



# 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



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

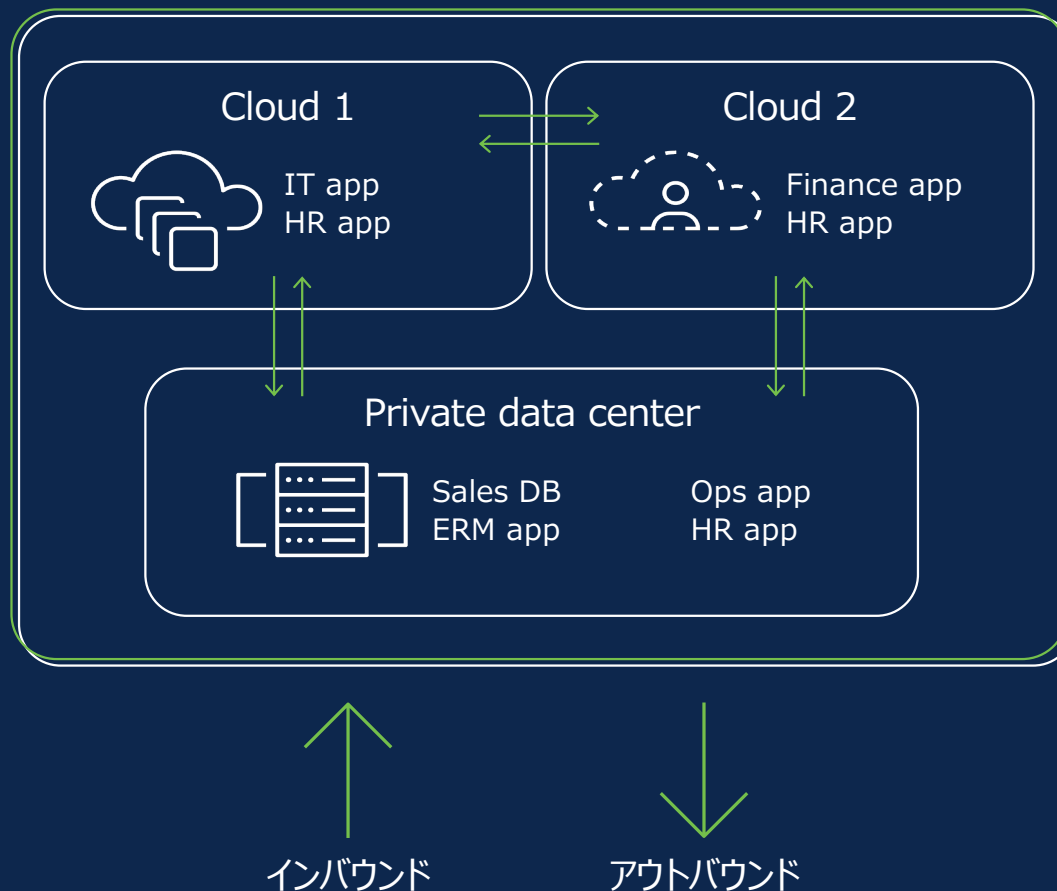
# クラウド化がもたらすネットワークの継続的な変化

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<sup>1</sup>

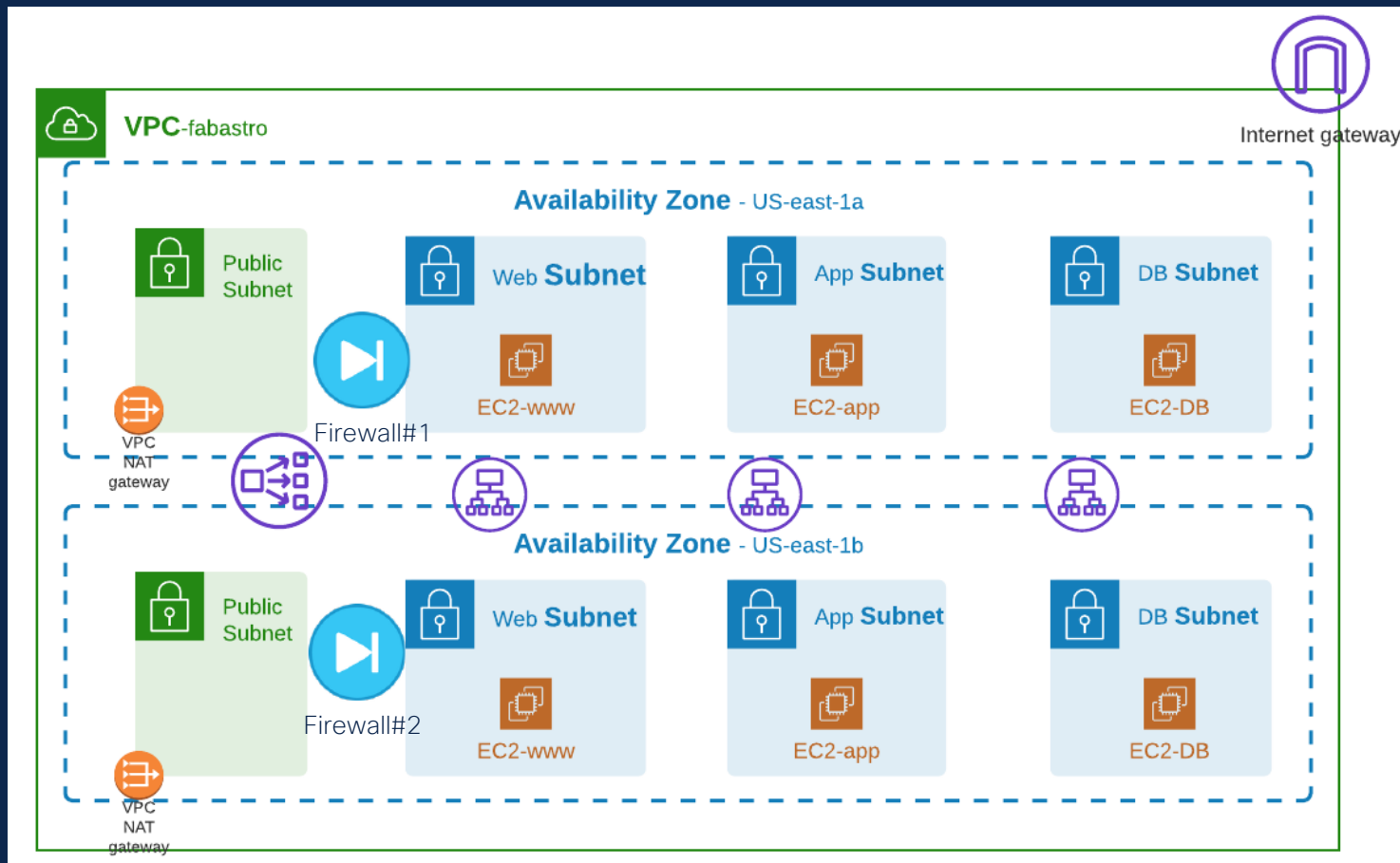
58%

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<sup>1</sup>



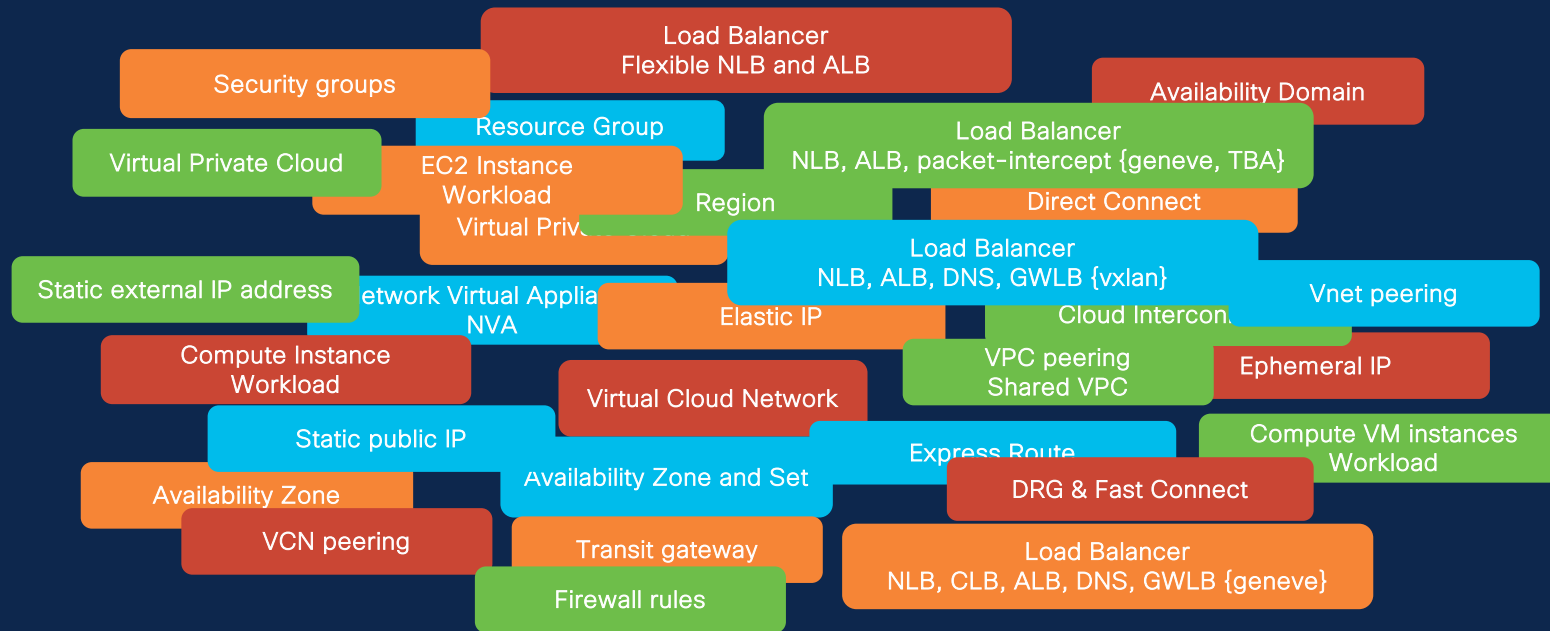
<sup>1</sup> 2022 Cisco Global Hybrid Cloud Trends Report

# クラウド上のアプリケーションをFirewallで守るには？





# 多すぎるクラウドネットワークのコンポーネント



Legend for cloud providers:

- Green bar: Google Cloud
- Blue bar: Microsoft Azure
- Orange bar: aws
- Red bar: 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

セキュリティチーム

IDS /IPS  
AWS Firewall  
Azure Firewall  
AWS Firewall Manager  
Azure Firewall Manager  
3rd party virtual firewall + manager  
Web Application Firewall  
Firewall-as-a-Service  
Cloud-native services  
DLP Solution  
Plus, more managers...

# 製品概要



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

# 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

ORACLE Cloud Search resources, services, documentation, and Marketplace

Compute

Instances in *mcd-demo compartment*

An [instance](#) is a compute host. Choose between virtual machines (VMs) and bare metal instances. The image that you use to launch an instance is called a [boot image](#).

Create Instance Actions

<input type="checkbox"/>	Name	State	Public IP	Private IP	Shape	OCPU count
<input type="checkbox"/>	<a href="#">ciscomcd-oci-egress-vgoyapgd</a>	Terminated	-	-	VM.Standard.E3.Flex	4
<input type="checkbox"/>	<a href="#">ciscomcd-oci-egress-wfuyhjl</a>	Terminated	-	-	VM.Standard.E3.Flex	4
<input type="checkbox"/>	<a href="#">ciscomcd-oci-ingress-yarvktex</a>	Running	132.145.156.153	10.252.1.152	VM.Standard.E3.Flex	4

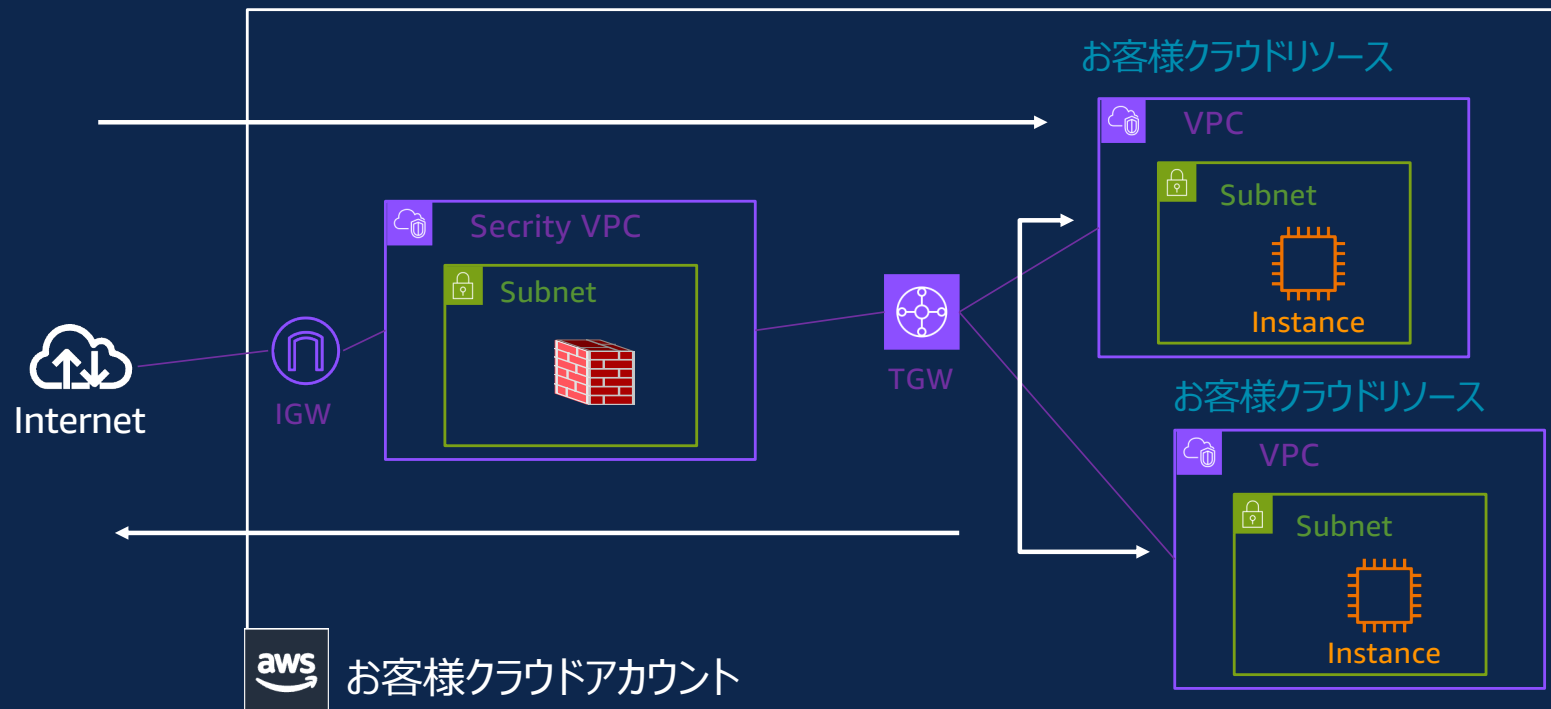
≠ FWaaS

# 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

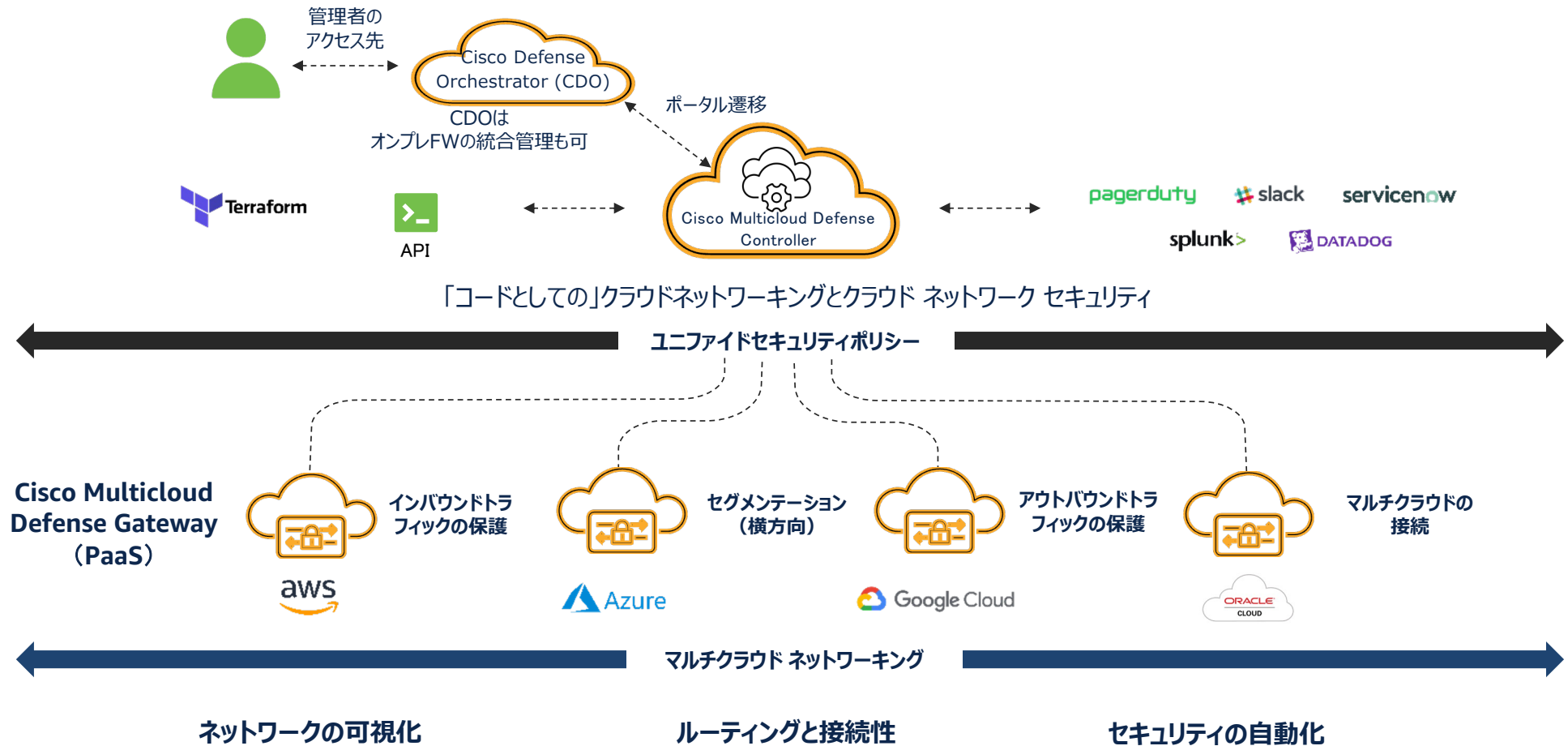
- Ingress
- Egress
- East - West(VPC間)

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



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

# 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

\*Full decryption is needed for FQDN filtering and FQDN-based firewall policy

# AWS



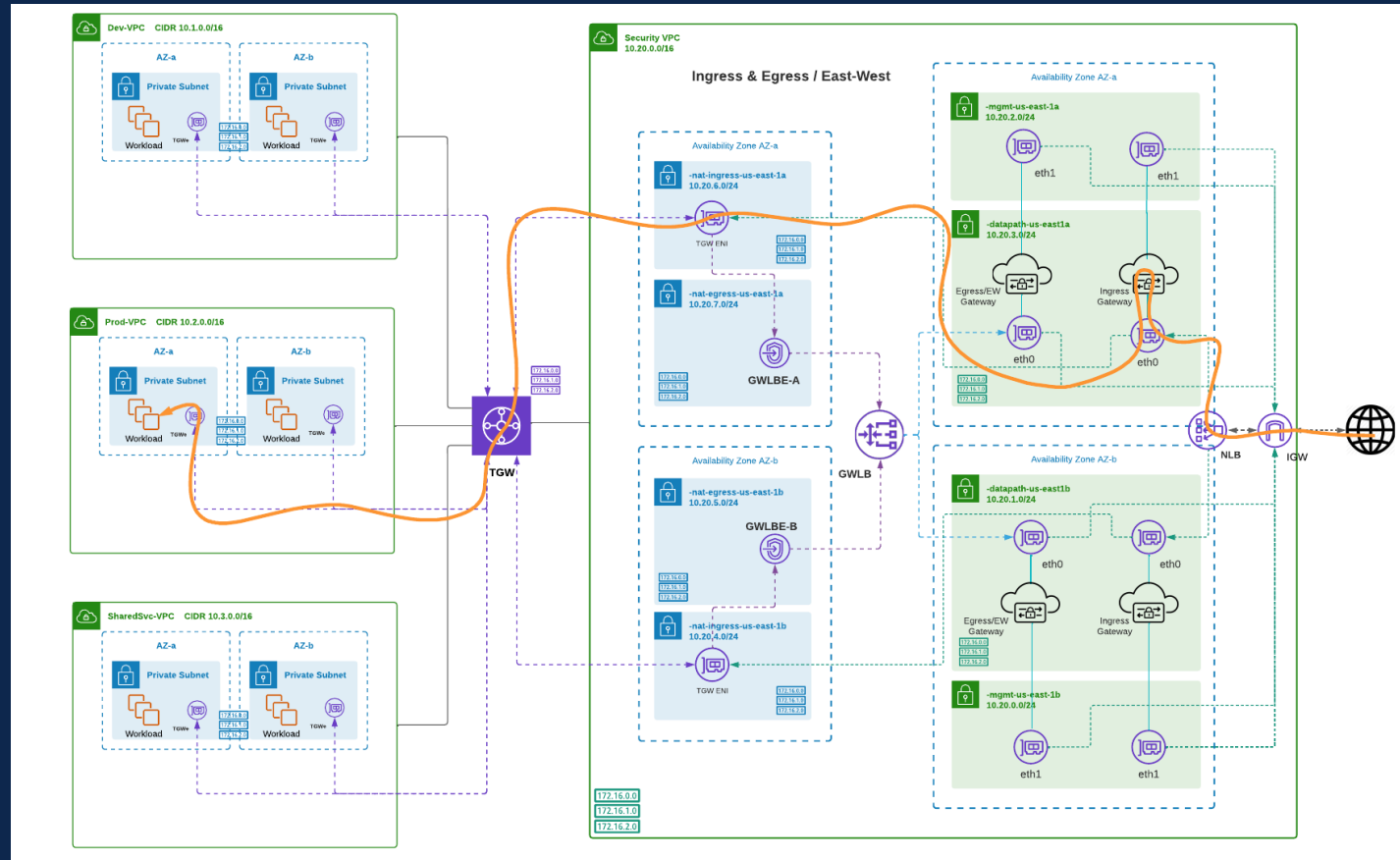
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



# 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



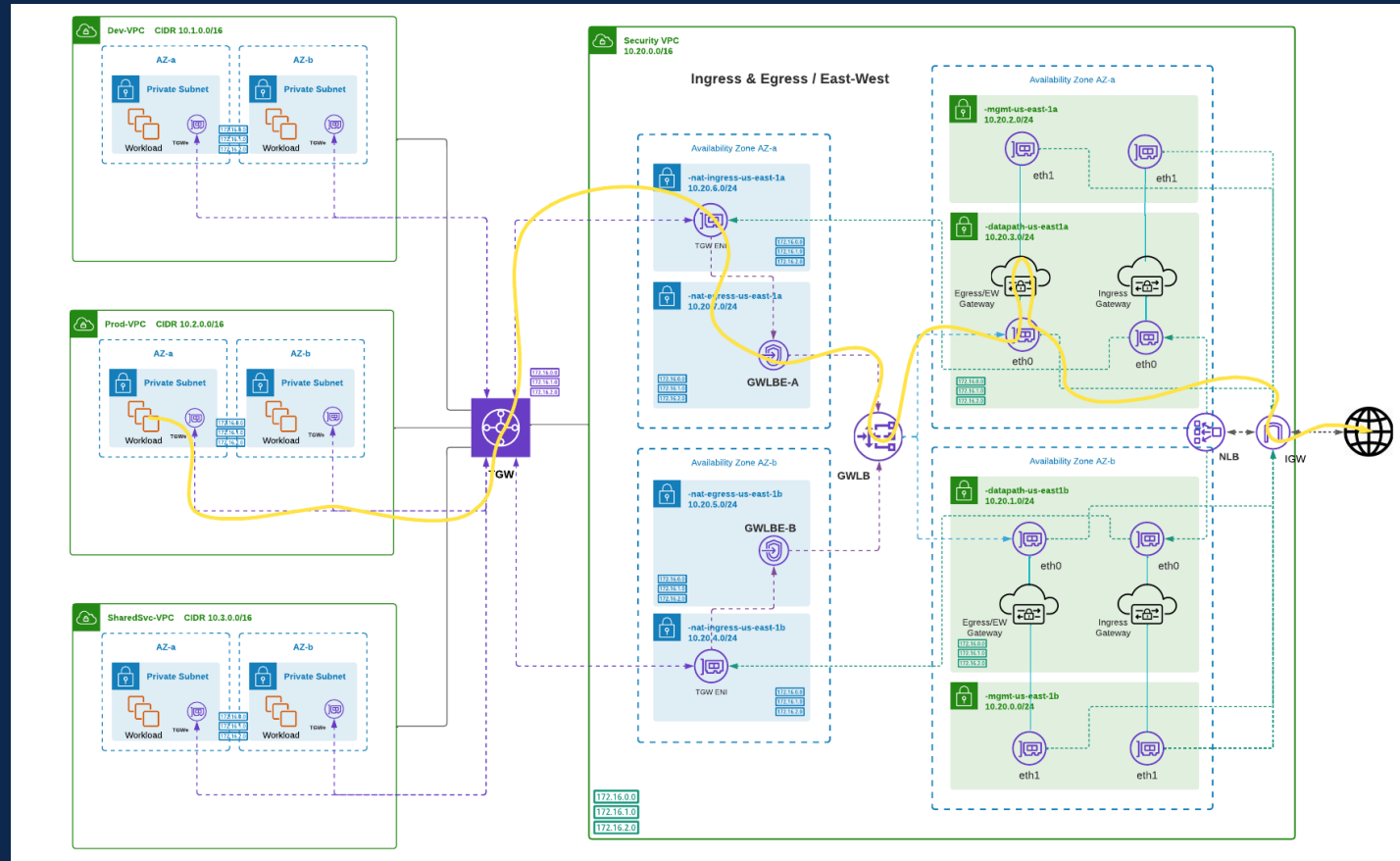
AWS Centralized – Ingress traffic inspection



# 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



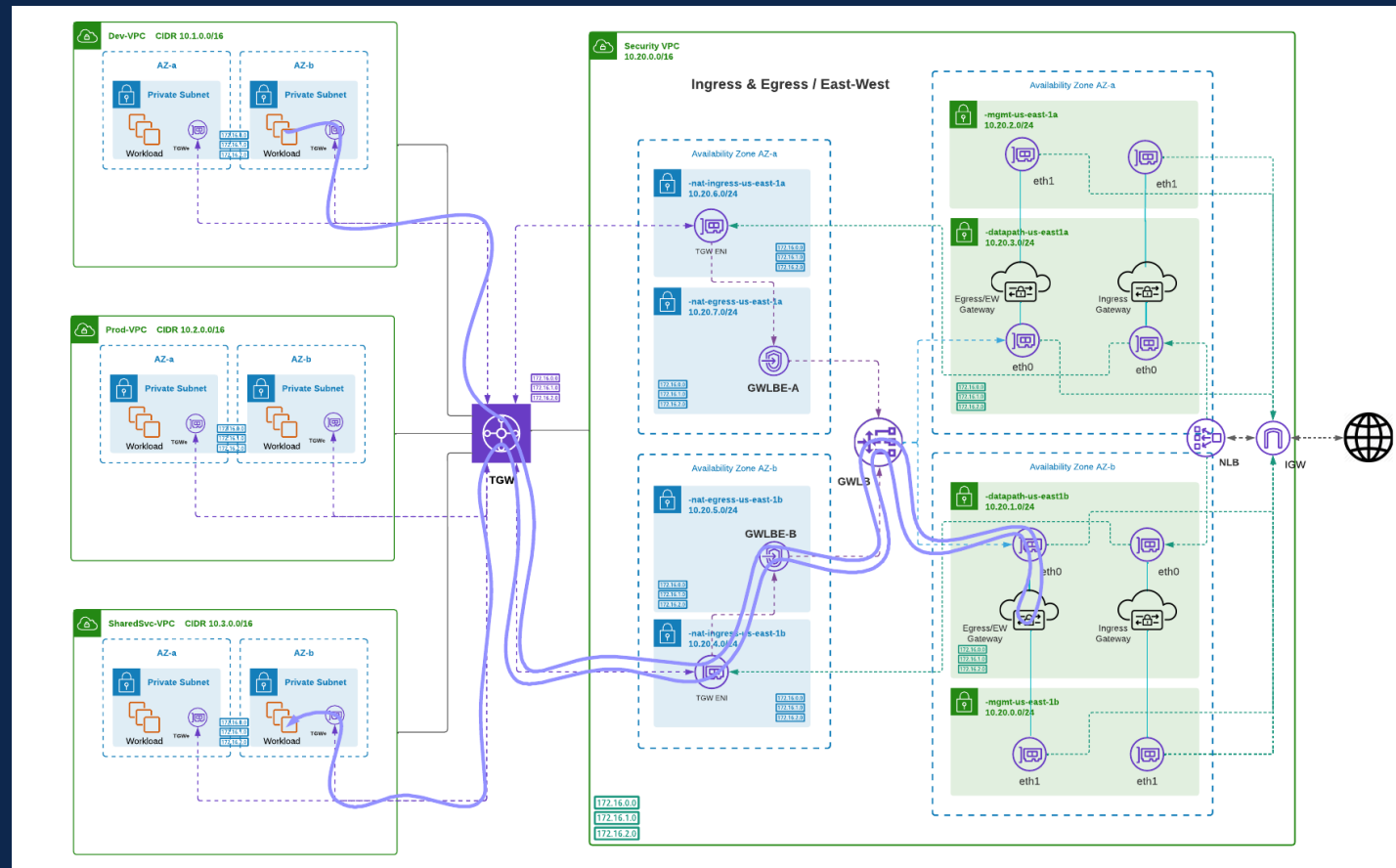
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Confidential

# 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



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Confidential

# Azure

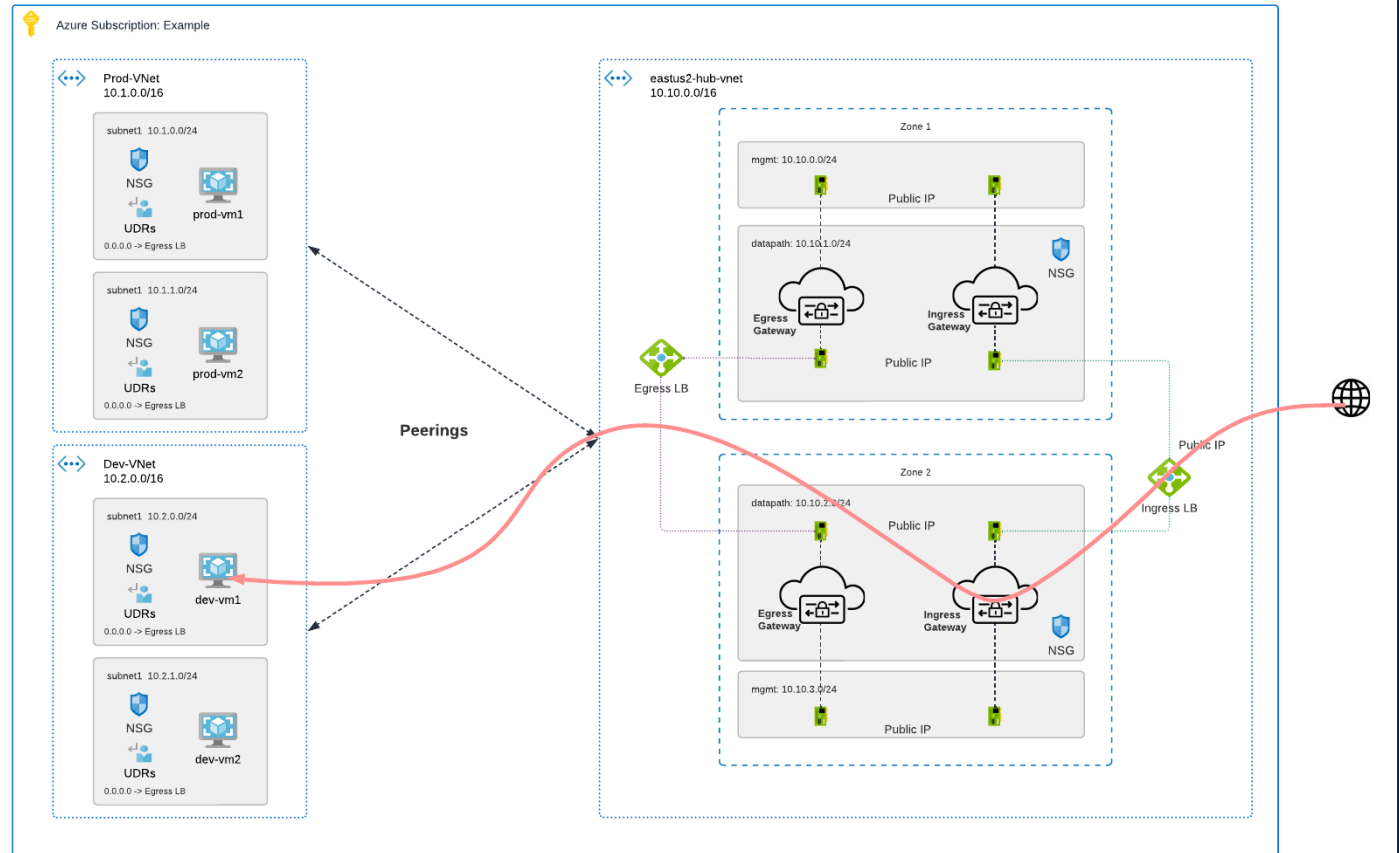


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Azure Centralized Ingress

Controller simplifies orchestration

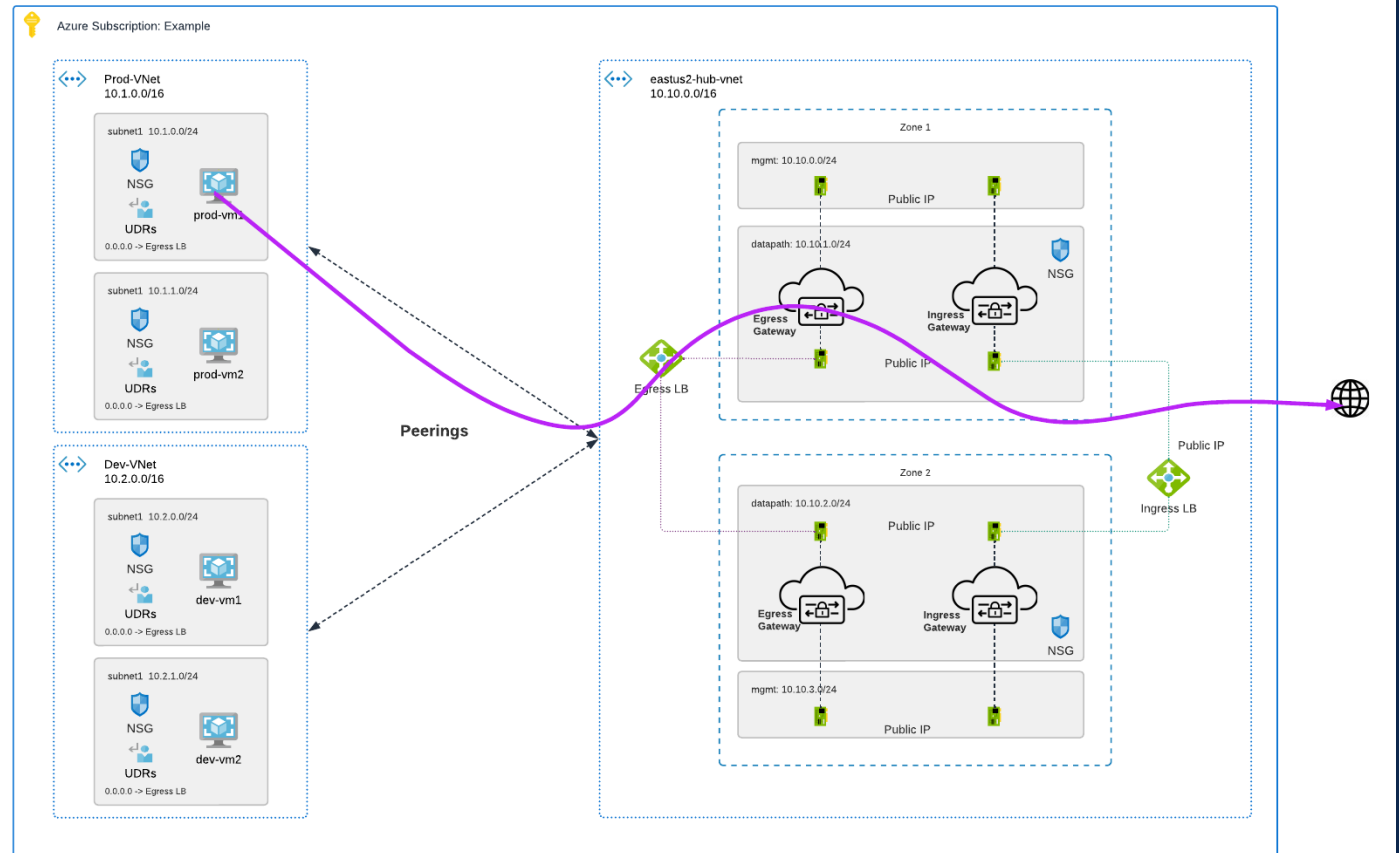
- Security VNet
- Load Balancer
- Multicloud Defense Gateways
  - Ingress Gateway
- Automation
  - Peering
  - Routing
  - Load balancer configuration
  - Autoscaling



# Azure Centralized Egress

## Controller simplifies orchestration

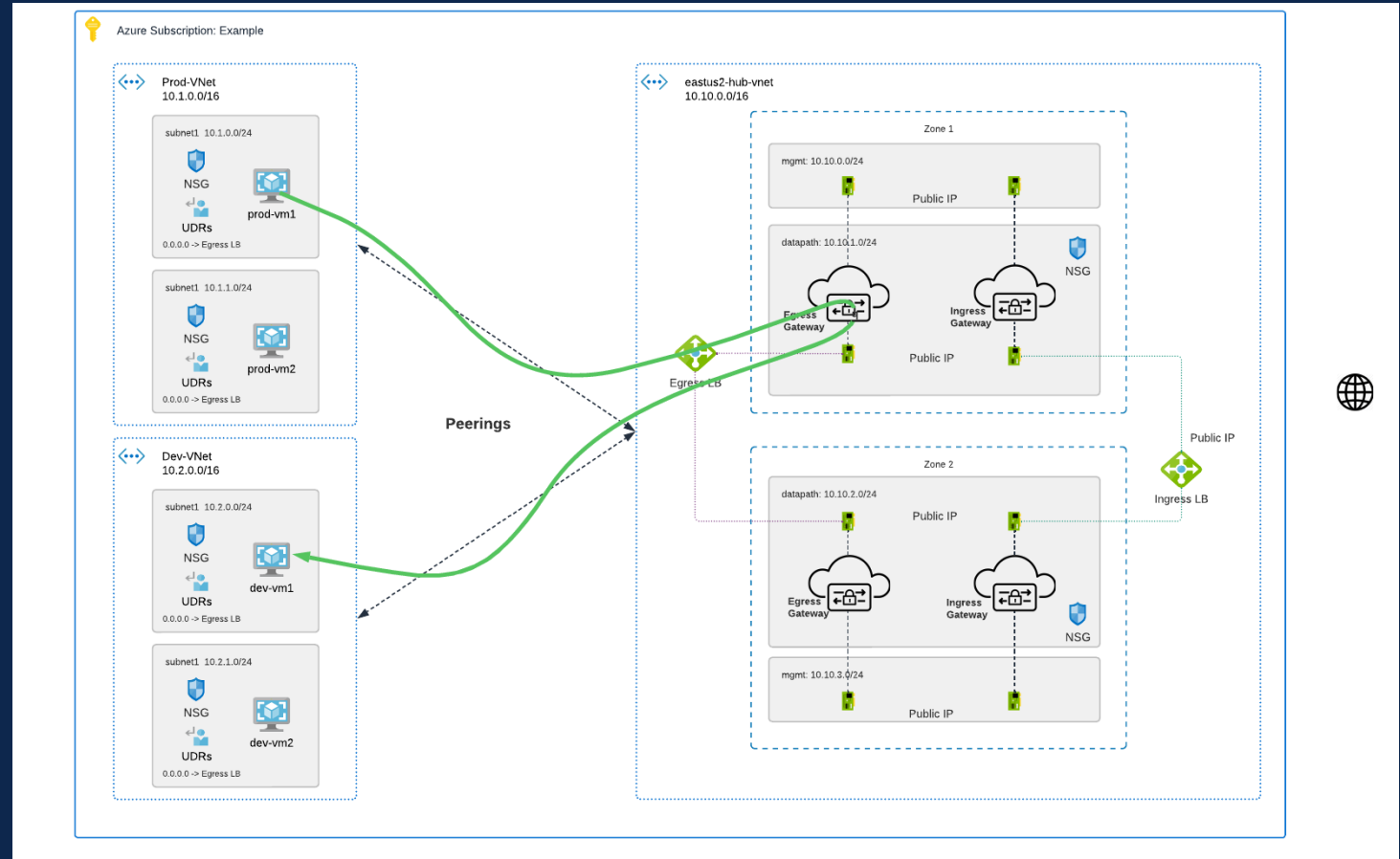
- Security VNet
- Network Load Balancers
- Multicloud Defense Gateways
  - Egress / East-West Gateway
- Automation
  - Peering
  - Routing
  - Load balancer configuration
  - Autoscaling



# Azure Centralized East-West

## Controller simplifies orchestration

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





# 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 ]

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 ]

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

Resource Level	Resource Tag	Resource Tag Value
RESOURCE_INSTANCE	env	prod



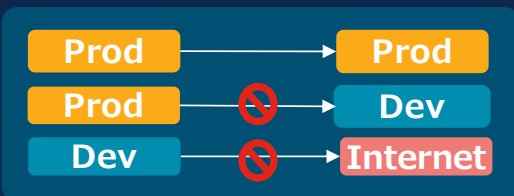
Name	Type	CSP Acct	Region	VPC/VNet
172.16.0.3	IP_ADDR	tmitsue-RunOn-GCP	Montreal   northamerica-northeast1	vpc-a
172.17.0.4	IP_ADDR	tmitsue-RunOn-GCP	Montreal   northamerica-northeast1	vpc-b
172.31.6.195	IP_ADDR	tmitsue-RunOn-AWS	US East (Ohio)   us-east-2	vpc-b512a1de
192.168.0.182	IP_ADDR	tmitsue-RunOn-AWS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

Public



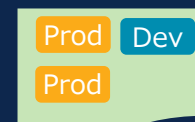
# クラウドリソースタグでマルチクラウドのポリシー制御

全クラウドで守るべき共通ポリシー

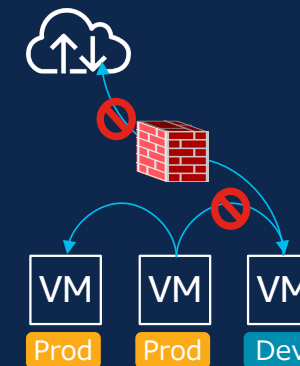
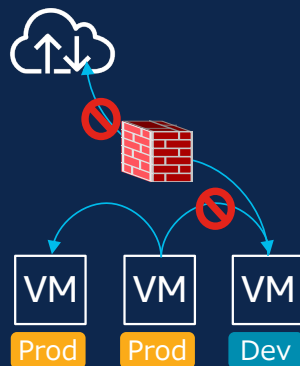
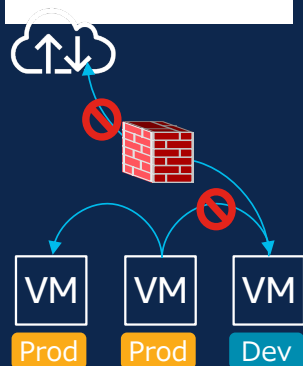


インベントリ情報の収集

(リソースタグ情報含む)



Google Cloud



# IaCによるフルオーケストレーション対応



```
EXPLORER
├── CISCOMCD-DEPLOY
│   ├── ciscomcd
│   │   ├── ciscomcd_gateway.tf U
│   │   ├── ciscomcd_policy_rule_set.tf U
│   │   ├── ciscomcd_service_vpc.tf U
│   │   ├── ciscomcd_spoke_vpc.tf U
│   │   ├── outputs.tf U
│   │   ├── provider.tf U
│   │   ├── variables.tf U
│   │   ├── .gitignore
│   │   ├── account1-us-east-1.tfvars
│   │   ├── ciscomcd-deploy.sh U
│   │   ├── main.tf
│   │   ├── provider.tf
│   │   ├── README.md
│   │   └── variables.tf
└── ciscomcd_gateway.tf U X
    ciscomcd > ciscomcd_gateway.tf > resource "ciscomcd_gateway" "ingress_gateway"
    1 # Cisco MCD Terraform Documentation
    2 # https://registry.terraform.io/providers/ciscomcd-security/ciscomcd/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 "ciscomcd_gateway" "ingress_gateway" {
    10     name                = var.ciscomcd_ingress_gateway_name
    11     csp_account_name    = var.ciscomcd_aws_account_name
    12     gateway_image       = var.ciscomcd_ingress_gateway_version
    13     instance_type       = var.ciscomcd_ingress_gateway_instance_type
    14     mode                 = "HUB"
    15     security_type       = var.ciscomcd_ingress_gateway_security_type
    16     policy_rule_set_id  = ciscomcd_policy_rule_set.ingress_policy.rule_set_id
    17     #policy_rule_set_id = data.ciscomcd_policy_rule_set.ingress_policy.rule_set_id
    18     ssh_key_pair        = var.ciscomcd_ingress_gateway_ssh_key_pair
    19     aws_iam_role_firewall = var.ciscomcd_firewall_role_name
    20     region              = var.aws_account_region
    21     vpc_id              = ciscomcd_service_vpc.service_vpc.id
    22     min_instances       = var.ciscomcd_ingress_gateway_autoscale_min
    23     max_instances       = var.ciscomcd_ingress_gateway_autoscale_max
    24     gateway_state       = var.ciscomcd_ingress_gateway_status
    25     # settings {
    26     #   name = "controller.use_internal_lb"
    27     #   value = var.ciscomcd_ingress_gateway_internal_lb
    28     # }
    29
    30
```

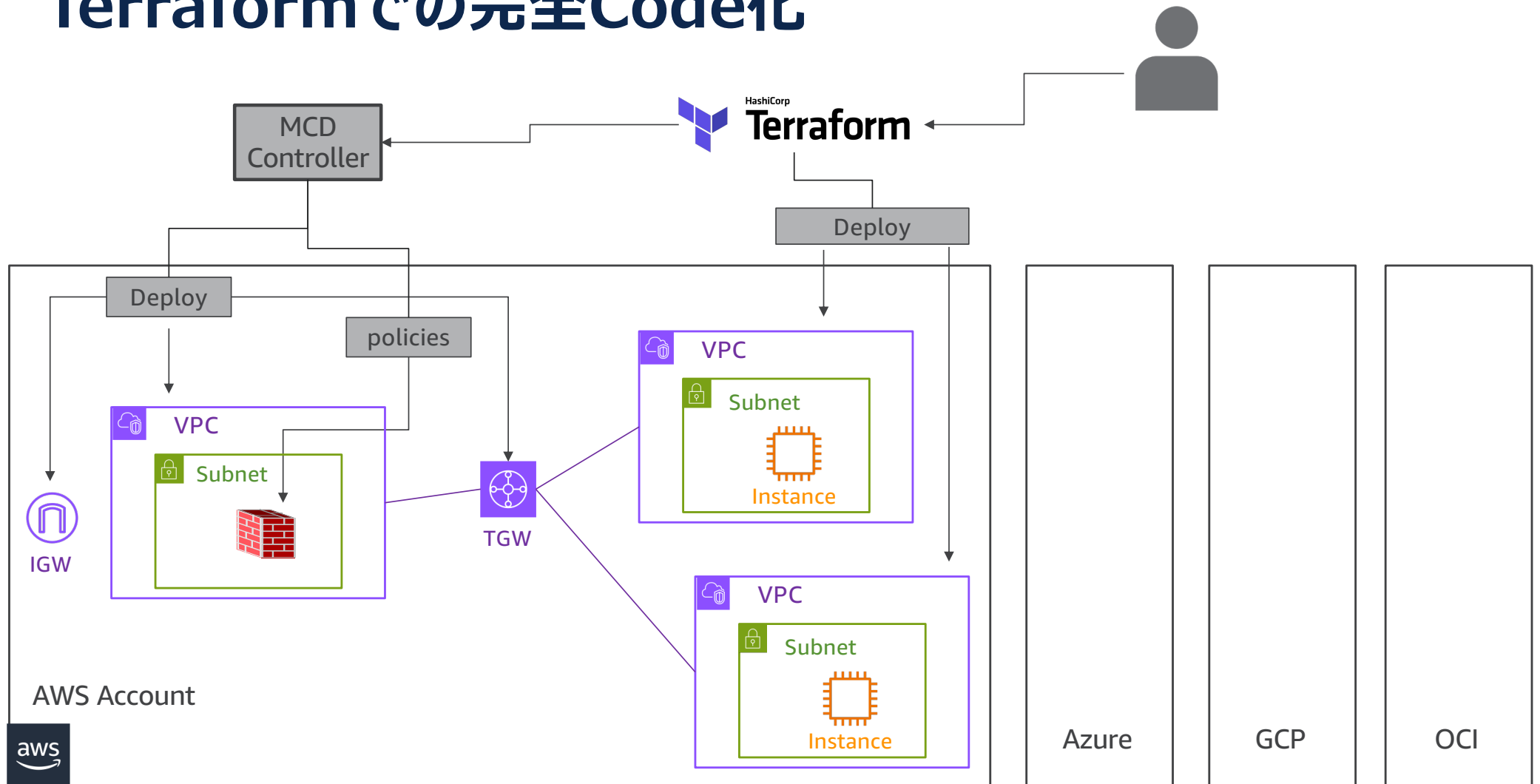
<https://registry.terraform.io/providers/CiscoDevNet/ciscomcd/latest/docs>



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

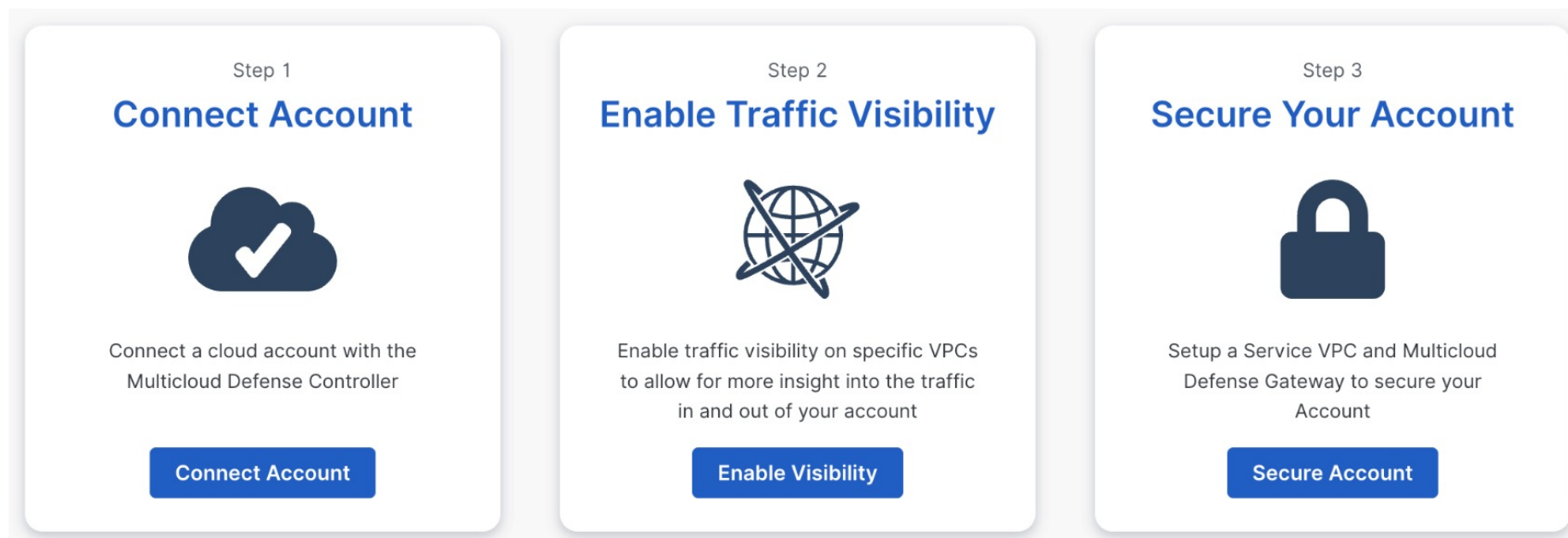
Cisco Confidential

# 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

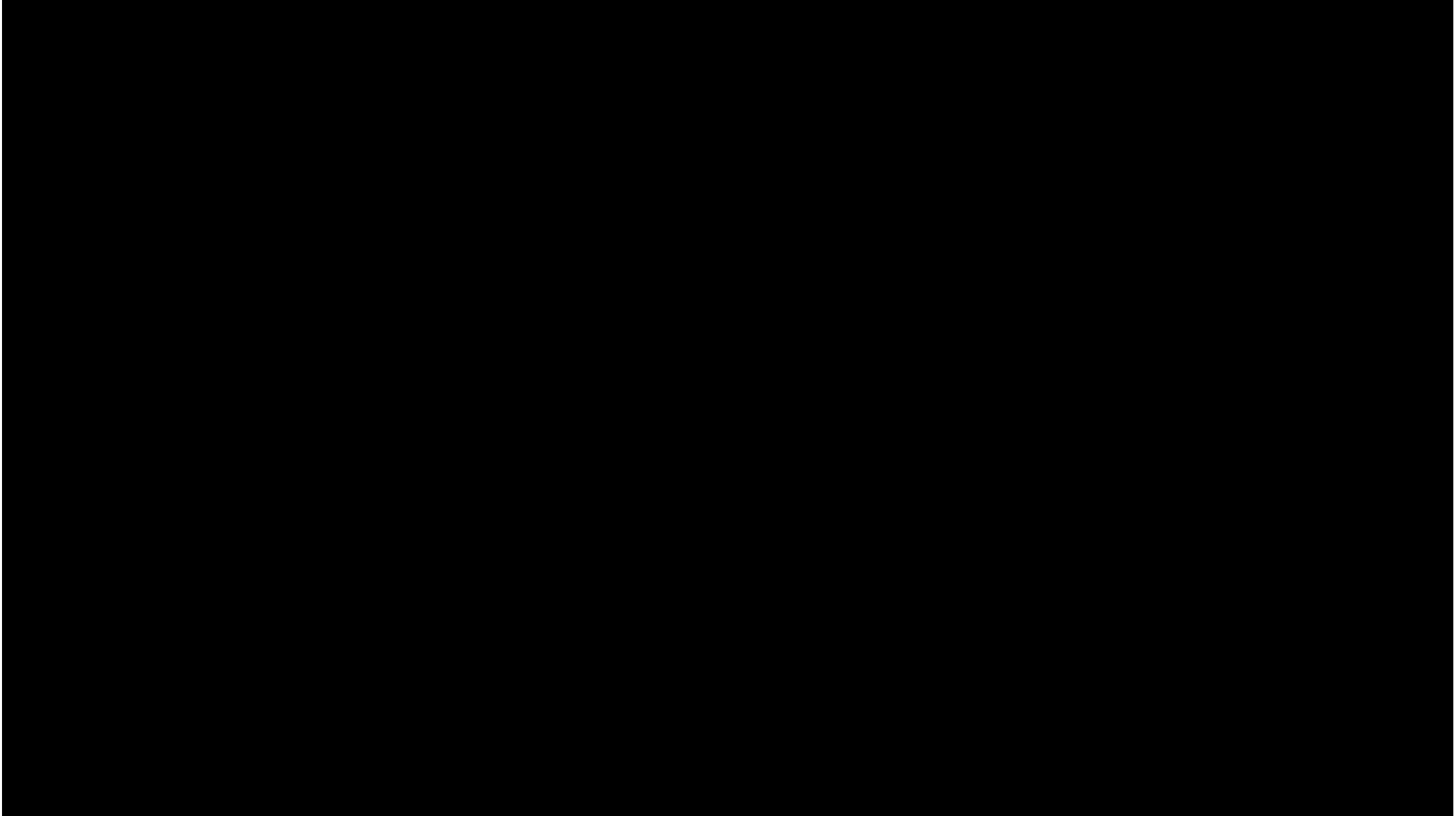


クラウドアカウントのオンボーディング  
(登録)

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)

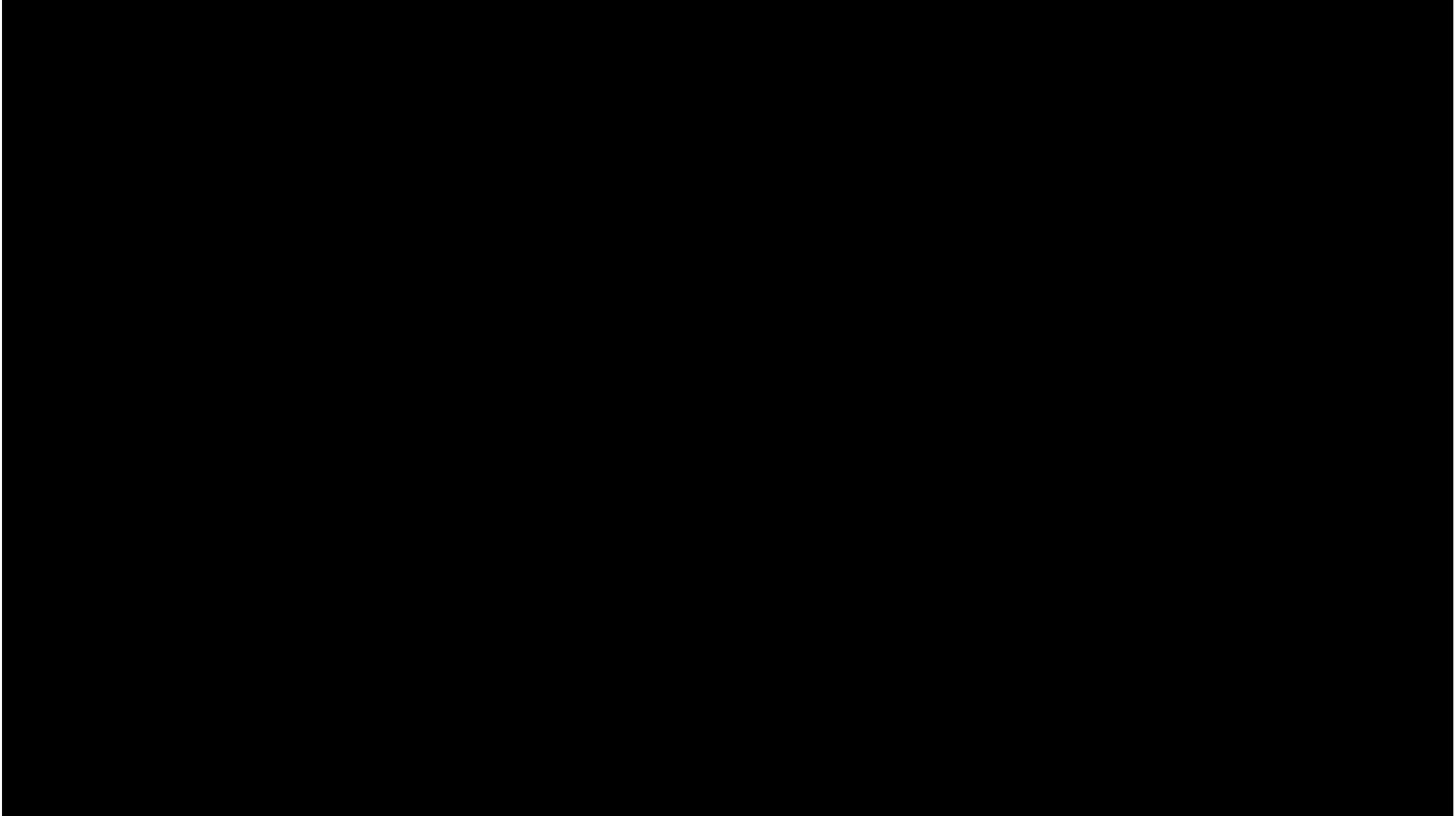
オーケストレーションとオートメーション  
(GWの構築と管理)

Onboarding



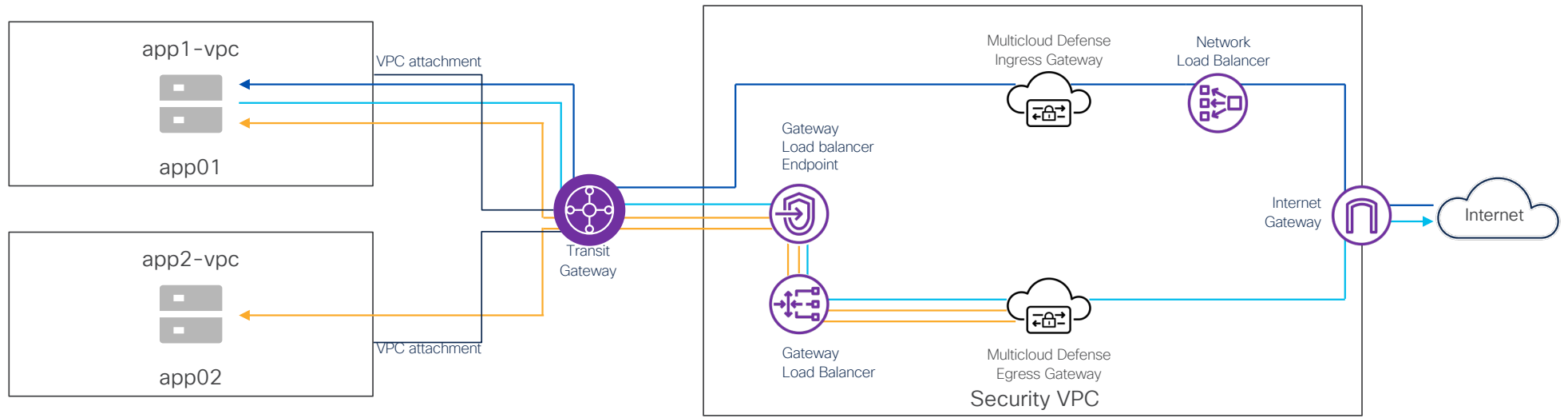
Visibility

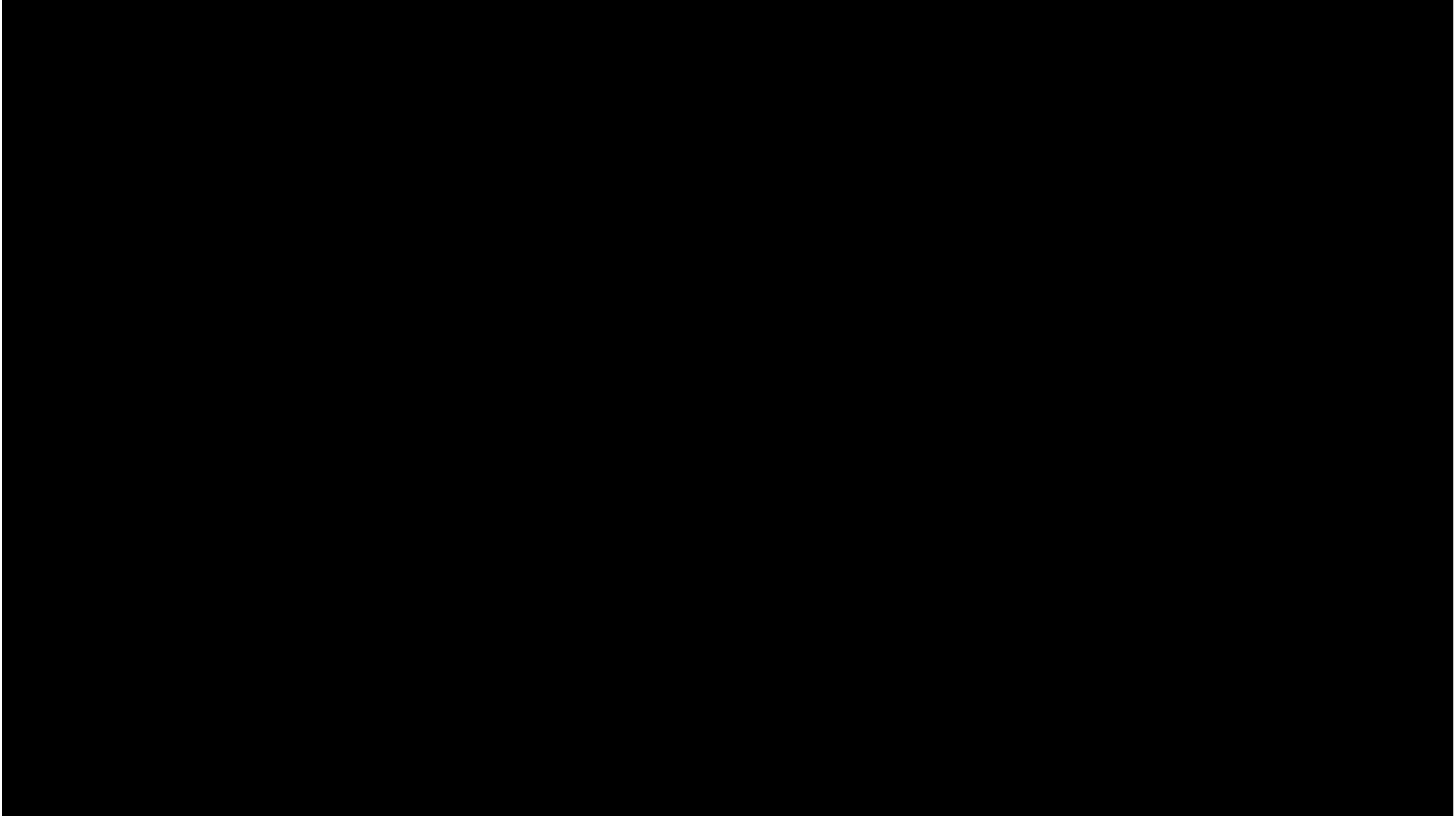




Secure your VPC

# Secure Your Account Demo





# 料金体系



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

# 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 × 24 (1日の時間) × 365 (1年の日数) × 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 (\$5/Month)

1Web ACLあたり

Rule (\$1/Month)

1Ruleあたり

Requests (\$0.60/100million requests)



# 最新アップデート



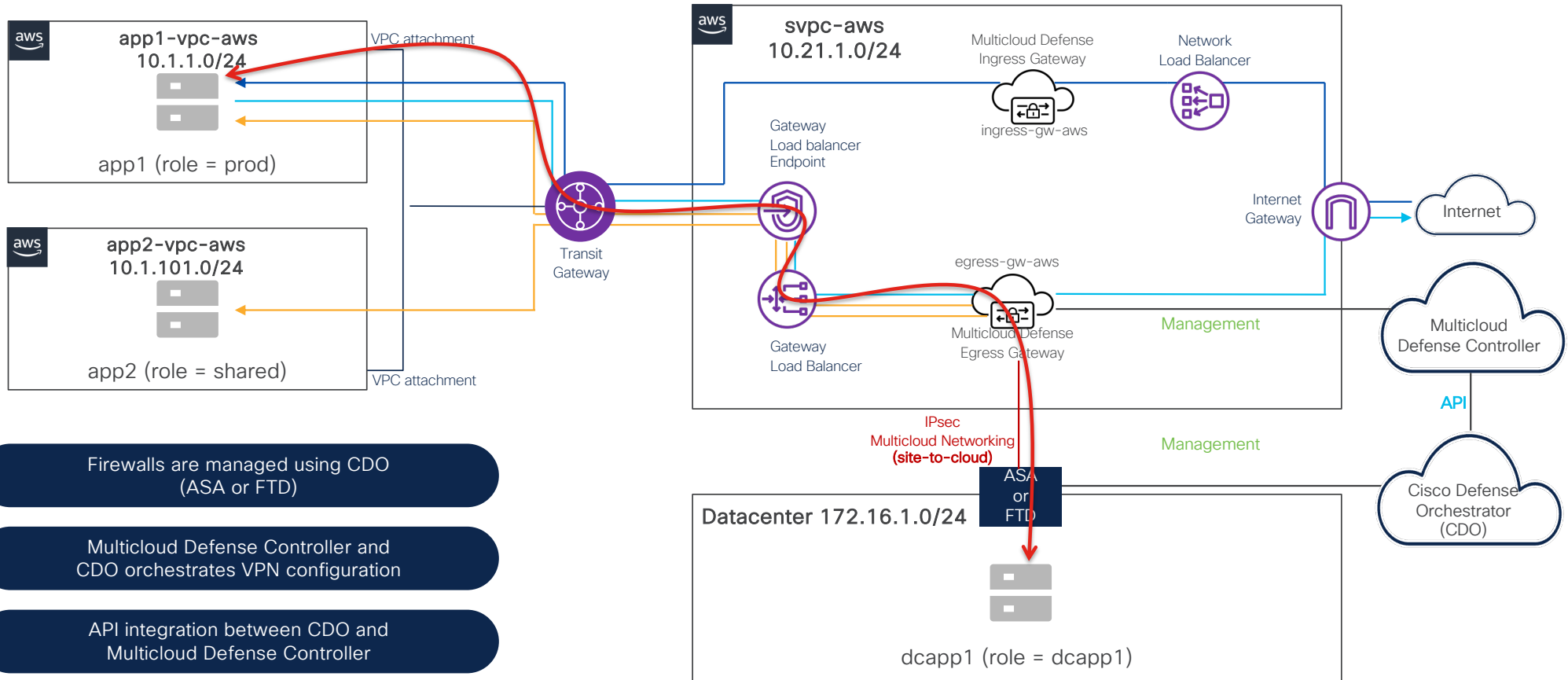
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



# 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

The screenshot displays the Cisco Multicloud Defense interface. The top navigation bar includes 'Dashboard', 'Discover', 'Investigate', 'Manage' (highlighted with a red box), 'Report', and 'Administration'. The user profile in the top right shows 'Admin: answami@cisc...' with a dropdown arrow. The left sidebar contains a 'Favorites' section and a 'Security Policies' section with various options like 'Rule Sets', 'Addresses', 'Services', 'Certificates', and 'FQDNs'. The 'Profiles' option is highlighted with a red box, and the 'BGP' option is also highlighted with a red box. The main content area is titled 'BGP Profiles: 4' and features a 'Filters and Search' section with a 'Switch to Advanced Search' link and a search input field. Below this are 'Create' and 'Actions' buttons, and a 'Refresh' button. A table lists the BGP profiles with columns for Name, In Use, LocalAS, IP, Neighbors, AS, and Last Modified. The table data is as follows:

<input type="checkbox"/>	Name	In Use	LocalAS	IP	Neighbors	AS	Last Modified
<input type="checkbox"/>	pod1-aws-bgp	●	65201	172.27.1.1, 172.26.1.1	65301, 65101		2024-04-18T20:39:19.028Z
<input type="checkbox"/>	pod1-azure-bgp	●	65301	172.27.1.2	65201		2024-04-18T20:40:29.245Z
<input type="checkbox"/>	pod2-aws-bgp	●	65202	172.26.2.1, 172.27.2.1	65102, 65302		2024-04-18T21:39:54.092Z
<input type="checkbox"/>	pod2-azure-bgp	●	65302	172.27.2.2	65202		2024-04-18T21:41:01.040Z

**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.

**Details** [Edit](#) Last Modified (Local): 2024-04-18 13:39:19

[General Settings](#) Terraform Export

**Properties**

Name pod1-aws-bgp

Description

Neighbors

Neighbor	
IPAddress	172.27.1.1
AutonomousSystem	65301
Neighbor	
IPAddress	172.26.1.1
AutonomousSystem	65101

**Details** [Edit](#) Last Modified (Local): 2024-04-18 13:39:19

General Settings [Terraform Export](#)

In order to export and use the selected ipsec object **pod1-aws-bgp**, you need to complete the following steps:

**Step 1:** Download the Terraform File [Download](#)

or

Copy the resource block below and insert it into your Terraform script.

```
resource "ciscoconfd_profile_bgp" "pod1-aws-bgp" {
  name = "pod1-aws-bgp"
  local_as = 65201
  neighbor {
    ip_address = "172.27.1.1"
    autonomous_system = 65301
  }
  neighbor {
    ip_address = "172.26.1.1"
    autonomous_system = 65101
  }
}
```

[COPY CODE](#)

**Step 2:** Execute Command:

```
terraform import "ciscoconfd_profile_bgp"."pod1-aws-bgp" 14
```

[COPY CODE](#)

# BGP Profile contd.

The screenshot displays the Cisco Multicloud Defense interface. The 'Manage' tab is active, showing a list of gateways. The gateway 'pod1-egress-gw-aws' is selected, and its configuration page is open. The 'BGP Profile' dropdown is set to 'pod1-aws-bgp'.

**Gateways: 6**

Name	Account	CSP Type
pod1-ingress-gw-aws	cisco-multicloud-defens	AWS
pod1-ingress-gw-azure	cisco-multicloud-defens	AZURE
pod2-egress-gw-azure	cisco-multicloud-defens	AZURE
pod1-egress-gw-azure	cisco-multicloud-defens	AZURE
pod2-egress-gw-aws	cisco-multicloud-defens	AWS
<b>pod1-egress-gw-aws</b>	<b>cisco-multicloud-defens</b>	<b>AWS</b>

**Configuration Details:**

- Ruleset: pod1-egress-policy
- Availability Zone: us-east-1a
- Mgmt. Subnet: subnet-04dea5de9730fef5e | pod1-svpc-aws-mgmt-us-east-1a
- Datapath Subnet: subnet-0fa17711d247b6e9 | pod1-svpc-aws-datapath-us-east-1a
- IAM Role for Firewall: ciscocomd-gateway-role
- Management Security Group: sg-0f01db1ff06dfeb5e | pod1-svpc-aws...
- Datapath Security Group: sg-0b2f1b3fbdad3cfd4 | pod1-svpc-aw...
- EBS Encryption:
- Packet Capture Profile: Select Packet Capture Profile
- Log Profile: Select Log Profile
- Metrics Forwarding Profile: Select Metrics Profile
- NTP Profile: Select NTP Profile
- Public IP:
- Disable Public IP:
- VPN Settings: BGP Profile: pod1-aws-bgp

# Configure site-to-cloud VPN

## Configure site-to-site VPN tunnel

The screenshot shows the Cisco Defense Orchestrator (CDO) interface for configuring a VPN. The top navigation bar includes the Cisco logo, 'Defense Orchestrator', and 'VPN'. A search bar is present with the text 'Search by tunnel name, device name, or IP'. The main content area displays a table with columns: Name, Status, Peer 1 Name, Peer 1 IP, Peer 2 Name, and Peer 2 IP. A dropdown menu is open over the 'VPN' menu item in the left sidebar, showing options: 'FTD Site-to-Site VPN', 'Site-to-Site VPN' (highlighted with a red box and a checkmark), 'FTD Remote Access VPN Configuration', 'ASA Remote Access VPN Configuration', and 'Remote Access Monitoring'. On the right side, a panel lists VPN types: 'Site-to-Site VPN ASA', 'Site-to-Site VPN FTD / ASA', 'Site-to-Site VPN Multicloud Defense' (highlighted with a red box), and 'SASE Tunnel ASA to Umbrella'. A blue '+' button is visible in the top right corner of the main content area.

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

The screenshot displays the Cisco Defense Orchestrator interface for creating a site-to-site VPN. The main heading is "Create Site-to-Site VPN". The left sidebar contains a navigation menu with options like Dashboard, Multicloud Defense, Inventory, Configuration, Policies, Objects, VPN (highlighted), Events & Monitoring, Analytics, Change Log, Jobs, Tools & Services, and Settings. The central area shows a progress indicator with four steps: 1. Peer Devices (active), 2. Tunnel Details, 3. IKE Settings, and 4. Finish. The configuration form includes a "Configuration Name" field containing "pod1-dc-to-aws". Below this are two peer configuration boxes. "Peer 1" includes fields for "Device 1" (pod1-asa-dc), "VPN Access Interface" (outside), "LAN Interfaces" (inside), and "Public IP (optional)" (13.56.122.71). "Peer 2" includes a field for "Device 2" (pod1-egress-gw-aws). A "Routing" section at the bottom has a "Networks" label and a dashed box with a "+ Add Networks" button. A "Next" button is located at the bottom right of the configuration area.

# Configure site-to-cloud VPN

## Step 2 – Configure VTI interfaces

The screenshot displays the Cisco Defense Orchestrator interface for configuring a Site-to-Site VPN. The main heading is "Create Site-to-Site VPN". The interface is divided into a sidebar menu on the left and a main configuration area on the right. The sidebar menu includes options like Dashboard, Multicloud Defense (marked as "New"), Inventory, Configuration, Policies, Objects, VPN (highlighted), Events & Monitoring, Analytics, Change Log, Jobs, Tools & Services, and Settings. The main configuration area shows a progress indicator with four steps: 1. Peer Devices, 2. Tunnel Details (current step), 3. IKE Settings, and 4. Finish. Below the progress indicator, there are two configuration cards for Peer 1 and Peer 2. Peer 1's Virtual Interface Tunnel IP is 172.26.1.1, and Peer 2's is 172.26.1.2. There are "Previous" and "Next" buttons at the bottom of the configuration area.



# Configure site-to-cloud VPN

## Step 3 – Configure Pre-Shared Key

The screenshot displays the Cisco Defense Orchestrator interface for configuring a Site-to-Site VPN. The main heading is "Create Site-to-Site VPN". On the left, a navigation menu includes "Dashboard", "Multicloud Defense" (marked as "New"), "Inventory", "Configuration" (with sub-items: Policies, Objects, VPN, Analytics, Change Log), and "Events & Monitoring" (with sub-item: Jobs). The "VPN" item is currently selected. The central area shows a progress indicator with four steps: "Peer Devices", "Tunnel Details", "IKE Settings" (the current step, highlighted with a blue circle and the number 3), and "Finish". The "Pre-Shared Key" configuration field is active, showing a text input with masked characters and a "Show" button. Below the key field are "Previous" and "Next" navigation buttons.

# Configure site-to-cloud VPN

## Step 4 – Deploy configuration on Firewall and Multicloud Defense Gateway

**Create Site-to-Site VPN**

- Peer Devices
- Tunnel Details
- IKE Settings
- 4 Finish**

Tunnel Name: pod1-dc-to-aws

**PEER DEVICES**

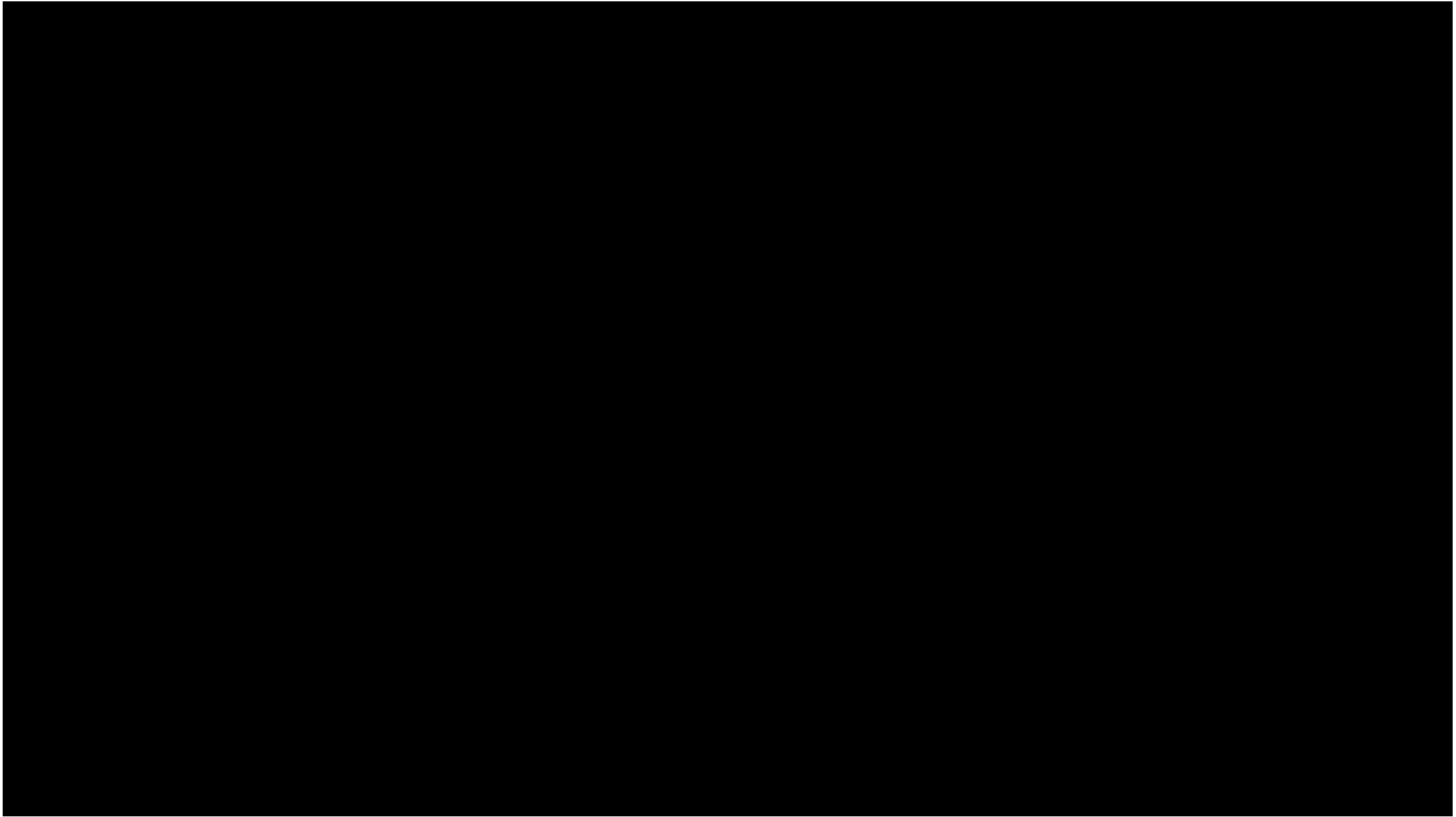
Device	pod1-asa-dc	pod1-egress-gw-aws
VPN Access Interface	outside	--
IP Address	172.16.1.15	--
Public IP Address	13.56.122.71	--
LAN Interfaces	inside	--
Networks	--	--

**TUNNEL DETAILS**

VTI Address	172.26.1.1	172.26.1.2
-------------	------------	------------

Deploy changes to ASA immediately ⓘ

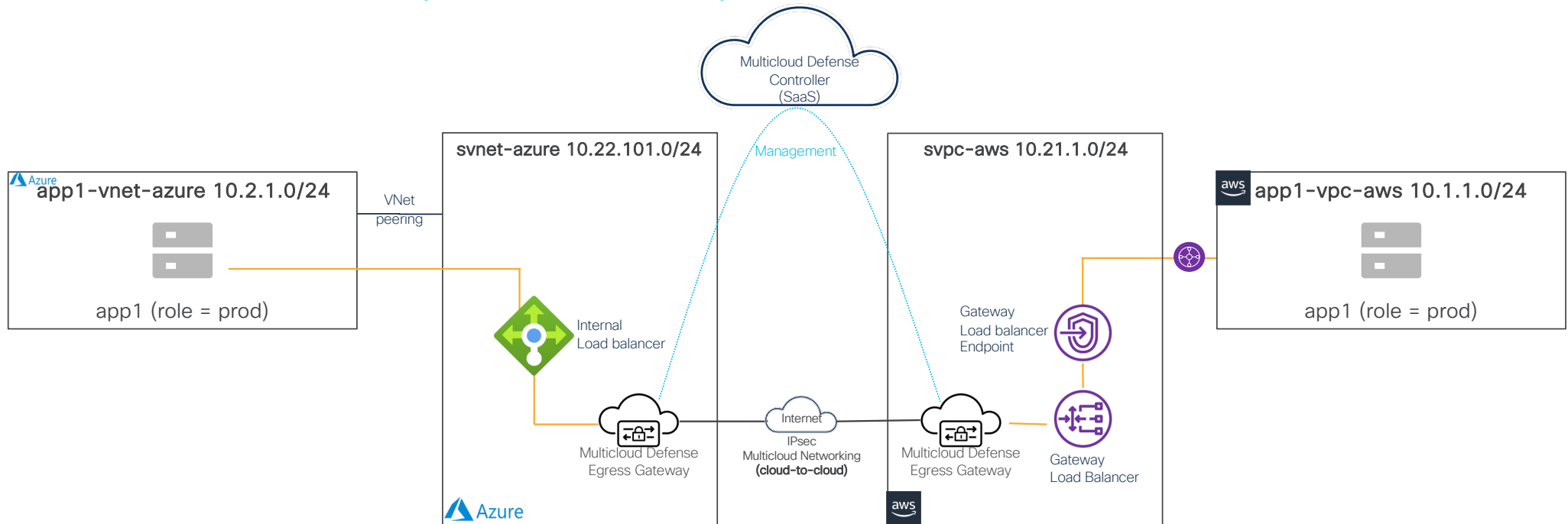
[Previous](#) [Submit](#)



# 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)

The screenshot displays the Cisco Multicloud Defense Controller interface. The top navigation bar includes 'Dashboard', 'Discover', 'Investigate', 'Manage', 'Report', and 'Administration'. The user is logged in as 'Admin: answami@cisc...'. The main content area is split into two panels. The left panel, titled 'Site-To-Site Connections: 4', shows a search bar and a table of existing connections. The right panel, titled 'Create VPN Connection', is the active configuration screen.

	Name	Device 1	Virtual Interface IP
<input type="checkbox"/>	pod2-azure-to-aws	52.254.17.73	172.27.2.1
<input type="checkbox"/>	pod2-dc-to-aws	3.80.231.87	172.26.2.2
<input type="checkbox"/>	pod1-dc-to-aws	18.234.229.63	172.26.1.2

**Create VPN Connection**

**Rule Details**

Name: pod1-azure-to-aws

**Device Details**

Device 1: pod1-egress-gw-azure

Device 1 Virtual Interface IP: 172.27.1.1

Device 2: pod1-egress-gw-aws

Device 2 Virtual Interface IP: 172.27.1.2

**Authentication**

Authentication: PreSharedKey

Authentication Value: \*

**IPsec Profile**

IPsec Profile: cisco-mcd-default-mcd-ipsec-pr...

Buttons: Cancel, Save

Multicloud Defense Controller configures Multicloud Defense Gateway in AWS and Azure



# Configure site-to-cloud VPN

## IPsec profile

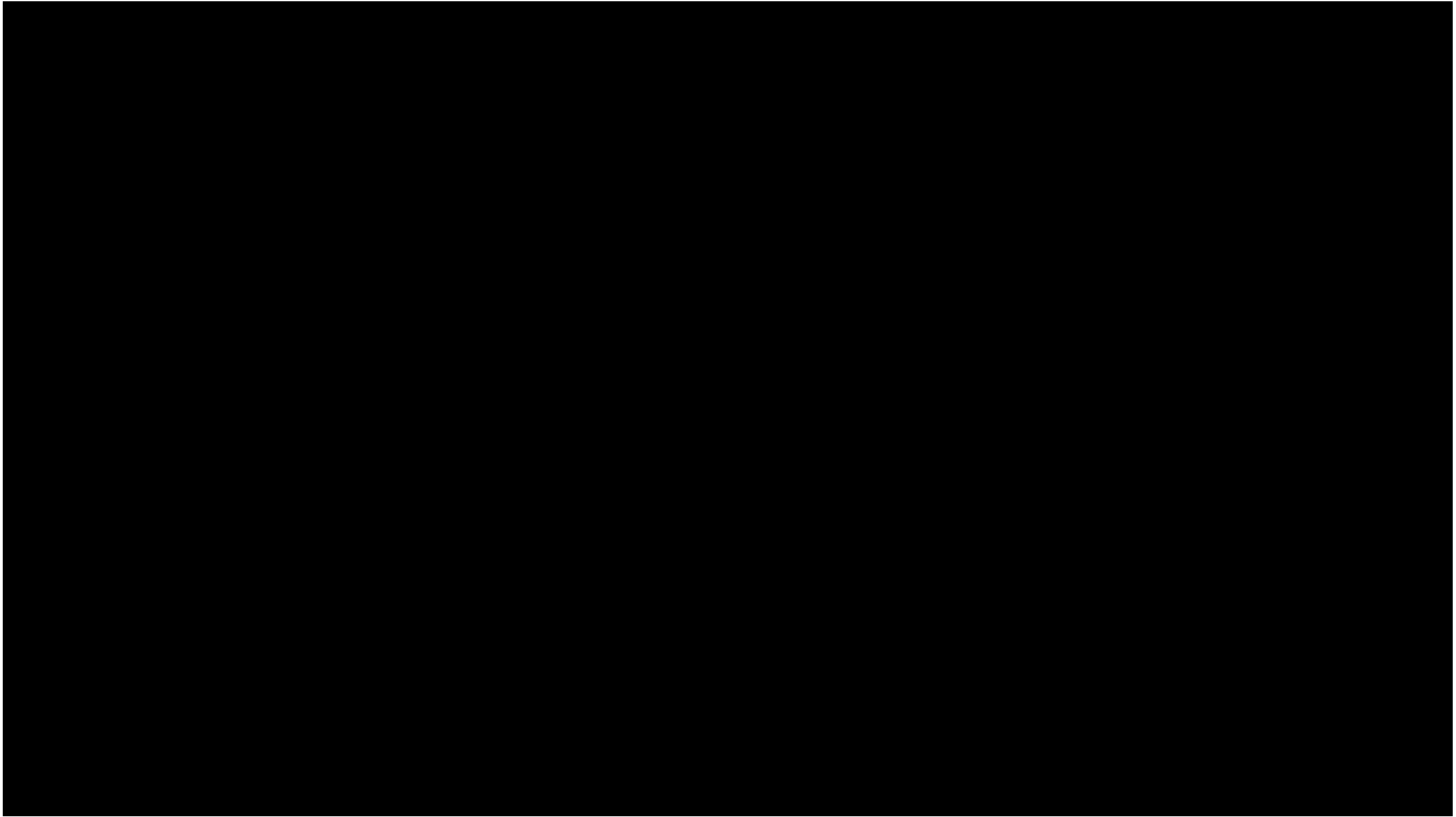
The screenshot displays the Cisco Multicloud Defense web interface. The top navigation bar includes 'Dashboard', 'Discover', 'Investigate', 'Manage', 'Report', and 'Administration'. The user is logged in as 'Admin: answami@cisc...' with a session ID of 'CDO\_cisco-multicloud\_defense\_lab01'.

The main content area is titled 'IPsec Profiles: 2'. It features a search bar and a table of profiles:

Name	In Use
<input type="checkbox"/> ciscomcd-default-asav-ipsec-profile	<input checked="" type="checkbox"/>
<input type="checkbox"/> ciscomcd-default-mcd-ipsec-profile	<input checked="" type="checkbox"/>

The 'Details' panel for the selected profile shows the following configuration:

- General Settings:** Terraform Export
- Name:** ciscomcd-default-mcd-ipsec-profile
- Description:** Cisco mcd ipsec profile
- IKE:**
  - DH Group:** Group 14, Group 15, Group 16, Group 19, Group 20, Group 21
  - Authentication:** SHA256, SHA
  - Encryption:** AES256, AES192, AES
  - Hash:** SHA256
  - key LifeTime:** 86400 seconds
  - IKE Version:** Version 2
- IPSec:**
  - Authentication:** SHA256, SHA
  - Encryption:** AES GCM 256, AES GCM 192, AES GCM
  - Mode:** ESP







The bridge to possible