

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



How to build a secure modern Hybrid cloud Environment

Fabien Gandola, Security TSA EMEA
BRKSEC-2444



#CiscoLiveAPJC

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 November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2444>



Objectives



No perfect
Solution... Yet



Need for a platform



Multiple paths to
securing Cloud &
Apps



Cisco can help with
this Journey

What (not) to expect



- No deep dive on Cisco Products
- No configuration guide
- No troubleshooting

What (not) to expect



- No deep dive on Cisco Products
- No configuration guide
- No troubleshooting
- No third-party solutions



- An outcome based approach to addressing concrete use cases
- Mostly about visibility and Segmentation
- Cisco Vision and Strategy
- Cisco current capabilities

Agenda

- Introduction
- A vision...
- What's available today:
 - On-prem
 - ✓ ACI
 - ✓ FTD
 - ✓ CSW
 - ✓ ISE
 - In the Cloud
 - ✓ Cloud Native security elements
 - ✓ FTDv/ Multicloud Defense
 - ✓ CSW
- Conclusion

About Me



Fabien Gandola

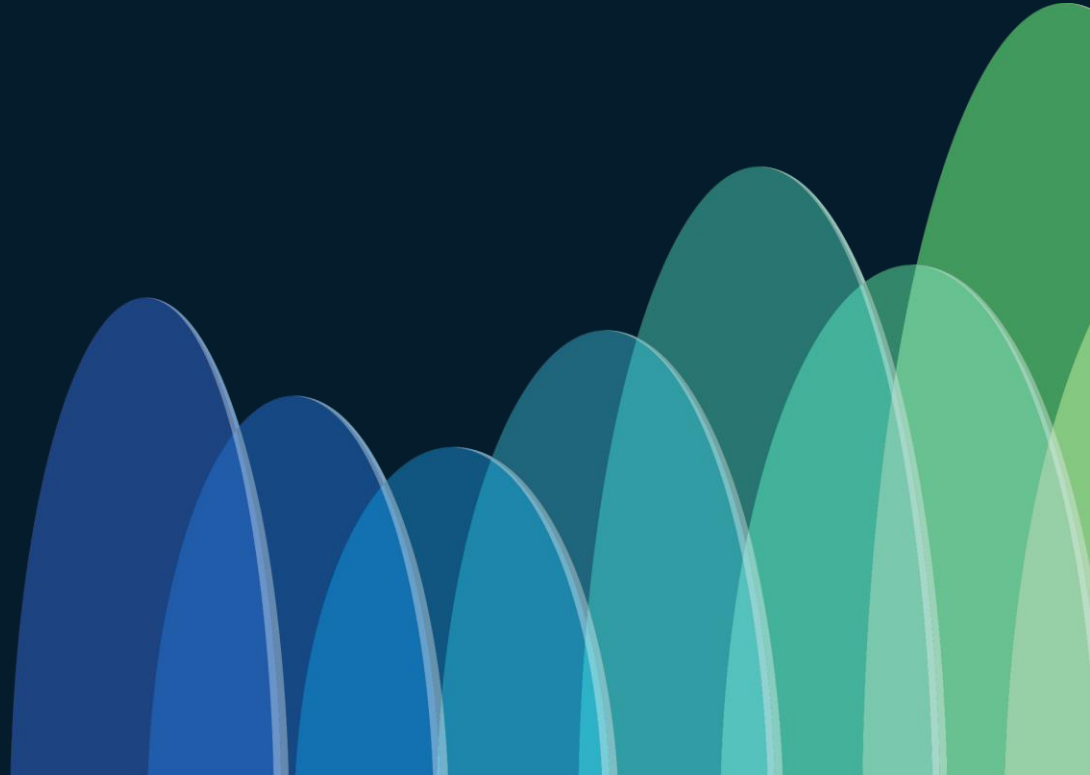
fgandola@cisco.com

TSA Cyber Security EMEA

25 years in Cisco



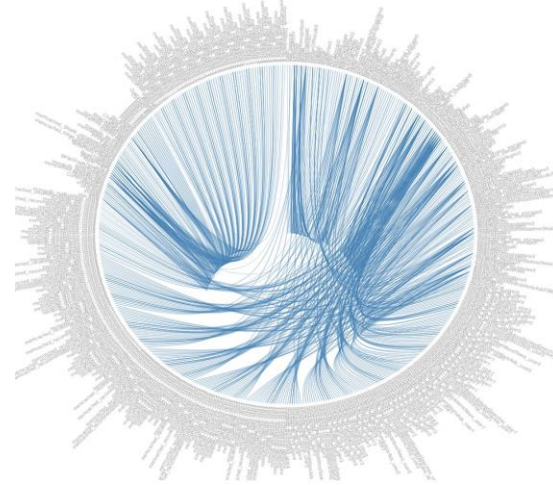
The challenges



Two obvious but key observations :

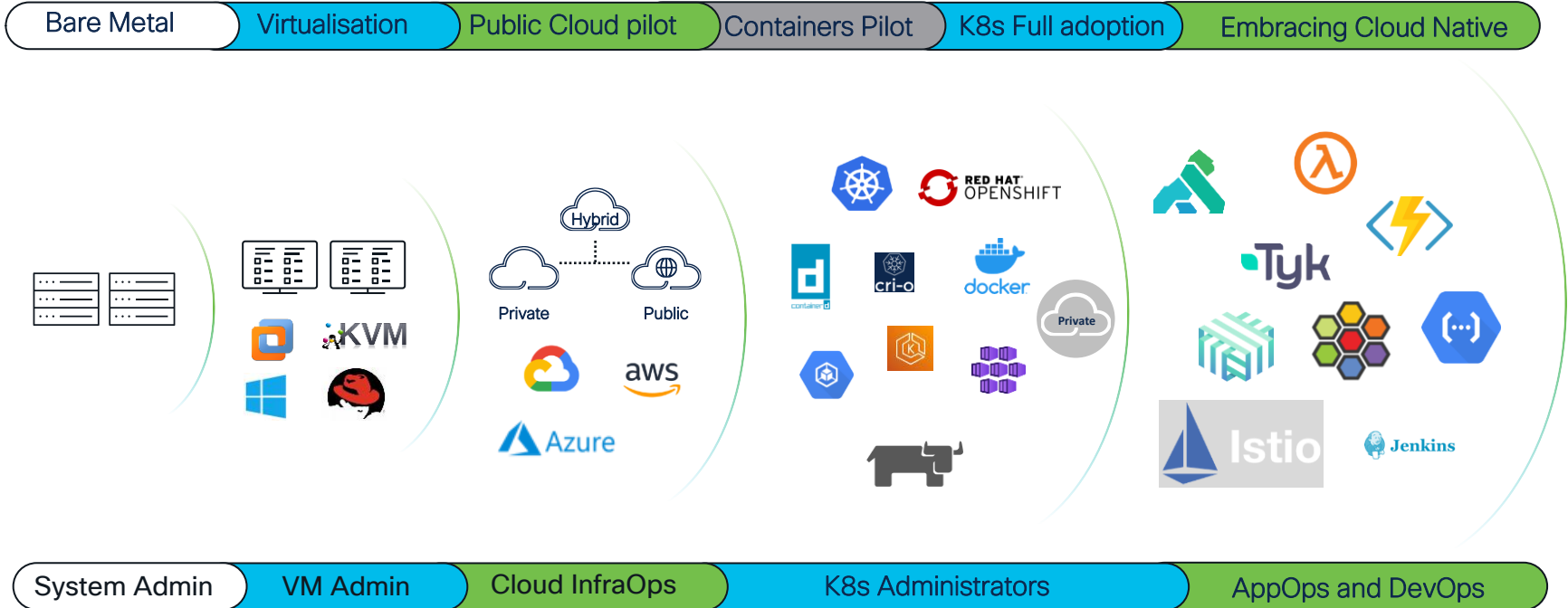


Applications are
critical to modern
businesses

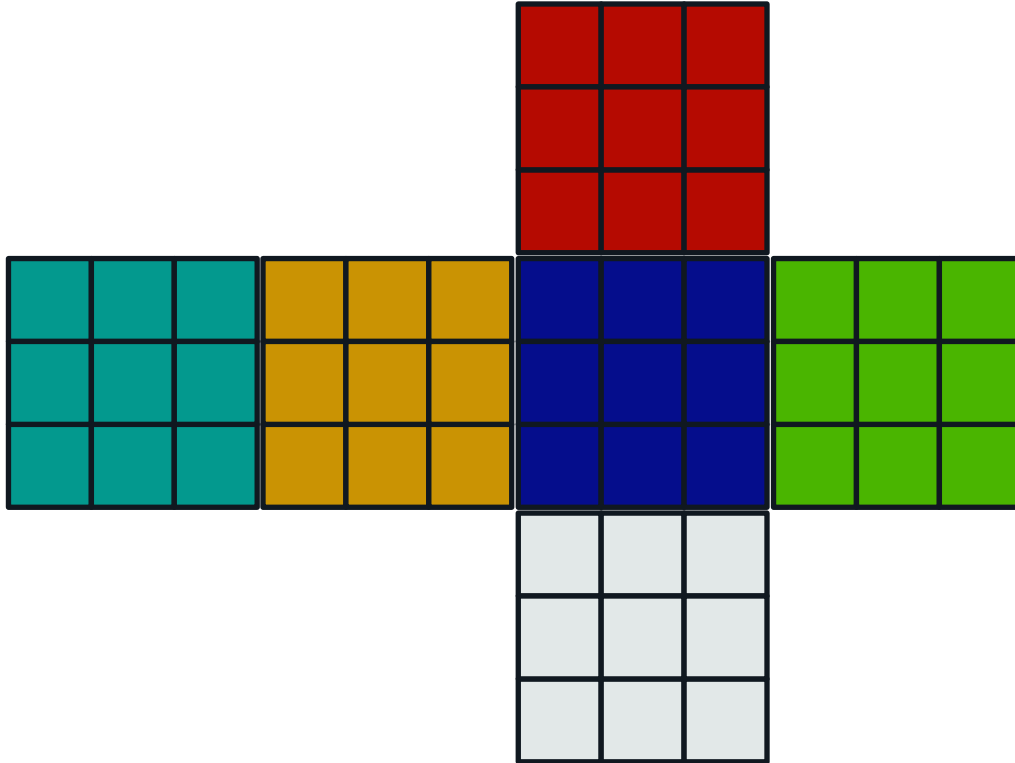


Applications have
dramatically evolved

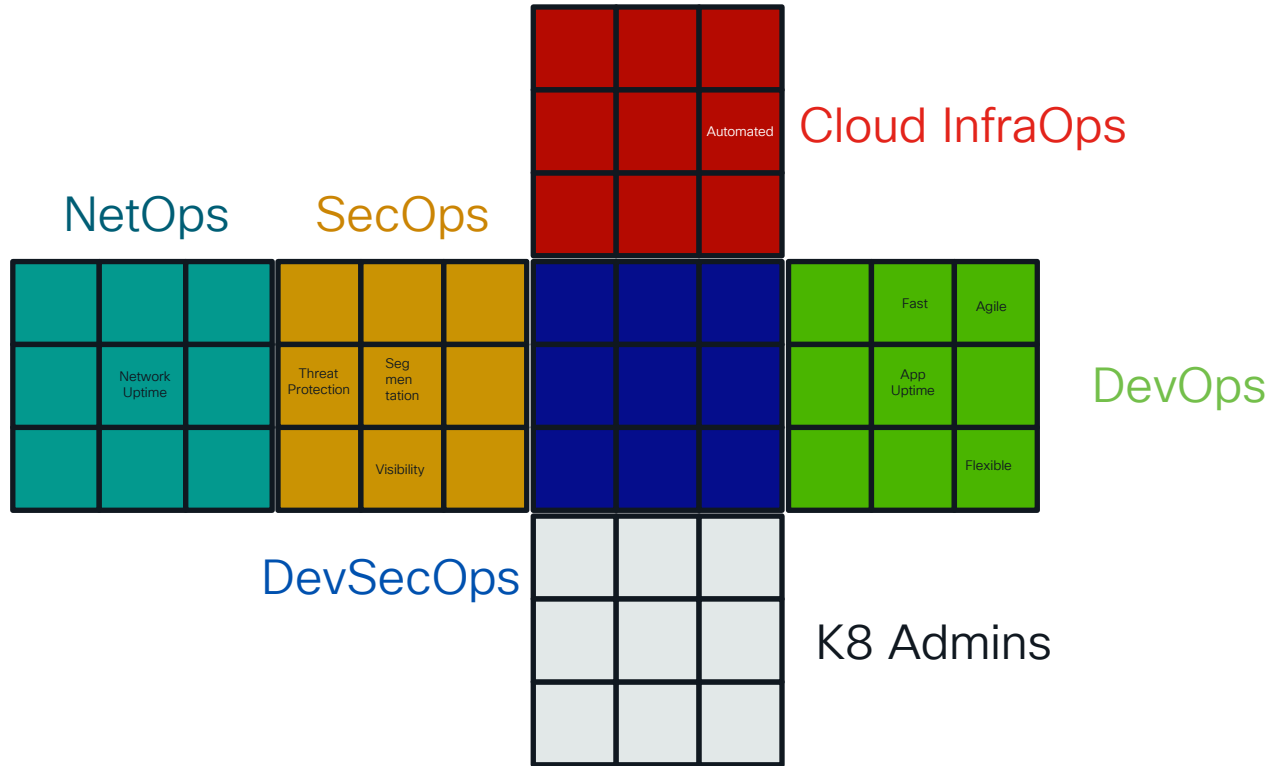
Application workloads evolution



Cloud Security Rubik's Cube



Cloud Security use cases



Some of the challenges...

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

I Have
A
Dream

Some ideas toward an ideal solution...

- Automatically discover new applications
- Understand the different ways 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

Telemetry (SIEM/SOAR/XDR)



Cisco Cloud Protection Suite

Cloud management (Security Cloud Control)

Visibility

Segmentation

Exploit Protection

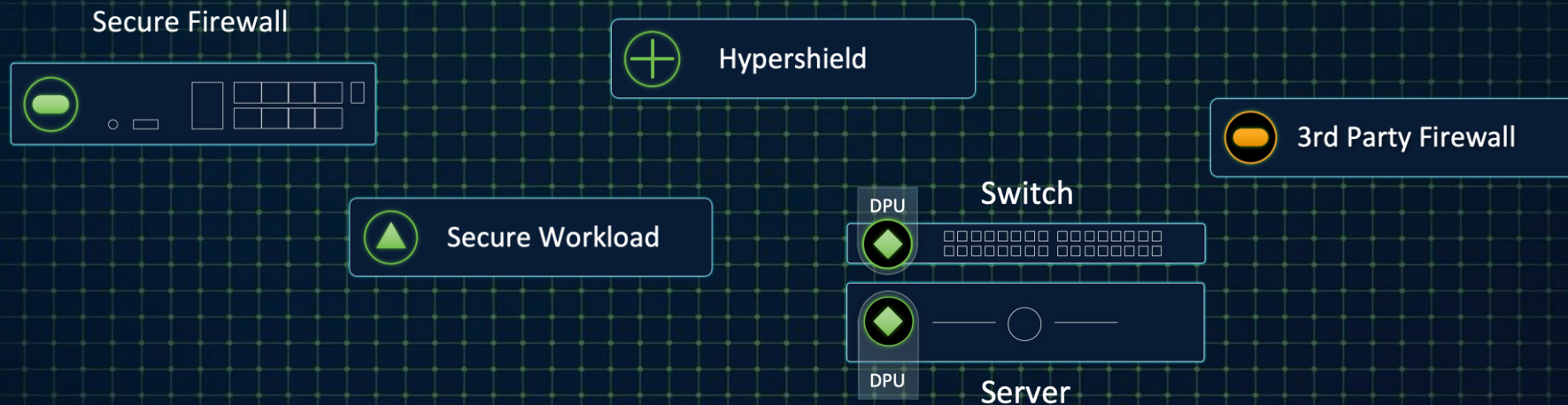
Future

AI

Identity Intelligence

Hardware

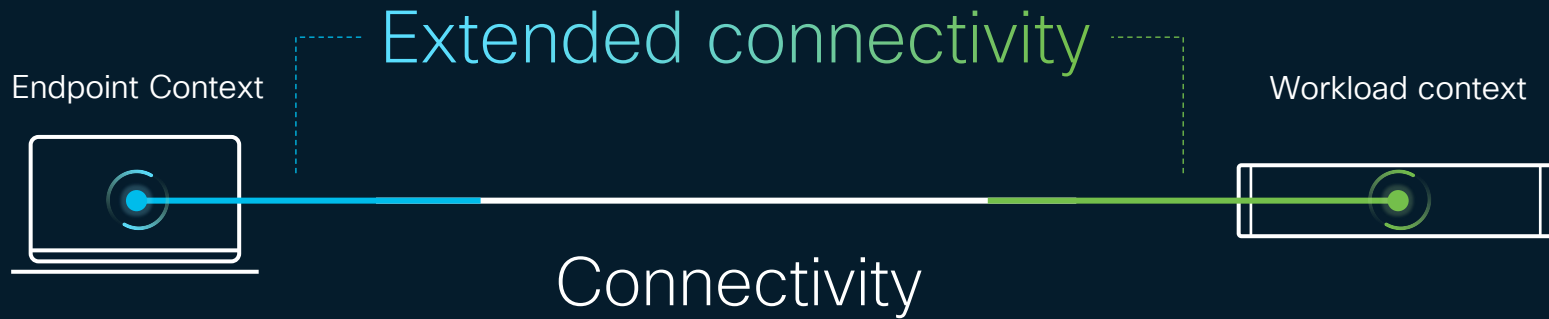
Security Cloud Control



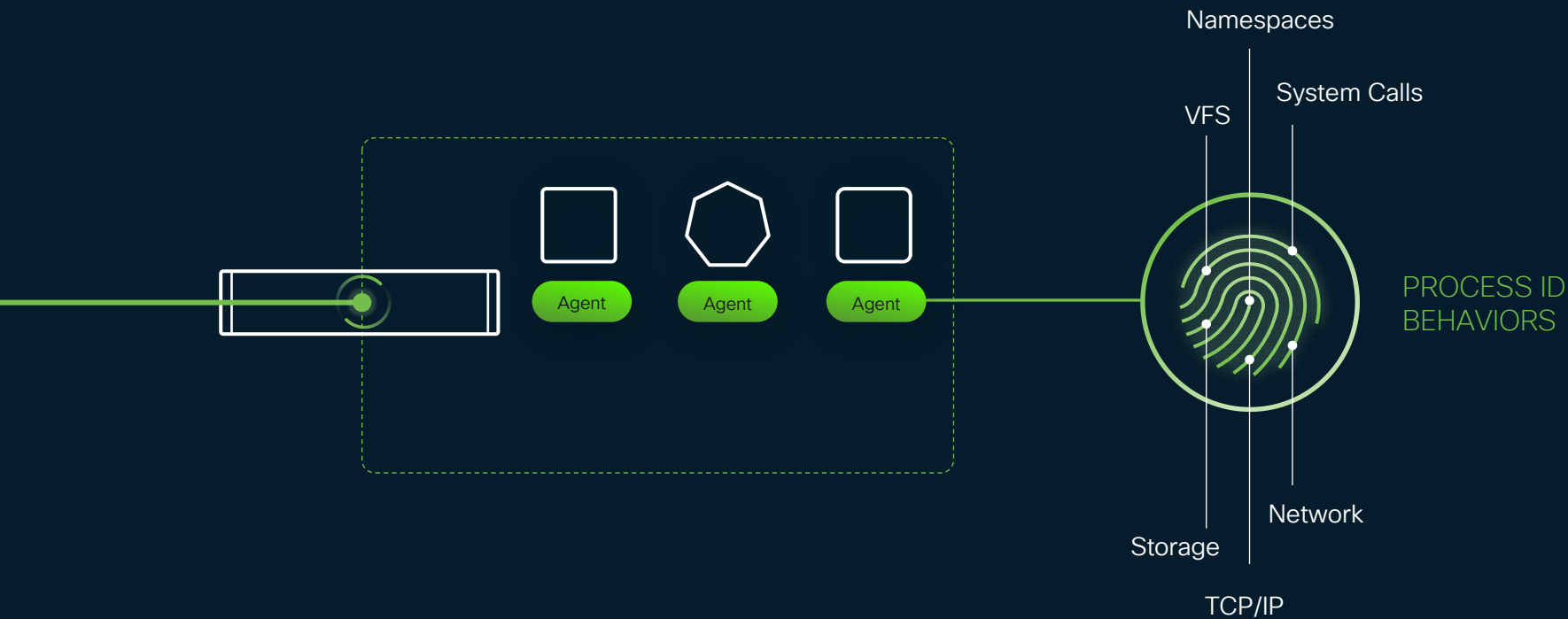
Extended connectivity

Optimal policy fit

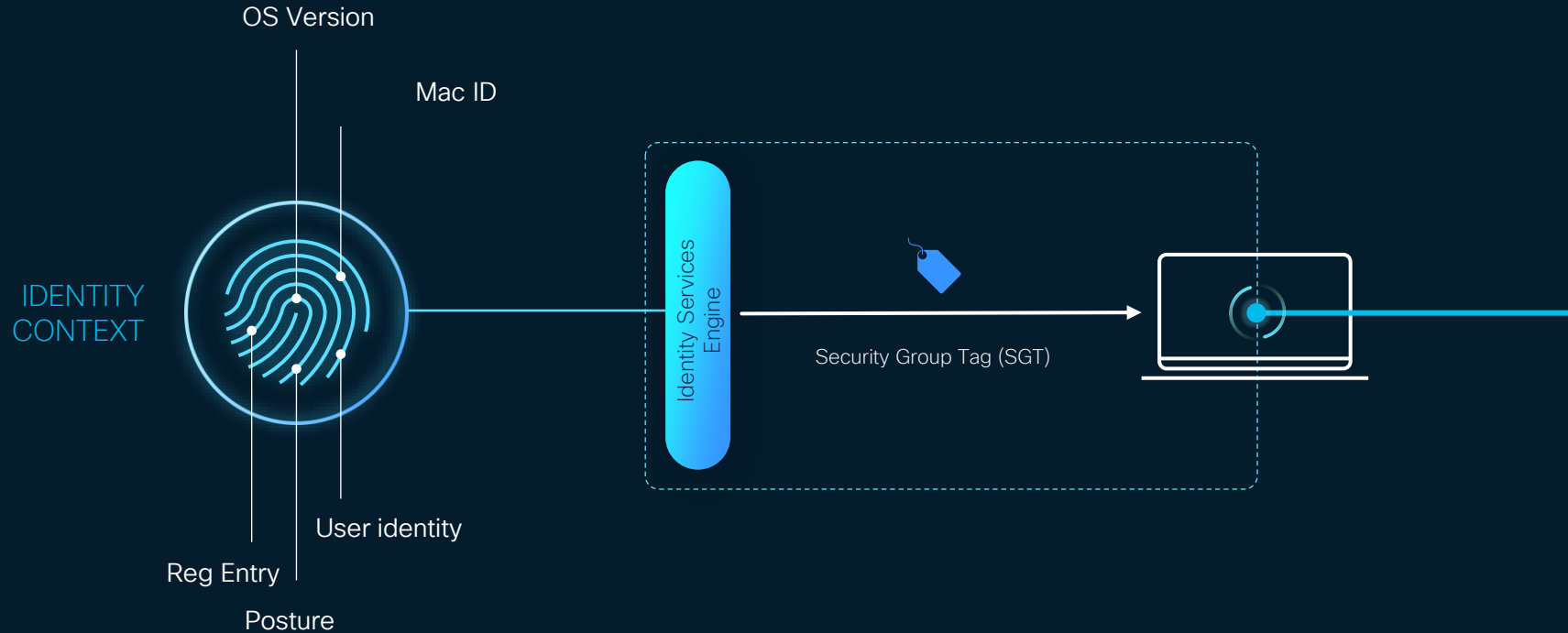
Evolves over time

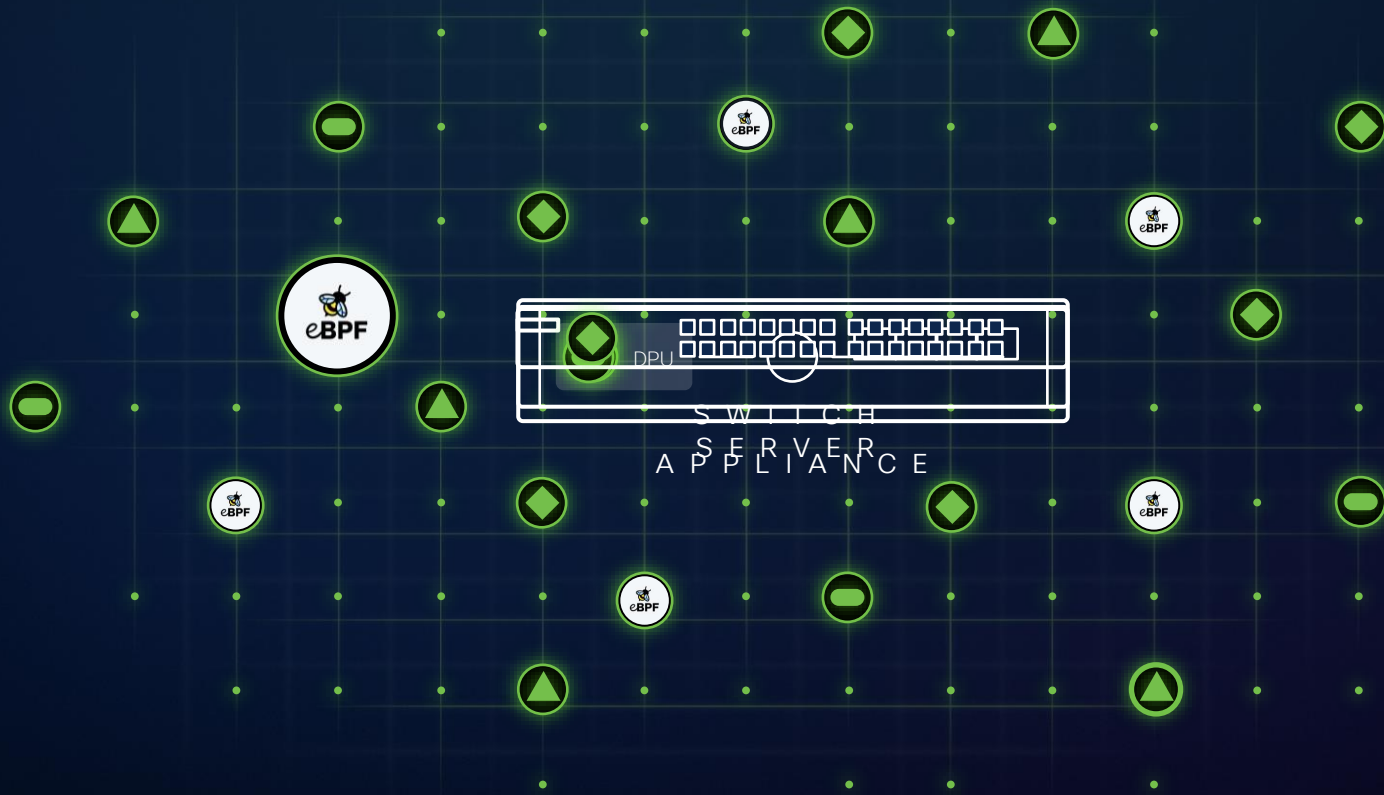


Workload context



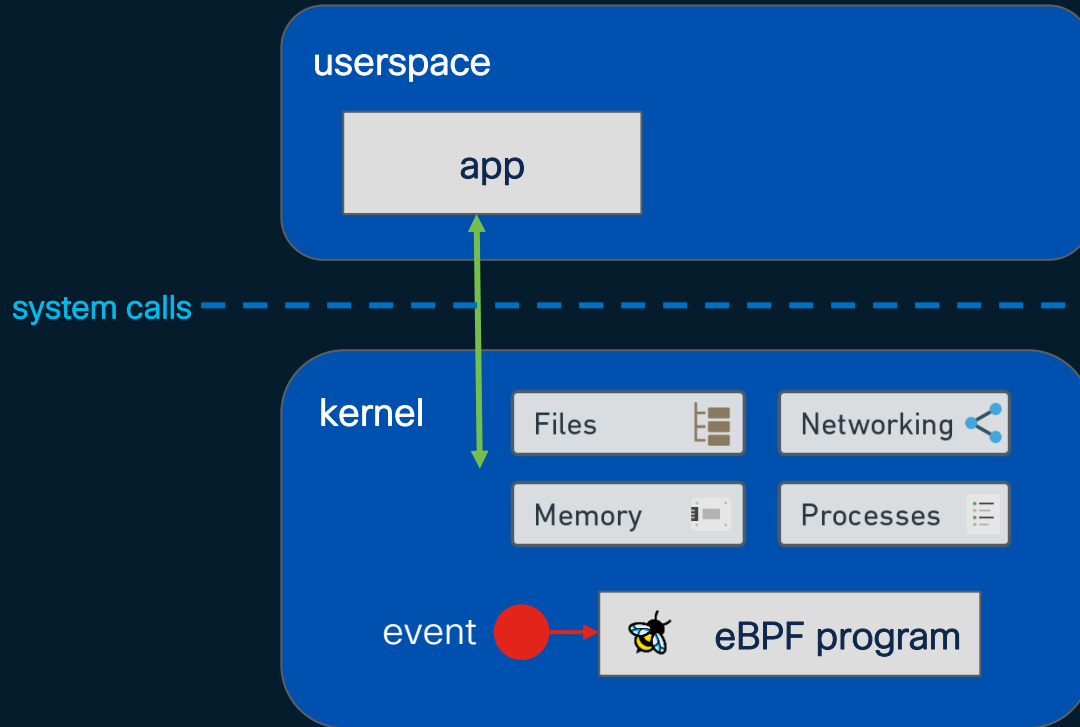
Endpoint context





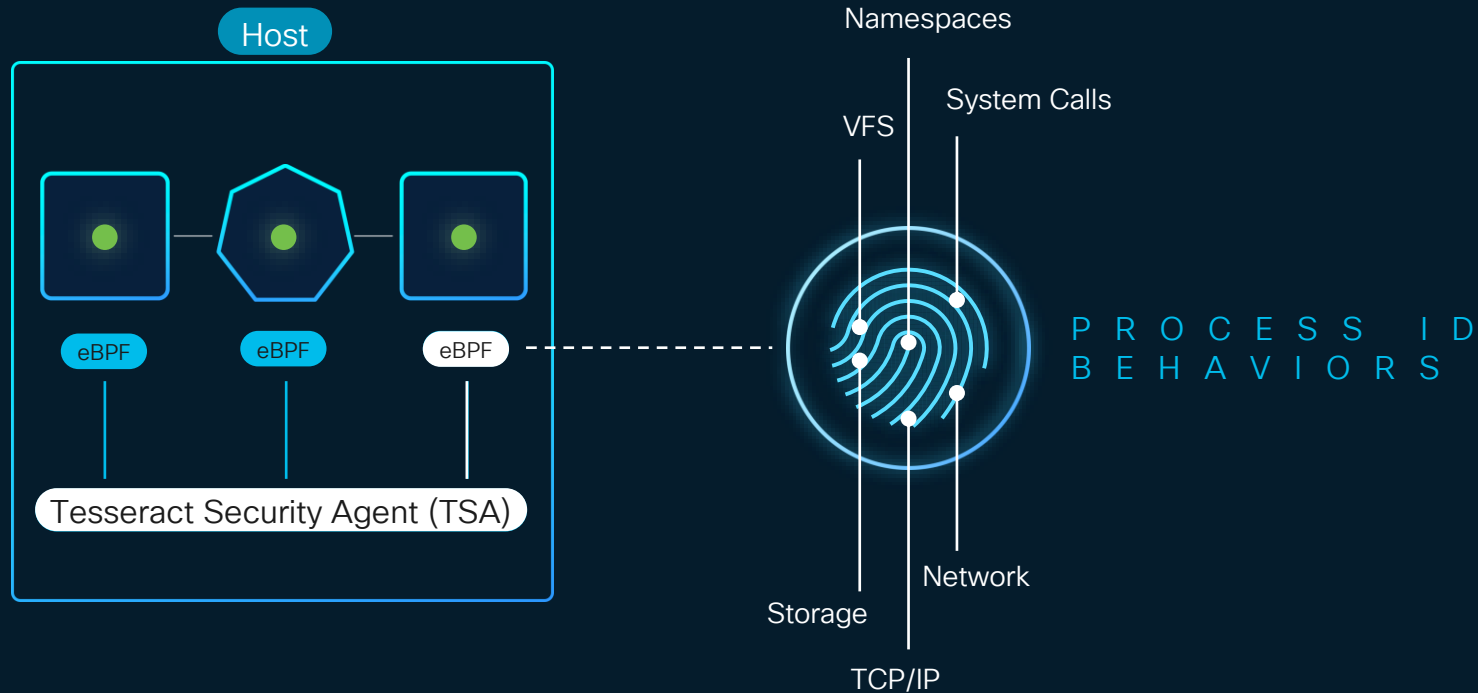
eBPF – extended Berkely Packet Filter

Makes the Linux kernel programmable in a secure and efficient way



Deep workload visibility and control

Hypershield



40+

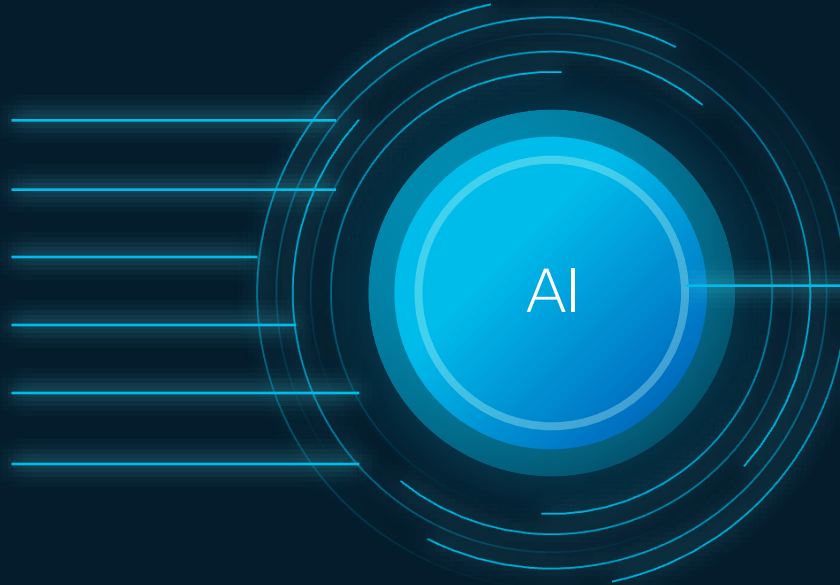
days to segment
an application

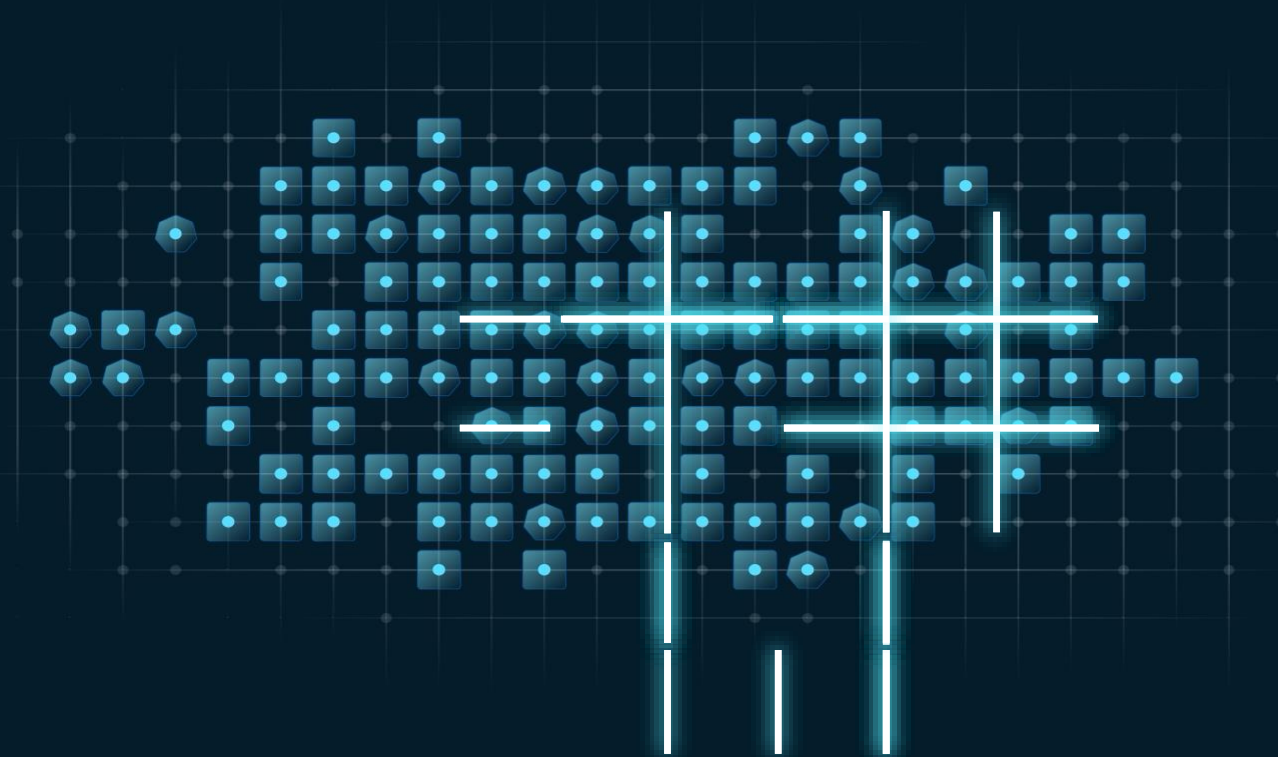


A
C
C
U
R
A
C
Y

T
I
M
E

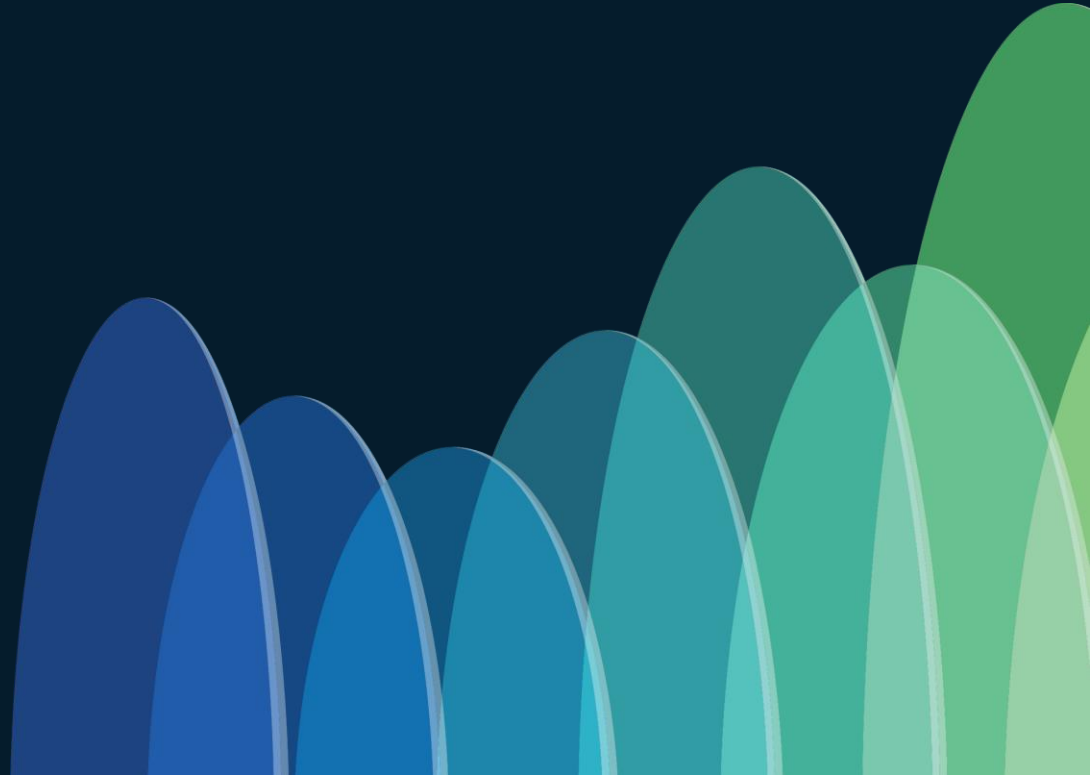
Network flows
Global customer data
Process behaviors
File changes
Threat intel updates (Talos)
Learned policy preferences
...



