

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect. The overall composition is dynamic and energetic.

CISCO *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Cisco Multicloud Defense

Consistently Secure the Multicloud

John M. Clark
Director, Solutions Engineering
BRKSEC-2145

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

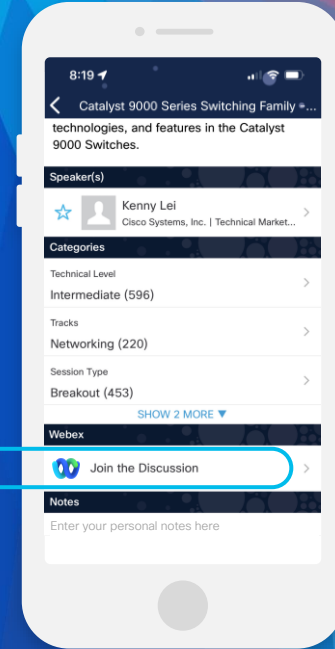
Questions?

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 December 22, 2023.

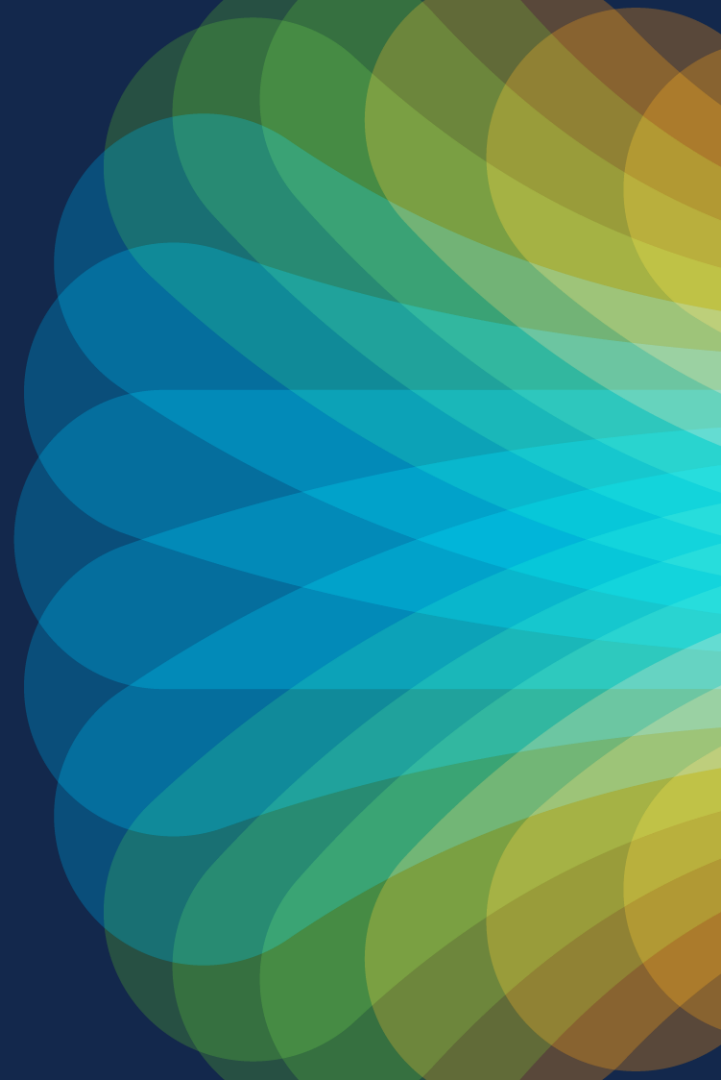


<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2145>

Agenda

- Introduction
- Use-cases
- Protection models
- Deployment architectures
- Access and demo

Cisco Multicloud Defense Introduction



Cisco Cloud Protection Suite

Cisco Security Cloud

Cisco Cloud Protection

Powered by the Talos threat intelligence team

Cisco User Protection

Cisco Breach Protection

Firewall Protection

Cloud Security Suite Focus, Drivers, Features



Multicloud Defense



Panoptica



Secure Workload

Suite Focus

Cloud-based network security

Multi-cloud CNAPP
(cloud-native application
protection platform)

Hybrid-cloud, zero-trust workload
security

Why Critical?

Consistent, automated, advanced
security implementation across
multi-cloud

Provides CNAPP protection to
multi-cloud workloads using
graph-based context

Zero-trust protection for hybrid-
cloud workloads utilizing
machine-driven policy lifecycle
automation

Business
Drivers

- Single-policy across cloud providers
- Avoids CSP tool sprawl
- Advanced in-line security controls
- SaaS delivered controller
- PaaS delivered security

- Agentless
- Context-based prioritization
- Dynamic Remediation
- Build to runtime protection

- Zero Trust / Least Privilege
- SaaS delivered
- Automated Policy Discovery
- Workload & container security
- Enforcement and Compliance

Security
Features

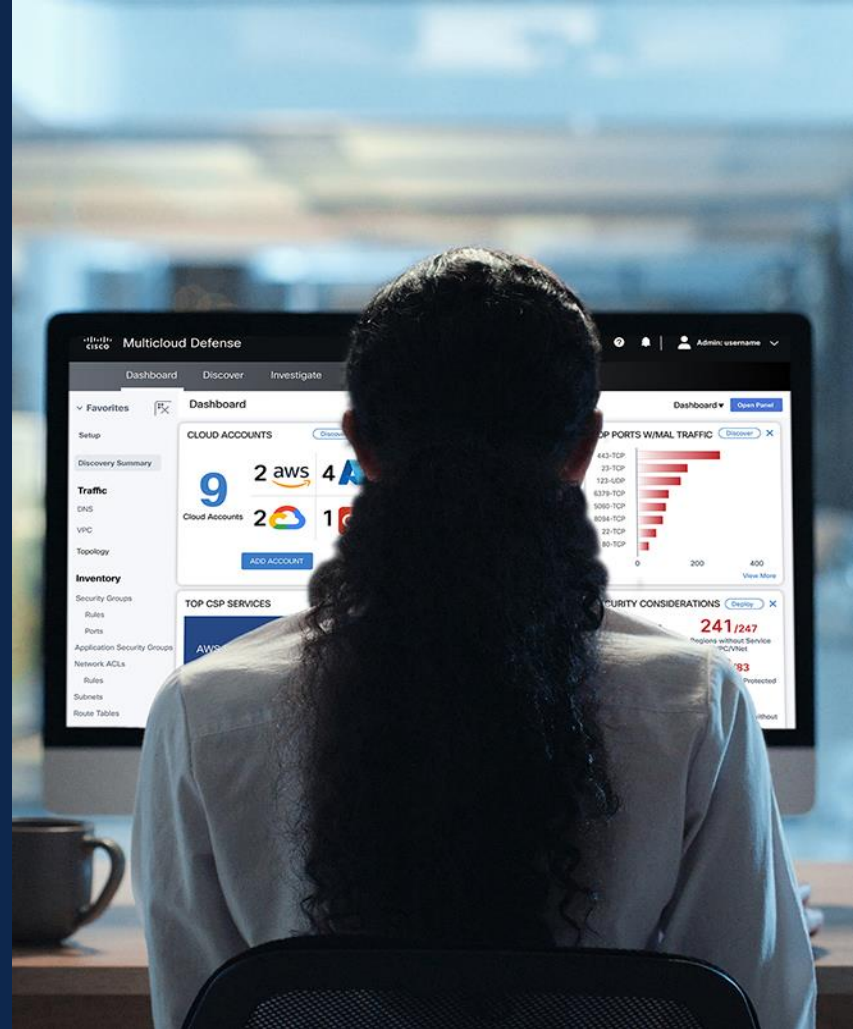
- ✓ WAF
- ✓ IDS / IPS
- ✓ Geo IP
- ✓ Malicious IP
- ✓ Antivirus
- ✓ FQDN Filtering
- ✓ URL Filtering
- ✓ DLP
- ✓ Cloud-native Identity

- ✓ Attack Paths
- ✓ CSPM
- ✓ CWP
- ✓ API Security
- ✓ CI/CD
Security
- ✓ Serverless
Protection

- ✓ Dynamic Policy
- ✓ CVE Identification
- ✓ Policy Simulation
- ✓ Threat Intelligence
- ✓ Flow and telemetry visibility
- ✓ Agent or Agentless

What is multicloud network security?

The convergence of **cloud agnostic networking** and **security** functions to **support and protect applications** against advanced threats **across multiple dynamic environments** and variable 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 Networks 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*

Multicloud Security Starts with Secure Networking



The network is the most impactful place for **securing workloads and data in the cloud**



Cloud networking is essential to security strategies **94%** believe that the secure cloud networking is important to their overall cloud security strategy

Cisco Multicloud Defense: 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

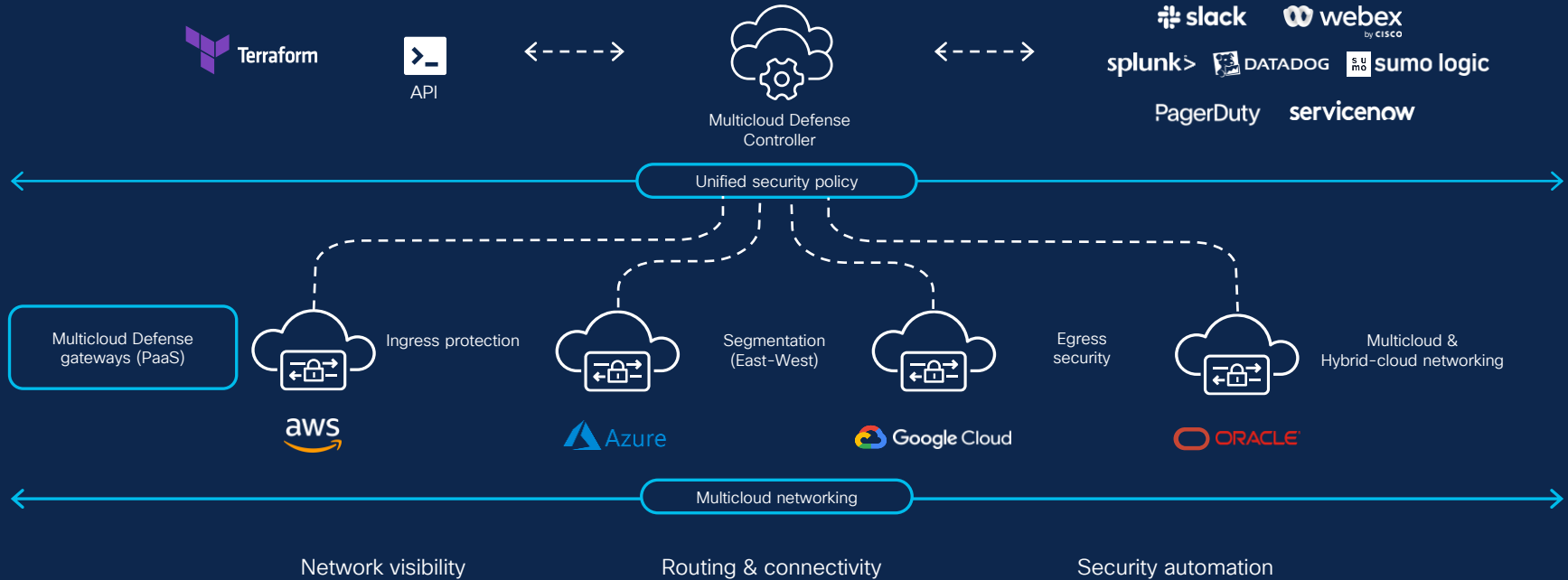
Site-to-Cloud

Ops visibility



Cisco Multicloud Defense

Combining multicloud **networking**, **automation**, and **cloud native network security**



Multicloud Defense customer feedback

“Provisioning time went from failure in hours, to success in minutes”

“Infrastructure cost reduction based on architecture and different failover methodology”

Sr. Director of Cloud, Leading Data Platform Company

“Very pleased with your ability to handle our shared infrastructure architecture for centralized protection”

Cloud Security Architect, Fortune 50 Financial Services Company

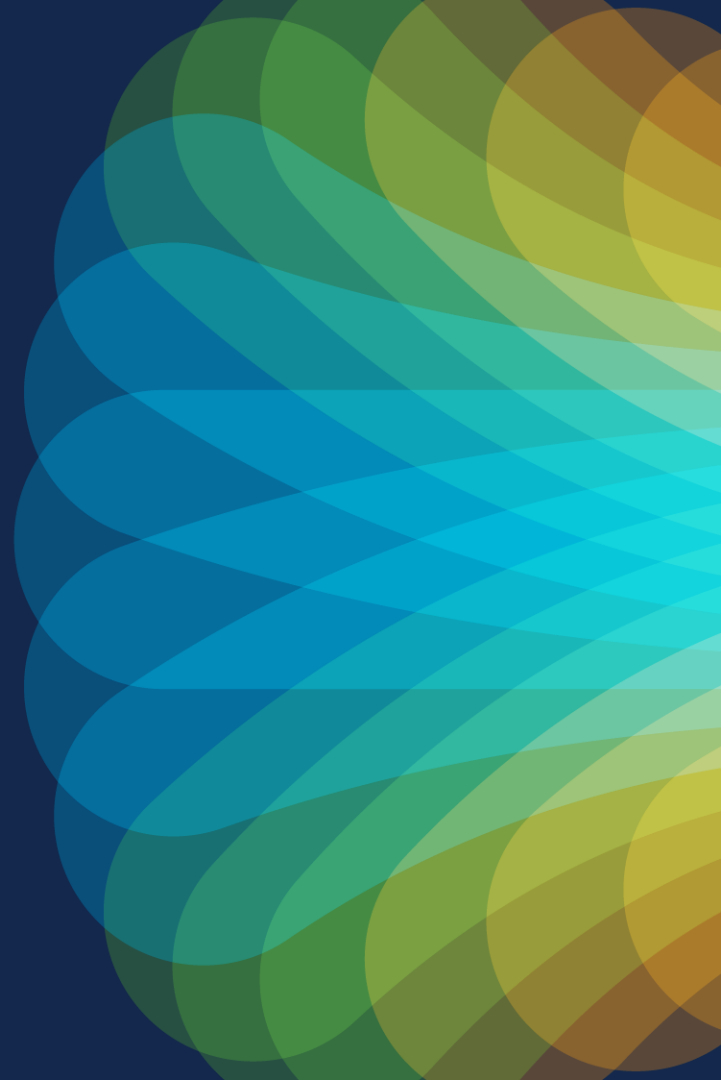
“What we just achieved in the last hour, is more than what we’ve been able to achieve in the past two years with AWS Firewall”

Cloud Architect, Fortune 500 Financial Services Company

“This is way faster. Minutes versus it would take us 20 days with our current Checkpoint Virtual Appliances.”

Global Cloud Architect, Global Retail Food Manufacturer

Cisco Multicloud Defense Use-cases



Critical Use Cases For Network Security Of Cloud Workloads



Ingress
protection



Egress
security



Segmentation

Why Critical?

Stop inbound threats for web and non-web apps

Block Command & Control, Botnets, Data Exfiltration

Mitigate Lateral Movement

Market Drivers

- Supply Chain Vulnerabilities
- Library Exploits (Log4Shell)
- Compliance

- Zero Days
- C2, Ransomware
- Compliance

- Zero Trust / Least Privilege
- Data Protection
- Compliance

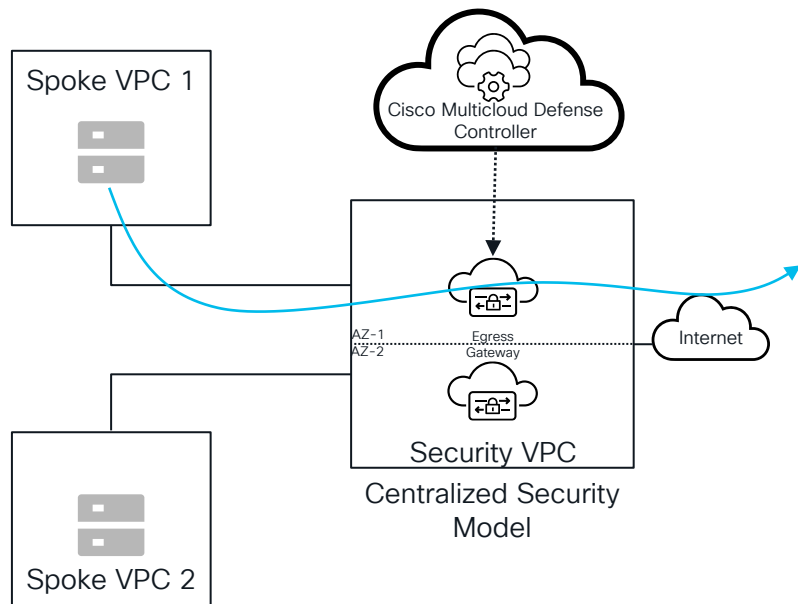
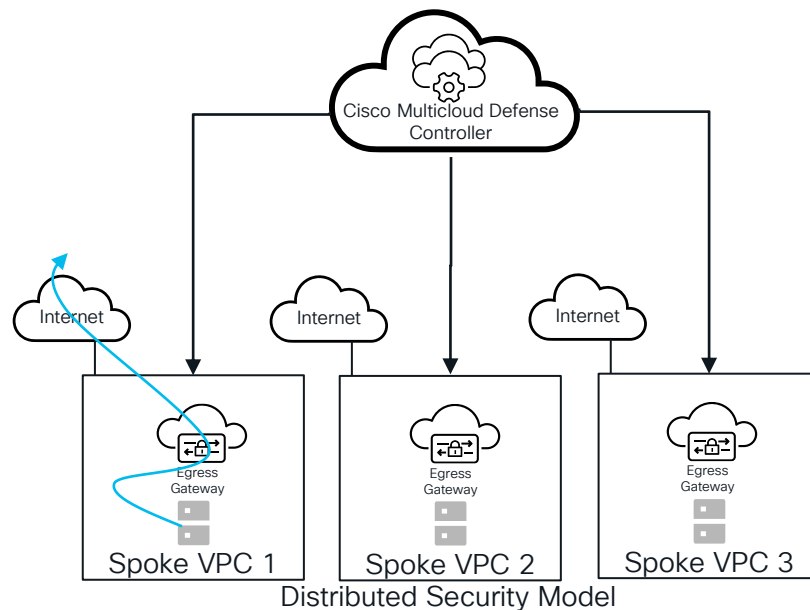
Security Controls

- ✓ WAF
- ✓ IDS / IPS
- ✓ Geo IP
- ✓ Malicious IP
- ✓ Antivirus

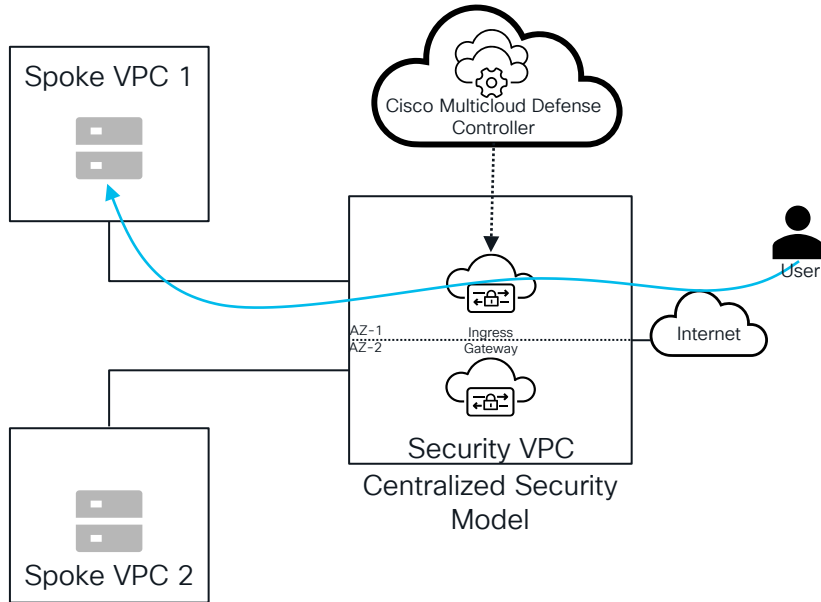
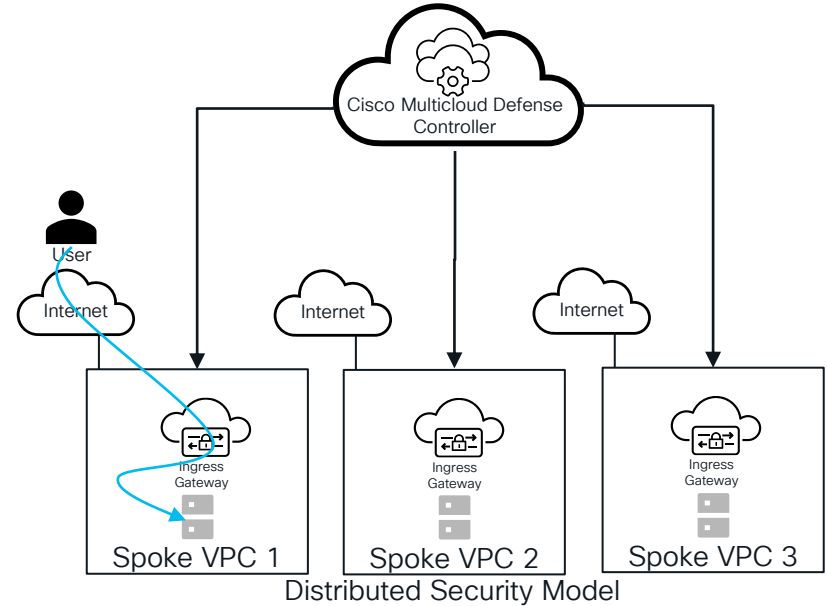
- ✓ FQDN Filtering
- ✓ URL Filtering
- ✓ DLP
- ✓ IPS / IDS
- ✓ Antivirus

- ✓ Cloud-native Identity
- ✓ IPS / IDS
- ✓ Antivirus

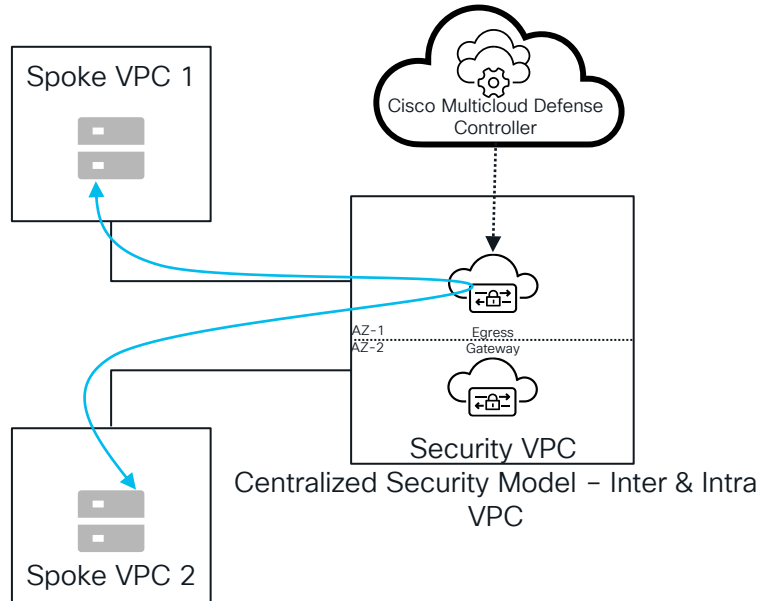
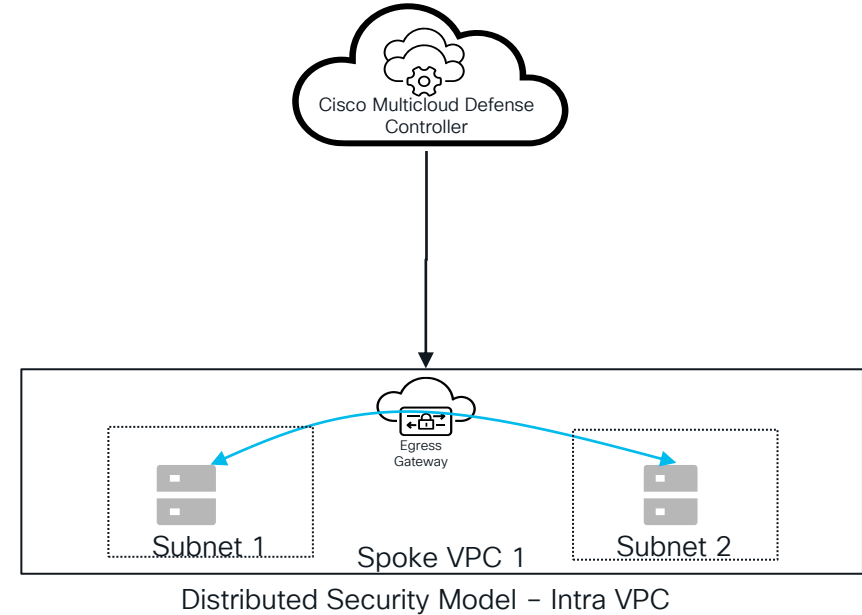
Egress



Ingress

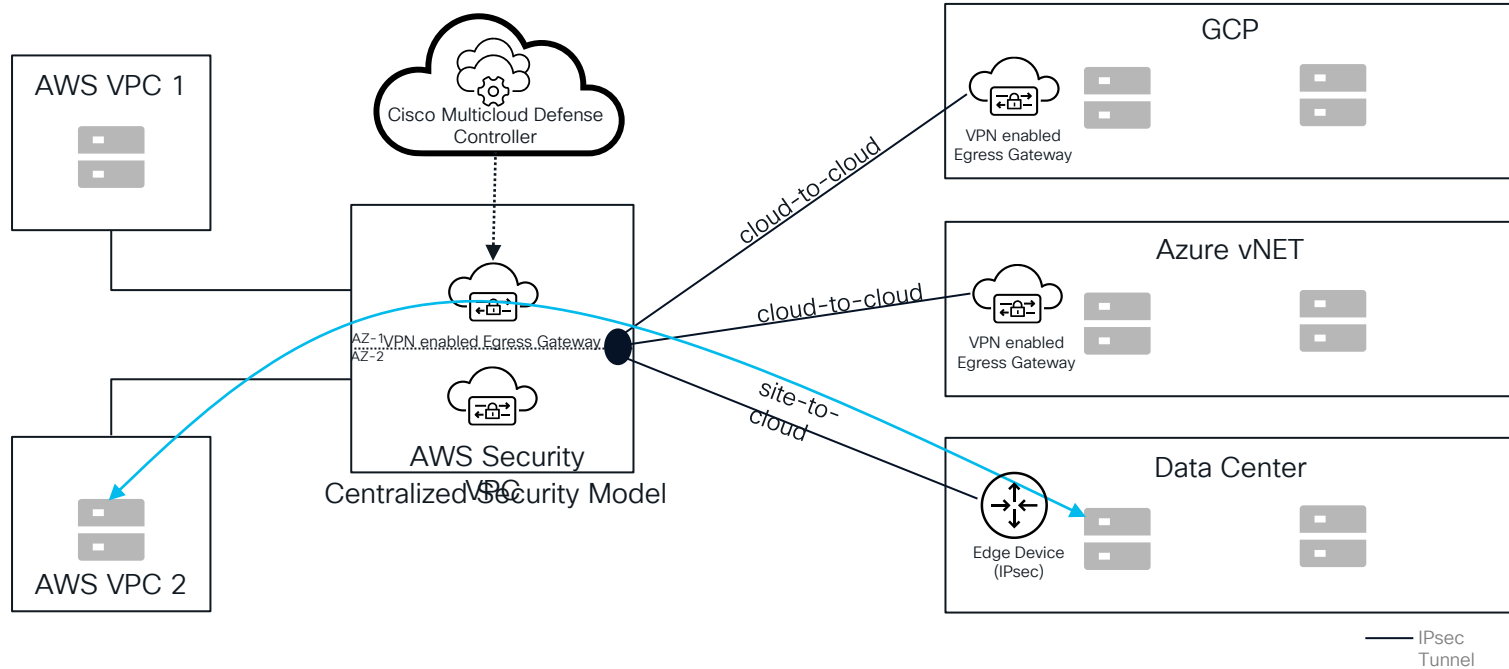


East-West Segmentation



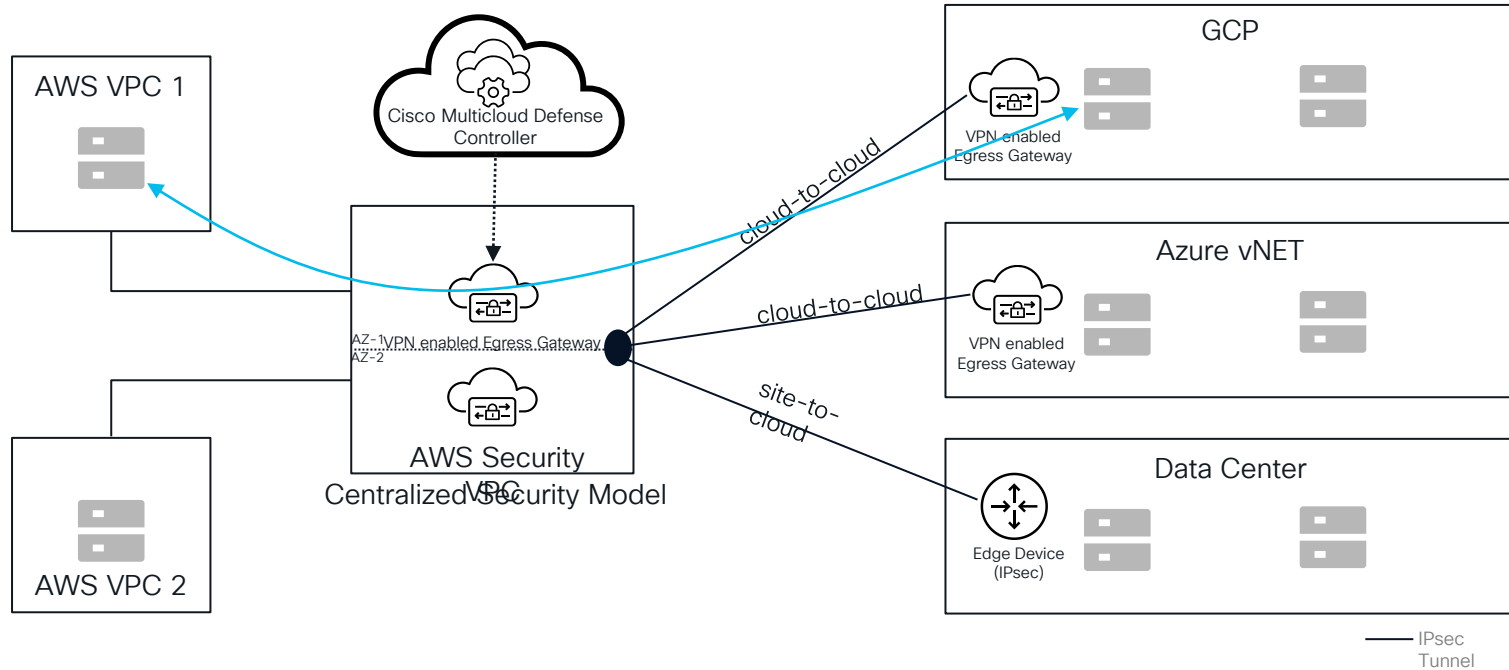
Multicloud Connectivity

site-to-cloud

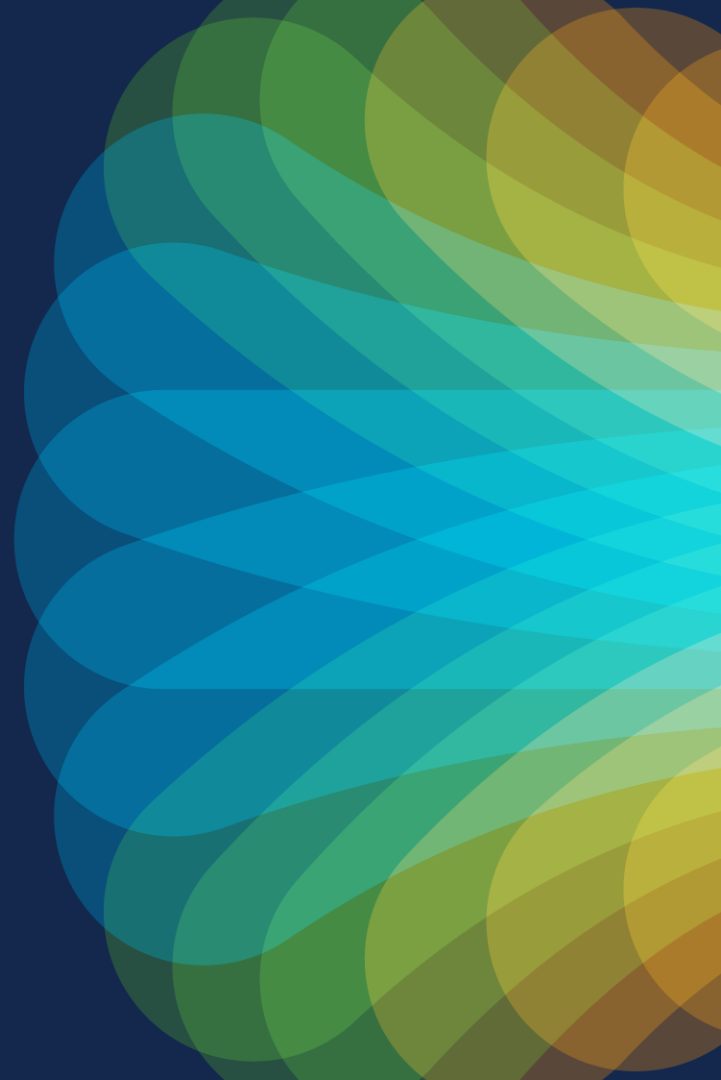


Multicloud Connectivity

cloud-to-cloud



Cisco Multicloud Defense Protection Models

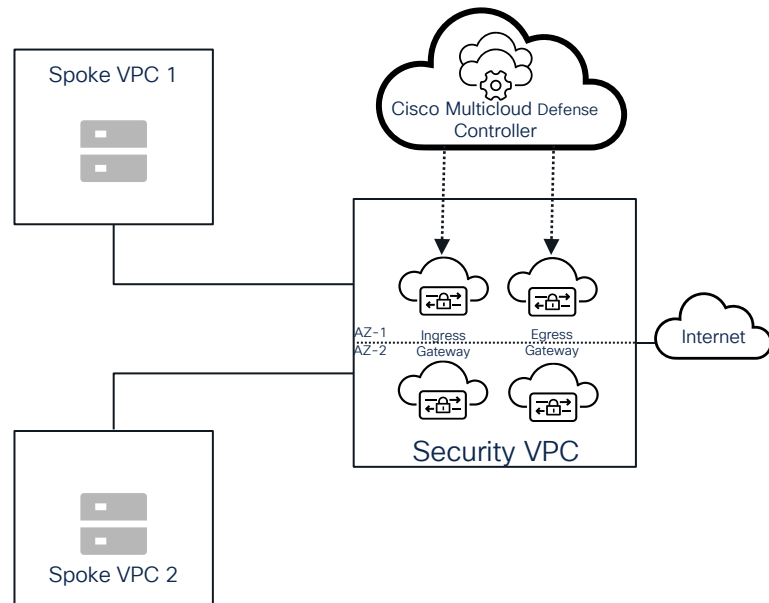


CISCO *Live!*



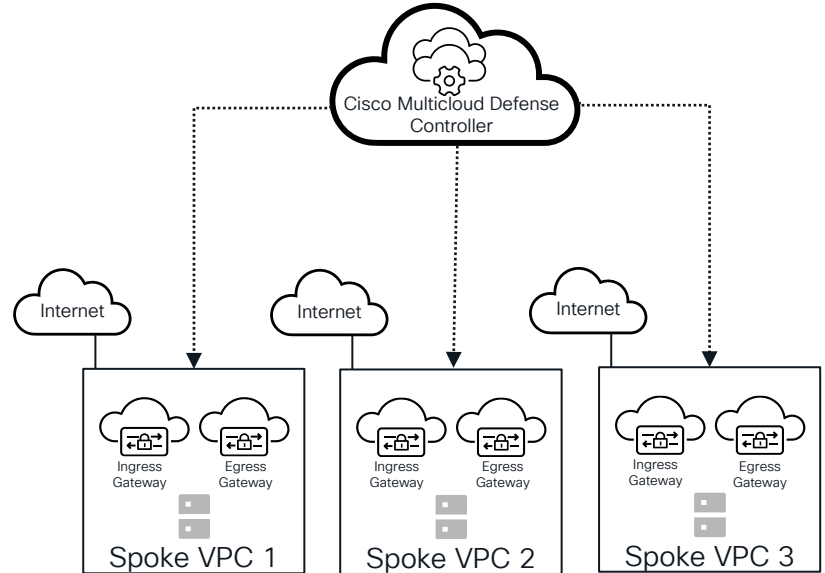
Centralized Protection Model

- Fully orchestrated and managed Security VPC/VNet
- Gateways are deployed in the security VPC/VNet
 - Self-healing, auto-scaling
 - Multi-zone for high availability
- Type of Multicloud Defense Gateways
 - Ingress (Inbound traffic)
 - Egress (Egress & East-West traffic)
- SaaS-based controller of Gateway lifecycle management for a true cloud-native aaS experience Ingress (Inbound traffic)
 - Instantiation, scalability, reliability, upgrade, management, hitless signature update
- No out-of-band configuration is needed on Gateways
- Multicloud Defense Gateway is available for AWS, Azure, GCP and OCI



Distributed Protection Model

- Gateways are deployed in spoke VPC/VNet
 - Self-healing, auto-scaling
 - Multi-zone for high availability
- Type of Multicloud Defense Gateways
 - Ingress (Inbound traffic)
 - Egress (Egress & E/W traffic)
- SaaS-based controller of Gateway lifecycle management for a true cloud-native aaS experience
 - Instantiation, scalability, reliability, upgrade, management, hitless signature update
- No out-of-band configuration is needed on Gateways
- Multicloud Defense Gateway is available for AWS, Azure, GCP and OCI



Fully Orchestrated



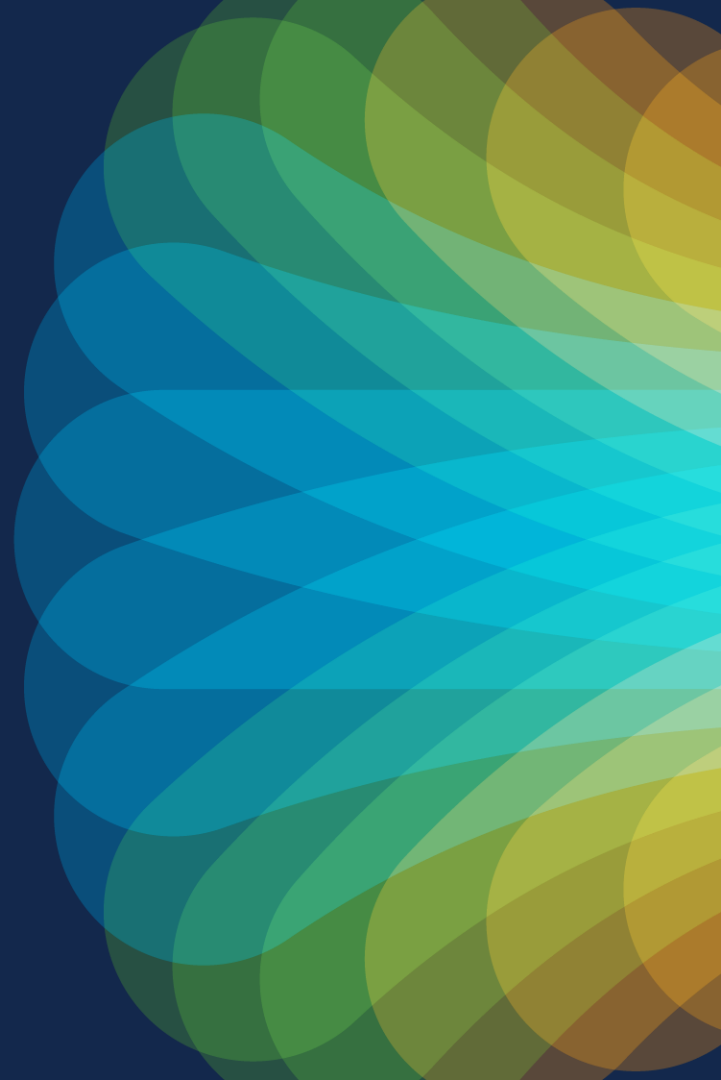
{ REST:API }

```
EXPLORER
├── CISCOMCD-DEPLOY
│   ├── ciscomcd
│   │   ├── ciscomcd_gateway.tf
│   │   ├── ciscomcd_policy_rule_set.tf
│   │   ├── ciscomcd_service_vpc.tf
│   │   ├── ciscomcd_spoke_vpc.tf
│   │   ├── outputs.tf
│   │   ├── provider.tf
│   │   ├── variables.tf
│   │   ├── .gitignore
│   │   ├── account1-us-east-1.tfvars
│   │   ├── ciscomcd-deploy.sh
│   │   ├── main.tf
│   │   ├── provider.tf
│   │   ├── README.md
│   │   └── variables.tf
│   └── ciscomcd_gateway.tf
└── ciscomcd_deploy.sh
```

```
1 # Cisco MCD Terraform Documentation
2 # https://registry.terraform.io/providers/cisco/ciscosecurity/ciscosecurity/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 "ciscosecurity_gateway" "ingress_gateway" {
10   name = var.ciscosecurity_ingress_gateway_name
11   csp_account_name = var.ciscosecurity_aws_account_name
12   gateway_image = var.ciscosecurity_ingress_gateway_version
13   instance_type = var.ciscosecurity_ingress_gateway_instance_type
14   mode = "HUB"
15   security_type = var.ciscosecurity_ingress_gateway_security_type
16   policy_rule_set_id = ciscosecurity_policy_rule_set.ingress_policy_rule_set_id
17   # policy_rule_set_id = data.ciscosecurity_policy_rule_set.ingress_policy_rule_set_id
18   ssh_key_pair = var.ciscosecurity_ingress_gateway_ssh_key_pair
19   aws_iam_role_firewall = var.ciscosecurity_firewall_role_name
20   region = var.aws_account_region
21   vpc_id = ciscosecurity_service_vpc.service_vpc_id
22   min_instances = var.ciscosecurity_ingress_gateway_autoscale_min
23   max_instances = var.ciscosecurity_ingress_gateway_autoscale_max
24   gateway_state = var.ciscosecurity_ingress_gateway_status
25   # settings {
26   #   name = "controller.use_internal_lb"
27   #   value = var.ciscosecurity_ingress_gateway_internal_lb
28   # }
29
30 }
```

```
POST {{baseURL}}/api/v1/gateway/run...
Body
1 {
2   "common": {
3     "acctName": "[[acctName]]",
4     "source": "RESTAPI",
5     "clientVersion": "CiscoMCD-2022"
6   },
7   "gateway": {
8     "cspAcctName": "AWS-Account3",
9     "name": "aws-egress-gw",
10    "description": "AWS EDGE Gateway",
11    "mode": "EDGE",
12    "type": "CLUSTER",
13    "minInstances": 1,
14    "maxInstances": 1,
15    "healthCheckPort": 65534,
16    "policyRuleSetId": 20,
17    "flags": {}
18  },
19  "settings": [
20    {
21      "name": "gateway.aws.ebs.encryption.key.default"
22    },
23    {
24      "name": "controller.gateway.assign_public_ip",
25      "value": "true"
26    },
27    {
28      "name": "gateway.fqdn_ip_cache.entry_ttl",
29      "value": "300"
30    }
31  ]
32 }
```

Cisco Multicloud Defense Deployment Architectures



AWS

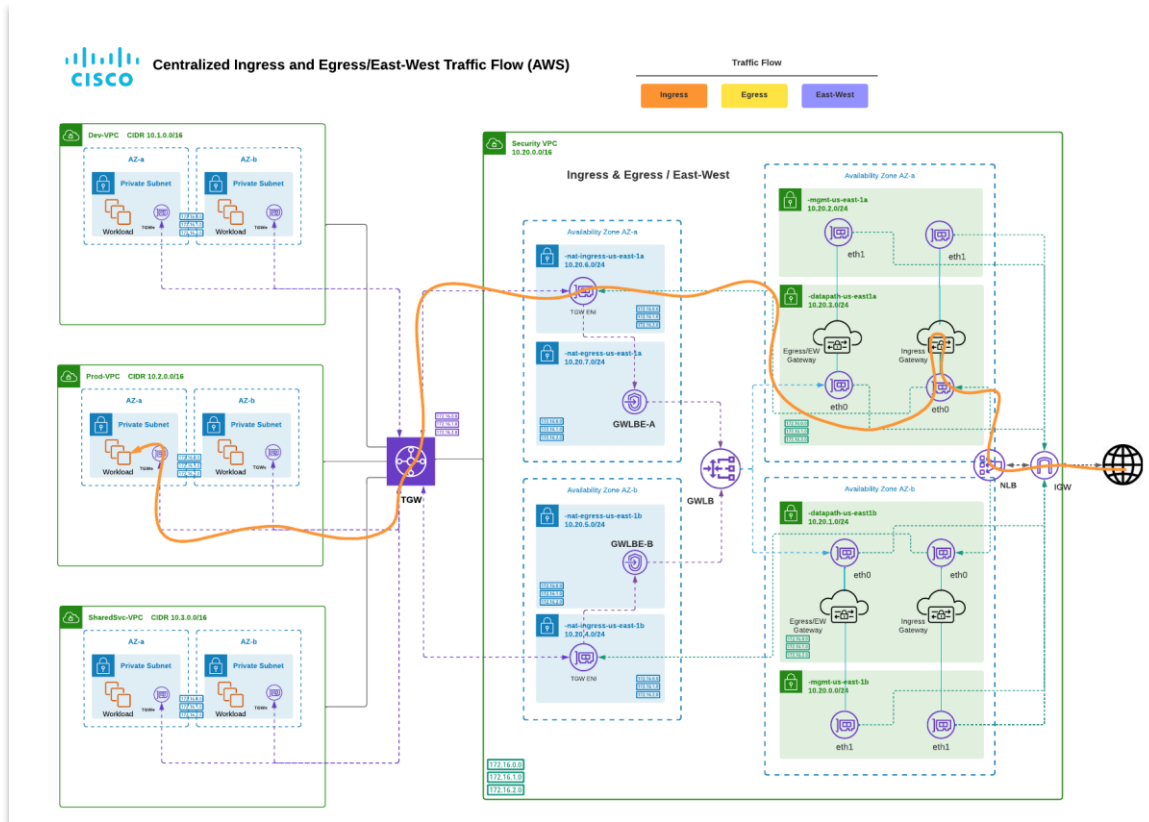
AWS Centralized Ingress

Overview

- Security VPC
- AWS Transit Gateway (TGW)
- Network Load Balancer (NLB) for Ingress traffic
- Ingress Gateways for traffic inspection

Orchestration

- Security VPC
- Network Load Balancer
- Multicloud Defense Gateways
 - Deployment
 - Insertion
 - Autoscaling
- AWS Transit Gateway
 - New or existing TGW
 - TGW attachment
 - Traffic engineering (routing)
- VPC subnet routing to TGW



AWS Centralized – Ingress traffic inspection

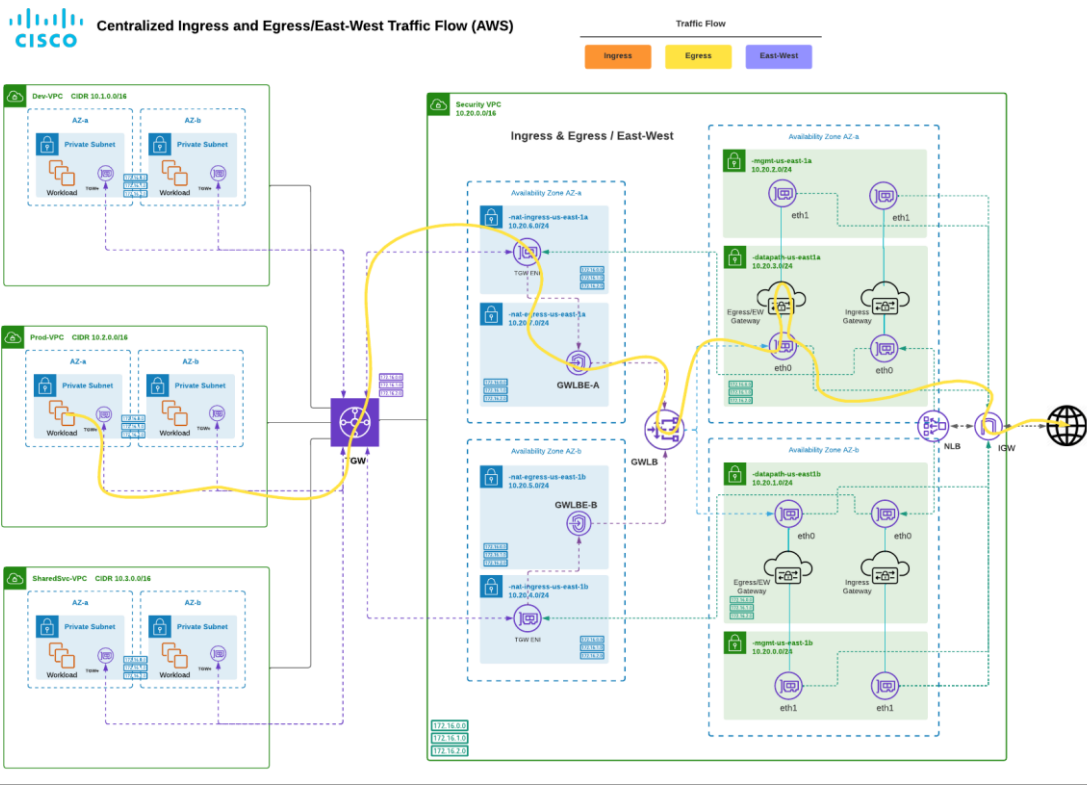
AWS Centralized Egress

Overview

- Security VPC
- AWS Transit Gateway (TGW)
- Gateway Load Balancer (GWLB) for Egress traffic
- Gateway Load Balancer Endpoint
- Egress / East-West Gateway for traffic inspection

Orchestration

- Security VPC
- Gateway Load Balancer (GWLB)
- Multicloud Defense Gateways
 - Deployment
 - Insertion
 - Autoscaling
- AWS Transit Gateway
 - New or existing TGW
 - TGW attachment
 - Traffic engineering (routing)
- VPC subnet routing to TGW



AWS Centralized – Egress traffic inspection

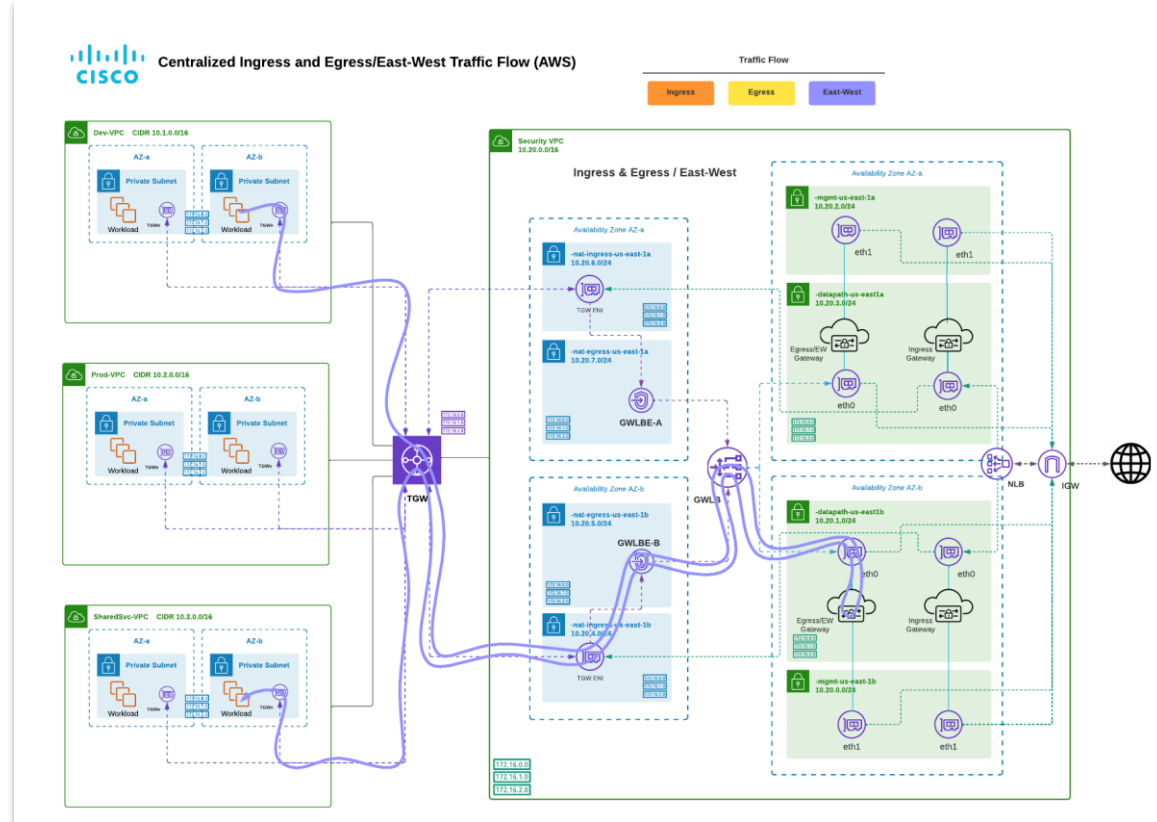
AWS Centralized East/West (Inter VPC)

Overview

- Security VPC
- AWS Transit Gateway (TGW)
- Gateway Load Balancer (GWLB) for EW traffic
- Gateway Load Balancer Endpoint
- Egress / East-West Gateway for traffic inspection

Orchestration

- Security VPC
- Multicloud Defense Gateways
 - Deployment
 - Insertion
 - Autoscaling
- AWS Transit Gateway
 - New or existing TGW
 - TGW attachment
 - Traffic engineering (routing)
- AWS GWLB for scalability
- VPC subnet route to TGW



AWS Centralized – East/West traffic inspection

AWS Centralized

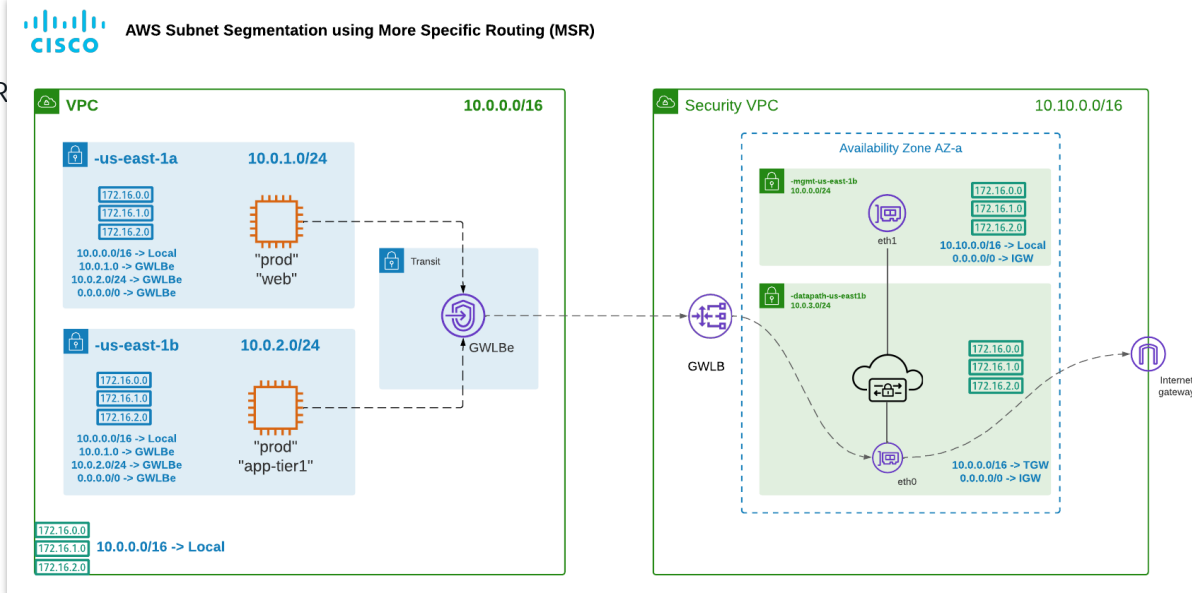
East-West – Intra VPC

Overview

- Uses AWS More Specific Routing (MSR)
- Security VPC
- Egress / East-West Gateway
- Gateway Load Balancer (GWLBe)

Orchestration

- Security VPC
- Multicloud Defense Gateways
 - Deployment
 - Insertion
 - Autoscaling
- VPC subnet route



AWS Centralized – East/West (Intra VPC)

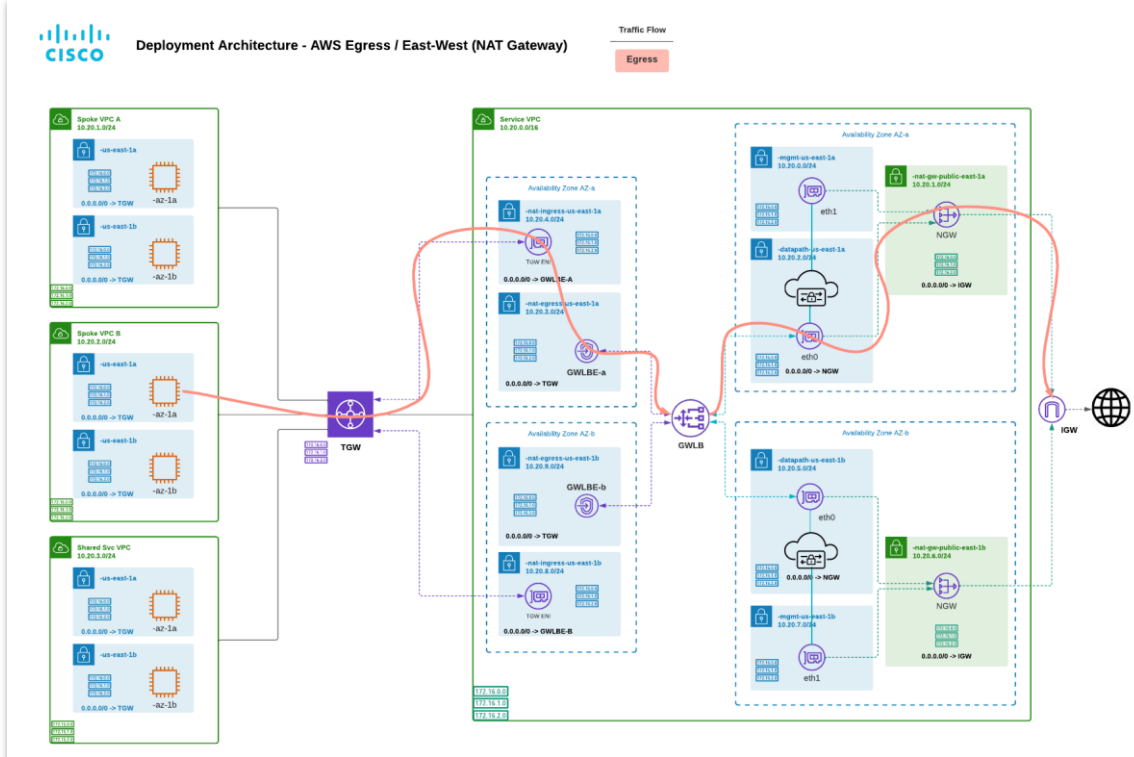
AWS Centralized Egress & East/West (NAT GW)

Overview

- Security VPC
- AWS Transit Gateway (TGW)
- Gateway Load Balancer (GWLB) for Egress / East-West traffic flow
- NAT Gateway for outbound traffic
- Egress / East-West Gateway traffic inspection

Orchestration

- Security VPC
- Multicloud Defense Gateways
 - Deployment
 - Insertion
 - Autoscaling
- AWS Transit Gateway
 - New or existing TGW
 - TGW attachment
 - Traffic engineering (routing)
- VPC subnet route to TGW
- NAT Gateway



AWS Centralized Egress & East/West (NAT GW)

AWS Centralized GWLB based Ingress / Egress

Overview

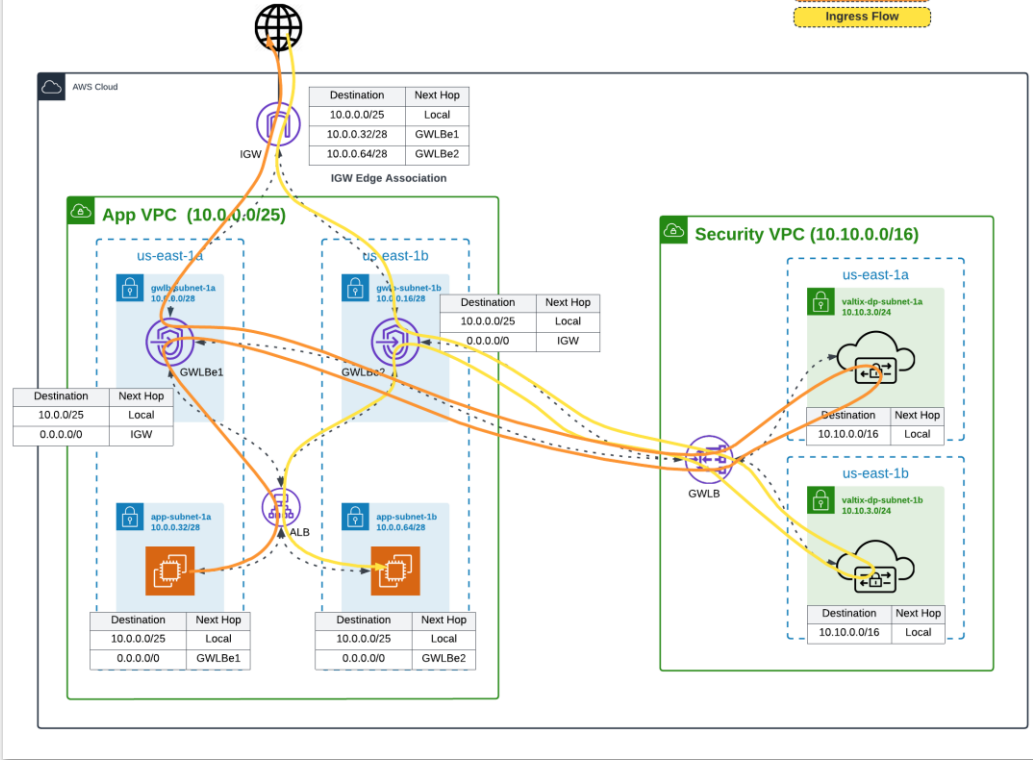
- Security VPC
- Transit Gateway
- Egress / East-West Gateway
- Gateway Load Balancer (GWLB) for Ingress and Egress traffic flow
- Gateway Load Balancer Endpoint
- NAT Gateway

Orchestration

- Security VPC
- Multicloud Defense Gateways
 - Deployment
 - Insertion
 - Autoscaling
- Transit Gateway
 - New or existing TGW
 - TGW attachment
 - Traffic engineering (routing)
- VPC subnet route to TGW



Reference Architecture - GWLB-based Ingress / Egress (AWS)



GWLB based Ingress / Egress traffic inspection

Azure

Azure Centralized Ingress

Overview

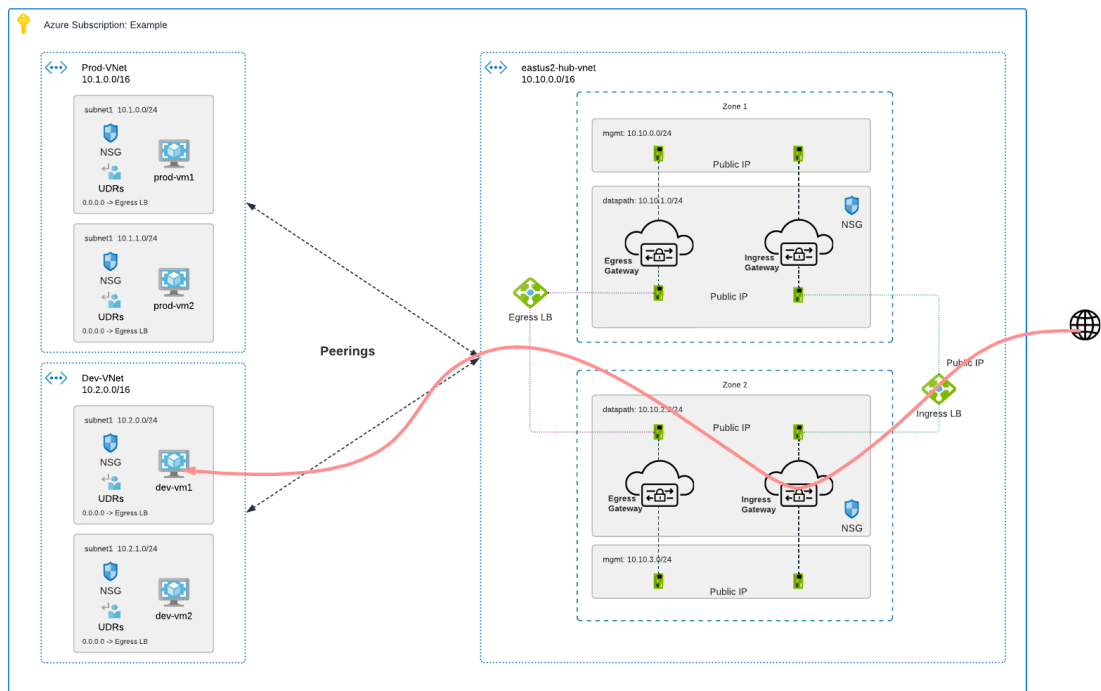
- Security VNet
- Ingress Gateway
- Internet-facing Load Balancer
- VNet Peering

Orchestration

- Security VNet
- Load Balancer
- Multicloud Defense Gateway
 - Ingress Gateway
- Automation
 - Peering
 - Routing
 - Load balancer configuration
 - Autoscaling



Architecture - Centralized (Azure)



Azure Centralized – Ingress Traffic Inspection

Azure Centralized Egress

Overview

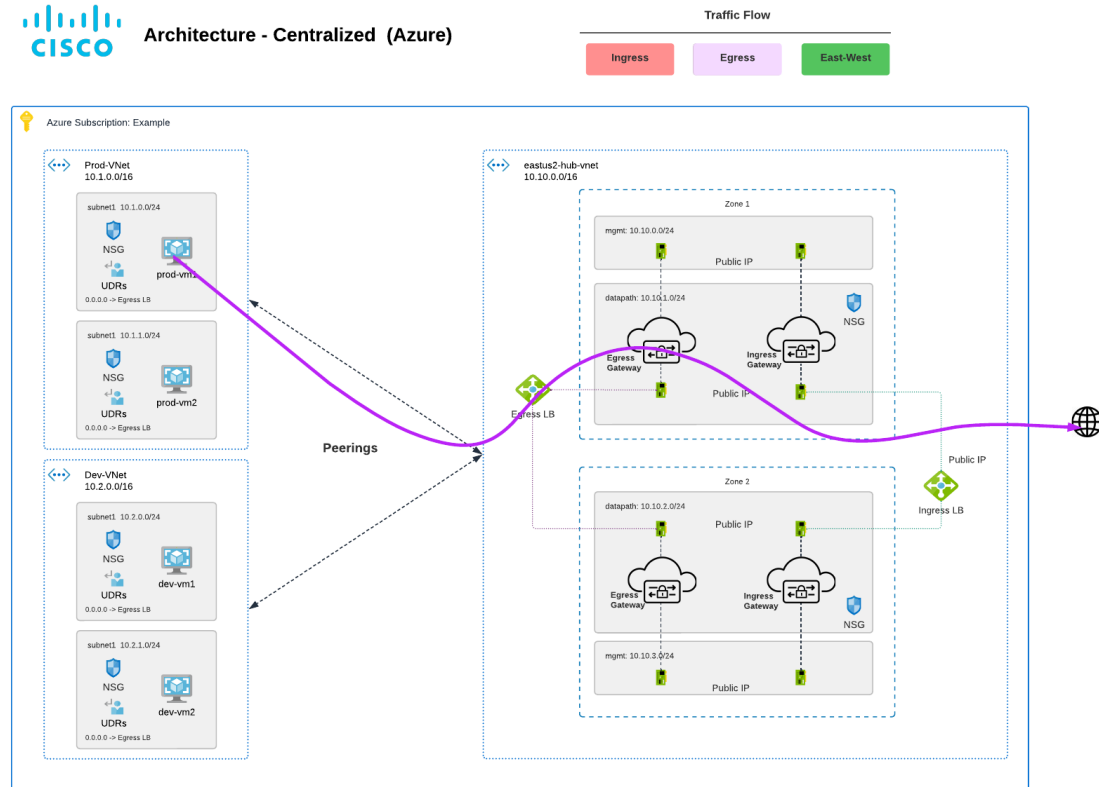
- Security VNet
- Egress / East-West Gateway
- Internal Load Balancer
- vNET Peering

Orchestration

- Security VNet
- Network Load Balancers
- Multicloud Defense Gateways
 - Egress / East-West Gateway
- Automation
 - Peering
 - Routing
 - Load balancer configuration
 - Autoscaling



Architecture - Centralized (Azure)



Azure Centralized – Egress Traffic Inspection

Azure Centralized East-West

Overview

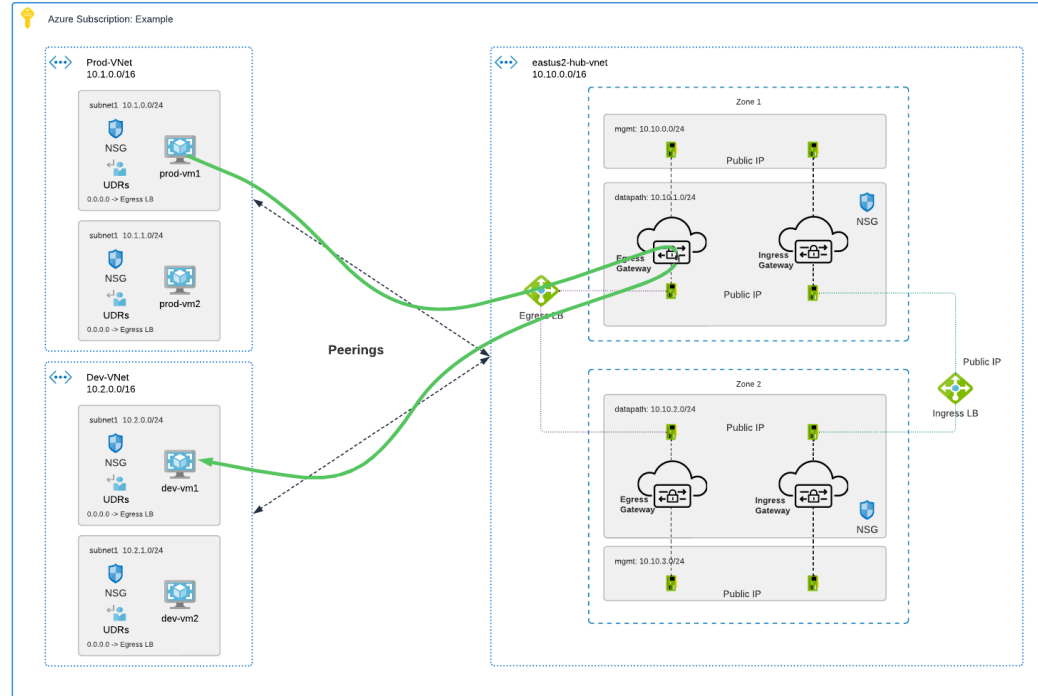
- Security VNet
- Egress / East-West Gateway
- Internal Load Balancer
- vNET Peering

Orchestration

- Security VNet
- Network Load Balancers
- Multicloud Defense Gateways
 - Egress / East-West Gateway
- Automation
 - Peering
 - Routing
 - Load balancer configuration
 - Autoscaling



Architecture - Centralized (Azure)



Azure Centralized – East-West Traffic Inspection

GCP

GCP Centralized Ingress

Overview

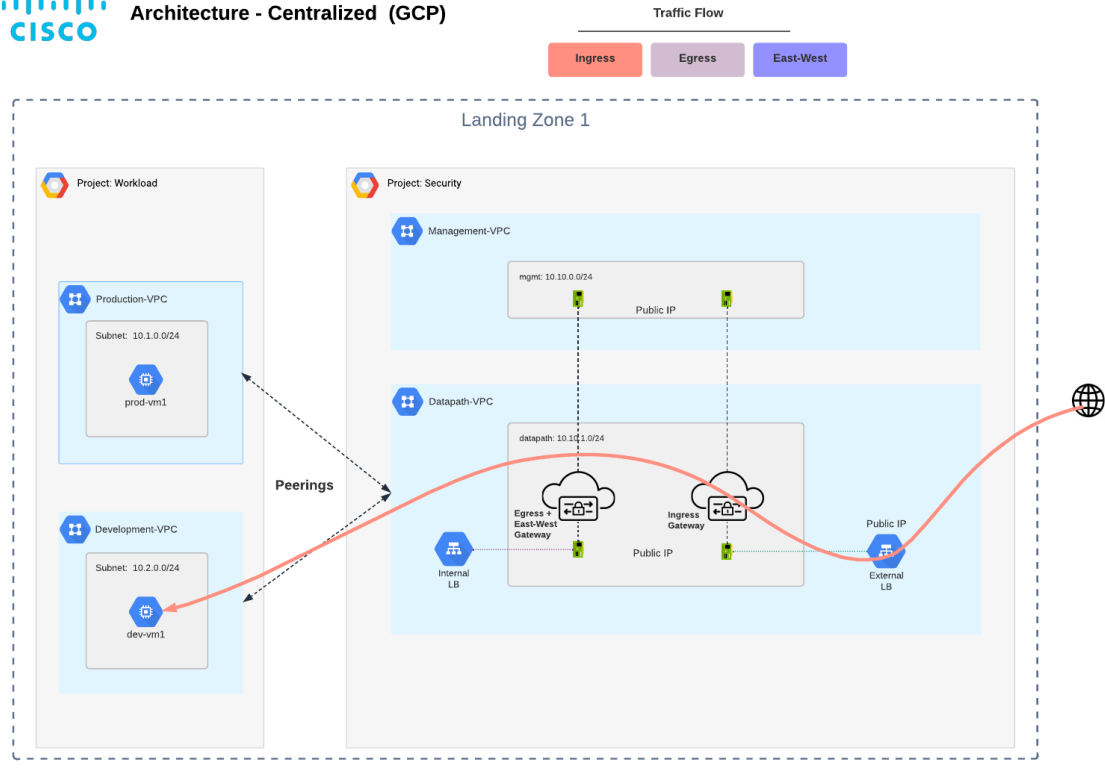
- Security VPC
- Ingress Gateway
- Internet Load Balancer
- VPC peering

Orchestration

- Security VPC
- Network Load Balancers
 - Internet
- Multicloud Defense Gateway
 - Ingress Gateway
- Automation
 - Peering
 - Routing
 - Load balancer configuration
 - Autoscaling



Architecture - Centralized (GCP)



GCP Centralized – Ingress Traffic Inspection

GCP Centralized Egress

Overview

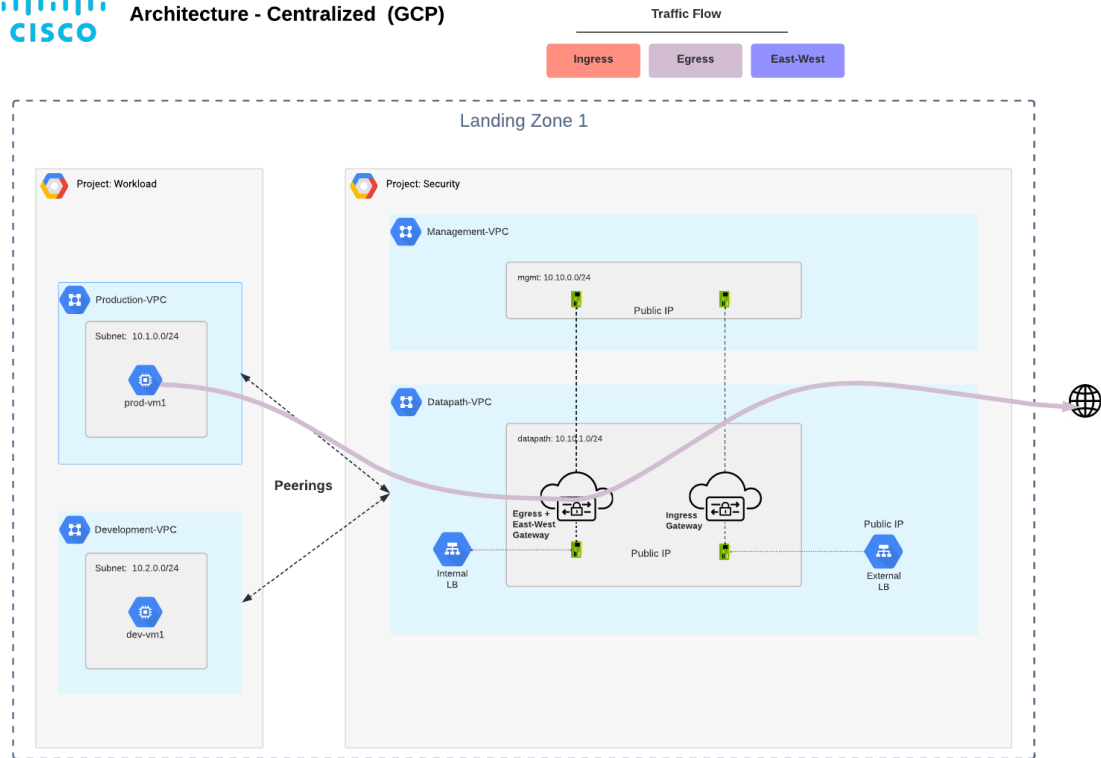
- Security VPC
- Egress Gateway
- Internal Load Balancer
- VPC peering

Orchestration

- Security VPC
- Network Load Balancers
 - Internal
- Multicloud Defense Gateway
 - Ingress Gateway
- Automation
 - Peering
 - Routing
 - Load balancer configuration
 - Autoscaling



Architecture - Centralized (GCP)



GCP Centralized – Egress Traffic Inspection

GCP Centralized East-West

Overview

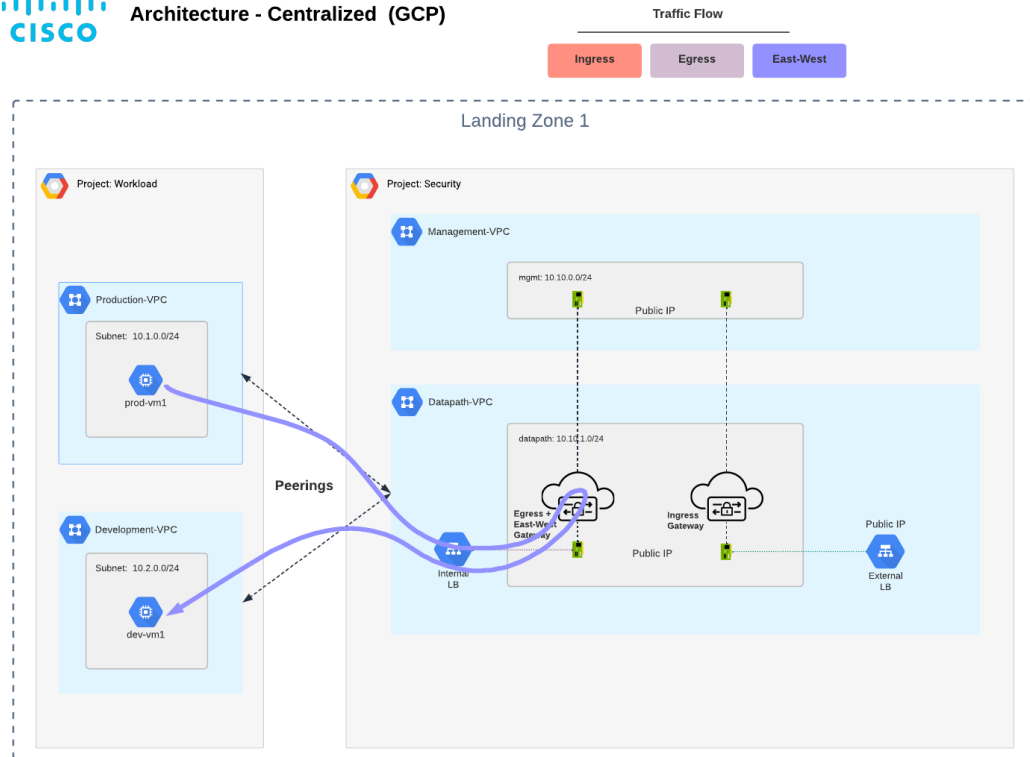
- Security VPC
- Egress Gateway
- Internal Load Balancer
- VPC peering

Orchestration

- Security VPC
- Network Load Balancers
 - Internal
- Multicloud Defense Gateway
 - Ingress Gateway
- Automation
 - Peering
 - Routing
 - Load balancer configuration
 - Autoscaling



Architecture - Centralized (GCP)



GCP Centralized – East-West Traffic Inspection

OCI

OCI Centralized Ingress

Overview

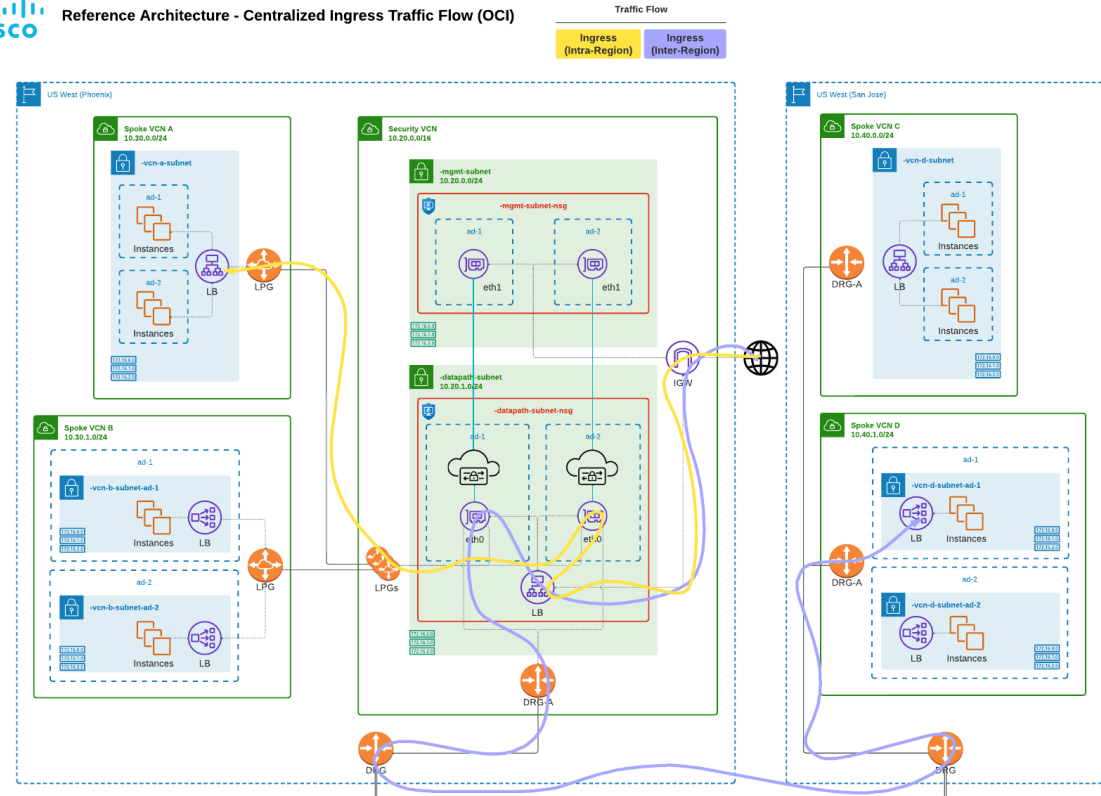
- Security VCN
- Ingress Gateway
- Internet Load Balancer
- LPG or DRG peering

Orchestration

- Security VNC
- Network Load Balancers
 - Internet
- Multicloud Defense Gateway
 - Ingress Gateway
- Automation
 - Load balancer configuration
 - Autoscaling



Reference Architecture - Centralized Ingress Traffic Flow (OCI)



OCI Centralized – Ingress Traffic Inspection

OCI Centralized Egress

Overview

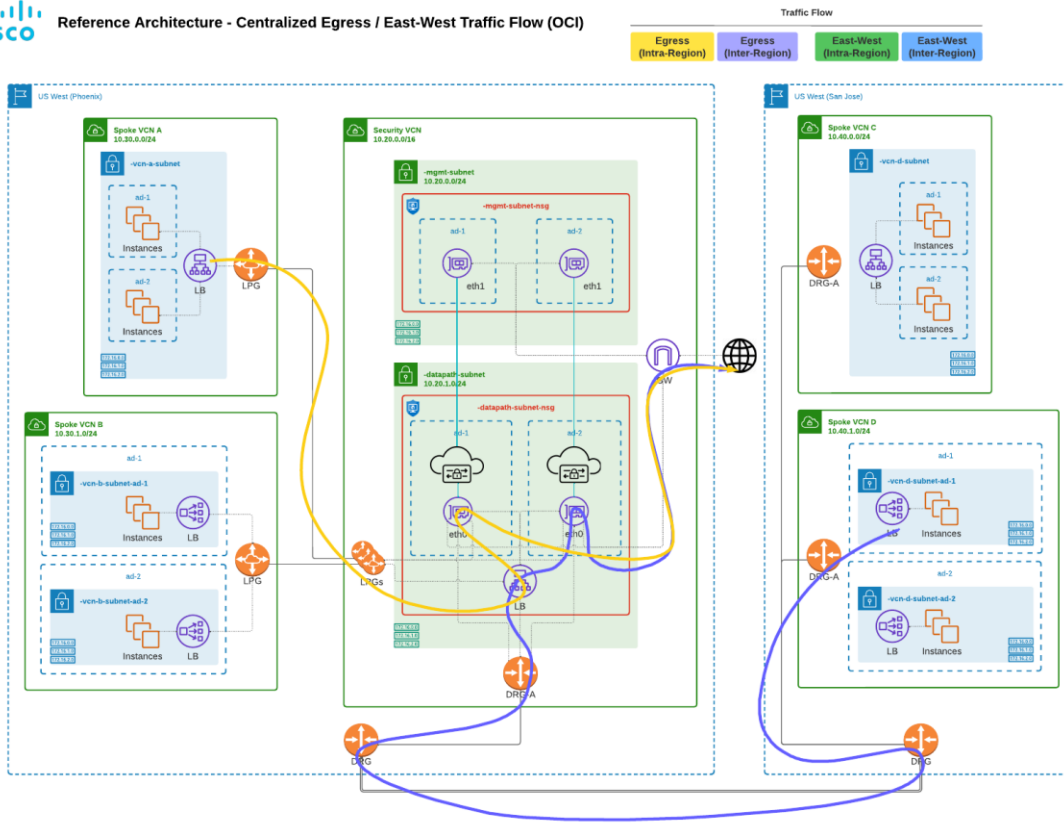
- Security VCN
- Egress / East-West Gateway
- Internal Load Balancer
- LPG or DRG peering

Orchestration

- Security VNC
- Network Load Balancers
 - Internal
- Multicloud Defense Gateway
 - Egress / East-West Gateway
- Automation
 - Load balancer configuration
 - Autoscaling



Reference Architecture - Centralized Egress / East-West Traffic Flow (OCI)



OCI Centralized – Egress Traffic Inspection

OCI Centralized East-West

Overview

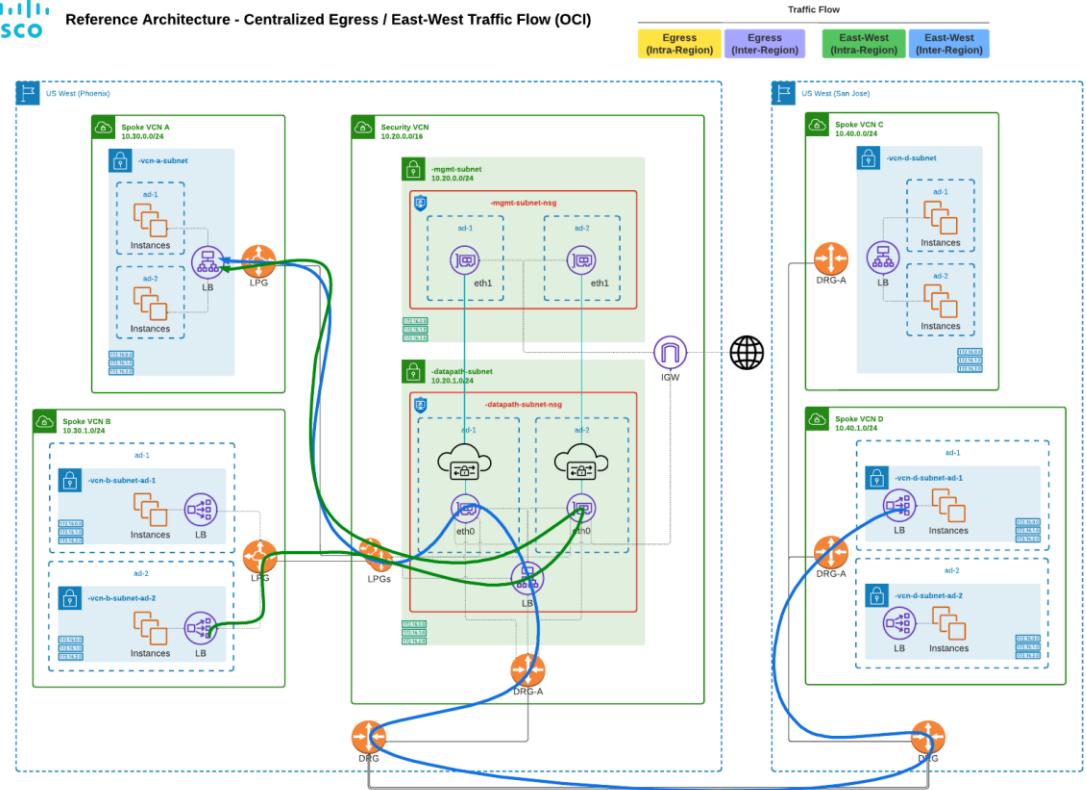
- Security VCN
- Egress / East-West Gateway
- Internal Load Balancer
- LPG or DRG peering

Orchestration

- Security VNC
- Network Load Balancers
 - Internal
- Multicloud Defense Gateway
 - Egress / East-West Gateway
- Automation
 - Load balancer configuration
 - Autoscaling

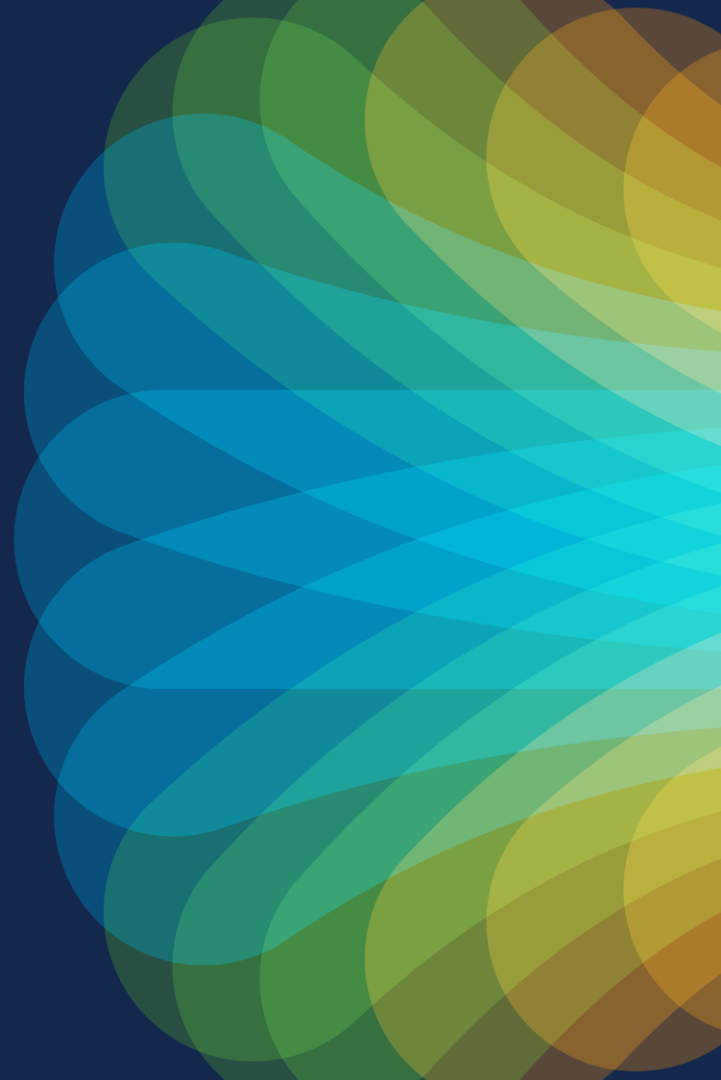


Reference Architecture - Centralized Egress / East-West Traffic Flow (OCI)



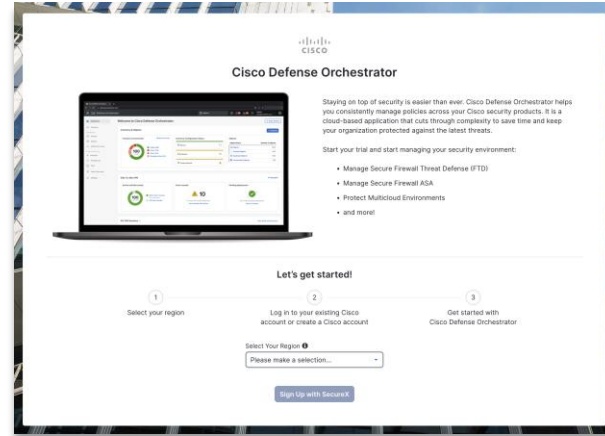
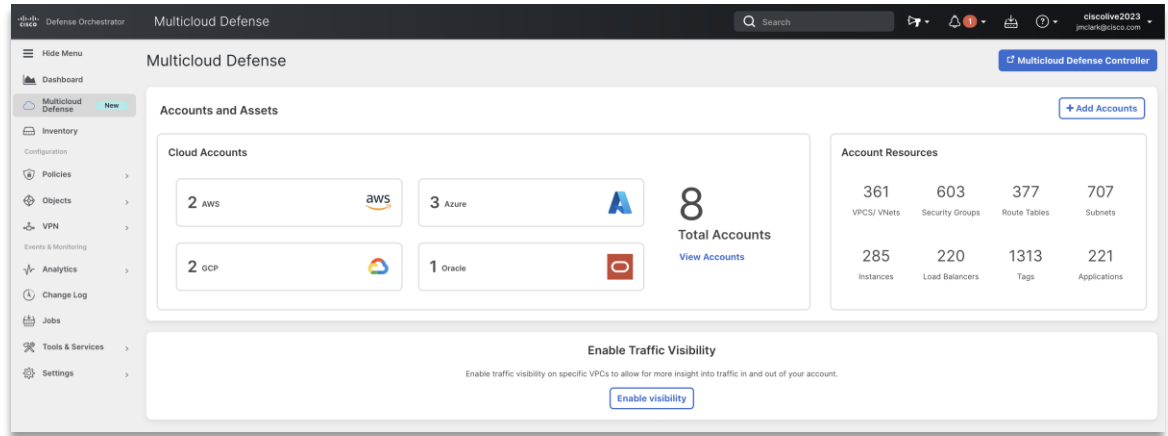
OCI Centralized - East-West Traffic Inspection

Cisco Multicloud Defense Access and Demo



How to access ...

- Not a CDO customer?
 - Go to getcdo.com
 - Establish a SecureX account
 - Setup MFA
 - Sign-in to CDO
 - Launch Multicloud Defense
- CDO customer!!
 - Sign-in to CDO
 - Launch Multicloud Defense



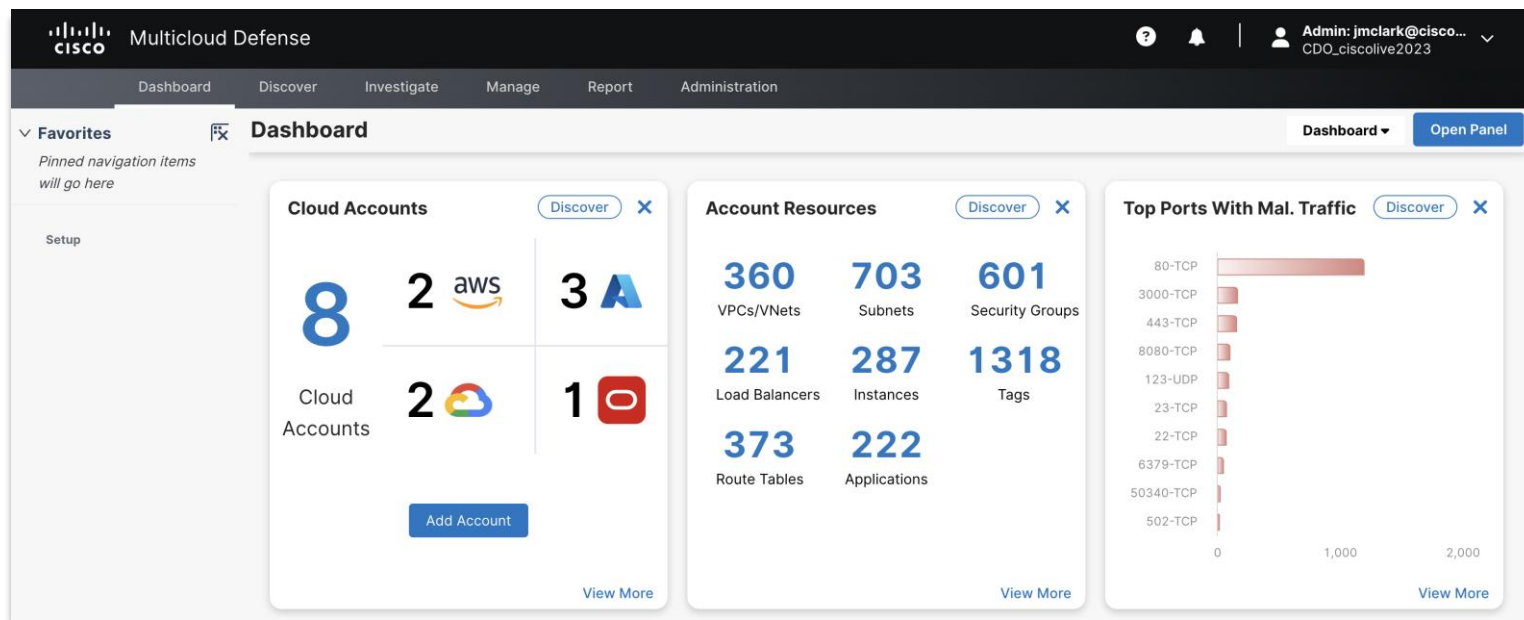
Multicloud Defense integration with Cisco Defense Orchestrator

The screenshot displays the Cisco Defense Orchestrator (CDO) interface for Multicloud Defense. The top navigation bar includes the Cisco logo, 'Defense Orchestrator', and 'Multicloud Defense'. A search bar and user profile 'ciscolive2023' are also present. The left sidebar contains a 'Hide Menu' button and a 'Dashboard' icon. The 'Multicloud Defense' menu item is highlighted with a red box. The main content area shows the 'Multicloud Defense' section with a '+ Add Accounts' button. Below this, the 'Accounts and Assets' section is visible, featuring a 'Cloud Accounts' grid with 8 total accounts (2 AWS, 3 Azure, 2 GCP, 1 Oracle) and an 'Account Resources' table. The 'Account Resources' table lists various resources and their counts: VPCS/ Vnets (360), Security Groups (601), Route Tables (373), Subnets (703), Instances (287), Load Balancers (221), Tags (1318), and Applications (222). At the bottom, there is a section to 'Enable Traffic Visibility' with a description and an 'Enable visibility' button.

Resource	Count
VPCS/ Vnets	360
Security Groups	601
Route Tables	373
Subnets	703
Instances	287
Load Balancers	221
Tags	1318
Applications	222

Seamlessly access Cisco Multicloud Defense from Cisco Defense Orchestrator portal

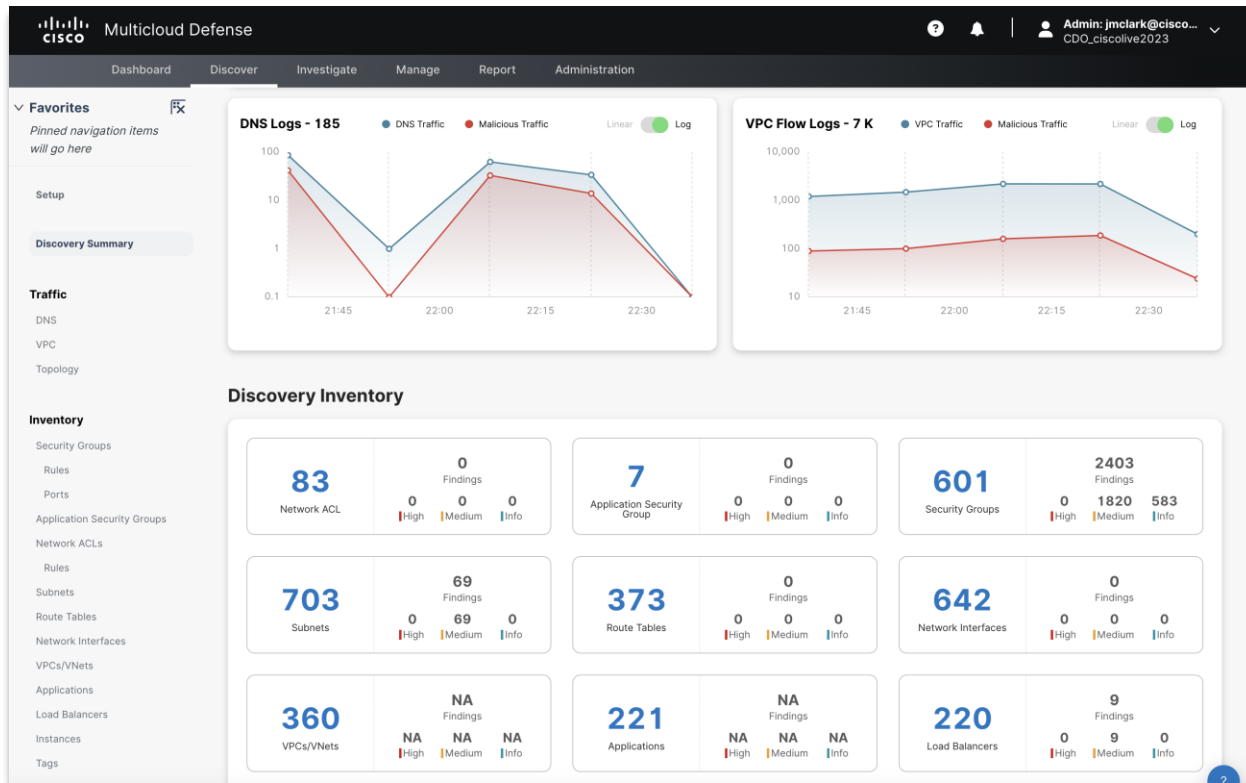
Multicloud Defense Dashboard



Discover, Deploy, and Defend

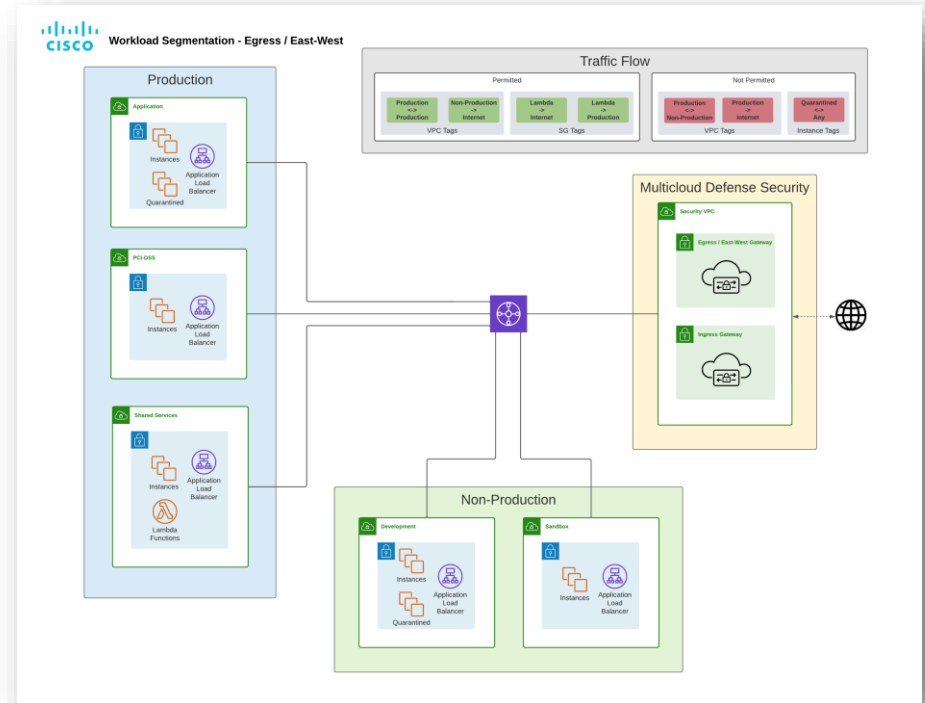
Orchestrator, manage, control and secure cloud infrastructure using Multicloud Defense

Multicloud Defense Dashboard



Demos

- Overview
 - Workflow
 - Topology
 - Policy
- Dynamic policy
 - Segmentation policy
 - VPCs, Instances and Security Groups
 - Cloud Native Tags
 - Advanced protection
 - FQDN, URL, IDS/IPS, and DLP



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



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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC