

The background features a vibrant, abstract design with overlapping, wavy bands of color in shades of blue, green, yellow, orange, and red. On the right side, a bright white light source radiates outwards, creating a starburst effect with sharp, colorful rays that fan across the entire image.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

How to Build a Secure Multi-Cloud Environment with Cisco Secure Workload and Multicloud defense.

Dirk Stoeckmann, TSA Workload Security Engineering
@dstoeckm
BRKSEC-1773

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

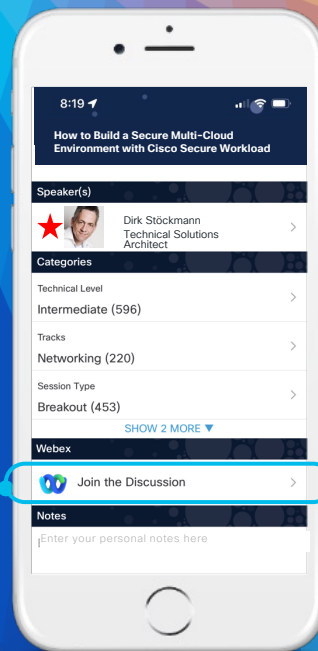
Questions?

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://cislive.ciscoevents.com/cislivebot/#BRKSEC-1773>



Agenda

- Why moving into the cloud
- Protection in the cloud: inbound, outbound and in the cloud
- Multicloud Defense
- Segmentation in the cloud or ZTNA
- Cisco Secure Workload

Who am I

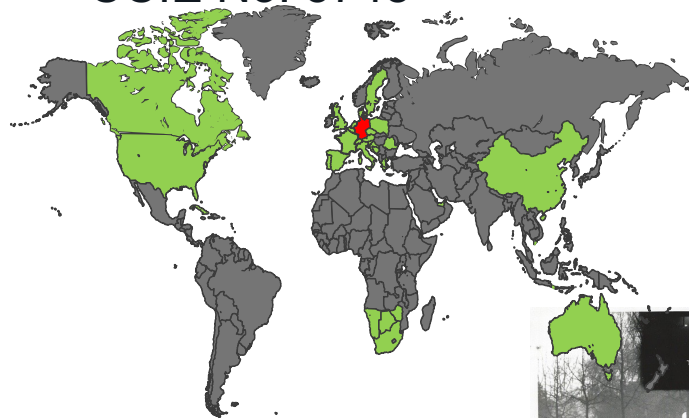
Married,
2 girls (18/14)
22+ years with Cisco



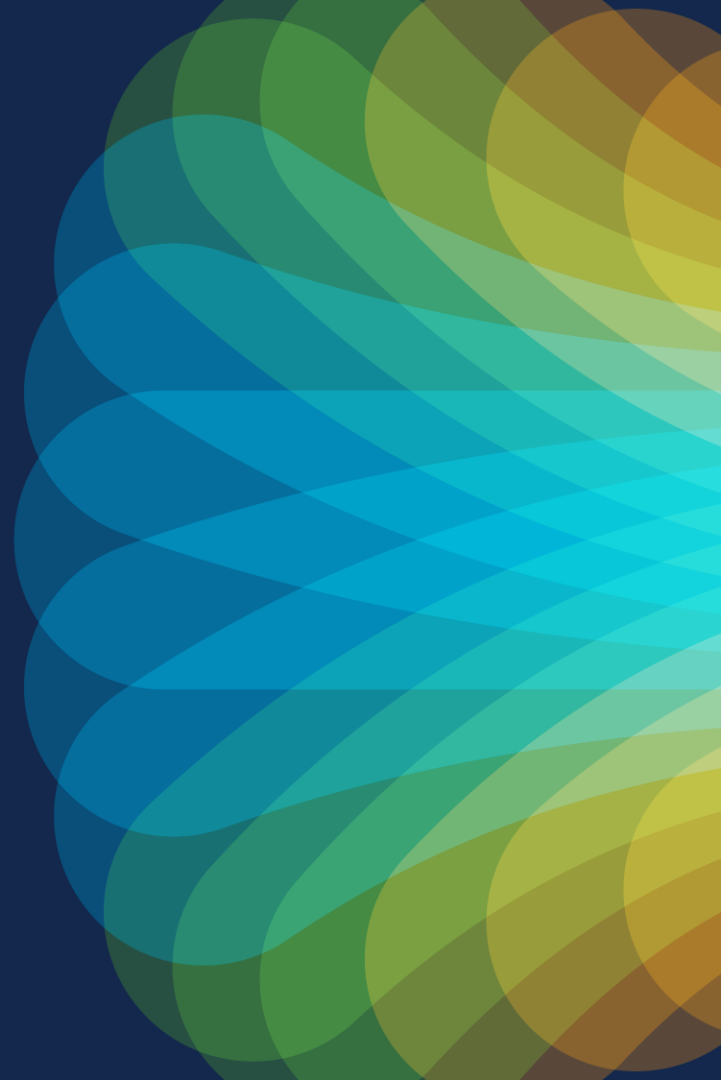
cisco *Live!*



Dirk
Stoeckmann
CCIE No. 5748



Why do customer move into the cloud



Cisco Global Hybrid Cloud Trends Report 2022

Security and complexity are the biggest challenges.

37% of respondents say security is a significant challenge when deploying hybrid cloud.

Collaboration is required for success.

55% of respondents have created a cross-functional team with technical and business representation.

50% of respondents have a centralized CloudOps and NetOps function to help ensure their organization's hybrid cloud strategy meets business objectives.



Base: All respondents (N = 2,577)

Cisco Global Hybrid Cloud Trends Report 2022

Developers are embracing hybrid cloud and Infrastructure as Code (IaC).

53% of organizations are moving workloads between on-premises

and cloud environments weekly.

58% are adopting Infrastructure as Code (IaC), and 44% are deploying cloud-native technologies to improve their security posture.

Hybrid cloud is driving the adoption of emerging technologies.

A significant percentage of respondents are deploying AIOps (45%), infrastructure automation (41%), and edge computing (41%).



Application workloads evolution

BM → VM
Rehosting

Maturing of containers

Serverless and more...

Before 2006

2006

2014

2016

2021

2022

Bare Metal

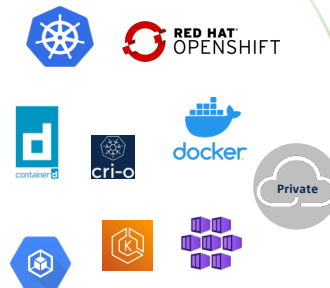


VM Admin

Cloud Architect

Public Cloud
Containerization
Replatform/Refactoring

K8s Mainstream
adoption



DevSecOps

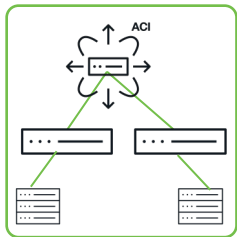


DevSecOps

NetSec + SecOps

But... what is an application workload?

Network Engineer



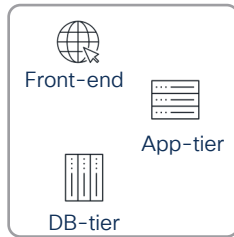
- Vlans/VRF
- Contracts
- Port

Firewall Engineer



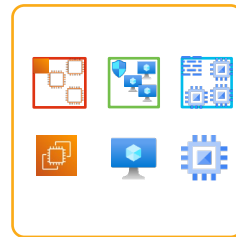
- ACL
- DPI
- Zones

Application Owners



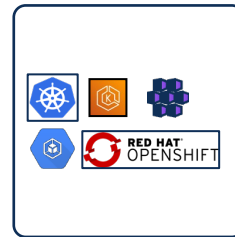
- Service
- VMs
- Baremetal

Cloud Architect



- Service
- VPC
- Instances

Cloud-Native Engineer



- Microservice
- Network Policy
- Pods/CNI

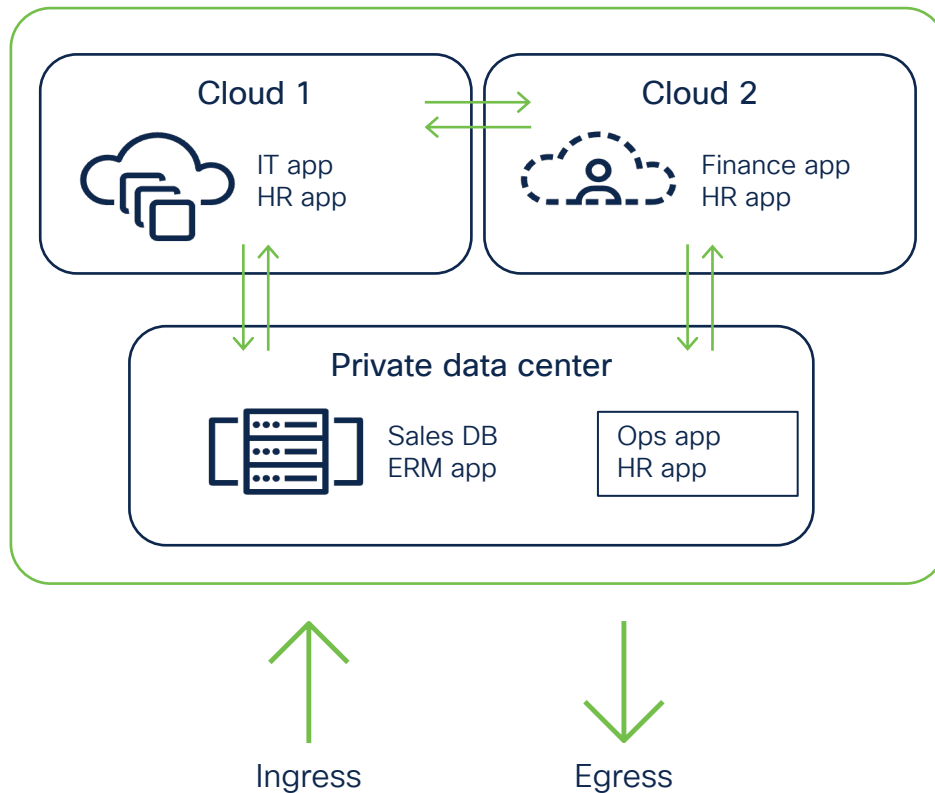
The network is constantly evolving

82%

of IT leaders
have adopted
hybrid cloud¹

58%

of IT leaders are
deploying 2 to 3
public IaaS clouds¹



¹ 2022 Cisco Global Hybrid Cloud Trends Report

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

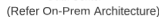


Setup and Maintenance

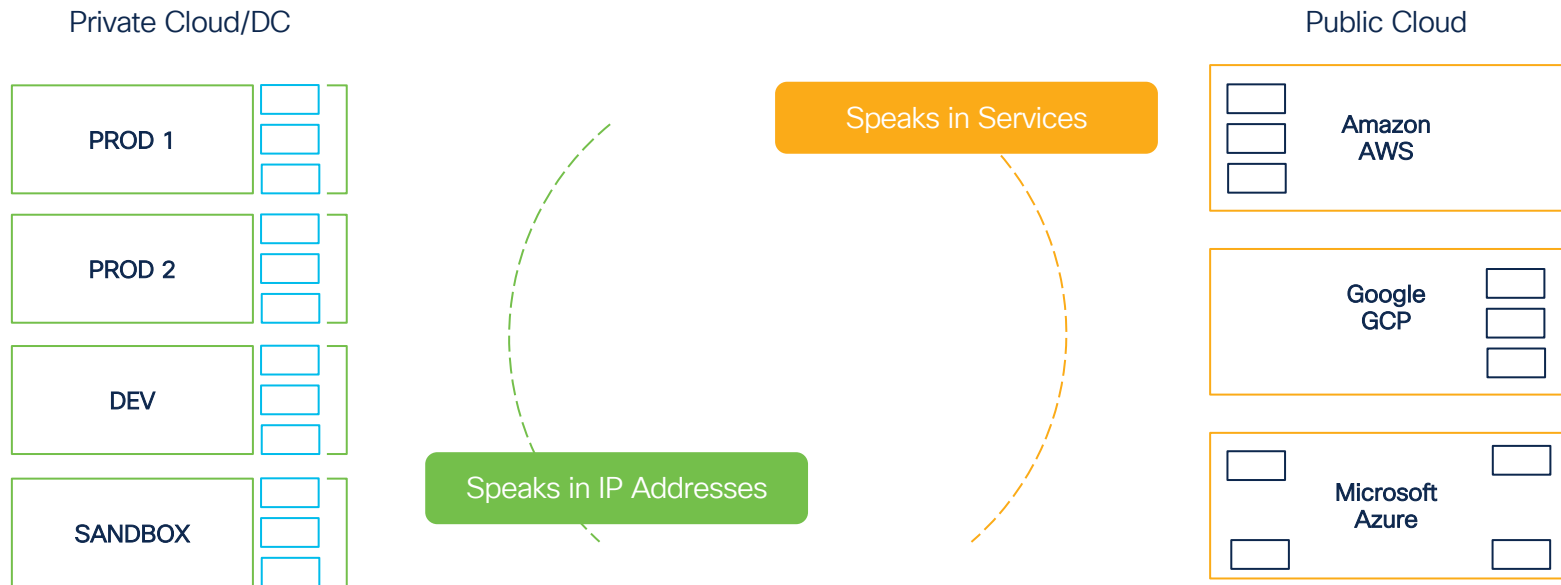
Long setup time and on-going maintenance for management & firewall leads to:

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

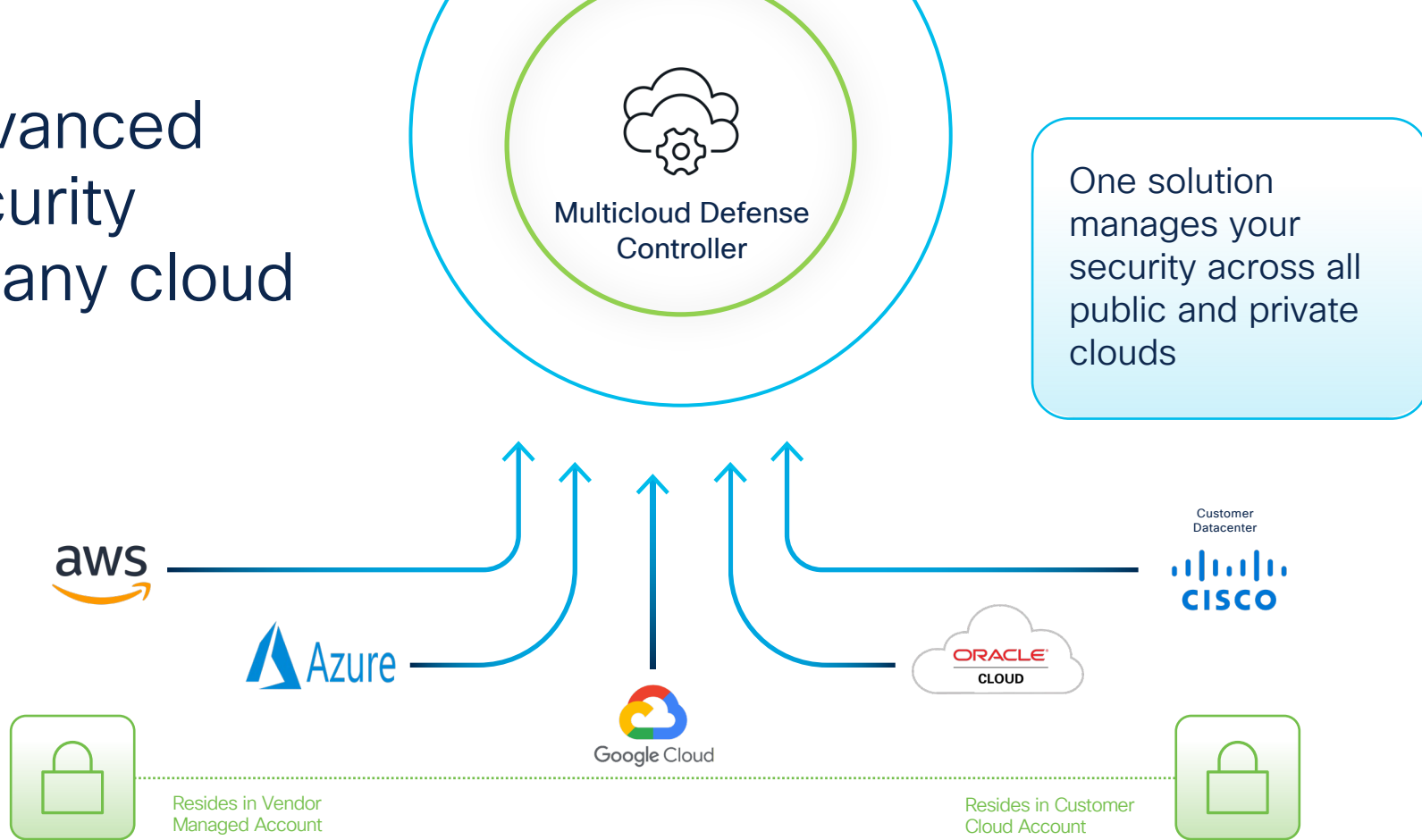
CISCO *Live!*



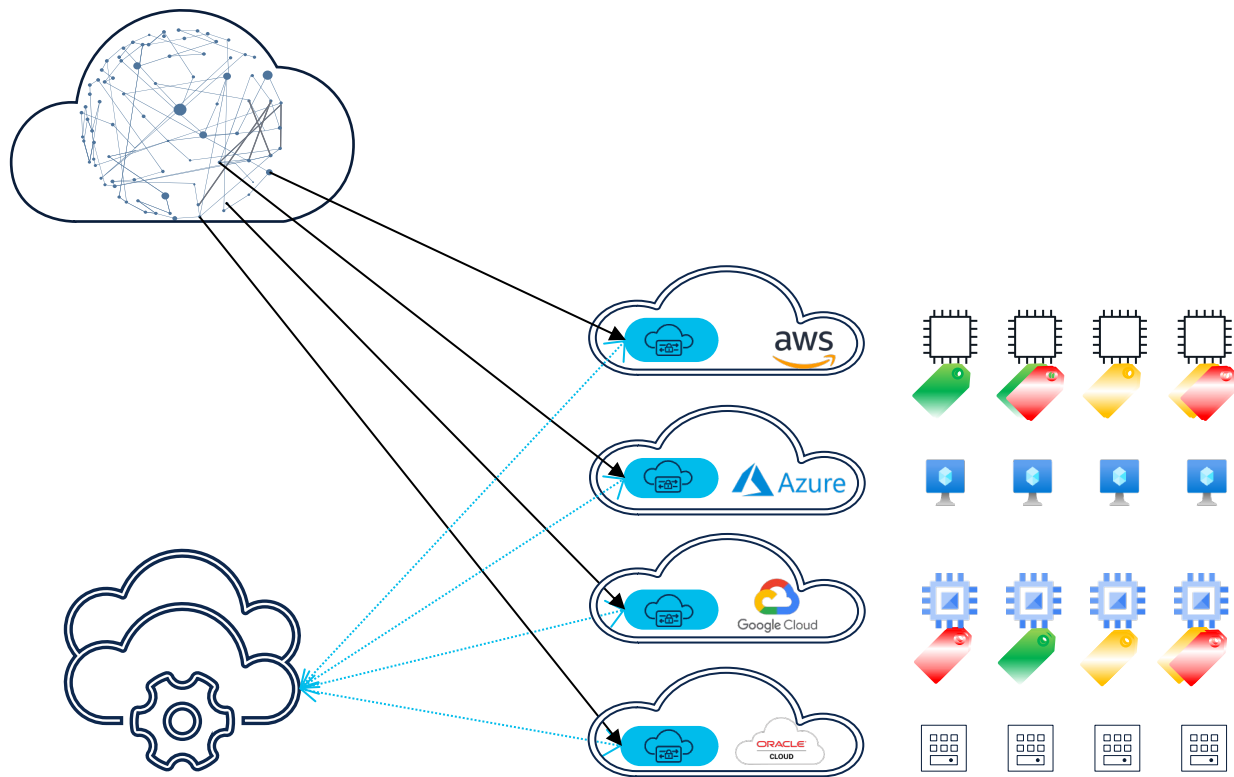
Modern applications are not monolithic



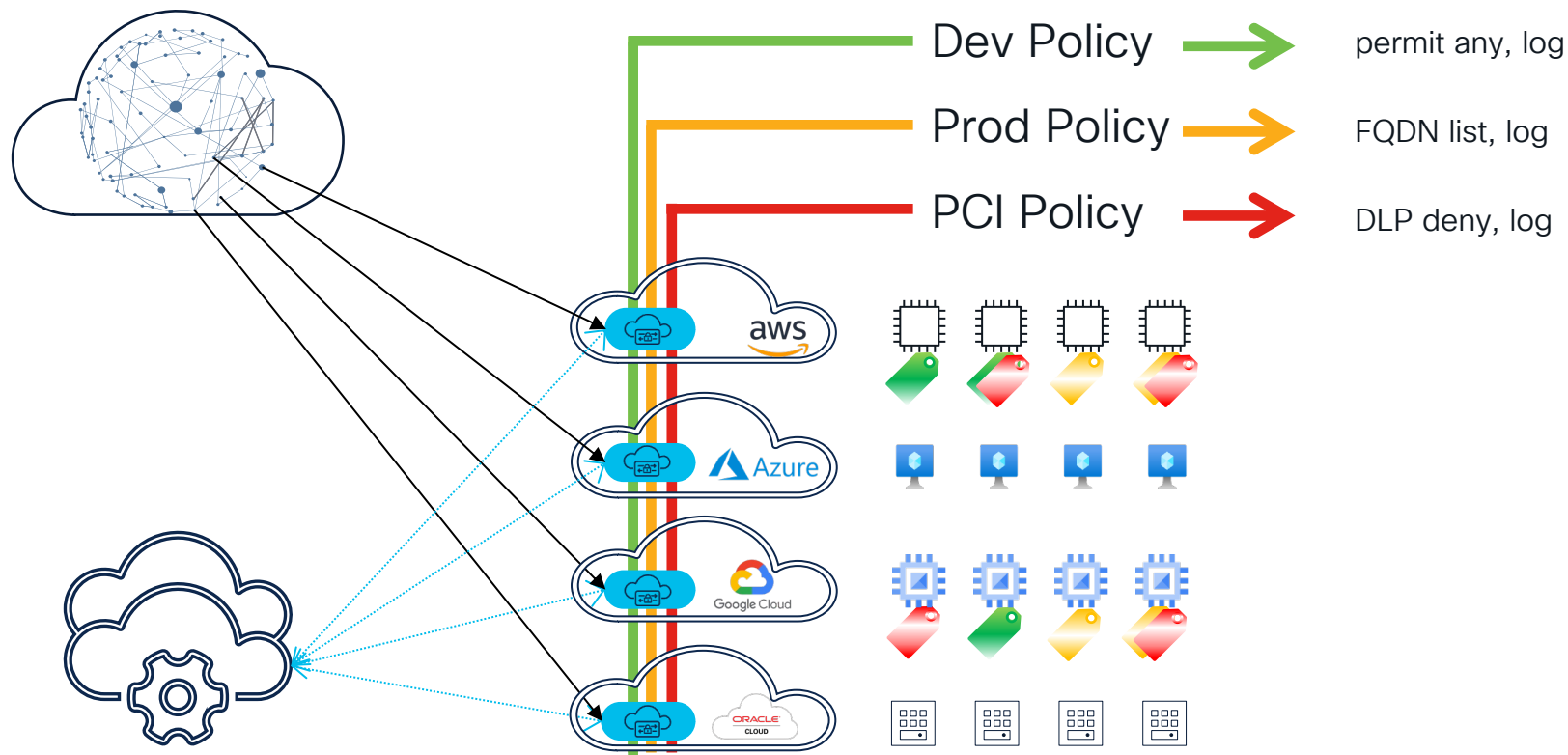
Advanced security for any cloud



Policy distribution



Policy distribution



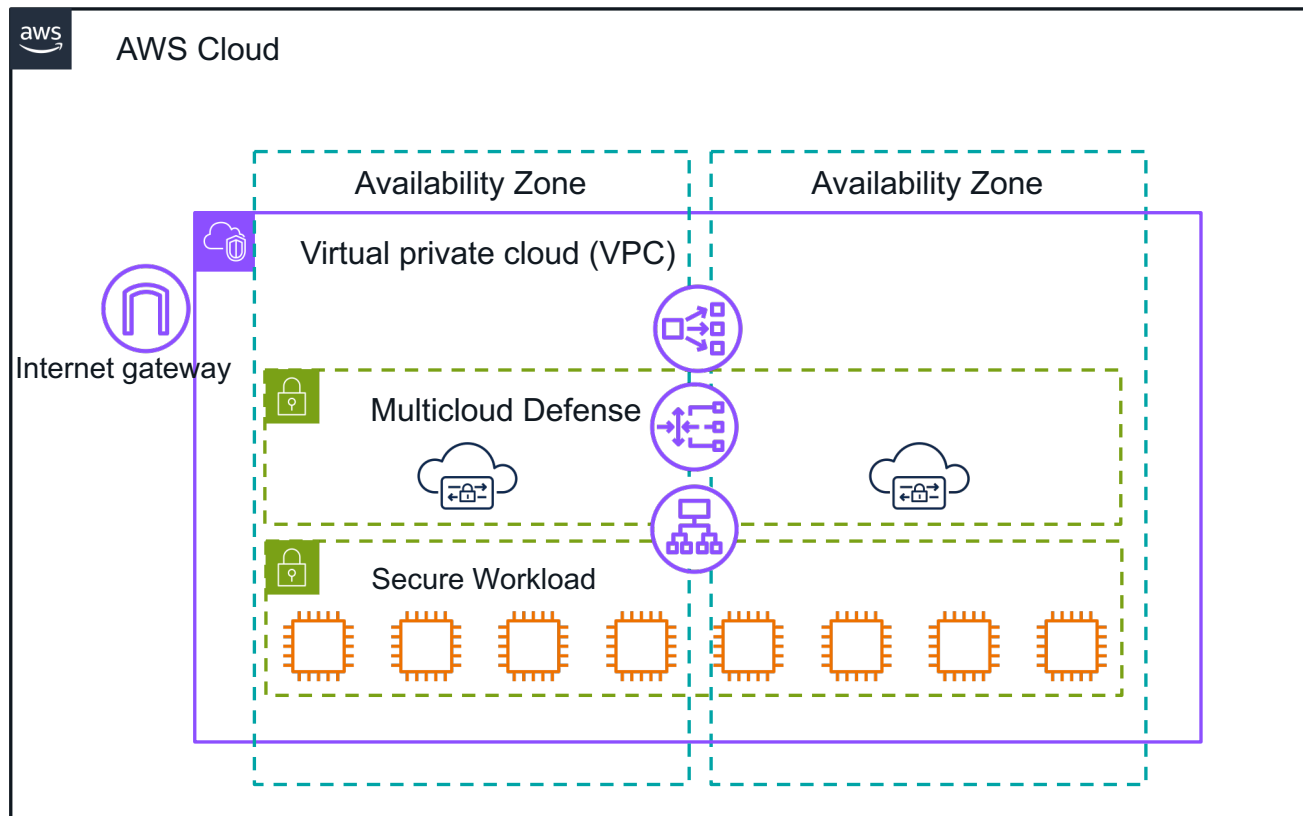
Simplifying the big picture



Layer 4-7



Layer 3-4



Simplifying the big picture



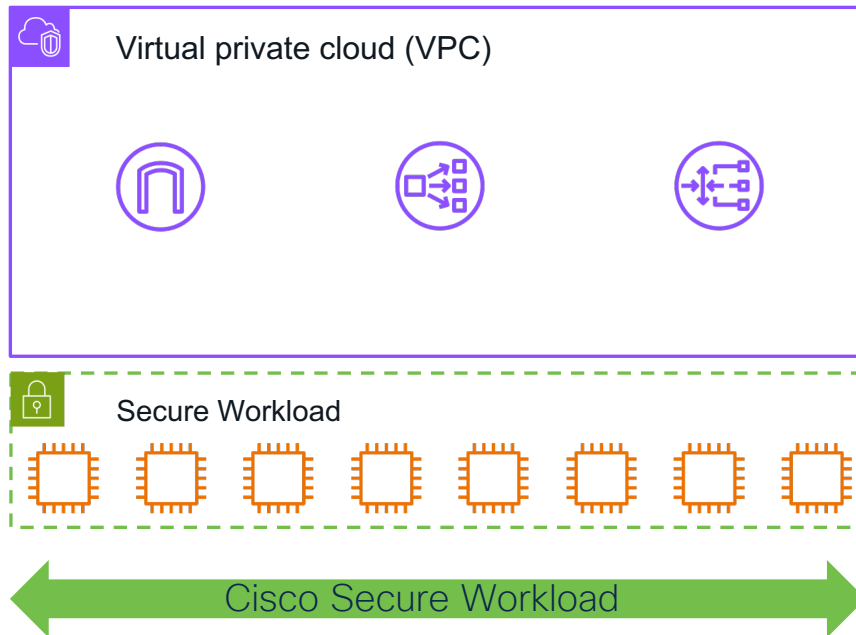
Layer 4-7



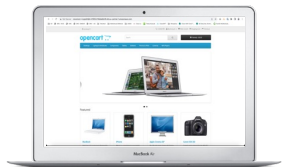
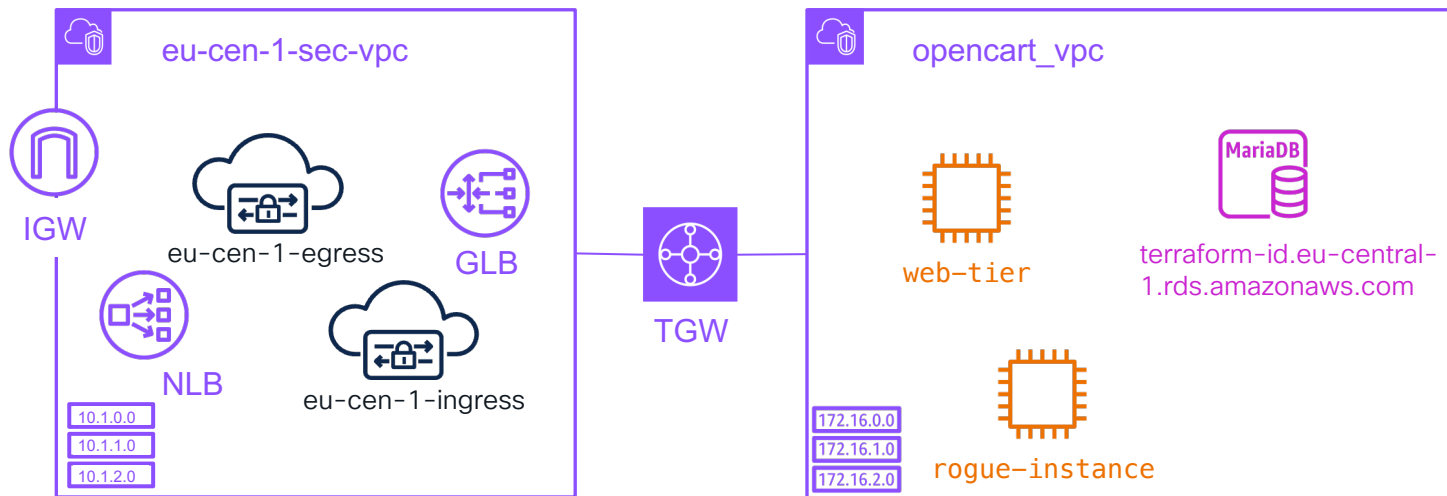
Multicloud
Defense



Layer 3-4

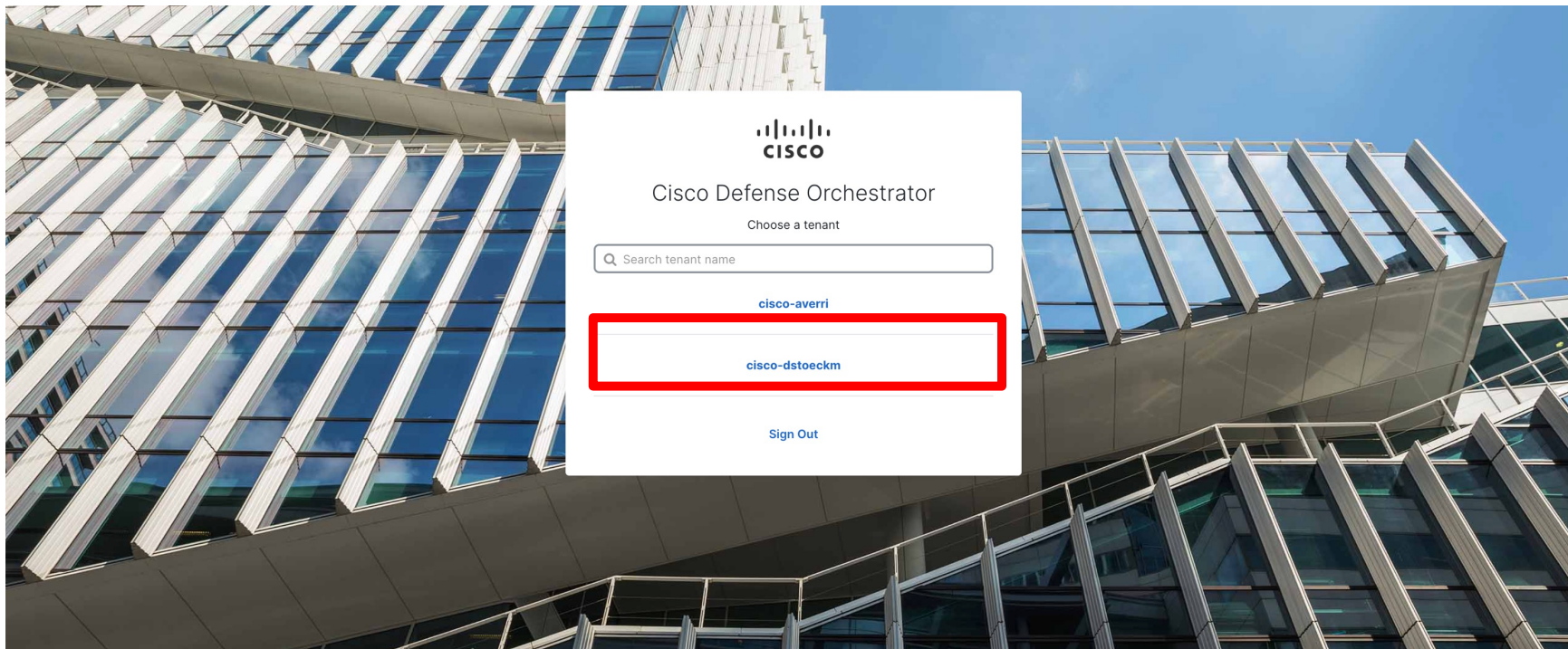


App to protect



How to get there

<https://www.defenseorchestrator.eu/>



Cisco Defence Orchestrator

defenseorchestrator.eu/multicloud-defense

Defense Orchestrator Multicloud Defense

Search

Hide Menu

Dashboard

Multicloud Defense New

Multicloud Defense Controller

Accounts and Assets

+ Add Accounts

Cloud Accounts

2 AWS 2 Azure 0 GCP 0 Oracle

4 Total Accounts View Accounts

Account Resources

26 VPCs/ VNets 33 Security Groups 27 Route Tables 76 Subnets

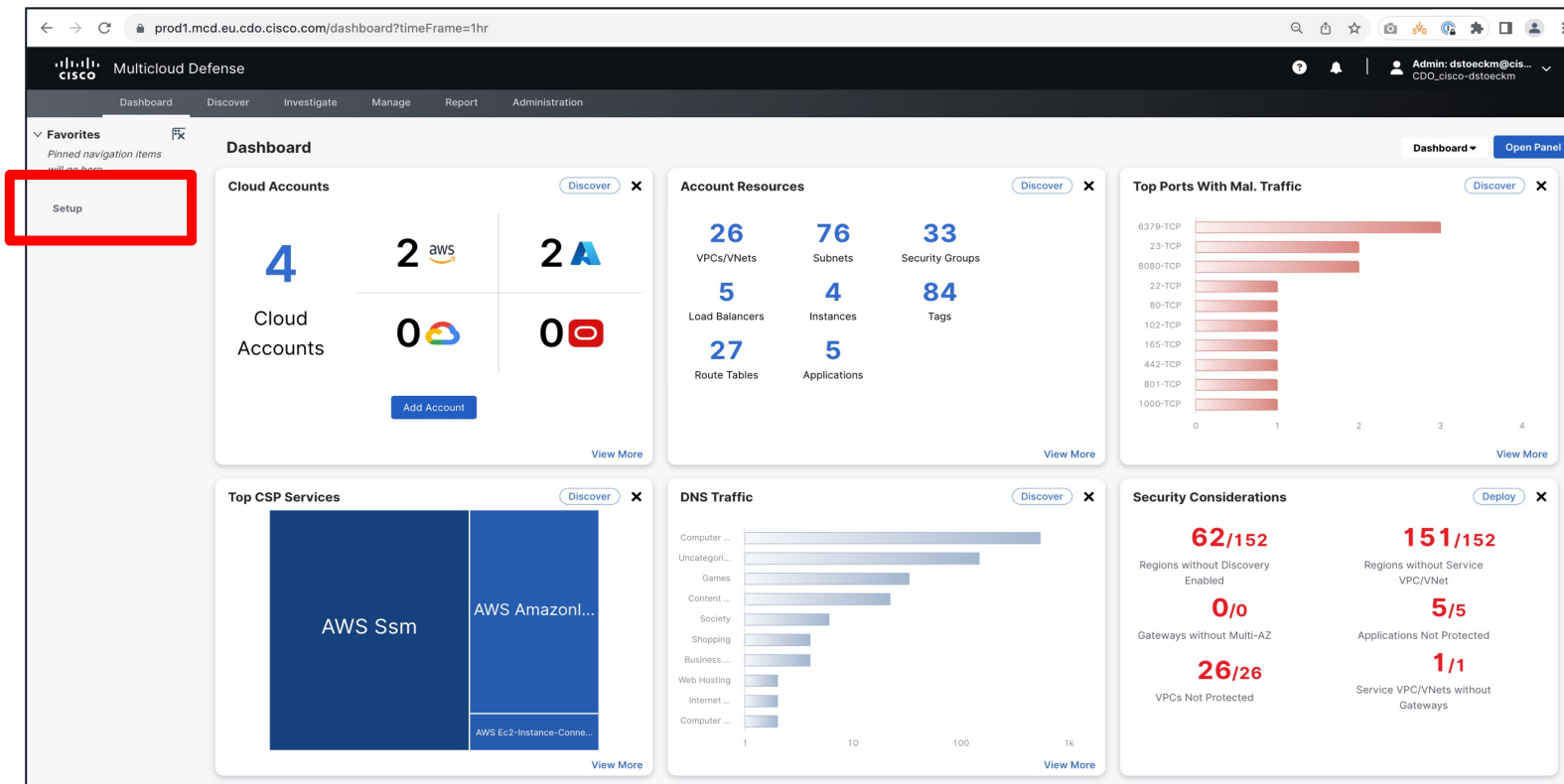
4 Instances 5 Load Balancers 84 Tags 5 Applications

Enable Traffic Visibility

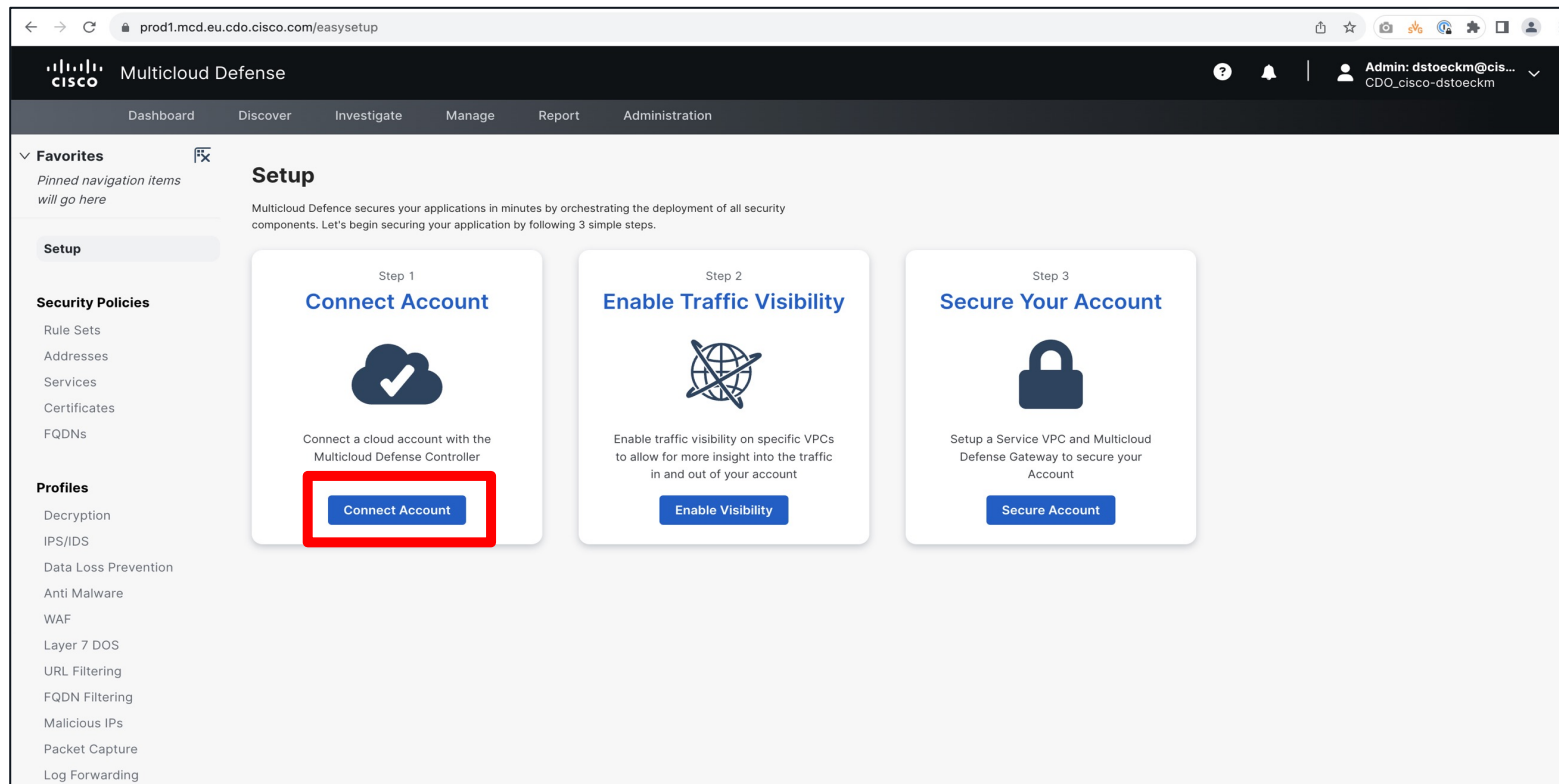
Enable traffic visibility on specific VPCs to allow for more insight into traffic in and out of your account.

Enable visibility

Multicloud Defense



Connect Account – Step 1



The screenshot shows the Cisco Multicloud Defense web interface. The browser address bar displays `prod1.mcd.eu.cdo.cisco.com/easysetup`. The page header includes the Cisco logo, the title "Multicloud Defense", and a user profile for "Admin: dstoeckm@cis...". A navigation bar contains links for Dashboard, Discover, Investigate, Manage, Report, and Administration. On the left, a sidebar lists "Favorites", "Setup", "Security Policies" (with sub-items like Rule Sets, Addresses, Services, Certificates, FQDNs), and "Profiles" (with sub-items like Decryption, IPS/IDS, Data Loss Prevention, Anti Malware, WAF, Layer 7 DOS, URL Filtering, FQDN Filtering, Malicious IPs, Packet Capture, Log Forwarding). The main content area is titled "Setup" and describes the goal of securing applications by orchestrating security components. It outlines three steps: Step 1: Connect Account, Step 2: Enable Traffic Visibility, and Step 3: Secure Your Account. Each step is represented by a card with an icon, a description, and a button. The "Connect Account" button in the Step 1 card is highlighted with a red rectangular box.

prod1.mcd.eu.cdo.cisco.com/easysetup

Multicloud Defense

Admin: dstoeckm@cis...
CDO_cisco-dstoeckm

Dashboard Discover Investigate Manage Report Administration

Setup

Multicloud Defence secures your applications in minutes by orchestrating the deployment of all security components. Let's begin securing your application by following 3 simple steps.

Step 1
Connect Account

Connect a cloud account with the Multicloud Defense Controller

Connect Account

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

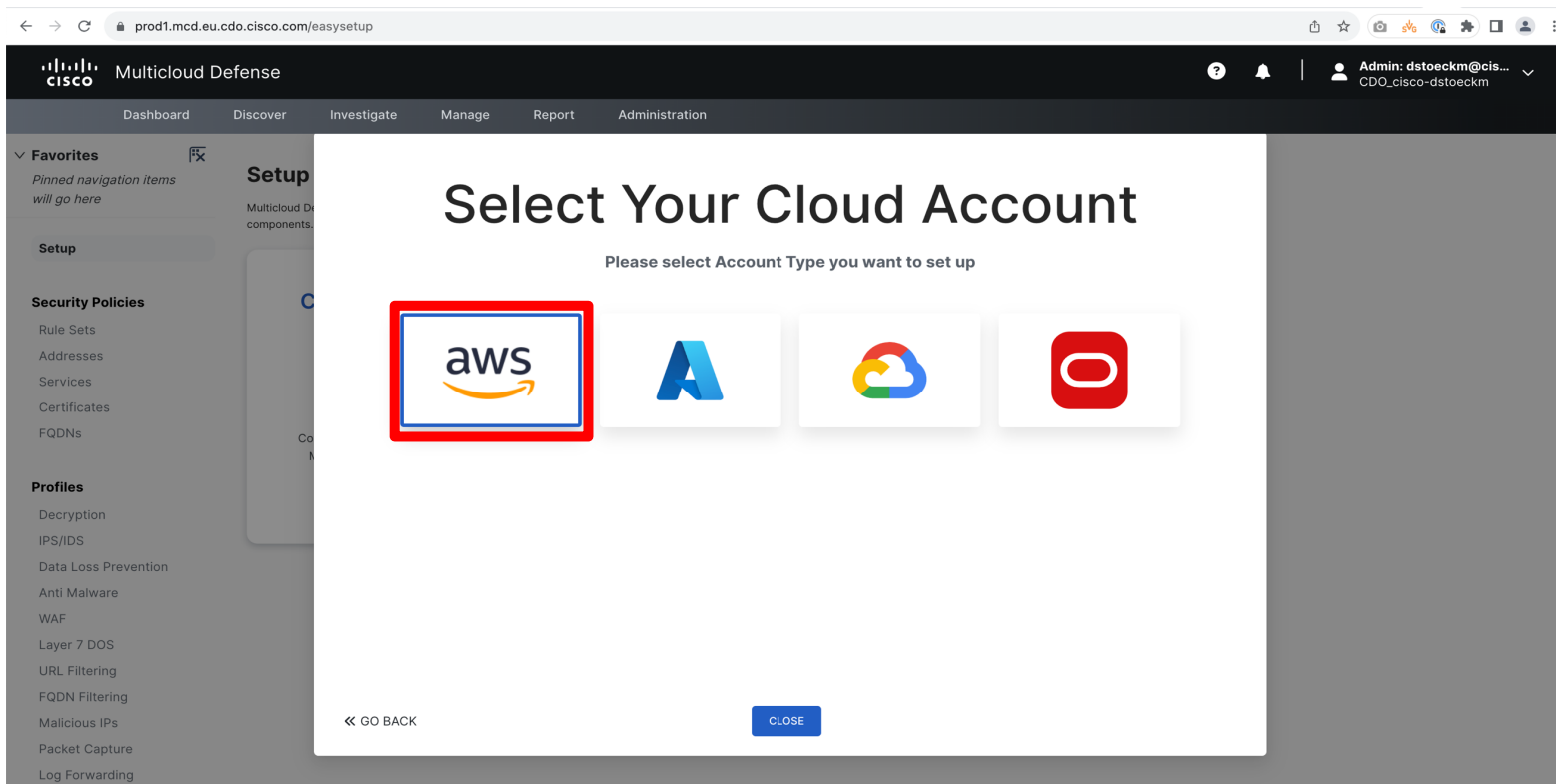
Enable Visibility

Step 3
Secure Your Account

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

Secure Account

Account setup



Account setup AWS

Connect Your AWS Account

We need to prepare your cloud account for integration with the MCD Controller.
For more information see [Documentation](#)



In your AWS account:

1

Launch Stack

CloudFormation Template

2

Copy and paste controller IAM role ARN from the CloudFormation stack output

AWS Account Number i

AWS Account Name i

Description i

Description (optional)

External ID i

bhzhnmeuorwserrknewtohobwcsshnbpkatzjtqpkbvnhbfrbtzhmydtkmz 📋

Controller IAM Role i

⏪ GO BACK

CANCEL

NEXT

Cloud Formation

CloudFormation > **Stacks** > Create stack

Quick create stack

Template

Template URL
https://valtx-public.s3.amazonaws.com/cloud-formation/mcd-all.yml

Stack description
Create 3 IAM Roles mcd-gateway-role that is assigned to Multicloud Defense gateway instances. mcd-controller-role is a cross account IAM role used by the Multicloud Defense Controller to manage the customer's AWS account (create gateway instances etc). mcd-inventory-role that enables posting of CloudTrail updates to the Multicloud Defense Controller. Create S3 bucket and enable CloudTrail to go this bucket. Enable Event notification on the S3 bucket to notify the Multicloud Defense Controller

Stack name

Stack name
cisco-mcd-resources

Stack name can include letters (A-Z and a-z), numbers (0-9) and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Multicloud Defense Deployment

Multicloud Defense Controller's Deployment Name (DO NOT CHANGE THIS unless you talk to Cisco)
Multicloud Defense Internal Deployment Name (If you launched this from the Multicloud Defense Dashboard, it's prefilled, otherwise talk to Cisco sales for the info).
prod1

Multicloud Defense Controller's Account Number (DO NOT CHANGE THIS unless you talk to Cisco)
Account number where the Multicloud Defense Controller Runs (If you launched this from the Multicloud Defense Dashboard, it's prefilled, otherwise talk to Cisco sales for the info)
878511901175

IAM Roles Configuration

External ID used for cross account IAM Role's Trust Settings (DO NOT CHANGE THIS unless you talk to Cisco)
External ID used by the IAM role as a trust relationship with the caller (If you launched this from the Multicloud Defense Dashboard, it's prefilled, otherwise leave it to the default and change it later during the account addition on Multicloud Defense Dashboard).
bzhnmneurwserrknewtohbwcshnbpkatztpakbvbfbrbtzhmydtkmbthlt

Cloud Formation

CloudFormation X

Prefix to use for the IAM roles created (letters and numbers only, no hyphens, underscores or any other special characters)

ciscomcd

Inventory/Discovery Configuration

S3 Bucket Name
Create S3 Bucket where VPC Flow Logs, DNS Query Logs and CloudTrail events are stored. Leave it to empty if you are not going to use Discovery/Real-time inventory Features

ciscomcd-cdo-cisco-dstoeckm-231113-123811

Number of days to keep the logs
Delete all objects (vpc flow logs, dns logs, cloudtrail logs) after days

1

Create a new CloudTrail (S3 Bucket is required) to enable real-time inventory
If you already have a multi-region CloudTrail in your account, choose false to skip CloudTrail creation.

true

Permissions

IAM role – optional
Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name: AWSServiceRoleForCloudFormationStackSetsOrgMember Remove

⚠ AWS CloudFormation will use this role for all stack operations. Other users that have permissions to operate on this stack will be able to use this role, even if they don't have permission to pass it. Ensure that this role grants the least privilege.

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have customised names. Check that the customised names are unique within your AWS account. [Learn more](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources with customised names.

Cancel Create **Create stack**

Cloud Formation

The screenshot displays the AWS CloudFormation console interface. On the left, the navigation pane shows 'CloudFormation' with sub-sections like 'Stacks', 'Stack details', 'StackSets', 'Exports', 'Designer', 'Registry', and 'Feedback'. The main area is titled 'cisco-mcd-resources' and shows the 'Stacks (1)' list with a filter for 'Active' status. The stack 'cisco-mcd-resources' is listed with a timestamp of '2023-11-13 14:49:35 UTC+0100' and a status of 'CREATE_IN_PROGRESS'. The right pane shows the 'Events (1)' tab for this stack, displaying a single event with the status 'CREATE_IN_PROGRESS' and the reason 'User Initiated'. The event is highlighted with a red underline.

Timestamp	Logical ID	Status	Status reason
2023-11-13 14:49:35 UTC+0100	cisco-mcd-resources	CREATE_IN_PROGRESS	User Initiated

Cloud Formation

The screenshot displays the AWS CloudFormation console interface. On the left, the 'CloudFormation' sidebar shows the 'Stacks' section with a list of stacks. The main panel shows the 'cisco-mcd-resources' stack details. The 'Resources' tab is selected, displaying a table of resources. A red box highlights the 'Status' column for all resources, which all show 'CREATE_COMPLETE'.

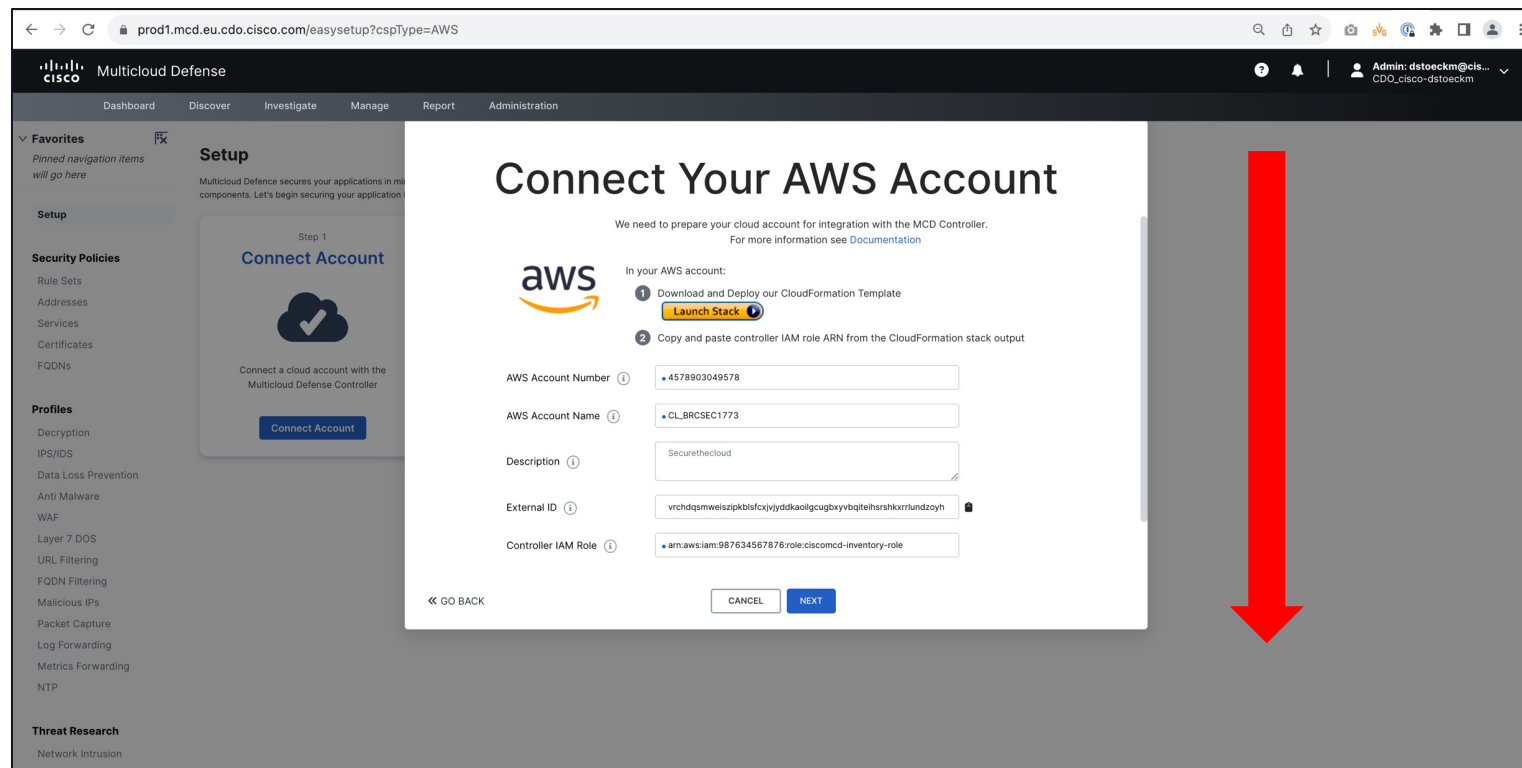
Logical ID	Physical ID	Type	Status	Module
MCDCloudTrail	ciscomcd-cloudtrail	AWS::CloudTrail::Trail	CREATE_COMPLETE	-
MCDCloudwatchEventRole	ciscomcd-inventory-role	AWS::IAM::Role	CREATE_COMPLETE	-
MCDControllerRole	ciscomcd-controller-role	AWS::IAM::Role	CREATE_COMPLETE	-
MCDGatewayInstanceRole	ciscomcd-gateway-role	AWS::IAM::InstanceProfile	CREATE_COMPLETE	-
MCDGatewayRole	ciscomcd-gateway-role	AWS::IAM::Role	CREATE_COMPLETE	-
MCDSSBucket	ciscomcd-cdo-cisco-dstoeckm-231113-134922	AWS::S3::Bucket	CREATE_COMPLETE	-
MCDSSBucketPolicy	ciscomcd-cdo-cisco-dstoeckm-231113-134922	AWS::S3::BucketPolicy	CREATE_COMPLETE	-

Cloud Formation

The screenshot shows the AWS CloudFormation console interface. On the left, the 'CloudFormation' sidebar is visible with options like 'Stacks', 'Stack details', 'StackSets', 'Exports', 'Designer', 'Registry', 'Spotlight', and 'Feedback'. The main panel displays the 'cisco-mcd-resources' stack. The 'Outputs' tab is selected and highlighted with a red box. Below the tab, there is a table of outputs. A green box highlights the table, and the text 'Not to be shared ;)' is overlaid on it.

Key	Value	Description	Export name
AccountNumber	-	-	-
MCDControllerRoleArn	-	-	-
MCDFirewallRoleName	-	-	-
MCDInventoryRoleArn	-	-	-
MCD53BucketArn	-	-	-
MCD53BucketName	-	-	-

Account setup



prod1.mcd.eu.cdo.cisco.com/easysetup?cspType=AWS

Multicloud Defense

Dashboard Discover Investigate Manage Report Administration

Setup

Step 1

Connect Account

Connect a cloud account with the Multicloud Defense Controller

Connect Your AWS Account

We need to prepare your cloud account for integration with the MCD Controller.
For more information see [Documentation](#)

aws

In your AWS account:

- 1 Download and Deploy our CloudFormation Template
[Launch Stack](#)
- 2 Copy and paste controller IAM role ARN from the CloudFormation stack output

AWS Account Number ① 4578903049578

AWS Account Name ① CL_BRCSEC1773

Description ① Securethecloud

External ID ① vrchdqmweiszpklbfcxjyldkkaolgcugbxvybqleharshkxrrlundzoyh

Controller IAM Role ① arn:aws:iam:987634567876:role:ciscomcd-inventory-role

GO BACK CANCEL NEXT

Threat Research
Network Intrusion

Account setup

prod1.mcd.eu.cdo.cisco.com/easysetup?cspType=AWS

Multicloud Defense

Dashboard Discover Investigate Manage Report Administration

Setup

Step 1
Connect Account

Connect a cloud account with the Multicloud Defense Controller

Connect Your AWS Account

In your AWS account:

- 1 Download and Deploy our CloudFormation Template
Launch Stack
- 2 Copy and paste controller IAM role ARN from the CloudFormation stack output

AWS Account Number ① 4578903049578

AWS Account Name ① CL_BRCSEC1773

Description ① Securethecloud

External ID ① vrchdqmweiszipkbisfxyjyddkaolgcugbyvbg@tehrshixrnlundzoyh

Controller IAM Role ① arn:aws:iam:987634567876:role:ciscomcd-controller-role

Inventory Monitor Role ① arn:aws:iam:987634567876:role:ciscomcd-inventory-role

GO BACK CANCEL NEXT

Discovery

CISCO Multicloud Defense

Dashboard Discover Investigate Manage Report Administration

Admin: dstoeckm@cis...
CDO_cisco-dstoeckm

✓ Favorites
Pinned navigation items will go here

Setup

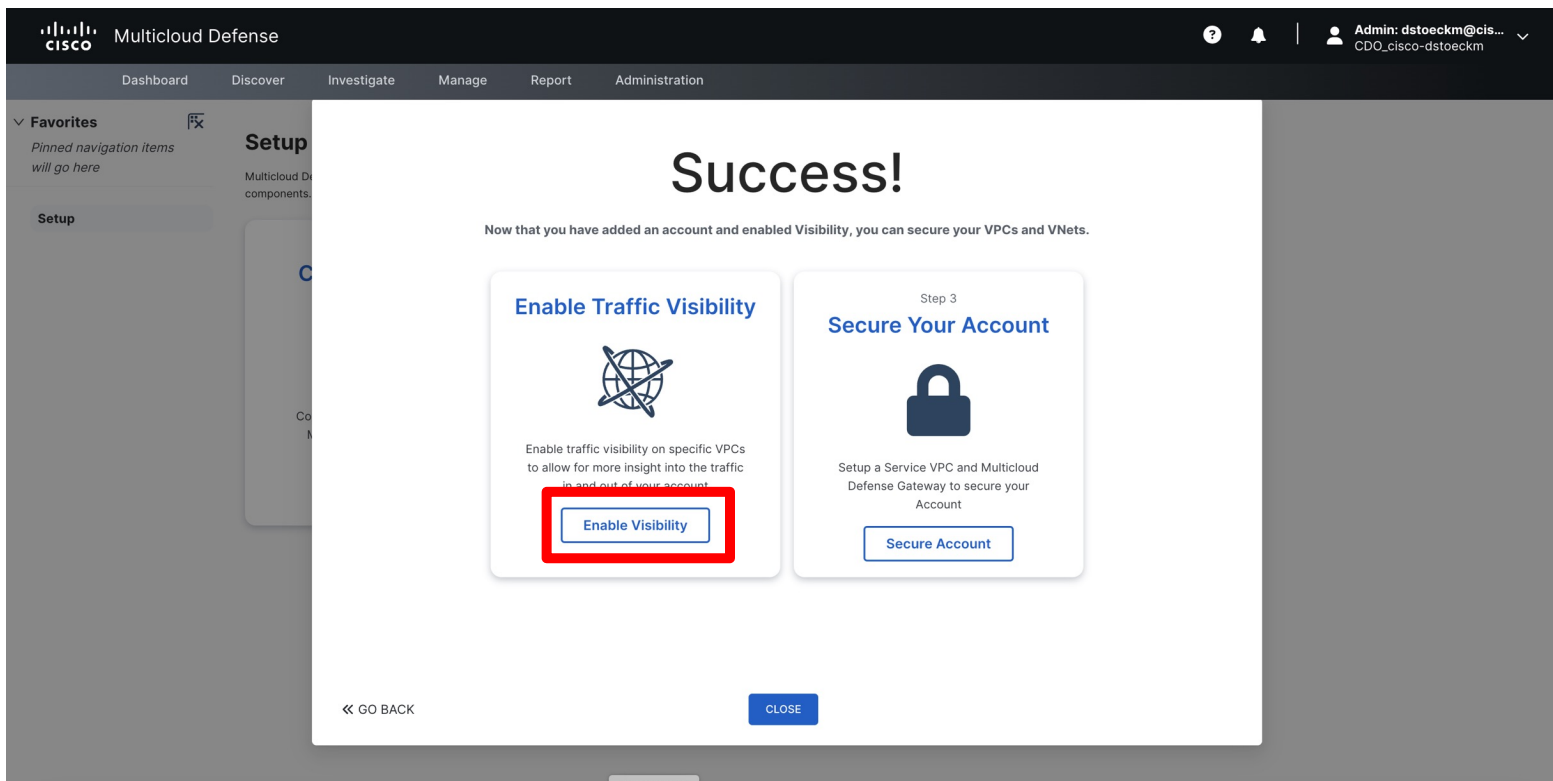
Discovering Assets

Doing our magic to discover all of your assets. done!

2 Cloud Accounts	17 Regions	36 Network ACL	144 Network ACL Rules
- Application Security Groups (Azure)	36 VPCs/VNets	109 Subnets	69 Security Groups
7 Load Balancers	29 Instances	87 Network Interfaces	231 Tags

« GO BACK CANCEL NEXT

Enable Traffic Visibility – Step 2



The screenshot shows the Cisco Multicloud Defense web interface. A modal window is displayed in the center with the heading "Success!". Below the heading, it states: "Now that you have added an account and enabled Visibility, you can secure your VPCs and VNets." The modal contains two main sections:

- Enable Traffic Visibility**: This section features a globe icon with a crossed-out arrow. Below the icon, it says: "Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account." At the bottom of this section is a button labeled "Enable Visibility", which is highlighted with a red rectangular border.
- Secure Your Account**: This section is labeled "Step 3" and features a padlock icon. Below the icon, it says: "Setup a Service VPC and Multicloud Defense Gateway to secure your Account." At the bottom of this section is a button labeled "Secure Account".

At the bottom left of the modal is a "GO BACK" link, and at the bottom right is a "CLOSE" button.

Traffic visibility

 Multicloud Defense

[Dashboard](#) [Discover](#) [Investigate](#) [Manage](#) [Report](#) [Administration](#)

▼ Favorites

Pinned navigation items will go here

Setup

Admin: dstoeckm@cis...
CDO_cisco-dstoeckm

?

🔔

Enable Traffic Visibility

This step enables Cisco Multicloud Defence to show you which VPCs might be compromised by connections to malicious sites by ingesting out of band traffic data (DNS queries, VPC/VNet flow logs) from your cloud account

CSP Account ⓘ

• dstoeckm_John-lab | AWS

✕

↻

Region ⓘ

• Europe (Frankfurt) eu-central-1

✕

↻

VPCs ⓘ

☒ Show All

	VPC Name ⓘ	VPC ID ⓘ	VPC ⓘ
☒	NA	vpc-079c23af1c7563512	<div>Saving...</div>

S3 Bucket ⓘ

• ciscomcd-cdo-cisco-dstoeckm-23...

✕

↻

ⓘ

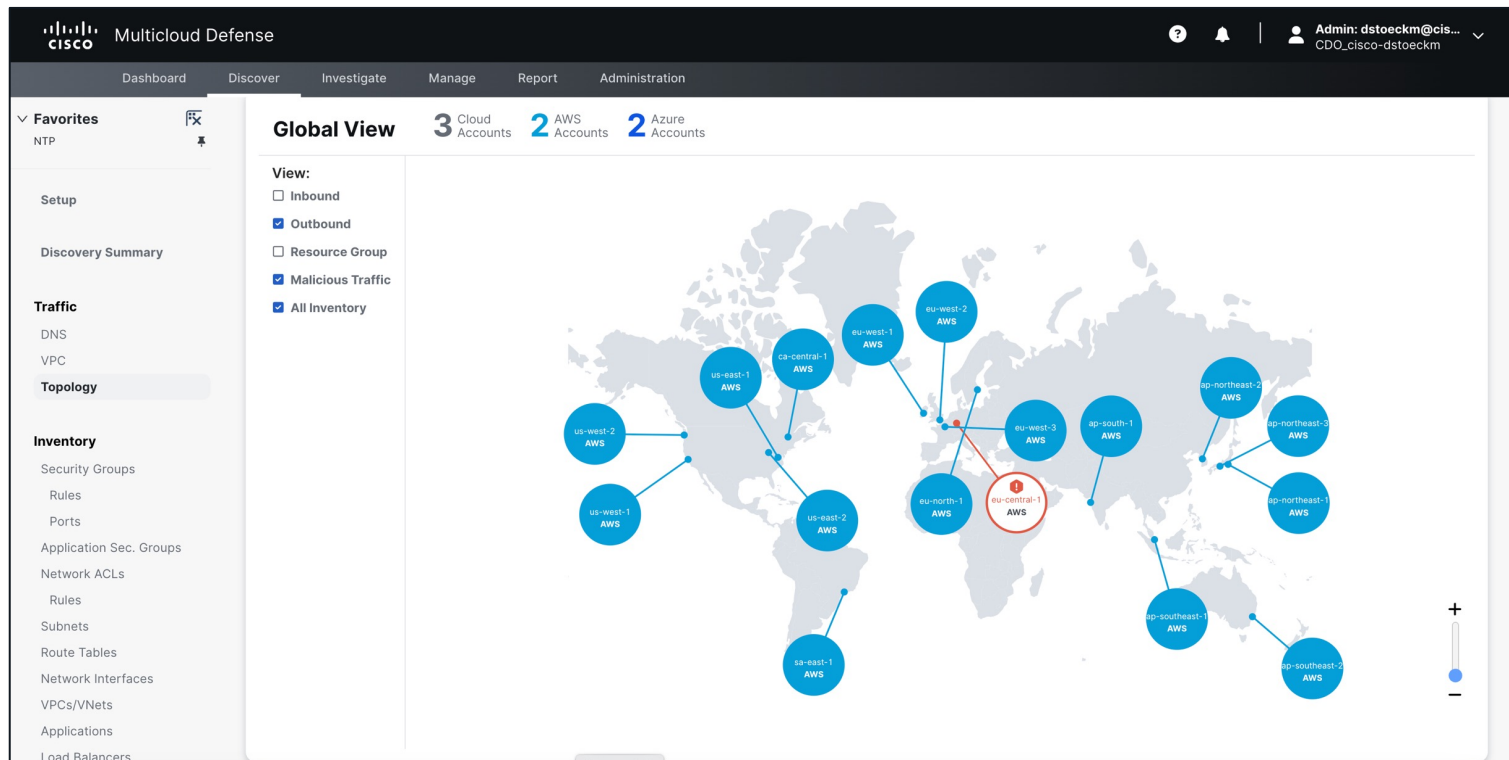
This is optional if you want to see the malicious traffic and threats in your cloud account. You can skip this and enable this later.

⏪ GO BACK

CANCEL

NEXT

Topology /Region



Topology /Region

Multicloud Defense

?

Admin: dstoeckm@cis...
CDO_cisco-dstoeckm

DashboardDiscoverInvestigateManageReportAdministration

▼ Favorites

NTP

Setup

Security Policies

Rule Sets

Addresses

Services

Certificates

FQDNs

Profiles

Decryption

IPS/IDS

Data Loss Prevention

Anti Malware

WAF

Layer 7 DOS

URL Filtering

FQDN Filtering

Malicious IPs

Packet Capture

Log Forwarding

Metrics Forwarding

General Information

AWS Account Name

dstoeckm_John-lab

Regions

eu-central-1 X

eu-north-1 X

eu-west-1 X

eu-west-2 X

eu-west-3 X

ap-northeast-1 X

ap-northeast-2 X

ap-northeast-3 X

ap-south-1 X

ap-southeast-1 X

ap-southeast-2 X

ca-central-1 X

sa-east-1 X

us-east-1 X

us-east-2 X

us-west-1 X

us-west-2 X

Refresh Interval (minutes)

60

Refresh Now

+

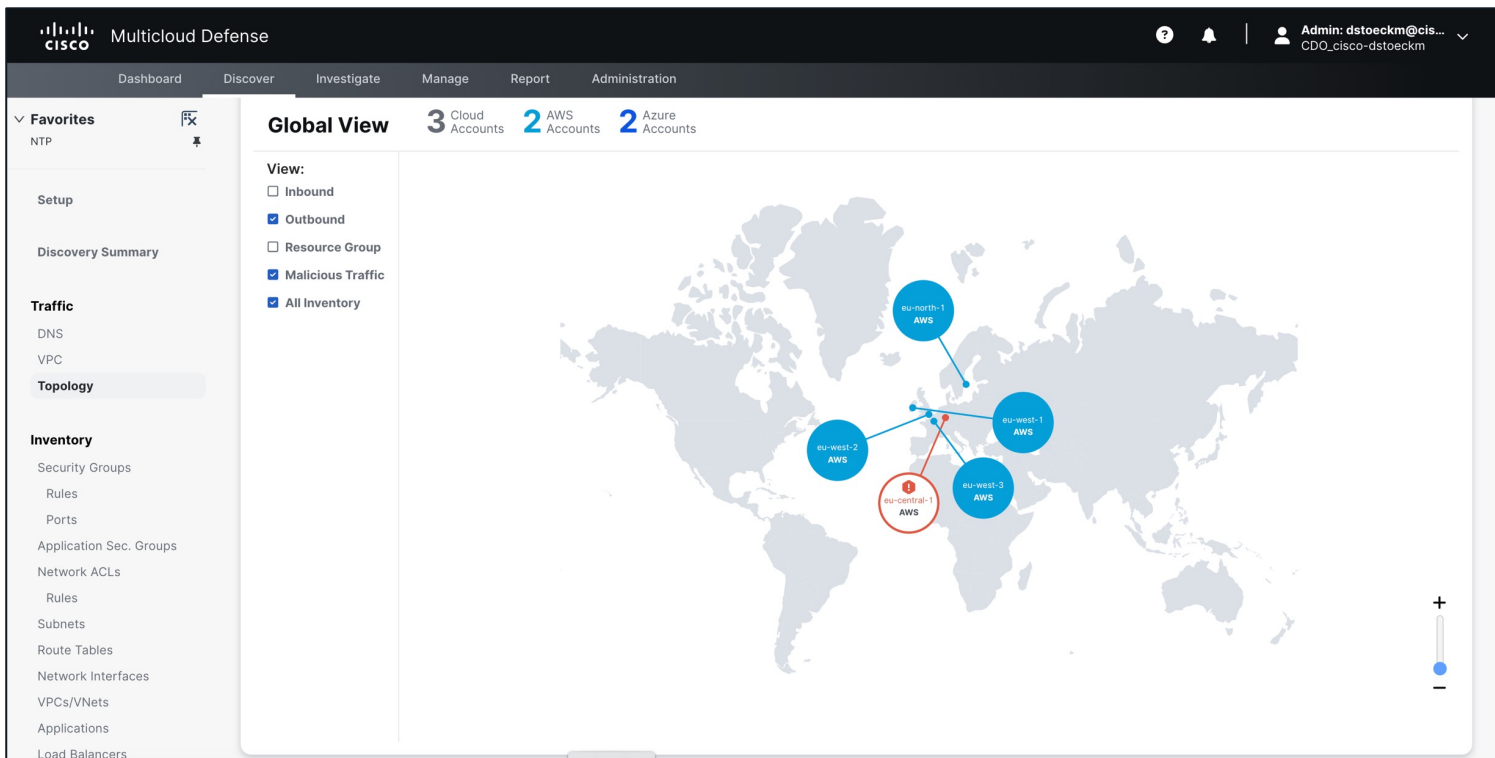
−

Note: Please ensure inventory IAM role is configured in the account page.