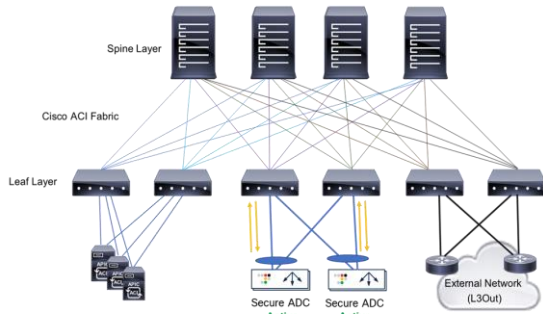


453 WORKLOADS
89 SERVERS
987,163 PROCESSES
567 CONNECTIONS

Back to what is
available today...



The way we are doing it traditionally...



SDN Infrastructure
(ACI, NSX,...)



Firewall
(FTD, ASA)



CISCO **SECURE**
Workload

Host based
Firewall

Shortest introduction to ACI ever...



ACI Devices Role

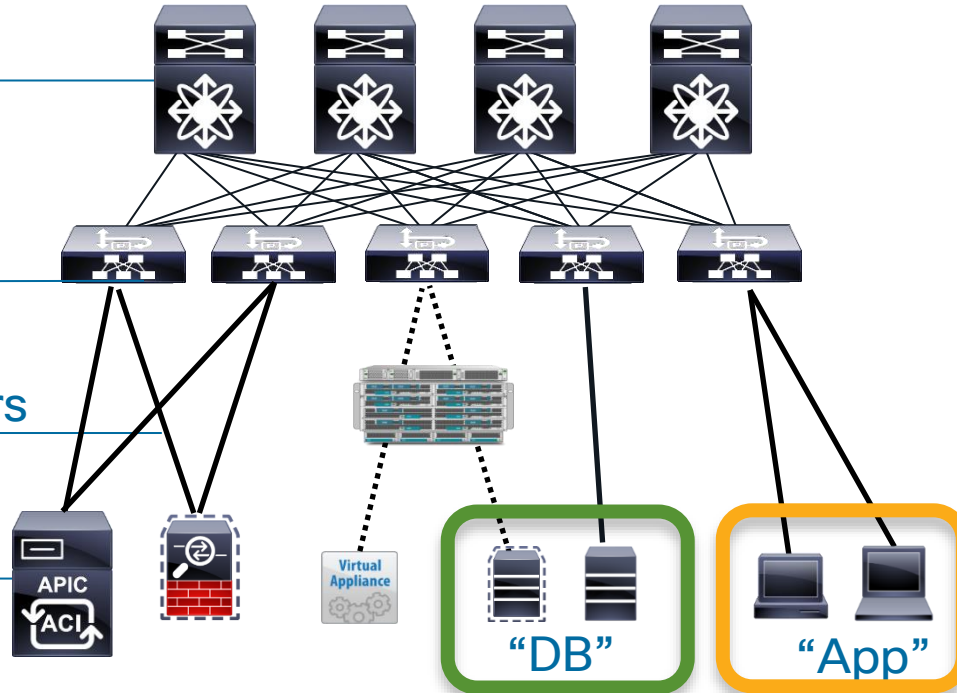
Spine Nodes

Leaf Nodes

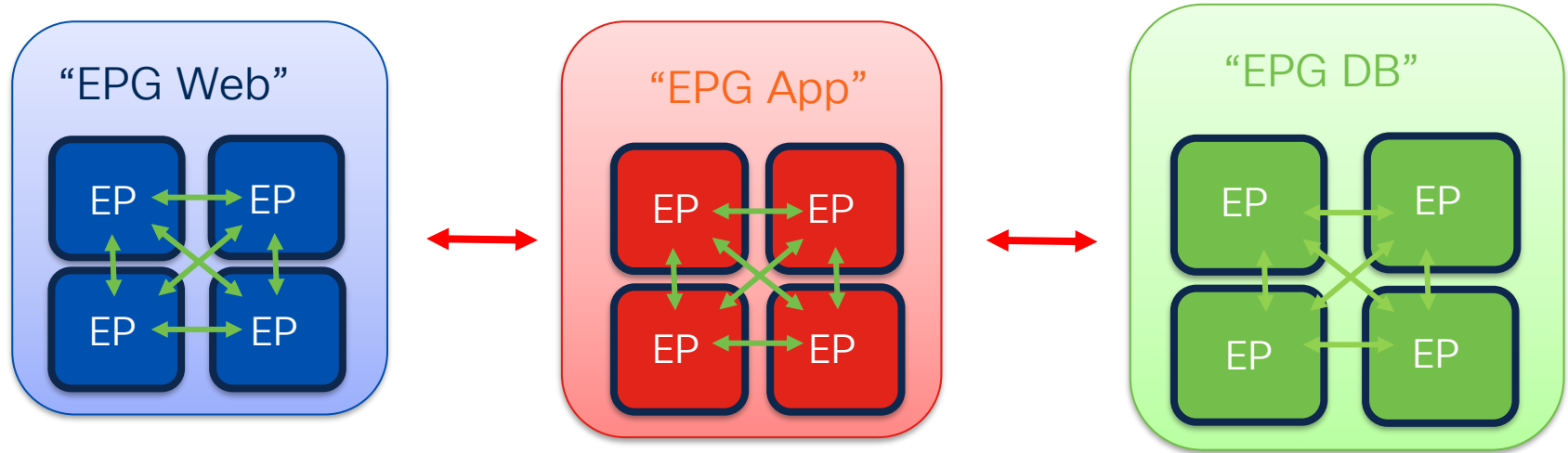
Service Producers

APIC Controller

Service Consumers



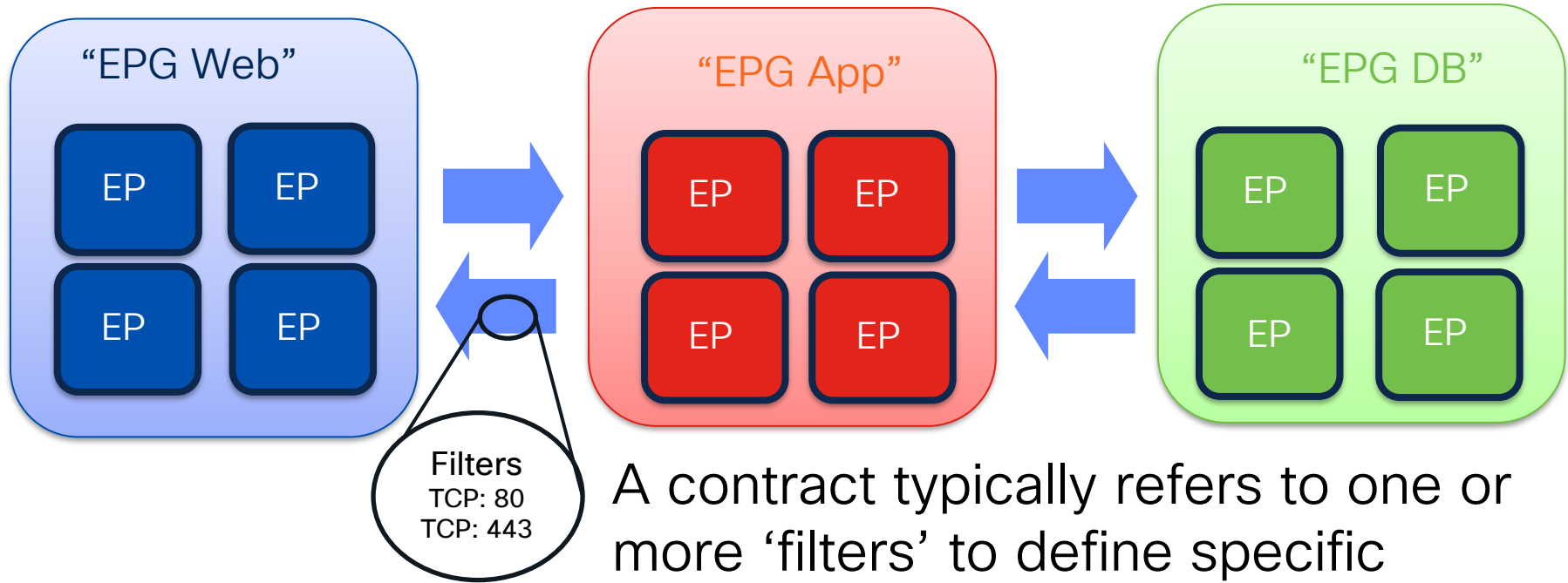
Endpoint Groups Communications



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

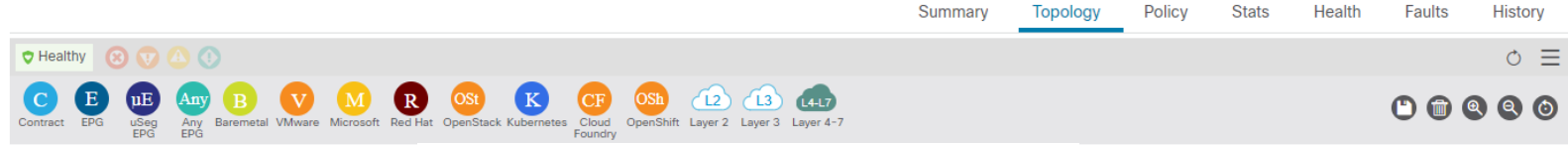
Communication between Endpoint groups is, by default, not permitted.

Contract : Kind of reflexive “Stateless” ACLs



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

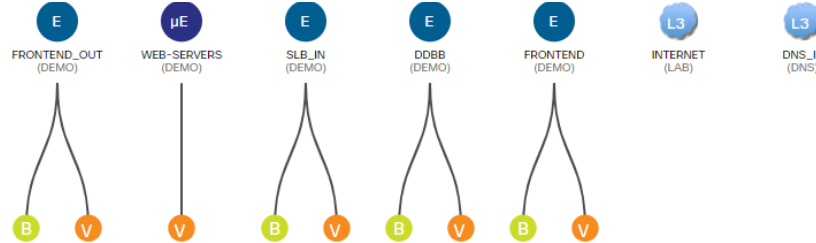
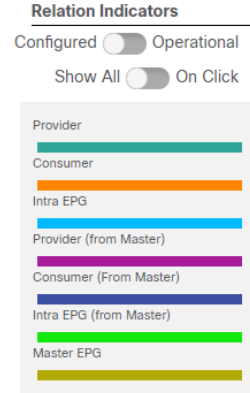
Application policy with contract



Contracts →

EPG →

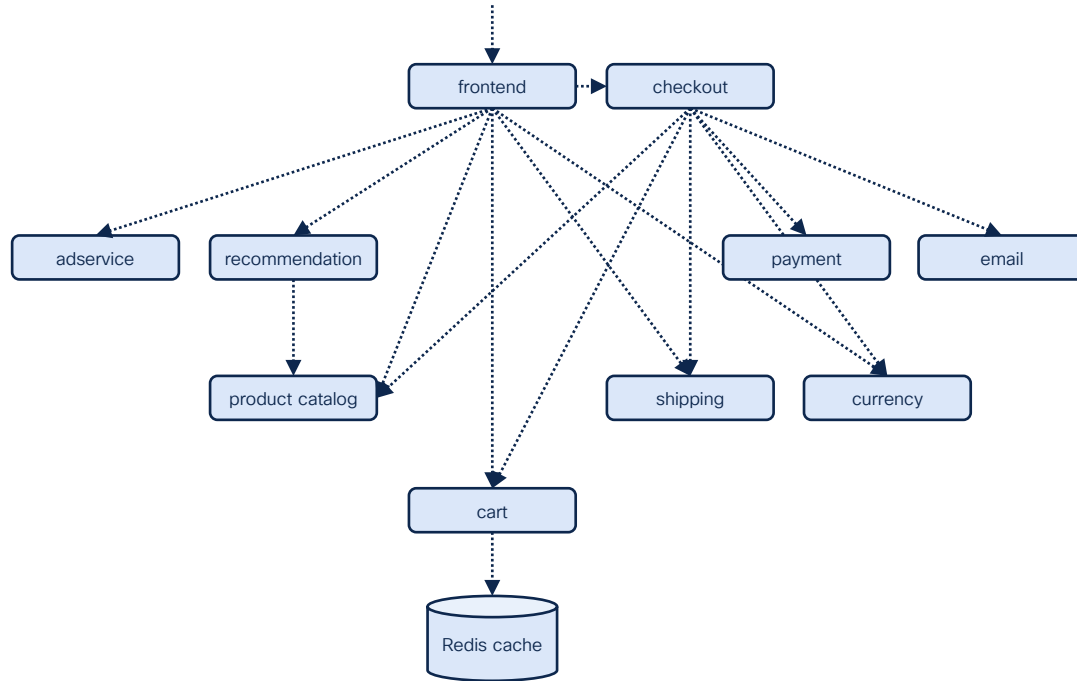
Form Factor →



Cancel Submit

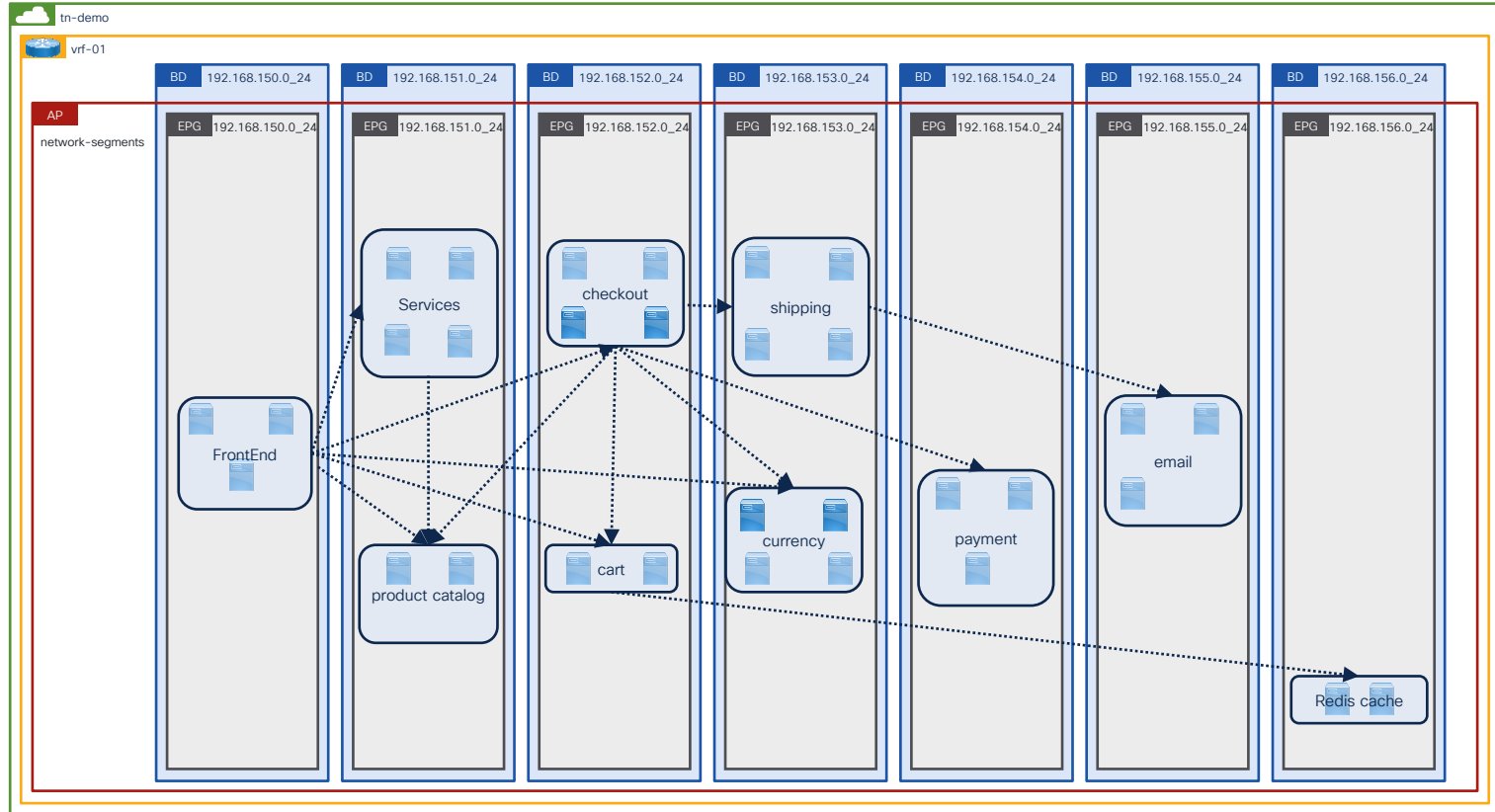
Online Boutique

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

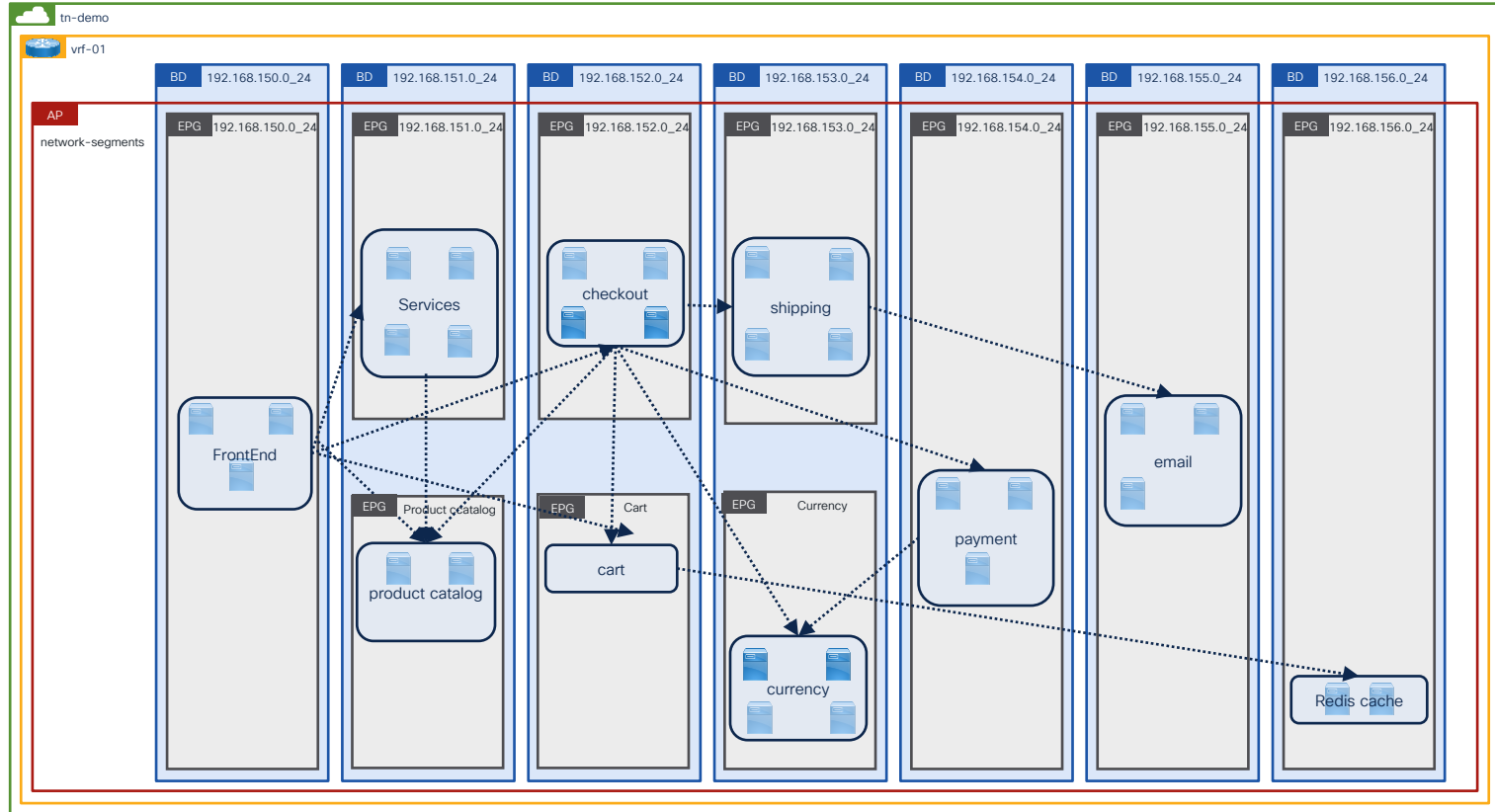


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart currency email payment product catalog shipping	TCP 7070 TCP 7000 TCP 8080 TCP 50051 TCP 3550 TCP 50051
frontend	adservice cart checkout currency product catalog recommendation shipping	TCP 9555 TCP 7070 TCP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

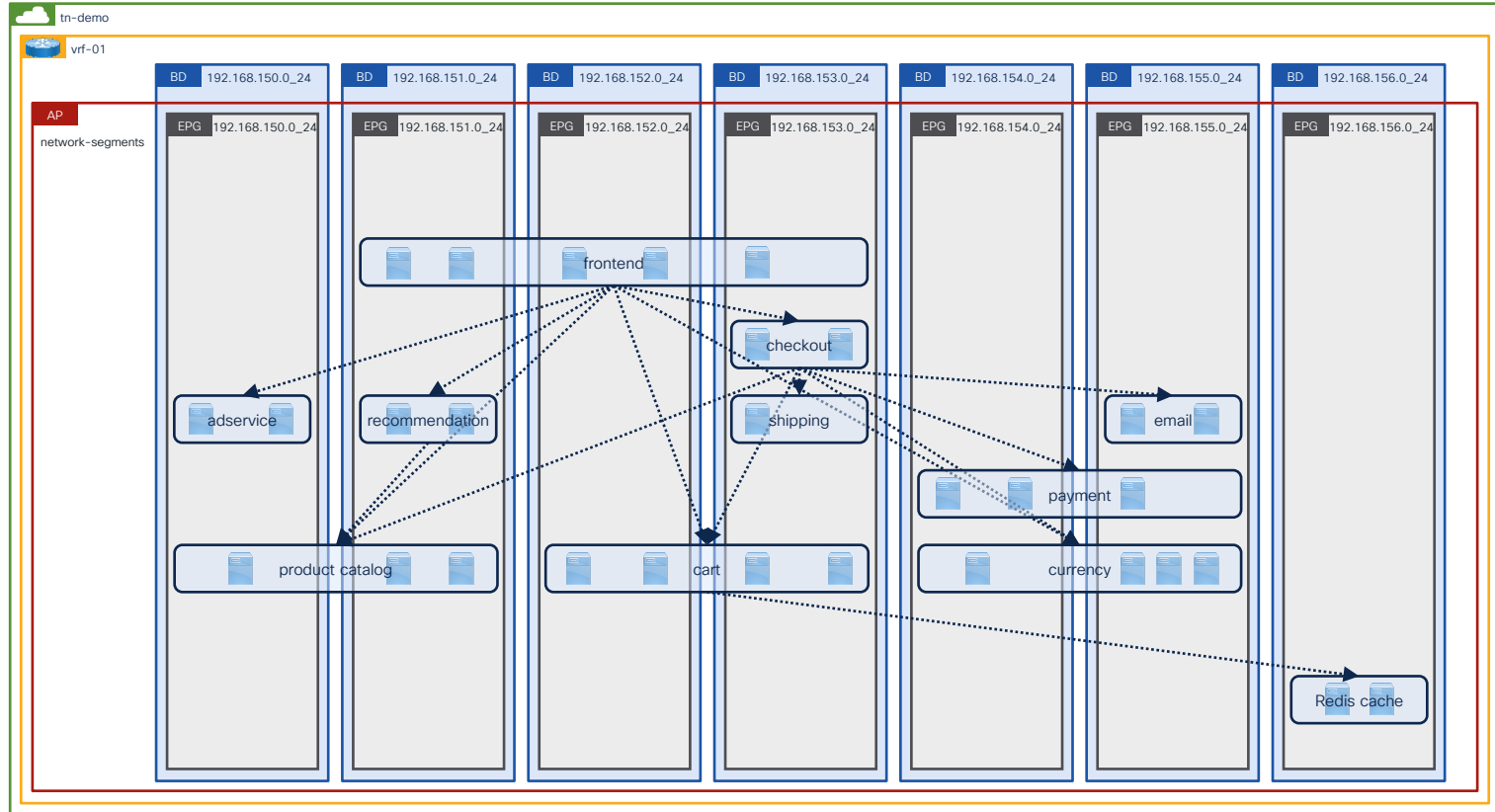
Where is our application running...?



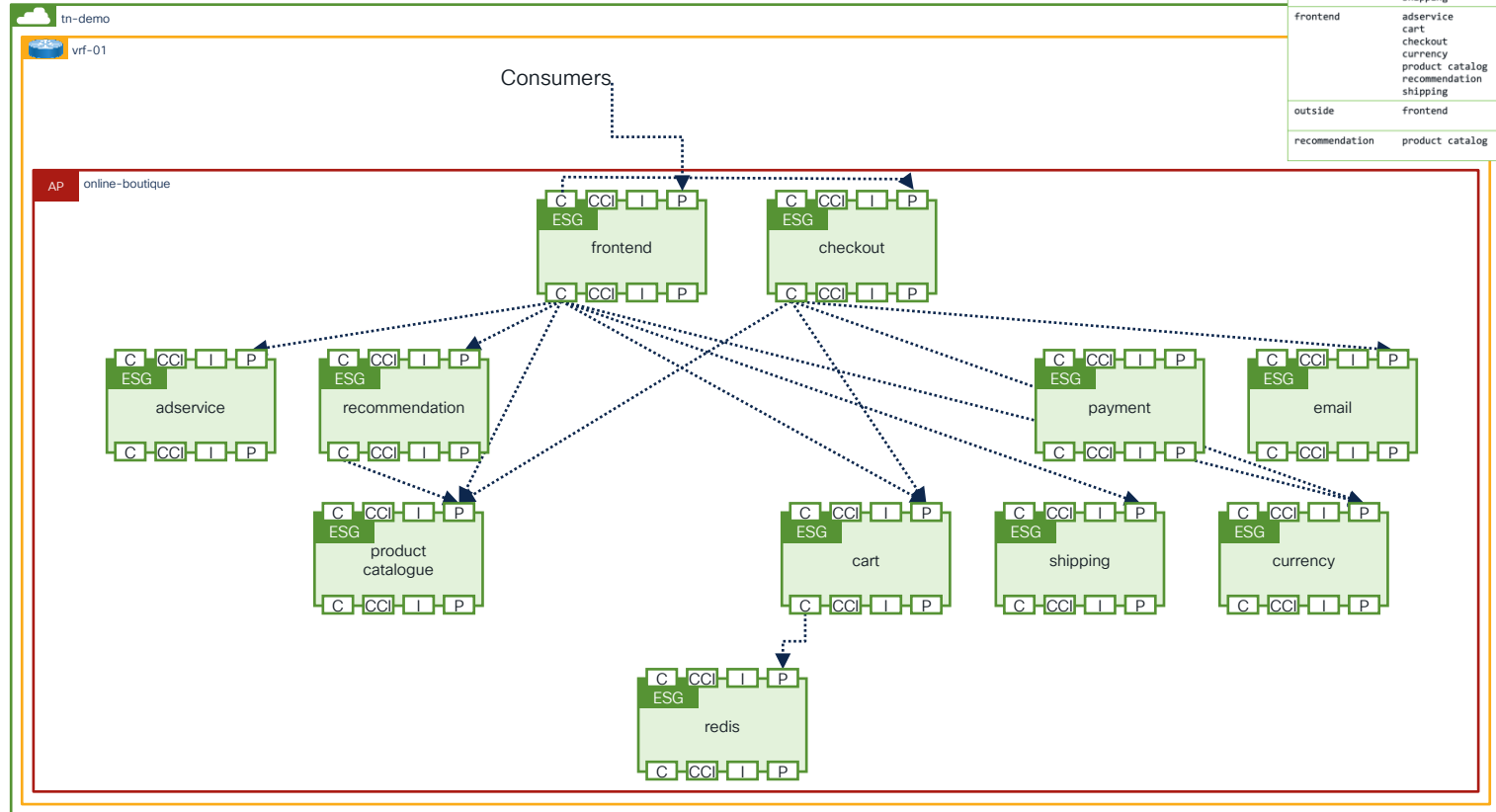
Where is our application running...?



Where is our application running...?

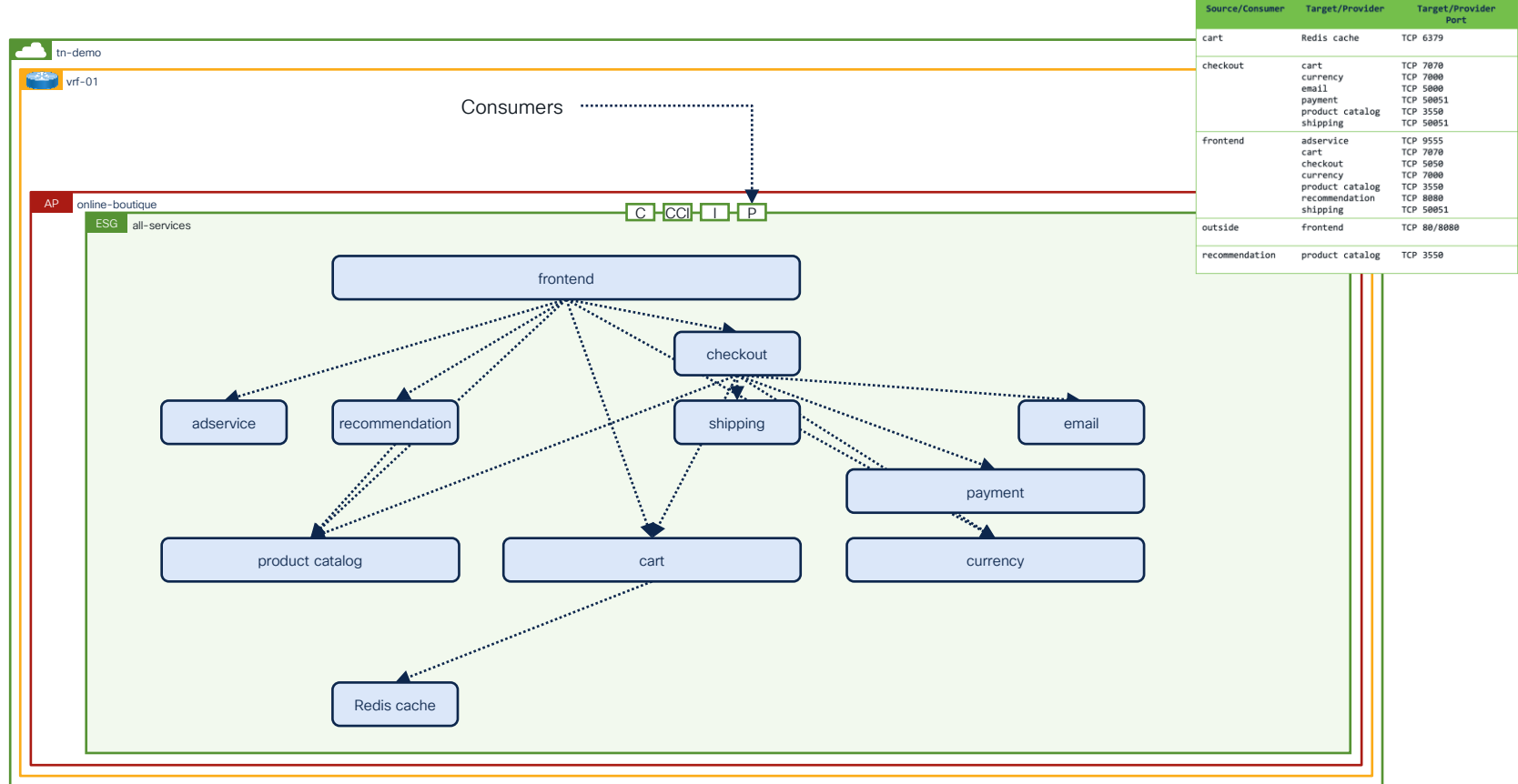


Application tiers across subnets



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
frontend	product catalog	TCP 3550
	shipping	TCP 50051
	adservice	TCP 9555
	cart	TCP 7070
outside	currency	TCP 5050
	checkout	TCP 7000
	product catalog	TCP 3550
	recommendation	TCP 8080
recommendation	shipping	TCP 50051
recommendation	product catalog	TCP 3550

Application tiers across subnets

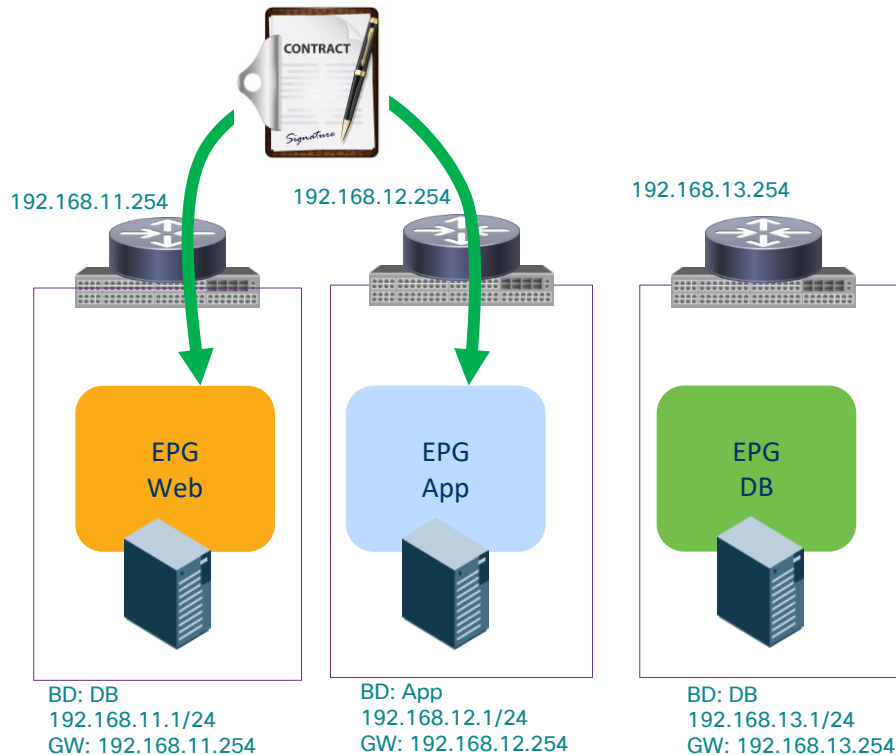


Secure Firewall Insertion



2 conditions for traffic reaching destination

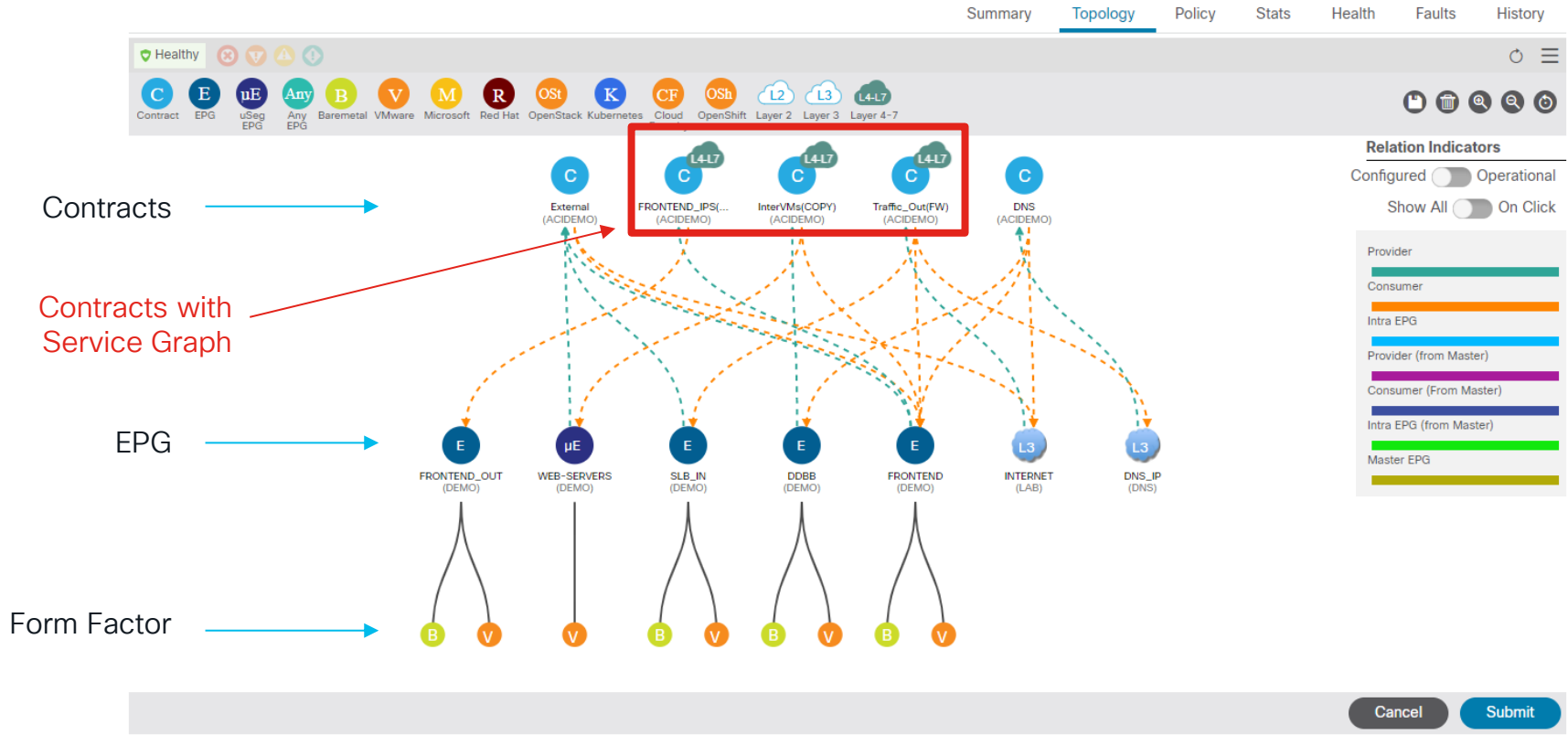
Before Service graph is deployed



ACI relies on :

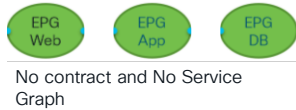
- ✓ Routing to forward traffic
- ✓ Contract to allow traffic

Attach a Service Graph to a contract

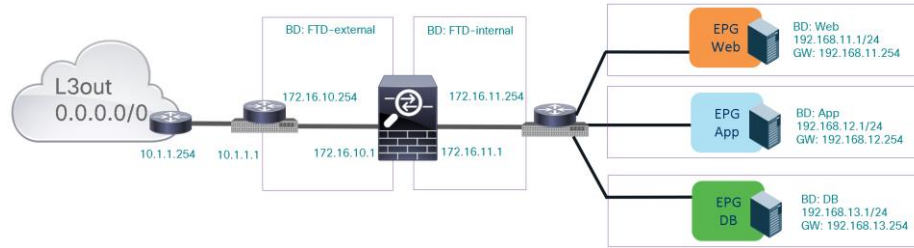


3 main ways to insert a Firewall in ACI

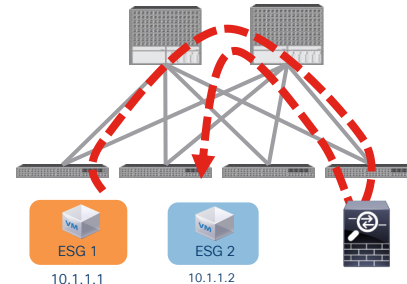
- “Network Stitching” Firewall Insertion



- Traditional Service

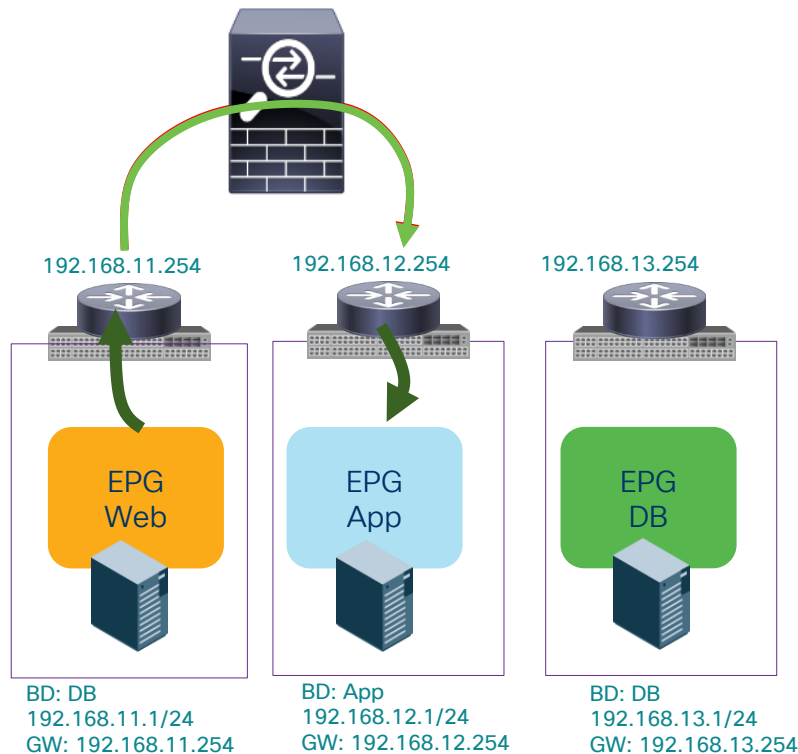


- Service Graph with PBR

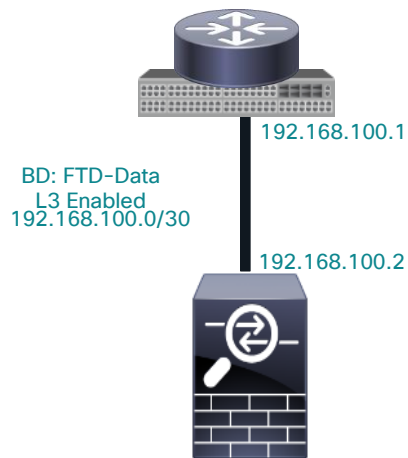


Policy Based Redirect is your Best Friend

With PBR Service Graph



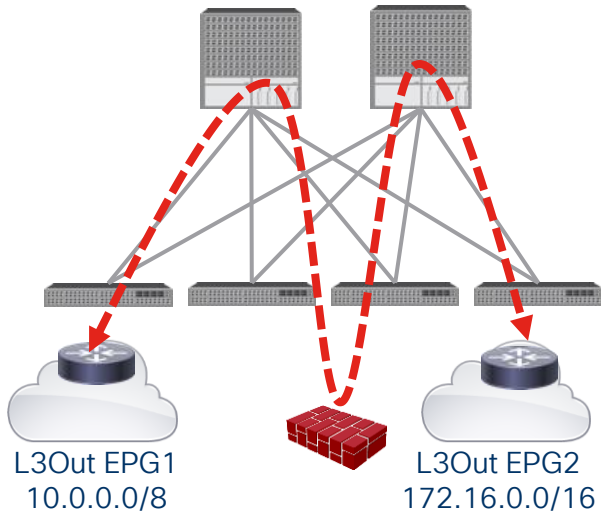
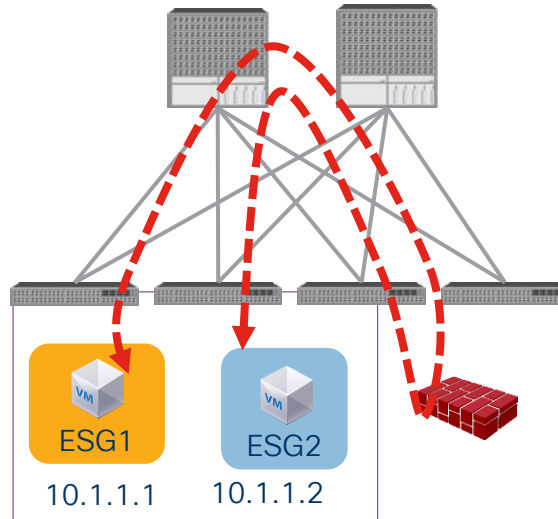
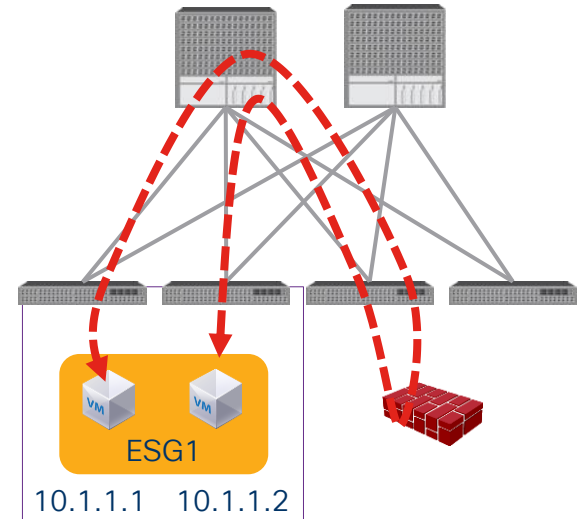
PBR redirects the traffic matching the **contract** to the **Security Service**



Where can we use PBR?

Wherever contracts can be applied!

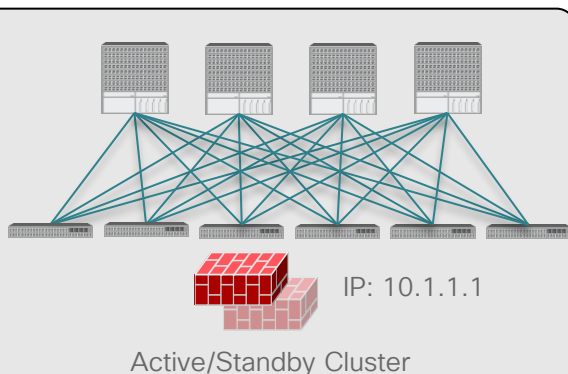
- Between EPGs or ESGs.
- Between L3Out EPGs.
- Between EPGs or ESGs in the same subnet.
- Between endpoints in the same EPG or ESG.



What are the Stateful HA options ?

One PBR destination IP
One Logical device with two concrete devices

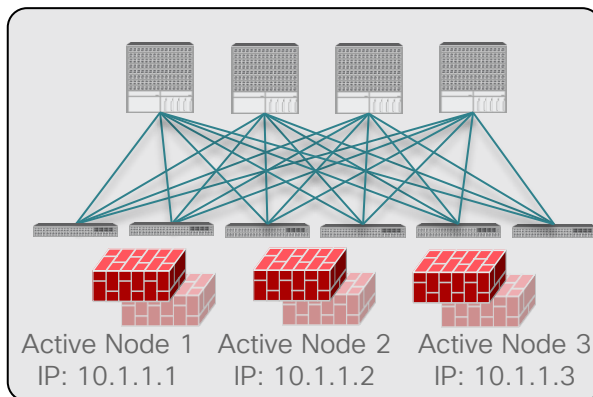
Single A/S Failover Node



- PBR is not mandatory
- The Active/Standby pair represents a single MAC/IP entry.

Multiple PBR destination IPs (Symmetric PBR)
One Logical device with multiple concrete devices

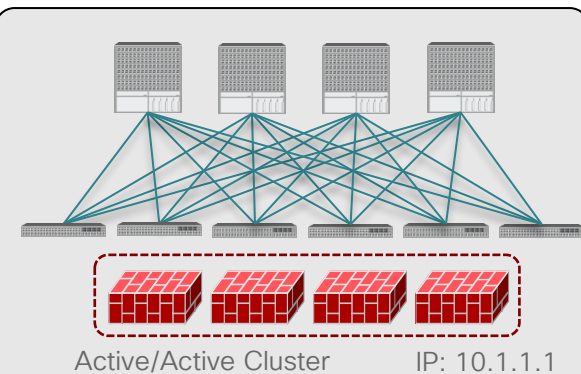
Several A/S Nodes



- PBR is required.
- Each Active node represent a unique MAC/IP entry.
- Use of Symmetric PBR to ensure each flow is handled by the same Active node in both directions

One PBR destination IP
One Logical device with one concrete device

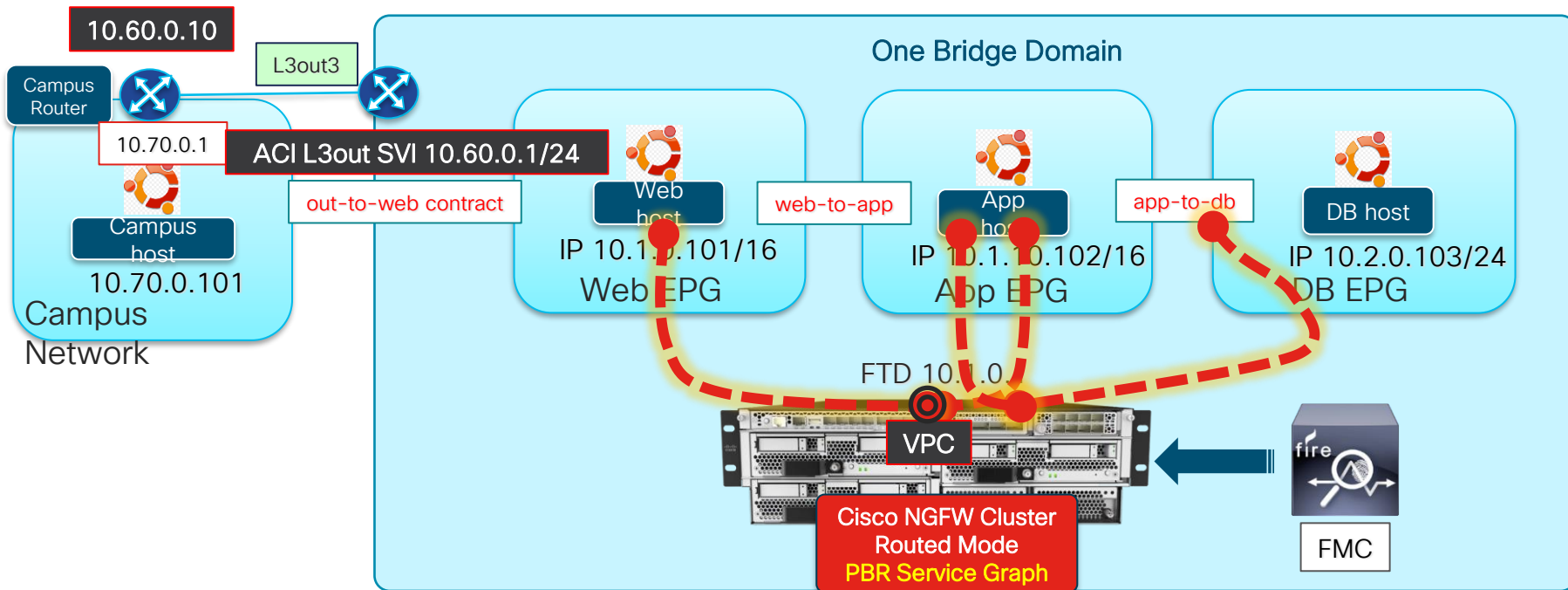
Active/Active Cluster



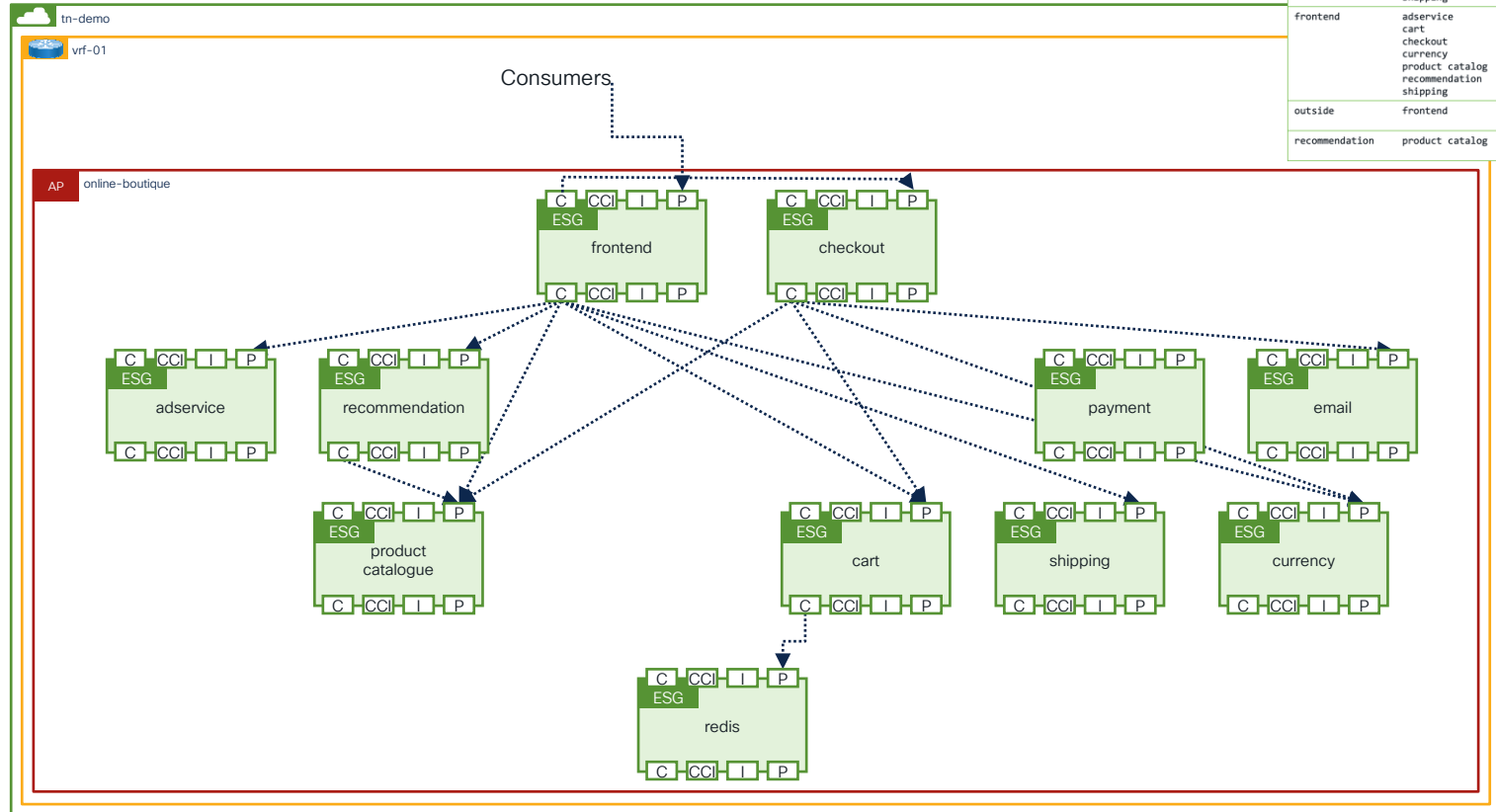
- PBR is required if the cluster is stretched across pods.
- The Active/Active cluster represents a single MAC/IP entry.
- Spanned Ether-Channel Mode supported with Cisco ASA/FTD platforms

Reuse a PBR Service Graph in Multiple Contracts

Keep the Firewall Network Config Simple

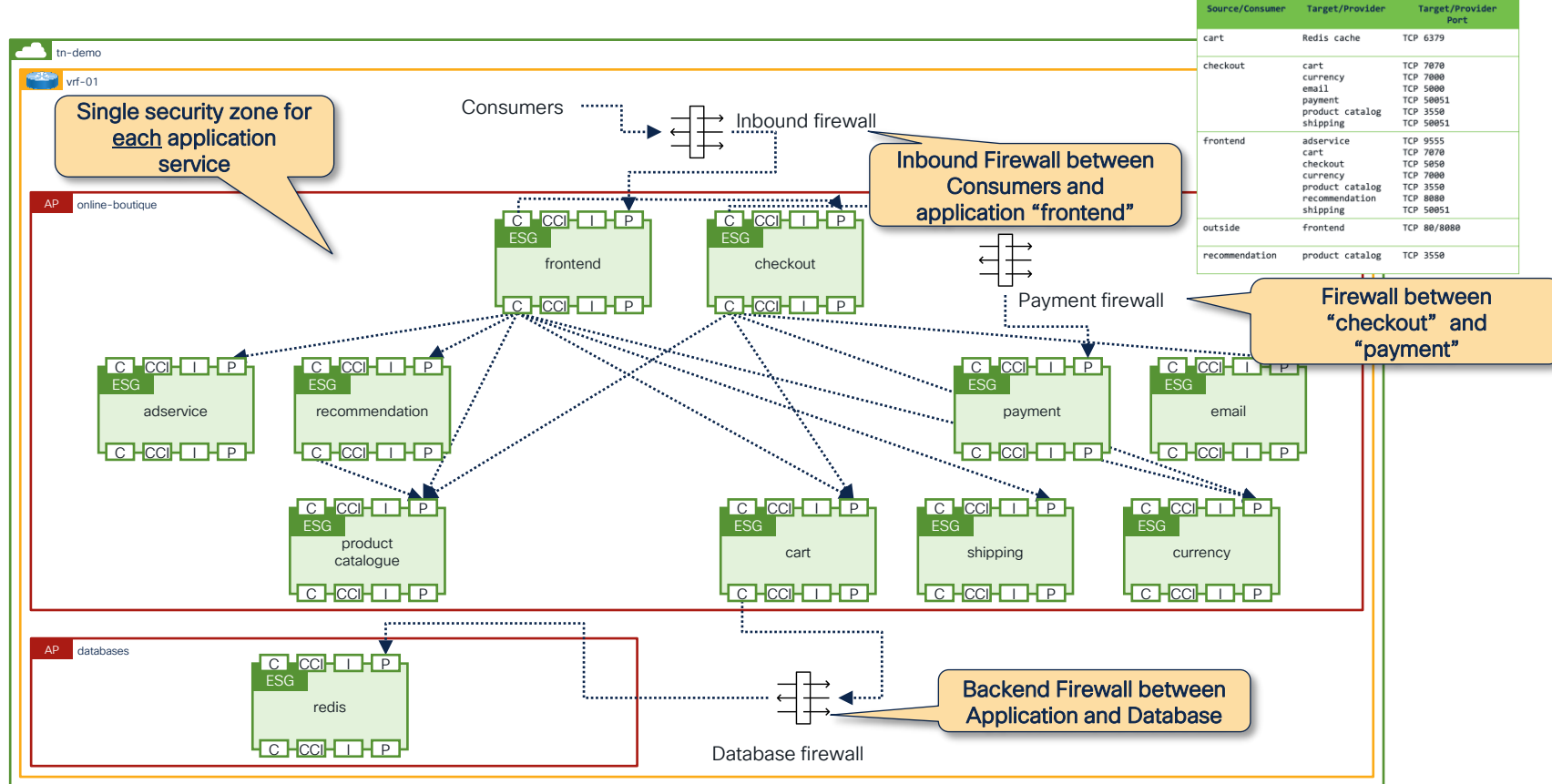


Application tiers across subnets

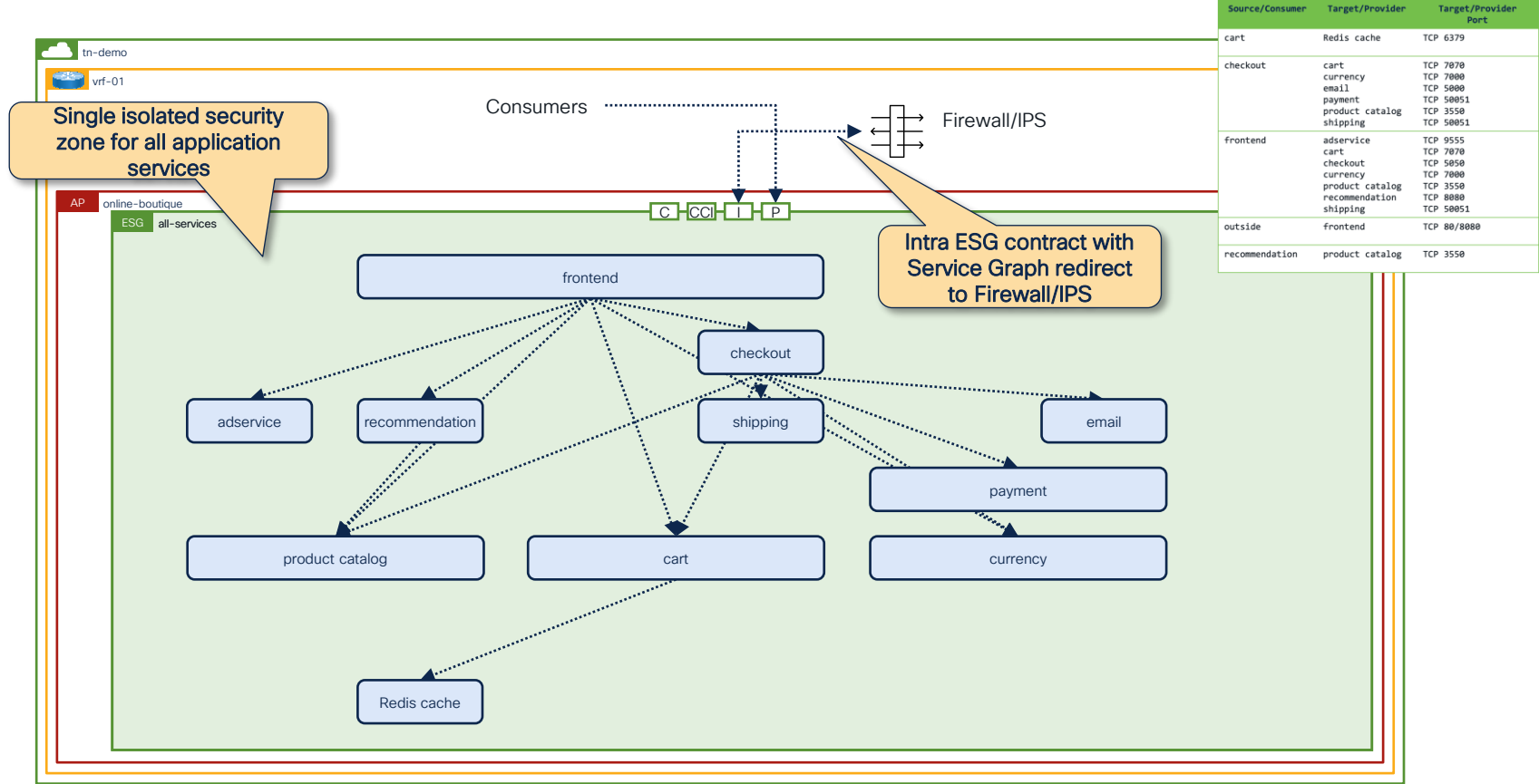


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
frontend	product catalog	TCP 3550
	shipping	TCP 50051
	adservice	TCP 9555
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

Complement ACI Contracts with Firewalls



Microsegment with FTD using Intra-ESG SG



Dynamic Attributes



FTD and ASA can leverage SGTs

Action

Block

Time Range

None

Zones

Networks

VLAN Tags

Users

Applications

Ports

URLs

Dynamic Attributes

Inspection

Logging

Comments

Available Attributes

Search by name or value

Security Group Tag

Employees

Guests

Network_Services

PCI_Servers

Point_of_Sale_Systems

Production_Servers

Production_Users

Quarantined_Systems

Add to Source

Add to Destination

Selected Source Attributes (1)

Security Group Tags

Developers

Add a Location IP Address

Add

Selected Destination Attributes (2)

Security Group Tags

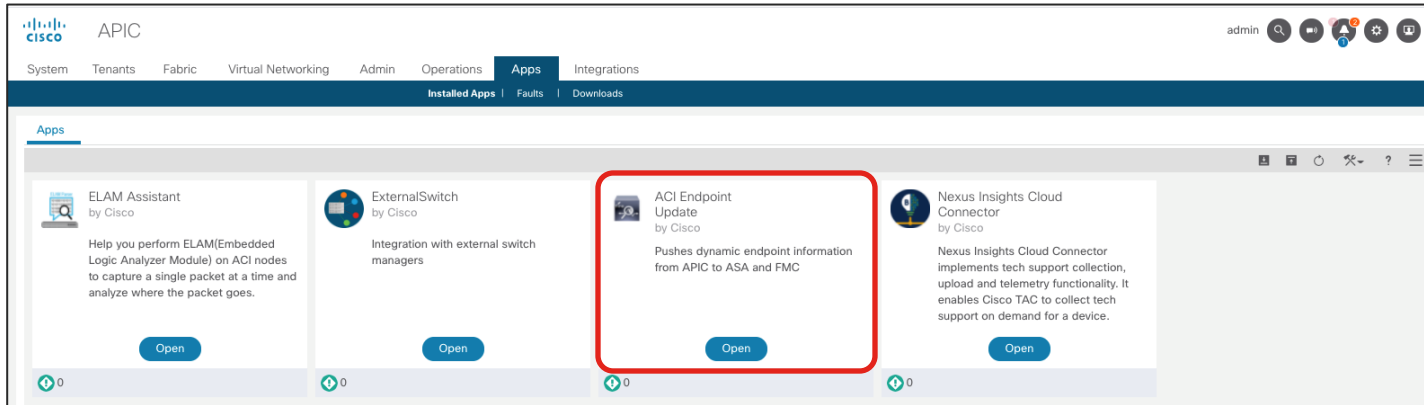
PCI_Servers

Point_of_Sale_Systems

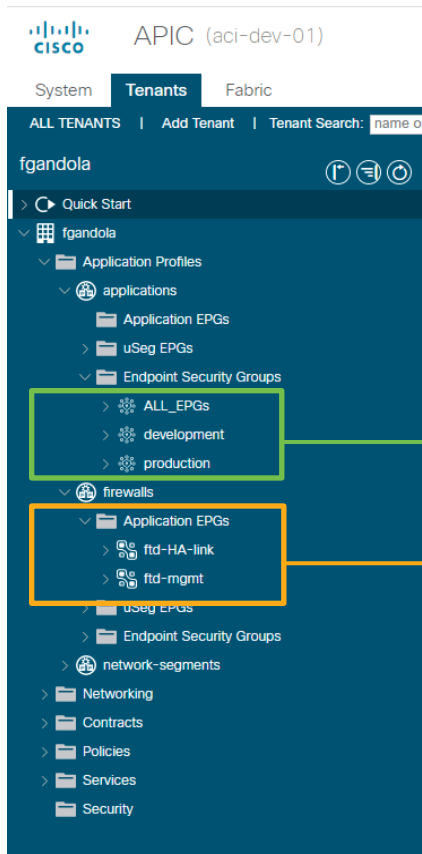
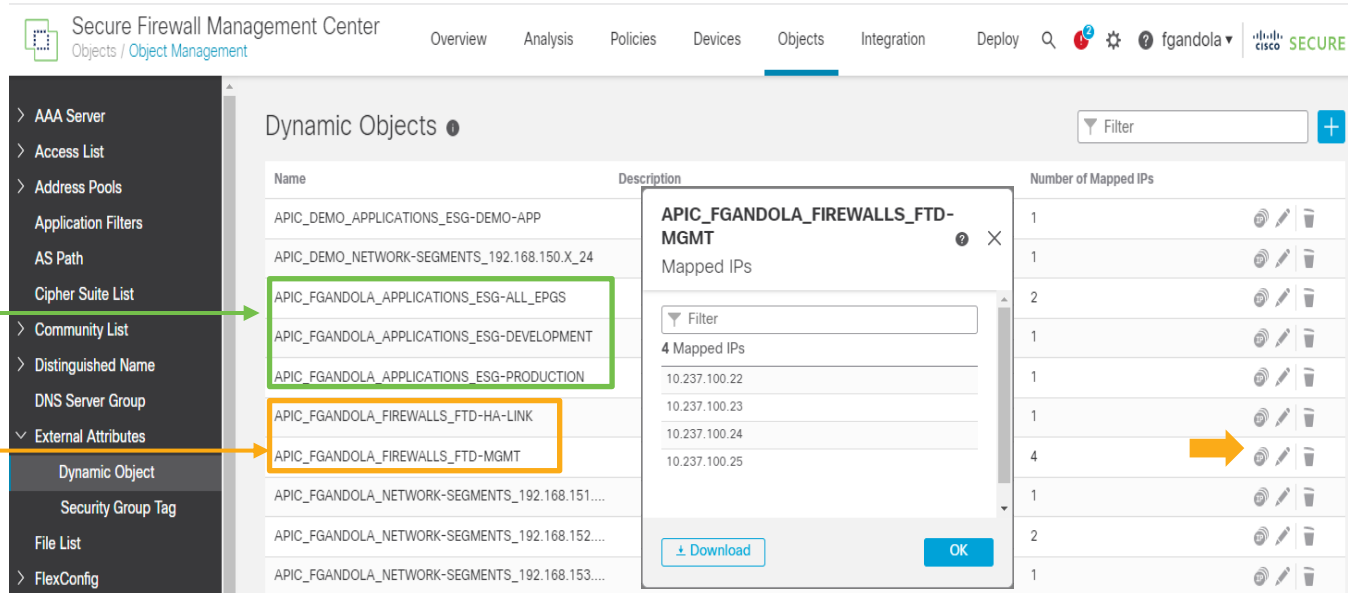
Attributes of the same type (for example, SGT) match the rule if any attribute is matched.
Attributes of different types match the rule only if all attributes are matched. [More info](#)

FMC App for APIC – FMC Endpoint Update

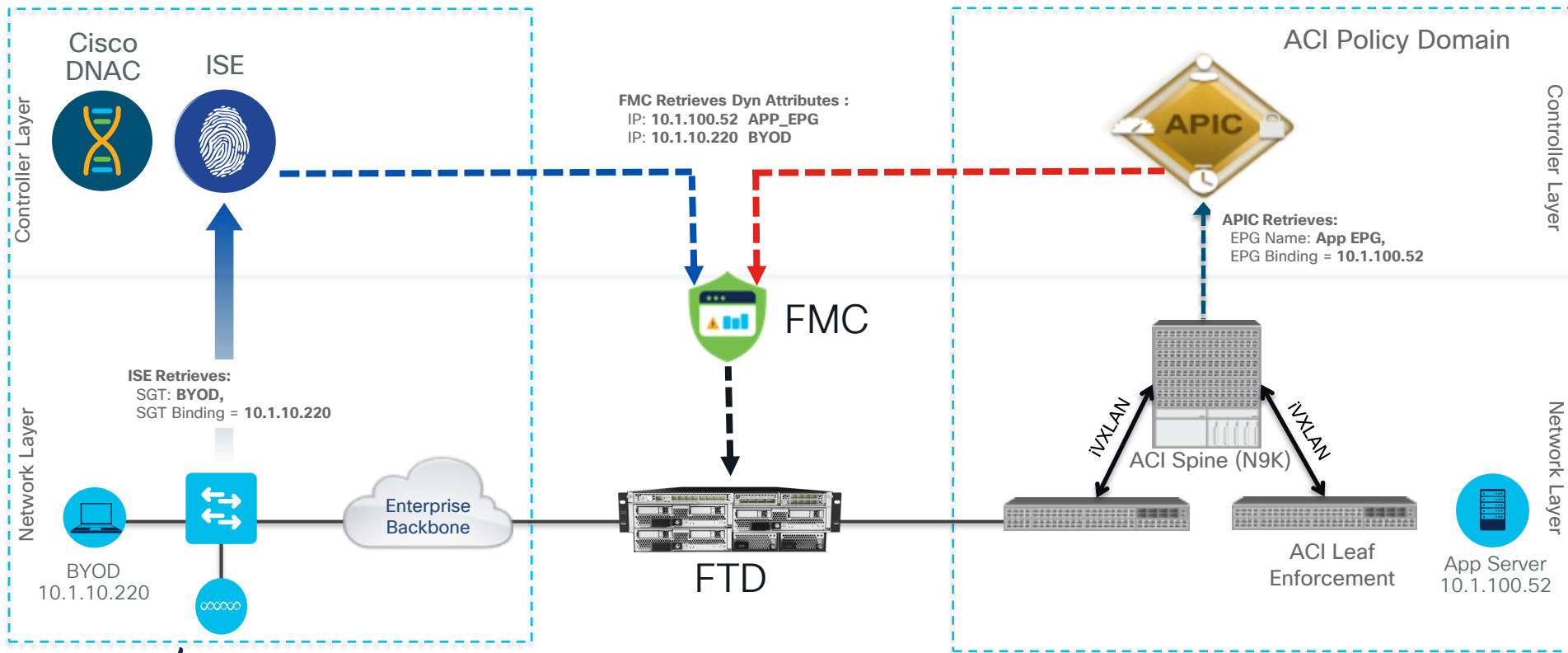
- App for APIC enables EPG updates to FMC Network Objects
- FMC is assigned per Tenant or use one FMC for all Tenants
- FTD can learn EPGs/ESGs without using a managed Service Graph
- Update interval, Tenant, Firewall Domains are configurable
- Auto-update/Dynamic Object support for deploying new config



FMC Learns EPGs/ESGs as Dynamic Attributes



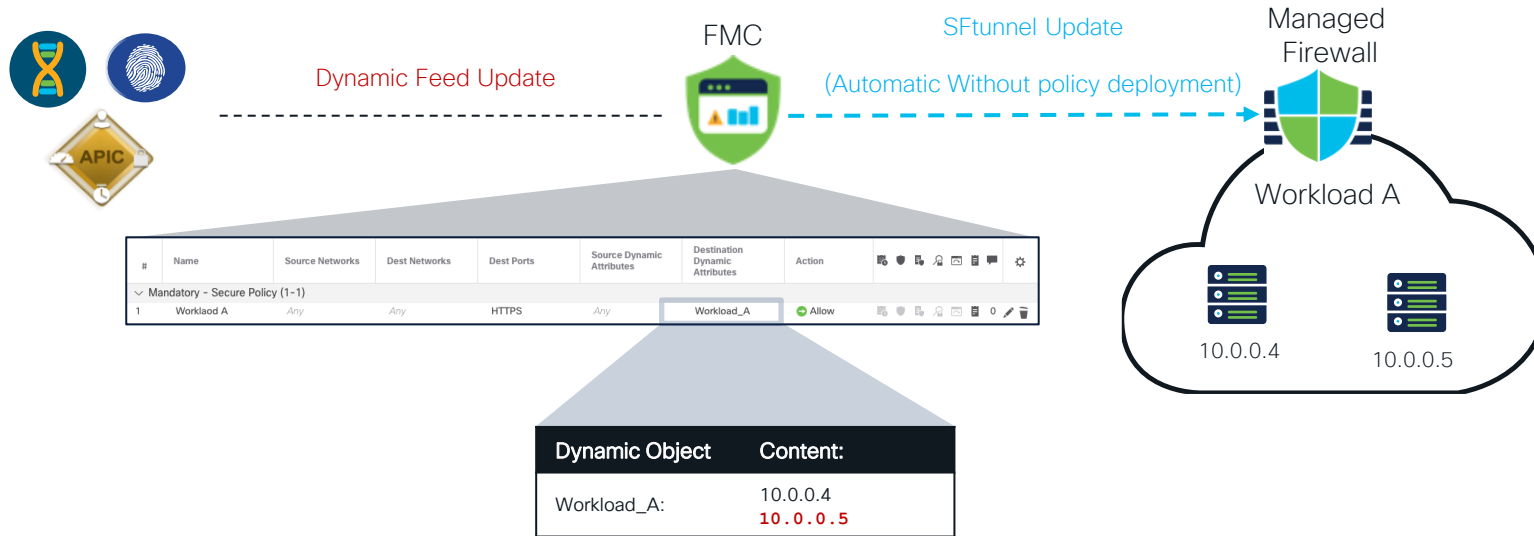
SGT/ACI Firepower Integration



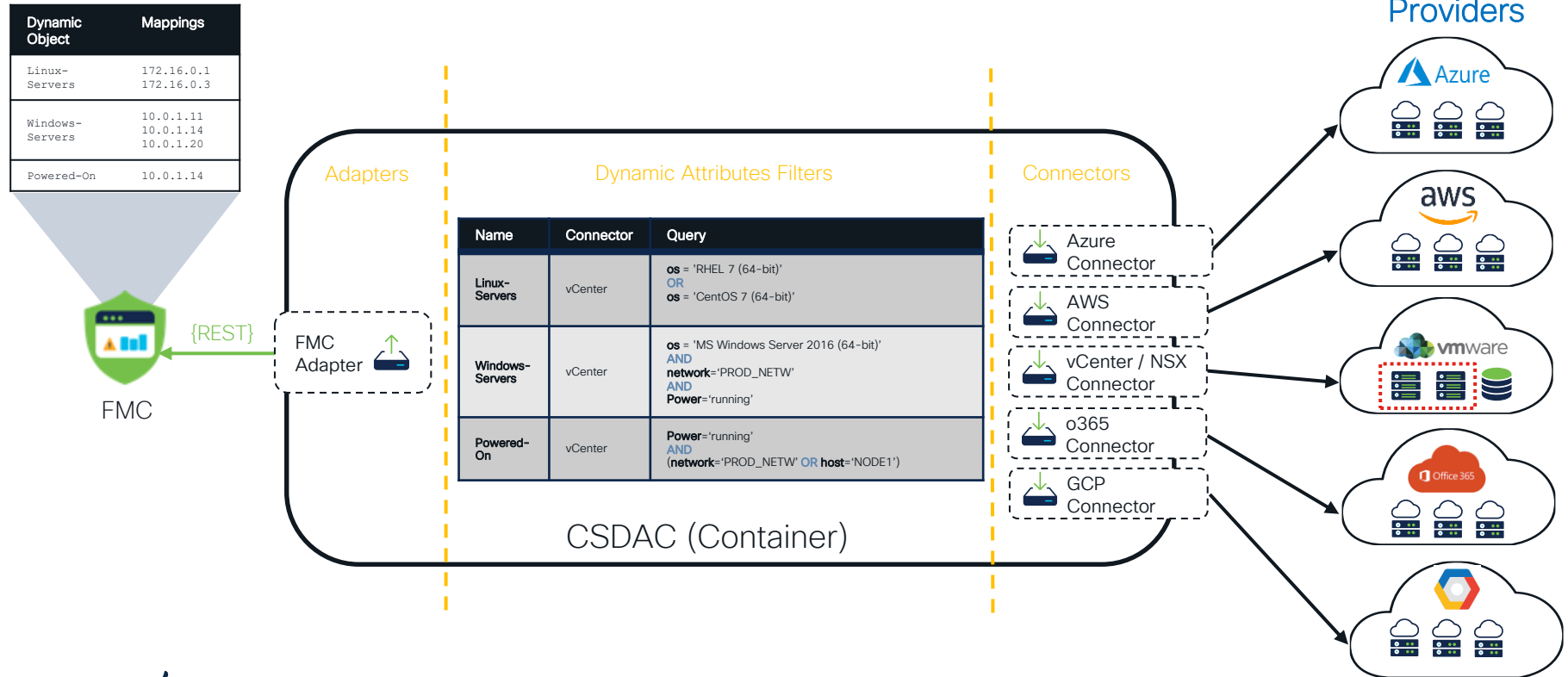
CISCO Live!

Dynamic Objects in Action

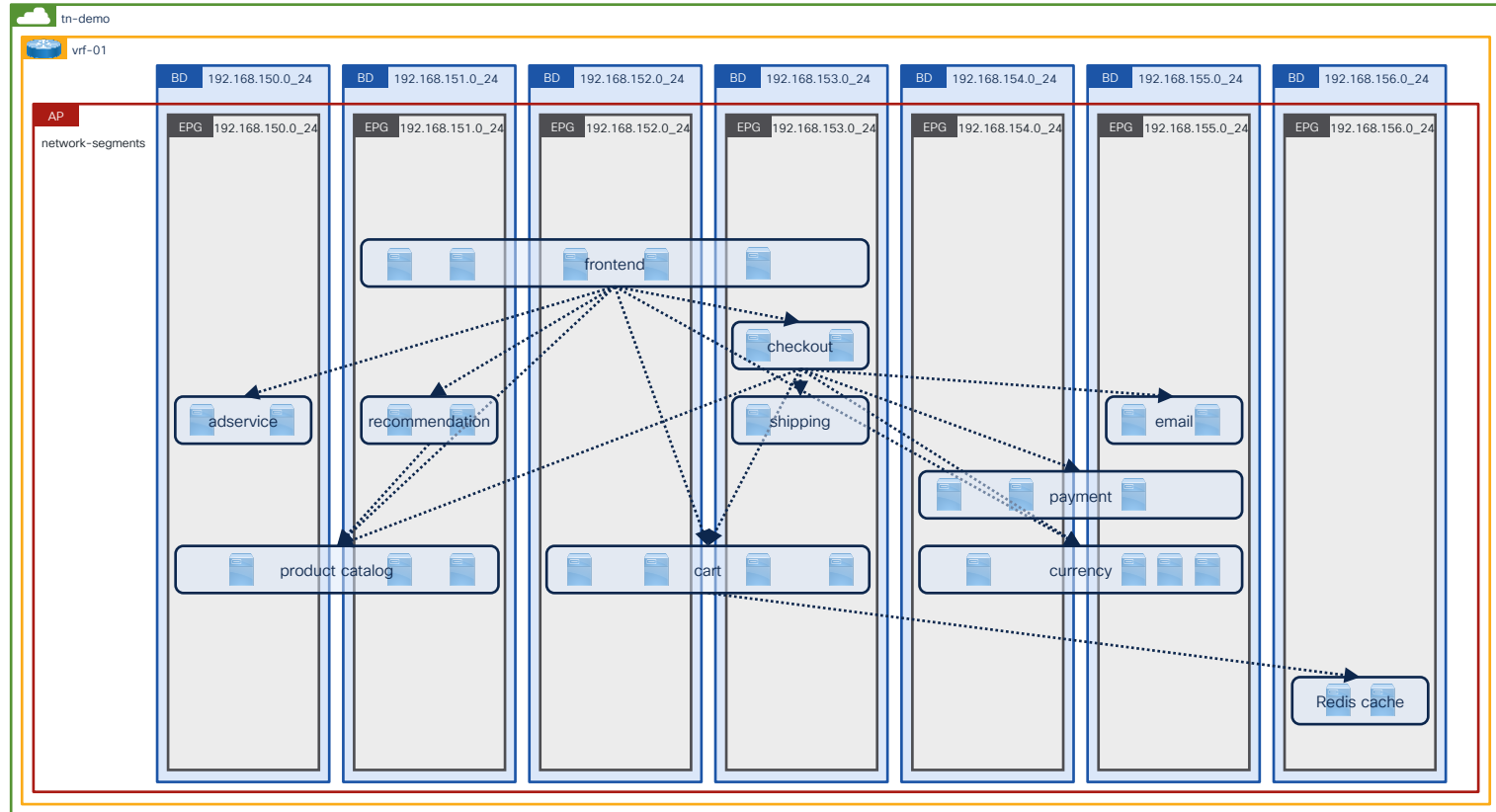
Automatic Without policy deployment



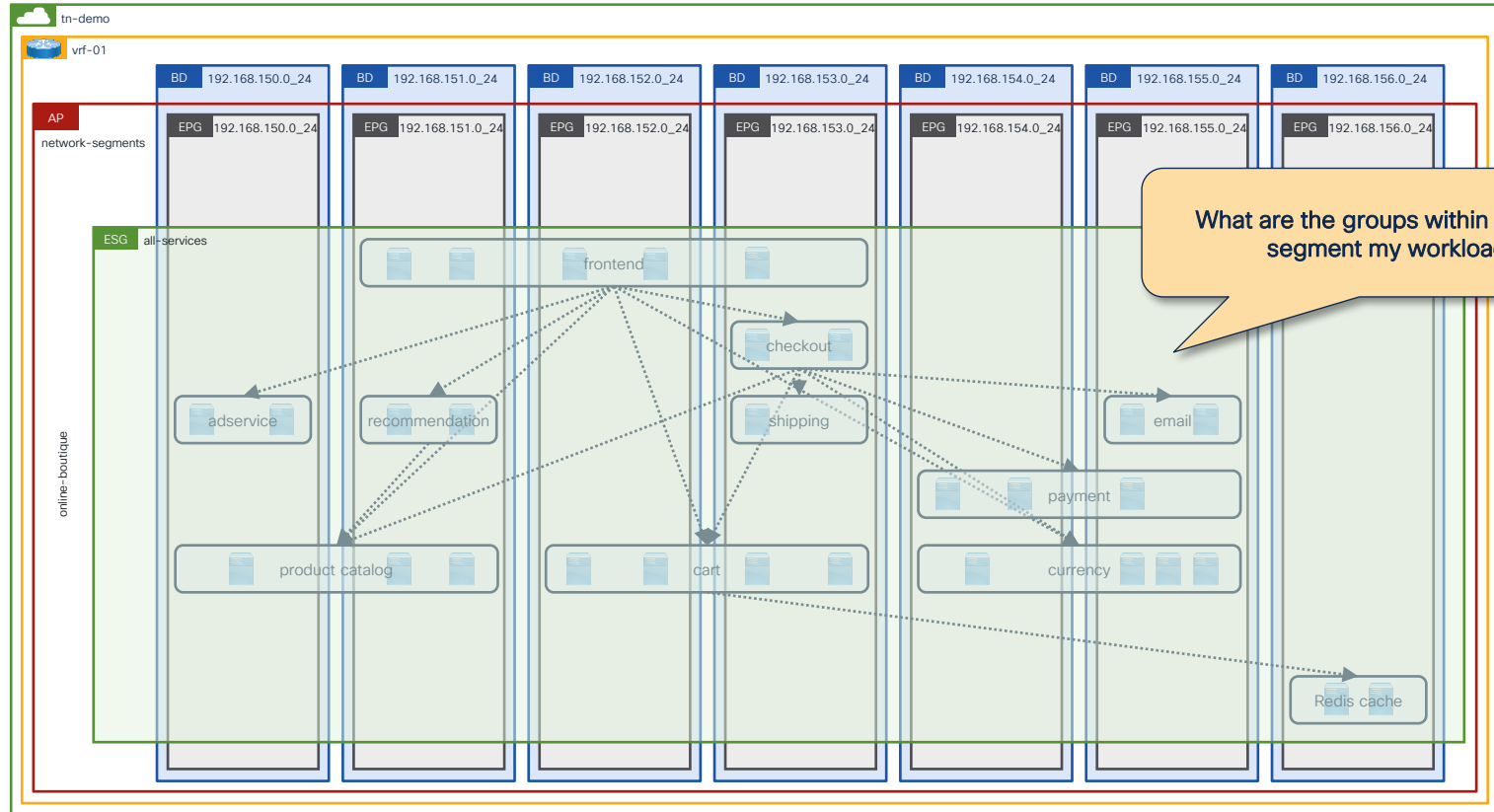
Architecture of the Dynamic Attributes Connector



Back to my Application across multiple EPGs...

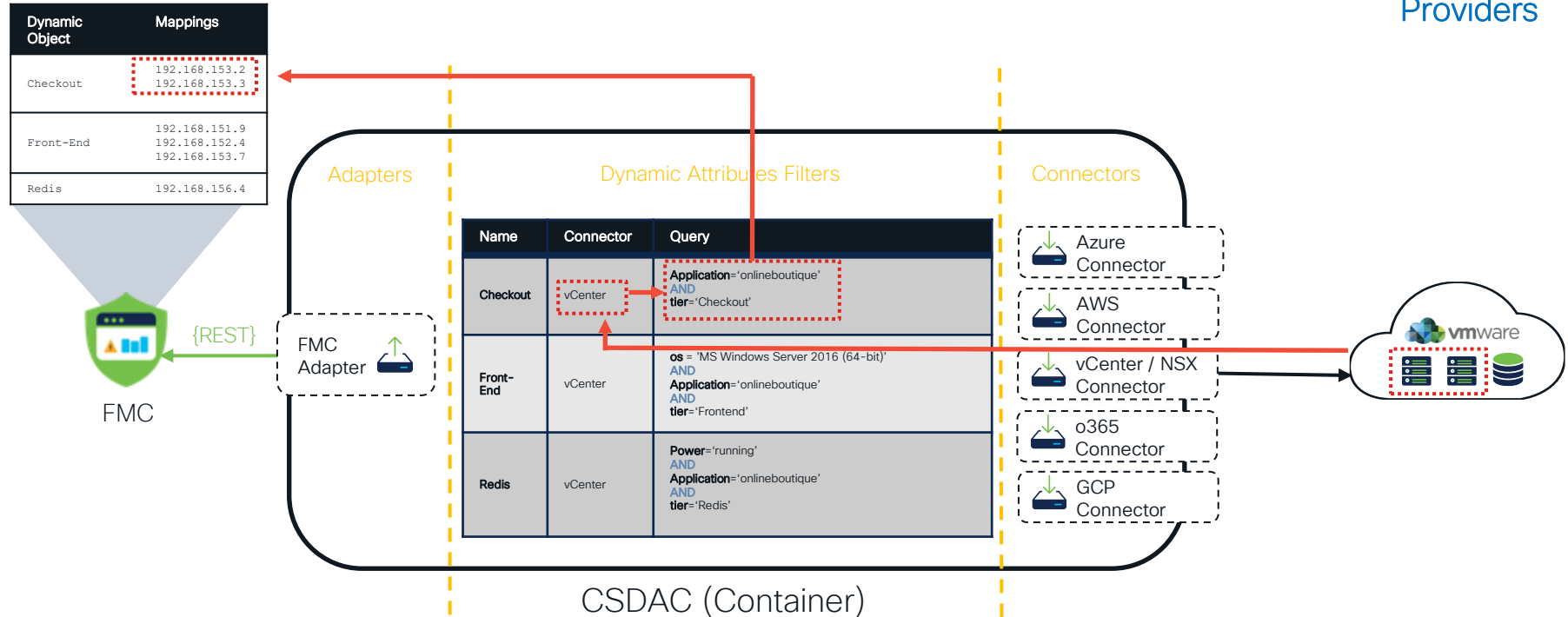


Keep my ACI design Simple

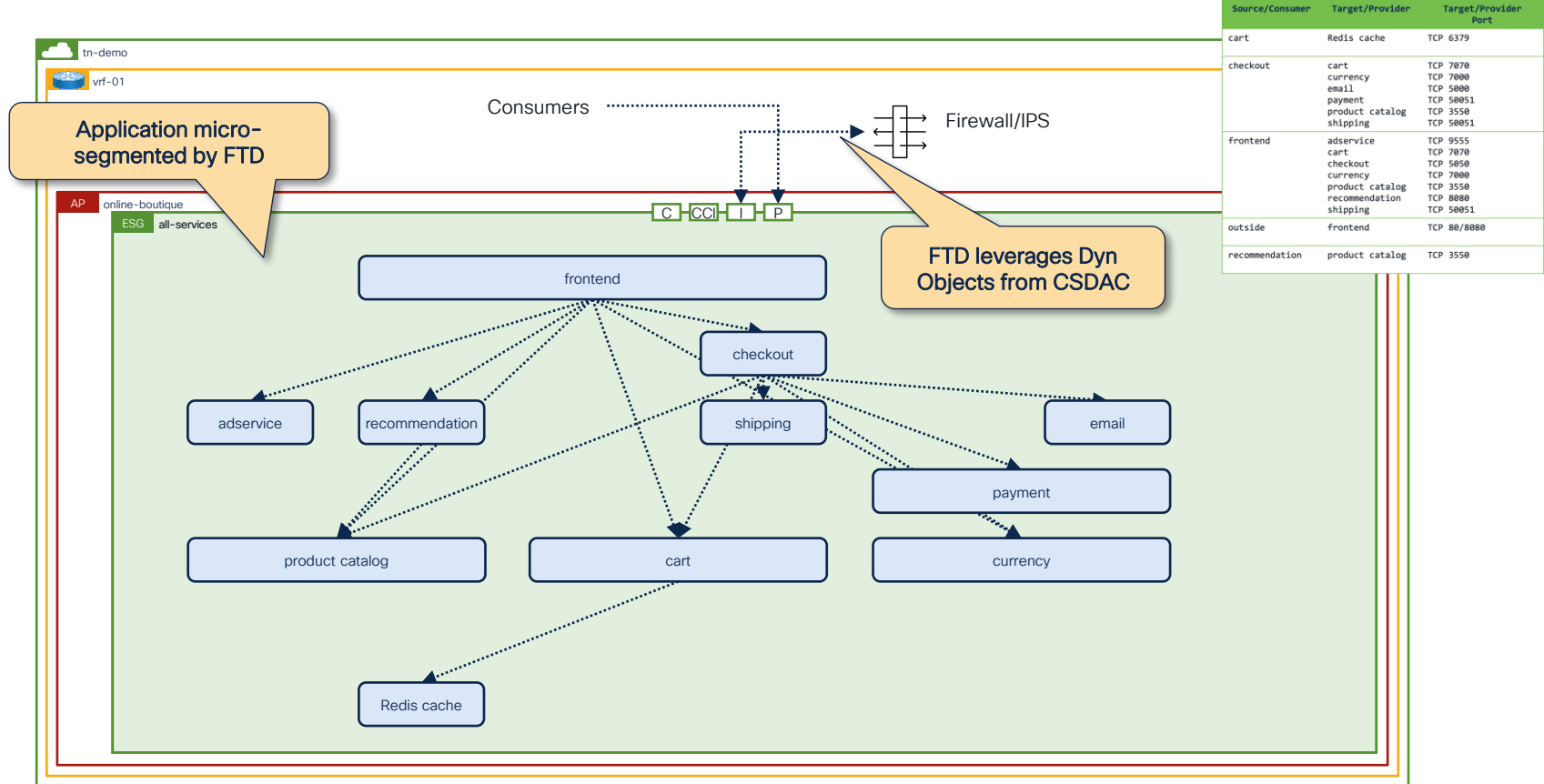


Architecture of the Dynamic Attributes Connector

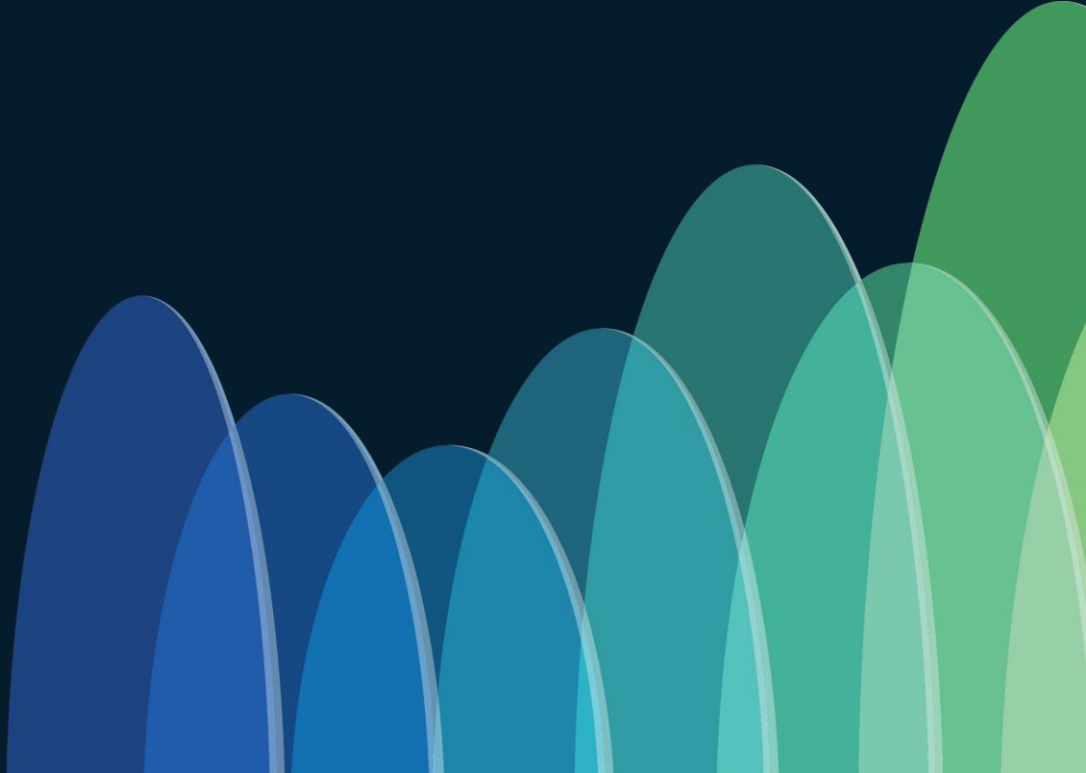
Providers



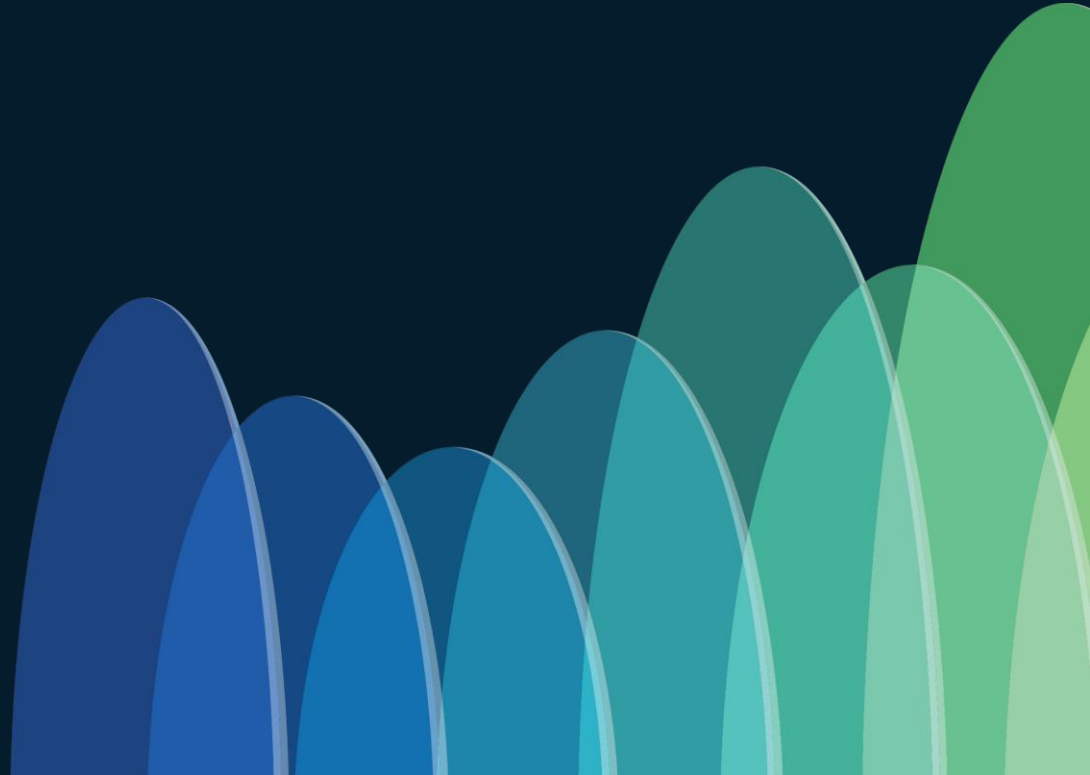
Microsegment with FTD using Intra-ESG SG



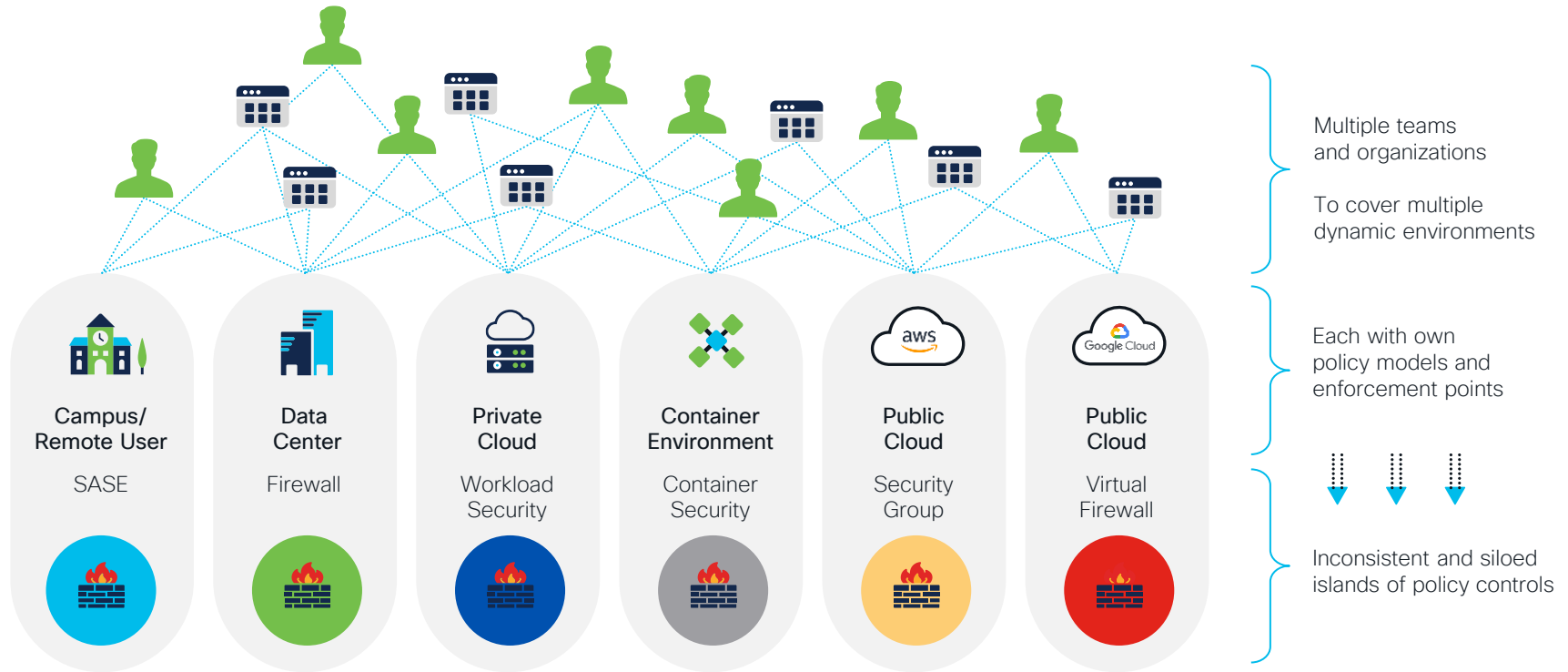
But if i don't use
FTD... I don't
have CSDAC...



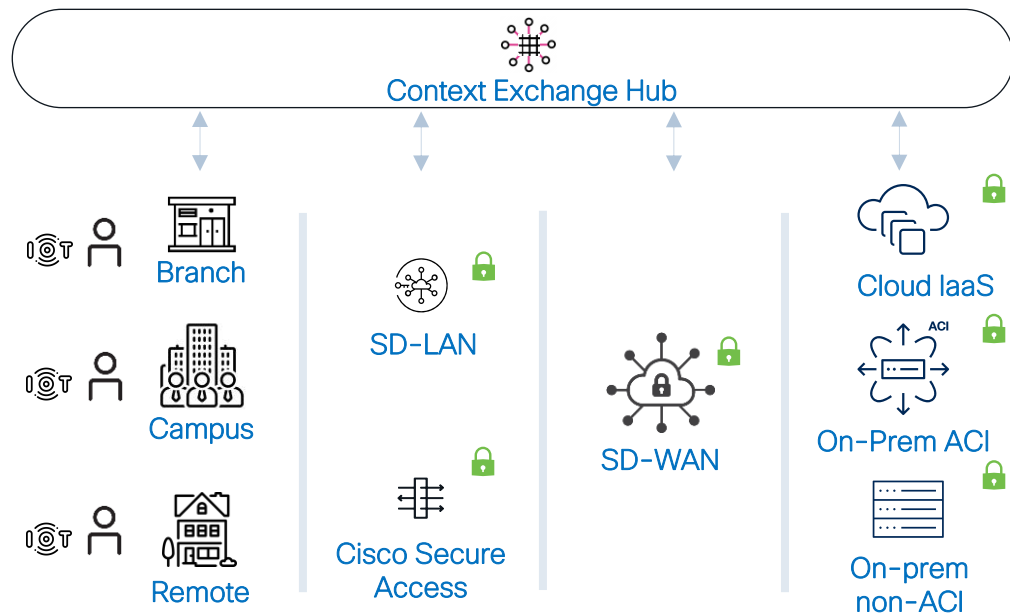
Common Policy with ISE



Why Common Policy: Policy complexity across hybrid environments



What Common Policy Enables



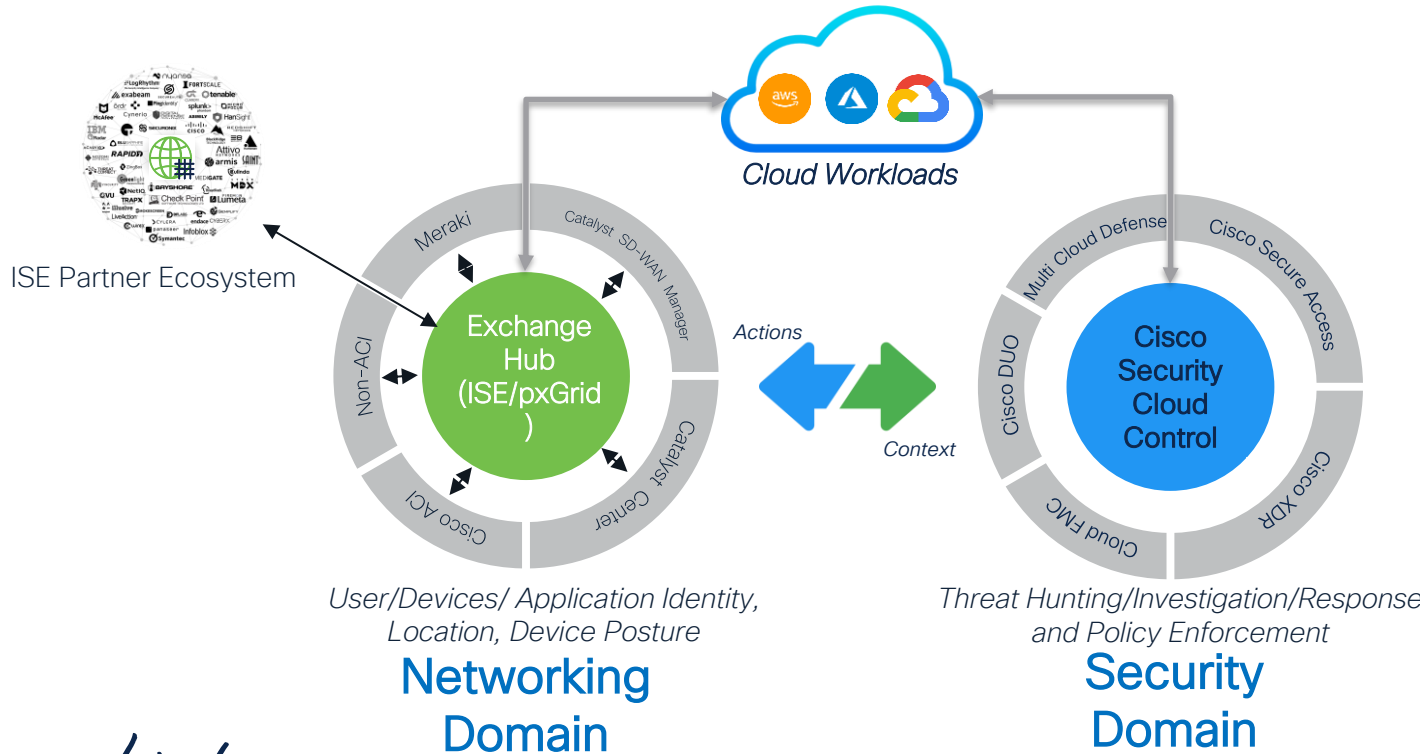
 Policy Enforcement Points: Consistent Policies

- ✓ Build context in its local domain and store it as standard security group tags (SGT)
- ✓ Share context everywhere, across networking and security domains
- ✓ Enforce consistent SGT based policies, enable simple and unified policy experience

✓ Context-aware policies for on-prem app and cloud workloads for multiple enforcement points

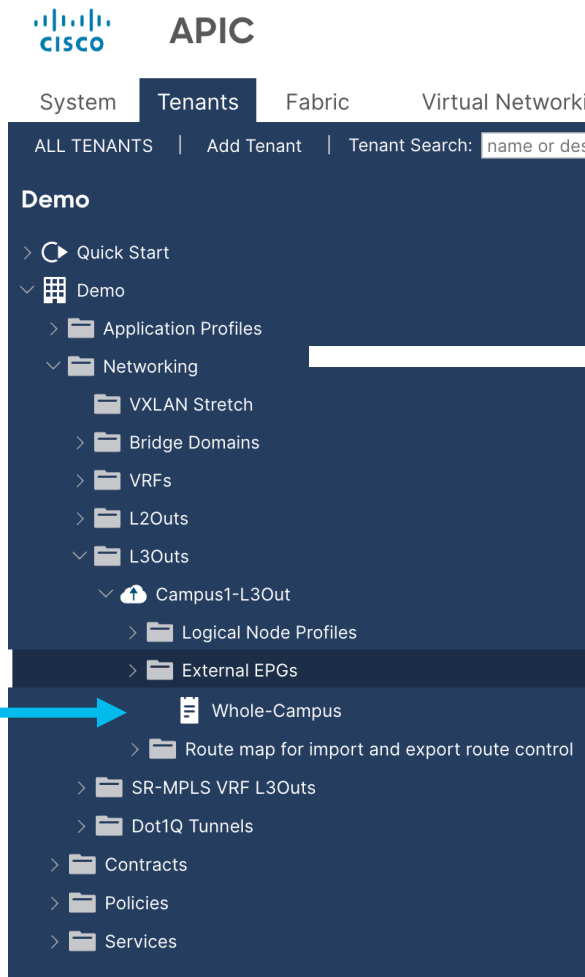
Common Policy for Cisco Networking Cloud

Normalizing and sharing context across domains

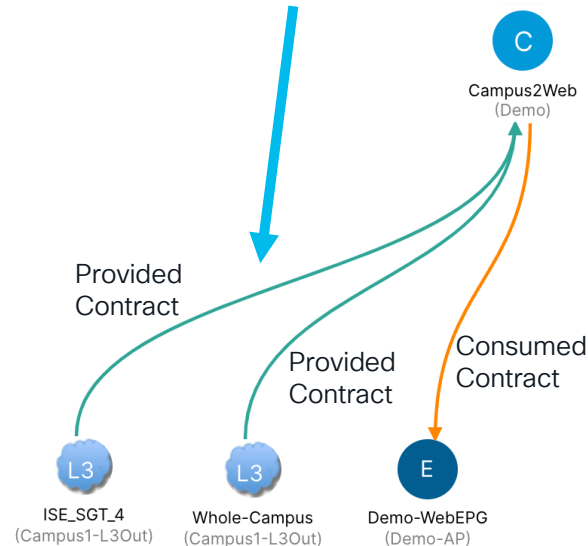


Rule Effect in APIC

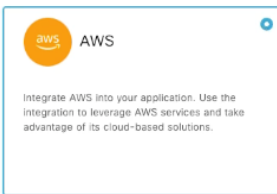
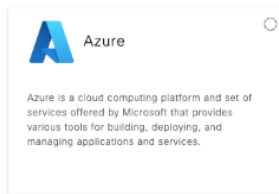
SGT added as External EPG



Newly added Group attached to existing Contract in APIC:



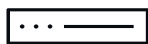
Context Learned from Cloud



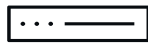
Classifying Cloud Workloads



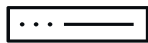
Selected Workload Attributes



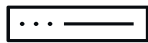
Name, IP, Security Group, Owner, OS, State...



Name, IP, Business Function, Created, State...



Name, IP, Updated, OS, State, Version...



Name, IP, Uptime, VPC, Created, Security Group...



ISE

ISE Dictionary

And / Or
Condition Assignment
Primary SGT To IP

Attributes used in classification table

Walk before you run...

How do my applications communicate ?

Does the application team know how the application communicate ?



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

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

Dynamically securing the Workload Infrastructure

Profile relationships

Full visibility of all application conversations

Automated policy

Unified policy across for all application workloads

Deploy controls

Fully automated, dynamic attribute-based enforcement

Monitor compliance

Identify communications that violate policy and block if desired



Secure your application workloads:

Learn

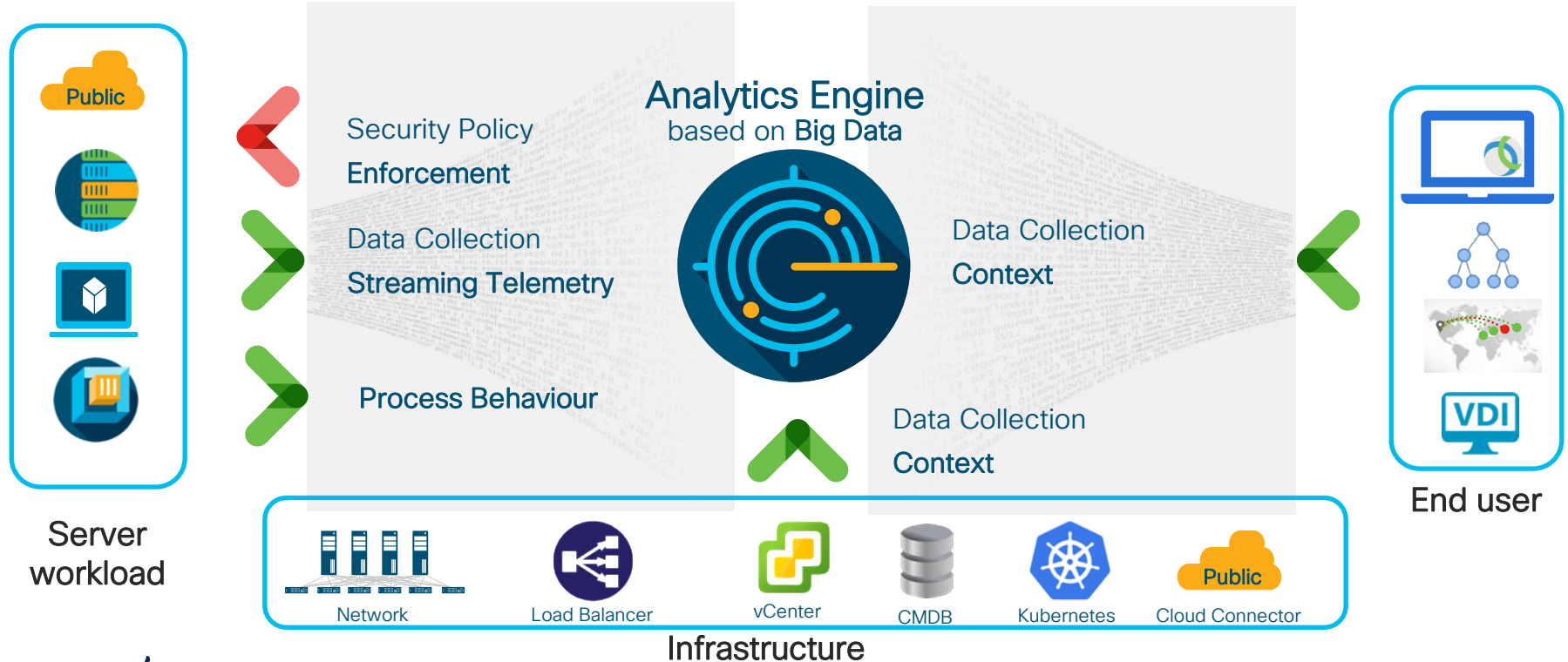
Build

Protect

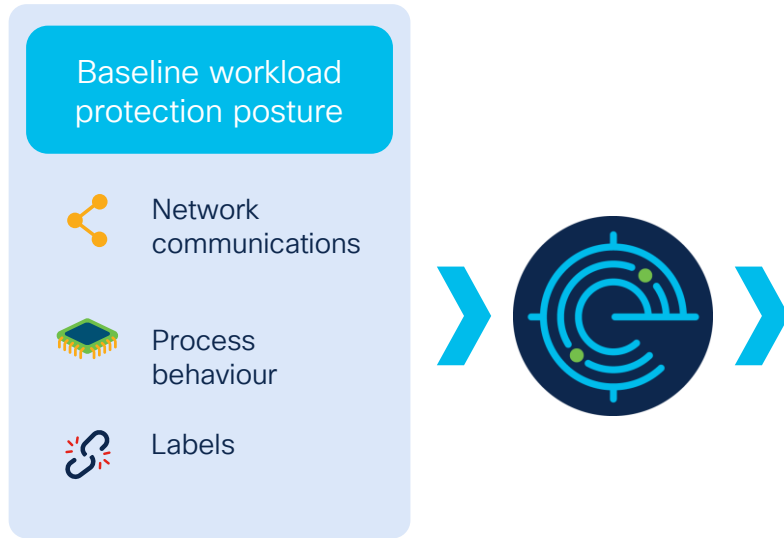
Assure



Secure Workload Architecture



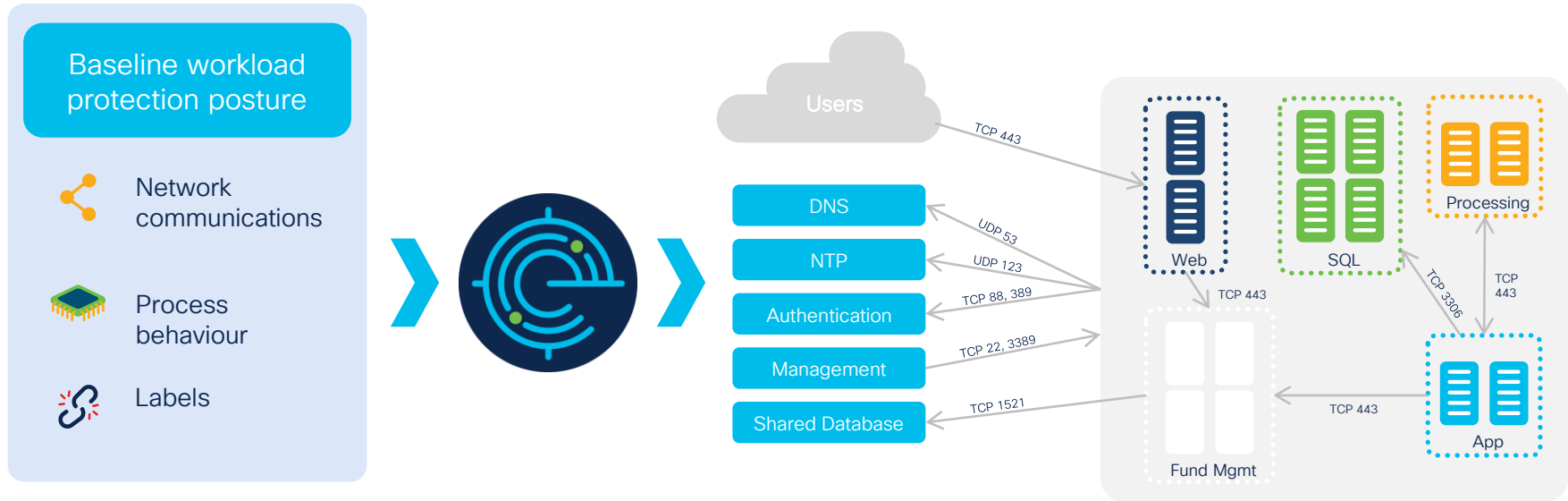
Automated Application Policy Discovery



Automated Application Policy Discovery



Automated Application Policy Discovery



Auto-generated policies

Policy list view

 Cisco Secure Workload

Workspaces

DusLab-InvoiceSystem

PRIMARY

Version 9

View Version History

Last Run: Feb 6, 2:38 PM

Automatically Discover Policies

Matching Inventories 8

Policies 14

Filters 4

Conversations 271

Provided Services 1

Policy Analysis

Enforcement Status

Enforcement

Filter Policies ...

Run Quick Analysis

Add Policy

Absolute and Default Policies 13

Catch All DENY

Grouped

Ungrouped

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

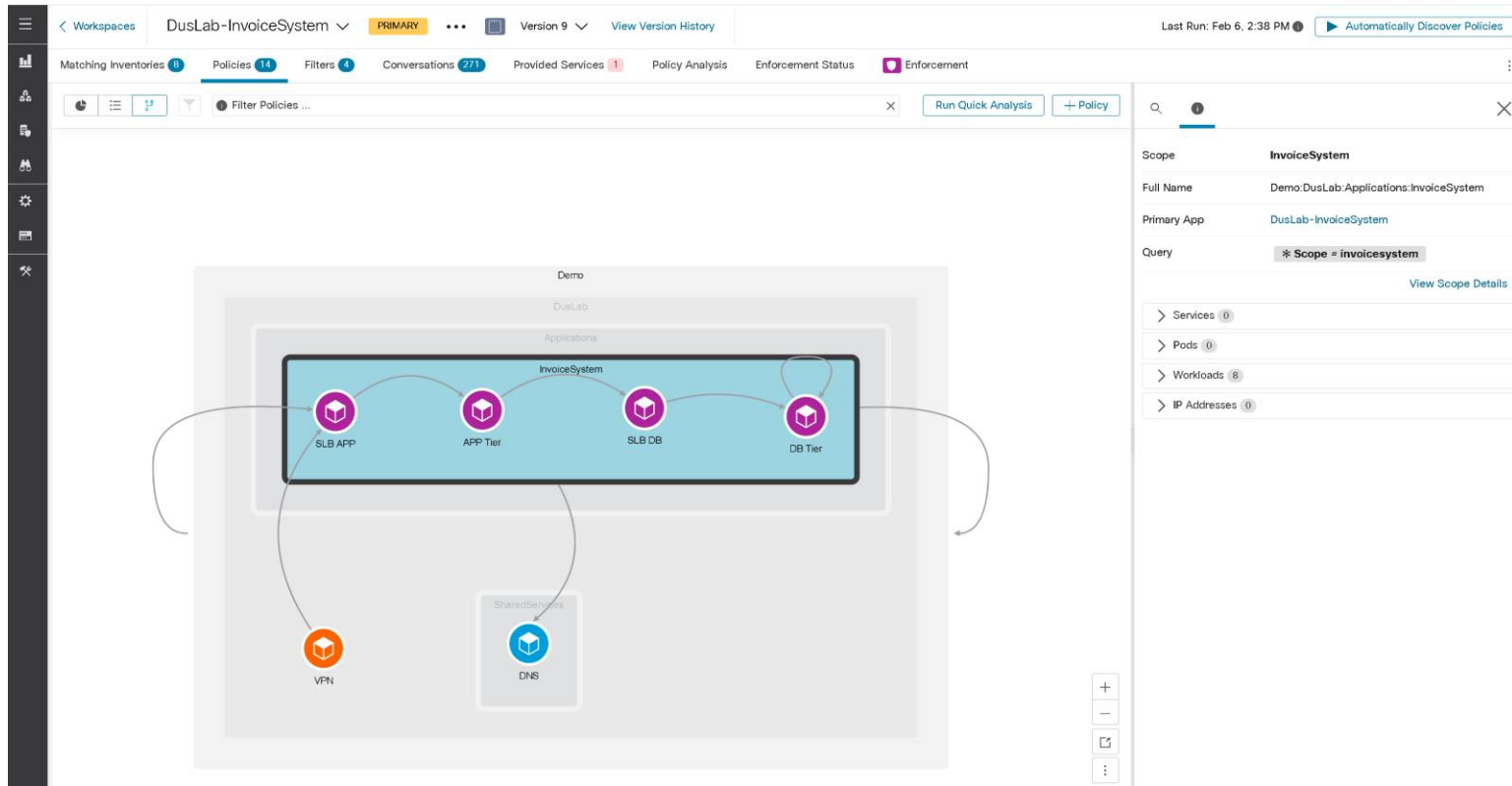
Rows per page: 20

Download table data as JSON

Download table data as CSV

Auto-generated policies

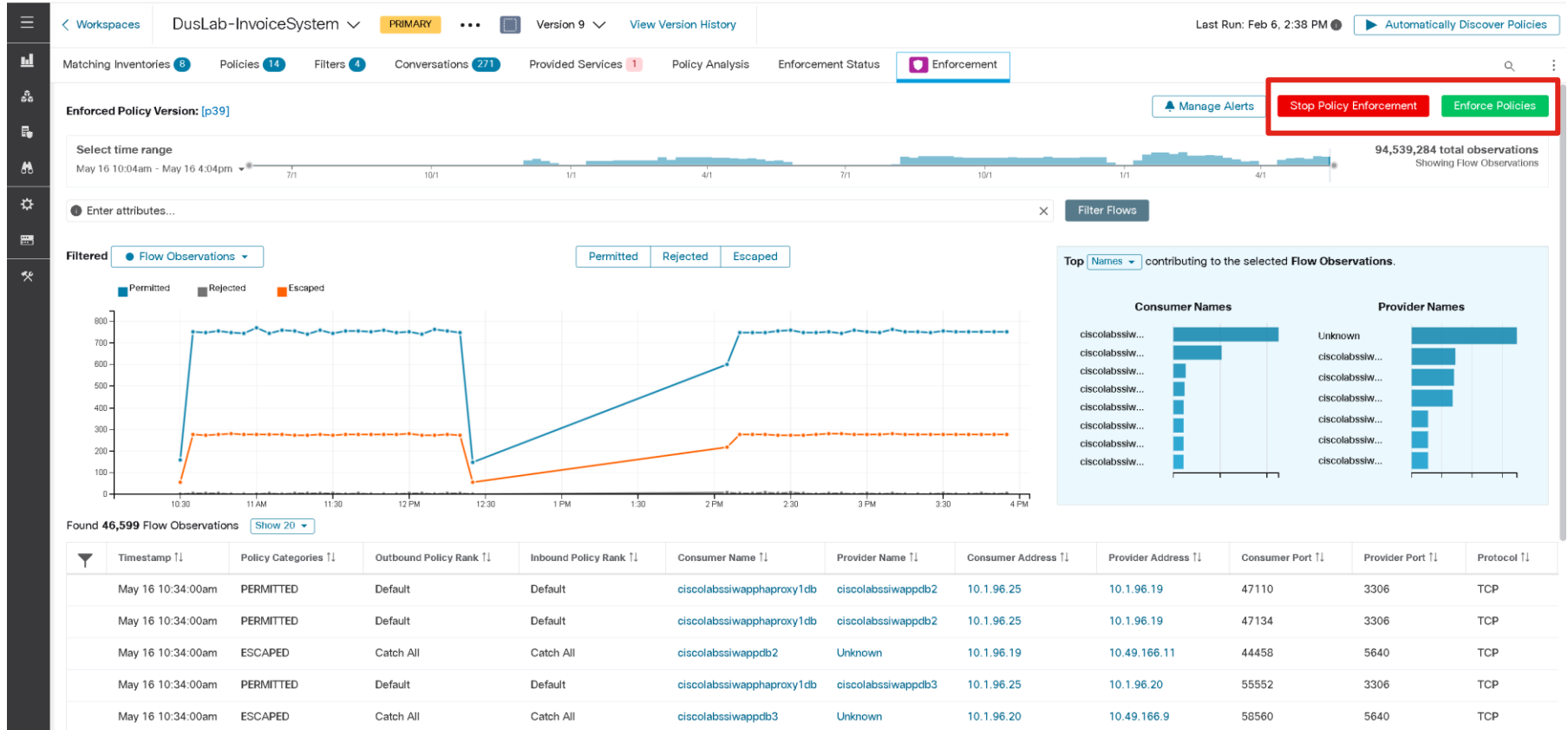
Canvas App view



One click away
from enforcement
with CSW



Policy ready to be enforced



Run Policy Experiment

Workspaces

DusLab-InvoiceSystem

Matching Inventories 8

Policies 14

Filters

Live Policy Analysis: p39

Select time range

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

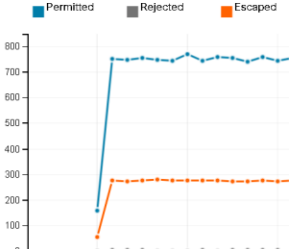
Enter attributes...

Filtered Flow Observations

Permitted

Rejected

Escaped



Found 47,211 Flow Observations

Show 20

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

Run Experiment

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

Name

CL US23 super screenshot

Start Date

05/14/2023 12:00 PM

End Date

05/15/2023 12:00 PM

Cancel

Run

Run: Feb 6, 2:30

Automatically Discover Policies

Alerts

Run Experiment

Analyze Latest Policies

94,539,896 total observations

Showing Flow Observations

to the selected Flow Observations.

Provider Names

Unknown

ciscotabssiw...

ciscotabssiw...

ciscotabssiw...

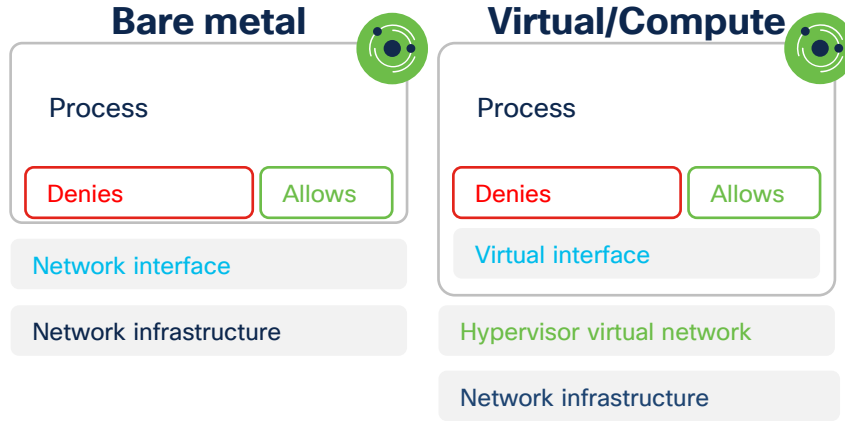
ciscotabssiw...

ciscotabssiw...

ciscotabssiw...

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

How does CSW enforce the Policy ?



Intent is rendered as security rules in native environment

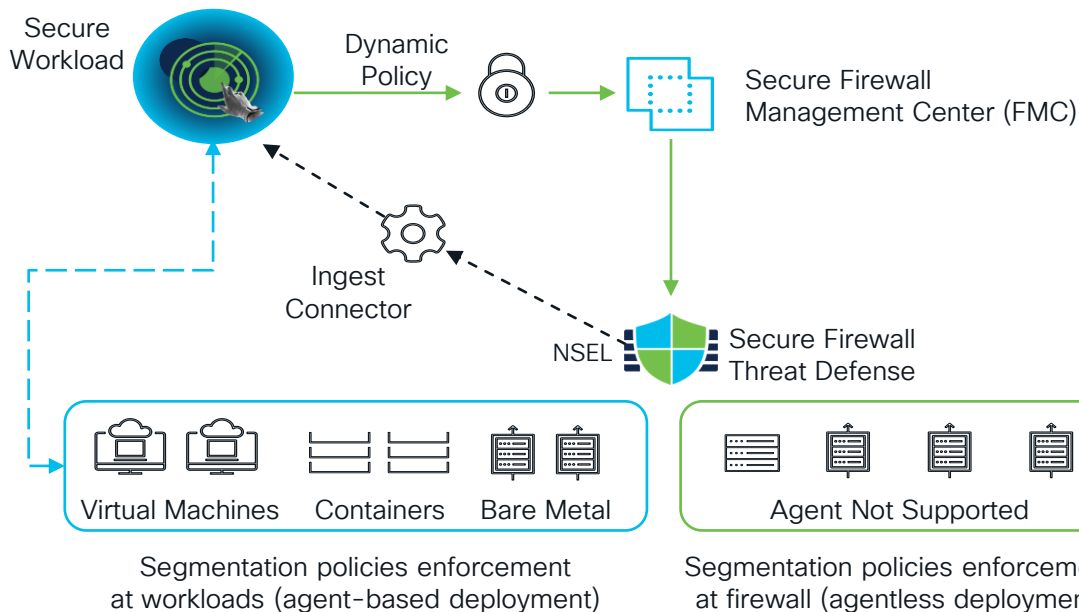
- IP sets on Linux servers
- Windows Advanced Firewall or Windows Filtering Platform on Windows servers

No big fan
of using agents ?



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

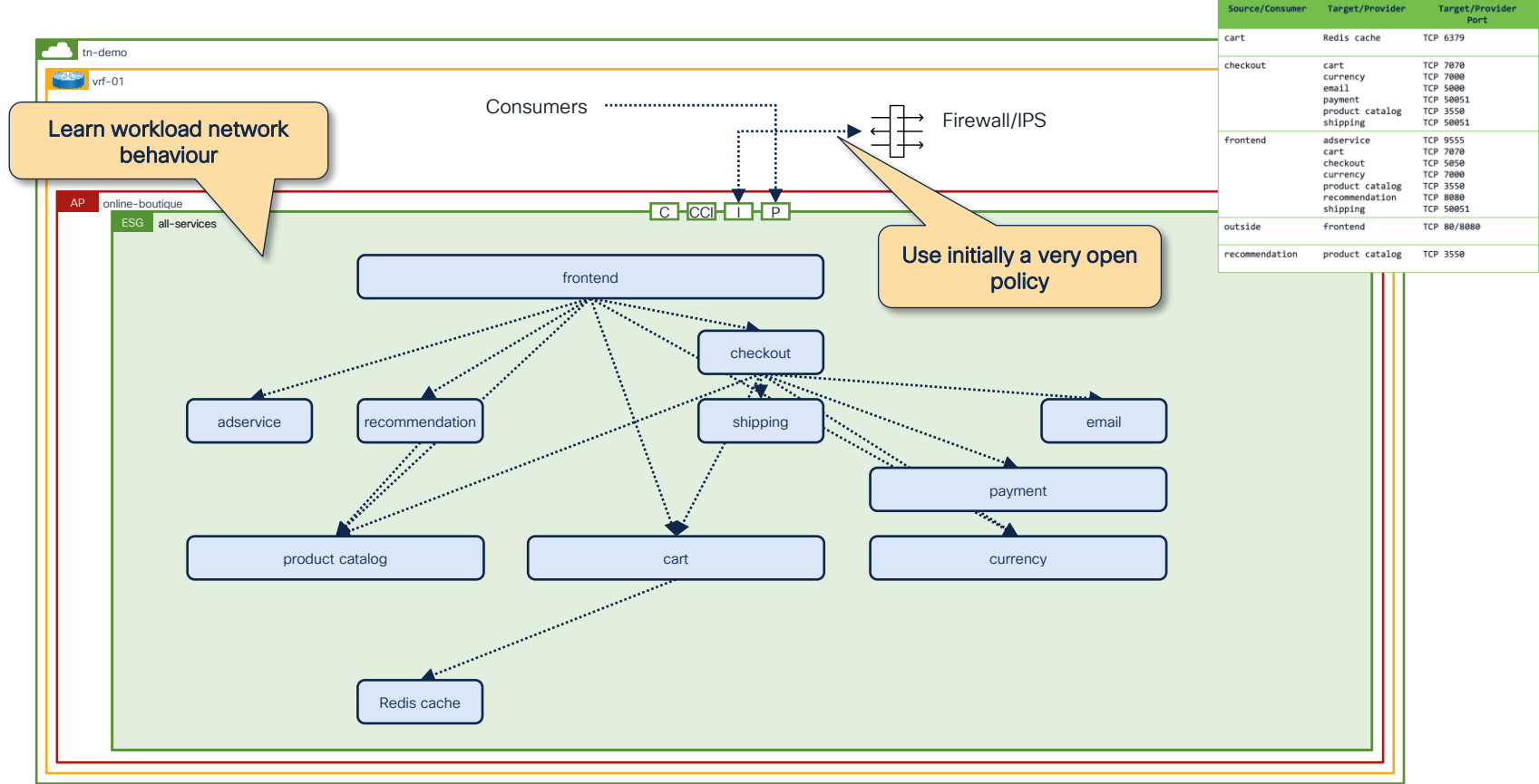


Topology aware policy enforcement



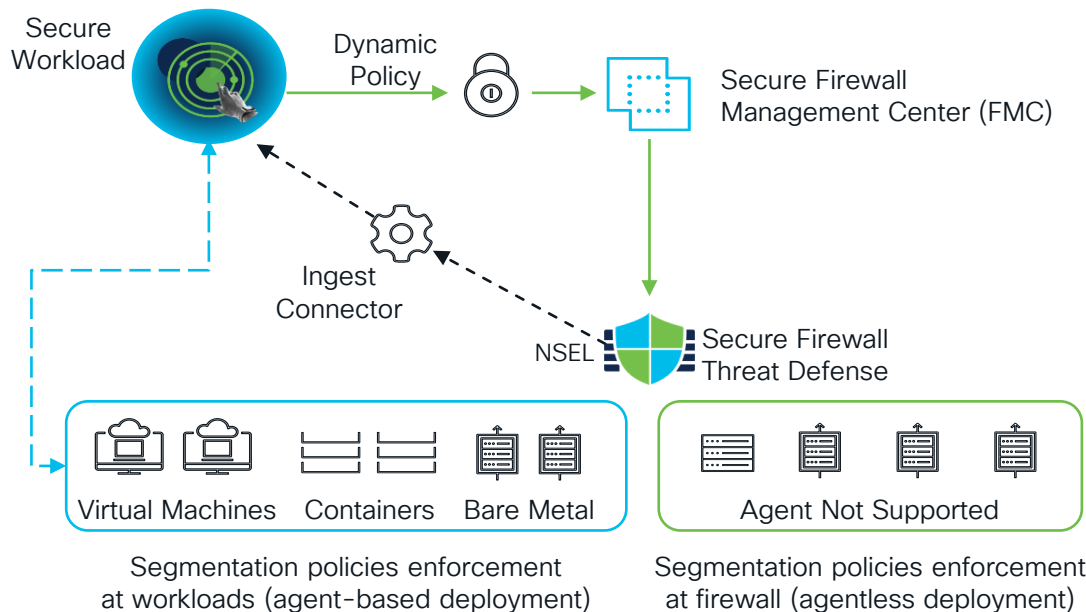
Support deployment across multicloud

Use FTD to generate Netflow data for CSW



CSW-FMC Integration And Enforcement

Defense-in-depth Use Case



Defense in depth



Support access control policy and dynamic object



Improved rule ordering



FMC domain awareness

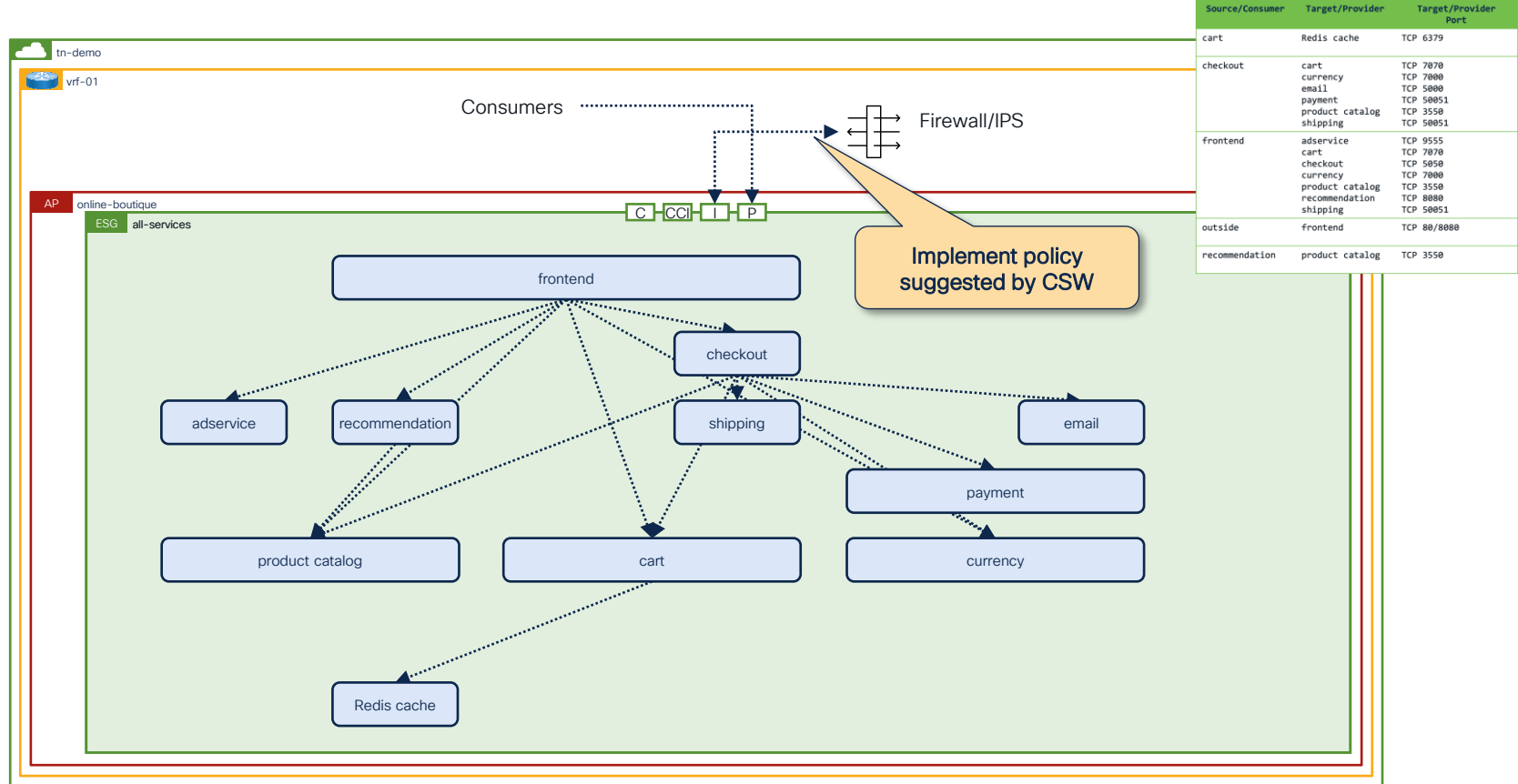


Topology aware policy enforcement

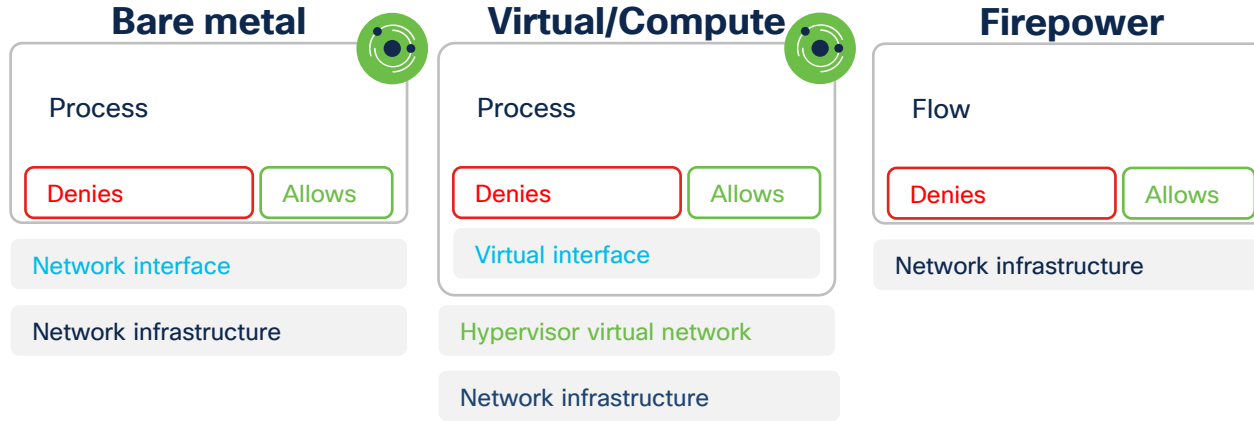


Support deployment across multicloud

Enforce automatically Policy from CSW



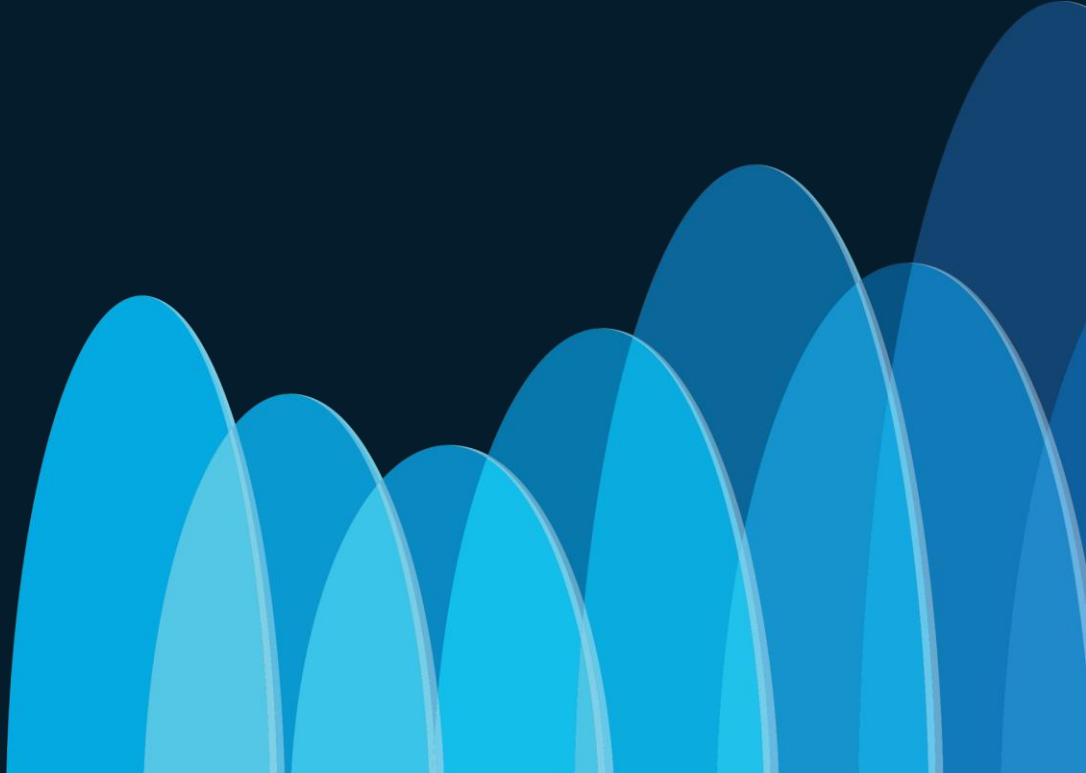
How does CSW enforce the Policy ?



Intent is rendered as security rules in native environment

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

Segmentation in the cloud



Three new parameters to consider in Cloud



Do you know what's in the
Cloud ?

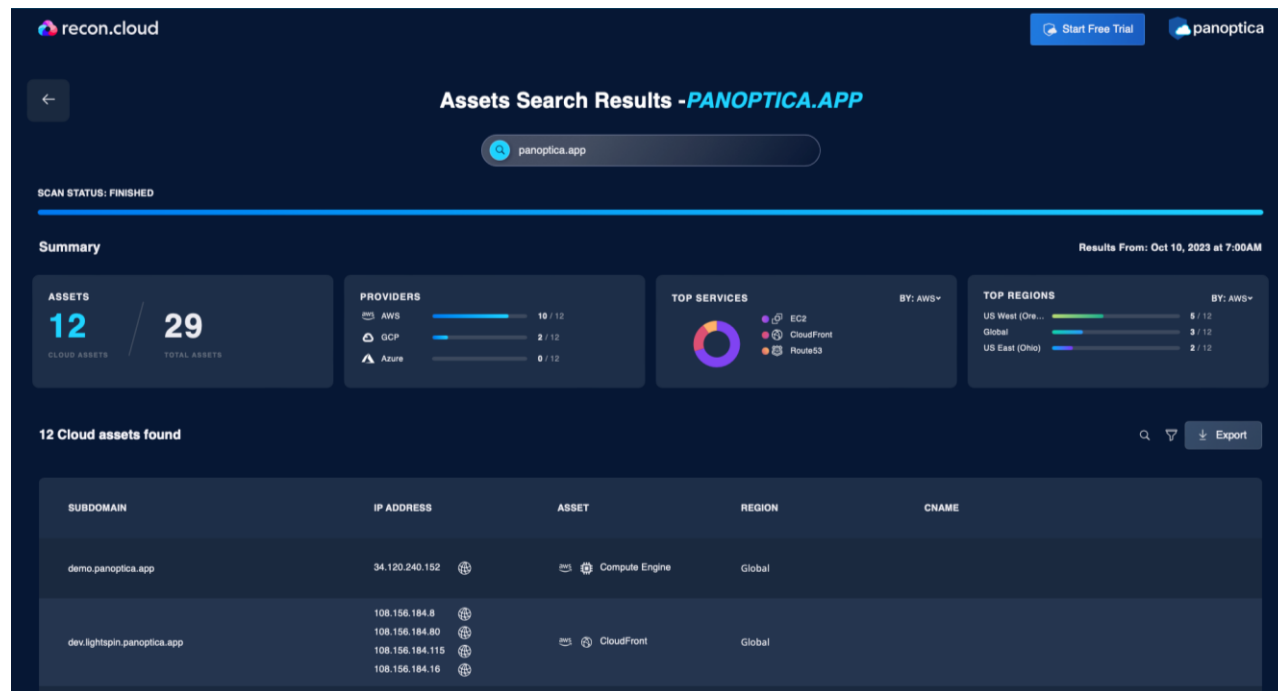
What your developers didn't tell you

- Apps are growing at a pace, and security has no clue till an incident/audit happened
- Can I get a view of my external facing apps?
- What cloud providers are being used?
- Are my external facing apps exposed or vulnerable?



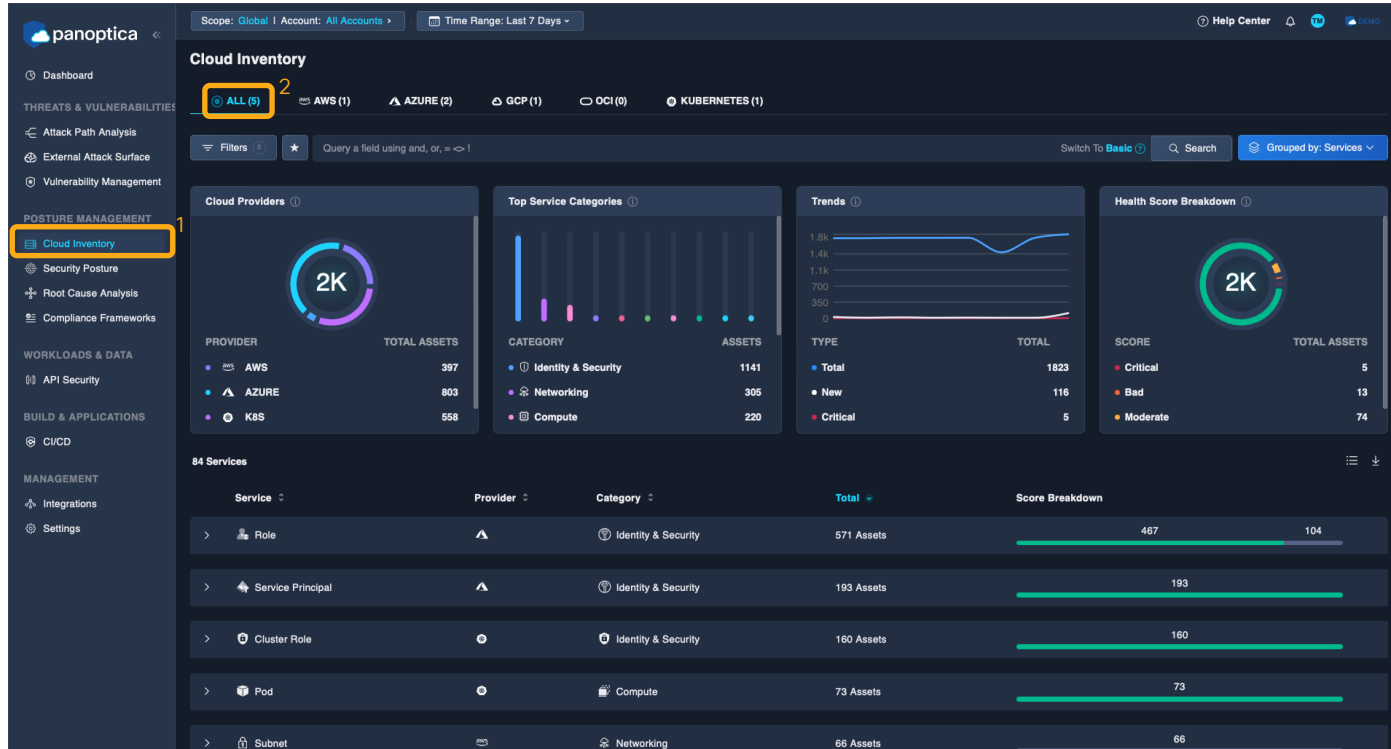
Explore your External Attack Surface

Recon.cloud is a free option that provides a view into your attack surface from the perspective of an attacker.



Cloud Inventory

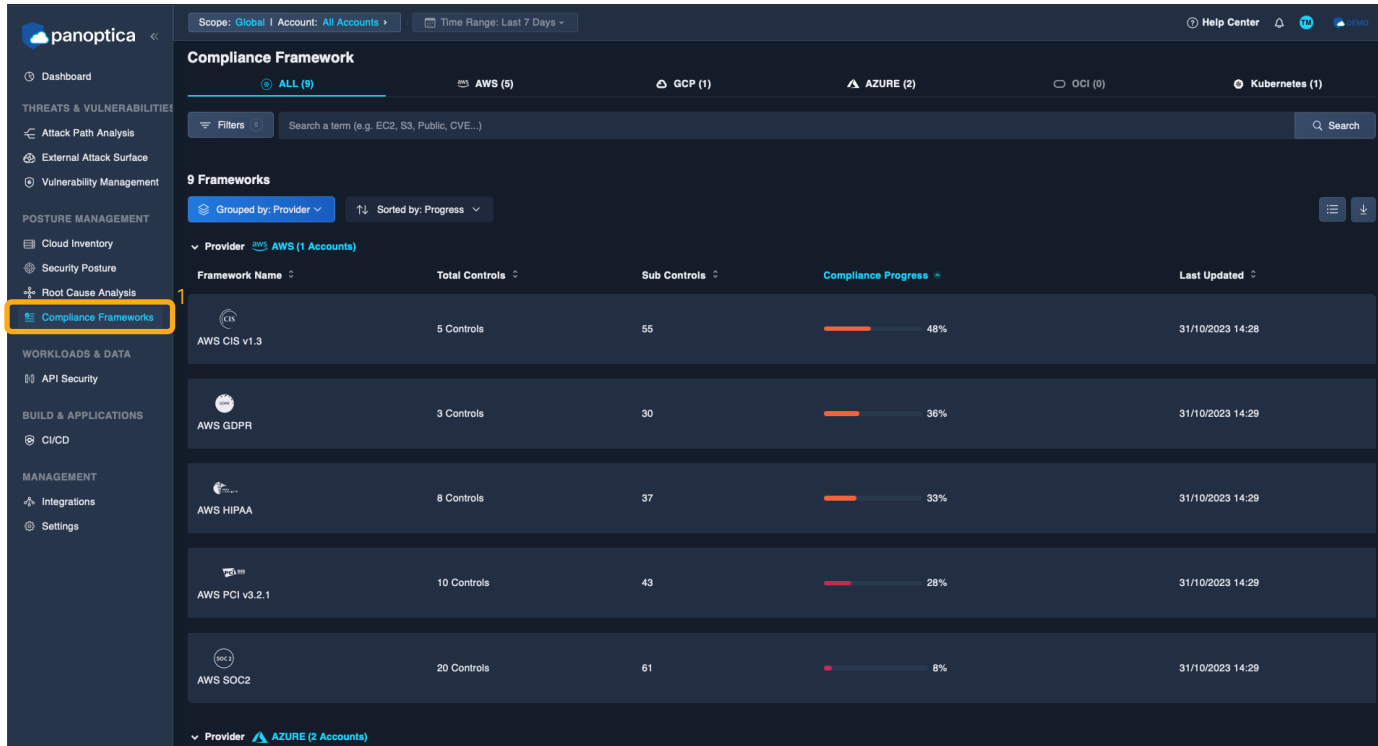
Unified view of assets across all your clouds



Comprehensive view of all your cloud assets, including health scores, trending information, and easy to navigate service groupings.

Compliance Framework

Establish cloud presence baselines against established standards



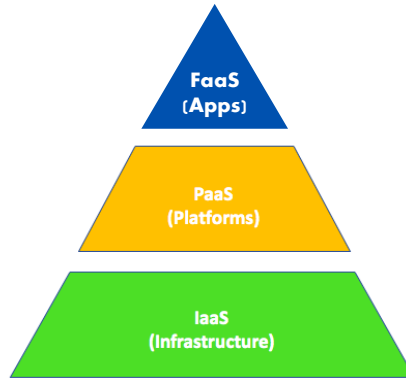
Businesses need to understand the overall health of their cloud and apps.

Panoptica provides a range of compliance frameworks against which you can gauge the relative security of their deployments.

Three new parameters to consider in Cloud

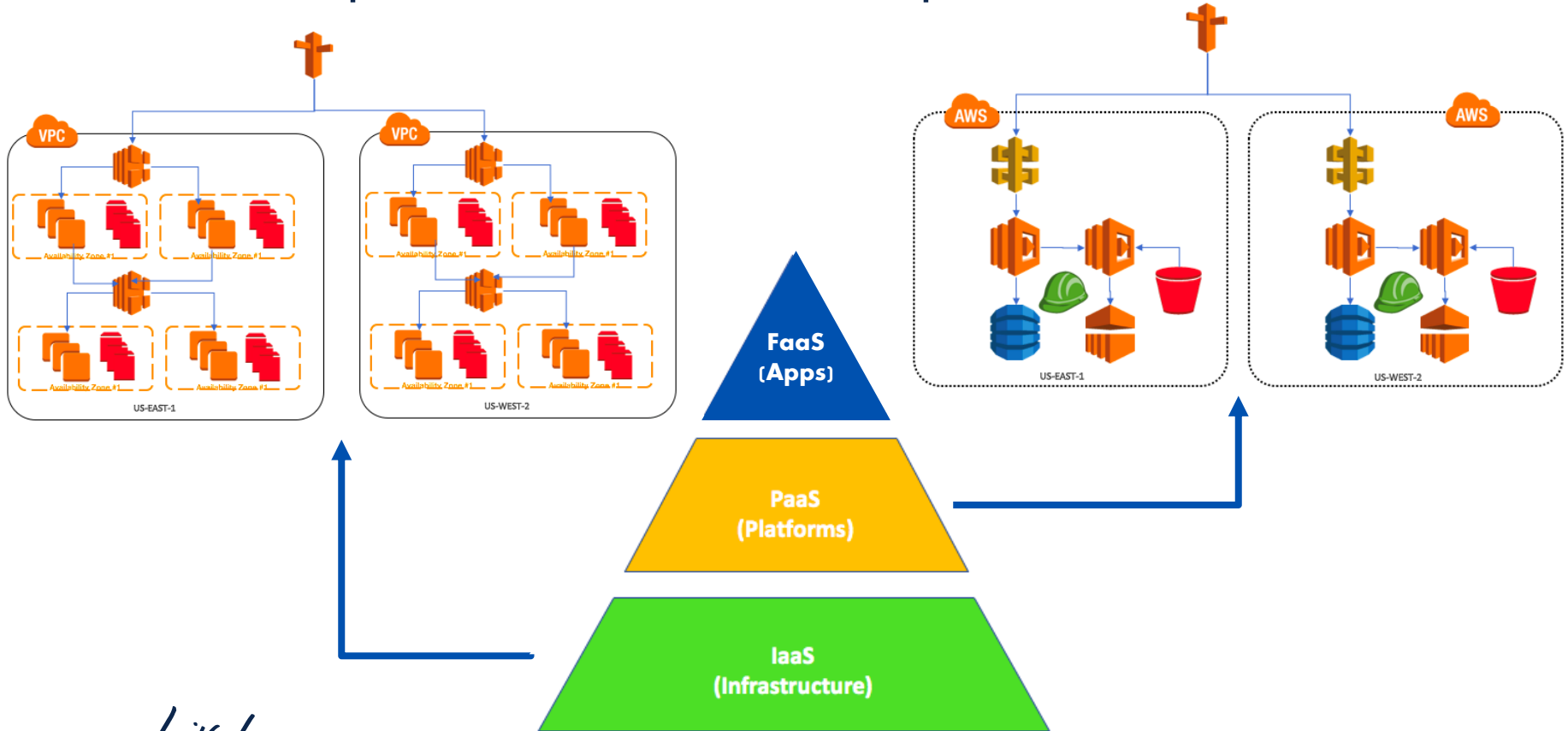


Do you know what's in the
Cloud ?

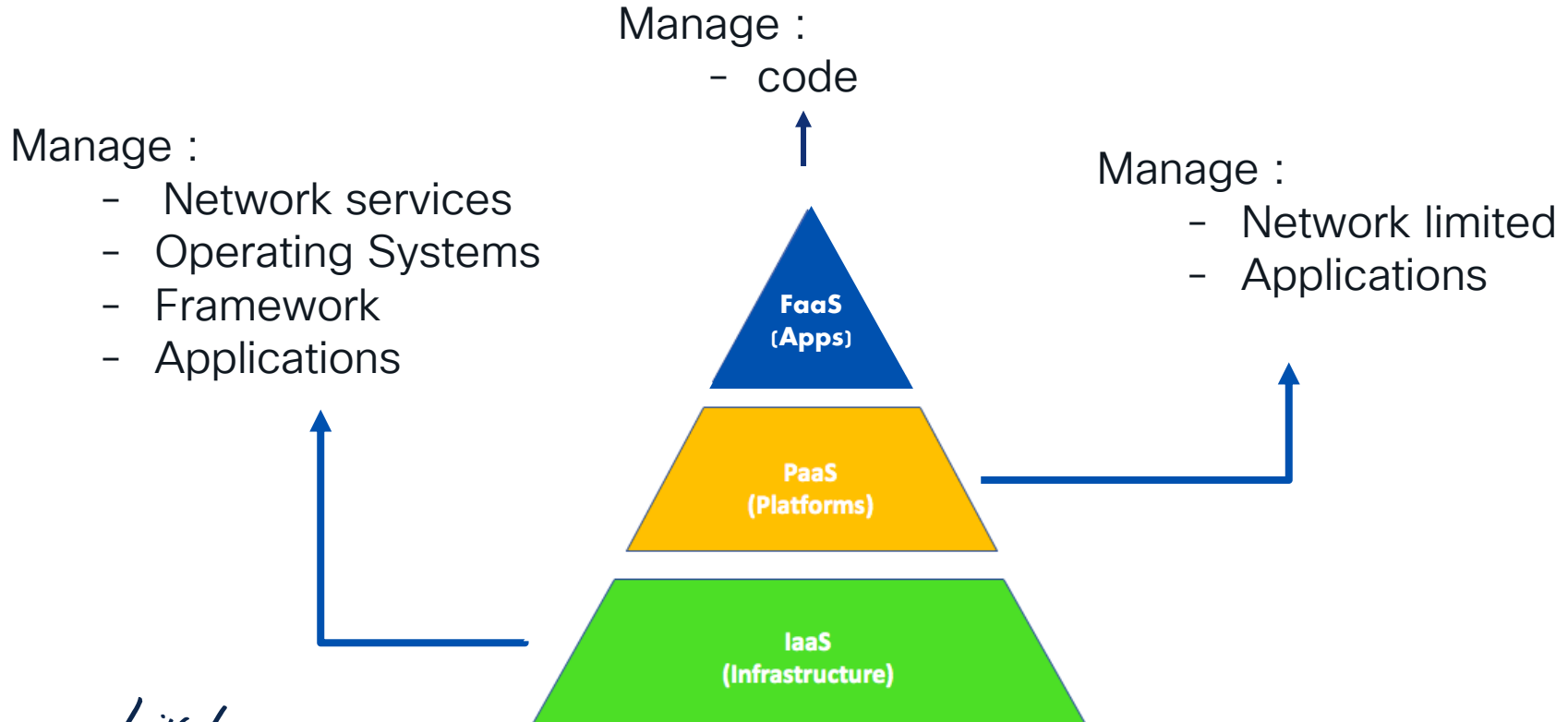


Public Cloud Service
Model

IaaS compared to PaaS Compared to FaaS



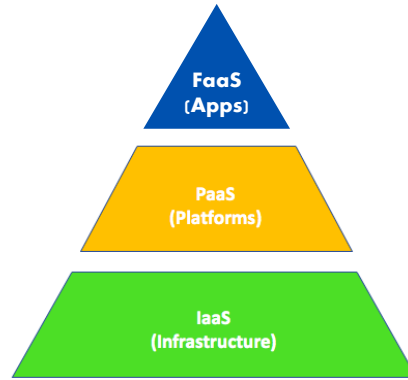
IaaS compared to PaaS Compared to FaaS



Three new parameters to consider in Cloud



Do you know what's in the Cloud ?

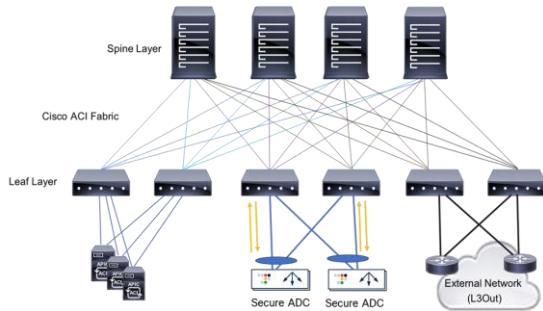


Public Cloud Service Model



New Infrastructure skills for each SCP

The way we are doing it traditionally...



SDN Infrastructure
(ACI, NSX,...)



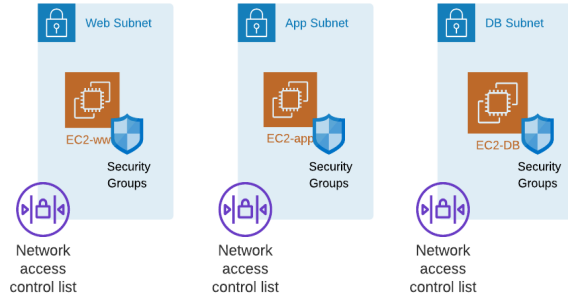
Firewall
(FTD,
ASA)



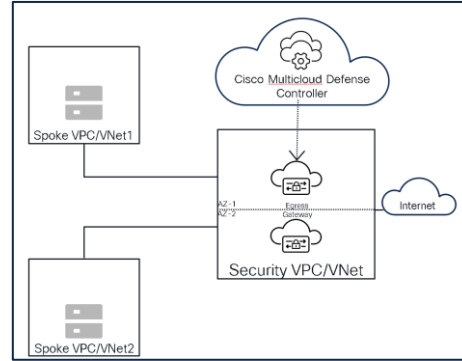
CISCO **SECURE**
Workload

Host based
Firewall

The way we do it in the Cloud...



Public Cloud
Infrastructure



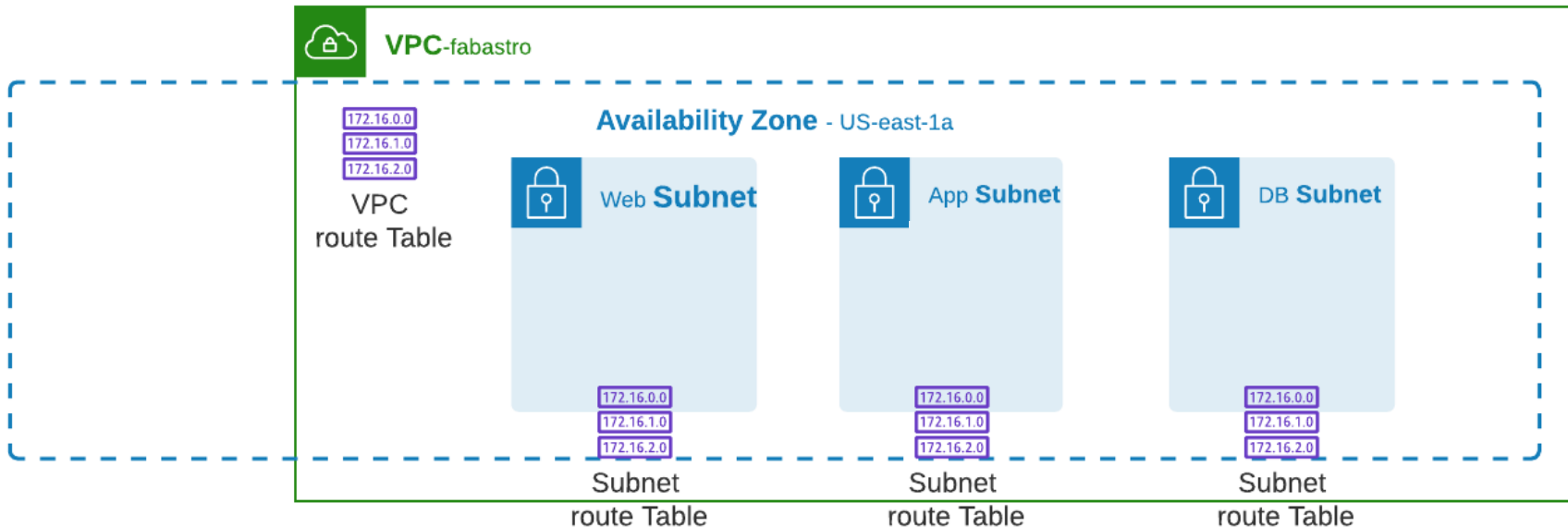
Firewall
(Multicloud Defense, FTDv)



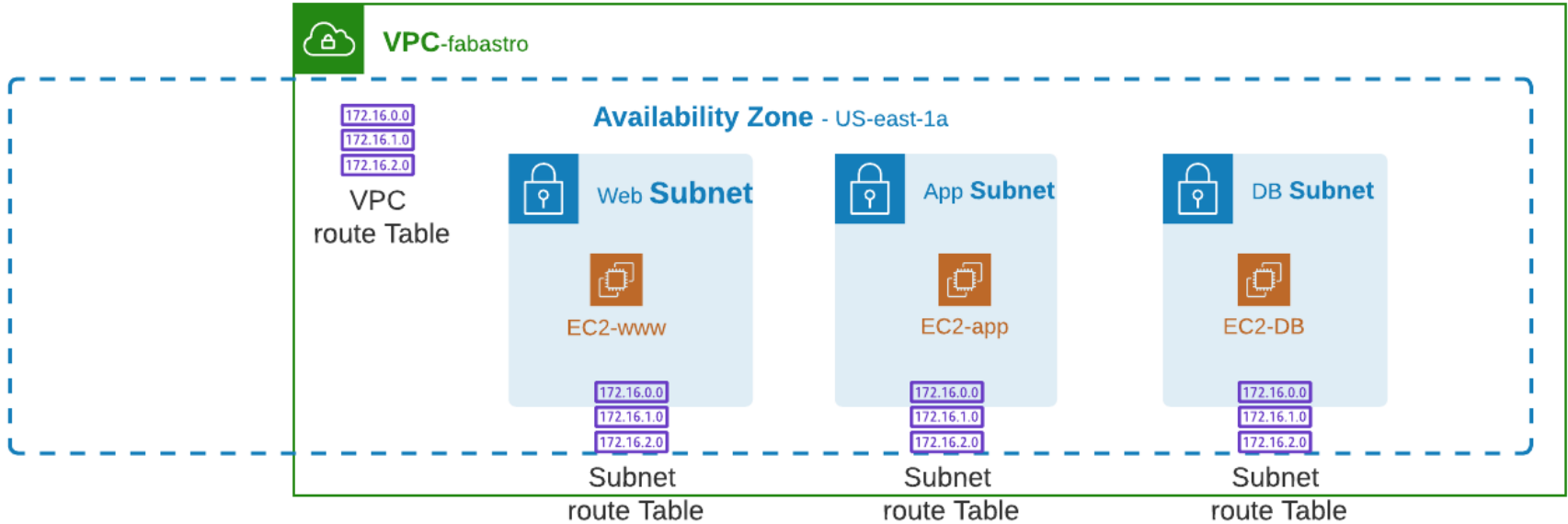
CISCO **SECURE**
Workload

Host based
Firewall

My VRF... VPC sort of (actually Route Tables)

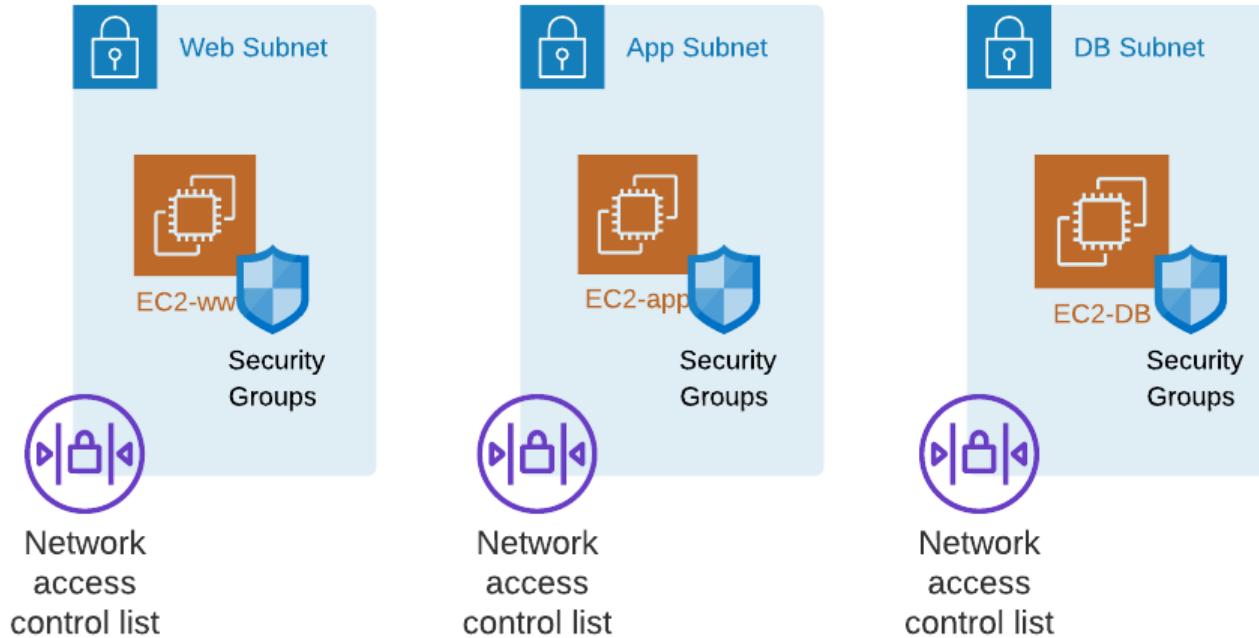


In AWS IaaS... my workloads = Instances



AWS Segmentation solutions

Security Groups and Network Access list

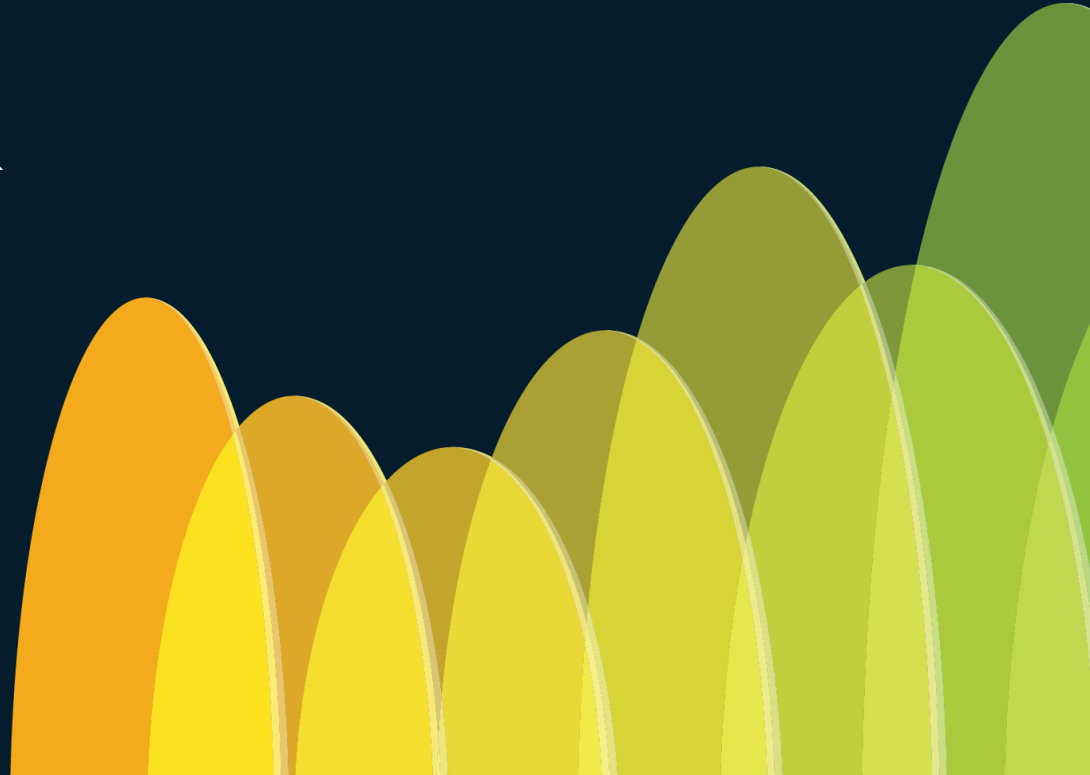


Use security group as Source within VPC

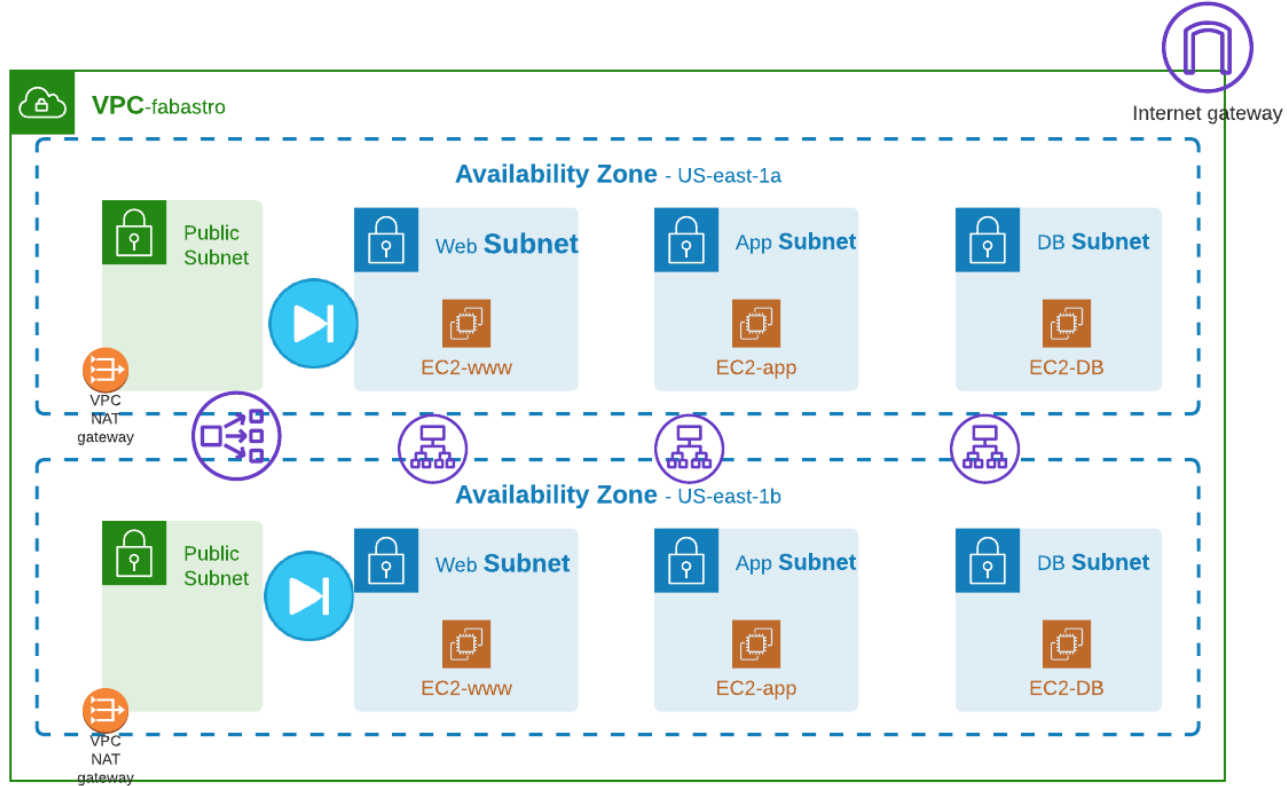
Inbound rules [Info](#)

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

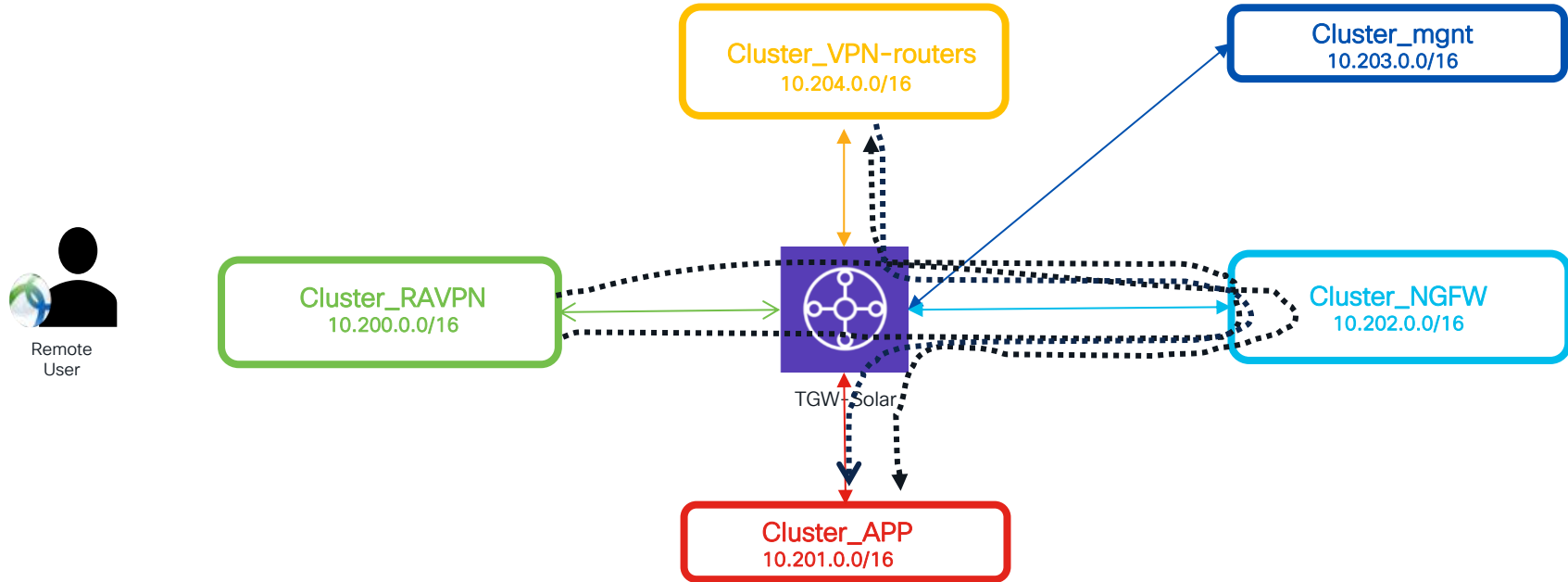
Back to Network security with Firewall



FTDv insertion with HA



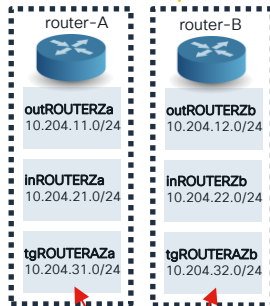
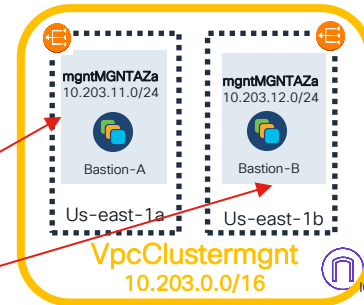
Security Insertion with Service VPC



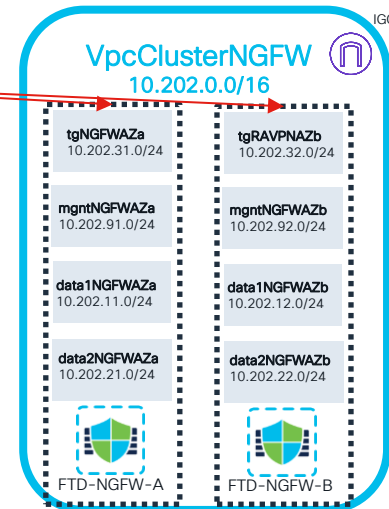


VpcClusterVPNrouters

10.204.0.0/16



IGClusterAPP

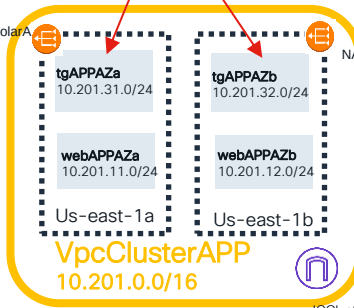


IGClusterNGFW

TransitGatewaySolar

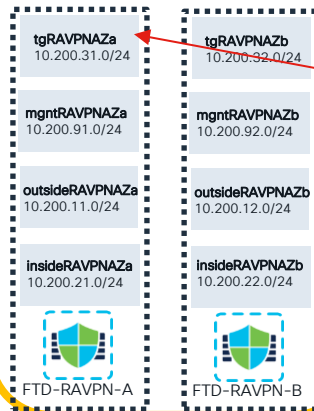
NATgw4websolarA

NATgw4websolarB

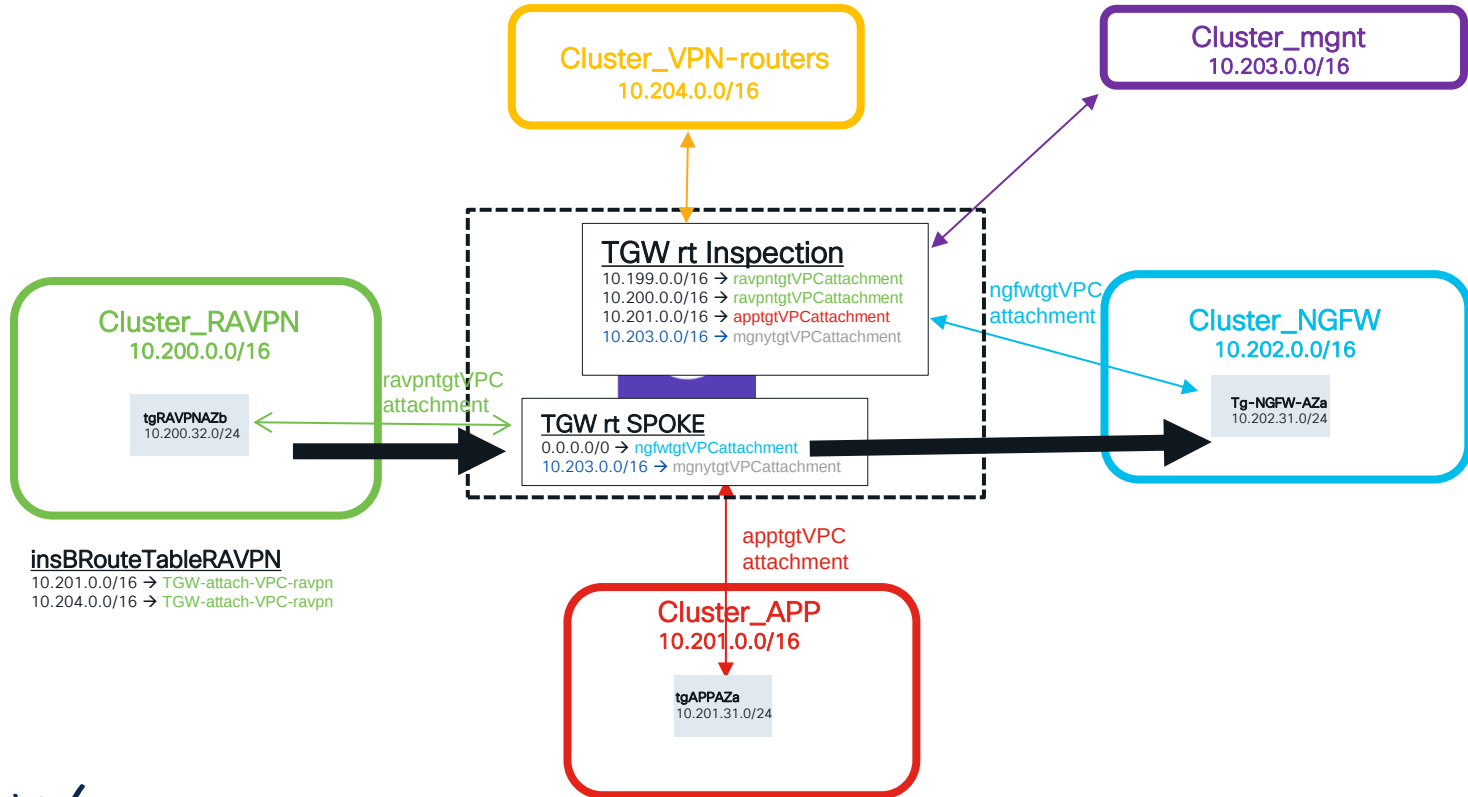


IGClusterAPP

IGClusterRAVPN

VpcClusterRAVPN
10.200.0.0/16Remote
User

Fastest TGW Introduction ever...

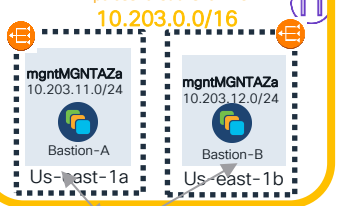


mgntTableMGNT

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

Cluster_mgnt

vpc-0884c73ab1840747e
10.203.0.0/16



IGClusterAPP

tgwrouteRAVPN

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

insARouteTableRAVPN

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

insBRouteTableRAVPN

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

mgntRouteTableRAVPN

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

outsideAZa TableRAVPN

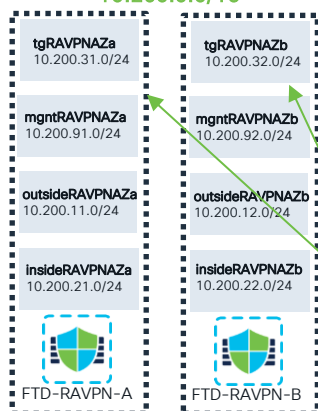
0.0.0.0/0 → IGClusterRAVPN

IGClusterRAVPN

Cluster_RAVPN

vpc-0bb0e7dc4edfa6848

10.200.0.0/16



TGW rt MGNT

10.202.0.0/16 → ngfwtgtVPCAttachment
10.200.0.0/16 → ravpntgtVPCAttachment
10.201.0.0/16 → apptgtVPCAttachment
10.204.0.0/16 → vproutertgtVPCAttachment



TransitGateway
Solar

TGW rt Inspection

10.199.0.0/16 → ravpntgtVPCAttachment
10.200.0.0/16 → ravpntgtVPCAttachment
10.201.0.0/16 → apptgtVPCAttachment
10.203.0.0/16 → mgnytgtVPCAttachment

TGW rt SPOKE

0.0.0.0/0 → ngfwtgtVPCAttachment
10.203.0.0/16 → mgnytgtVPCAttachment

apptgtVPCAttachment

NATgw4websolarA

tgAPPAZaRouteTableAPP

0.0.0.0 → IGClusterAPP

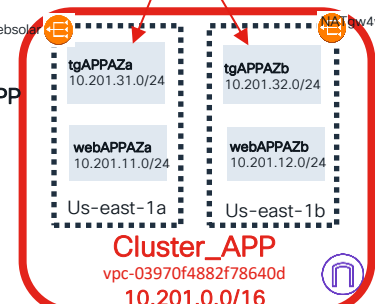
APP rt web Aza

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

Cluster_APP

vpc-03970f4882f78640d

10.201.0.0/16



Cluster_NGFW

vpc-031a746e4abb1b2ed

10.202.0.0/16



IGClusterNGFW

egwlbendpointRouteNGFW

10.202.101.0/24 → LOCAL
0.0.0.0 → ngfwtgtVPCAttachment

tgAZa RouteNGFW

10.202.0.0/16 → LOCAL
0.0.0.0/0 → egwlbNGFWEndpointa
10.203.0.0/16 → ngfwtgtVPCAttachment

tgAZb RouteNGFW

10.202.0.0/16 → LOCAL
0.0.0.0/0 → egwlbNGFWEndpointb
10.203.0.0/16 → ngfwtgtVPCAttachment

mgntTableNGFW

10.203.0.0/16 → mgnytgtVPCAttachment
0.0.0.0/0 → IGClusterAPP

APP rt web Azb

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

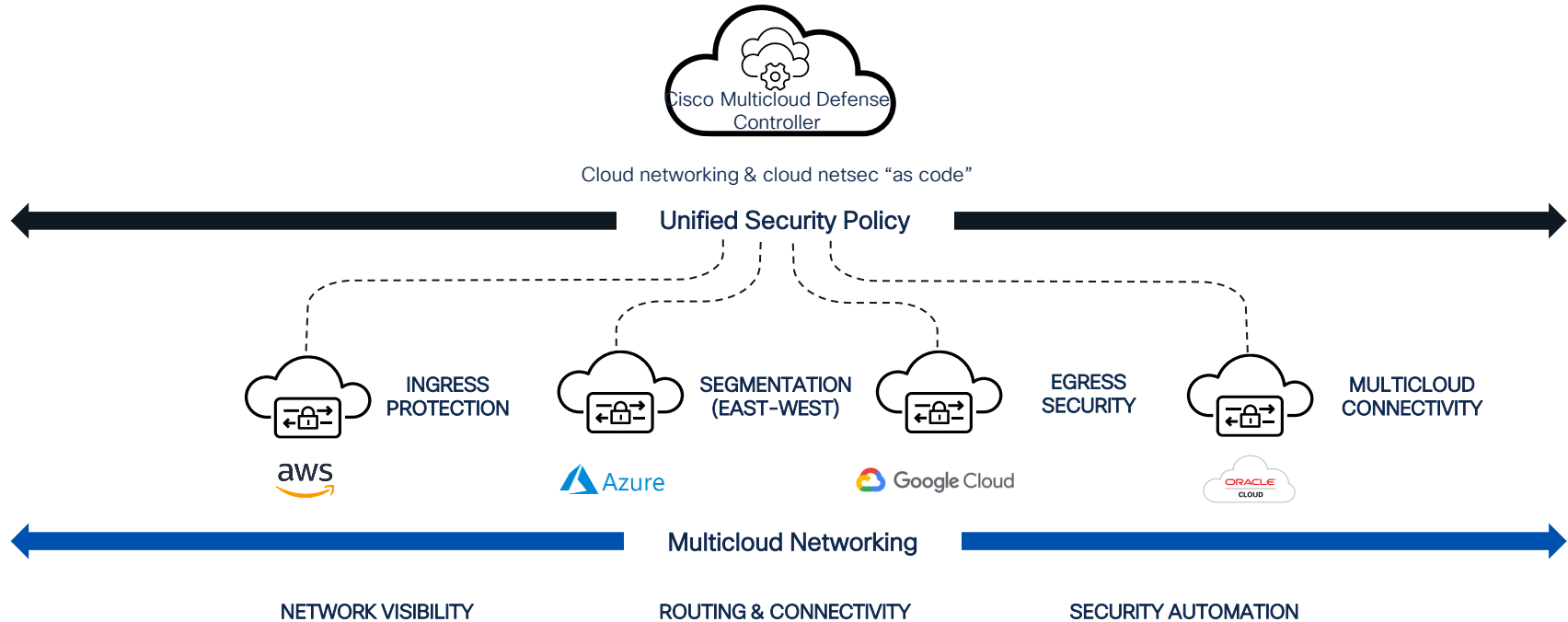
cisco Live!

Simplify operations with Multicloud Defense



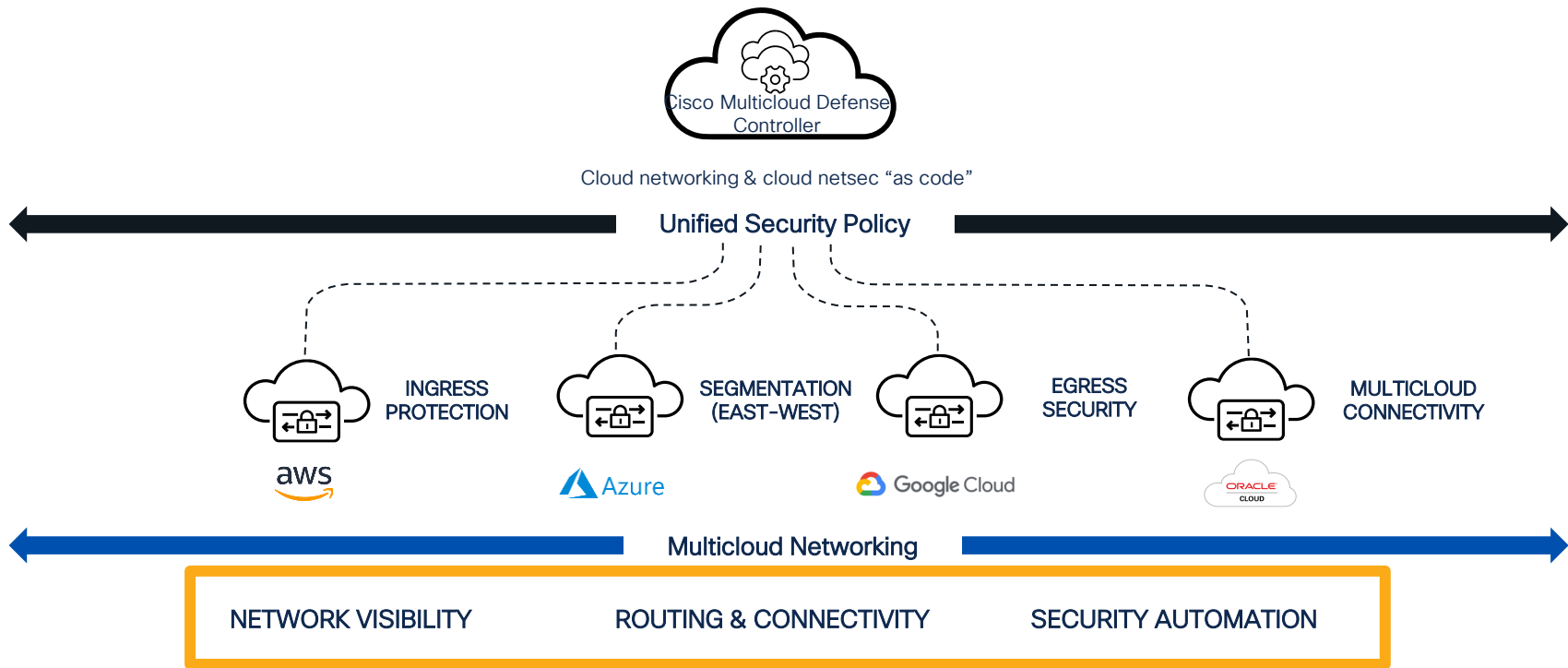
Cisco Multicloud Defense

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



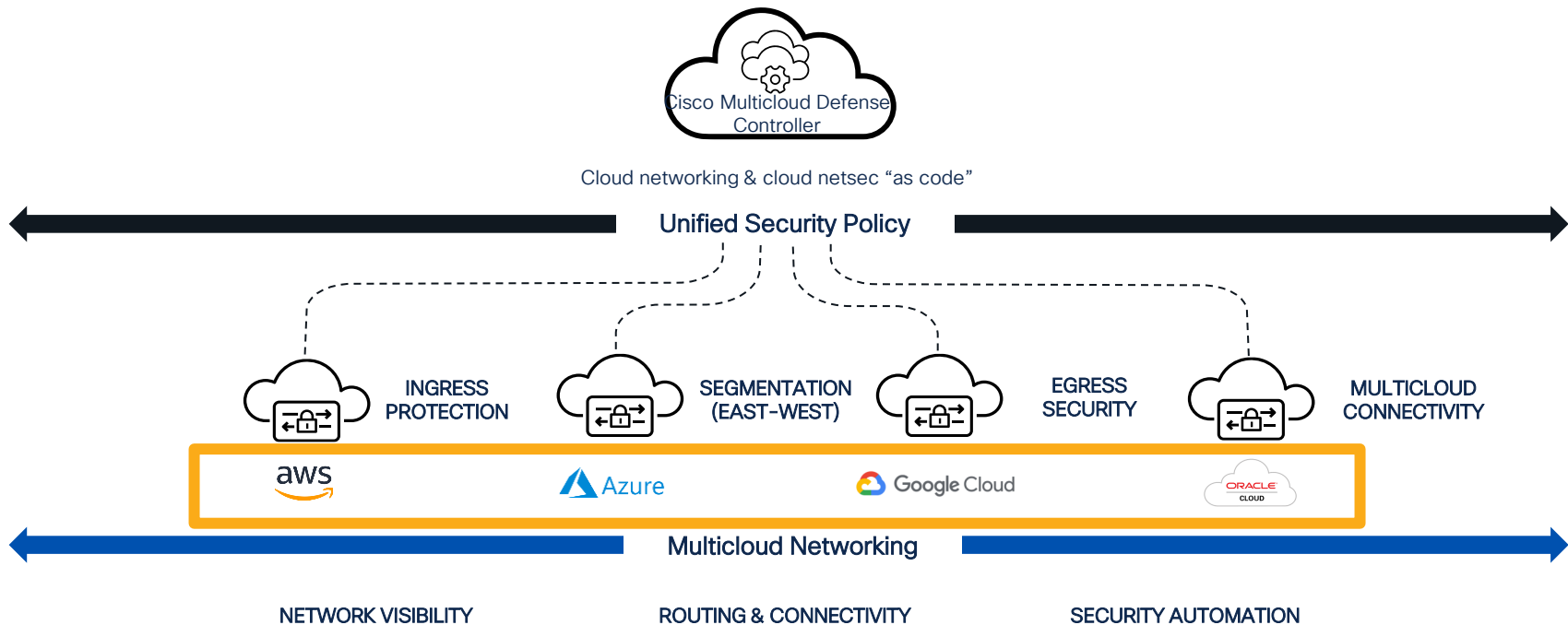
Cisco Multicloud Defense

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



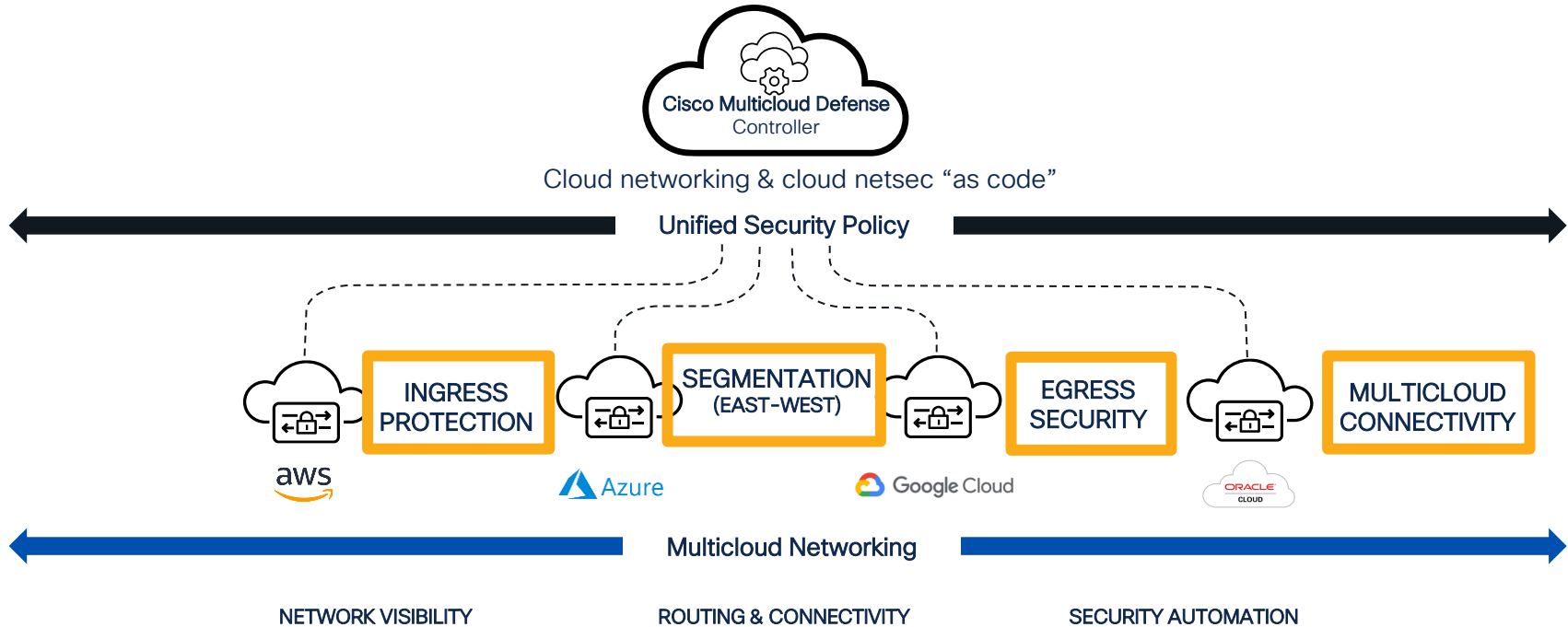
Cisco Multicloud Defense

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



Cisco Multicloud Defense

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



Fully Orchestrated



{ REST:API }

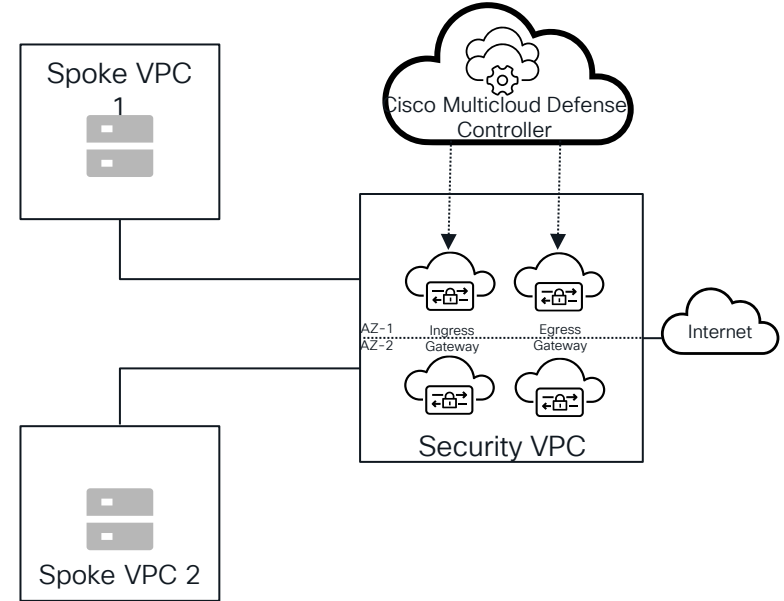
```
1 # Cisco MCD Terraform Documentation
2 # https://registry.terraform.io/providers/cisco/cisco-mcd/latest/docs
3 # AWS Terraform Documentation
4 # https://registry.terraform.io/providers/hashicorp/aws/latest/docs
5
6 # Create a new Cisco MCD Ingress Gateway Stack
7 # If the desire is to destroy the Gateway Stack, comment out the resource block
8 # If the desire is to create the Gateway Stack, uncomment out the resource block
9 resource "cisco_mcd_gateway" "ingress_gateway" {
10   name = var.cisco_mcd_ingress_gateway_name
11   csp_account_name = var.cisco_mcd_aws_account_name
12   gateway_image = var.cisco_mcd_ingress_gateway_version
13   instance_type = var.cisco_mcd_ingress_gateway_instance_type
14   mode = "HUB"
15   security_type = var.cisco_mcd_ingress_gateway_security_type
16   policy_rule_set_id = cisco_mcd_policy_rule_set.ingress_policy_rule_set_id
17   #policy_rule_set_id = data.cisco_mcd_policy_rule_set.ingress_policy_rule_set_id
18   ssh_key_pair = var.cisco_mcd_ingress_gateway_ssh_key_pair
19   aws_iam_role_firewall = var.cisco_mcd_firewall_role_name
20   region = var.aws_account_region
21   vpc_id = cisco_mcd_service_vpc.service_vpc_id
22   min_instances = var.cisco_mcd_ingress_gateway_autoscale_min
23   max_instances = var.cisco_mcd_ingress_gateway_autoscale_max
24   gateway_state = var.cisco_mcd_ingress_gateway_status
25   settings {
26     # name = "controller.use_internal_lb"
27     # value = var.cisco_mcd_ingress_gateway_internal_lb
28   }
29 }
30
```

```
POST /api/v1/gateway/run...

{
  "common": {
    "acctName": "{{acctName}}",
    "source": "RESTAPI",
    "clientVersion": "CiscoMCD-2022"
  },
  "gateway": {
    "cspAccountName": "AWS+Account3",
    "name": "aws-egress-gw",
    "description": "AWS EDGE Gateway",
    "mode": "EDGE",
    "type": "CLUSTER",
    "minInstances": 1,
    "maxInstances": 1,
    "healthCheckPort": 65534,
    "policyRuleSetId": 20,
    "flags": {
      "GATEWAY_FLAGS_EGRESS_FIREWALL",
      "GATEWAY_FLAGS_AWS_GATEWAY_LB"
    }
  },
  "settings": [
    {
      "name": "gateway.aws.egress.key.default"
    },
    {
      "name": "controller.gateway.assign_public_ip",
      "value": "true"
    },
    {
      "name": "gateway.fqdn_ip_cache.entry_ttl"
    }
  ]
}
```

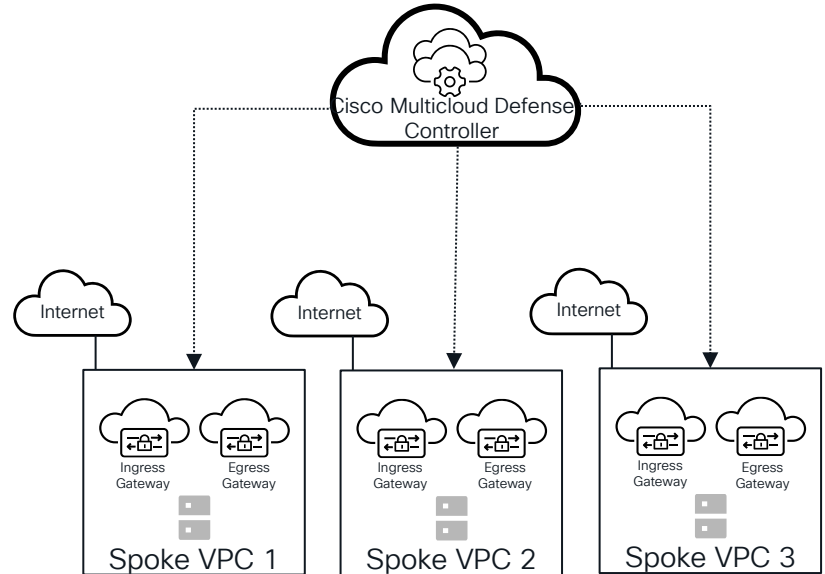
Centralized Security Model

- Gateways are deployed in the security VPC/VCN
 - Autoscale aware
 - Multi-AZ aware
- Type of Multicloud Defense Gateways
 - Ingress (Inbound traffic)
 - Egress (Egress & E/W traffic)
- The controller handles the lifecycle management of gateways for a true cloud-native aaS experience
 - Instantiation
 - Scalability
 - Reliability
 - Upgrade



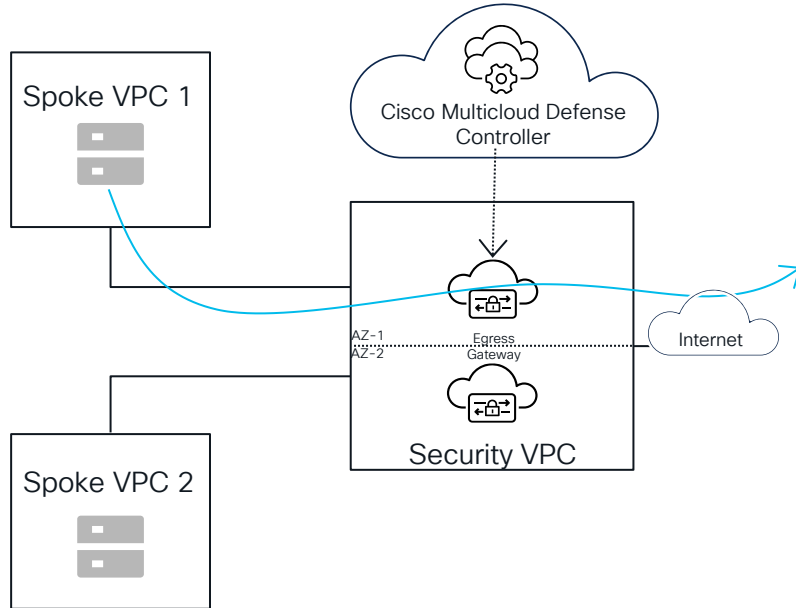
Distributed Security Model

- Gateways are deployed in the security VPC/VCN
 - Autoscale aware
 - Multi-AZ aware
- Type of Multicloud Defense Gateways
 - Ingress (Inbound traffic)
 - Egress (Egress & E/W traffic)
- The controller handles the lifecycle management of gateways for a true cloud-native aaS experience
 - Instantiation
 - Scalability
 - Reliability
 - Upgrade

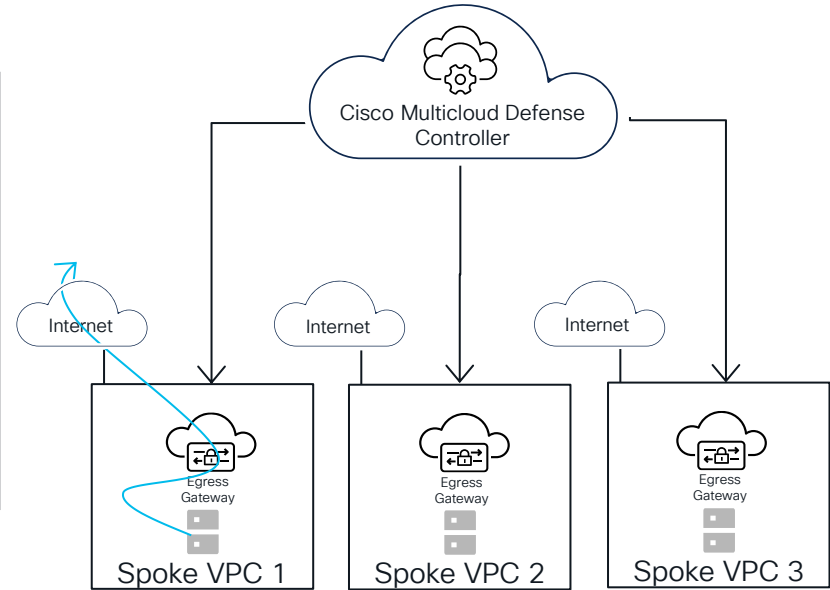


Egress

Centralized Security Model

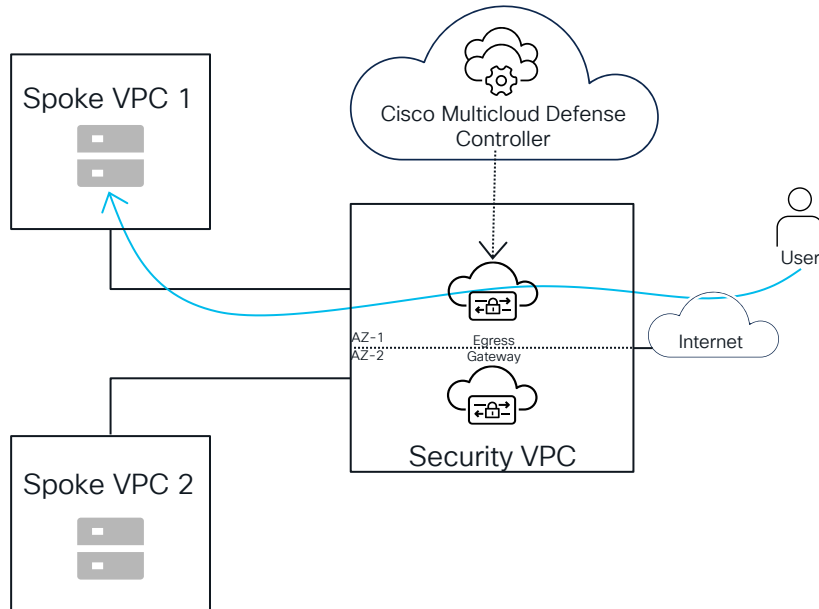


Distributed Security Model

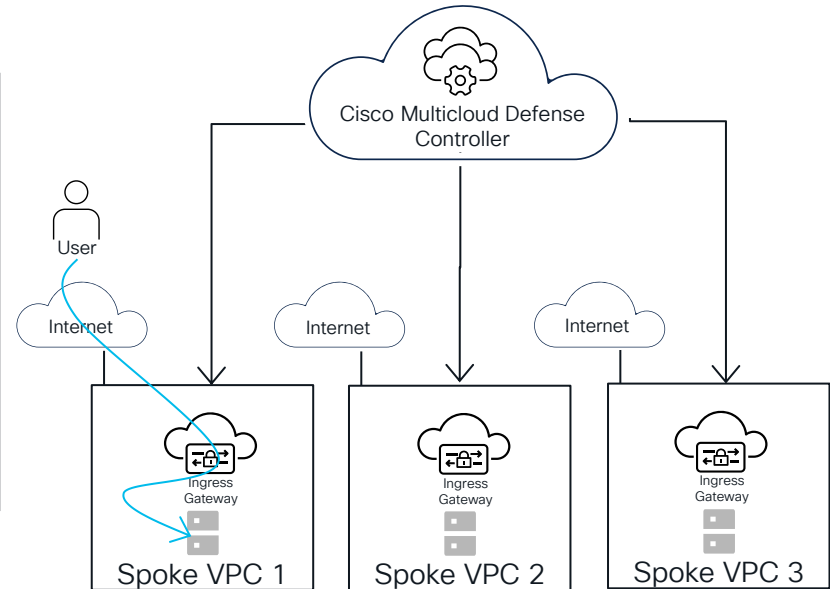


Ingress

Centralized Security Model



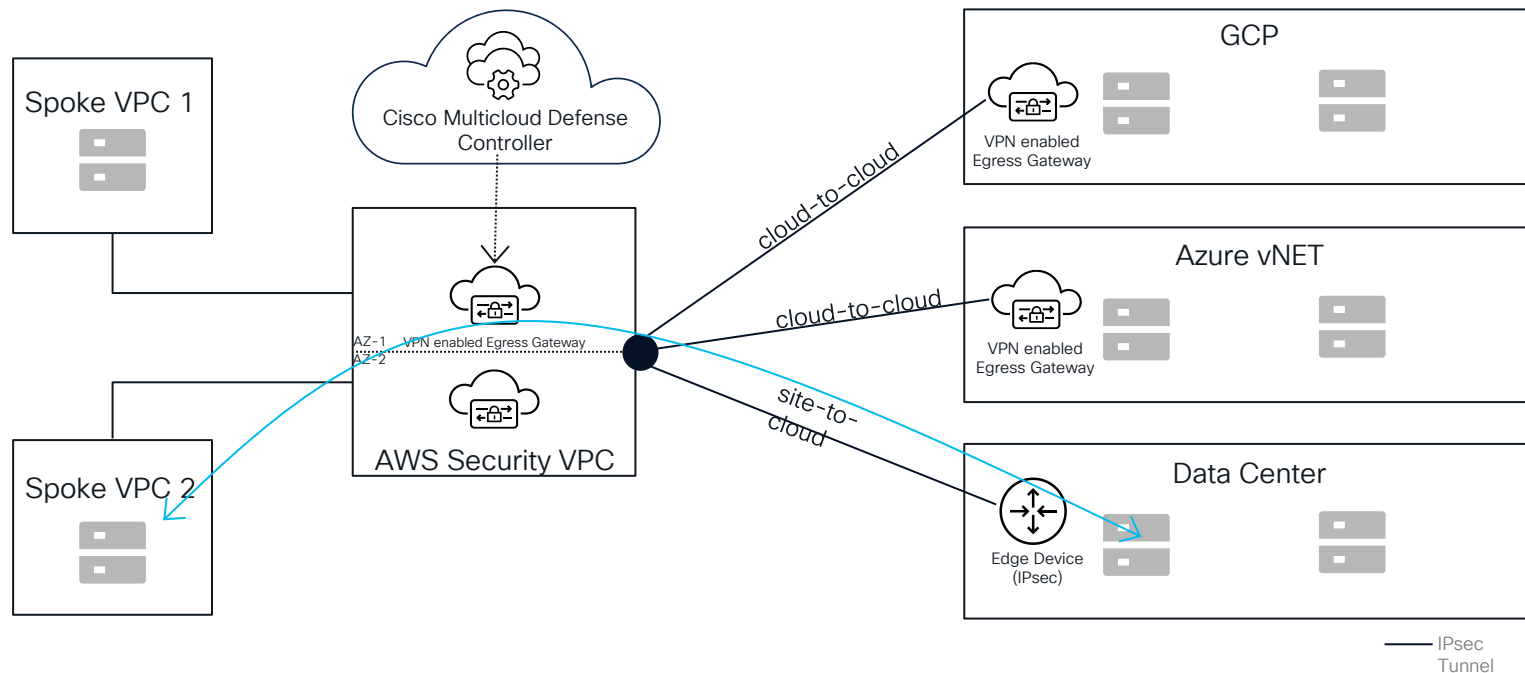
Distributed Security Model



Multicloud Connectivity

site-to-cloud

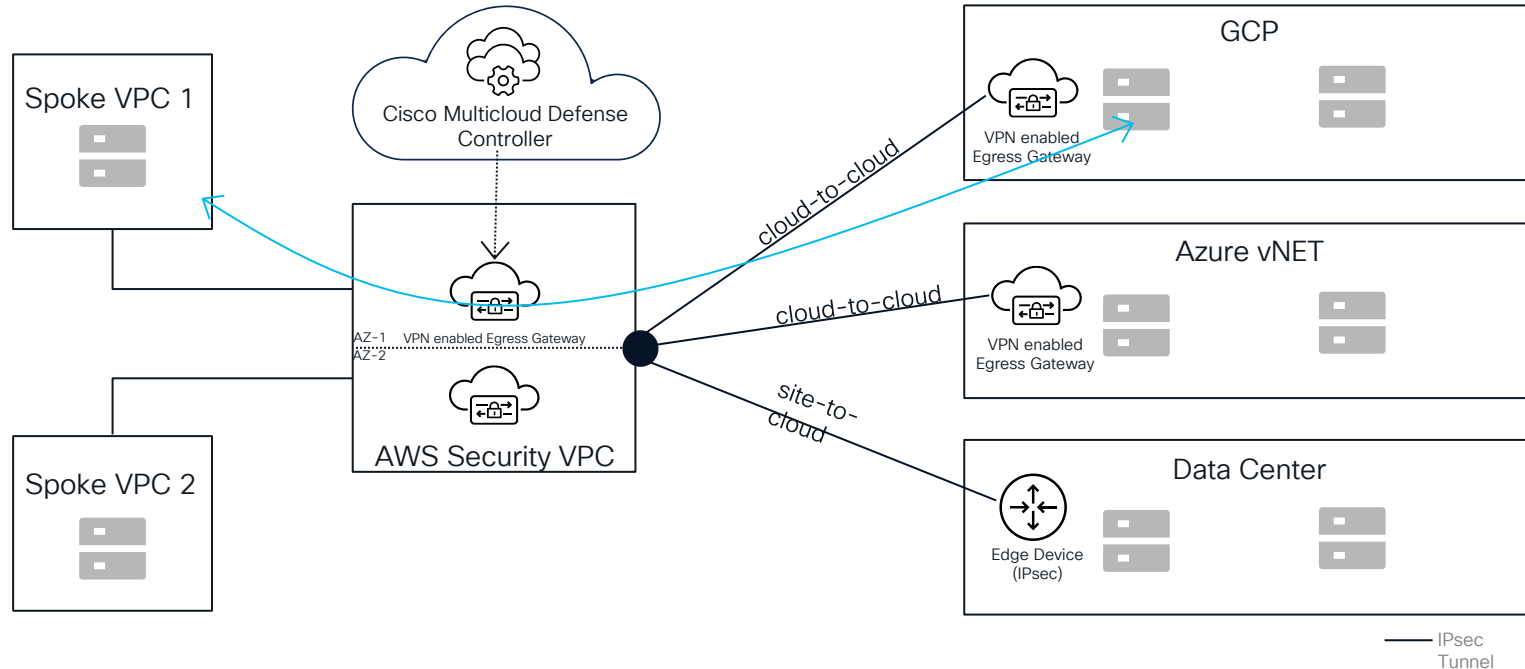
Centralized Security Model



Multicloud Connectivity

cloud-to-cloud

Centralized Security Model



Very Complex Setup Process

The screenshot displays the Cisco Multicloud Defense web interface. The browser address bar shows the URL `prod1.mcd.eu.cdo.cisco.com/easysetup`. The page header includes the Cisco logo and the title "Multicloud Defense". A navigation bar contains links for Dashboard, Discover, Investigate, Manage, Report, and Administration. The user is logged in as "Admin: dstoeckm@cis..." with the email "CDO_cisco-dstoeckm".

The main content area is titled "Setup" and includes a sub-header: "Multicloud Defence secures your applications in minutes by orchestrating the deployment of all security components. Let's begin securing your application by following 3 simple steps." The setup process is divided into three steps, each with a title, an icon, a description, and a button:

- Step 1: Connect Account**
Icon: Cloud with a checkmark.
Description: Connect a cloud account with the Multicloud Defense Controller.
Button: [Connect Account](#)
- Step 2: Enable Traffic Visibility**
Icon: Globe with a magnifying glass.
Description: Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account.
Button: [Enable Visibility](#)
- Step 3: Secure Your Account**
Icon: Padlock.
Description: Setup a Service VPC and Multicloud Defense Gateway to secure your Account.
Button: [Secure Account](#)

The left sidebar contains a "Favorites" section with a note "Pinned navigation items will go here". Below this are two main sections: "Security Policies" and "Profiles".

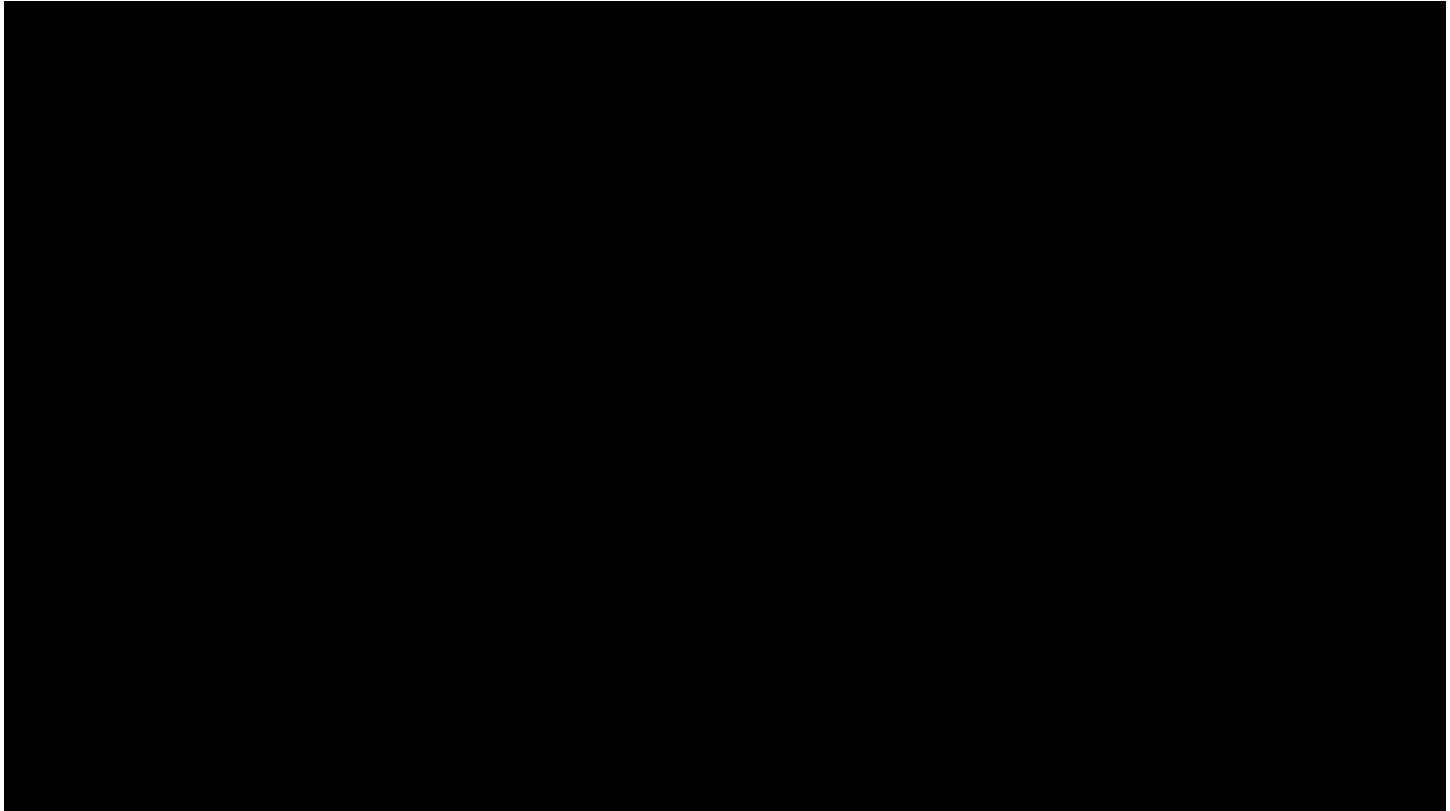
Security Policies

- Rule Sets
- Addresses
- Services
- Certificates
- FQDNs

Profiles

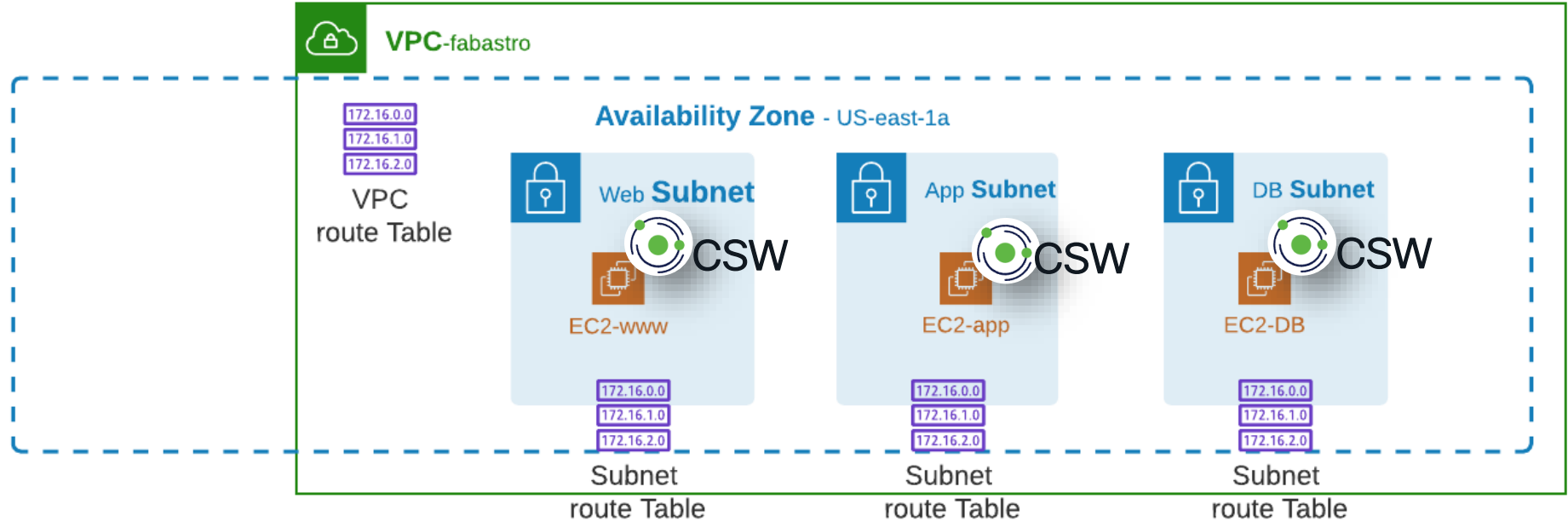
- Decryption
- IPS/IDS
- Data Loss Prevention
- Anti Malware
- WAF
- Layer 7 DOS
- URL Filtering
- FQDN Filtering
- Malicious IPs
- Packet Capture
- Log Forwarding

Multicloud Defense Demo

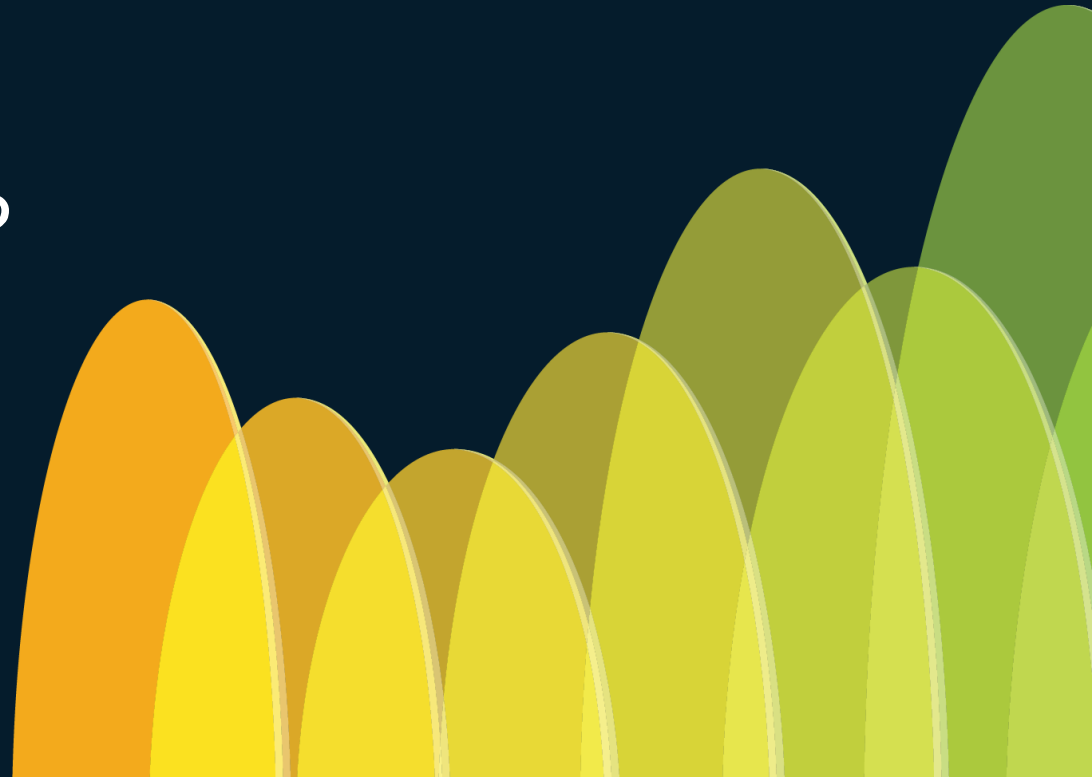


What about MicroSegmentation ?

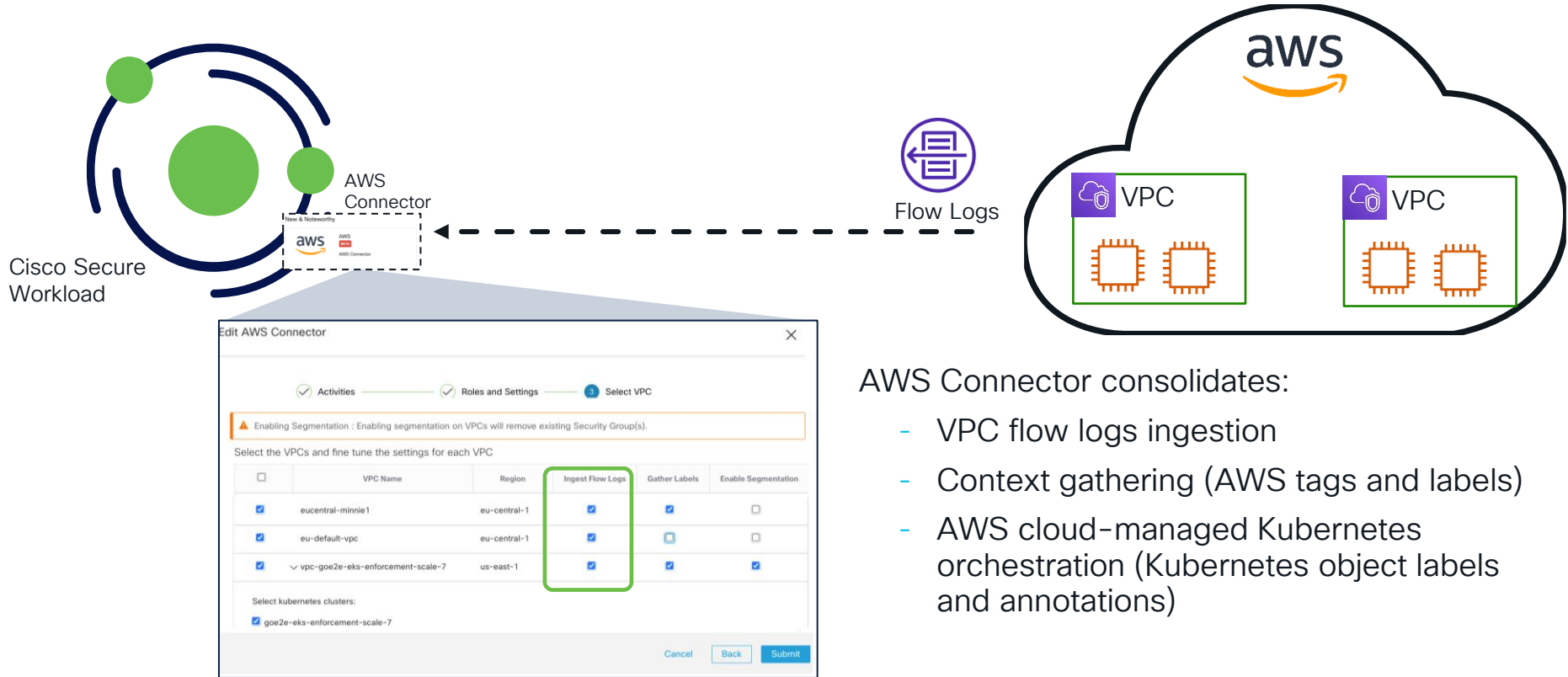
Leveraging Cisco Secure Workload to segment within a VPC or a subnet



You said agent ?



Cisco Secure Workload Cloud-Based Sources

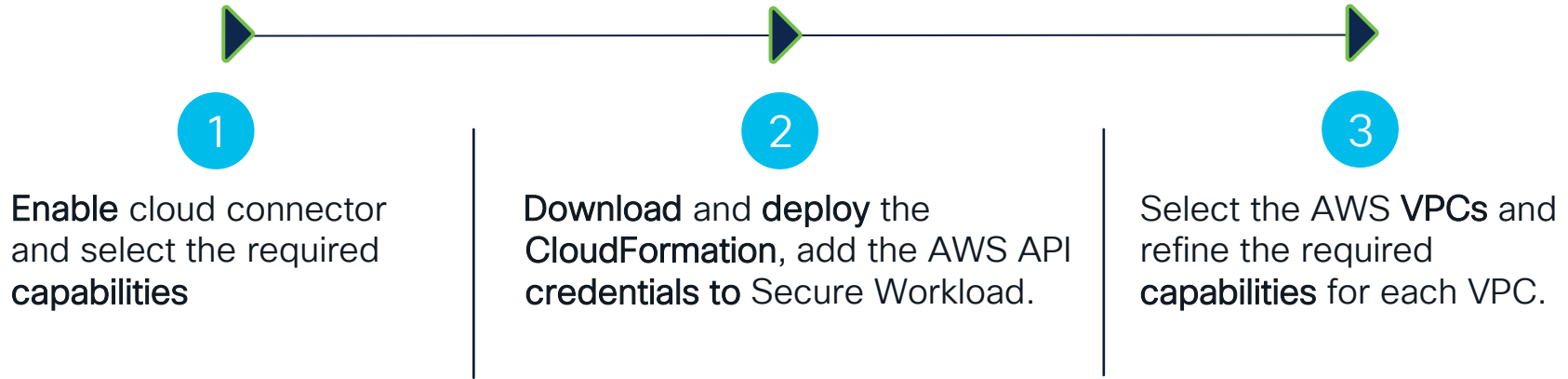


AWS Connector consolidates:

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

AWS Connector

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



AWS Connector – Select Capabilities

1 Enable and configure the connector capabilities



The 'Edit AWS Connector' dialog shows a progress bar with four steps: 1 Activities, 2 Roles and Settings, 3 Select VPC, and 4 View Groups. The 'Name of the connector' field is set to 'AWS'. Under 'Select Activities to be performed with Cisco Secure Workload on your AWS Resources', the following are selected: ☒ Gather Labels, ☒ Ingest Flow Logs, and ☒ Segmentation. The 'Managed kubernetes services' checkbox is unchecked. A note states: 'The recommended AWS (IAM) roles and permissions depend on the selections you make above.' At the bottom right are 'Cancel', 'Back', and 'Next' buttons.

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

Activities Roles and Settings Select VPC

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

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

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

Additional Help

- > Create a Cloud Formation Stack
- > Create a New User
- > Example Commands

Access Key

Secret Key

Does your network require HTTP Proxy to reach AWS?

Please provide your proxy URL:

Full Scan Interval seconds

Delta Scan Interval seconds

AWS Limits

Security Groups Per Region

Security Groups Per Network Interface

Rules per Security Group



AWS Connector – Select VPCs

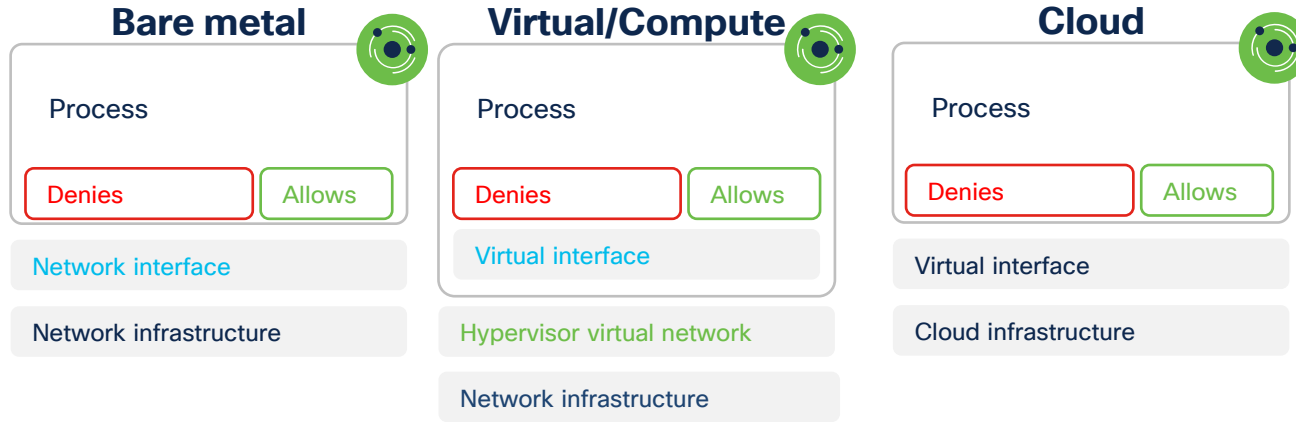
3

- 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	☒	☒	☒

How does CSW enforce the Policy ?



Intent is rendered as security rules in native environment

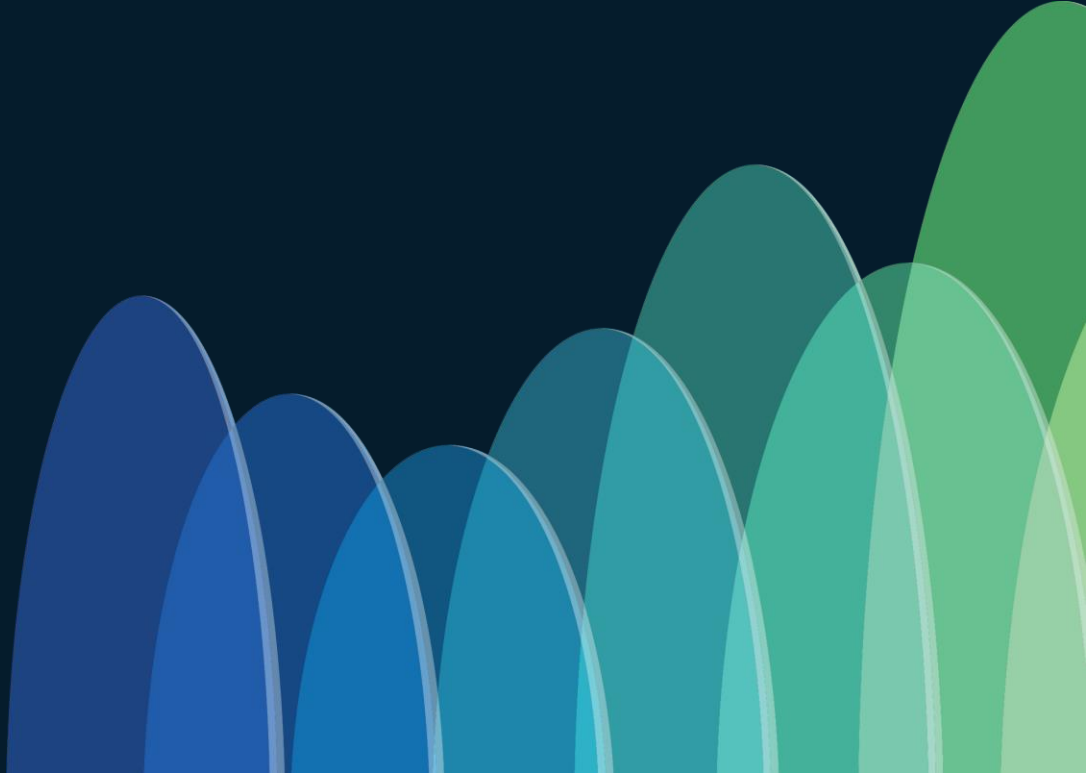
- IP sets on Linux servers
- Windows Advanced Firewall or Windows Filtering Platform on Windows servers
- Public cloud: AWS with Security Group and Azure with Network Security Group

Zoning & (Micro)Segmentation Demo

The screenshot displays the AWS Management Console interface for the us-west-2 region. The left sidebar shows the navigation menu with categories like EC2 Dashboard, Tags, Limits, Instances, Images, Elastic Block Store, and Network & Security. The main content area is titled 'Instances (9) Info' and shows a table of running EC2 instances. The table columns include Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 D. The instances listed are dev-storage-1, dev-sql-1, dev-web-1, dev-storage-2, dev-sql-2, dev-web-2, aws-sapphire-prod-sql, aws-sapphire-prod-web, and aws-sapphire-prod-nfs. All instances are in a 'Running' state and have '2/2 checks passed' for status checks. The availability zones are us-west-2c, us-west-2b, and us-west-2a.

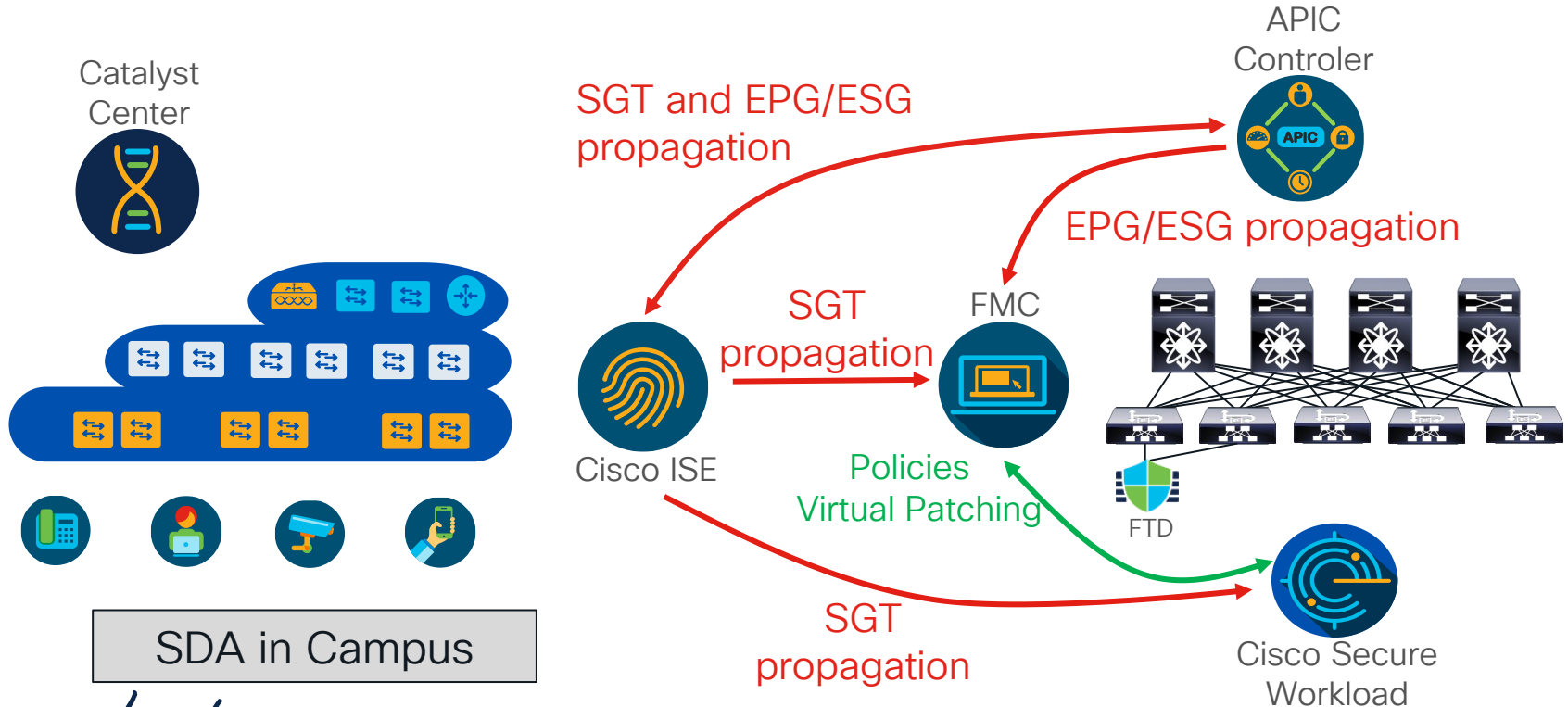
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
dev-storage-1	i-0fc7b1de63344f911	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	-
dev-sql-1	i-0b063fd1cbeb0914d	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	-
dev-web-1	i-0aa5be3edb1ef3226	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	-
dev-storage-2	i-050e049948215bdd5	Running	t2.micro	2/2 checks passed	No alarms	us-west-2b	ec2-34-213-2
dev-sql-2	i-04201f6c2fcef88c	Running	t2.micro	2/2 checks passed	No alarms	us-west-2b	ec2-35-163-1
dev-web-2	i-0fd95bc88828304f1	Running	t2.micro	2/2 checks passed	No alarms	us-west-2b	ec2-34-209-1
aws-sapphire-prod-sql	i-0ee56c4a4238156f	Running	t2.micro	2/2 checks passed	No alarms	us-west-2a	-
aws-sapphire-prod-web	i-07cf51cb82e99cf9b	Running	t2.micro	2/2 checks passed	No alarms	us-west-2a	-
aws-sapphire-prod-nfs	i-05f7cda90d27d276f	Running	t2.micro	2/2 checks passed	No alarms	us-west-2a	-

Summary of the solutions



End to end Segmentation

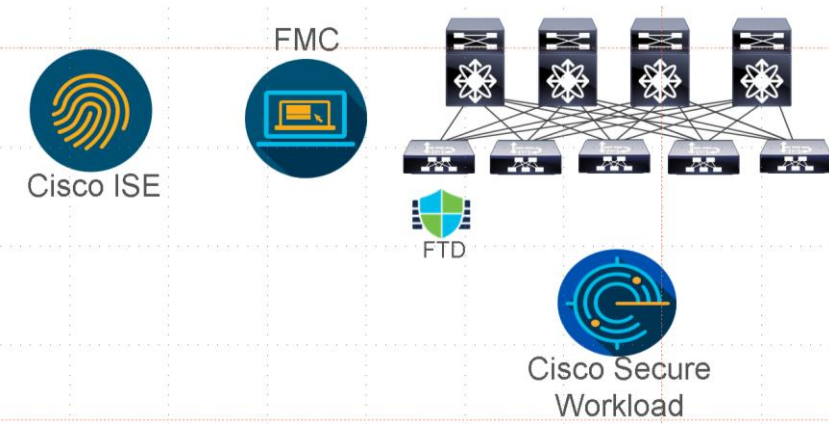
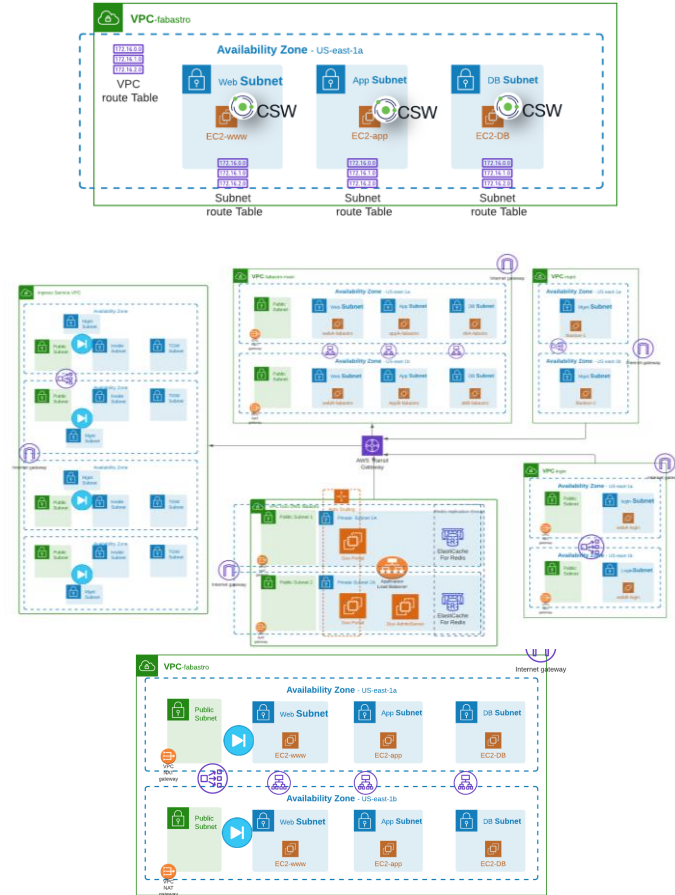
On prem



cisco *Live!*

Moving to Hybrid

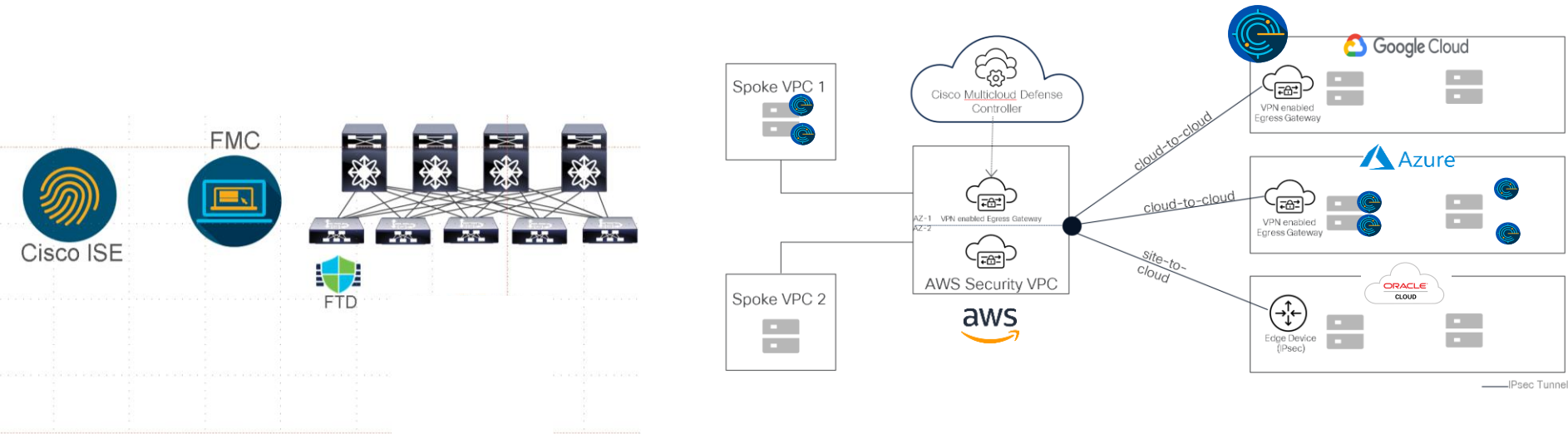
FTD on prem and Single Cloud provider



cisco Live!

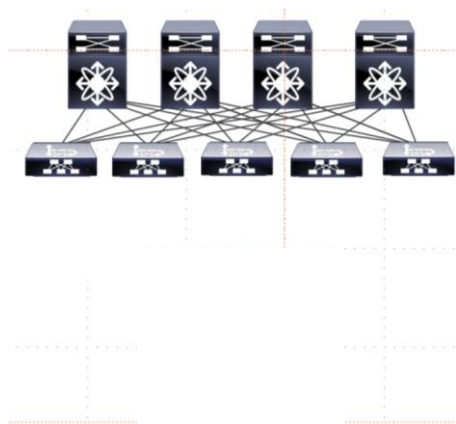
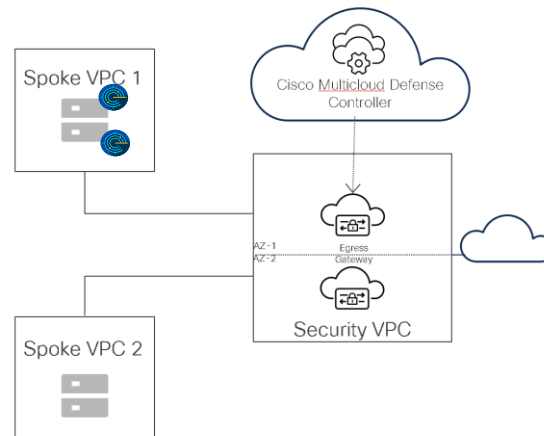
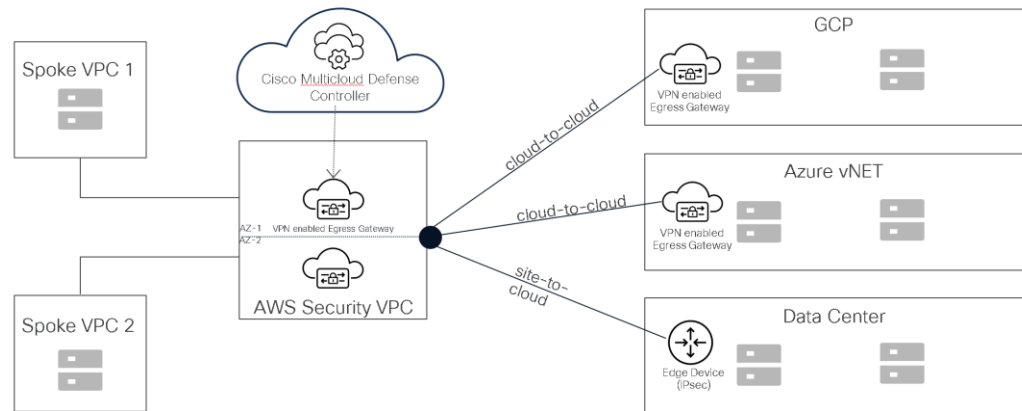
Moving to Hybrid – Multi Cloud

FTDF on Prem and Multi cloud



Moving to Hybrid

No FTD on Prem



—IPsec Tunnel

Objectives



No perfect
Solution... Yet



Need for a platform



Multiple paths to
securing Cloud &
Apps



Cisco can help with
this Journey

Complete Your Session Evaluations



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



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC