Cisco Multicloud Defense

~クラウドセキュリティの最前線~

シスコシステムズ合同会社
満江　貴之

Jul 2024

Agenda

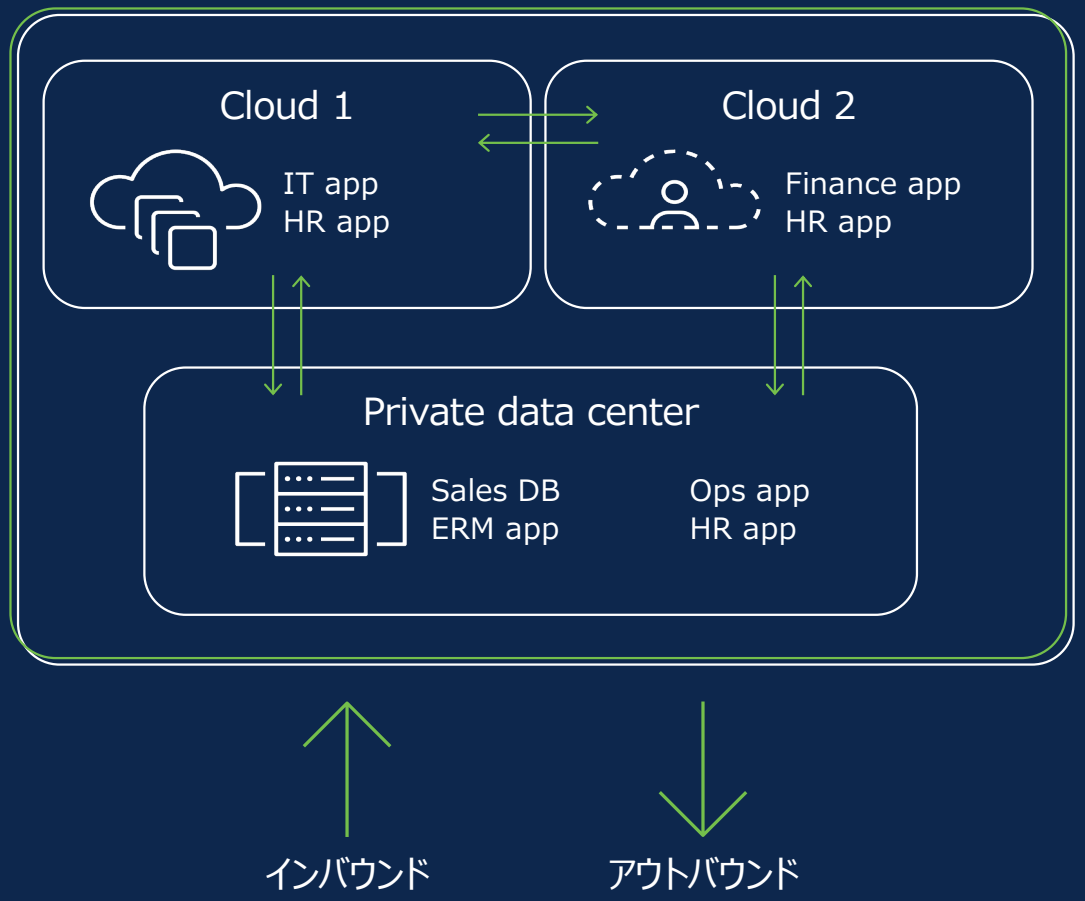
1. 背景と課題
2. 製品概要
3. デプロイメントデザインと各種機能
4. Demo
5. 料金体系
6. 最新アップデート機能

背景と課題

クラウド化がもたらすネットワークの継続的な変化

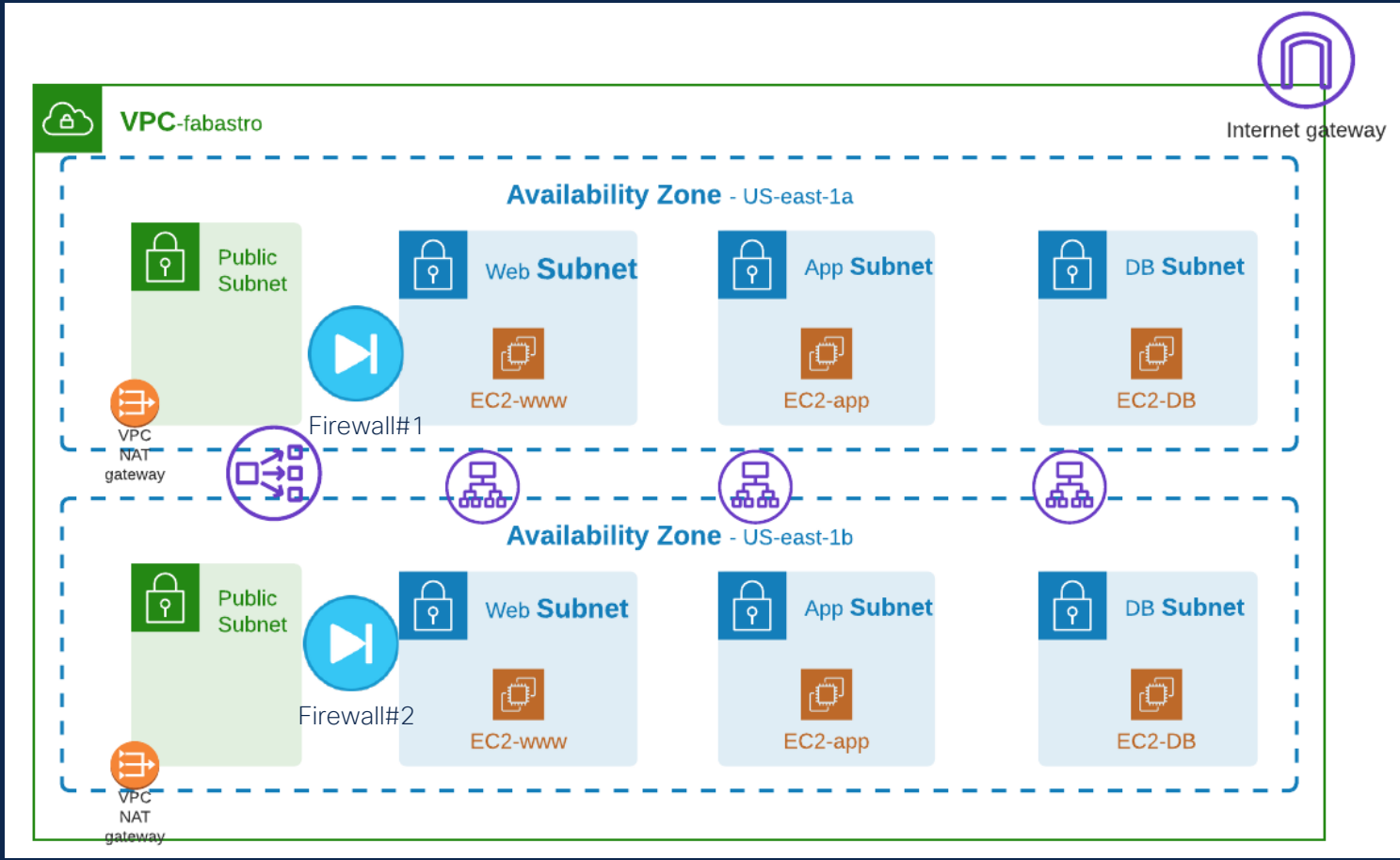
82% のITリーダーがハイブリッドクラウドアーキテクチャを採用している[1]

58% の組織が２つまたは３つのパブリックIaaSクラウドを利用[1]

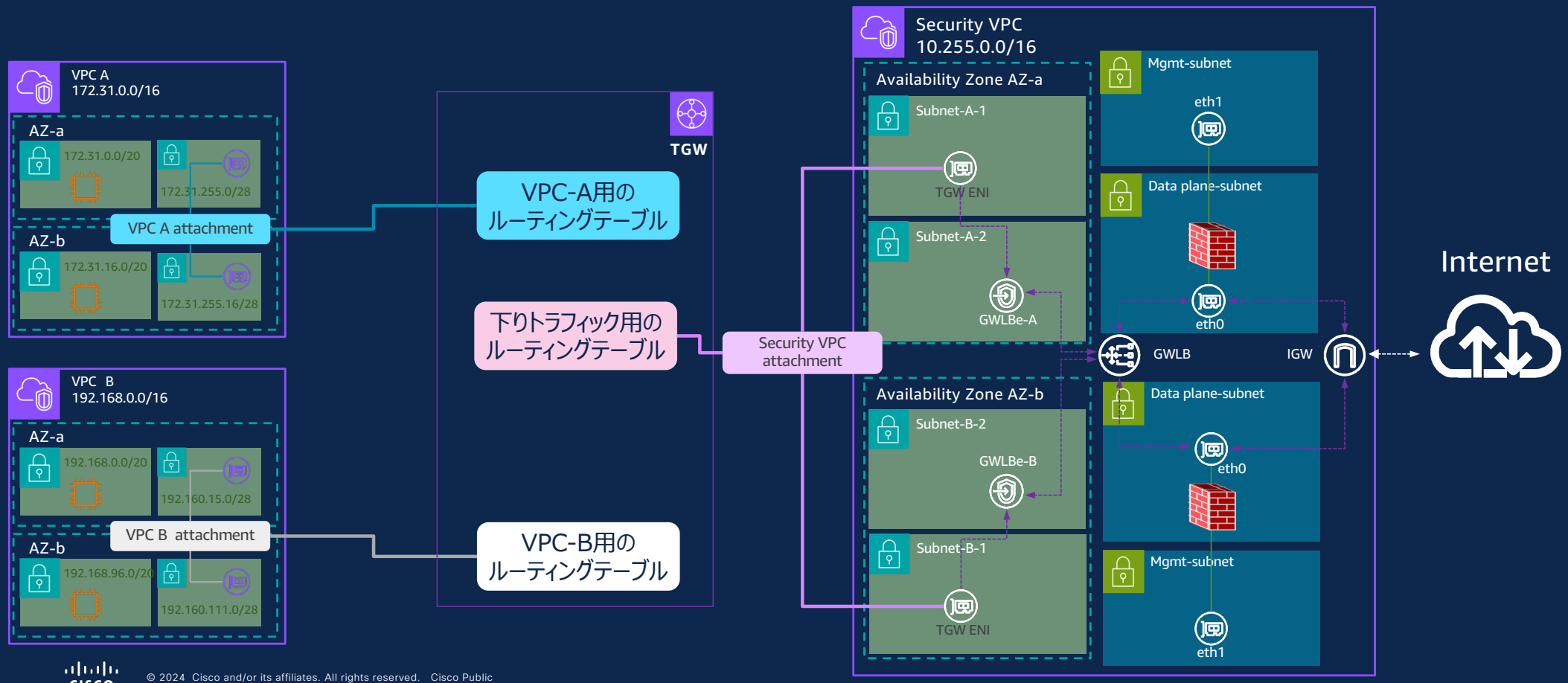


[1] 2022 Cisco Global Hybrid Cloud Trends Report

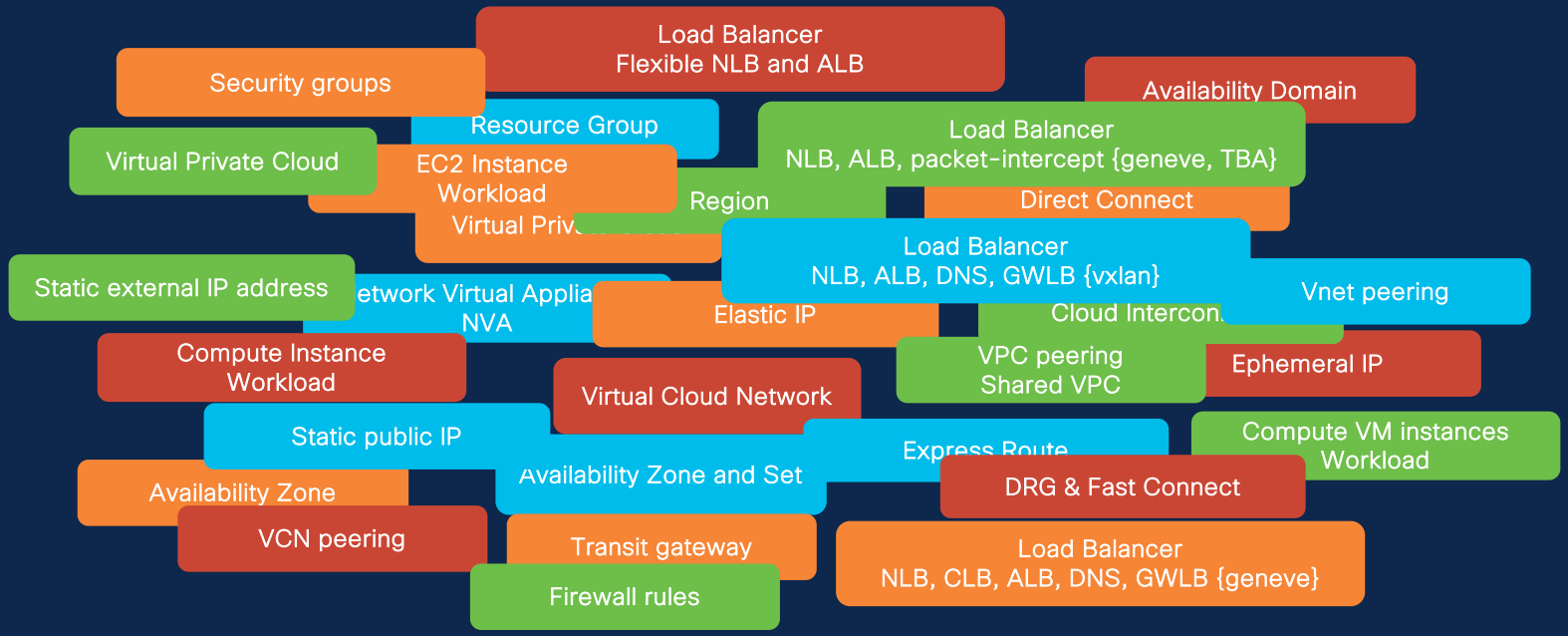
クラウド上のアプリケーションをFirewallで守るには？



クラウド上に仮想 Firewall を展開するには？



多すぎるクラウドネットワークのコンポーネント



Google Cloud

Microsoft Azure

aws

ORACLE CLOUD

オンプレミスとの違い

Dynamic

- 動的なIPアドレスアサイン
- 容易に追加可能なサブネット

Ephemeral

- 常に増減
- 生まれては消える

クラウド特有の環境に対応できる
セキュリティオペレーションの重要性

ポイント・ソリューションによる複雑化

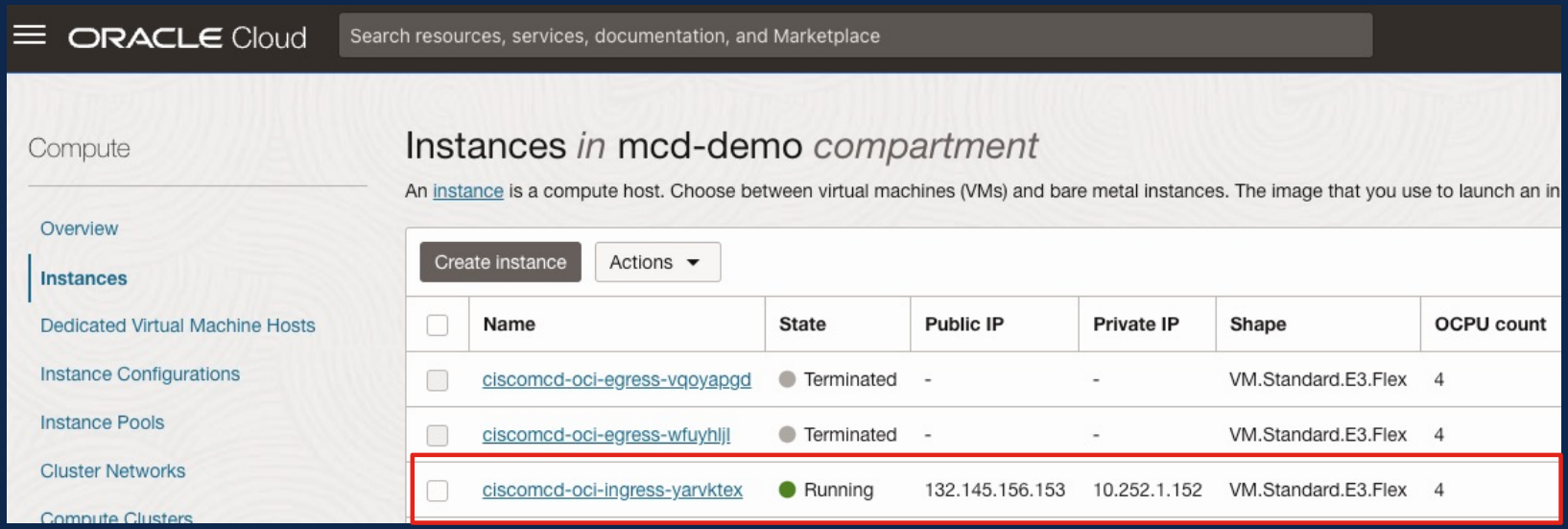
機能毎に細分化されたポイントソリューションを使うほどより多くの管理ツールが必要となり、断片化されたセキュリティ・スタックが形成される

結果としてセキュリティギャップや管理のサイロ化を生み、セキュリティチームは常に振り回されることになる

製品概要

製品のコンセプト

お客様のクラウドアカウントに“PaaS”のインスタンスとしてFirewallを設置する



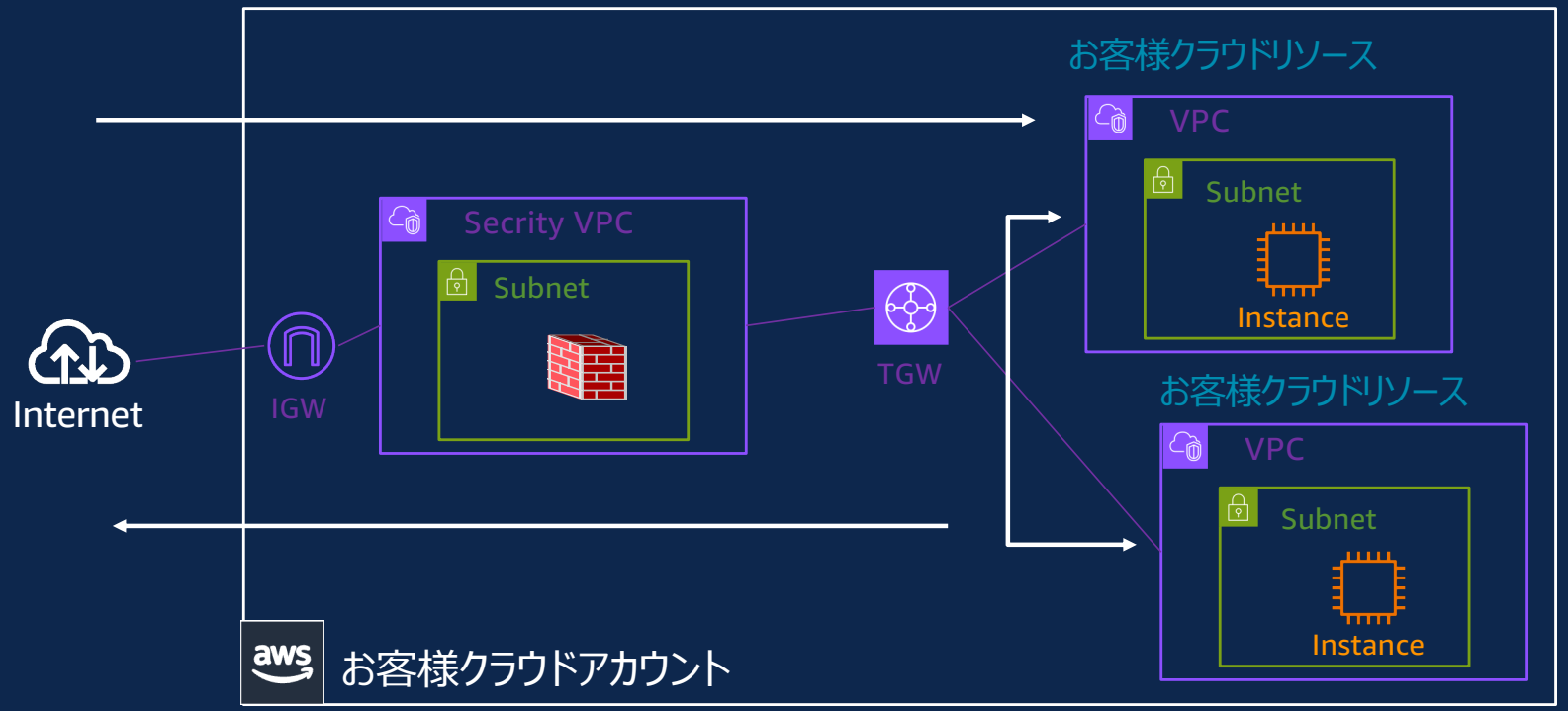
≠ FWaaS

デザインのコンセプト

Firewall設置用のVPCを作成した上でお客様VPCからの
トラフィックがFirewallを通るように各種リソースを作成＆設定

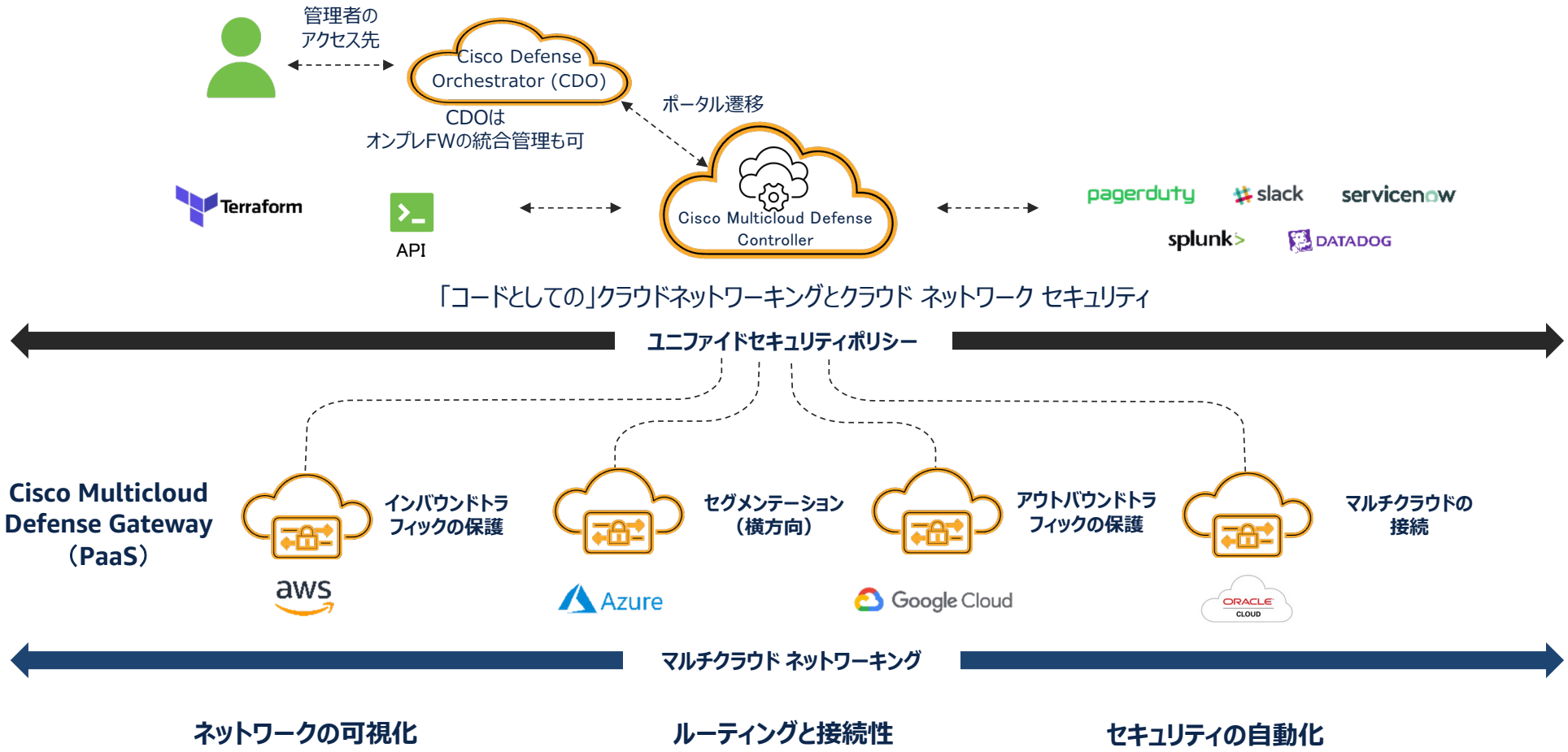
- **Ingress**
- **Egress**
- **East - West(VPC間)**

以上３方向のトラフィックを対象にしたトラフィック監査



Cisco Multicloud Defense

マルチクラウド ネットワーキング、自動化、クラウドネイティブのネットワークセキュリティ制御を 1 つに結合



デプロイメントデザインと各種機能

包括的な脅威対策機能を多方向で提供

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
- New Fully orchestrated IPsec VPN
  (site-to-cloud & cloud-to-cloud)

East/West

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

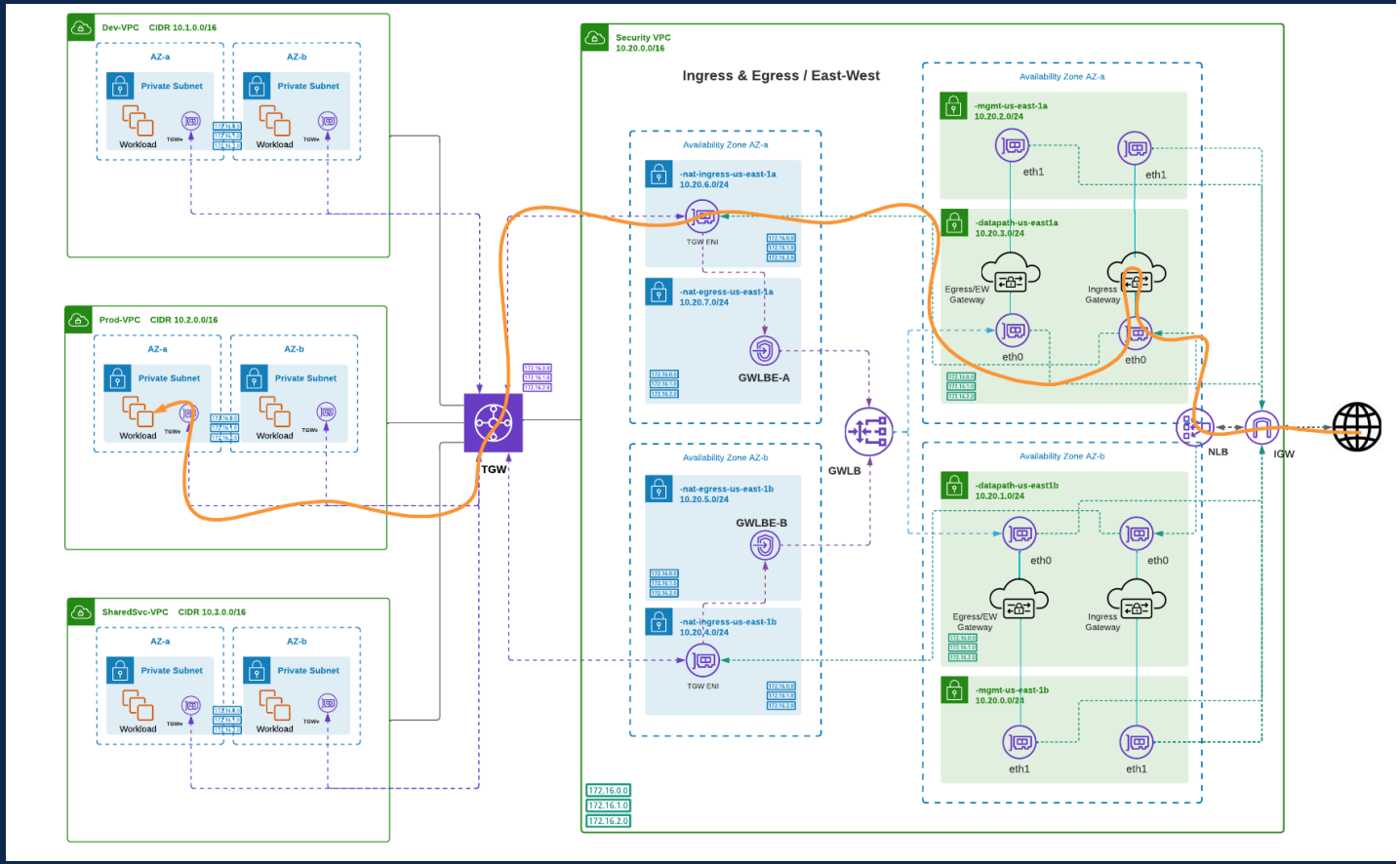
No TLS decryption is needed
Forwarding mode is available on Multicloud Defense Gateway

AWS

AWS Centralized
Ingress

Controller simplifies 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

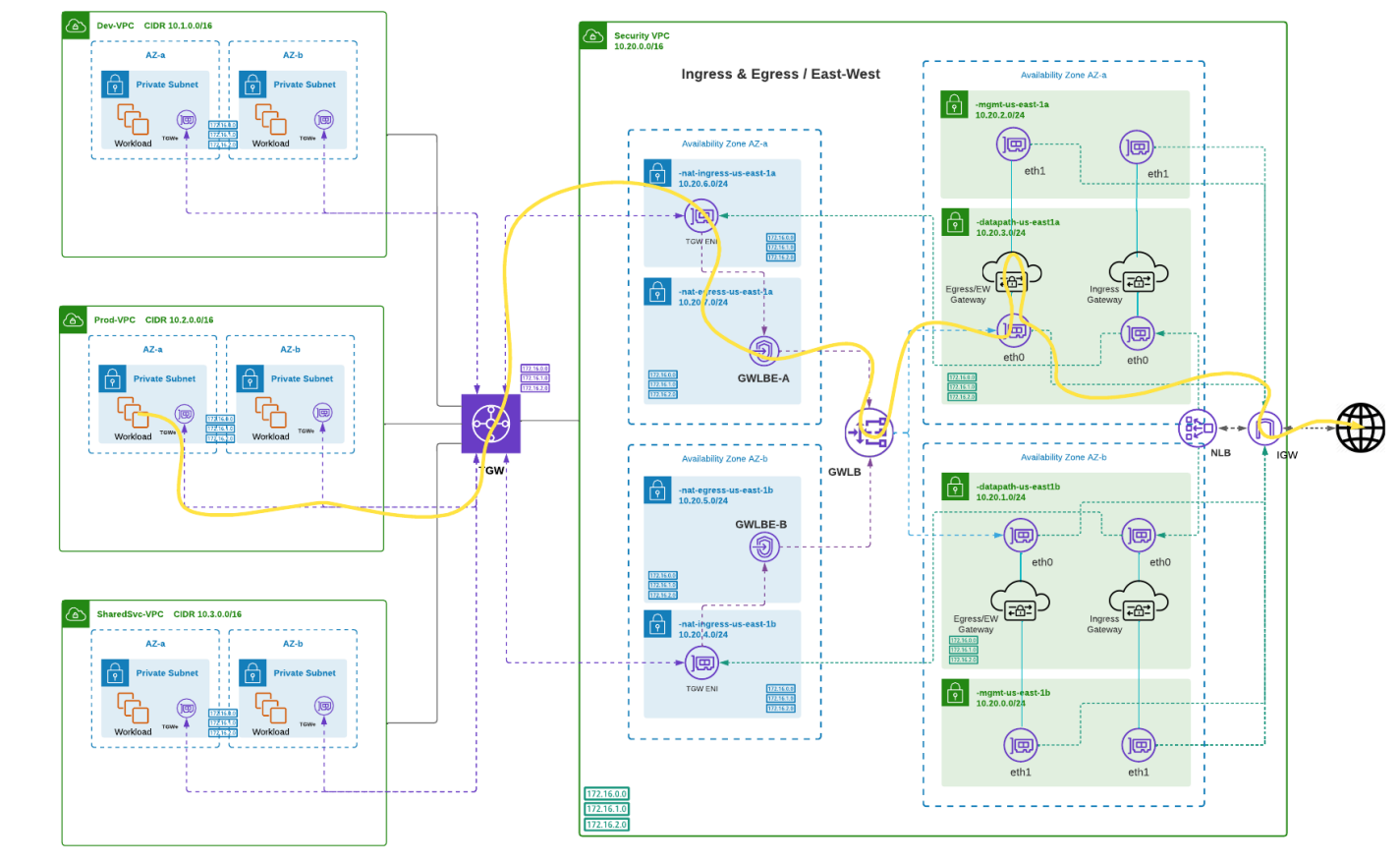


AWS Centralized – Ingress traffic inspection

AWS Centralized
Egress

Controller simplifies 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

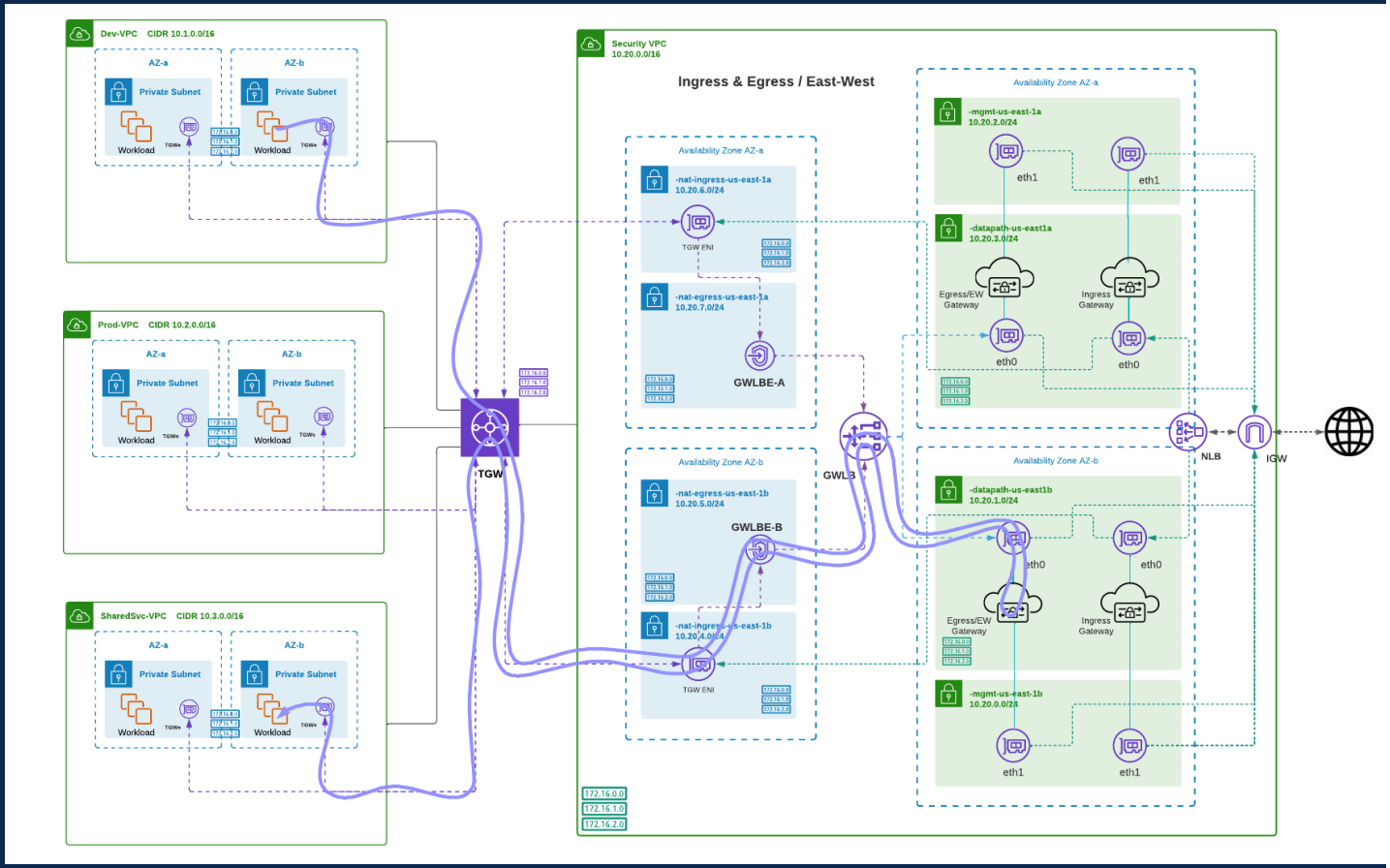


AWS Centralized – Egress traffic inspection

AWS Centralized
East-West (Inter-VPC)

Controller simplifies orchestration

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



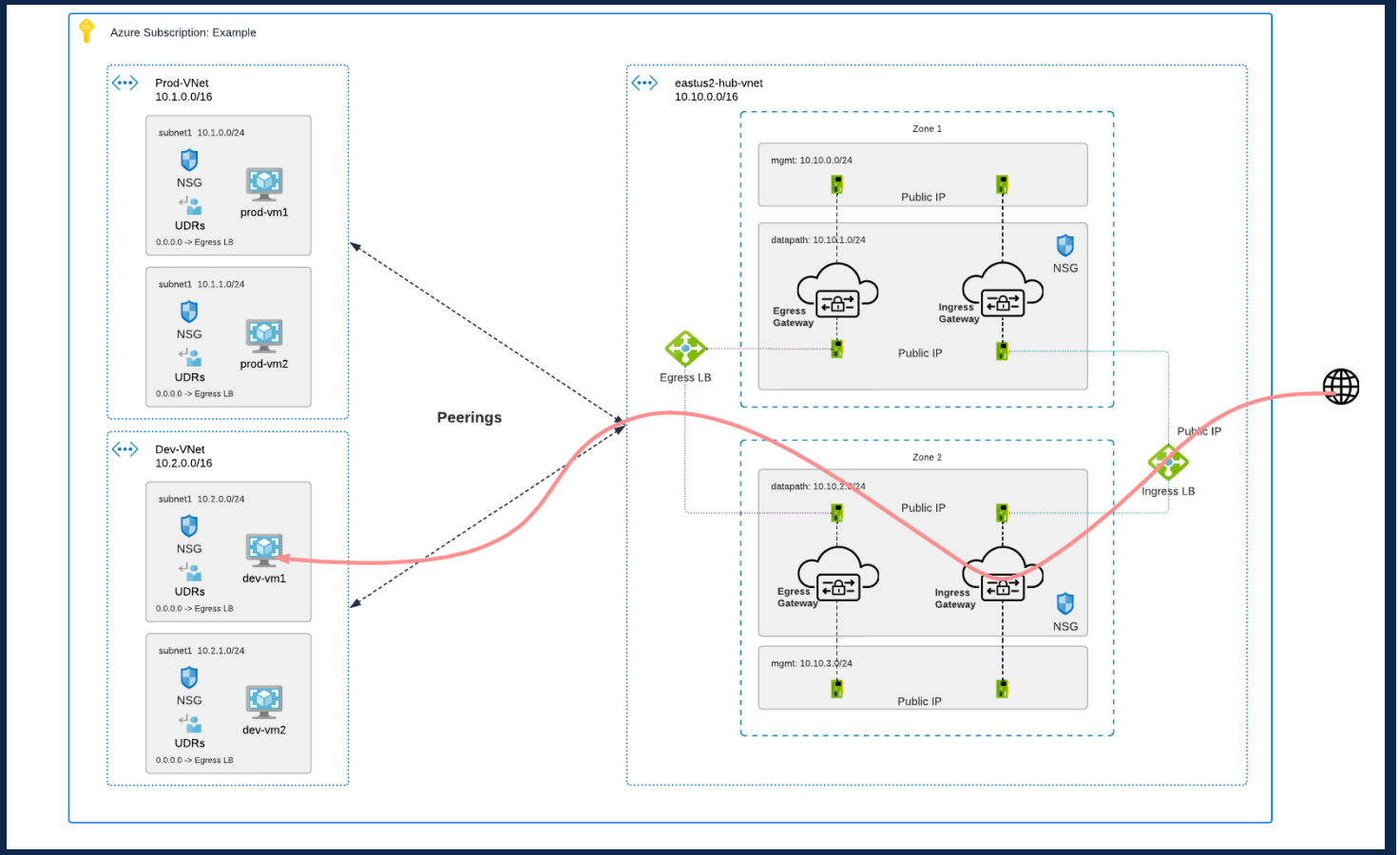
AWS Centralized – East-West traffic inspection

Azure

Azure Centralized
Ingress

Controller simplifies orchestration

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

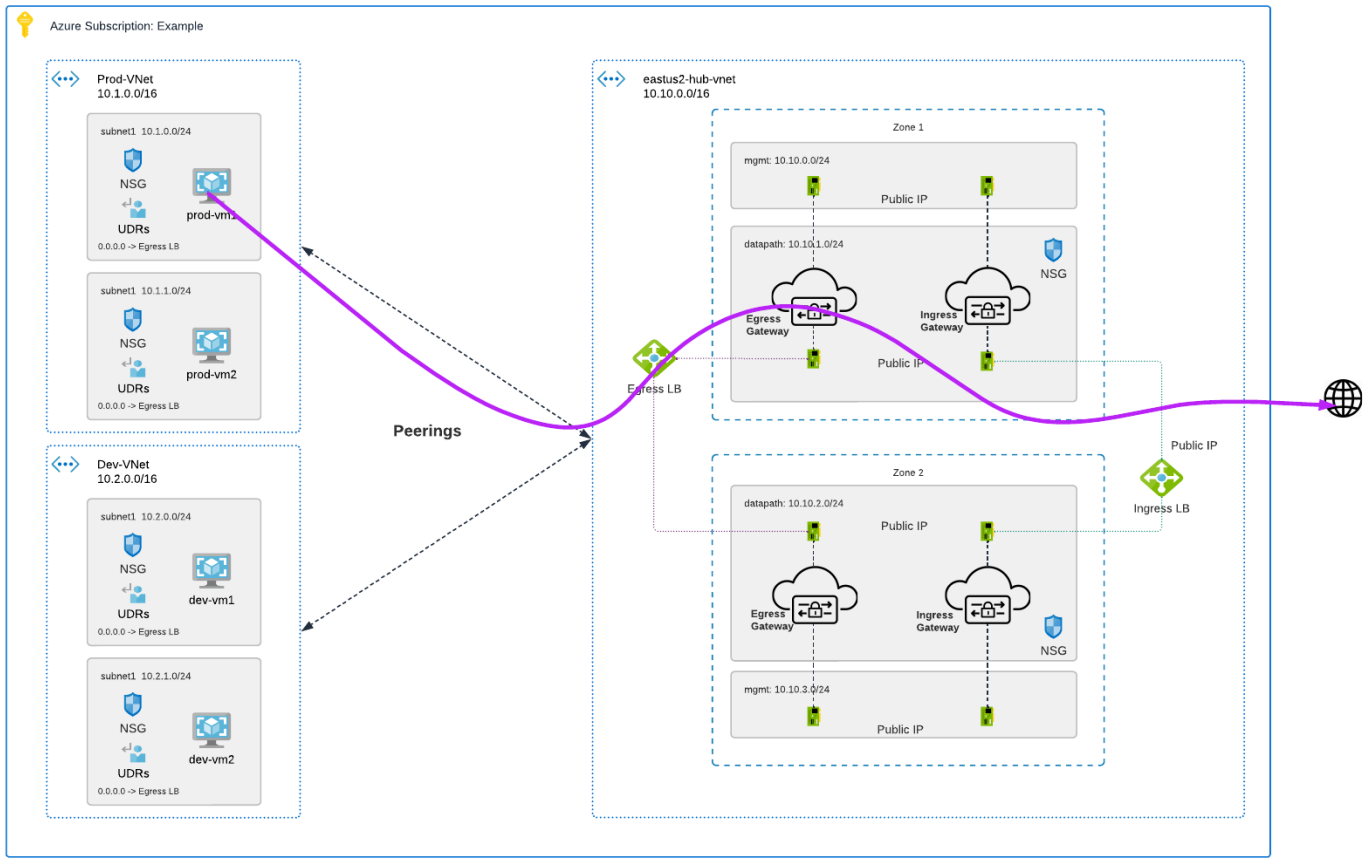


Azure Centralized – Ingress traffic inspection

Azure Centralized
Egress

Controller simplifies orchestration

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

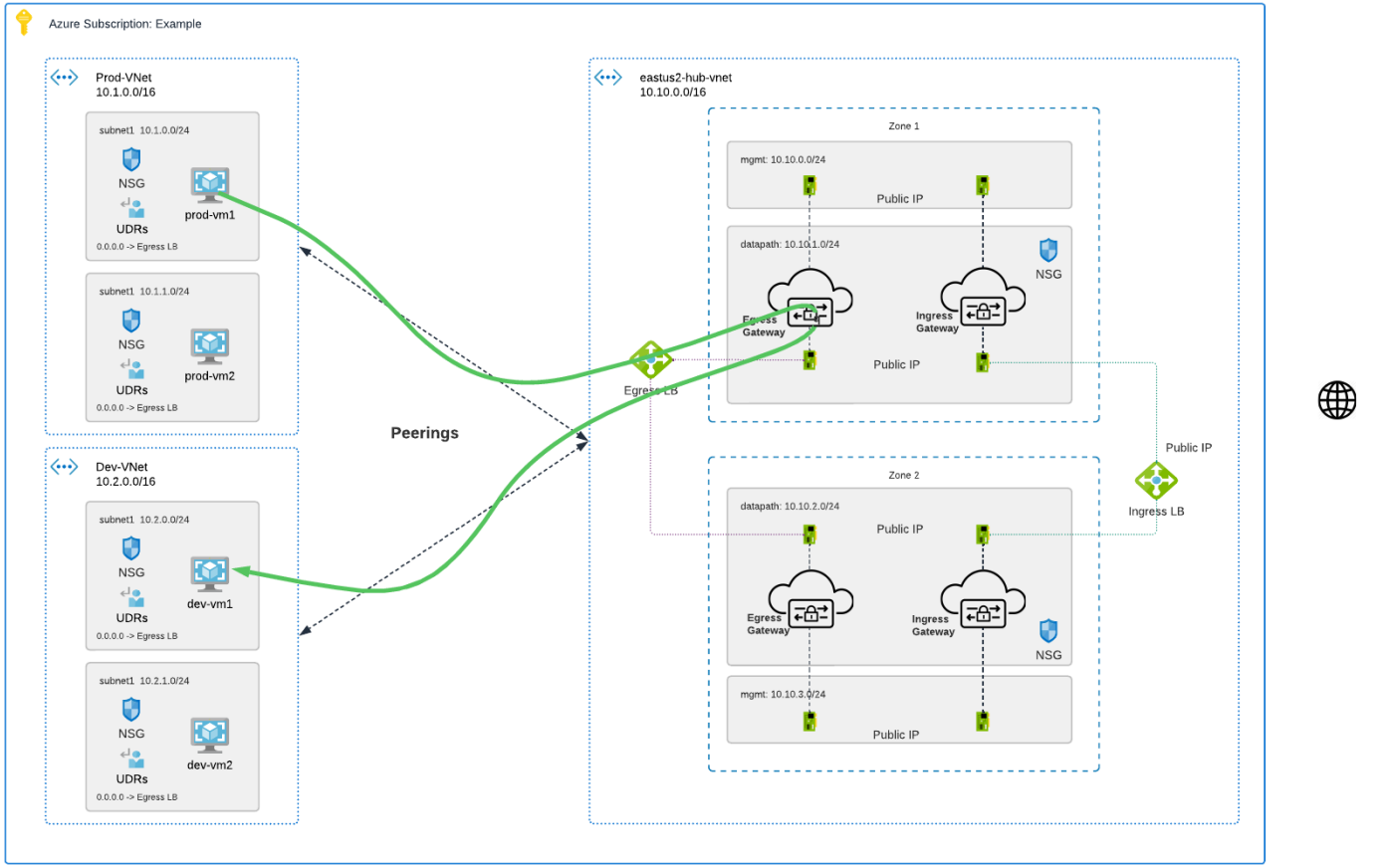


Azure Centralized – Egress traffic inspection

Azure Centralized
East-West

Controller simplifies orchestration

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



Azure Centralized – East-West traffic inspection

クラウドリソースタグを活用したオブジェクトグループ

[インスタンスの情報]

Details

General Information

Name	Prod-A-1
Instance ID	i-0c4fde9fca7107943
State	STOPPED
Region	us-east-2
CSP Acct Name	tmitsue-RunOn-AWS
CSP Instance Type	t2.micro
Num Interfaces	1
Num Security Groups	1
VPC ID	vpc-b512a1de

Tags

key	value
env	prod
Name	Prod-A-1

Public

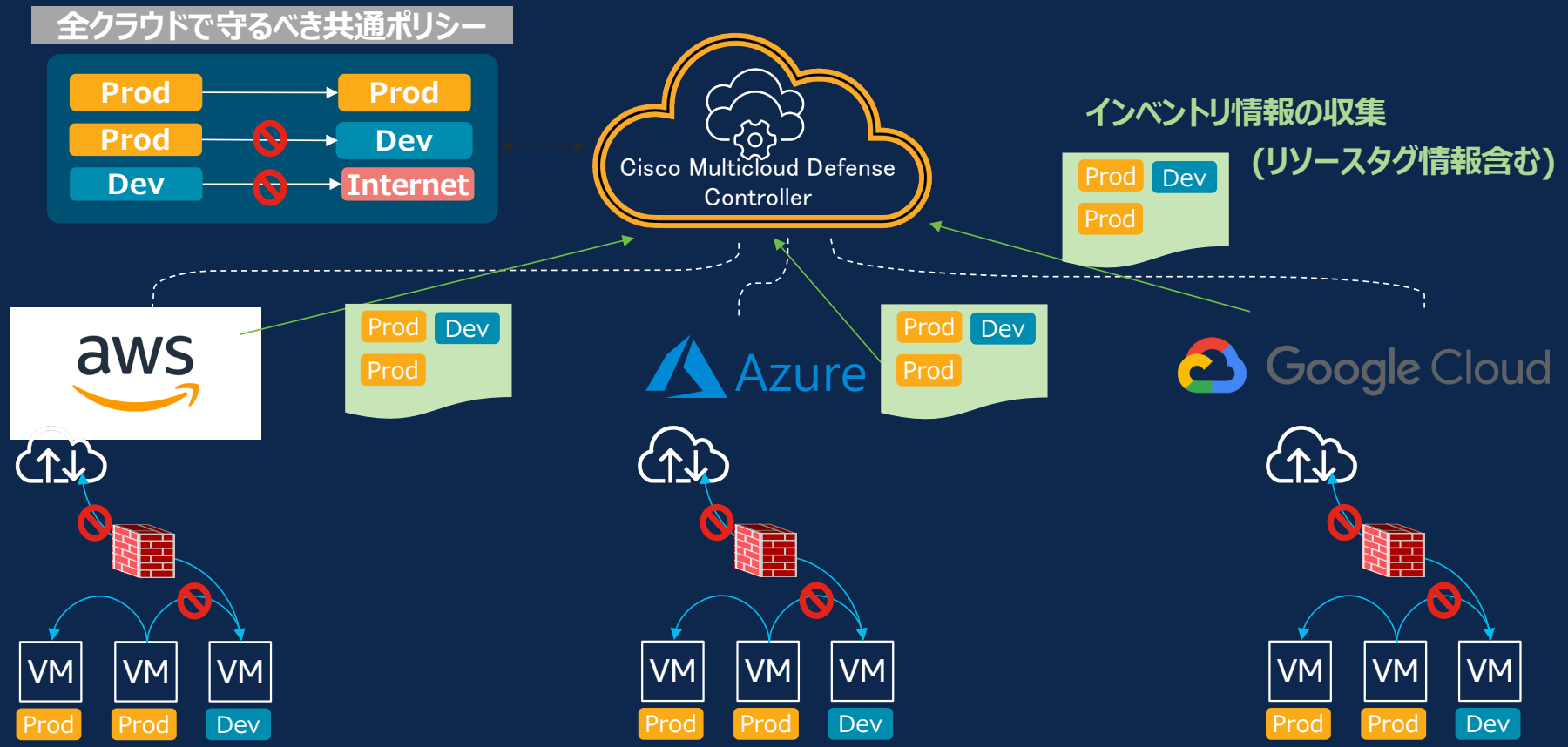
リソースタグの情報をベースにセグメントをオブジェクト化

[Addressオブジェクト]

Resource Level	Resource Tag	Resource Tag Value
RESOURCE_INSTANCE	env	prod

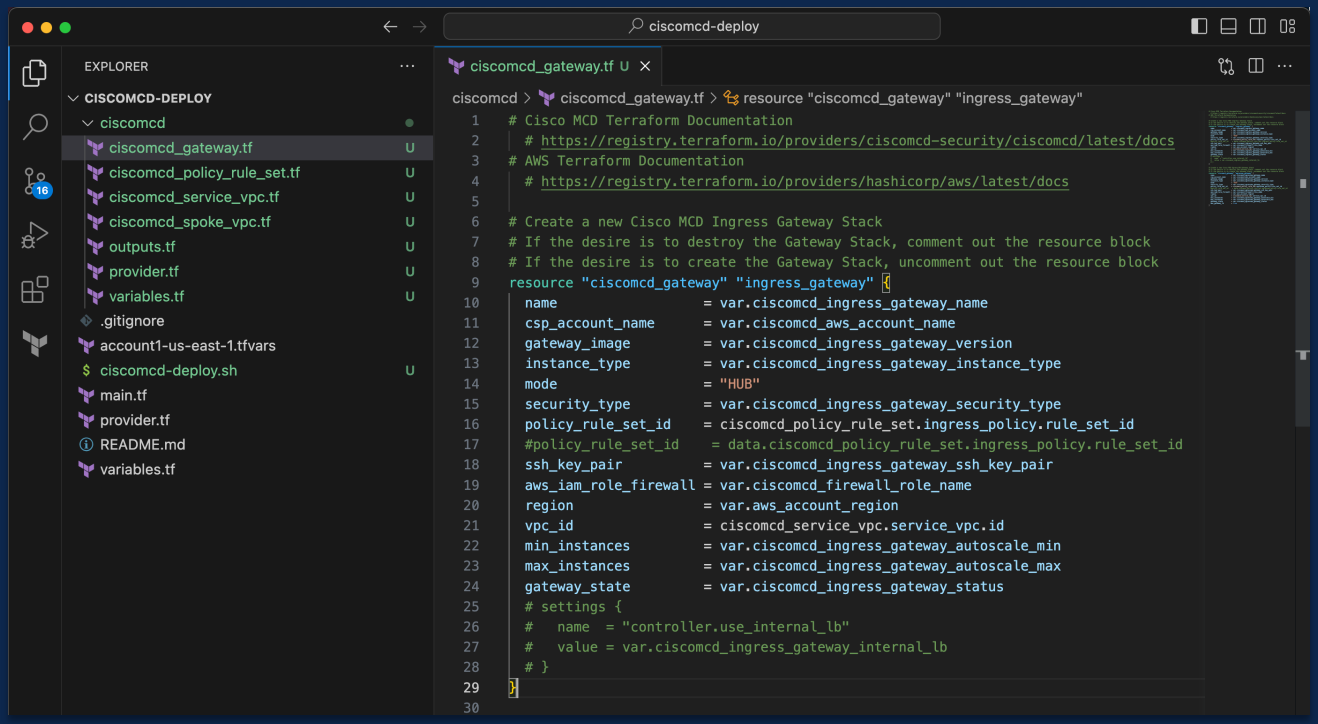
Name	Type	CSP Acct	Region	VPC/VNet
172.16.0.3	IP_ADDR	tmitsue-RunOn-GCP	Montreal | northamerica-northeast1	vpc-a
172.17.0.4	IP_ADDR	tmitsue-RunOn-GCP	Montreal | northamerica-northeast1	vpc-b
172.31.6.195	IP_ADDR	tmitsue-RunOn-AWS	US East (Ohio) | us-east-2	vpc-b512a1de
192.168.0.182	IP_ADDR	tmitsue-RunOn-AWS	US East (Ohio) | us-east-2	vpc-0dc7151f81464c6cf

クラウドリソースタグでマルチクラウドのポリシー制御



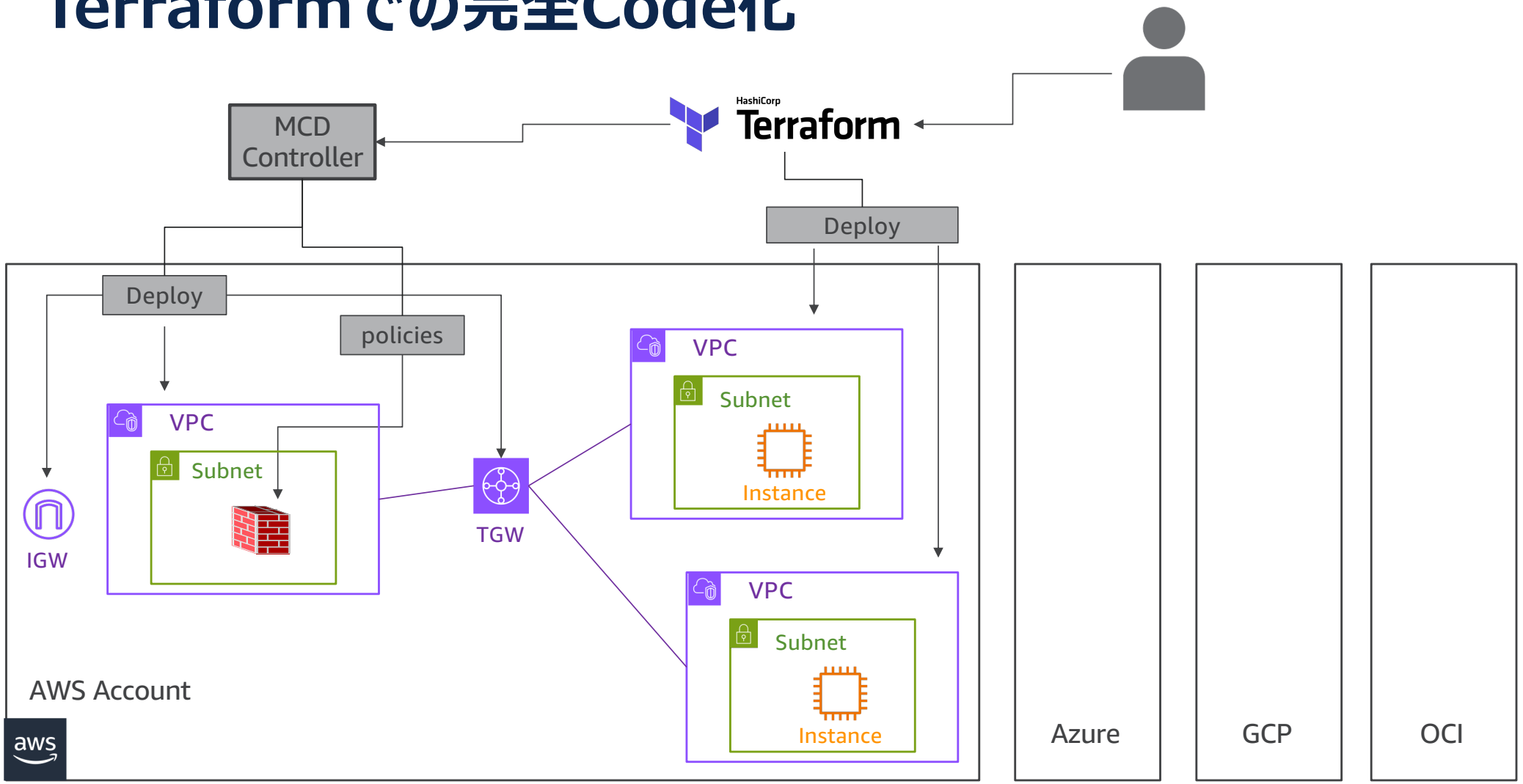
IaCによるフルオーケストレーション対応

HashiCorp Terraform



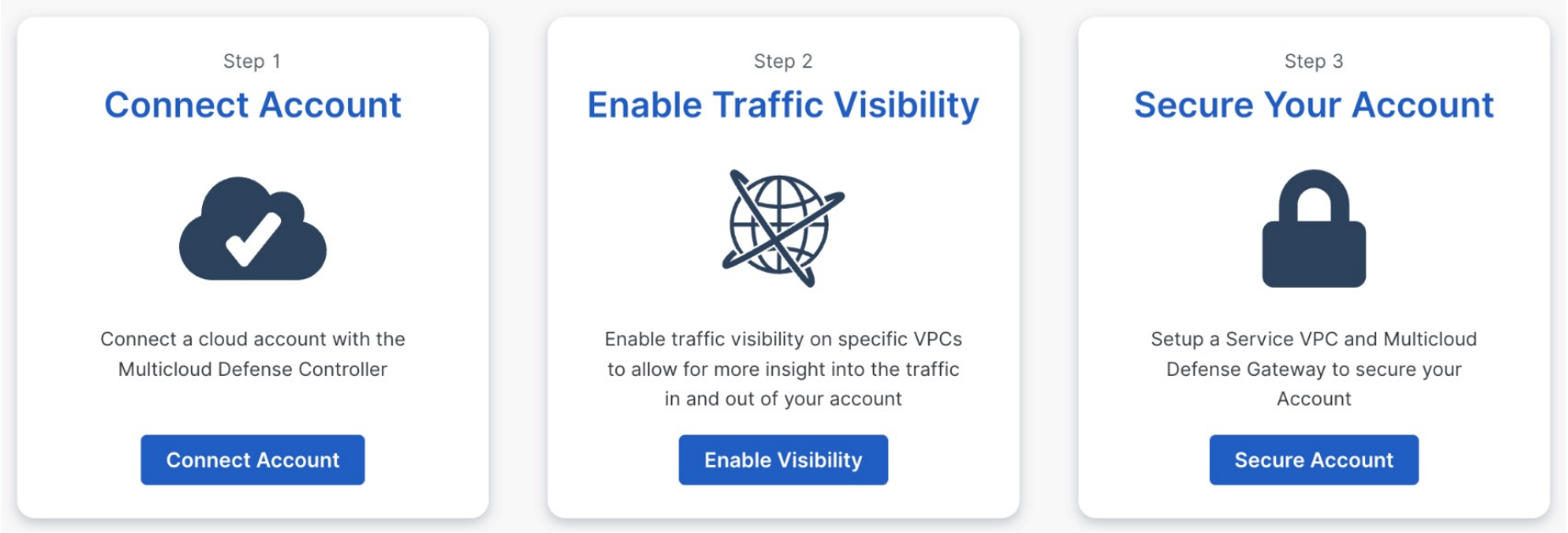
https://registry.terraform.io/providers/CiscoDevNet/ciscomcd/latest/docs

Terraformでの完全Code化



Demo

Cisco Multicloud Defenseによる マルチクラウド環境保護までの3ステップ

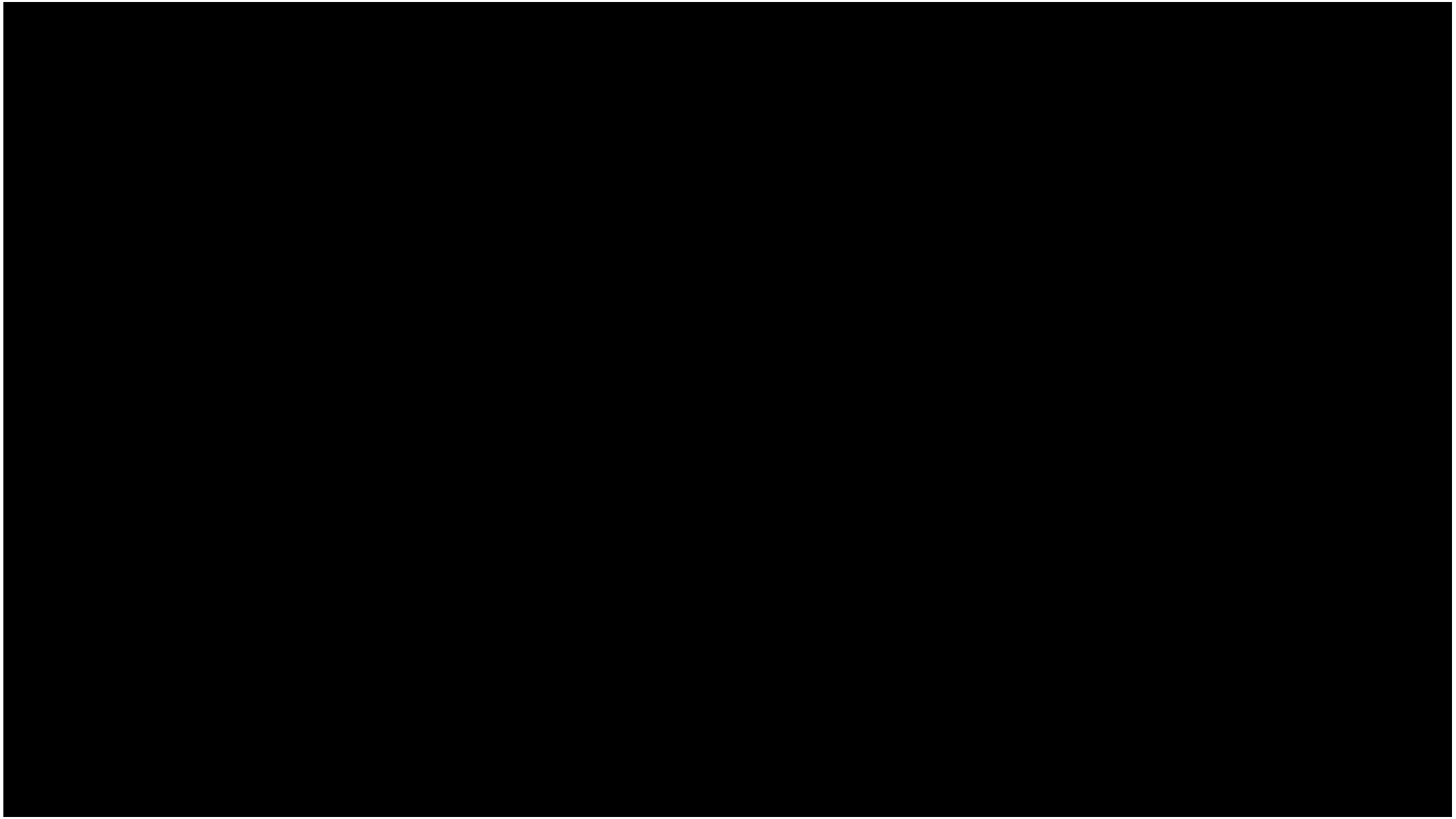


クラウドアカウントのオンボーディング
（登録）

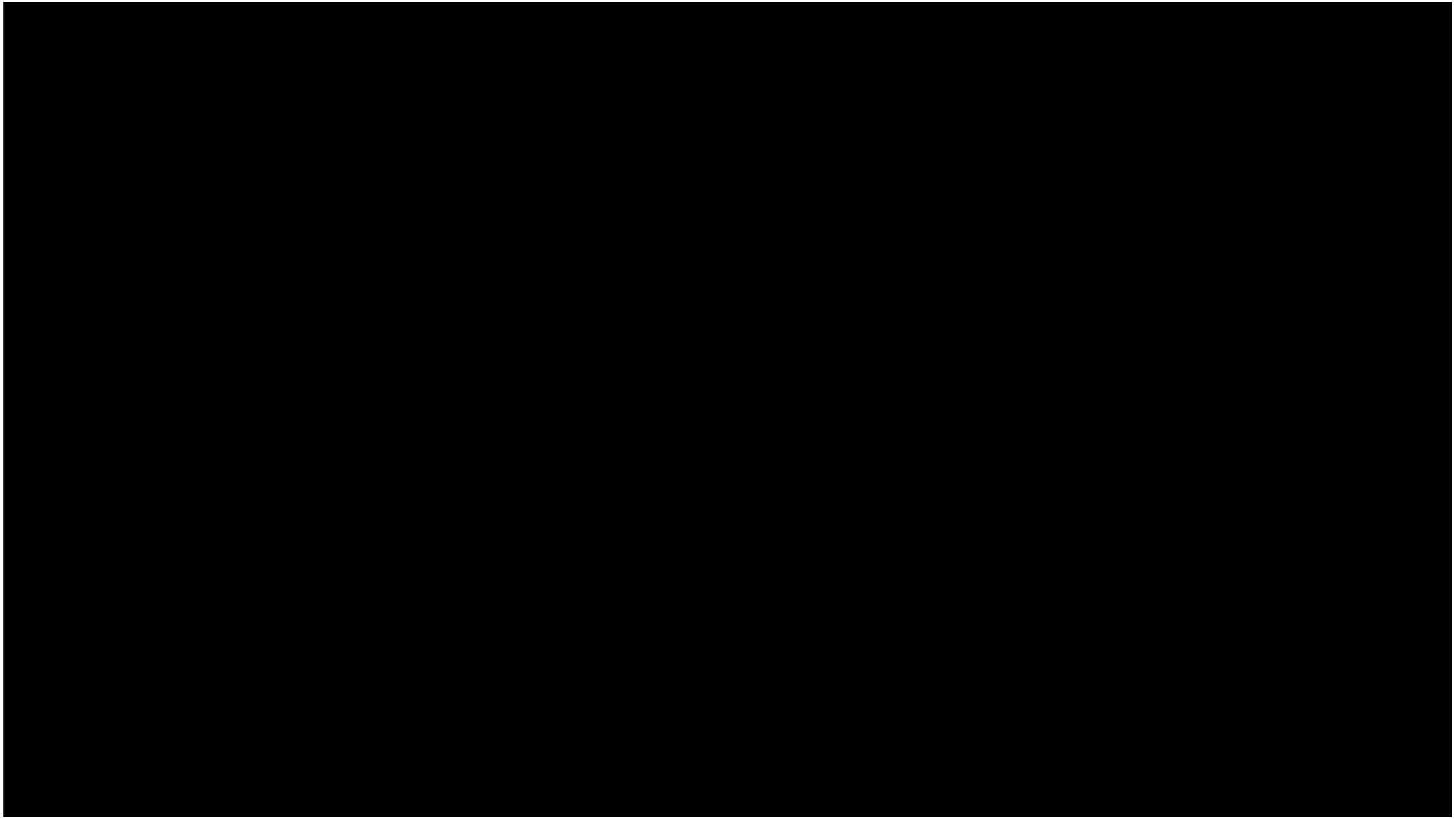
DNS クエリ & VPC/NSG フローログの
有効化
（クラウドアセットの可視化）

オーケストレーションとオートメーション
（GWの構築と管理）

Onboarding

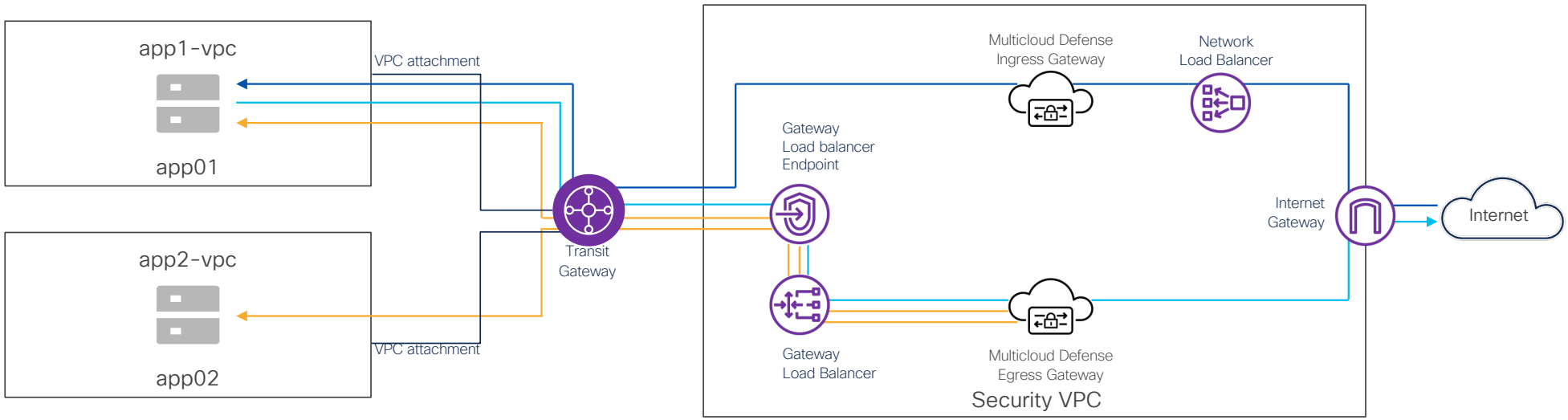


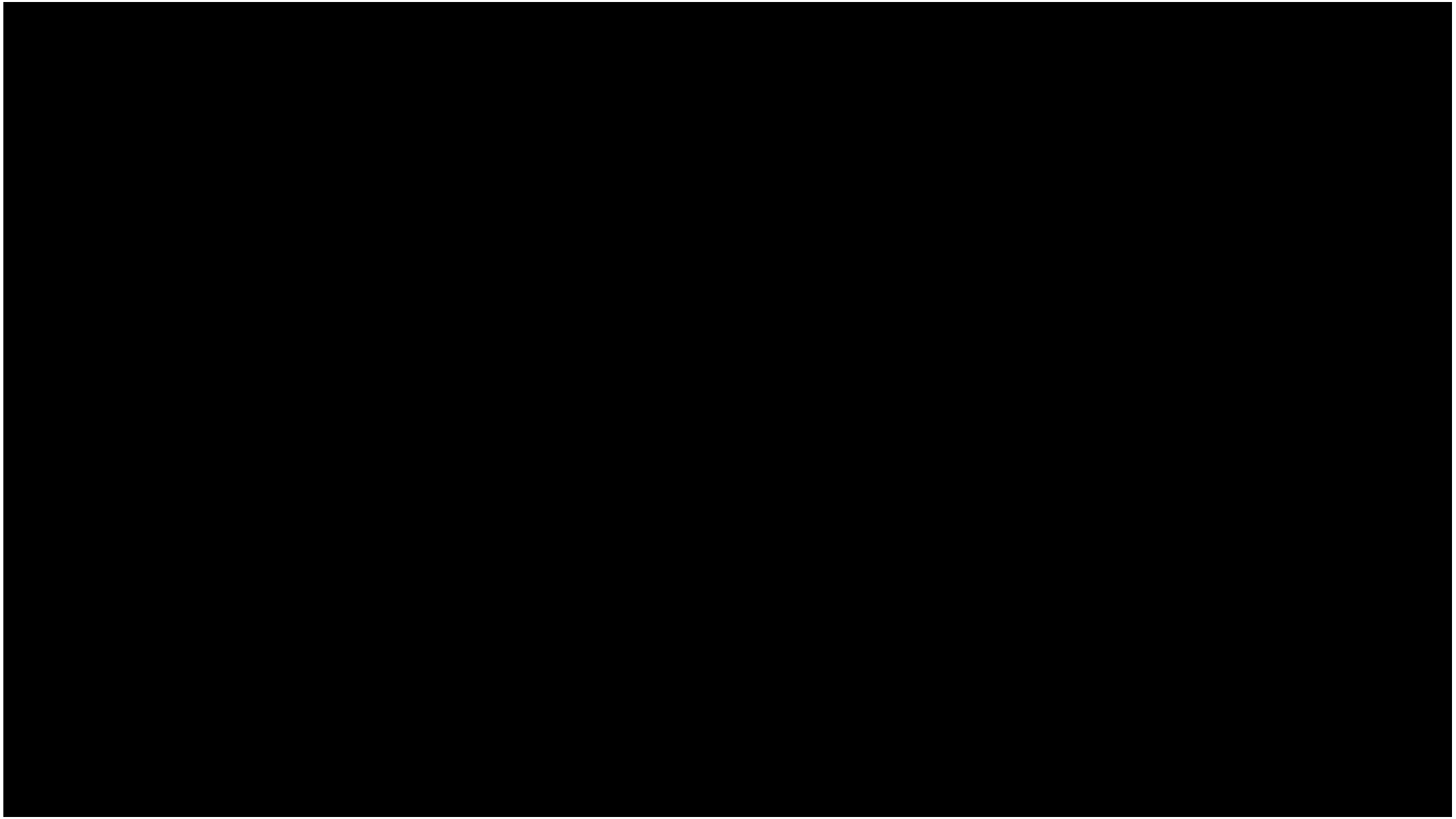
Visibility



Secure your VPC

Secure Your Account
Demo





料金体系

ライセンス

- Advantage と Premier ライセンスの 2 種類を用意
- 製品ライセンスは、すべて (クラウド) 環境に渡ってゲートウェイ時間を集計した消費量に基づく (従量課金ではない)
  ※ 必要な層のゲートウェイ時間数
- 1年/3年/5年のサブスクリプションを用意
- ゲートウェイ時間の計算方法 = ゲートウェイ数 x 24 (1日の時間) x 365 (1年の日数) x 期間 (1年/3年/5年)
  ※ 1台のゲートウェイを1年間24時間365日稼働させると、8760時間となる

	Advantage	Premier
Visibility	✓	✓
Unlimited accounts	✓	✓
FQDN egress filtering (outbound)	✓	✓
Malicious IP and geography-based blocking	✓	✓
IPS / IDS	✓	✓
Cisco Talos® Threat Intelligence	✓	✓
TLS decryption	✓	✓
3rd-party integrations	✓	✓
URL filtering		✓
DLP (block exfiltration)		✓
Web application firewall		✓
API rate limiting		✓
Antivirus		✓
Multicloud connectivity		Coming soon
Hybrid segmentation		Coming soon

AWSの場合

Multicloud Defense

インスタンスの料金 (AWSへの支払い)

m5.large	($0.096/h)
m5.xlarge	($0.192/h)
m5.2xlarge	($0.384/h)

} 3サイズのインスタンスから選択

GW稼働時間 (Ciscoへの支払い)

AWS Firewall + AWS WAF

Network Firewall Endpoint	($0.395/h)
Network Firewall Traffic Processing	($0.065/GB)
Network Firewall Advanced Inspection Endpoint	($1.095/h)
Network Firewall Advanced Inspection Traffic Processing	($0.005/GB)

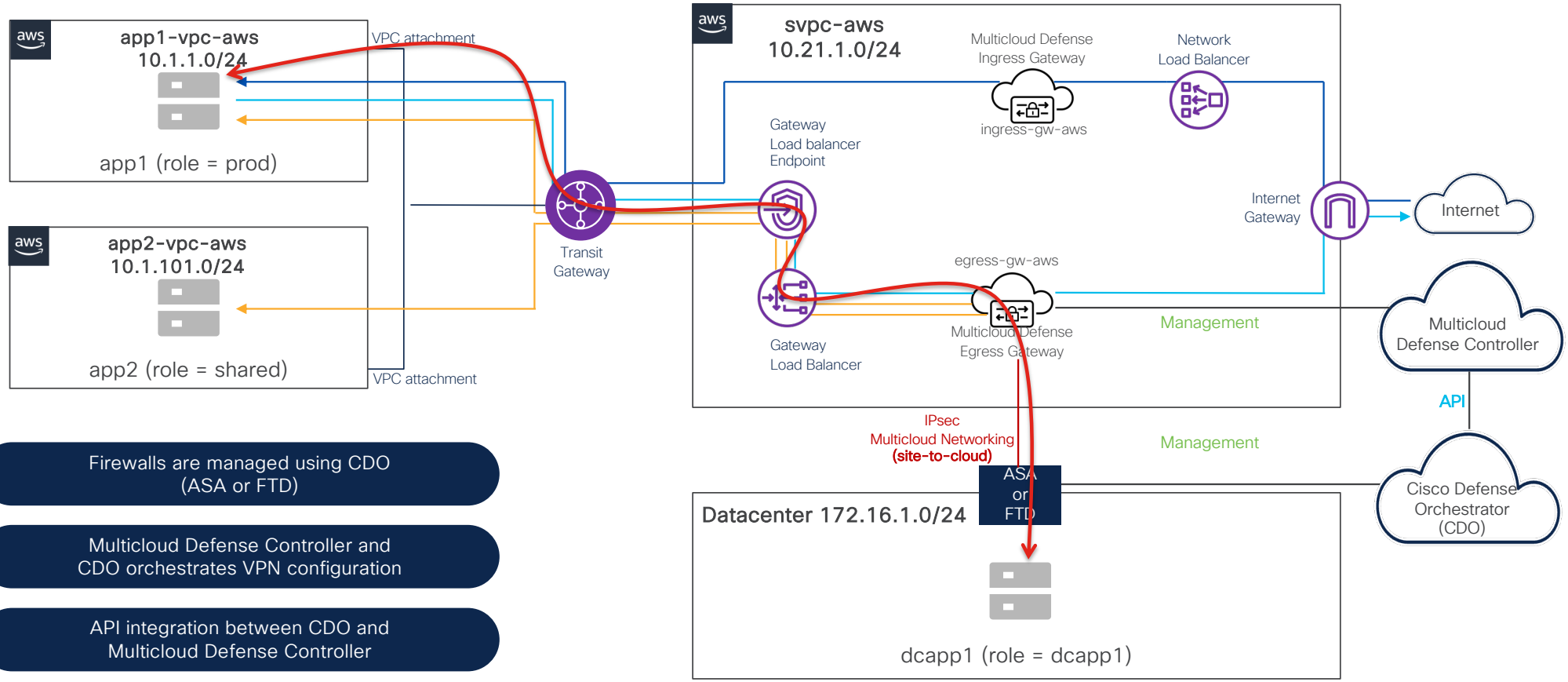
Web ACL	1Web ACLあたり ($5/Month)
Rule	1Ruleあたり ($1/Month)
Requests	($0.60/100million requests)

最新アップデート

Site-to-cloud VPN

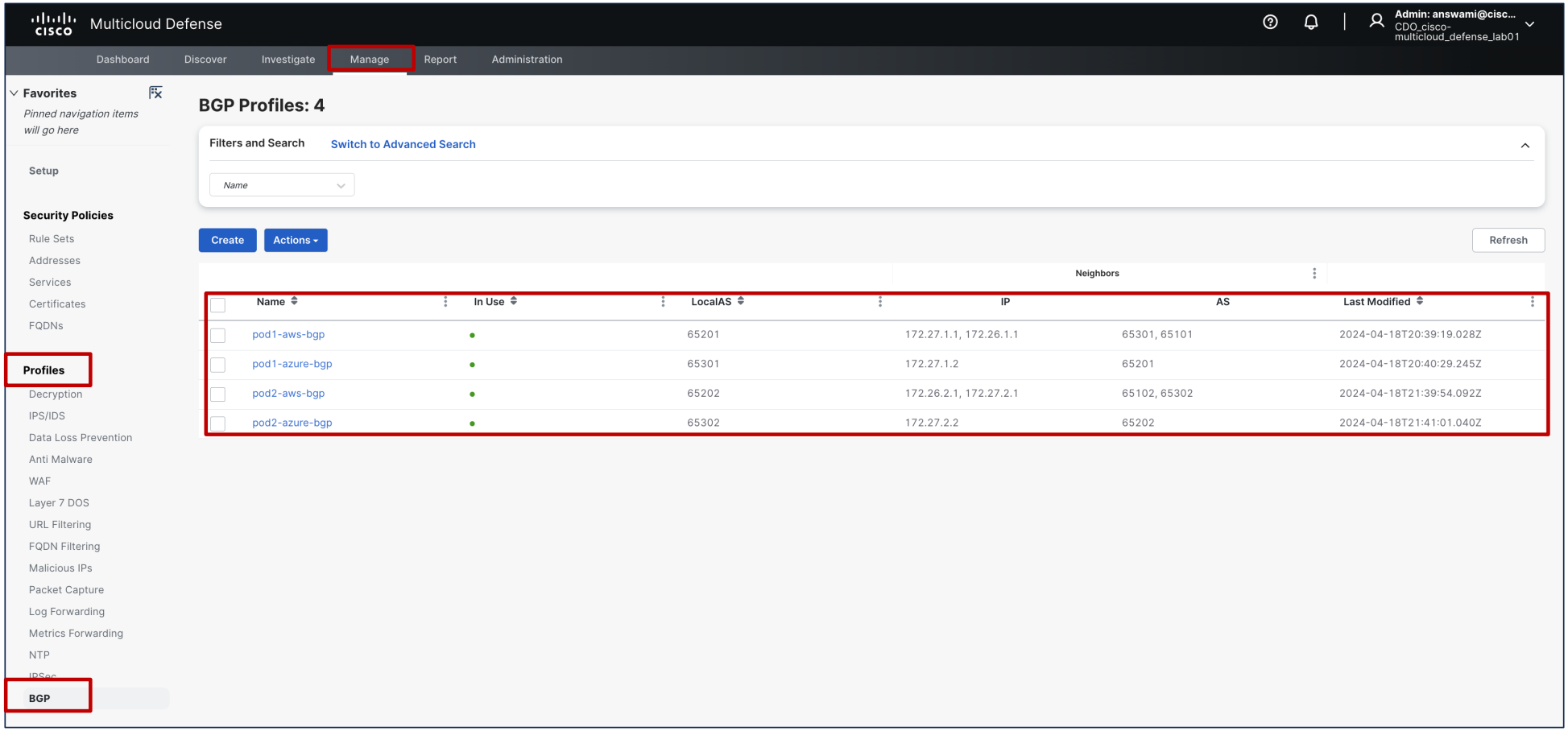
Multicloud Networking

site-to-cloud connectivity (Centralized security model)



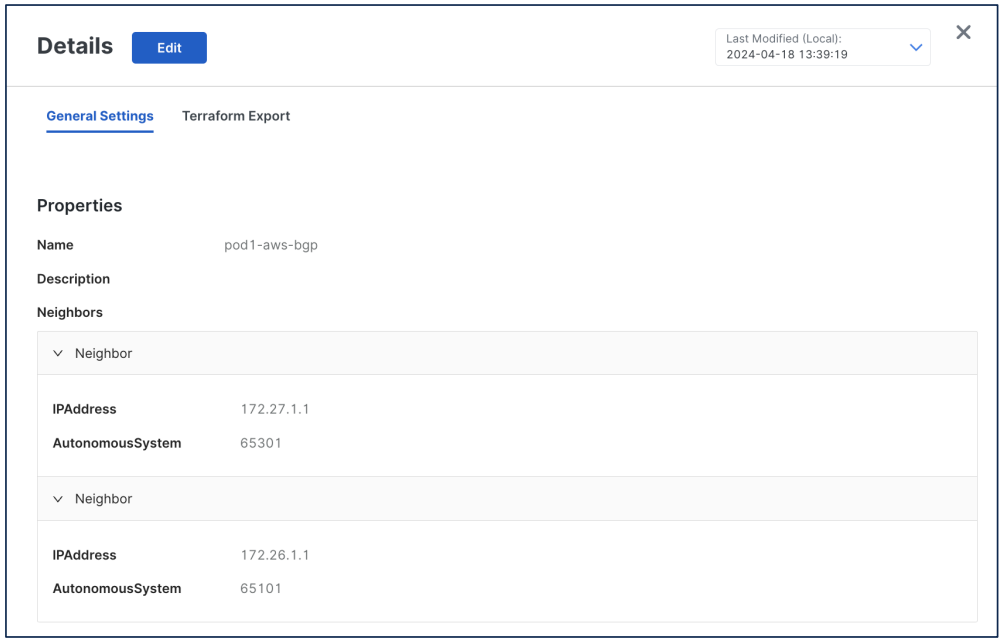
- Firewalls are managed using CDO (ASA or FTD)
- Multicloud Defense Controller and CDO orchestrates VPN configuration
- API integration between CDO and Multicloud Defense Controller

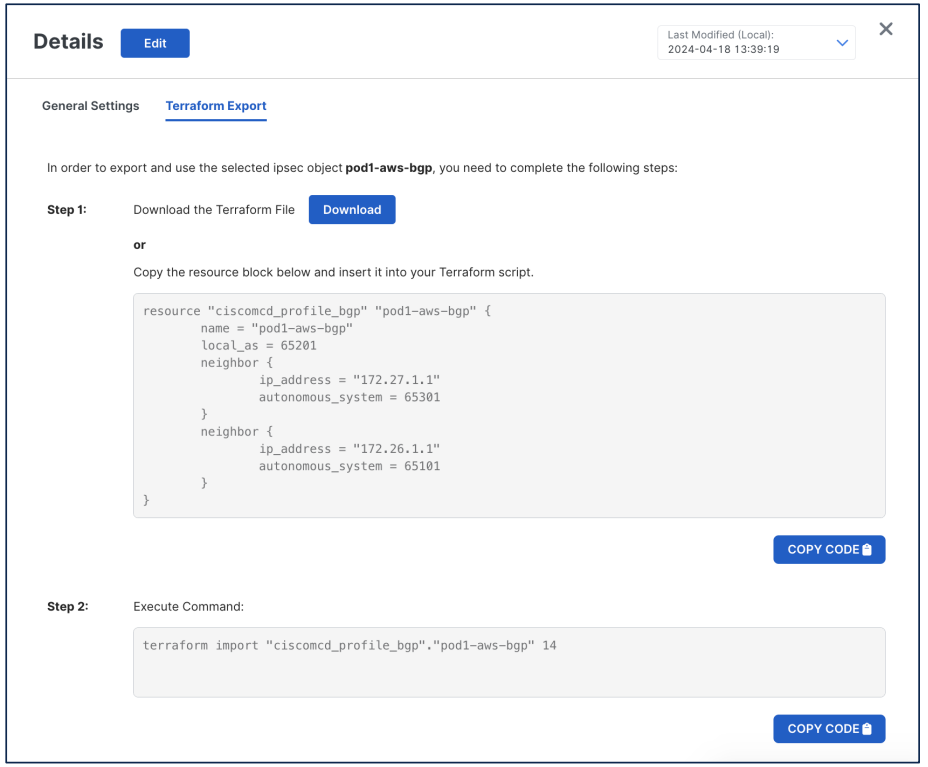
BGP Profile



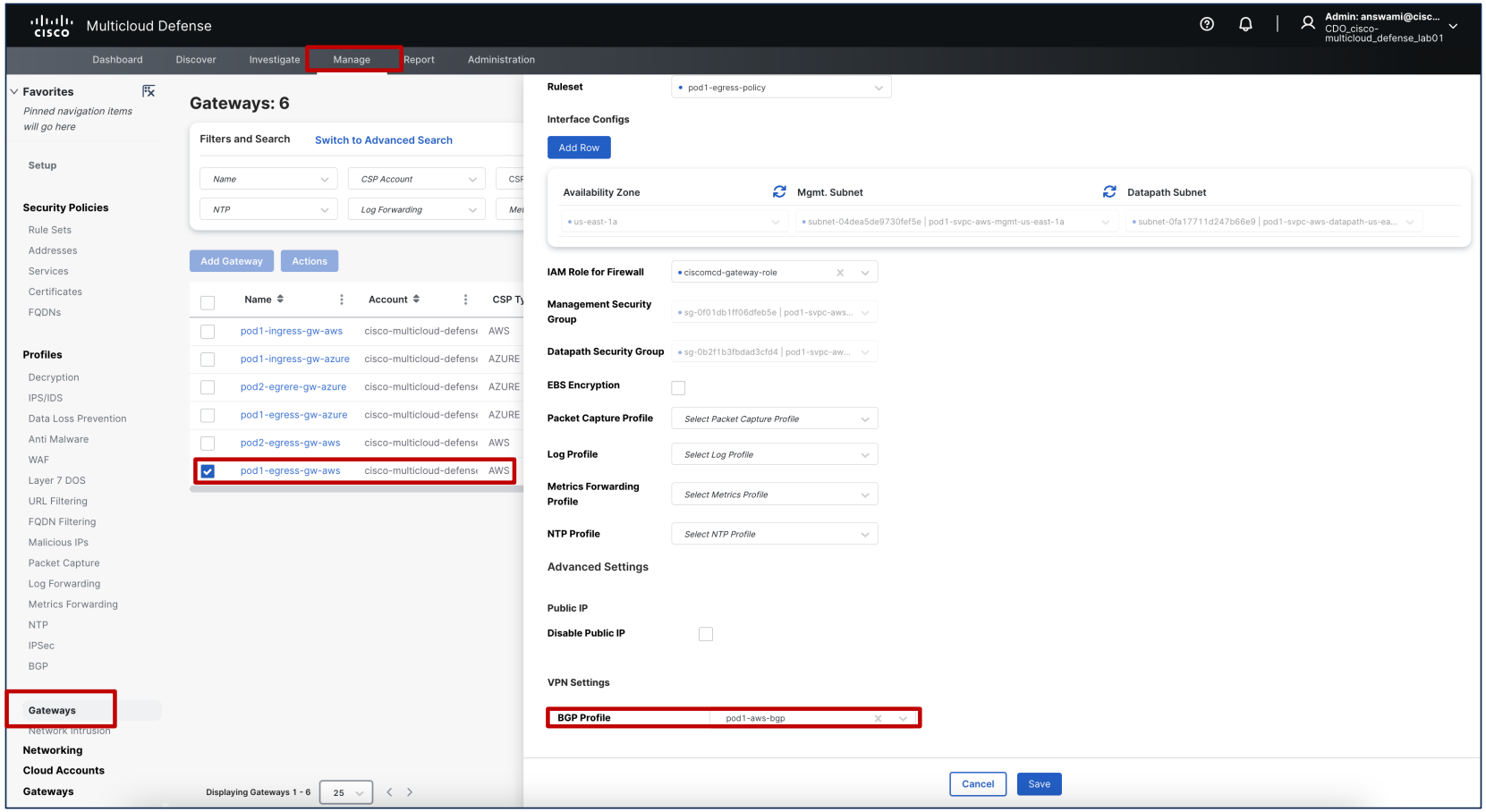
Note: On premise ASA/FTD BGP configuration is not yet supported in CDO, so it must be done *by hand*. UI configuration coming soon

BGP Profile contd.



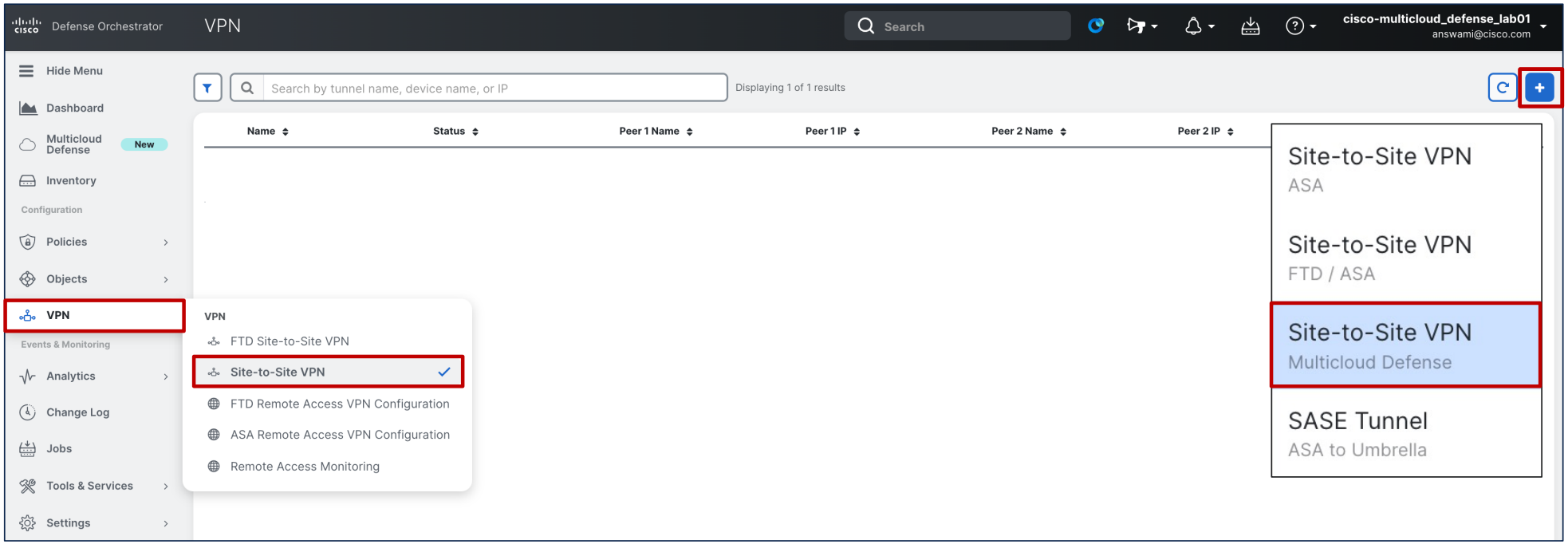


BGP Profile contd.



Configure site-to-cloud VPN

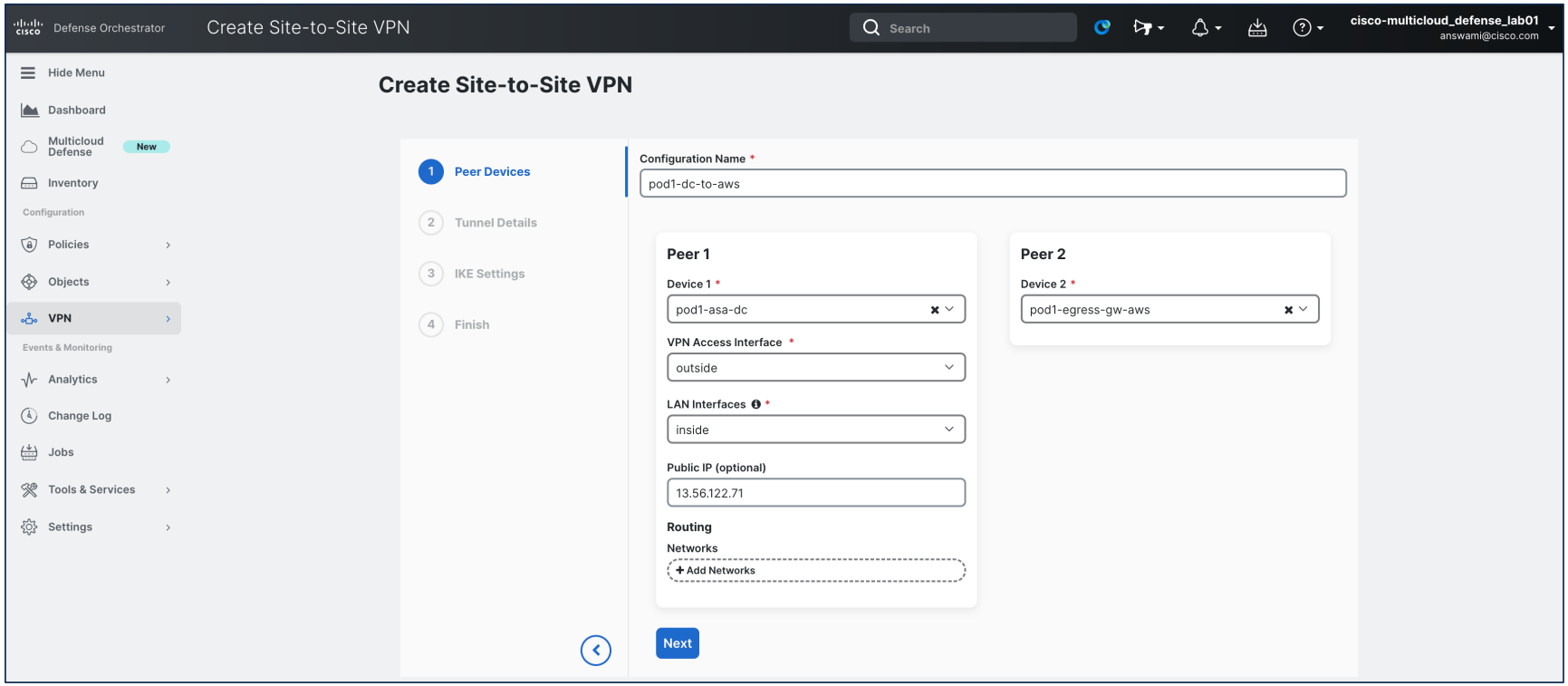
Configure site-to-site VPN tunnel



CDO orchestrates VPN configuration on the firewall
CDO talks Multicloud Defense controller and orchestrates VPN configuration on the Gateway

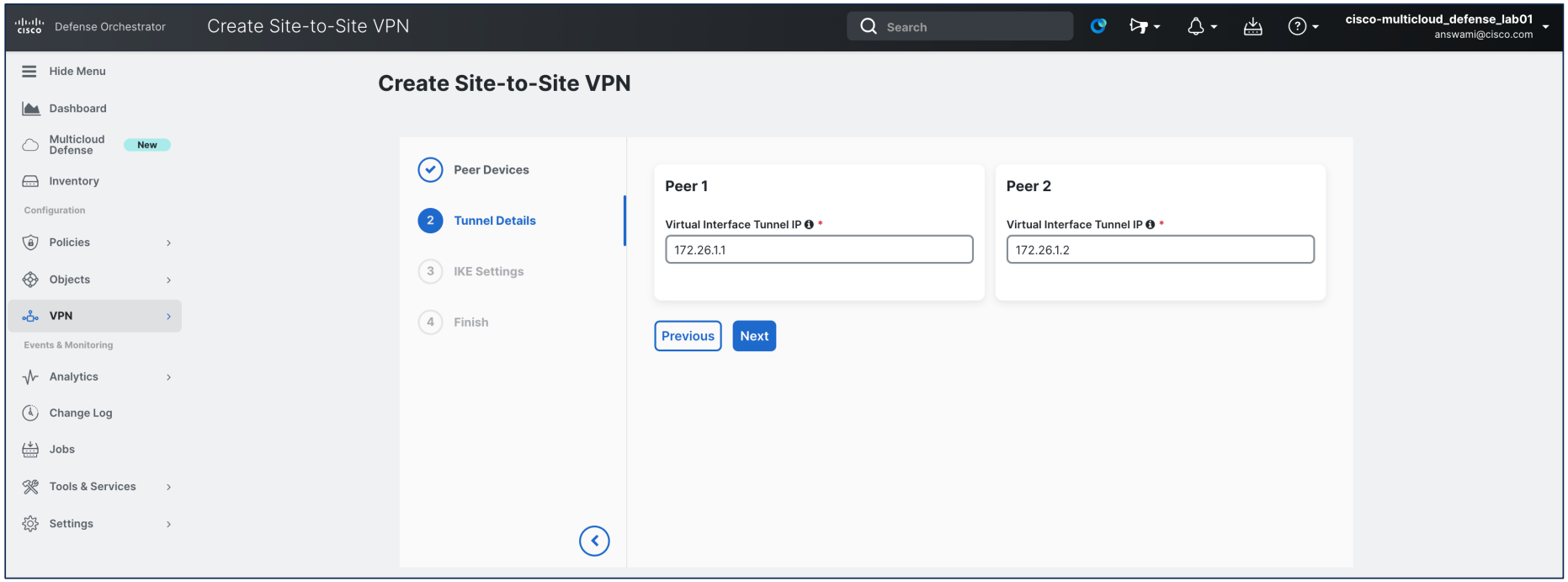
Configure site-to-cloud VPN

Step1 – Create site-to-site VPN tunnel



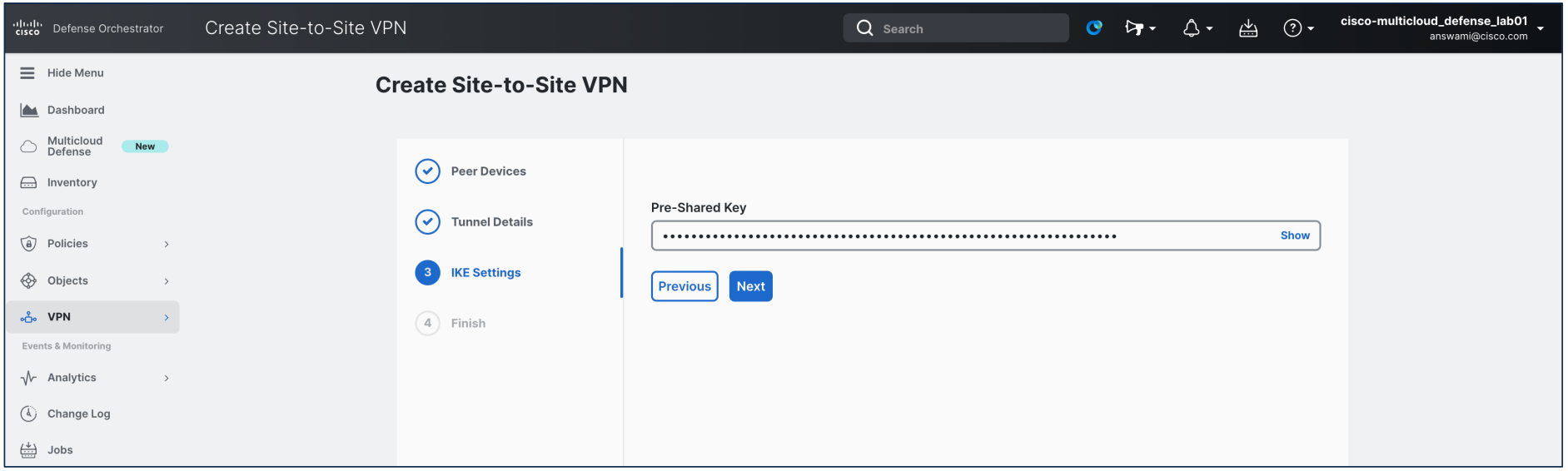
Configure site-to-cloud VPN

Step 2 – Configure VTI interfaces



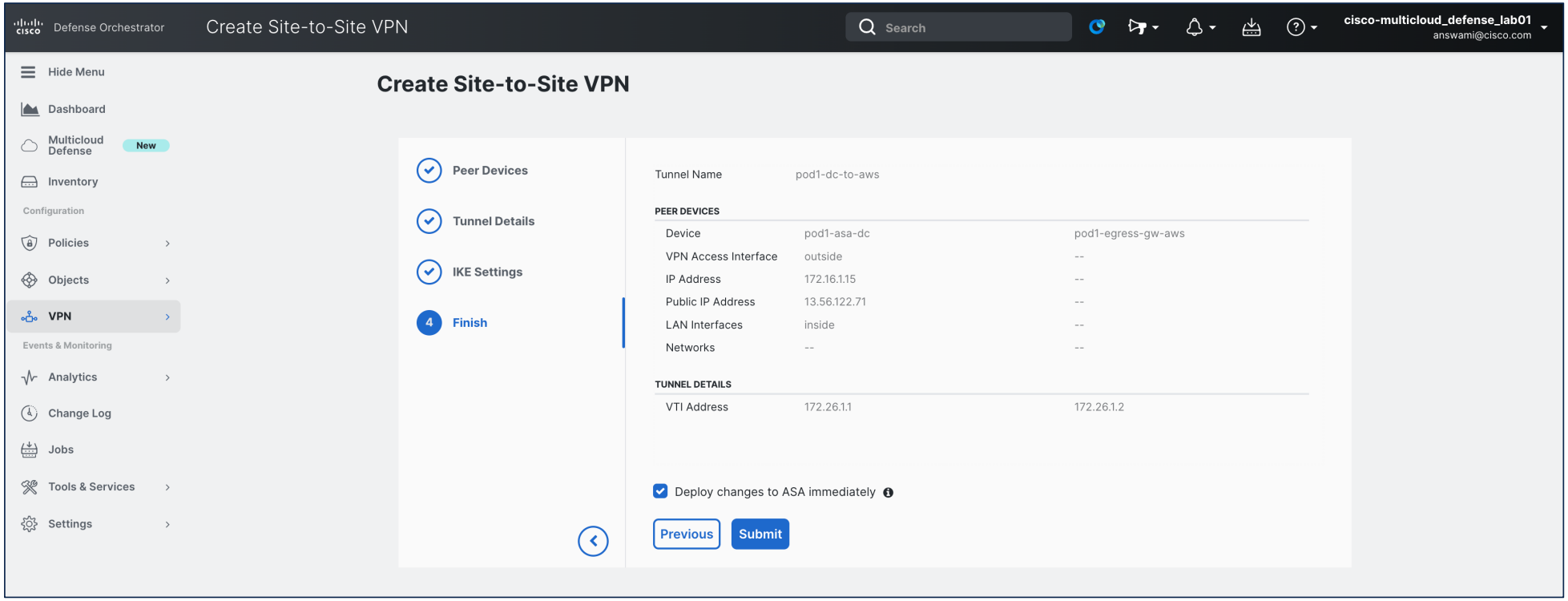
Configure site-to-cloud VPN

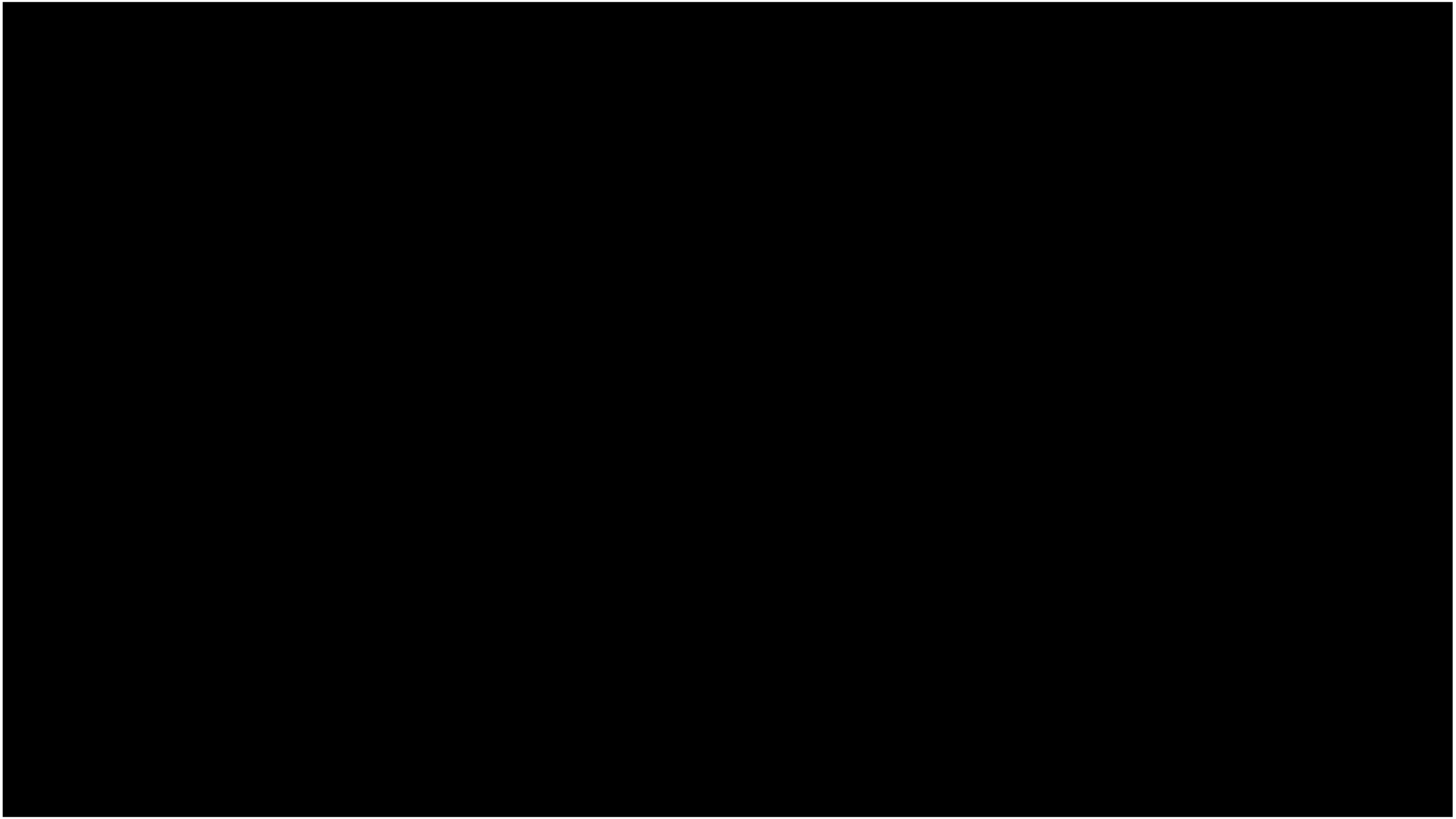
Step 3 – Configure Pre-Shared Key



Configure site-to-cloud VPN

Step 4 – Deploy configuration on Firewall and Multicloud Defense Gateway

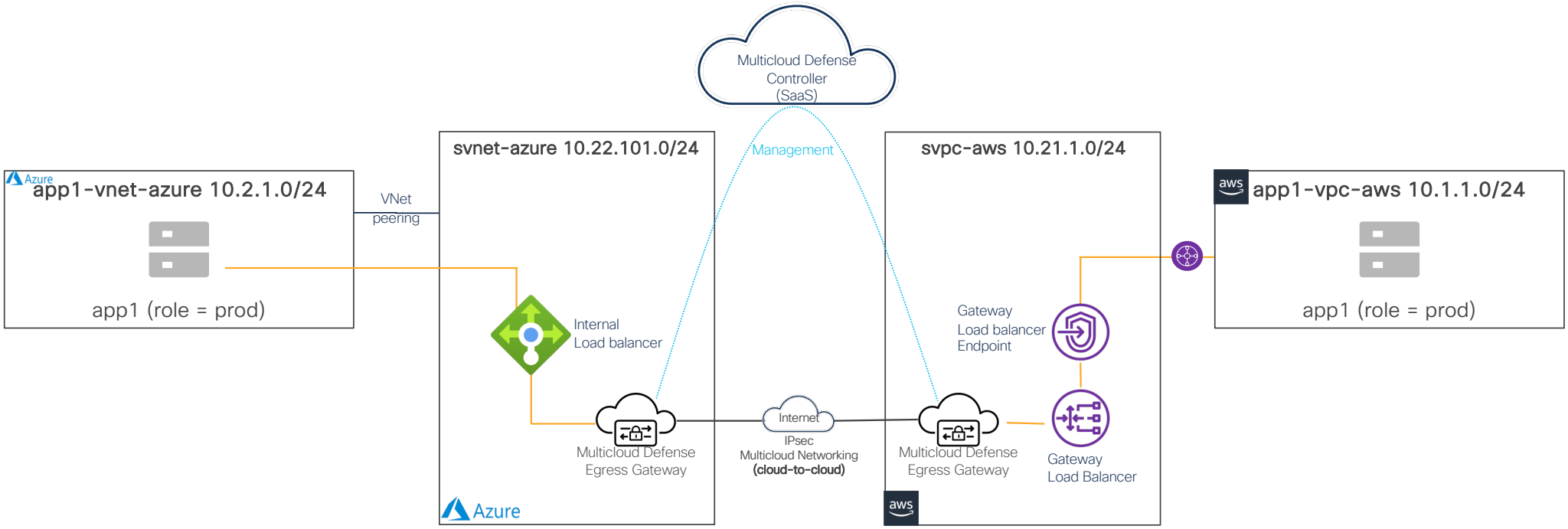




Cloud-to-cloud VPN

Multicloud Networking

cloud-to-cloud connectivity (Centralized security model)



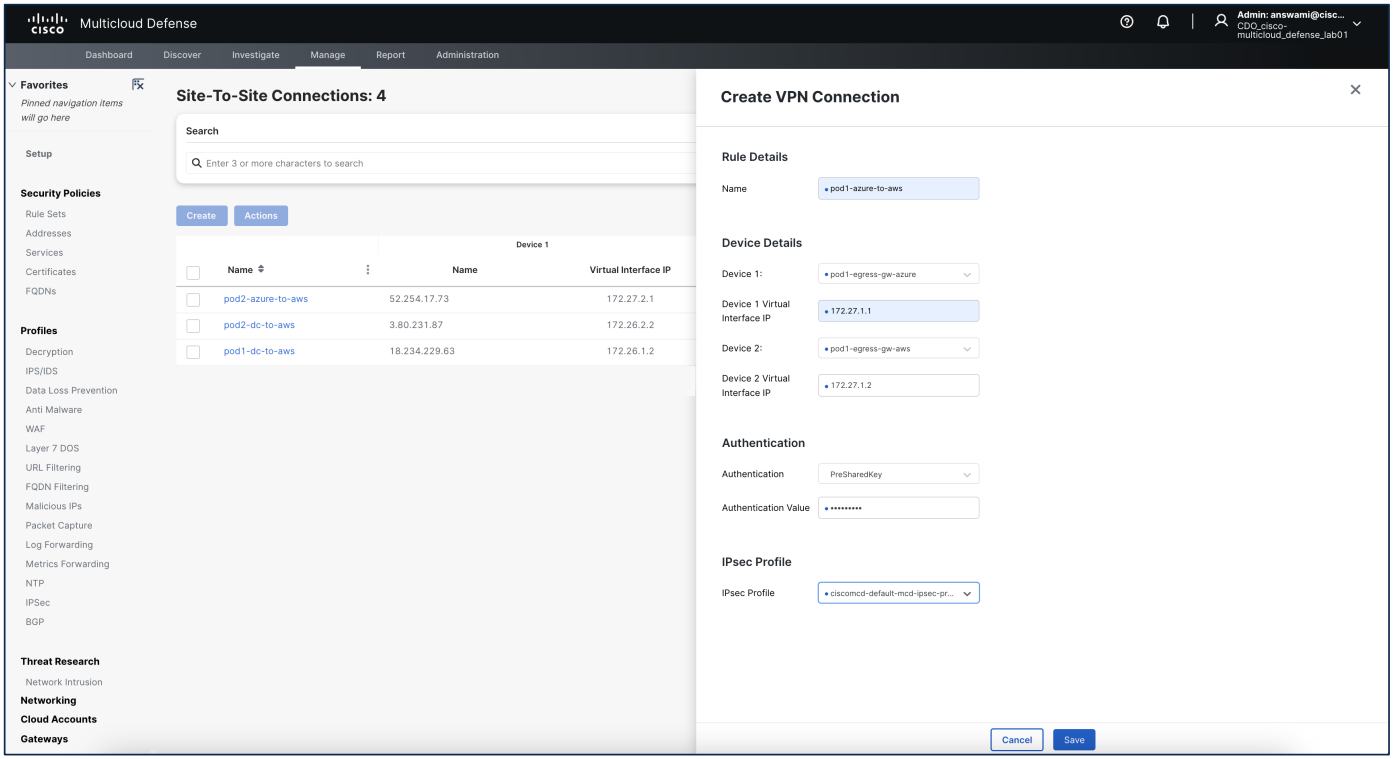
Controller orchestrates VPN configuration

Securely connect cloud environment using fully-orchestrated VPN tunnels

Automated traffic steering

Configure site-to-cloud VPN

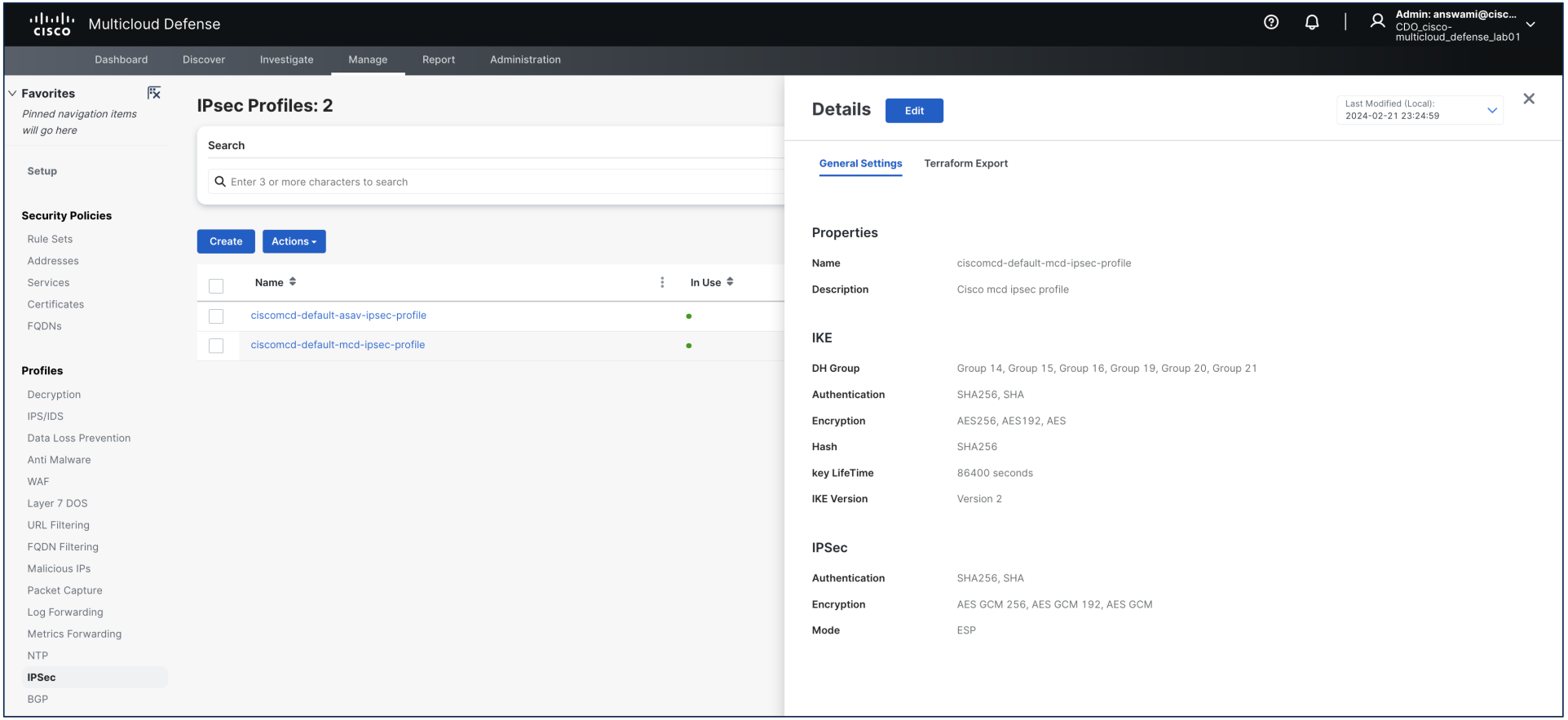
Step1 – add new cloud-to-cloud VPN (Multicloud Defense Controller)

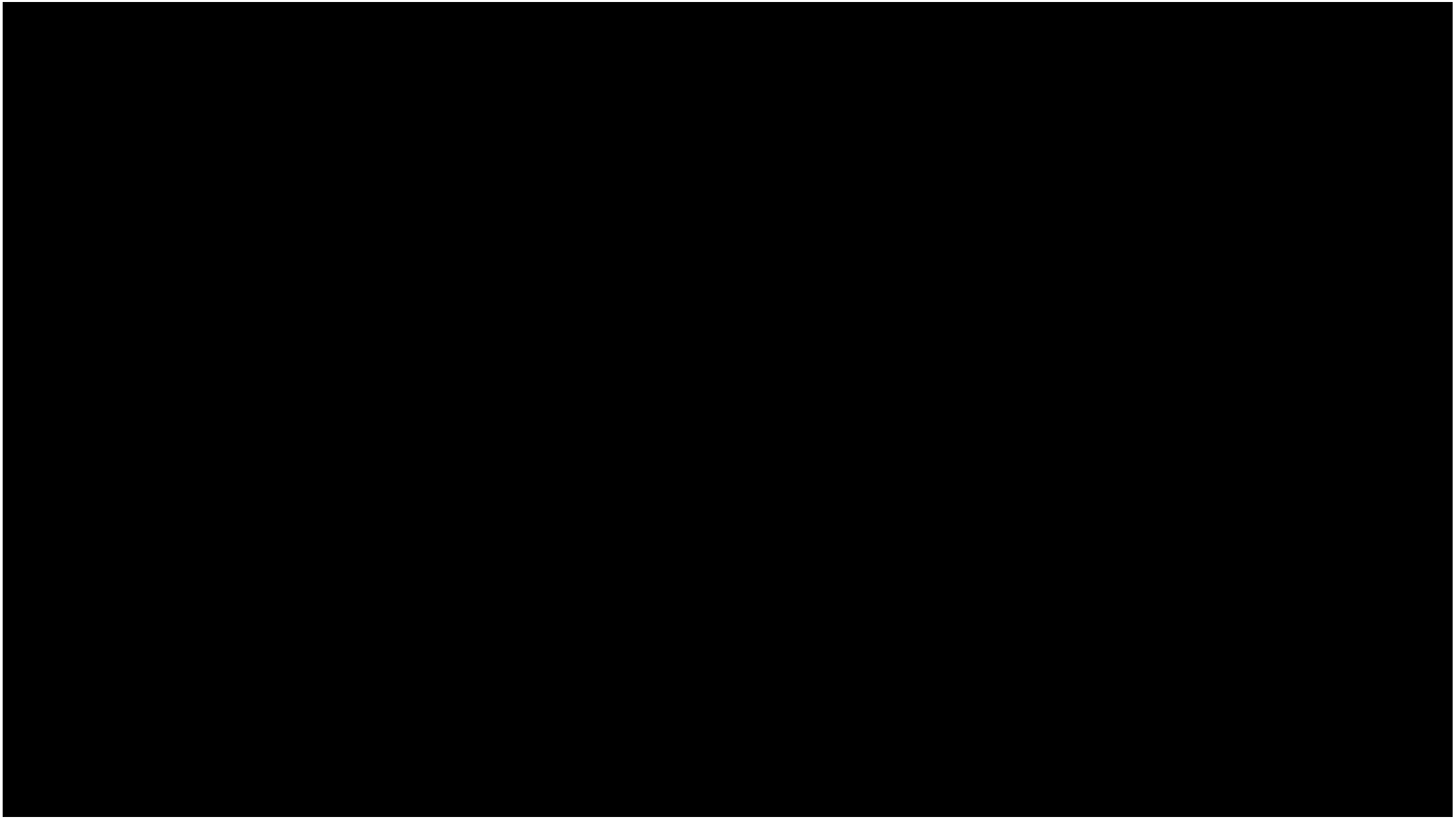


Multicloud Defense Controller configures Multicloud Defense Gateway in AWS and Azure

Configure site-to-cloud VPN

IPsec profile





The bridge to possible