

Securing Multicloud Environments - Multicloud Defense gateways and Cisco Secure Firewall

cisco Live !

Akshay Dubey
Customer Delivery Engineering Technical Leader

Cisco Webex App

Questions?

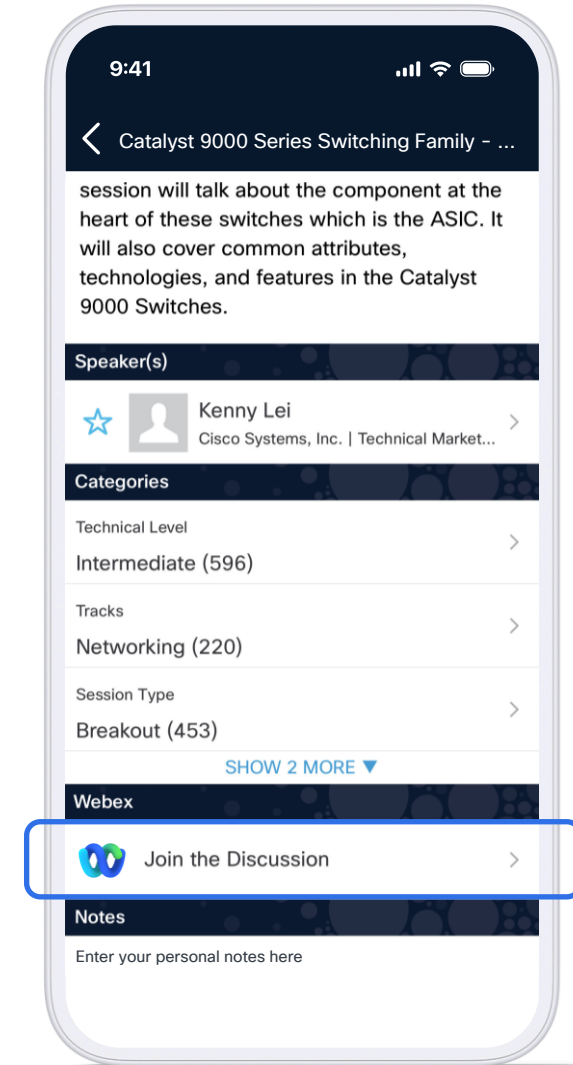
Use Cisco Webex App to chat with the speaker after the session

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.

Contact me: aksdubey@cisco.com



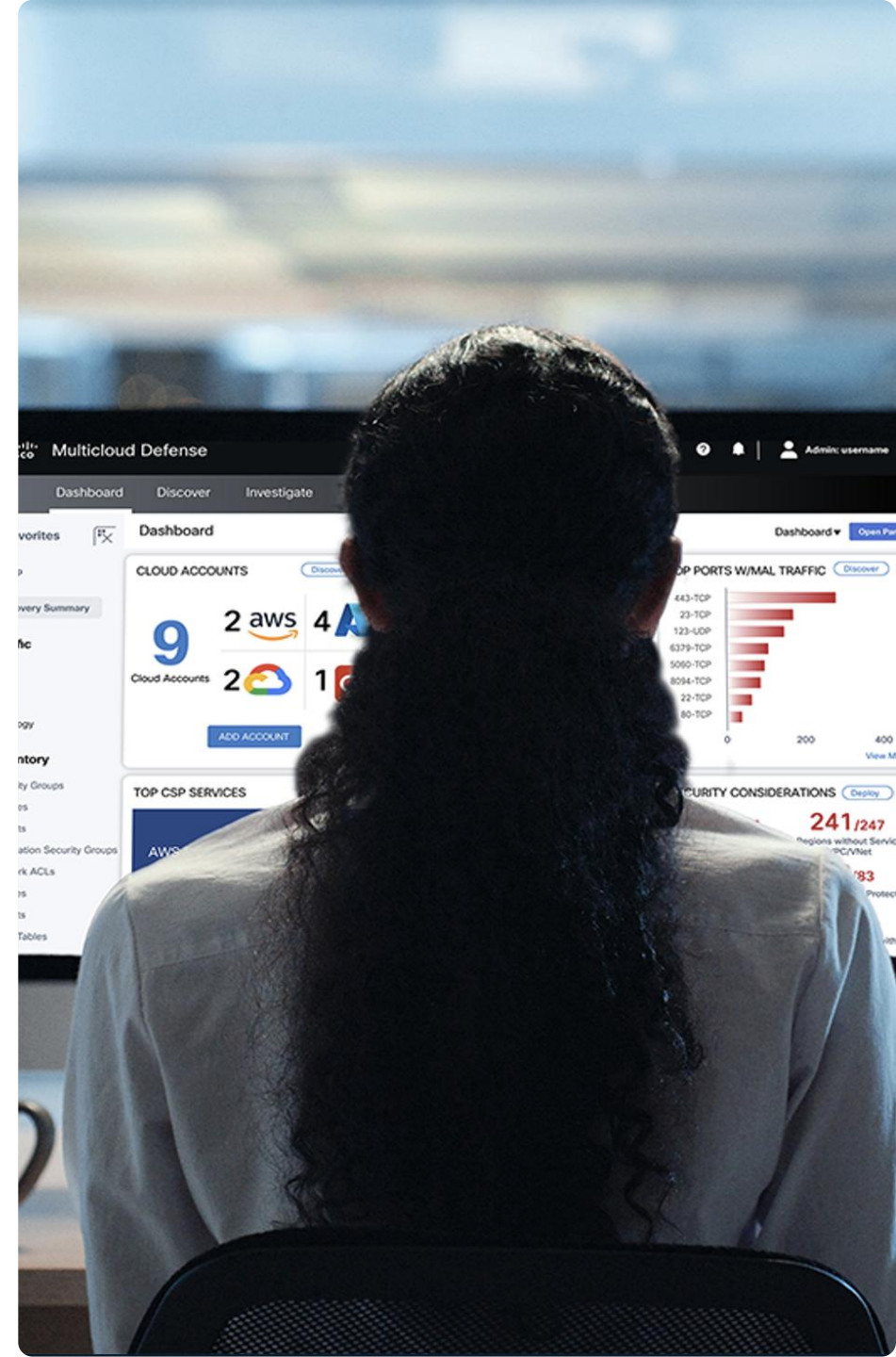
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2423>

Agenda

- 01 Multicloud Security
- 02 Cisco Cloud Security
- 03 Multicloud Defense Overview
- 04 Deployment Modes
- 05 FTDv Deployment Modes
- 06 FTDv Orchestration
- 07 IaaS using Terraform
- 08 Resources

What is Multicloud Network Security?

- Unified Networking and Security
- Cloud Agnostic
- Advanced Threat Protection
- Multi-Environment Support
- Flexible for application architectures



Cloud Challenges

Cloud is different than on-prem network



Dynamic Environment

Frequent changes in the environment leads to:

- Unprotected Resources
- Stale Policies



Cloud speak different languages

Each cloud provider has its own nuances or proprietary components which leads to:

- Multiple tools for multicloud
- Expertise needed for each cloud



Setup and Maintenance

Long setup time and on-going maintenance for management & firewall leads to:

- Slower go-to-market time
- Higher operational expense

Securing Multicloud is **Complex and Fragmented**



Lift and Shift On Prem

*Slows Down
Delivery for the
Business*



Cloud Service Provider Security

*Inadequate,
Fragmented*



Multi-Cloud Networking Vendors

*Security Is an
Afterthought*

The Secure Multicloud Networking Platform

Hybrid Cloud Policy

Advanced security to flexibly protect enterprise cloud workloads

Asset Visibility

Tag-based policy

Infrastructure as Code

Compliance

Cloud Network Security as-a-service

Advanced security to flexibly protect enterprise cloud workloads

Segmentation

Web protection

Intrusion prevention

Egress filtering

Multicloud and Hybrid Networking

Workflow and orchestration delivered at cloud speed

Routing

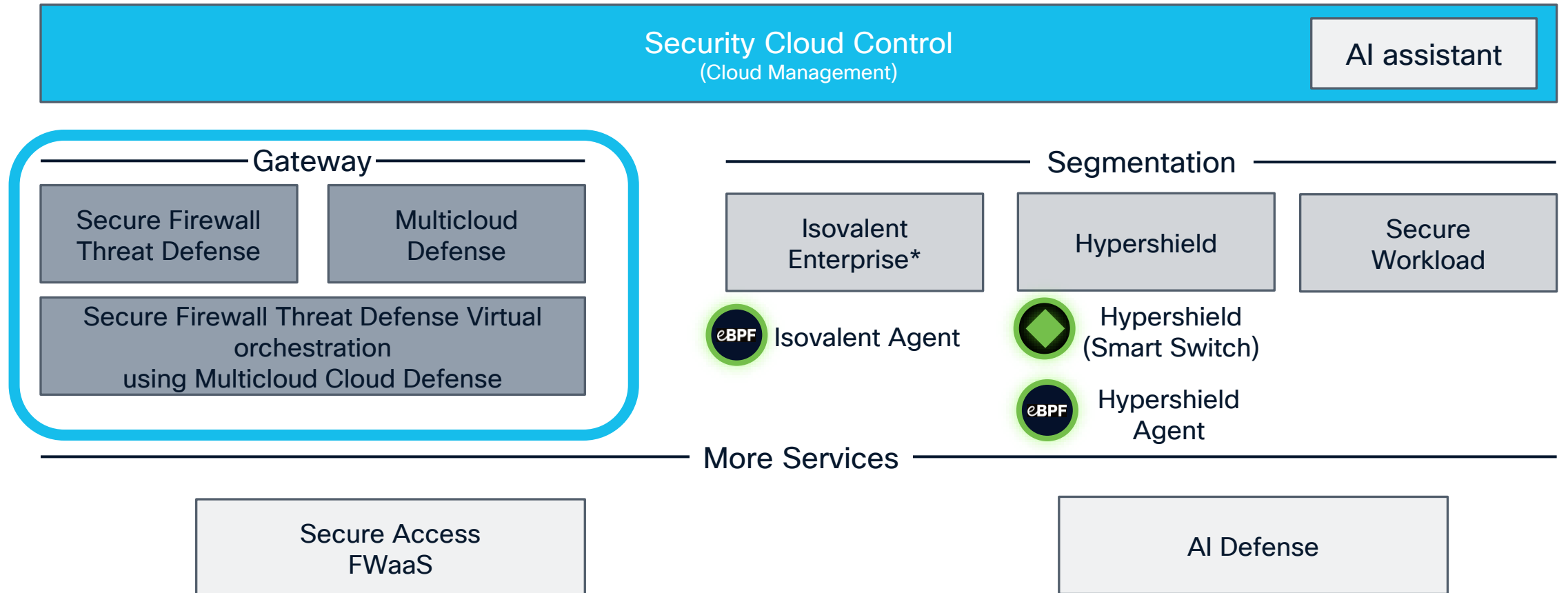
Cloud-to-Cloud

Site-to-Cloud

Ops visibility



Cisco Cloud Security

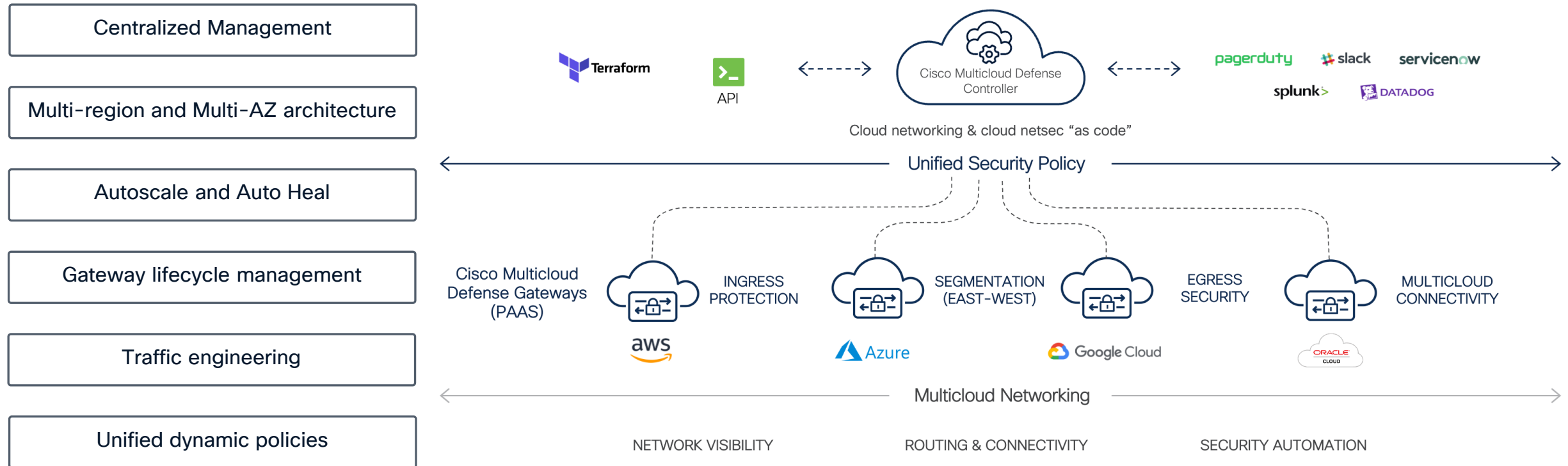


* Currently not included in the Security Cloud Control

Multicloud Defense Overview

Multicloud Defense

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



Multicloud Defense Gateway

Single Pass Architecture

Instance Size
2, 4, and 8 vCPU

Availability
AWS, Azure, GCP and OCI

Modes
Proxy and Forwarding

Use Case

Ingress Inspection

Egress Inspection

East/West Inspection

Multicloud Networking



Ingress
Gateway

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



Egress
Gateway

- ✓ URL filtering
- ✓ Forward proxy
- ✓ TLS decrypt
- ✓ FQDN filtering*
- ✓ FQDN-based firewall policy
- ✓ DLP
- ✓ IDS / IPS
- ✓ Antivirus
- ✓ Fully orchestrated IPsec VPN
(site-to-cloud & cloud-to-cloud)

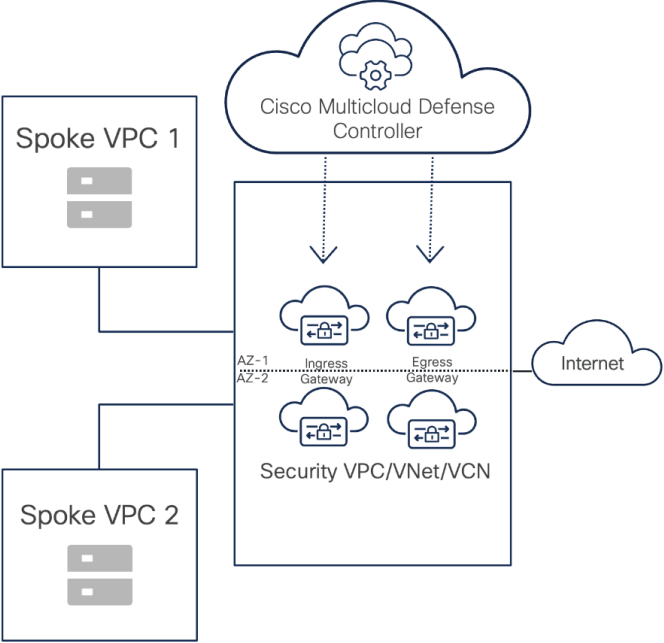
* No TLS decryption is needed

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

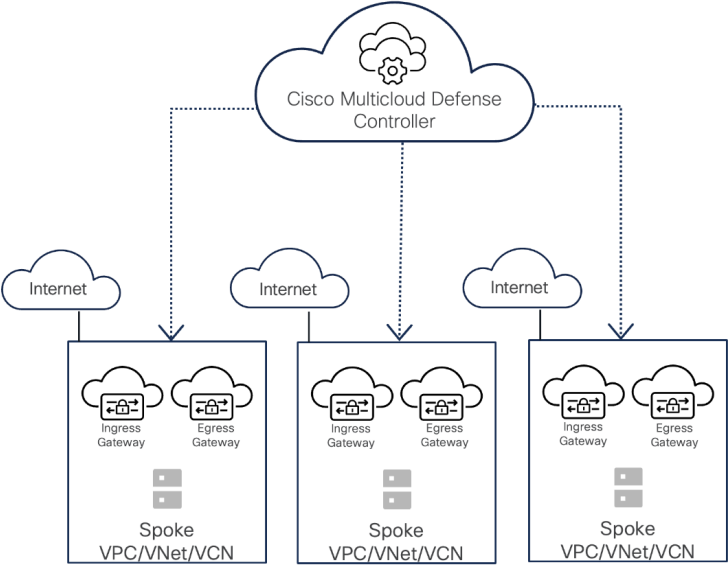
Deployment Modes

Security Models

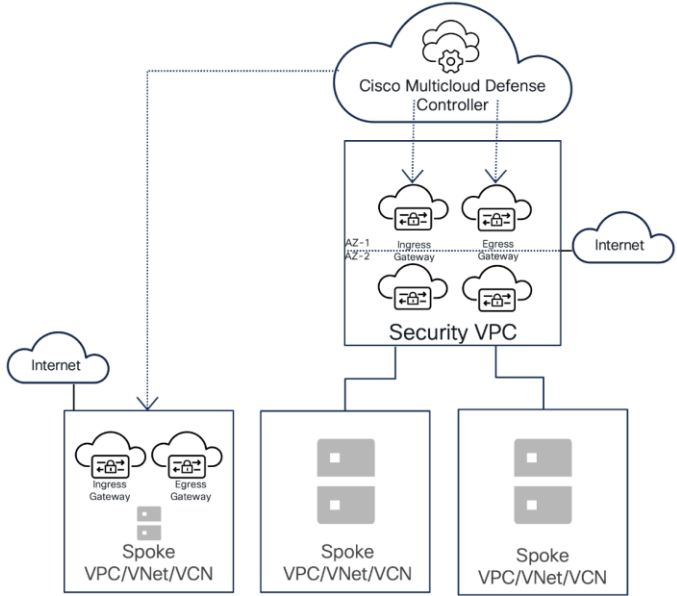
Centralized Security Model



Distributed Security Model



Combined Security Model



Secure multicloud infrastructure in mins with Cisco Multicloud Defense

Step 1

Connect Account



Connect a cloud account with the Multicloud Defense Controller

Connect Account

Securely onboard Cloud accounts

Step 2

Enable Traffic Visibility



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

Enable Visibility

Enable DNS query & VPC/NSG flow logs

Step 3

Secure Your Account



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

Secure Account

Orchestration and Automation

Deployment Model

Secure Your Account

You can secure your account via a centralized hub and spoke model or by using a distributed model.

Centralized



A Service VPC/VNet is deployed to host all security infrastructure with all application VPCs attached to Service VPC/VNet (Hub and Spoke). Multicloud Defense will completely orchestrate the deployment of Service VPC/VNet and the necessary components.

Distributed



Deploy Multicloud Defense Gateway in each application VPC. This requires the user to orchestrate routing and subnet deployment to host Multicloud Defense Gateway.



For more information about our architecture, please go to:
<https://docs.defenseorchestrator.com/multicloud/index.html> 

« GO BACK

CANCEL

NEXT

Centralized Security Model

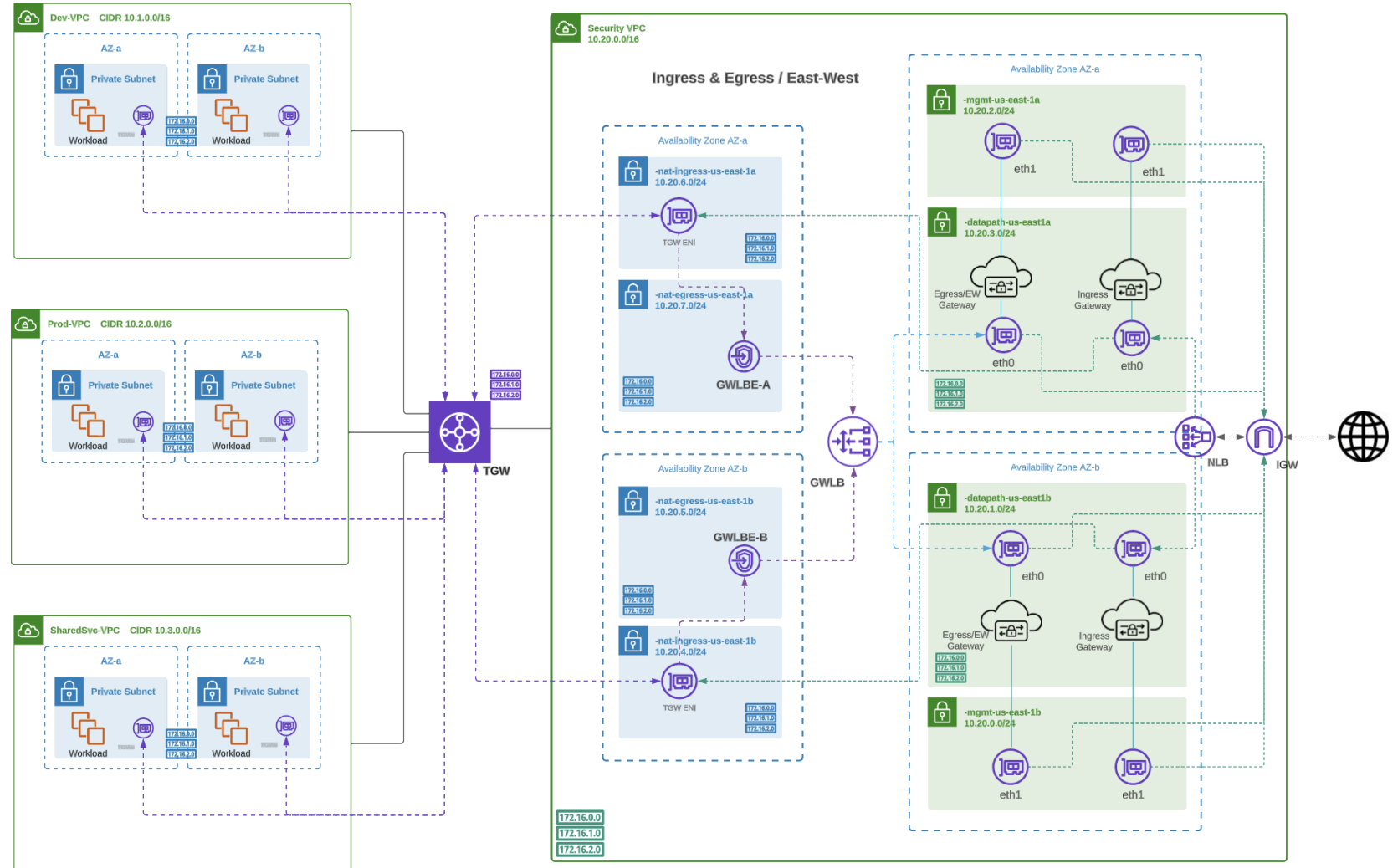
Amazon Web Services

Orchestration

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

Lifecycle management

Ingress and Egress Gateway



Centralized Security Model

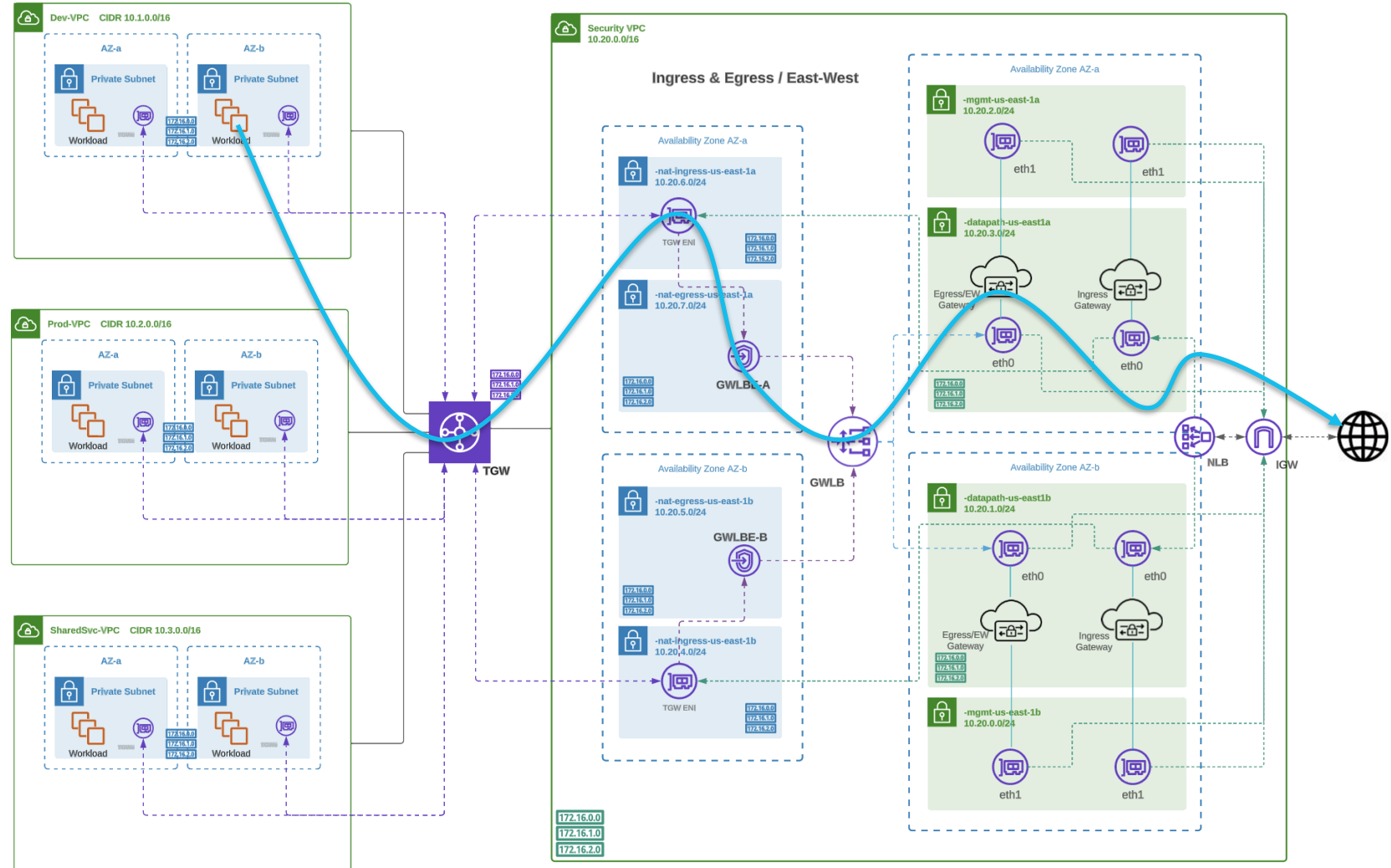
Amazon Web Services

Orchestration

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

Lifecycle management

Ingress and Egress Gateway



Centralized Security Model

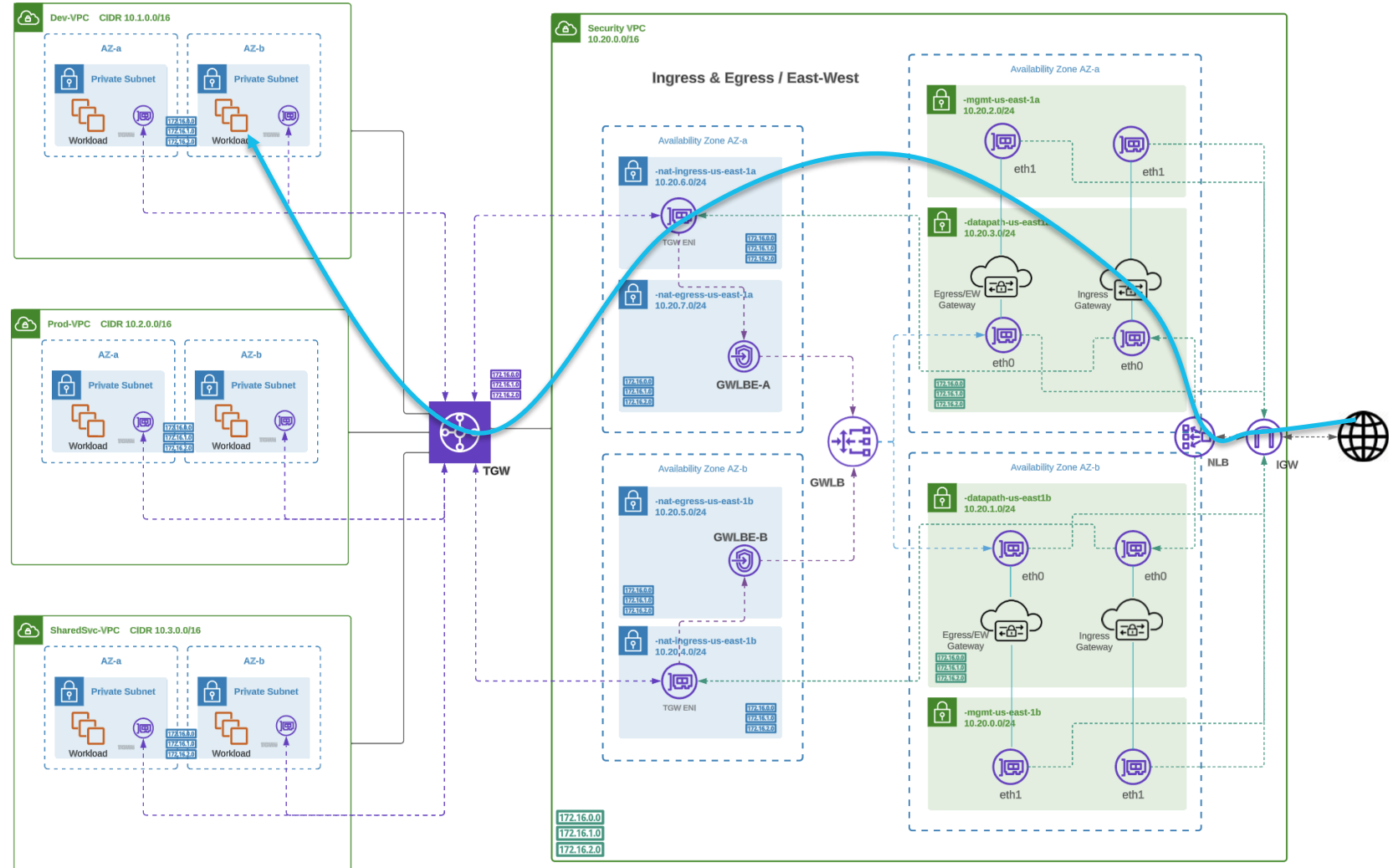
Amazon Web Services

Orchestration

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

Lifecycle management

Ingress and Egress Gateway



Centralized Security Model

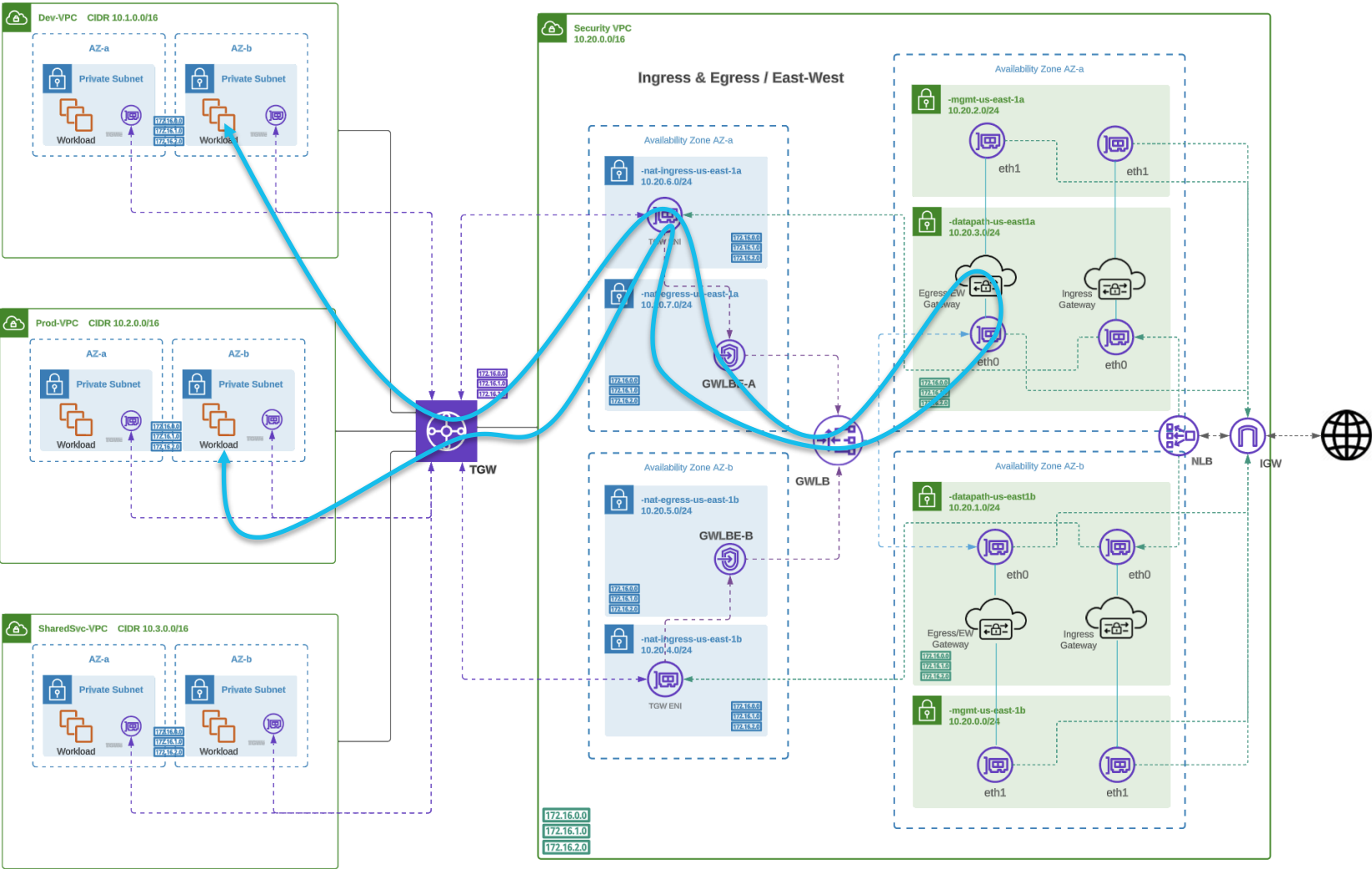
Amazon Web Services

Orchestration

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

Lifecycle management

- Ingress and Egress Gateway



Centralized Security Model

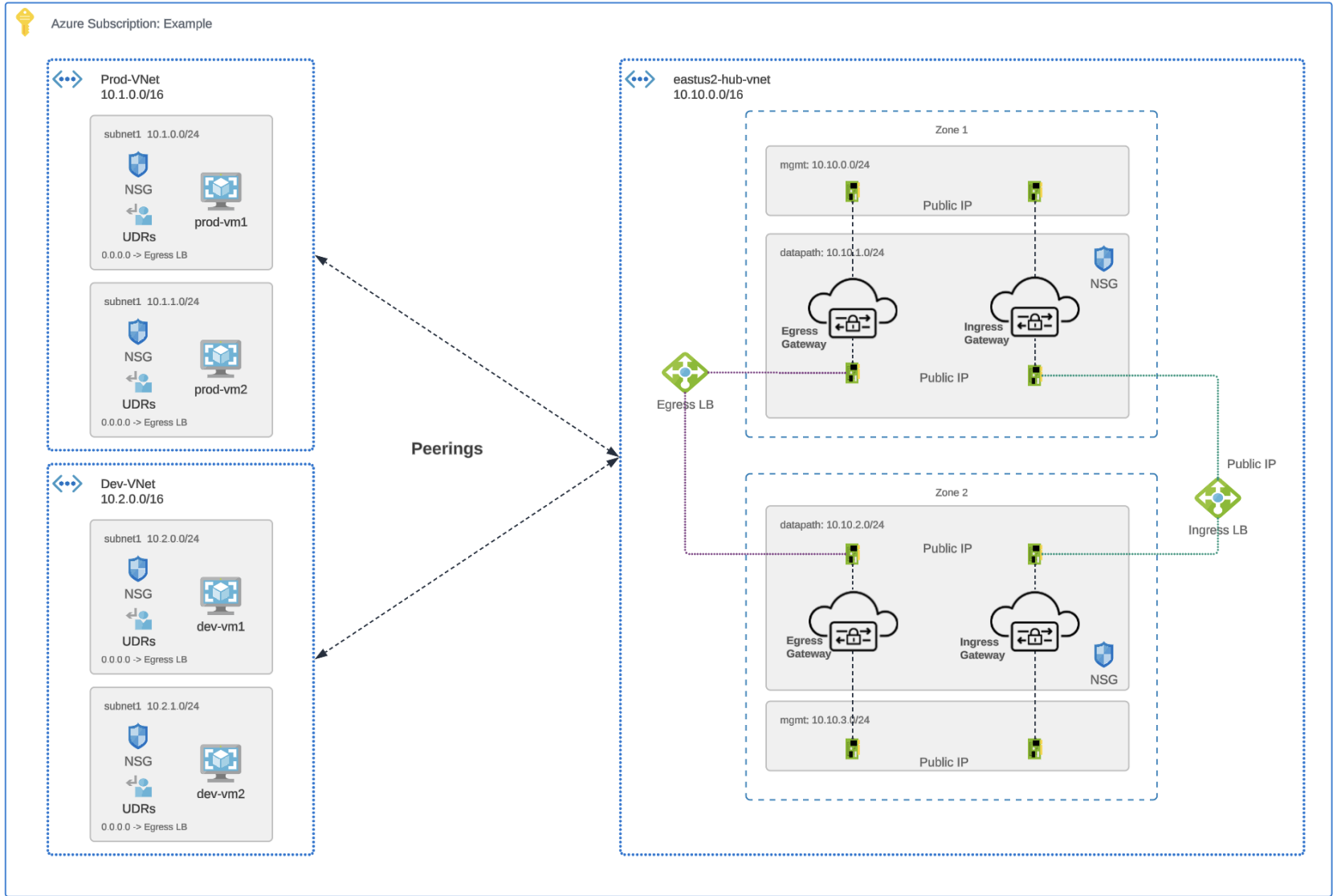
Azure

Orchestration

Security vNET
Network Load Balancer
Public Load Balancer
vNET peering
Autoscale and auto heal
Traffic Engineering – Route Table

Lifecycle management

Ingress and Egress Gateway



Centralized Security Model

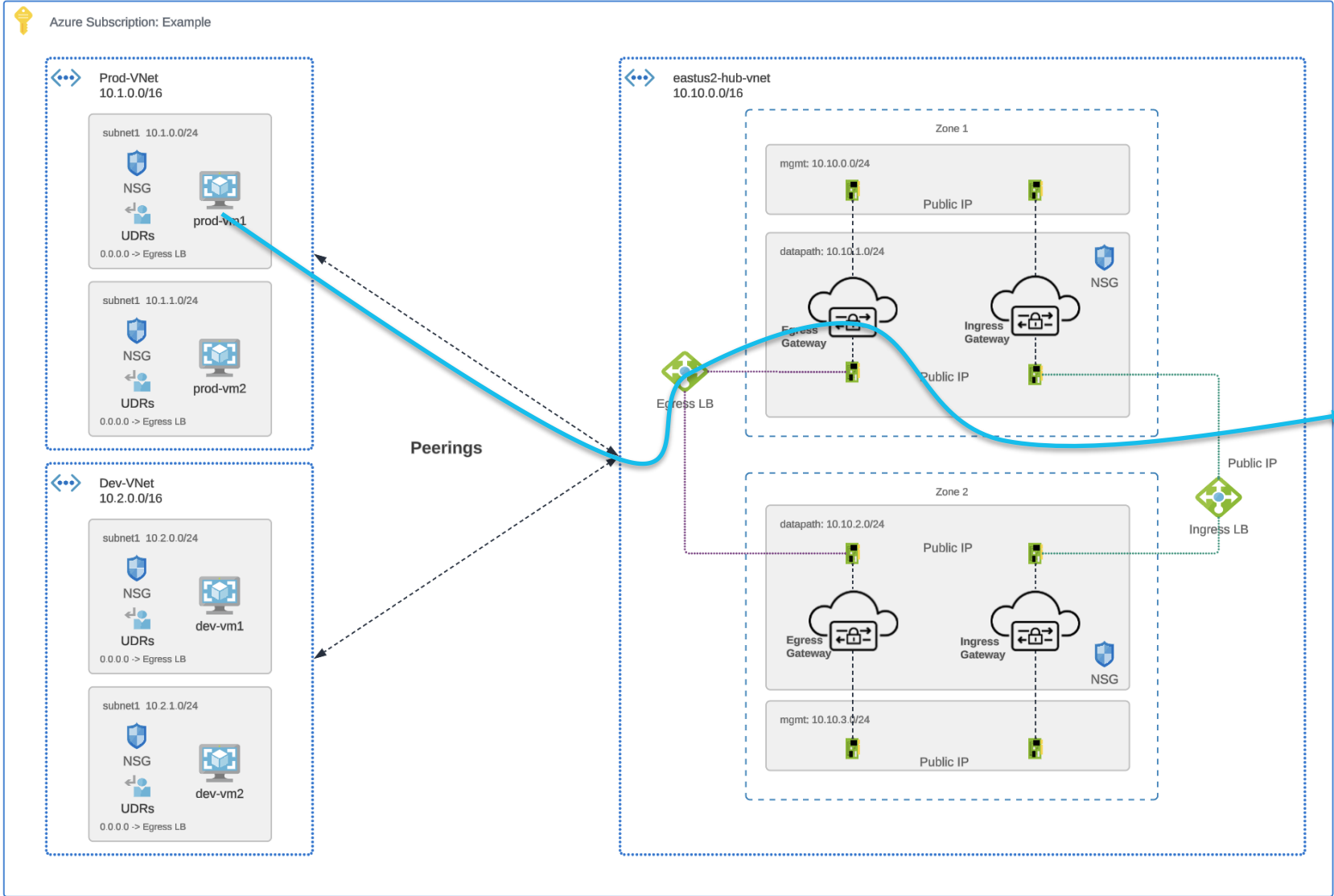
Azure

Orchestration

Security vNET
Network Load Balancer
Public Load Balancer
vNET peering
Autoscale and auto heal
Traffic Engineering – Route Table

Lifecycle management

Ingress and Egress Gateway



Centralized Security Model

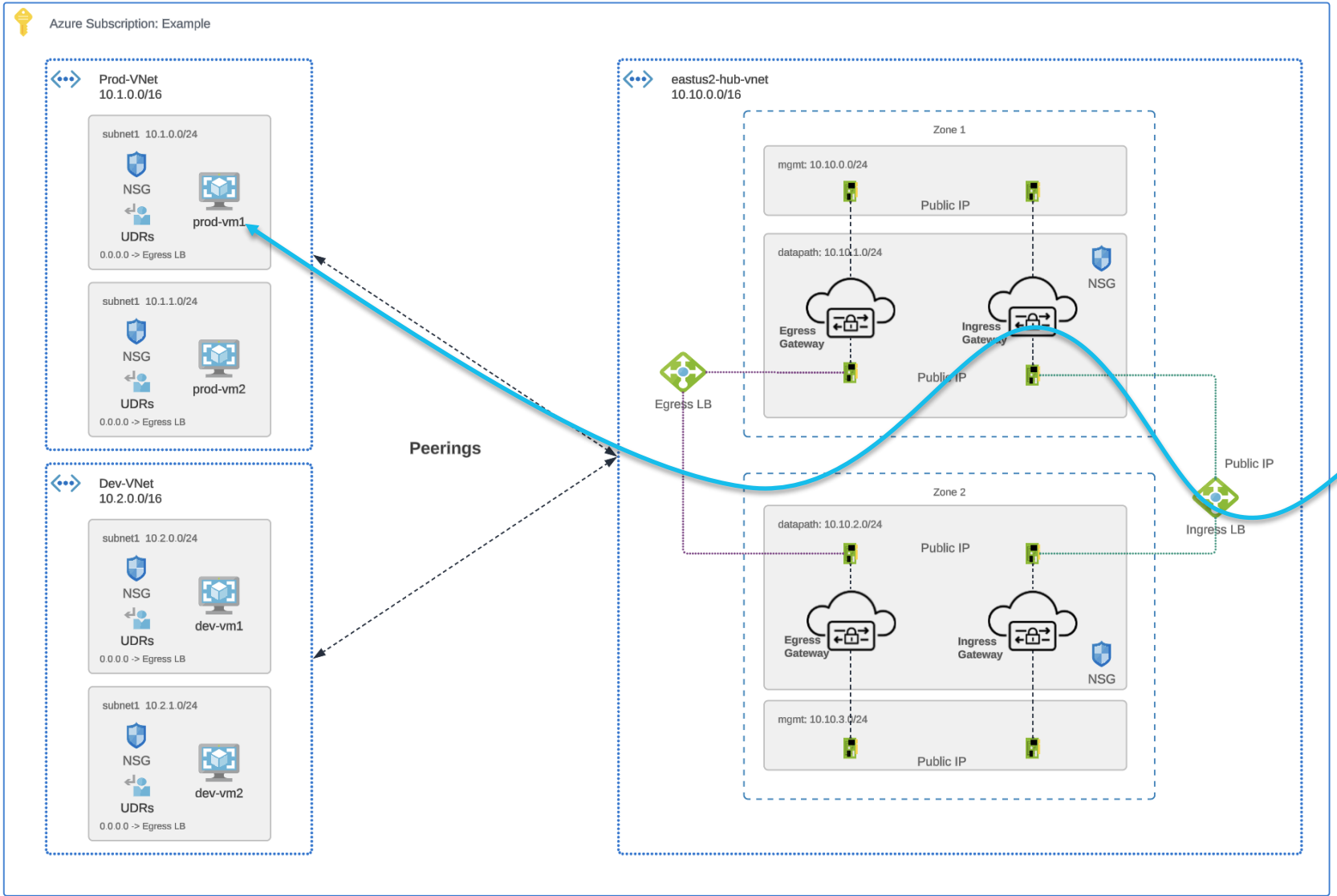
Azure

Orchestration

- Security vNET
- Network Load Balancer
- Public Load Balancer
- vNET peering
- Autoscale and auto heal
- Traffic Engineering – Route Table

Lifecycle management

- Ingress and Egress Gateway



Centralized Security Model

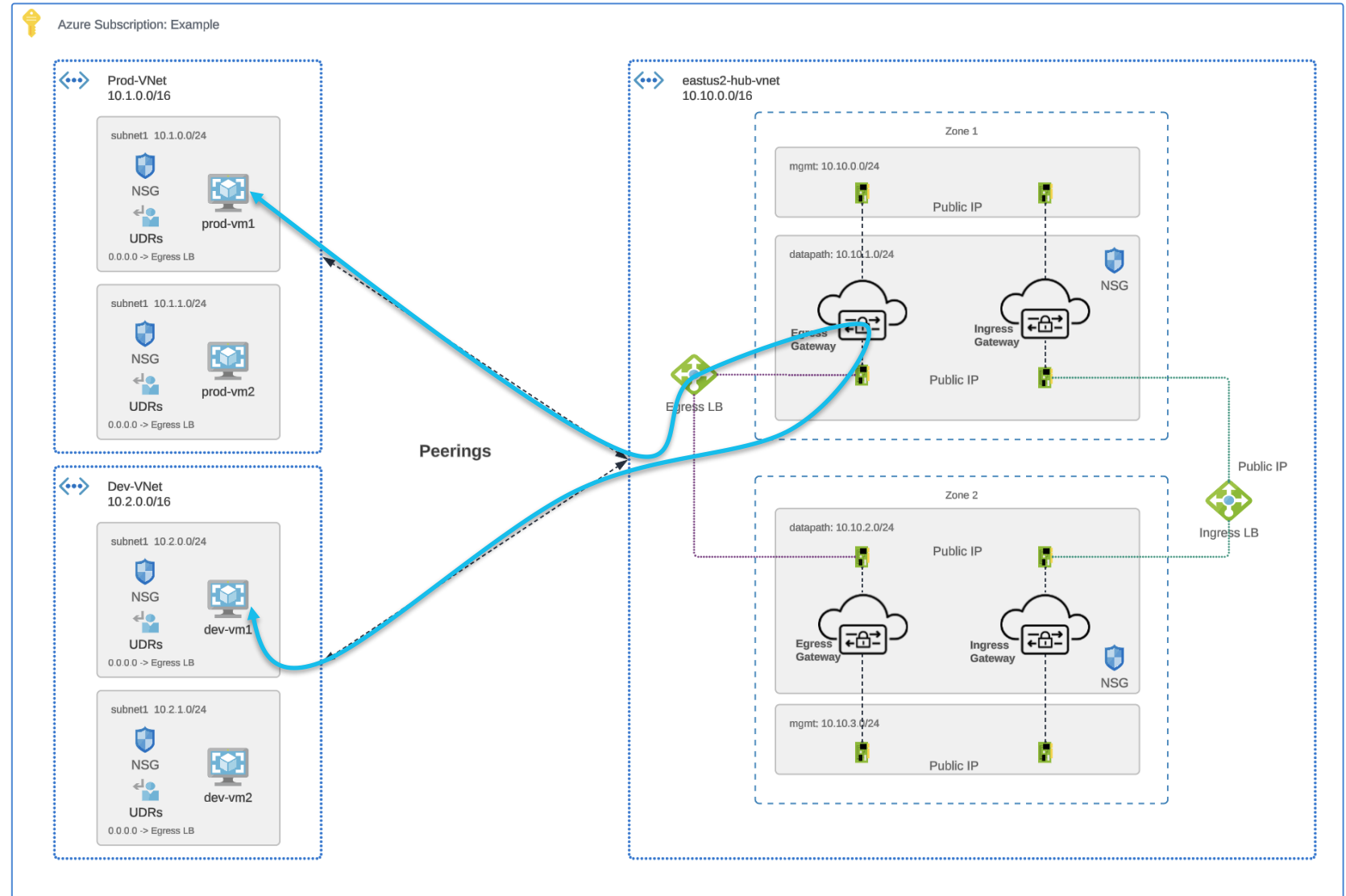
Azure

Orchestration

Security vNET
Network Load Balancer
Public Load Balancer
vNET peering
Autoscale and auto heal
Traffic Engineering – Route Table

Lifecycle management

Ingress and Egress Gateway



Centralized Security Model

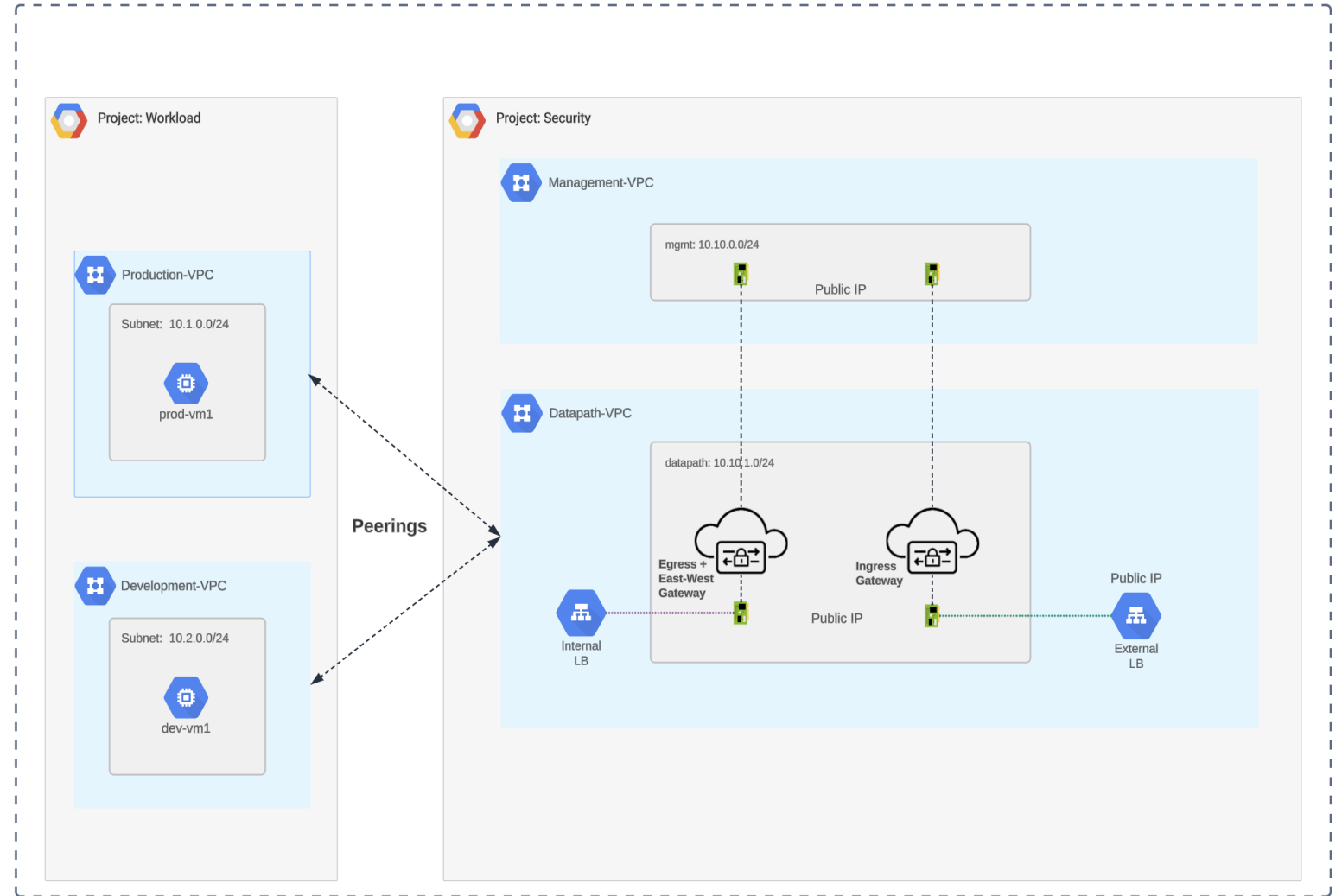
Google Cloud Platform

Orchestration

Security VNET
Internal Load Balancer
External Load Balancer
VPC peering
Autoscale and auto heal
Traffic Engineering – Route Table

Lifecycle management

Ingress and Egress Gateway



Centralized Security Model

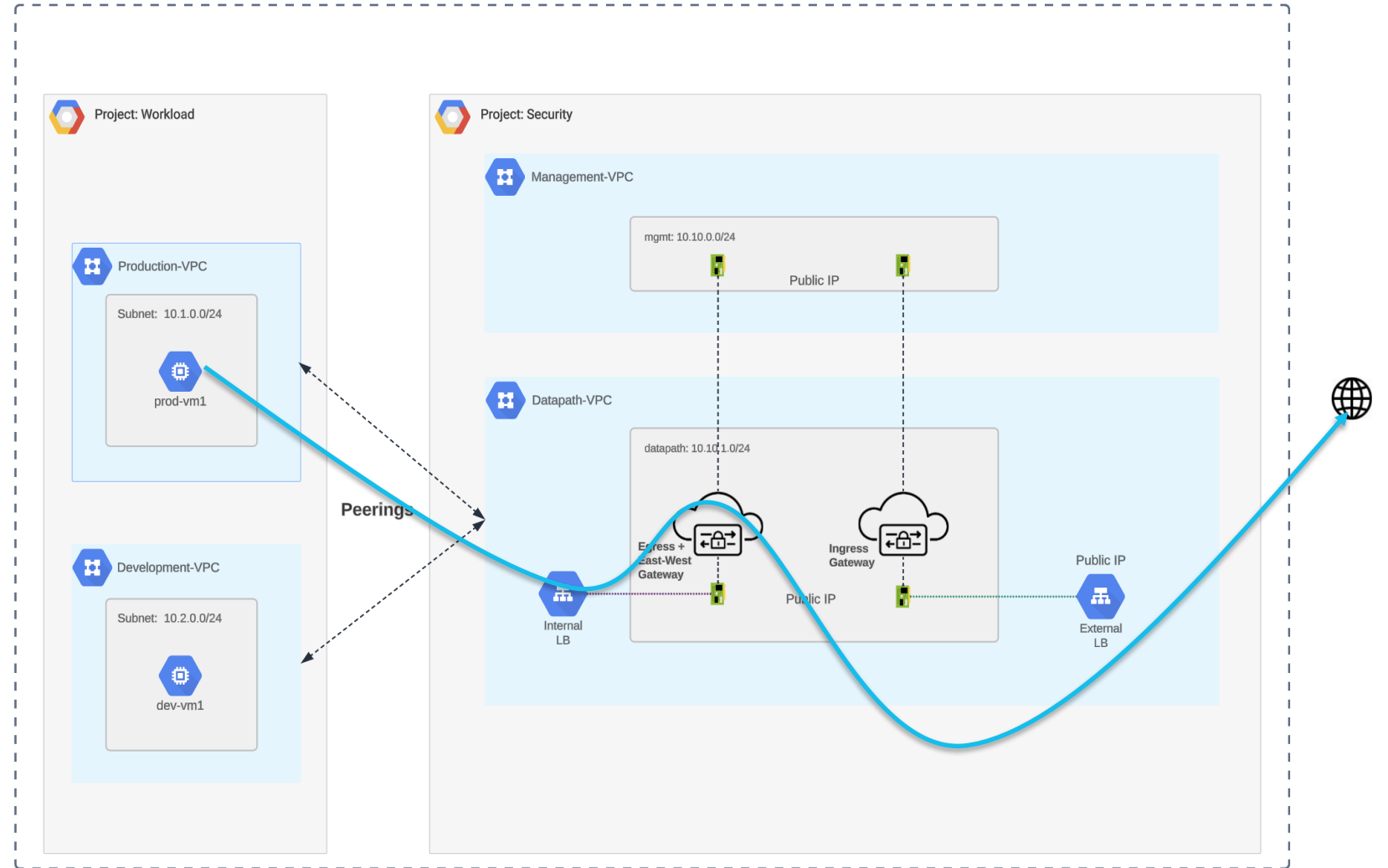
Google Cloud Platform

Orchestration

Security VNET
Internal Load Balancer
External Load Balancer
VPC peering
Autoscale and auto heal
Traffic Engineering – Route Table

Lifecycle management

Ingress and Egress Gateway



Centralized Security Model

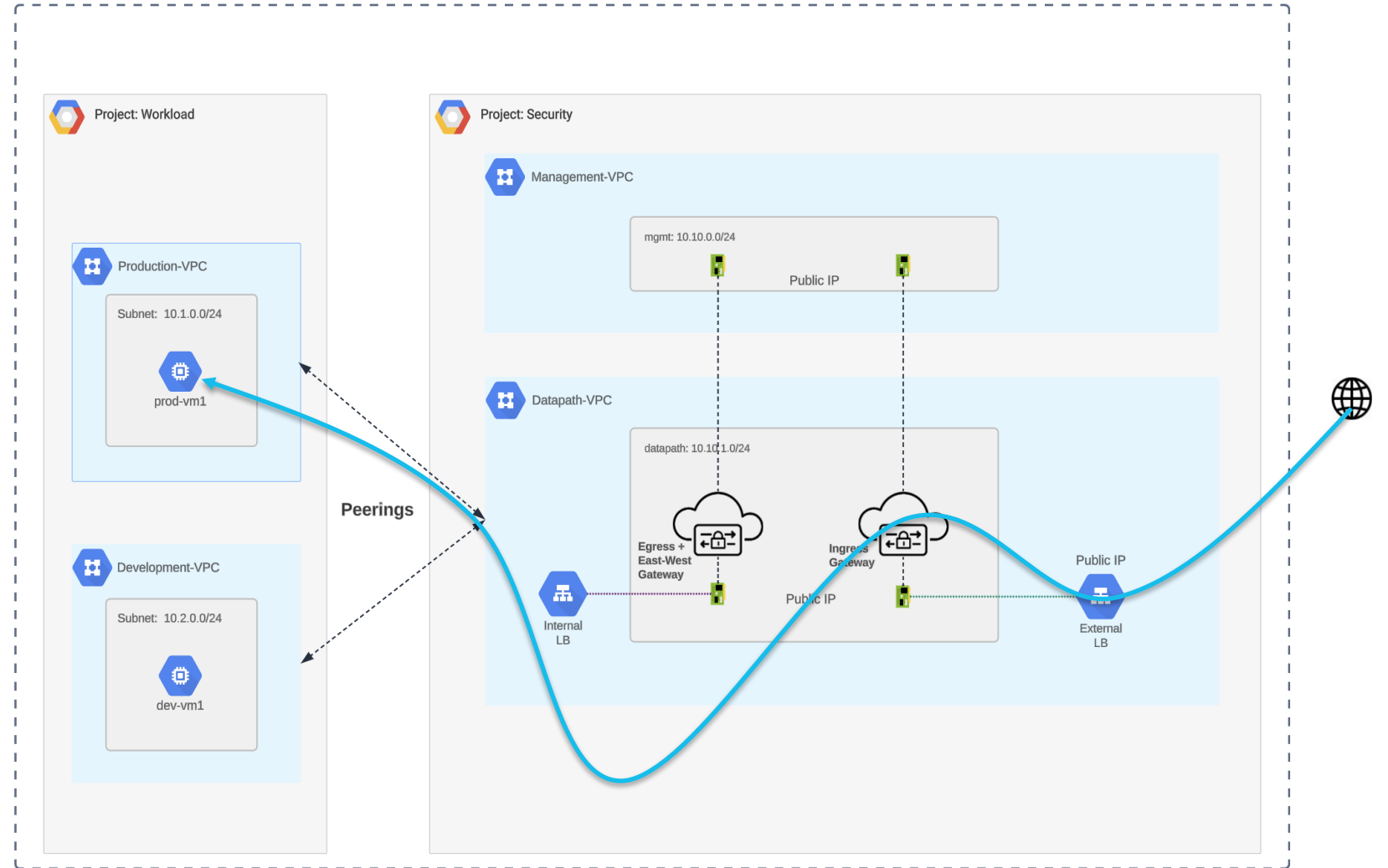
Google Cloud Platform

Orchestration

Security VNET
Internal Load Balancer
External Load Balancer
VPC peering
Autoscale and auto heal
Traffic Engineering – Route Table

Lifecycle management

Ingress and Egress Gateway



Centralized Security Model

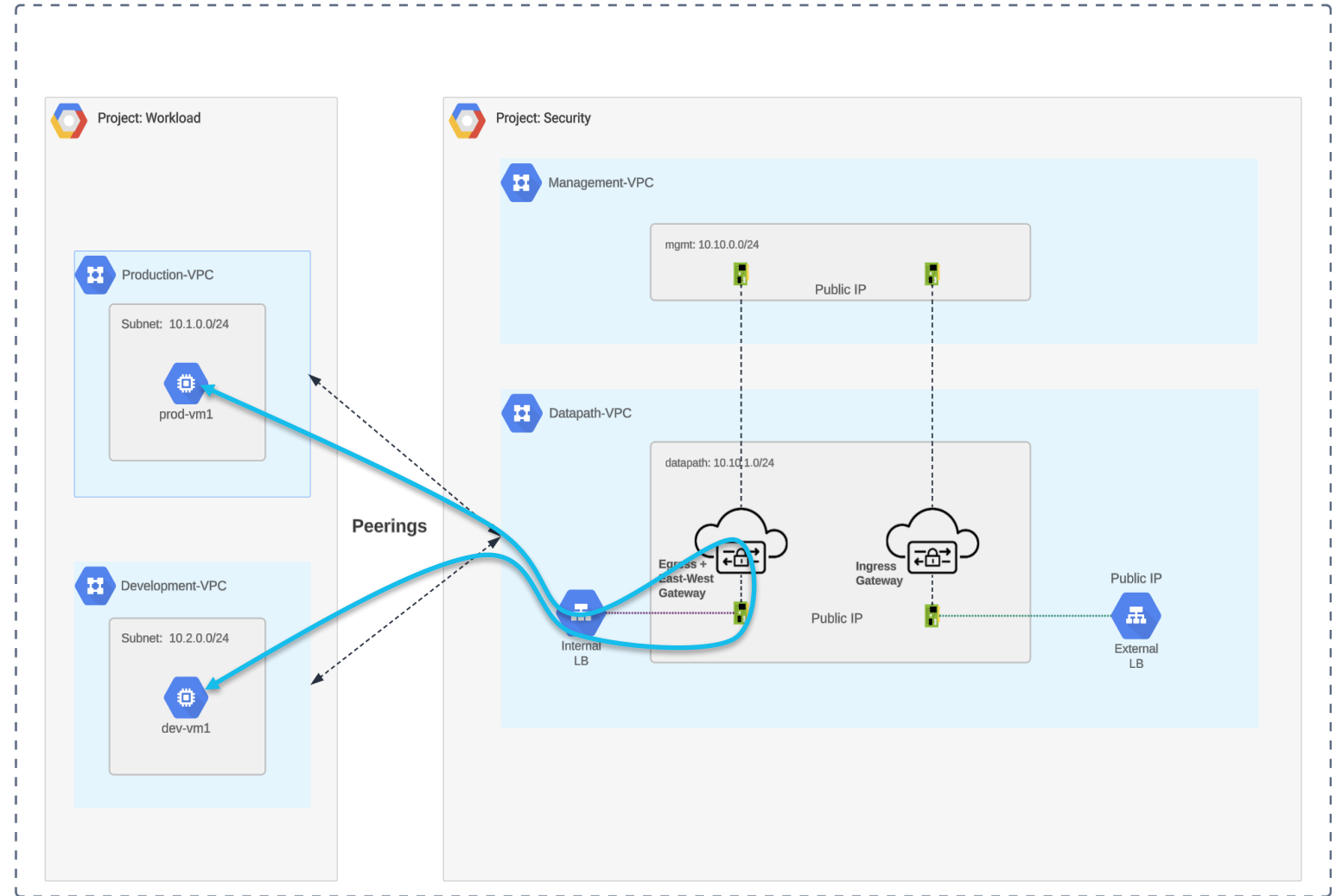
Google Cloud Platform

Orchestration

Security VNET
Internal Load Balancer
External Load Balancer
VPC peering
Autoscale and auto heal
Traffic Engineering – Route Table

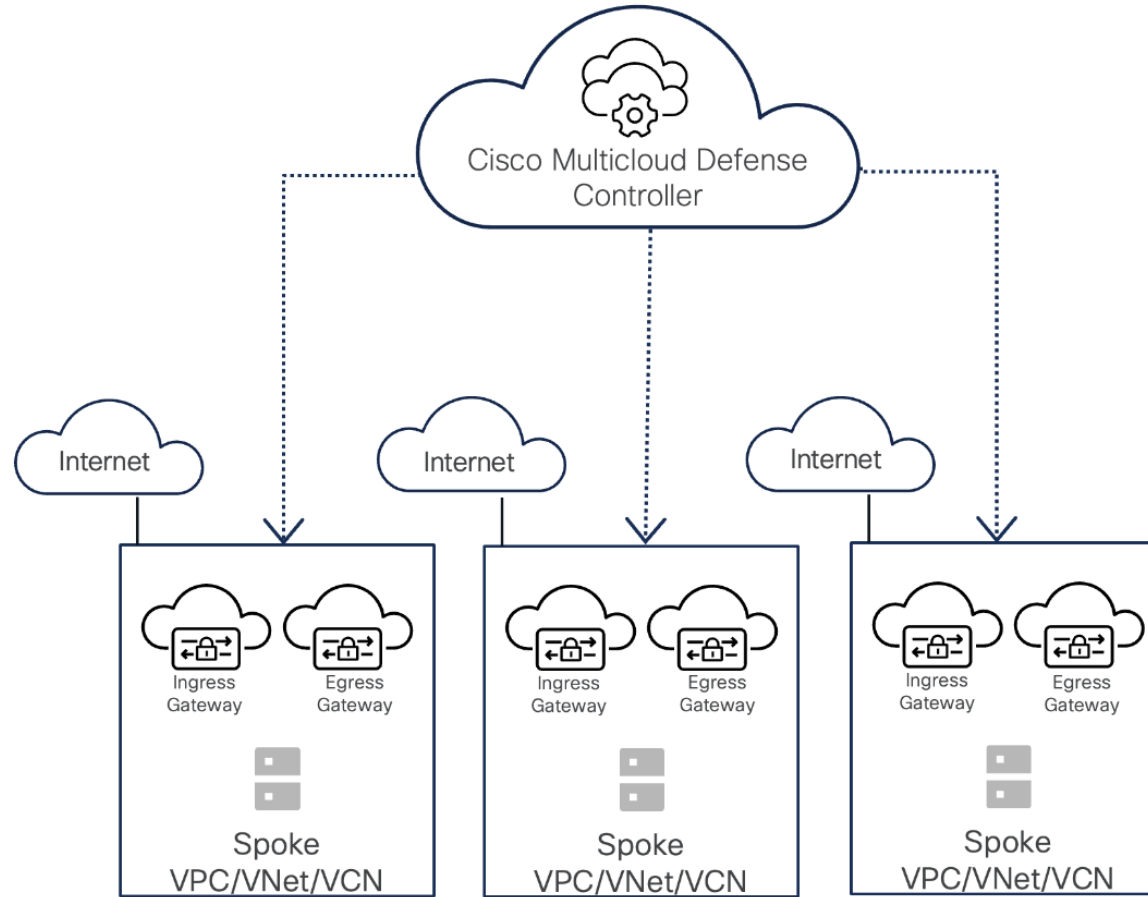
Lifecycle management

Ingress and Egress Gateway



Distributed Model

AWS, Azure, GCP and OCI



Securely building bridges between infrastructures

Multicloud Networking

Cloud-to-cloud connectivity

Site-to-cloud connectivity

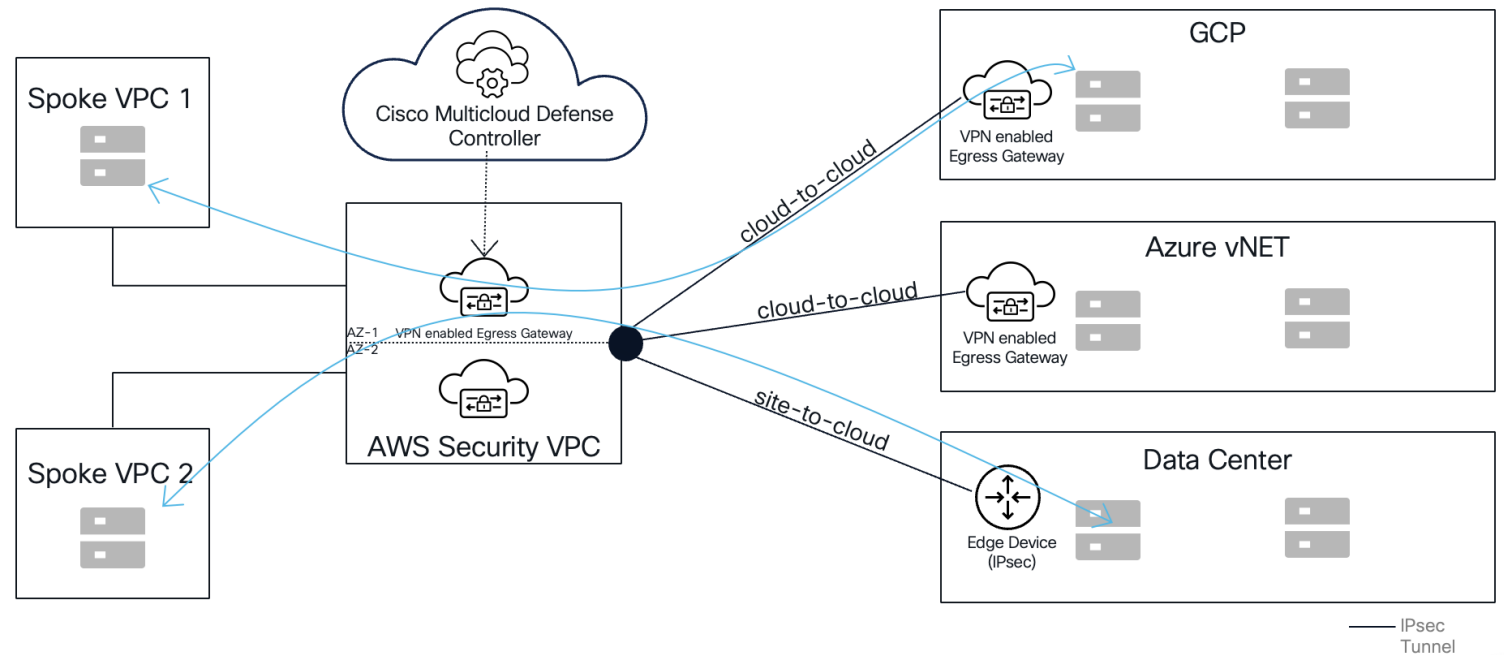
Centralized and Distributed Security Model supported

Orchestration and Automation

VPN and BGP Support

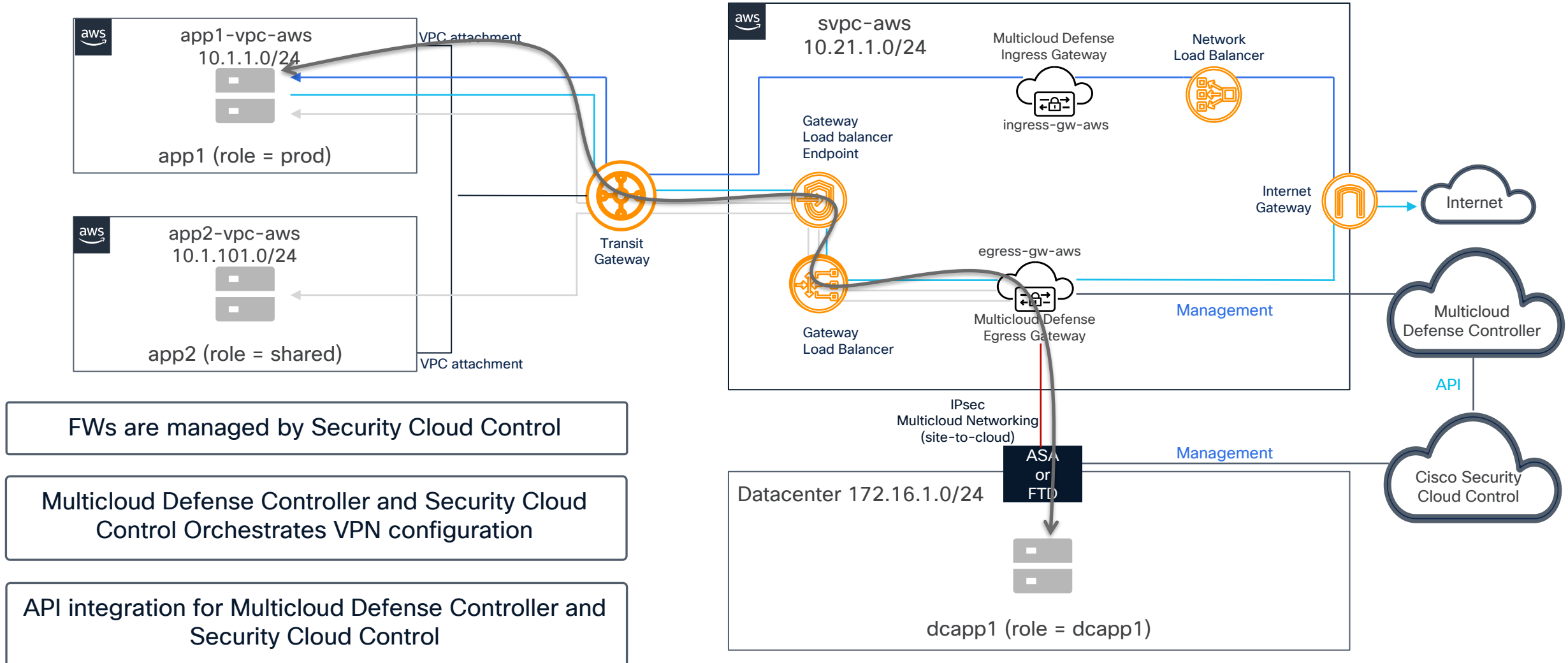
Simplified Operations

Advanced Security



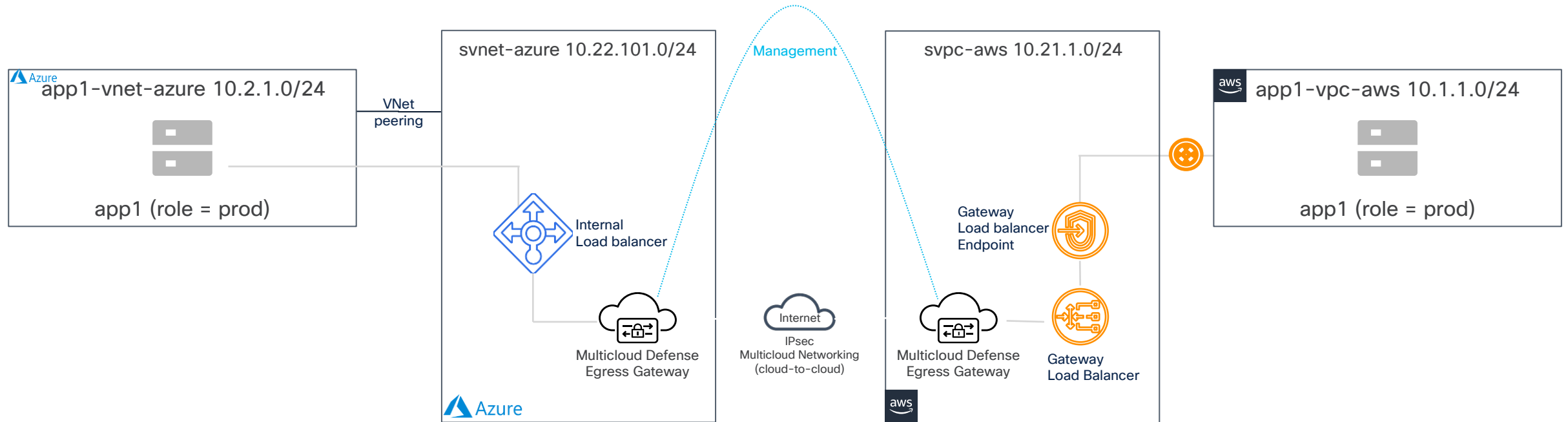
Multicloud Networking

Site-to-cloud connectivity: Centralized Security Model



Multicloud Network

Cloud-to-cloud (Centralized Security Model)



Controller Orchestrates VPN configuration

Automated Traffic Steering

Securely connect cloud environment using fully-orchestrated VPN tunnels

FTDv Overview and Deployment Modes

Secure Firewall Threat Defense Virtual

Private Cloud



Public Cloud



Gov/IC Cloud



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

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

Cloud Leadership

Clustering & Auto Scaling

Integration with cloud native
services & infrastructure

Accelerated Networking

Smart & Tiered Licensing

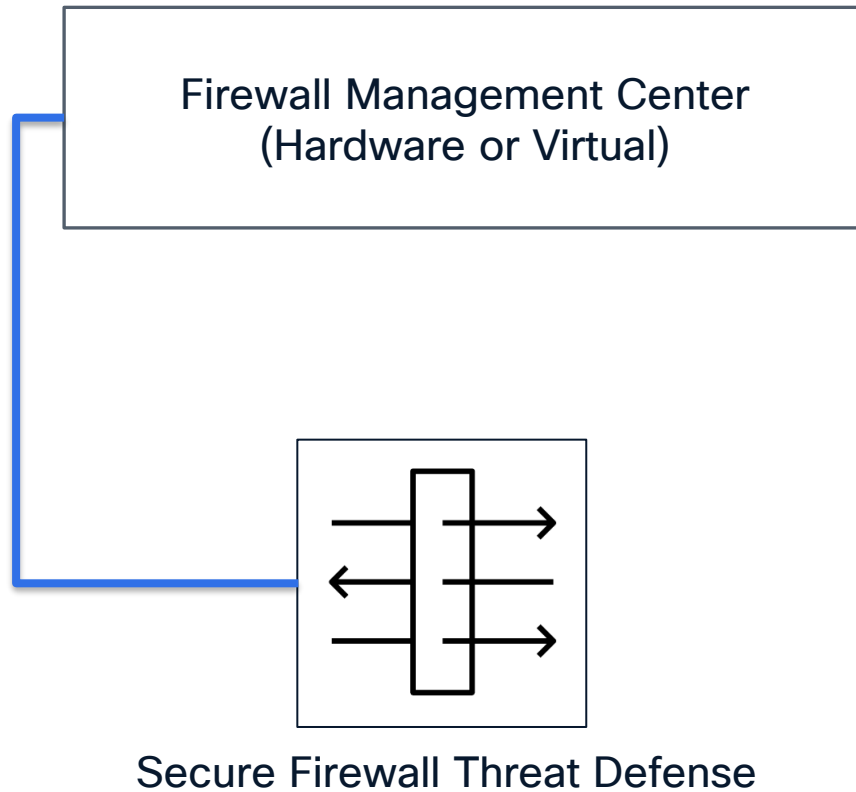
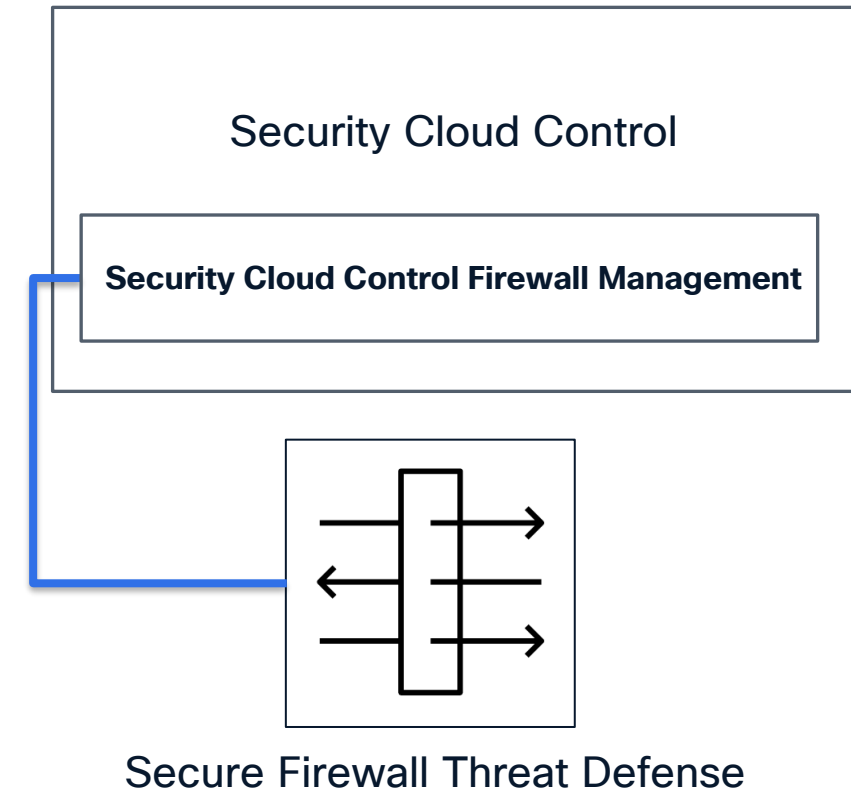
Dynamic Policy

Quickstarts, Infrastructure as
Code and Automation

Gateway Load balancer
integration

Snapshots

Firewall Management



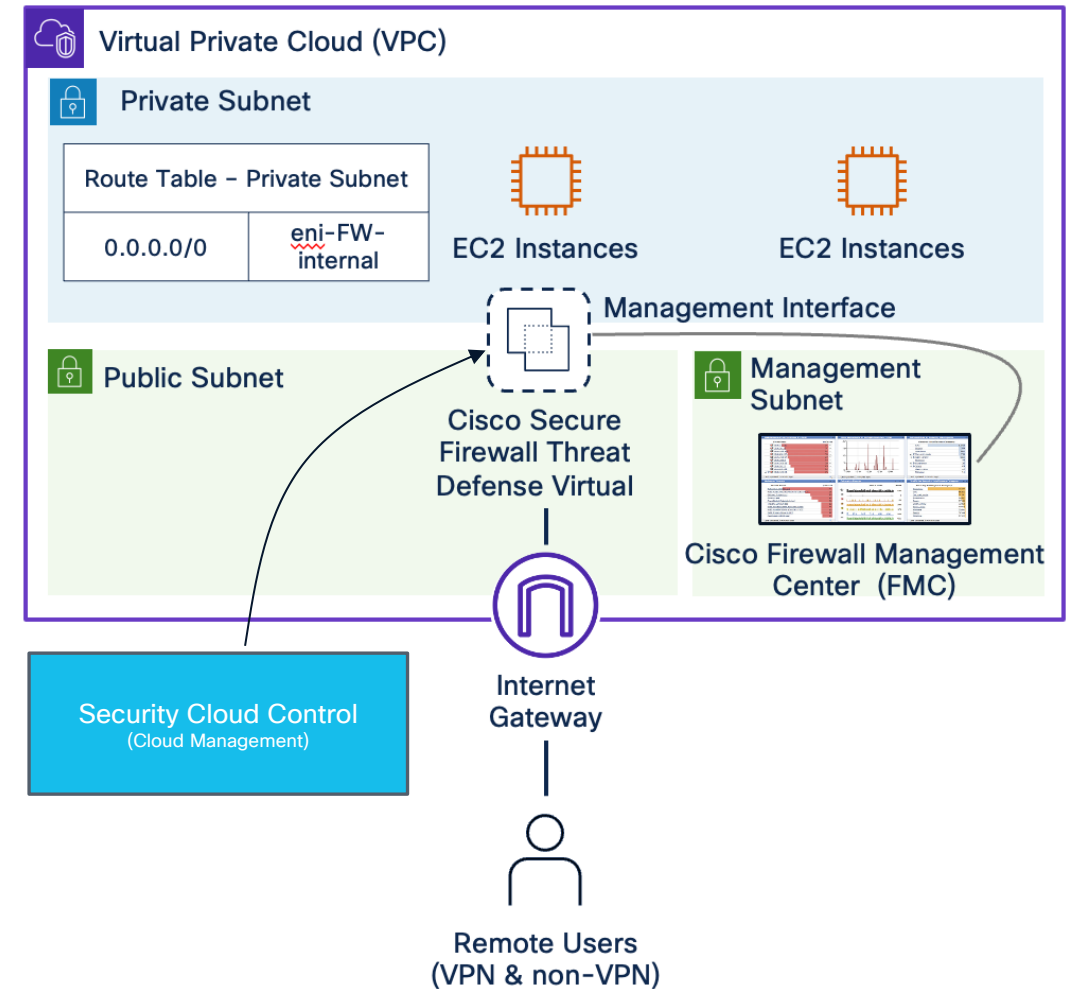
Deployment Modes

Routed Mode

- Secure Firewall and Firewall Management Center are available in Marketplace
- **Management options:** Security Cloud Control or Firewall Management Center
- Supports for BYOL and PAY-G
- Acts as a next-hop for workloads/EC2 instances

Use-cases

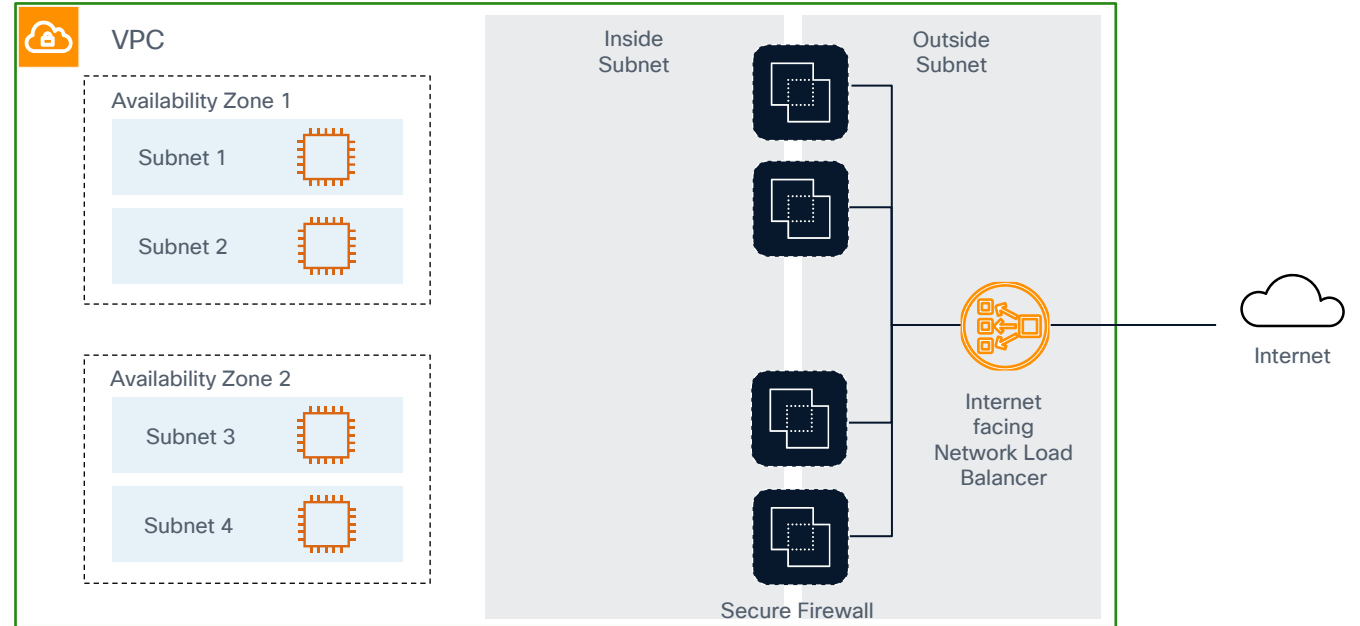
- Stateful FW
- VPN
- AVC
- IPS/IDS
- URL-Filtering
- Malware Protection



Cisco Secure Firewall Threat Defense Virtual – Routed Mode

Secure Firewall Threat Defense

- Multiple Firewalls behind AWS NLB or ALB
 - NLB health check for fault tracking
 - Support for multi-AZ deployment
 - FQDN-based NAT on Cisco Firewall
 - Manual scale
 - SNAT is required for traffic symmetry
-
- Firewalls are managed by Security Cloud Control or Firewall Management Center

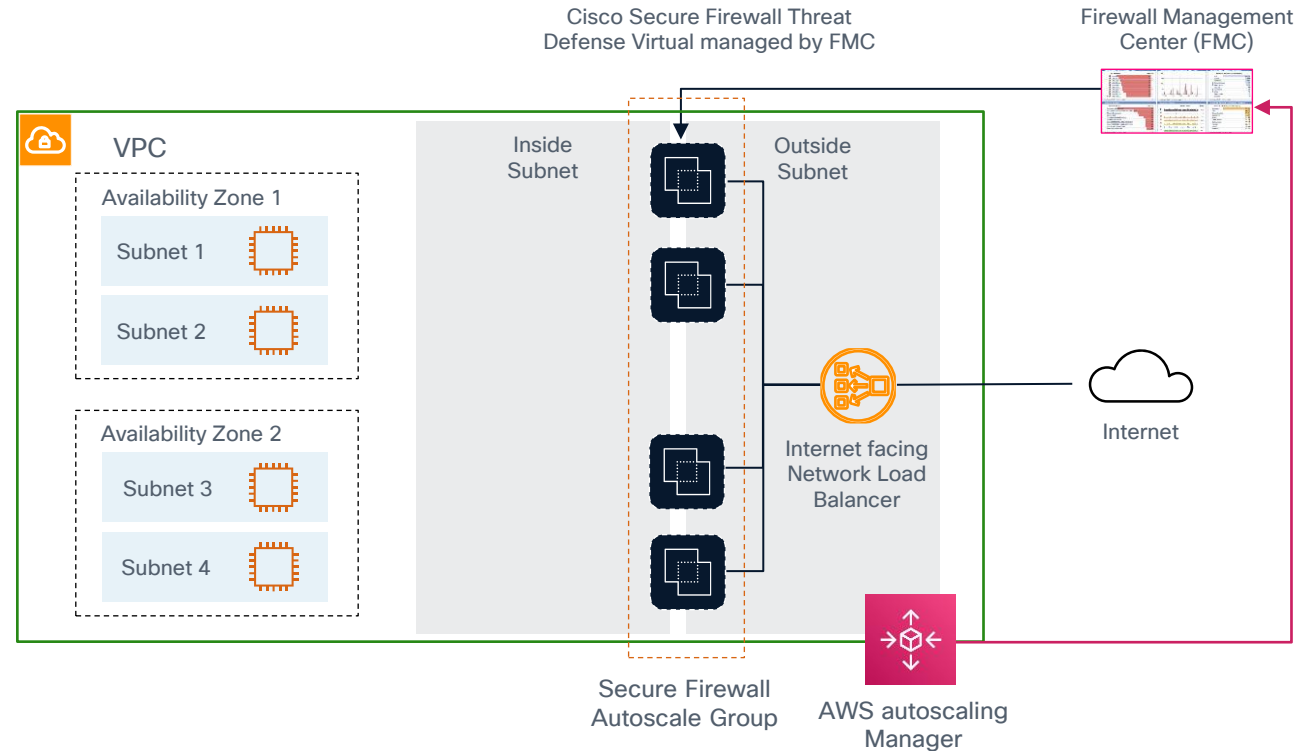


Multiple Firewalls behind AWS NLB/ALB

Secure Firewall Threat Defense

Autoscale

- Autoscale is supported
 - AWS, Azure, GCP and OCI
- Firewall can be managed by Firewall Management Center or Security Cloud Control
- Support for BYOL and PAY-G

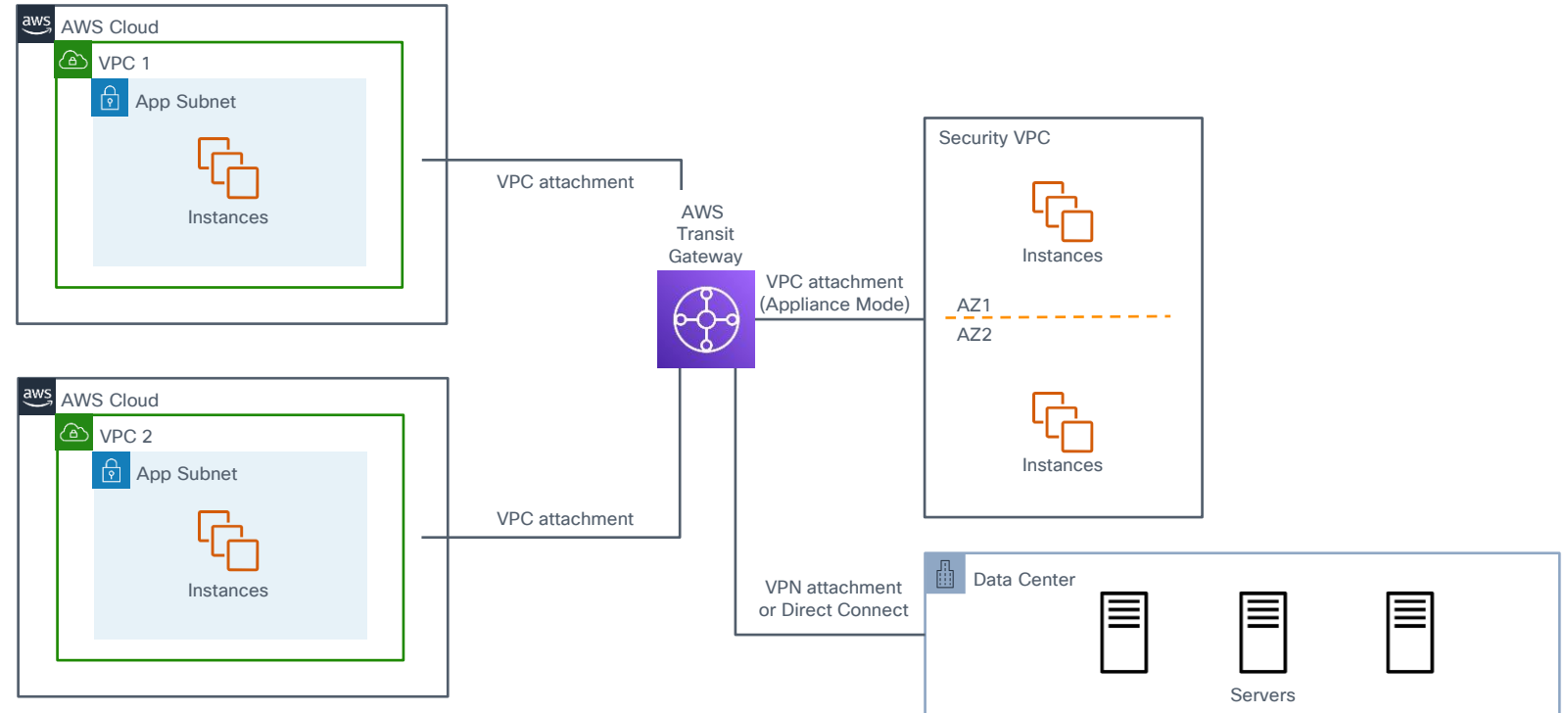


Secure Firewall Autoscale

Secure Firewall Multi-AZ architecture

Transit Gateway

- Secure Firewall can be deployed in multi-az architecture
- Transit Gateway is supported for VPC connectivity
 - VPC attachment
 - VPN attachment
 - Appliance mode attachment

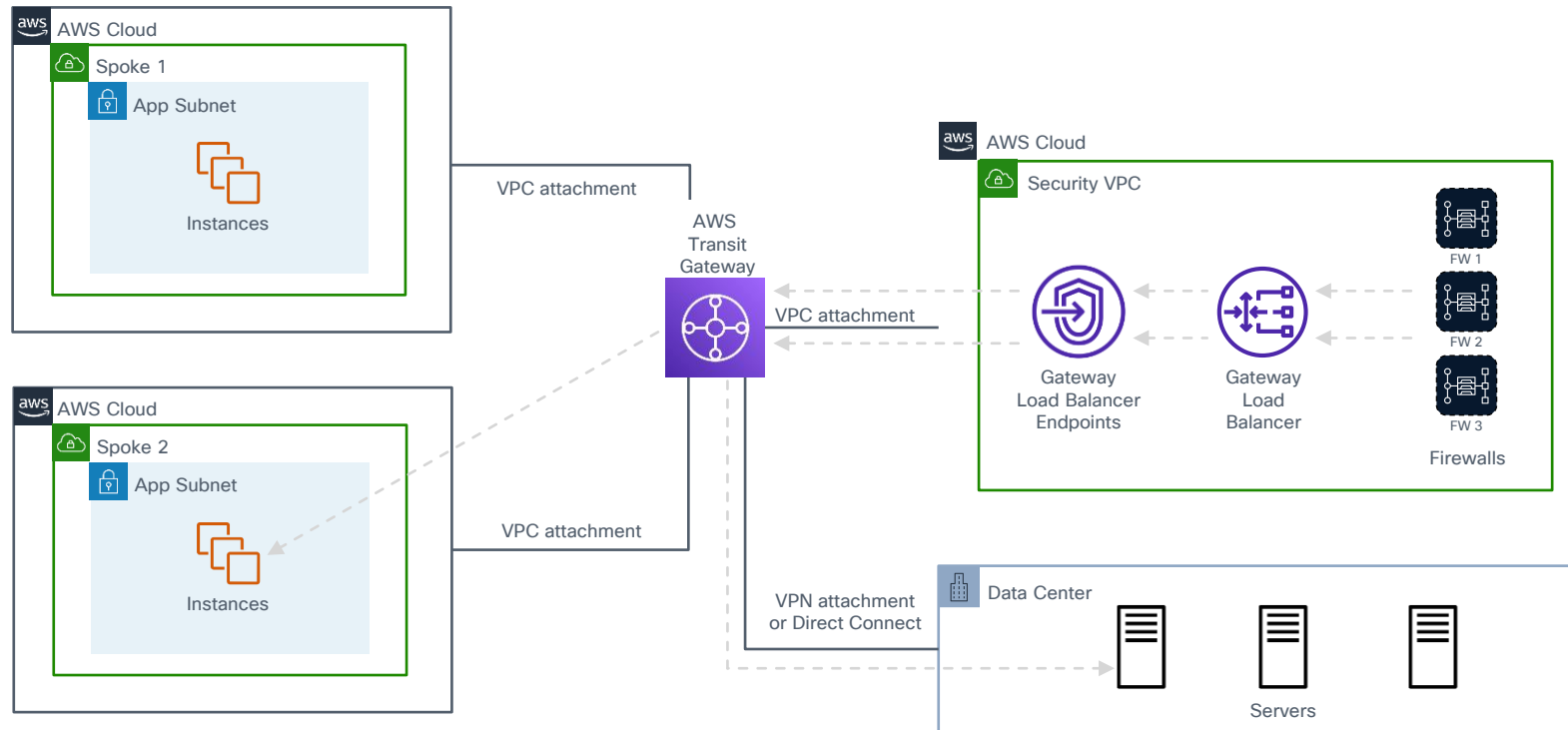


Secure Firewall TGW Multi-AZ architecture

Secure Firewall Multi-AZ architecture

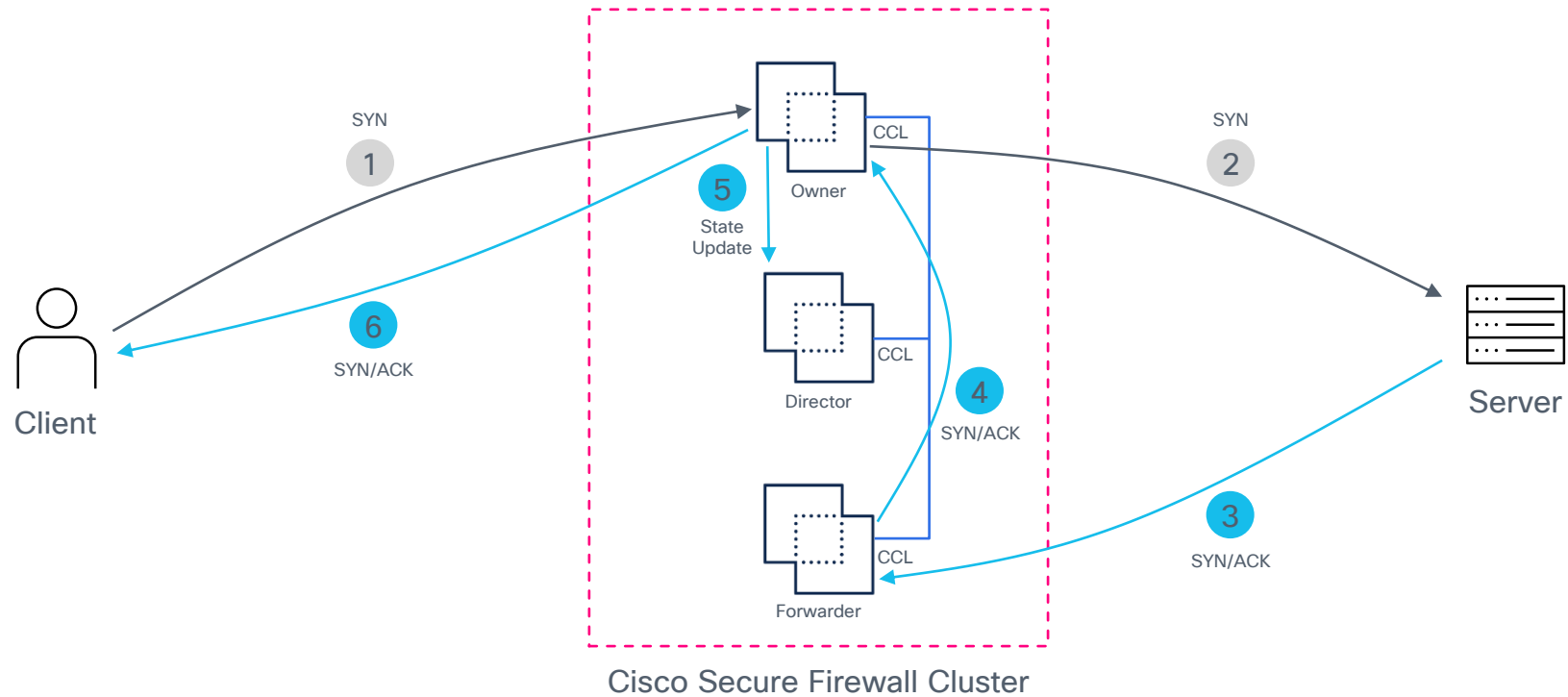
Gateway Load Balancer

Gateway Load Balancer helps you easily deploy, scale, and manage your third-party virtual appliances. It gives you one gateway for distributing traffic across multiple virtual appliances while scaling them up or down, based on demand. This decreases potential points of failure in your network and increases availability.



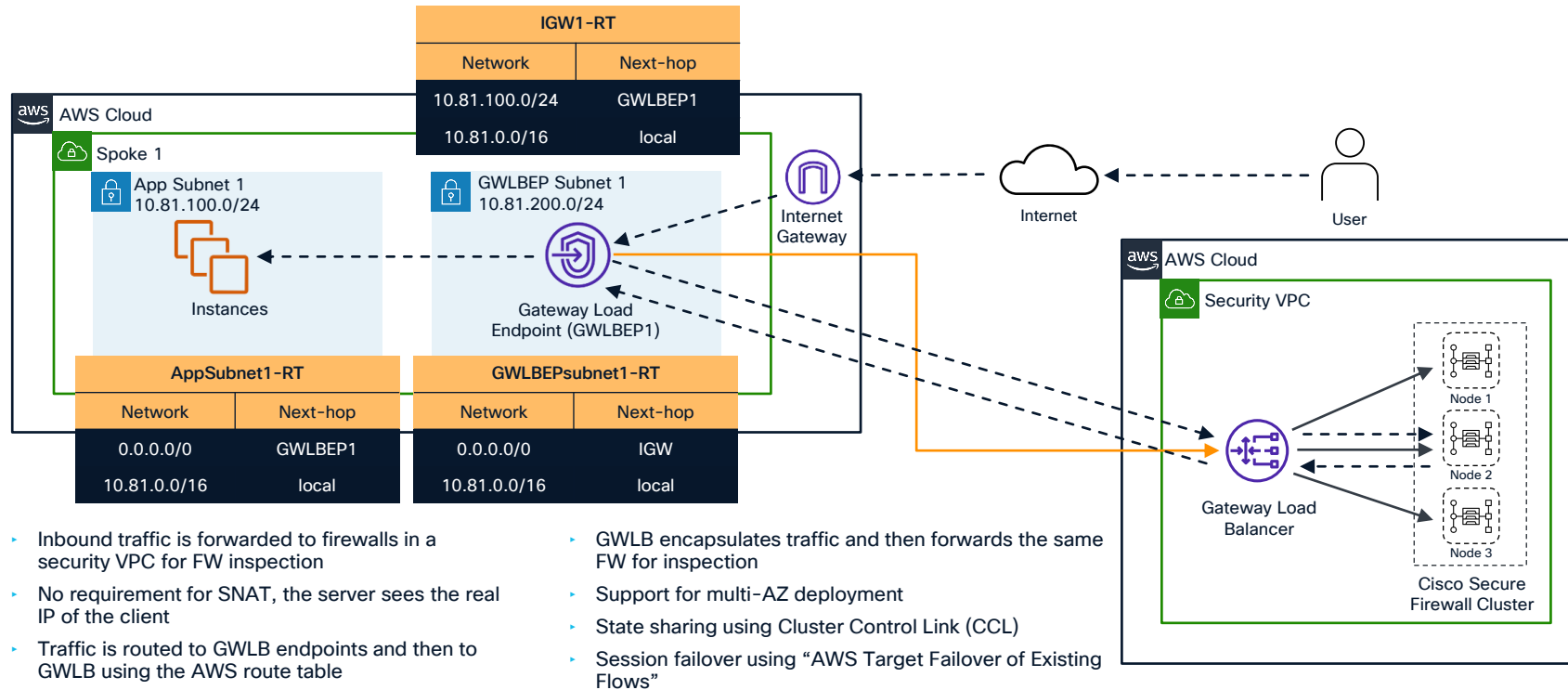
Secure Firewall GWLB architecture

Secure Firewall Cluster Overview



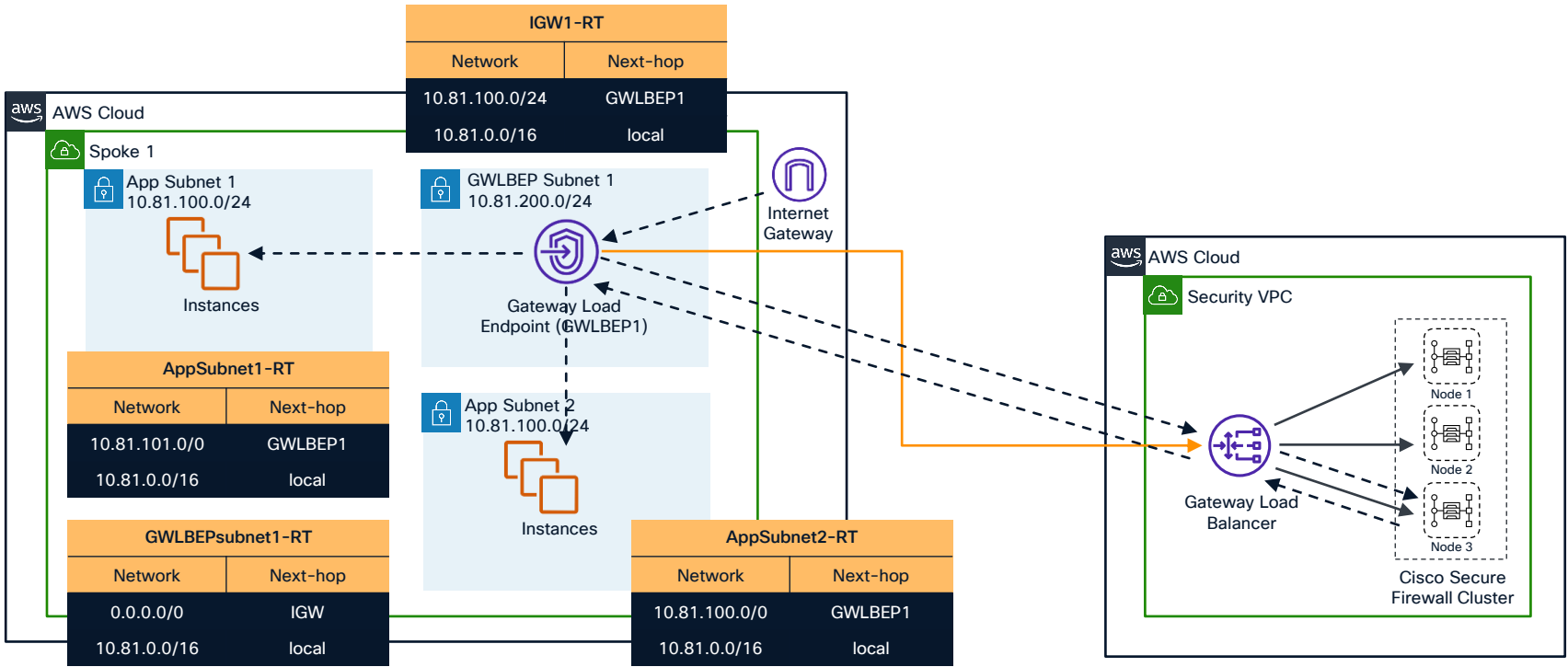
Secure Firewall Virtual Threat Defense Clustering

Ingress Protection - AWS



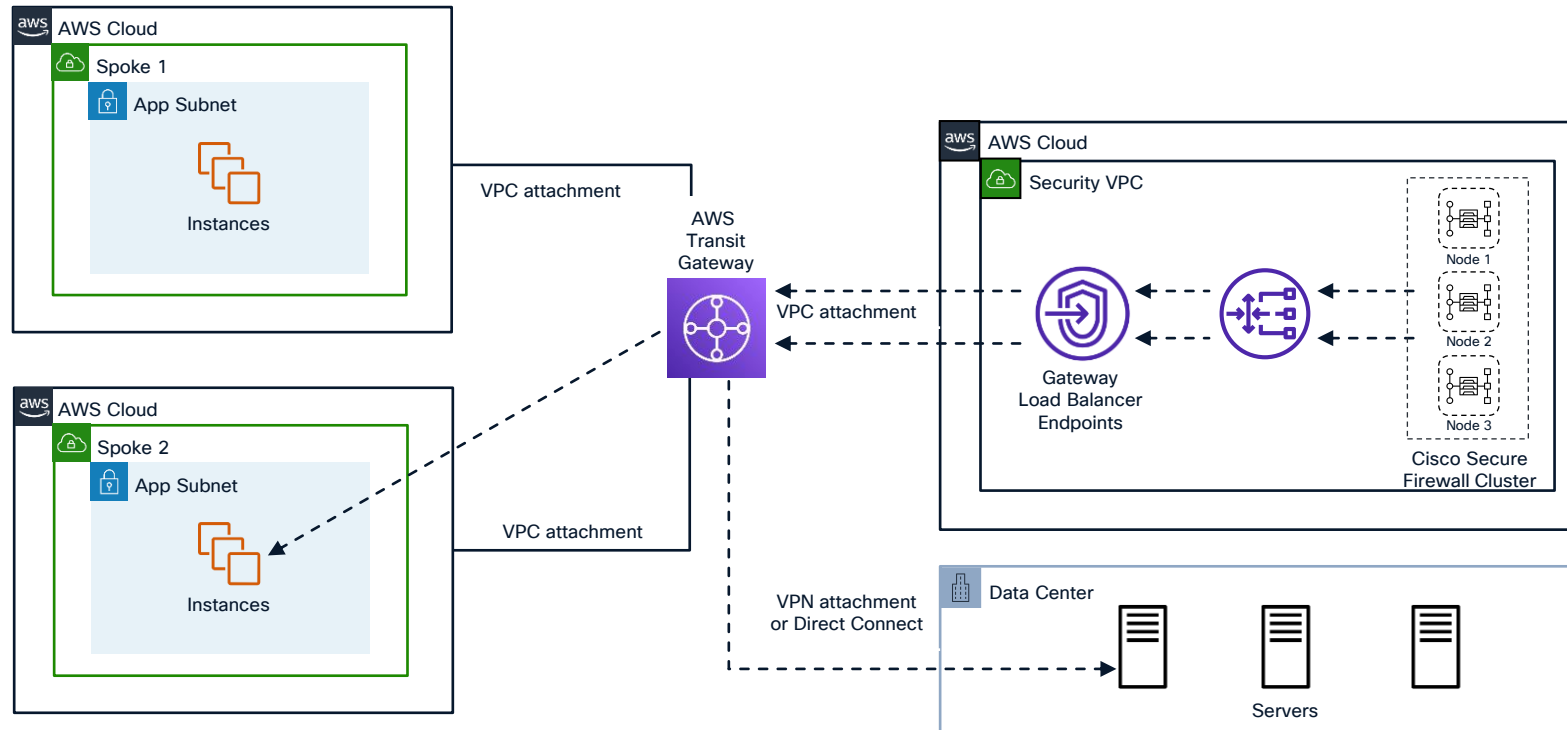
Secure Firewall Virtual Threat Defense Clustering

East/West Protection - AWS



Secure Firewall Virtual Threat Defense Clustering

East/West Protection - AWS



Secure Firewall Threat Defense Virtual orchestrated by Multicloud Defense Controller

Why?

- Deploying virtual firewall autoscale in the cloud is manual and complex
- Customers must configure cloud elements (VPCs, subnets, security groups, route tables, routes, and auto-scaling logic) themselves
- Slower deployments (increased risk of human errors)
- Requires advanced cloud expertise
- Customers seek the simplicity of Multicloud Defense while retaining FTDv as their enforcement point to align with their on-premises FTD model

What's new?

- Integrating Cisco FTDv deployment into Multicloud Defense
- Automating VPC, subnet, and security group creation
- Simplifying route table and peering setup
- Enabling automatic FTDv onboarding to cdFMC
- Adding auto-scaling capability of FTDv from the MCD controller
- Simplifying FTDv licensing with hourly based licensing model
- Egress and E/W Protection for AWS and Azure environments

Improved Licensing

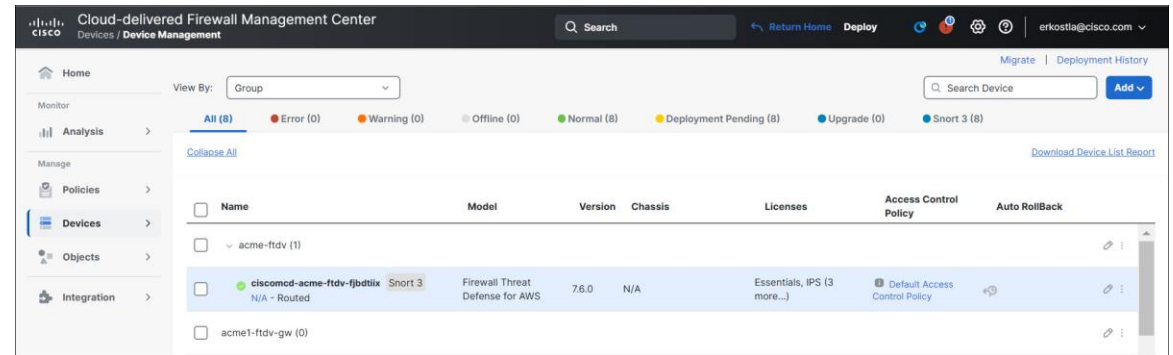
- BYOL – Bring your own license
- Hourly license model – Premier License (TMC = Threat, Malware and URL Filtering)



AI generated image

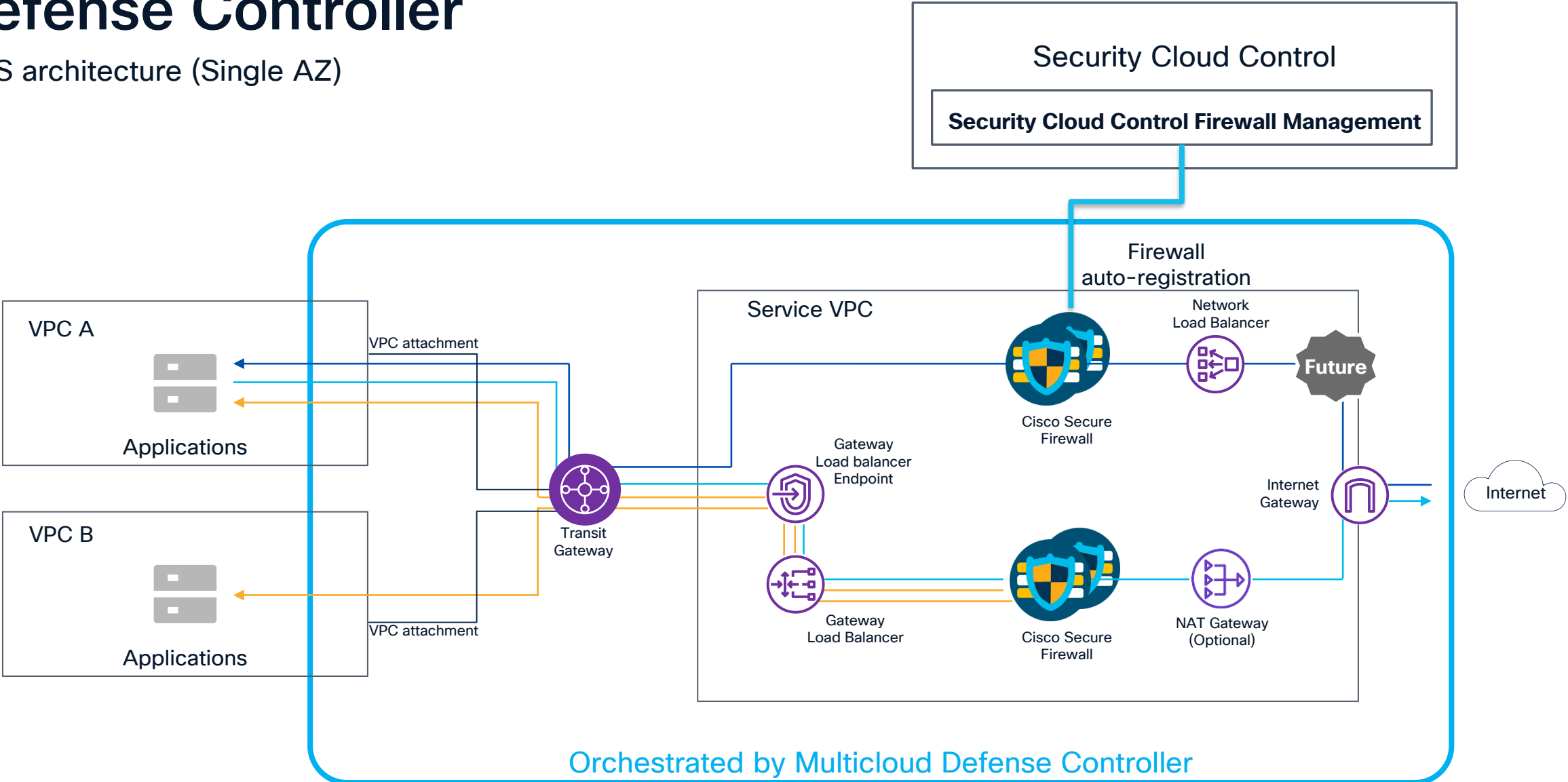
Secure Firewall Threat Defense Virtual orchestrated by Multicloud Defense Controller

- 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
 - 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
- For policy consistency, any existing ACP can be utilized



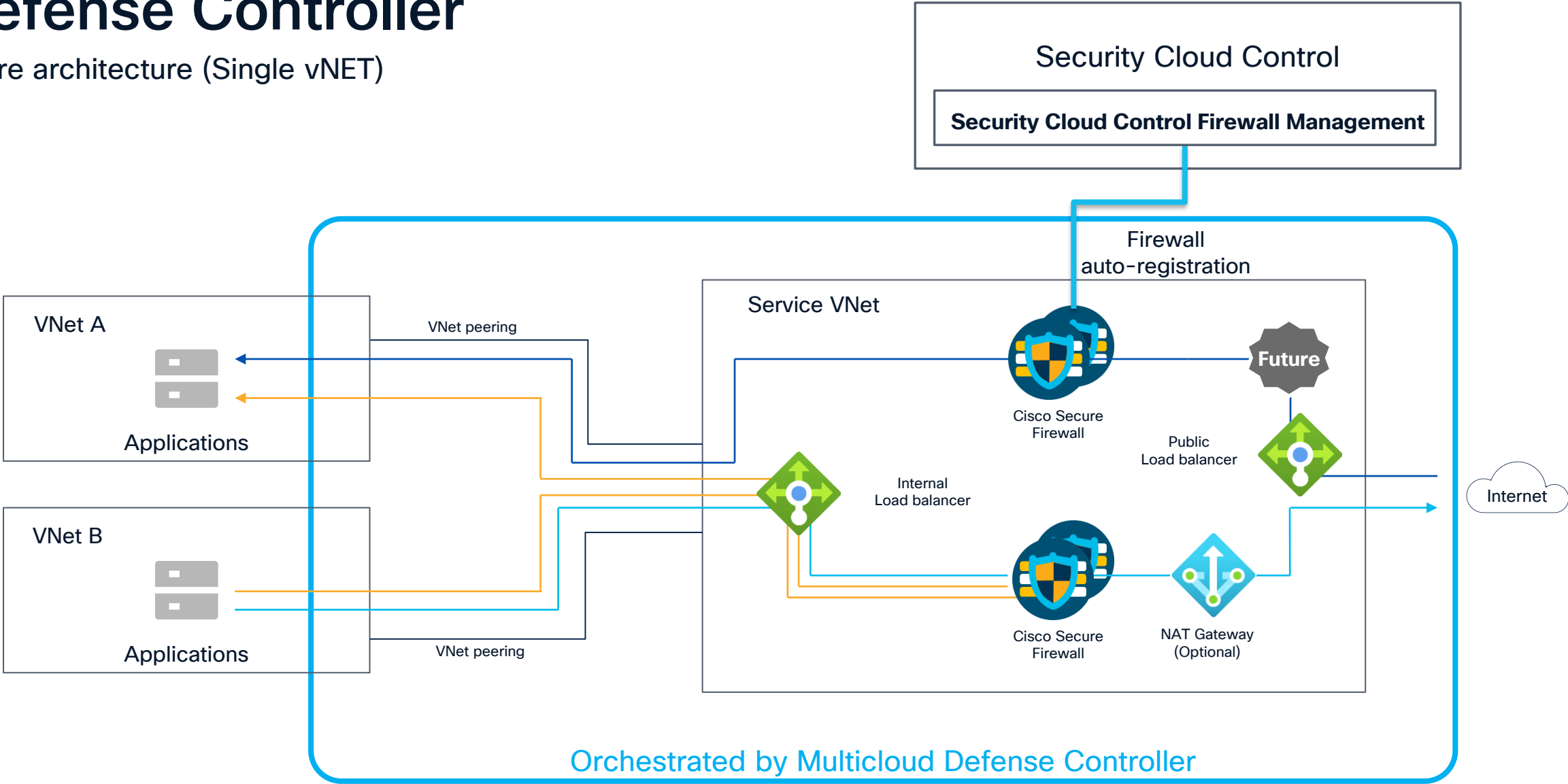
Cisco Secure Firewall Virtual Orchestrated by Multicloud Defense Controller

AWS architecture (Single AZ)



Cisco Secure Firewall Virtual Orchestrated by Multicloud Defense Controller

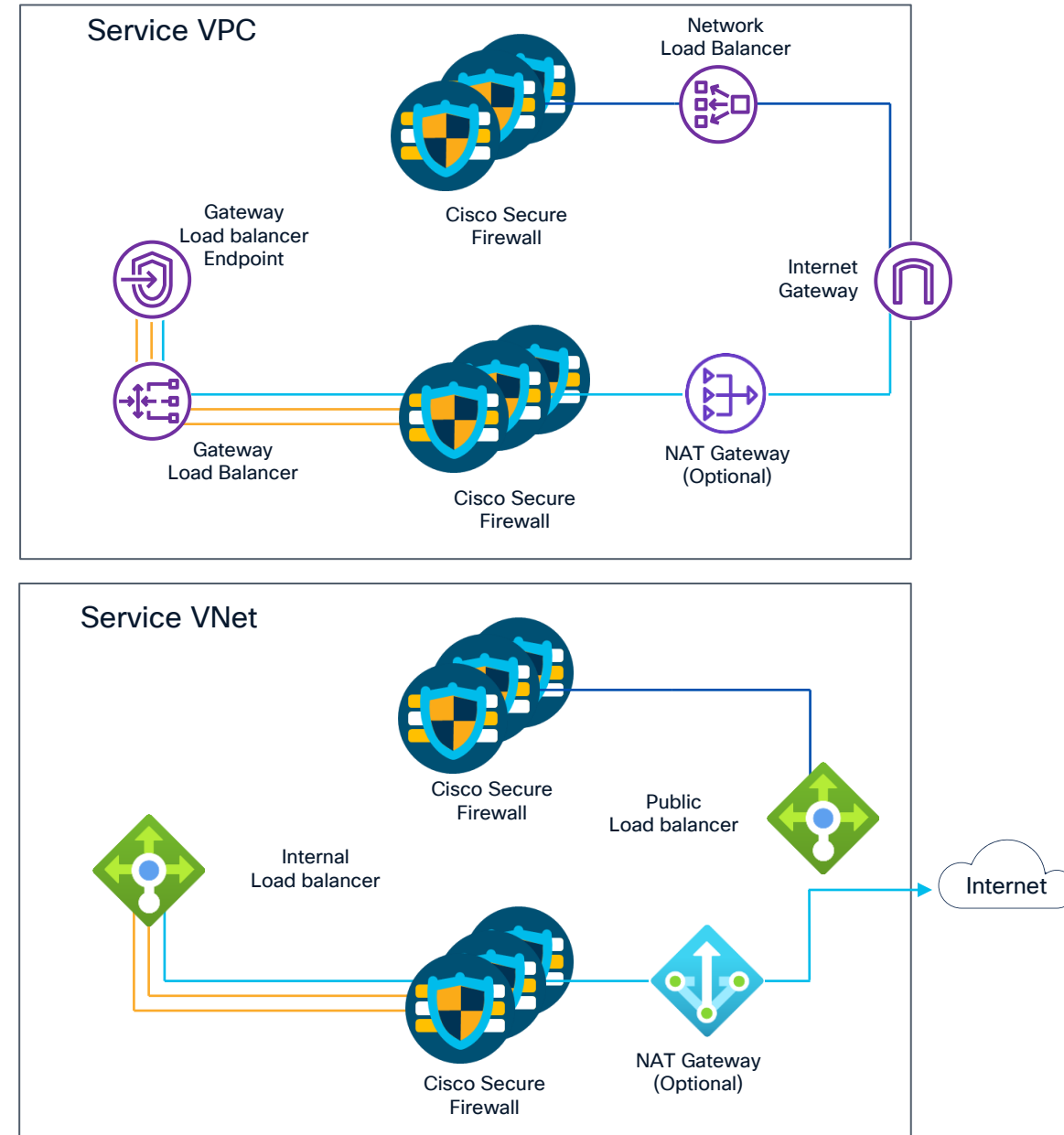
Azure architecture (Single vNET)



Autoscaling

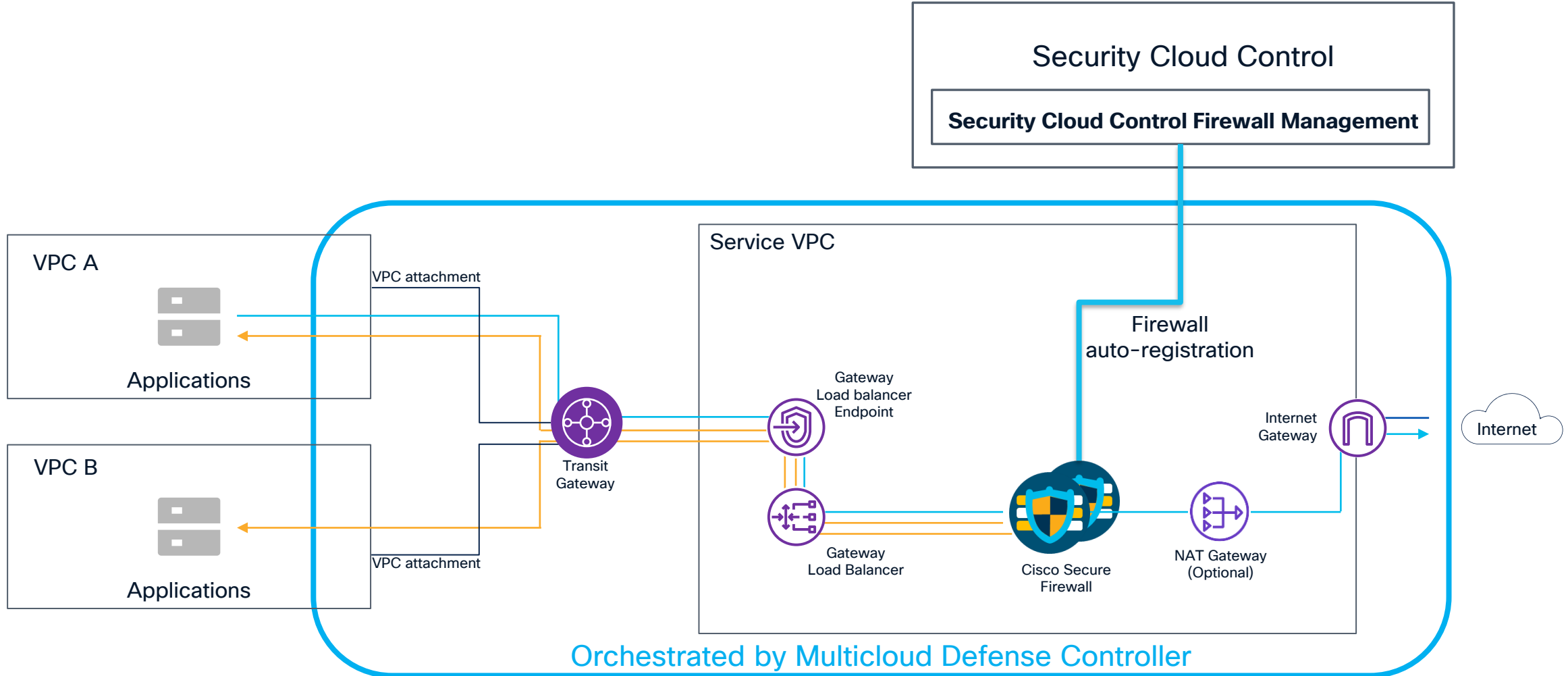
Multicloud Defense controller handles autoscaling of FTDv

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



FTDv Orchestration

Secure Firewall Orchestration by Multicloud Defense Demo



Security Cloud ControlCisco 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

Dashboard

Discover X

1

Cloud Accounts

1 aws

0 A

0

0

Add Account

View More

Account Resources

Discover X

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 X

No Data

View More

DNS Traffic

Discover X

No Data

View More

Favorites

Home

Inventory

Investigate

Policies

Infrastructure

Reports

System and Accounts

IaaS using Terraform

Terraform Provider

Provider documentation:

<https://registry.terraform.io/providers/CiscoDevNet/ciscomcd/latest/docs>

Sample Code:

<https://github.com/aksdubeypub/multicloud-terraform>

<https://github.com/CiscoDevNet/Multicloud-Defense>

How to use this provider

To install this provider, copy and paste this code into your Terraform configuration. Then, run `terraform init`.

Terraform 0.13+

```
terraform {  
  required_providers {  
    ciscomcd = {  
      source = "CiscoDevNet/ciscomcd"  
      version = "25.9.2"  
    }  
  }  
}  
  
provider "ciscomcd" {  
  # Configuration options  
}
```

Useful Resources

Resources

Terraform Lab:

<https://github.com/CiscoDevNet/mcd-aws-terraform-workshop>

<https://ciscolearning.github.io/cisco-learning-codelabs/posts/tc-multicloud-defense-spotlight-2024/#0>

SCC Terraform:

<https://registry.terraform.io/providers/CiscoDevNet/sccfm/latest/docs>

Automating Deployments using Terraform:

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2025/pdf/DEVNET-2435.pdf>

Complete your session evaluations



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



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



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



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



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

Thank you

CISCO Live !

