The bridge to possible

Resilience and Scaling for Security Solutions in the Public Cloud

Eric Kostlan, Technical Marketing Engineer

BRKSEC-3457

"Reconciliation"- Dustin Koa Art

```
ubuntu@Azure200 :~ $ ping -c 1 10.200.101.6 > /dev/null
ubuntu@Azure200 :~ $ ping -c 1 10.200.101.8 > /dev/null
ubuntu@Azure200 :~ $ arp -an
? (10.200.101.1) at 12:34:56:78:9a:bc [ether] on eth0
? (10.200.101.6) at 12:34:56:78:9a:bc [ether] on eth0
? (10.200.101.8) at 12:34:56:78:9a:bc [ether] on eth0
ubuntu@Azure200 :~ $
```

"The public cloud is easy to learn. Step 1. Forget everything you know about networking."

Ancient Technical Marketing Maxim

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Webex App

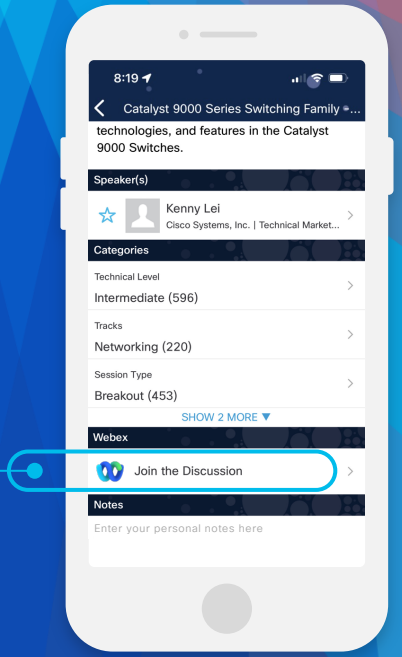
Questions?

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 December 22, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-3457

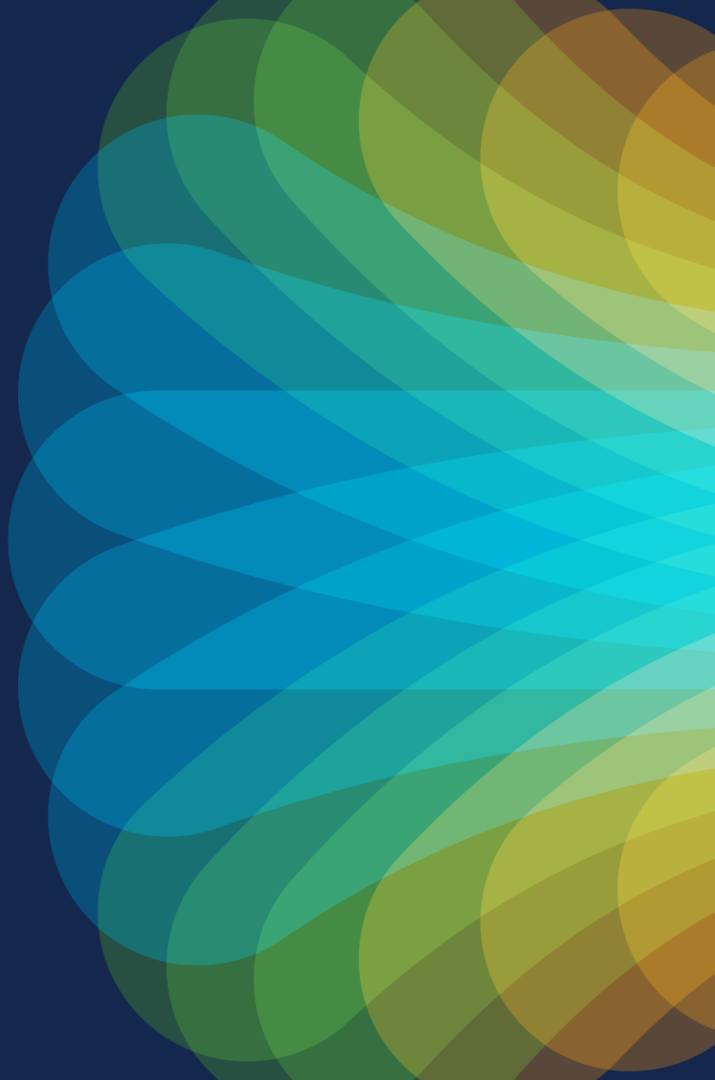
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction
- Load Balancers
- High Availability and Resilience
- Cisco Secure Firewall
- Cisco Multicloud Defense
- Cisco Secure Workload
- Conclusion

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Introduction



“When the Internet was first introduced to the public in the 1990s, many people were skeptical about conducting financial transactions online due to security risks. The lack of established security measures and the fear of online fraud made it difficult for people to trust the Internet for commercial purposes.”

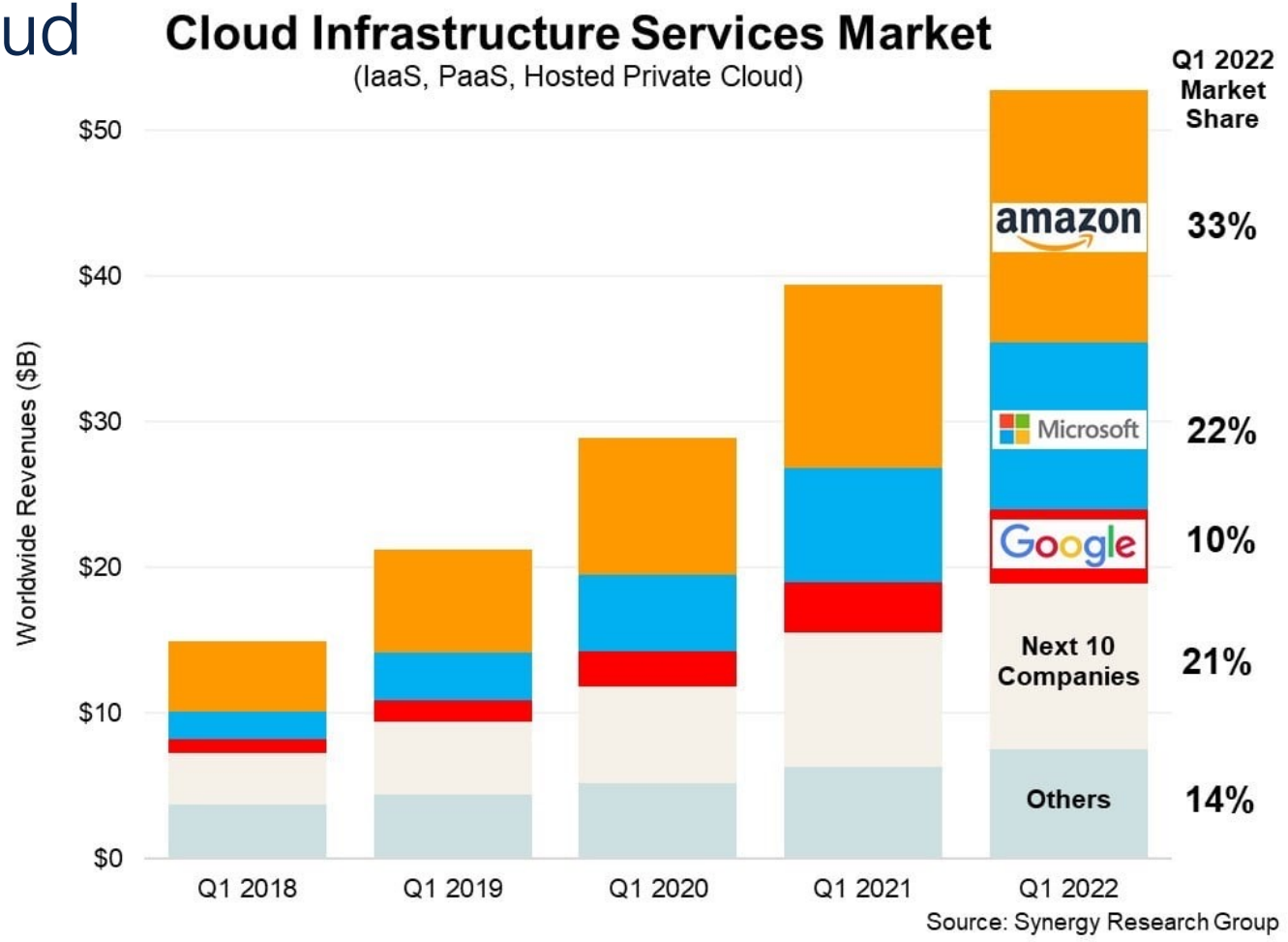
ChatGPT

“But the value proposition was too great to wait for security. History repeats itself with the rush to the public cloud. Security can only attempt to keep up.”

Human

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Public Cloud Market

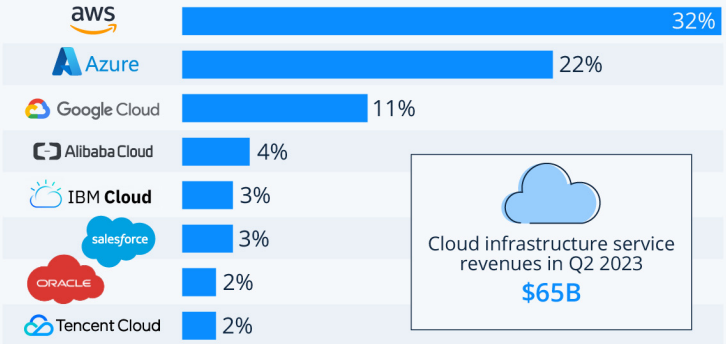


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Public Cloud Market Share

Amazon Maintains Lead in the Cloud Market

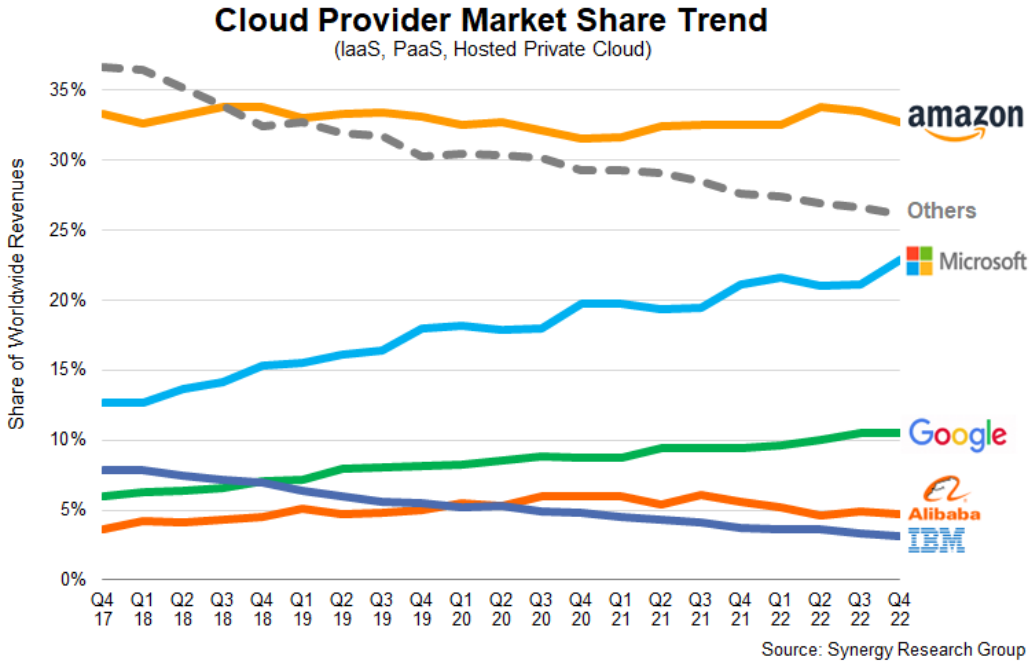
Worldwide market share of leading cloud infrastructure service providers in Q2 2023*



* Includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services

Source: Synergy Research Group

statista



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

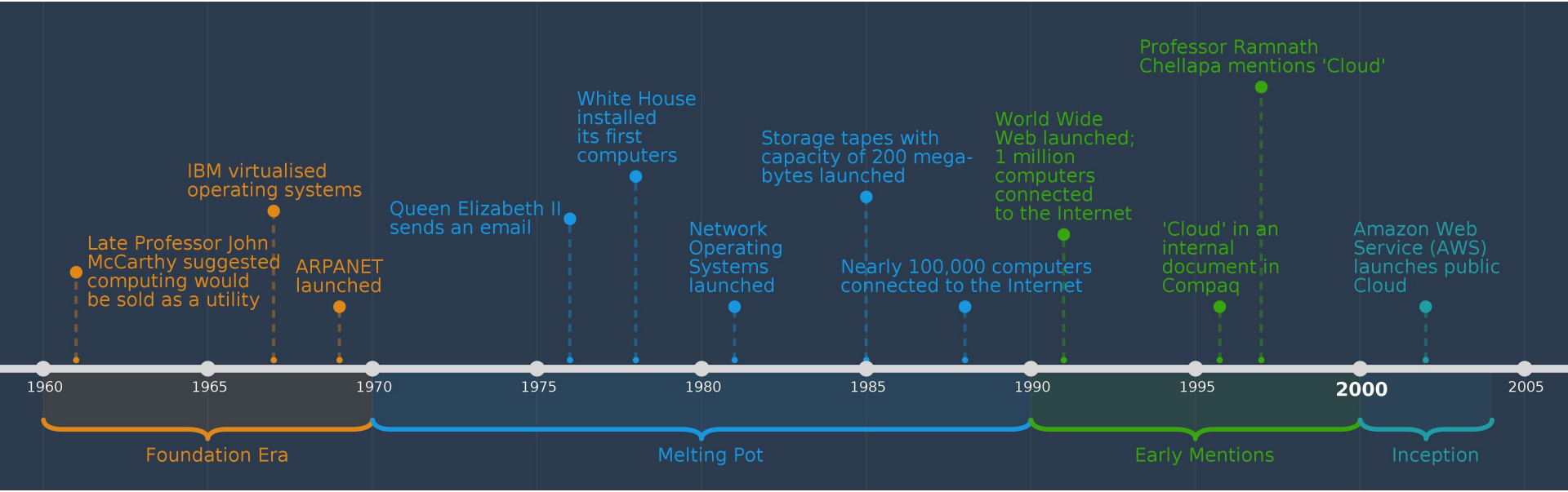
*“Keep in mind: ‘AWS’ stands for ‘Amazon **Web Services**’.”*

Ancient Technical Marketing Maxim

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

History of the Public Cloud

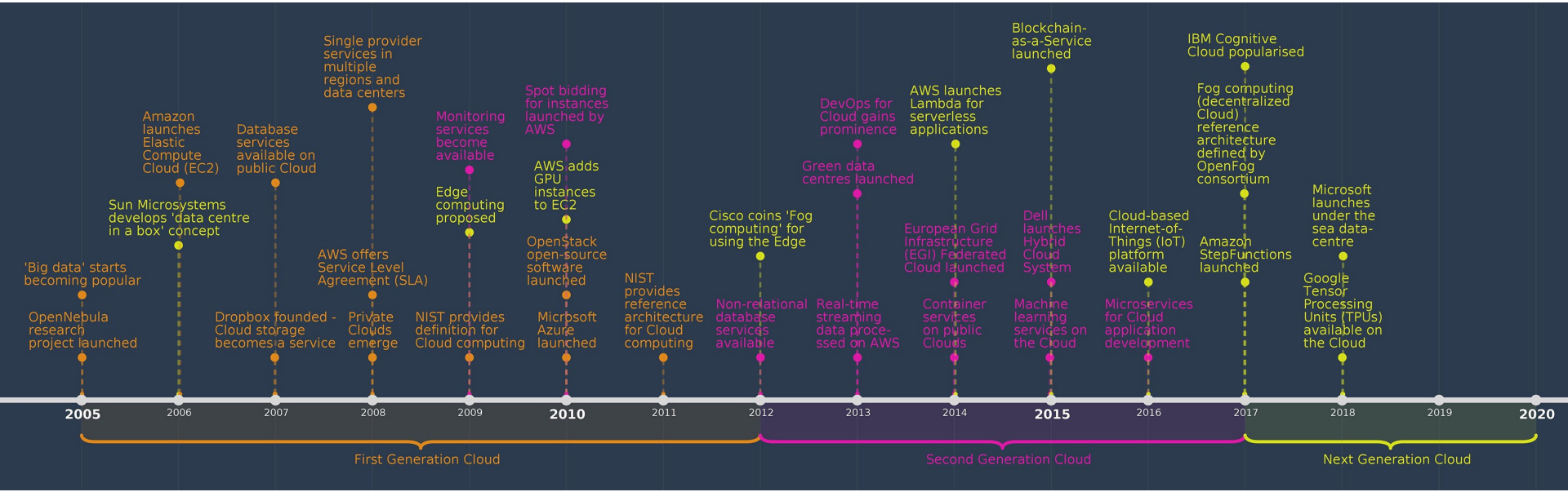
Source: Blesson Varghese, *History of the Cloud*, 2019



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

History of the Public Cloud

Source: Blesson Varghese, *History of the Cloud*, 2019



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Public Cloud Security Coevolution

- Customers are rushing to deploy in the public cloud
  - Some customers think they can replicate their enterprise networks in the public cloud
  - Most know better
- Security vendors partner with public cloud provides to facilitate coevolution
  - Public cloud providers are evolving to prove broader networking capabilities
  - Example: gateway load balancers for service insertion

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is *Scale* in the Public Cloud?

- Scaling volume of traffic
  - Load Balancing
- Scaling connectivity
  - Remote access VPN
  - Intracloud connectivity (AWS Transit Gateway, Azure vWAN Hub)
  - Intercloud connectivity (AWS VPG, Azure VNG, Multicloud Defense*)
- Accelerating application development
  - Complex application dependencies and associated security challenges
- Scaling visibility – including dynamic attributes

*Feature coming soon

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancers

- Network Load Balancers
- Application Load Balancers
- Gateway Load Balancers
- DNS Load Balancers

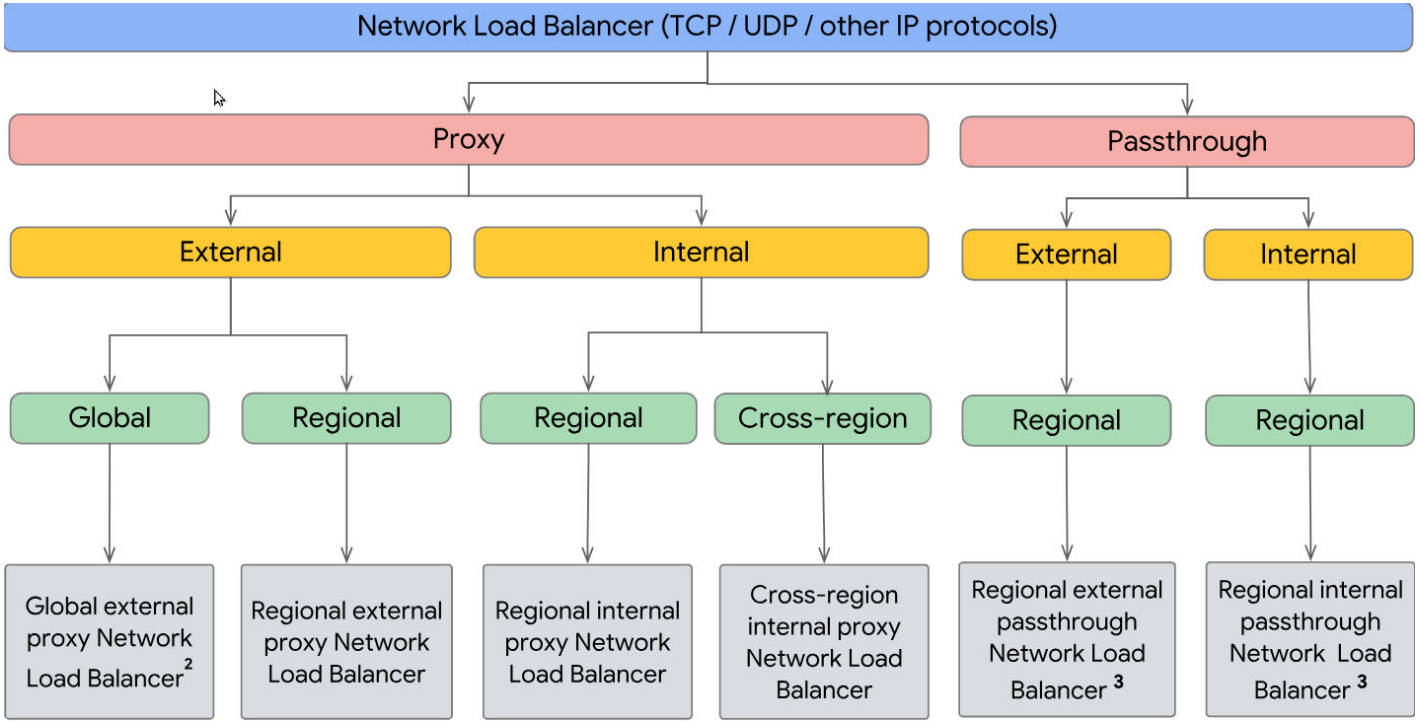
Network Load Balancers (NLBs)

- External (public) load balancers
  - Frontend service definition
  - NAT
    - Destination NAT is motivated by behavior of backend servers. Typically, backend servers expect traffic to be addressed to them.
    - Not necessary for firewalls. You may want to preserve the destination IP if a single load balancer has multiple frontend IPs (Azure *Floating IP* feature)
- Internal load balancers
  - Used for east-west and outbound traffic
  - Azure ILB can handle all ports and protocols (HA port feature)
  - GCP ability to handle all ports and protocols is in review

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

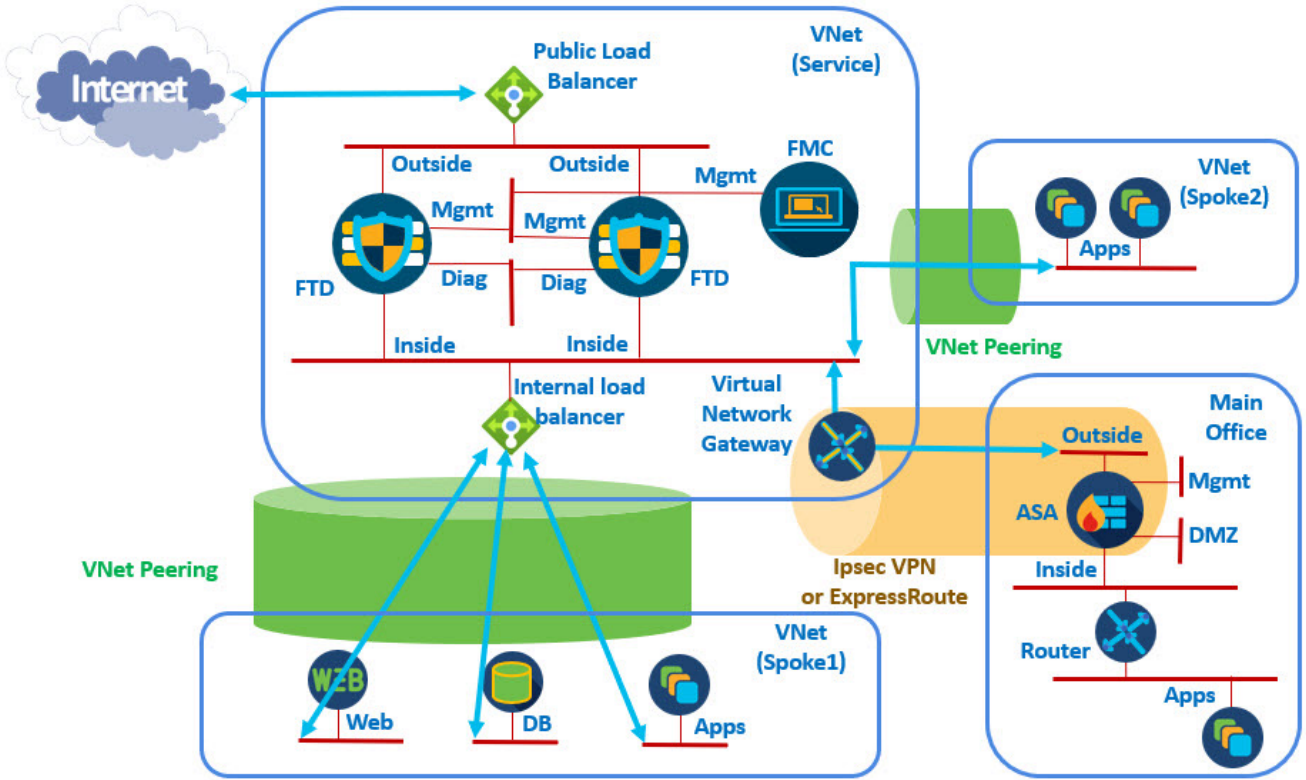
GCP Network Load Balancers

https://cloud.google.com/load-balancing/docs/choosing-load-balancer



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Load Balancer Sandwich (Azure)

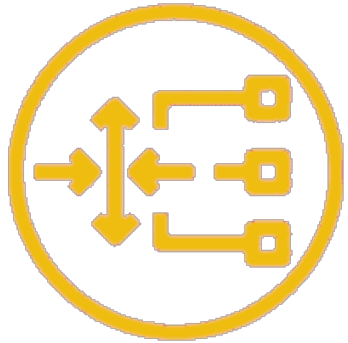


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Gateway Load Balancers (GLBs)

The right way to do service insertion in the public cloud!

- Traditional load balances were designed to scale application servers, not firewalls
- Public cloud providers are adopting gateway load balancers (GWLBs) to address this need
  - AWS introduced it in November 2020
  - Azure introduced it in November 2021
- GWLBs allow transparent insertion of firewalls into the data path.



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

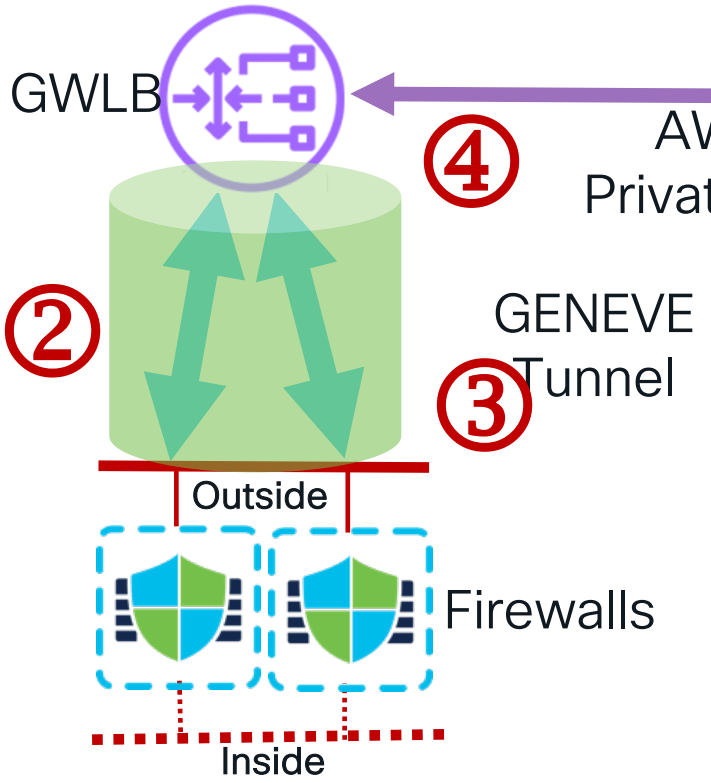
AWS GWLB, GWLB Endpoint (GWLBe), and Endpoint Service

- GWLB
  - Forwards traffic to the firewalls **inside a GENEVE tunnel**
  - Load balances between firewalls in a Target Group
  - Does not modify packets or packet headers
  - Forwards all packets associated with a particular connection to the same firewall

- GWLB endpoint
- Endpoint service
  - At most one endpoint service per GWLB
  - Associates one or more GWLBes to a GWLB
  - Creates a private link between the GWLB and GWLBe

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

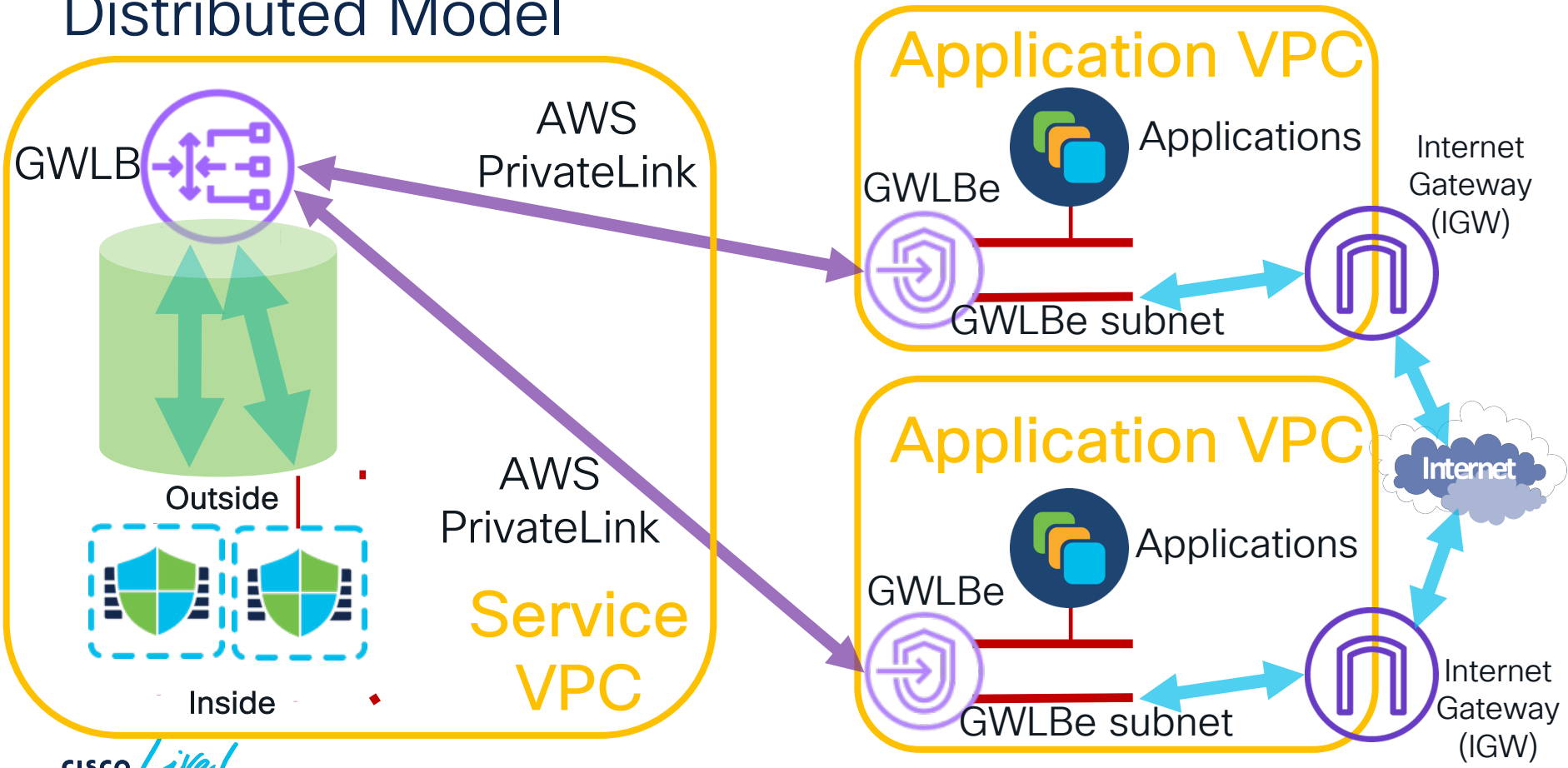
Traffic Flow Between the GWLBe, GWLB, and Firewalls



1. Traffic is forwarded from the GWLBe to the GWLB across PrivateLink
2. Traffic is forwarded to one of the Firewalls in the GWLB Target Group
3. Traffic is processed by the firewall and returned to the load balancer
4. Traffic is returned to the GWLBe

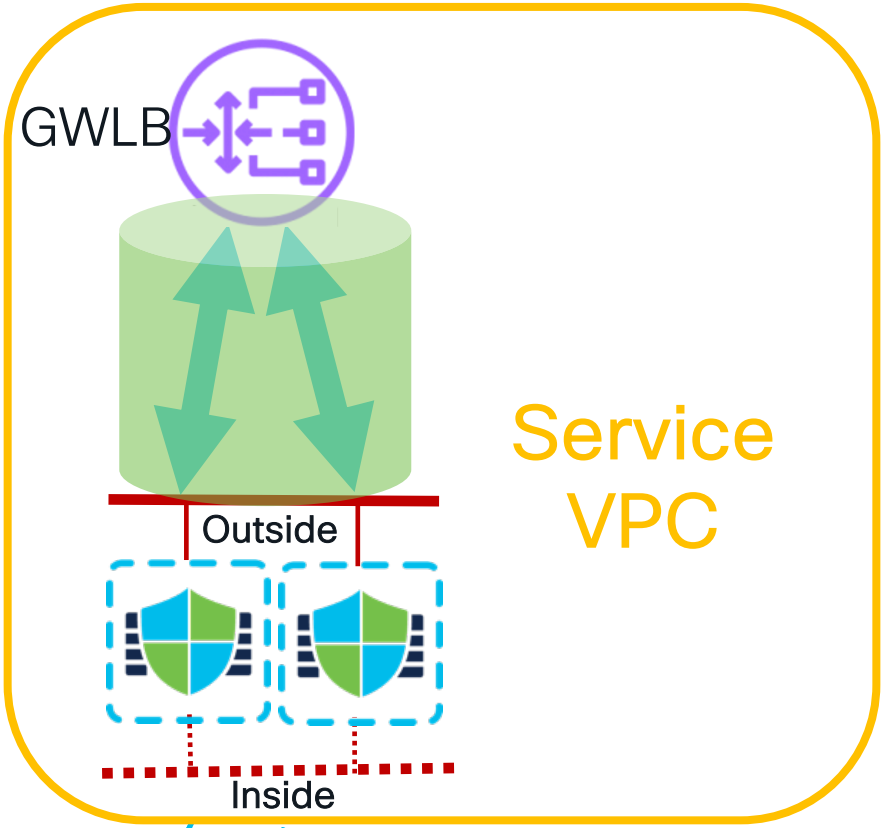
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

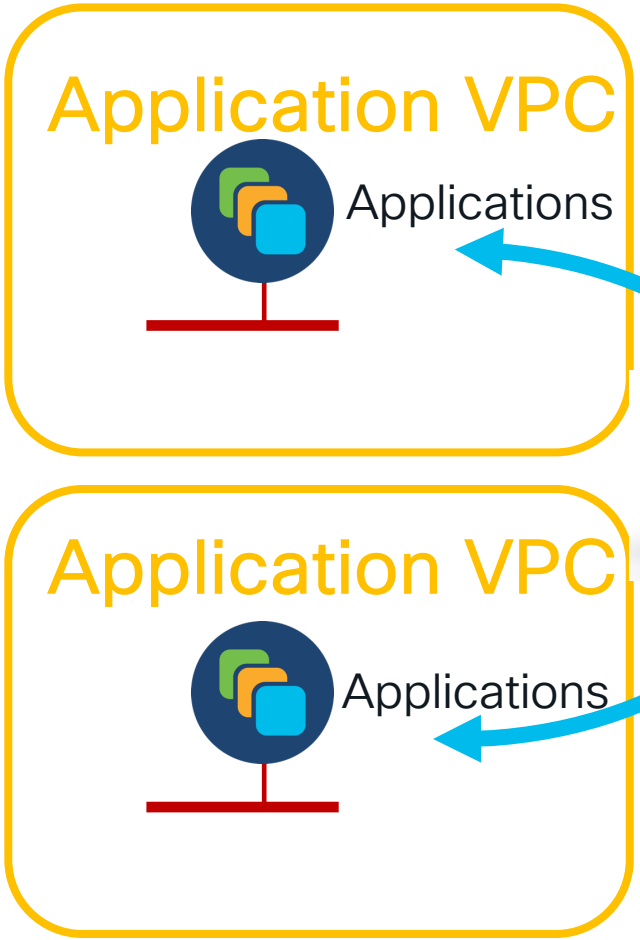
North/South and Outbound Traffic Distributed Model



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

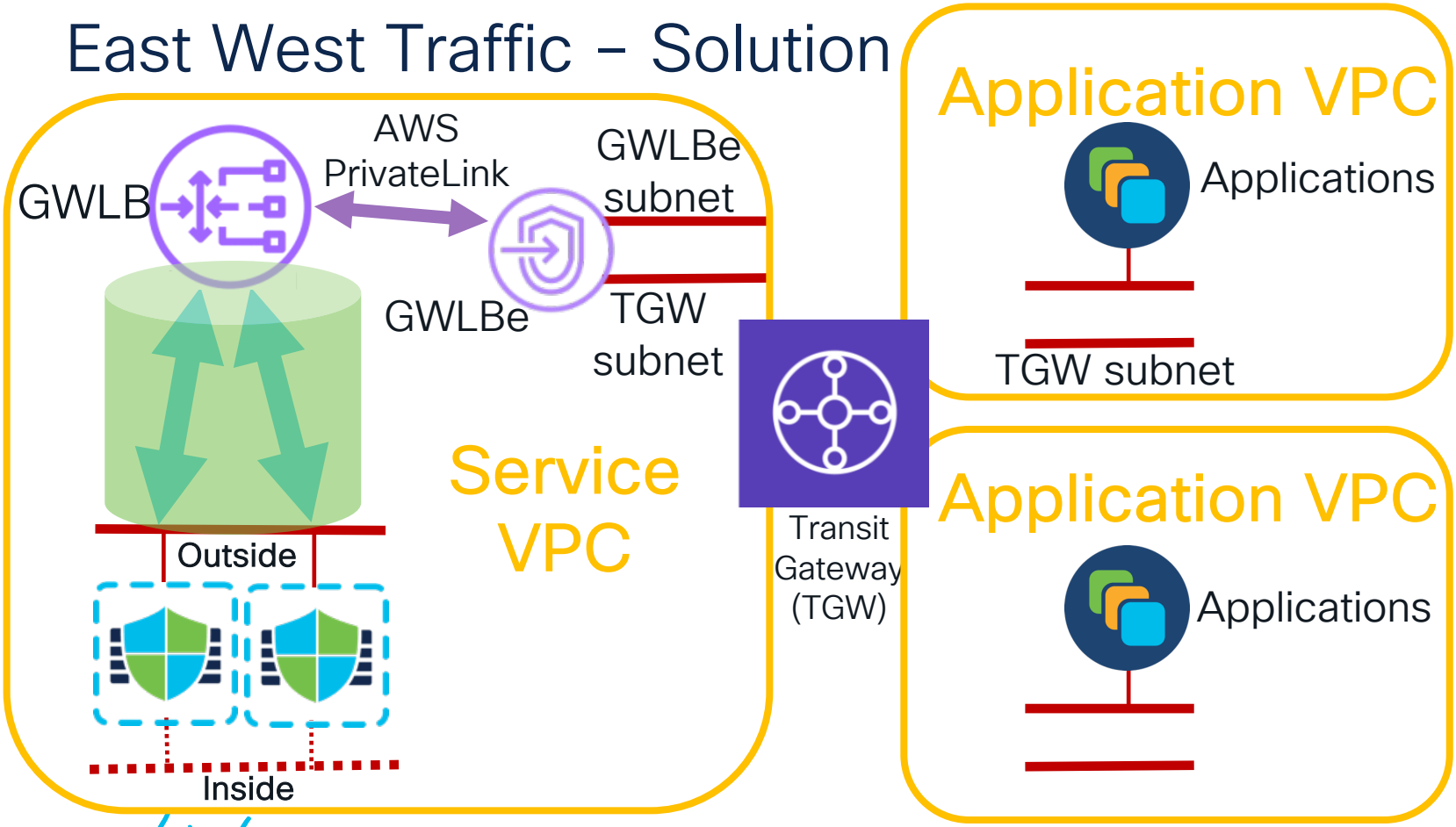
East West Traffic – Problem





© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

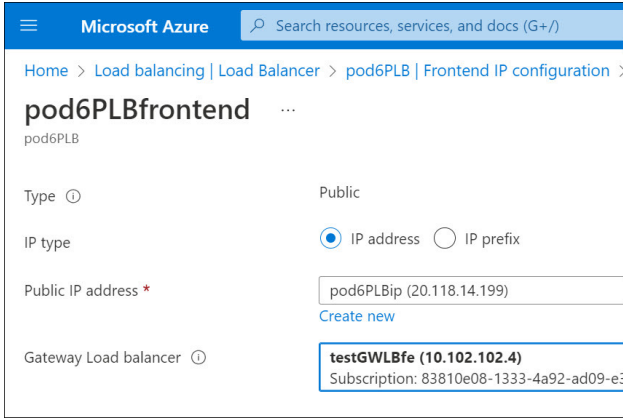
East West Traffic – Solution

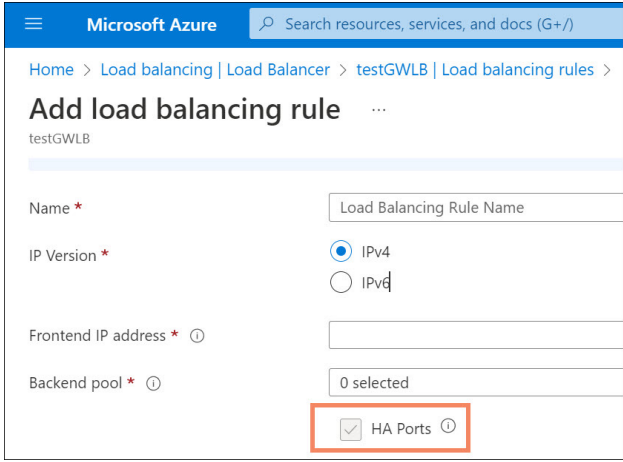


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Azure GWLB

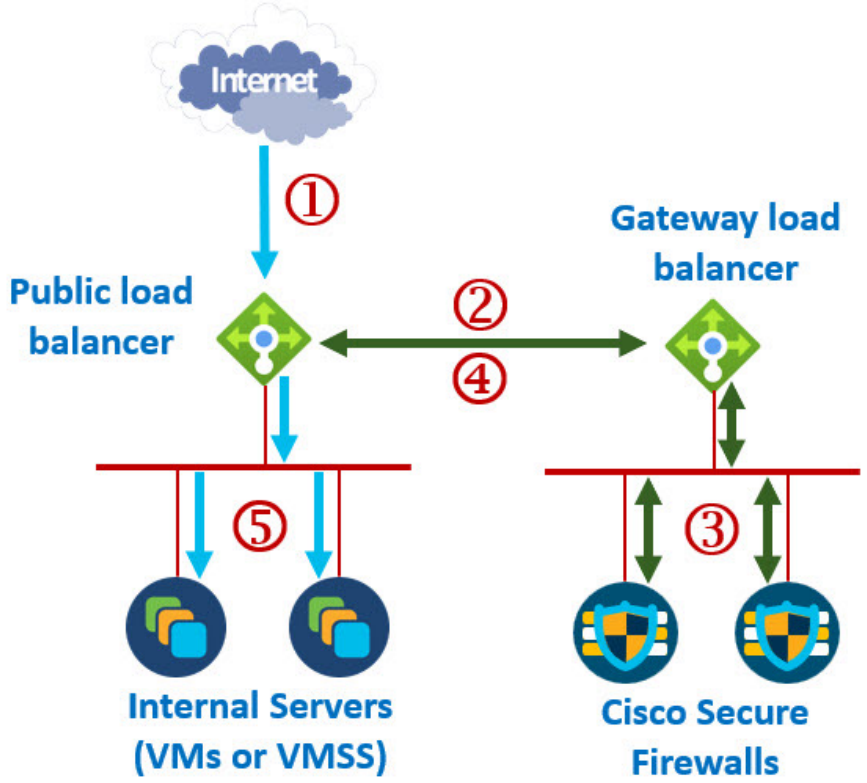
- Associated with a (standard SKU) public load balancer or network interface.
  - Network interface must have a (standard SKU) public IP.
  - Does not currently support East-West traffic.
- Transparently intercepts traffic
  - Requires no Azure routing changes
- Traffic received by the GWLB is load-balanced between backend pool devices
  - Uses VXLAN over UDP
  - Always load balances all ports and protocols





© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Packet Flow in Azure GWLB with Public Load Balancer



① Inbound flow uses public IP of public load balancer.

