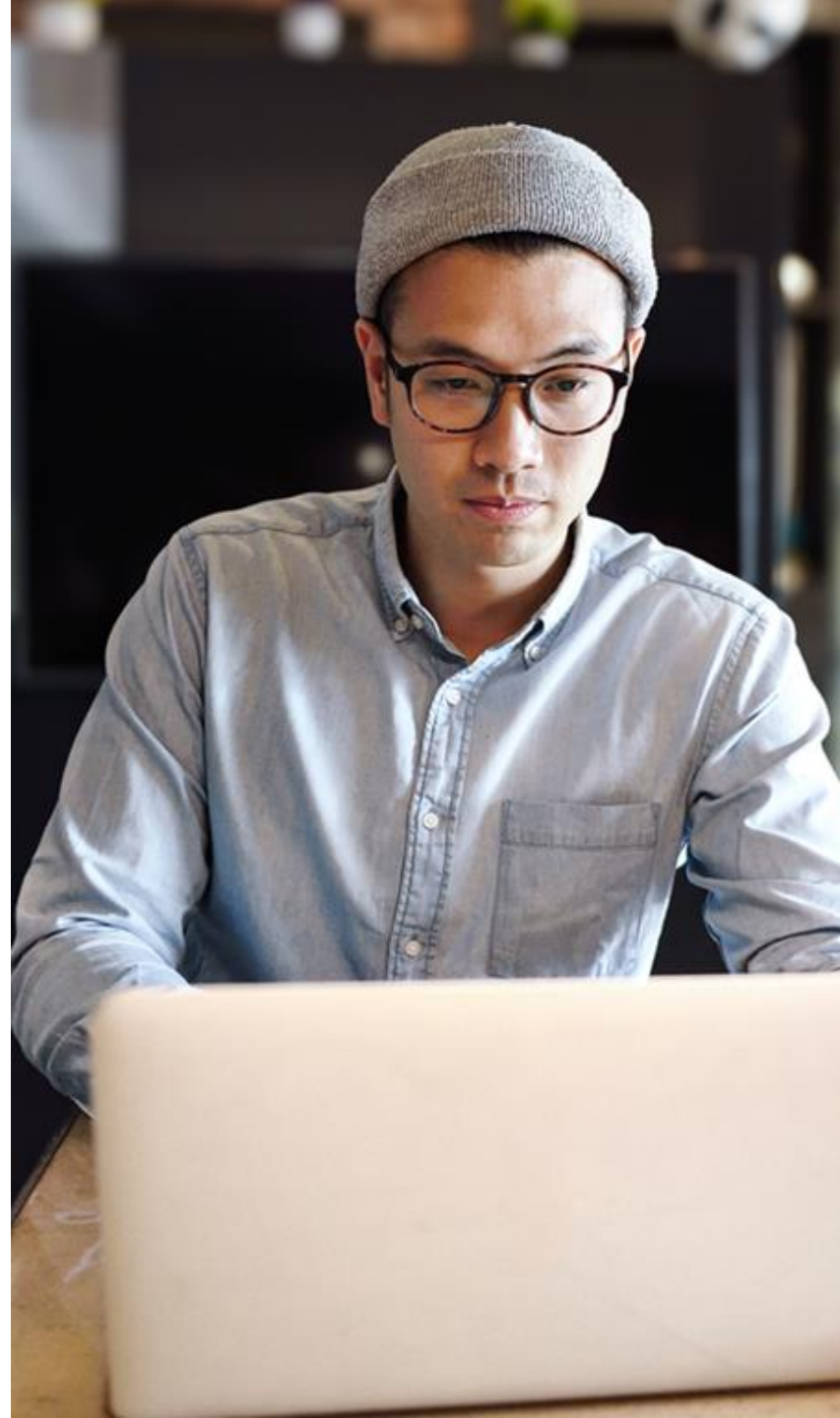
Monitorear, administrar y proteger desde la nube: Cisco Defense Orchestrator y Multicloud Defense

Comunidad de Cisco

Leonel Matus – Technical Consulting Engineer
Omar De Felipe – Technical Consulting Engineer
Sergio Eduardo Lázaro – Technical Consulting Engineer

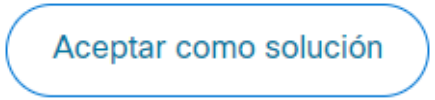
Jueves 1 de agosto de 2024



Conecte, Interactúe, ¡Colabore!

Soluciones

Ayuda a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución” u otórgales un voto de utilidad.



Votos de utilidad

¡Resalta el esfuerzo de otros miembros!

Los votos útiles motivan a otros miembros que colaboran en la comunidad, a seguir ayudándonos a contestar las preguntas abiertas, y ofreciéndoles la oportunidad de ganar premios. ¡Reconoce su esfuerzo!

Premios Spotlight Awards

¡Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros!

Los premios Spotlight Awards se otorgan trimestralmente para reconocer a los miembros más destacados.

Conoce a los ganadores de Febrero-Abril 2024

¡Ahora también puedes nominar a un candidato! Haga clic aquí

Nuestros expertos

Leonel Matus

Technical Consulting Engineer

Cuenta como más de seis años de experiencia prestando soporte en equipos de Seguridad, principalmente en Firewalls. Se unió a cisco en 2021 como Technical Consulting Engineer para el equipo de Firewall/Firepower.

Actualmente es parte del equipo de Cloud Security, en donde se especializa en diferentes tecnologías como Cisco Defense Orchestrator, Multicloud Defense e Email Security.

Leonel cuenta con las certificaciones de CCNP Security y Cisco Firepower Specialist. .

Nuestros expertos

Omar De Felipe

Technical Consulting Engineer

Omar se unió a Cisco en 2022 como Security Technical Consulting Engineer en el equipo de Secure Network Analytics, proporcionando soporte a las tecnologías de Secure Network Analytics Enterprise y Cloud, así como Cisco Telemetry Broker.

Posteriormente migró al nuevo equipo de soporte para Multicloud Defense Gateway, y actualmente soporta Cisco Defense Orchestrator, Secure Email Gateway, Secure Web Appliance, entre otras.

Nuestros expertos

Sergio E. Lázaro

Technical Consulting Engineer

Se se unió a Cisco en 2018 como Technical Consulting Engineer en el equipo de Email Security, dando soporte para clientes a nivel mundial en múltiples tecnologías como Email Security, Web Security y Cisco Defense Orchestrator.

Actualmente cuenta con las certificaciones de CCNP Security y VMware Certified Professional–Data Center Virtualization

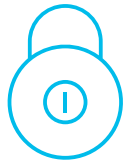
slido

Join at

slido.com

#6095 300

Agenda



1. Cisco Defense Orchestrator (CDO)
2. Multicloud Defense
3. Navegación en la GUI y sus 3 etapas de protección
4. Multicloud Defense en acción (demostración)

Cisco Defense Orchestrator (CDO)

¿Que es CDO?

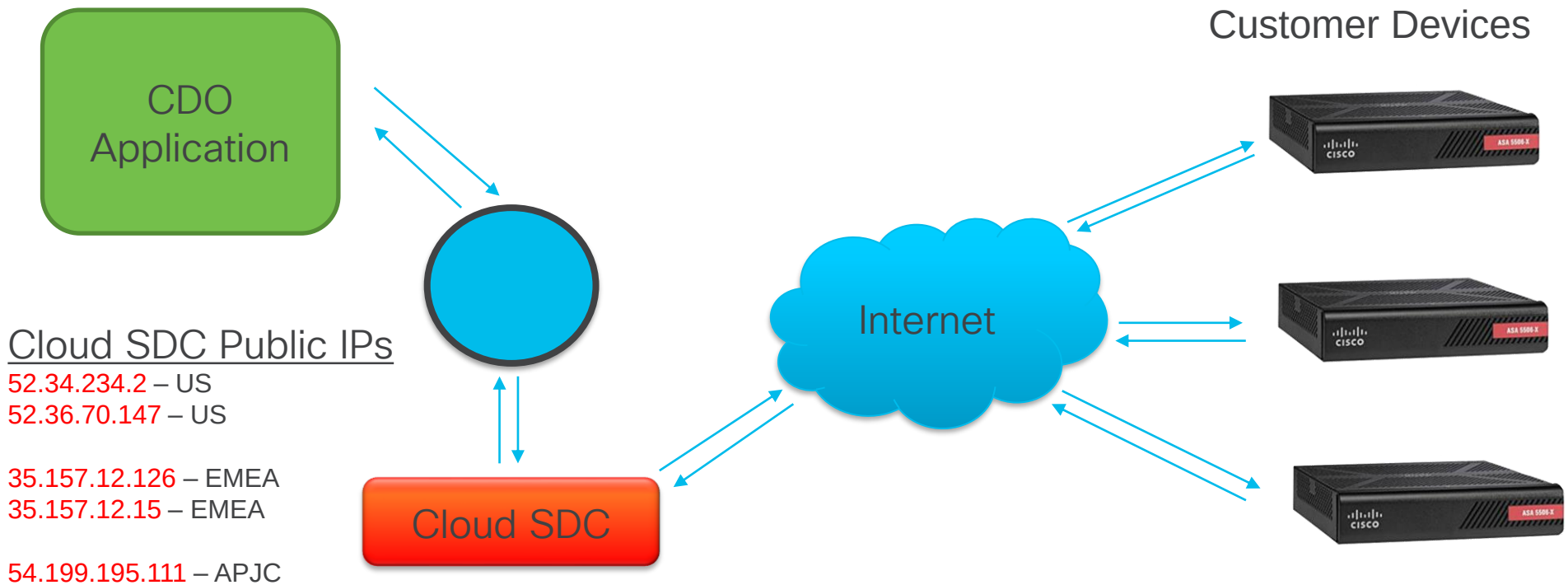
- Plataforma en la nube para gestión centralizada de varios productos de seguridad de Cisco Garantiza políticas consistentes y óptimas.
- Capacidades de automatización
- Soporte para políticas Firepower
- Capacidades de registro de cambios, copias de seguridad programadas y actualizaciones, etc.

¿Qué no es CDO?

No reemplaza a FMC/FDM

CDO sólo sabe cómo manejar ciertos aspectos de la configuración del dispositivo.

Arquitectura de CDO



Arquitectura de CDO

- CDO tiene un diseño donde se pueden ejecutar múltiples inquilinos, lo que significa que puede tener múltiples subdivisiones para el cliente y tener usuarios y superadministradores dentro de cada inquilino.
- Los tenant pueden tener múltiples usuarios
- Cada cliente puede tener varios inquilinos en una organización
- Los datos siempre se mantienen separados entre inquilinos y organizaciones por seguridad

Secure Device Connector (SDC)

-Cloud
-On-prem

Secure Device Connector

- Un SDC puede admitir 500 dispositivos administrados
- Los clientes pueden usar el conector en la nube (predeterminado) o un SDC local
- Cada inquilino de CDO puede tener un número ilimitado de SDC

Active poll

0

Join at

slido.com

#6095 300

¿Qué dispositivos puede administrar desde Cisco Defense Orchestrator? (CDO)

a) ASAs

0%

b) Cisco IOS devices

0%

c) FTDs

0%

d) Todos los anteriores

0%

Acceso CDO

Acceso CDO

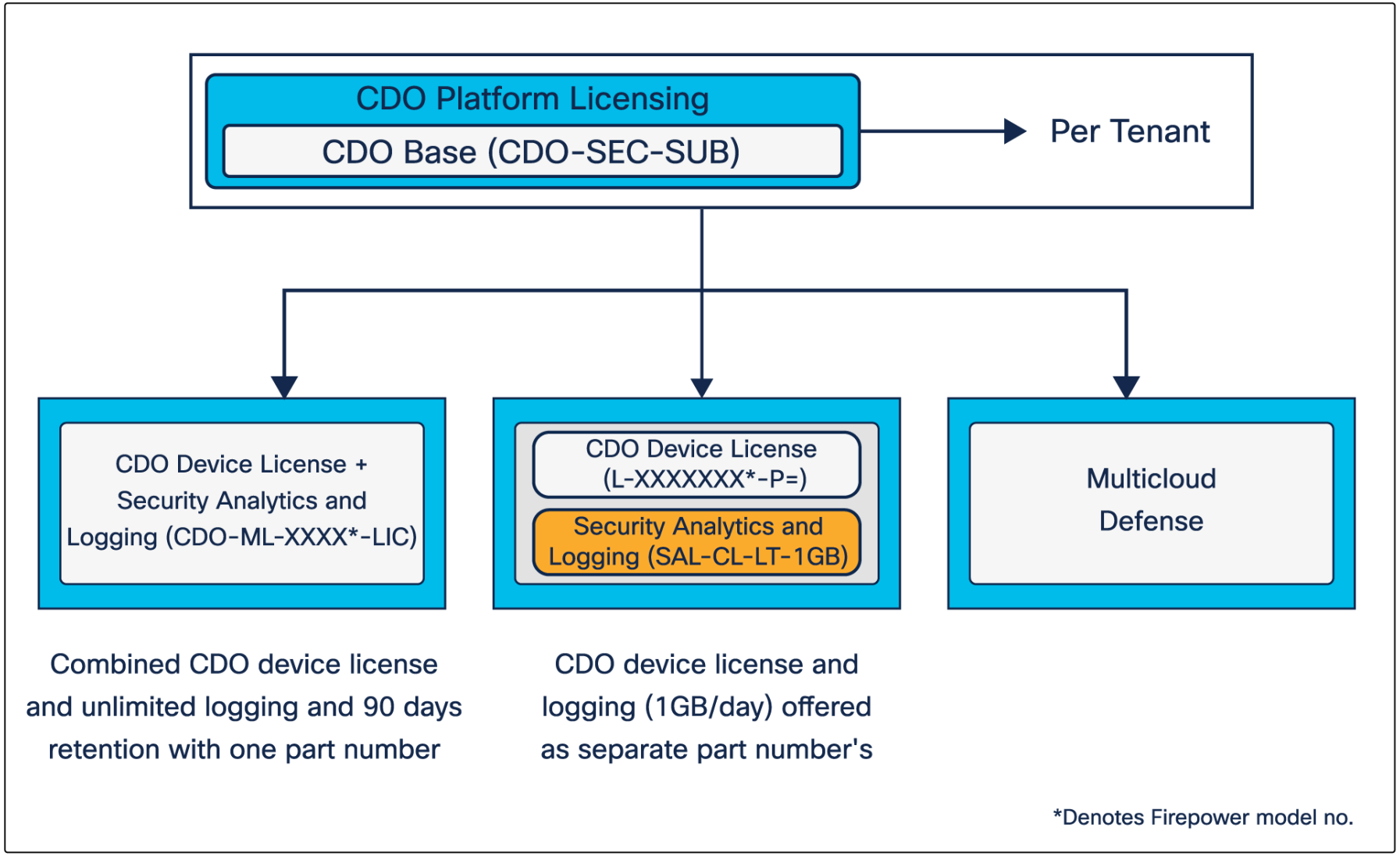
2 Métodos :

- https://sign-on.security.cisco.com/

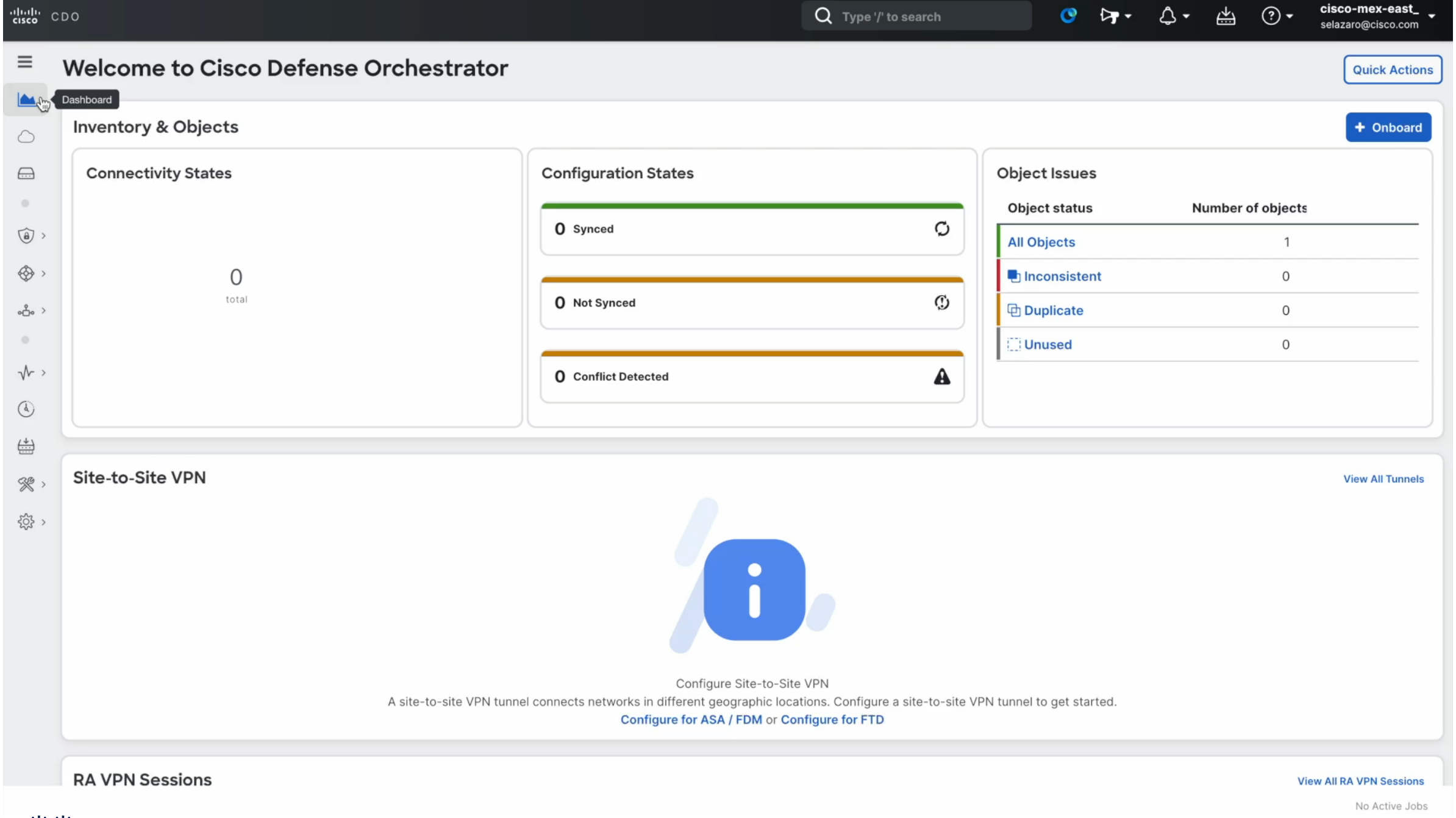
- https://www.defenseorchestor.com
- https://www.defenseorchestrator.eu
- https://www.apj.cdo.cisco.com

CDO
Licenciamiento

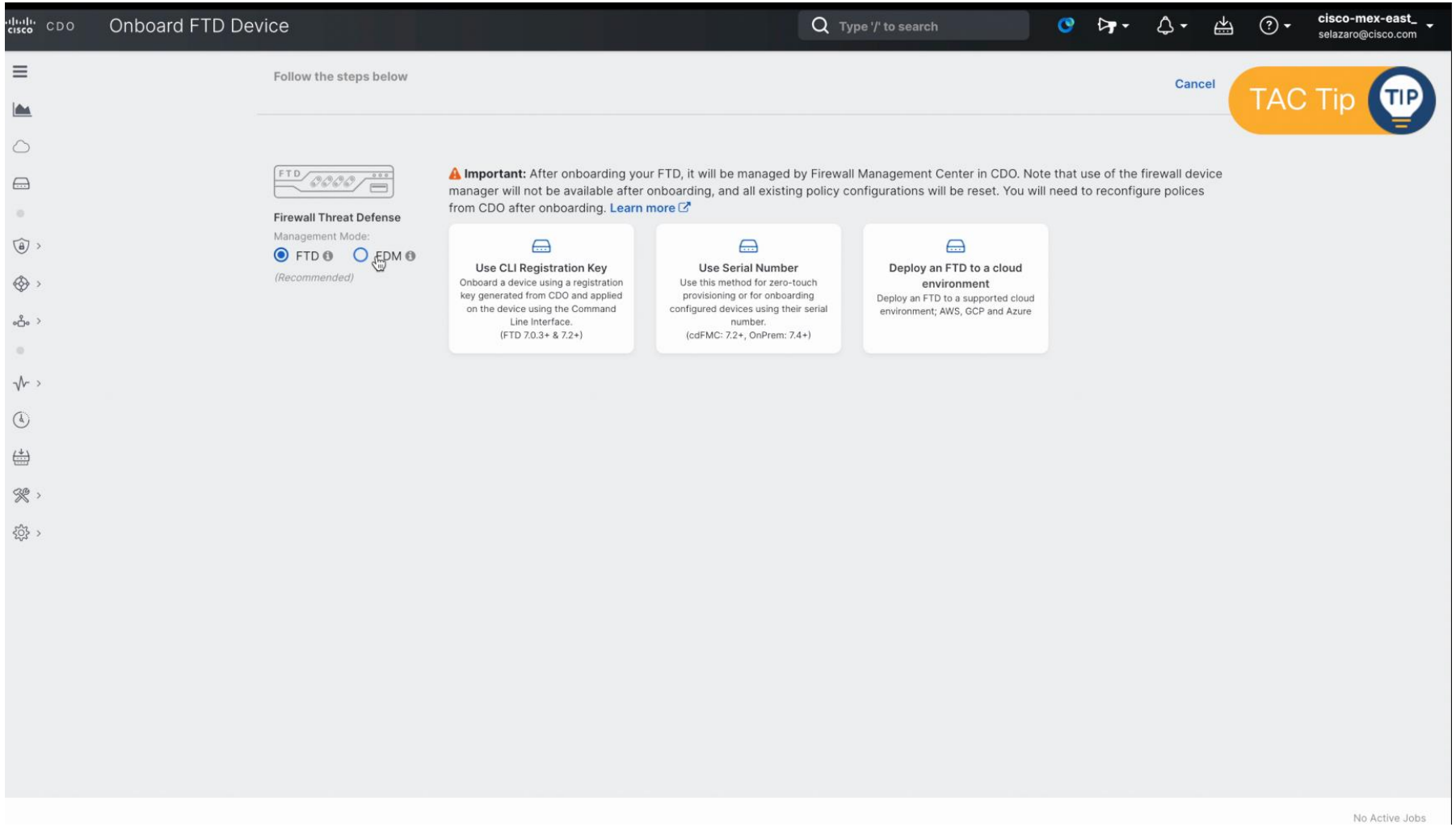
CDO licenciamiento



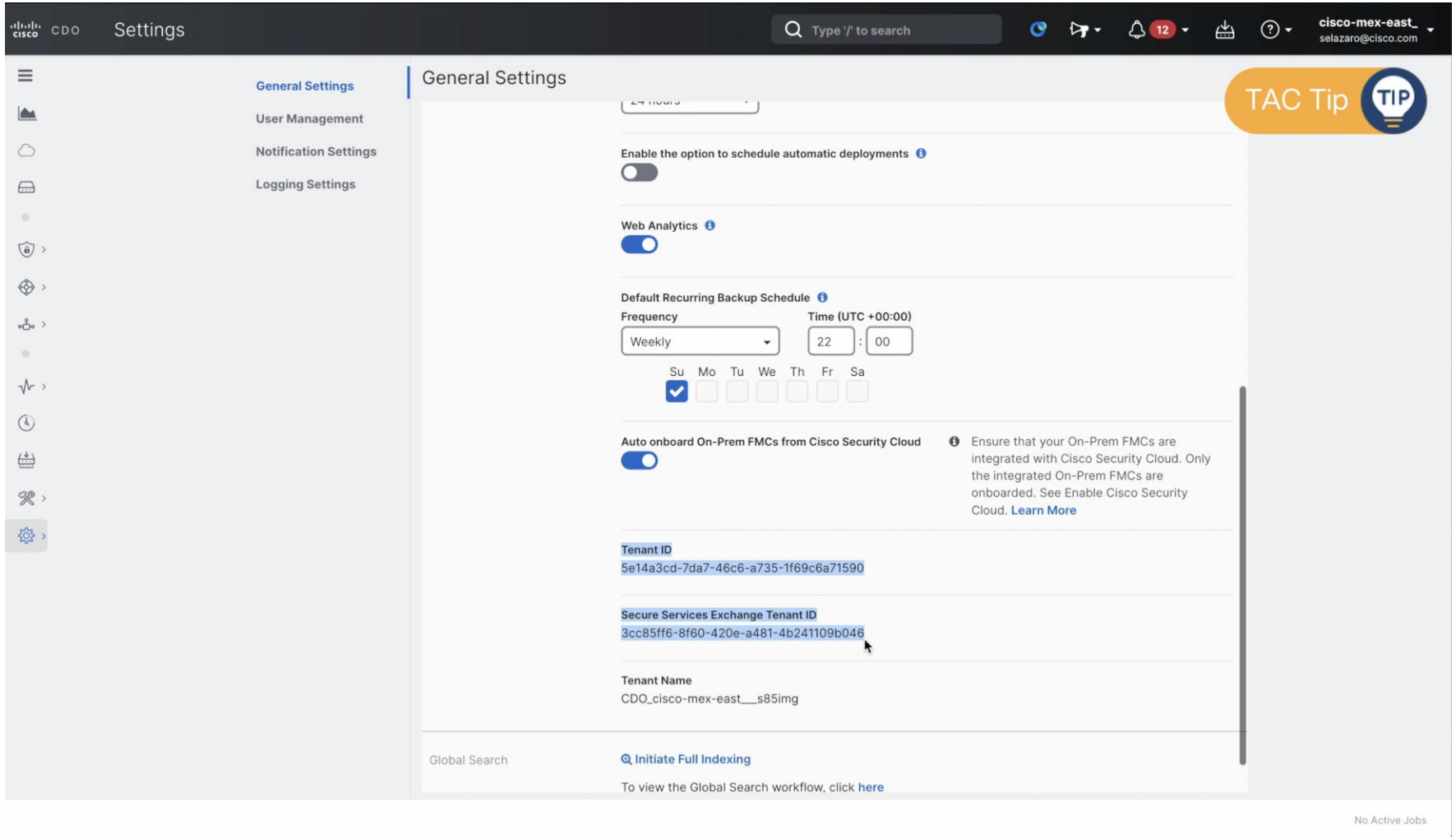
CDO Lab



TAC Tip



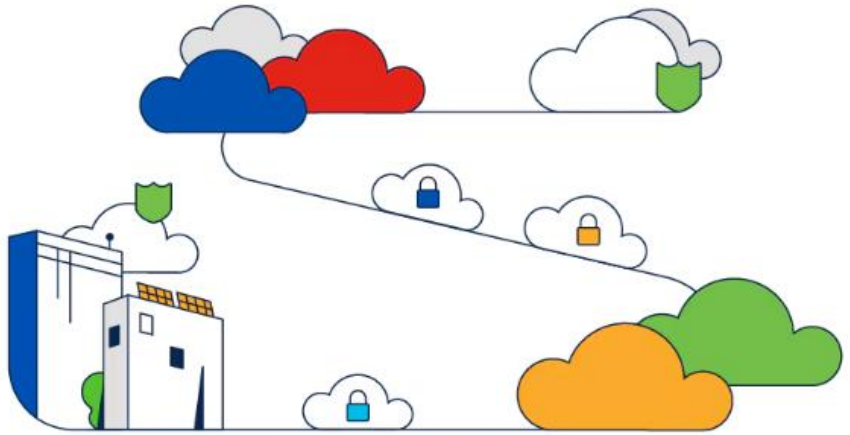
TAC Tip



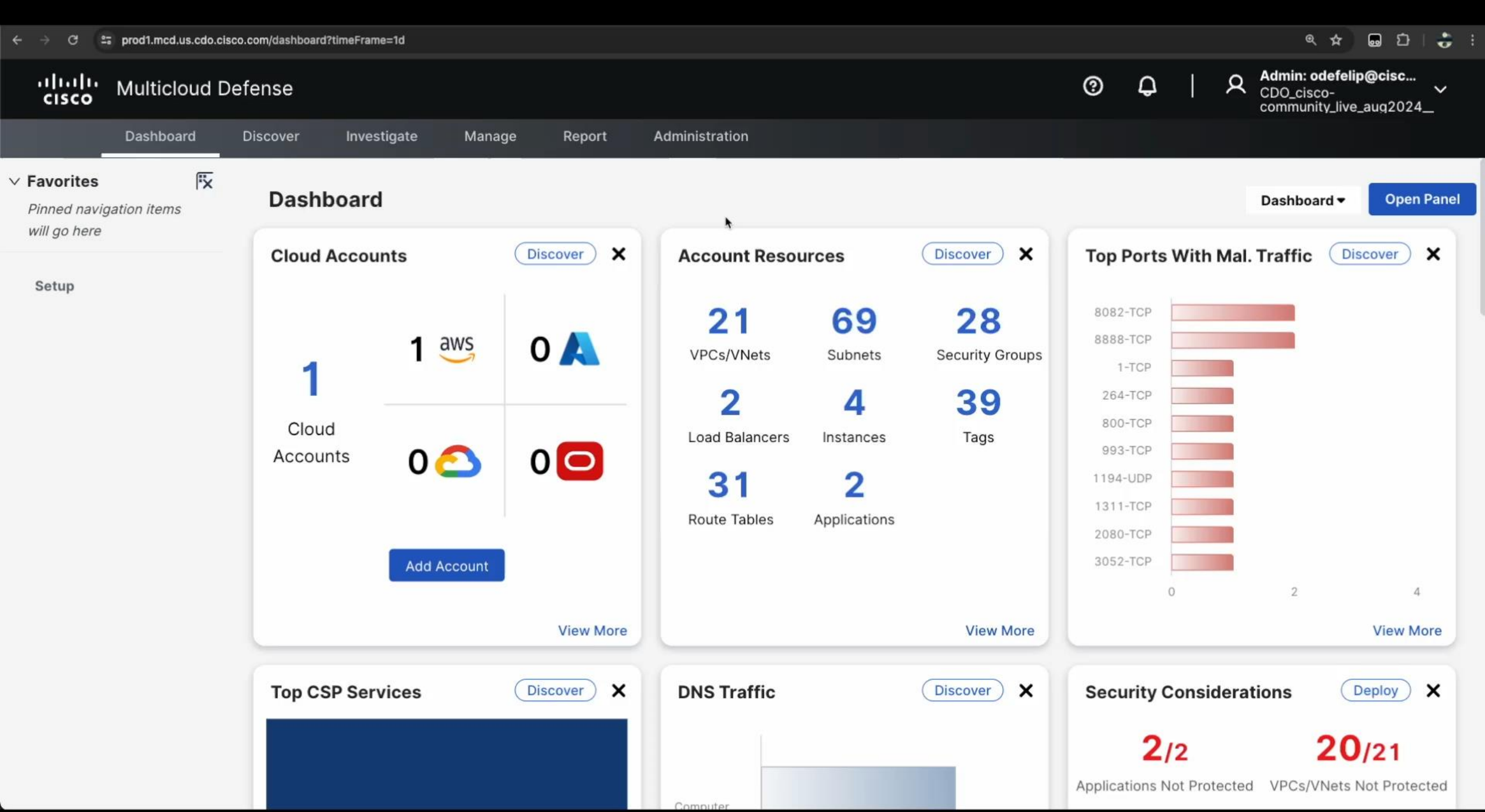
Multicloud Defense

¿Qué es Multicloud Defense?

Multicloud Defense es una solución de SaaS de seguridad de la nube que protege y monitorea tus recursos en diferentes nubes privadas y públicas.



Navegación en la GUI y sus 3 etapas de protección


prod1.mcd.us.cdo.cisco.com/dashboard?timeFrame=1d
Multicloud Defense
Admin: odefelip@cisc...
CDO_cisco-community_live_aug2024_
Dashboard
Discover
Investigate
Manage
Report
Administration
Favorites
Pinned navigation items will go here
Setup
Dashboard
Dashboard
Open Panel
Cloud Accounts
Discover
1
Cloud Accounts
1 aws
0
0
0
Add Account
View More
Account Resources
Discover
21
VPCs/VNets
69
Subnets
28
Security Groups
2
Load Balancers
4
Instances
39
Tags
31
Route Tables
2
Applications
View More
Top Ports With Mal. Traffic
Discover
8082-TCP
8888-TCP
1-TCP
264-TCP
800-TCP
993-TCP
1194-UDP
1311-TCP
2080-TCP
3052-TCP
0
2
4
View More
Top CSP Services
Discover
DNS Traffic
Discover
Computer
Security Considerations
Deploy
2/2
Applications Not Protected
20/21
VPCs/VNets Not Protected

Active poll

0

Join at

slido.com

#6095 300

¿En qué etapa de Multicloud Defense puede visualizar el tráfico de sus recursos?

a) Conexión

0%

b) Monitoreo

0%

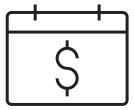
c) Protección

0%

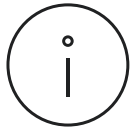
Tres pasos para la protección de tus recursos

- 1er Fase: Conecta tu cuenta de Cloud Service Provider (CSP)
- 2da Fase: Monitorea tus recursos
- 3ra Fase: Protege tus recursos

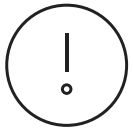
Licencias para Multicloud Defense



La licencia del producto se basa en la cantidad de horas compradas. Más información aquí.



Hasta el momento, existen dos niveles de licencia: “Advantage” y “Premier”.



No hay interrupción del servicio por sobreconsumo.

Diferencias entre advantage y premier

	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		✔

Security Suites

Multicloud Defense Gateway está incluido dentro de la security suite de seguridad en la nube.

Active poll

0

Join at

slido.com

#6095 300

¿Qué significan las siglas CSP?

a) Cisco Solution Provider

0%

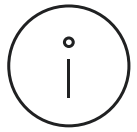
b) Cloud Solution Provider

0%

c) Cloud Service Provider

0%

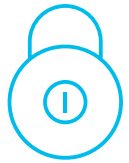
Ambiente de prueba



DCloud tiene disponible una demo de Multicloud Defense aquí.

Multicloud Defense en acción (demostración)

Agenda para la demostración de las tres fases



1. Conexión con una cuenta de AWS
2. Configuración de monitoreo en una S3 bucket
3. Configuración de la VPC de servicio y las gateways

Primera Fase

defenseorchestrator.com

Defense Orchestrator

Type '/' to search

7

community_live_aug2024
odefelip@cisco.com

Hide Menu

Dashboard

Multicloud Defense

Inventory

Configuration

Policies

Objects

VPN

Events & Monitoring

Analytics

Change Log

Jobs

Tools & Services

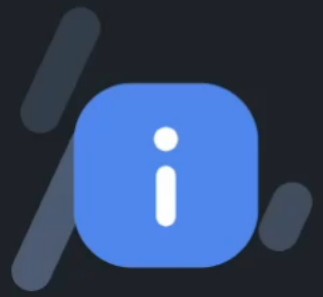
Settings

Welcome to Cisco Defense Orchestrator

Quick Actions

Inventory & Objects

+ Onboard



Onboard a Device or Service

Onboard ASAs, FTDs or other devices or services to begin your CDO Experience

Version 97b980f9f99c4f1e7b5e676f21dbc9c65ea0ea21 | CDO Status

No Active Jobs

Segunda Fase

Favorites

Pinned navigation items will go here

Setup

Security Policies

- Rule Sets
- Addresses
- Services
- Certificates
- FQDNs

Profiles

- Decryption
- IPS/IDS
- Data Loss Prevention
- Anti Malware

Threat Research

Networking

Cloud Accounts

Gateways

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

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

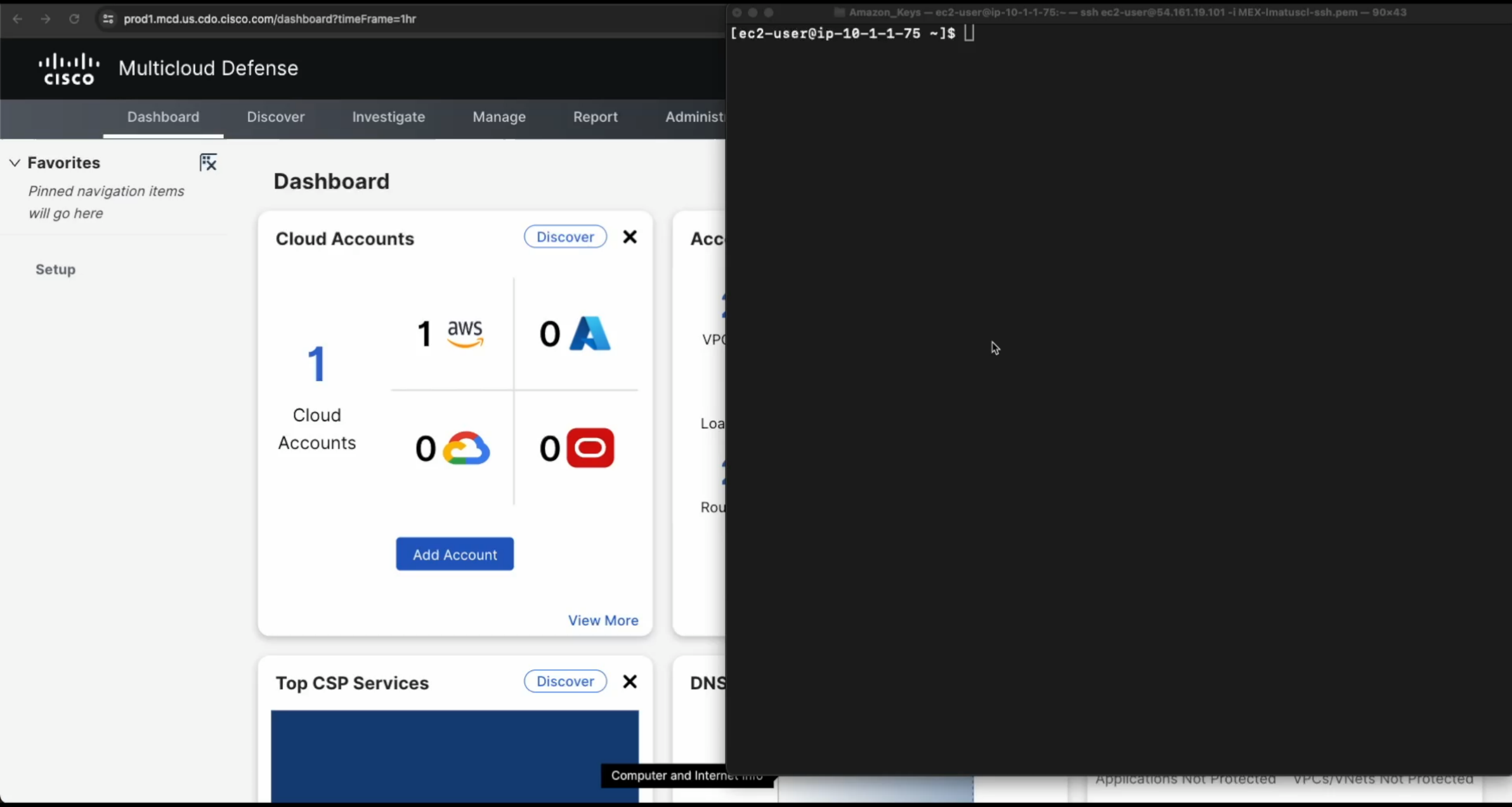
Step 3

Secure Your Account

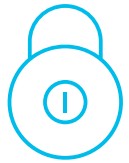
Setup a Service VPC and Multicloud Defense Gateway to secure your Account

Secure Account

Tercera Fase

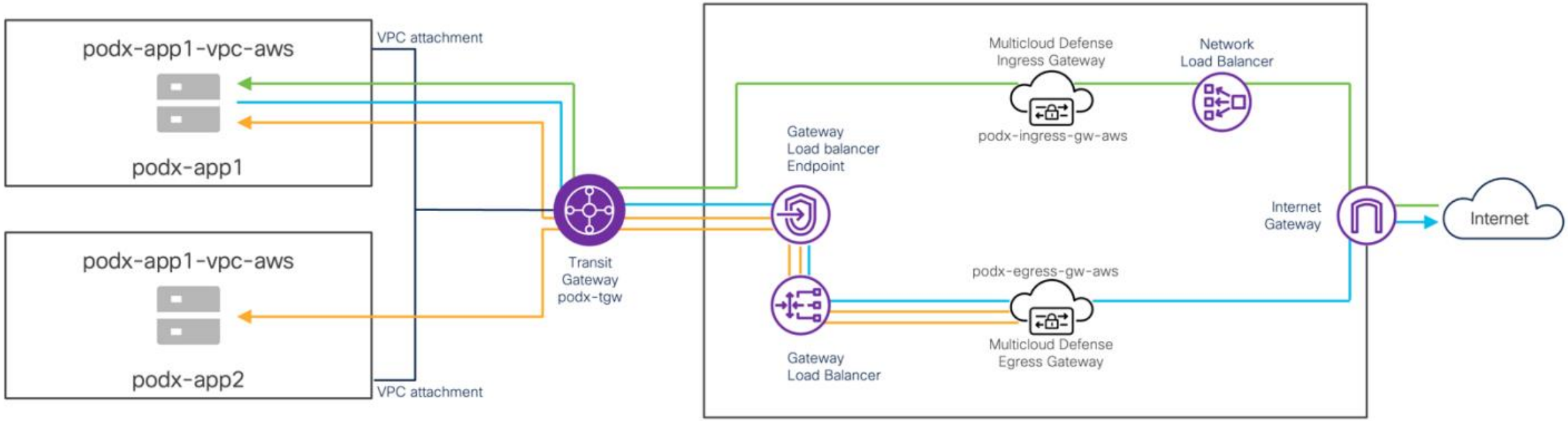

prod1.mcd.us.cdo.cisco.com/dashboard?timeFrame=1hr
Multicloud Defense
Dashboard
Discover
Investigate
Manage
Report
Administ
Favorites
Pinned navigation items will go here
Setup
Dashboard
Cloud Accounts
Discover
1
Cloud Accounts
1
0
0
0
Add Account
View More
Top CSP Services
Discover
Computer and Internet Info
DNS
Applications Not Protected
VPCs/VNets Not Protected
Amazon_Keys — ec2-user@ip-10-1-1-75:~ — ssh ec2-user@54.161.19.101 -i MEX-lmatuscl-ssh.pem — 90×43
[ec2-user@ip-10-1-1-75 ~]$

A continuación:



1. Arquitectura de Multicloud Defense en la nube
2. Diferencia entre tipos de Gateways
3. Tráfico a través de los Gateways
4. Estructura de una ruleset
5. Perfiles de Seguridad
6. Troubleshooting

Arquitectura centralizada en AWS



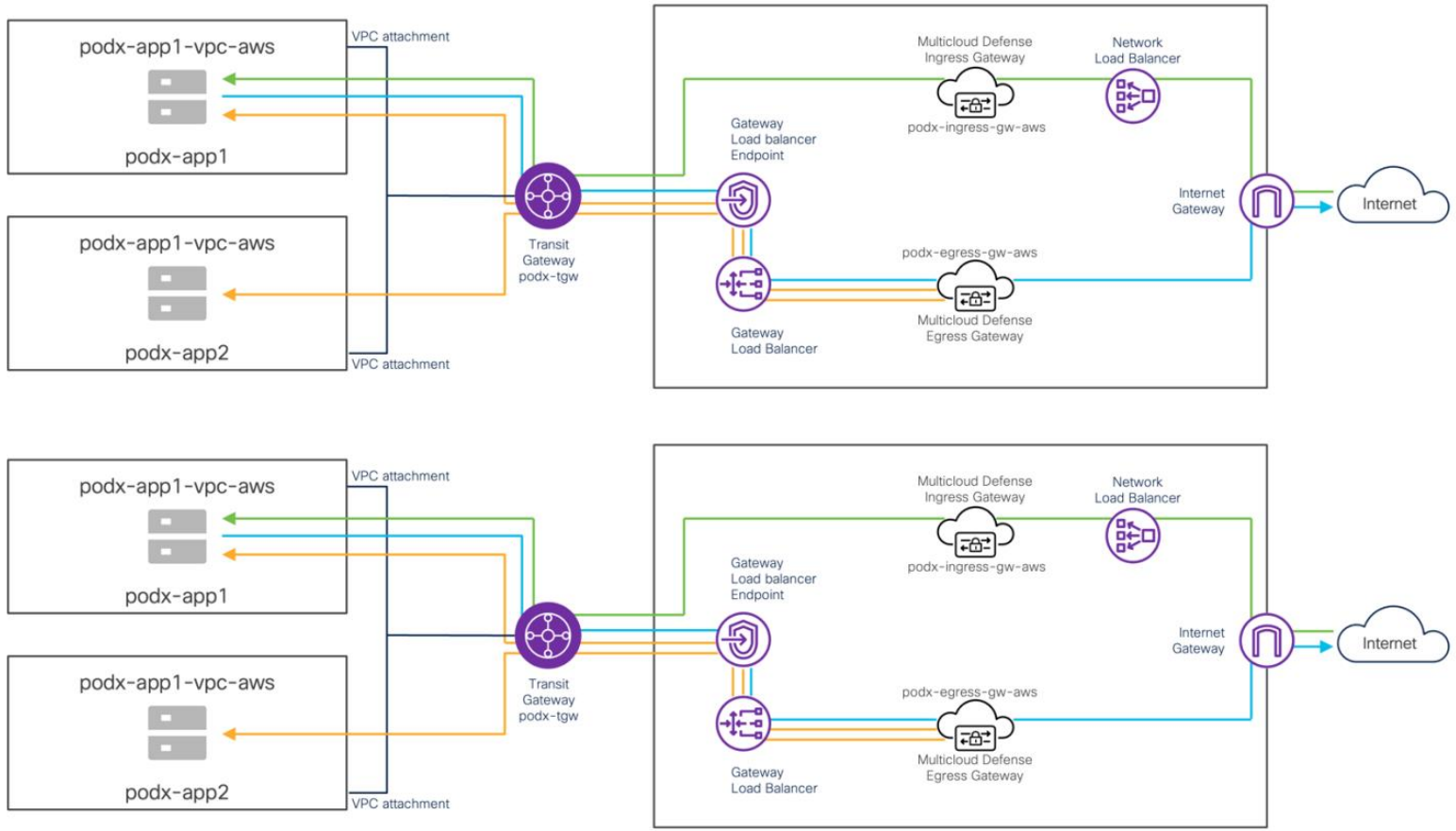
1. Gateways.
2. GWLB y NWLB.
3. Tráfico Entrante
4. Tráfico Saliente
5. Tráfico East West

Multicloud Defense Gateways en alta disponibilidad

TAC Tip

AZ-us-east-1a

AZ-us-east-1b



Active poll

0

Join at

slido.com

#6095 300

¿Cuáles son las regiones soportadas para Multicloud Defense?

a) US

0%

b) EU

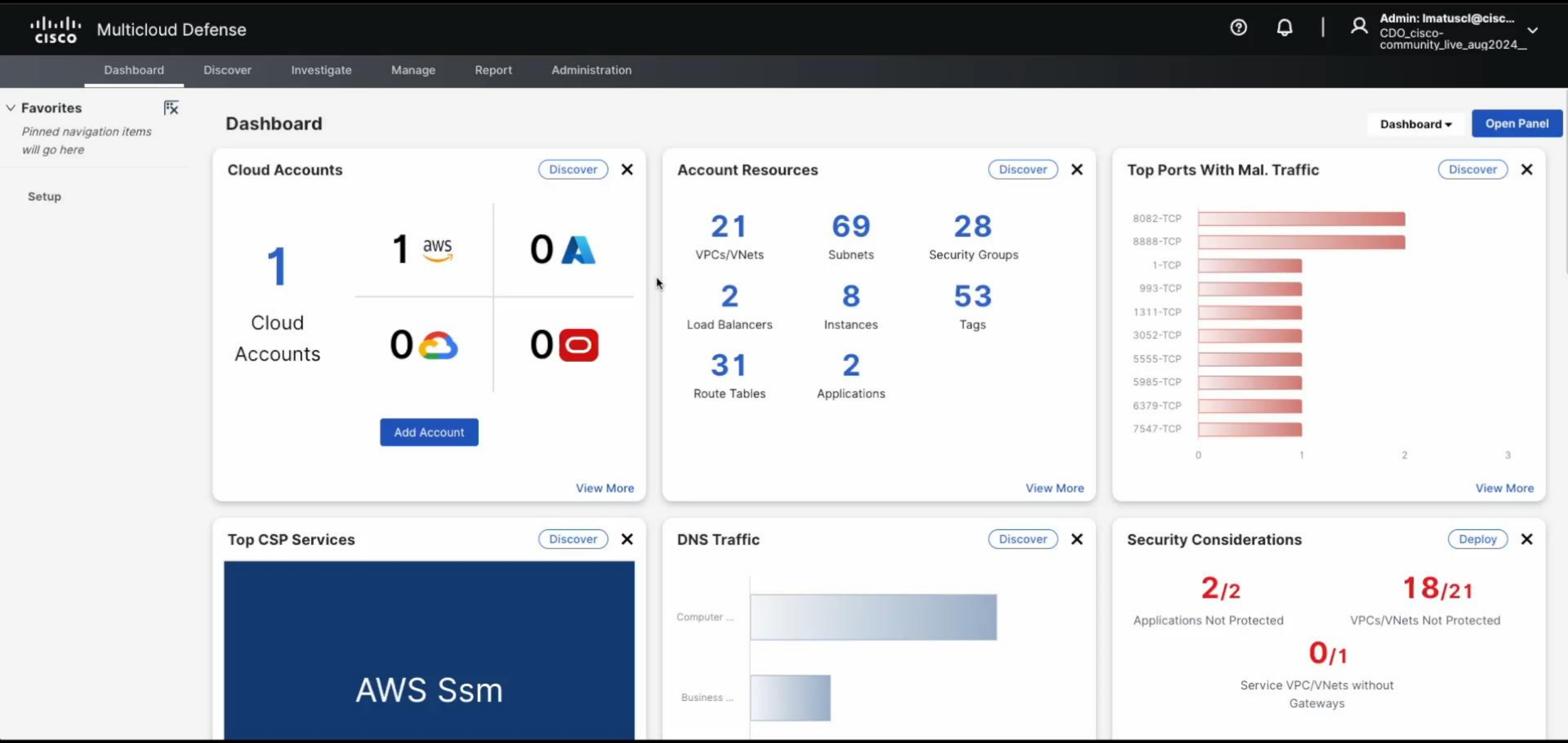
0%

c) APJ

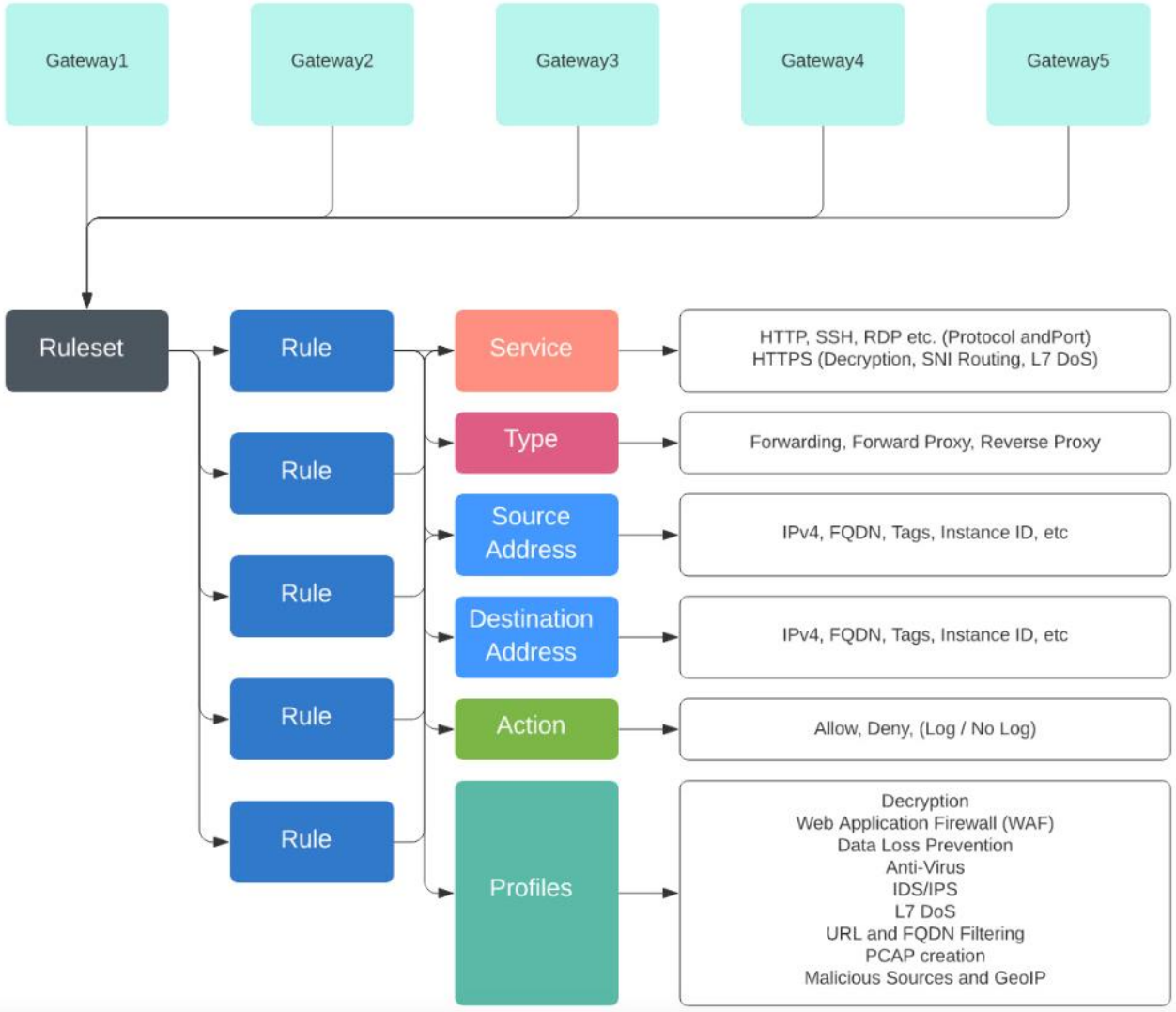
0%

d) Todas las anteriores

0%


Multicloud Defense
Admin: lmatuscl@cisc...
CDO_cisco-community_live_aug2024__
Dashboard
Discover
Investigate
Manage
Report
Administration
Favorites
Pinned navigation items will go here
Setup
Dashboard
Dashboard
Open Panel
Cloud Accounts
Discover
1
Cloud Accounts
1 aws
0
0
0
Add Account
View More
Account Resources
Discover
21
VPCs/VNets
69
Subnets
28
Security Groups
2
Load Balancers
8
Instances
53
Tags
31
Route Tables
2
Applications
View More
Top Ports With Mal. Traffic
Discover
8082-TCP
8888-TCP
1-TCP
993-TCP
1311-TCP
3052-TCP
5555-TCP
5985-TCP
6379-TCP
7547-TCP
0
1
2
3
View More
Top CSP Services
Discover
AWS Ssm
DNS Traffic
Discover
Computer ...
Business ...
Security Considerations
Deploy
2/2
Applications Not Protected
18/21
VPCs/VNets Not Protected
0/1
Service VPC/VNets without Gateways

Estructura de una ruleset



Egress and East/West Gateway(s)
Protege el tráfico saliente y este/oeste proporcionando capacidades de seguridad.

Ingress Gateway(s)
Protege el tráfico entrante proporcionando capacidades de seguridad.

Ingress Gateway

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

Egress Gateway

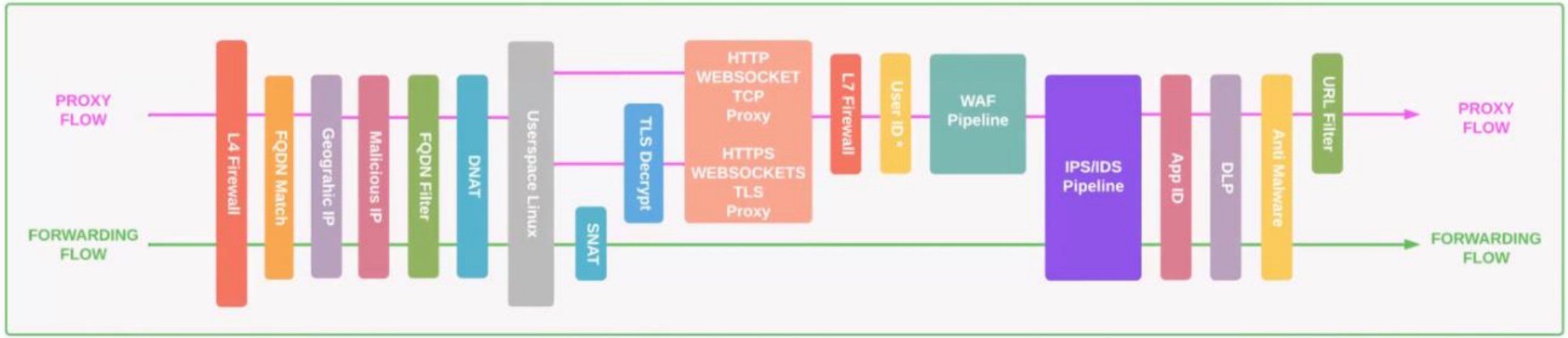
Egress

- URL filtering
- Forward Proxy
- TLS decyrpt
- FQDN filtering*
- FQDN-based firewall policy
- DLP
- IDS / IPS
- Antivirus

East/West

- FQDN filtering
- IDS / IPS
- Antivirus
- L4 firewall
- Micro-segmentation
- FQDN-based firewall policy

Multicloud Defense Gategay Pipeline



Inspection Function	Threat Database Vendor Used
Intrusion Prevention System (IPS)	Cisco Talos
Malware & Ransomware Protection	Cisco Talos
Web Application Firewall (WAF)	Trustwave (800 prepackaged app specific profiles)
DNS Filtering	Brightcloud (used by leading vendors)
FQDN/URL filtering	Brightcloud (used by leading vendors)
GeoIP	Maxmind
Malicious IPs	Trustwave
Cloud AppIDs Legacy AppIDs	Valtix created Cloud Services AppIDs OpenAppID

Favorites

Pinned navigation items will go here

Setup

Dashboard

Dashboard ▾ | Open Panel

Cloud Accounts

Discover

1 Cloud Accounts

1 aws | 0 Azure | 0 GCP | 0 Oracle

Add Account

View More

Account Resources

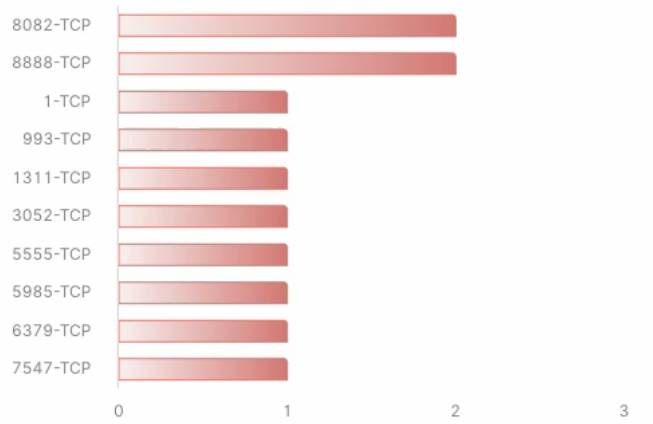
Discover

21 VPCs/VNets	69 Subnets	28 Security Groups
2 Load Balancers	8 Instances	53 Tags
31 Route Tables	2 Applications	

View More

Top Ports With Mal. Traffic

Discover



View More

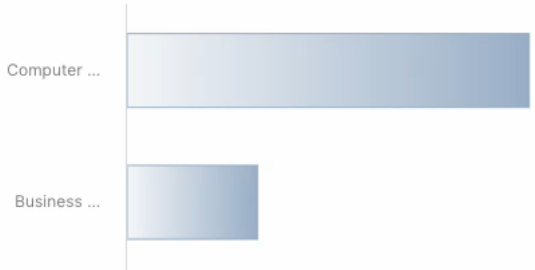
Top CSP Services

Discover

AWS Ssm

DNS Traffic

Discover



Security Considerations

Deploy

2/2 Applications Not Protected

18/21 VPCs/VNets Not Protected

0/1 Service VPC/VNets without Gateways

Active poll

0

Join at

slido.com

#6095 300

¿Desde dónde se puede acceder al Multicloud Defense Controller?

a) Desde el sitio web multicloud.cisco.com

0%

b) A través del portal de Malware Analytics

0%

c) A través del portal de Defense Orchestrator

0%

Multicloud Defense

Admin: lmatuscl@cisc...
CDO_cisco-community_live_aug2024__

Dashboard | Discover | Investigate | Manage | Report | Administration

Favorites

Pinned navigation items will go here

Setup

Dashboard

Dashboard | Open Panel

Cloud Accounts

Discover

1 Cloud Accounts

1 aws | 0 Azure | 0 GCP | 0

Add Account

View More

Account Resources

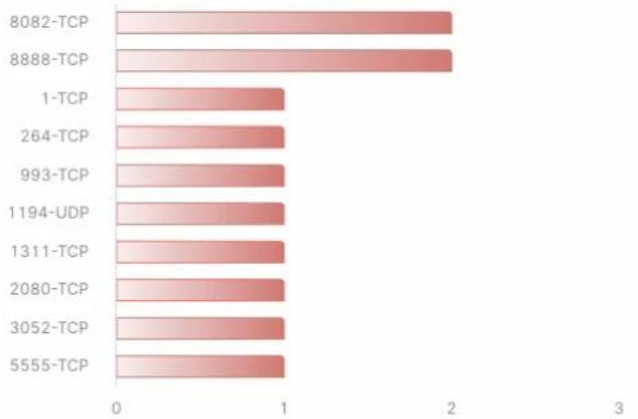
Discover

21 VPCs/VNets	69 Subnets	28 Security Groups
2 Load Balancers	8 Instances	53 Tags
31 Route Tables	2 Applications	

View More

Top Ports With Mal. Traffic

Discover



View More

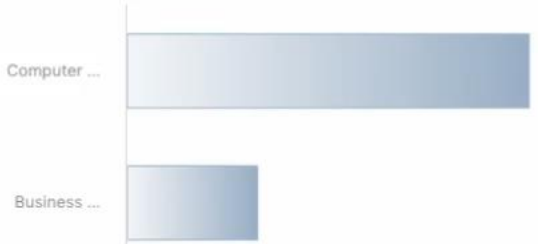
Top CSP Services

Discover

AWS Ssm

DNS Traffic

Discover



Security Considerations

Deploy

2/2 Applications Not Protected

18/21 VPCs/VNets Not Protected

0/1 Service VPC/VNets without Gateways

Q&A

¿Aún tiene dudas?

Si hizo una pregunta en el panel de preguntas y respuestas o regresa a la comunidad en los días posteriores a nuestro webinar ¡Nuestros expertos aún pueden ayudarlo!

Participe en el foro Ask Me Anything (AMA) antes del viernes 9 de agosto de 2024

Haga valer su opinión

Responda a nuestra encuesta para...

- Sugerir nuevos temas
- Calificar a nuestros expertos y el contenido
- Enviar sus comentarios o sugerencias

¡Ayúdenos respondiendo a 5 preguntas de opción múltiple!

Al término de esta sesión, se abrirá una encuesta en su navegador.

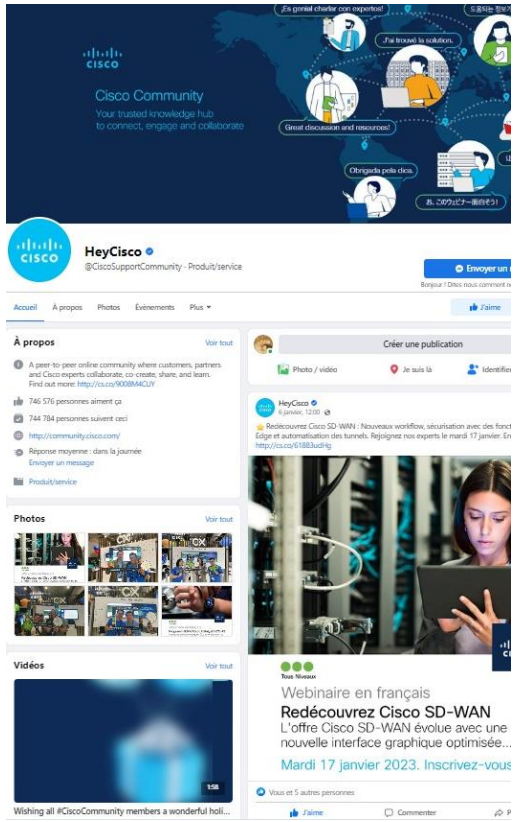
Nuestras Redes Sociales

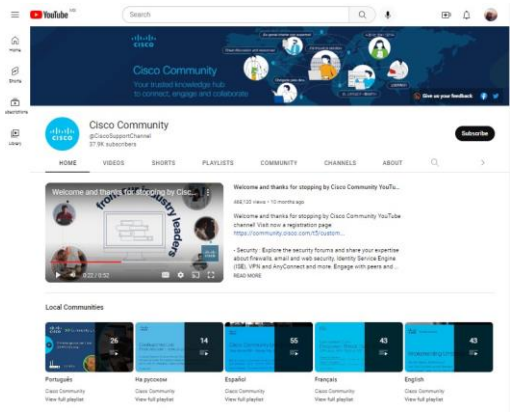
LinkedIn
[Cisco Community]

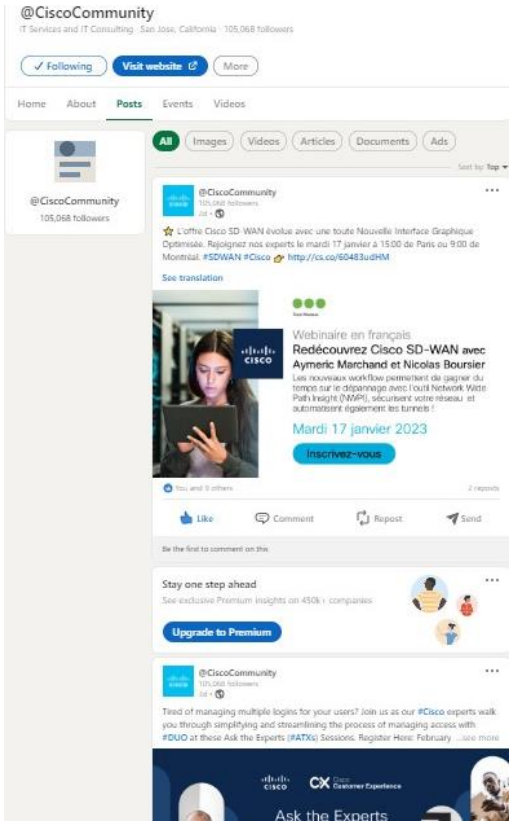
Twitter
[@CiscoCommunity]

YouTube
[CiscoCommunity]

Facebook
[CiscoCommunity]







The bridge to possible