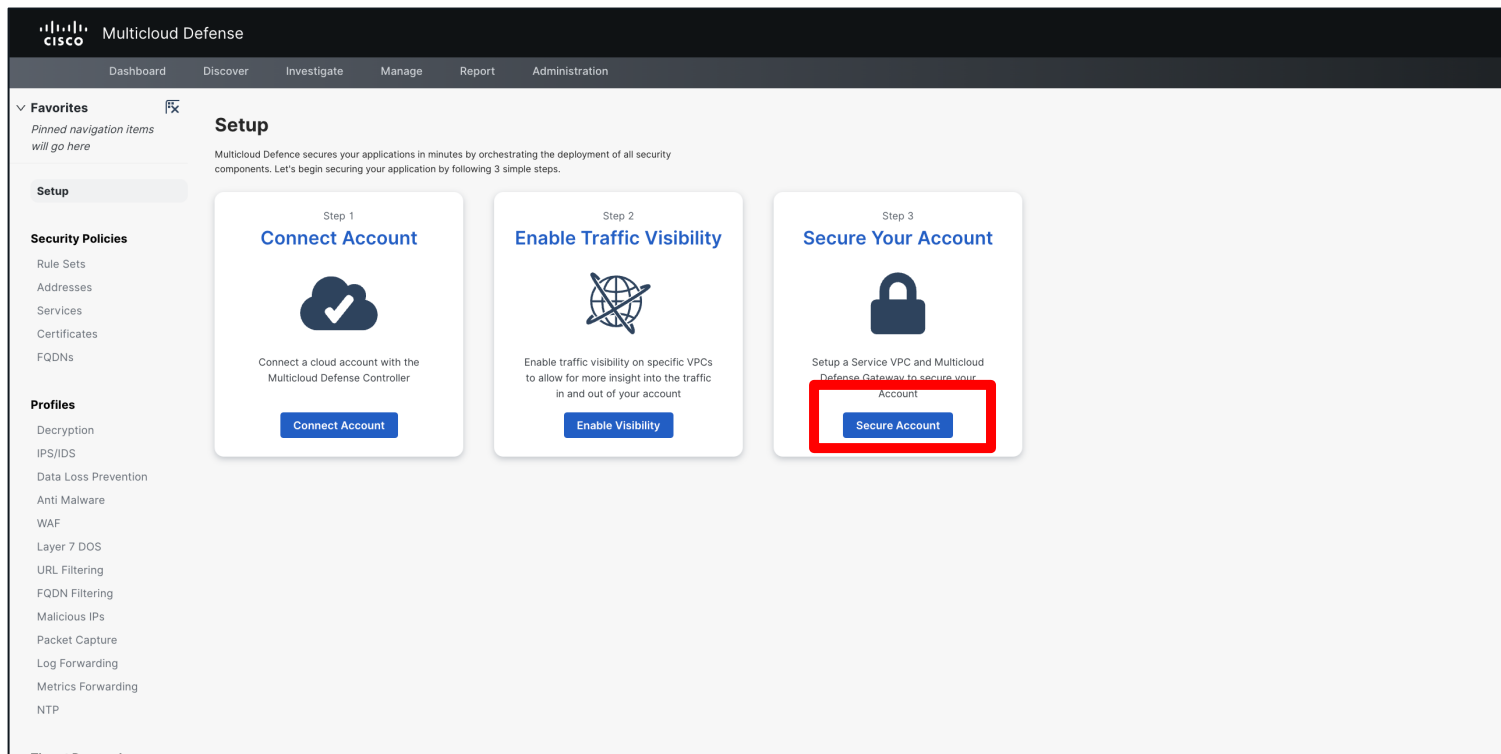
Cancel

Save & Continue

Topology /Region



Secure Your Account – Step 3



Multicloud Defense

Dashboard Discover Investigate Manage Report Administration

Setup

Multicloud Defense secures your applications in minutes by orchestrating the deployment of all security components. Let's begin securing your application by following 3 simple steps.

Step 1: Connect Account

Connect a cloud account with the Multicloud Defense Controller

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

Step 3: Secure Your Account

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

Connect Account **Enable Visibility** **Secure Account**

Security Policies

- Rule Sets
- Addresses
- Services
- Certificates
- FQDNs

Profiles

- Decryption
- IPS/IDS
- Data Loss Prevention
- Anti Malware
- WAF
- Layer 7 DOS
- URL Filtering
- FQDN Filtering
- Malicious IPs
- Packet Capture
- Log Forwarding
- Metrics Forwarding
- NTP

Secure Your Account

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**

Secure Your Account

Secure Your Account

To secure your account with a scalable centralized hub model, you'll need to first create a Service VNET (Security VNET)

Step 1: Add a Service VPC/VNet

Name

CSP Account [X](#) [+](#)

Region [X](#) [+](#)

CIDR Block

Availability Zones

- ☒ eu-central-1a
- ☐ eu-central-1c
- ☐ eu-central-1b

Transit Gateway [X](#) [+](#)

[<< GO BACK](#) [CANCEL](#) [NEXT](#) [SKIP >>](#)

Secure Your Account

Secure Your Account

Region ¹

CIDR Block ¹

Availability Zones ¹ ☒ eu-central-1a
☐ eu-central-1c
☐ eu-central-1b

Transit Gateway ¹

Transit Gateway Name ¹

Auto accept shared attachments ¹ ☐

Use NAT Gateway ¹ ☐

ⁱ This will act as a centralized security point to protect all your VPCs. For more information, please refer to our documentation [link](#)

« GO BACK SKIP »

Secure Your Account

The screenshot shows the Cisco Multicloud Defense console interface. The top navigation bar includes 'Dashboard', 'Discover', 'Investigate', 'Manage', 'Report', and 'Administration'. The left sidebar lists various categories: Favorites, Setup, Security Policies, Profiles, Threat Research, Cloud Accounts, and Gateways. The main content area displays the 'Secure Your Account' setup wizard. The wizard is currently at Step 2: Add a Gateway. A success message is shown: 'Service VPC/VNet created successfully'. The wizard steps are: Step 1: Connect Account, Step 2: Add a Gateway, and Step 3: Enable Traffic. The 'Connect Account' step is completed, and the 'Add a Gateway' step is in progress. The 'Enable Traffic' step is not yet started. The success message is displayed in a black box with white text. The wizard also includes a 'GO BACK' button and 'CANCEL' and 'NEXT' buttons.

Secure Your Account – Step 2 add GW

The screenshot shows the Cisco Multicloud Defense interface. On the left is a sidebar with navigation menus: Favorites, Setup, Security Policies, Profiles, Threat Research, Cloud Accounts, and Gateways. The main content area displays the 'Secure Your Account' wizard. Step 1, 'Connect Account', is completed. Step 2, 'Add a Gateway', is active. The wizard title is 'Secure Your Account' with the subtitle 'Deploy Multicloud Defense Gateway in Service VPC/VNet for policy enforcement'. The configuration fields are as follows:

- Account: `dstoeckm_john-lab`
- Service VPC/VNet: `eu-central-1-sec-vpc | vpc-0...`
- Instance Type: `2 Virtual CPU | AWS_M5_1...`
- MCD Gateways: ☒ Ingress ☒ East-West & Egress
- Ingress Gateway Name: `ingress-eu-central-1-gw-01`
- Ingress Gateway Policy Ruleset: `valix-sample-ingress-policy | Gateways: none`
- East-West & Egress Gateway Name: `egress-eu-central-1-gw-01`

At the bottom of the wizard are buttons for '<< GO BACK', 'CANCEL', and 'NEXT'.

Secure Your Account – Step 2 add GW

Secure Your Account

Deploy Multicloud Defense Gateway in Service VPC/VNet for policy enforcement

MCD Gateways ⓘ ☒ Ingress ☒ East-West & Egress

Ingress Gateway Name ⓘ ingress-eu-central-1-gw-01

Ingress Gateway Policy Ruleset ⓘ vattx-sample-ingress-policy
Gateways: none

East-West & Egress Gateway Name ⓘ ingress-eu-central-1-gw-01

East-West & Egress Gateway Policy Ruleset ⓘ vattx-sample-egress-policy
Gateways: none

Gateway IAM Role Name ⓘ clisco-mcd-gateway-role

SSH Key Pair ⓘ terraform-mcd-key

⏪ GO BACK CANCEL **NEXT**

Secure Your Account – Step 2 add GW

The screenshot shows 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: dstoeckm@cisco' with the email 'dstoeckm@cisco'. The main content area displays a 'Setup' wizard with three steps: 'Step 1: Connect Account', 'Step 2: Enable Traffic Visibility', and 'Step 3: Secure Your Account'. A large 'Success!' message is centered on the screen, stating 'Your account is now secured. You can setup another account if you want, or close this to continue.' Below this message are three cards corresponding to the setup steps. A modal dialog box is open in the foreground, titled 'Success', with a green checkmark icon. It contains the text: 'Successfully created egress-eu-central-1-gw-01 gateway' and 'Successfully created ingress-eu-central-1-gw-01 gateway'. The modal has 'GO BACK' and 'CLOSE' buttons at the bottom.

Secure Your Account – Step 2 add GW

The screenshot displays the Cisco Multicloud Defense web interface. A central modal window titled "Success!" is overlaid on the main dashboard. The modal contains the following text and elements:

- Success!**
- Your account is now secured. You can setup another account if you want, or close this to continue.
- A progress bar with three steps:
 - Step 1: Connect Account** (Cloud icon with checkmark). Description: Connect a cloud account with the Multicloud Defense Controller. Button: **Connect Account**.
 - Step 2: Enable Traffic Visibility** (Globe icon). Description: Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account. Button: **Enable Visibility**.
 - Step 3: Secure Your Account** (Lock icon). Description: Setup a Service VPC and Multicloud Defense Gateway to secure your Account. Button: **Secure Account**.
- Navigation buttons at the bottom: **<< GO BACK** and **CLOSE**.

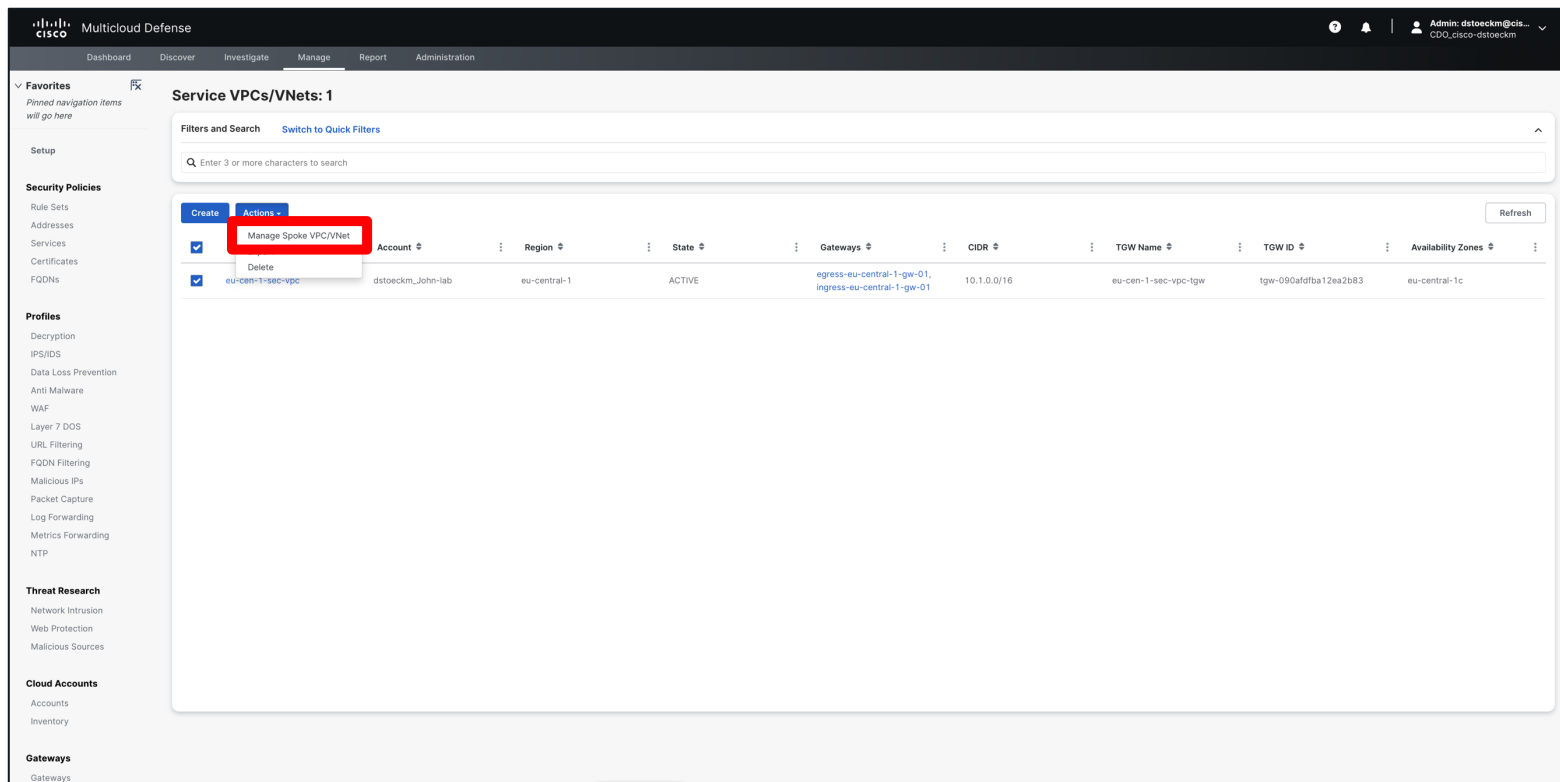
The background interface shows a sidebar with categories like Favorites, Security Policies, Profiles, Threat Research, Cloud Accounts, and Gateways. The top navigation bar includes Dashboard, Discover, Investigate, Manage, Report, and Administration. The user is logged in as Admin: dstoeckm@cis...

AWS GW status

The screenshot displays the AWS Management Console interface for the EC2 service. The left sidebar shows navigation options like EC2 Dashboard, EC2 Global View, Events, and various instance types. The main content area is titled 'Instances (2)' and shows a table of two running instances. The first instance is 'ciscomcd-egress-eu-central-1-gw-01-s...' with ID 'i-0f78ae5ec81310eb5', and the second is 'ciscomcd-ingress-eu-central-1-gw-01-...' with ID 'i-092cc6493e89e1690'. Both are m5.large instances in the eu-central-1c availability zone, with status 'Initializing'. The bottom of the console shows a 'Select an instance' button.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
ciscomcd-egress-eu-central-1-gw-01-s...	i-0f78ae5ec81310eb5	Running	m5.large	Initializing	View alarms +	eu-central-1c	-	18.159.253.242	3.71.218.178	-
ciscomcd-ingress-eu-central-1-gw-01-...	i-092cc6493e89e1690	Running	m5.large	Initializing	View alarms +	eu-central-1c	-	3.125.160.249	3.77.119.65	-

Connect app_vpc to sec_vpc



The screenshot displays the Cisco Multicloud Defense interface. The left sidebar contains navigation menus for Favorites, Security Policies, Profiles, Threat Research, Cloud Accounts, and Gateways. The main content area is titled 'Service VPCs/VNets: 1' and includes a search bar and a table of service VPCs/VNets. The 'Actions' menu for the 'eu-cen-1-sec-vpc' is highlighted, showing options like 'Manage Spoke VPC/VNet' and 'Delete'.

	Account	Region	State	Gateways	CIDR	TGW Name	TGW ID	Availability Zones
☒	dstoeckm_john-lab	eu-central-1	ACTIVE	egress-eu-central-1-gw-01, ingress-eu-central-1-gw-01	10.1.0.0/16	eu-cen-1-sec-vpc-tgw	tgw-090afdfba12ea2b83	eu-central-1c

Connect app_vpc to sec_vpc

The screenshot shows the Cisco Multicloud Defense console interface. The top navigation bar includes tabs for Dashboard, Discover, Investigate, Manage, Report, and Administration. The user is logged in as Admin: dstoeckm@cisco.com. The left sidebar contains a navigation menu with sections: Favorites, Setup, Security Policies, Profiles, Threat Research, Cloud Accounts, and Gateways. The main content area is titled "eu-cen-1-sec-vpc" and includes a note: "Add a route in the route table(s) in these vpcs: Destination: <service-vpc-cidr> Target: <Transit-gw-id>. Look at the documentation for more details". Below this, there are two tabs: "Spoke VPCs for Current Account" and "Spoke VPCs for External Account". The "Spoke VPCs for Current Account" tab is active, showing a table with columns: Account, Region, VPC, Route Tables, TOW Attachment Subnet, and Status. The table has one row with the following data: Account: dstoeckm_john-lab, Region: eu-central-1, VPC: opencart_vpc | vpc-079c23af1... (with a dropdown menu open showing "Select Option" and "opencart_vpc | vpc-079c23af1c7563512 | 192.31.0.0/16"), Route Tables: View/Edit, TOW Attachment Subnet: View/Edit, and Status: (empty). The dropdown menu for the VPC column is open, showing "Select Option" and "opencart_vpc | vpc-079c23af1c7563512 | 192.31.0.0/16".

Connect app_vpc to sec_vpc

The screenshot displays the Cisco Multicloud Defense console interface. The top navigation bar includes tabs for Dashboard, Discover, Investigate, Manage, Report, and Administration. The user is logged in as Admin: dstoeckm@cisco.com.

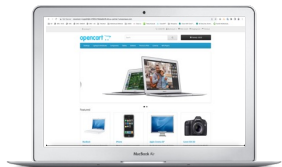
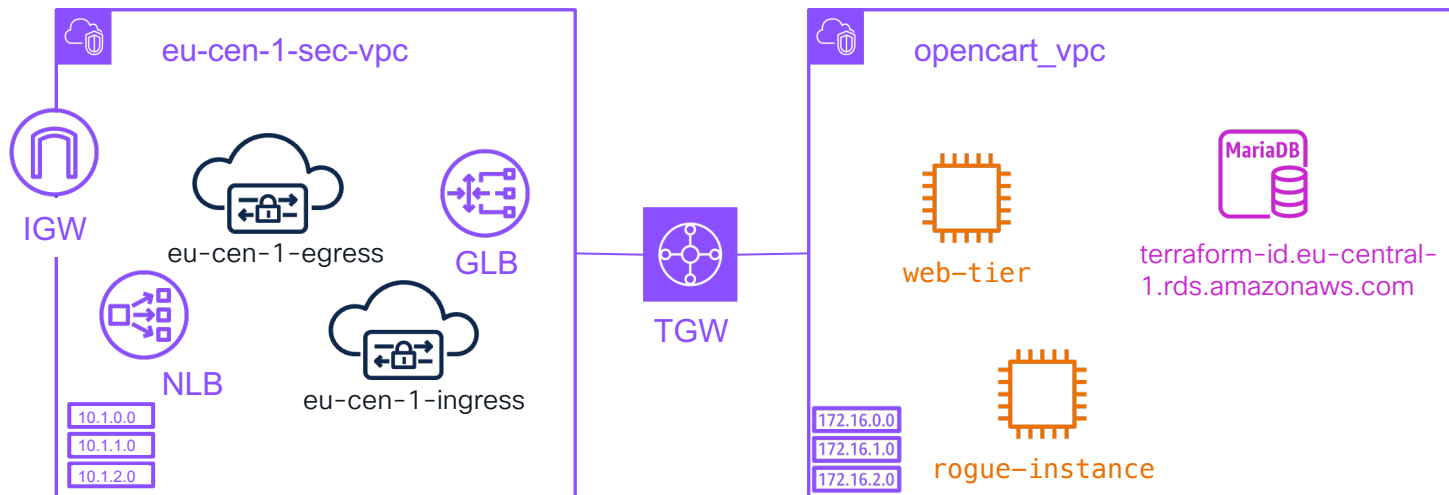
The left sidebar contains a 'Favorites' section with a pinned item 'eu-cen-1-sec-vpc'. Below this are sections for 'Setup', 'Security Policies' (Rule Sets, Addresses, Services, Certificates, FQDNs), 'Profiles' (Decryption, IPS/IDS, Data Loss Prevention, Anti Malware, WAF, Layer 7 DOS, URL Filtering, FQDN Filtering, Malicious IPs, Packet Capture, Log Forwarding, Metrics Forwarding, NTP), 'Threat Research' (Network Intrusion, Web Protection, Malicious Sources), 'Cloud Accounts' (Accounts, Inventory), and 'Gateways'.

The main content area is titled 'Manage Spoke VPCs for > eu-cen-1-sec-vpc'. It includes a note: 'Add a route in the route table(s) in these vpcs: Destination: <service-vpc-cidr> Target: <Transit-gw-id>. Look at the documentation for more details'. Below this are two tabs: 'Spoke VPCs for Current Account' and 'Spoke VPCs for External Account'. The 'Current Account' tab is active, showing a table with columns 'Account', 'Region', and 'VPC'. The table contains one entry: 'dstoeckm_john-lab' in the 'eu-central-1' region, with 'opencart' as the VPC.

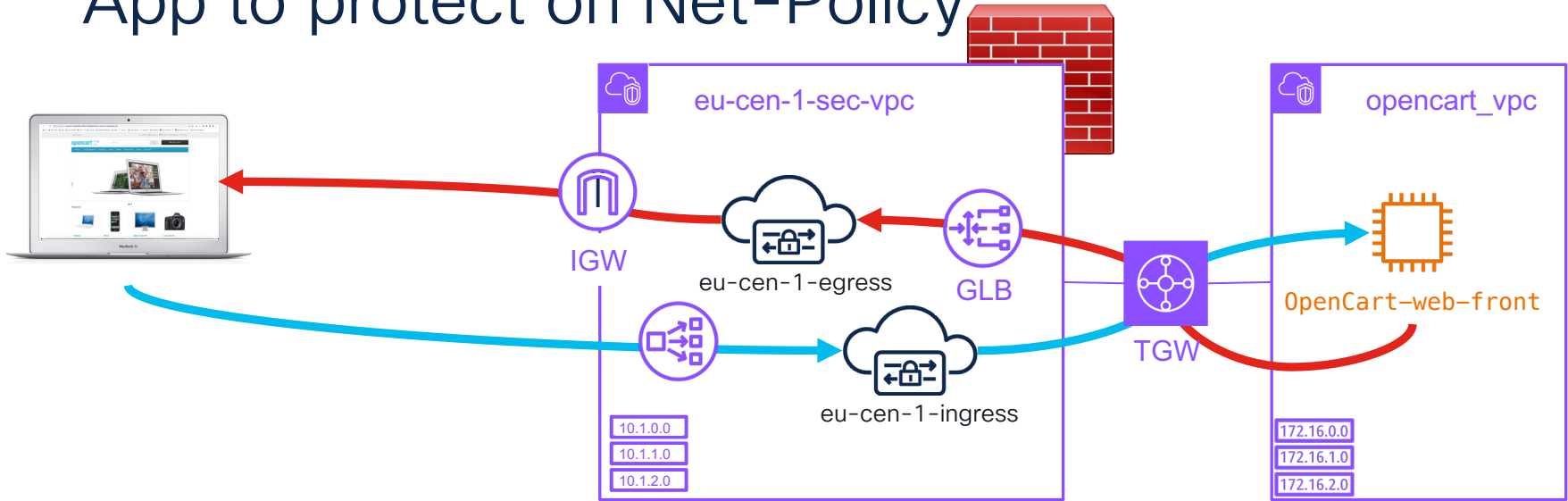
On the right side, there is a panel titled 'Update route tables of spoke VPCs'. It contains a 'Route Table' section with a table showing the selected route table 'rtb-06975782294bba982' and its associated subnets. Below this is a 'Routes' table:

Destination	Target	State
172.31.0.0/16	local	✓ Active
0.0.0.0/0	tgw-0ea7ec080251506eb	Disabled
0.0.0.0/0	tgw-090afdfba12ea2b83	✓ Active

App to protect



App to protect on Net-Policy



Reverse proxy: 22,80 → OpenCart-web-front

eu-cen-1-egress: 8080 ← Forwarding proxy

Apply rules

prod1.mcd.euo.cisco.com/manage/policy?rulesetID=1&rulesetType=DEFAULT&ruleID=11

Multicloud Defense

Dashboard Discover Investigate Manage Report Administration

Save Rules Confirmation

Are you sure you want to save your changes?