② Flow is forwarded transparently from the public load balancer to the gateway load balancer.

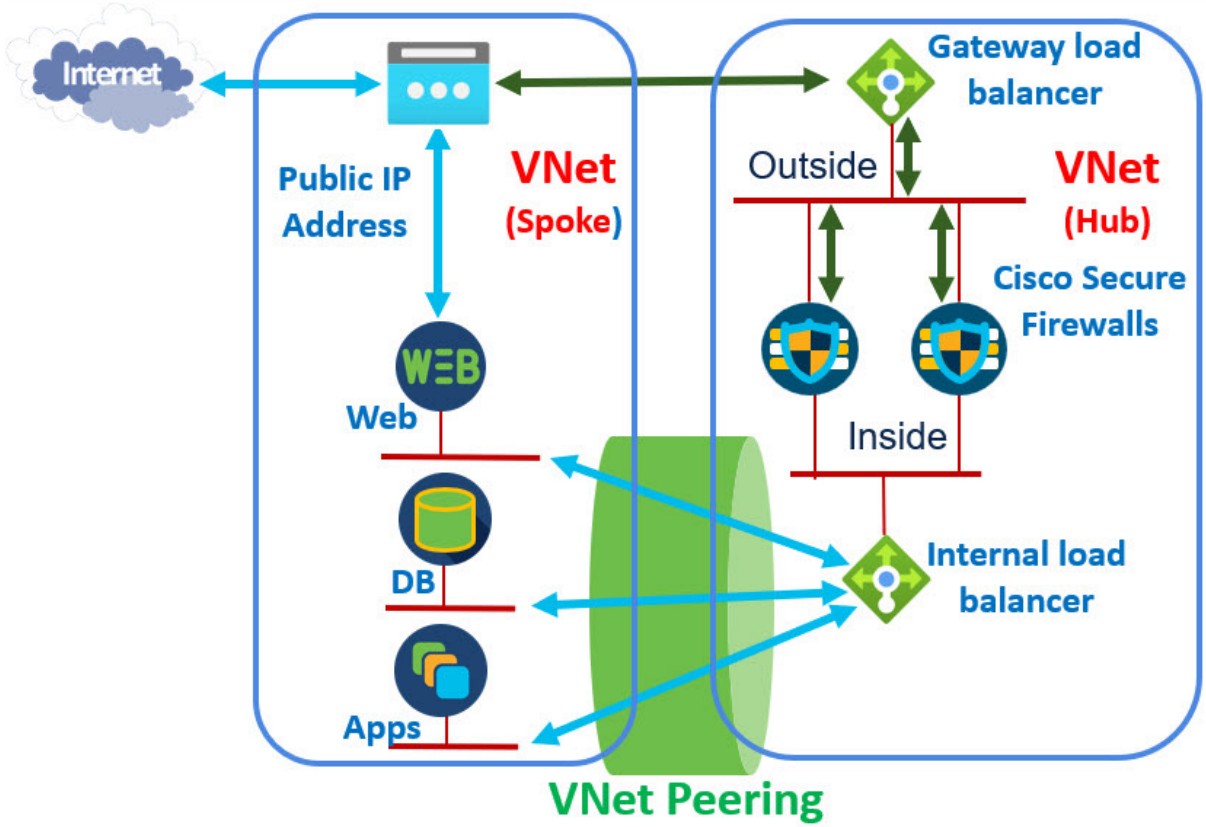
③ Flow is inspected by a firewall and returned to the gateway load balancer.

④ Flow is returned to the public load balancer.

⑤ Flow is forwarded to an internal server.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

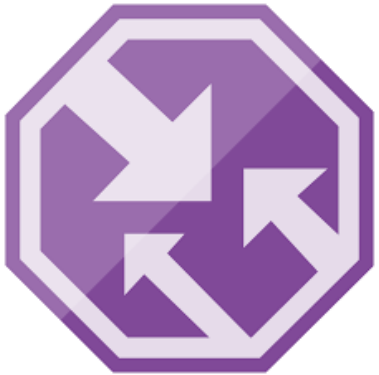
Combining Azure GWLB and ILB



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

DNS Load Balancers

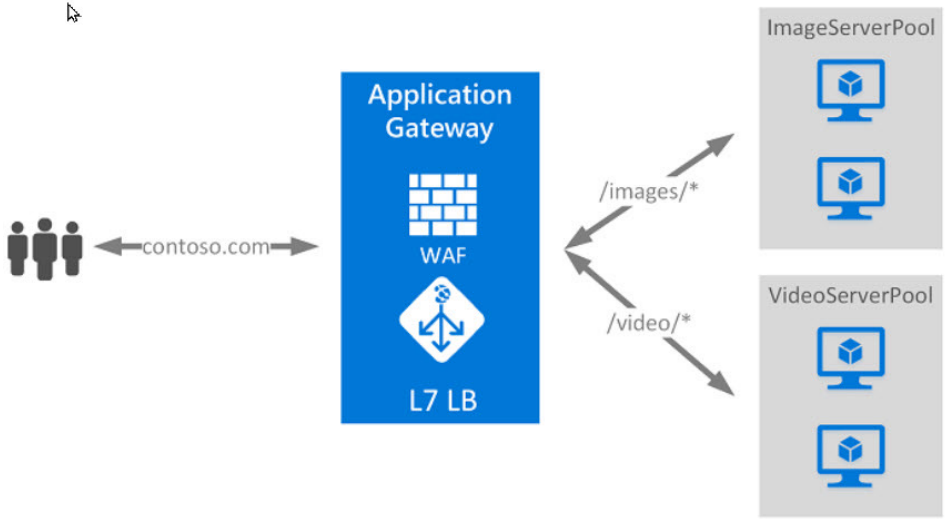
- Works by updating DNS
  - Modifies A/AAAA records or CNAME records
  - Data path does not go through separate entity
- Ideal for load balancing remote access VPN
- Examples:
  - AWS Route53
  - Azure Traffic Manager



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Application Load Balancers (ALBs)

- Uses layer 7 information to load balance traffic
- Key use case is HTTP/HTTPS
  - Can direct different URLs (with the same FQDN) to different backend devices
  - Can direct requests to different backend devices based on media type
  - Can terminate TLS connects, offloading encryption/decryption from backend servers



Note: ALBs are not generally used in front of security solutions

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Autoscale

- Security solutions (static) scaling can be expensive and wasteful
- To address this, many security solutions use autoscaling (adding and removing instances based on load)
- Typically used behind NLBs and GPBs (and ALBs for applications)
- Often utilize cloud native capabilities
  - AWS: auto scaling groups, lambda functions
  - Azure: virtual machine scale sets (VMSS), logic apps, function apps
  - GCP: instance group, Google functions
- Autoscale also can provide resilience as unhealthy nodes can be replaced

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

High Availability and Resilience

High Availability in the Public Cloud

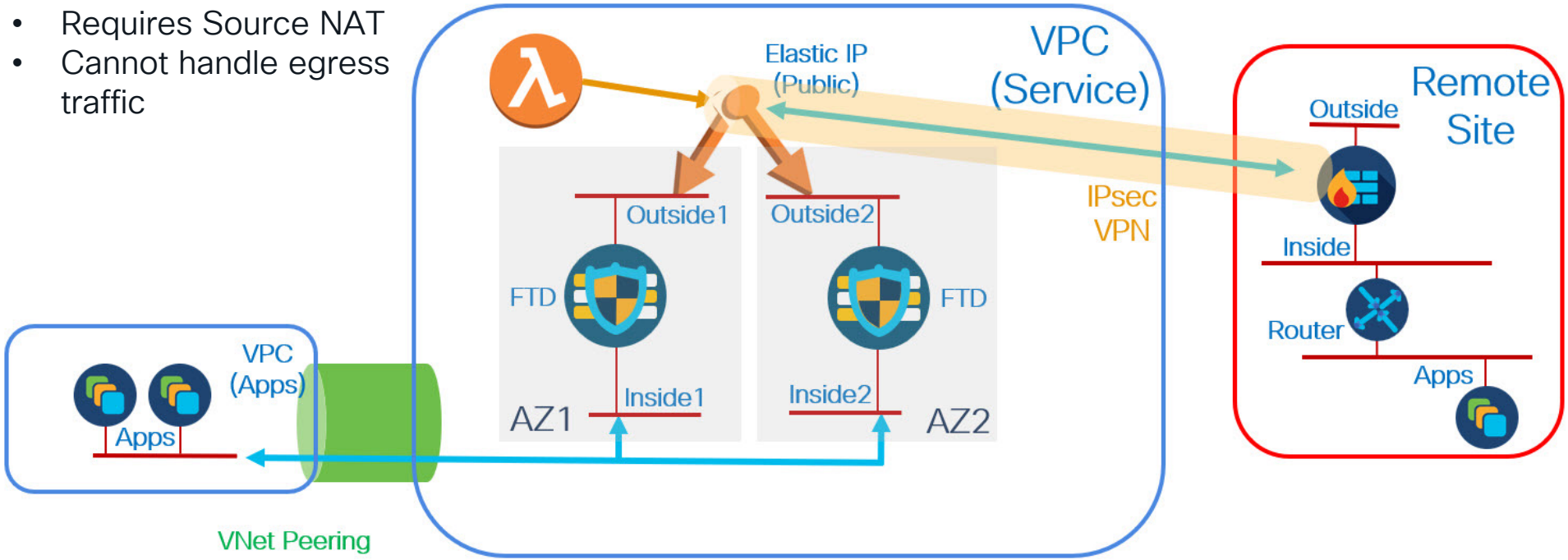
- Approaches
  - Using load balancer health checks (usually active-active)
  - Using public cloud serverless infrastructure (usually active-standby)
    - AWS Lambda Layer
    - Azure Function Apps
    - GCP Functions
- Key limitations
  - Lack of layer two semantics -- cannot advertise new address with ARP
  - IP addresses are often pinned to the network interface objects
  - Time required for load balancers to detect unhealthy hosts is too long
  - Time required for API calls to public cloud providers is too long

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demonstration: IPsec Tunnel Failover Using AWS Lambda Functions

IPsec HA Scenario 1 – VPC Peering

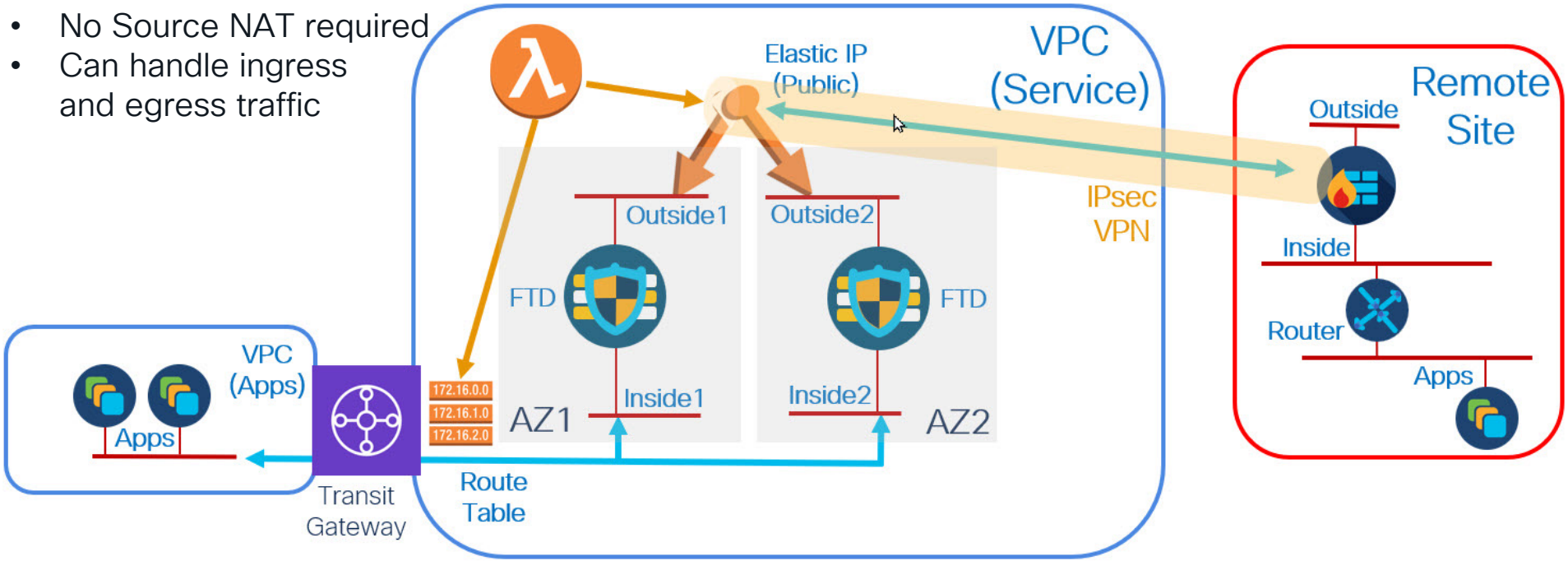
- Requires Source NAT
- Cannot handle egress traffic



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

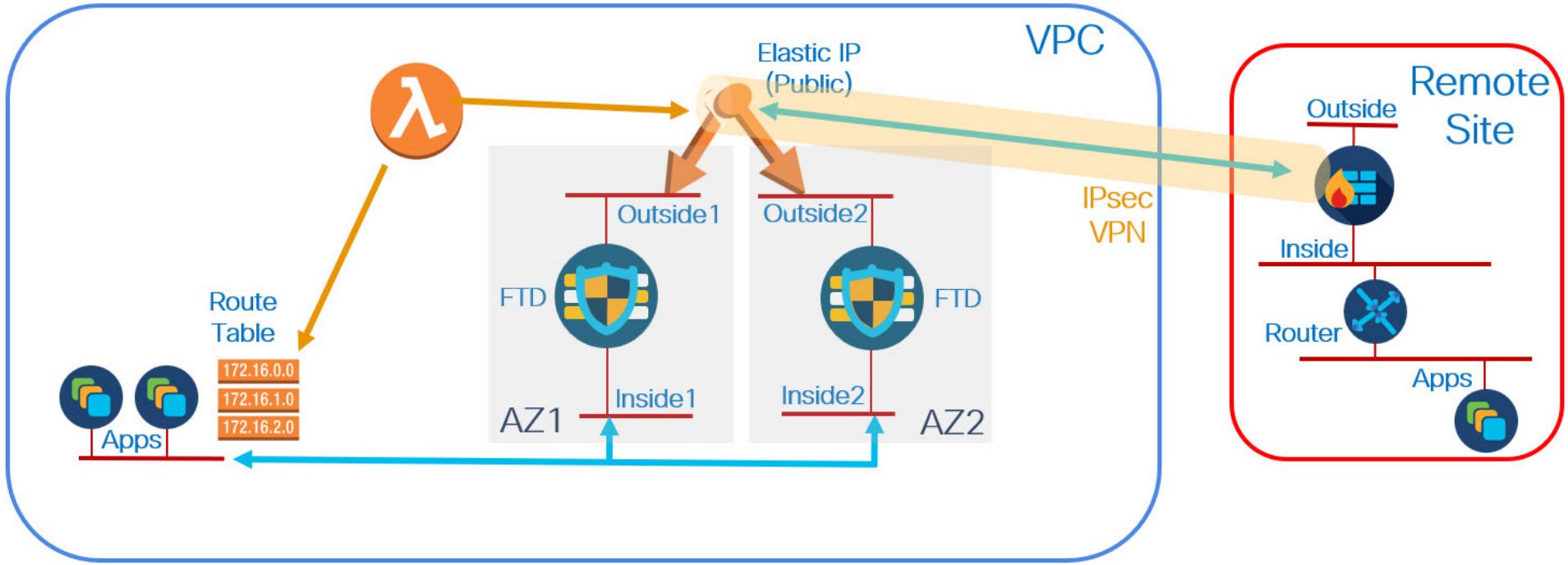
IPsec HA Scenario 2 – Transit Gateway

- No Source NAT required
- Can handle ingress and egress traffic



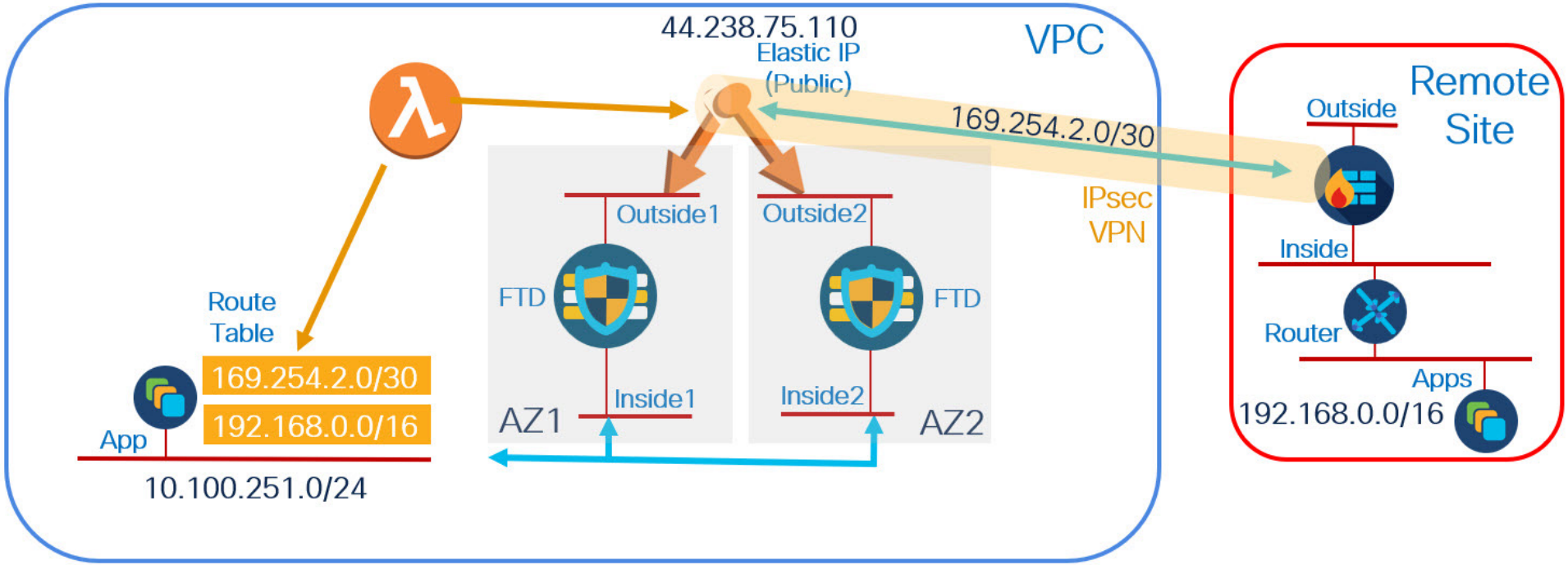
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec HA Scenario 3 – Simplified Test Deployment



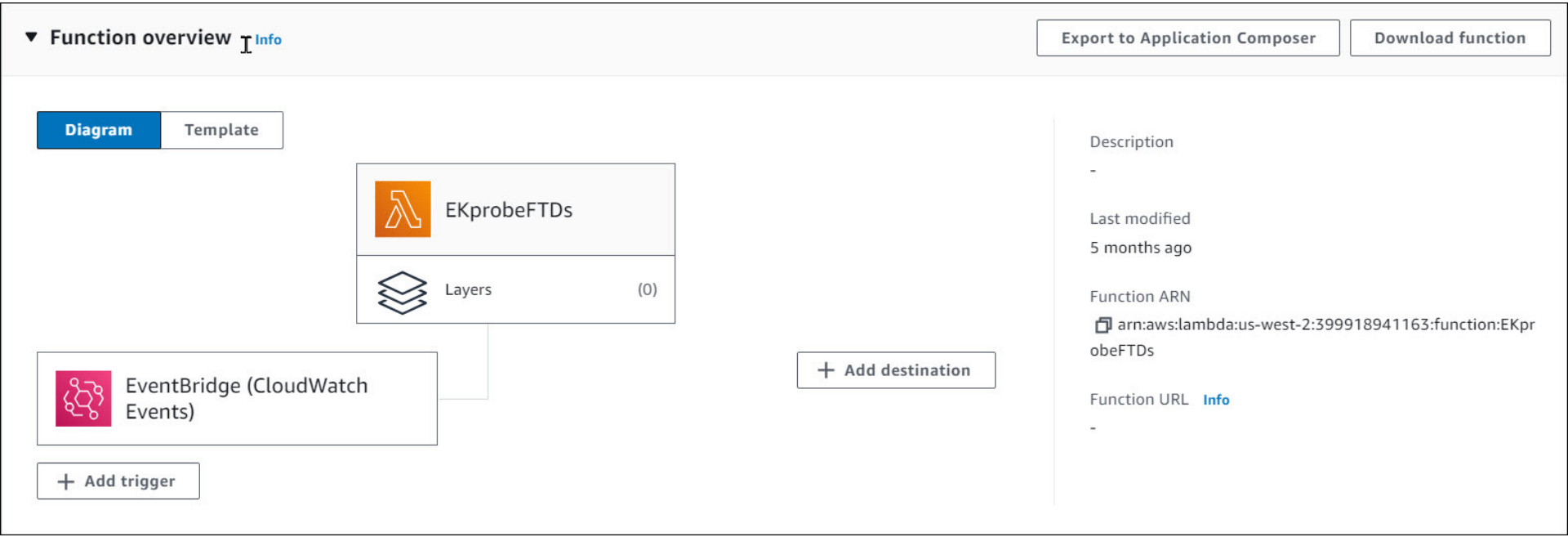
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec HA Scenario 3 – Demo Deployment



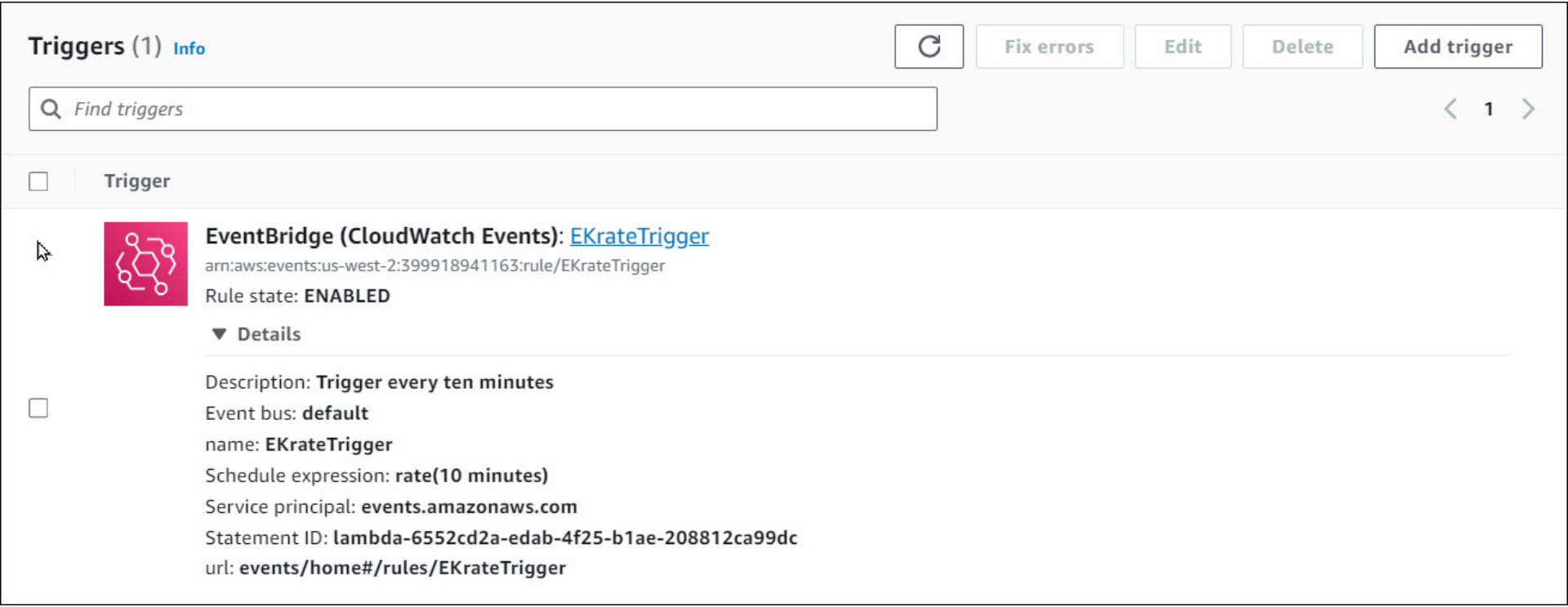
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lambda Function



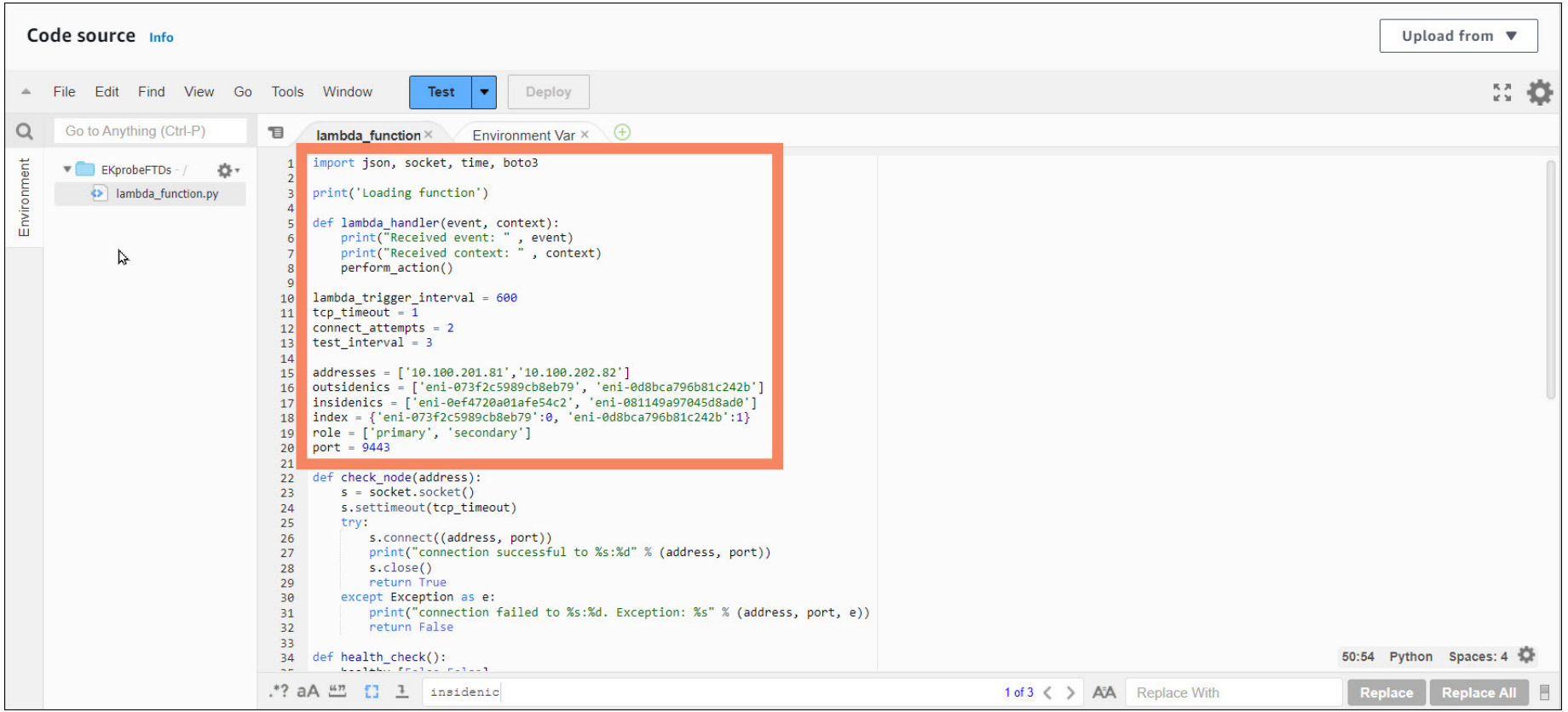
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lambda Function Trigger



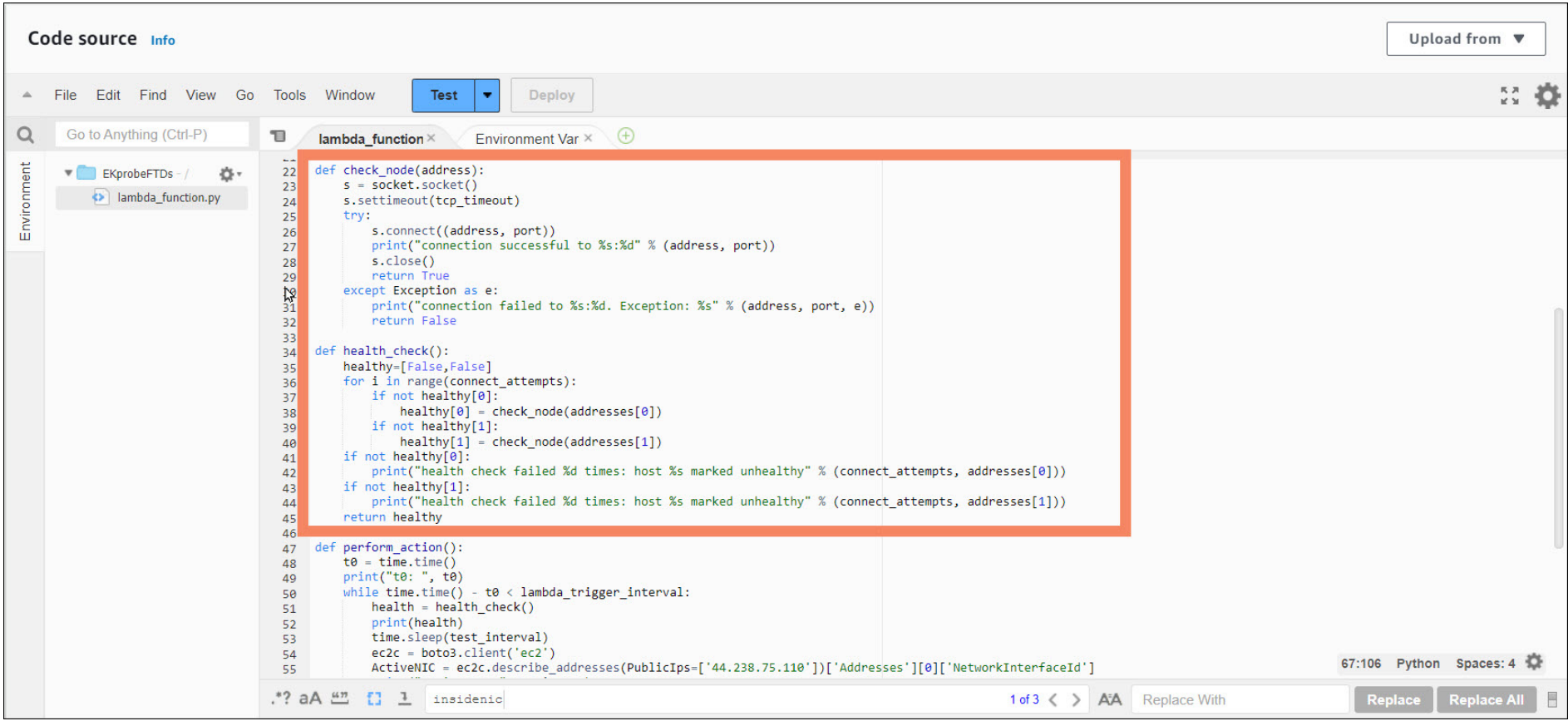
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lambda Function Code – Slide 1 of 3



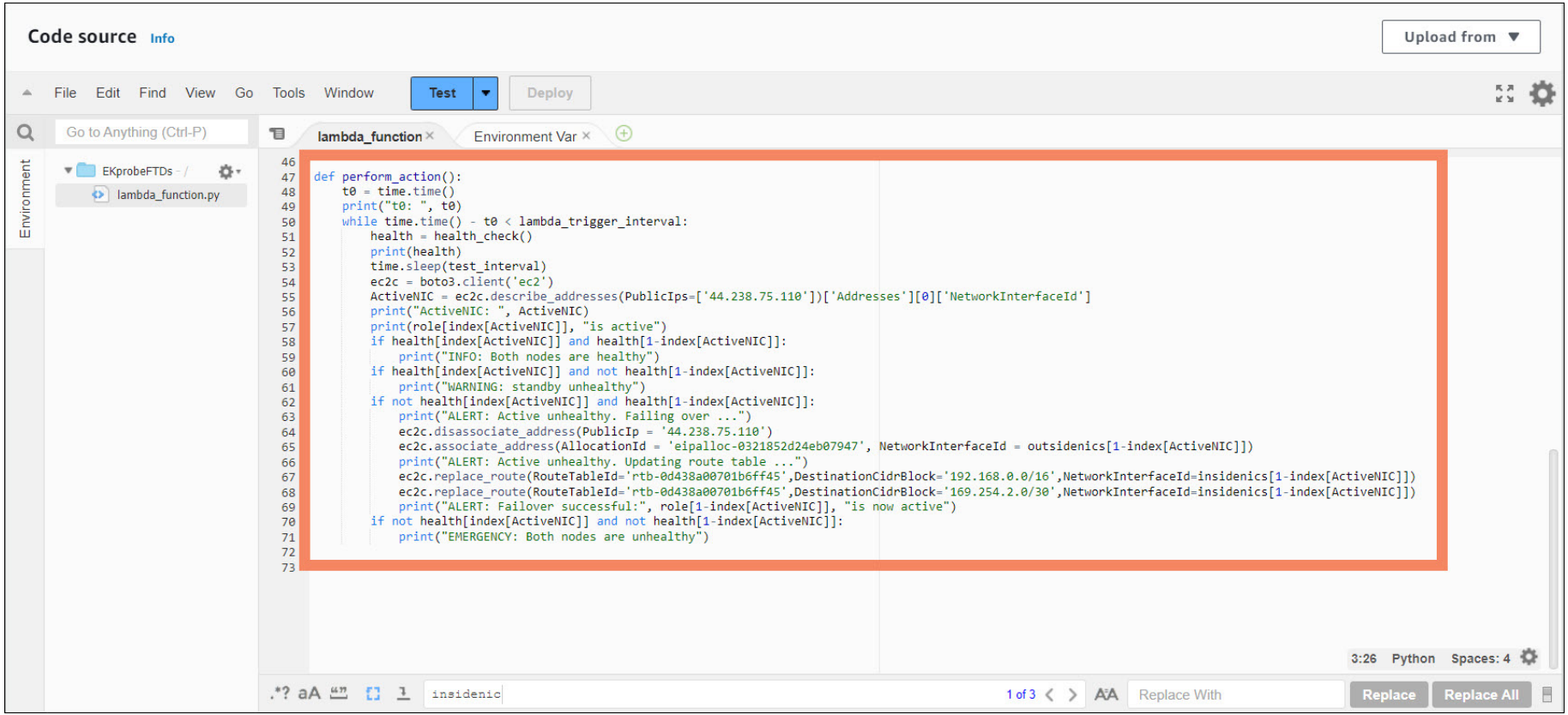
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lambda Function Code – Slide 2 of 3

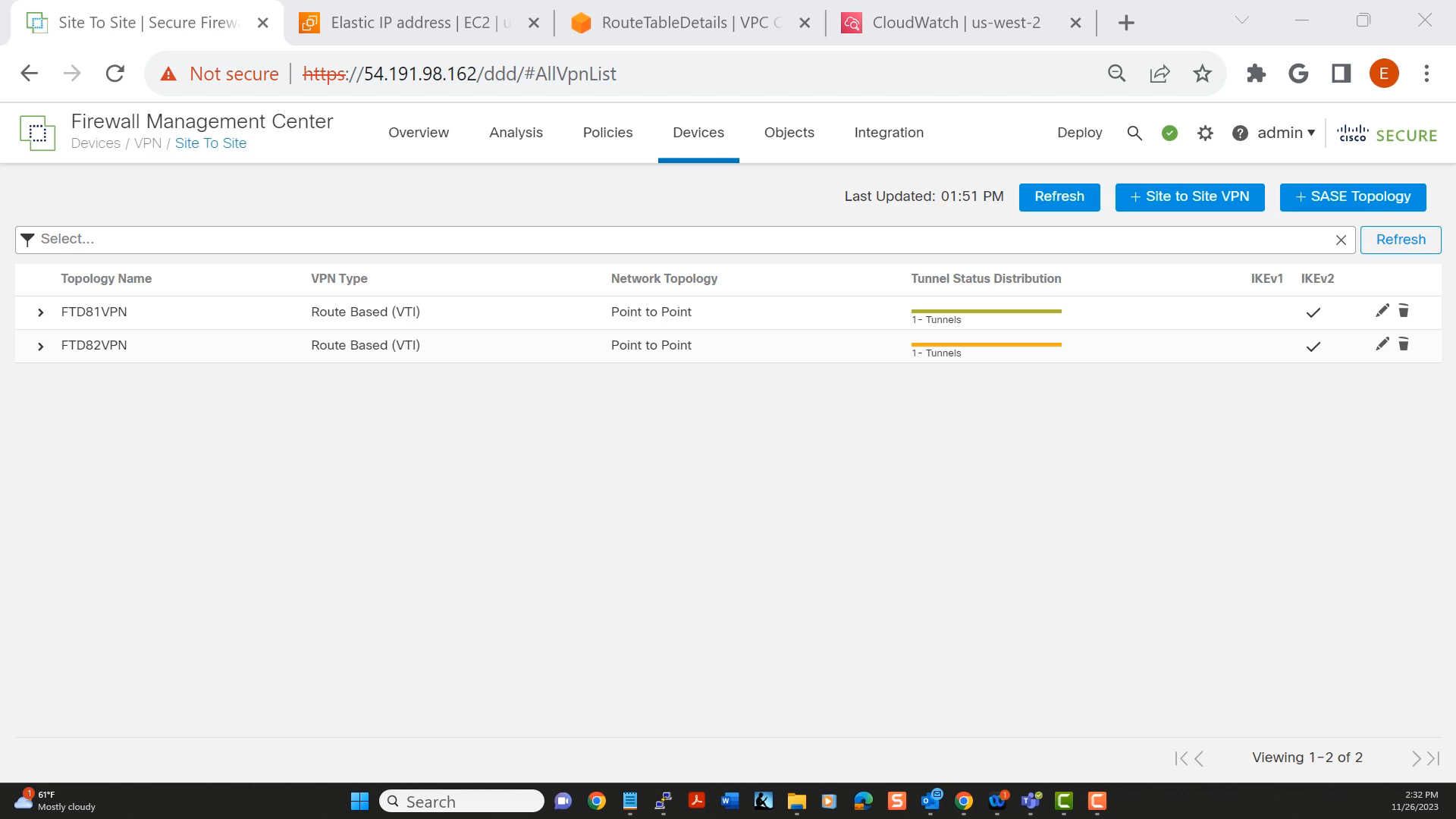


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lambda Function Code – Slide 3 of 3



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public



Site To Site | Secure Firew | Elastic IP address | EC2 | u | RouteTableDetails | VPC C | CloudWatch | us-west-2

Not secure | ~~https~~://54.191.98.162/ddd/#AllVpnList

Firewall Management Center
Devices / VPN / Site To Site

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin | SECURE

Last Updated: 01:51 PM | Refresh | + Site to Site VPN | + SASE Topology

Select... | Refresh

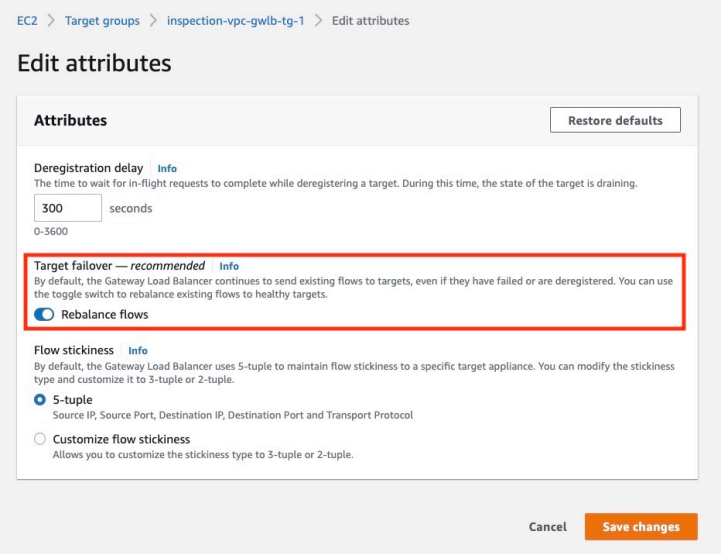
Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
FTD81VPN	Route Based (VTI)	Point to Point	1- Tunnels		✓
FTD82VPN	Route Based (VTI)	Point to Point	1- Tunnels		✓

Viewing 1-2 of 2

61°F Mostly cloudy | Search | 2:32 PM 11/26/2023

Target Failover in AWS

- Moves existing connections from unhealthy nodes to healthy nodes.
- Only available for Gateway Load Balancers, disabled by default
- To configure this setting with the AWS CLI, use the **modify-target-group-attributes** command
  with the following key value pairs:
  - Key=**target_failover.on_deregistration** and Value= **no_rebalance** (default) or **rebalance**
  - Key=**target_failover.on_unhealthy** and Value= **no_rebalance** (default) or **rebalance**
- These attributes are also available in the AWS Cloud Formation Templates.



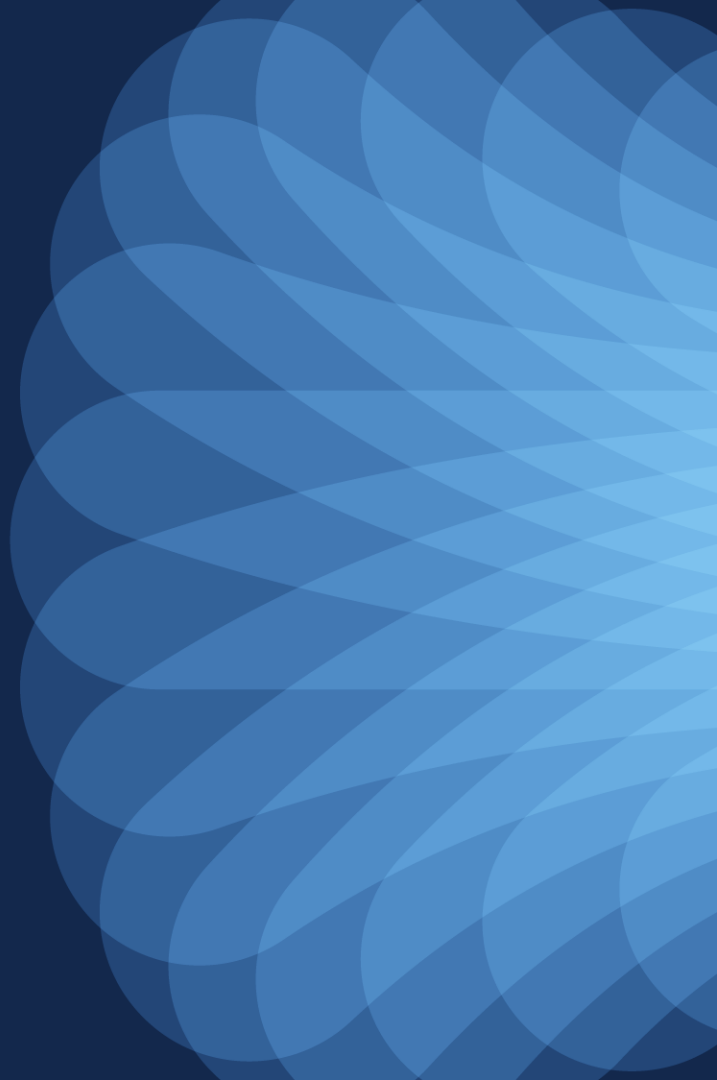
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Target Failover in Azure and GCP

- Target Failover in Azure
  - Currently Azure GWLBs and NLBs do not perform target failover.
  - Even when a target becomes unhealthy, the load balancers forward the remaining packets of existing flows to the same host.
- Target Failover in GCP
  - Called connection persistence. This is a legacy feature in all GCP load balancers.
    - DEFAULT_FOR_PROTOCOL (default). Move existing UDP a healthy target. Keep (persist) sending TCP packets to the unhealthy target.
    - NEVER_PERSIST. Move existing UDP and TCP connections to a healthy target.
    - ALWAYS_PERSIST. Keep (persist) sending UDP and TCP packets to the unhealthy target.

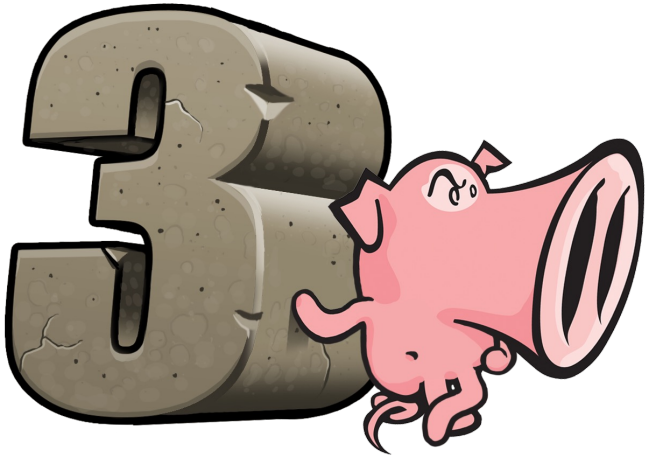
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Firewall



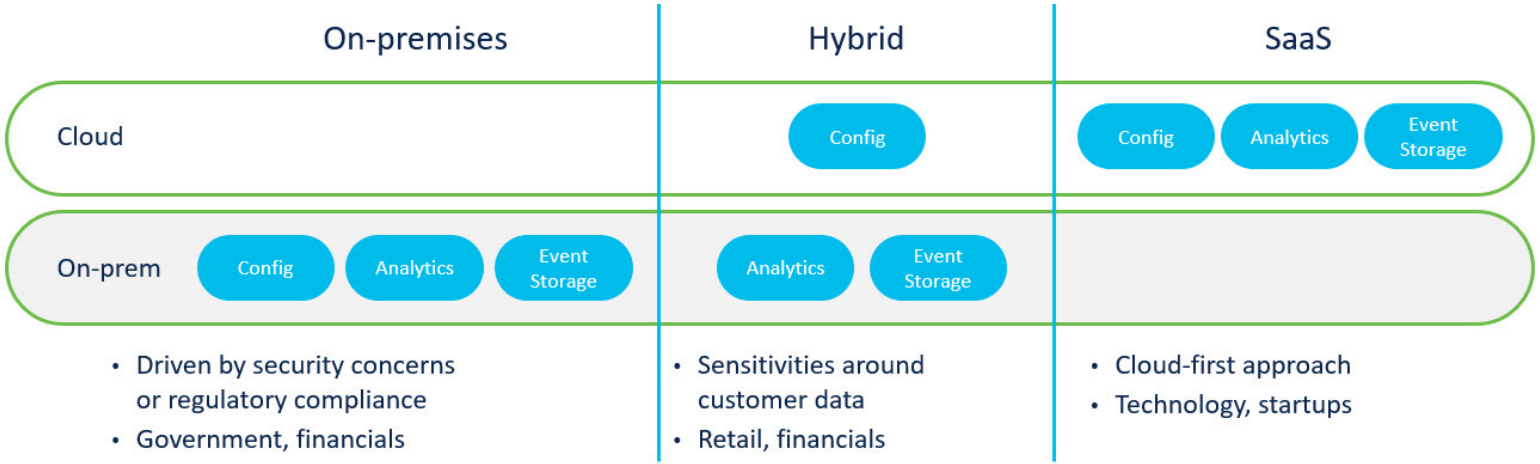
Cisco Secure Firewall Overview

- Stateful Firewall
  - Layer 1 (inline pairs/inline sets)
  - Layer 2 (bridge groups/BVIs)
  - Layer 3 and 4 (routed interfaces)
- NGIPS – Next-Generation Intrusion Prevention System
- AMP – Advanced Malware Protection
- VPN – Virtual Private Network
- URL – URL filtering
- SI – Security Intelligence



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Firewall Management



- On Premises: Firewall Management Center (FMC)
- SaaS: Cisco Defense Orchestrator (CDO) with built-in cloud delivered FMC

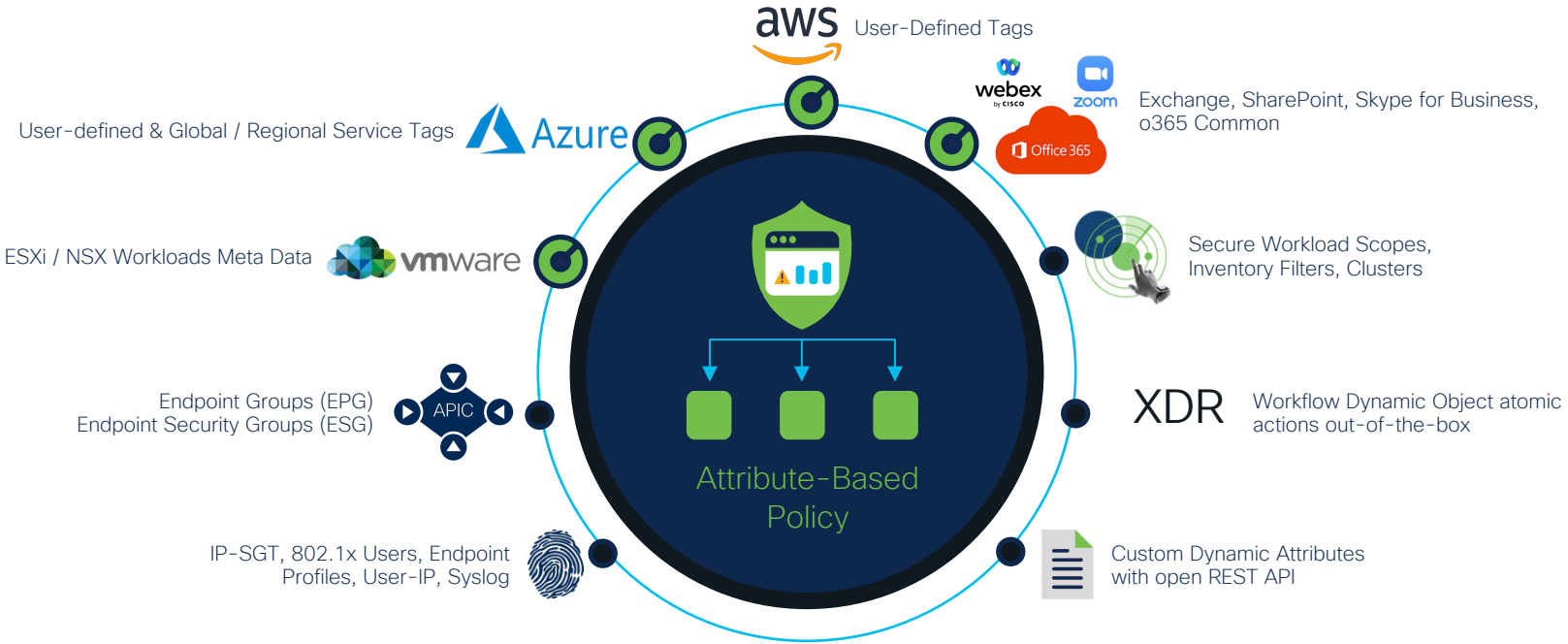
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Firewall in the Multi-cloud

- Clustering
- Dynamic Policy
- Better integration with public cloud infrastructure
- Infrastructure as Code and Automation
- Accelerated Networking
- Gateway Load balancer integration
- Auto Scaling
- Snapshot support

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

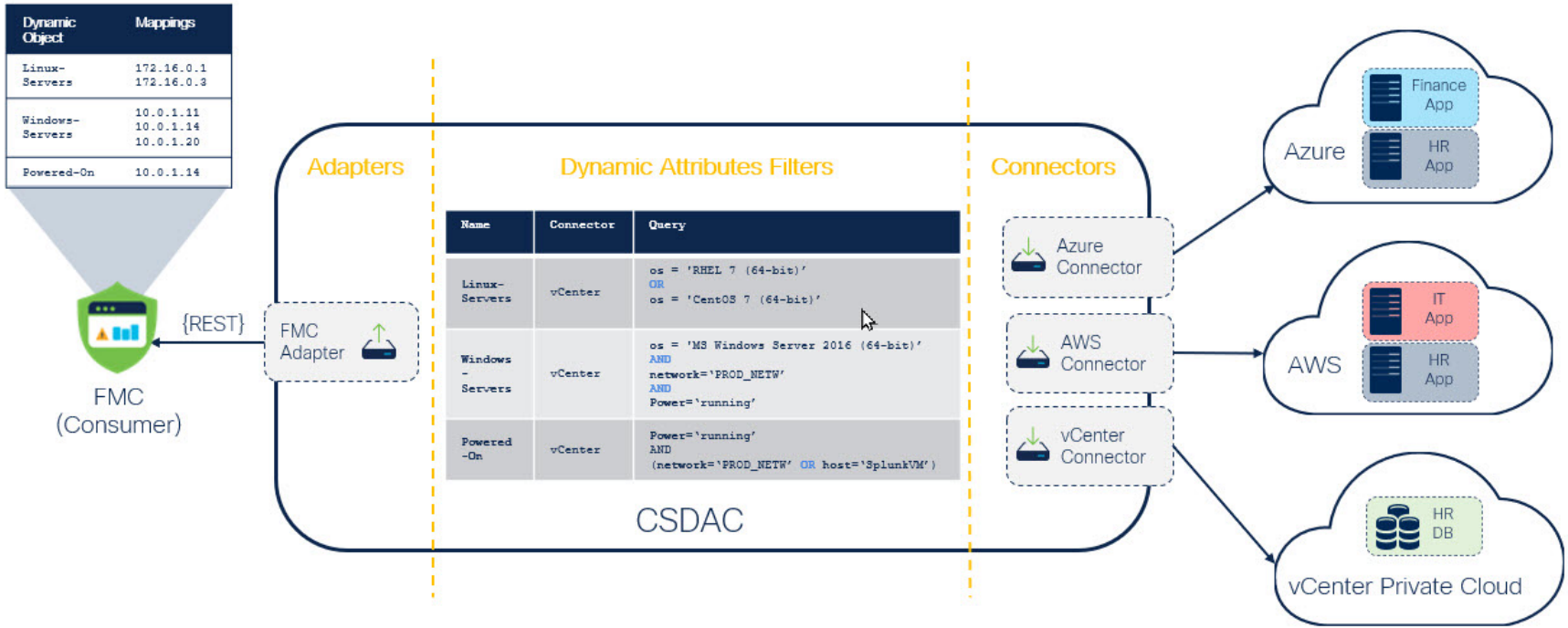
Dynamic Attributes and Security Policies



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Dynamic Attribute Connector (CSDAC)

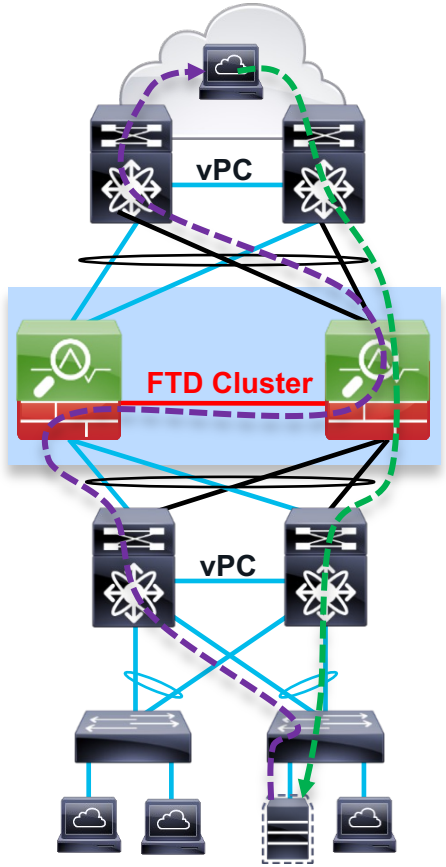
Stand-alone VM, SaaS offering, or Integrated into on-premises FMC



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Clustering Cisco Secure Firewall

- Combines multiple Cisco Secure Firewalls into a single logical device
  - Allows pay as you grow sizing – nodes can be added to existing clusters
  - Up to 16 nodes, depending on platform
- *May* provide resilience – dependent on external load balancing
  - Physical devices can use EtherChannel with LACP to provide resilience.
  - Virtual devices require load balancers capable of connection rehashing.
- Originally to cluster physical Cisco ASA firewall
  - Later extended to Cisco Secure Firewall Threat Defense (FTD)
  - Recently extended to virtual devices



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Porting Cisco Clustering to the Public Clouding

Physical Cluster

- Data interfaces have two modes.
  - Individual interface mode – different IP addresses on different nodes (rarely used)
  - Spanned interface mode with EtherChannel
- CCL uses proprietary protocol over IP.
  - Increase MTU by 100 Bytes for cluster link.
- CCL uses broadcast for internode communication.
  - Uses dynamic node discovery

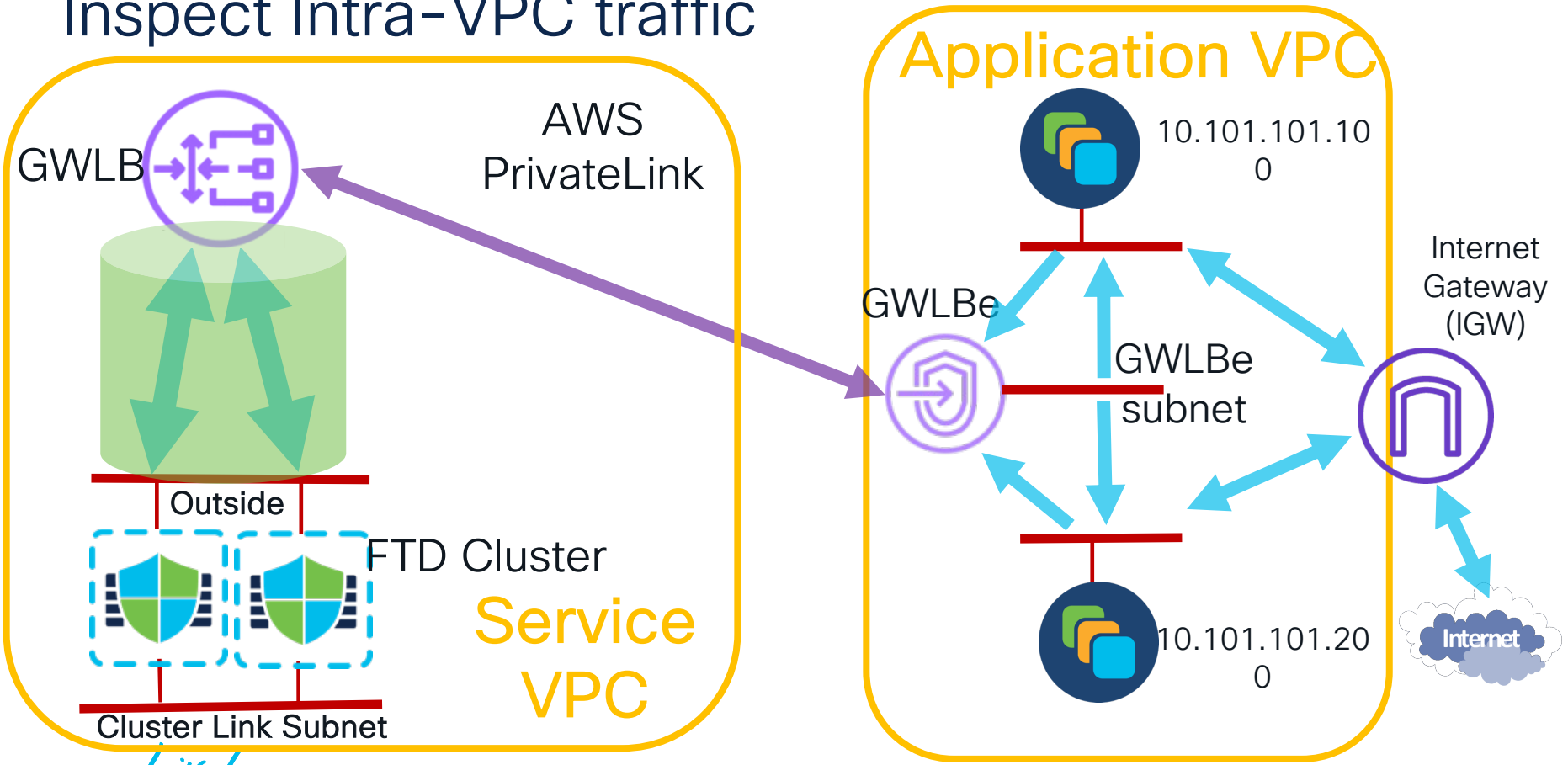
Virtual Cluster

- Data interfaces on each node use different IP addresses.
- CCL uses VXLAN over UDP.
  - Increase MTU by 160 Bytes for cluster link.
- CCL uses unicast for internode communication.
  - Requires static peer list

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demonstration: AWS Target Failover with Cisco Secure Firewall Cluster

Demonstration Topology
Inspect Intra-VPC traffic

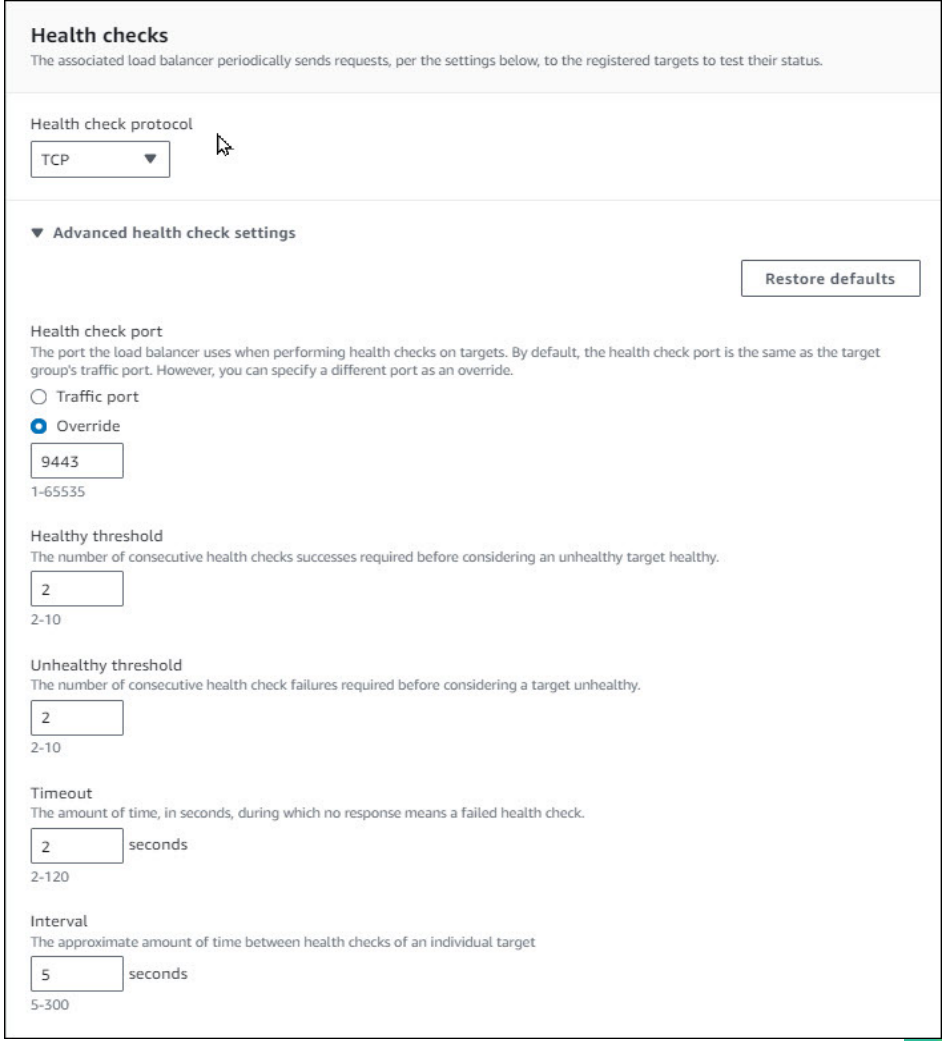


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Health Probe Settings

Defaults:

- Healthy threshold = 5
- Unhealthy threshold = 2
- Timeout = 5
- Interval = 10



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security

Details

arn:aws:elasticloadbalancing:us-west-2:399918941163:targetgroup/FTDvCluster/00d56815e5d166aaed

Target type	Protocol : Port	VPC	Load balancer
IP	GENEVE: 6081	vpc-0ce26a614c1c149d1	FTDvClusterGLB

Total targets	Healthy	Unhealthy	Unused	Initial	Draining
2	2	0	0	0	0

▶ **Distribution of targets by Availability Zone (AZ)**

Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets | Monitoring | Health checks | Attributes | Tags

Health check settings

Edit

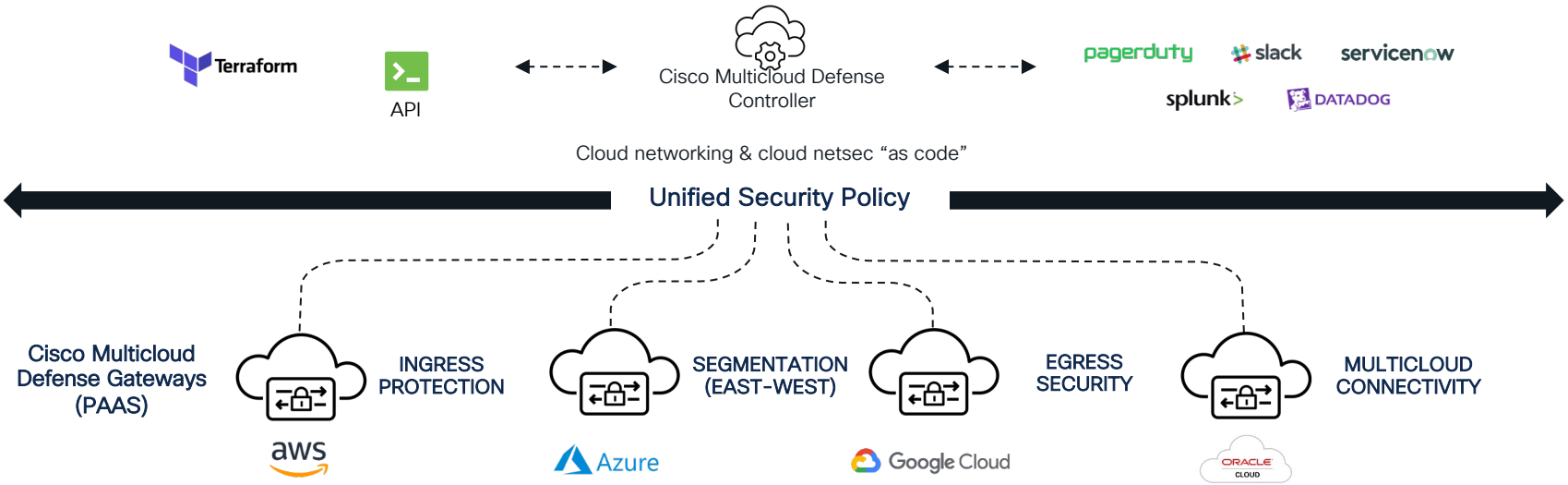
Protocol	Port	Healthy threshold	Unhealthy threshold
TCP	9443	2 consecutive health check successes	2 consecutive health check failures

Timeout	Interval
2 seconds	5 seconds

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

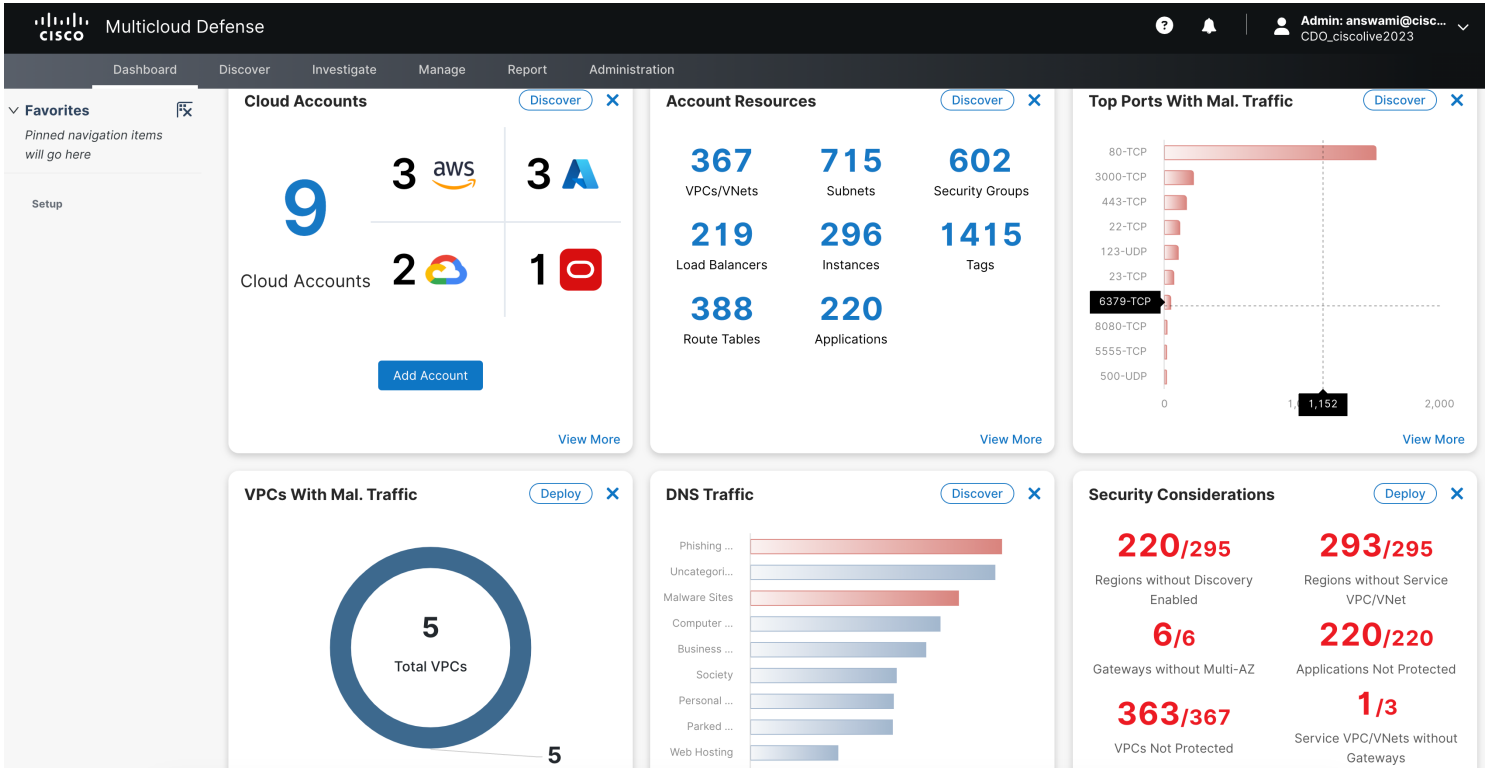
Cisco Multicloud Defense

Cisco Multicloud Defense



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Multicloud Inventory and Visibility



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Multicloud Defense Gateway

Ingress Gateway

- ✓ Reverse Proxy
- ✓ TLS decrypt
- ✓ WAF – L7 DoS
- ✓ IDS / IPS
- ✓ Antivirus
- ✓ Geo IP
- ✓ Malicious IP

Egress Gateway

Egress

- ✓ URL filtering
- ✓ Forward proxy
- ✓ TLS decrypt
- ✓ FQDN filtering*
- ✓ FQDN-based firewall policy
- ✓ DLP
- ✓ IDS / IPS
- ✓ Antivirus

East/West

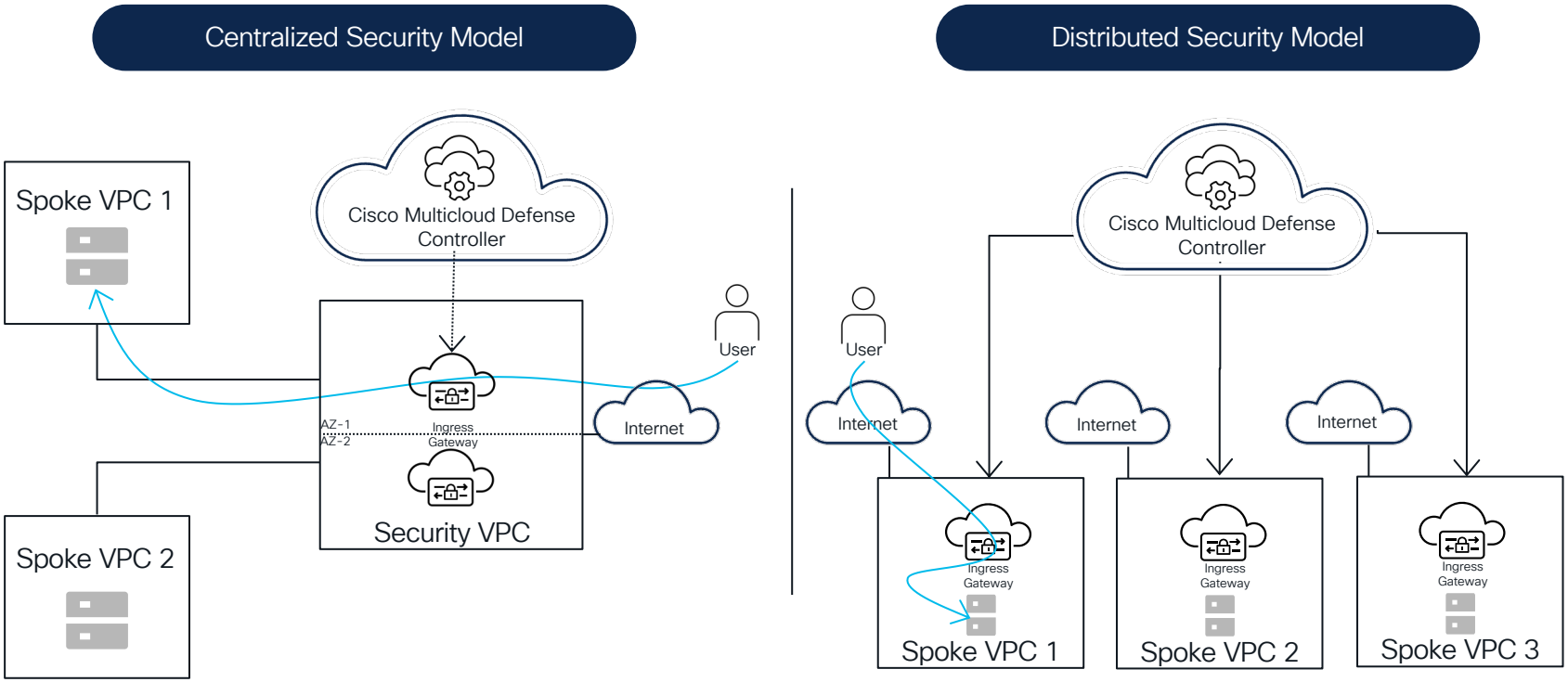
- ✓ FQDN filtering
- ✓ IPS / IDS
- ✓ Antivirus
- ✓ Micro-segmentation
- ✓ FQDN-based firewall policy
- ✓ TLS decrypt

** No TLS decryption is needed*

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Centralized and Distributed Model

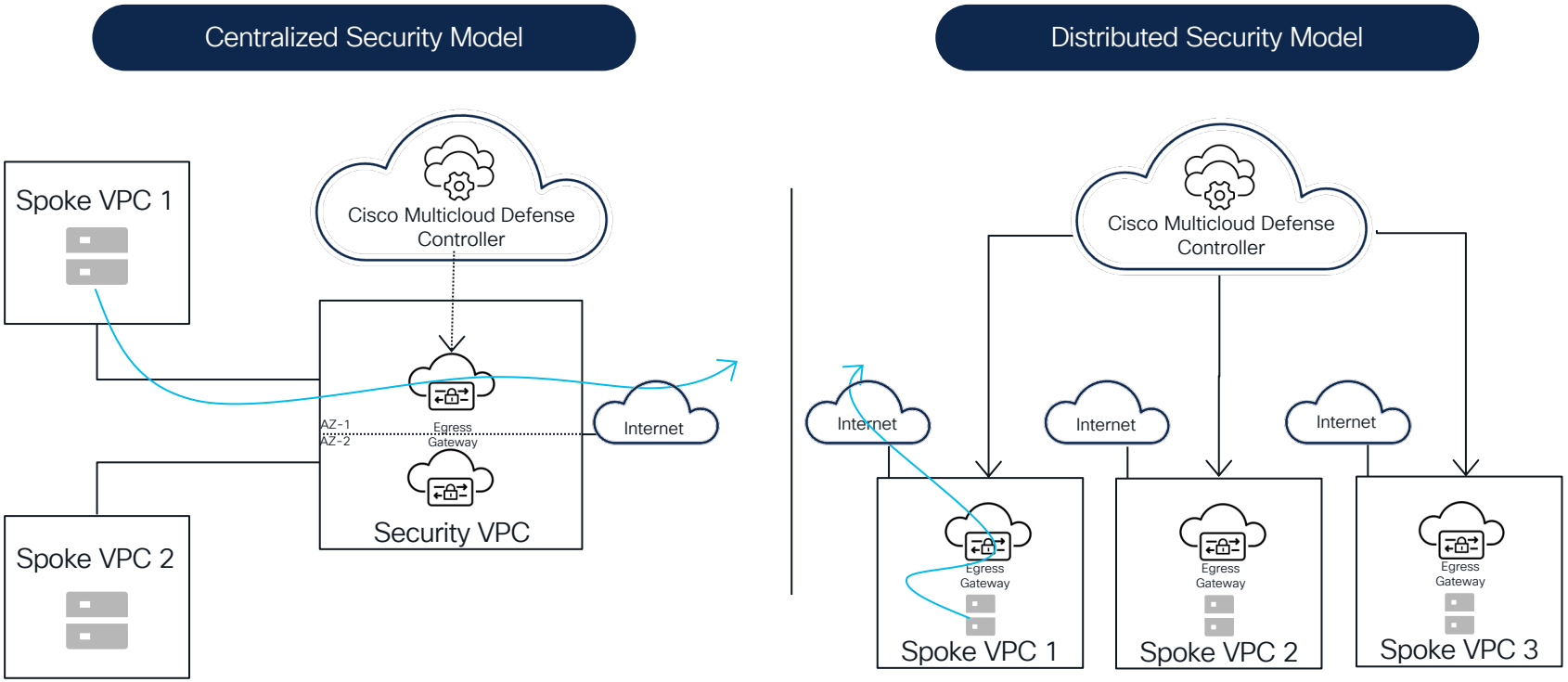
Ingress Traffic



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Centralized and Distributed Model

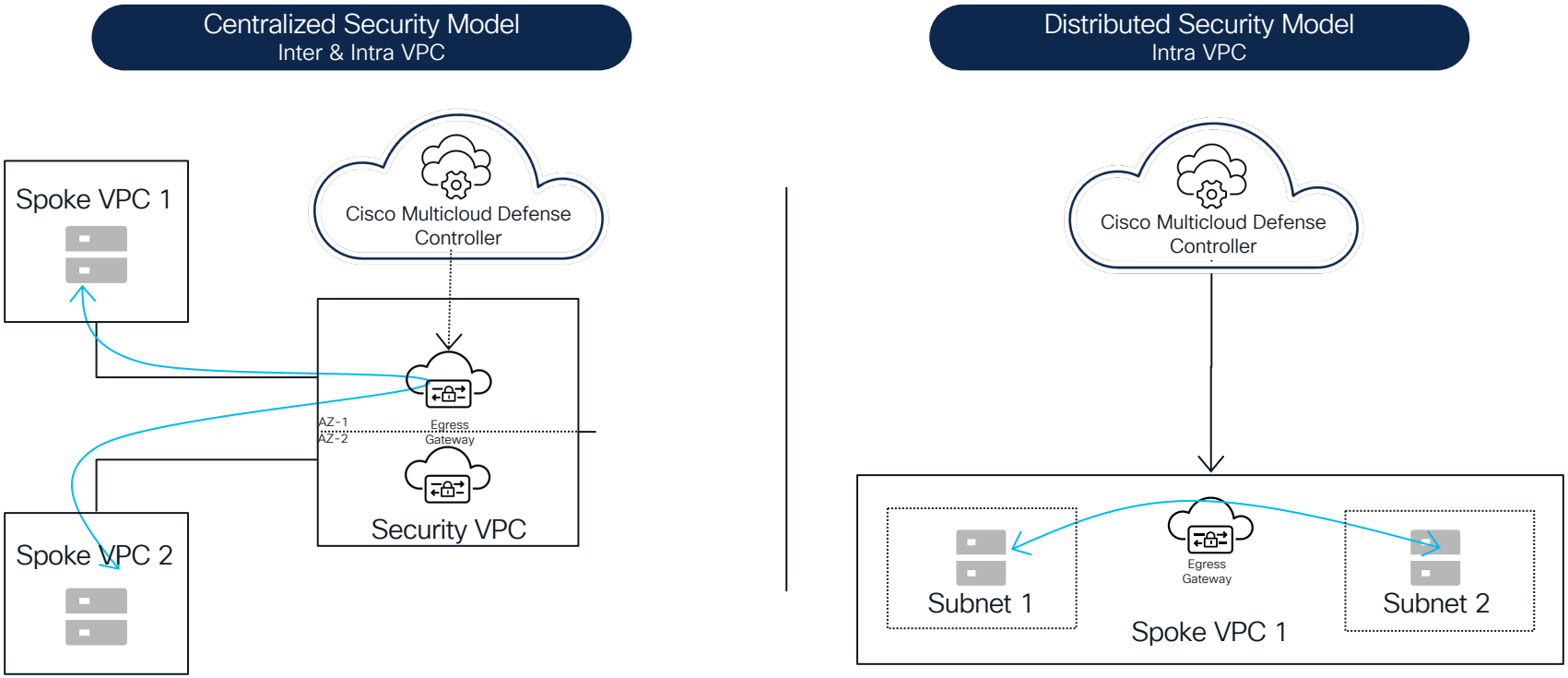
Egress Traffic to Internet



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Centralized and Distributed Model

East-West Traffic through Egress Gateway



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

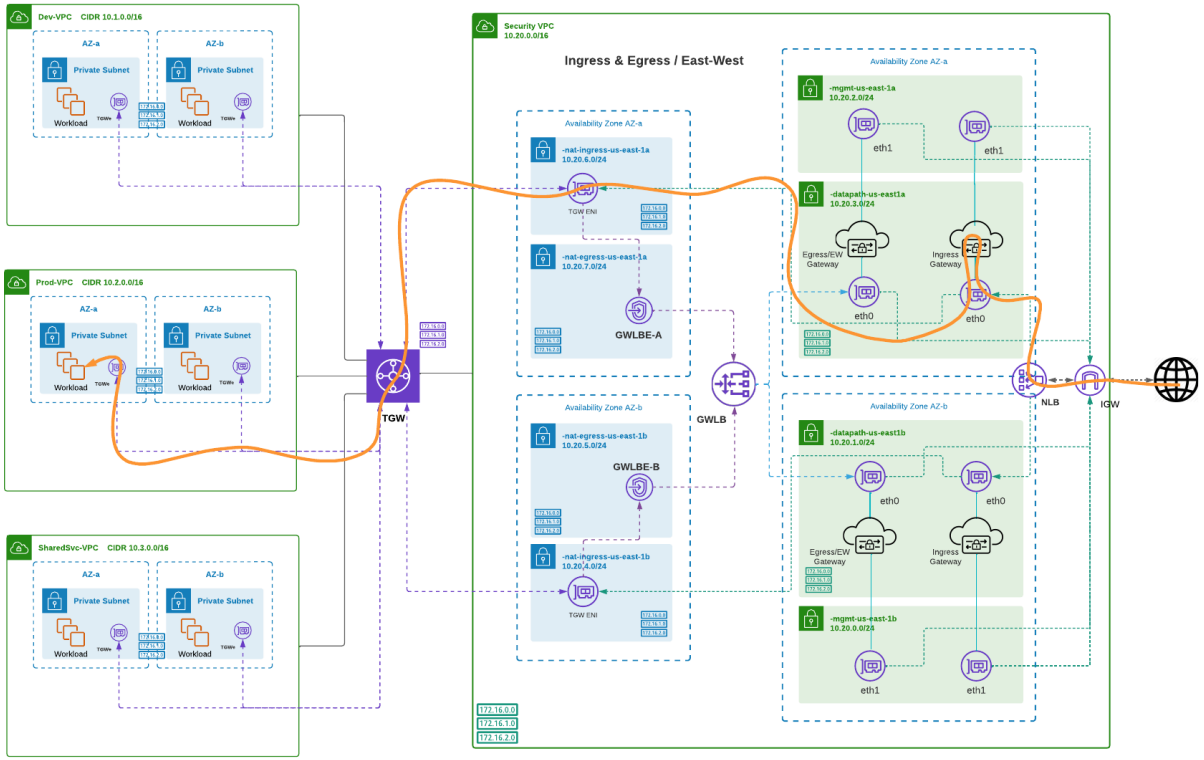
Connectivity for Centralized Model – Automation

- (All clouds) Creation of Service VPC
- AWS
  - Deployment of new transit gateway
  - Integration with existing transit gateway
  - Updates VPC and TGW route tables
- Azure/GCP/OCI
  - Hub and spoke topology with VNet/VPC/VCN peering
  - Updates route tables
- (All clouds) Routing updates

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

AWS Centralized Model

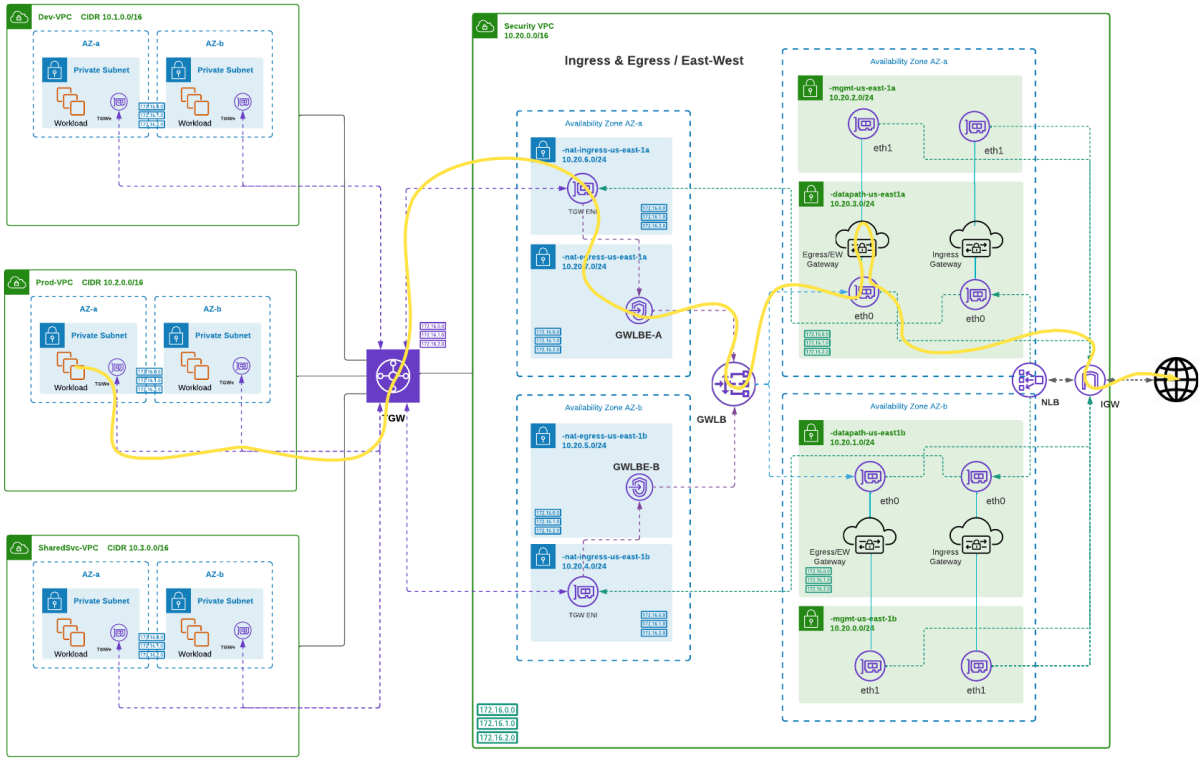
Ingress



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

AWS Centralized Model

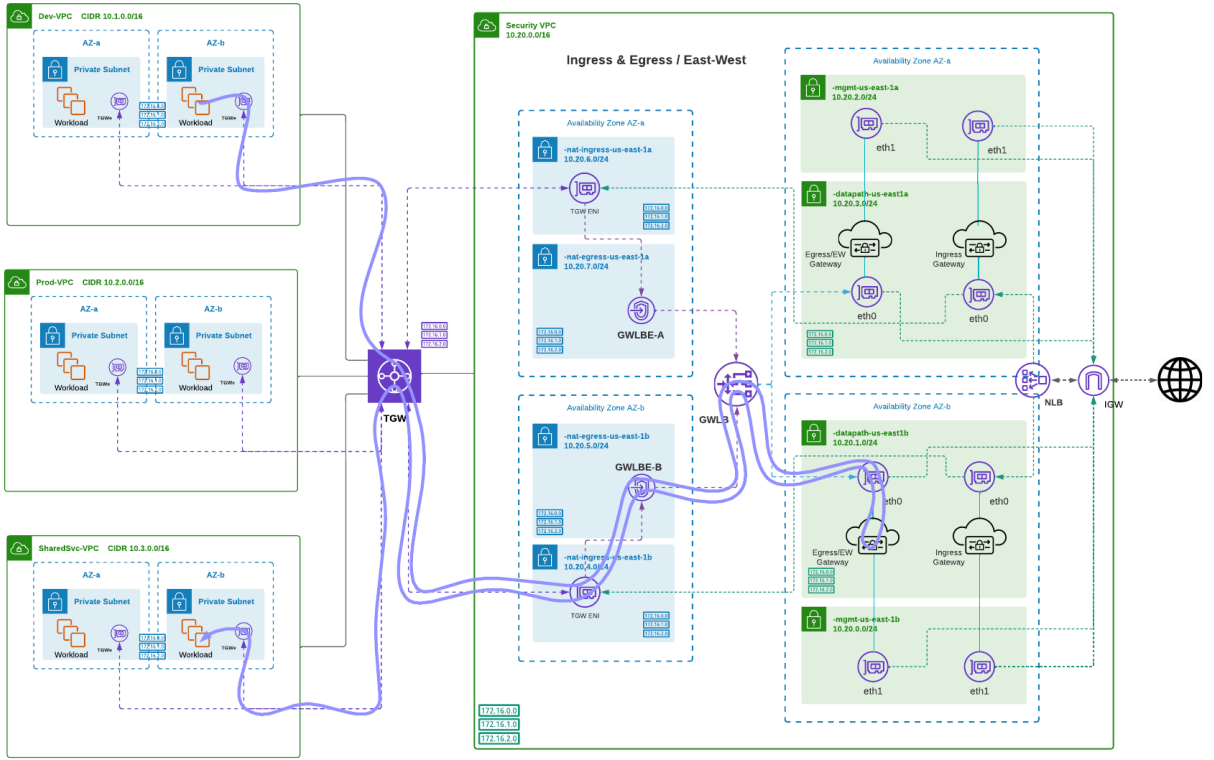
Egress



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

AWS Centralized Model

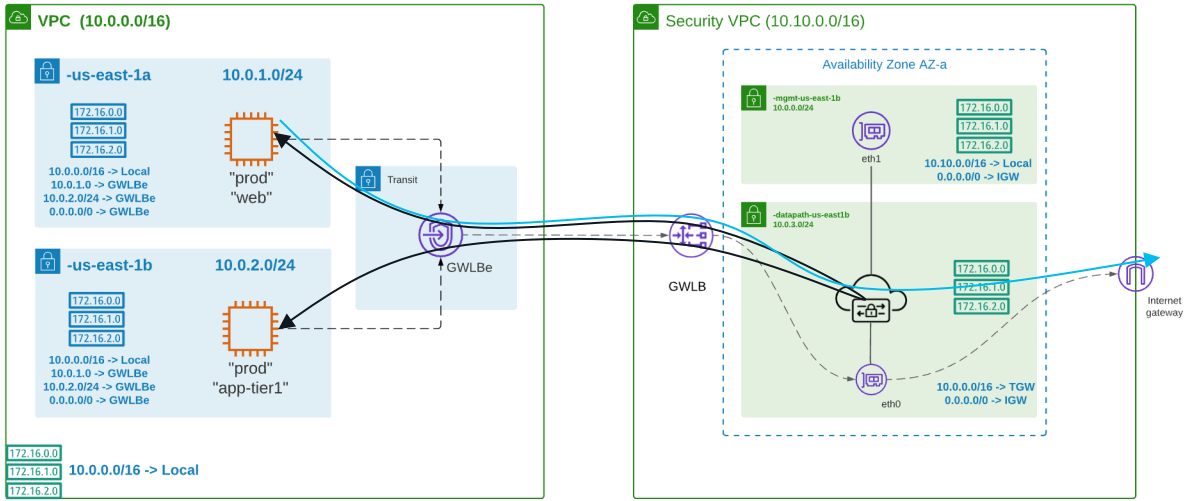
East-West Inter-VPC



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

AWS Centralized Model

East-West Intra-VPC

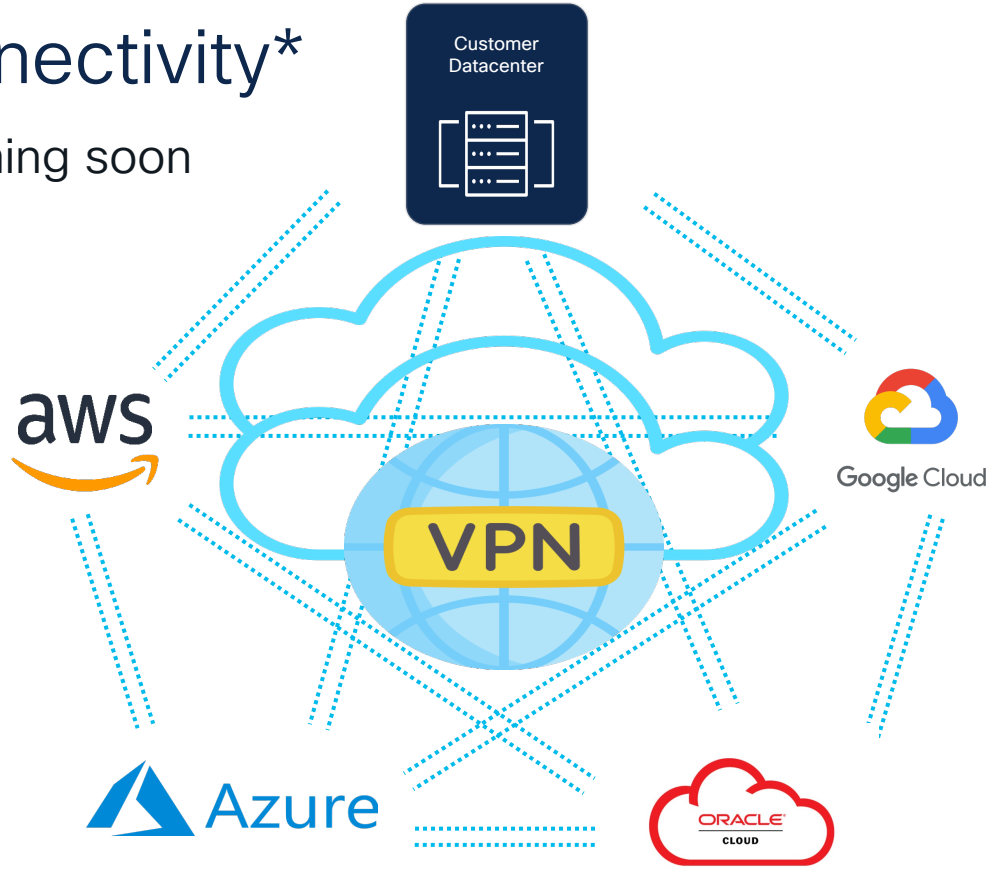


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling Intercloud Connectivity*

- Autoscaling
- Self-Healing
- Automation
- Operation Simplicity
- Distributed
- Built-in Advanced Security

* Coming soon



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

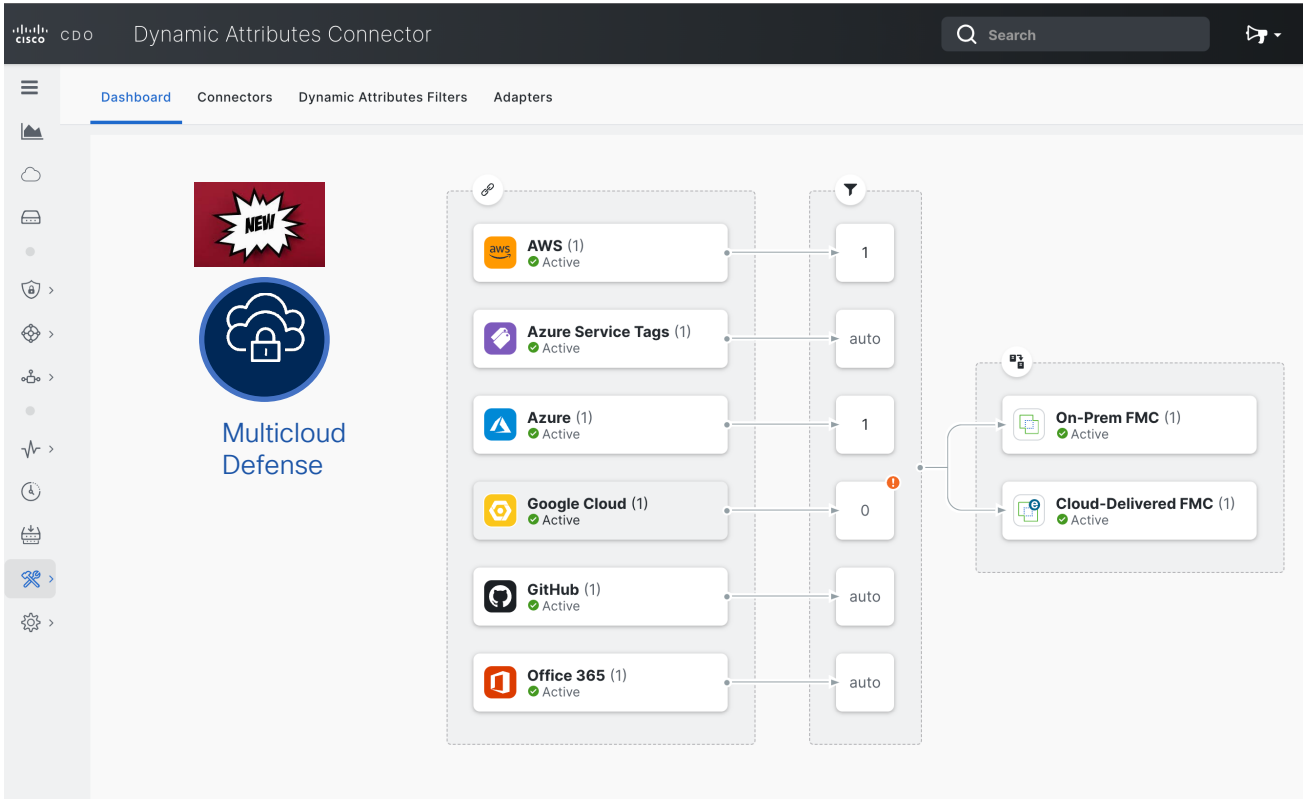
Demonstration: Cisco Multicloud Defense

Coming Soon to Multicloud Defense

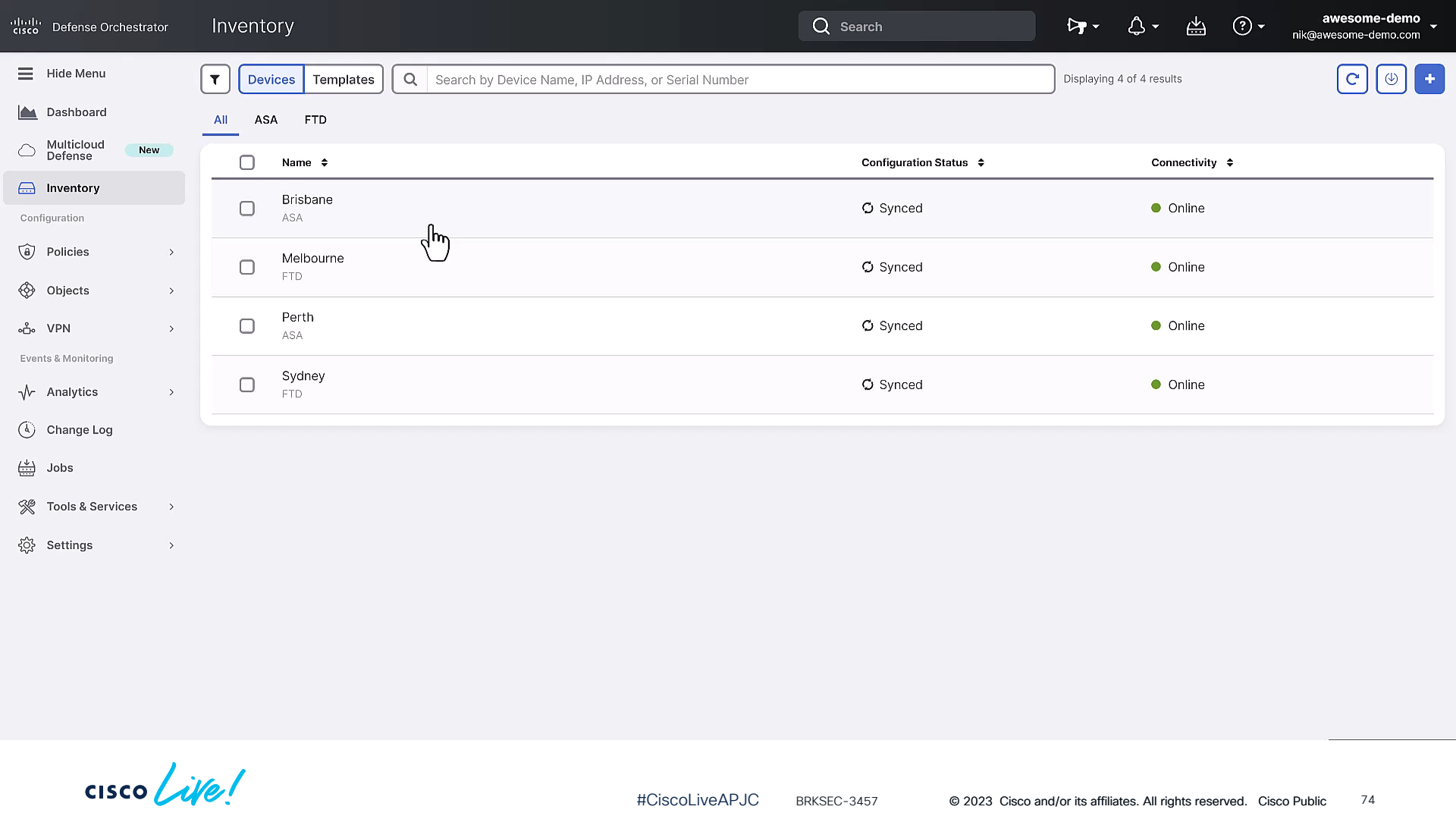
- Integration with Cisco Secure Dynamic Access Connector (CSDAC)
  - Currently CSDAC only sends attributes to FMCs (and then to Cisco Secure Firewall)
- Shared Objects
  - Objects create on Cisco Secure Firewalls can be used by Multicloud Defense
- IPsec VPN
  - Multicloud Defense includes creation of site-to-site VPNs
  - Cloud to cloud
  - On-premise to cloud

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

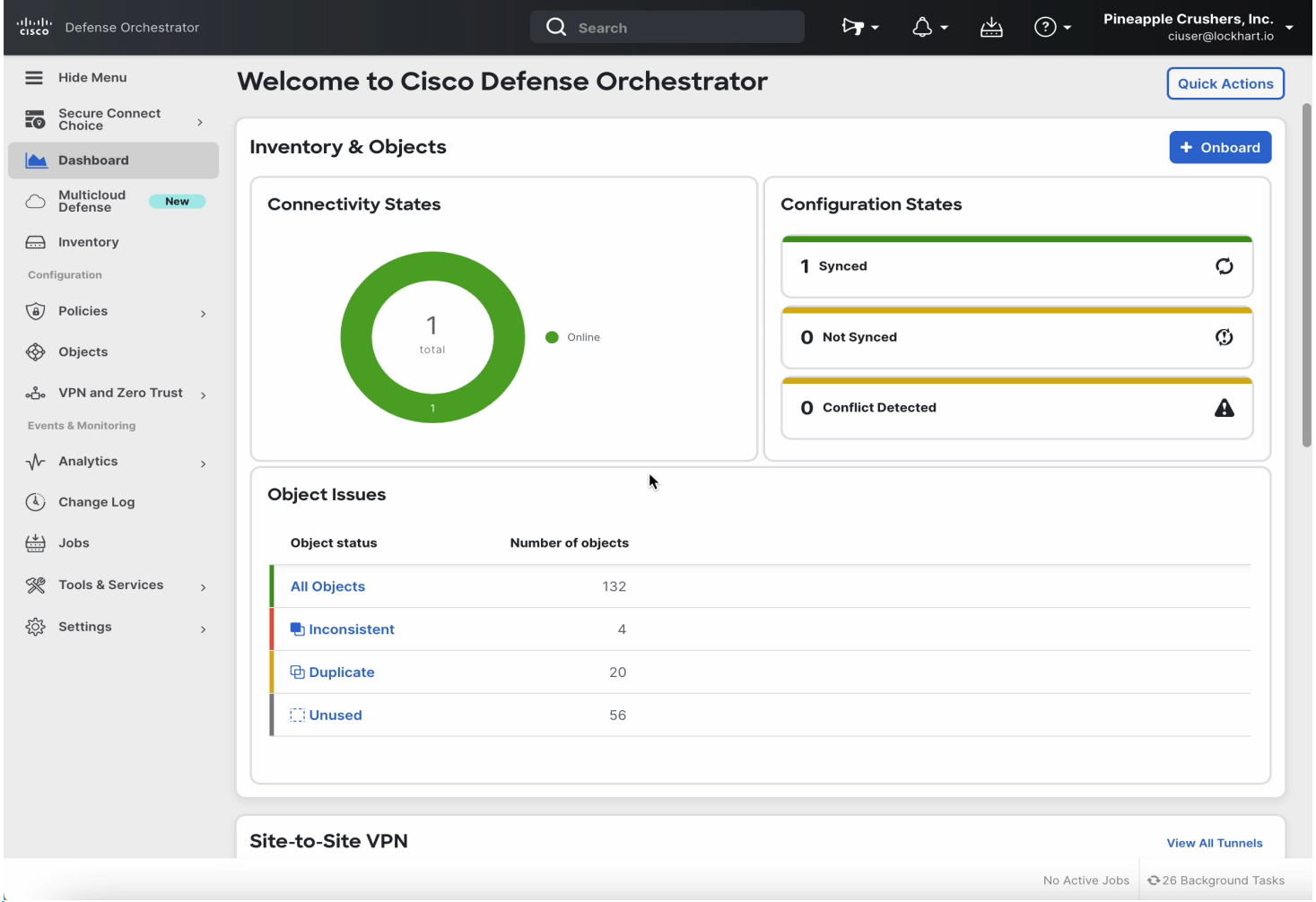
Integration with CSDAC



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public



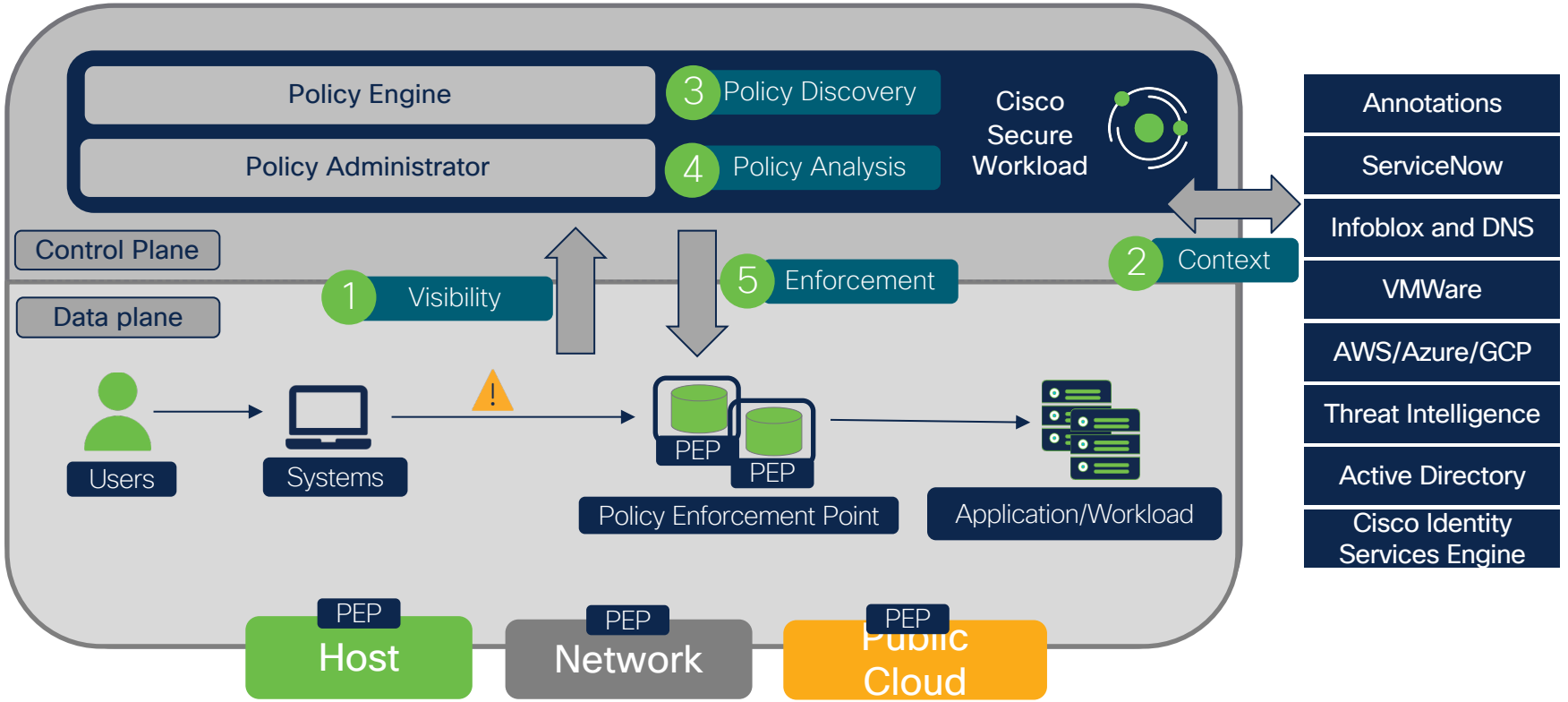
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

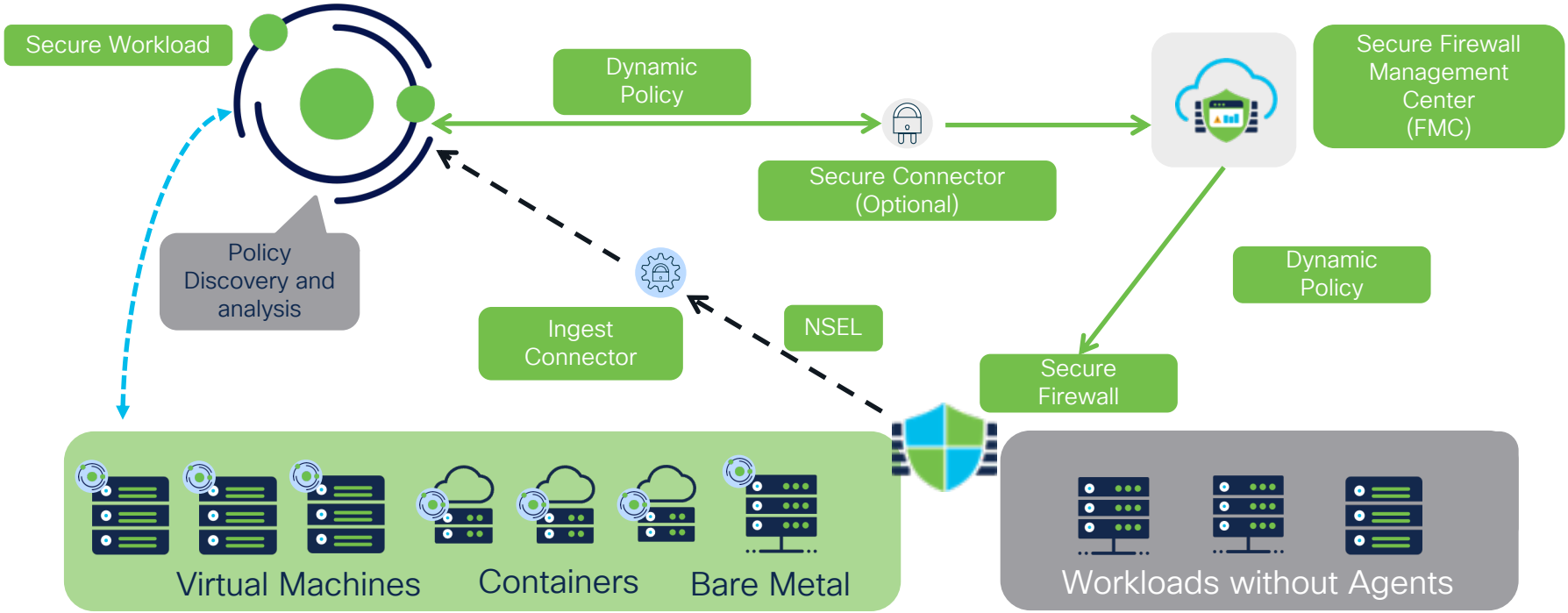
Cisco Secure Workload

Cisco Secure Workload Architecture



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agentless Segmentation Using Secure Firewall



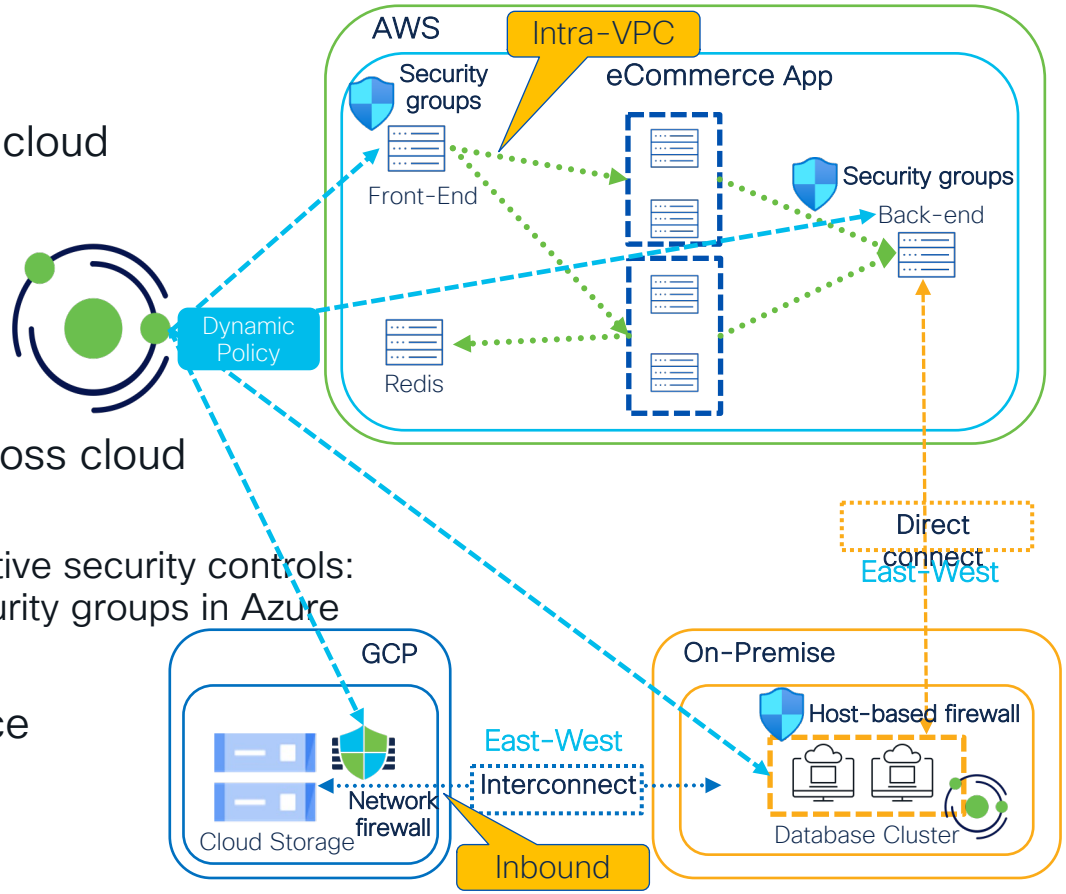
Segmentation policies enforcement at workloads

Segmentation policies enforcement at firewall

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

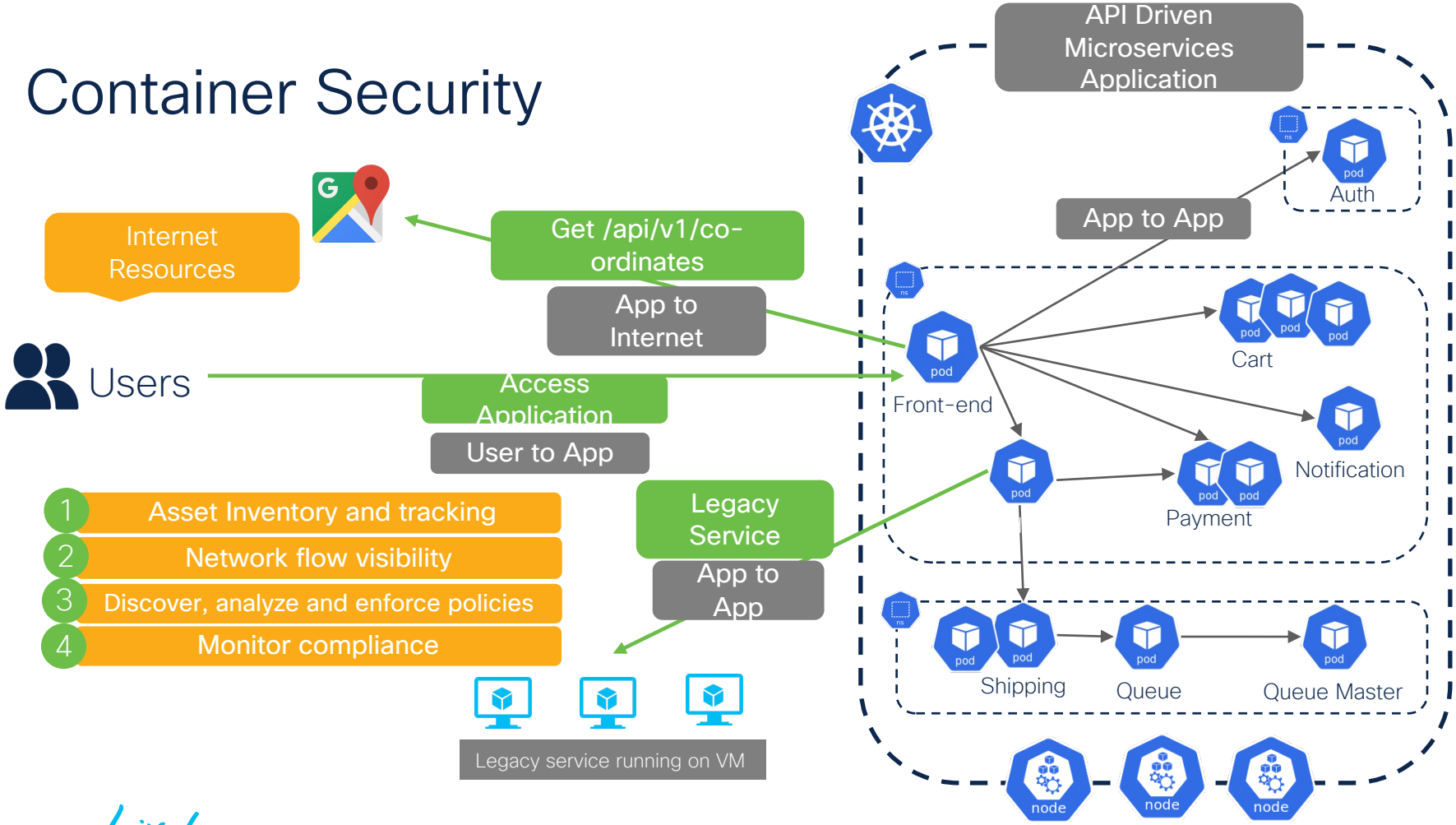
Multicloud Visibility and Segmentation

- Agentless flow visibility from multi-cloud environment
  - Support for AWS, Azure and GCP
- Contextual awareness using cloud tags and metadata
- Consistent policy orchestration across cloud providers
  - Agentless enforcement with cloud native security controls: security groups in AWS, network security groups in Azure and GCP native network firewall.
- Real-time update of policies at pace with cloud infrastructure updates.



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Container Security



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Conclusion

cisco Live!

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.

Meet the Expert Opening Hours:

Tuesday	**3:00pm – 7:00pm**
Wednesday	**11:15am – 7:00pm**
Thursday	**9:30am – 4:00pm**
Friday	**10:30am – 1:30pm**

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

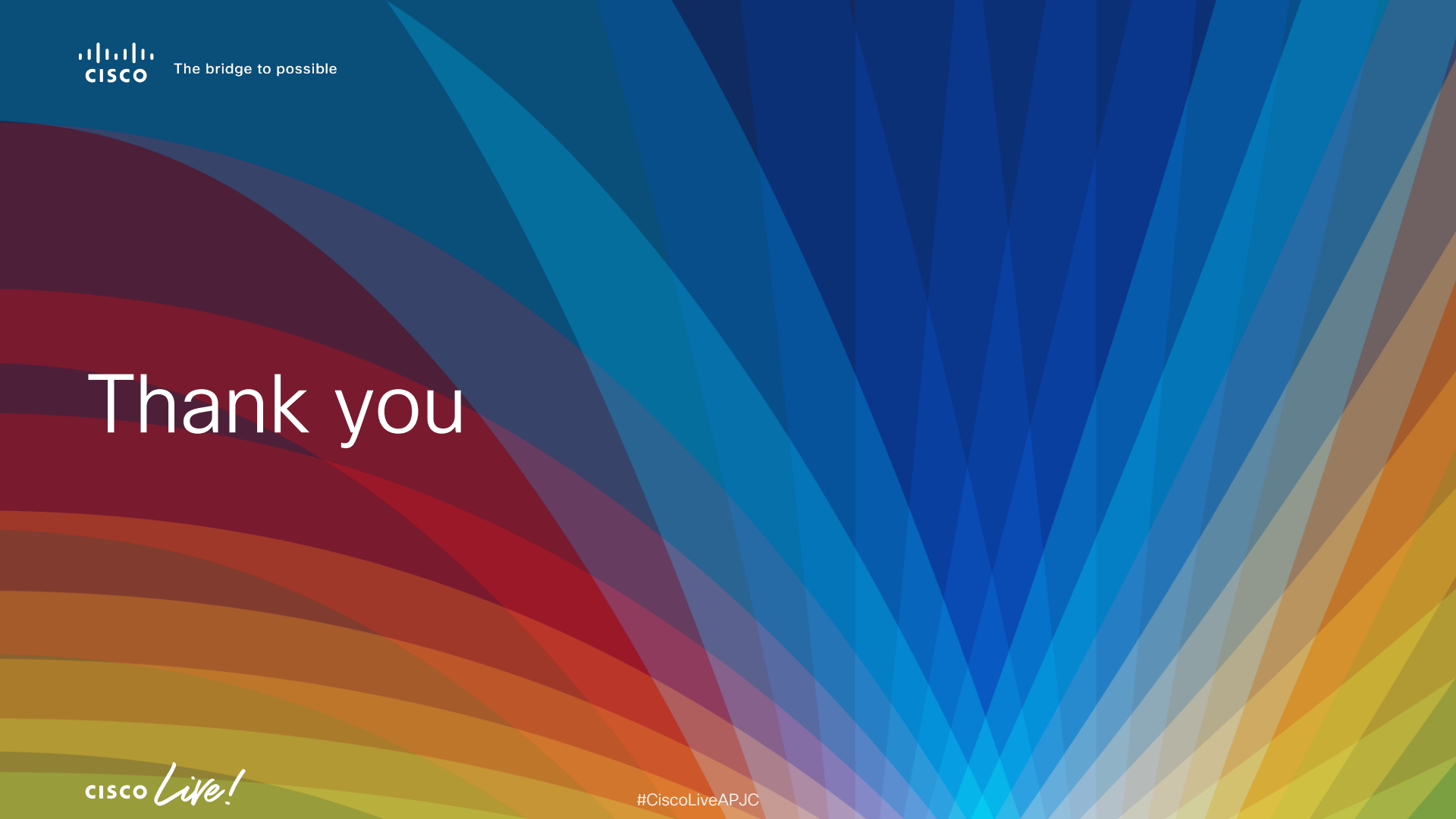
- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Participating in user research gives you a place to share your thoughts and experiences to influence the future of Cisco Secure products.

You'll hear from us at most once every 90 days.

You'll hear from us at most once every 90 days.
Participate is completely optional. You can opt out at any time.


cisco
The bridge to possible
Thank you
cisco Live!
#CiscoLiveAPJC

cisco Live!

Let's go

#CiscoLiveAPJC