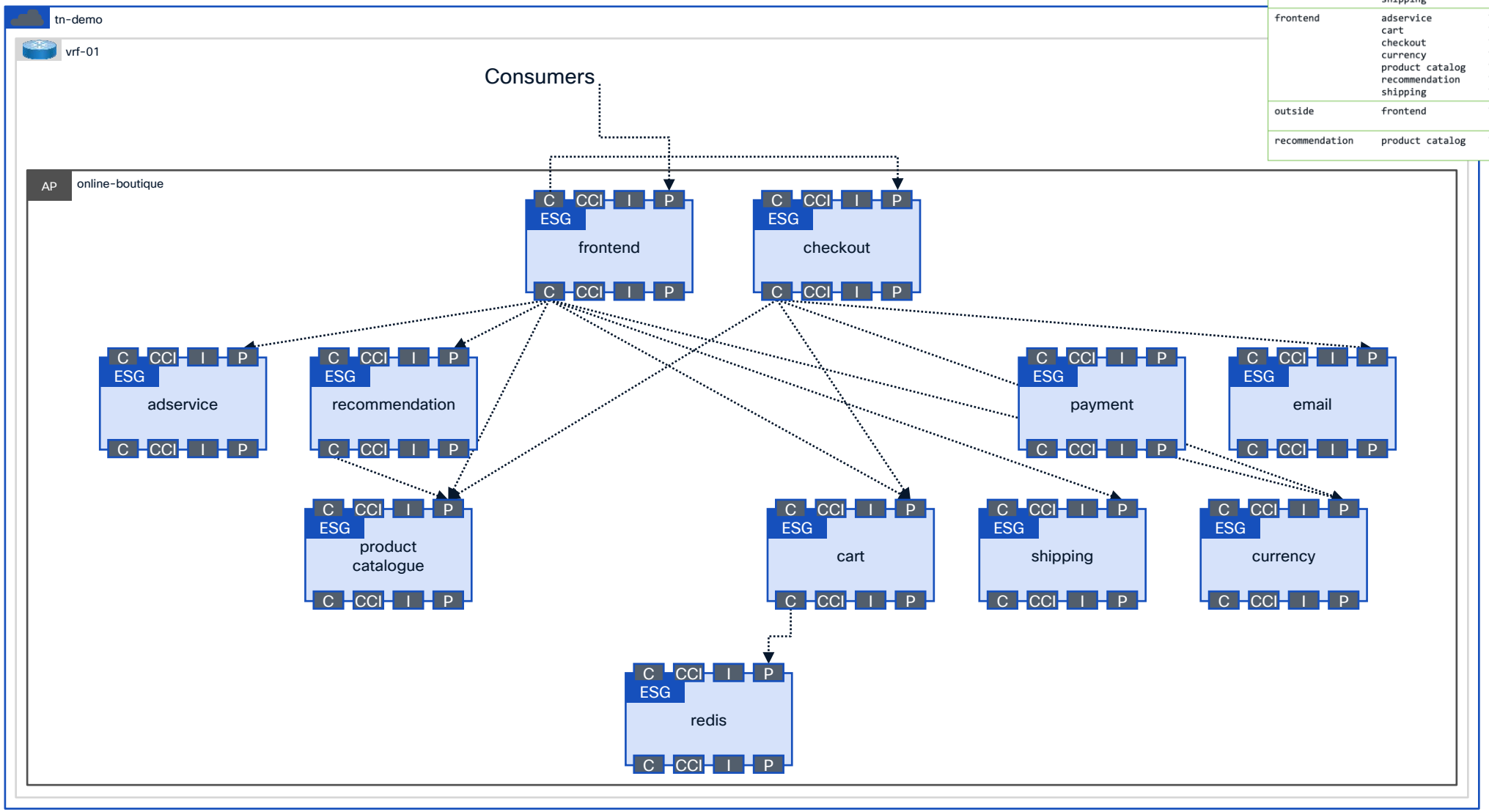


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

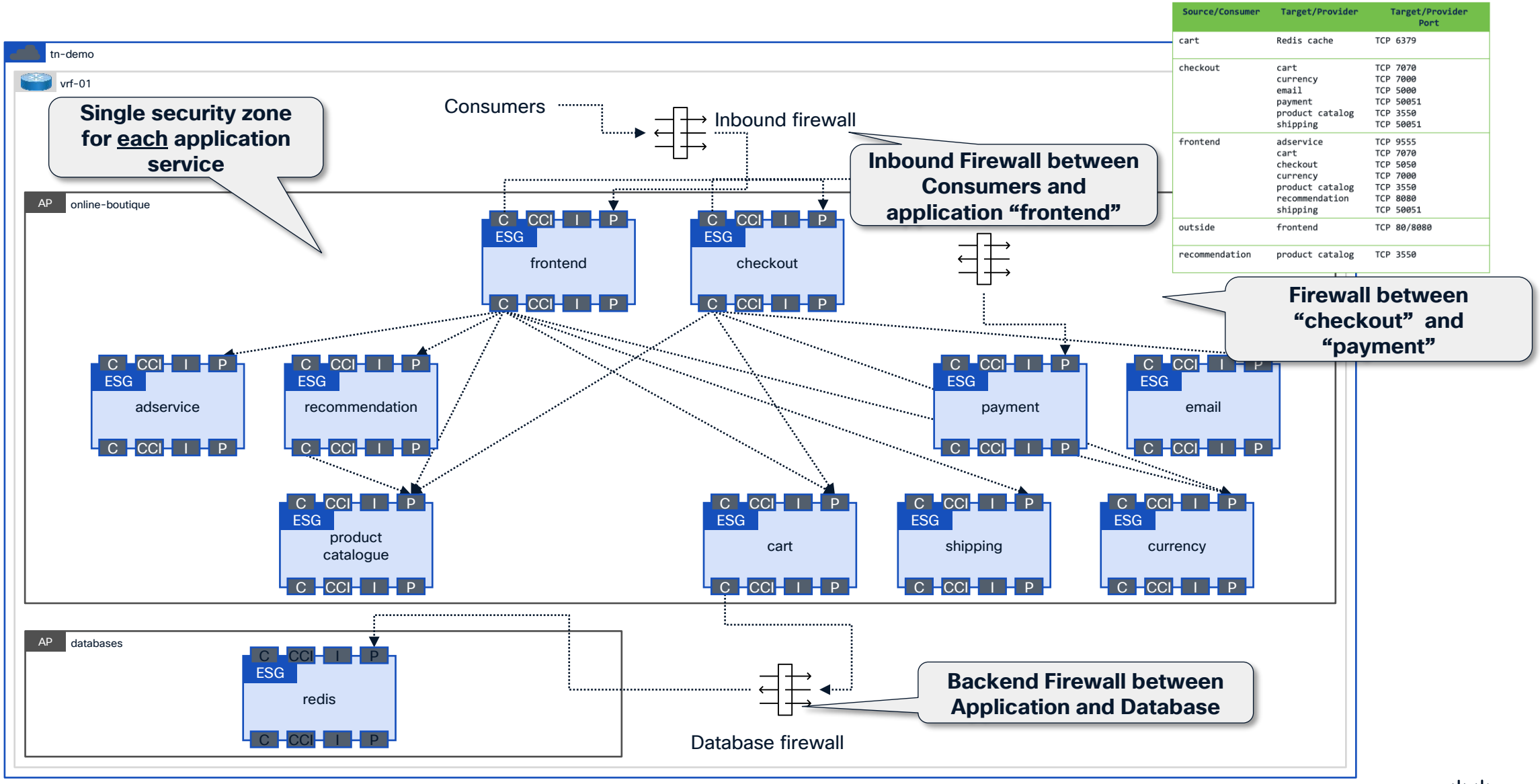
Application tiers across subnets

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
	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



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

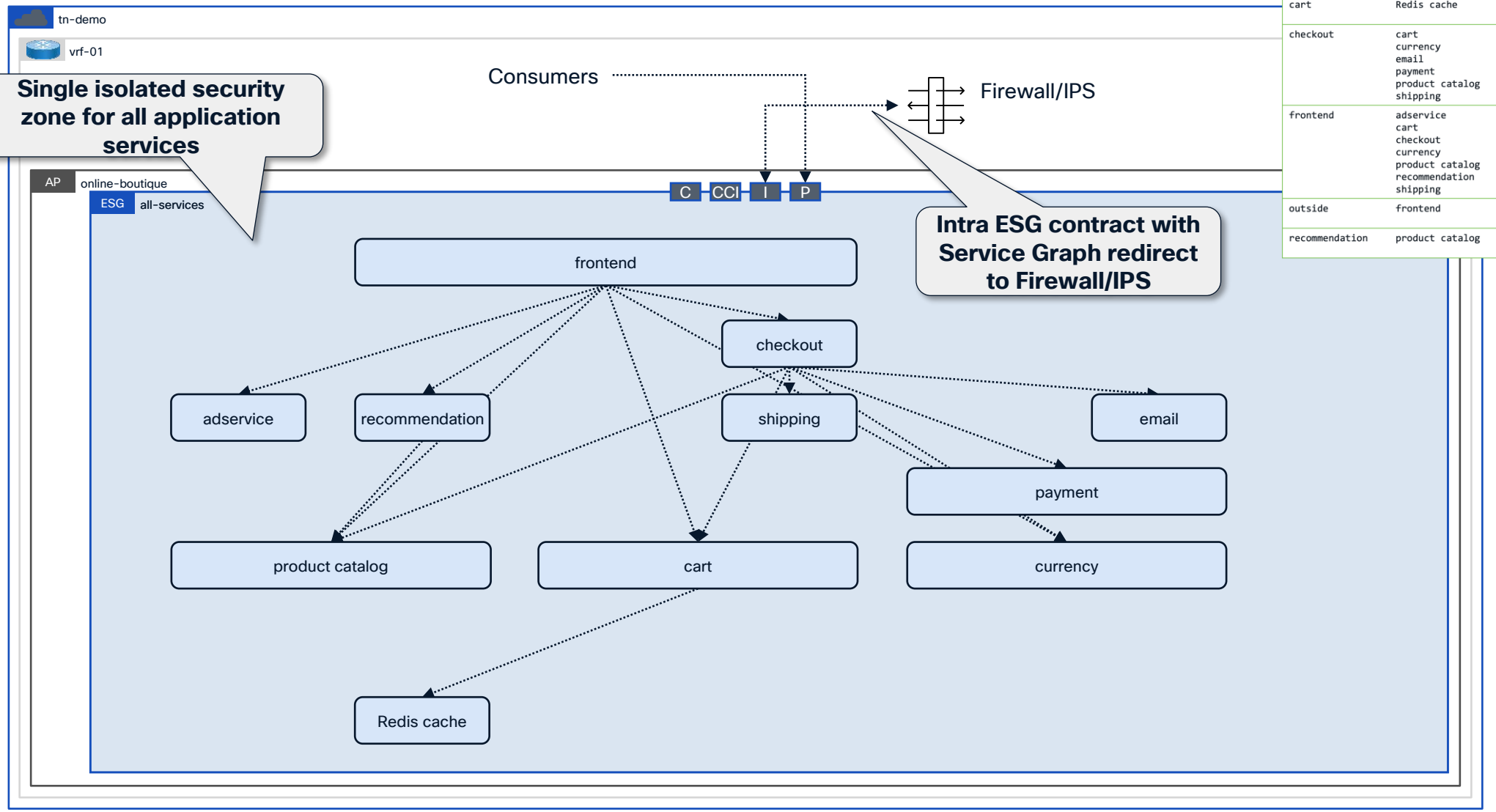
Complement ACI Contracts with Firewalls



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
	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

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

Microsegment with FTD using Intra-ESG SG



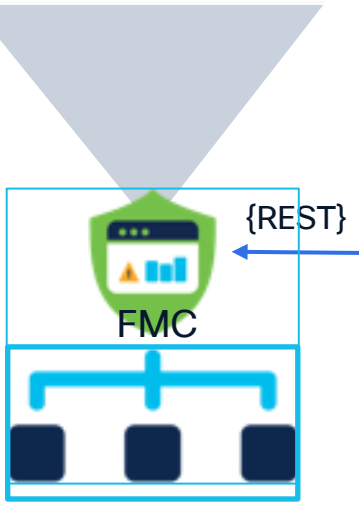
Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

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

Doing more with Dynamic Attributes Connector

Dynamic Object	Mappings
Linux-Servers	172.16.0.1 172.16.0.3
Windows-Servers	10.0.1.11 10.0.1.14 10.0.1.20
Powered-On	10.0.1.14



Adapters

FMC Adapter

Dynamic Attributes Filters

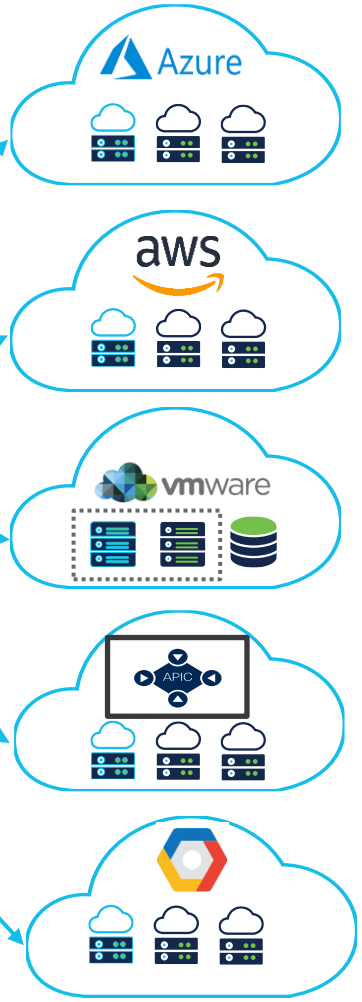
Name	Connector	Query
Linux-Servers	vCenter	**os** = 'RHEL 7 (64-bit)' OR **os** = 'CentOS 7 (64-bit)'
Windows-Servers	vCenter	**os** = 'MS Windows Server 2016 (64-bit)' AND **network**='PROD_NETW' AND **Power**='running'
Powered-On	vCenter	**Power**='running' AND (**network**='PROD_NETW' OR **host**='NODE1')

CSDAC (Container)

Connectors

- Azure Connector
- AWS Connector
- vCenter / NSX Connector
- APIC Connector
- GCP Connector

Providers

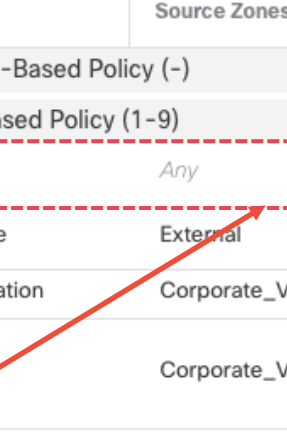


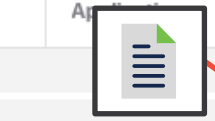
© 2025 Cisco and/or its affiliates. All rights reserved.

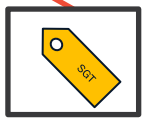
cisco

Attribute Based Policy

#	Name	Source Zones	Dest Zones	Users	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	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	A
2	IoT Support Service	External	IoT_VN	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Pri	Corporate_VN	Data_Center_Edge	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	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



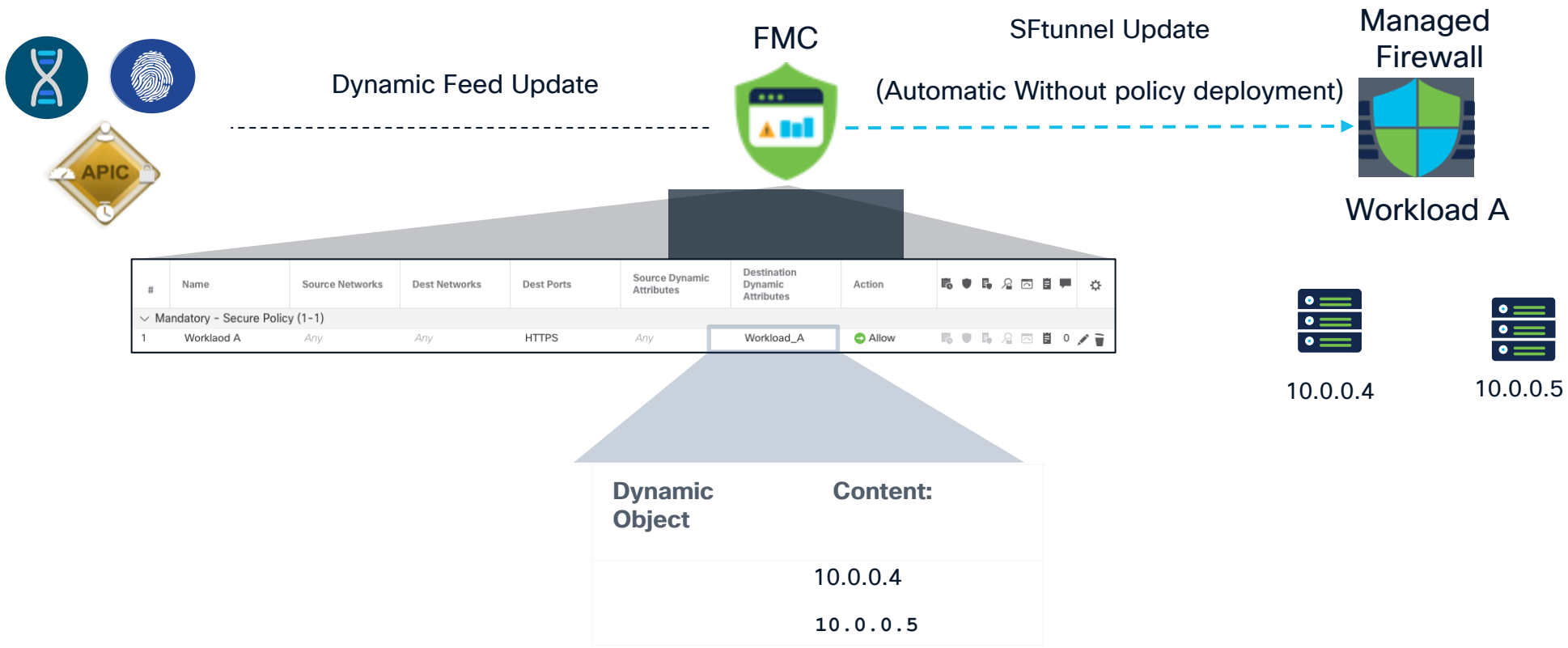




© 2025 Cisco and/or its affiliates. All rights reserved.

Dynamic Objects in Action

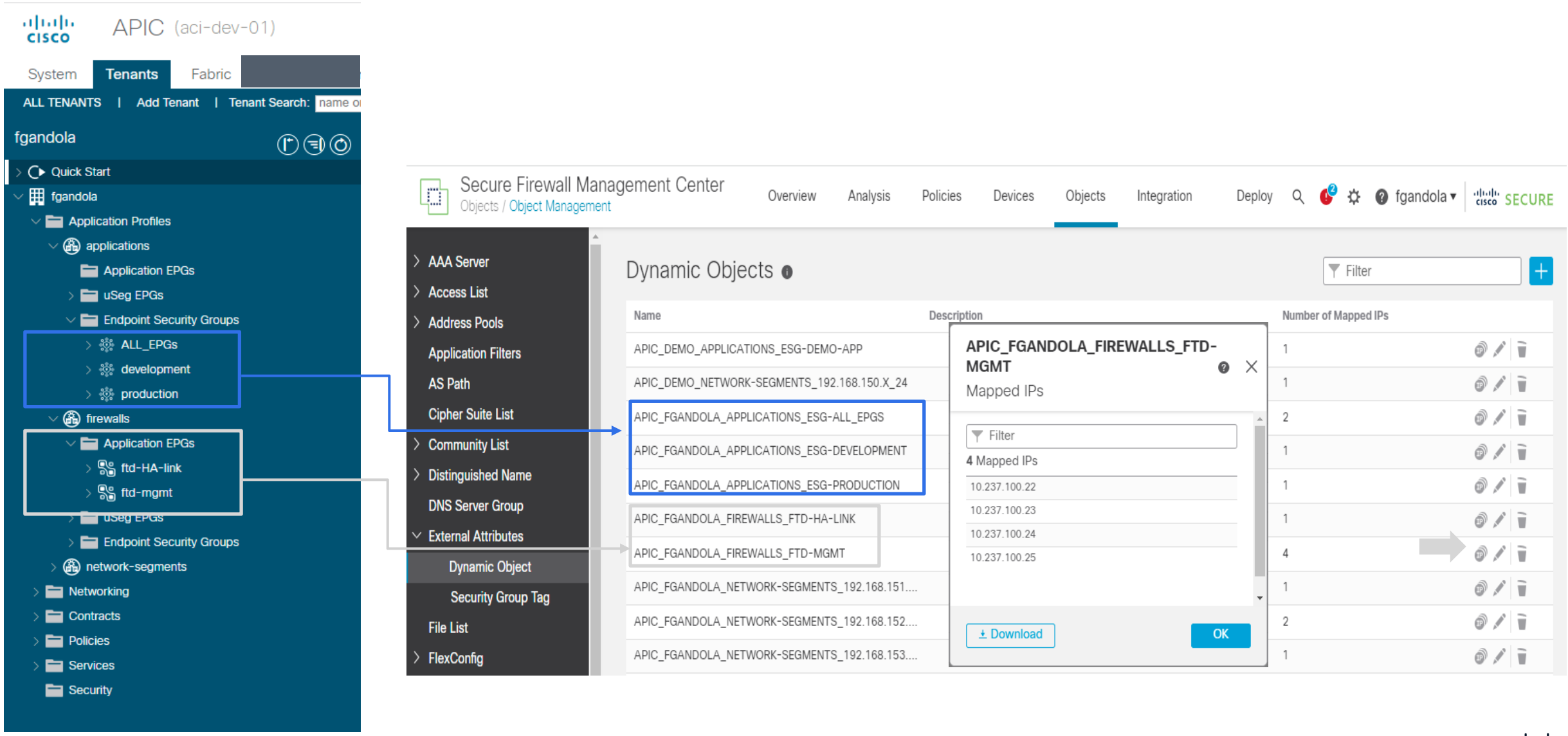
Automatic Without policy deployment



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

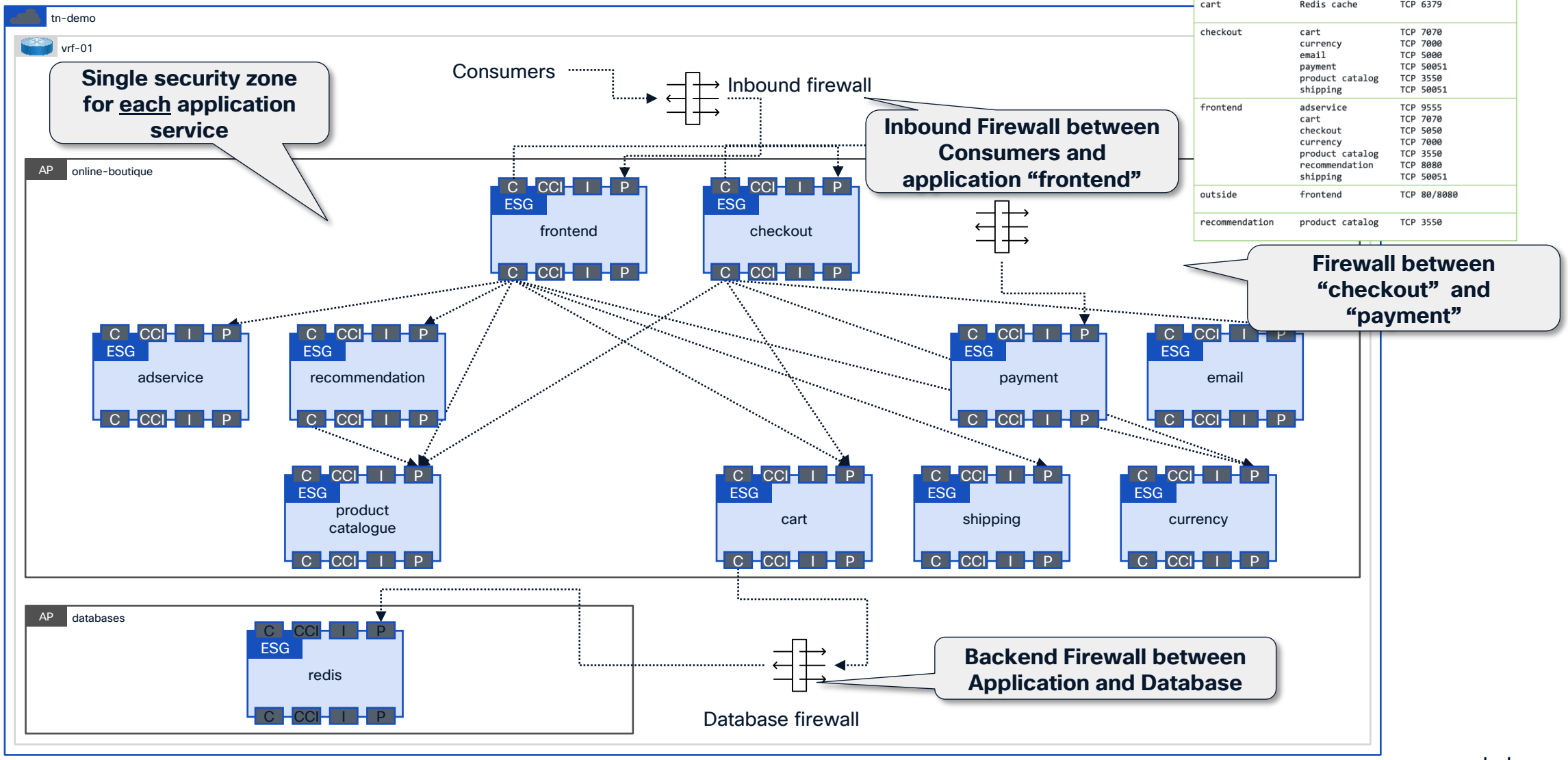
cisco

Establish Trust – FMC Learns EPGs/ESGs



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

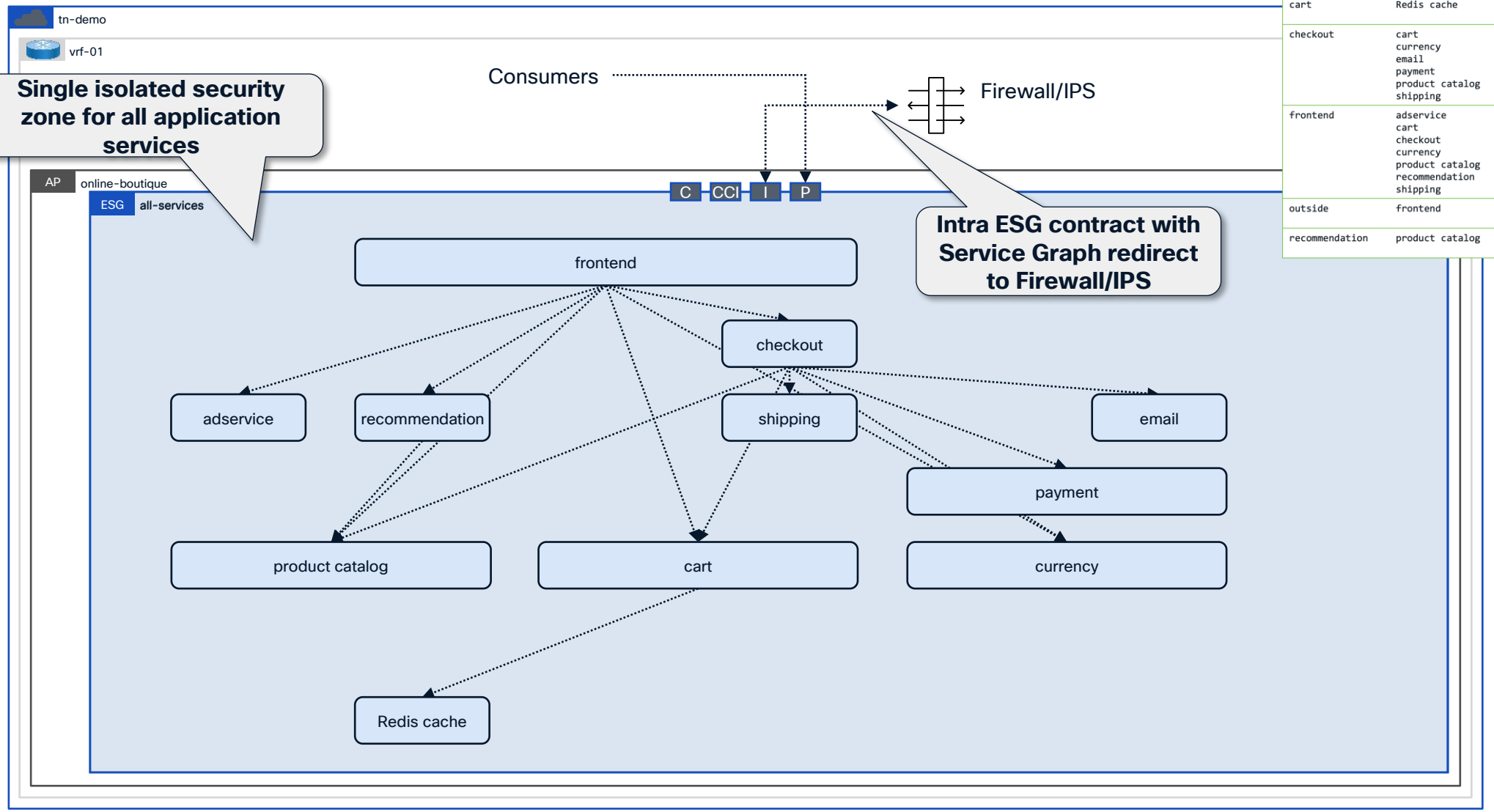
Leverage CSDAC to use EPG and ESG in your FTD policy



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
	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

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

Use CSDAC to use Dynamic Group in FTD

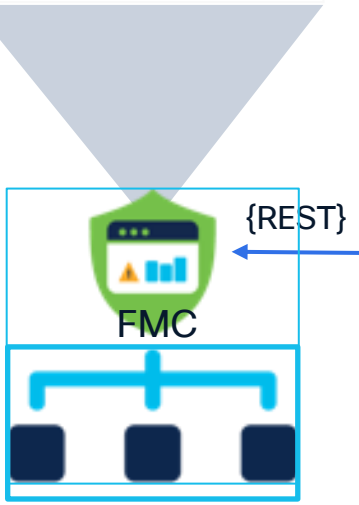


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

Doing more with Dynamic Attributes Connector

Dynamic Object	Mappings
Linux-Servers	172.16.0.1 172.16.0.3
Windows-Servers	10.0.1.11 10.0.1.14 10.0.1.20
Powered-On	10.0.1.14



Adapters

FMC Adapter

Dynamic Attributes Filters

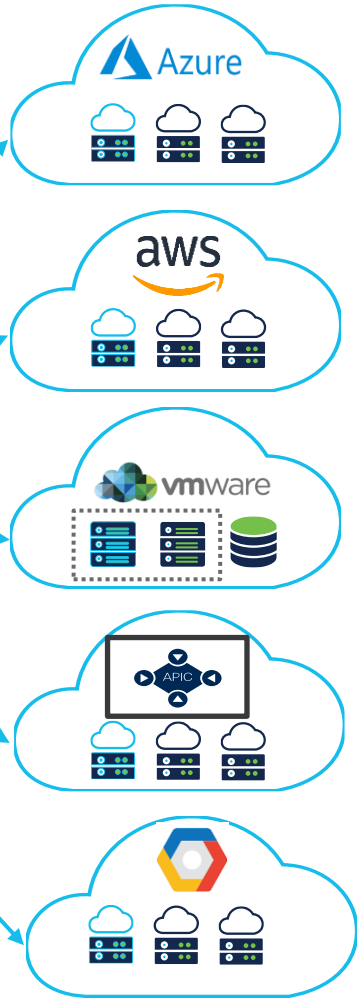
Name	Connector	Query
Linux-Servers	vCenter	**os** = 'RHEL 7 (64-bit)' OR **os** = 'CentOS 7 (64-bit)'
Windows-Servers	vCenter	**os** = 'MS Windows Server 2016 (64-bit)' AND **network**='PROD_NETW' AND **Power**='running'
Powered-On	vCenter	**Power**='running' AND (**network**='PROD_NETW' OR **host**='NODE1')

CSDAC (Container)

Connectors

- Azure Connector
- AWS Connector
- vCenter / NSX Connector
- APIC Connector
- GCP Connector

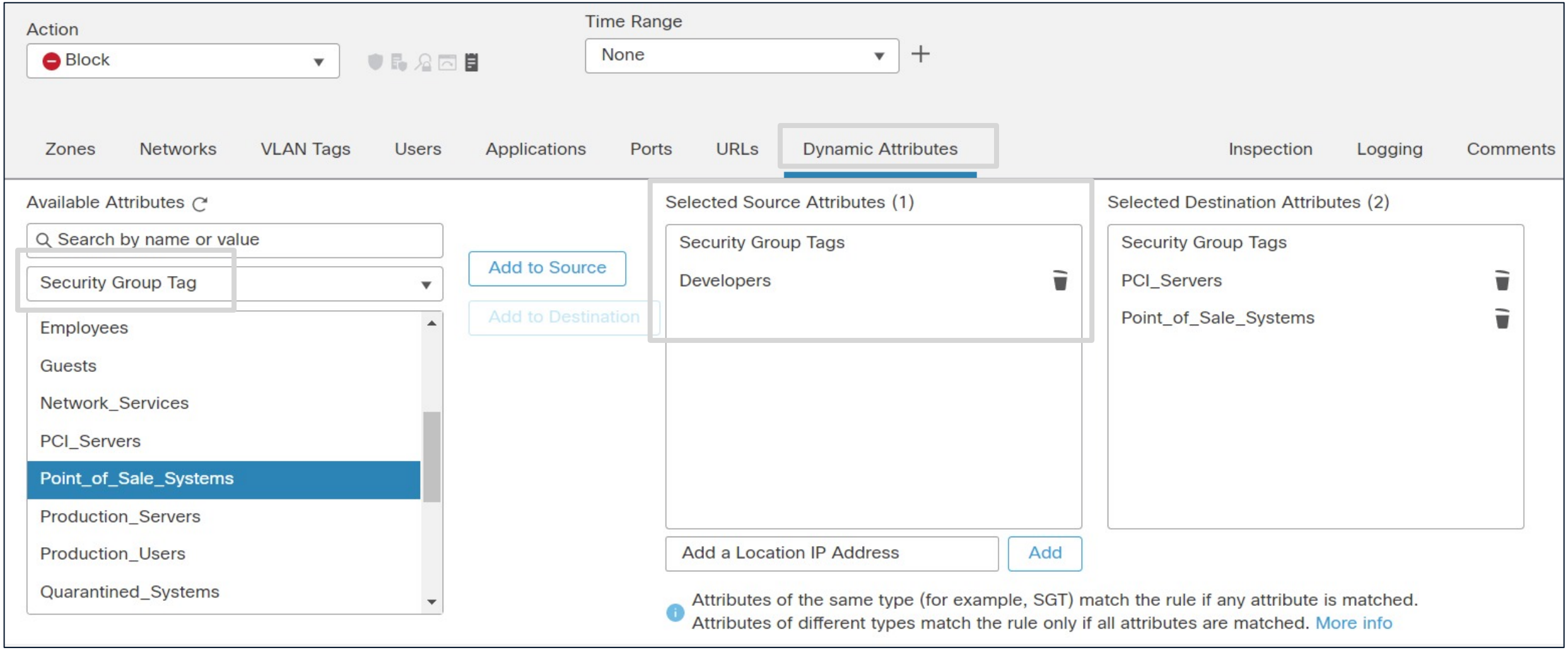
Providers



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

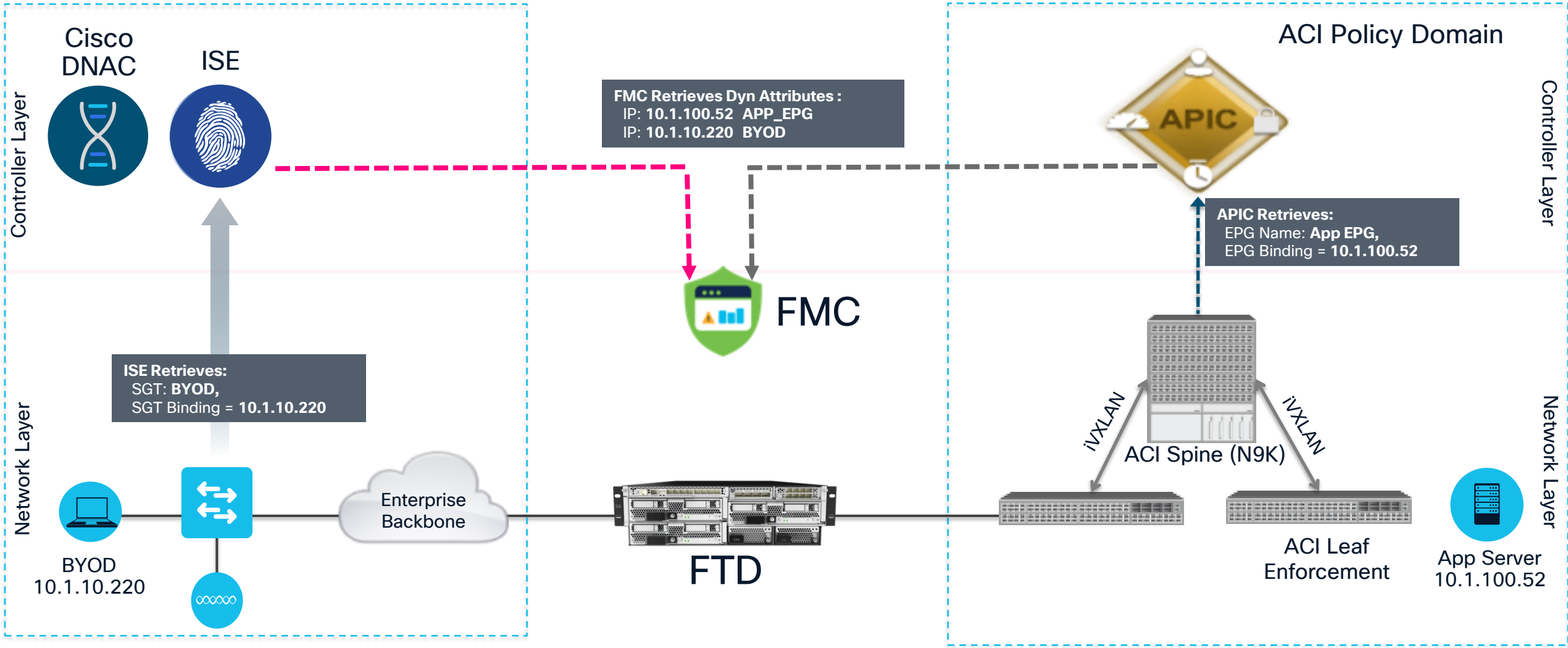
cisco

Establish Trust – FTD/ASA can leverage SGTs



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

Use dynamic attributes to enforce trust

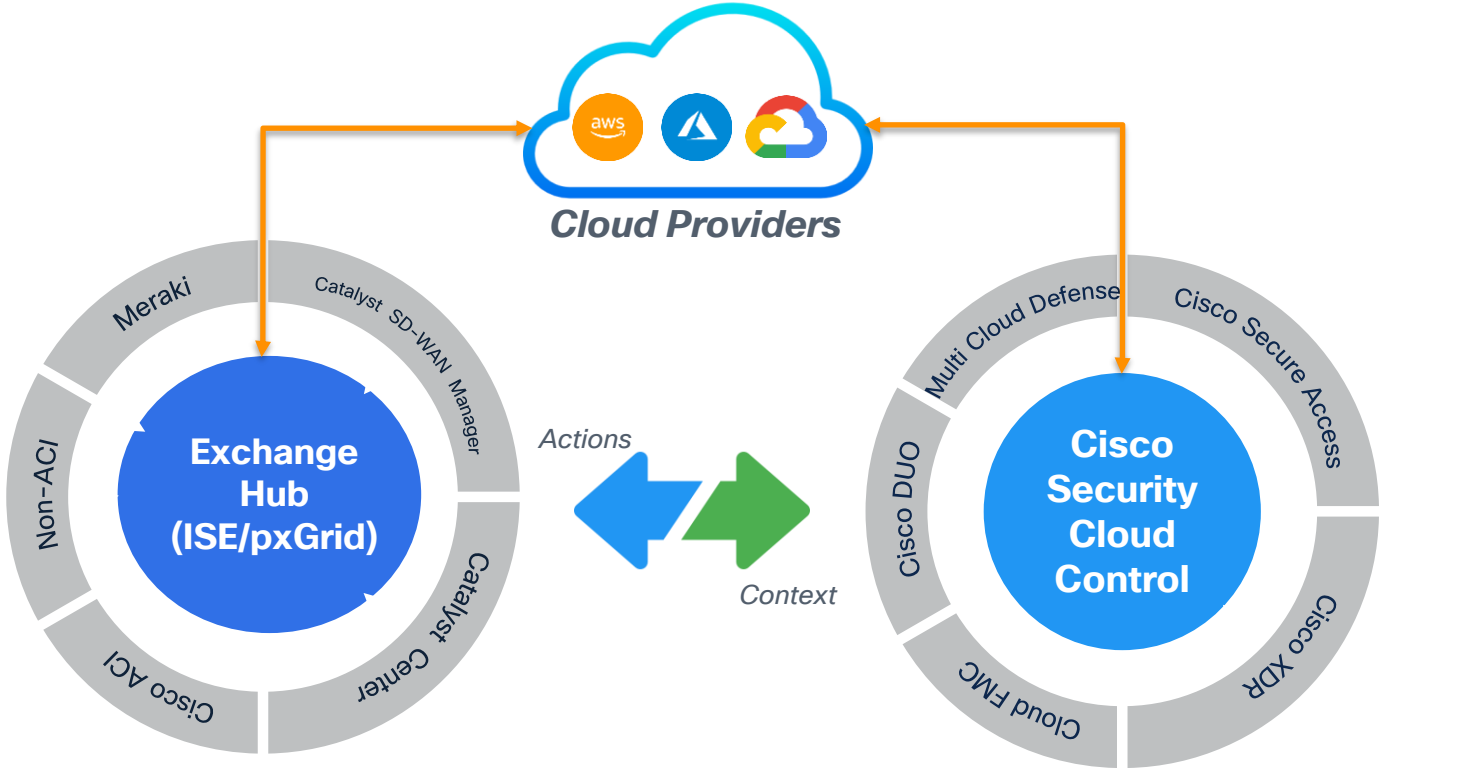


© 2025 Cisco and/or its affiliates. All rights reserved.

Alternatively establish trust with Cisco ISE

Normalizing and sharing context across domains

ISE Partner Ecosystem



User/Devices/ Application Identity, Location, Device Posture

Networking Domain

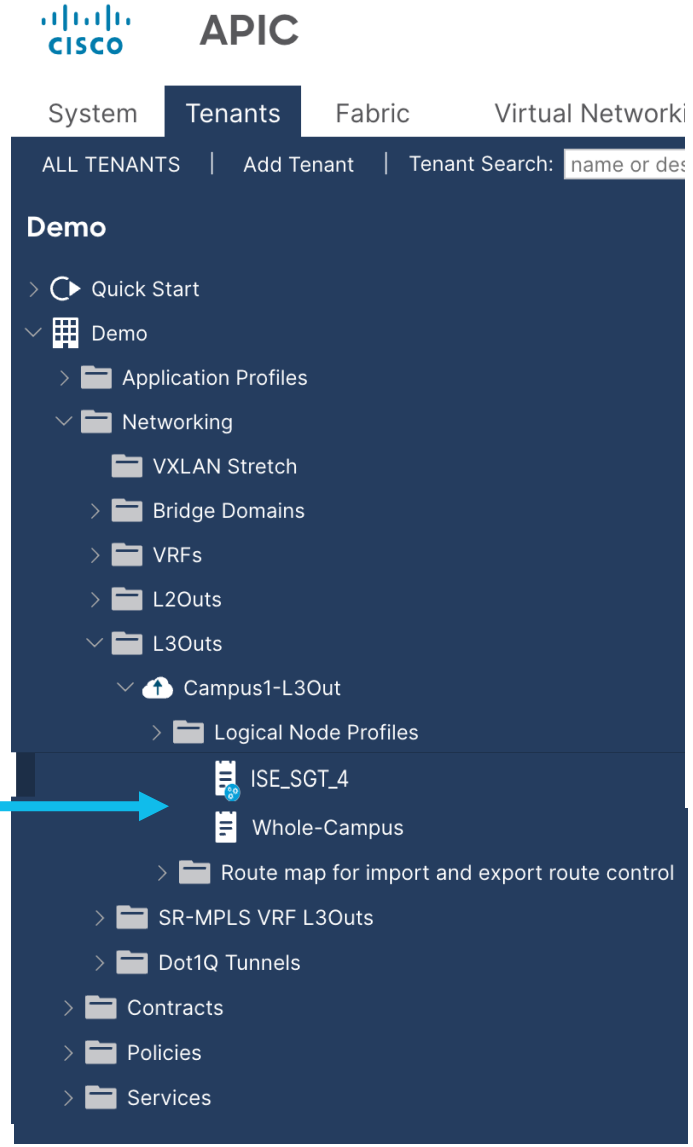
Threat Hunting/Investigation/Response and Policy Enforcement

Security Domain

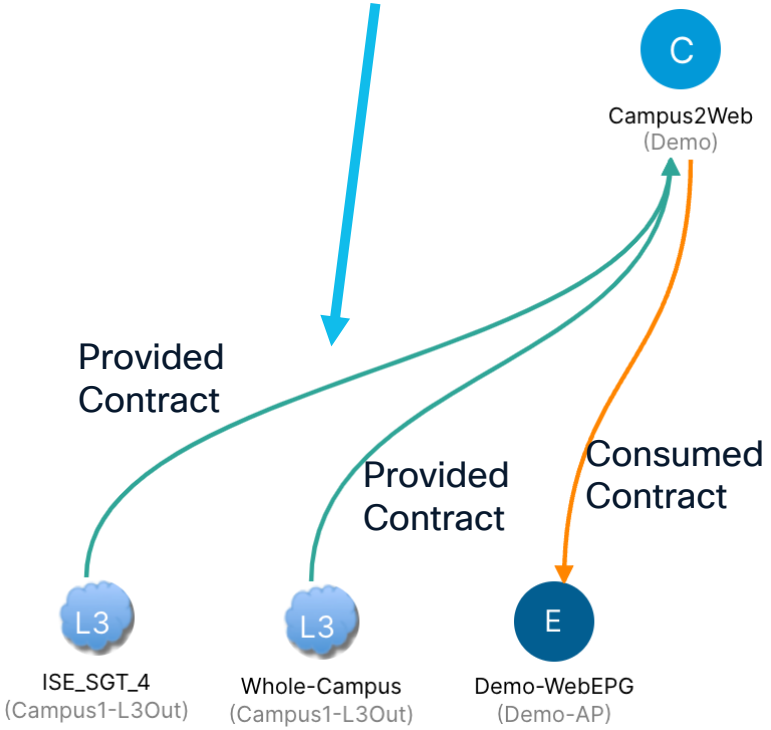
© 2025 Cisco and/or its affiliates. All rights reserved.

Context Sent to ACI

SGT added as External EPG



Newly added Group attached to existing Contract in APIC:



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

cisco

Walk before you run...

How do my applications communicate ?

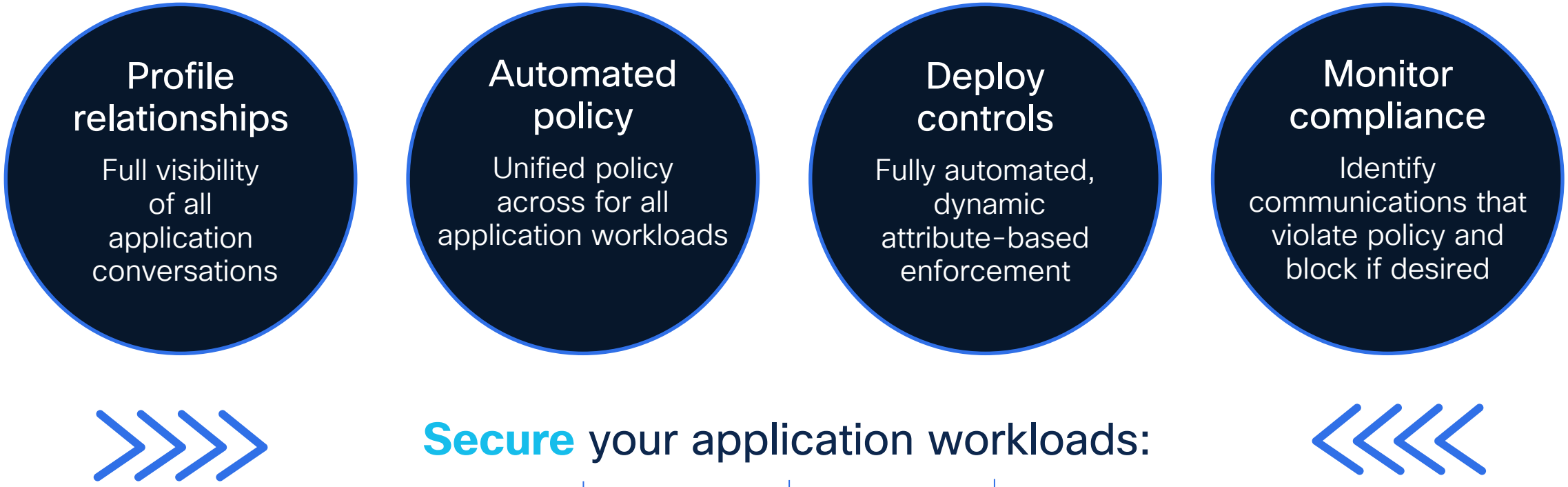
What are the services I must allow for this application to work?

Does the application team know how the application communicate ?

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

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

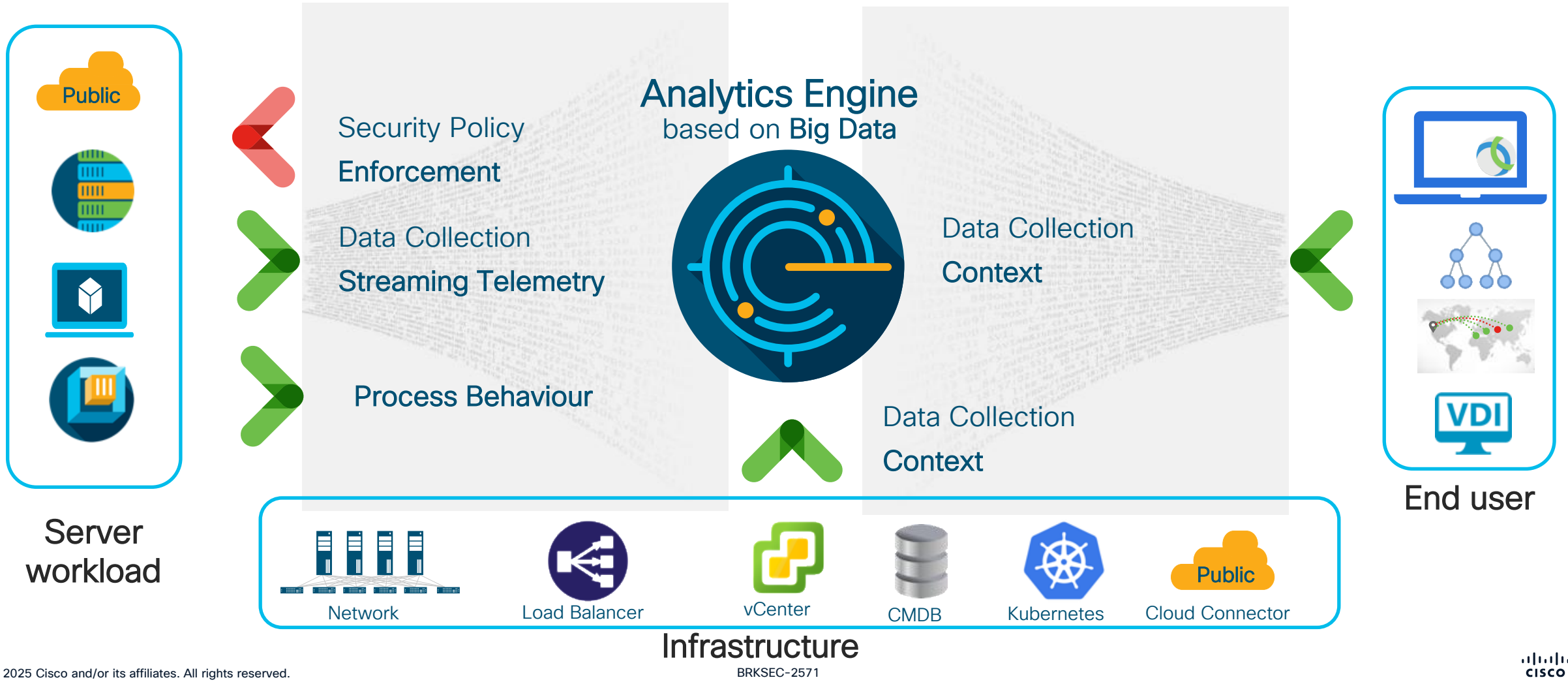
Dynamically securing the Workload Infrastructure



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

cisco

Secure Workload Architecture



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

Automated Application Policy Discovery

Baseline workload protection posture

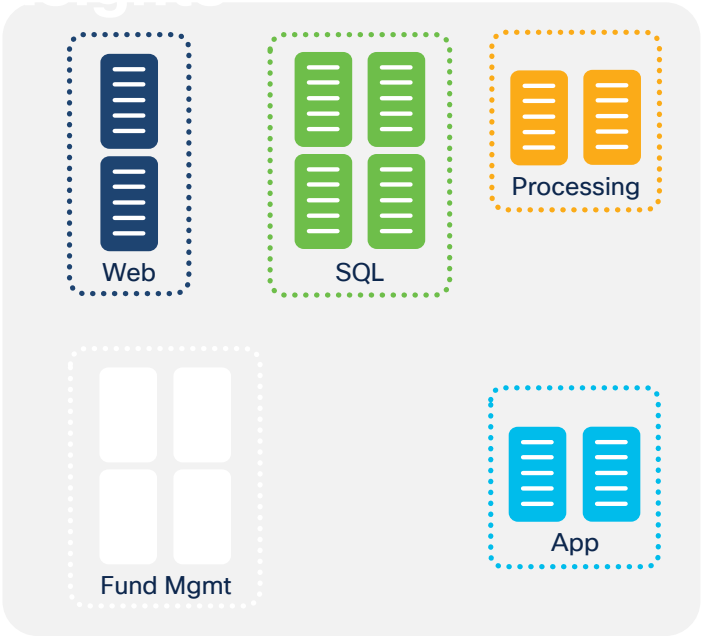
- Network communications
- Process behaviour
- Labels

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

Automated Application Policy Discovery

Baseline workload protection posture

- Network communications
- Process behaviour
- Labels

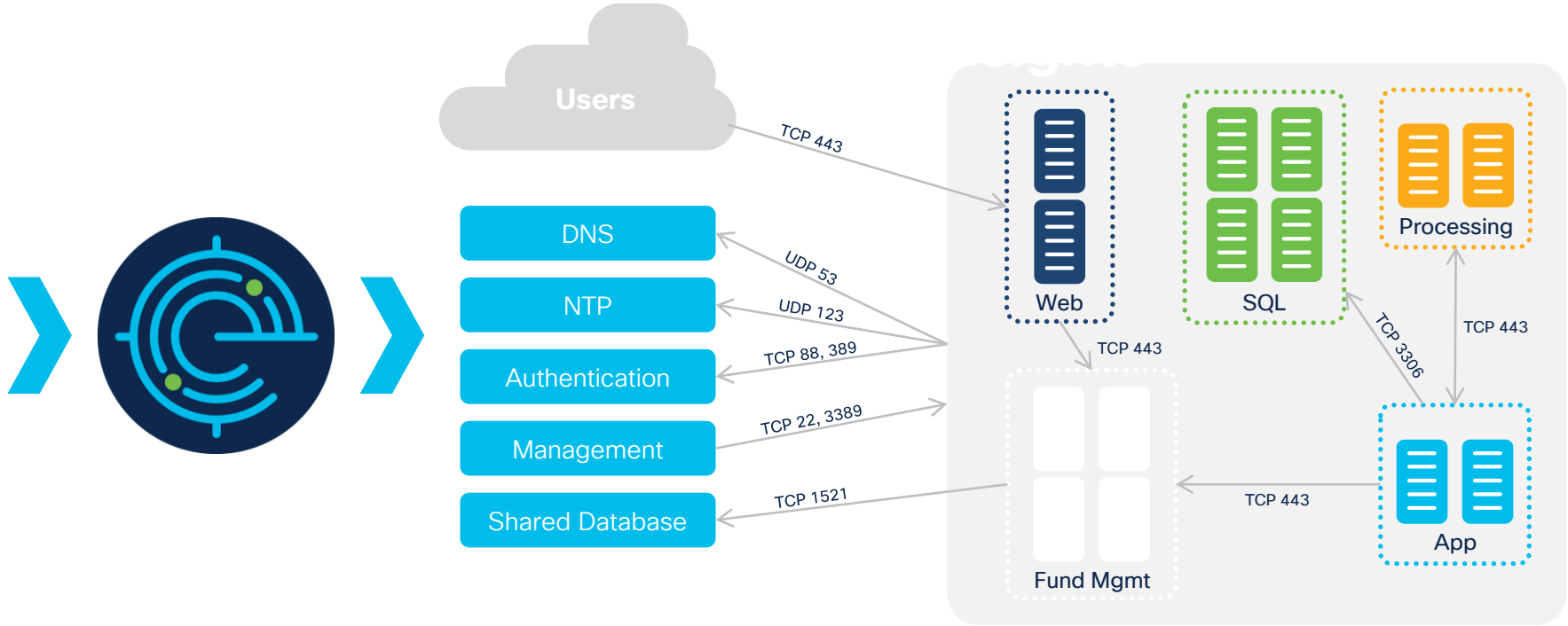


© 2025 Cisco and/or its affiliates. All rights reserved.

Automated Application Policy Discovery

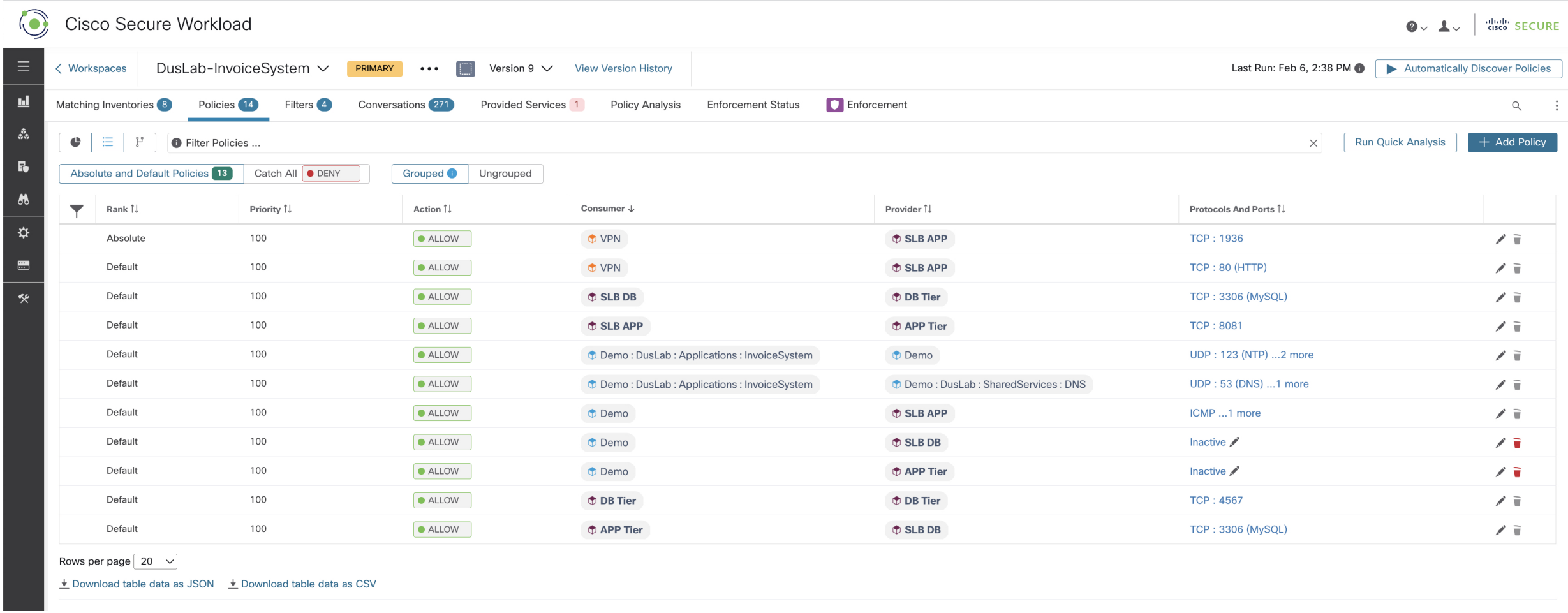
Baseline workload protection posture

- Network communications
- Process behaviour
- Labels



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

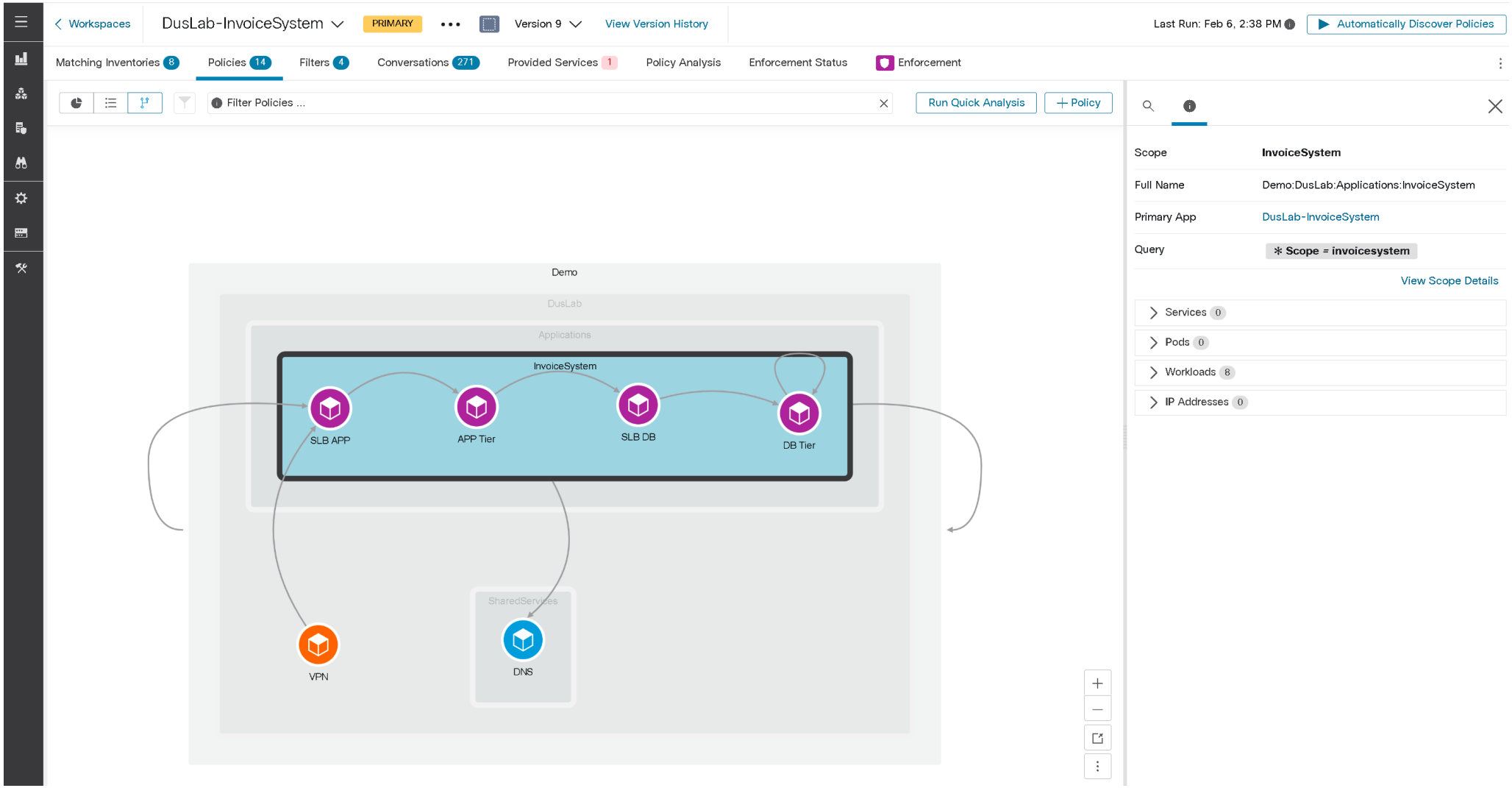
Auto-generated policies
Policy list view



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

Auto-generated policies

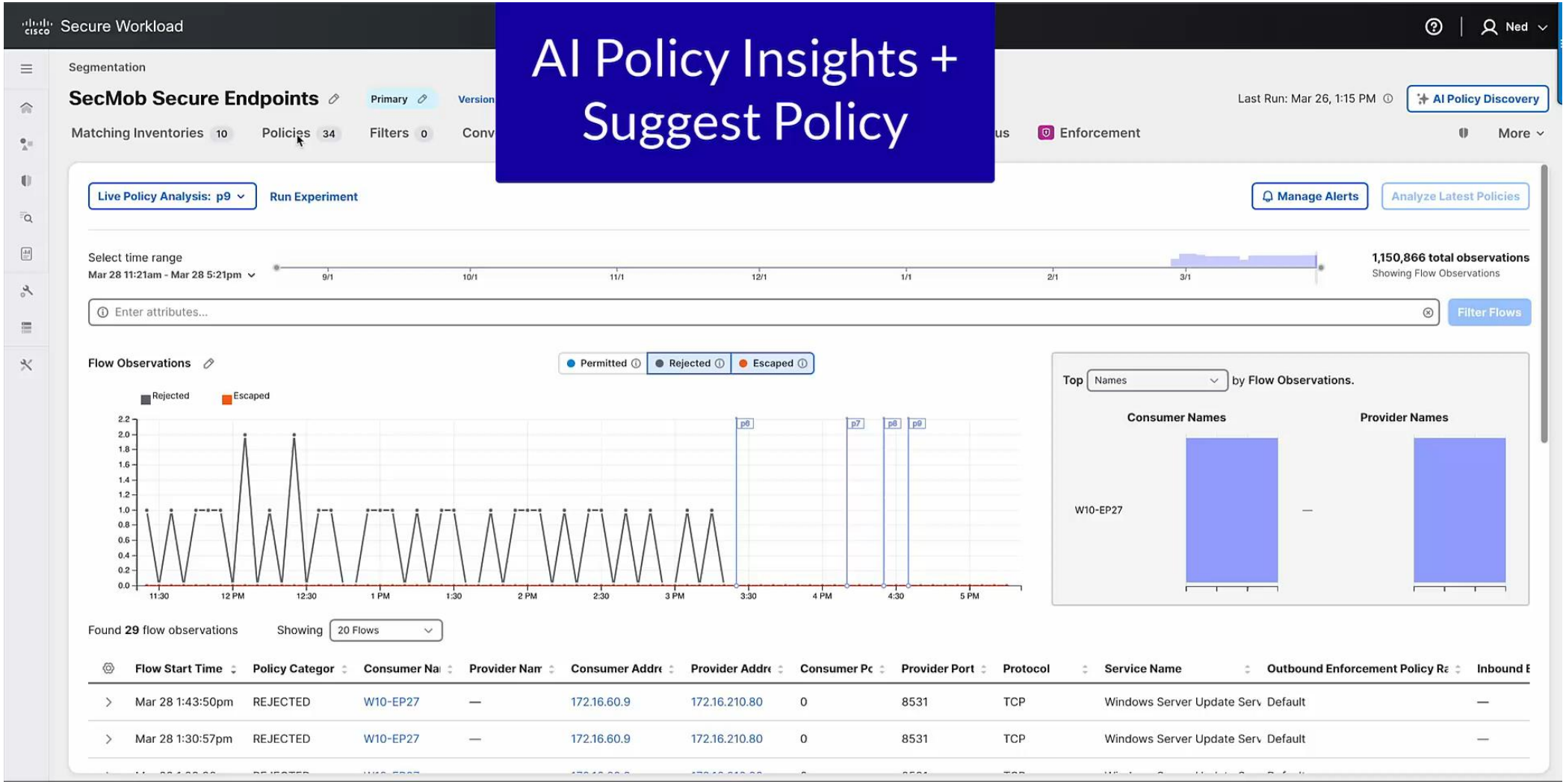
- Canvas App view



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

Policy Lifecycle Mgmt. AI Policy Insights / Suggested Policy

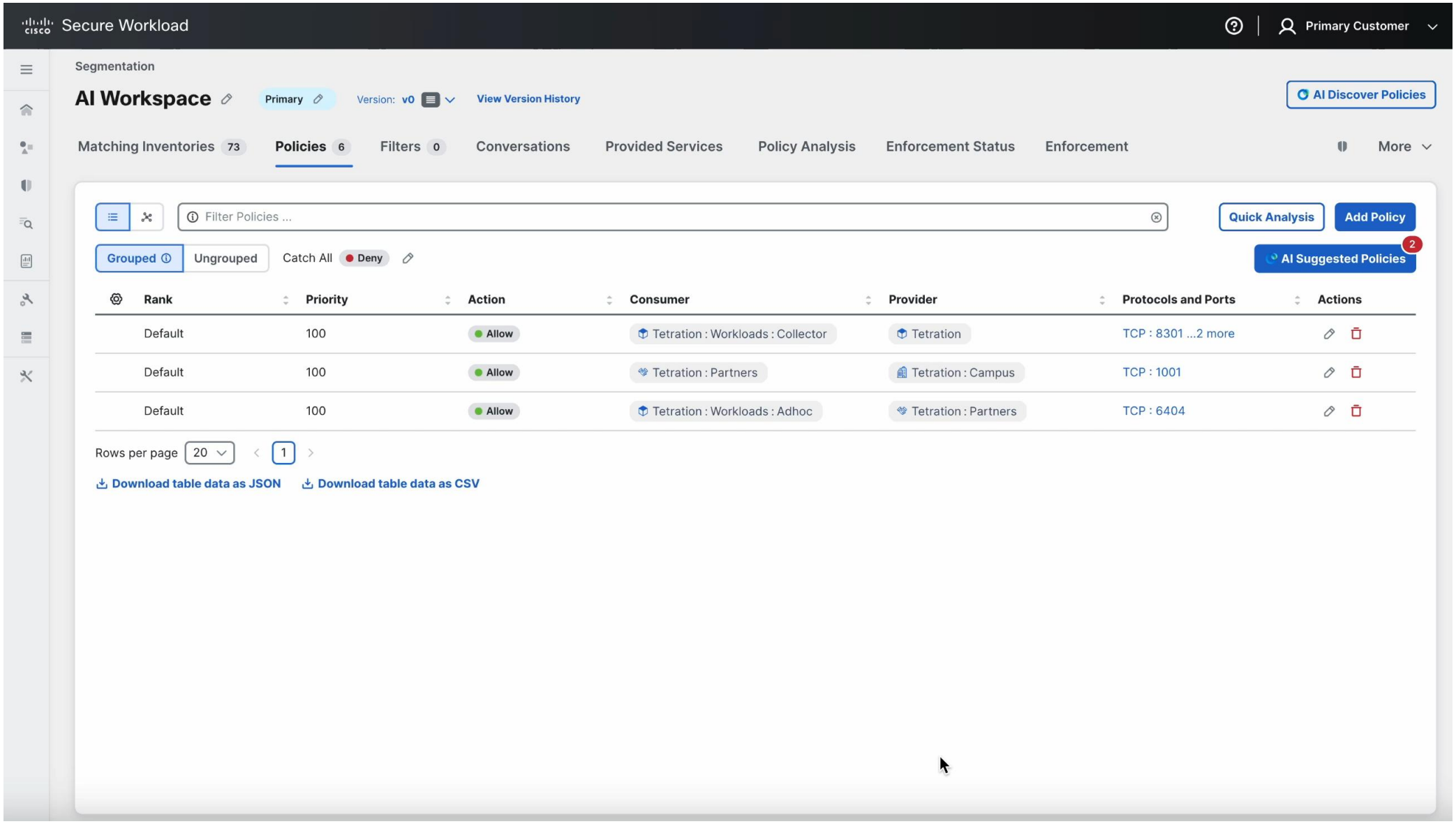
Available Now -3.10.1



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

AI Suggested Policies

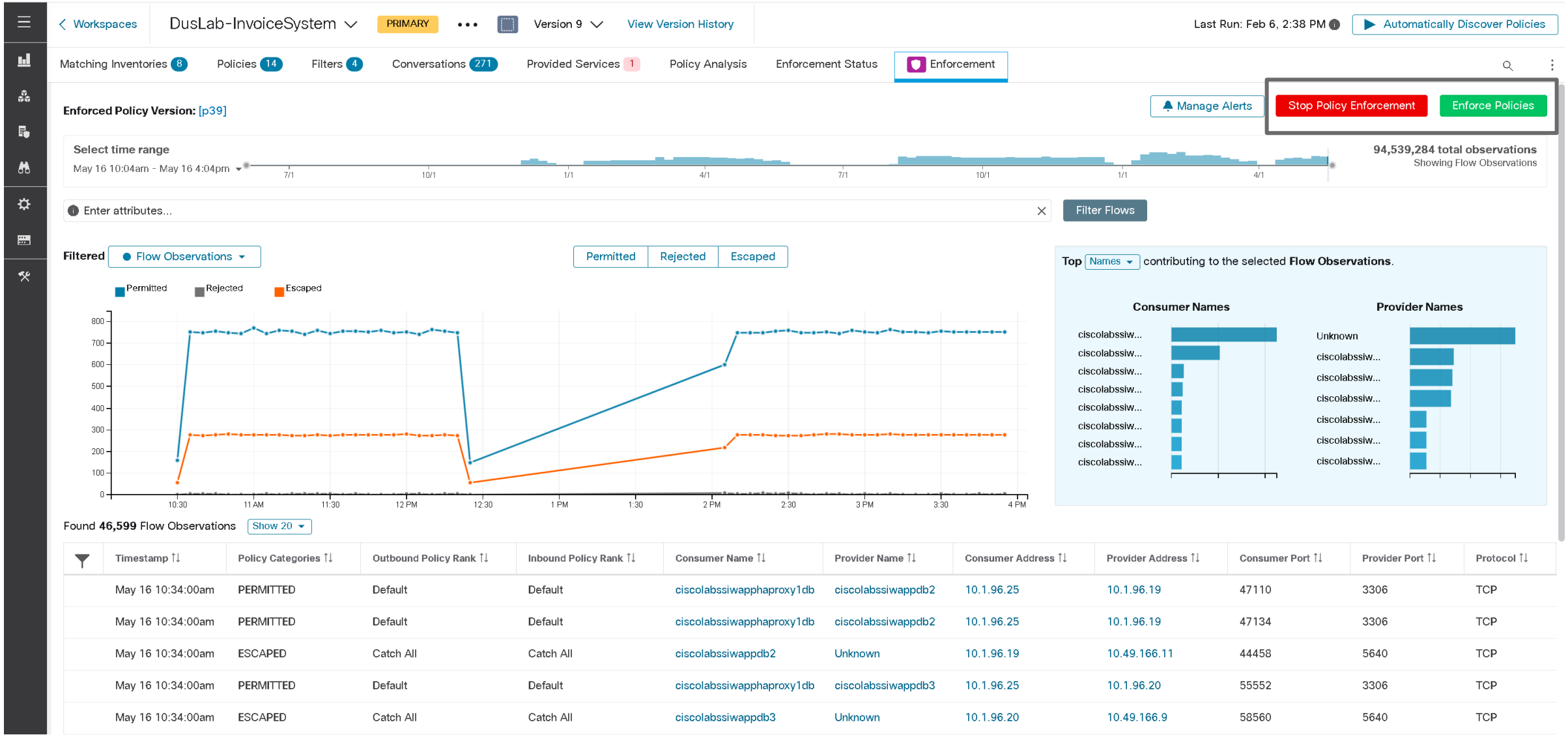
Available Now -3.10.4



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

One click away from enforcement with CSW

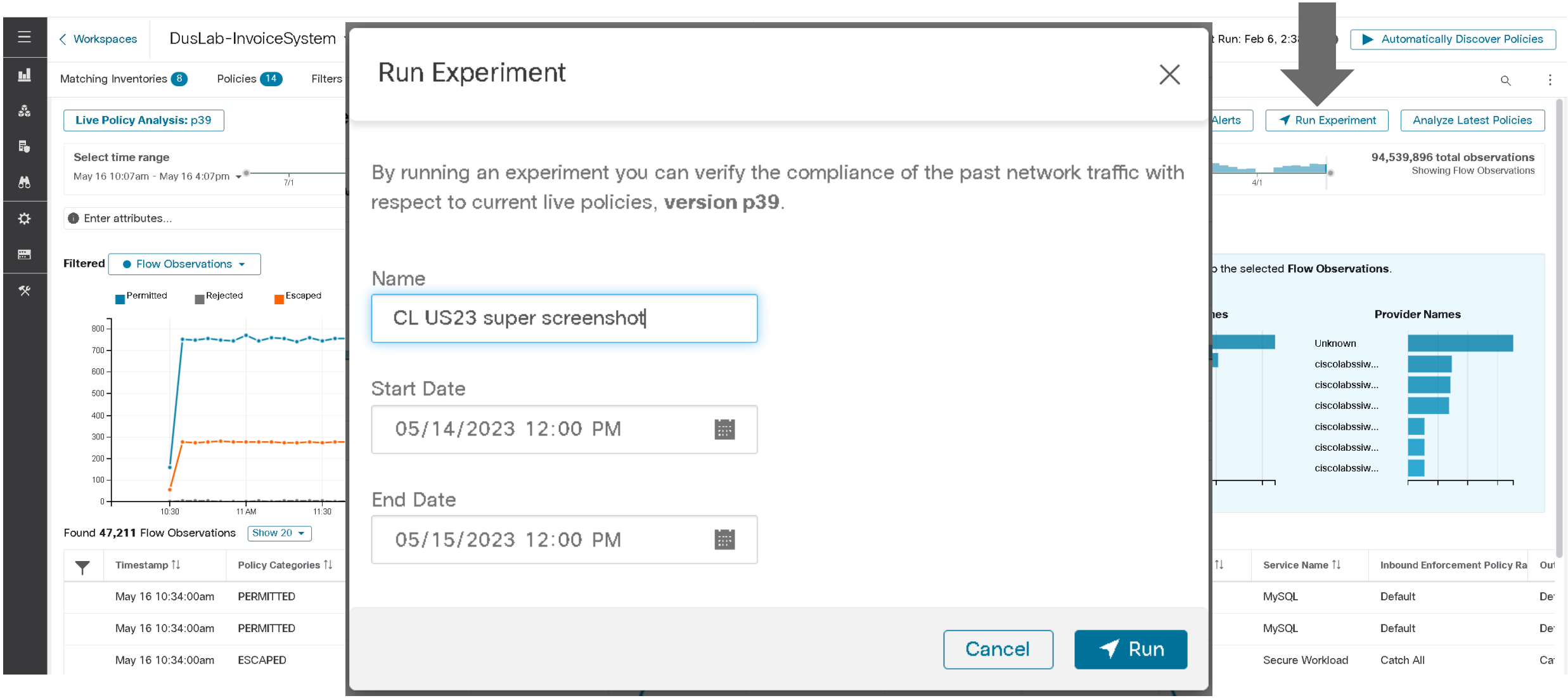
Policy ready to be enforced



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

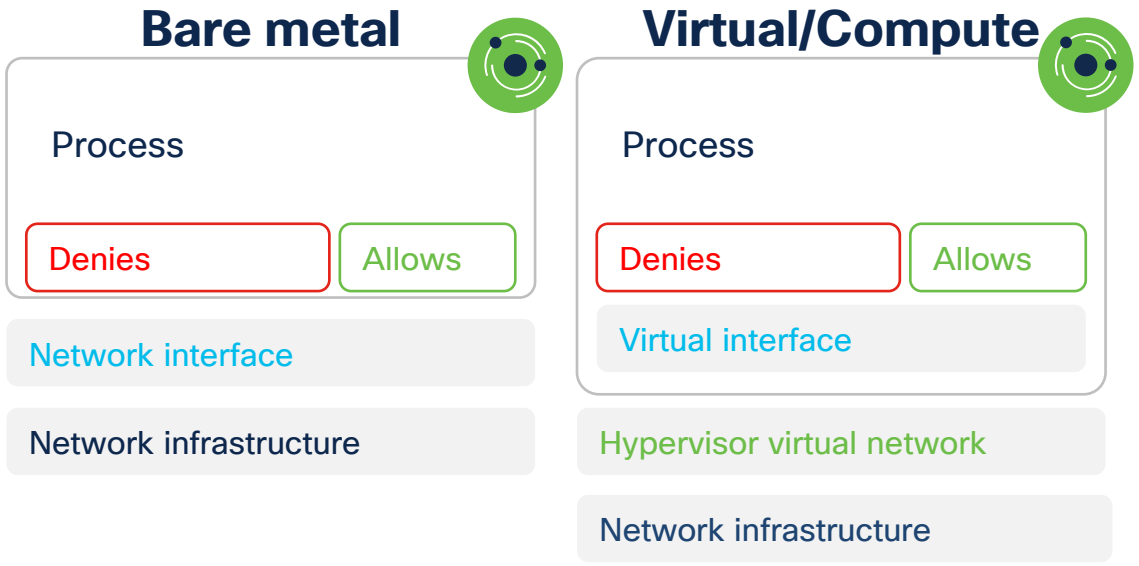
© 2025 Cisco and/or its affiliates. All rights reserved.

Run Policy Experiment



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

How does CSW enforce the Policy ?



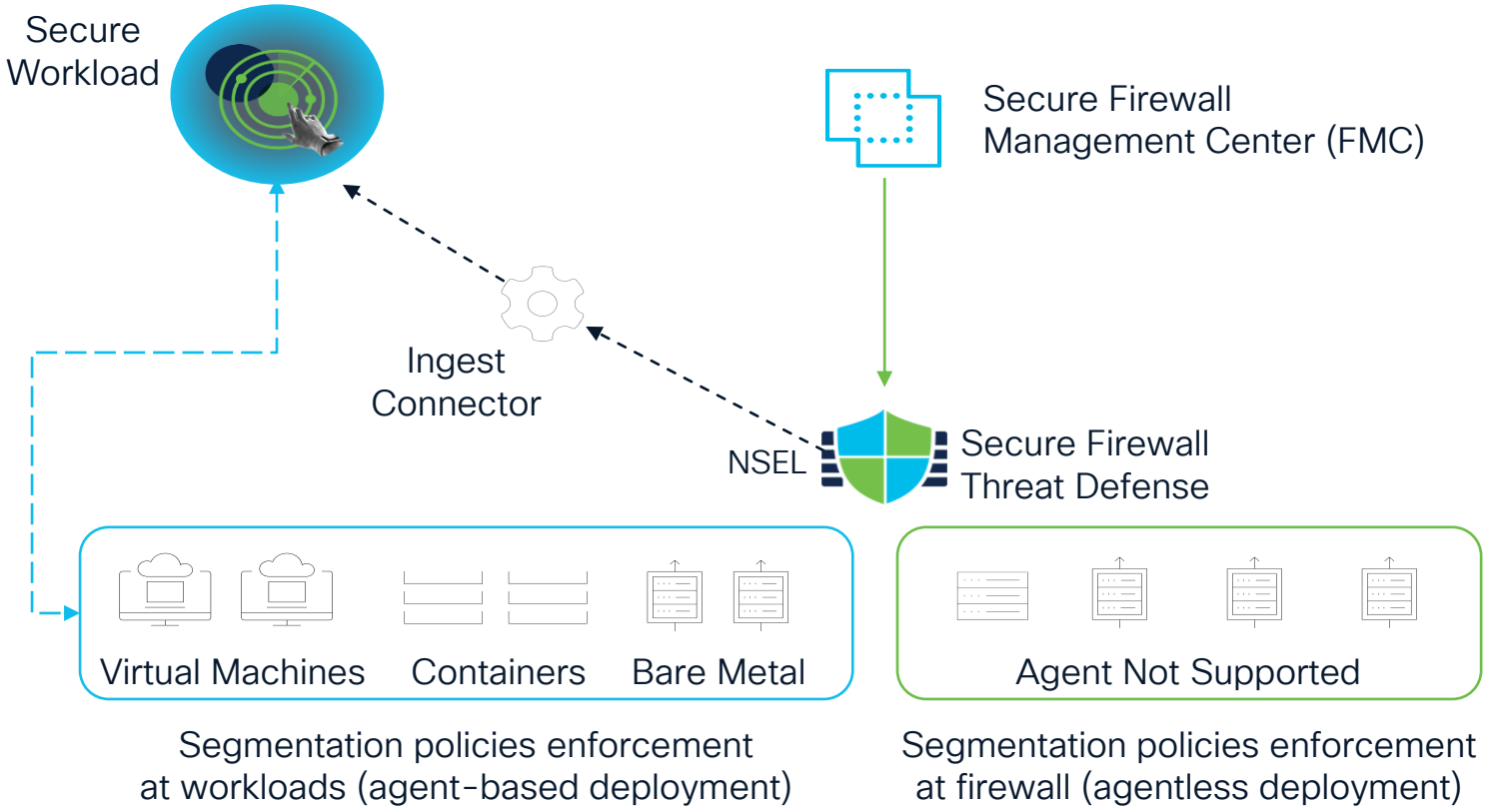
Intent is rendered as security rules in native environment

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

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

CSW-FMC Integration And Enforcement

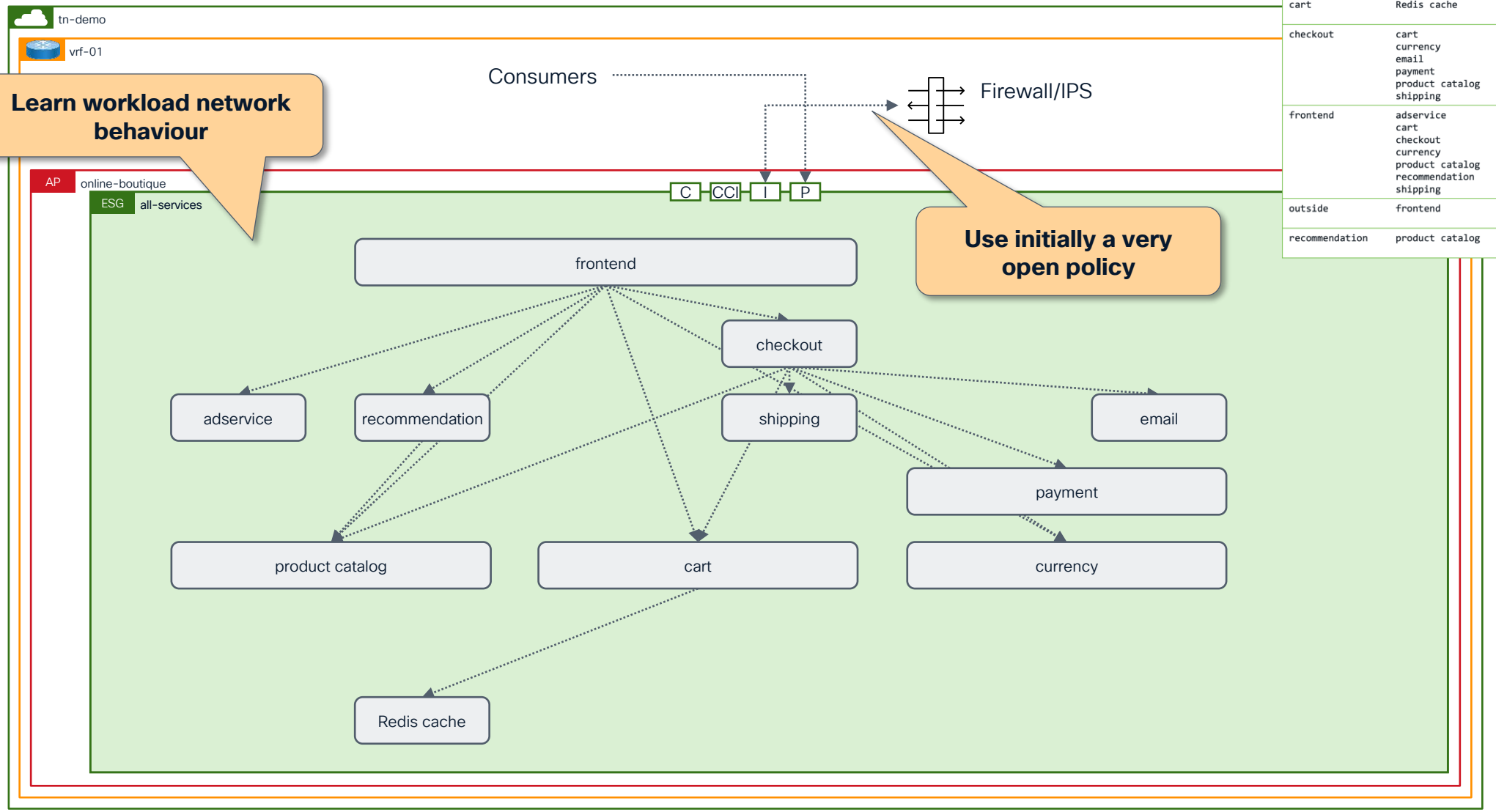
Defense-in-depth Use Case



- Defense in depth
- Support access control policy and dynamic object
- Improved rule ordering
- FMC domain awareness
- Topology aware policy enforcement
- Support deployment across multicloud

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

Use FTD to generate Netflow data for CSW

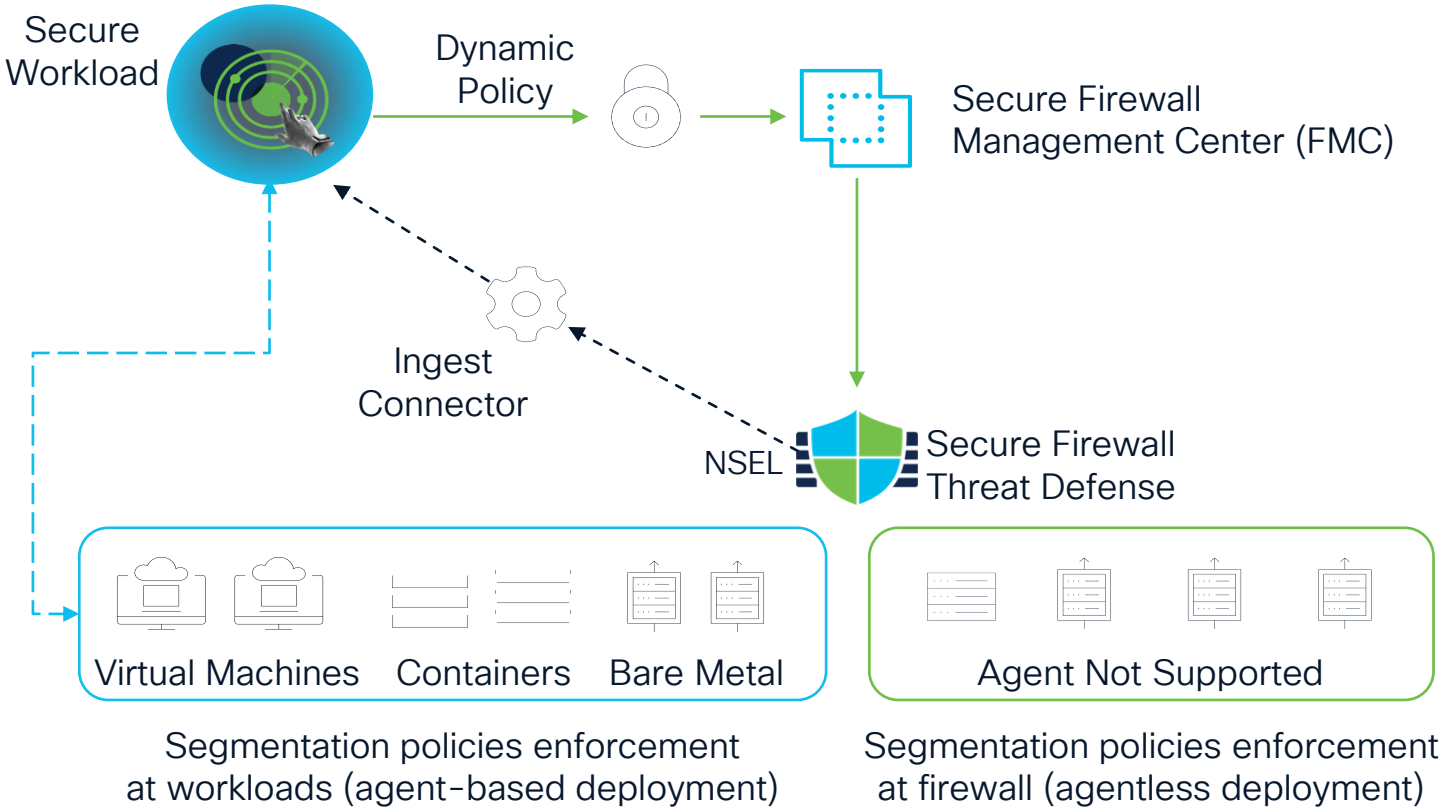


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

CSW-FMC Integration And Enforcement

Defense-in-depth Use Case

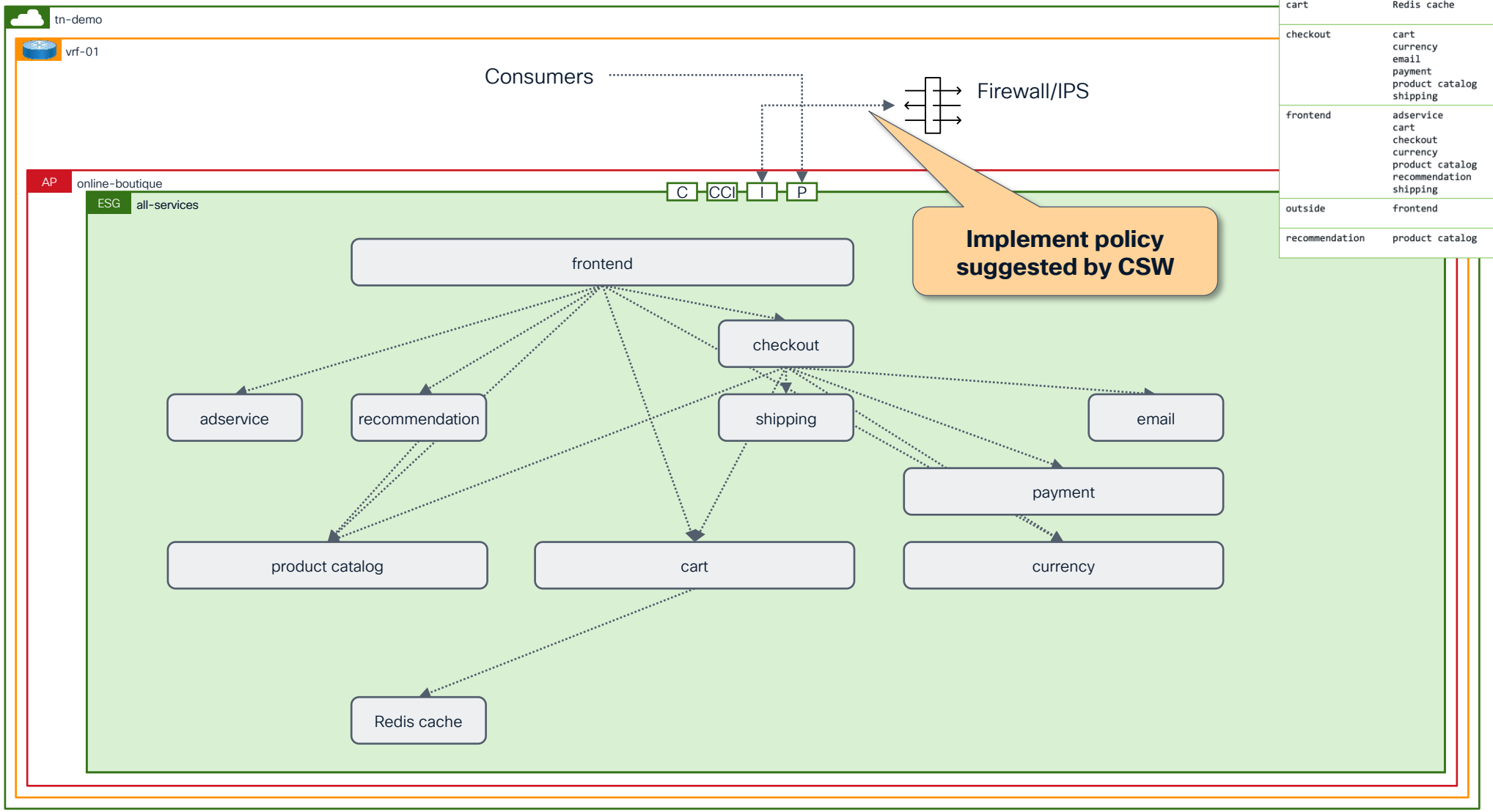


- Defense in depth
- Support access control policy and dynamic object
- Improved rule ordering
- FMC domain awareness
- Topology aware policy enforcement
- Support deployment across multicloud

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

cisco

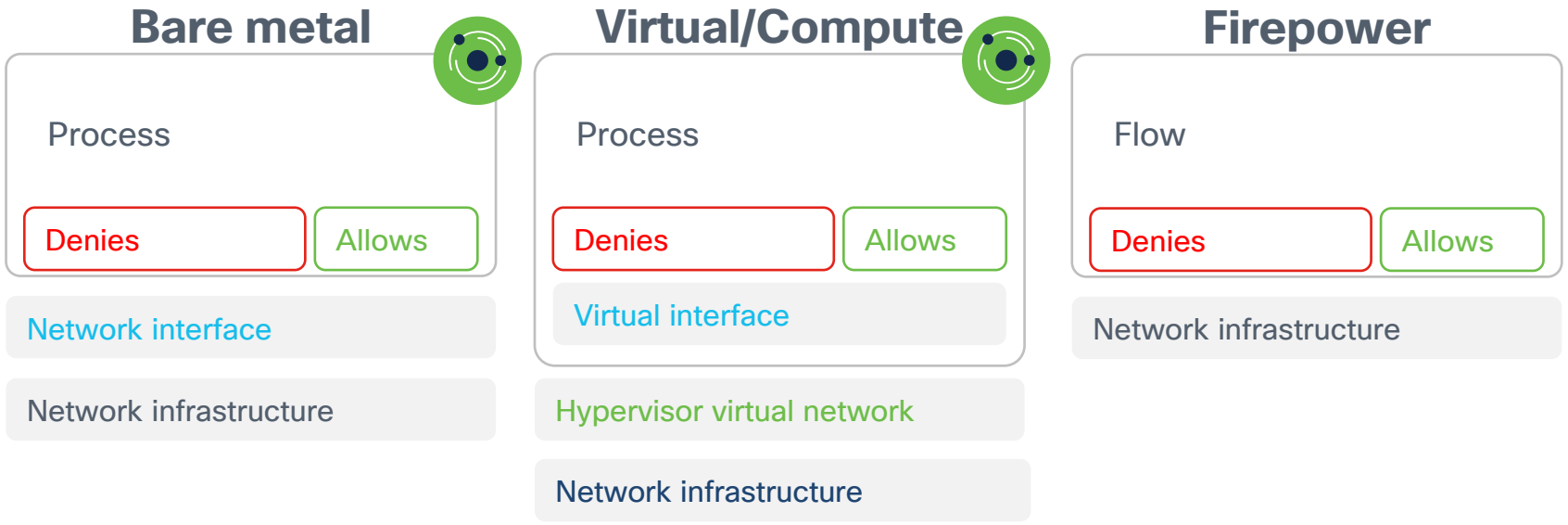
Enforce automatically Policy from CSW



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
	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

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

How does CSW enforce the Policy ?



Intent is rendered as security rules in native environment

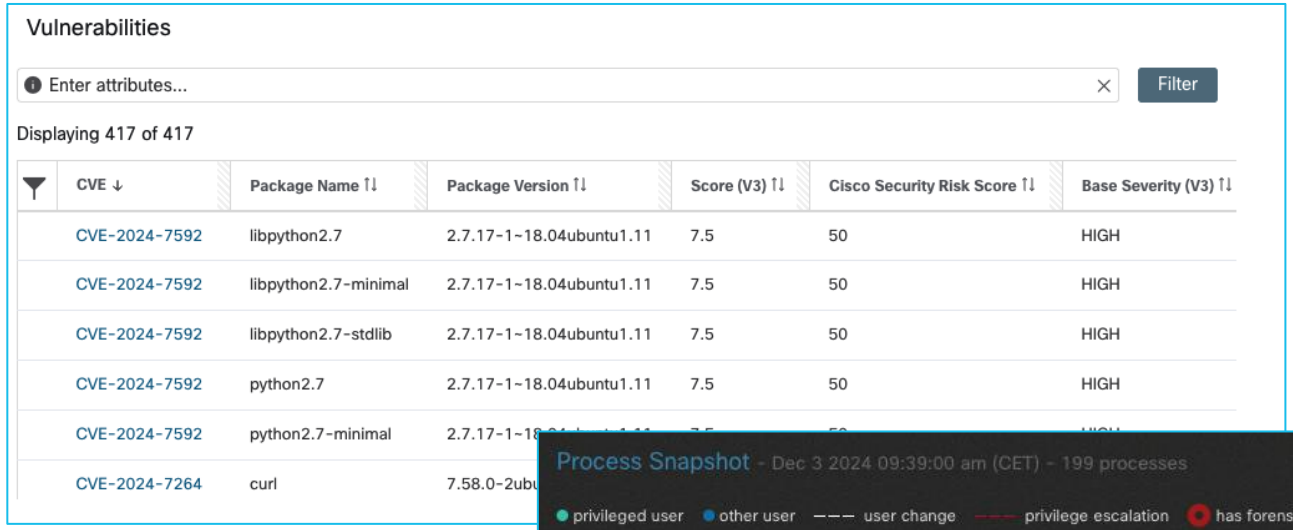
- IP sets on Linux servers
- Windows Advanced Firewall or Windows Filtering Platform on Windows servers
- Access Policies in Firepower Threat Defense

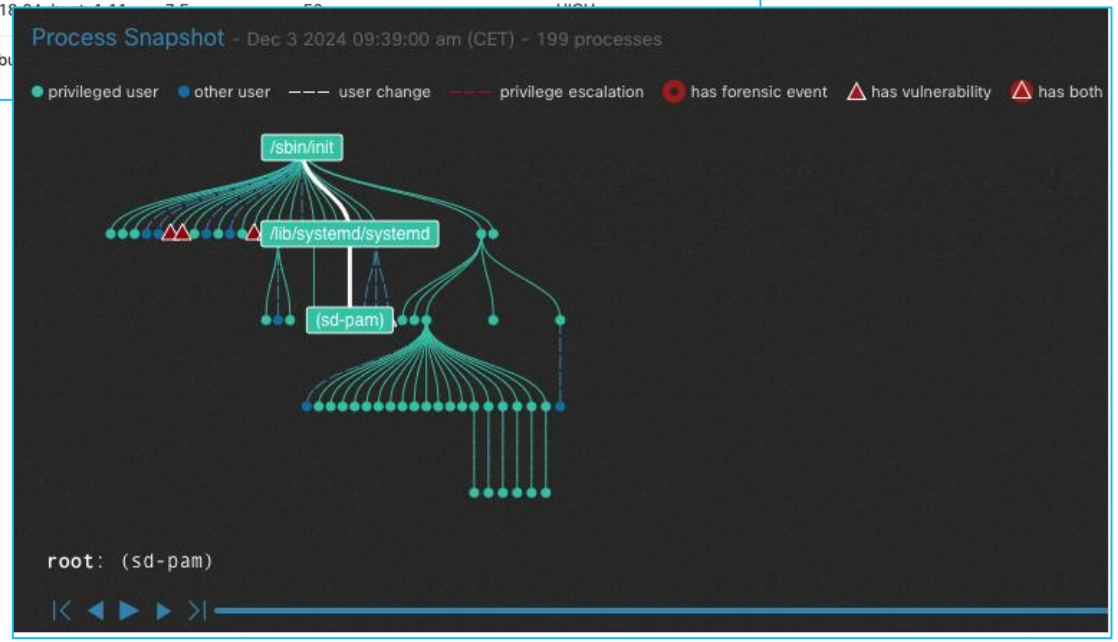
© 2025 Cisco and/or its affiliates. All rights reserved.

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

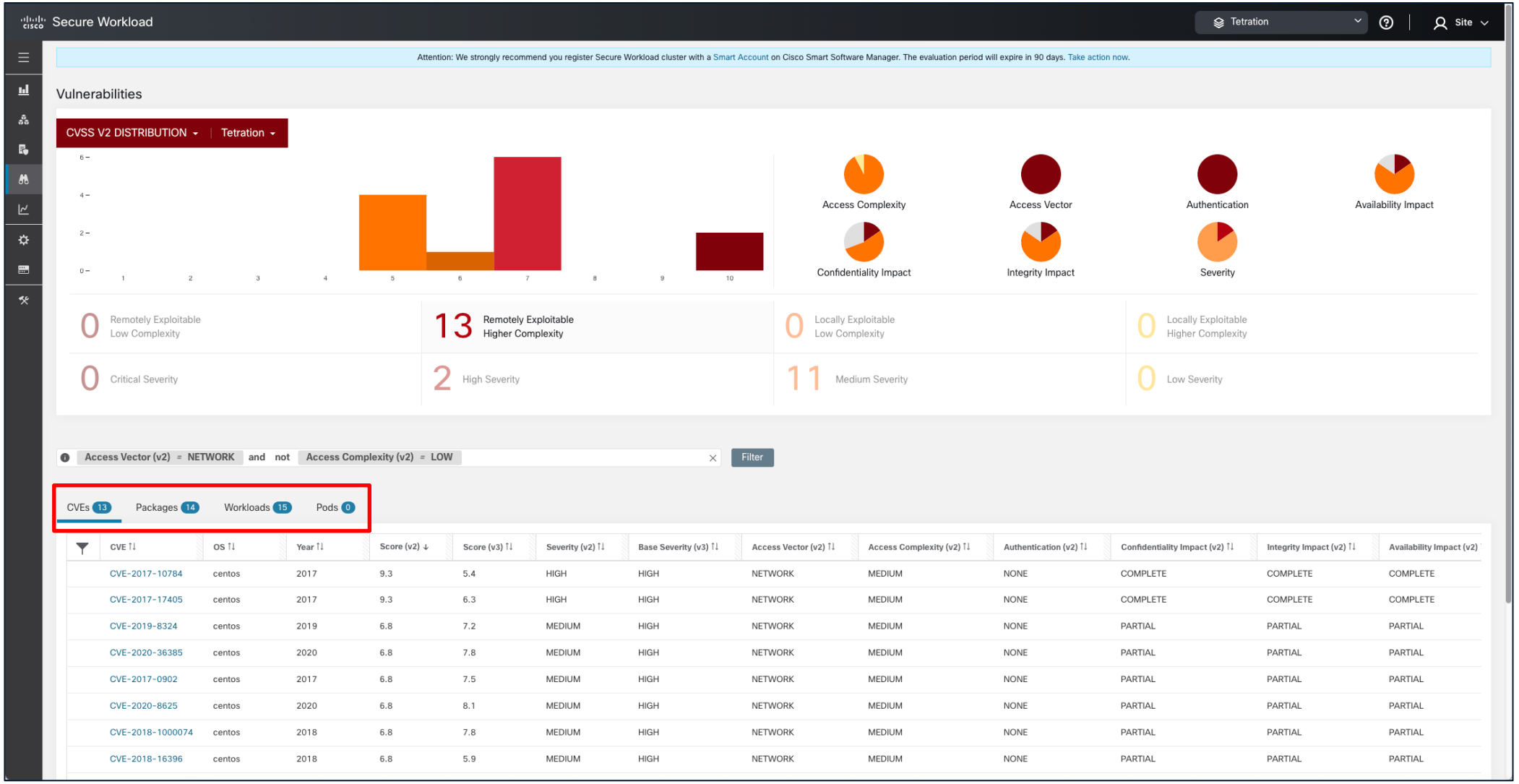




© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

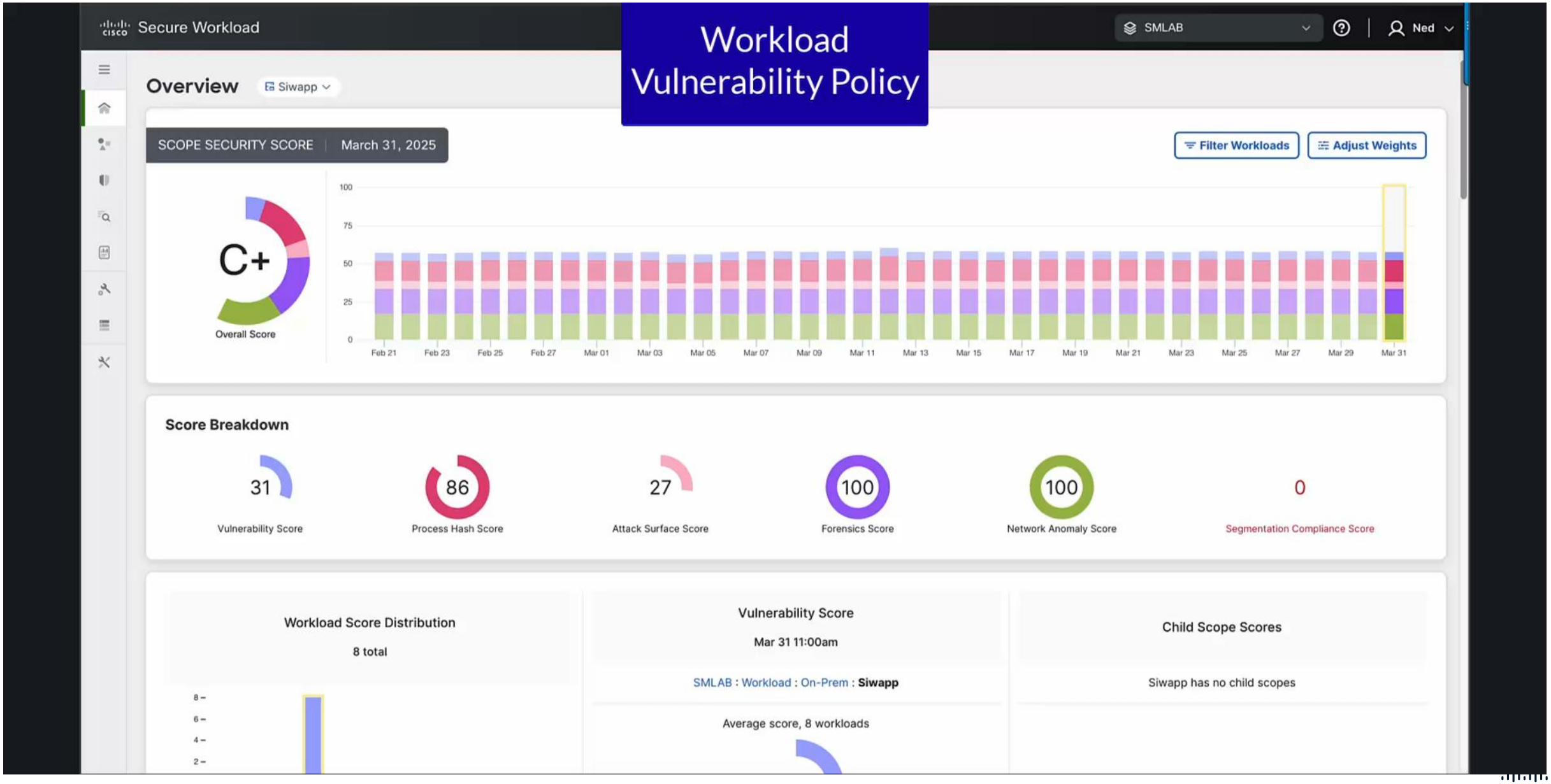
Cisco Secure Workload



CVE	OS	Year	Score (v2)	Score (v3)	Severity (v2)	Base Severity (v3)	Access Vector (v2)	Access Complexity (v2)	Authentication (v2)	Confidentiality Impact (v2)	Integrity Impact (v2)	Availability Impact (v2)
CVE-2017-10784	centos	2017	9.3	5.4	HIGH	HIGH	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE
CVE-2017-17405	centos	2017	9.3	6.3	HIGH	HIGH	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE
CVE-2019-8324	centos	2019	6.8	7.2	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2020-36385	centos	2020	6.8	7.8	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2017-0902	centos	2017	6.8	7.5	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2020-8625	centos	2020	6.8	8.1	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2018-1000074	centos	2018	6.8	7.8	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2018-16396	centos	2018	6.8	5.9	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL

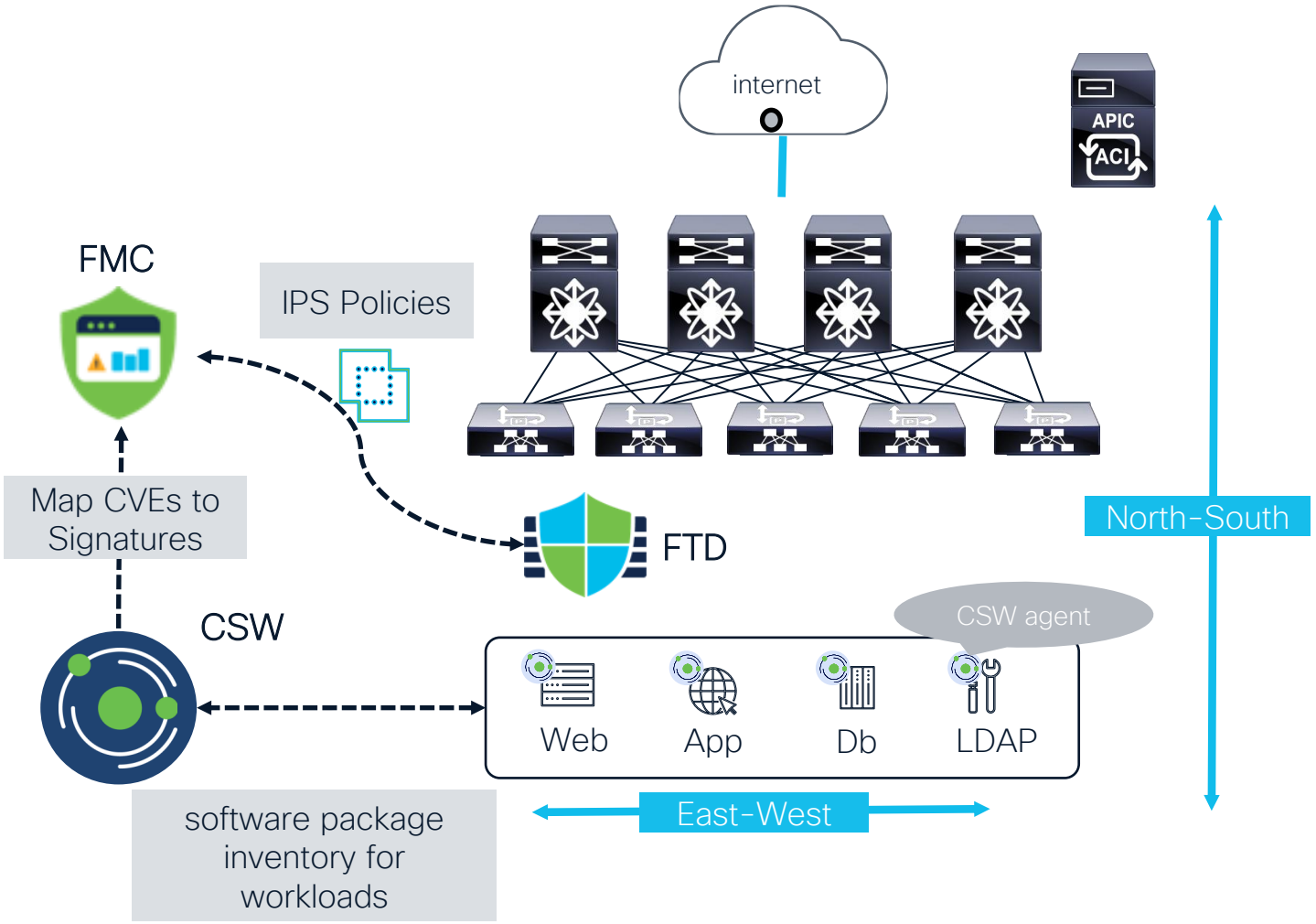
© 2025 Cisco and/or its affiliates. All rights reserved.

Differentiator: Prioritized Vulnerability Policy



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

Virtual patching – Cisco Secure Firewall



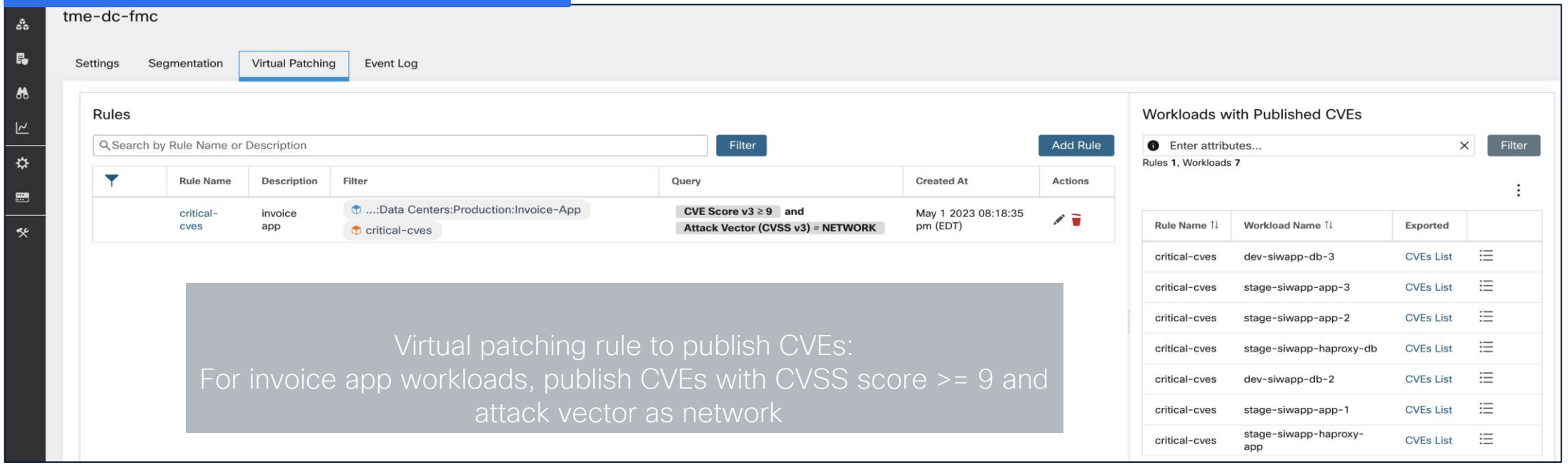
- Secure Workload agents collects CVE data from workloads
- Publish specific CVE data to Firewall Management Center
- Use Firewall recommendations to generate precise IPS policy
- Apply precise IPS policy to protect against CVE exploits

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

cisco

Virtual patching – Cisco Secure Firewall

CSW: Manage > Connector > FMC > Virtual Patching



FMC: Analysis > Hosts > Third party vulnerabilities

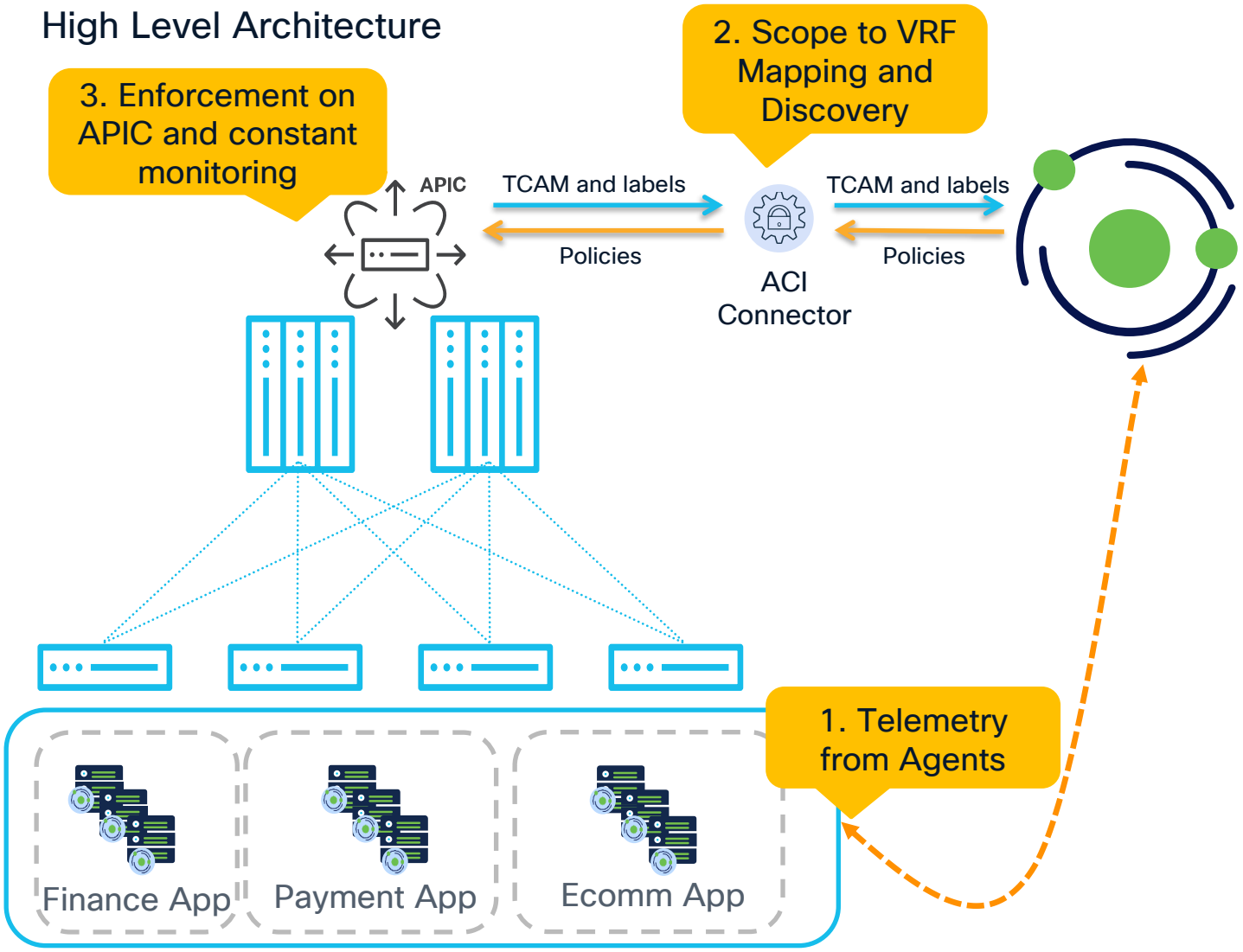
Vulnerability Source	Vulnerability ID	IP Address	Port	Bugtraq ID	CVE ID	SVID	Snort ID	Title	Description
CSW|d5341dbb-4b4f-31f8-5845-111fb6fbc537|1	2000042	192.168.18.7			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030004Z
CSW|d5341dbb-4b4f-31f8-5845-111fb6fbc537|1	2000073	192.168.18.6			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

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

ACI Integration

New 4.0

High Level Architecture



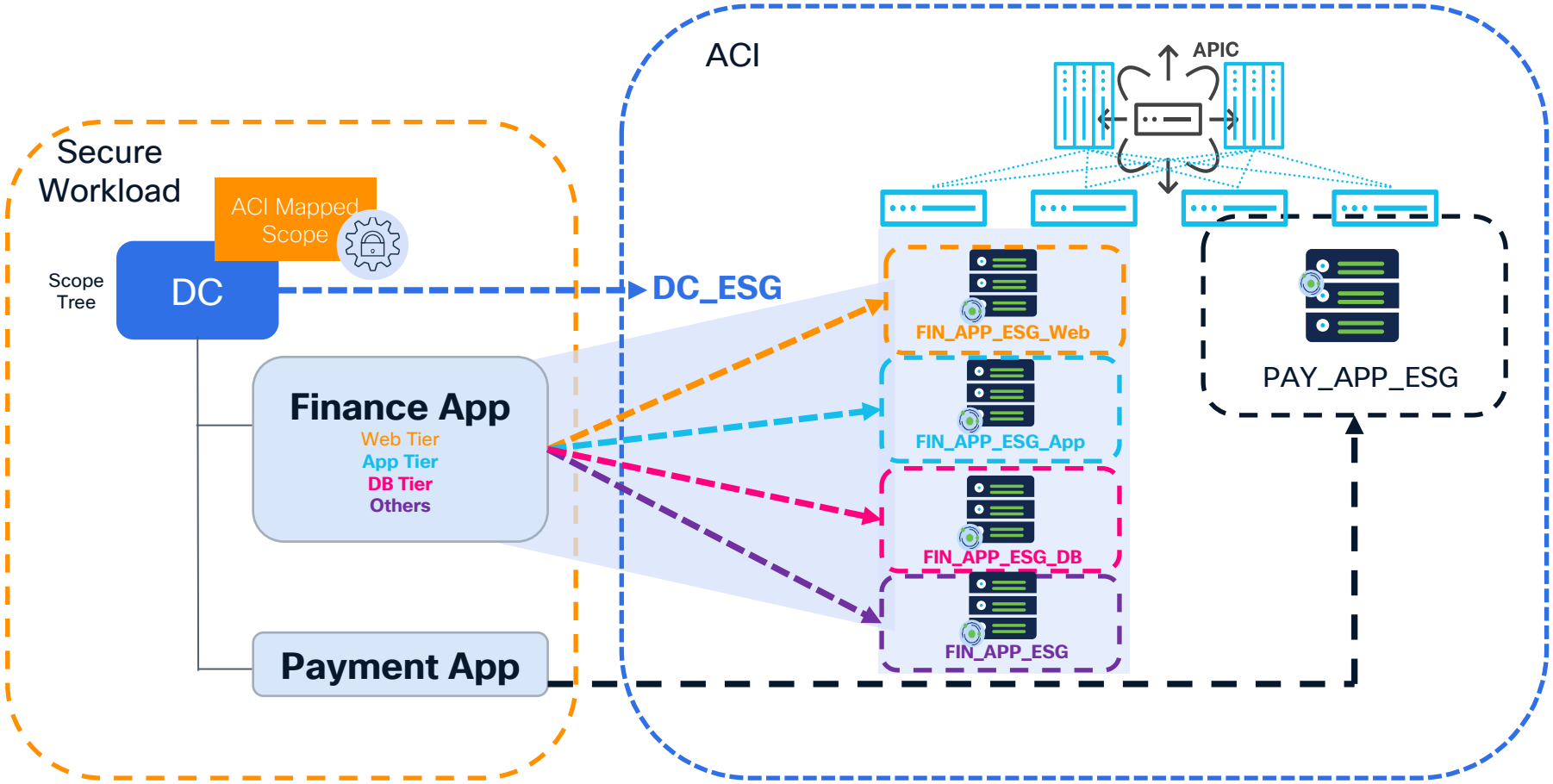
Integration Highlights

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

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

cisco

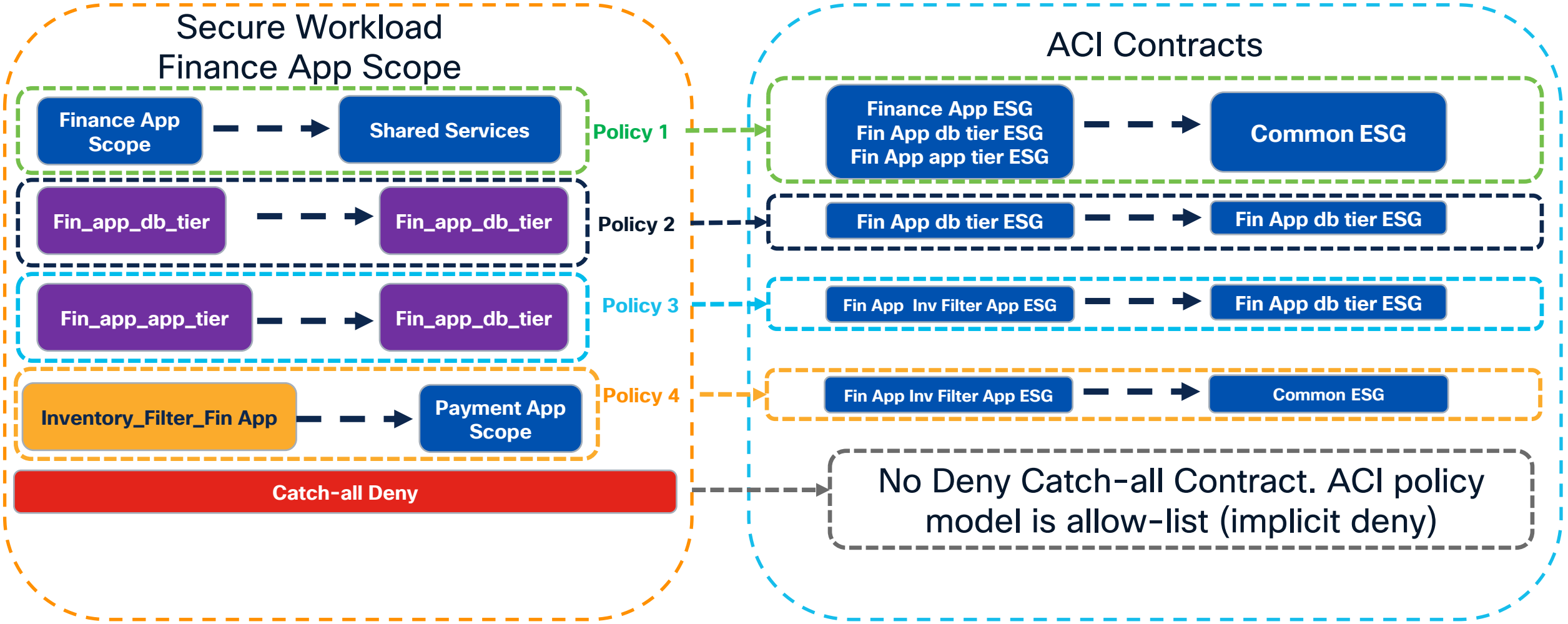
Secure Workload Objects and Policy Mapping



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

cisco

Secure Workload Policies to ACI Contracts



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

cisco

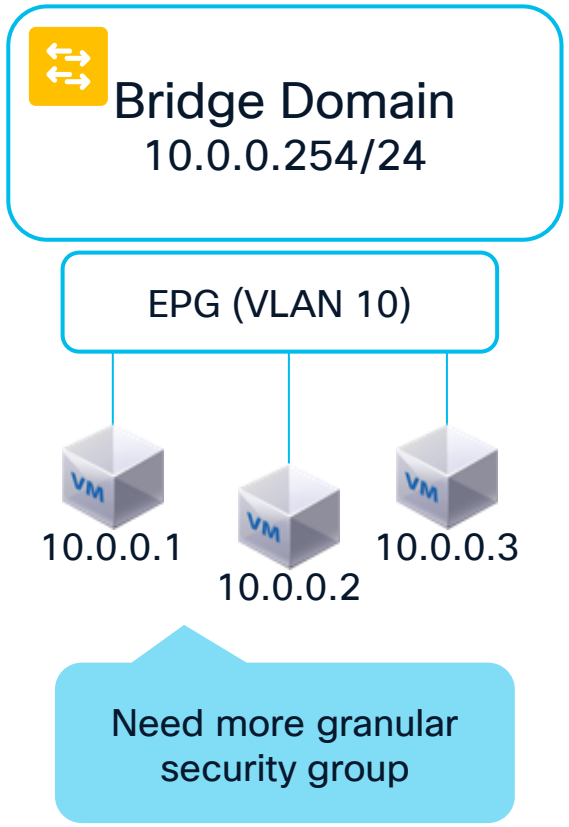
Network Centric & Application Centric Design

Network Centric

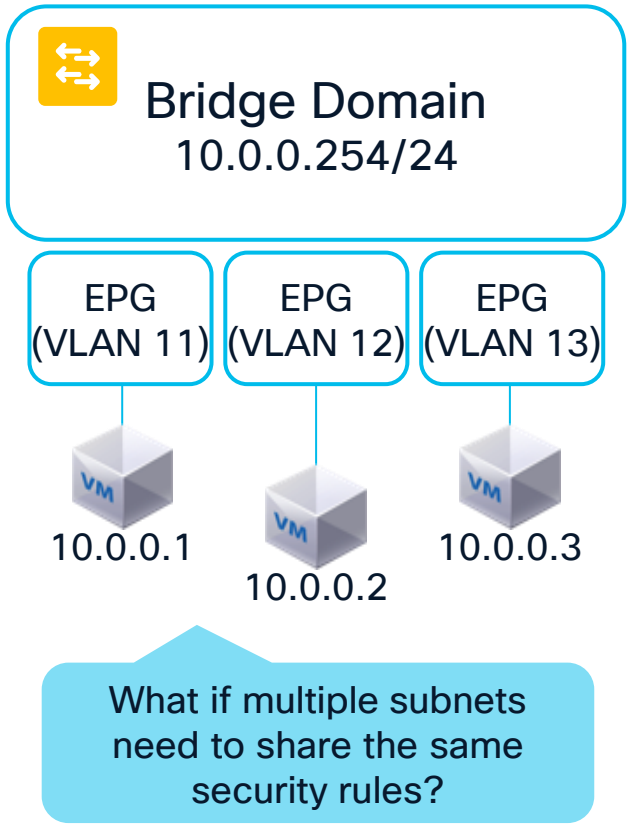
Application Centric

== 5.0 ==
Endpoint Security Group (ESG)

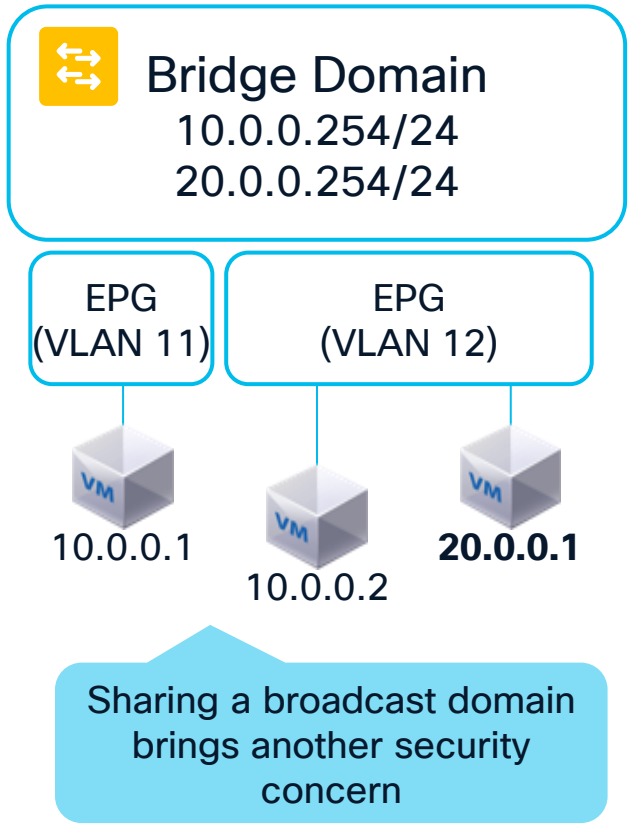
A security group in 1 subnet



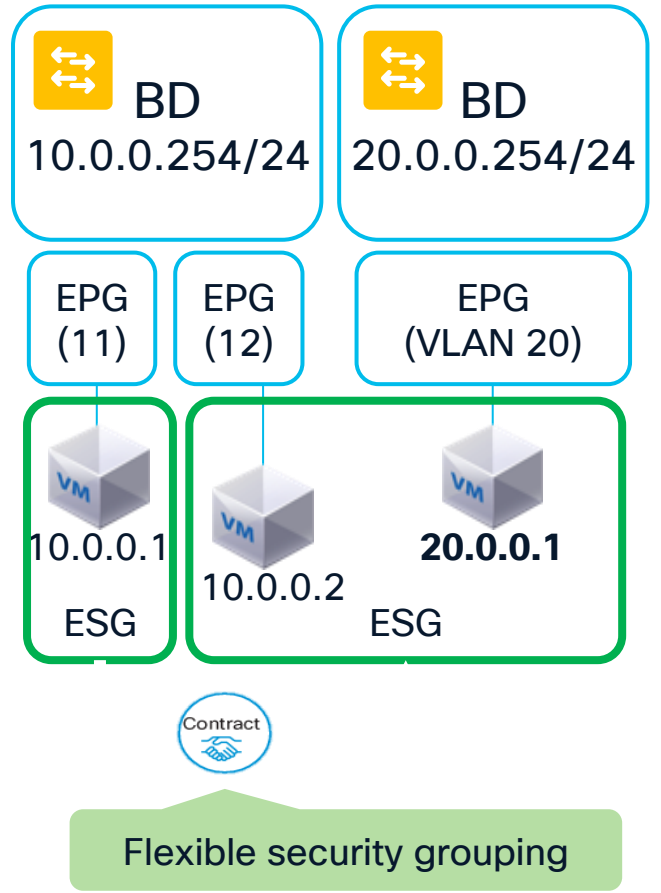
Multiple security groups in 1 subnet



Security groups across subnets



Security groups **across bridge domains**

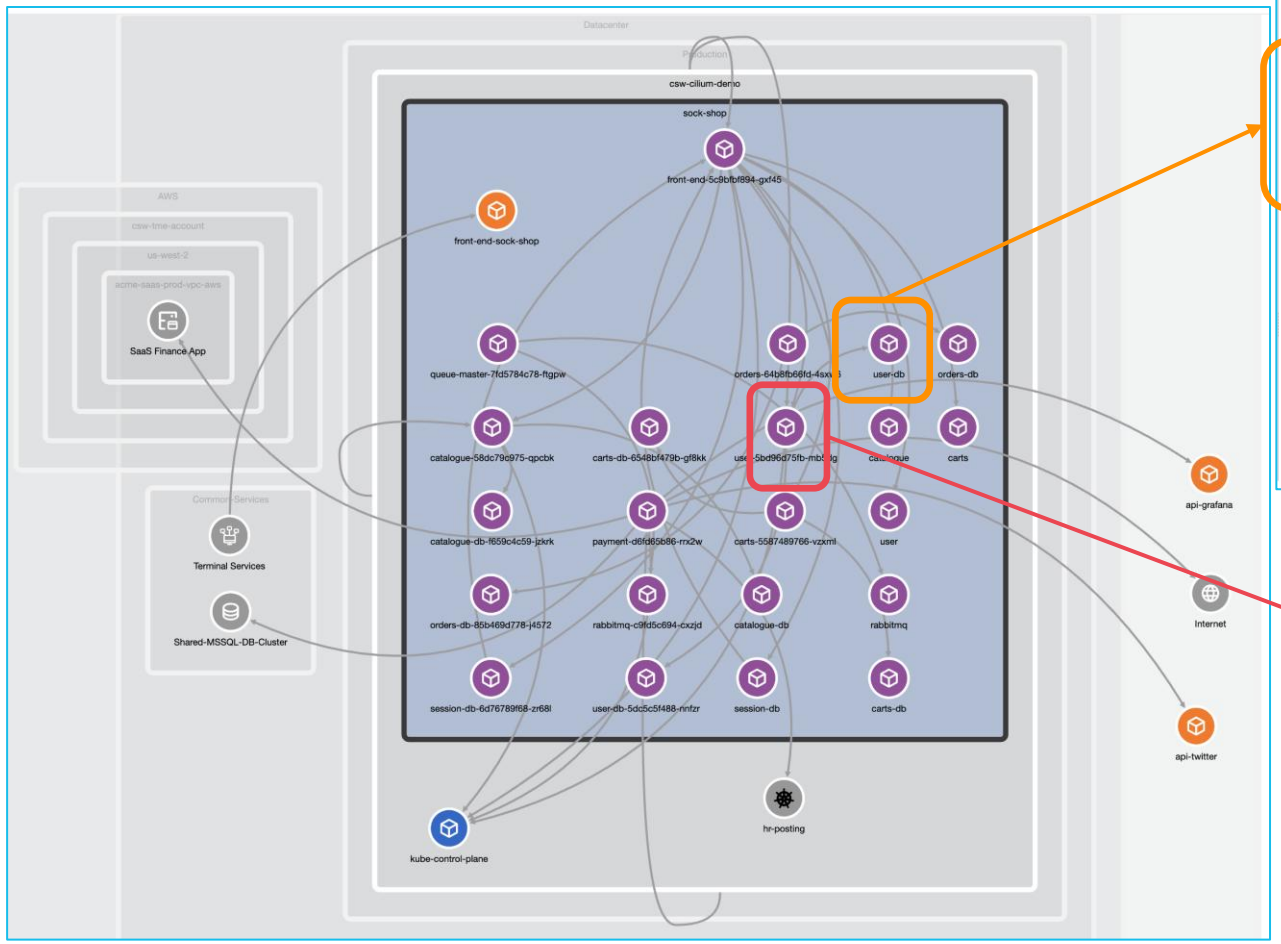


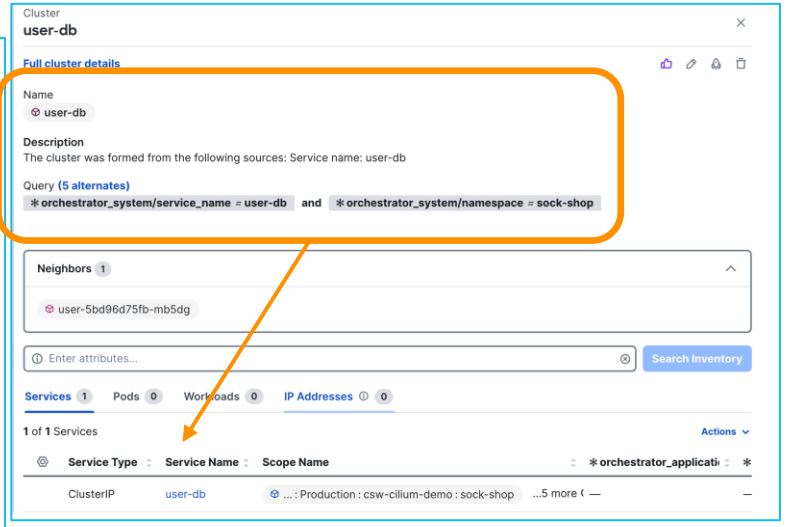
© 2025 Cisco and/or its affiliates. All rights reserved.

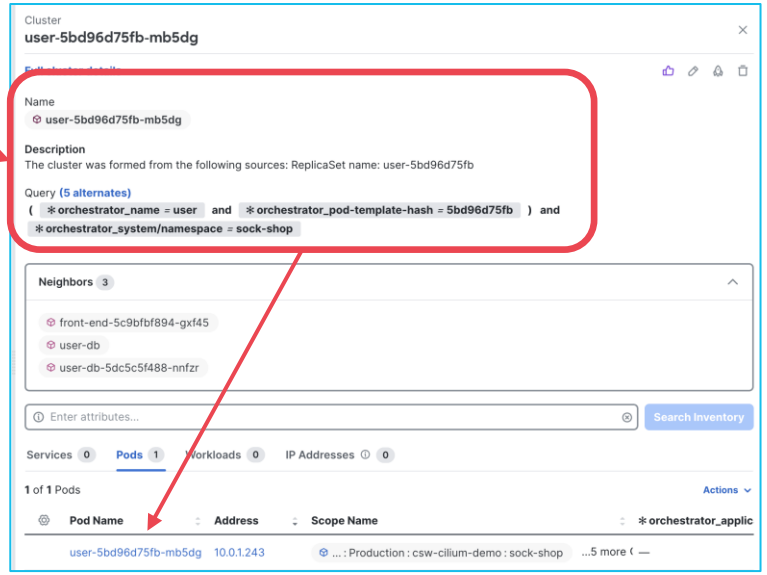
Bare Metal...virtual... What about Containers ???

Application Dependency Mapping

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



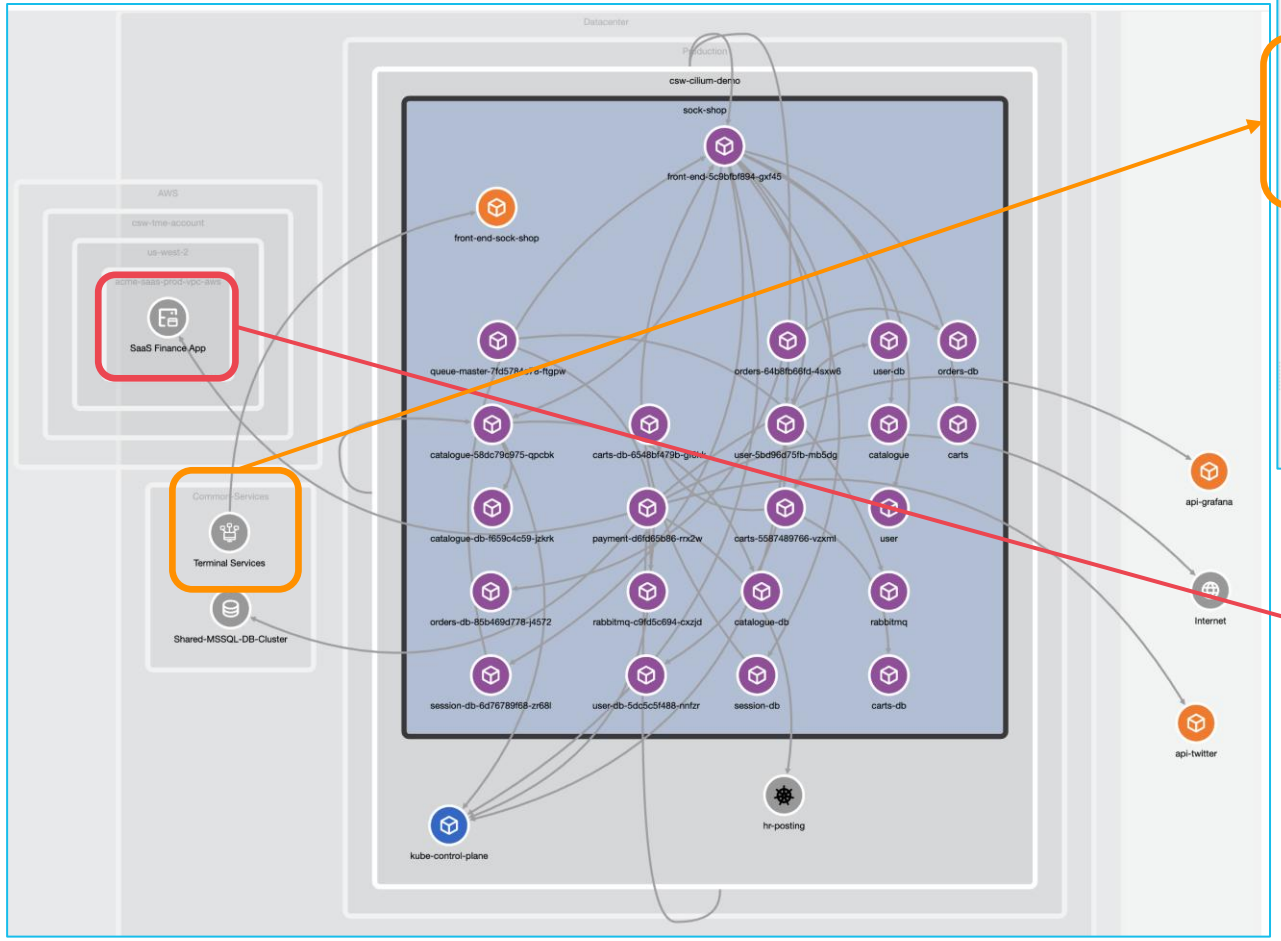


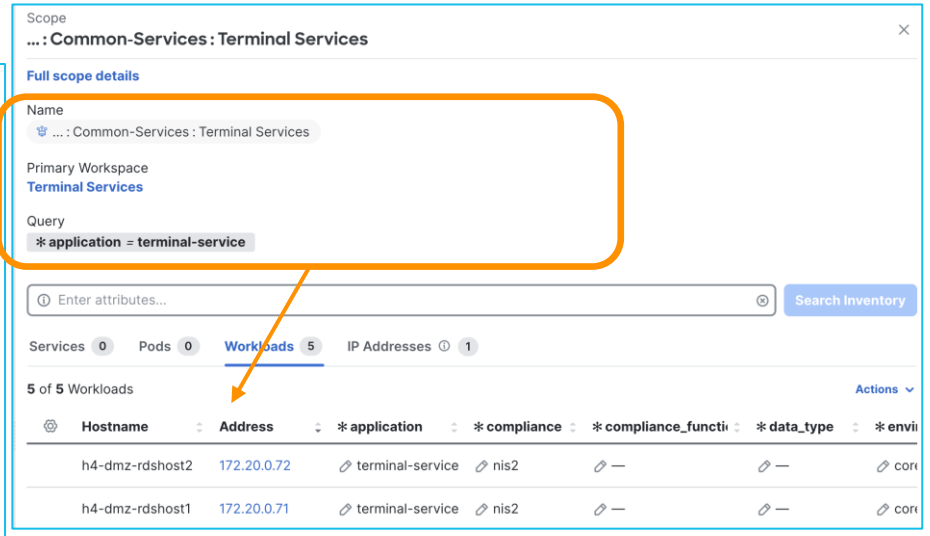


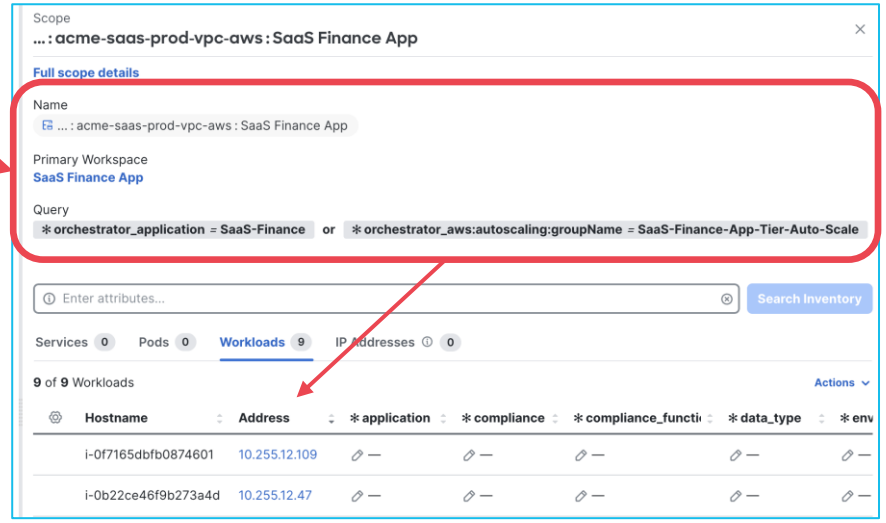
© 2025 Cisco and/or its affiliates. All rights reserved.

Application Dependency Mapping

Kubernetes Policy Discovery – End-to-End Discovery





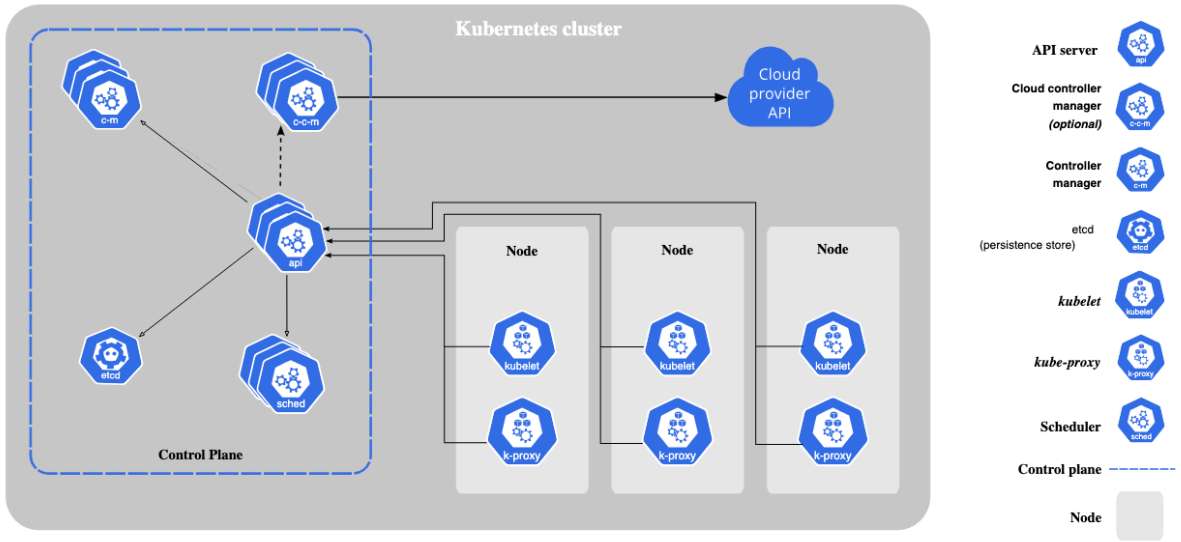


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Moving to cloud Native

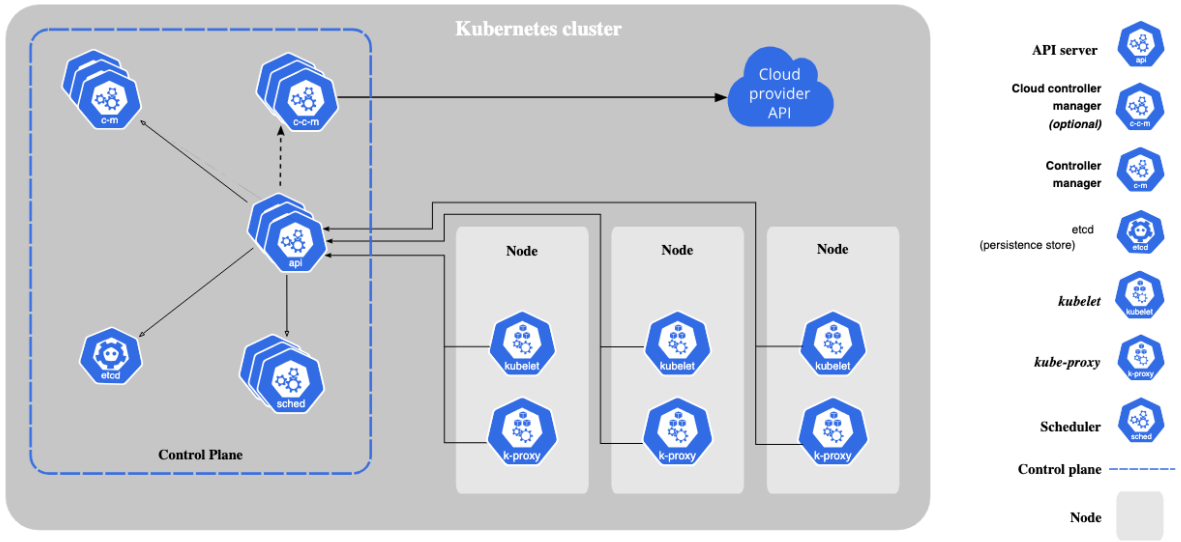
Why Do Customers Use Kubernetes?



- **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.

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

Why Do Customers Use Kubernetes?

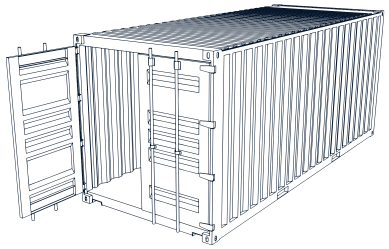


- **Scalability**
  Kubernetes allows applications to scale up or down automatically based on demand, ensuring optimal performance and cost efficiency for both small businesses and large enterprises.
- **High Availability & Reliability**
  Kubernetes provides automated failover, self-healing, and load 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.

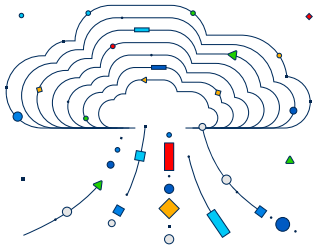
© 2025 Cisco and/or its affiliates. All rights reserved.

Kubernetes - The New Standard To Deploy Applications

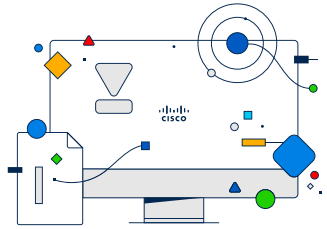
A Hybrid and Multi-Cloud Infrastructure Layer Supporting Both Modern & Legacy Workloads



Containers



AI / ML Workloads



Legacy VM Workloads

Kubernetes

Bare Metal

vmware by Broadcom

aws

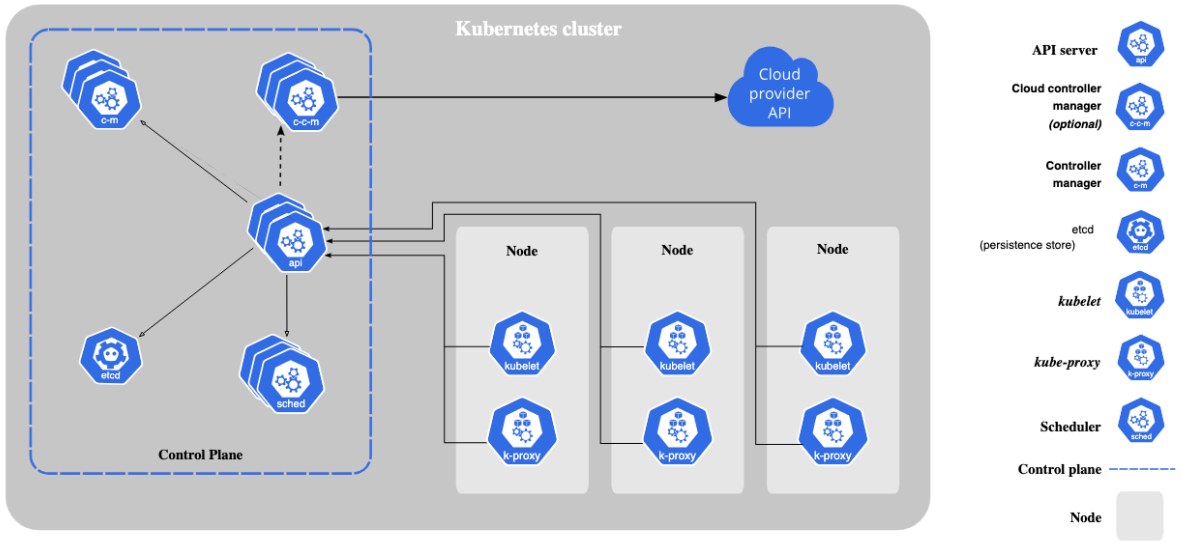
Azure

Google Cloud

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

cisco

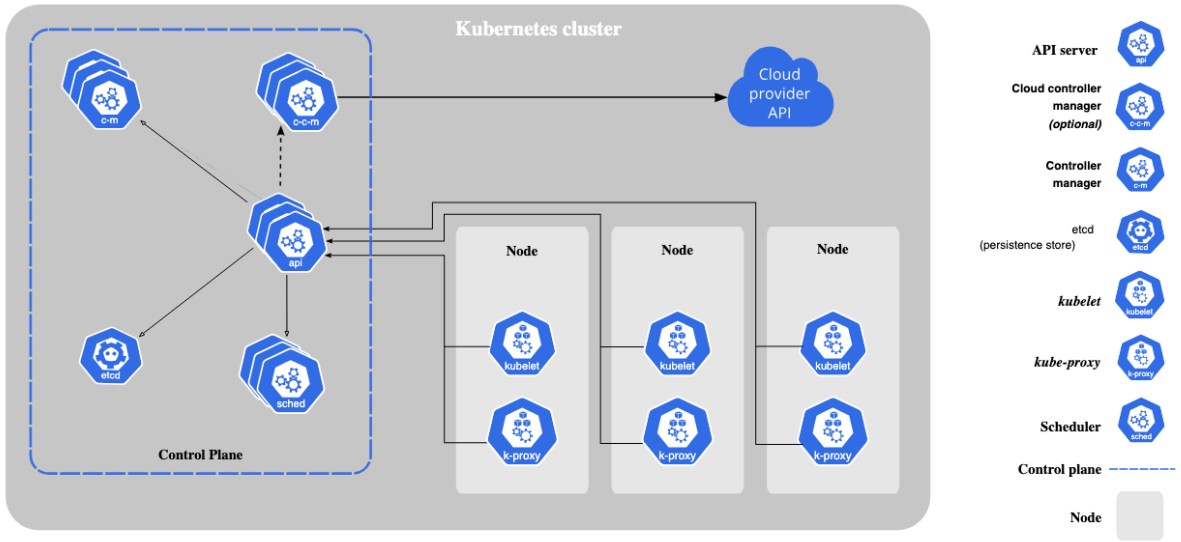
Why Do Customers Use Kubernetes?



- **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.

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

Why Do Customers Use Kubernetes?

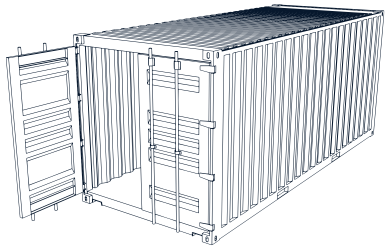


- **Scalability**
  Kubernetes allows applications to scale up or down automatically based on demand, ensuring optimal performance and cost efficiency for both small businesses and large enterprises.
- **High Availability & Reliability**
  Kubernetes provides automated failover, self-healing, and load 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.

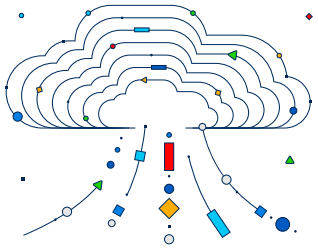
© 2025 Cisco and/or its affiliates. All rights reserved.

Kubernetes - The New Standard To Deploy Applications

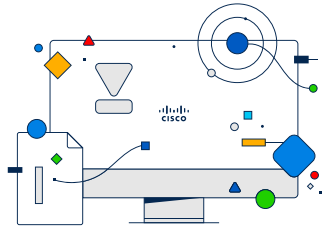
A Hybrid and Multi-Cloud Infrastructure Layer Supporting Both Modern & Legacy Workloads



Containers



AI / ML Workloads



Legacy VM Workloads

Kubernetes

Bare Metal

vmware by Broadcom

aws

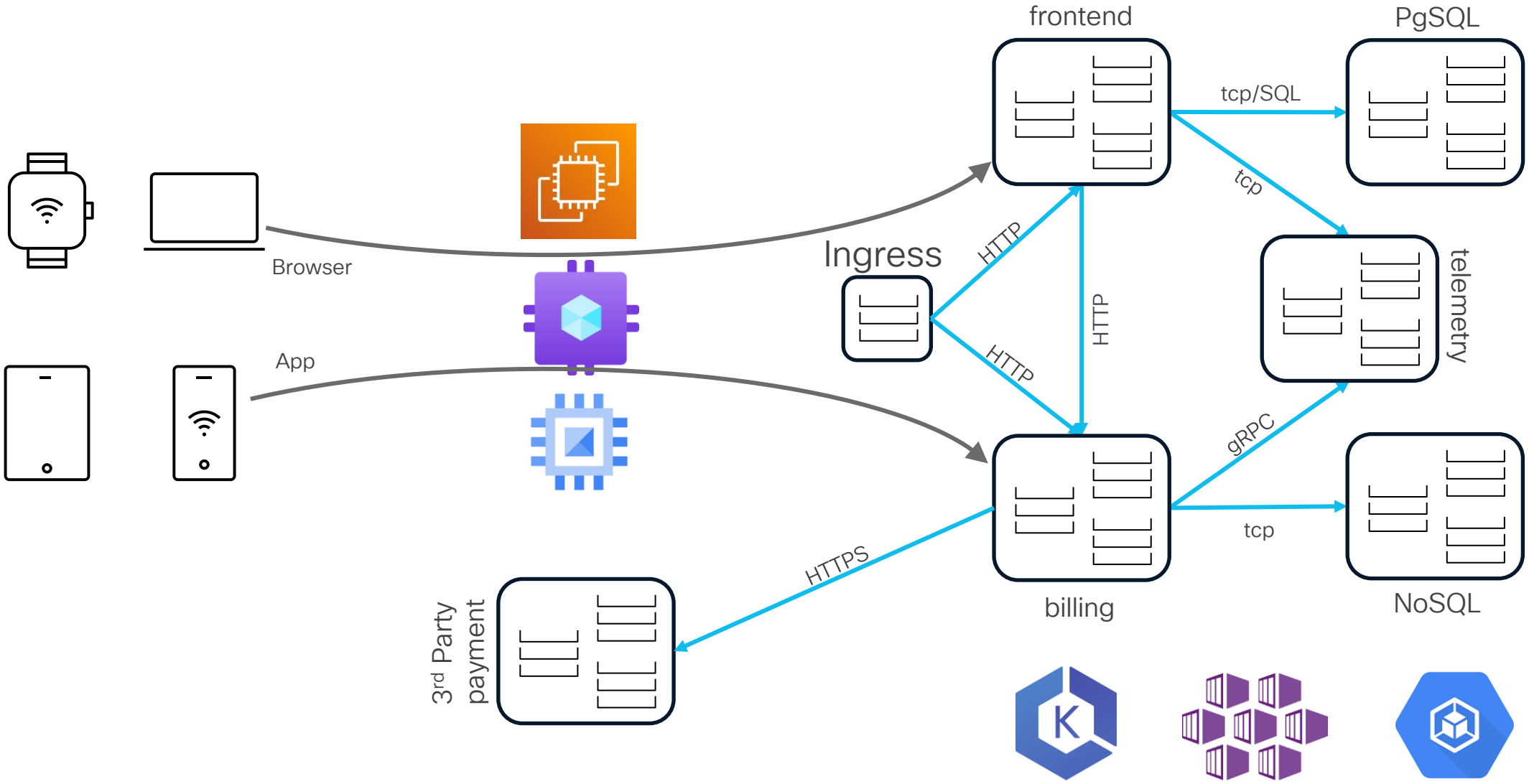
Azure

Google Cloud

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

cisco

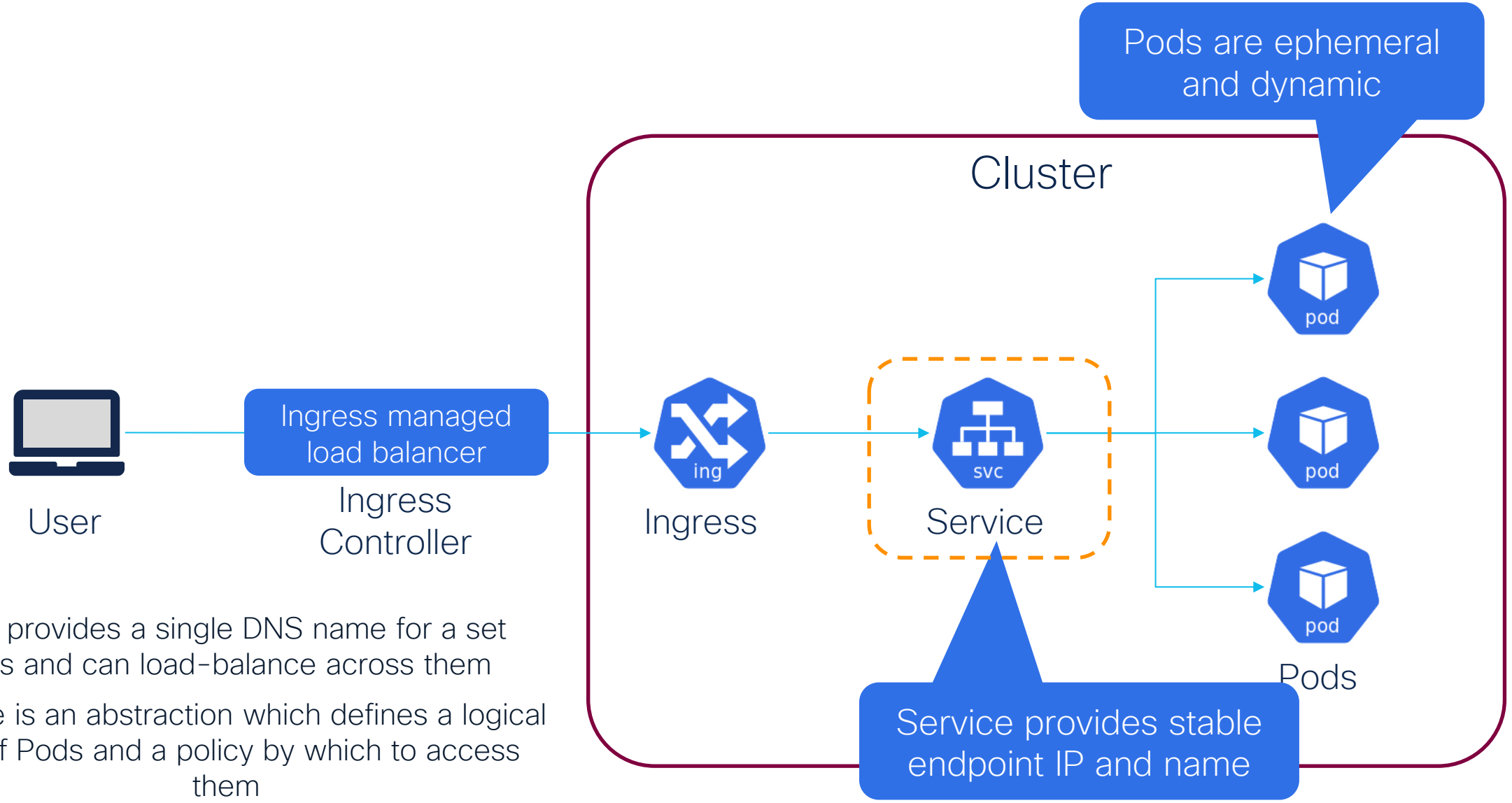
Ok but, where is my network ?



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

cisco

Key K8 Components – Services



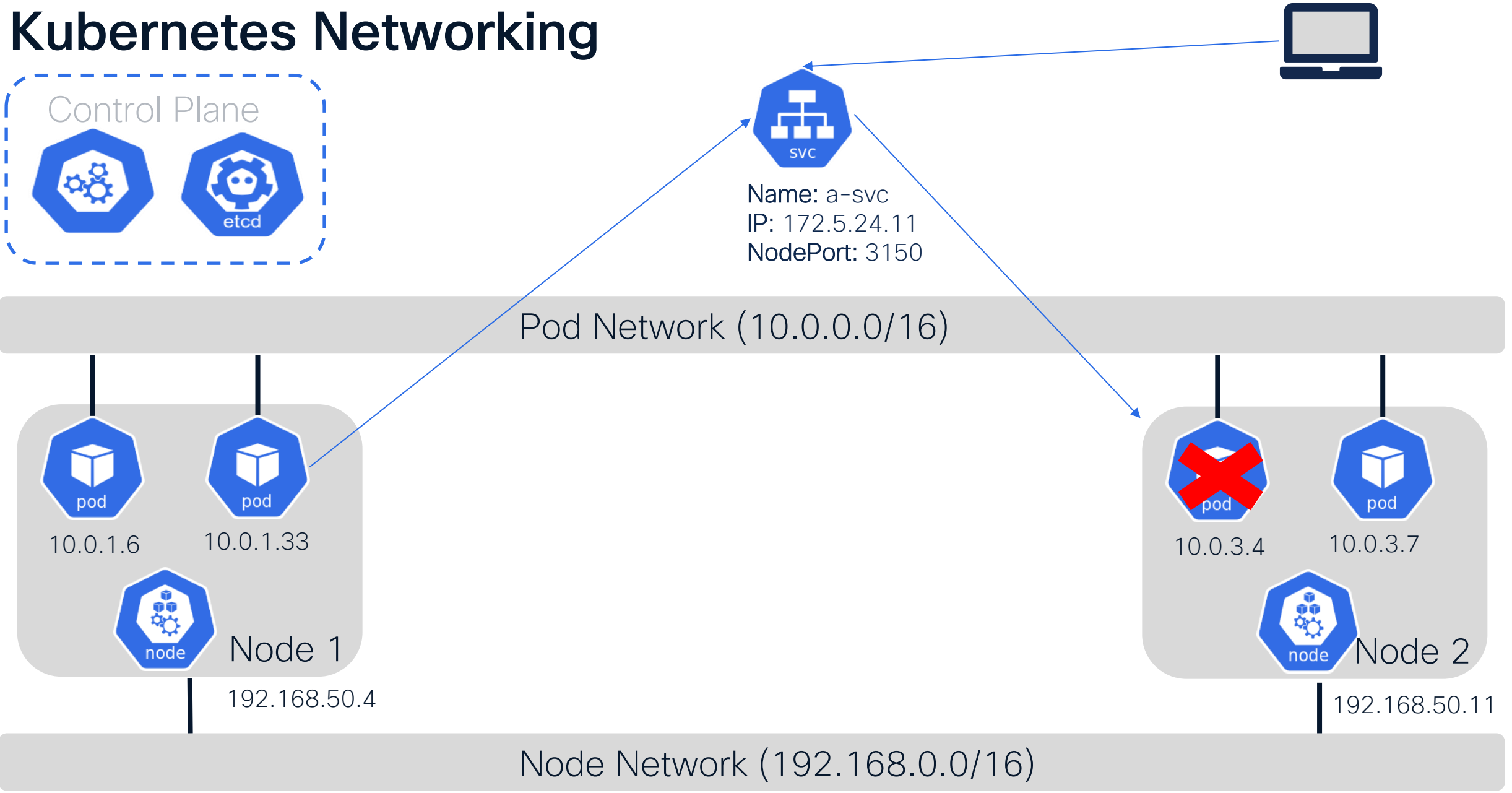
Service provides a single DNS name for a set of Pods and can load-balance across them

Service is an abstraction which defines a logical set of Pods and a policy by which to access them

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

cisco

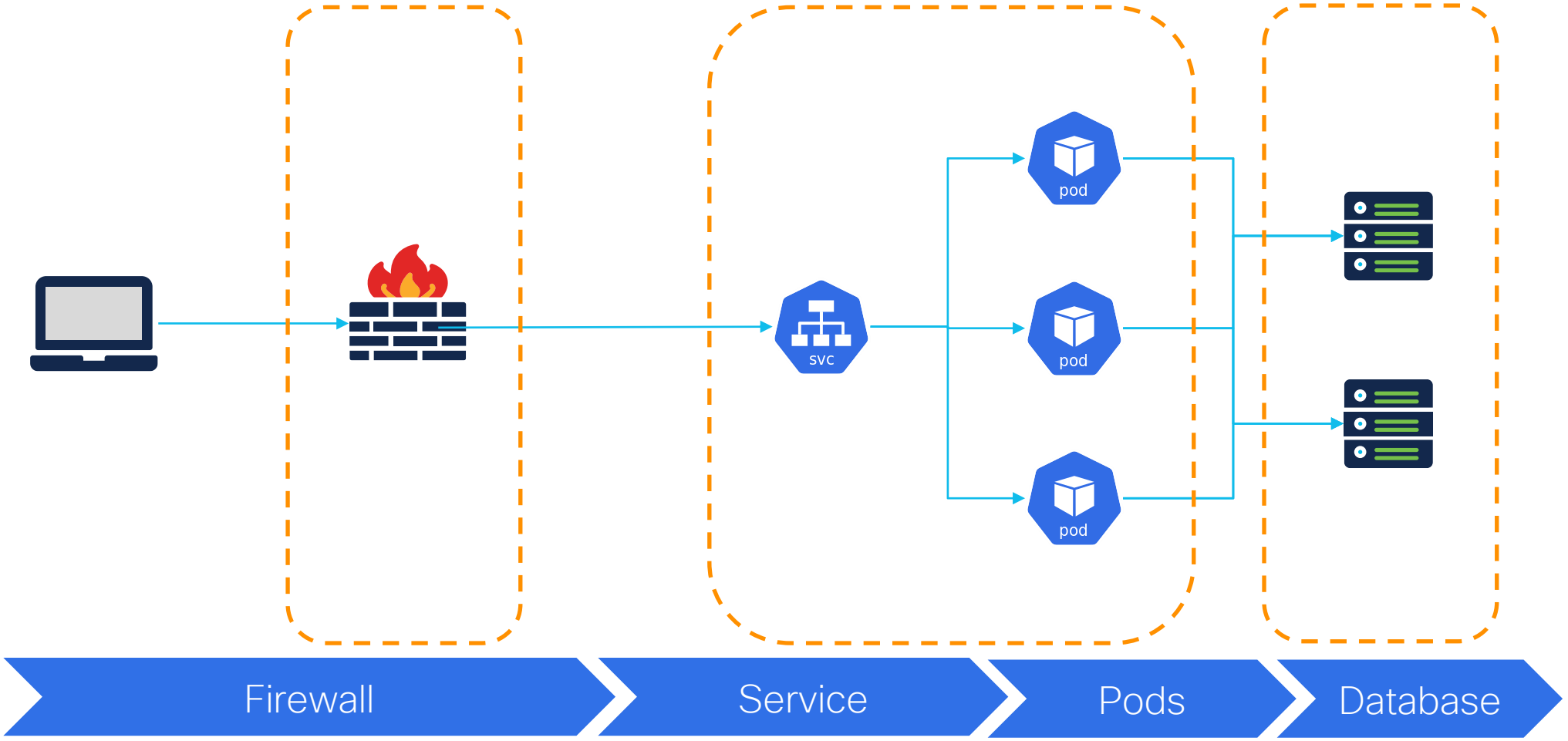
Kubernetes Networking



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

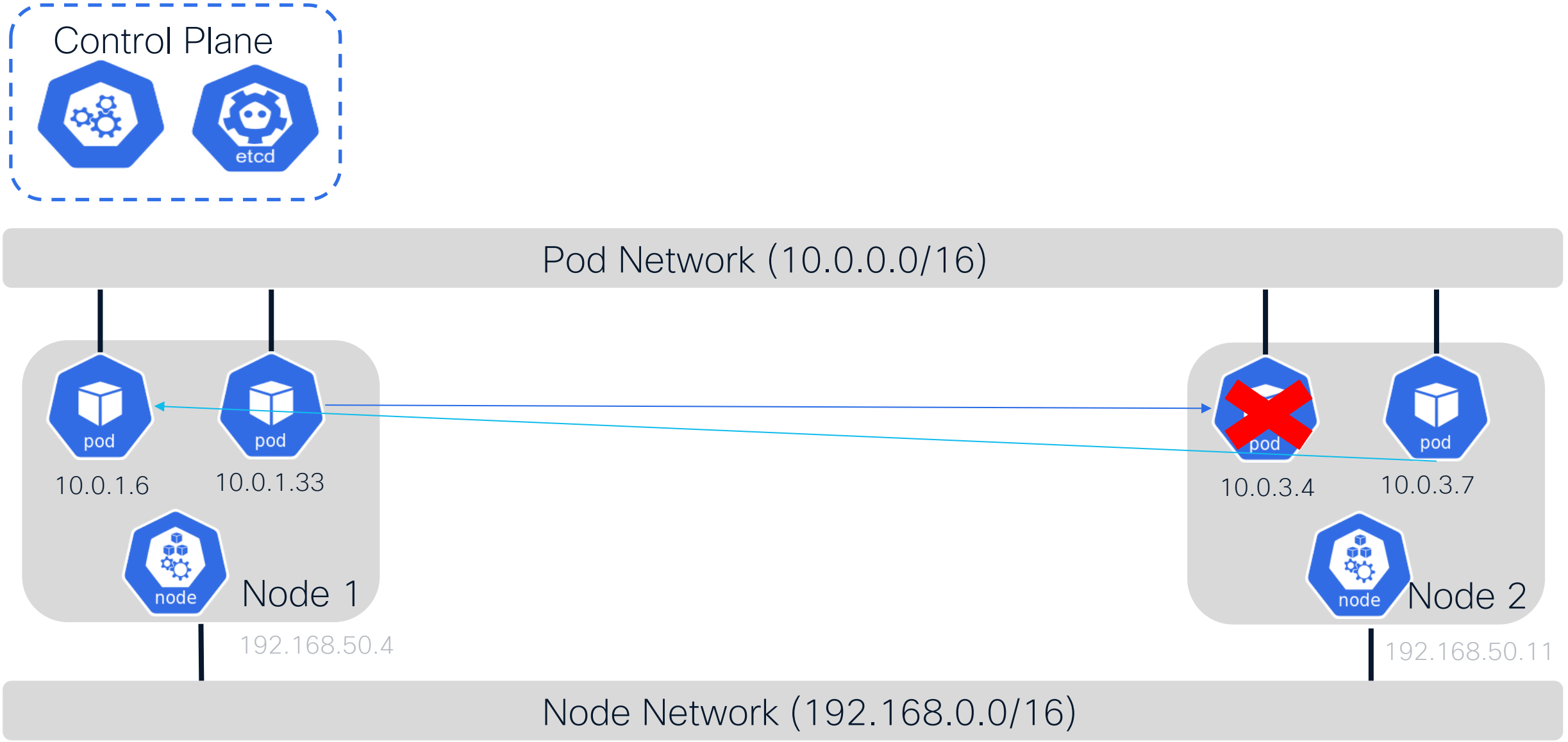
cisco

Complicated Policy Enforcement



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

Kubernetes Networking

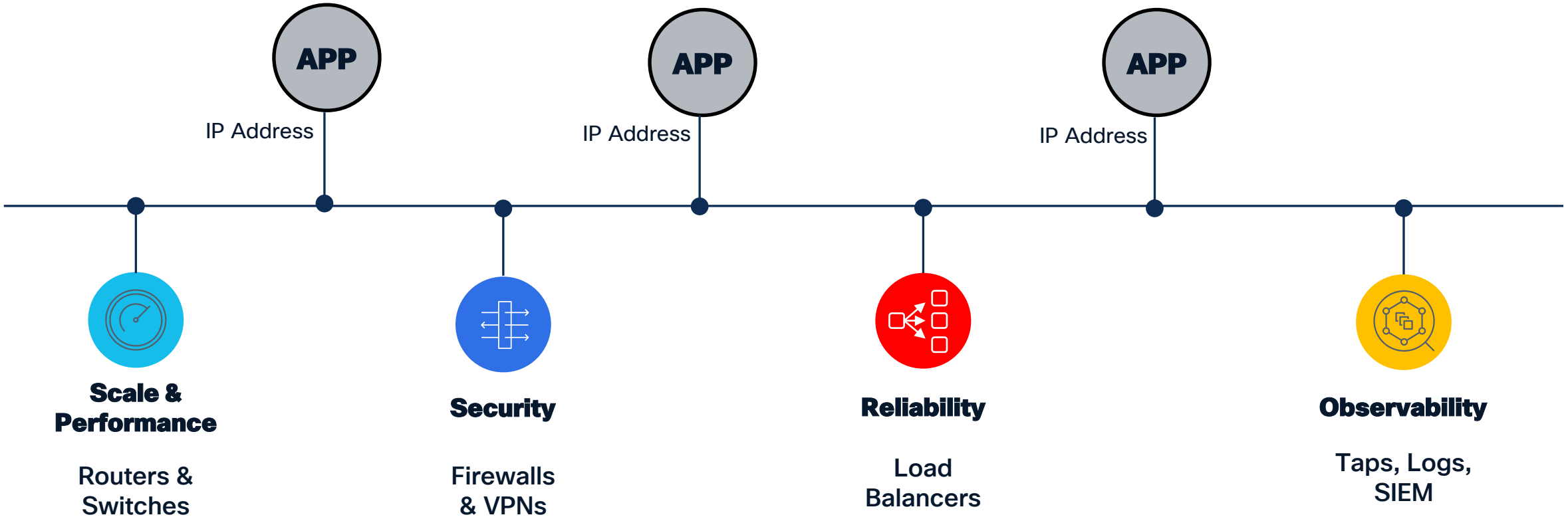


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

The Network has Always Been Essential to Applications

But Kubernetes Environments Are Challenging for Enterprise Infrastructure Teams

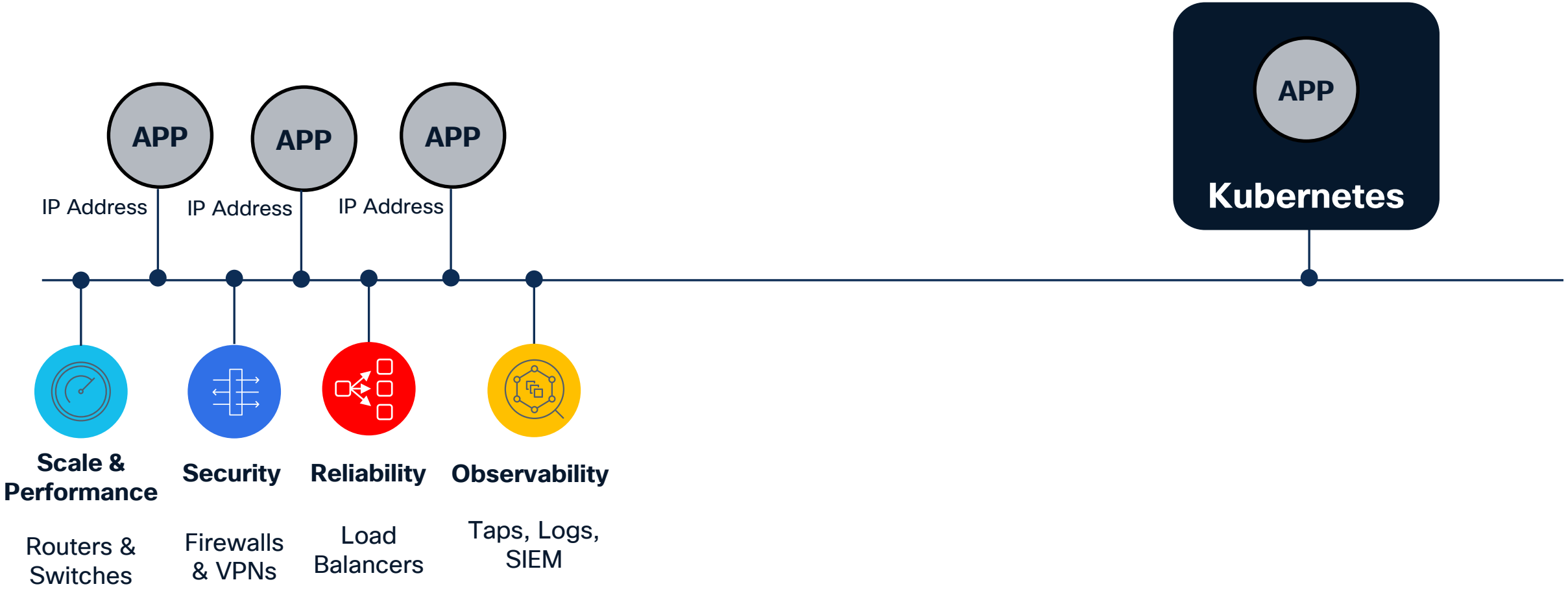


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

The Network has Always Been Essential to Applications

But Kubernetes Environments Are Challenging for Enterprise Infrastructure Teams

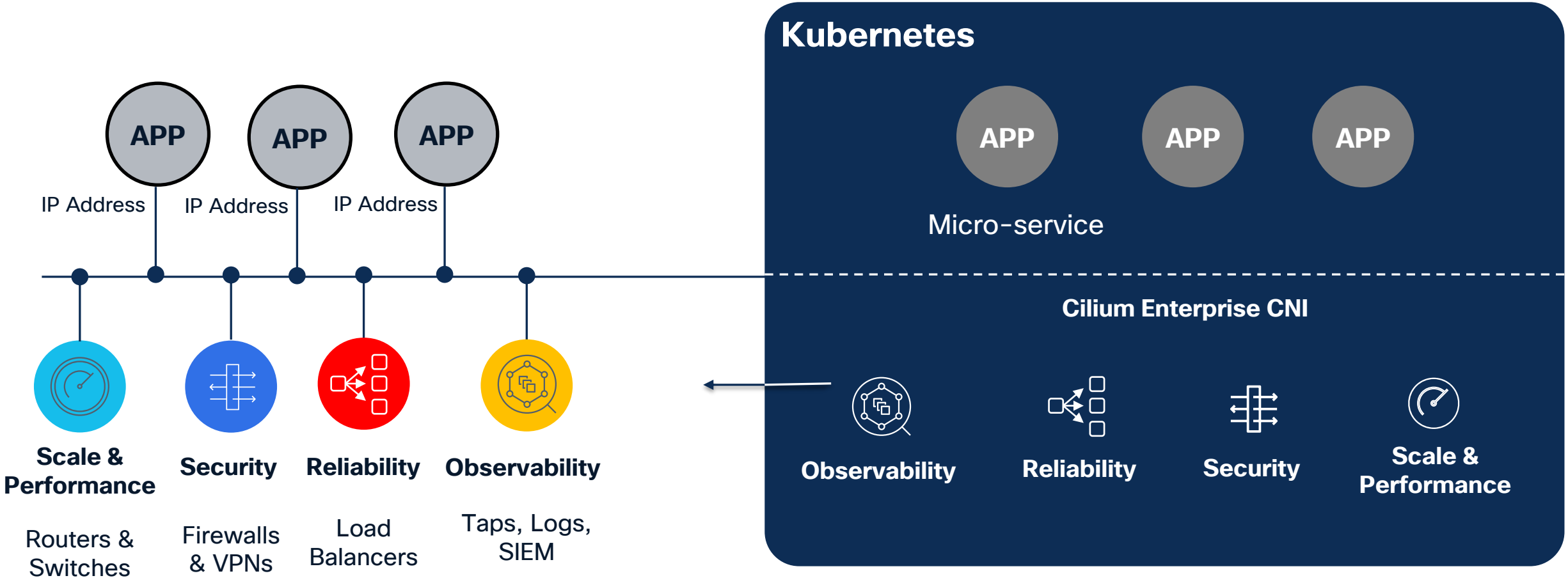


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

The Network has Always Been Essential to Applications

But Kubernetes Environments Are Challenging for Enterprise Infrastructure Teams



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

cisco

eBPF powers many things

Capabilities For Your Cloud Native Journey

Service Mesh

RESILIENCE AUTHENTICATION TRAFFIC MANAGEMENT

cilium Service Mesh

Ingress Gateway API spiffe

Observability

METRICS TRACING SERVICE MAP LOGS

cilium Hubble

SIEM JSON fluentd Grafana OpenTelemetry

Networking

ENCRYPTION LOAD-BALANCING NETWORK POLICY NETWORKING

cilium CNI

IPsec
Wireguard

Kubernetes
DSR • Maglev

DNS • L7
L3/L4

IPv4 • IPv6 • Overlay • BGP
Egress Gateway • Multi-Cluster

Runtime Security

OBSERVABILITY
ENFORCEMENT

Tetragon

SIEM JSON fluentd

Kubernetes Container VM Metal

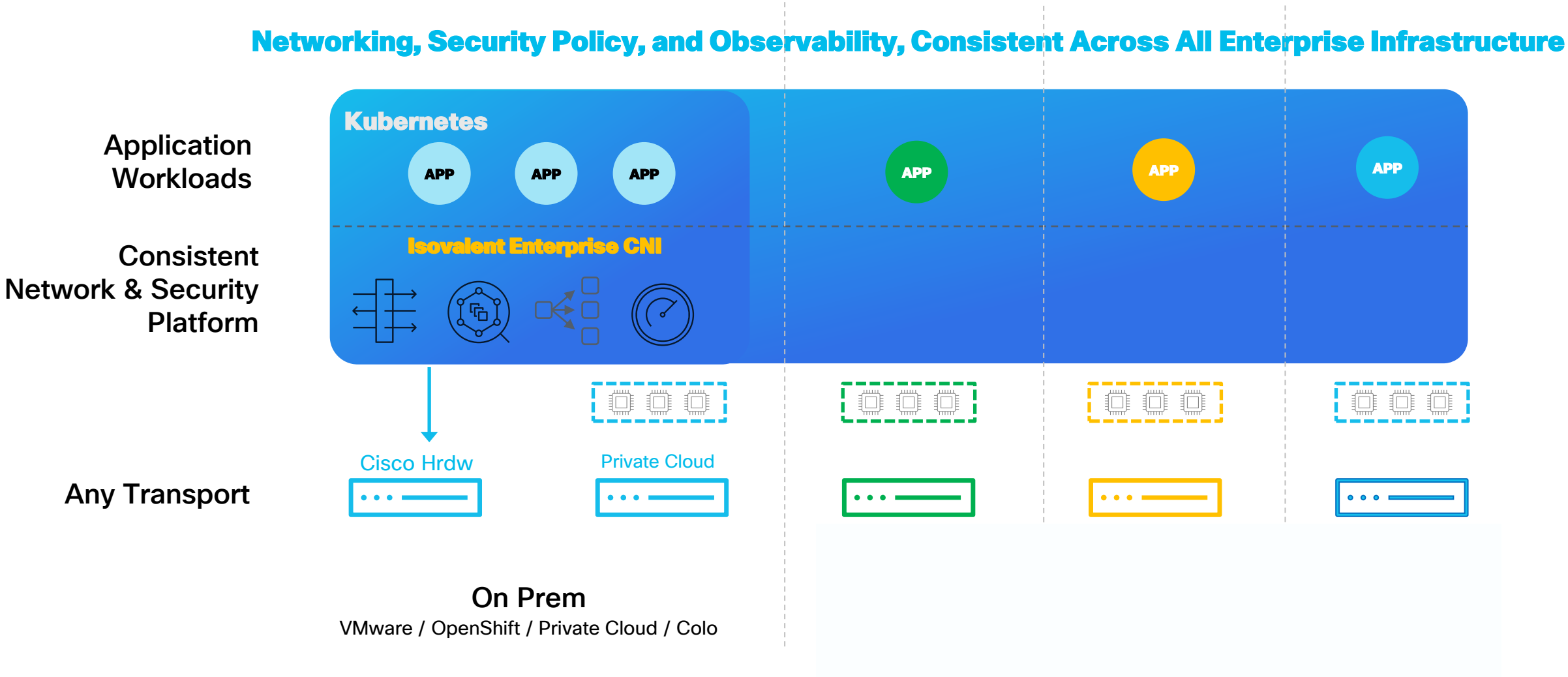
aws Google Cloud Azure Alibaba Cloud Red Hat OpenShift vmware

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

cisco

This is Why Cisco Acquired Isovalent.

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



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

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.

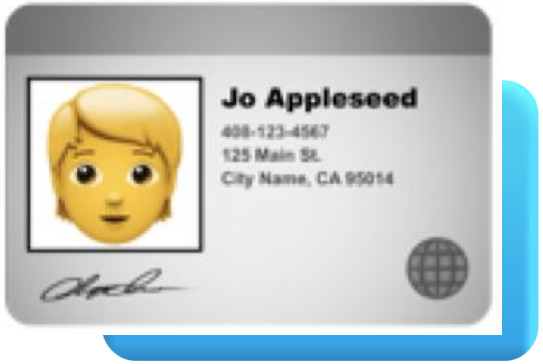
Benefits
Provides observability, security, and traffic management without altering application code.

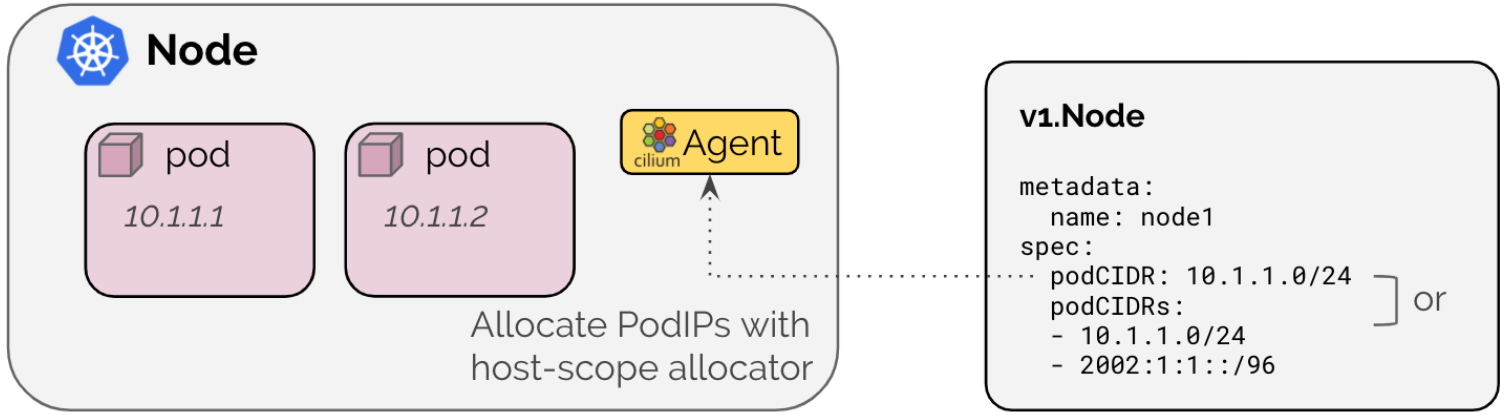
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

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/

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

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                          |
+-------------------------------------------------------------+
```

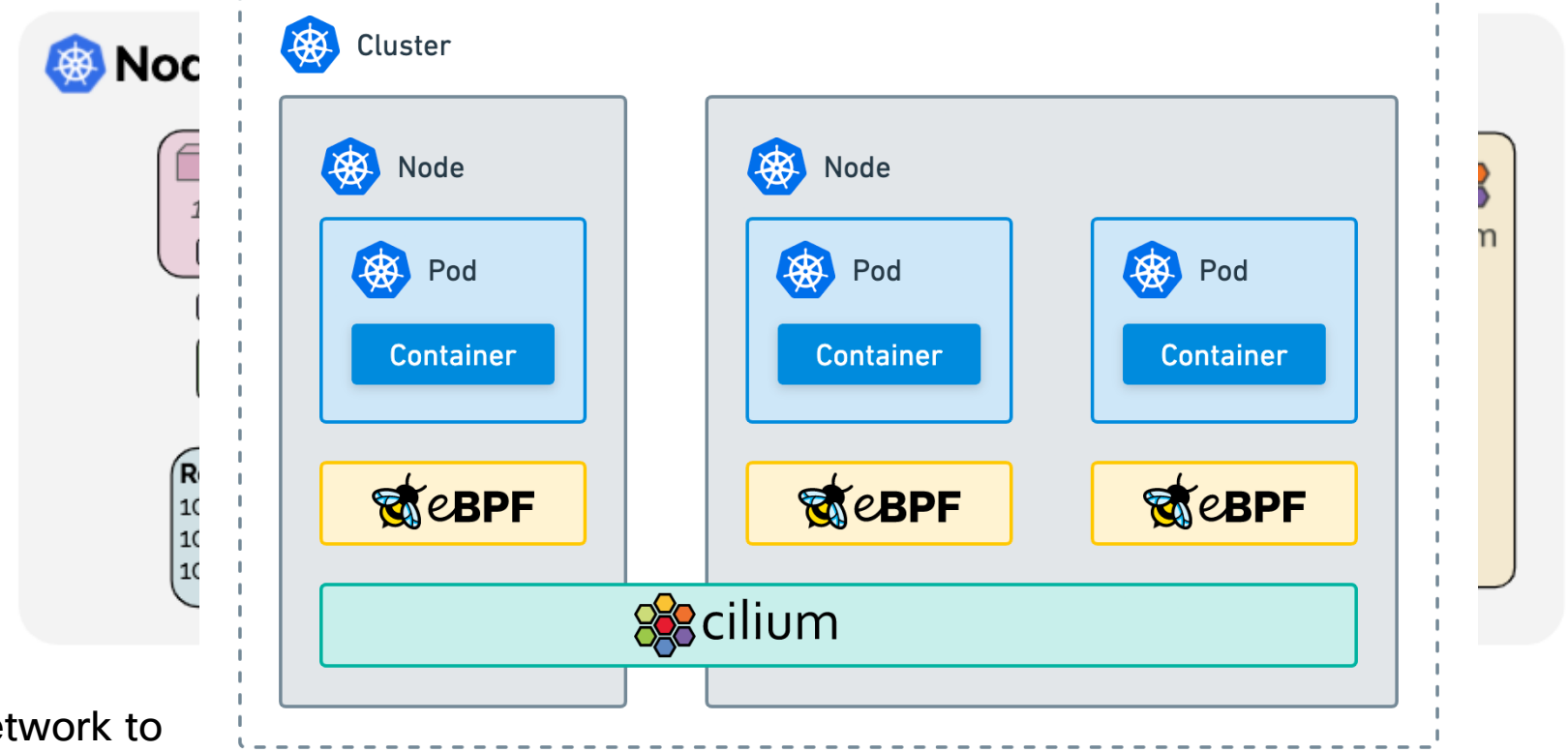
https://isovalent.com/labs/tetragon-getting-started/

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

cisco

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.

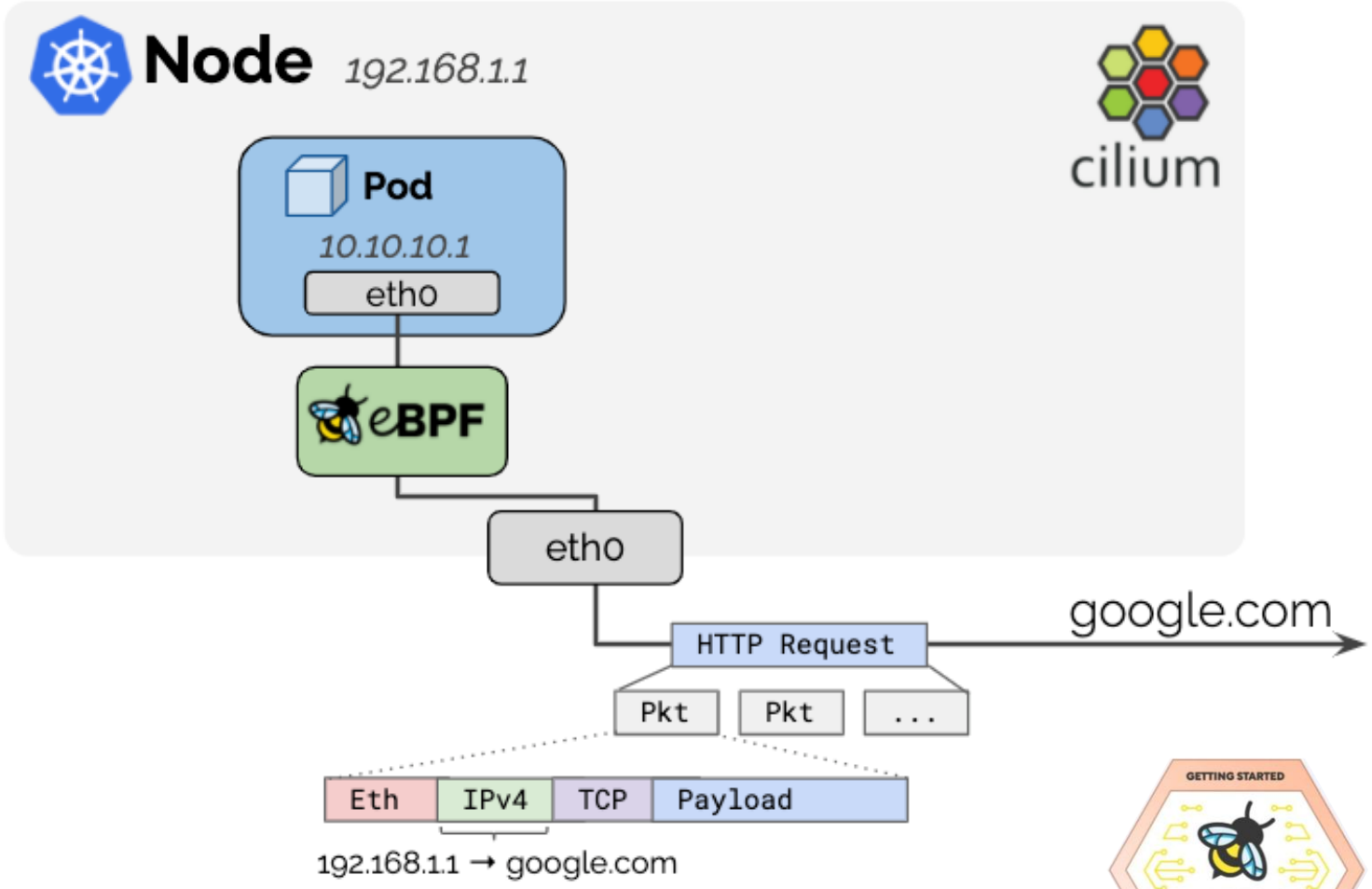
https://isovalent.com/labs/cilium-lb-ipam-l2-announcements

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

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.

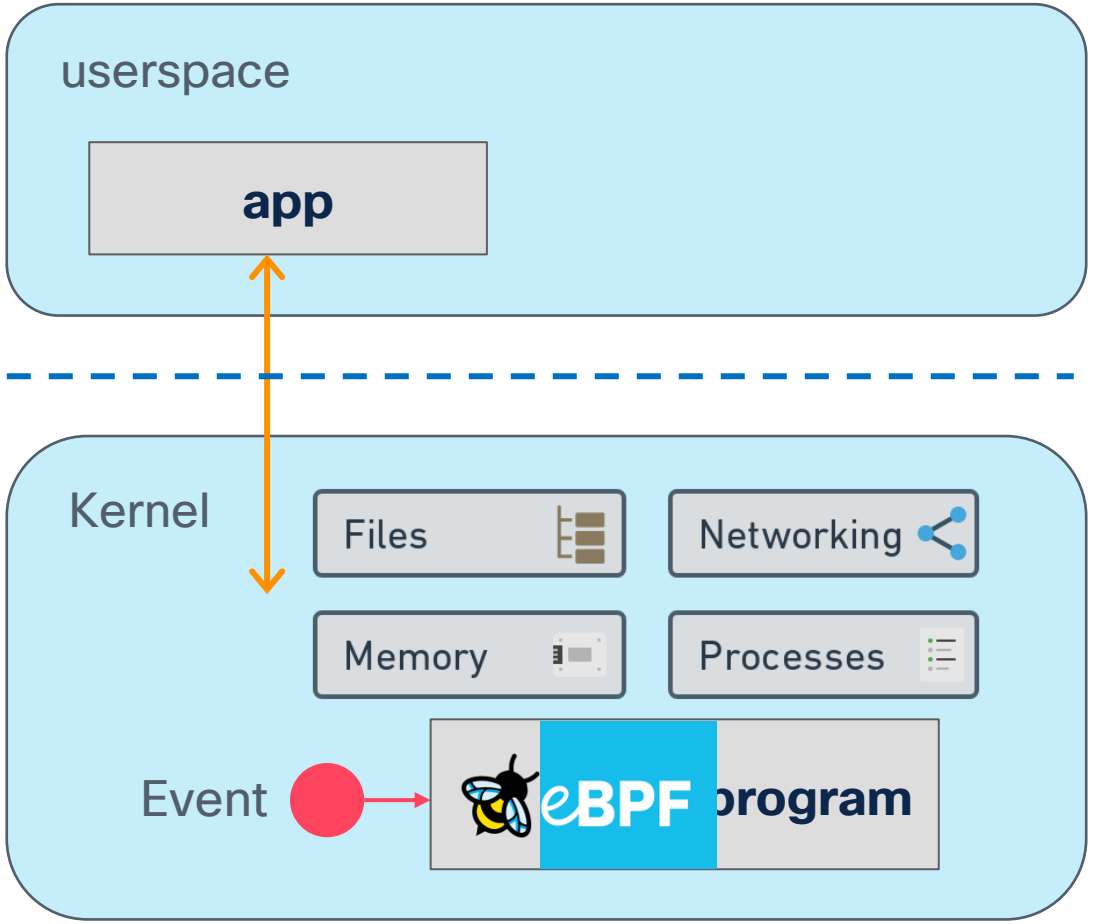


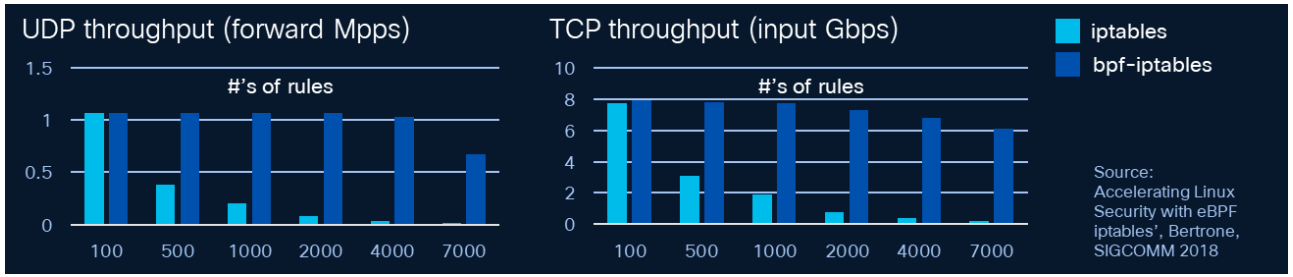
https://isovalent.com/labs/ebpf-getting-started/

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

eBPF – Extended Berkely Packet Filter

Makes the kernel programmable in a secure and efficient way





System calls

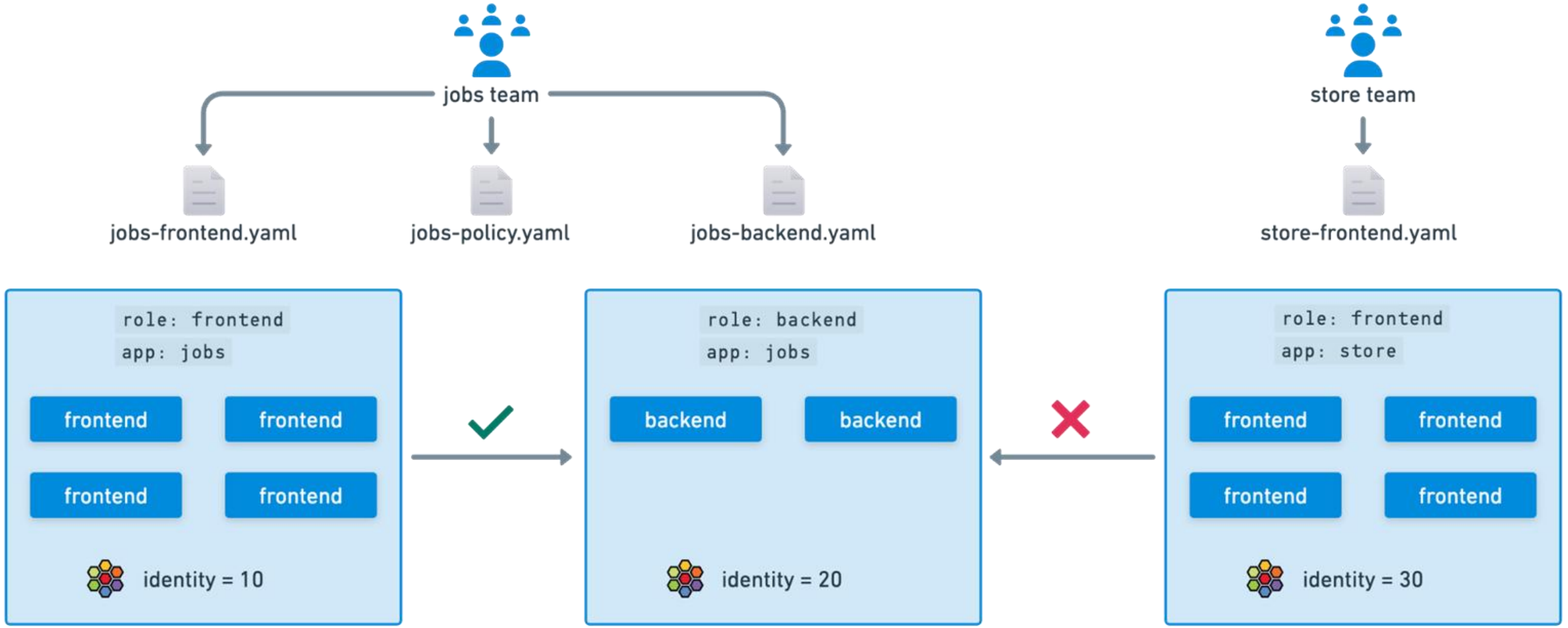
- eBPF runs in a restricted execution environment
- Before eBPF script is compiled:
  - Verifier ensures things such as memory safety
  - Hardening process
    (program execution protection, mitigation against spectre, constant blinding, ...)
- eBPF can only access pre-approved kernel functions and data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

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

cisco

Micro-Segmentation

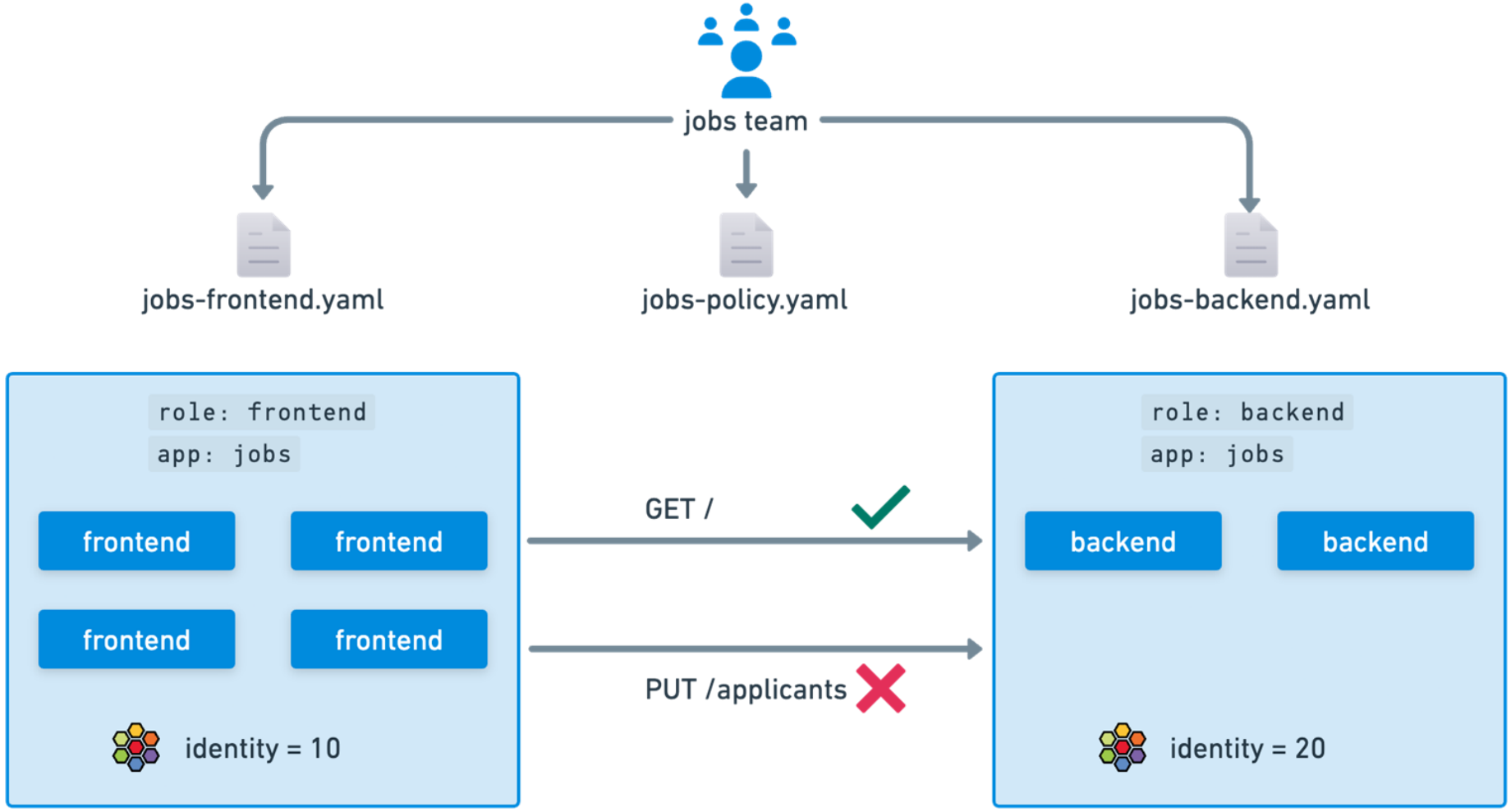
Label based East-West Application or Multi-tenet Security Enforcement



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

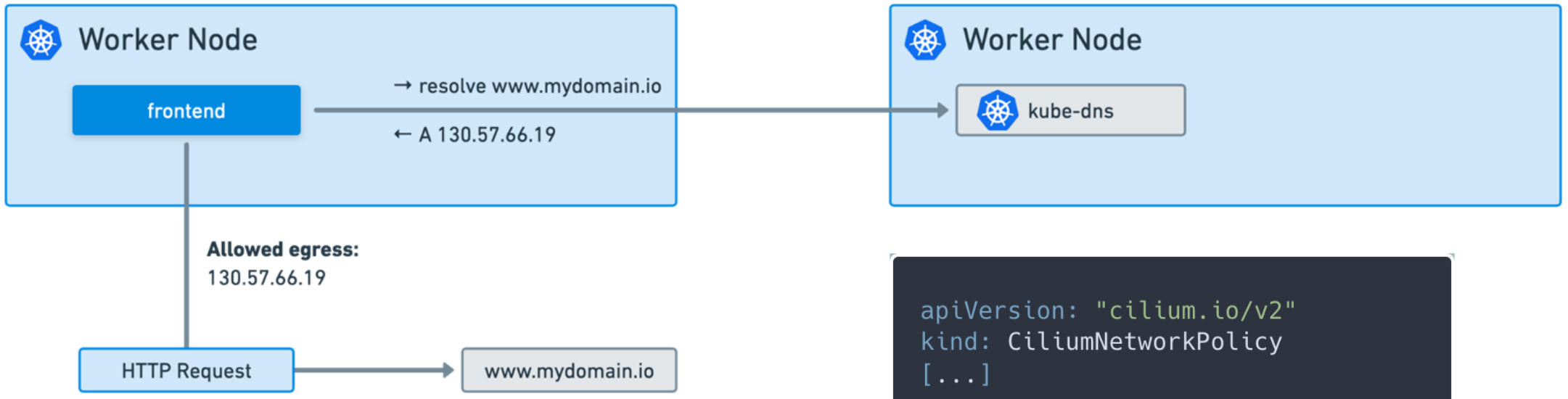
API-Aware Security

Safely Secure API Endpoints by filtering Protocols, Methods and Paths



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

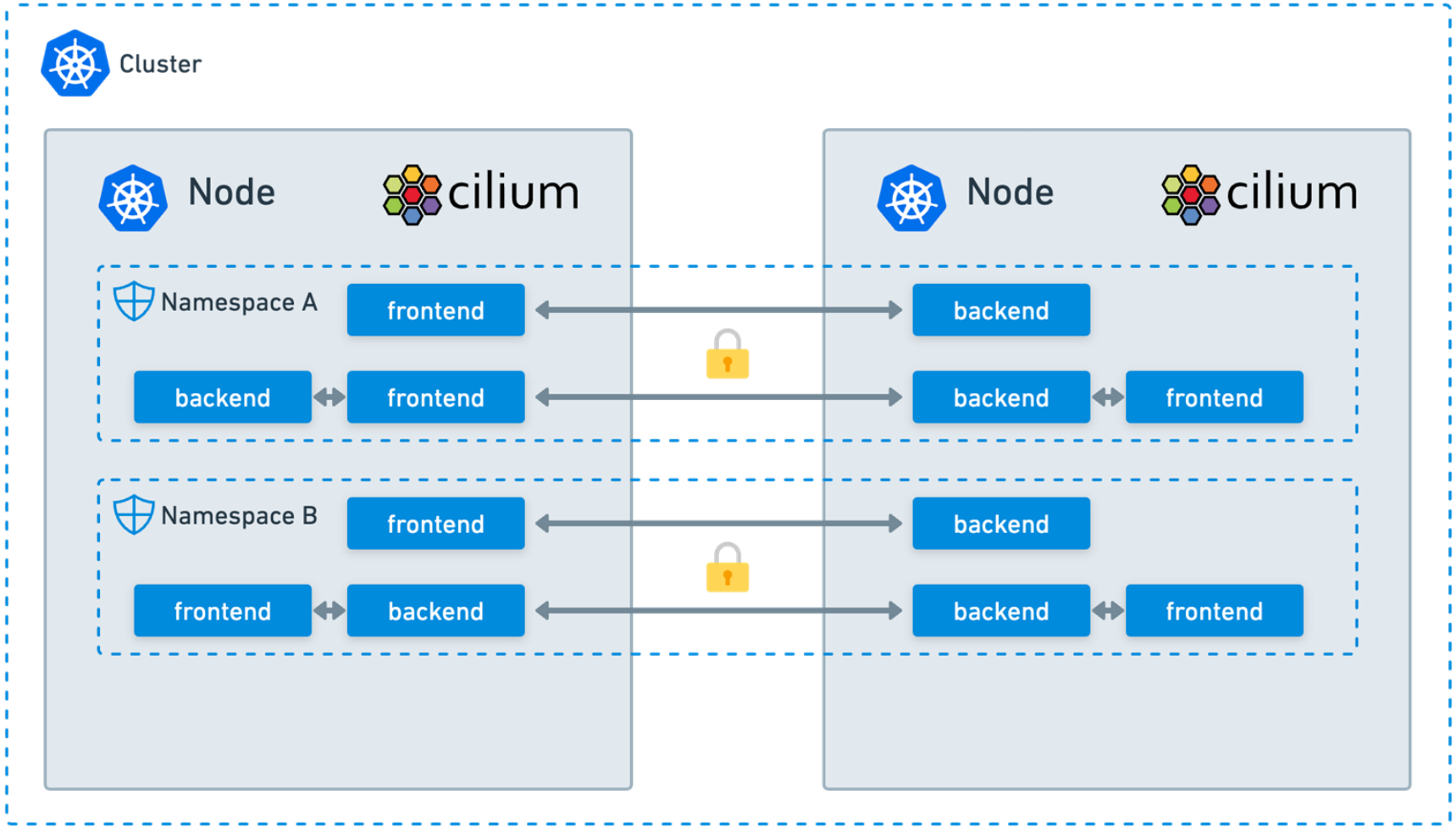
DNS-aware Cilium Network Policy




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

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

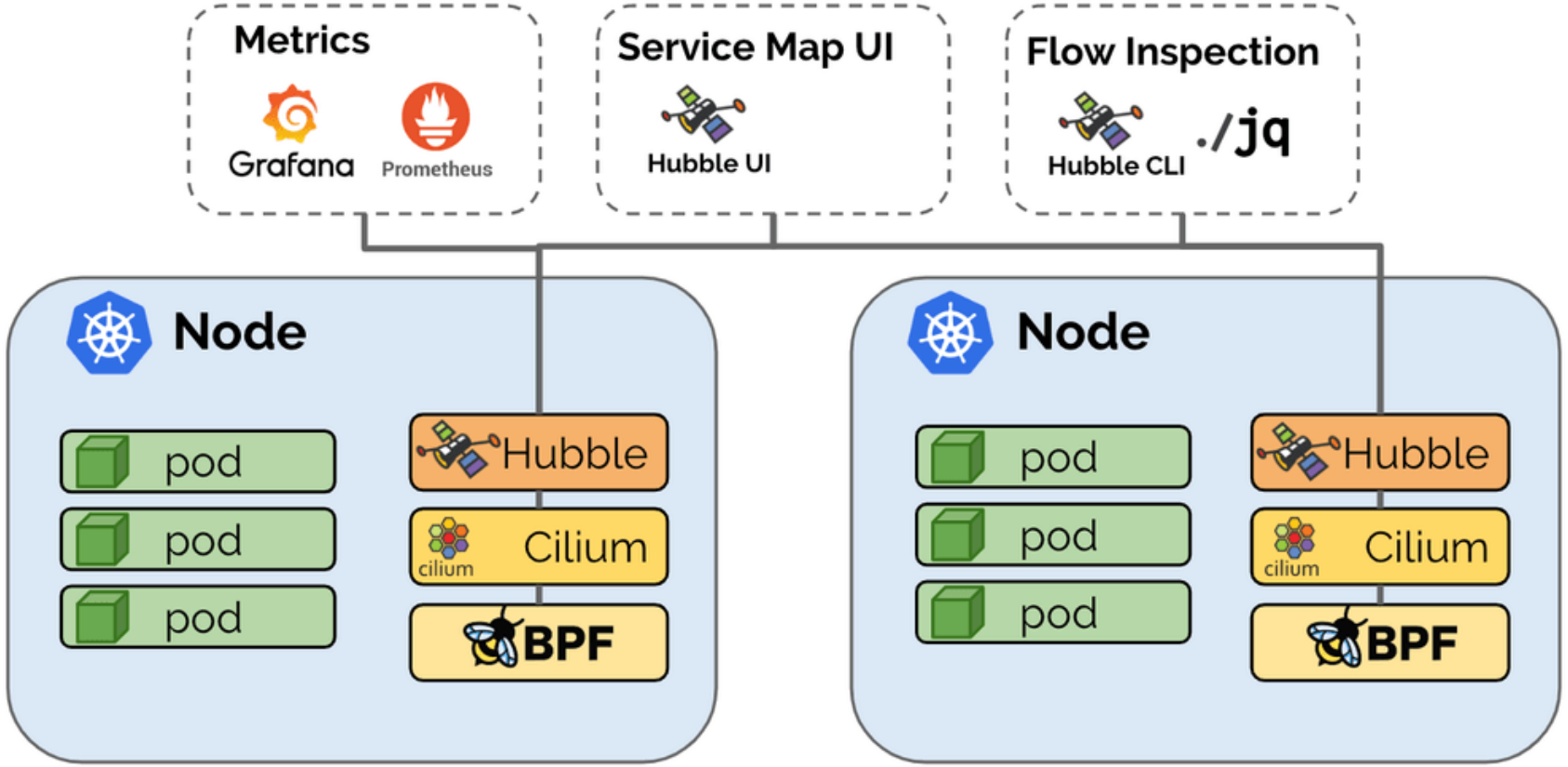
Transparent Data Encryption



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

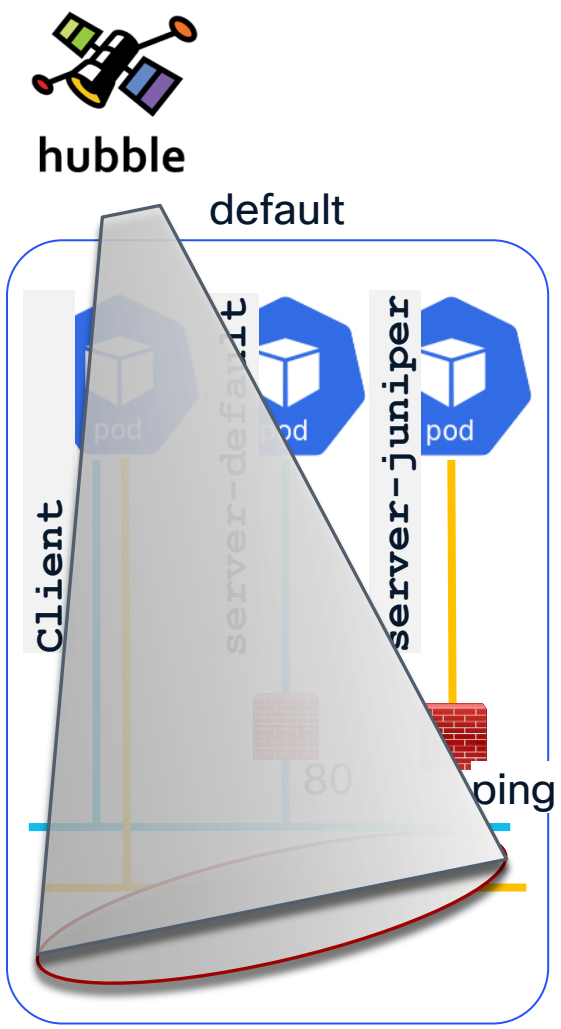
Hubble CLI

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.



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

Basic Lab Deployment – Netpolicy - validate



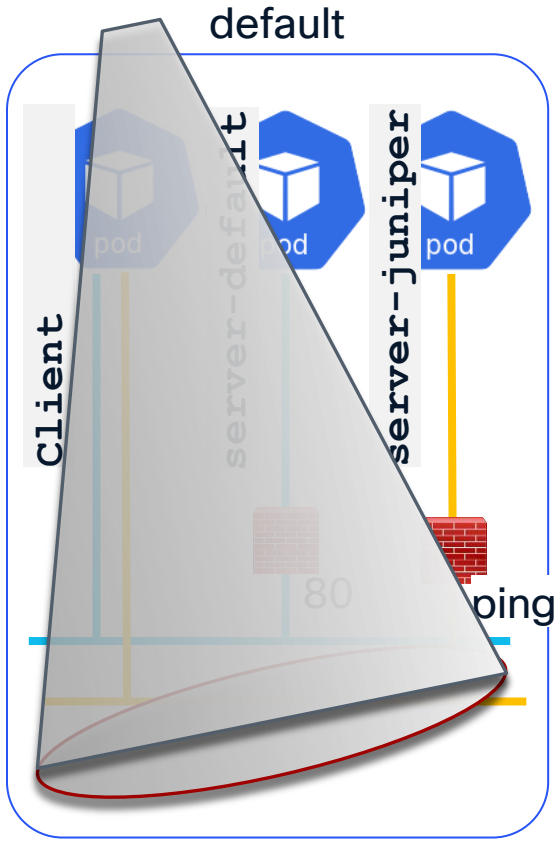

```
root@server:~# hubble observe --pod client --protocol icmp
..~ client (ID:12606) -> server-default (ID:3255) to-stack FORWARDED (ICMPv4 EchoRequest)
..~ client (ID:12606) <> server-default (ID:3255) policy-verdict:none INGRESS DENIED (ICMPv4 Ec
..~ client (ID:12606) <> server-default (ID:3255) Policy denied DROPPED (ICMPv4 EchoRequest)
..~ client (ID:61243) -> server-jupiter (ID:31088) policy-verdict:L4-Only EGRESS ALLOWED (ICMPv
..~ 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 Ech
..~ client (ID:12606) <> server-default (ID:3255) Policy denied DROPPED (ICMPv4 EchoRequest)
```

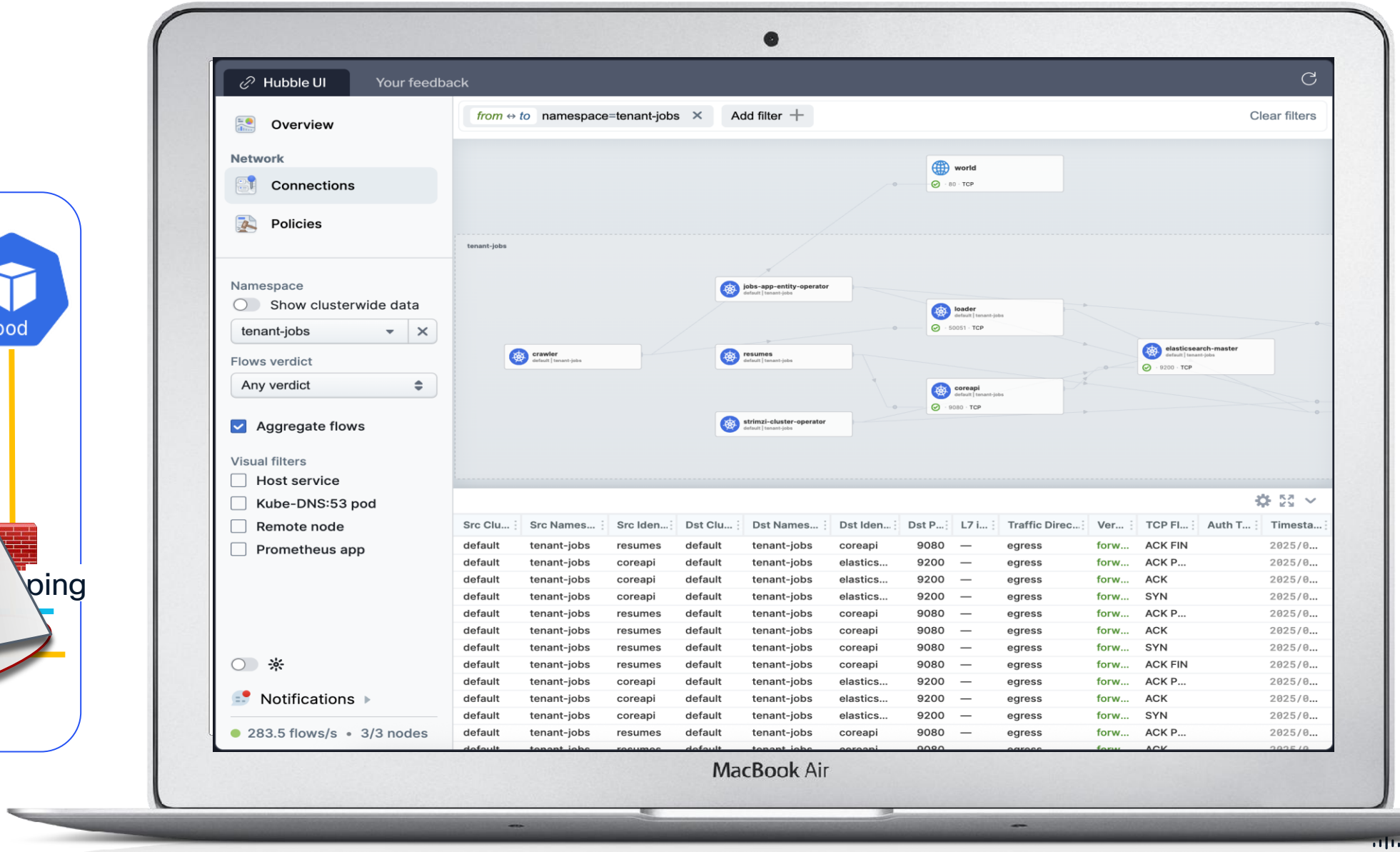
MacBook Air

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

Basic Lab Deployment – Netpolicy - validate

hubble



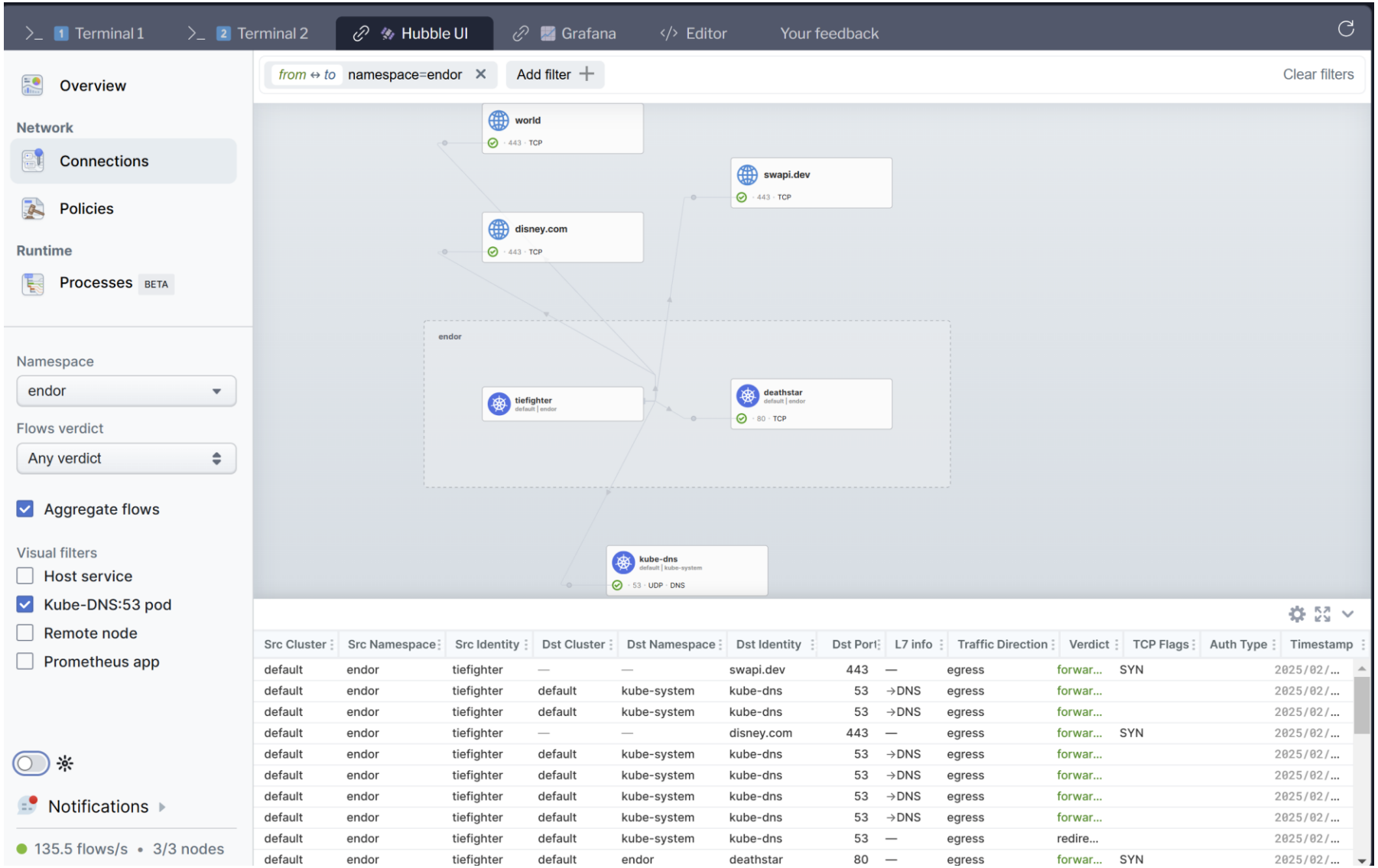


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

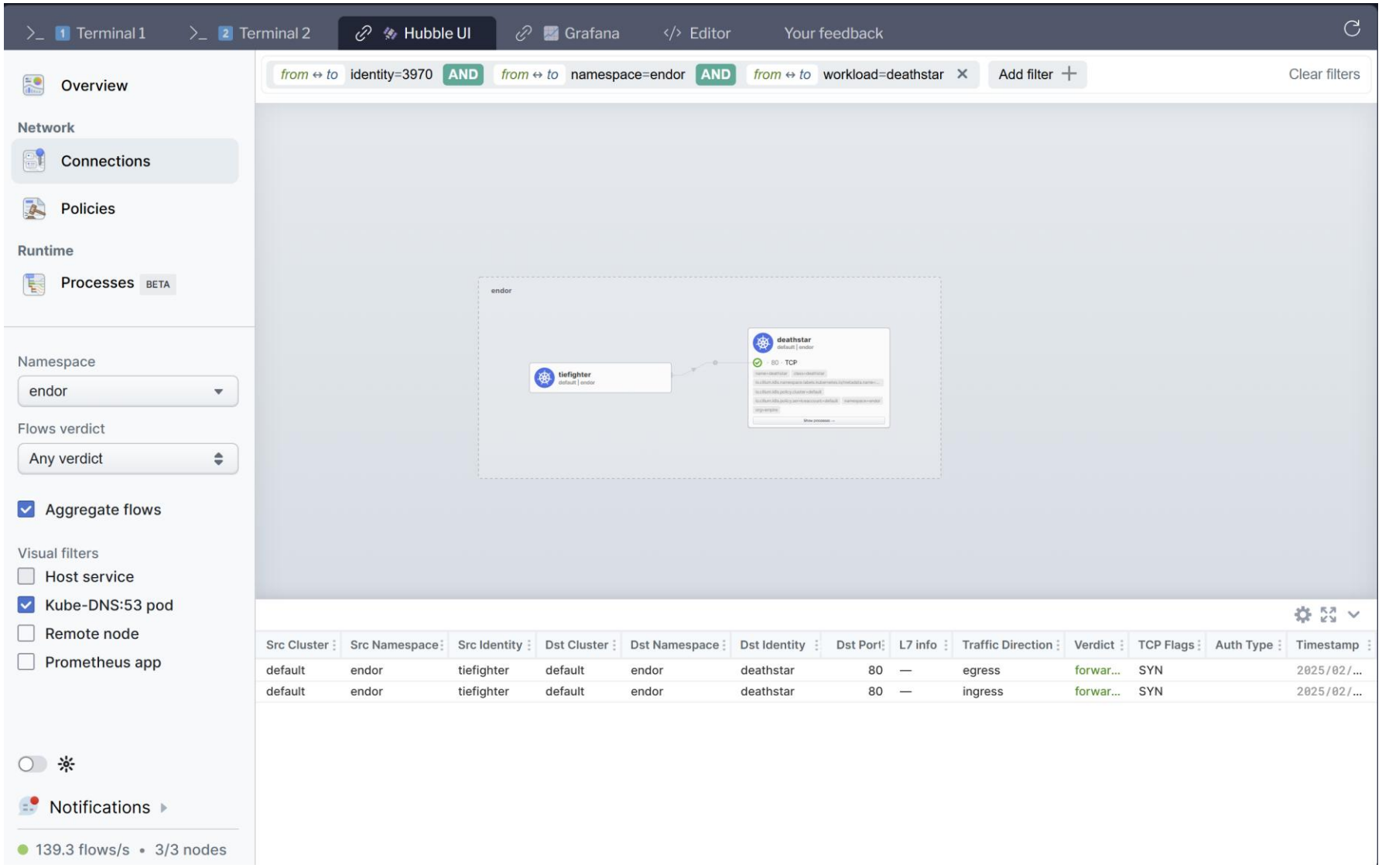
Is there a GUI?

Start with App Dependency Map & DNS visibility



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

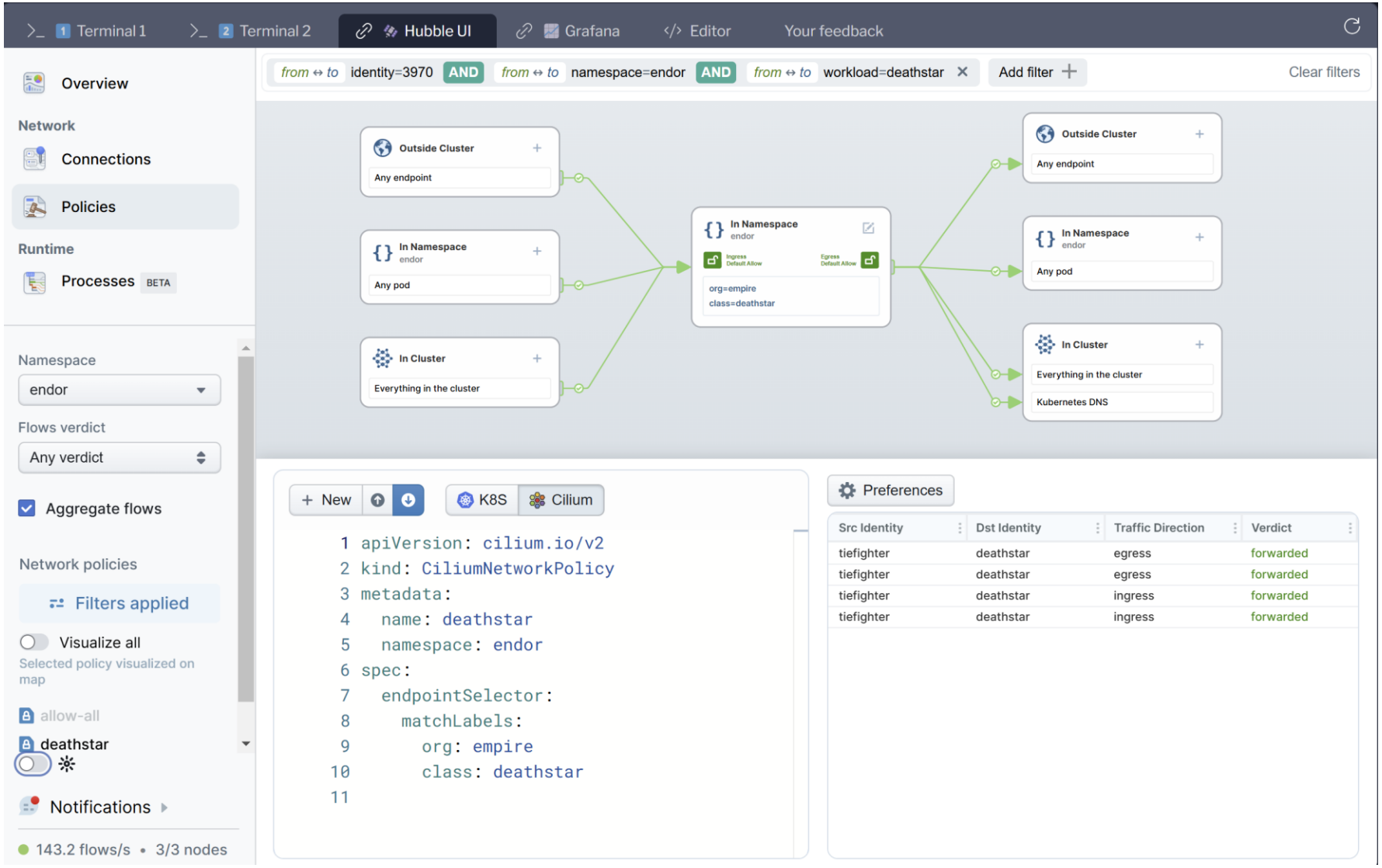
Explore microservice interactions



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

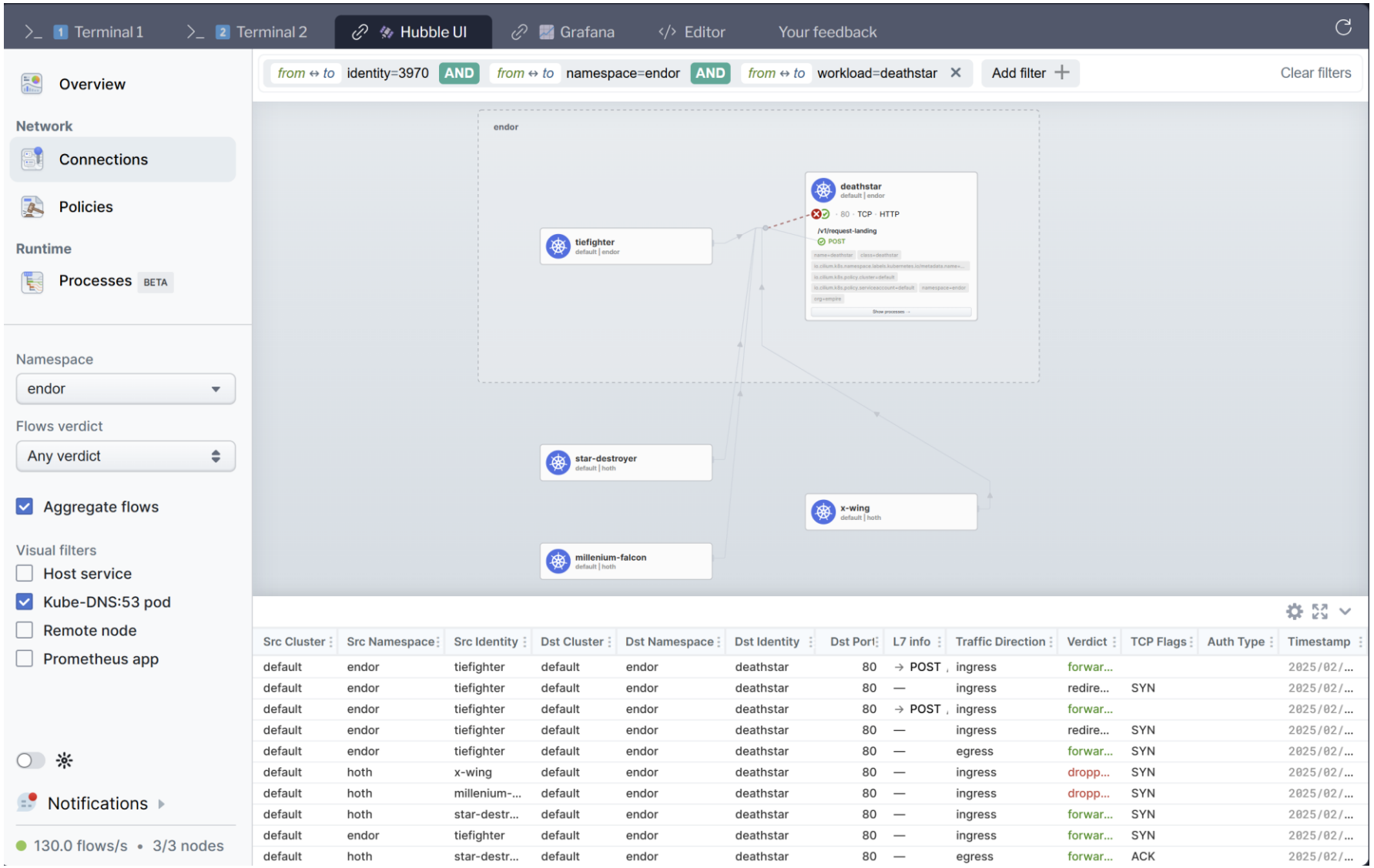
cisco

Visualize policy



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

Add layer 7 visibility and enforcement

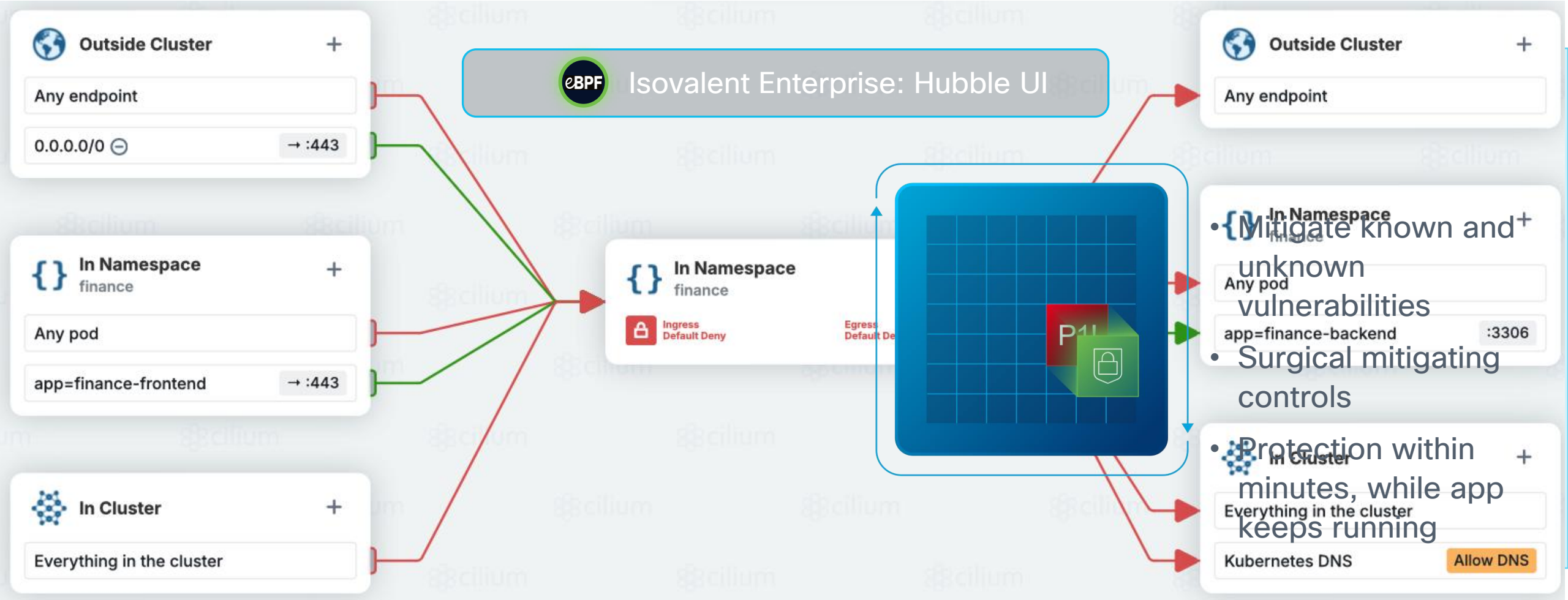


© 2025 Cisco and/or its affiliates. All rights reserved.

Manual

Innovations from Isovalent Automated by Hypershield

Autonomous



- Mitigate known and unknown vulnerabilities
- Surgical mitigating controls
- Protection within minutes, while app keeps running

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

Zero Trust coverage for apps from on-premises to cloud

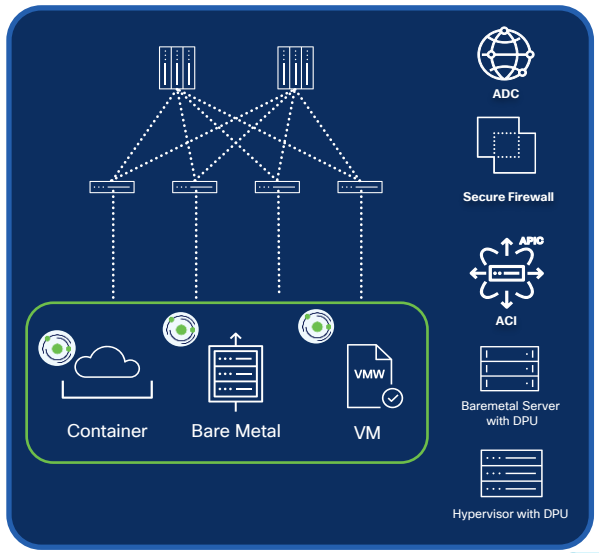
Agent

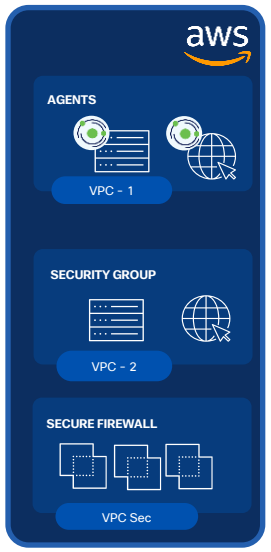
Cisco Security Cloud Control with Hybrid Mesh Firewall

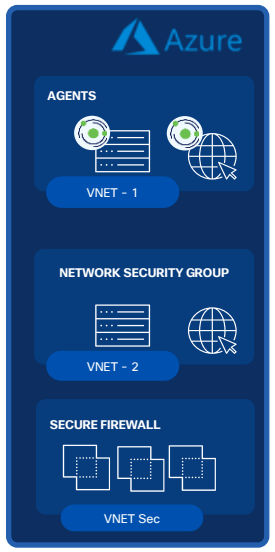
Agentless

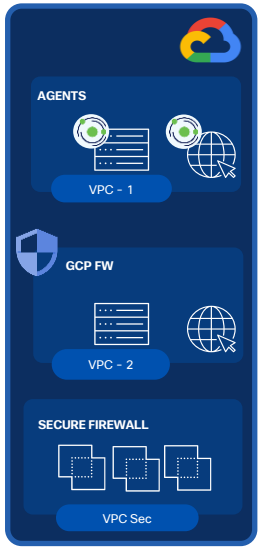
Anywhere

- Windows Desktop
- Windows Server
- IBM AIX
- Oracle Solaris
- Oracle Linux
- Centos, Rocky, Alma Linux
- Ubuntu, Debian
- SUSE Linux
- RedHat Linux
- Amazon Linux
- OpenShift
- Kubernetes









On Premise

Public Cloud

Bare Metal Servers

Virtual Machines

Containers

On-Prem

- Loadbalancer (ADC)
- Firewalls
- Data Center Fabric (SDN)
- NVIDIA Smart NIC (DPU)

AWS, GCP, Azure

- Security Group
- Network Security Group
- Cloud Network Firewall
- Multicloud Defense*
- NVIDIA Smart NIC (DPU)

User Identity | Tags and Labels | Vulnerability

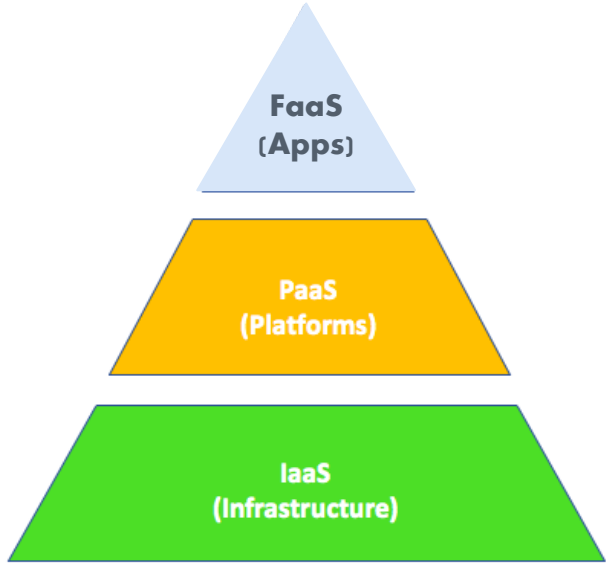
Threat Feed | Application Encryption | Domain/FQDN | Cisco Security Risk Score

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

Moving to the Cloud...

Two new parameters to consider in Cloud

New Infrastructure skills for each Service Cloud Providers



Public Cloud Service Model

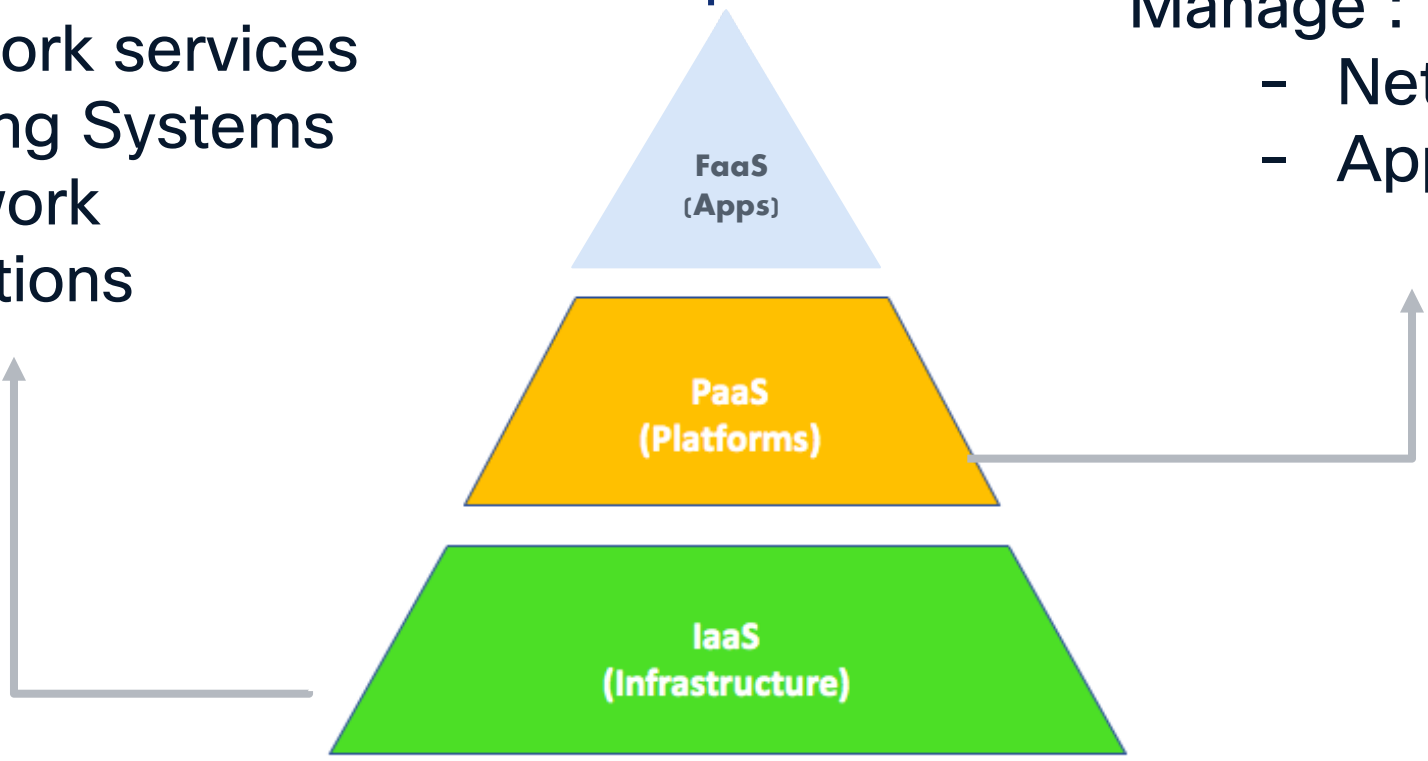
© 2025 Cisco and/or its affiliates. All rights reserved.

IaaS compared to PaaS Compared to FaaS

Manage :
- code

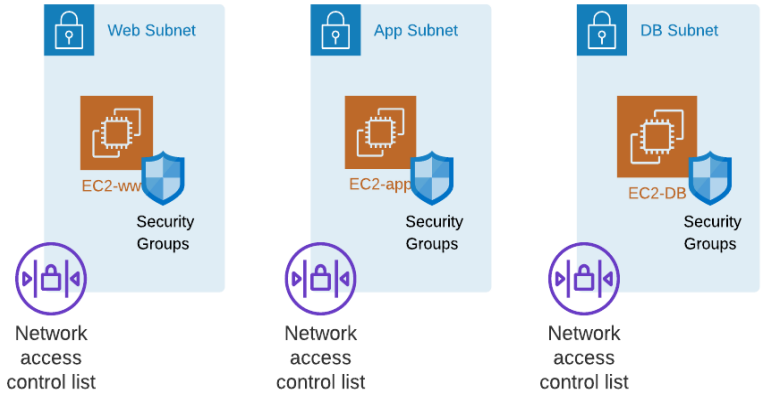
Manage :
- Network services
- Operating Systems
- Framework
- Applications

Manage :
- Network limited
- Applications

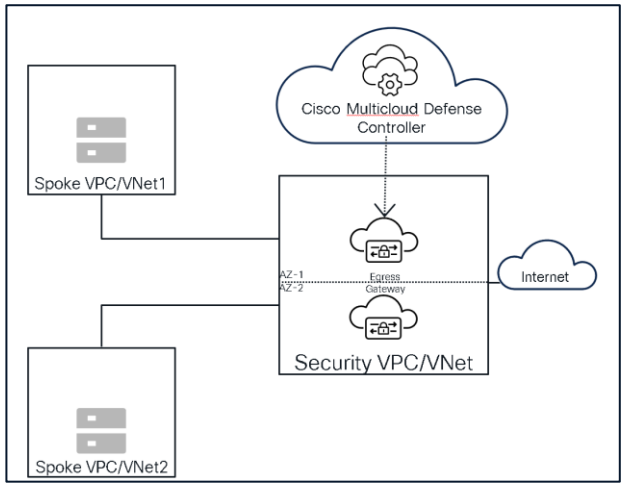


© 2025 Cisco and/or its affiliates. All rights reserved.

The way we do it in the Cloud...



Public Cloud Infrastructure



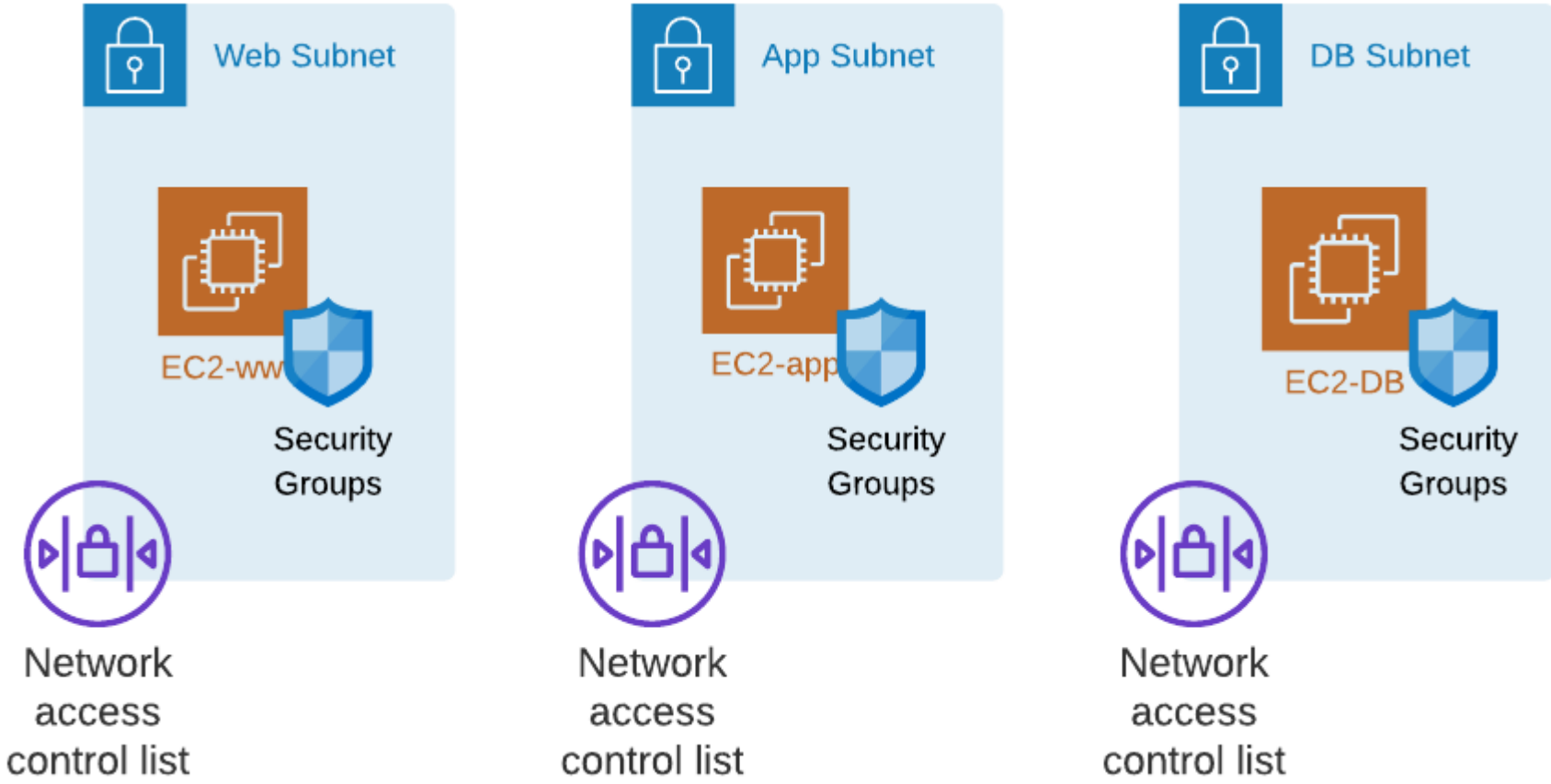
Firewall (Multicloud Defense, FTDv)

Host based Firewall

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

Macrosegmentation in the Cloud

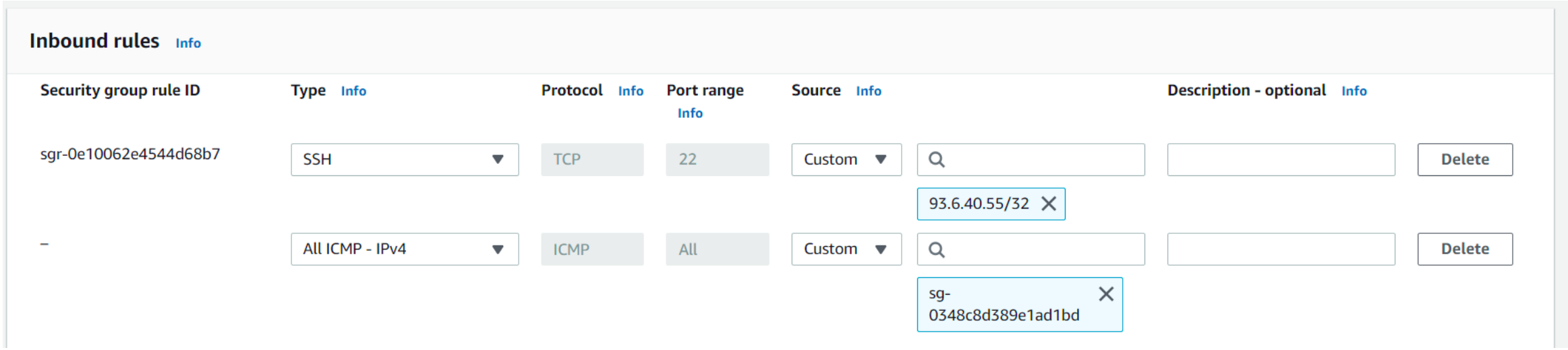
Security Groups and Network Access list



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

cisco

Use security group as Source within VPC

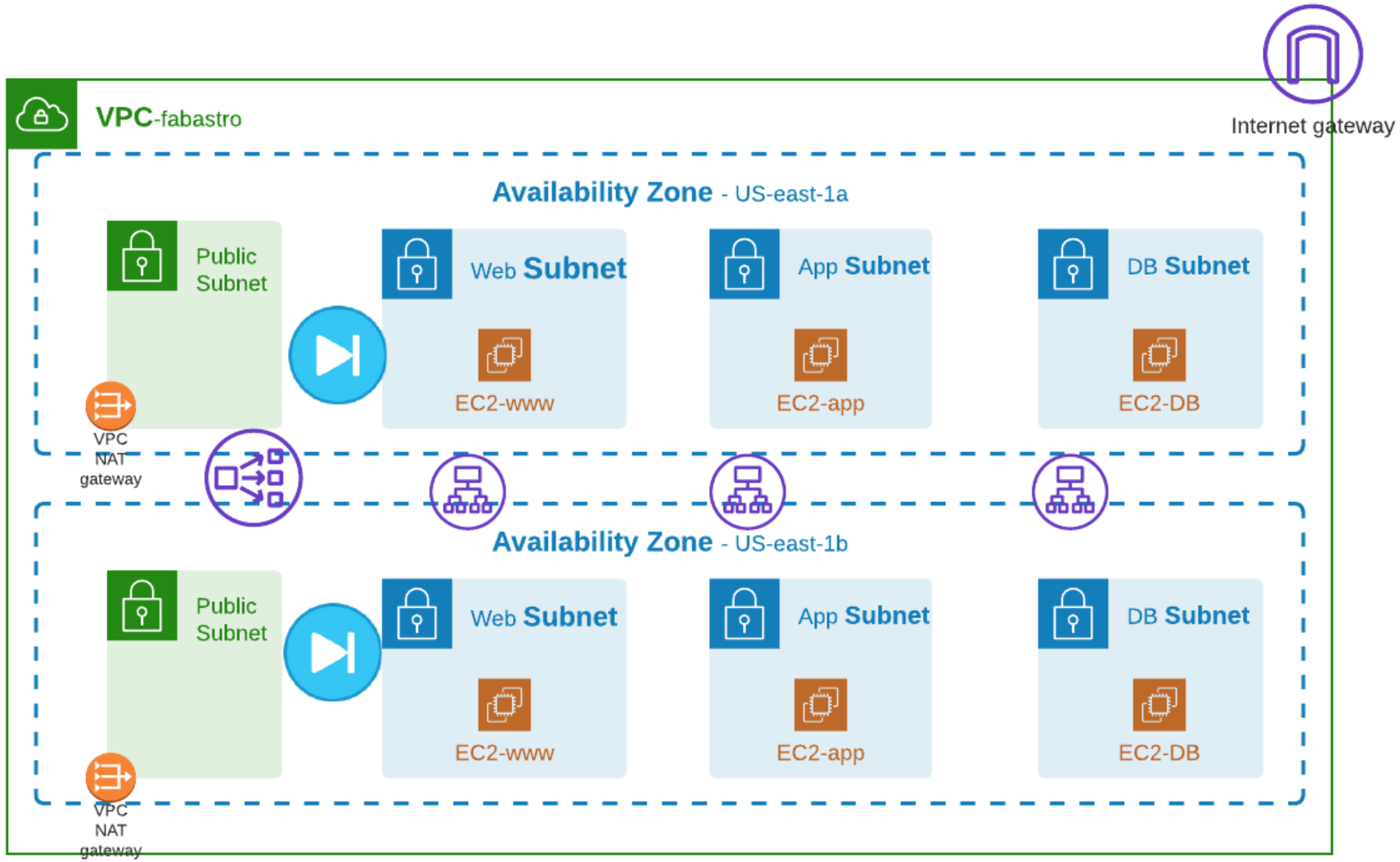


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Back to Network security with Firewall

FTD insertion with HA



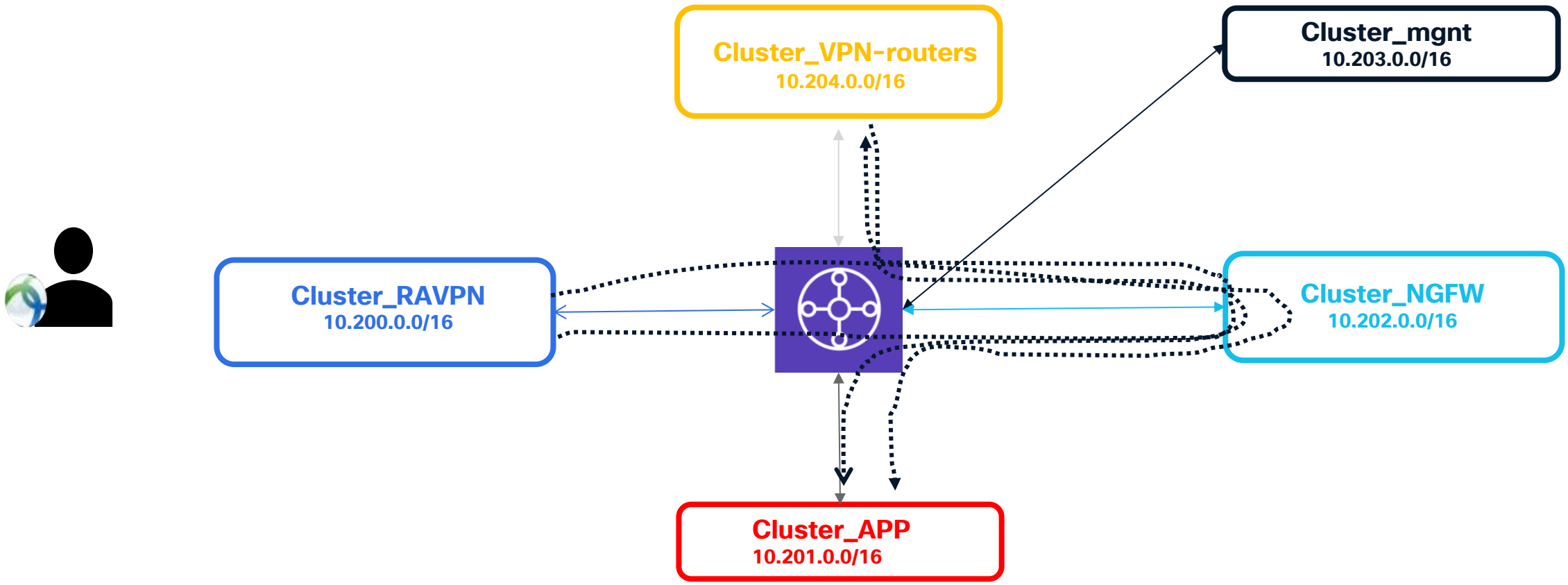
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

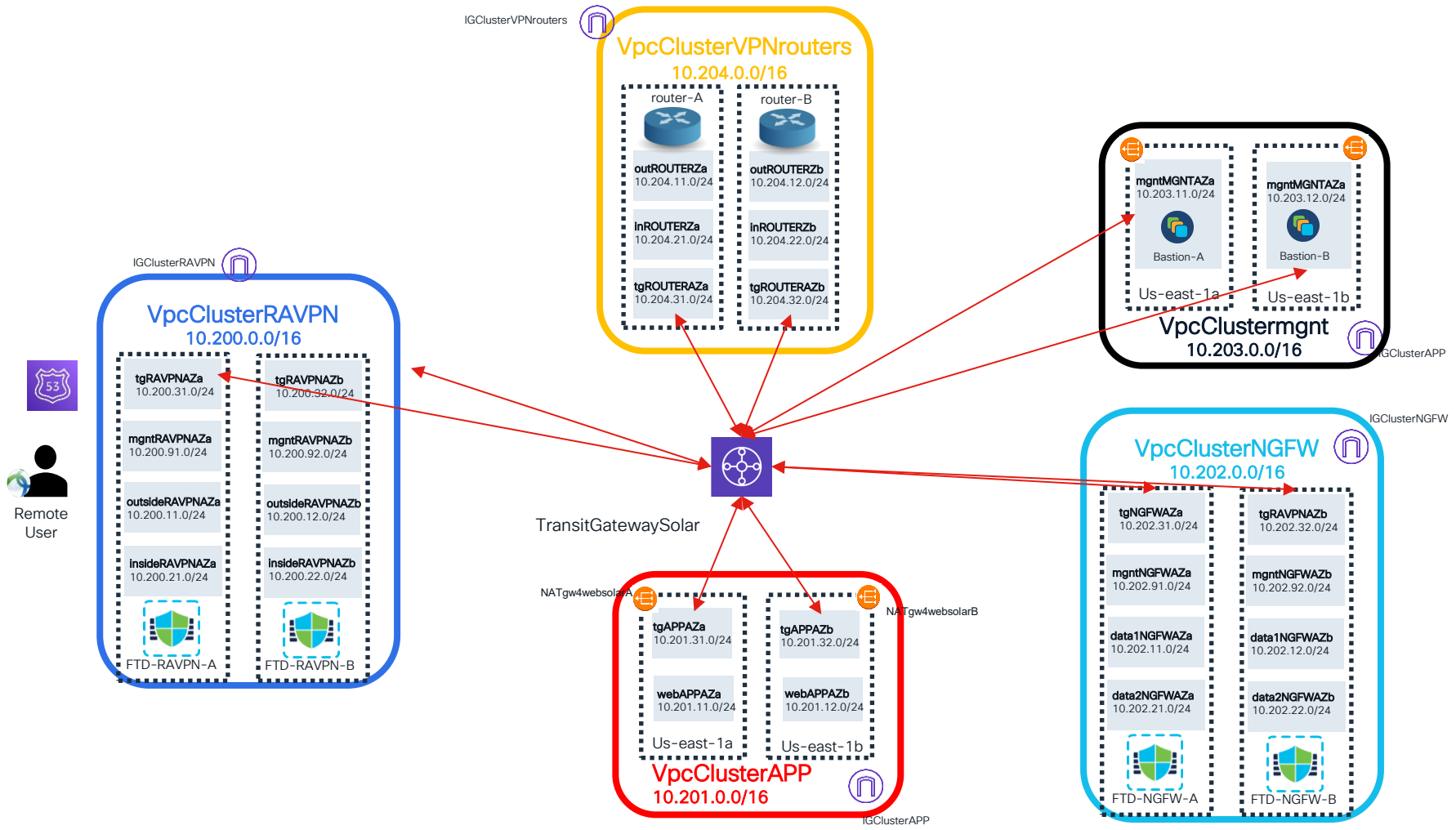
Limits of this design

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

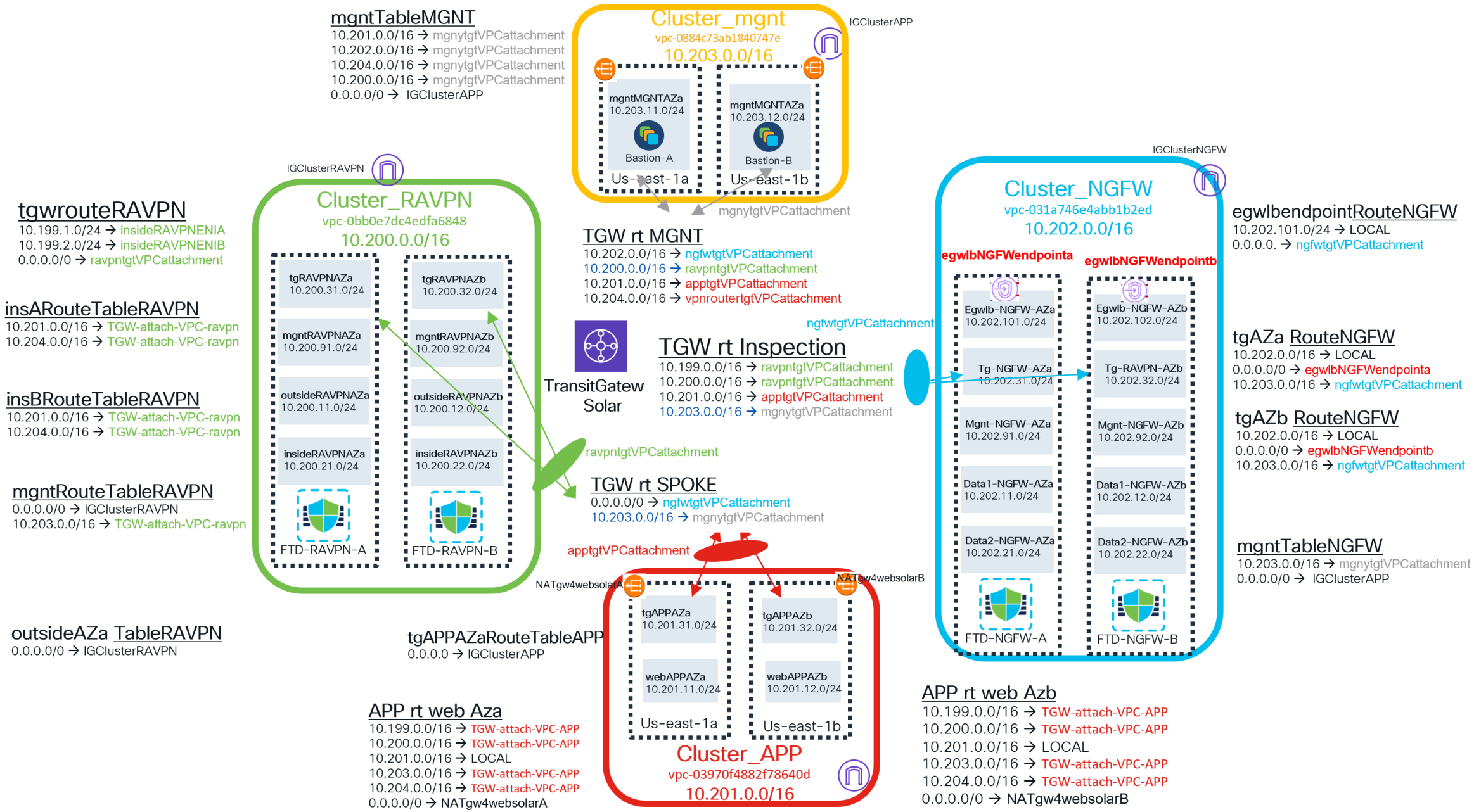
Security Insertion with Service VPC



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



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



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

Multi-Cloud Security configuration complexity

What do we need to configure?

Security VPCs

VPC and DNS Flow Log capture

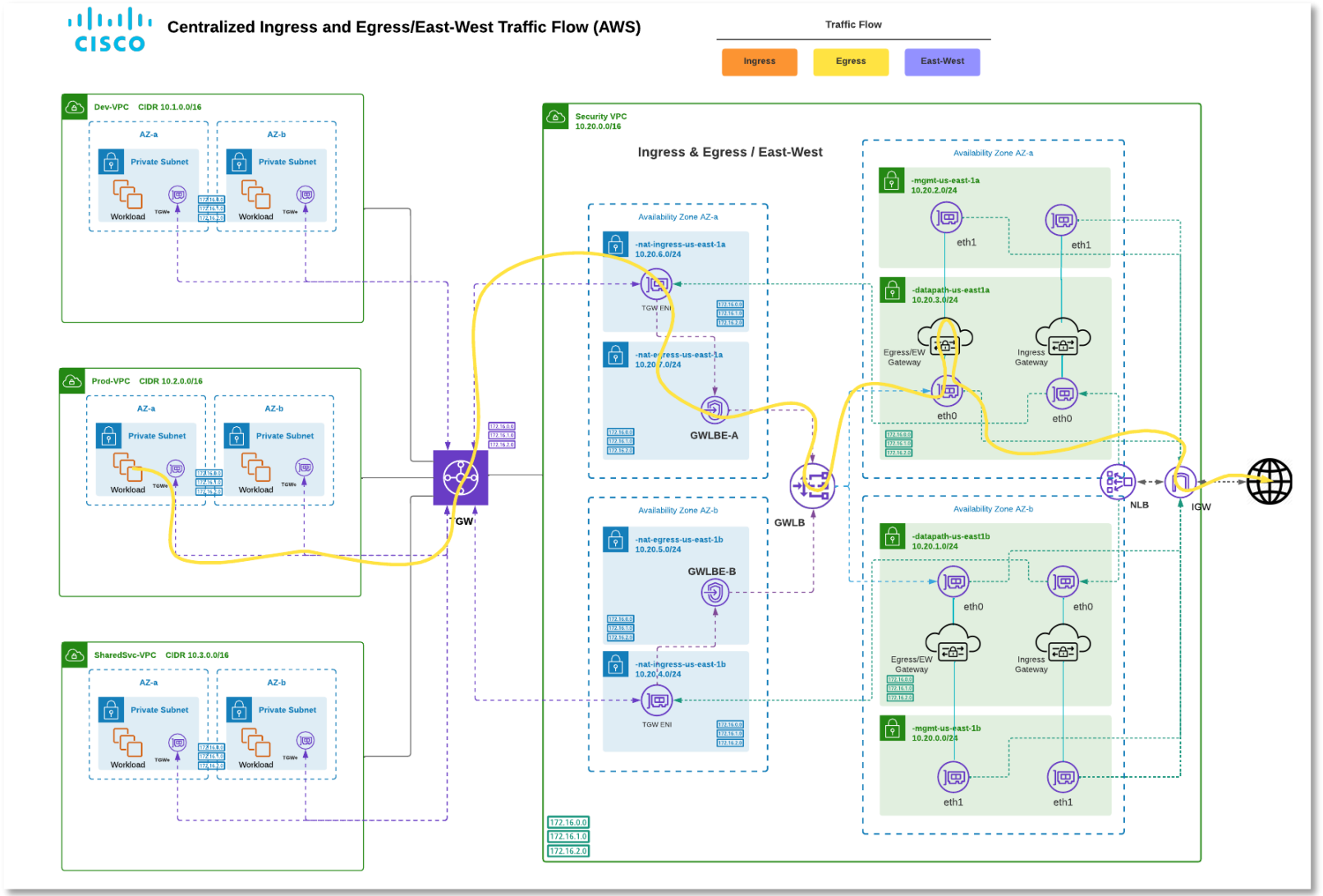
Network Load Balancer

Gateway Load Balancers

Multicloud Defense Gateways
(Deployment, Insertion, Autoscaling)

AWS Transit Gateways
(New or existing, TGW attachment)

VPC subnet routing to TGW



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

Cisco Multicloud Defense automates orchestration

What do we need to configure?

Security VPCs

VPC and DNS Flow Log capture

Gateway Load Balancers

Multicloud Defense Gateways

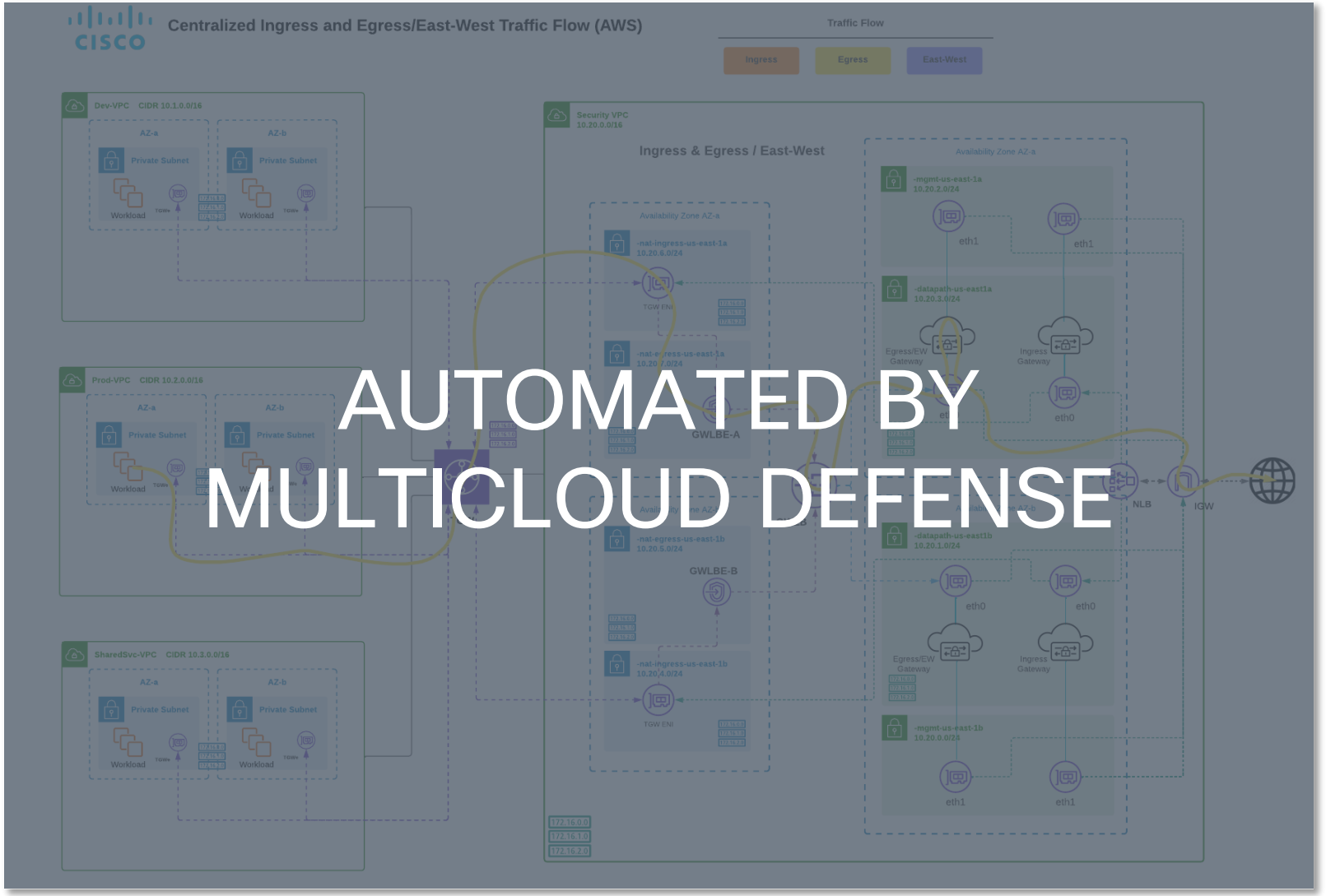
(Deployment, Insertion, Autoscaling)

AWS Transit Gateways

(New or existing, TGW attachment)

VPC subnet routing to TGW

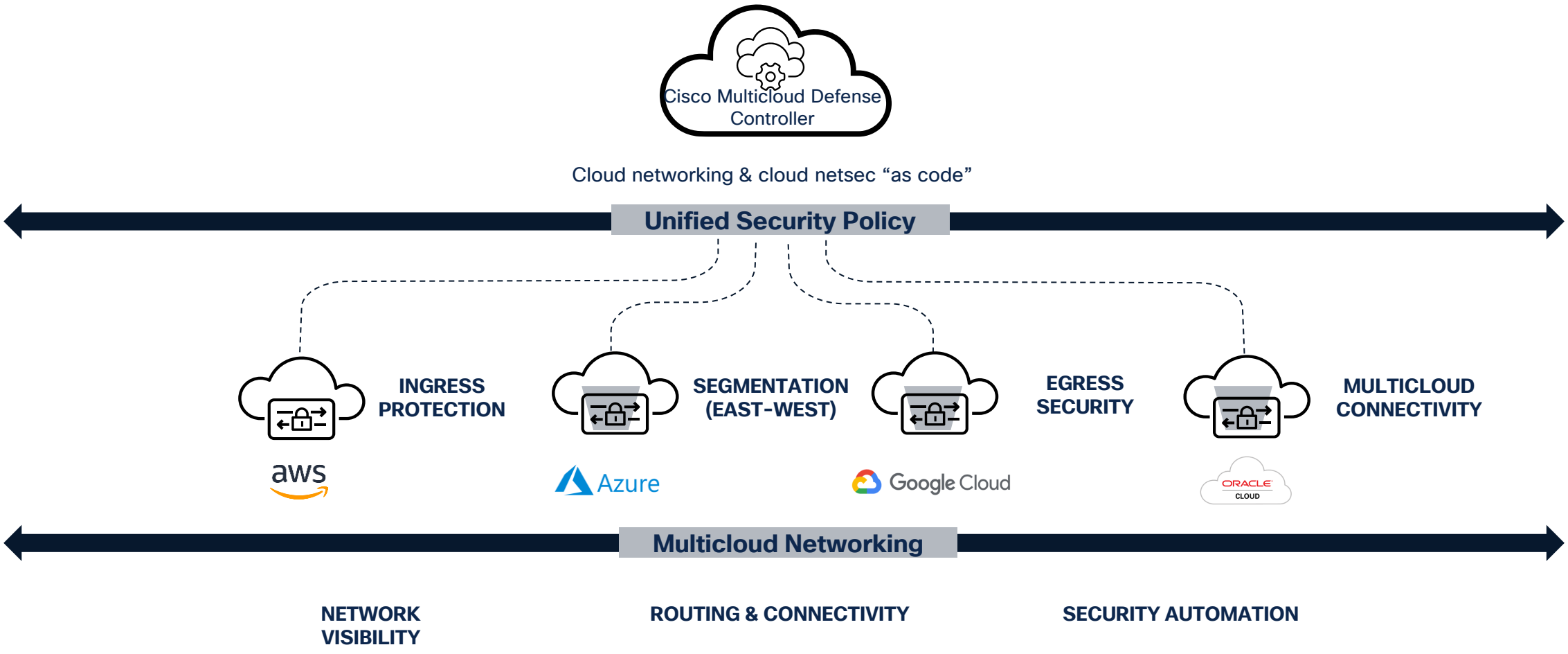
AUTOMATED BY MULTICLOUD DEFENSE



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

Cisco Multicloud Defense

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

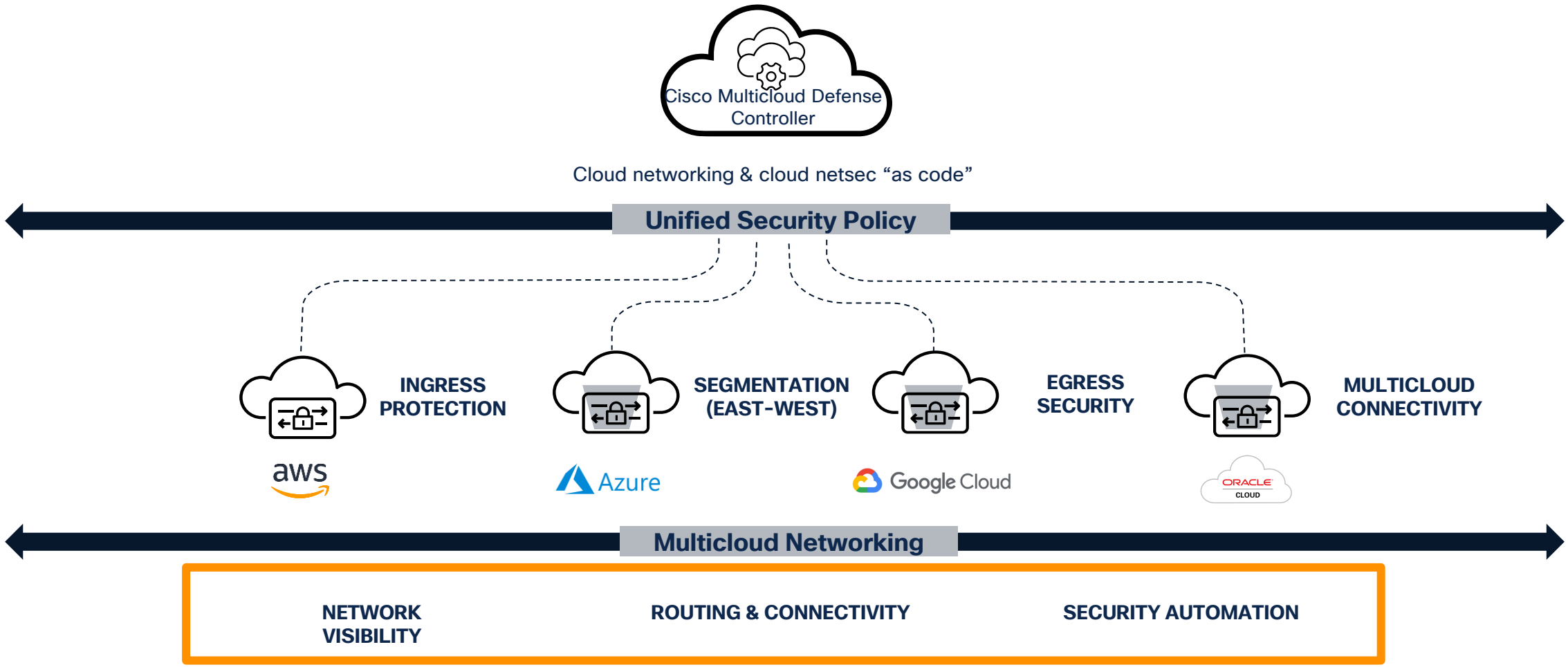


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Cisco Multicloud Defense

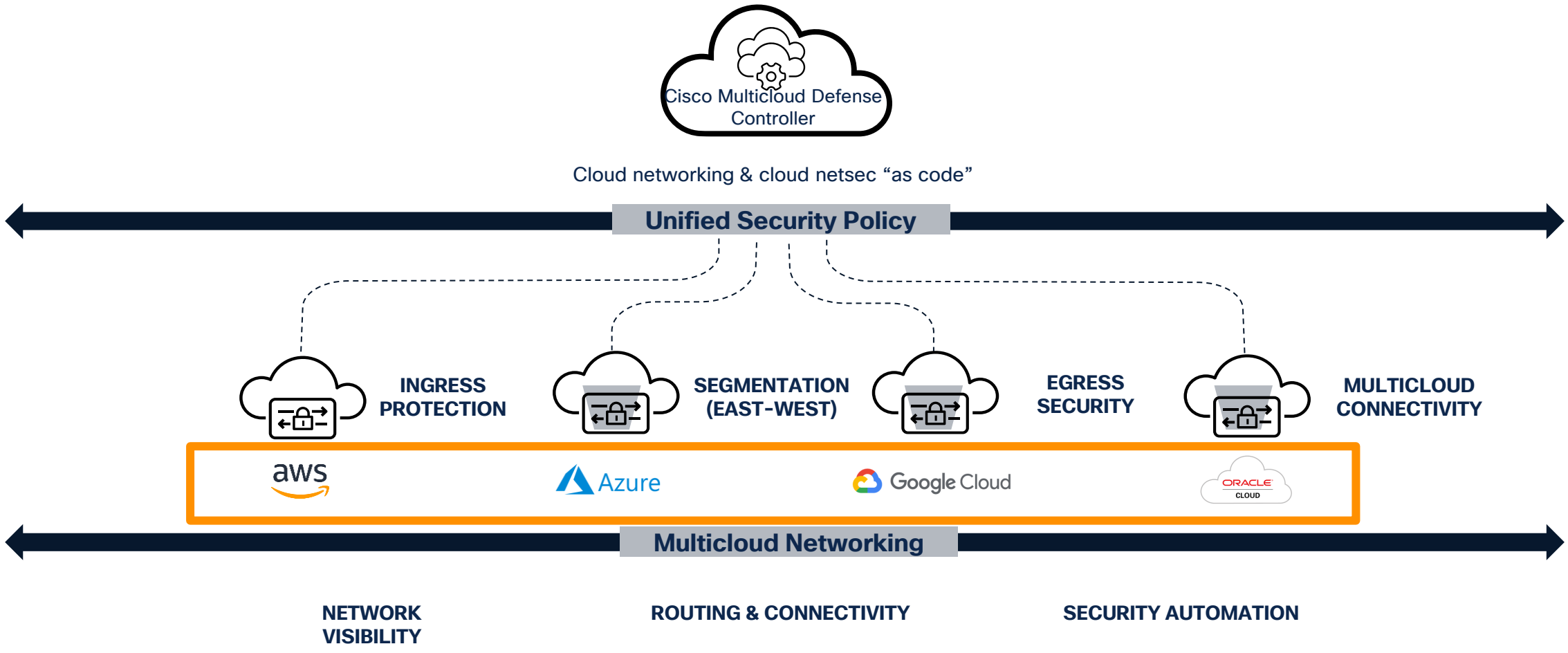
Combining multicloud networking, automation, and cloud-native network security controls



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

Cisco Multicloud Defense

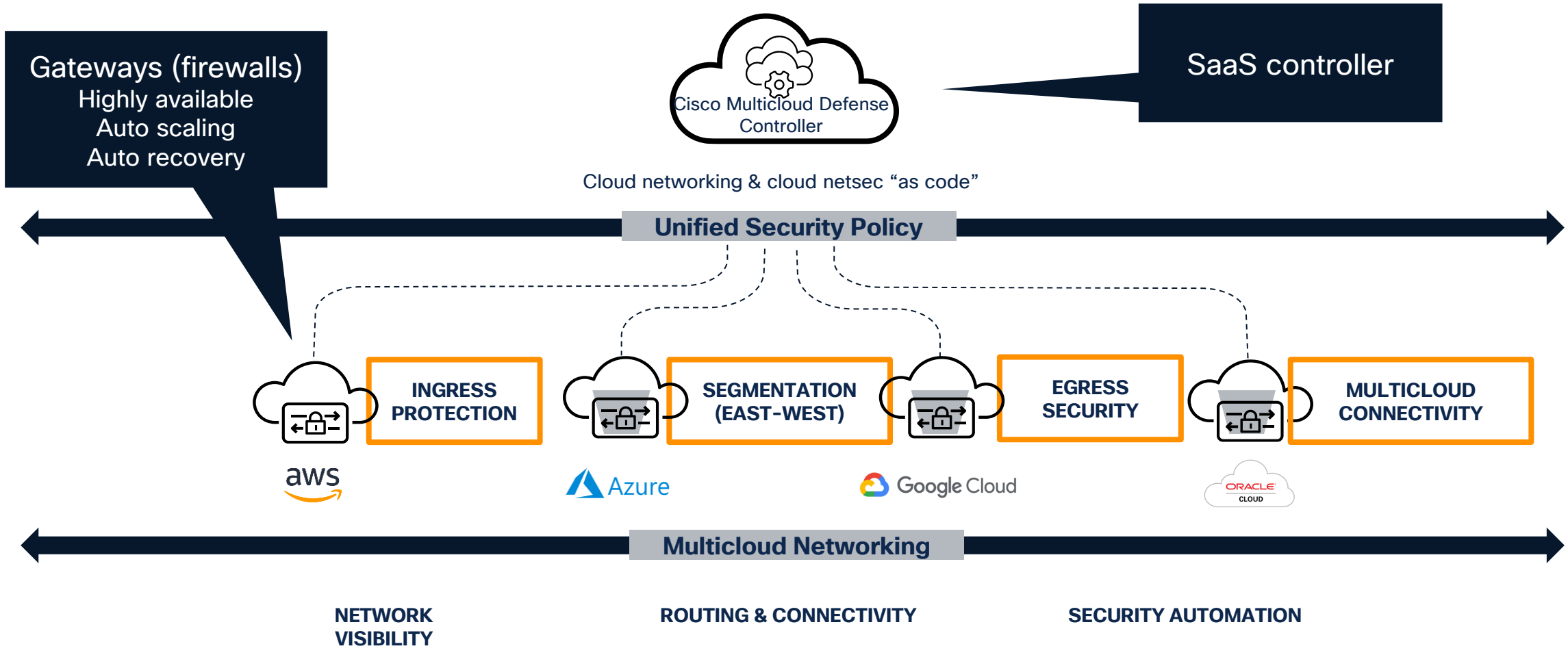
Combining multicloud networking, automation, and cloud-native network security controls



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

Cisco Multicloud Defense

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

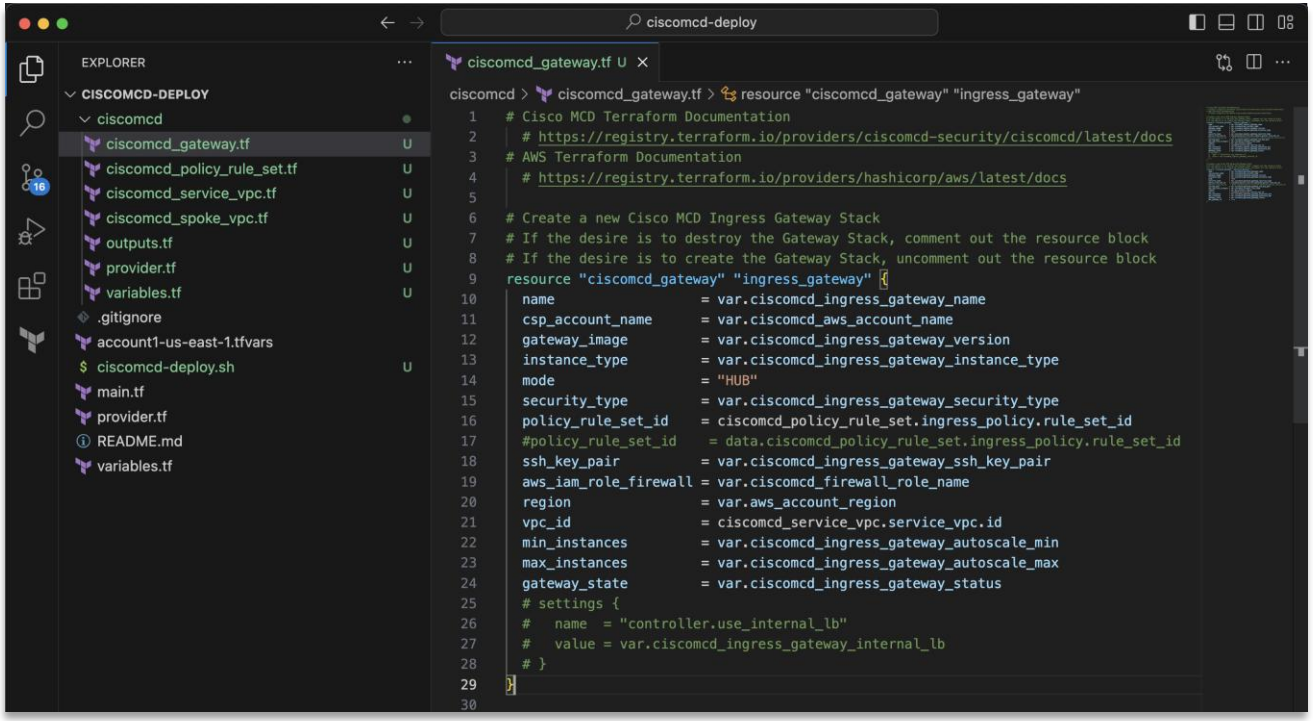


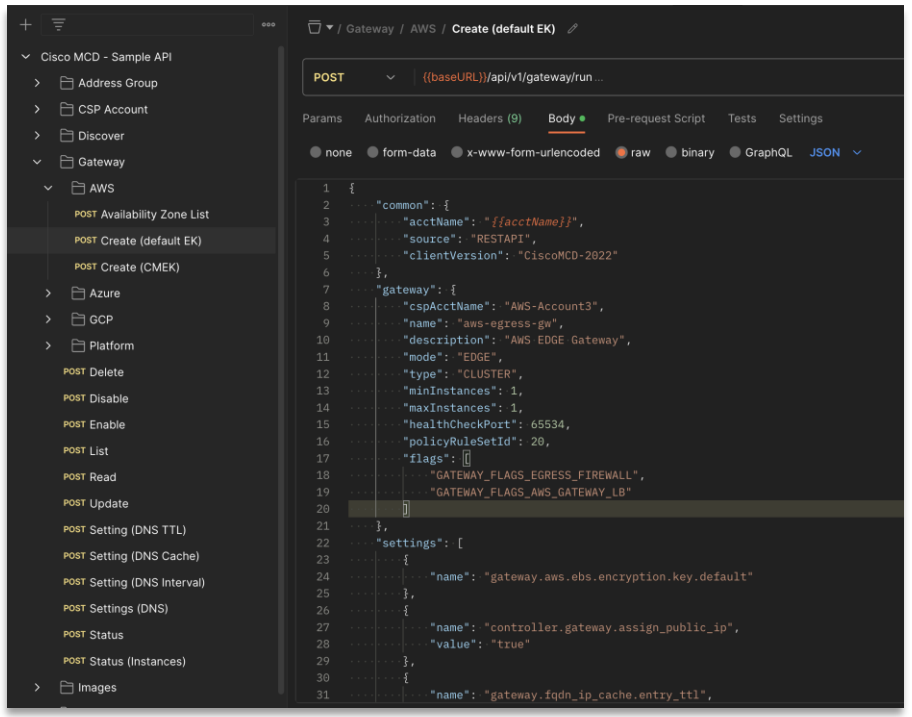
© 2025 Cisco and/or its affiliates. All rights reserved.

Fully Orchestrated

HashiCorp Terraform

{ REST:API }





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

cisco

Secure multicloud infrastructure in mins with Cisco Multicloud Defense

Step 1

Connect Account

Connect a cloud account with the Multicloud Defense Controller

Connect Account

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

Step 3

Secure Your Account

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

Secure Account

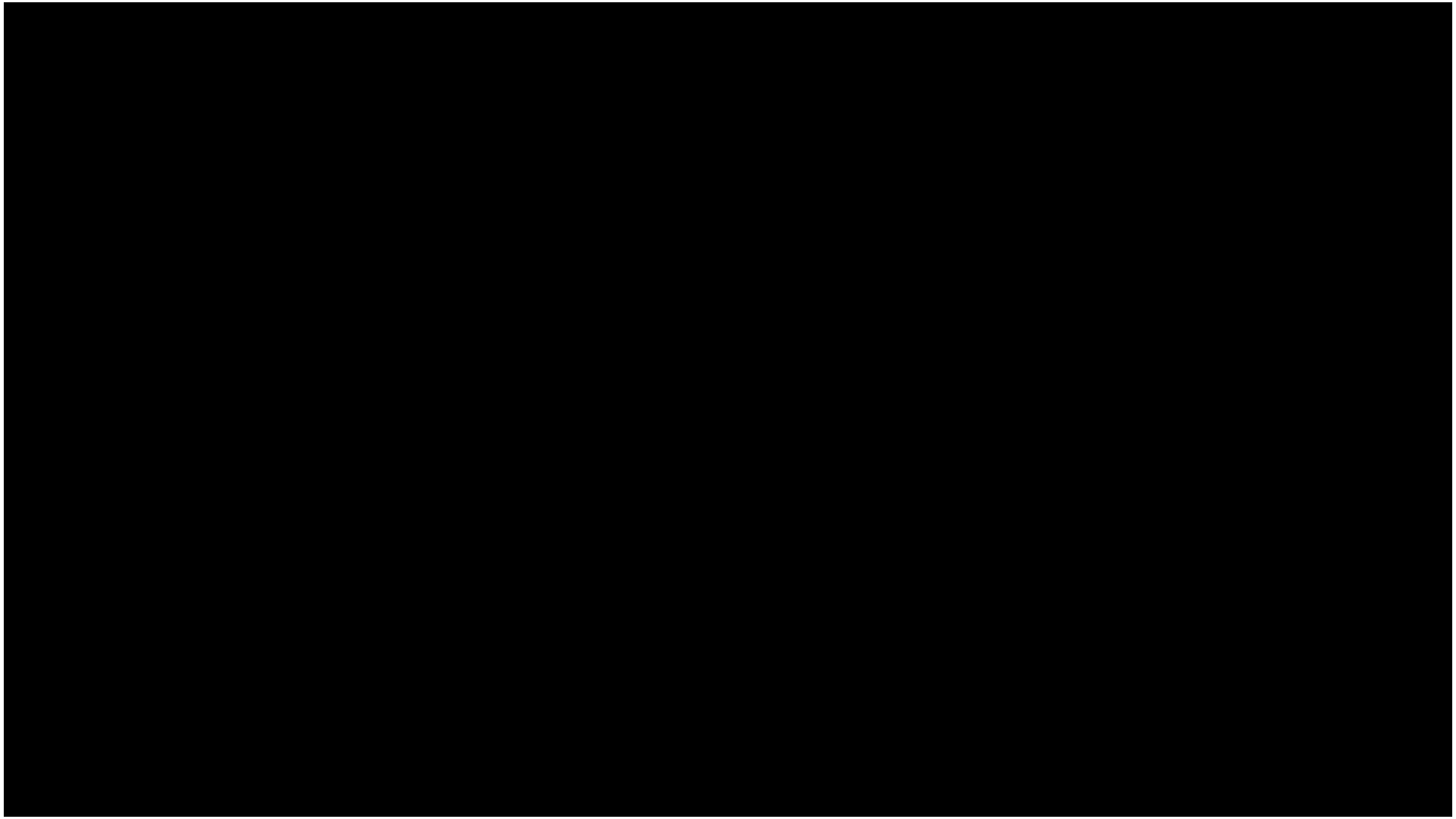
Securely onboard Cloud accounts

Enable DNS query & VPC/NSG flow logs

Orchestration and Automation

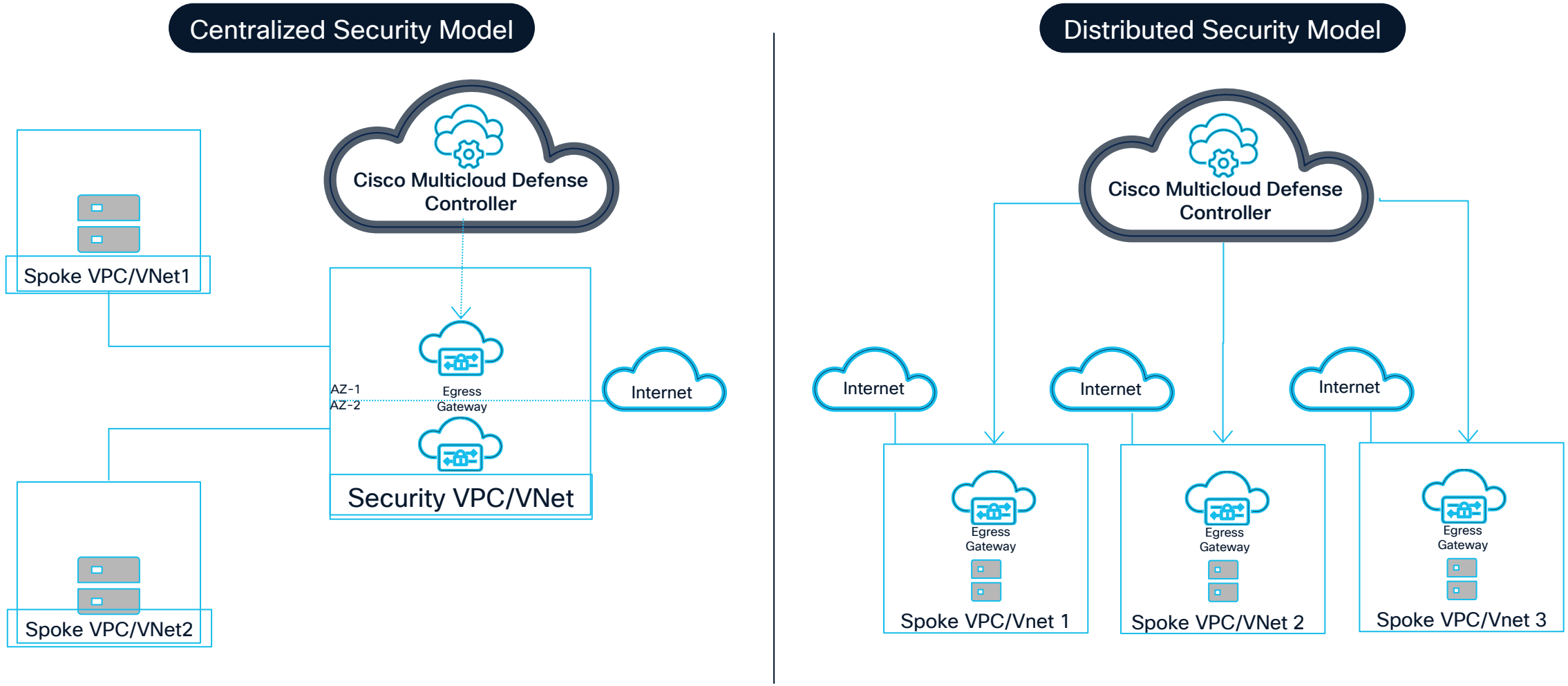
© 2025 Cisco and/or its affiliates. All rights reserved.

Multicloud Defense Demo



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

Deployment Models



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

Centralized Security Model

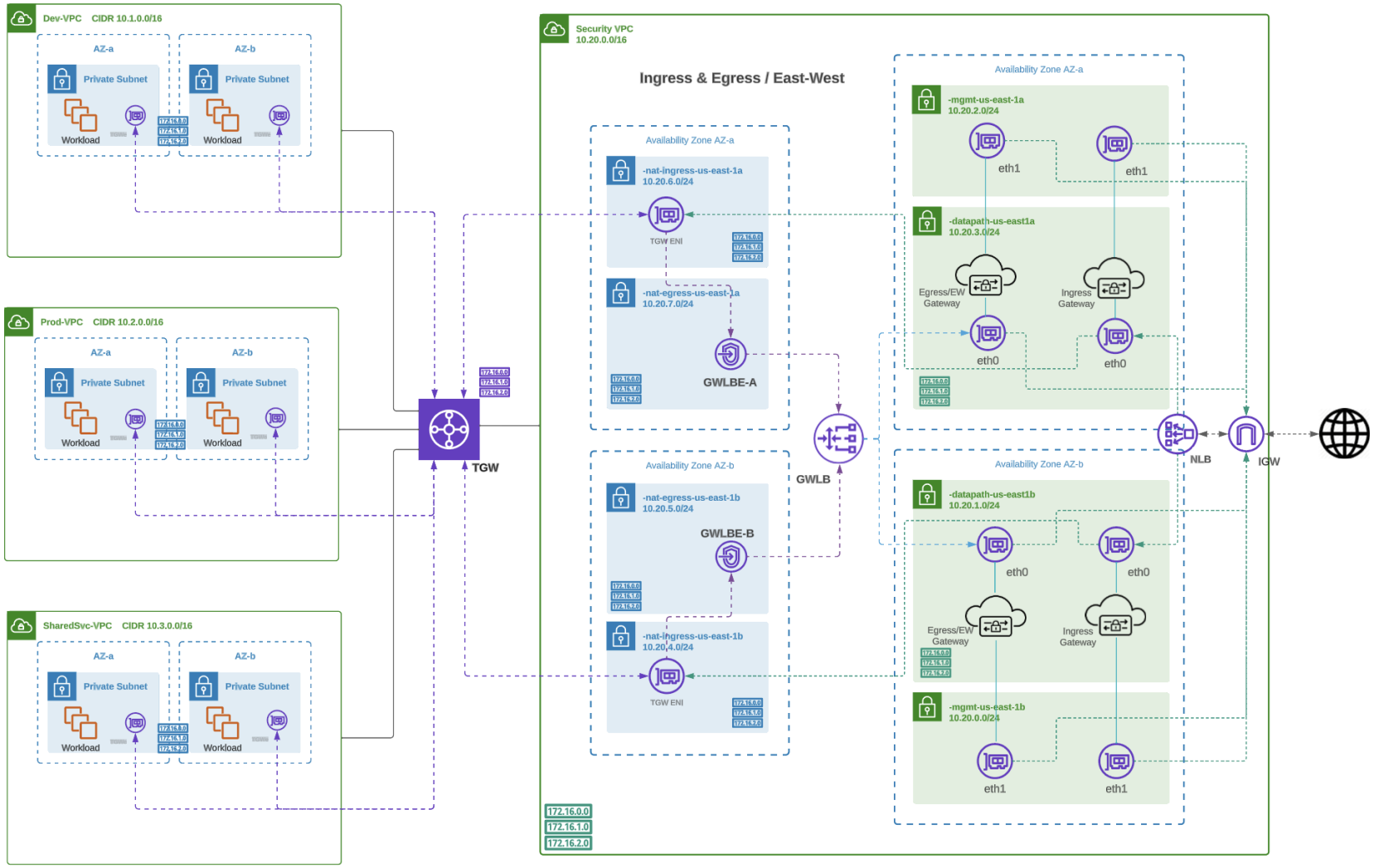
Amazon Web Services

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



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

Centralized Security Model – Egress Traffic

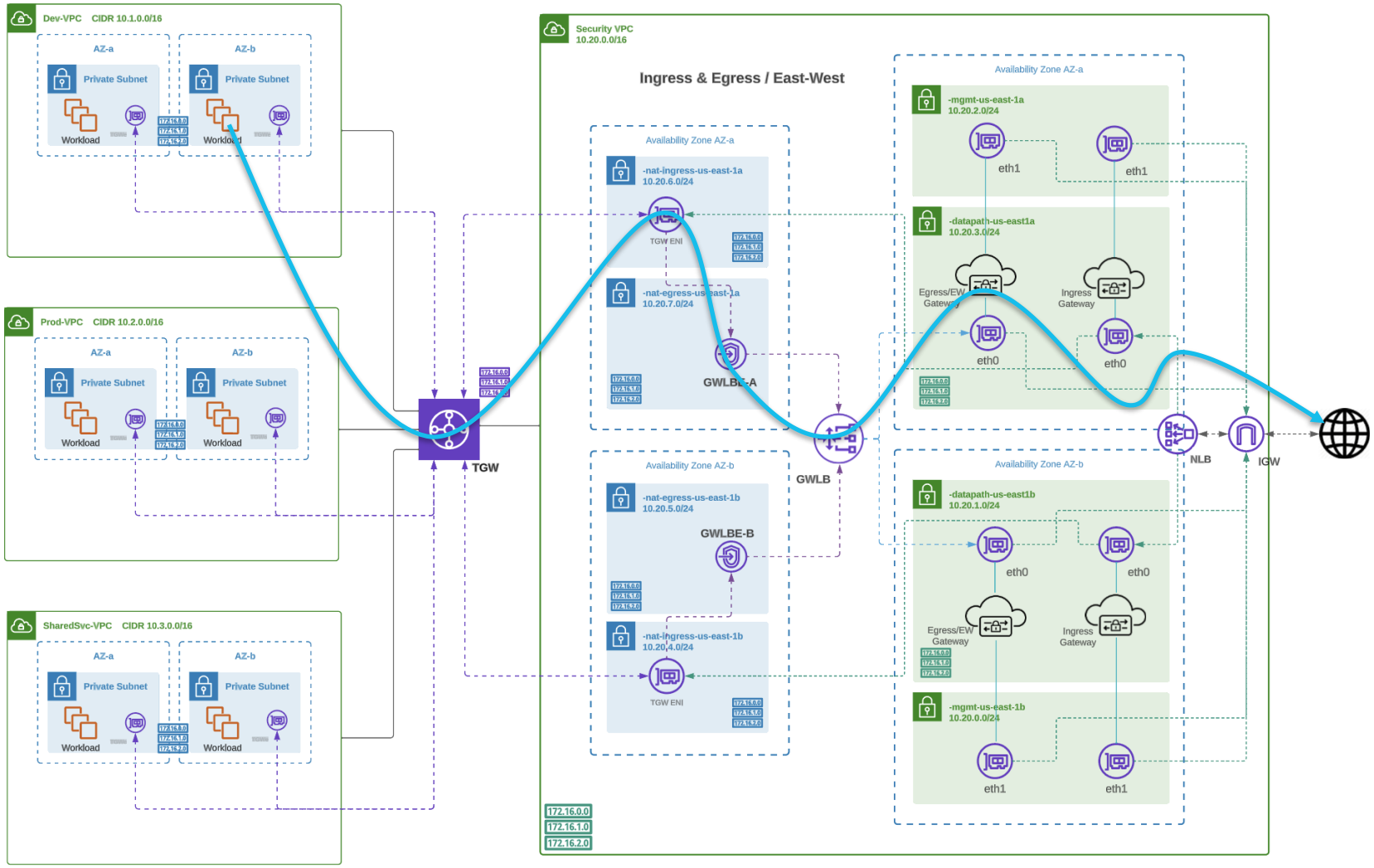
Amazon Web Services

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



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

Centralized Security Model – Ingress Traffic

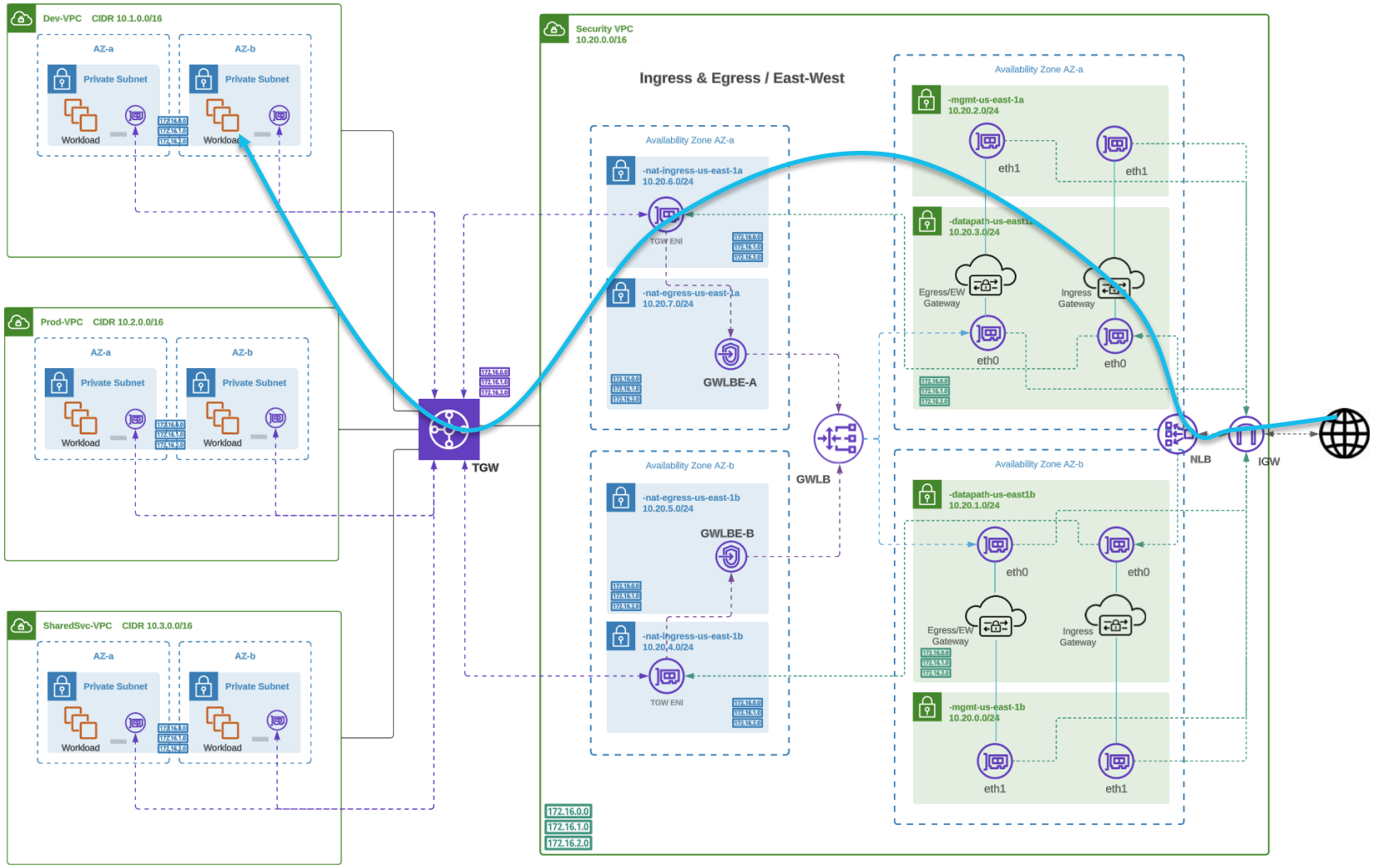
Amazon Web Services

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



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

Centralized Security Model _ East/West Segmentation

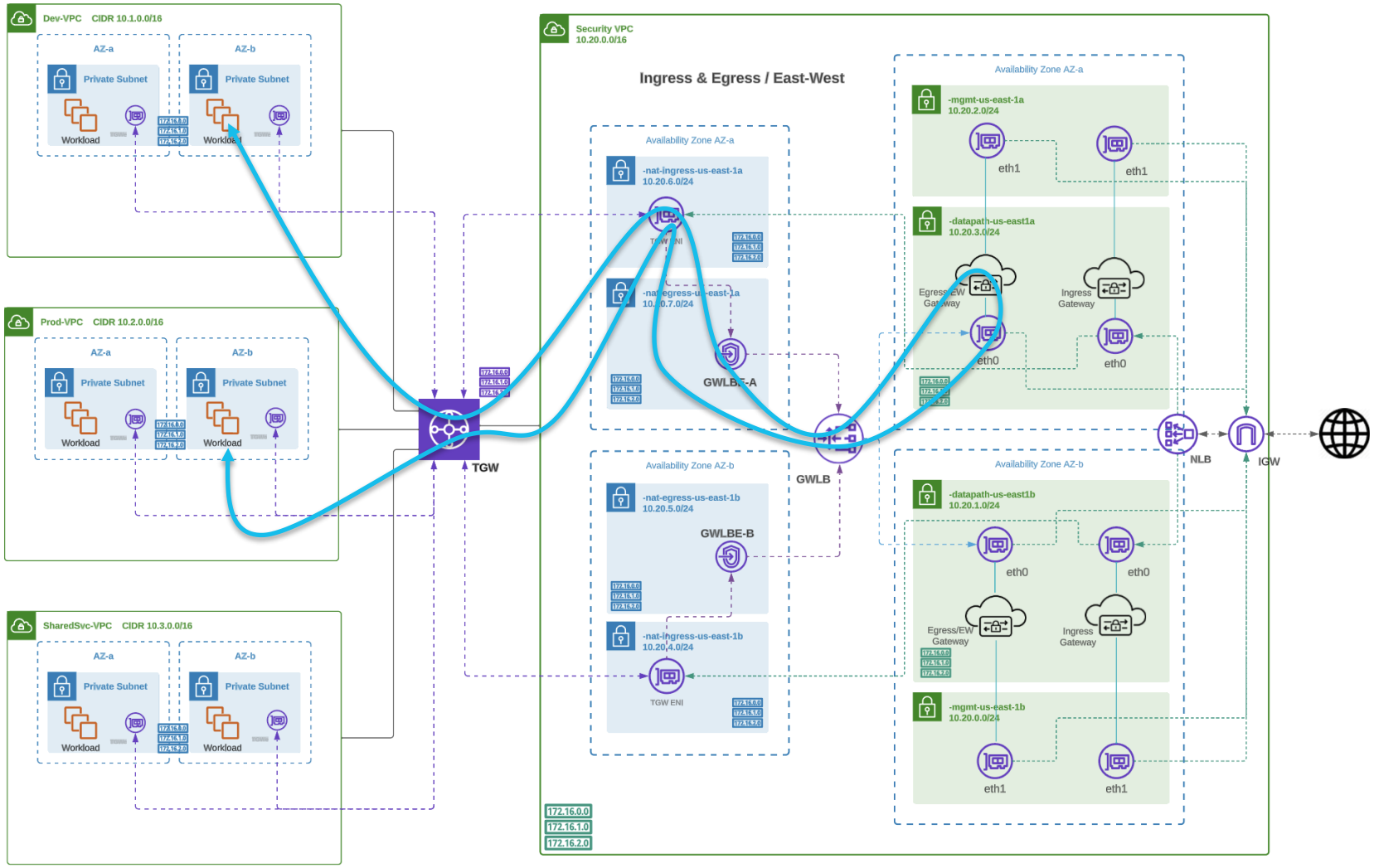
Amazon Web Services

Orchestration

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

Lifecycle management

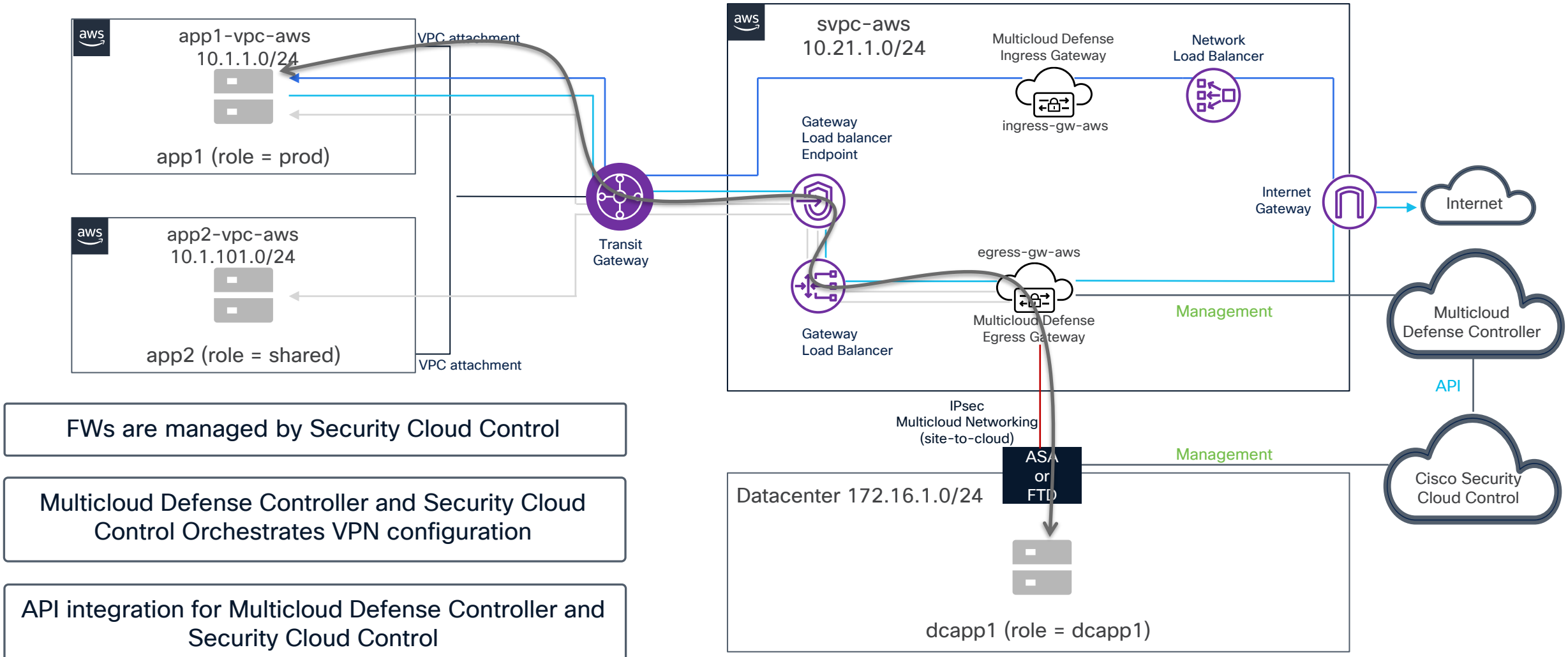
Ingress and Egress Gateway



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

Multicloud Networking

Site-to-cloud connectivity: Centralized Security Model



FWs are managed by Security Cloud Control

Multicloud Defense Controller and Security Cloud Control Orchestrates VPN configuration

API integration for Multicloud Defense Controller and Security Cloud Control

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

But I use FTD on Prem...

Secure Firewall Threat Defense Virtual

Private Cloud

HyperFlex
NUTANIX
KVM
openstack
vmware ESXi

Public Cloud

aws
Google Cloud Platform
Microsoft Azure
rackspace technology
ORACLE CLOUD INFRASTRUCTURE
EQUINIX
Alibaba Cloud
alkira

Gov/IC Cloud

aws
Microsoft Azure
Google Cloud Platform

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

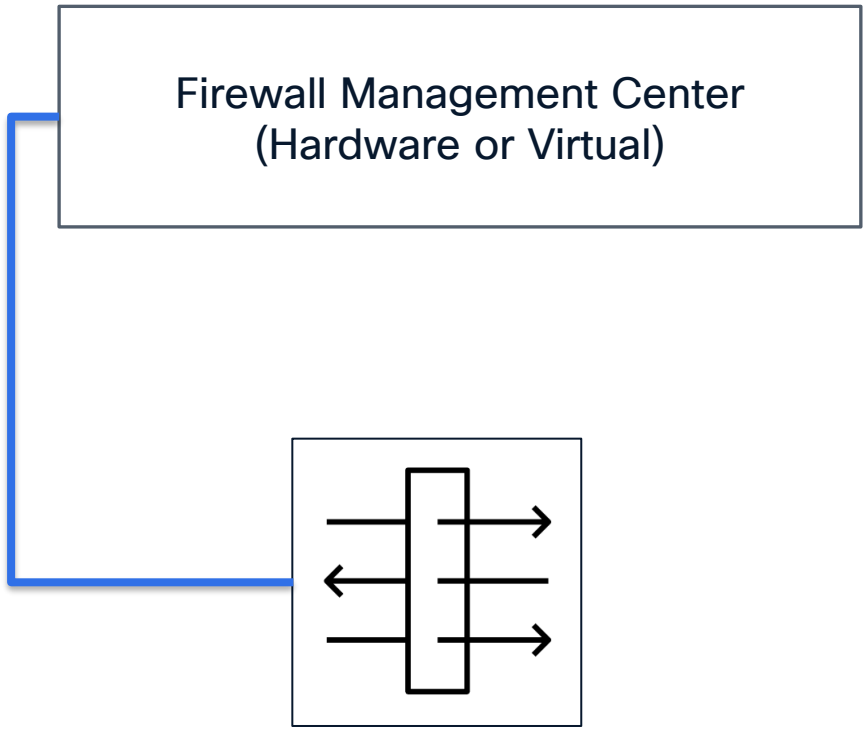
FTDv5 (100Mbps), FTDv10 (1 Gbps), FTDv20 (3 Gbps), FTDv30 (5 Gbps), FTDv50 (10 Gbps), and FTDv100 (16 Gbps)

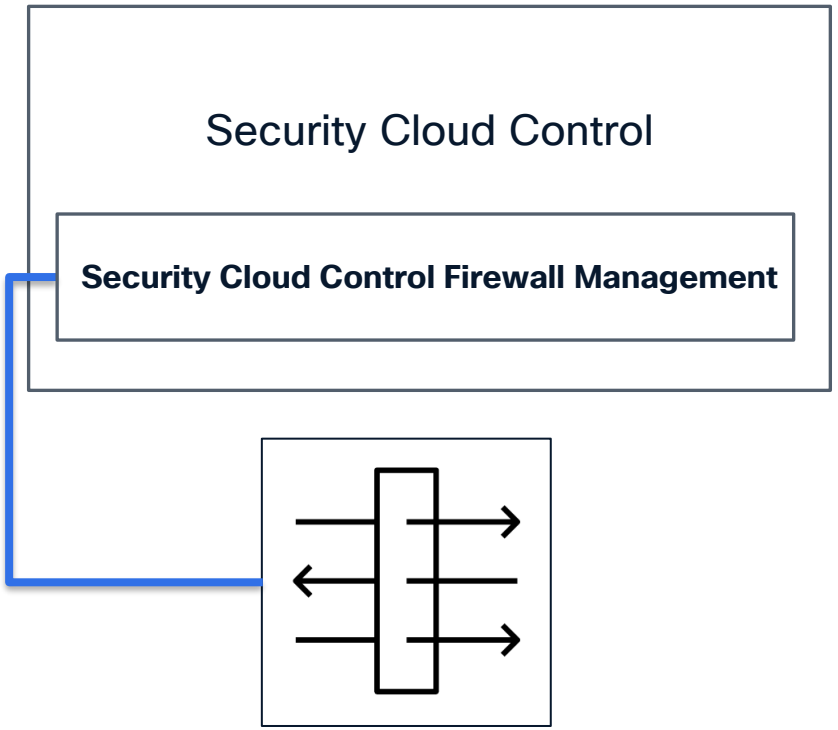
Cloud Leadership

- 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

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

Firewall Management

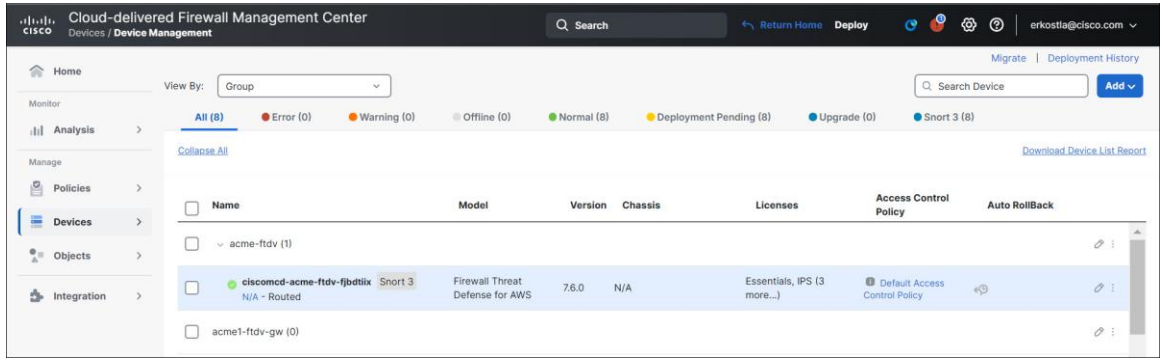




© 2025 Cisco and/or its affiliates. All rights reserved.

Secure Firewall Threat Defense Virtual orchestrated by Multicloud Defense Controller

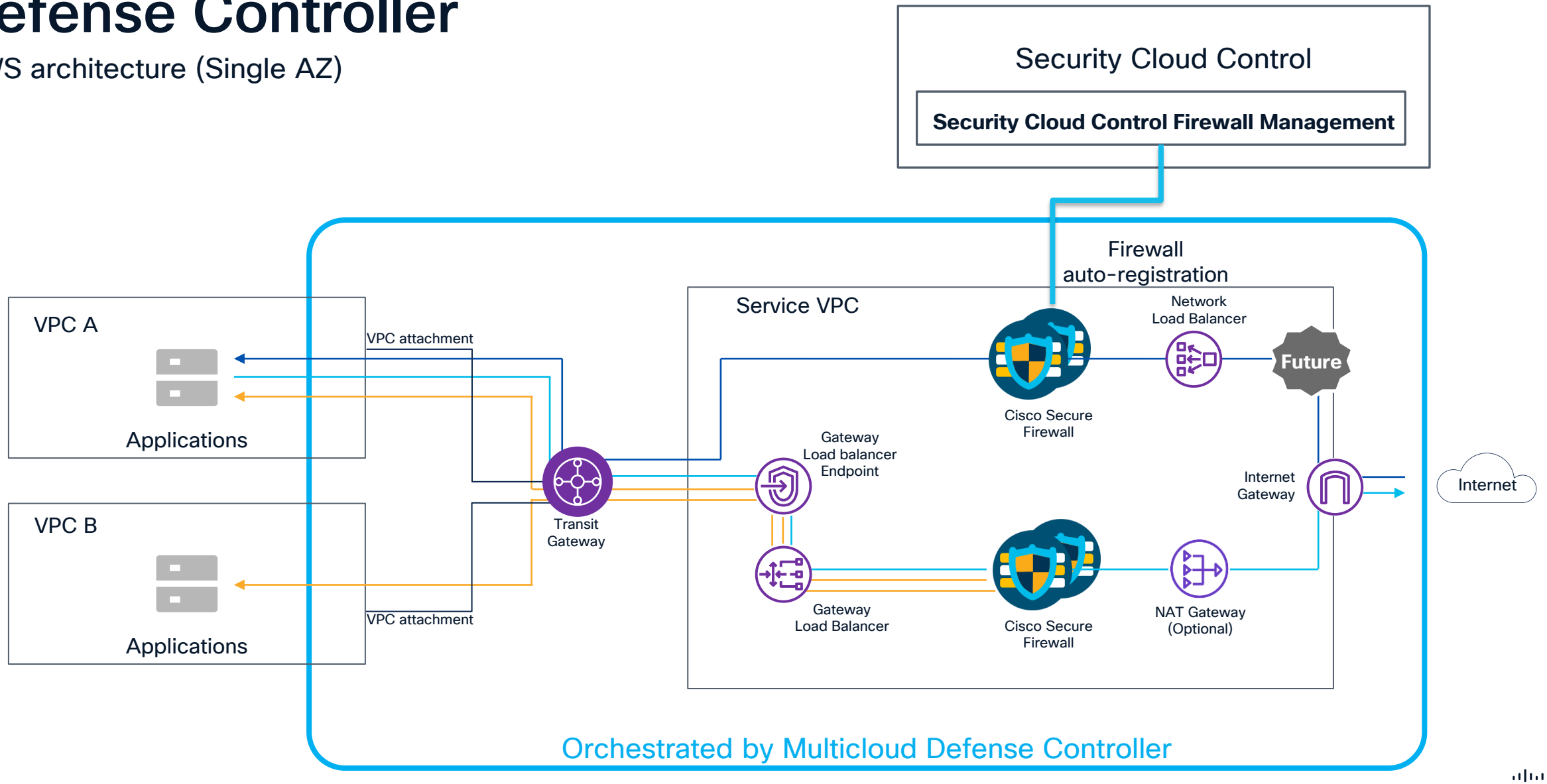
- Simplifies Secure Firewall (FTDv) deployment
  - Deploy one or more firewalls, along with load balancers
  - Configures all necessary routing
  - Identical workflow for all public cloud providers
- Simplifies Secure Firewall (FTDv) operations
  - Automatically scales in or out FTDv's to adjust to load
  - 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



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

Cisco Secure Firewall Virtual Orchestrated by Multicloud Defense Controller

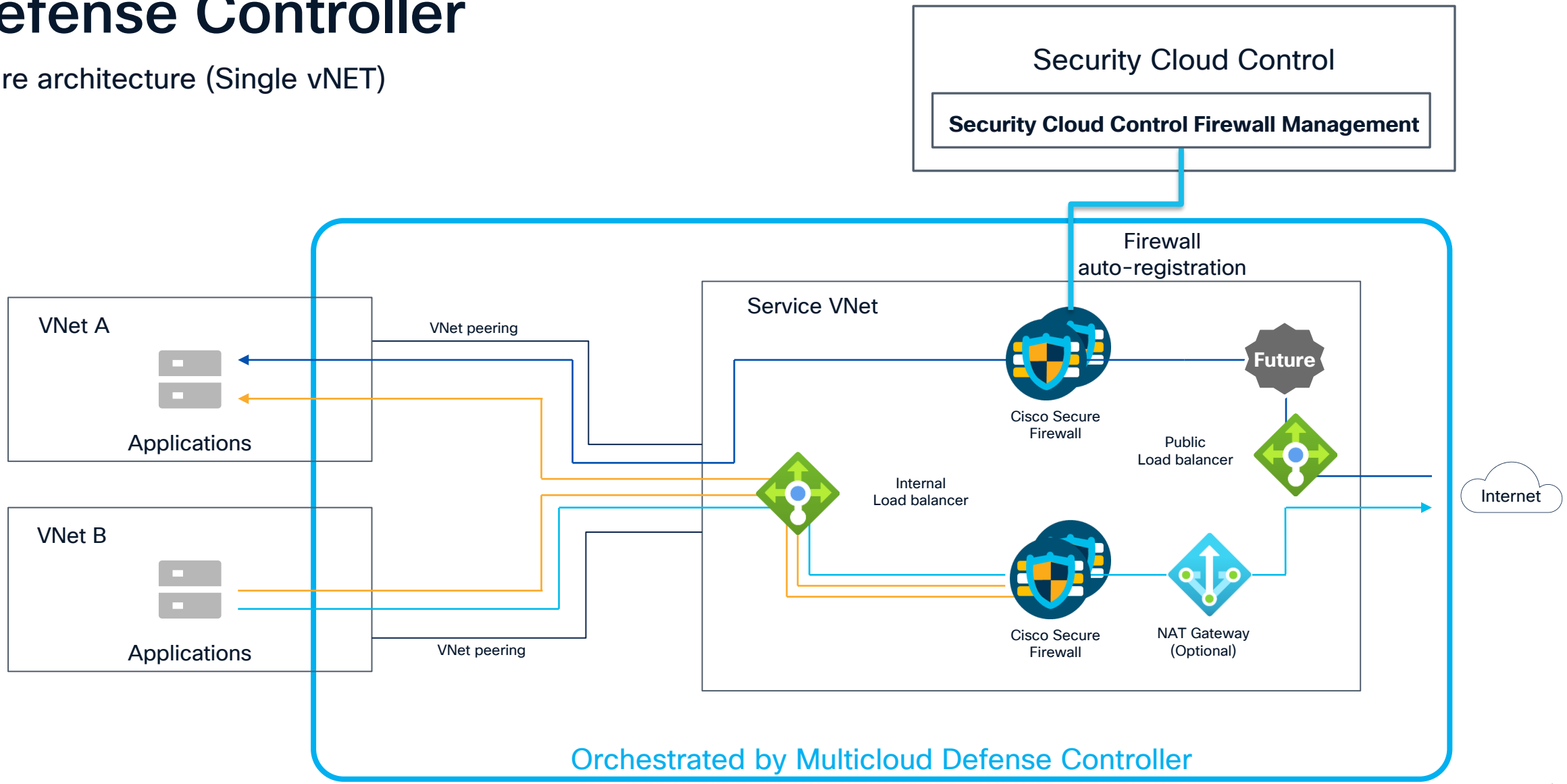
AWS architecture (Single AZ)



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

Cisco Secure Firewall Virtual Orchestrated by Multicloud Defense Controller

Azure architecture (Single vNET)

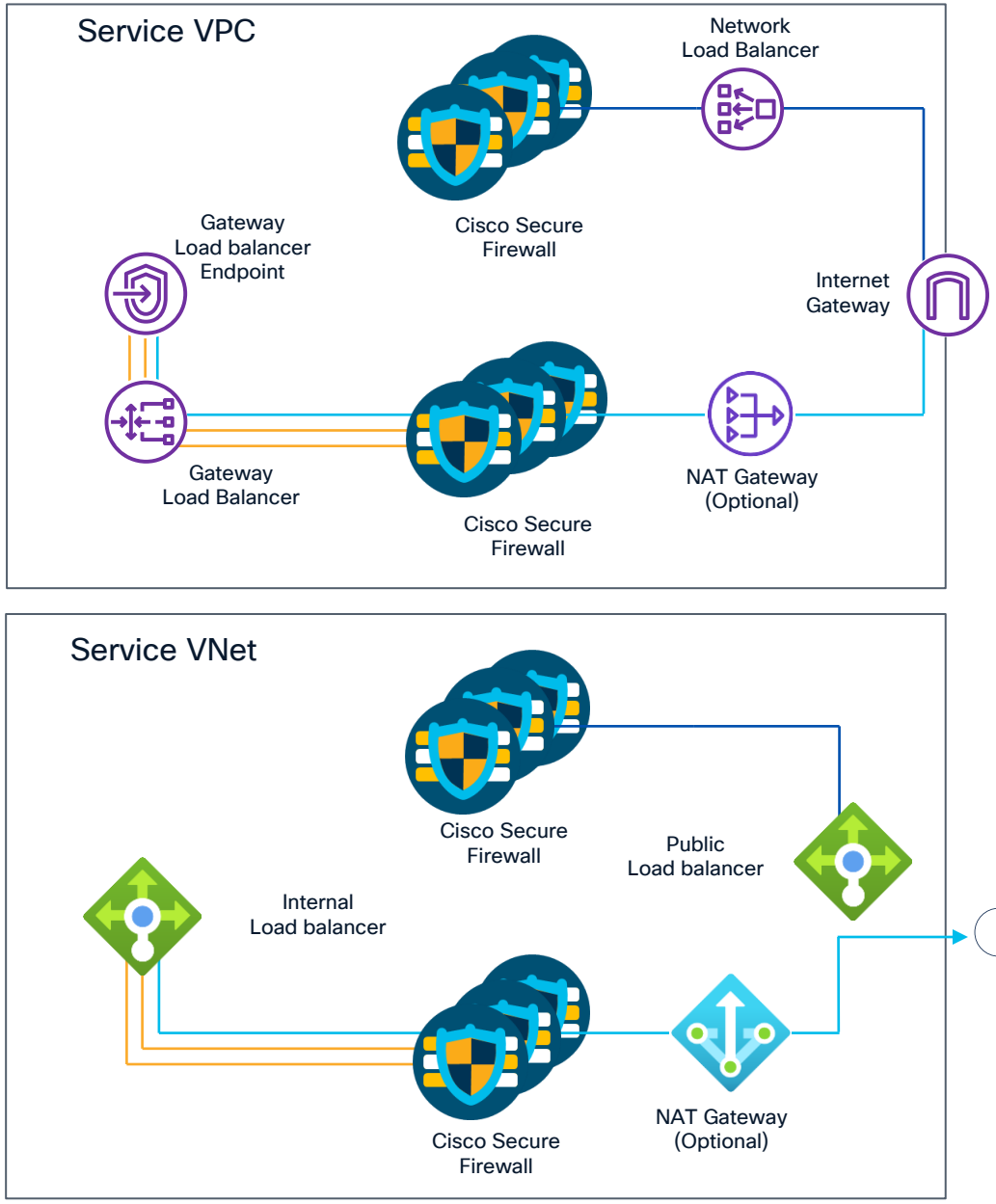


© 2025 Cisco and/or its affiliates. All rights reserved.

Autoscaling

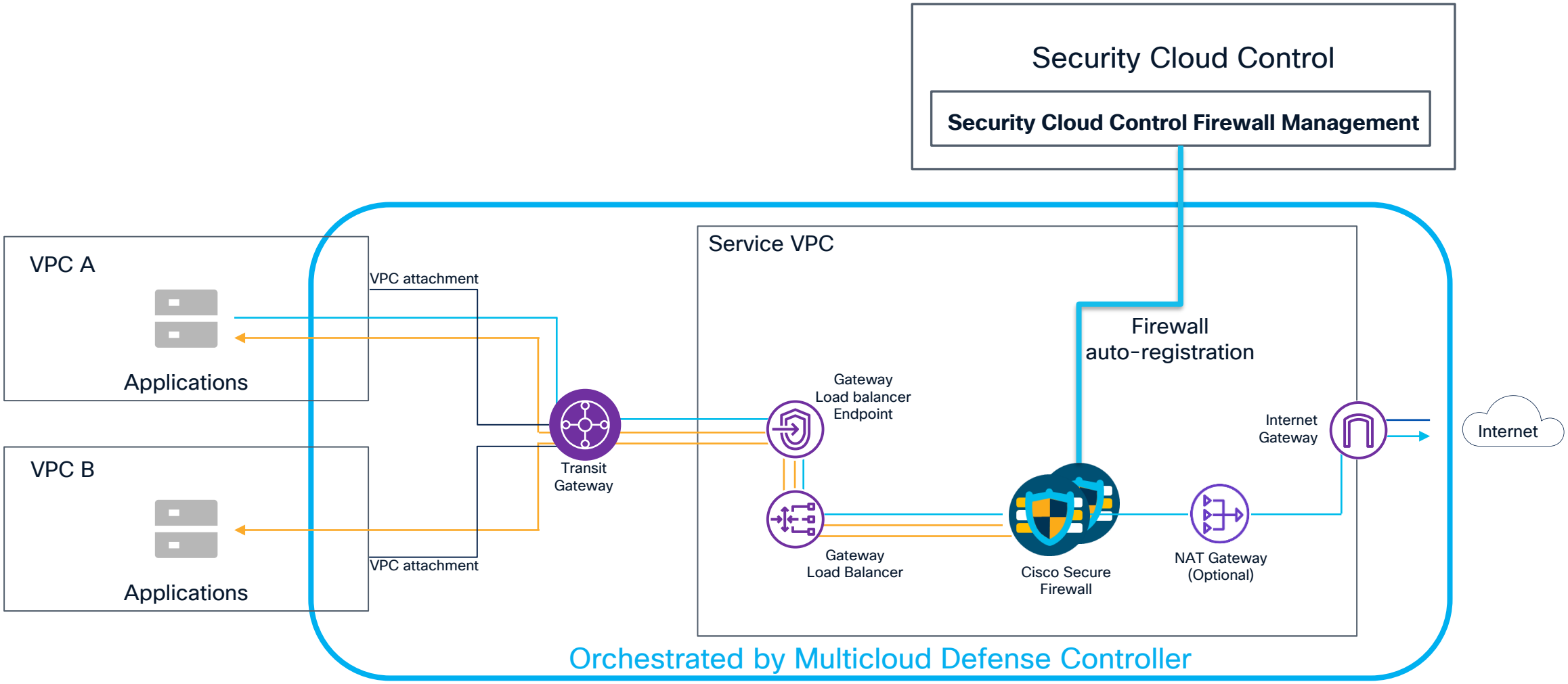
Multicloud Defense controller handles autoscaling of FTDv

- 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**

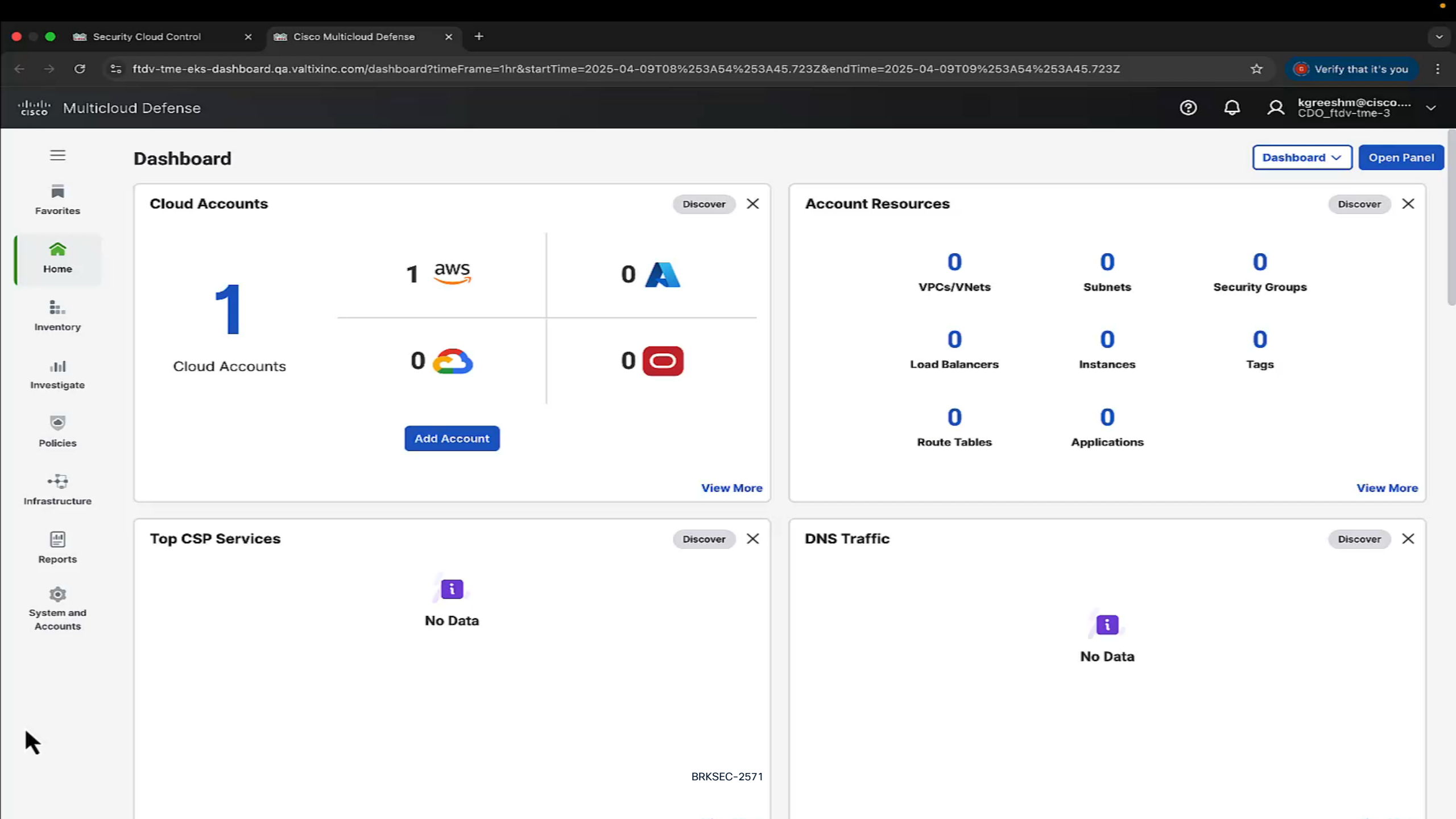


© 2025 Cisco and/or its affiliates. All rights reserved.

Secure Firewall Orchestration by Multicloud Defense Demo



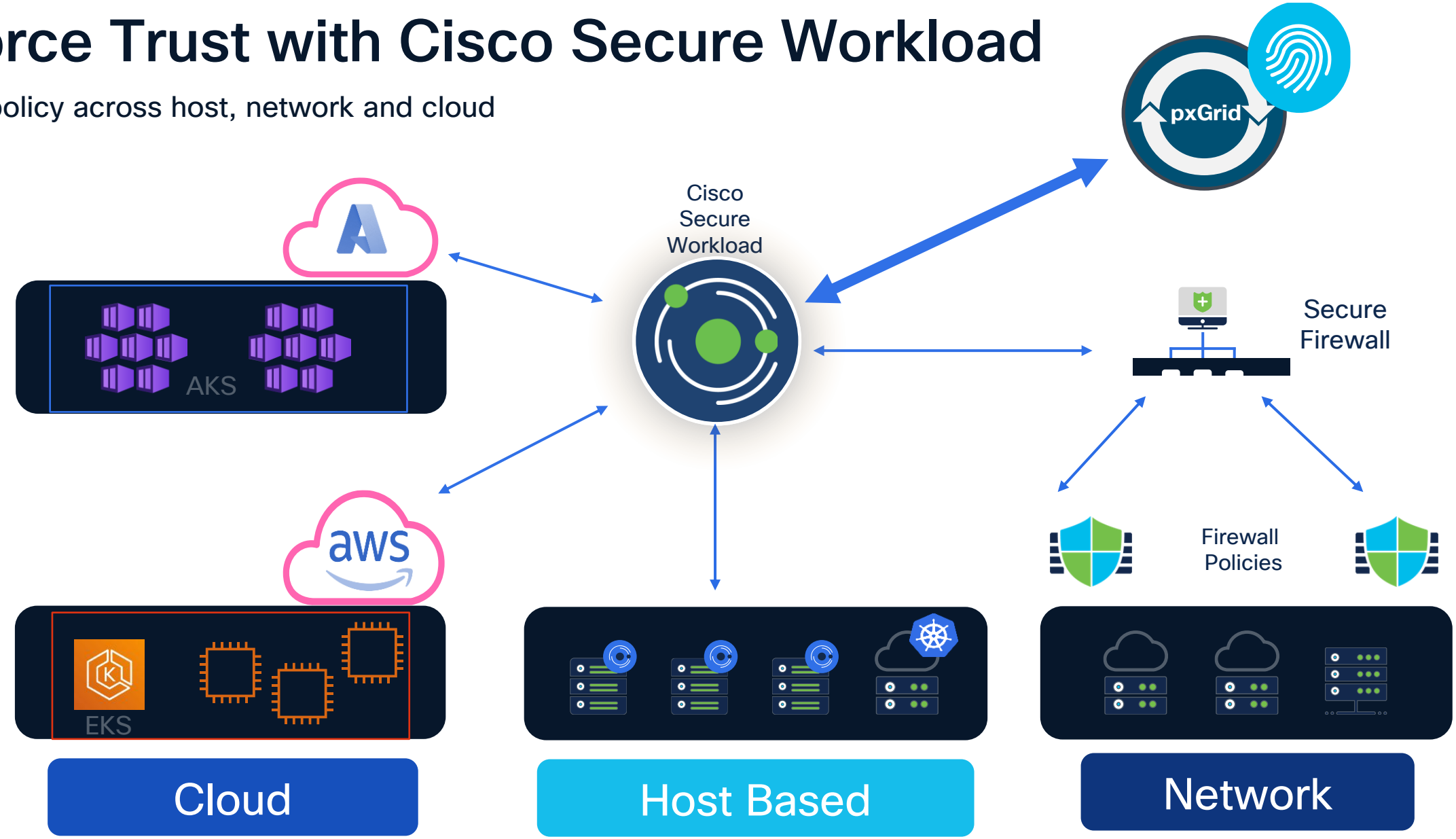
© 2025 Cisco and/or its affiliates. All rights reserved.


Security Cloud Control
Cisco Multicloud Defense
ftdv-tme-eks-dashboard.qa.valtixinc.com/dashboard?timeFrame=1hr&startTime=2025-04-09T08%253A54%253A45.723Z&endTime=2025-04-09T09%253A54%253A45.723Z
Verify that it's you
Multicloud Defense
kgreeshm@cisco....
CDO_ftdv-tme-3
Favorites
Home
Inventory
Investigate
Policies
Infrastructure
Reports
System and Accounts
Dashboard
Dashboard
Open Panel
Cloud Accounts
Discover
1
Cloud Accounts
1 aws
0
0
0
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
DNS Traffic
Discover
No Data
BRKSEC-2571

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

Enforce Trust with Cisco Secure Workload

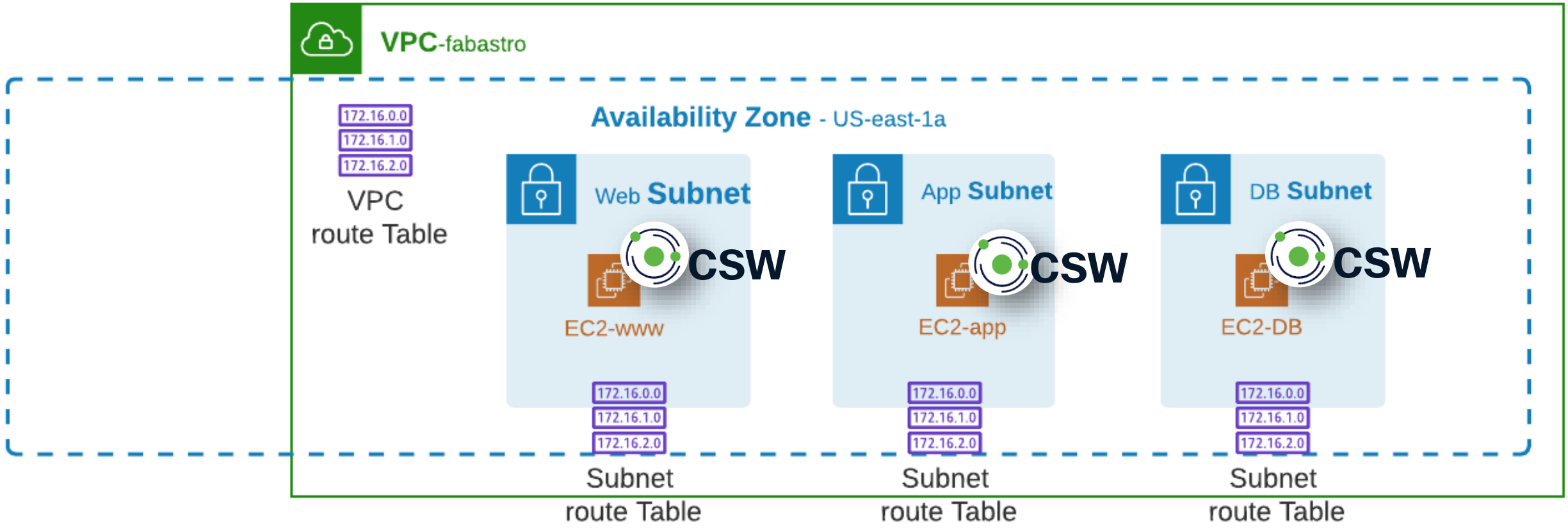
Unified policy across host, network and cloud



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

Improving Security in IaaS Model

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

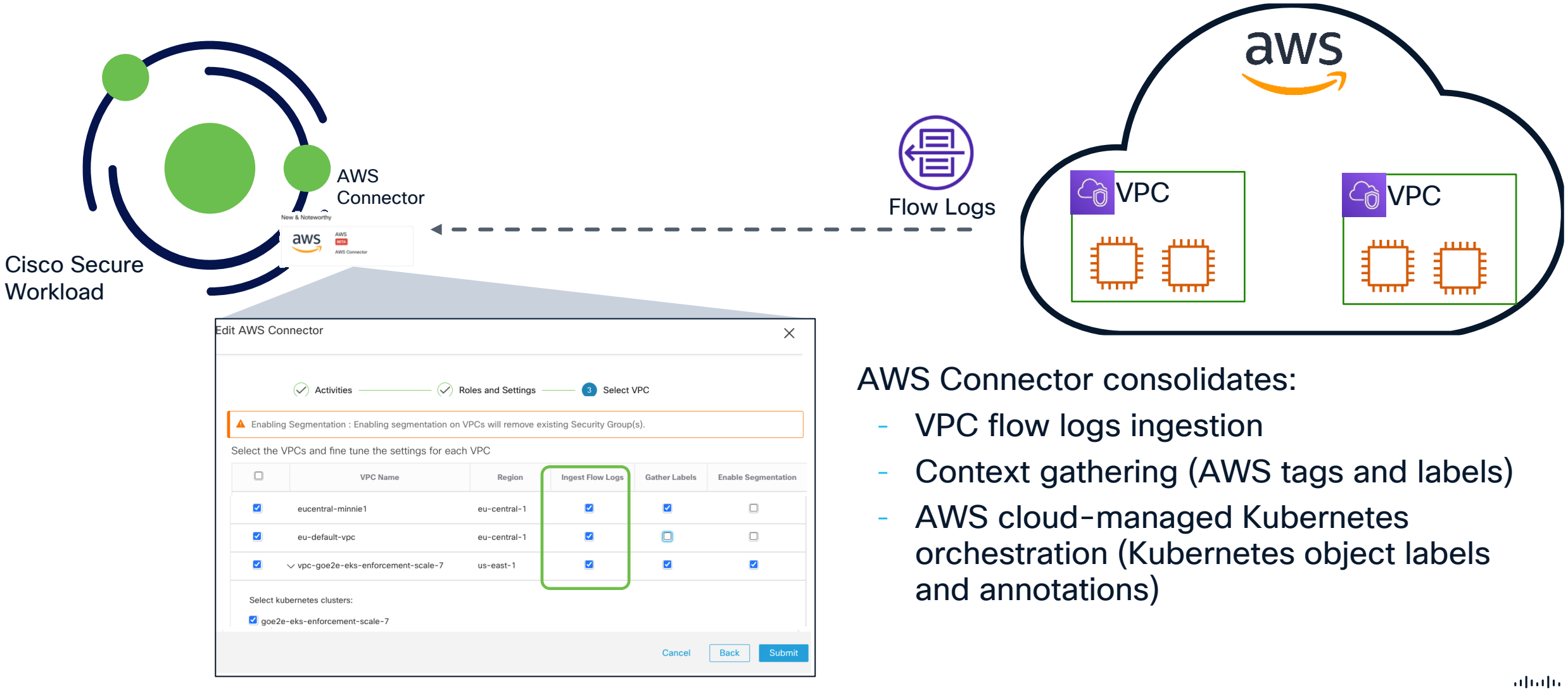


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

No big fan of using agents ?

Cisco Secure Workload Cloud-Based Sources



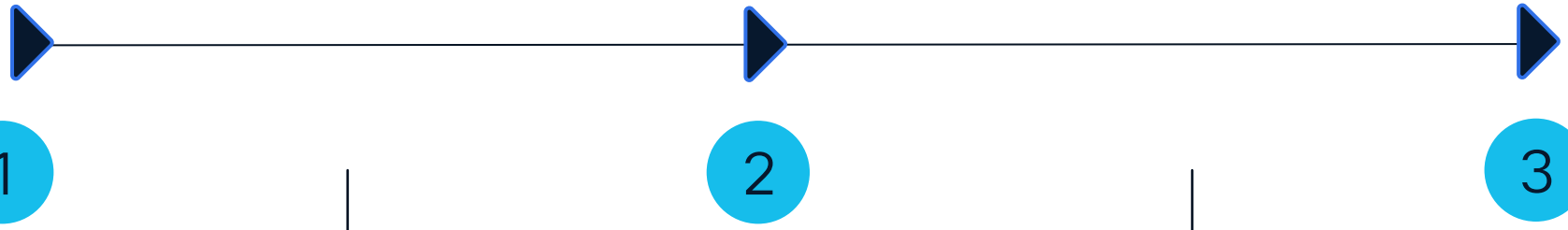
AWS Connector consolidates:

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

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

AWS Connector

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



1

Enable cloud connector and select the required **capabilities**

2

Download and **deploy** the **CloudFormation**, add the AWS API **credentials to** Secure Workload.

3

Select the AWS **VPCs** and refine the required **capabilities** for each VPC.

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

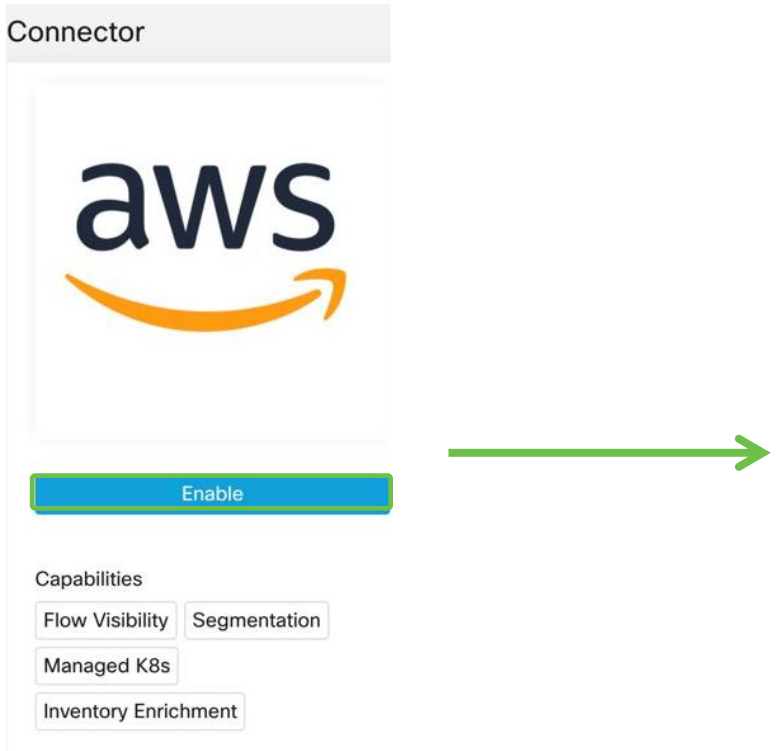
cisco

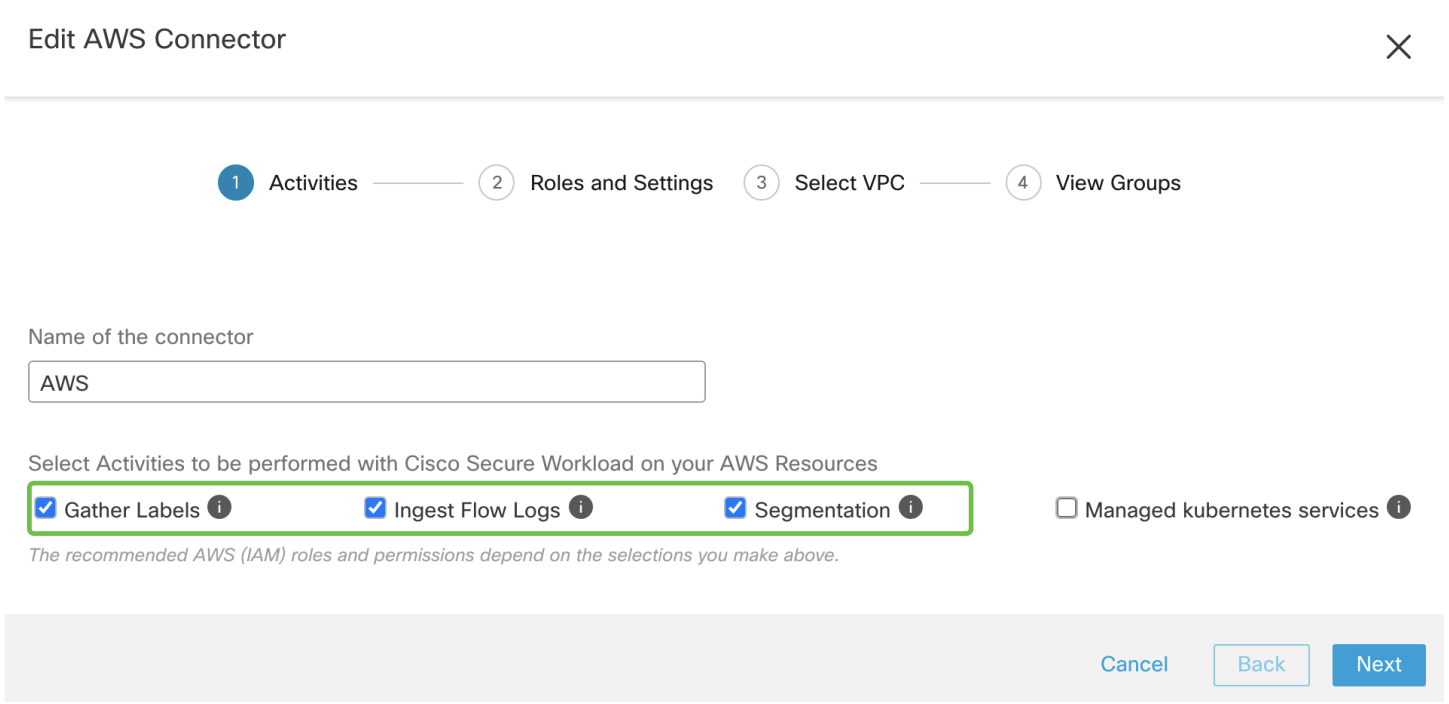
AWS Connector – Select Capabilities

Cisco Live 2022 FOR REFERENCE TECSEC-2711

1

Enable and configure the connector capabilities





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

cisco

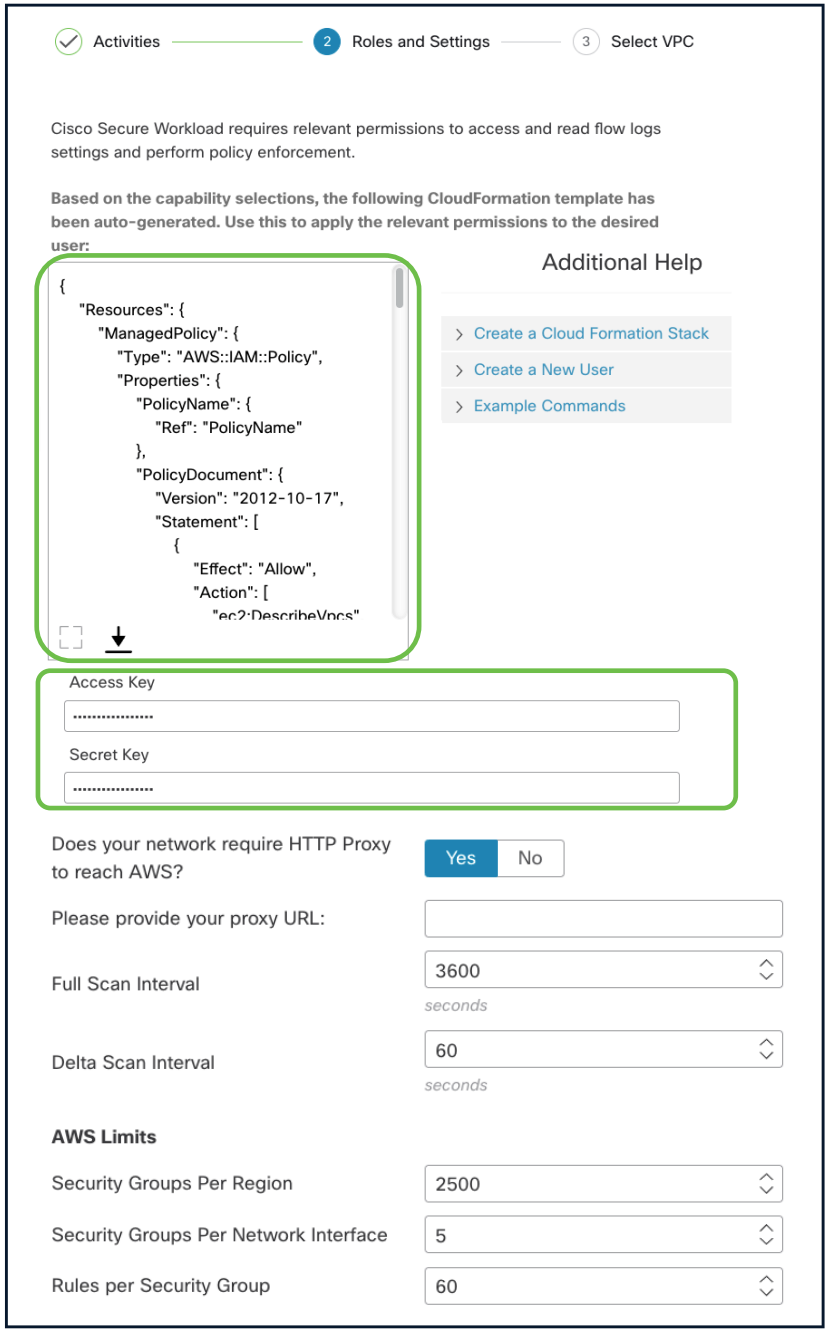
AWS Connector - IAM

2

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



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

AWS Connector – Select VPCs

3

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

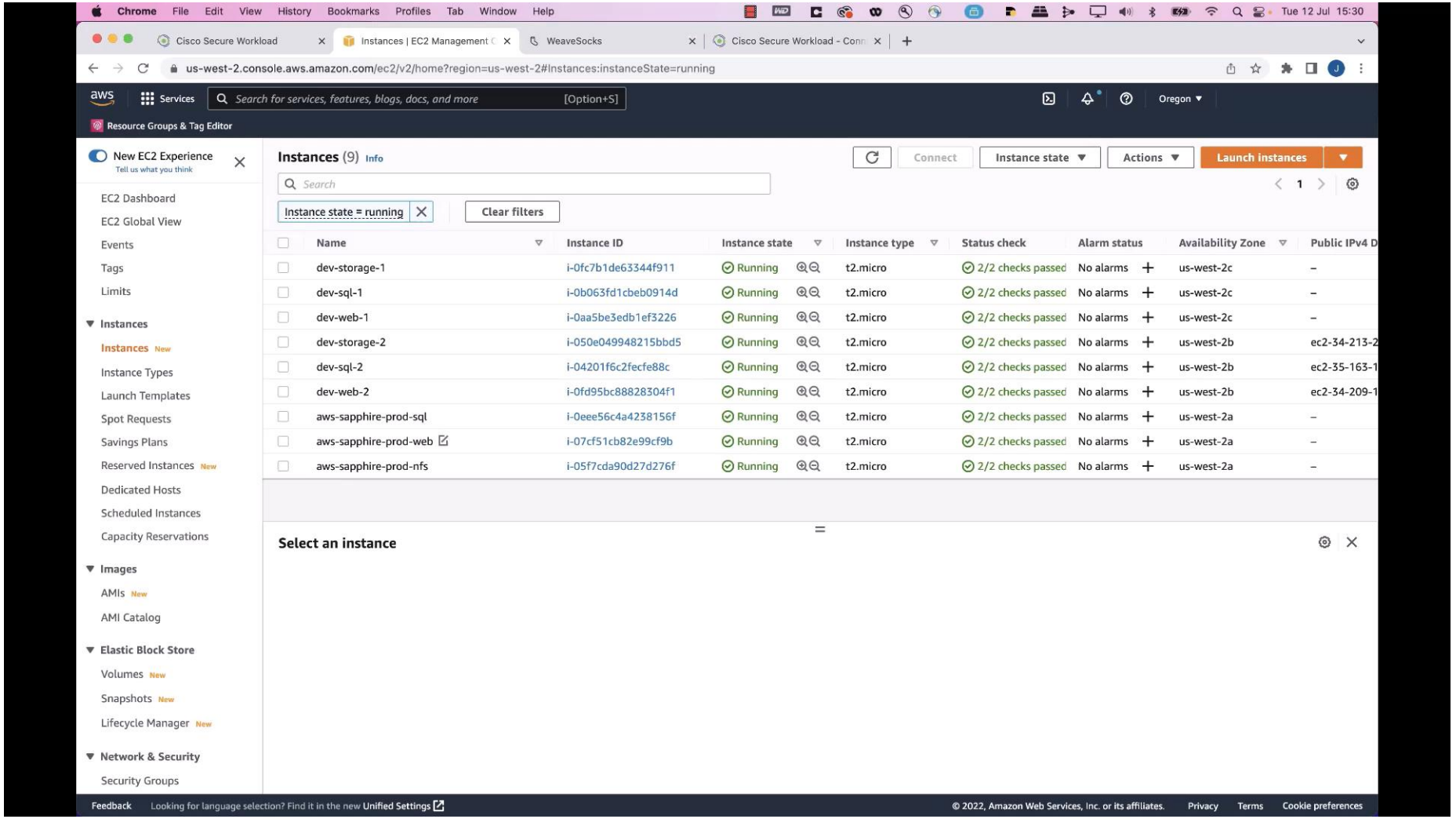
Edit AWS Connector

☐	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	☑	☑	☑

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

cisco

Zoning & (Macro/Micro)Segmentation Demo



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

Conclusion

Zero Trust for Applications Everywhere

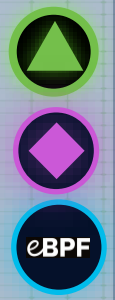
Hybrid Mesh Platform

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

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

cisco

Complete your session evaluations

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

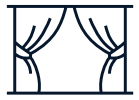
Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

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

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

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

Thank you

cisco Live !

CISCO