Changes from:

#	Name	Type	Source Address	Destination Address	Service	Action	IPS Profile
1	SystemHC-65534-65534	HealthCheck	any	any	SystemHC-65534-65534	ALLOW_NOLOG	
2	valtix-sample-ingress-allow	ReverseProxy	any	Gateway	valtix-sample-backend-app	ALLOW_LOG	valtix-sample-alanced-alert
3	opencart	ReverseProxy	internet	Gateway	opencart_app_rev_proxy	ALLOW_LOG	
4	ansible_access	ReverseProxy	internet	Gateway	opencart_ssh_rev_proxy	ALLOW_LOG	

Changes to:

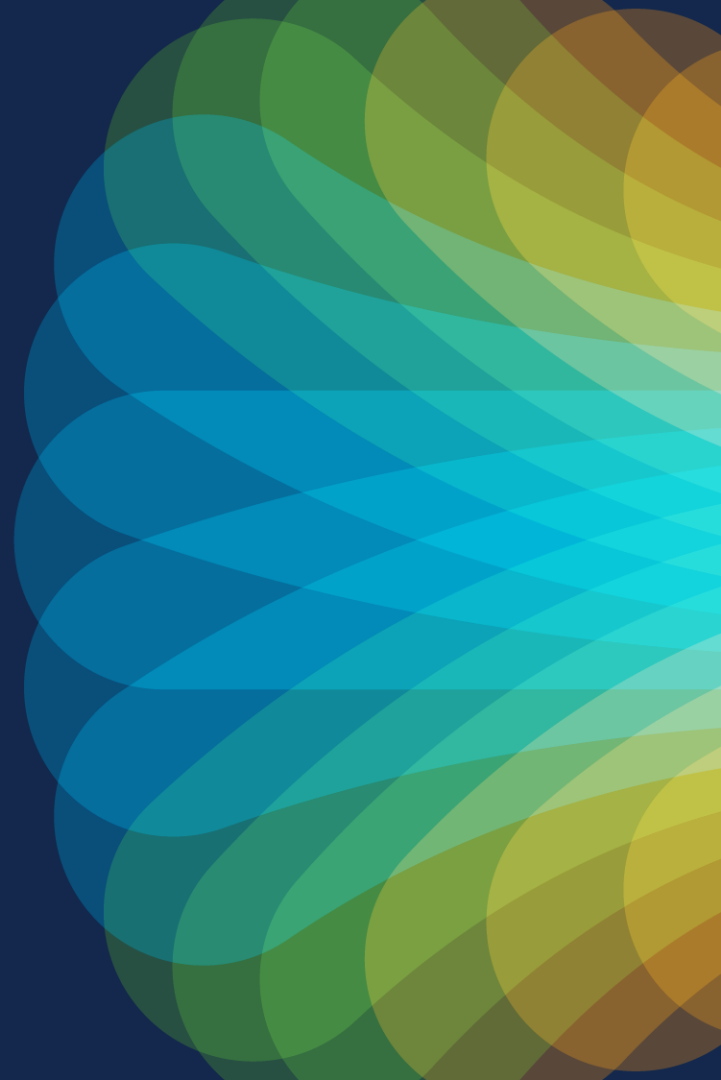
#	Name	Type	Source Address	Destination Address	Service	Action	IPS Profile
1	SystemHC-65534-65534	HealthCheck	any	any	SystemHC-65534-65534	ALLOW_NOLOG	
2	valtix-sample-ingress-allow	ReverseProxy	any	Gateway	valtix-sample-backend-app	ALLOW_LOG	valtix-sample-alanced-alert
3	opencart_ingress_80	ReverseProxy	internet	Gateway	opencart_app_rev_proxy	ALLOW_LOG	
4	opencart_ingress_22	ReverseProxy	internet	Gateway	opencart_ssh_rev_proxy	ALLOW_LOG	

Cancel Save

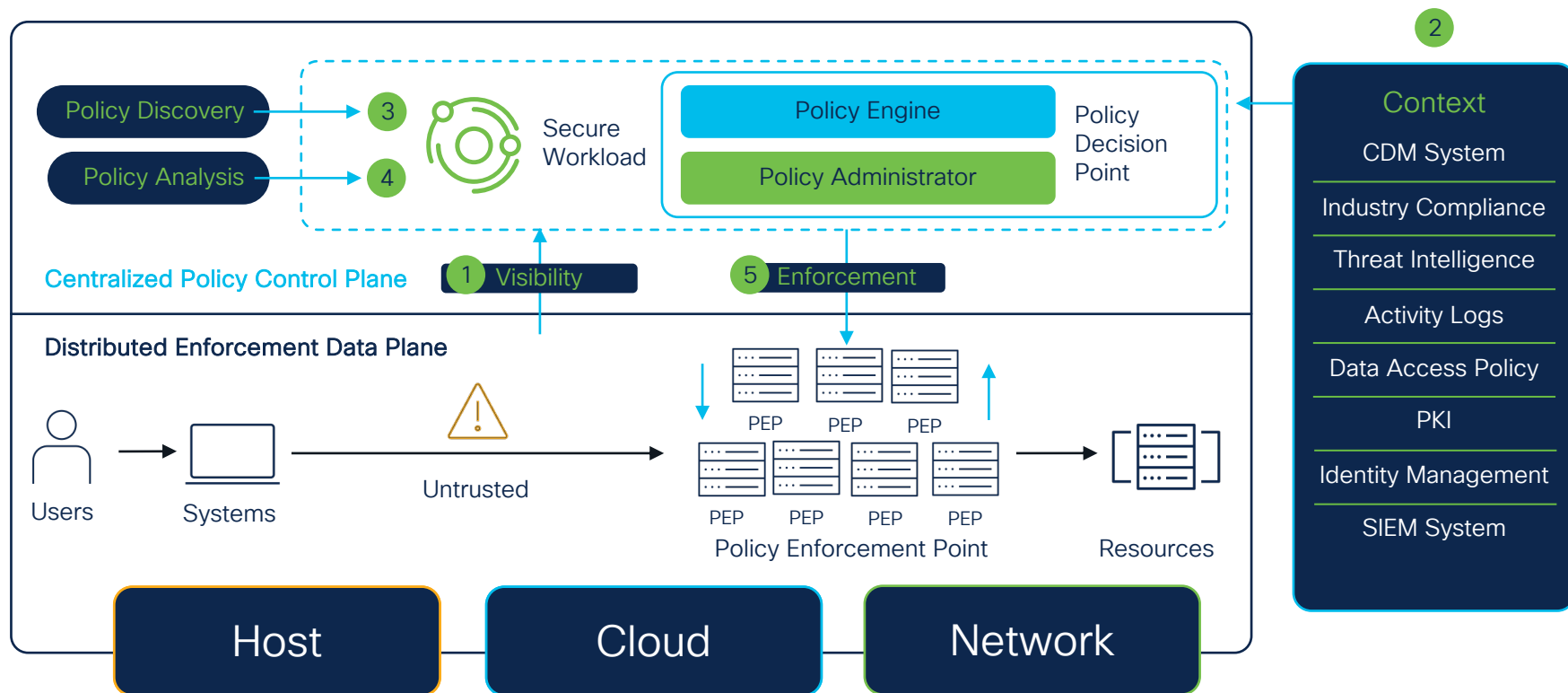


Demo

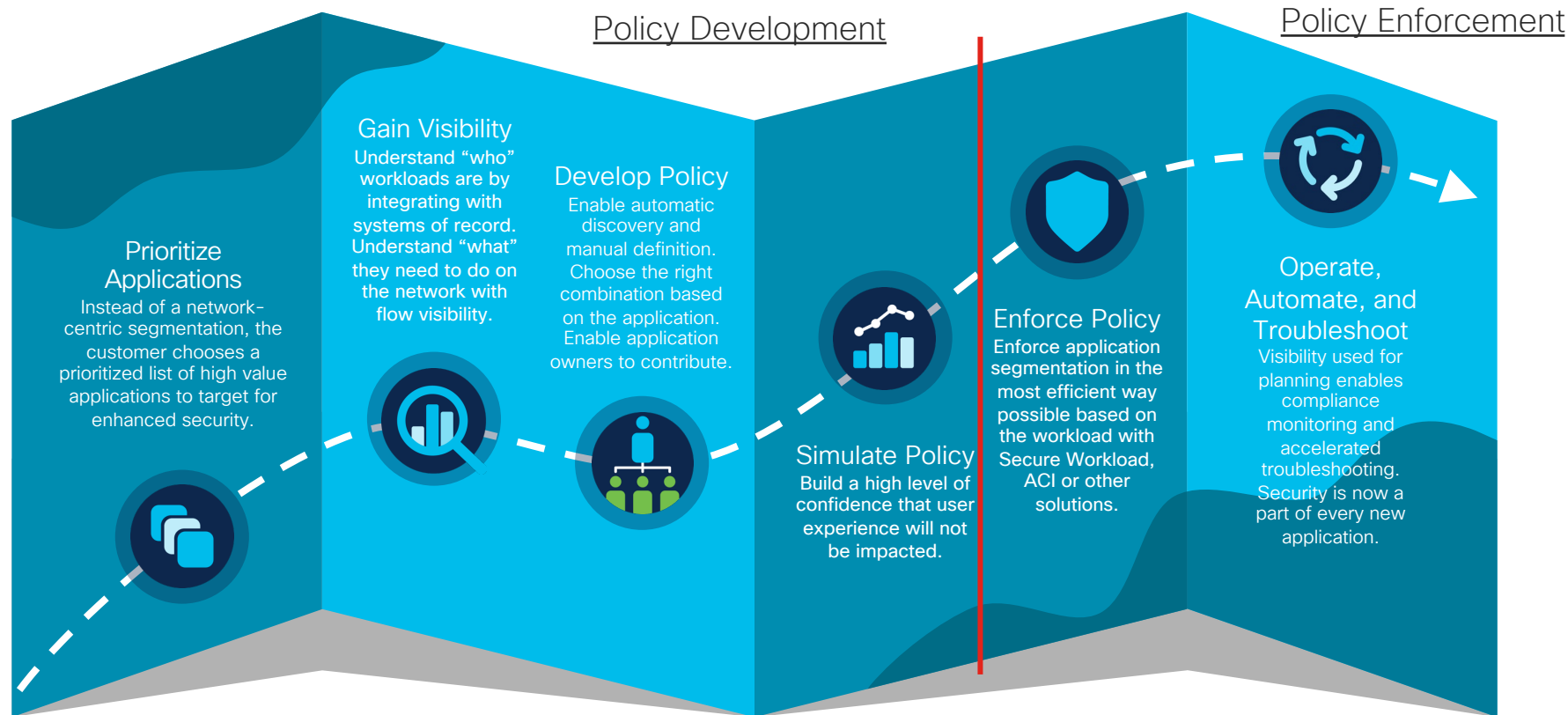
Cisco Secure Workload cloud connector



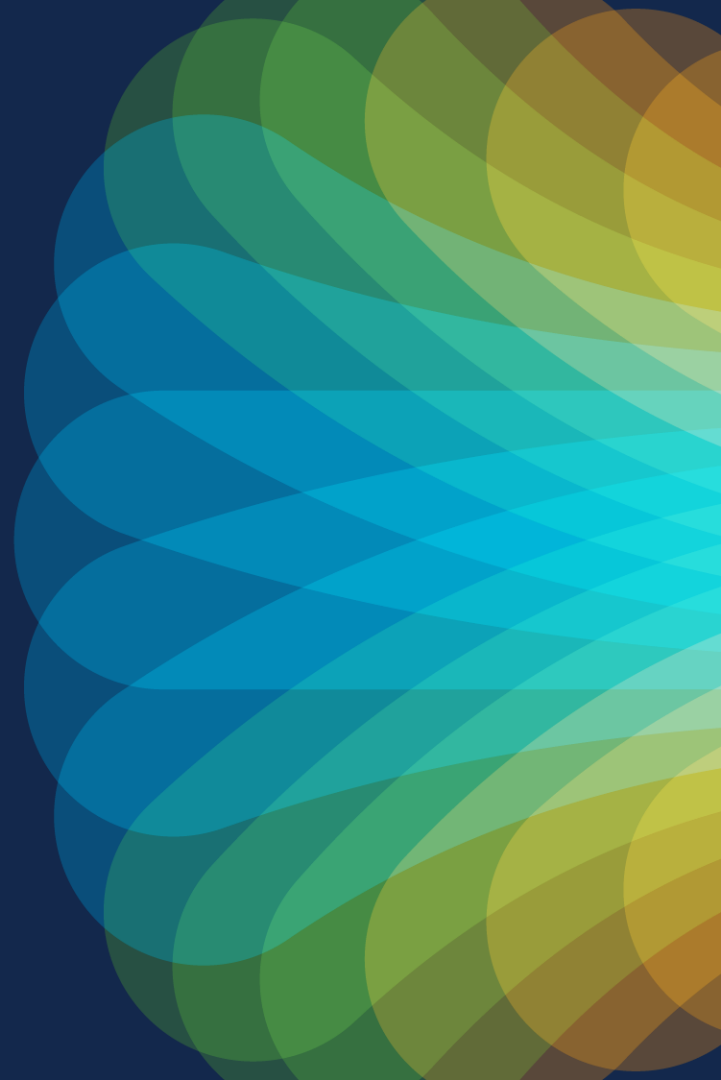
Secure Workload and NIST 800-207



Steps to Application Segmentation



Micro segmentation overview



A composite image with a dark, moody background. On the left, a person wearing a grey hoodie and a white mask with a wide, toothy grin is visible. In the center, a computer monitor displays a web application titled 'Past due invoices'. The application has a table with the following data:

Number	Customer Name	Date	Due Date	Status
ASET-8	Sampla, Inc	6/17/19	2/16/21	Overdue
ASET-4	Big Kahuna Burger	1/17/19	6/16/21	Overdue
ASET-1	Resistor and Switches	11/9/18	4/4/21	Overdue
ASET-2	Alford Biscuit	11/4/18	9/23/19	Overdue
ASET-7	Initech	10/18/18	6/28/21	Overdue

Below the table is a link that says 'view all 101 invoices'. The monitor is on a desk, and a keyboard is partially visible at the bottom. On the right side of the image, there is a circular inset showing two stylized, cartoonish figures of a man and a woman in conversation.

[Welcome, user!](#) / [Settings](#) / [Logout](#)

Dashboard

Invoices

Recurring Invoices

Customers

Estimates

Products

Search

[Status: Opened](#) / [Closed](#) / [Overdue](#) / [Drafts](#)

[Sort](#)

[Filter](#)

[Series](#)

[Customer](#)

[Tag](#)

Receipts

\$239,335.25

Due

\$24,187.97

Overdue

\$2,813.97

V/A 10%

\$20,368.28

V/A 6%

\$1,900.06

V/A 7%

\$2,621.06

IPP*

(\$9,864.00)

Total

\$262,149.22

Net

\$242,223.88

Taxes

\$14,925.33

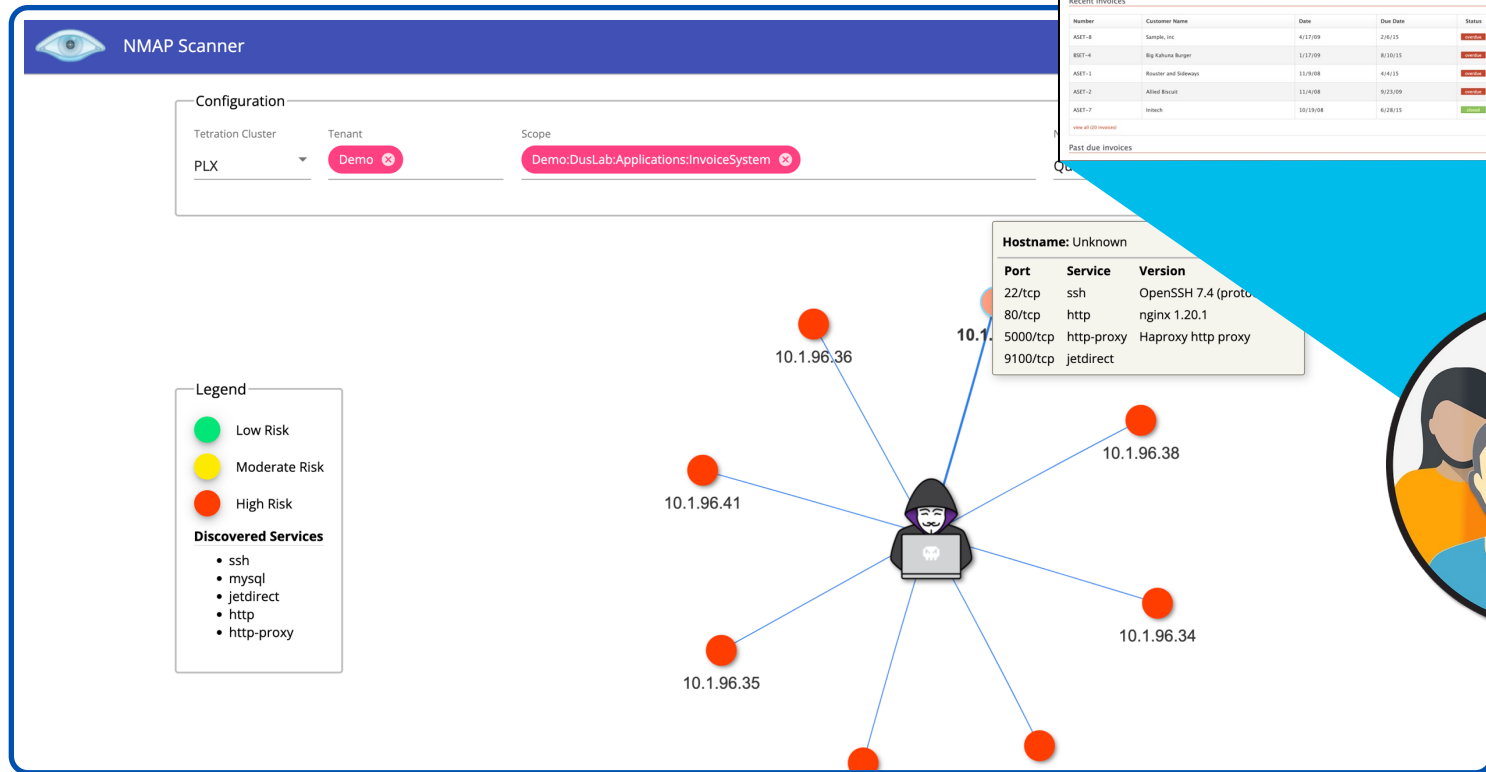
Recent Invoices

Number	Customer Name	Date	Due Date	Status	Due	Total
ASST-8	Sample, Inc.	6/17/08	2/6/15	PAID	\$720.48	\$12,247.42 View
ASST-4	Big Kahuna Burger	3/1/08	8/10/15	PAID	\$156.95	\$3,995.18 View
ASST-1	Revisor and Solicitors	11/9/08	4/4/15	PAID	\$90.04	\$11,407.92 View
ASST-2	Alfred Brucet	11/4/08	9/22/09	PAID	\$1,346.00	\$22,375.79 View
ASST-7	Intech	10/19/08	6/28/15	PAID		\$8,131.10 View

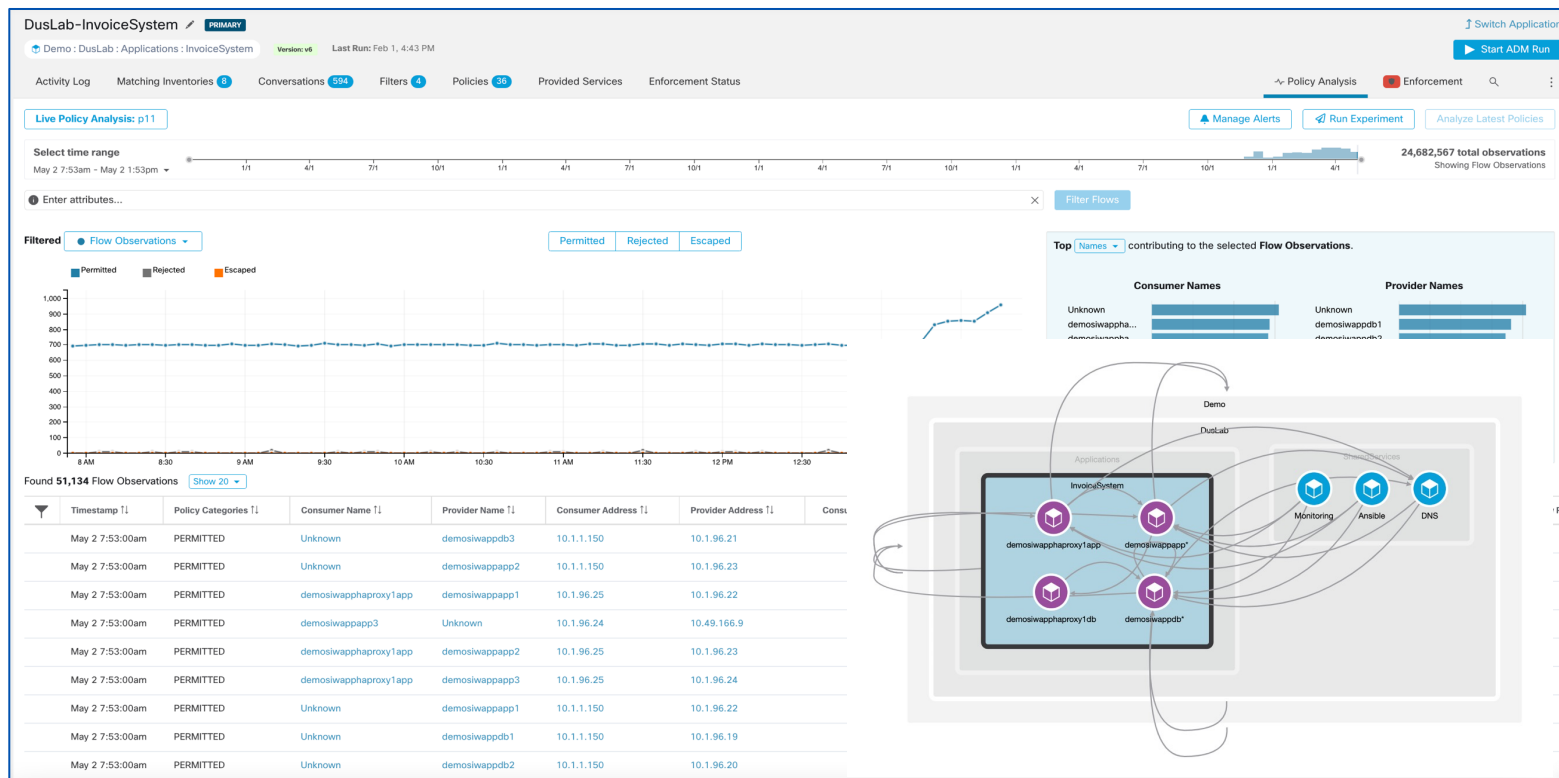
[View all \(20\) invoices](#)



What do we see from outside?



Policy analytics and control



[Welcome, user!](#) / [Settings](#) / [Logout](#)

Dashboard

Invoices

Recurring Invoices

Customers

Estimates

Products

Search

[Status: Opened](#)
[Closed](#)
[Overdue](#)
[Drafts](#)

[Sort](#)
[Filter](#)

[Series](#)
[Customer](#)

[Tag](#)

Receipts

\$239,335.25

Due

\$2,618,987

Overdue

\$2,813.97

IVA 10%

\$20,368.28

IVA 6%

\$1,900.06

IVA 7%

\$2,621.06

IRPF

(\$9,864.00)

Total

\$262,149.22

Net

\$242,285.18

Taxes

\$14,925.33

Recent Invoices

Number	Customer Name	Date	Due Date	Status	Due	Total
ASIT-8	Sampla, Inc	6/17/08	2/6/15	PAID	\$720.48	\$12,247.42 View
ASIT-4	Big Kefano Burger	1/1/08	8/10/15	PAID	\$156.95	\$3,995.18 View
ASIT-1	Revisor and Soloway	11/9/08	4/4/15	PAID	\$90.04	\$11,407.92 View
ASIT-2	Alfred Brucet	11/4/08	9/25/09	PAID	\$1,346.00	\$22,375.79 View
ASIT-7	Intech	10/19/08	6/28/15	PAID		\$8,131.10 View

[View all \(20\) invoices](#)



What do we see now from outside?

**NMAP Scanner**

Configuration

Tetration Cluster

Tenant

Scope

PLX

Demo

Demo:DusLab:Applications:InvoiceSystem

Legend

Low Risk

Moderate Risk

High Risk

Discovered Services

- http



10.1.96.40

Hostname: Unknown

Port	Service	Version
80/tcp	http	nginx 1.20.1



swapp

Dashboard Invoices Recurring Invoices Customers Estimates Products

Search: From: To: By: Tag: Search Reset

Status: Opened | Closed | Overdue | Drafts Send: Series: Customer: Tag:

Receipts	\$259,335.25	I/A 10%	\$20,268.28	Total	\$262,149.22
Due	\$2,813.97	I/A 4%	\$1,900.06	I/A 4%	\$147,223.88
Overdue	\$2,813.97	I/A 7%	\$1,621.06	Items	\$14,975.13
		IBP:	(\$9,864.08)		

Recent invoices

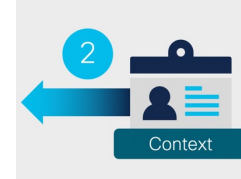
Number	Customer Name	Date	Due Date	Status	Due	Total
ASST-8	Sample, Inc	6/17/09	7/6/15	Overdue	\$720.48	\$13,287.42
ASST-4	Big Kahuna Burger	1/17/09	6/10/15	Overdue	\$176.95	\$3,995.19
ASST-1	Roulette and Sideways	11/9/08	4/4/15	Overdue	\$90.04	\$13,467.82
ASST-2	Allied Broadcast	11/4/08	9/23/09	Overdue	\$1,566.00	\$22,370.79
ASST-7	Intech	10/19/08	6/28/15	Overdue	\$8,110.14	\$8,110.14

View all 100 invoices

Past due invoices

Context

TAG – LABEL – ANNOTATION



Key: Value

Context

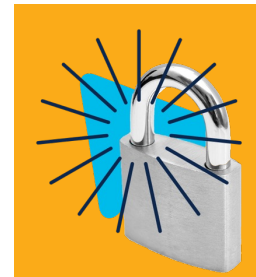
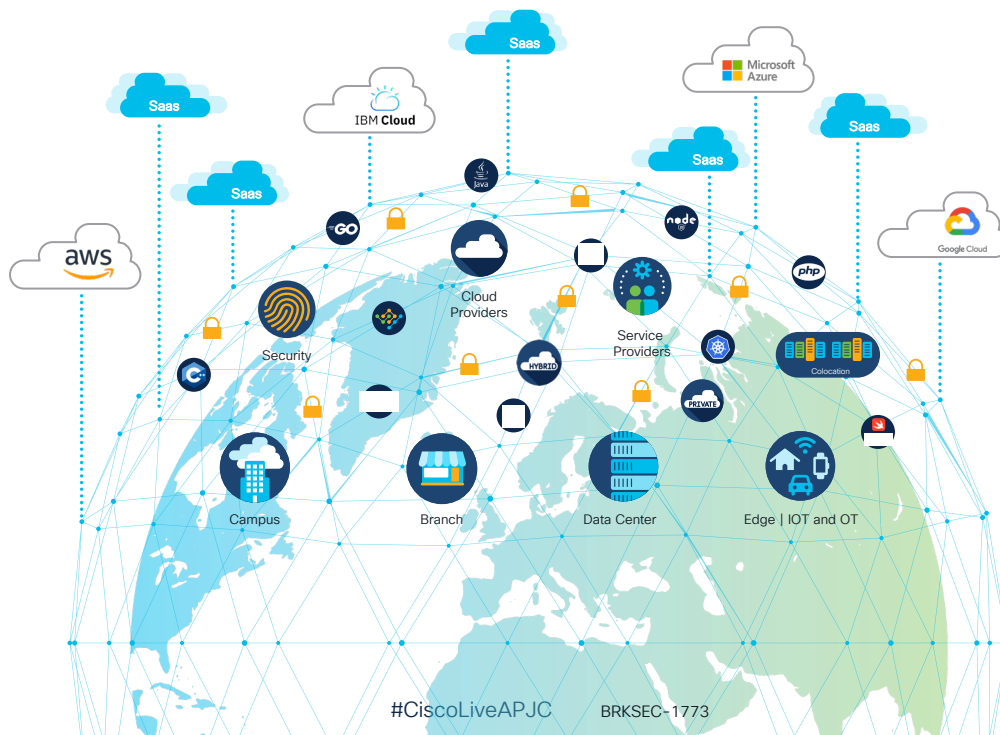
TAG – LABEL – ANNOTATION



Key:	Value
Last name:	Mustermann
Maiden name:	Gabler
First name:	Erika
Date of birth:	12.08.1983
Place of birth:	Berlin
Document ID:	LZ6311T47

Cisco Secure Workload cloud connector

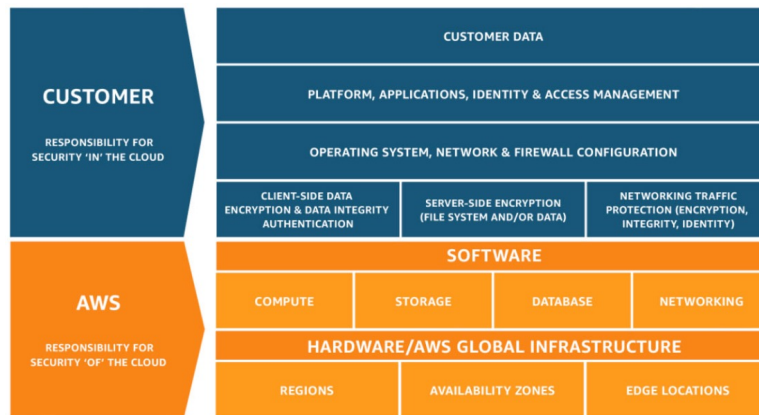
The internet is your runtime



AWS – Shared Responsibility Model

AWS responsibility “Security of the Cloud” – AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility “Security in the Cloud” – Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the **AWS-provided firewall (called a security group)** on each instance.

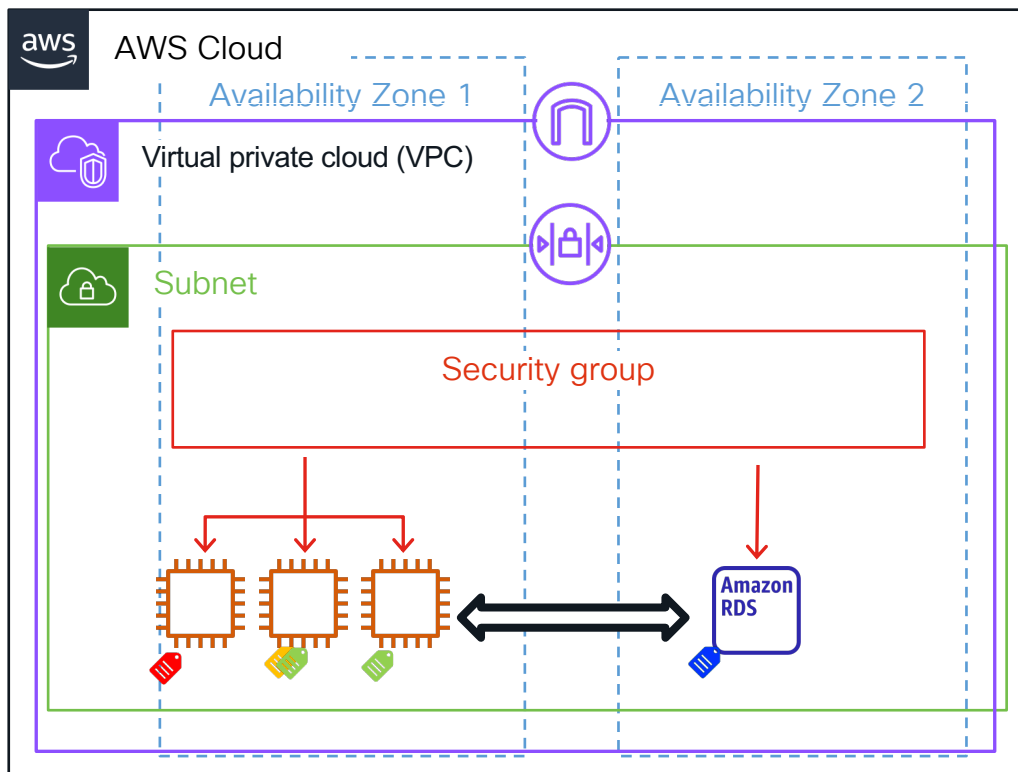


<https://aws.amazon.com/compliance/shared-responsibility-model/>
<https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>
<https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate>

AWS



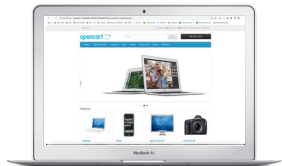
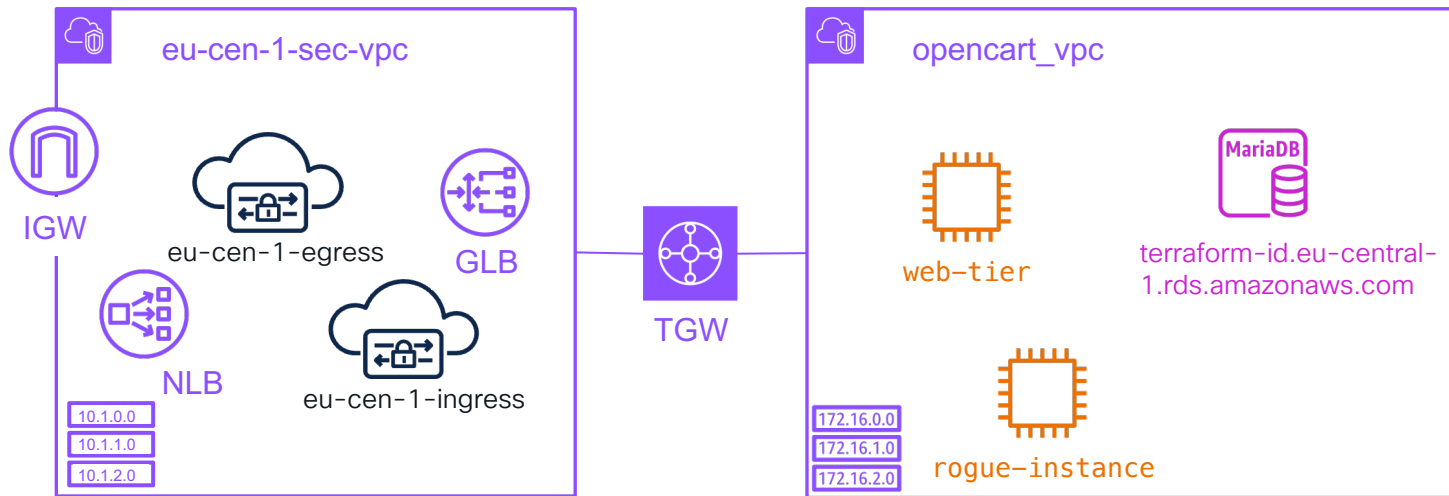
AWS ~~Limitations~~ Quotas



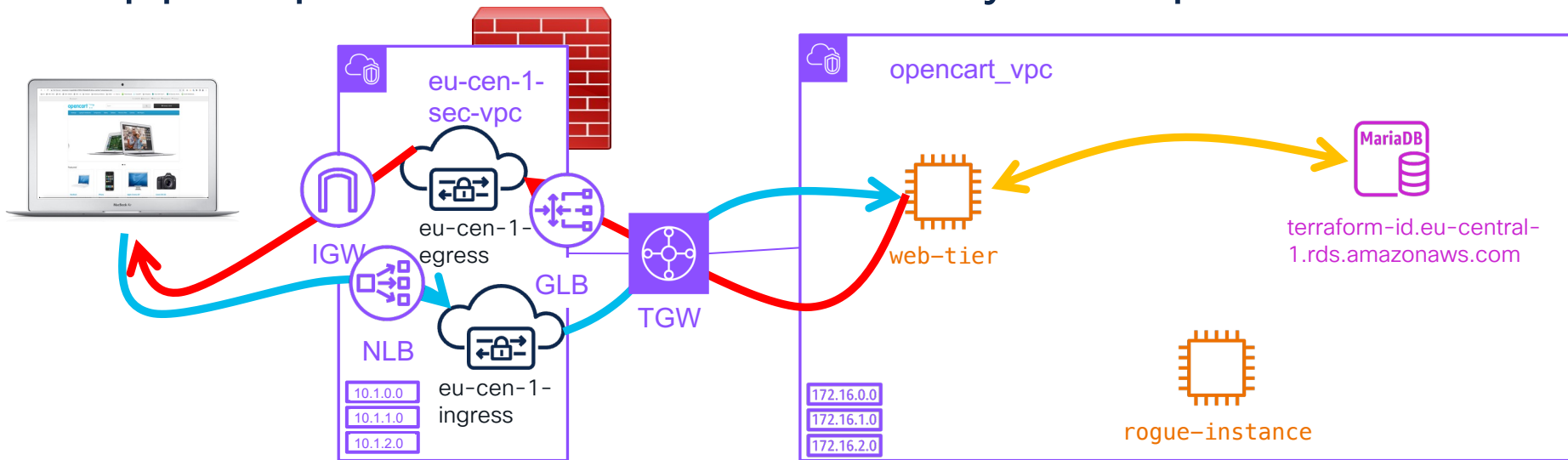
VPC and subnets

Name	Default	Adjustable
VPCs per Region	5	Yes
VPC security groups per Region	2500	Yes
Inbound or outbound rules per security group	60	Yes
Security groups per network interface	5	Yes (up to 16)

App to protect



App to protect on AWS Security Group



eu-cen-1-sec-vpc : 22,80 → OpenCart-web-front

eu-cen-1-sec-vpc : 8080 ← Forwarding proxy

Web-tier ← 3306 → RDS

AWS Connector setup prerequisite

The screenshot shows the AWS Management Console interface for a VPC. The left sidebar contains navigation links for VPC dashboard, EC2 Global View, and various VPC resources. The main content area displays the details for the VPC 'vpc-079c23af1c7563512 / opencart_vpc'. The details are organized into a table with columns for VPC ID, State, DNS hostnames, and DNS resolution. Below the details, the 'Flow logs' section is visible, showing a single log entry with a custom format. A tooltip is displayed over the 'Custom' link, showing the format string: '\$(srcaddr) \$(dstaddr) \$(srcport) \$(dstport) \$(protocol) \$(packets) \$(bytes) \$(start) \$(end) \$(action) \$(log-status) \$(interface-id) \$(tcp-flags) \$(flow-direction)'.

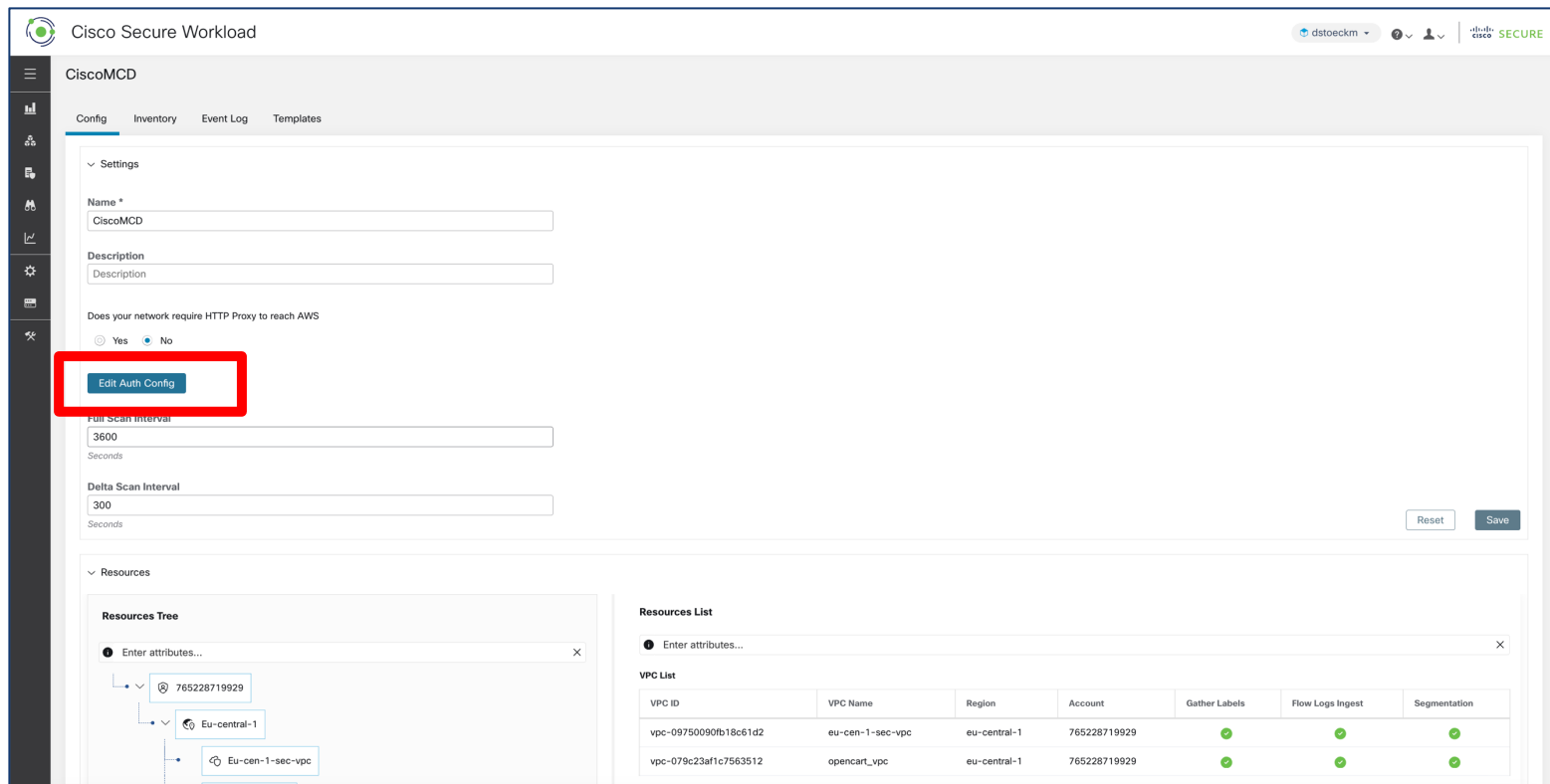
Details			
VPC ID	State	DNS hostnames	DNS resolution
vpc-079c23af1c7563512	Available	Enabled	Enabled
Tenancy	DHCP option set	Main route table	Main network ACL
Default	dopt-0fc1e93c9ffc0c518	rtb-06975782294bbe982	acl-0d0d134d184a90f01
Default VPC	IPv4 CIDR	IPv6 pool	IPv6 CIDR (Network border group)
Yes	172.31.0.0/16	-	-
Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups	Owner ID	
Disabled	-	765228719929	

Flow logs (1/1)				
role ARN	Cross account IAM role	Maximum aggregation interval	Creation time	State
-	-	1 minute	Tuesday, 28 November 2023 at 15:58:3...	Active

AWS Connector setup

The screenshot shows the Cisco Secure Workload interface. At the top, the header includes the Cisco logo, 'Cisco Secure Workload', and a user profile 'dstoeckm'. Below the header, a navigation bar shows 'Back to Connectors' and 'AWS Connectors'. A warning banner states: 'The cluster is unhealthy. There are platform alerts in the cluster. Please change your Tenant preference to [Default](#) and check the Alerts page.' The main content area is titled 'AWS Connectors' and features the AWS logo, a button 'Configure your new connector here', and descriptive text: 'Ingest cloud inventory metadata, ingest flow data for AWS-based workloads, ingest metadata from EKS (Elastic Kubernetes Services), and enforce policy.' Below this are links for 'Getting Started Guide' and 'Generate Templates'. A modal dialog box is open in the center with the title 'Are you sure?' and a close button (X). The dialog text reads: 'AWS CloudFormation template with the roles and policies required for the capabilities you wish to enable need to be **generated** and uploaded to AWS. Without this step, you will not be able to successfully create an AWS Connector Config. Proceed?' At the bottom of the dialog are 'No' and 'Yes' buttons.

AWS Connector setup



Cisco Secure Workload

dstoeckm

CiscoMCD

Config Inventory Event Log Templates

Settings

Name *

CiscoMCD

Description

Description

Does your network require HTTP Proxy to reach AWS

☐ Yes ☒ No

Edit Auth Config

Full Scan Interval

3600

Seconds

Delta Scan Interval

300

Seconds

Reset Save

Resources

Resources Tree

Enter attributes...

765228719929

Eu-central-1

Eu-cen-1-sec-vpc

Resources List

Enter attributes...

VPC List

VPC ID	VPC Name	Region	Account	Gather Labels	Flow Logs Ingest	Segmentation
vpc-09750090fb18c61d2	eu-cen-1-sec-vpc	eu-central-1	765228719929	✓	✓	✓
vpc-079c23af1c7563512	opencart_vpc	eu-central-1	765228719929	✓	✓	✓

AWS Connector setup

The screenshot displays the Cisco Secure Workload management console. At the top, the header shows 'Cisco Secure Workload' and a user profile 'dstoeckm'. A navigation bar includes links for 'Back to Connectors', 'Back to AWS Connectors', and 'CiscoMCD'. A status banner indicates 'The cluster is unhealthy. There are platform alerts in the cluster. Please change your Tenant preference to Default and check the Alerts page.'

The main content area is titled 'CiscoMCD' and features tabs for 'Config', 'Inventory', 'Event Log', and 'Templates'. The 'Inventory' tab is active, showing a tree view on the left under 'Resources' with nodes for '765228719929', 'Eu-central-1', 'Eu-cen-1-sec-vpc', and 'Opencart_vpc'. A 'Convert to Scope' button is highlighted with a red box at the bottom of this tree.

On the right, the 'Inventory Table' section shows a search bar and a table with columns 'Address 1' and 'OS 1'. It displays two rows of IP addresses: '172.31.1.49' and '172.31.7.247'. Below the table, a 'Rows per page' dropdown is set to '5', and a pagination control shows '1'.

AWS Connector setup

Cisco Secure Workload

Back to Connectors / Back to AWS Connectors / CiscoMCD

CiscoMCD

Config Inventory Event Log Templates

Resources

Enter attributes...

765228719929

Eu-central-1

Eu-cen-1-sec-vpc

Opencart_vpc

Convert To Scope

Convert Resources to Scope For security and privacy reasons, you must change the default password before configuring this device. ScopeName Secure Workload created a hierarchical group of the regions and VPCs in AWS, which can form the basis of a comprehensive view of the applications on your network. This map helps you understand the source and destination of traffic flows, and simplifies policy creation and management.

Select a parent containing your cloud inventory (e.g. Internal:Cloud) and review auto-created groups:

dstoeckm:aws

- aws
1 New Child
- eu-central-1
1 New Child
- opencart_vpc

Cancel Save

Convert To Scope

Organisation of apps in AWS

Cisco Secure Workload

Scopes and Inventory

No Draft Changes ⓘ

Filter Scopes...

6 Scopes

- dstoeckm
1 / 5 Children
Inventory: 20
Uncategorized: 13
- aws
1 / 4 Children
Inventory: 7
- eu-central-1
2 / 3 Children
Inventory: 7
Uncategorized: 1
- Applications
1 / 1 Children
Inventory: 2
Uncategorized: 1
- OpenCart-EU-central-1
0 Children
Inventory: 2
- eu-cen-1-sec-vpc
0 Children
Inventory: 4

Query

* orchestrator_system/orch_type = aws or * Datacenter = aws

Query

* orchestrator_system/region = eu-central-1 or * location = eu-central-1

Query

* orchestrator_system/virtual_network_id = vpc-079c23af1c7563512
or * orchestrator_Scope = application

Query

* orchestrator_app_name = opencart
or * app_name = opencart

Query

* orchestrator_system/virtual_network_id = vpc-09750090fb18c61d2

How to organize applications based on defined labels derived from orchestrator, APIs or manual (CSV).

Policy mapping AWS

Cisco Secure Workload

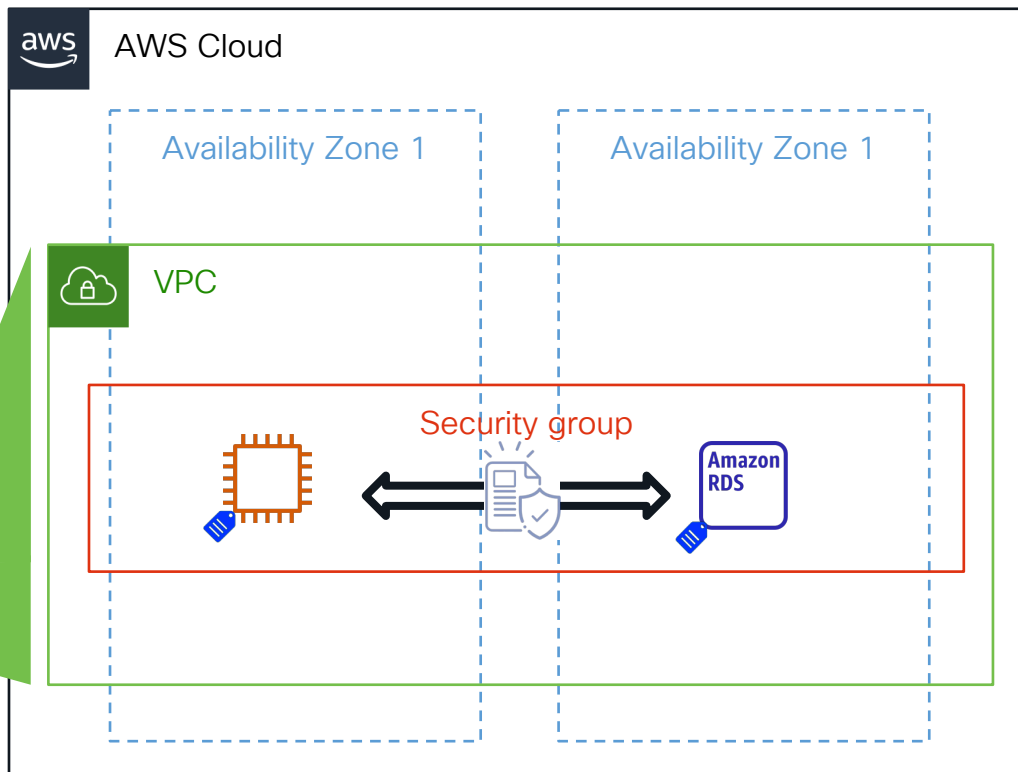
Scopes and Inventory

No Draft Changes ⓘ

Filter Scopes...

6 Scopes

- dstoeckm**
1 / 5 Children
Inventory: 20
Uncategorized: 13
- aws**
1 / 4 Children
Inventory: 7
- eu-central-1**
2 / 3 Children
Inventory: 7
Uncategorized: 1
- Applications**
1 / 1 Children
Inventory: 2
Uncategorized: 1
 - OpenCart-EU-central-1**
0 Children
Inventory: 2
- eu-cen-1-sec-vpc**
0 Children
Inventory: 4



Setting the workspaces up

The screenshot displays the Cisco Secure Workload web interface. On the left is a dark sidebar menu with options: Overview, Organize, Defend (selected), Segmentation, Enforcement Status, Policy Templates, Forensic Rules, Investigate, Reporting, Manage, Workloads, User Access, Service Settings, Platform, and Troubleshoot. The main content area has a top banner stating 'The cluster is unhealthy. There are platform alerts in the cluster. Please change your Tenant preference to Default and check the Alerts page.' Below this is a horizontal bar with tabs: Draft Policies, Analyzed Policies, Enforced Policies, and Policy Requests. The main content area shows a shield icon with three sub-shields and the text 'No Workspaces, create one'. It explains that workspaces are containers for defining, analyzing, and enforcing policies and provides an 'Add Workspace' button. A link to the user guide is also present.

Setting the workspaces up

The screenshot displays the Cisco Secure Workload Segmentation interface. A modal dialog titled "Create New Workspace" is open, allowing the user to define a new workspace. The dialog contains the following fields and options:

- Name:** eu-cen-1-sec-vpc
- Description:** Scope for BRKSEC-1773
- Scope:** dstoeckm:aws:eu-central-1:eu-cen-1-sec-vpc
- Buttons:** Cancel, Create

The background interface shows a tree view of workspaces under the "dstoeckm" scope, including "aws", "eu-central-1", and "Applications". The "eu-central-1" workspace is currently selected, showing its children: "OpenCart-EU-central-1" and "eu-cen-1-sec-vpc".

Below the workspace tree, the "Enforcement Readiness" section provides a summary of the workload health, policy discovery, and policy analysis. The "Parent Scopes" table lists the workspace hierarchy and their enforcement status.

Scope	Primary Workspace	Analysis	Enforcement
dstoeckm	N/A	N/A	N/A
dstoeckm:aws	N/A	N/A	N/A
dstoeckm:aws:eu-central-1	N/A	N/A	N/A
dstoeckm:aws:eu-central-1:Applications	N/A	N/A	N/A

Adding policy

The screenshot displays the Cisco Secure Workload management console. The main view is the 'Policies' tab for the workload 'OpenCart-EU-central-1'. It shows a table of existing policies with columns for Rank, Priority, Action, Consumer, Provider, and Protocols and Ports. A 'Filter Policies' dialog is open, showing 'Absolute and Default Policies' with a 'Catch All' filter set to 'DENY'. A 'Run Quick Analysis' button and an 'Add Policy' button are visible. On the right, a 'Scope' panel shows details for 'OpenCart-EU-central-1', including its full name, primary app, and a query filter: '* orchestrator_app_name = opencart or * app_name = opencart'.

Rank	Priority	Action	Consumer	Provider	Protocols and Ports
Default	100	ALLOW	OpenCart-web-front	aws: eu-central-1: eu-cen-1-sec-vpc	TCP: 8080 (HTTP)
Default	100	ALLOW	OpenCart-web-front	AWS-RDS	TCP: 3306 (MySQL)
Default	100	ALLOW	aws: eu-central-1: eu-cen-1-sec-vpc	OpenCart-web-front	TCP: 22 (SSH) ...1 more

Rows per page: 20

[Download table data as JSON](#) [Download table data as CSV](#)

Scope: OpenCart-EU-central-1

Full Name: dstoeckm:aws:eu-central-1:Applications:OpenCart-EU-central-1

Primary App: OpenCart-EU-central-1

Query: * orchestrator_app_name = opencart or * app_name = opencart

[View Scope Details](#)

> Workloads 1

> IP Addresses 1

Final policy

The screenshot displays the Cisco Secure Workload management console. The main view shows a policy configuration for 'OpenCart-EU-central-1'. The policy is defined by a query: `*orchestrator_app_name = opencart or *app_name = opencart`. The policy is applied to the 'OpenCart-EU-central-1' application, which is part of the 'eu-central-1' region. The application is composed of 'AWS-RDS' and 'OpenCart-web-front' components. The policy is enforced on the 'eu-cen-1-sec-vpc' network. The interface includes a sidebar with navigation options, a top navigation bar with tabs for Matching Inventories, Policies, Filters, Conversations, Provided Services, Policy Analysis, Enforcement Status, and Enforcement. A right-hand pane shows details for the selected policy, including its scope, full name, primary app, and query. The main area displays a diagram of the application architecture, showing the relationship between the application components and the network.

AWS view of the policy – Inbound

sg-0bba6f584db7d0e97 - csw_f63cc1a5_1689404760_000_1701188576

Details

Security group name csw_f63cc1a5_1689404760_000_1701188576	Security group ID sg-0bba6f584db7d0e97	Description Cisco Secure Workload Security group for npc version(1689404760) with filtersHash(f63cc1a5)	VPC ID vpc-079c23af1c7563512
Owner 765228719929	Inbound rules count 8 Permission entries	Outbound rules count 5 Permission entries	

Inbound rules (8)

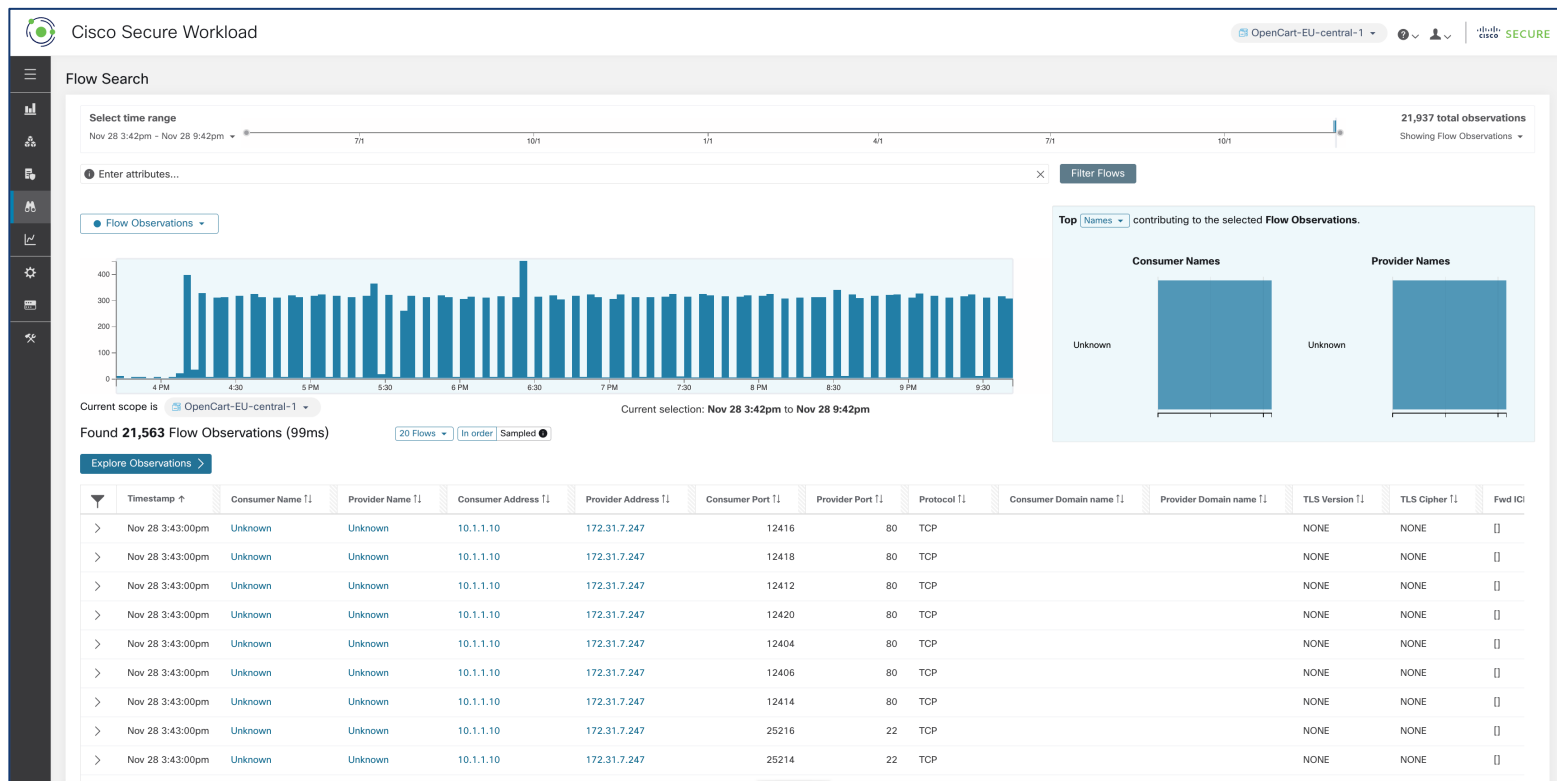
	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
☐	-	sg-042cc6e8e47b6c3fb	IPv4	SSH	TCP	22	10.1.0.17/32	PolicyId=DEFAULT:100...
☐	-	sg-09c9016467b807252	IPv4	SSH	TCP	22	52.29.181.1/32	PolicyId=DEFAULT:100...
☐	-	sg-0ae2c5eef143528a6	IPv4	HTTP	TCP	80	3.68.118.152/32	PolicyId=DEFAULT:100...
☐	-	sg-0d924d6ceaaba9a1	IPv4	HTTP	TCP	80	10.1.0.17/32	PolicyId=DEFAULT:100...
☐	-	sg-058512d62e68fb686	IPv4	SSH	TCP	22	10.1.1.10/32	PolicyId=DEFAULT:100...
☐	-	sg-0ff627e8c31a07eea	IPv4	HTTP	TCP	80	52.29.181.1/32	PolicyId=DEFAULT:100...
☐	-	sg-0034114002272530b	IPv4	SSH	TCP	22	3.68.118.152/32	PolicyId=DEFAULT:100...
☐	-	sg-0f0cb9a02af98b021	IPv4	HTTP	TCP	80	10.1.1.10/32	PolicyId=DEFAULT:100...

AWS view of the policy – outbound

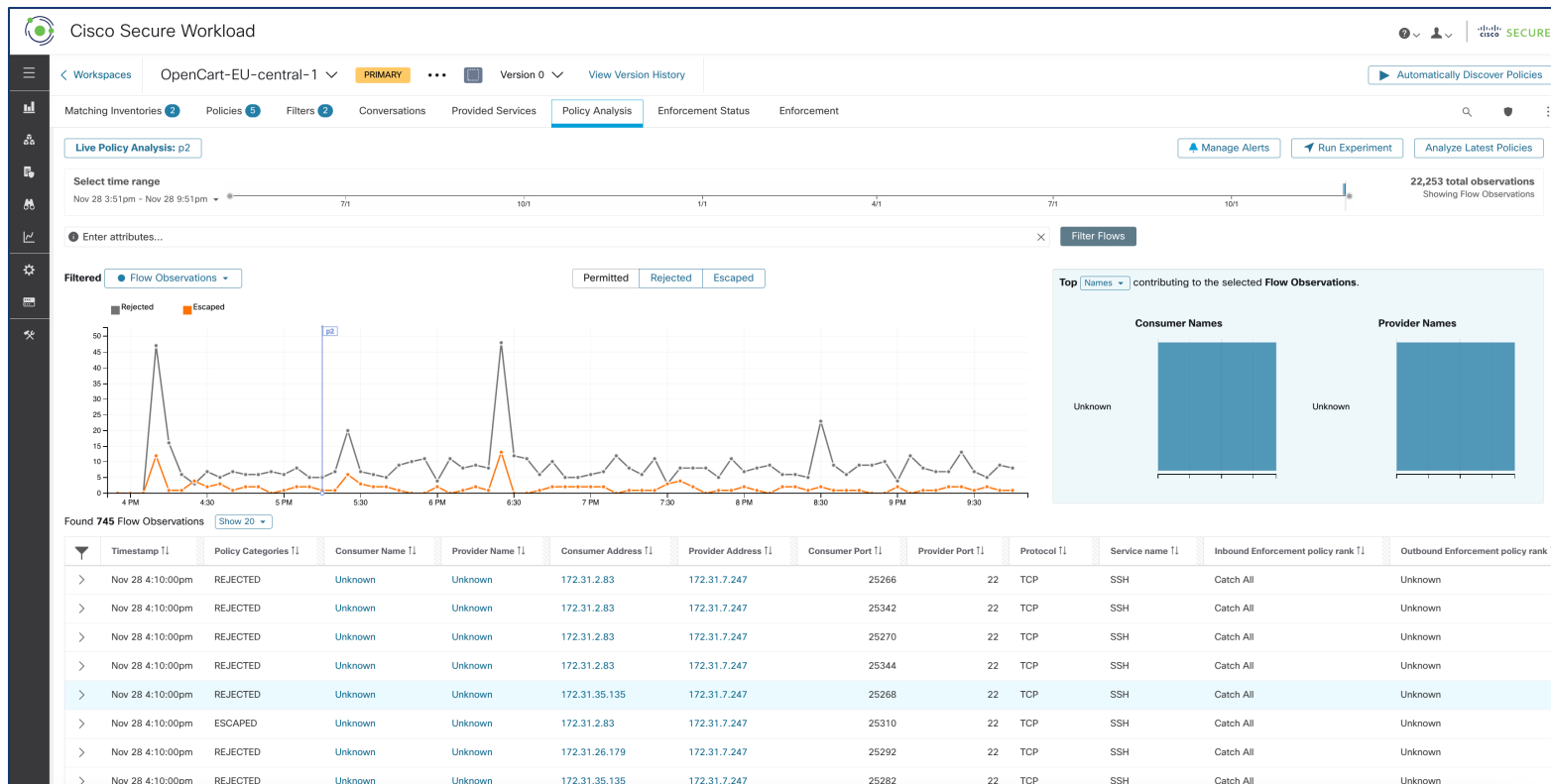
The screenshot displays the AWS Management Console interface. The left-hand navigation pane shows the 'Virtual private cloud' section expanded, with 'Security groups' selected. The main content area shows the details for the security group 'sg-0bba6f584db7d0e97 - csw_f63cc1a5_1689404760_000_1701188576'. The 'Outbound rules' tab is active, showing a list of 5 rules. The rules table includes columns for Name, Security group rule ID, IP version, Type, Protocol, Port range, Destination, and Description. The rules are as follows:

	Name	Security group rule ID	IP version	Type	Protocol	Port range	Destination	Description
☐	-	sgr-00f9a185aa640a587	IPv4	MYSQL/Aurora	TCP	3306	172.31.12.42/32	PolicyId=DEFAULT:100...
☐	-	sgr-063ae0d079b752c64	IPv4	Custom TCP	TCP	8080	10.1.0.66/32	PolicyId=DEFAULT:100...
☐	-	sgr-07db7b649cab4f575	IPv4	Custom TCP	TCP	8080	10.1.1.94/32	PolicyId=DEFAULT:100...
☐	-	sgr-017cd7dfdf9352d05	IPv4	Custom TCP	TCP	8080	3.68.66.202/32	PolicyId=DEFAULT:100...
☐	-	sgr-08cad1ef97f94ed45	IPv4	Custom TCP	TCP	8080	18.184.103.116/32	PolicyId=DEFAULT:100...

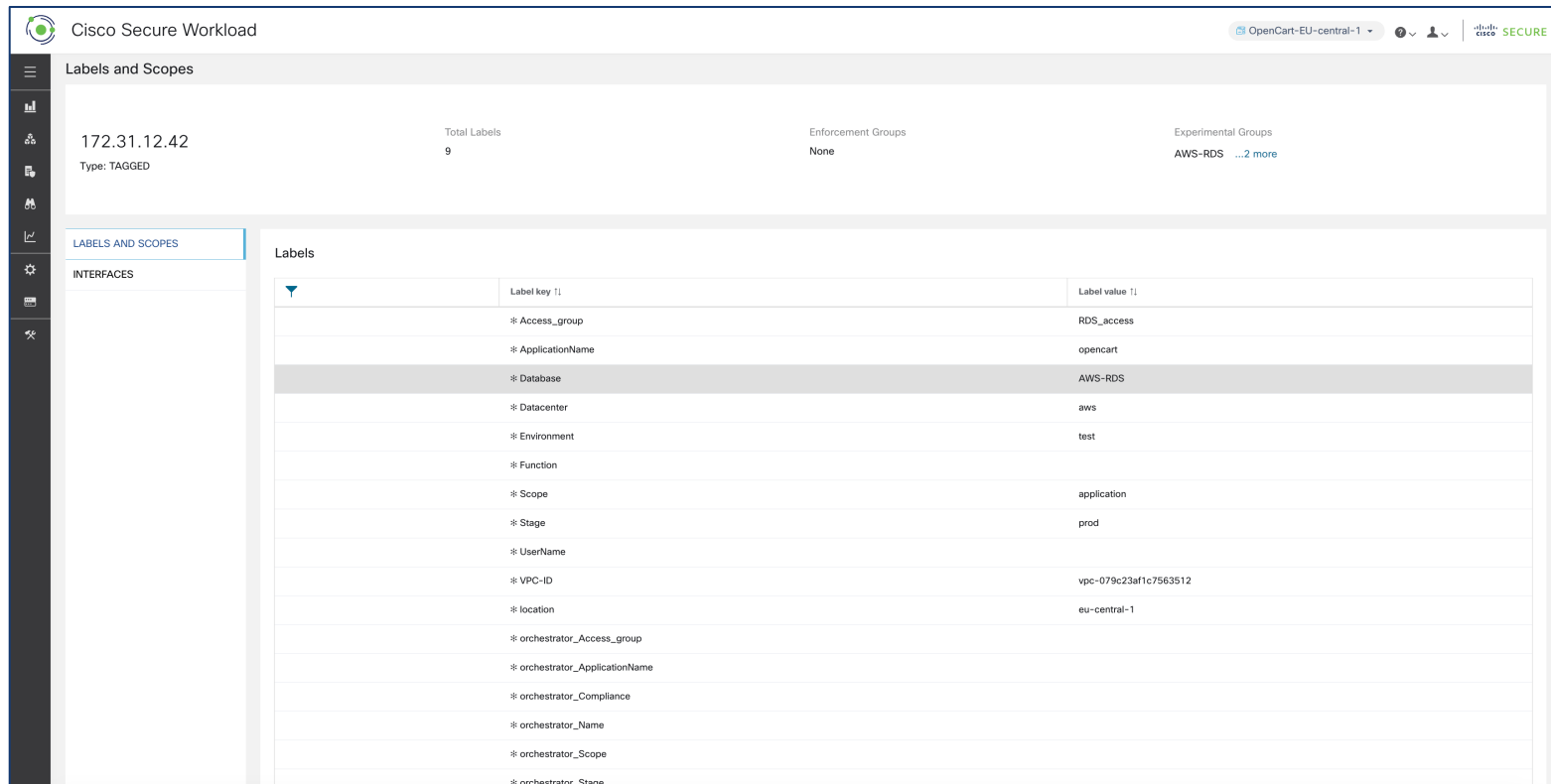
Traffic of the application workspace



Policy analysis view



AWS Ingested Labels



The screenshot displays the Cisco Secure Workload interface. At the top, the title bar shows 'Cisco Secure Workload' and a dropdown menu set to 'OpenCart-EU-central-1'. Below the title bar, the main header area displays 'Labels and Scopes' and the IP address '172.31.12.42' with 'Type: TAGGED'. To the right, it shows 'Total Labels: 9', 'Enforcement Groups: None', and 'Experimental Groups: AWS-RDS ...2 more'.

On the left sidebar, there is a menu with 'LABELS AND SCOPES' and 'INTERFACES'. The 'LABELS AND SCOPES' section is active, showing a table of labels.

Label key [1]	Label value [1]
* Access_group	RDS_access
* ApplicationName	opencart
* Database	AWS-RDS
* Datacenter	aws
* Environment	test
* Function	
* Scope	application
* Stage	prod
* UserName	
* VPC-ID	vpc-079c23af1c7563512
* location	eu-central-1
* orchestrator_Access_group	
* orchestrator_ApplicationName	
* orchestrator_Compliance	
* orchestrator_Name	
* orchestrator_Scope	
* orchestrator_Stage	

Policy based on Label

The screenshot displays the Cisco Secure Workload management console. The main view is the 'Filters' tab, which shows a table of suggested clusters generated by automatic policy discovery algorithms. The table has columns for Name, Matching Inventory T1, Confidence T1, Dynamic T1, and Approved T1. Two clusters are listed: 'AWS-RDS' and 'OpenCart-web-front'. The 'AWS-RDS' cluster is highlighted, and its details are shown in a sidebar on the right. The sidebar includes a search bar, a 'Cluster' section with the name 'AWS-RDS', a 'Cluster Actions' section with icons for delete, edit, and execute, a 'Name' field with the value 'AWS-RDS', a 'Description' field, and a 'Query' field with the value '* Database = AWS-RDS'. Below these fields are links for 'Edit Cluster Query' and 'View Cluster Details'. The sidebar also shows a 'Workloads' section with a count of 0, an 'IP Addresses' section with a count of 1, and a 'Neighbors' section with a count of 1.

Cisco Secure Workload

OpenCart-EU-central-1 PRIMARY Version 0 View Version History

Matching Inventories 2 Policies 5 Filters 2 Conversations Provided Services Policy Analysis Enforcement Status Enforcement

Enter attributes...

Clusters 2 Inventory Filters 1

Clusters are suggested groups generated by the Automatic Policy Discovery algorithms.

Name ↑	Matching Inventory T1	Confidence T1	Dynamic T1	Approved T1
AWS-RDS	1	Approved	✓	✓
OpenCart-web-front	1	Approved	✓	✓

Rows per page 50

Create Cluster

Cluster AWS-RDS

Cluster Actions

Name AWS-RDS

Description

Query * Database = AWS-RDS

Edit Cluster Query View Cluster Details

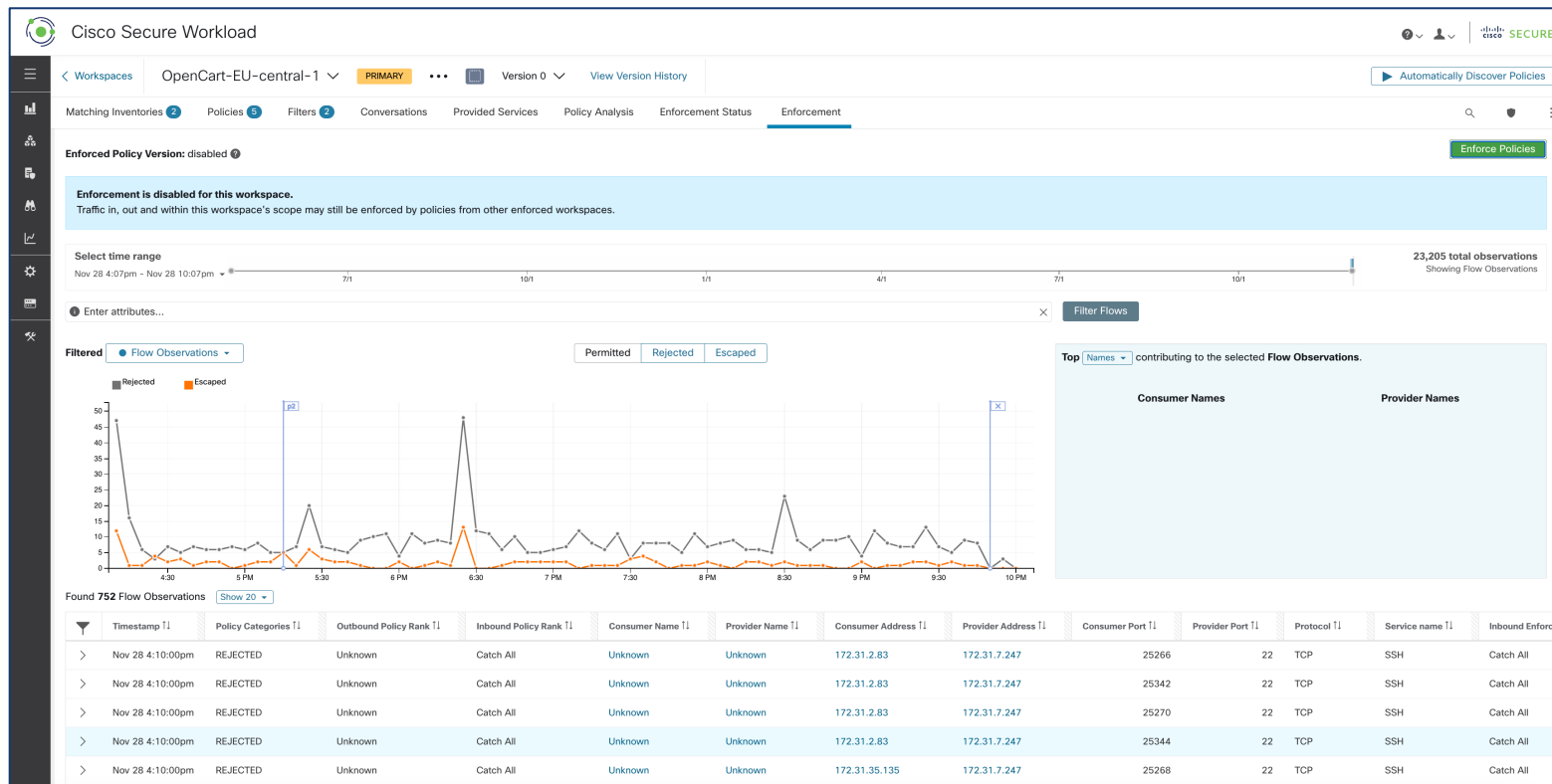
Workloads 0

IP Addresses 1

Address 172.31.12.42

Neighbors 1

Enforcement



Enforcement

Update Enforced Policies

Enforcement Readiness — 2 Review Policy Updates — 3 Impacted Workloads — 4 Impacting Policies — 5 Review & Enforce

Related to [Applications : OpenCart-EU-central-1](#)

Select the version of policies to enforce.

Version Latest Policies

5 / 5 policy changes selected for enforcement

Filter Policies ...

Absolute No matching changes

Default Added 4 Removed 0

Priority	Action	Consumer	Provider	Protocols and Ports
100	ALLOW	aws : eu-central-1 : eu-cen-1-sec-vpc	OpenCart-web-front	TCP : 22 (SSH) ... 1 more
100	ALLOW	OpenCart-web-front	aws : eu-central-1 : eu-cen-1-sec-vpc	TCP : 8080 (HTTP)
100	ALLOW	OpenCart-web-front	AWS-RDS	TCP : 3306 (MySQL)

Catch All

Change Catch All Action from ALLOW to DENY

Cancel Previous Next

Enforcement

Update Enforced Policies

Enforcement Readiness

2 Review Policy Updates

3 Impacted Workloads

4 Impacting Policies

5 Review & Enforce

Related to

... : Applications : OpenCart-EU-central-1

Select the version of policies to enforce.

Version

Latest Policies

5 / 5 policy changes selected for enforcement

Filter Policies ...

Download

Absolute

No matching changes

Default

Added 4

Removed 0

	Priority	Action	Consumer	Provider	Protocols and Ports
>	100	ALLOW	... : aws : eu-central-1 : eu-cen-1-sec-vpc	OpenCart-web-front	TCP : 22 (SSH) ... 1 more
	100	ALLOW	OpenCart-web-front	... : aws : eu-central-1 : eu-cen-1-sec-vpc	TCP : 8080 (HTTP)
	100	ALLOW	OpenCart-web-front	AWS-RDS	TCP : 3306 (MySQL)

Catch All

Change

Catch All Action

from

ALLOW

to

DENY

Cancel

Previous

Next

>

Nov 28 4:10:00pm

REJECTED

Unknown

Catch All

Unknown

Unknown

172.31.35.135

172.31.7.247

25268

22

TCP

SSH

Catch All

Security Group Policies

OpenCart-EU-central-1

Scopes and Inventory / Inventory Profile / Security Group Policies

The cluster is unhealthy. There are platform alerts in the cluster. Please change your Tenant preference to [Default](#) and check the Alerts page.

172.31.7.247
 Type: TAGGED

Total Security Groups
1

Total Concrete Policies
4

Total Labels
20

Enforcement Groups
None

Experimental Groups
OpenCart-web-front ...2 more

LABELS AND SCOPES

INTERFACES

ENFORCEMENT HEALTH

CONCRETE POLICIES

SECURITY GROUP POLICIES

Security Group Policies

Enter attributes...

Displaying 3 out of 3 security group policies

Interface	Security Group ID	Security Group Name	Actions	Direction	Protocol	Source Inventories	Source Port range	Destination Inventories	Destination Port range
eni-09b5b7ef89c8405f1	sg-0bace6ba8c876b219	csw_205fe0bb_1689405313_1	ALLOW	INGRESS	TCP	3.68.66.202/... ...7 more	any	any	80
eni-09b5b7ef89c8405f1	sg-0bace6ba8c876b219	csw_205fe0bb_1689405313_1	ALLOW	INGRESS	TCP	3.68.66.202/... ...7 more	any	any	22
eni-09b5b7ef89c8405f1	sg-0bace6ba8c876b219	csw_205fe0bb_1689405313_1	ALLOW	EGRESS	TCP	any	any	3.68.66.202/... ...7 more	8080



Demo

CISCO *Live!*

Azure



Organisation of apps

Scopes and Inventory

Scopes No Draft Changes ⓘ

Filter Scopes... ✕

24 Scopes and 13 Inventory Filters ⓘ

- ▼ **Demo** Inventory: 5,864
4 / 36 Children Uncategorized: 5,637
- > **dstoeckm-AWS** Inventory: 0
1 / 3 Children
- > **DusLab** Inventory: 227
5 / 26 Children Uncategorized: 7
- Internet** Inventory: 0
0 Children
- ▼ **dstoeckm-azure** Inventory: 0
1 / 3 Children
- ▼ **westeurope** Inventory: 0
1 / 2 Children
- ▼ **PLX-Demo-Vnet** Inventory: 0
1 / 1 Children
- ▼ **OpenCart-Azure** Inventory: 0
0 Children

For Azure

Query

```
* orchestrator_system/orch_type = azure
```

Query

```
* orchestrator_system/region = westeurope
```

Query

```
* orchestrator_system/virtual_network_id = cd303134ceb9e8dd0bfa930a578e048430010e91
```

Query

```
* orchestrator_system/cluster_name = AZURE
```

How to organize applications based on defined labels derived from orchestrator, APIs or manual (CSV).

Policy mapping Azure

Scopes and Inventory

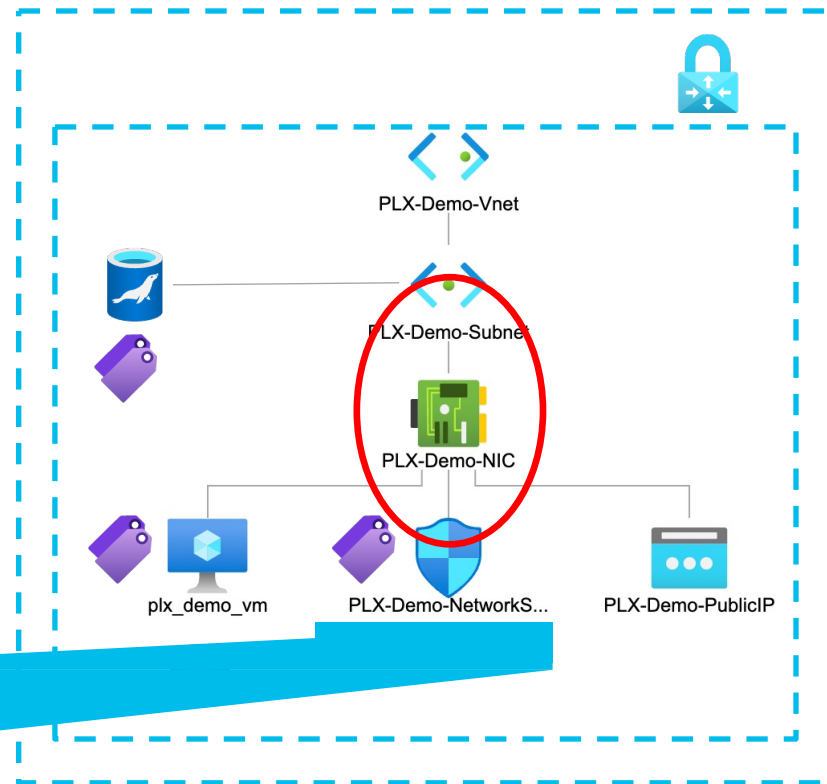
Scopes No Draft Changes ⓘ

Filter Scopes... ✕

24 Scopes and 13 Inventory Filters ⓘ

- ▼ Demo
4 / 36 Children
Inventory: 5,470
Uncategorized: 5,241
- ▼ dstoeckm-azure
1 / 3 Children
Workspaces: 0
Total Workspaces: 1
- ▼ westeurope
1 / 2 Children
Workspaces: 0
Total Workspaces: 1
- ▼ PLX-Demo-Vnet
1 / 1 Children
Workspaces: 0
Total Workspaces: 1
- ▼ OpenCart-Azure
0 Children
Workspace: 1
Total Workspaces: 1

azure-OpenCart Primary



Cisco Secure Workload

Azure Connector

 Cisco Secure Workload

[Demo](#)   

[Back to Connectors](#)

Connector



Azure **BETA** 

Enabled on Nov 16th, 2022

[Enable Another](#)

[Edit Connector](#)

[Delete Connector](#)

Capabilities

[Inventory Enrichment](#)

[Flow Visibility](#) [Segmentation](#)

[Managed K8s](#)

Info Azure

HTTP Proxy: <http://proxy.esl.cisco.com:80> Total Virtual Networks: 1

Full Scan Interval: 3600 seconds Total Kubernetes Clusters: 0

Delta Scan Interval: 60 seconds IAM Policy: 

VNet ID	VNet Name	Region	Gather Labels	Flow Logs Ingest	Segmentation
cd303134ceb9e8dd0bfa930a578e048430010e91	PLX-Demo-Vnet	westeurope	enabled	enabled	enabled

Address 	* Orchestrator_system/Cluster_id 	* Orchestrator_system/Cluster_name 	* Orchestrator_system/Interface_id 	* Orchestrator_system/Machine_id 	* Orchestrator_system/Machine_name 
10.0.1.4	cd303134ceb9e8dd0bfa930a578e048430010e91	AZURE	PLX-Demo-NIC	9a15abb8-bd91-4c30-8f05-3bb04ea15288	plx_demo_vm

Rows per page  40  **1** 

Azure Ingested Labels

 Cisco Secure Workload

Demo





Labels and Scopes

10.0.1.4

 Azure Type: TAGGED

Total Security Groups

0

Total Concrete Policies

2

Total Labels

14

Enforcement Groups

Demo

Experimental Groups

Demo

LABELS AND SCOPES

INTERFACES

ENFORCEMENT HEALTH

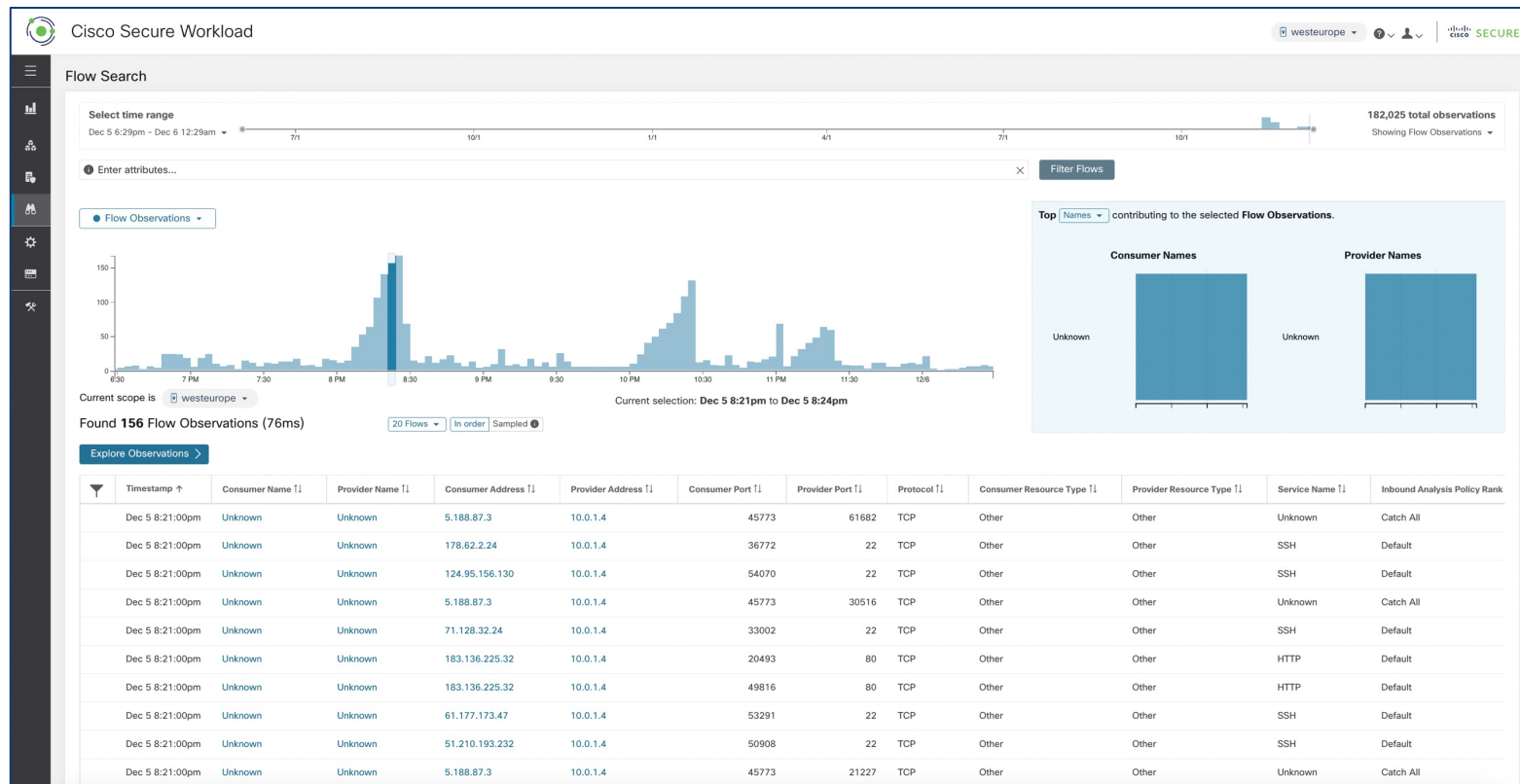
CONCRETE POLICIES

SECURITY GROUP POLICIES

Labels

Label key ↑	Label value ↓
* orchestrator_system/machine_id	9a15abb8-bd91-4c30-8f05-3bb0ea15288
* orchestrator_system/region	westeurope
* orchestrator_Tier	web-tier
* orchestrator_system/workload_type	vm
* orchestrator_system/segmentation_enabled	true
* orchestrator_system/machine_name	plx_demo_vm
* orchestrator_system/virtual_network_id	cd303134ceb9e8dd0bfa930a578e048430010e91
* orchestrator_system/cluster_id	cd303134ceb9e8dd0bfa930a578e048430010e91
* orchestrator_system/orch_type	azure
* orchestrator_system/resource_group	RG-PLX-Demo

Cisco Secure Workload



Cisco Secure Workload

The screenshot displays the Cisco Secure Workload management console. The interface includes a top navigation bar with the product name, user profile, and a 'SECURE' status indicator. Below this is a workspace selector showing 'azure-OpenCart' as the active workspace, with a 'PRIMARY' tag and a 'Version 0' dropdown. A horizontal menu contains various tabs: Matching Inventories, Policies (selected), Filters, Conversations, Provided Services, Policy Analysis, Enforcement Status, and Enforcement. A search bar for 'Filter Policies ...' is present, along with 'Run Quick Analysis' and '+ Policy' buttons.

The main area features a hierarchical diagram of the environment. It starts with a 'Demo' node, which branches into 'dstoeckm-azure', then 'westeurope', then 'PLX-Demo-Vnet', and finally 'OpenCart-Azure'. Inside the 'OpenCart-Azure' box, there are two nodes: 'Azure-VM' and 'Azure-MariaDB'. A blue callout box with the number '2' points to the 'Azure-VM' node. A table is overlaid on the diagram, showing the policy configuration:

Action	Priority	Protocols and Ports
ALLOW	100	TCP: 22, 80

On the right side, a search results pane is open, displaying details for the 'OpenCart-Azure' scope. It lists the 'Full Name' as 'Demo:dstoeckm-azure:westeurope:PLX-Demo-Vnet:OpenCart-Azure', the 'Primary App' as 'azure-OpenCart', and the 'Query' as '*orchestrator_system/cluster_name = AZURE or *app_name = opencart'. There is a 'View Scope Details' link. Below the query, there are expandable sections for 'Services' (0), 'Pods' (0), 'Workloads' (0), and 'IP Addresses' (2).

Azure view on the policy – Inbound rules

Microsoft Azure

Home > All resources > PLX-Demo-NetworkSecurityGroup

All resources
Cisco-CSW-Sales

Filter for any field...

Name ↑

- diag736a3b339641a647
- maria-db-opencart
- NetworkWatcher_westeurope
- PLX-Demo-NetworkSecurityGroup**
- PLX-Demo-NetworkSecurityGroup
- PLX-Demo-NIC
- PLX-Demo-OsDisk
- PLX-Demo-PublicIP
- PLX-Demo-Vnet
- plx_demo_vm

PLX-Demo-NetworkSecurityGroup | Inbound security rules

Network security group

Search

+ Add Hide default rules Refresh Delete Give feedback

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings

- Inbound security rules**
- Outbound security rules

Network interfaces
Subnets
Properties
Locks

Monitoring

- Alerts
- Diagnostic settings
- Logs
- NSG flow logs

Automation

- Tasks (preview)
- Export template

Help

Page 1 of 1

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
☐ 100	CSW Policy 1	53,123	Udp	10.0.1.4/32	Any	✓ Allow
☐ 102	CSW Policy 3	22,80,443	Tcp	10.0.1.4/32	Any	✓ Allow
☐ 105	⚠ CSW Policy 6	22,80	Tcp	Any	Any	✓ Allow
☐ 107	⚠ CSW Policy Inbou...	Any	Any	Any	Any	✗ Deny
☐ 65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
☐ 65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	✓ Allow
☐ 65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

Azure view on the policy – Outbound Rules

Microsoft Azure

Home > All resources > PLX-Demo-NetworkSecurityGroup

All resources
Cisco-CSW-Sales

Filter for any field...

Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
101	CSW Policy 2	53,123	Udp	Any	Any	Allow
103	CSW Policy 4	22,80,443	Tcp	Any	Any	Allow
104	CSW Policy 5	3306	Tcp	Any	13.69.105.208/32	Allow
106	CSW Policy 7	22,80	Tcp	Any	10.0.1.4/32	Allow
108	CSW Policy Outbound ...	Any	Any	Any	Any	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

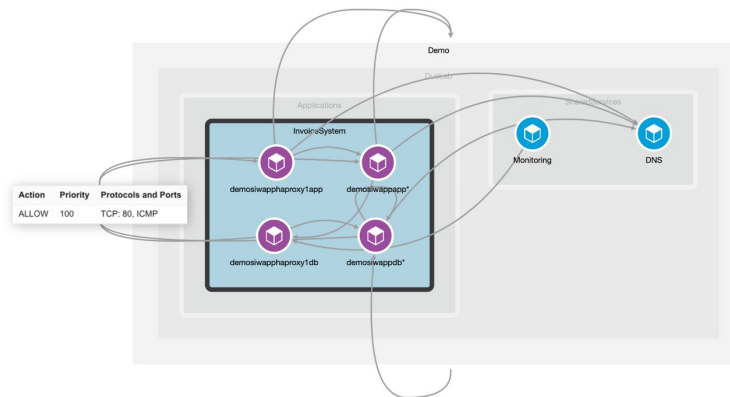
Page 1 of 1

https://an.micronsoft.com/fu/link?linkid=2174617

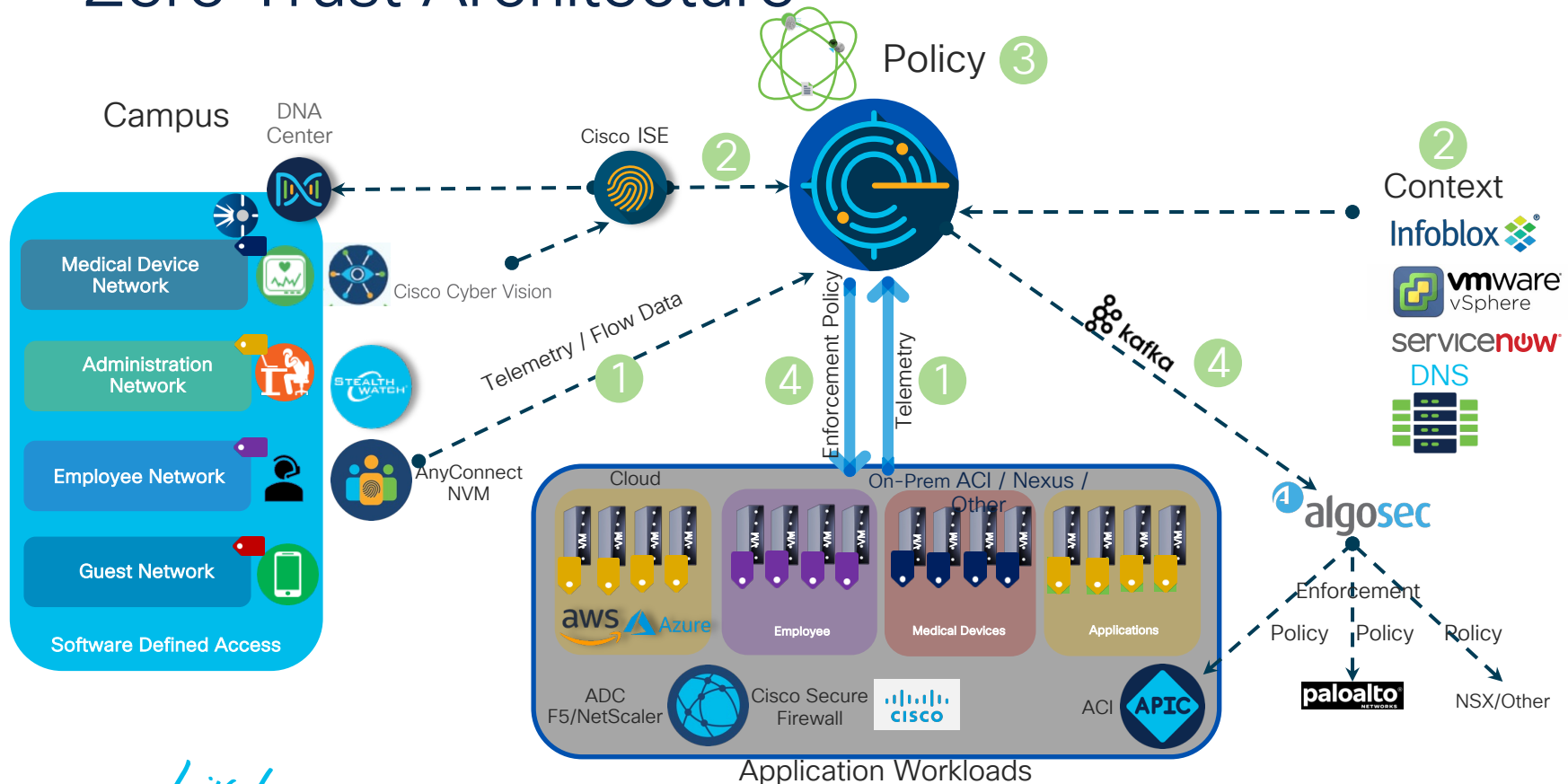
Conclusion

Cloud protection strategy

- Protect your app / deployment from access from the beginning
- Build a policy from outside in
- Work as close as possible to cloud native controls. Use label / tags
- Continuously optimise your policy, established process for policy live cycle
- Include application owner and NetSecOps from the beginning

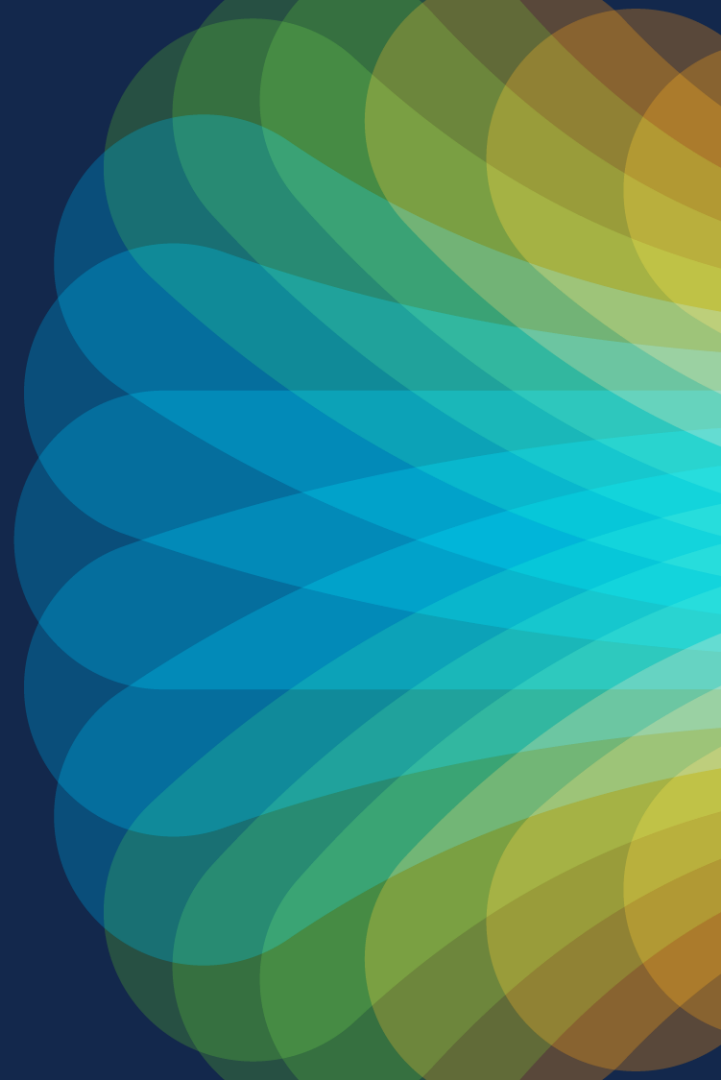


Zero Trust Architecture

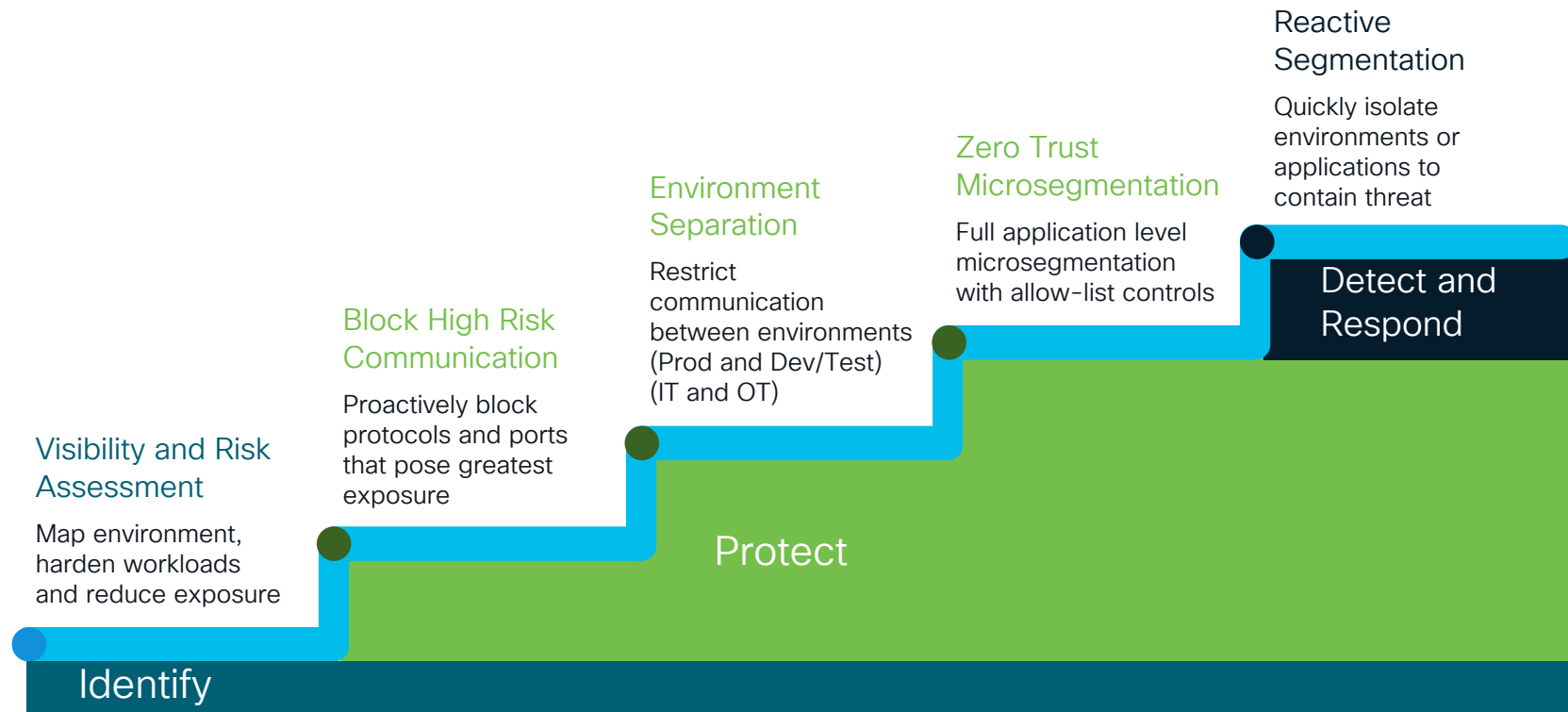


Almost
finished...

Summary



Steps to Zero Trust





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 of the slide is a vibrant, abstract graphic. It features a series of overlapping, wavy bands of color in a rainbow spectrum, transitioning from red and orange on the left to yellow and green on the right. On the right side, there is a bright, multi-colored sunburst or starburst effect that radiates outwards, with colors ranging from blue and purple to yellow and green. The overall composition is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLiveAPJC