cisco Live !

Cisco’s SASE Approach-Unifying Networking, Identity, and Security

Fay-Ann Lee
Sr. Technical Engineer Marketing

BRKSEC-2286

Cisco Webex App

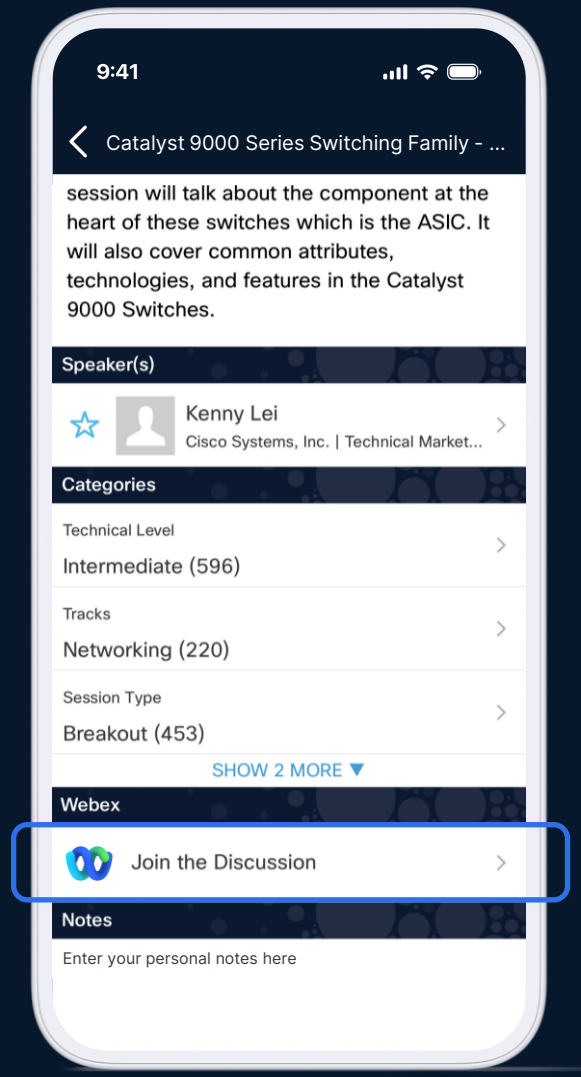
Questions?

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 June 13, 2026.



https://ciscolive.ciscoevents.com/clamer26/
BRKSEC-2286

About Me

- SASE/SSE Sr. Technical Leader
- Wife + Mom
- Being outdoors

Agenda

01 Overview

02 Connectivity & Context

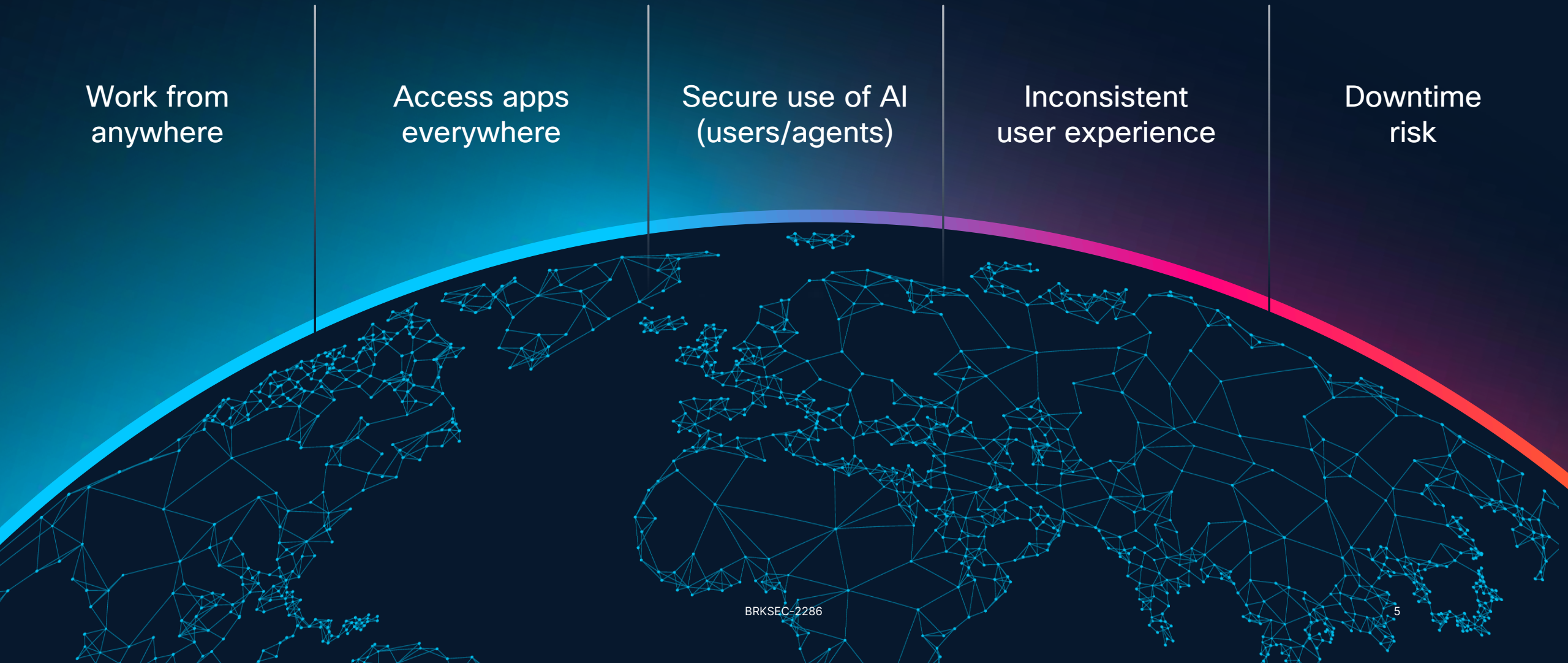
03 Use Cases & Demos

04 Wrap-Up

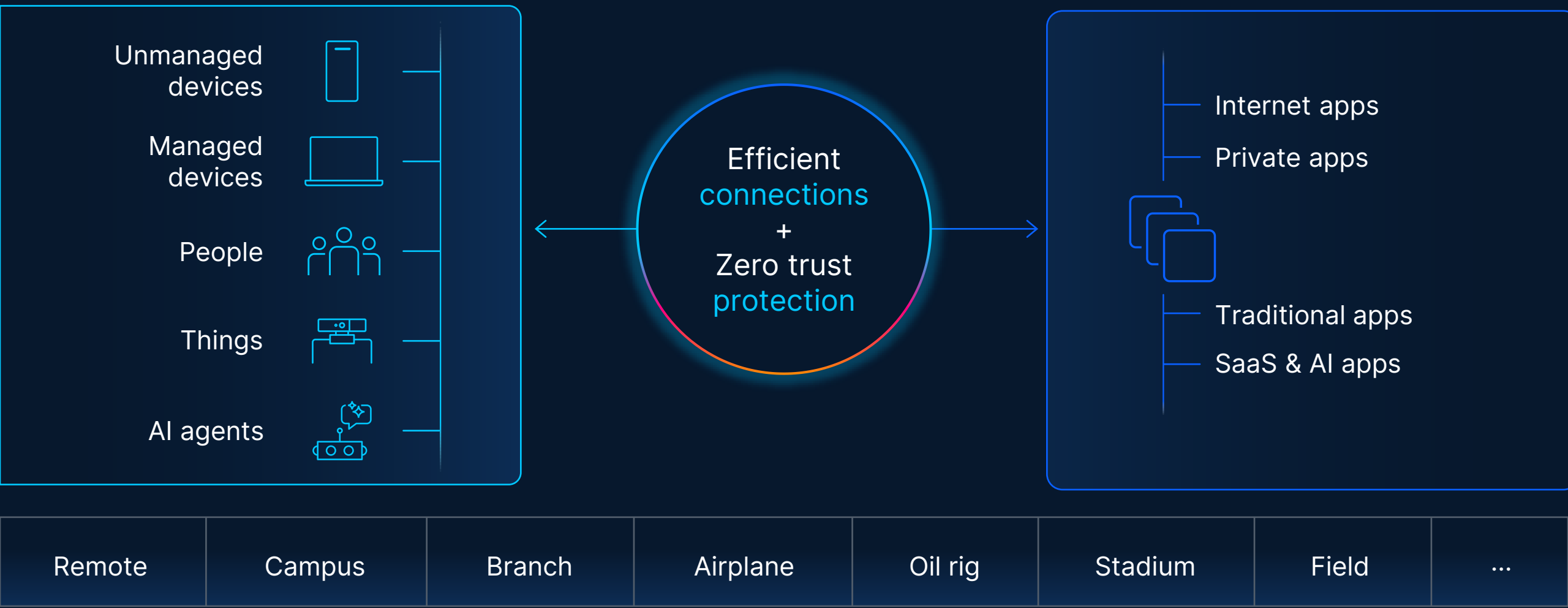
Hidden slides: For your review

Securing the distributed edge

While protecting AI use



The distributed edge and AI complicates zero trust



Cisco SASE

Converged cloud-native secured connectivity grounded in zero trust

Cisco SASE

Secure SD-WAN
Commercial and Enterprise

+

Secure Services Edge
Cisco Secure Access

+

Identity First
ISE + Identity Intelligence

Outcomes and Our Journey

Experienced through Common Platform
One platform to manage SASE operations

Shared Platform Services
Operational efficiency through unified RBAC, APIs, Logging

AI based Unified Policy Engine
Natural language policy management for simpler security outcomes

Common objects/SGTs
Define once, use objects everywhere across SASE experiences

Identity Intelligence
Create one converged view of identity across an organization

End-to-End Observability and Troubleshooting
Unified observability, assurance and troubleshooting experience powered by AI Canvas, ThousandEyes

Cisco SASE

Secure SD-WAN
Commercial and Enterprise

+

Secure Services Edge
Cisco Secure Access

+

Identity First
ISE + Identity Intelligence

Outcomes and Our Journey

Experienced through Common Platform
One platform to manage SASE operations

Shared Platform Services
Operational efficiency through unified RBAC, APIs, Logging

AI based Unified Policy Engine
Natural language policy management for simpler security outcomes

Common objects/SGTs
Define once, use objects everywhere across SASE experiences

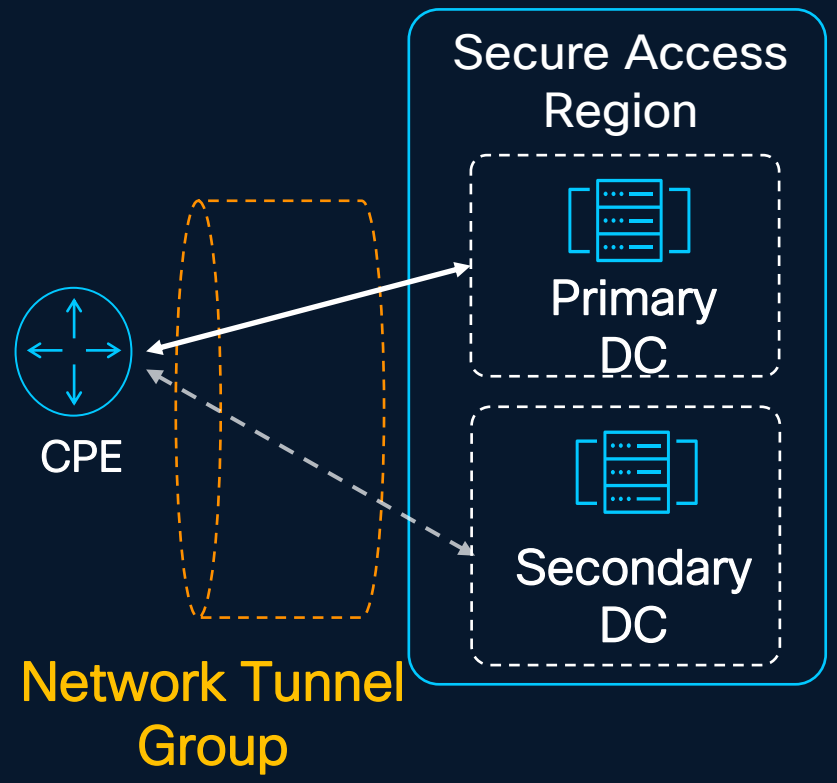
Identity Intelligence
Create one converged view of identity across an organization

End-to-End Observability and Troubleshooting
Unified observability, assurance and troubleshooting experience powered by AI Canvas, ThousandEyes

Connectivity & Context

What is a Network Tunnel Group?

Region based tunnel redundancy



- Any IPSec capable device
- Network Tunnel Groups (NTGs)
  - A pair of IPSec tunnels: primary and secondary for redundancy
  - Connected to different pre-defined DC locations
  - Within the same region
  - Provides intra-region failover
- Failover
  - IKE Dead Peer Detection
  - BGP keepalive/hold-down timers
- 1G per tunnel capacity
  - Use multiple tunnels to increase bandwidth
  - ECMP supported

Multiple Tunnels with ECMP

Solution:

CPE varies the local tunnel id for each tunnel to maintain uniqueness using “+”delimiter and Tunnel Tag

Secure Access IKE control node will strip out the “+” delimiter and Tunnel Tag to maintain authentication and connectivity to a single NTG

Example:

System generated NTG Hub Tunnel IKEv2 ID:
tunnel-id@<orgid>-628670429-sse.cisco.com

Unique Local IKEv2 ID configured on CPE:
tunnel-id+<tunnel tag1>@<orgid>-628670429-sse.cisco.com
tunnel-id+<tunnel tag2>@<orgid>-628670429-sse.cisco.com
...
tunnel-id+<tunnel tag10>@<orgid>-628670429-sse.cisco.com

Secure Access IPsec headend strips off “+<tunnel tag>”
tunnel-id~~+<tunnel tag1>~~@<orgid>-628670429-sse.cisco.com

The Evolution of Network Access Security

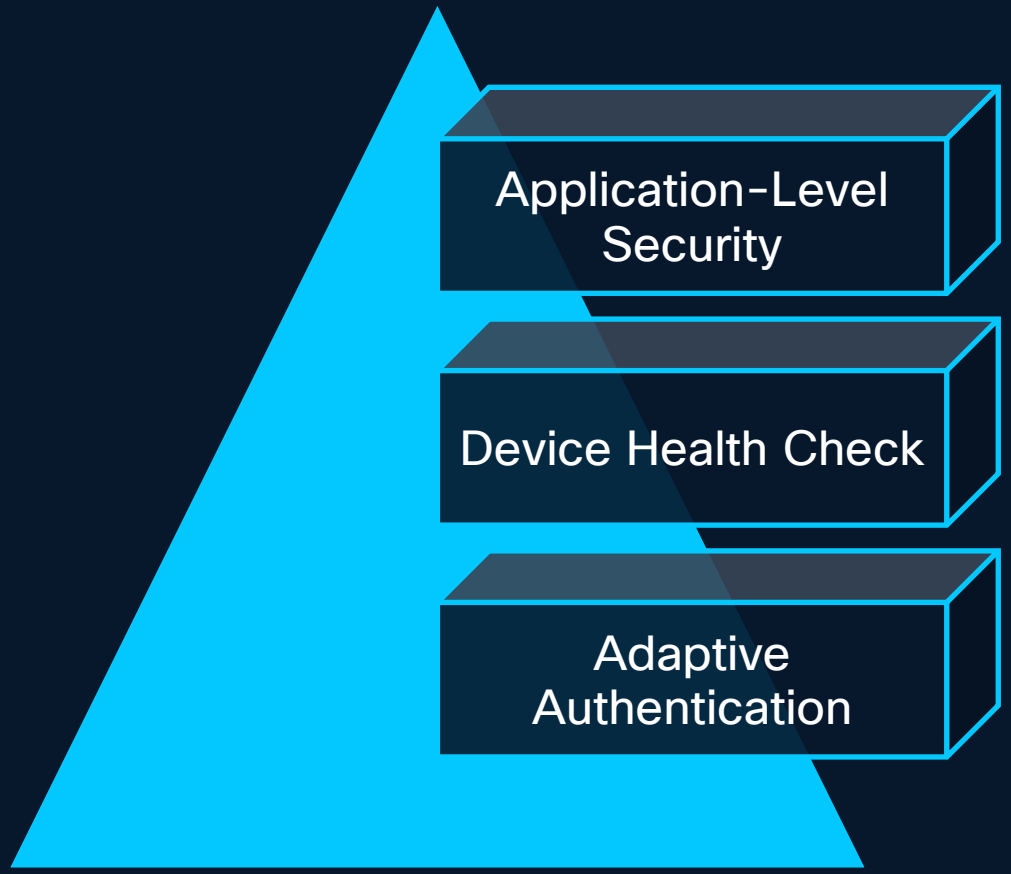
Poor Context Awareness

Relies solely on network-level identifiers like an IP address (e.g., 192.168.2.101), which provides no visibility into who is accessing the network or the state of their device.

Rich Context Awareness

Leverages comprehensive data points--including user identity, device posture, location, and time--to make intelligent, dynamic decisions, ensuring that access is granted only when the context is verified and secure.

Cisco Duo: Trusted Access



Adaptive Authentication

Duo evaluates login context. Unusual locations/new devices trigger MFA or block attempts.

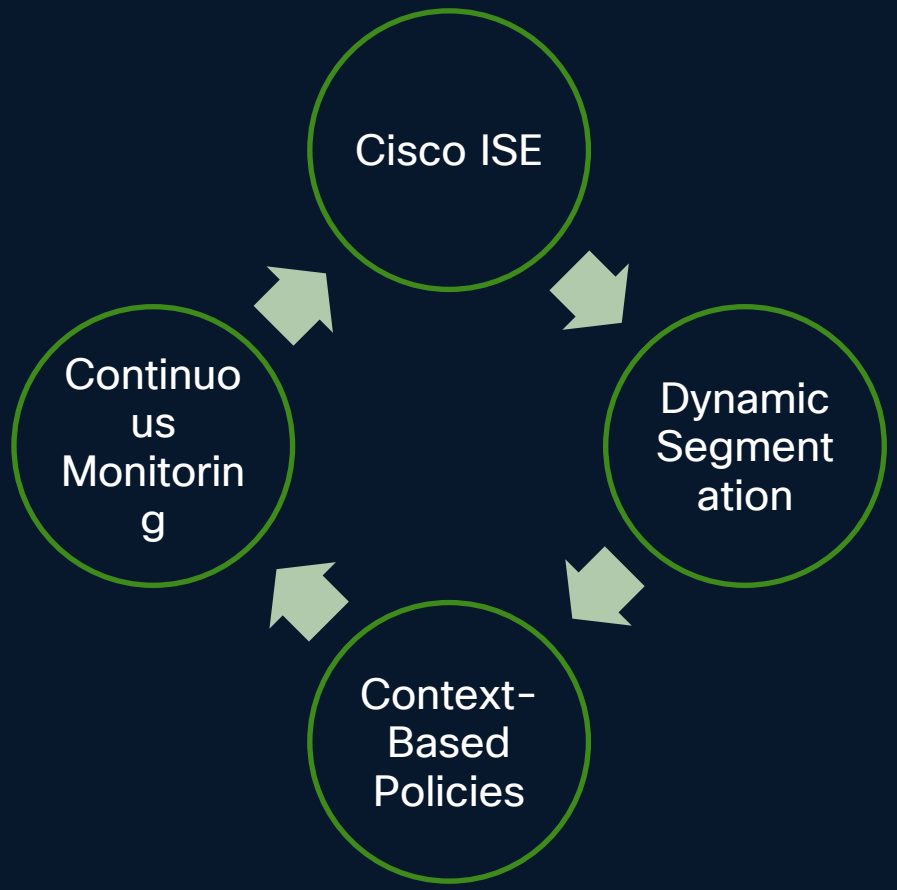
Device Health Check

Performs posture check: verifies OS updates, disk encryption, & active security software. Non-compliant devices are restricted until remediated.

Application-Level Security

Moves beyond network perimeter security. Applies context-aware policies to individual apps, ensuring users meet specific criteria to access critical data, even when inside the network.

Cisco ISE: Network Access Control



Dynamic Segmentation
ISE identifies all devices (wired/wireless/VPN) and assigns Security Group Tags (SGTs) based on user role and context.

Context-Based Policies
Enforces access via Who, What, Where, When, How. Contractors get internet access; employees on managed laptops get full access.

Continuous Monitoring
ISE tracks network changes. If a device status shifts, ISE auto-quarantines it to prevent lateral movement.

Core Capabilities: Cisco ISE and Duo

Cisco ISE

- Deep visibility into users, devices (including IoT), and applications
- Secures network access and contains threats
- Provides rich contextual information
- Performs posture checks to ensure compliance

Cisco Duo

- Authenticates users and verifies devices before access
- Provides strong MFA, device trust, and SSO
- Enables passwordless login capabilities
- Prevents unauthorized access and credential breaches

Visualizing and Normalizing Identity

Sources

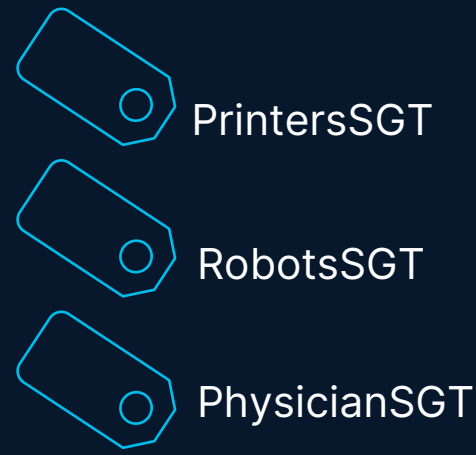
Cisco Technology Alliance Partners (MDM vendors,

RADIUS AAA

Network devices with built in sensors that reveal device type

Workload Integrations (AWS, Azure, GCP, Vmware) with ISE

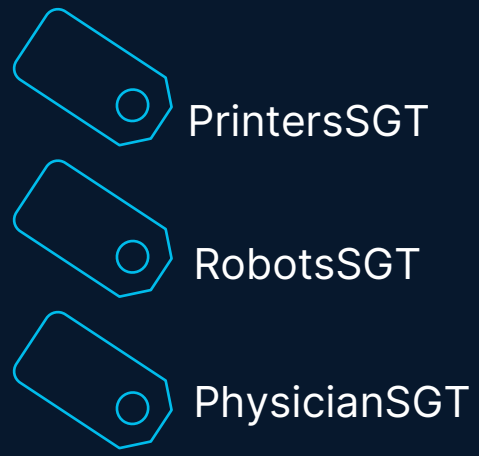
Create Context-aware Identity Groups (SGTs)



Unifying Identity

Create Context-aware Identity Groups (SGTs)

Consume context from its local domain



Share

Share context everywhere, across networking and security domains

pxGrid

pxGrid Cloud

REST API

Syslog

Common Identity

Enforce consistent access with a unified policy experience

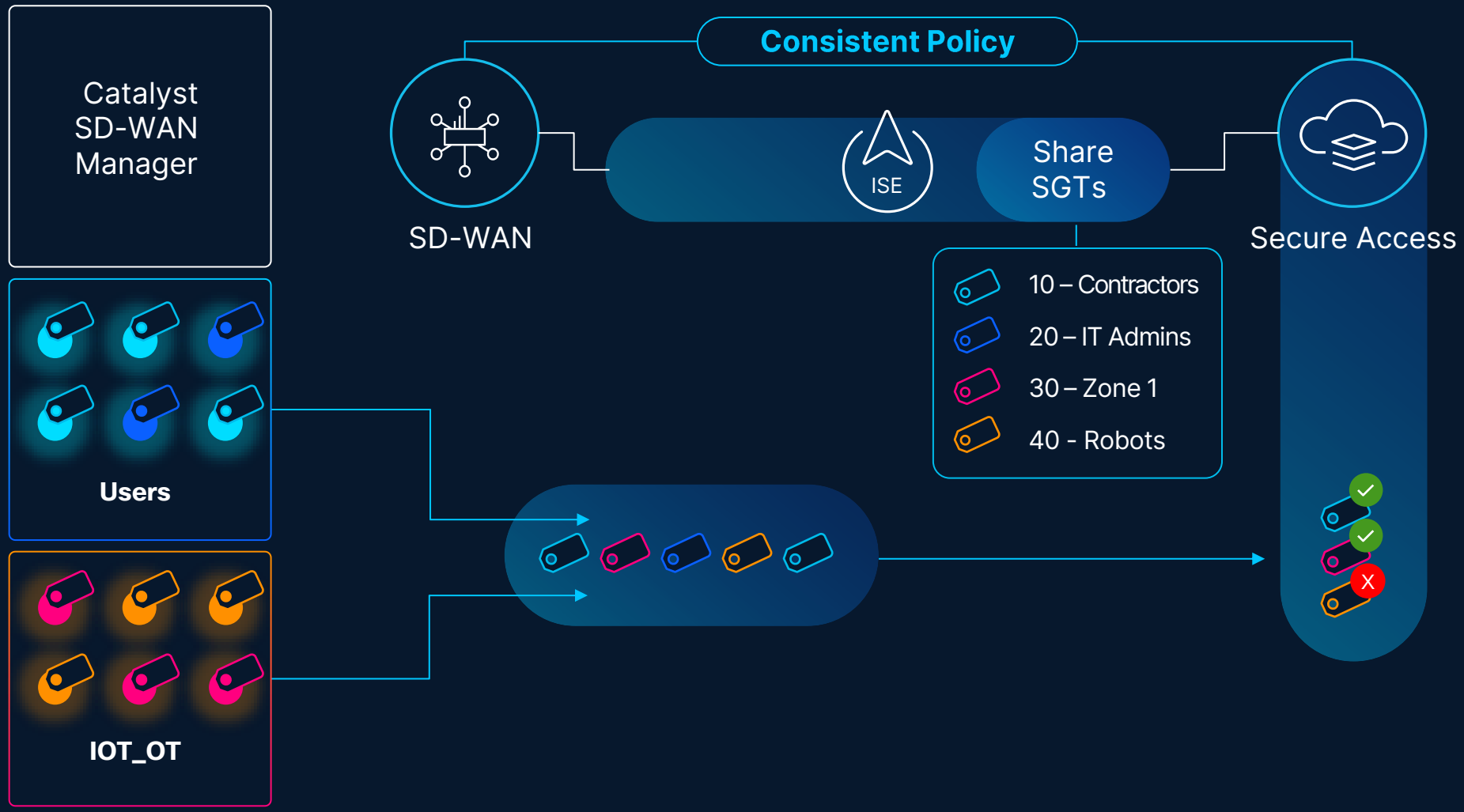
Common Identity

Campus / Branch | Data Center | Cloud

Identity Services Engine (ISE)

Leverage SGTs for granular access control

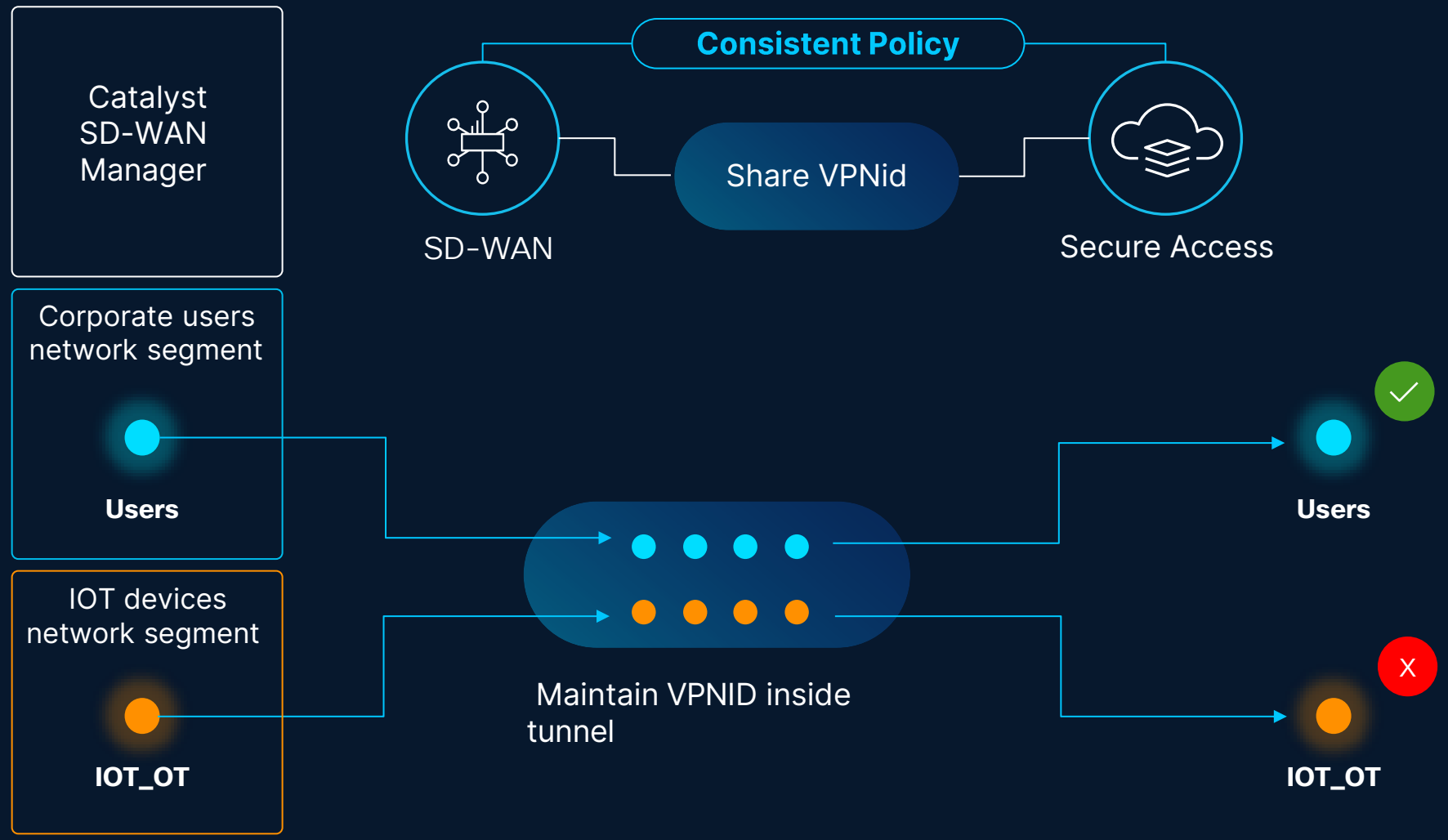
- SGT Based Policy across network & Cloud
- Maintain micro segmentation through Secure Access
- Uniquely identify devices and traffic based on context from ISE
- Apply policy to SGT Based identity



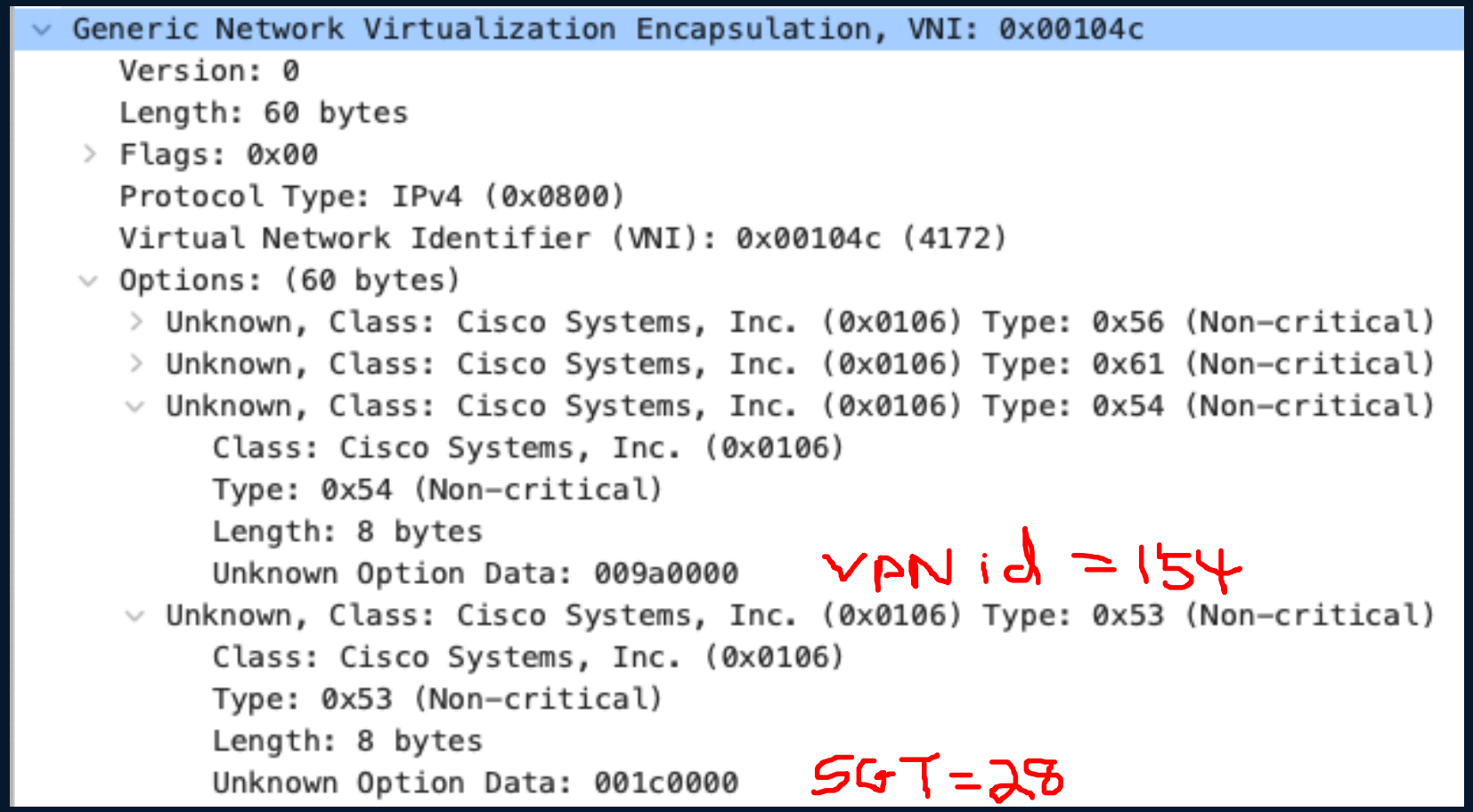
Catalyst SD-WAN

VPNid support for consistent segmentation

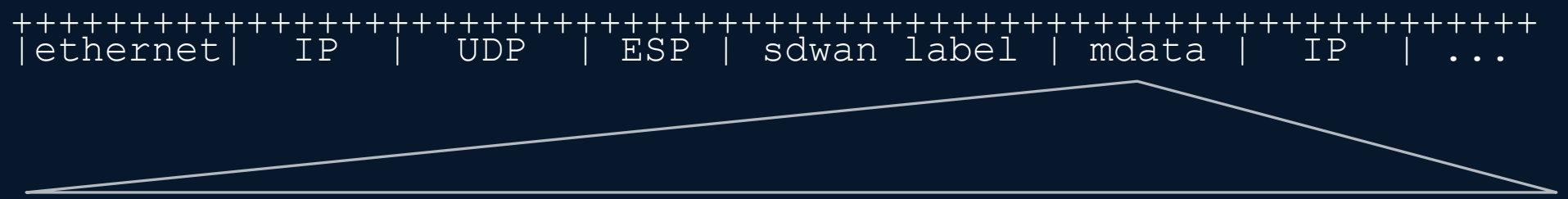
- VPNiD Based policy across both SDWAN & Secure Access
- Maintain segmentation in branch & in the cloud



Packet Format

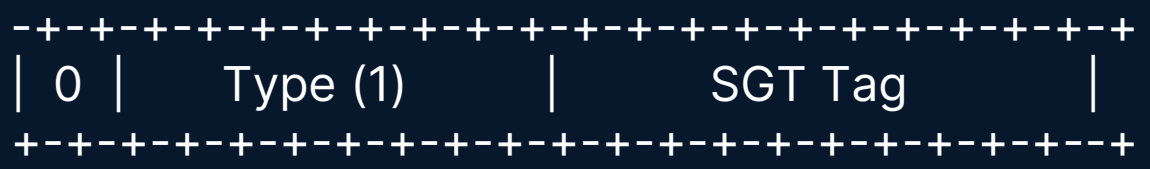


Packet Format



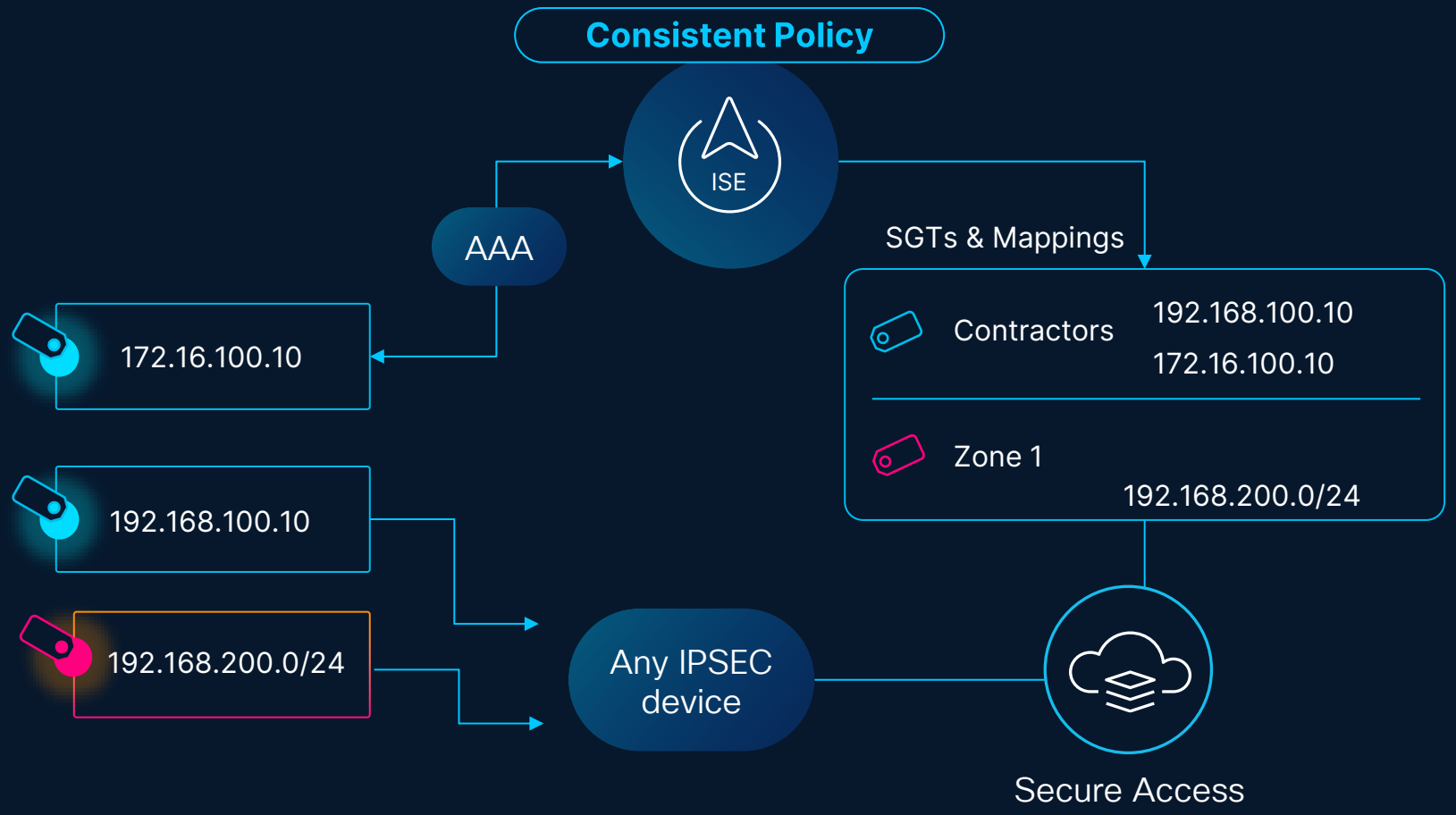
Carrying VPN ID

Carrying SGT



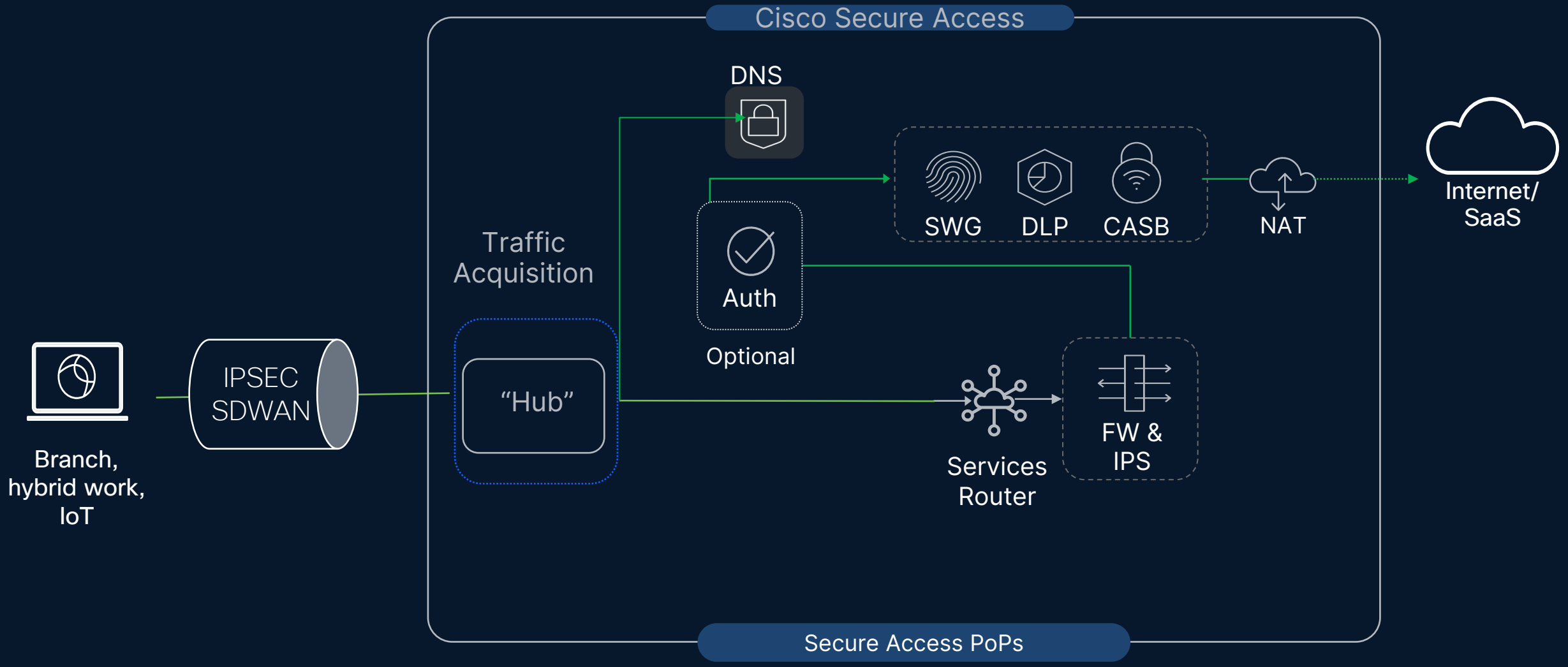
Common context awareness from network to cloud

- SGT Based Policy across network & Cloud
- Maintain micro segmentation through Secure Access
- Uniquely identify devices and traffic based on context from ISE
- Apply policy to SGT Based identity

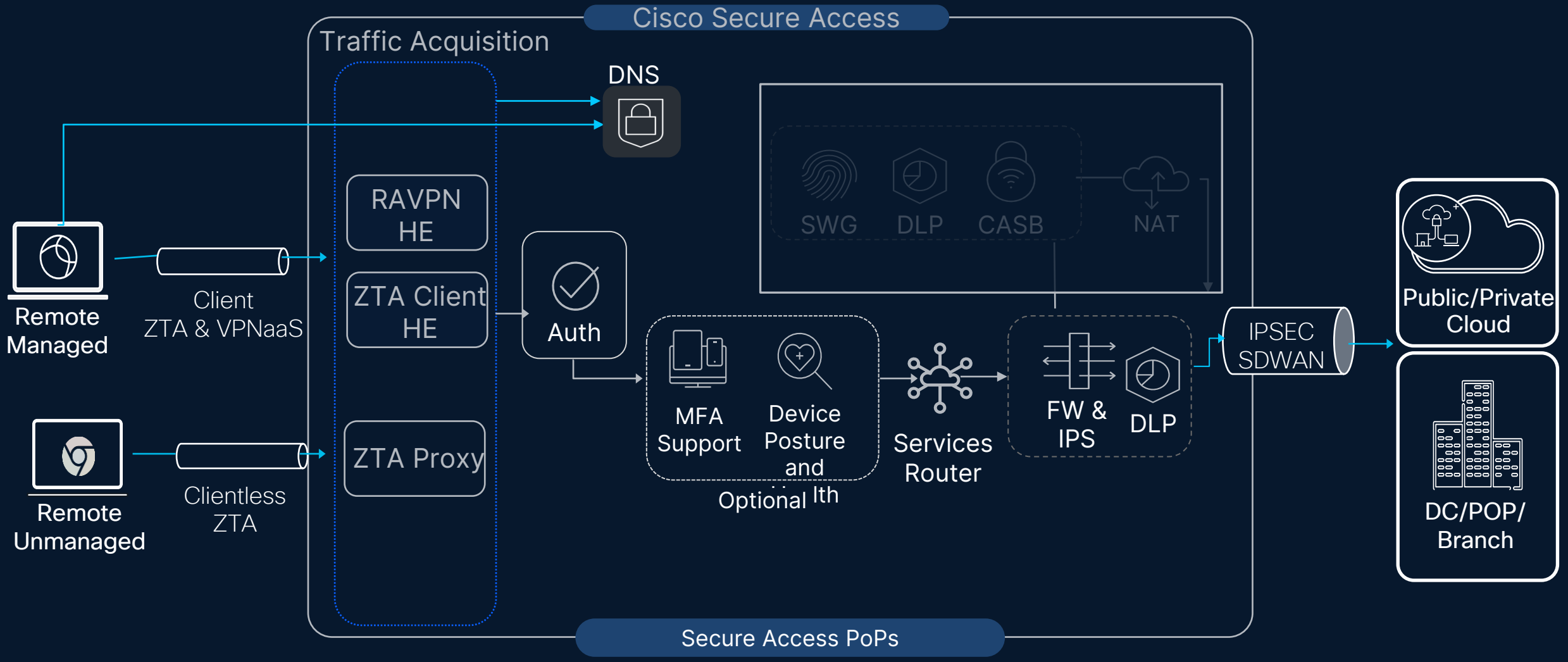


Use Cases

Secure Internet Access (SIA)

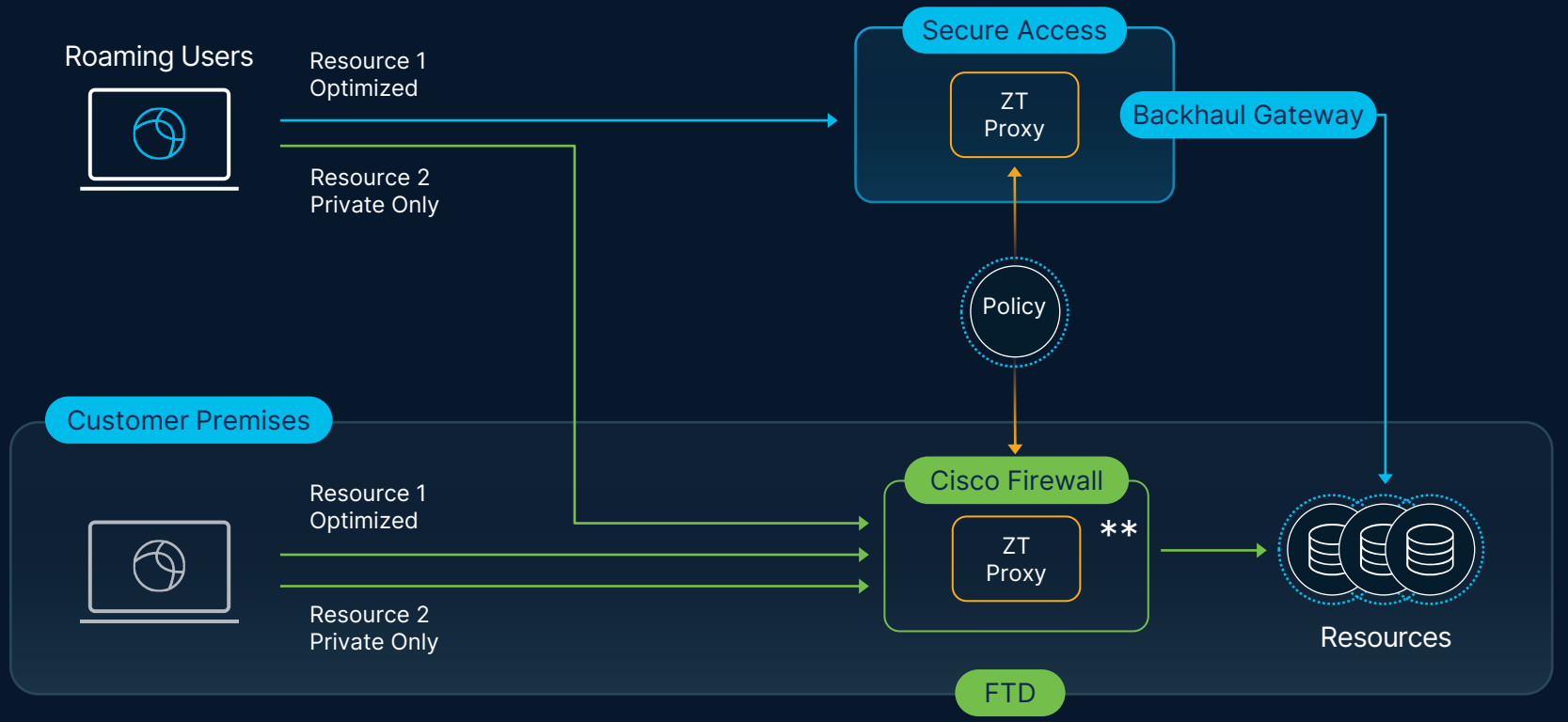


Secure Private Access (SPA)



Hybrid Private Access for flexible enforcement

Single set of ZTNA policies used in cloud and on-premise

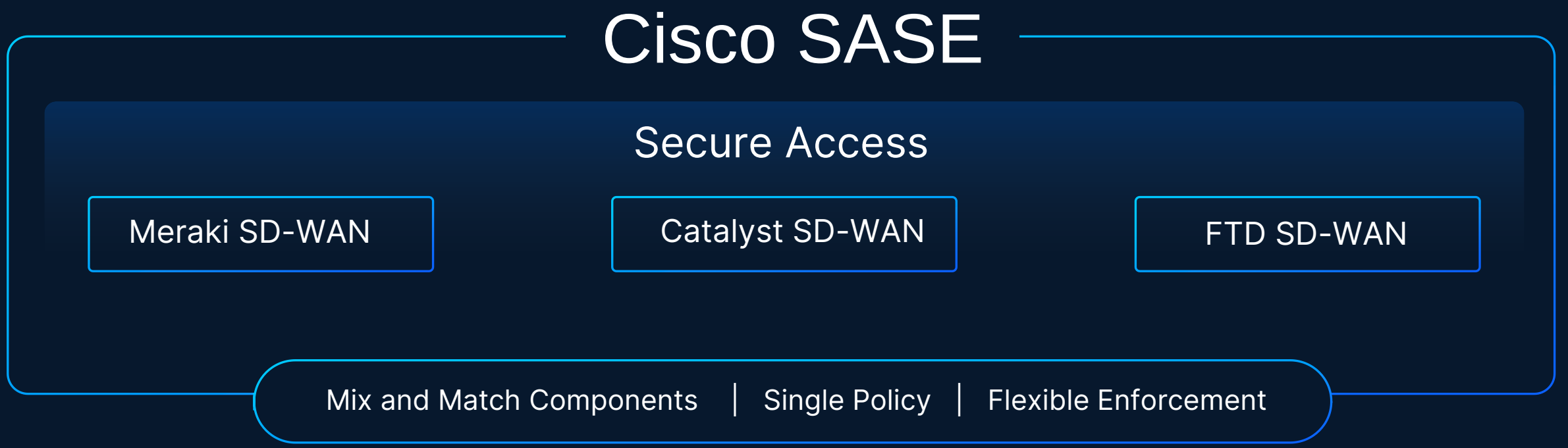


** Roadmap: policy enforcement on 8k routers

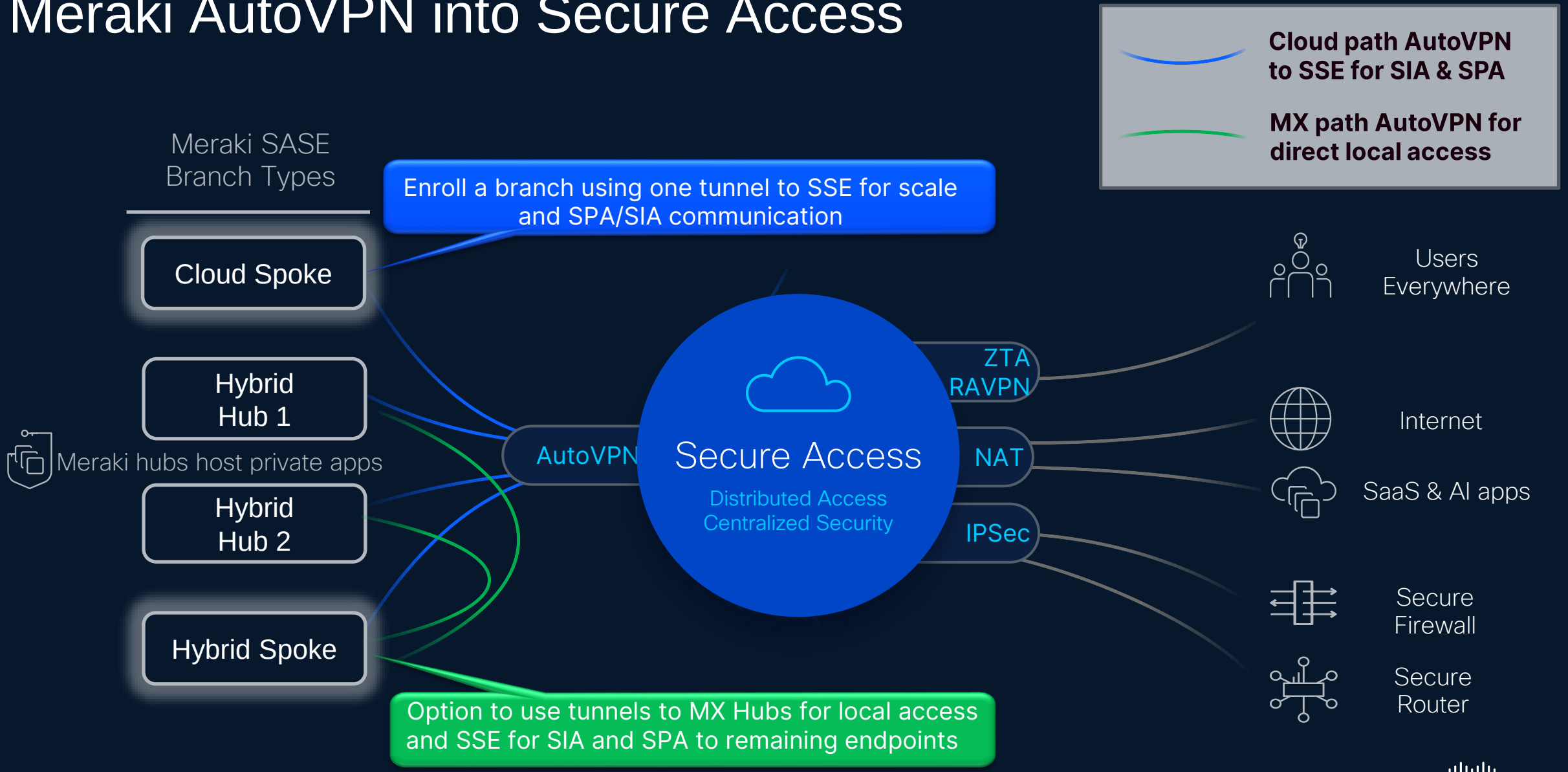
Demos

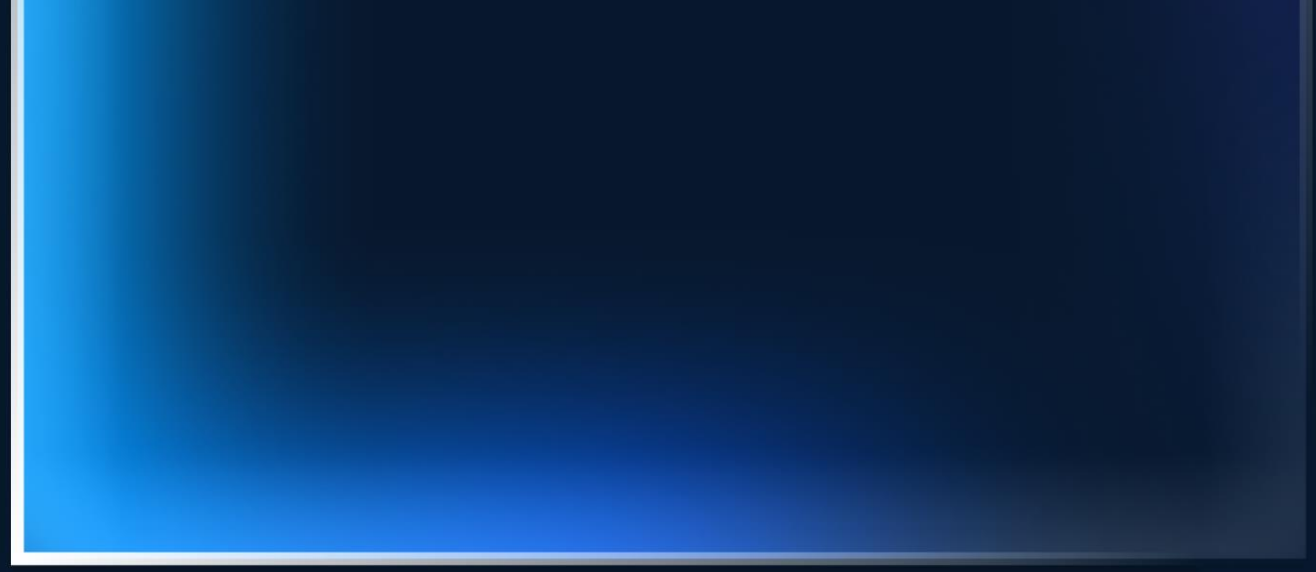
SASE: Secure Access integrated with Cisco SD-WAN

Your security strategy for a hyper-distributed world

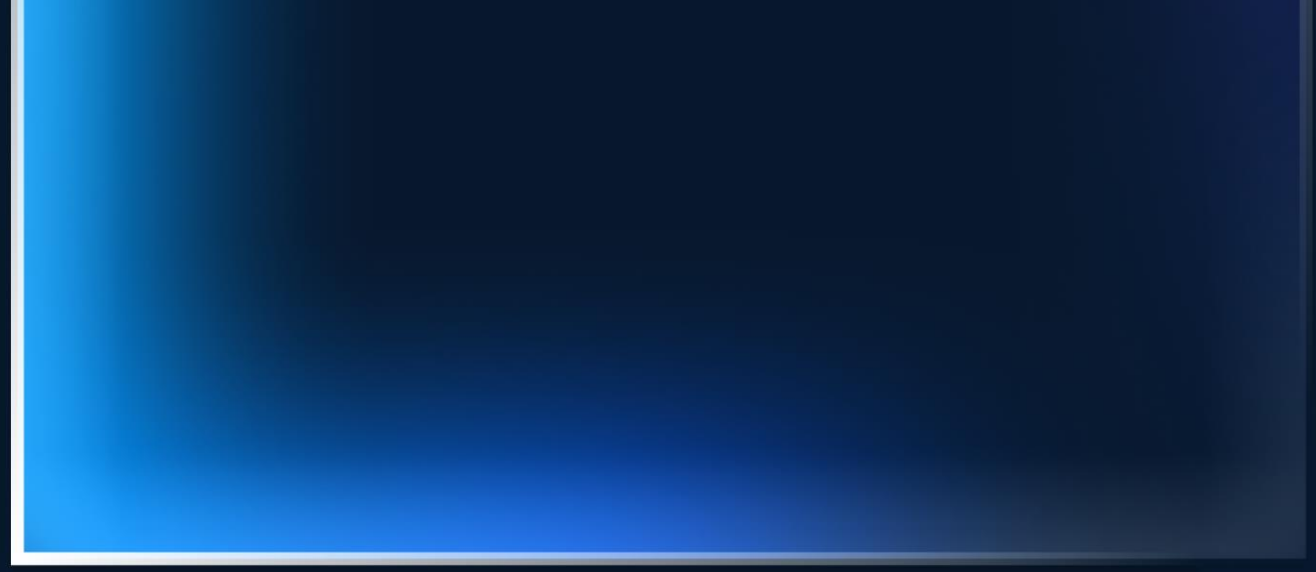


Meraki AutoVPN into Secure Access





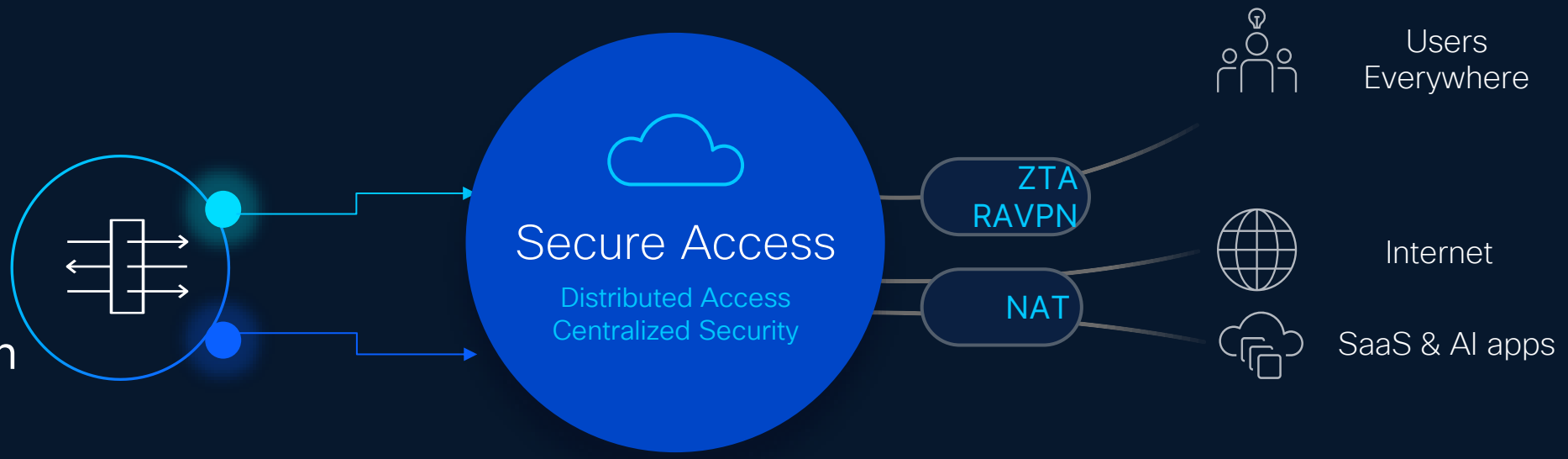
Cisco SASE with Meraki

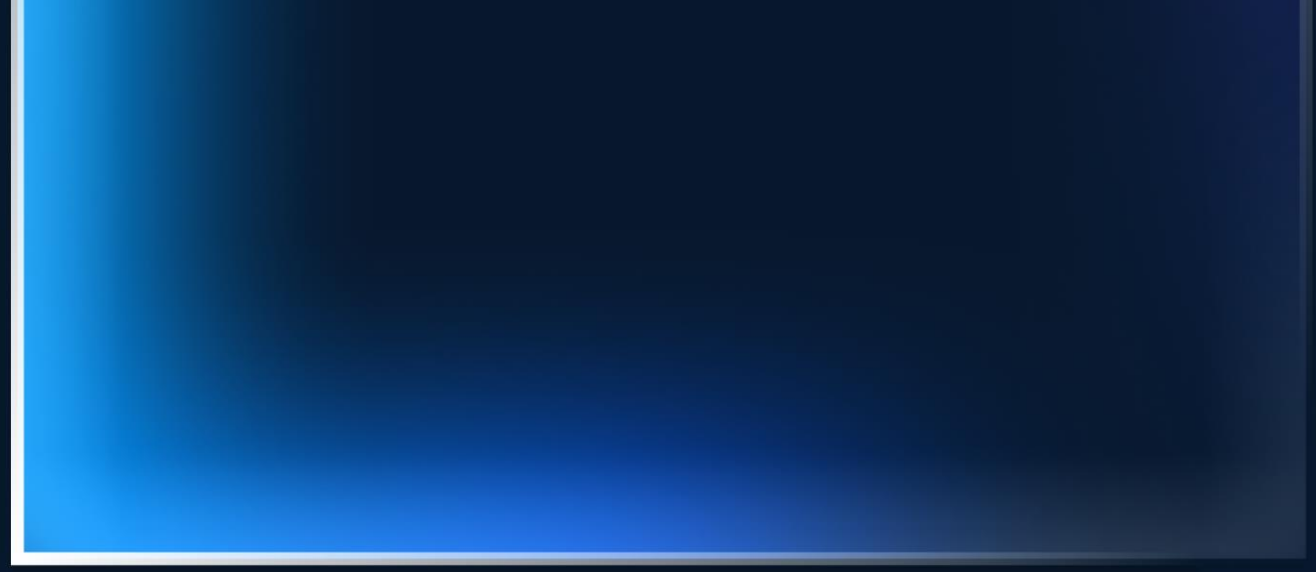


SDWAN integration with LAN switches and access points

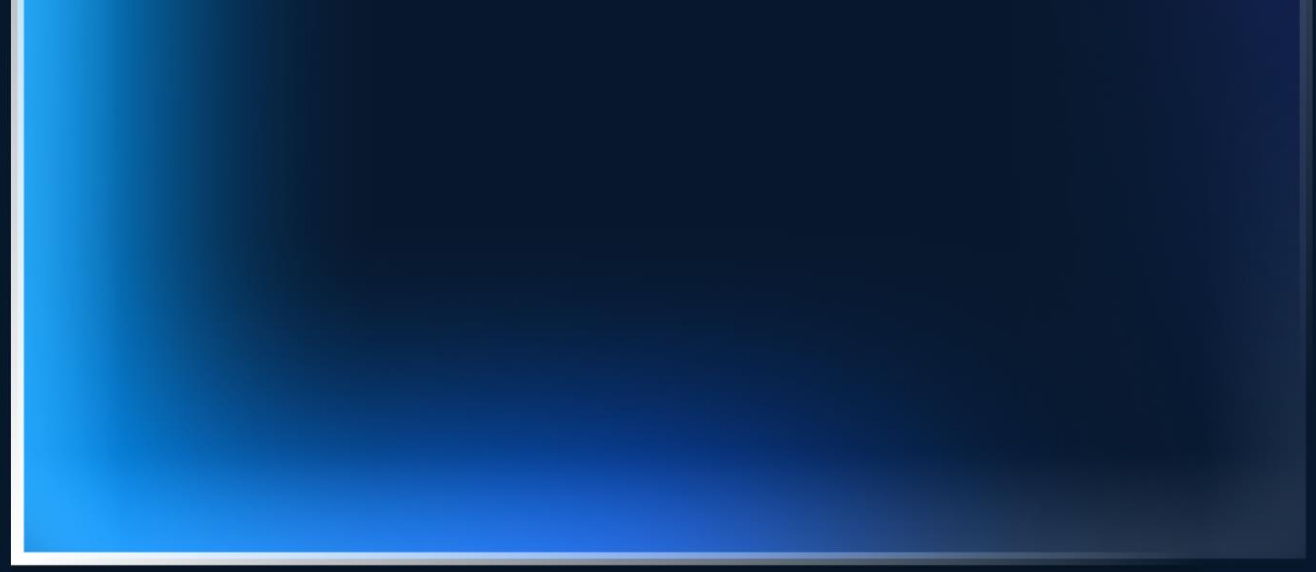
Secure Firewall into Secure Access

- The SASE wizard simplifies tunnel creation by automating multiple steps
- Offload internet security to Secure Access
- Data Loss Prevention
- AI Guardrails/AI Semantic Security





SASE with FTD Demo



Cisco SASE with Catalyst

The high cost of fragmented operations
Challenges of managing SASE

Disjointed Experience

Siloed management consoles for SD-WAN & Security

Fragmented identity & access control (RBAC)

No unified sign-on experience

Inconsistent Security Posture

Drifting policies across Network & Security layers

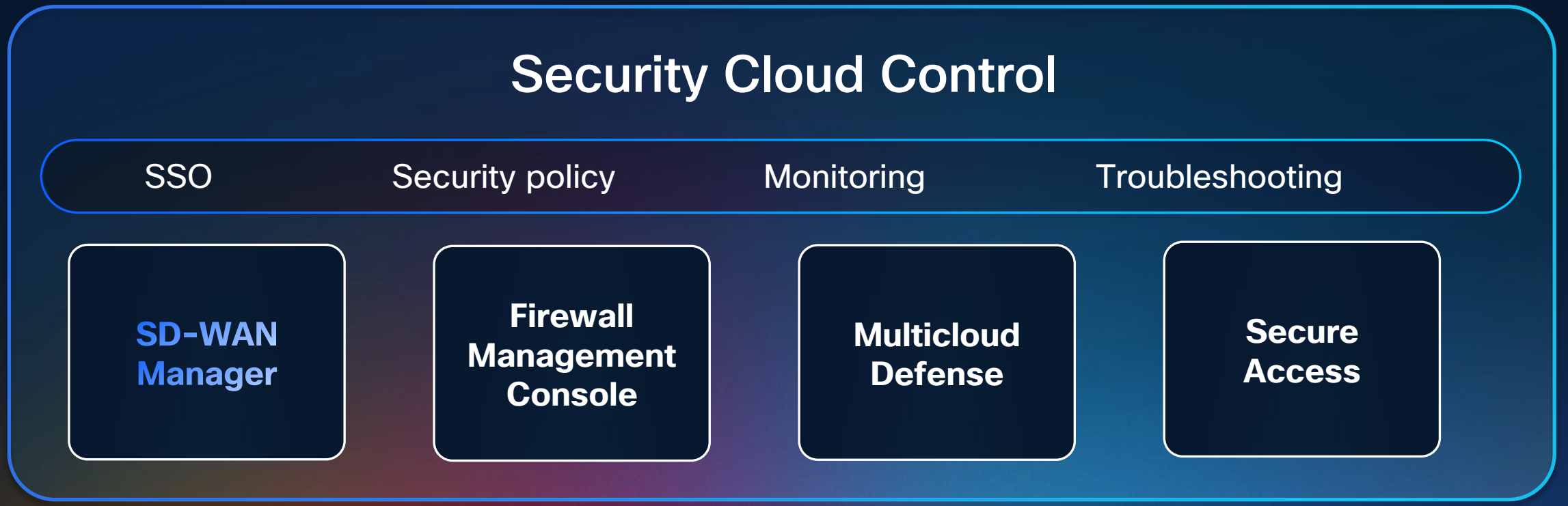
Duplicated objects – no single source of truth

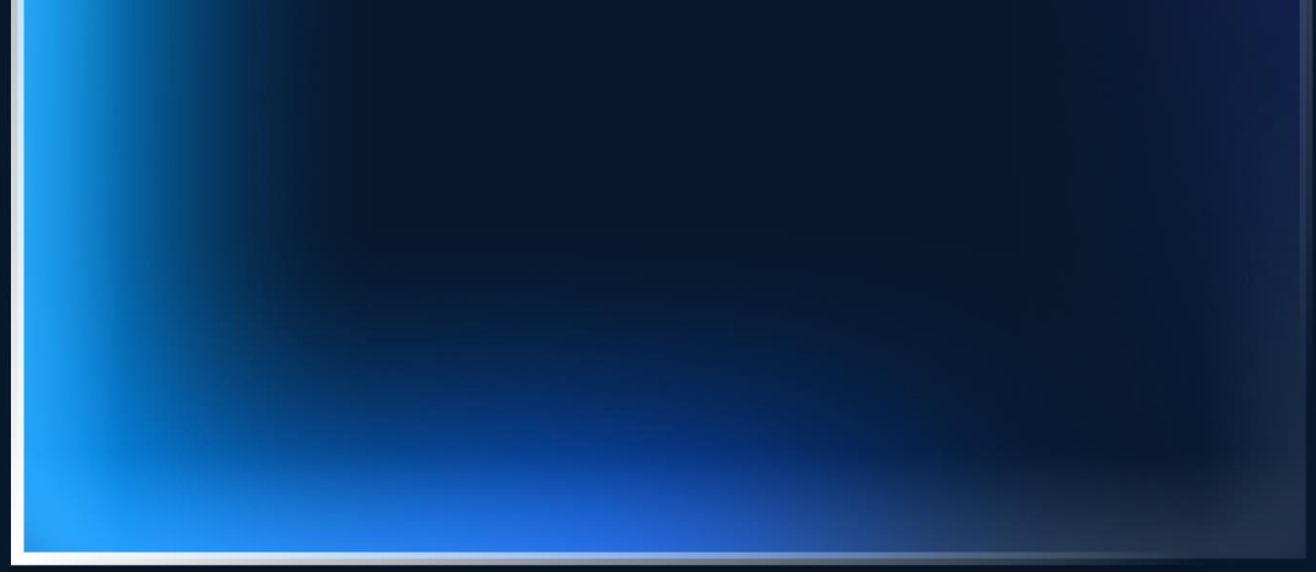
Blind Spots

Decoupled monitoring creates troubleshooting dead-ends

Lack of end-to-end correlation

Rich, centralized management for SecOps



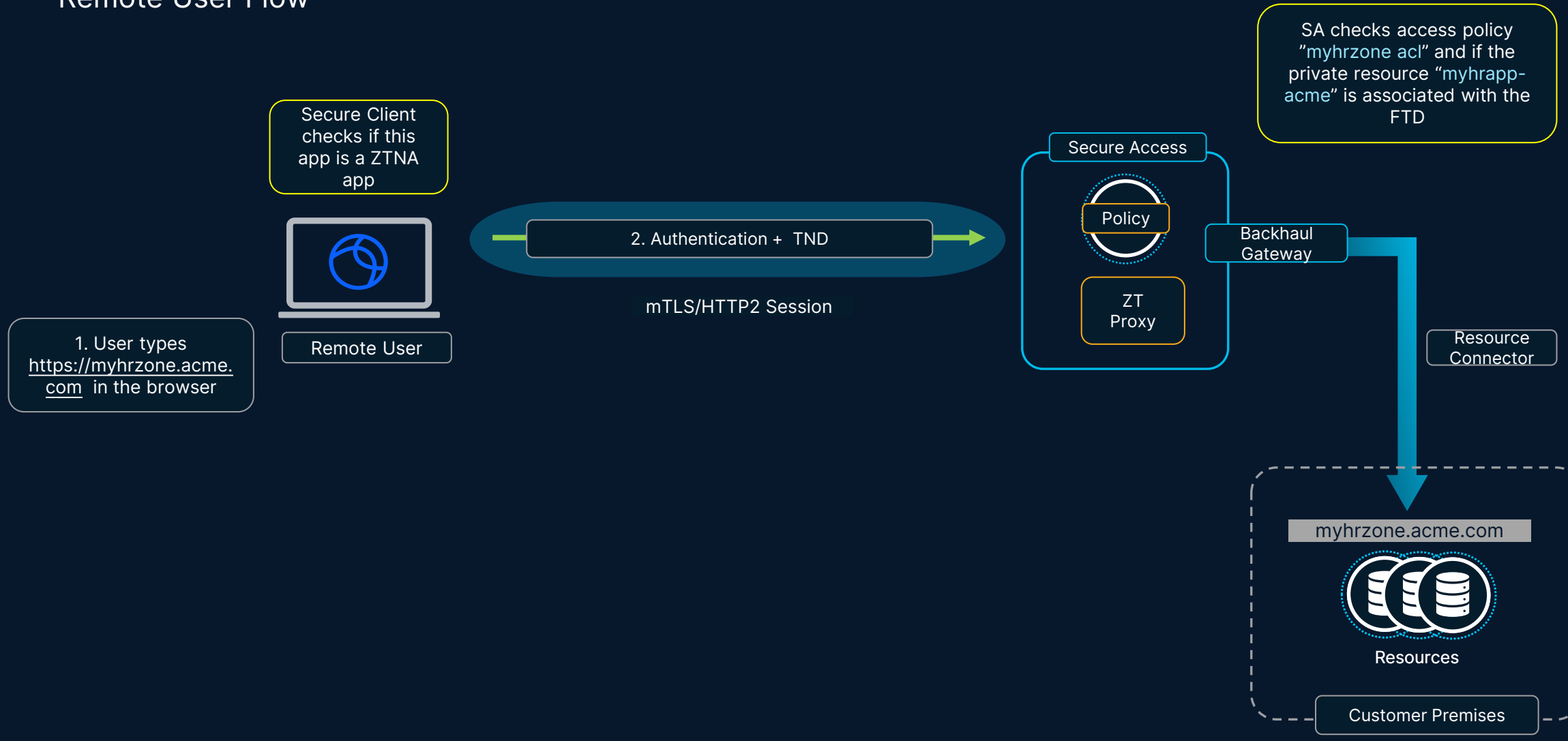


SASE with Catalyst SD-WAN Demo

Cisco Hybrid Private Access with Firepower Threat Defense

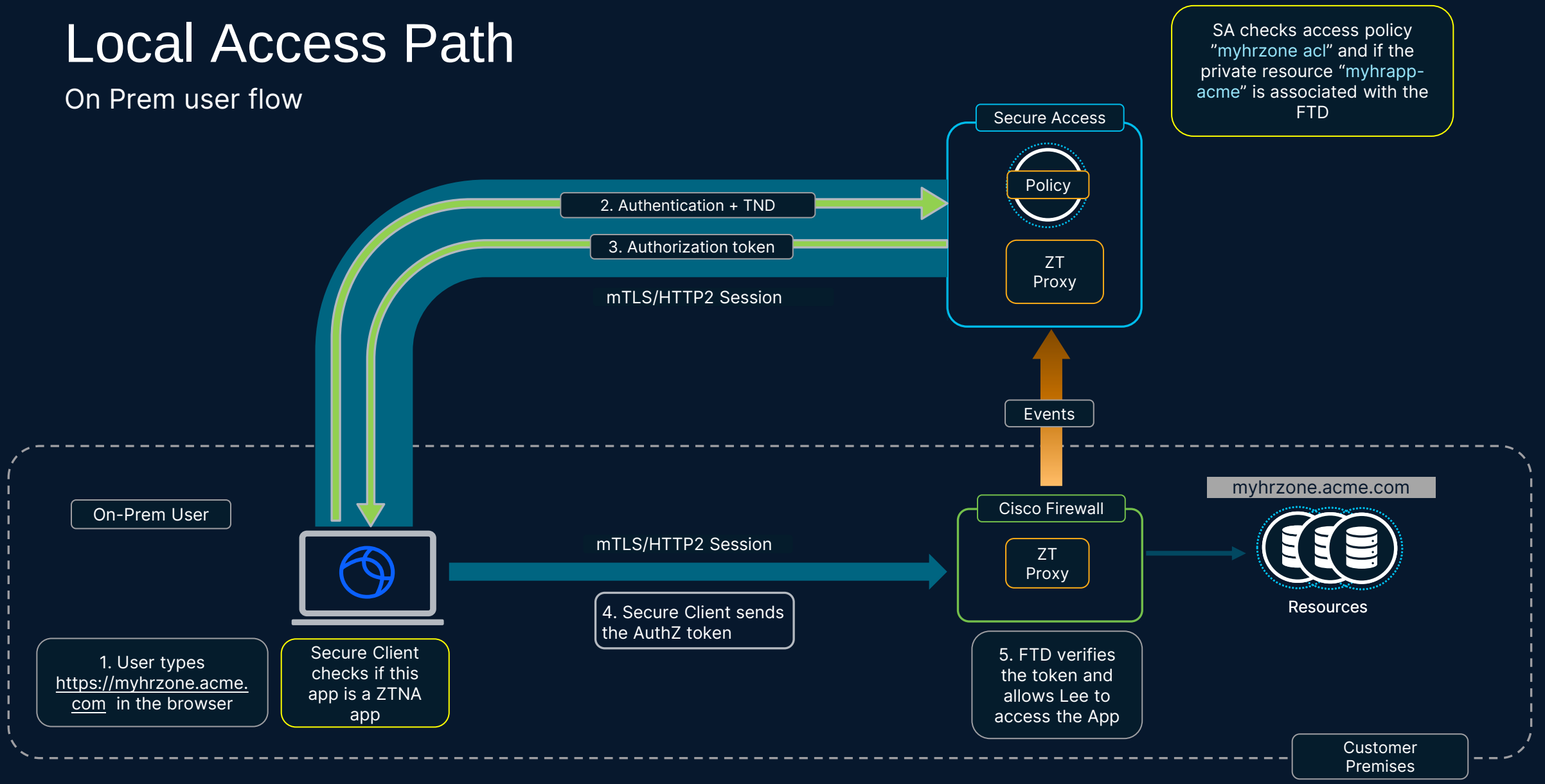
Cloud Access Path

Remote User Flow

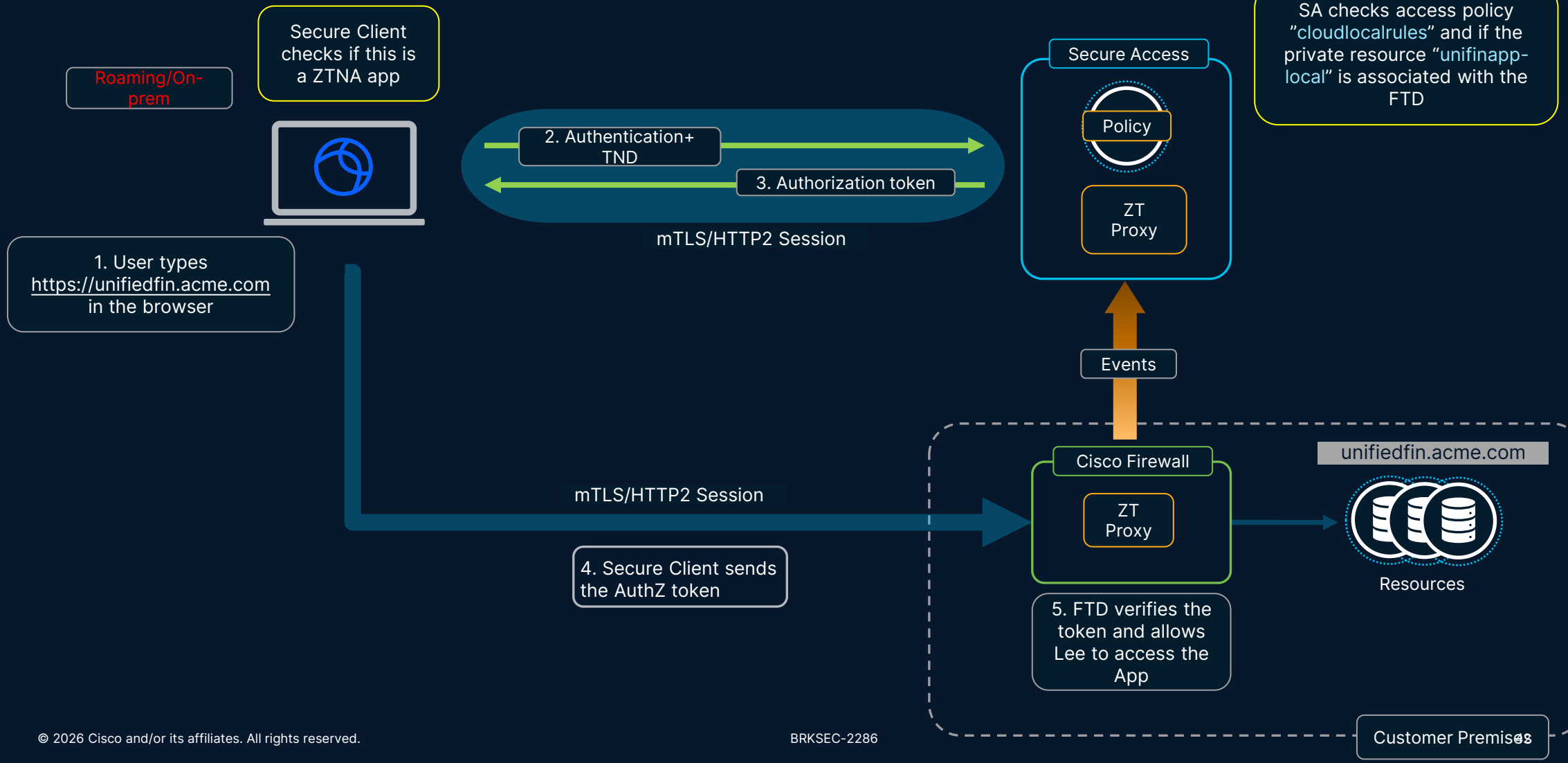


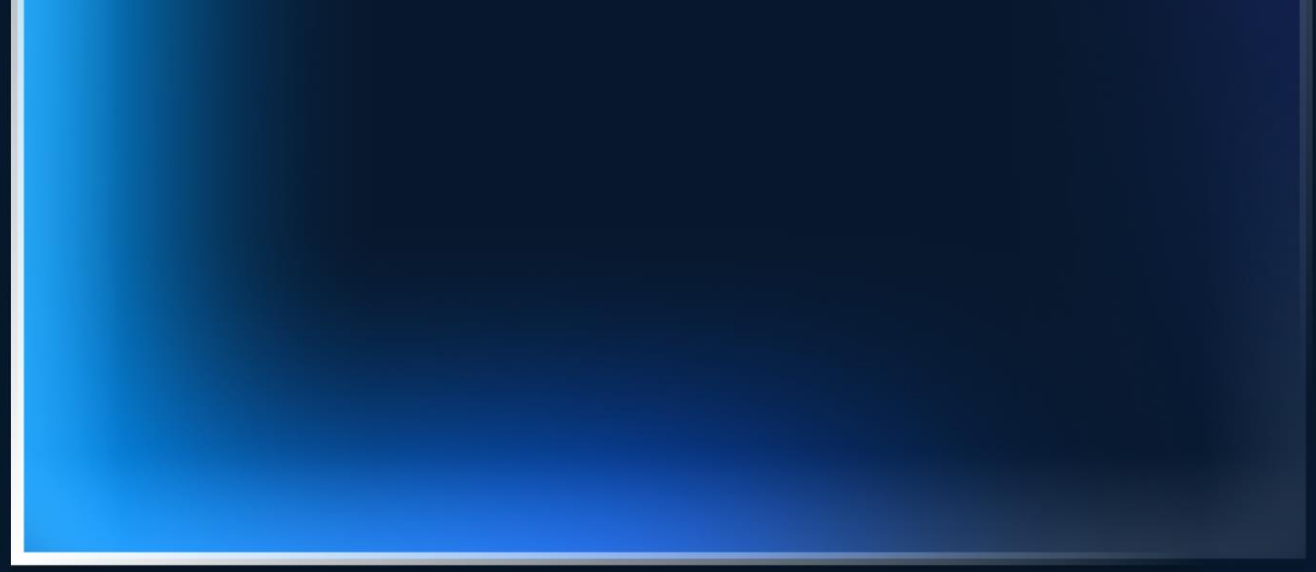
Local Access Path

On Prem user flow



Something

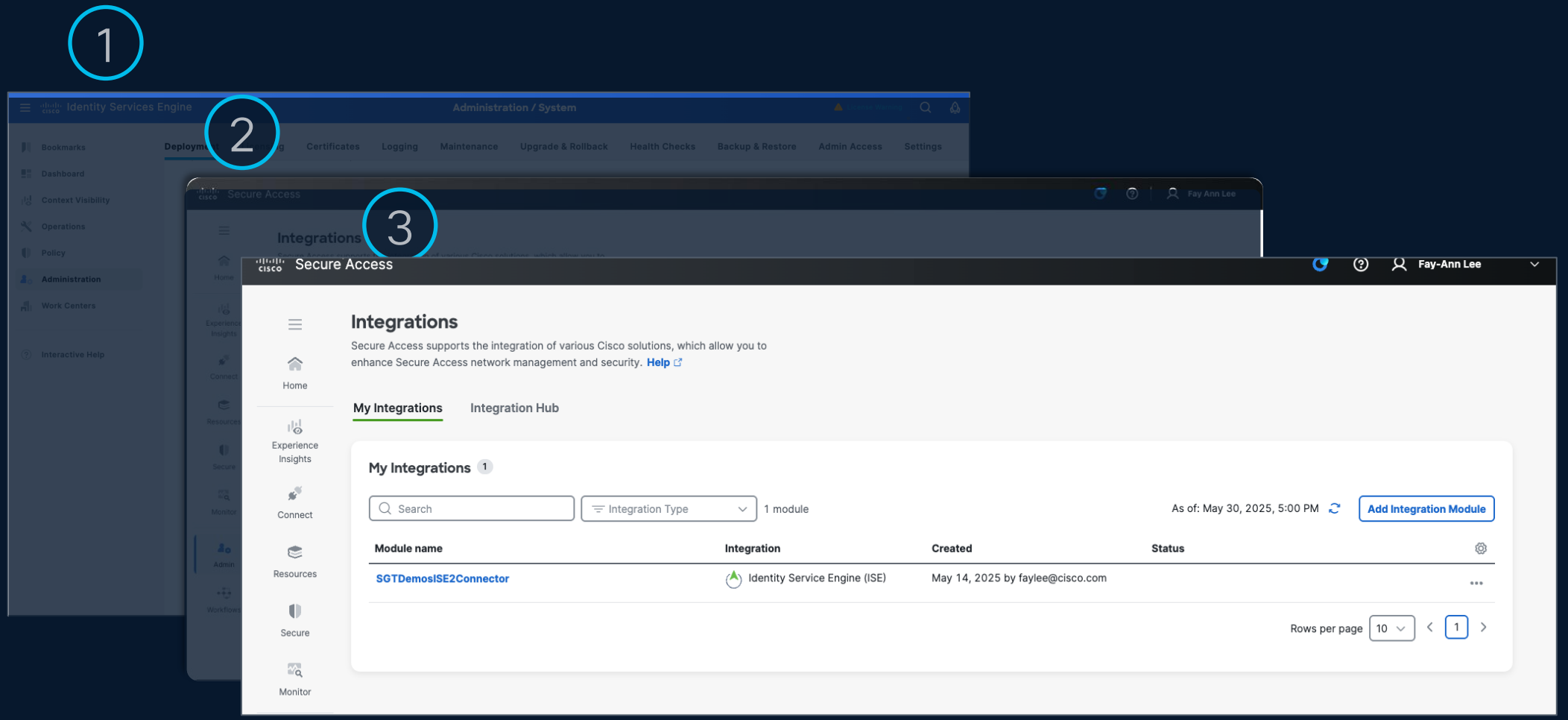




Hybrid Private Access Demo

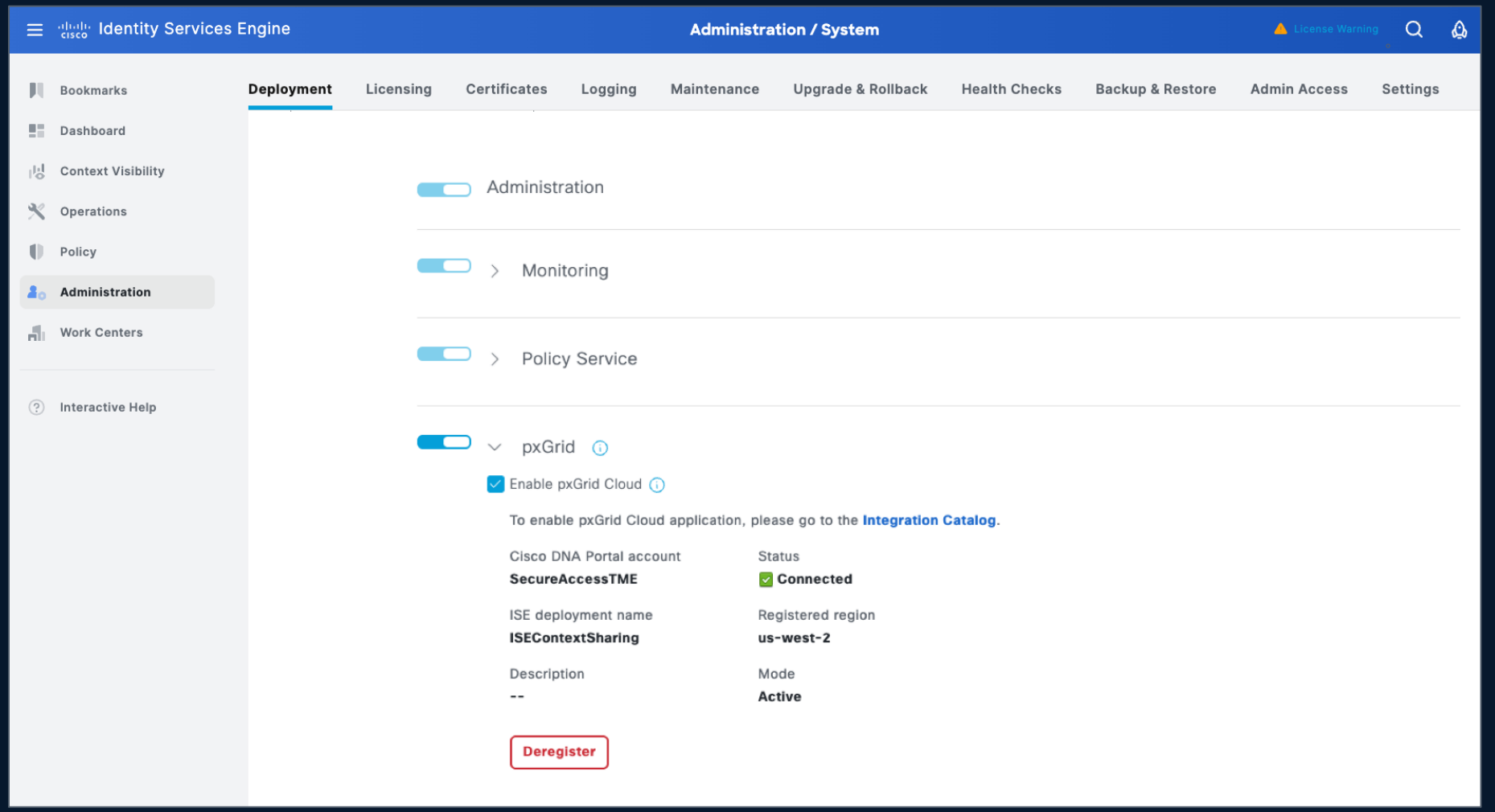
Configuration

Sharing Context-Aware Identity to Secure Access



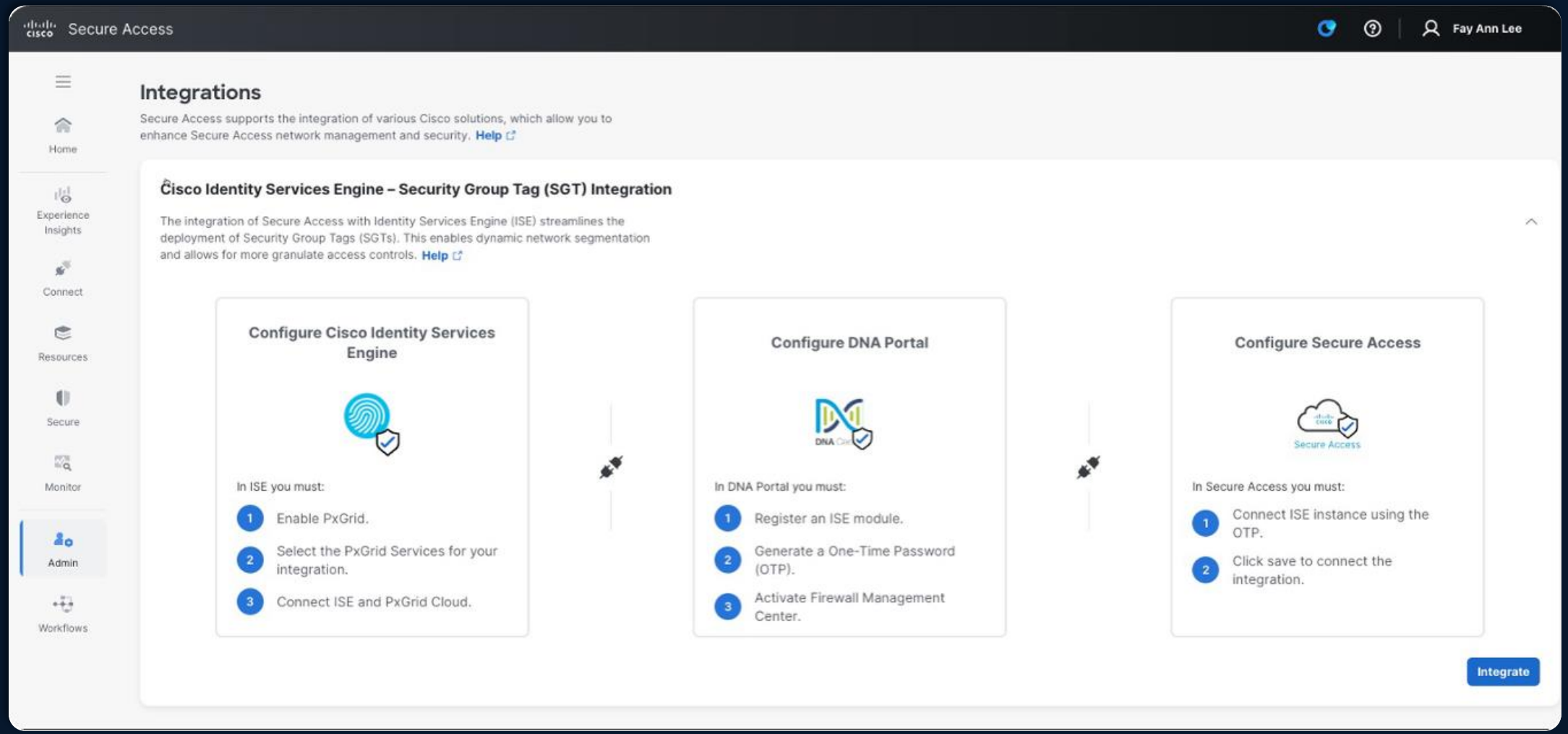
Sharing Context-Aware Identity to Secure Access

1



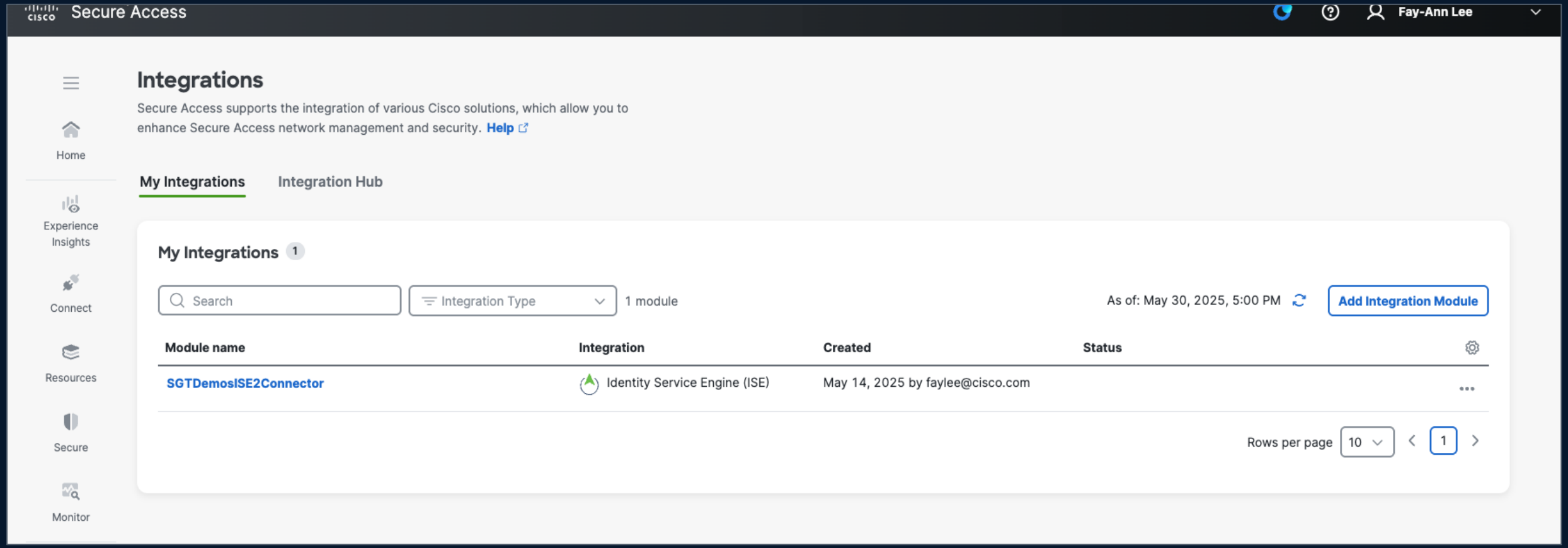
Sharing Context-Aware Identity to Secure Access

2

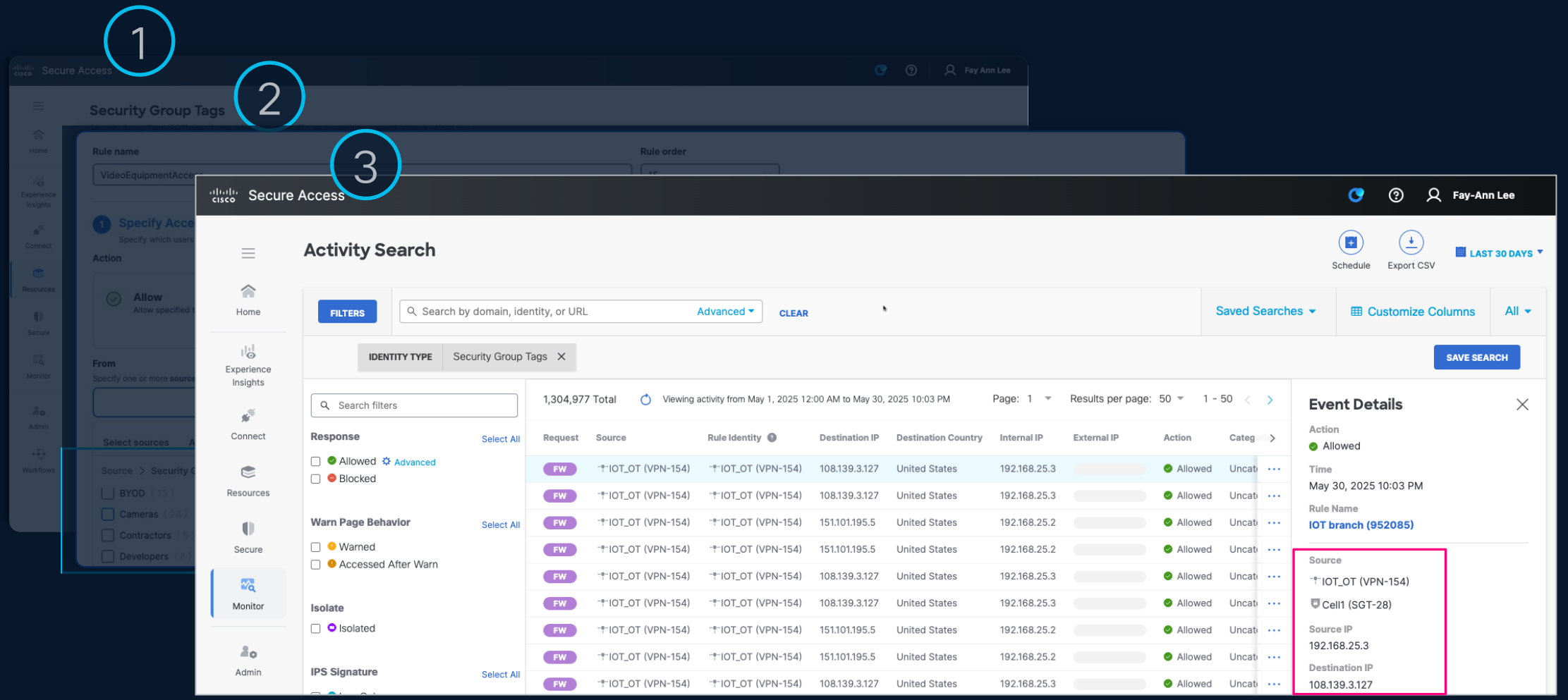


Sharing Context-Aware Identity to Secure Access

3

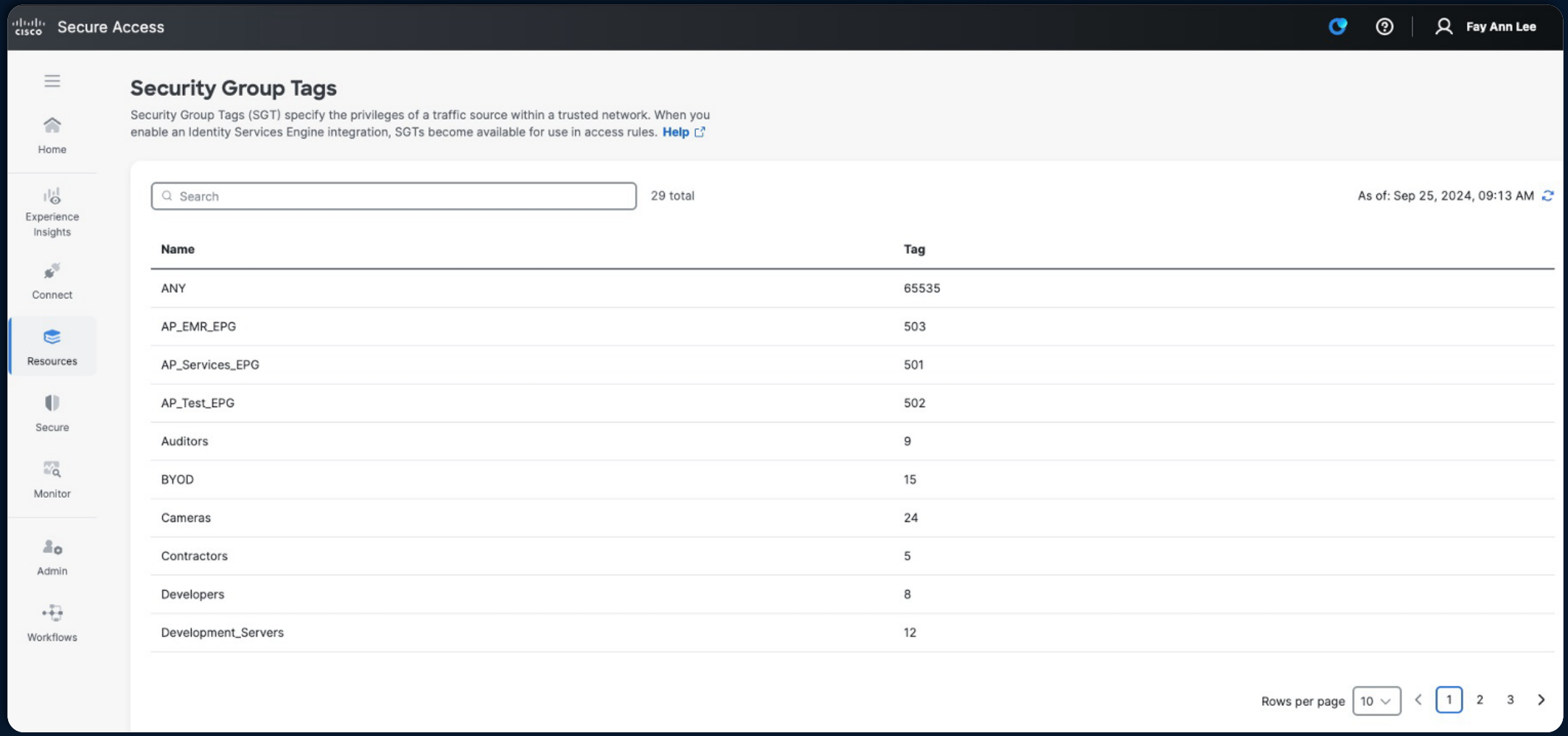


Leveraging SGTs in Cloud based policy enforcement



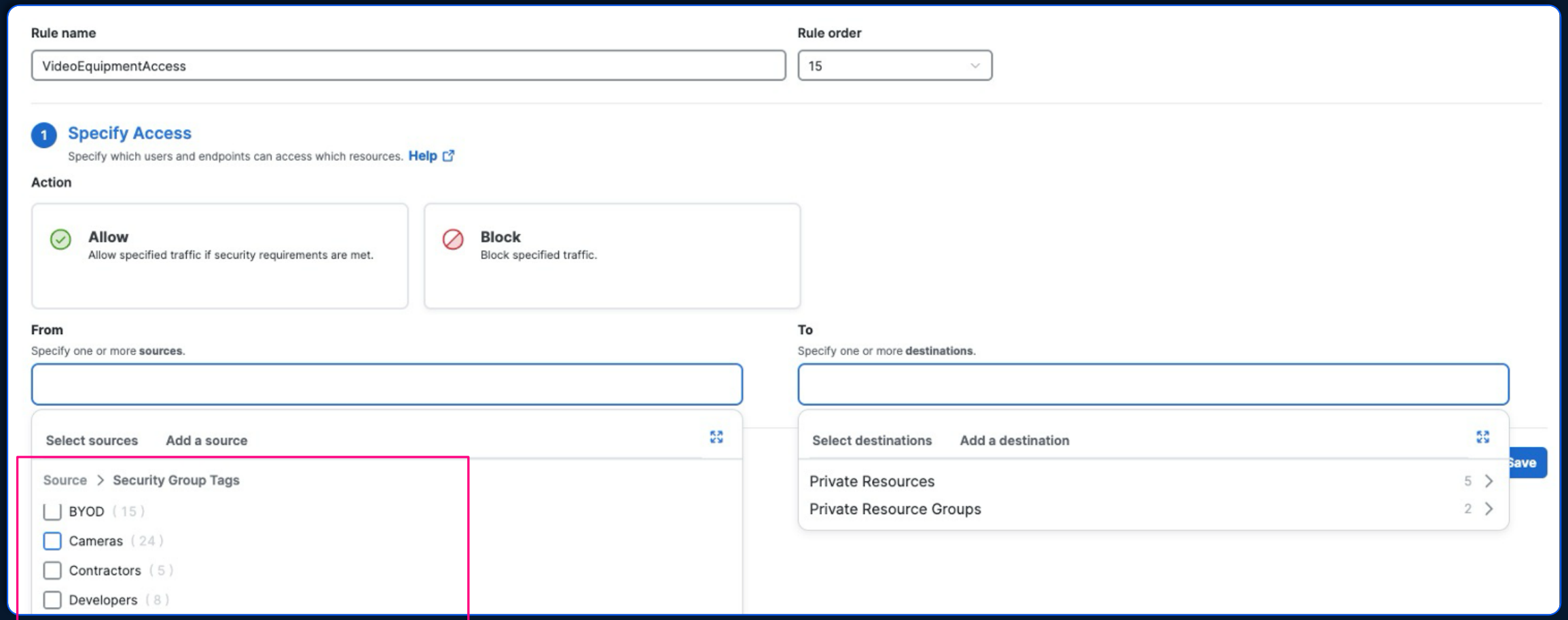
Leveraging SGTs in Cloud based policy enforcement

1



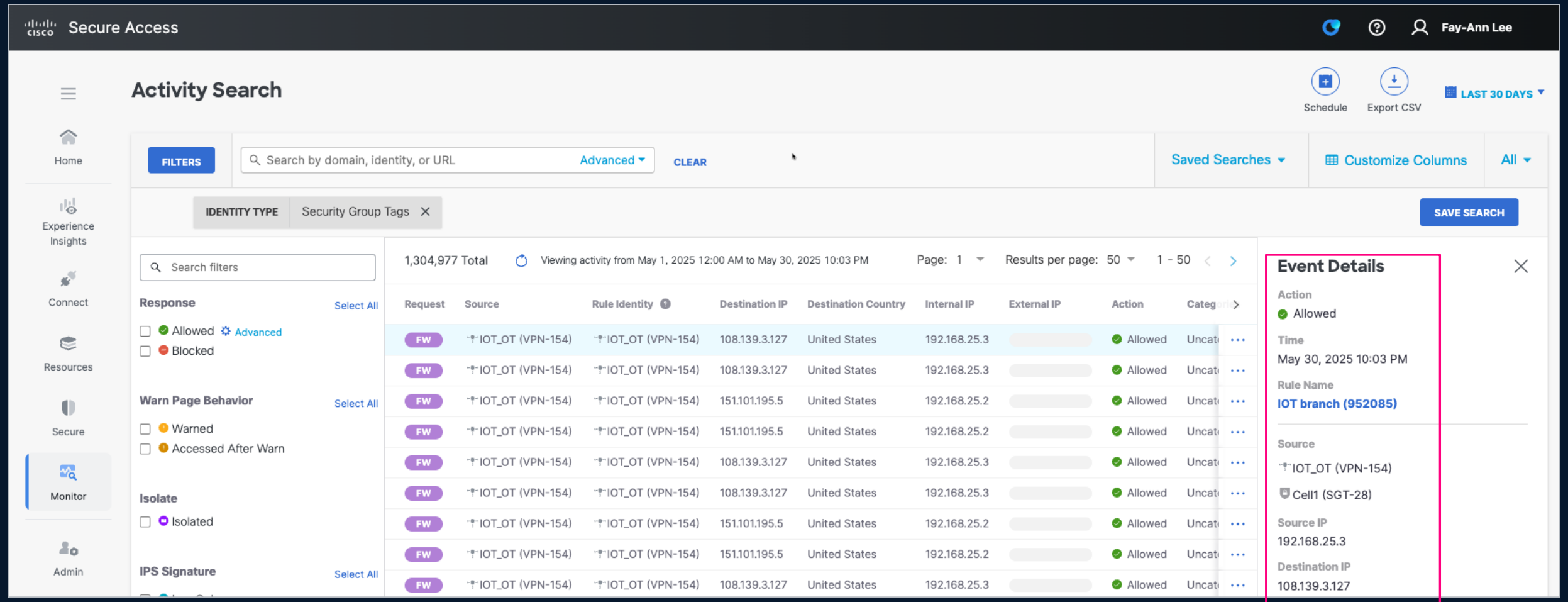
Leveraging SGTs in Cloud based policy enforcement

2

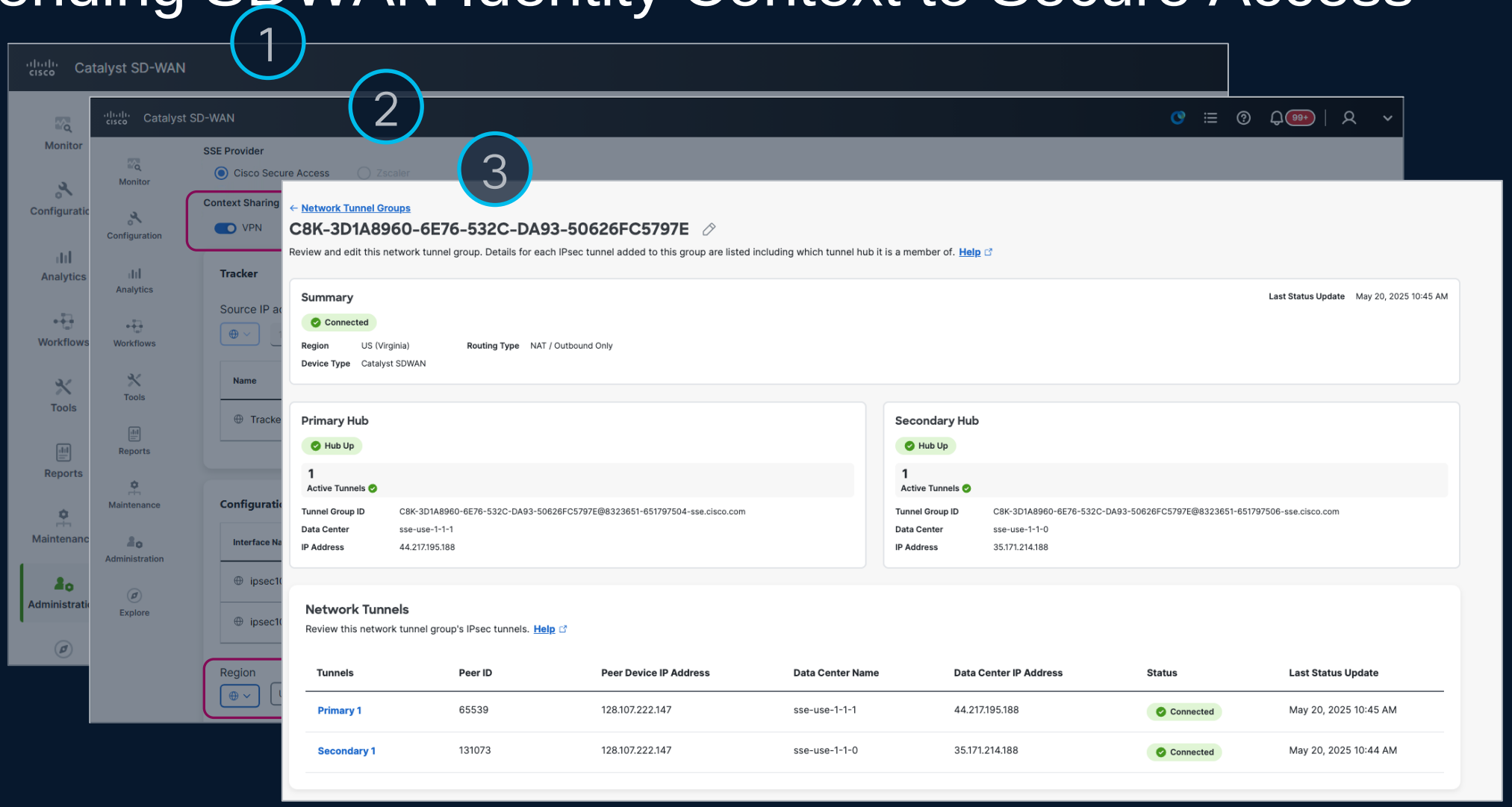


Leveraging SGTs in Cloud based policy enforcement

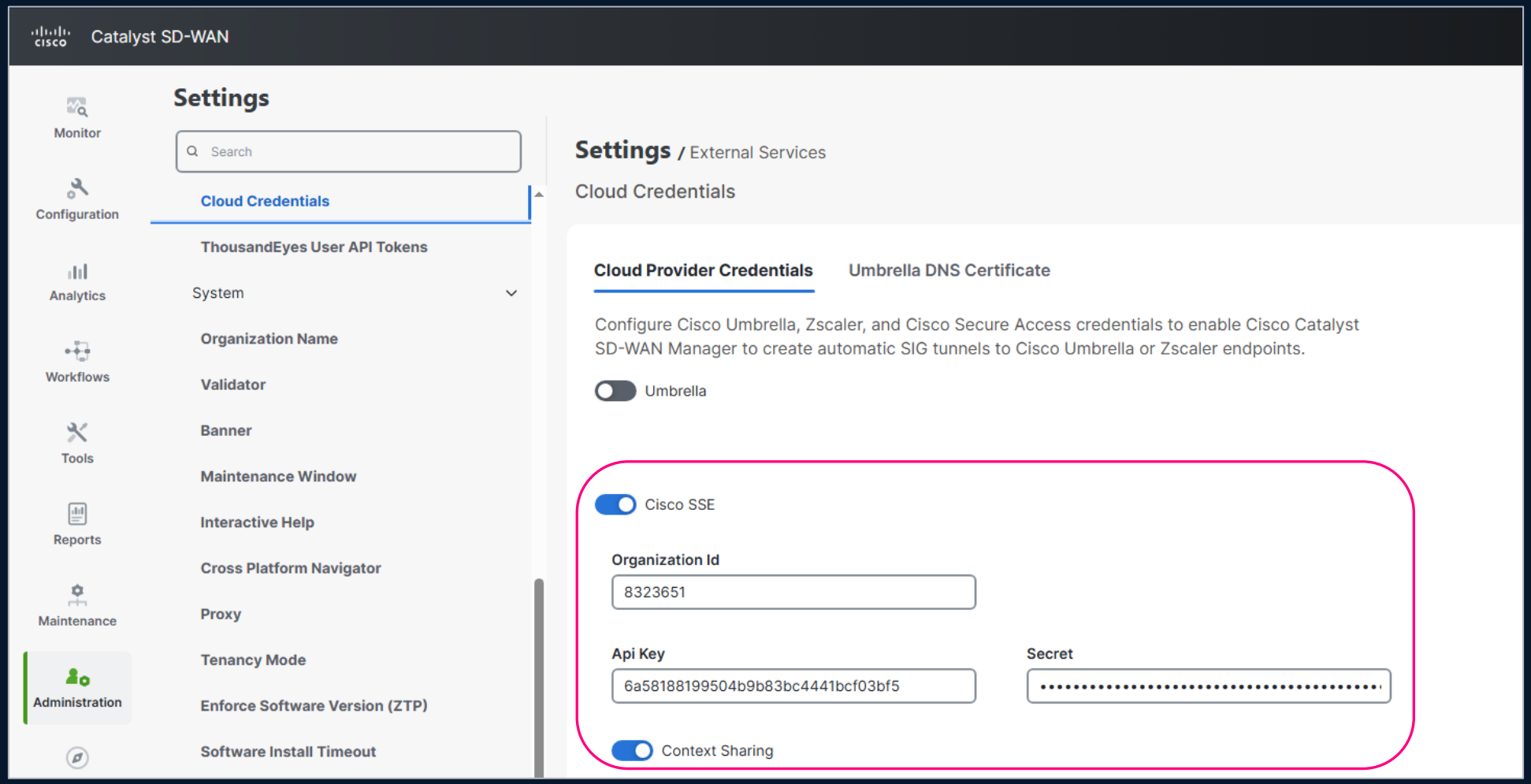
3



Extending SDWAN Identity Context to Secure Access

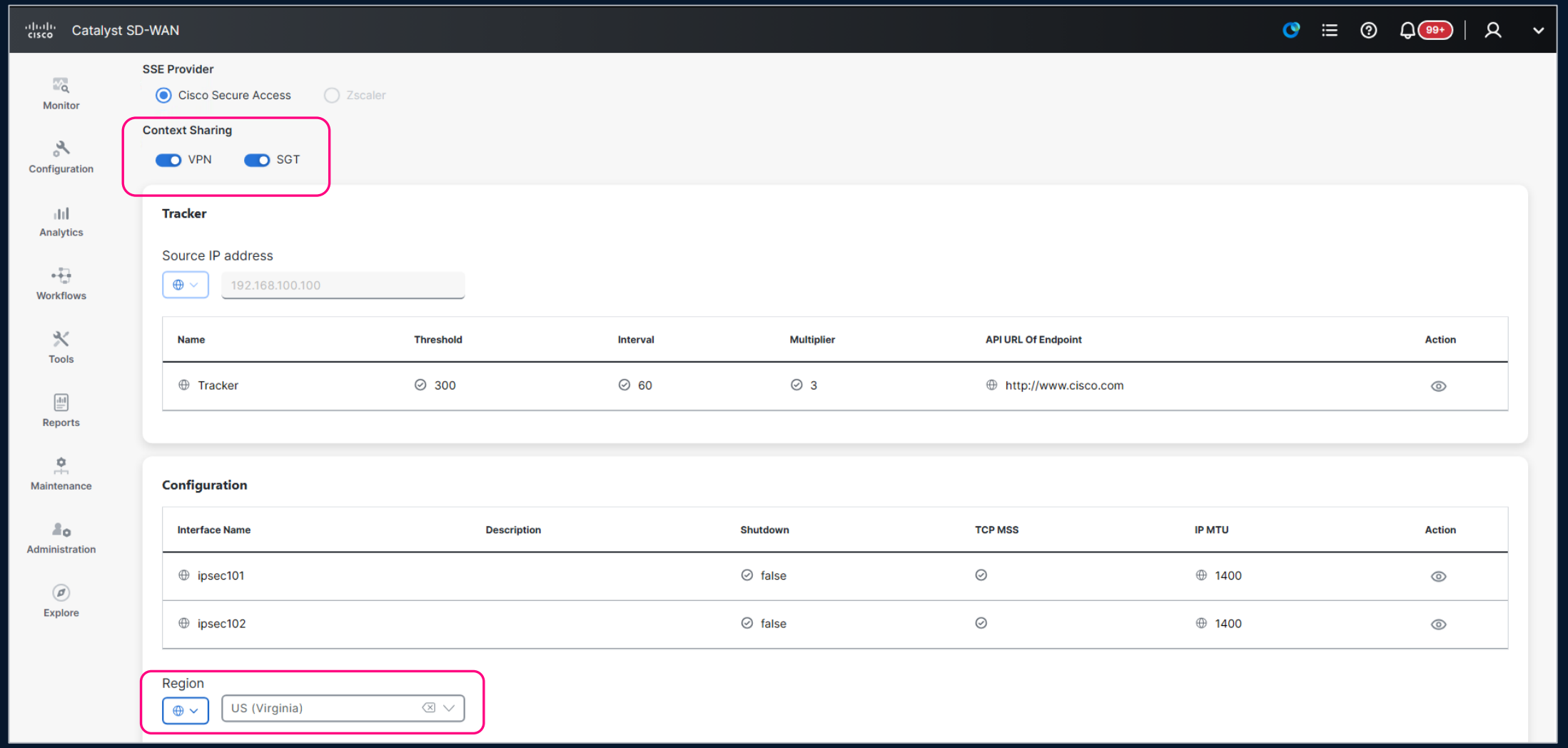


Extending SDWAN Identity Context to Secure Access



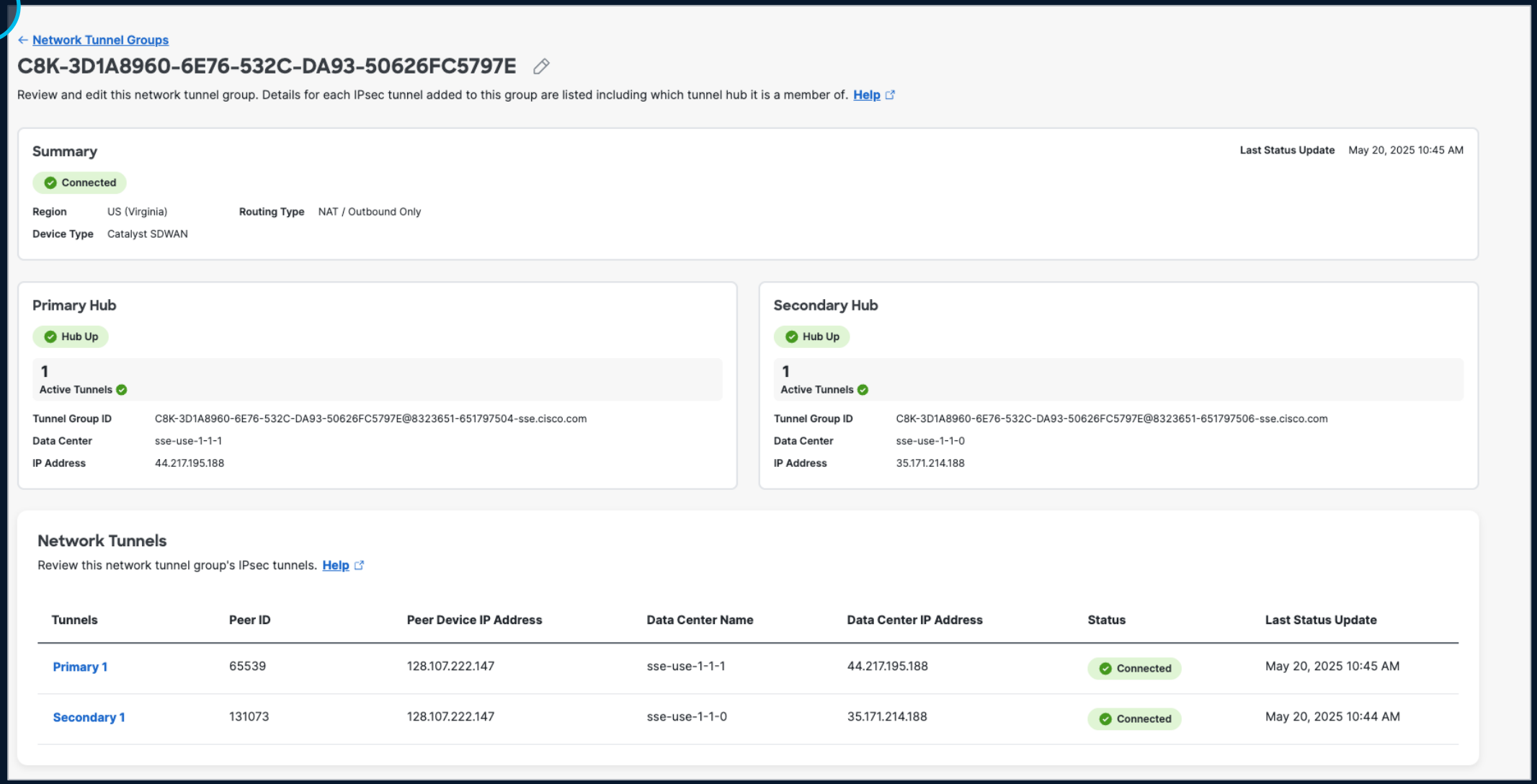
Extending SDWAN Identity Context to Secure Access

2



Extending SDWAN Identity Context to Secure Access

3



SDWAN SGT Configuration Sample

Carry SGT through the tunnels to Secure Access
interface {{interfaceName_Tunnel1}}
cts manual

!

interface {{interfaceName_Tunnel2}}
cts manual

!
Map specific traffic in the VRFs with a SGT (used when there is no ISE integration or SGT propagated from elsewhere)

cts role-based sgt-map vrf <id#> x.x.x.x sgt <#>

Wrap- Up

Additional Sessions

- Cisco Catalyst SD-WAN Start Here
- Simplifying Your SASE Implementation with Meraki SD-WAN and Cisco Secure Access to Deliver Zero Trust for the Network
- From Zero-to-Zero Trust Hero: Secure Access tips and tricks for an SSE deployment
- Zero Day, Zero Trust Troubleshooting with Secure Access: End-to-End Visibility from Client to Private App

Secure Access Trainings

- June 22-26, 2026 CST Virtual https://learningnetworkstore.cisco.com/ilt/cartland/?offeringId=7b21c6c2-37fa-11f1-88c8-aa0e2f8fbda2
- July 27-31, 2026 EST Raleigh, NC https://learningnetworkstore.cisco.com/ilt/cartland/?offeringId=4e5a6516-399c-11f1-b135-424a55f4d37d
- August 17-21, 2026 IST Virtual https://learningnetworkstore.cisco.com/ilt/cartland/?offeringId=86a0f2b1-4018-11f1-8399-e2156eb9622e
- September 14-18, 2026 CST https://learningnetworkstore.cisco.com/ilt/cartland/?offeringId=f3c1998f-3806-11f1-b96e-325abbec0450
- September 21-25, 2026 CEST Virtual https://learningnetworkstore.cisco.com/ilt/cartland/?offeringId=da44194c-4018-11f1-9092-163c28934104
- September 28-October 2, 2026 Richardson, TX https://learningnetworkstore.cisco.com/ilt/cartland/?offeringId=9a79bb44-5558-11f1-944a-e215405bf7be

Cisco SASE

Secure SD-WAN
Commercial and Enterprise

+

Secure Services Edge
Cisco Secure Access

+

Identity First
ISE + Identity Intelligence

Trusted access for people, things, and AI agents

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2027.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education

Visit the Cisco Showcase for related demos

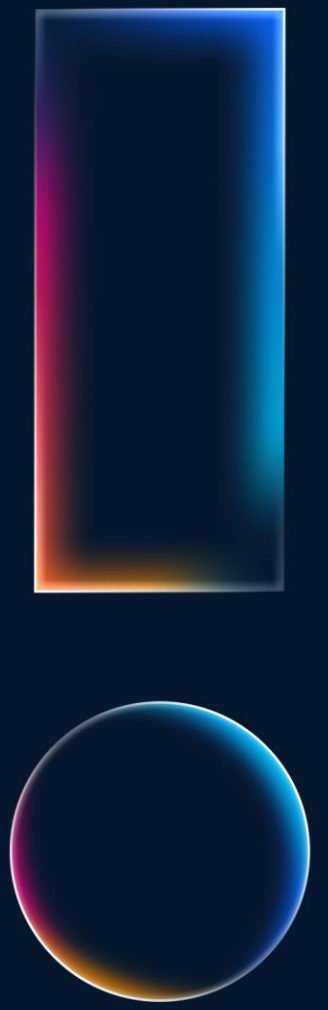
Book your one-on-one Meet the Engineer meeting

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

cisco Live !

Thank you




CISCO