

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

Fay-Ann Lee
Sr. Technical Engineer Marketing

Cisco Webex App

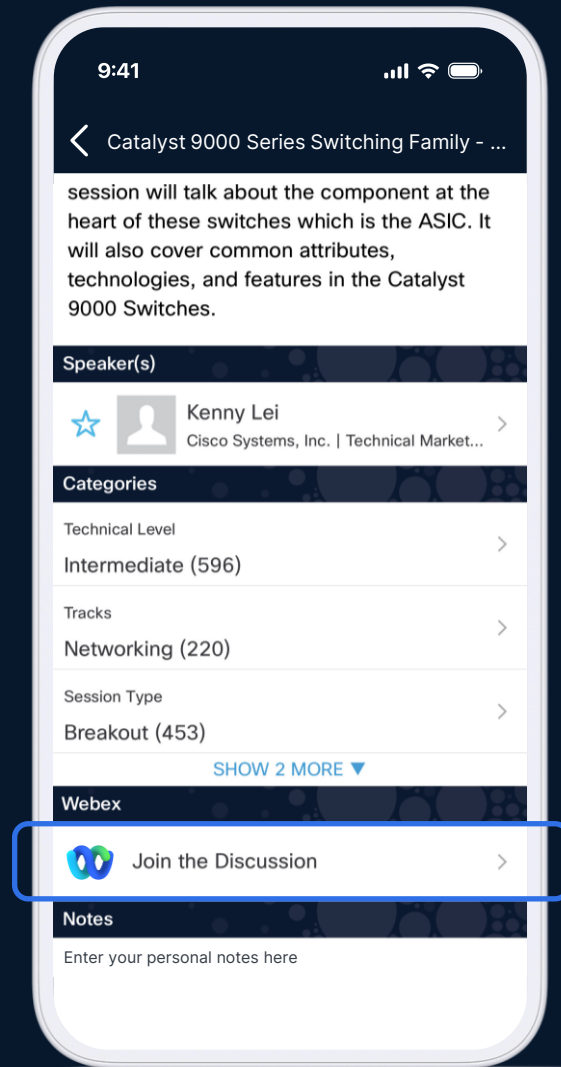
Questions?

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

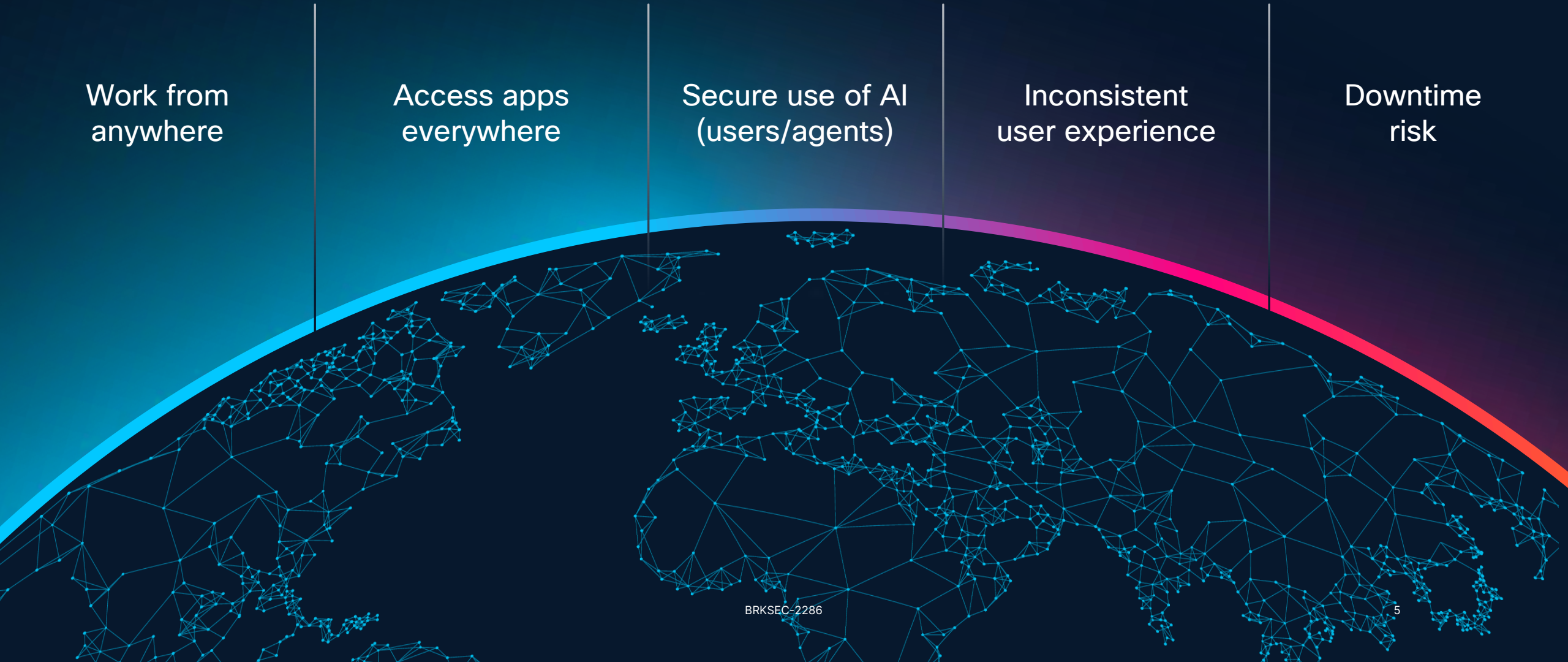
Work from
anywhere

Access apps
everywhere

Secure use of AI
(users/agents)

Inconsistent
user experience

Downtime
risk



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

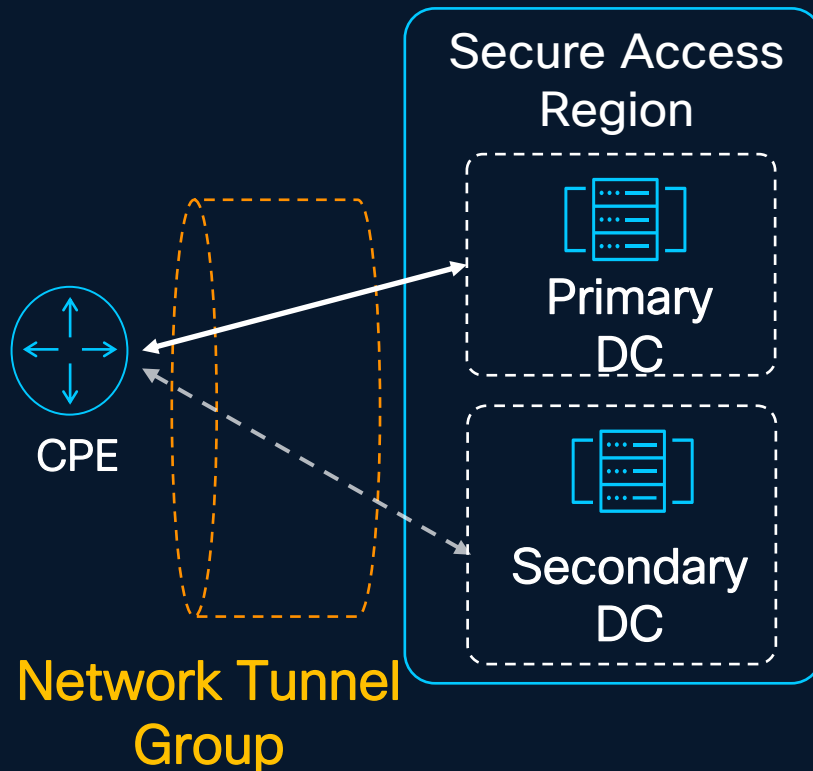
Unified observability, assurance and
troubleshooting experience powered by
AI Canvas, ThousandEyes



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:

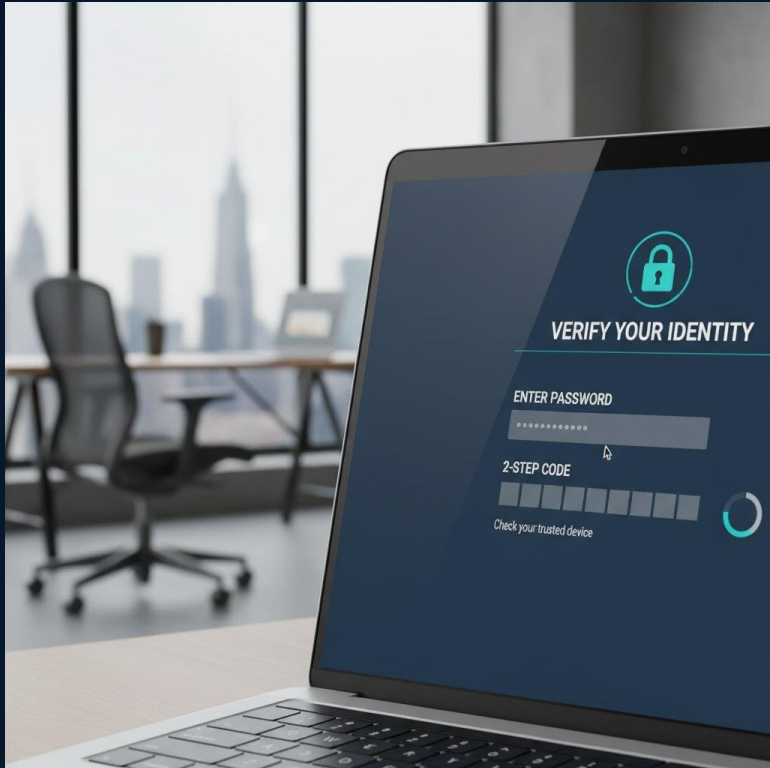
tunnel-id+<tunnel tag1>@<orgid>-628670429-sse.cisco.com
tunnel-id+<tunnel tag2>@<orgid>-628670429-sse.cisco.com
...
tunnel-id+<tunnel tag10>@<orgid>-628670429-sse.cisco.com

Secure Access IPsec headend strips off “+<tunnel tag>”

tunnel-id+~~+<tunnel tag1>~~@<orgid>-628670429-sse.cisco.com



The Evolution of Network Access Security



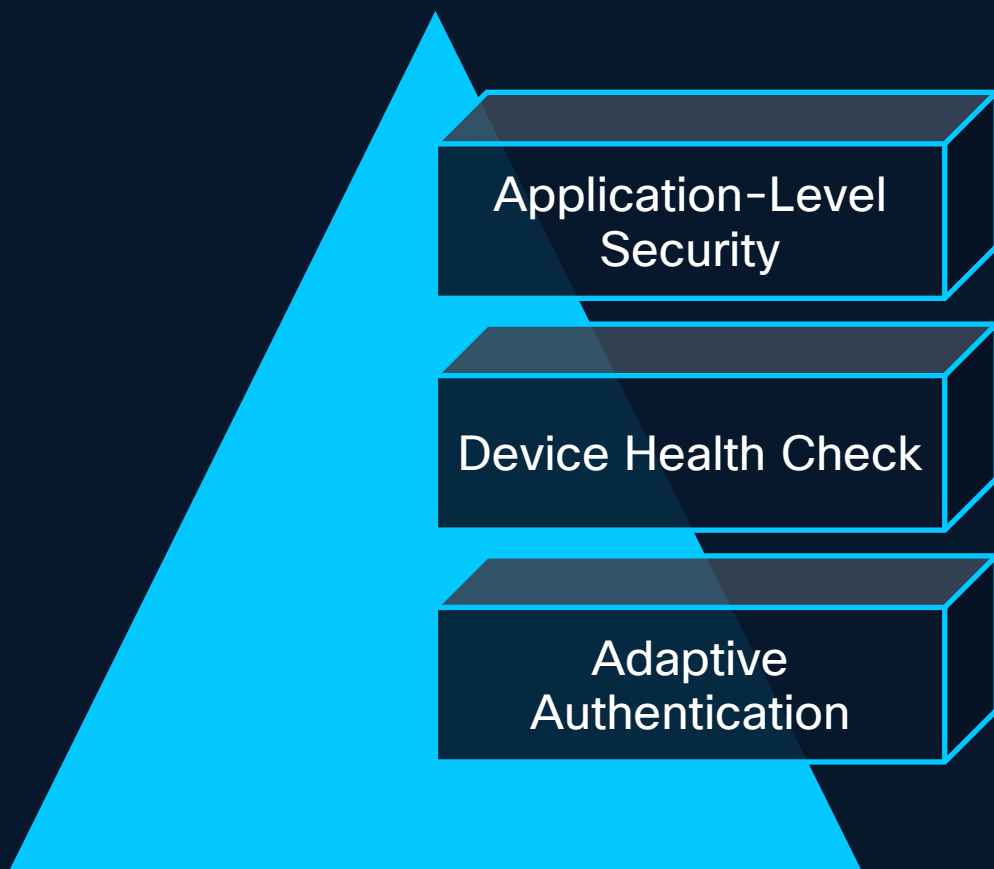
Poor Context Awareness

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.

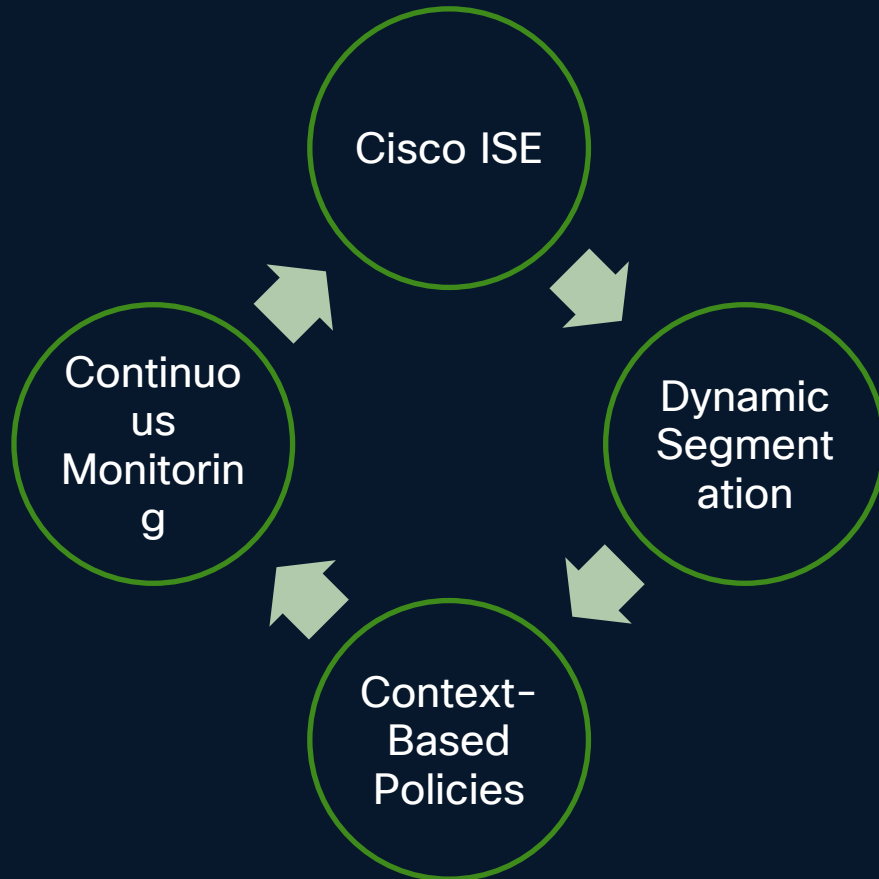
Device Health Check

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)



PrintersSGT



RobotsSGT



PhysicianSGT

Unifying Identity

Create Context-aware Identity Groups (SGTs)

Consume context from its local domain



PrintersSGT



RobotsSGT



PhysicianSGT

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

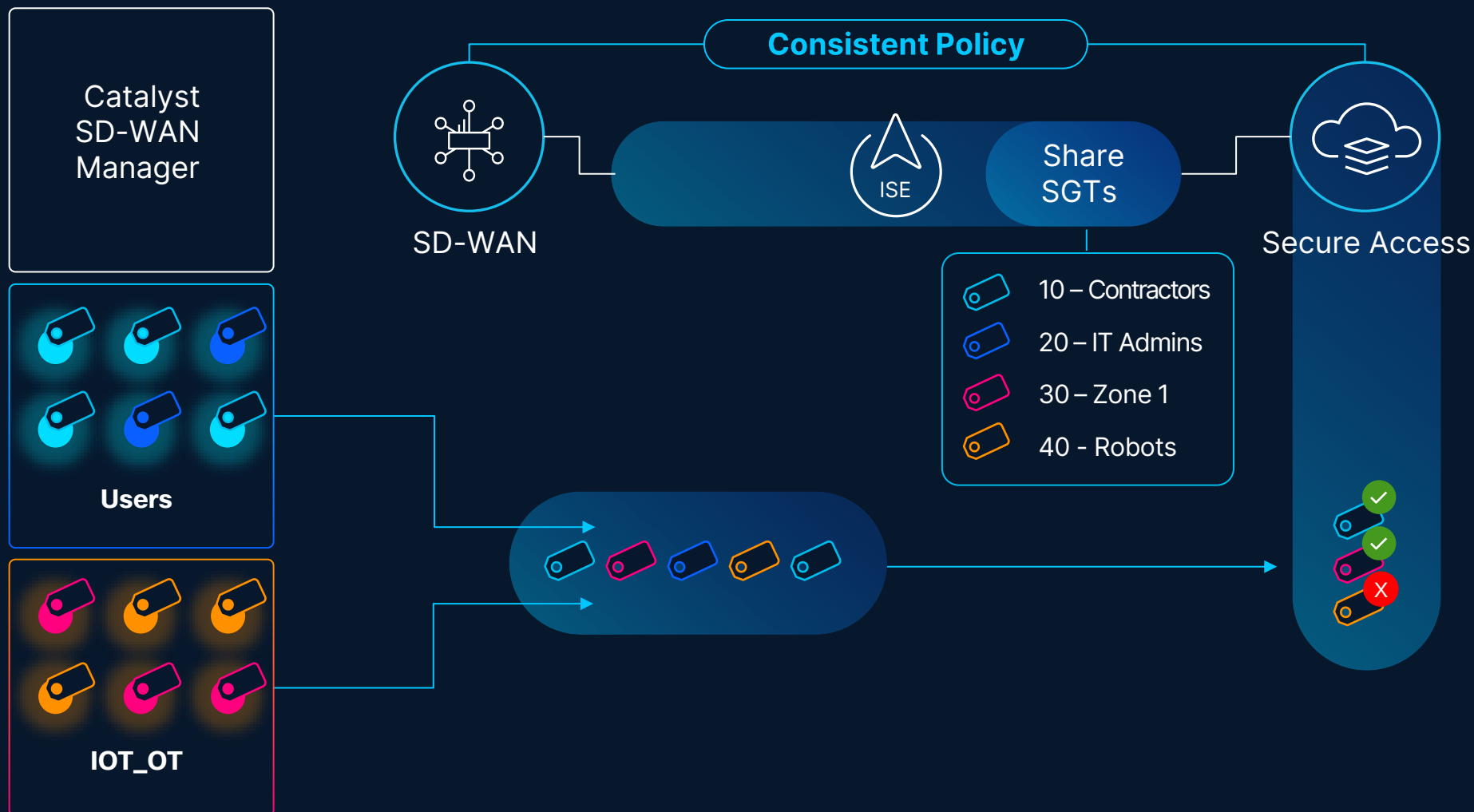
Data Center

Cloud

Identity Services Engine (ISE)

Leverage SGTs for granular access control

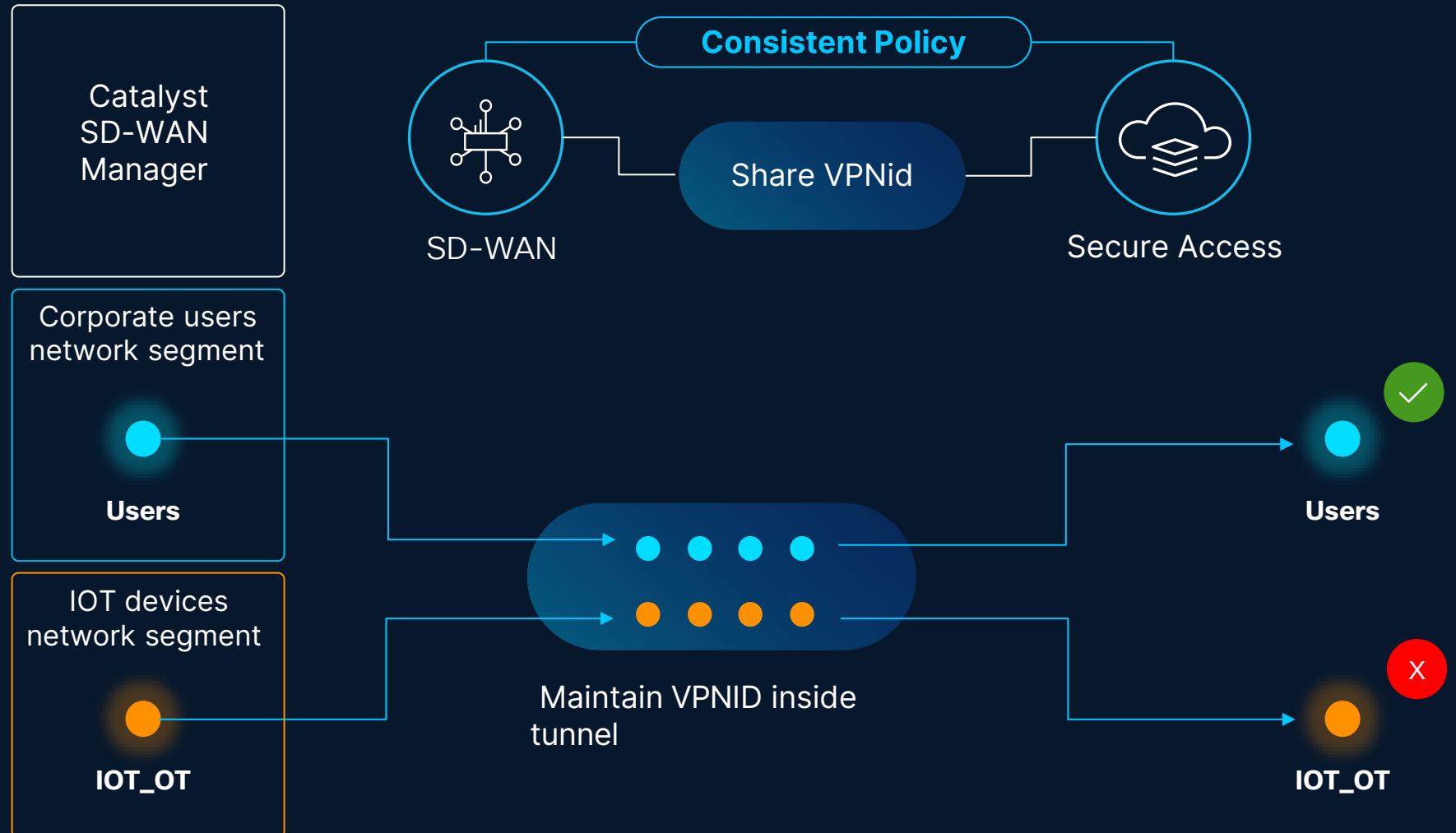
- SGT Based Policy across network & Cloud
- Maintain micro segmentation through Secure Access
- Uniquely identify devices and traffic based on context from ISE
- Apply policy to SGT Based identity



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

Generic Network Virtualization Encapsulation, VNI: 0x00104c

Version: 0

Length: 60 bytes

> Flags: 0x00

Protocol Type: IPv4 (0x0800)

Virtual Network Identifier (VNI): 0x00104c (4172)

Options: (60 bytes)

> Unknown, Class: Cisco Systems, Inc. (0x0106) Type: 0x56 (Non-critical)

> Unknown, Class: Cisco Systems, Inc. (0x0106) Type: 0x61 (Non-critical)

✓ Unknown, Class: Cisco Systems, Inc. (0x0106) Type: 0x54 (Non-critical)

Class: Cisco Systems, Inc. (0x0106)

Type: 0x54 (Non-critical)

Length: 8 bytes

Unknown Option Data: 009a0000

VPN id = 154

✓ Unknown, Class: Cisco Systems, Inc. (0x0106) Type: 0x53 (Non-critical)

Class: Cisco Systems, Inc. (0x0106)

Type: 0x53 (Non-critical)

Length: 8 bytes

Unknown Option Data: 001c0000

SGT = 28



Packet Format

```

+++++
|ethernet|  IP  |  UDP  |  ESP  | sdwan label | mdata |  IP  |  ...

```

Carrying VPN ID

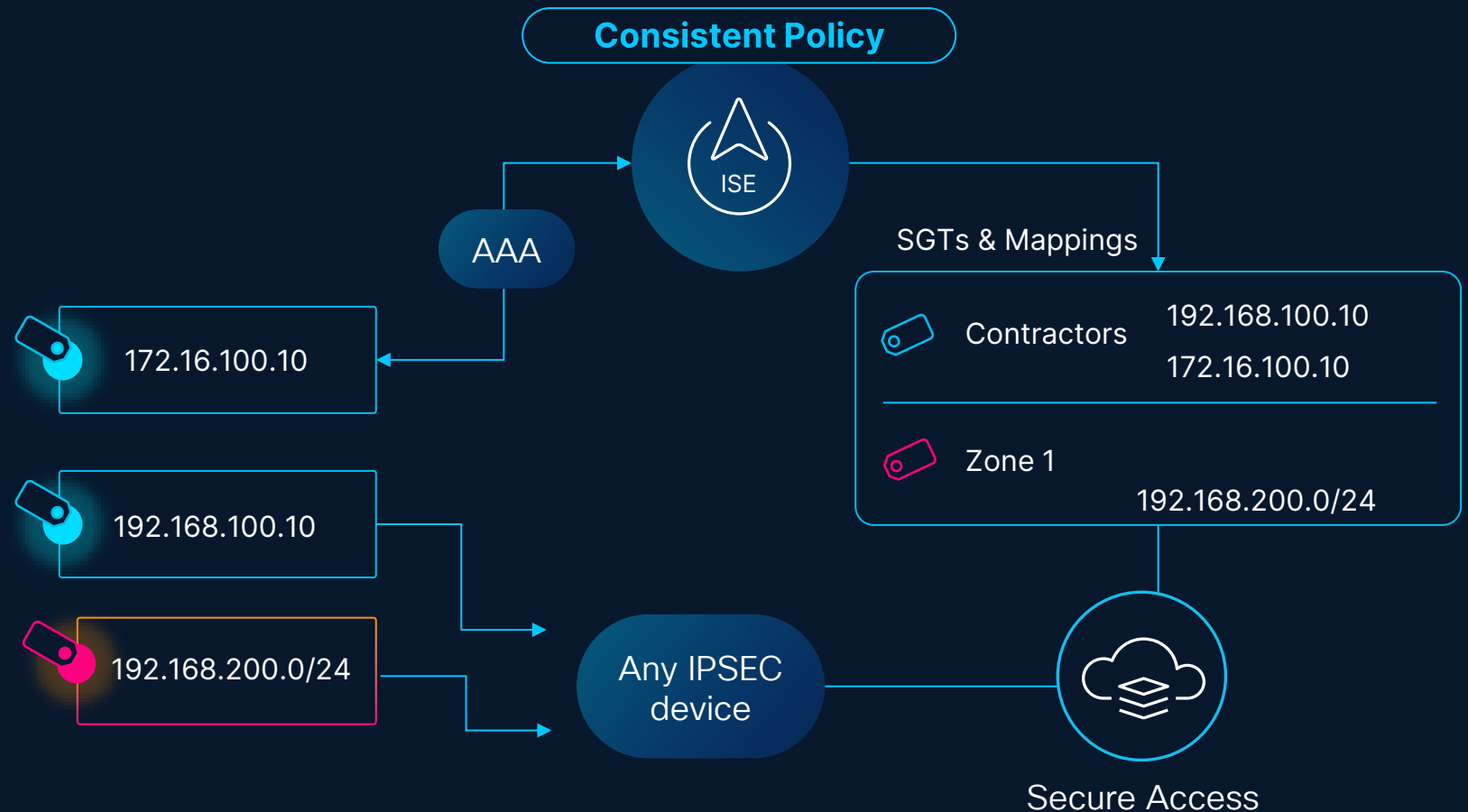
0	Type (0xc)	VPN ID
---	------------	--------

Carrying SGT

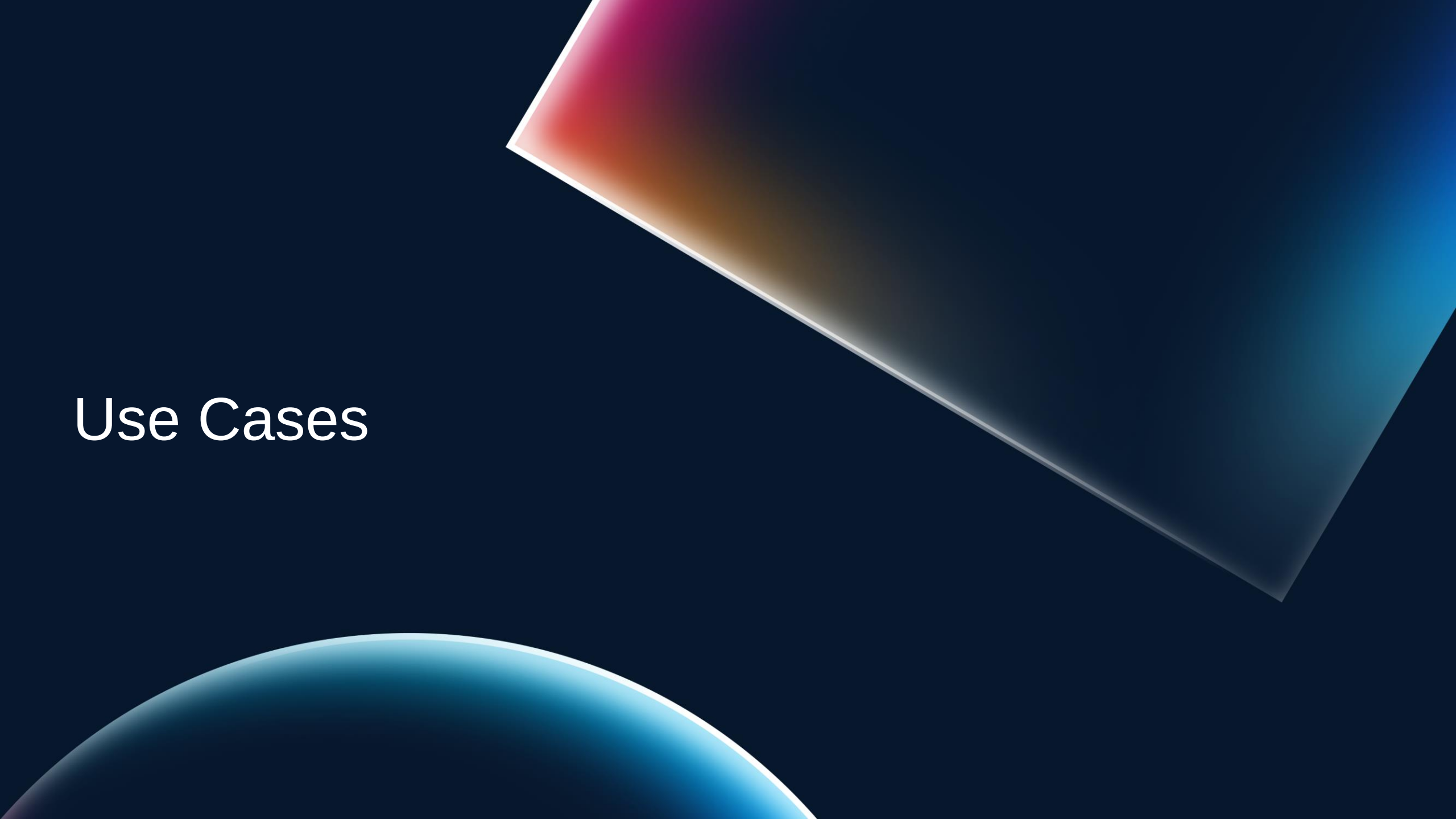
0	Type (1)	SGT Tag
---	----------	---------

Common context awareness from network to cloud

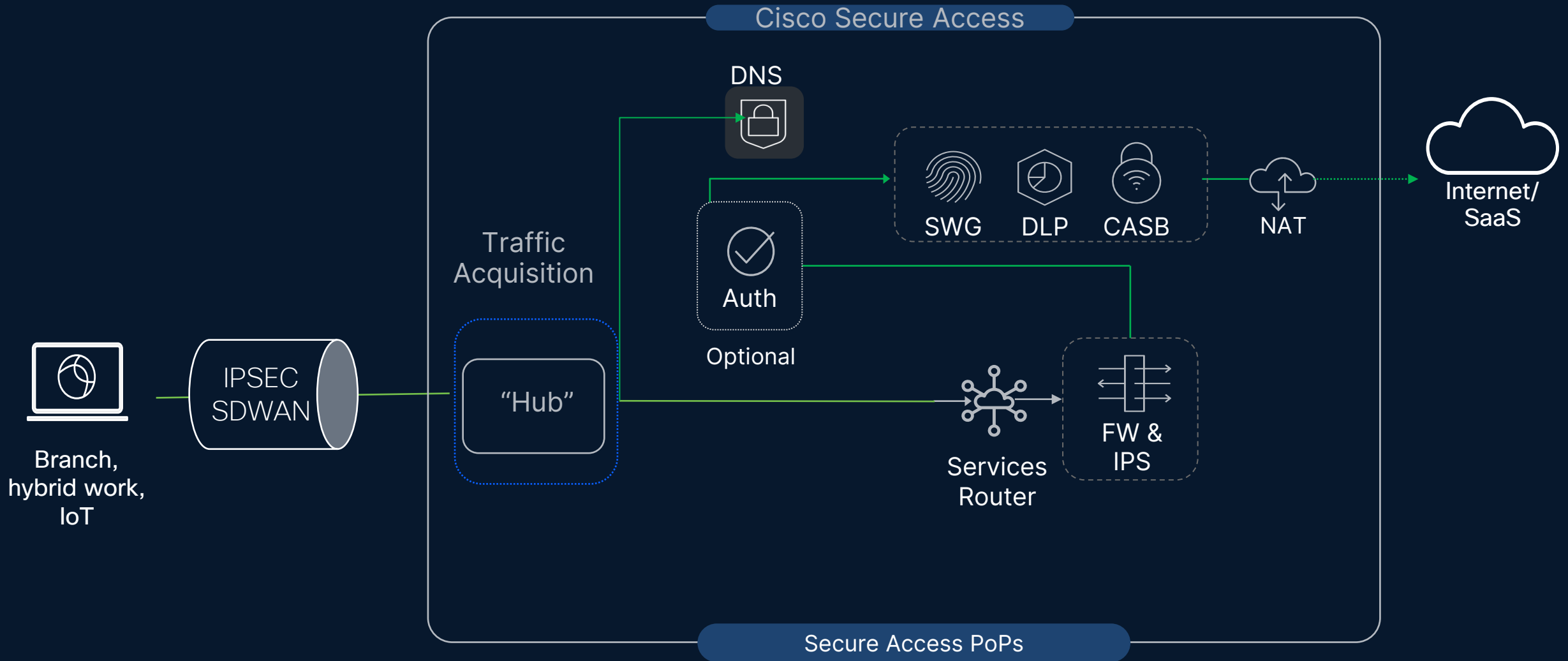
- SGT Based Policy across network & Cloud
- Maintain micro segmentation through Secure Access
- Uniquely identify devices and traffic based on context from ISE
- Apply policy to SGT Based identity



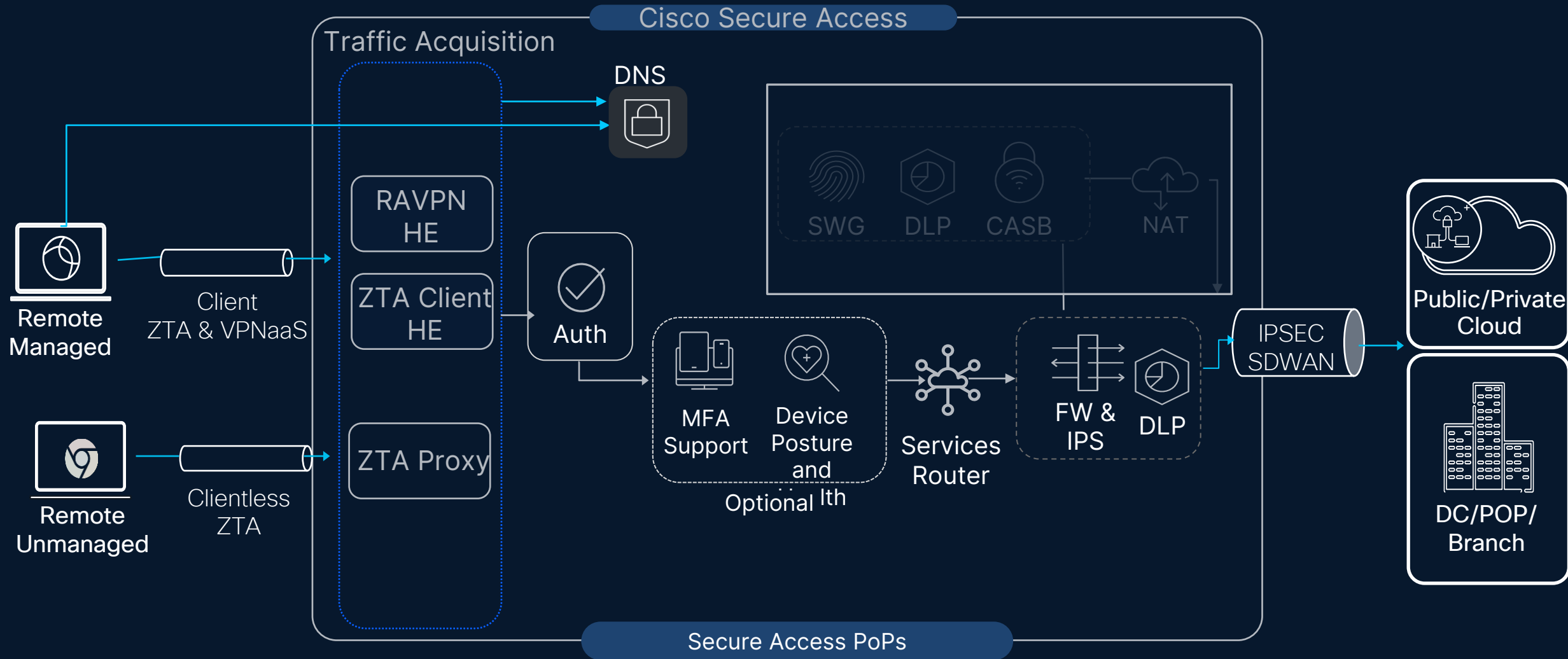
Use Cases



Secure Internet Access (SIA)

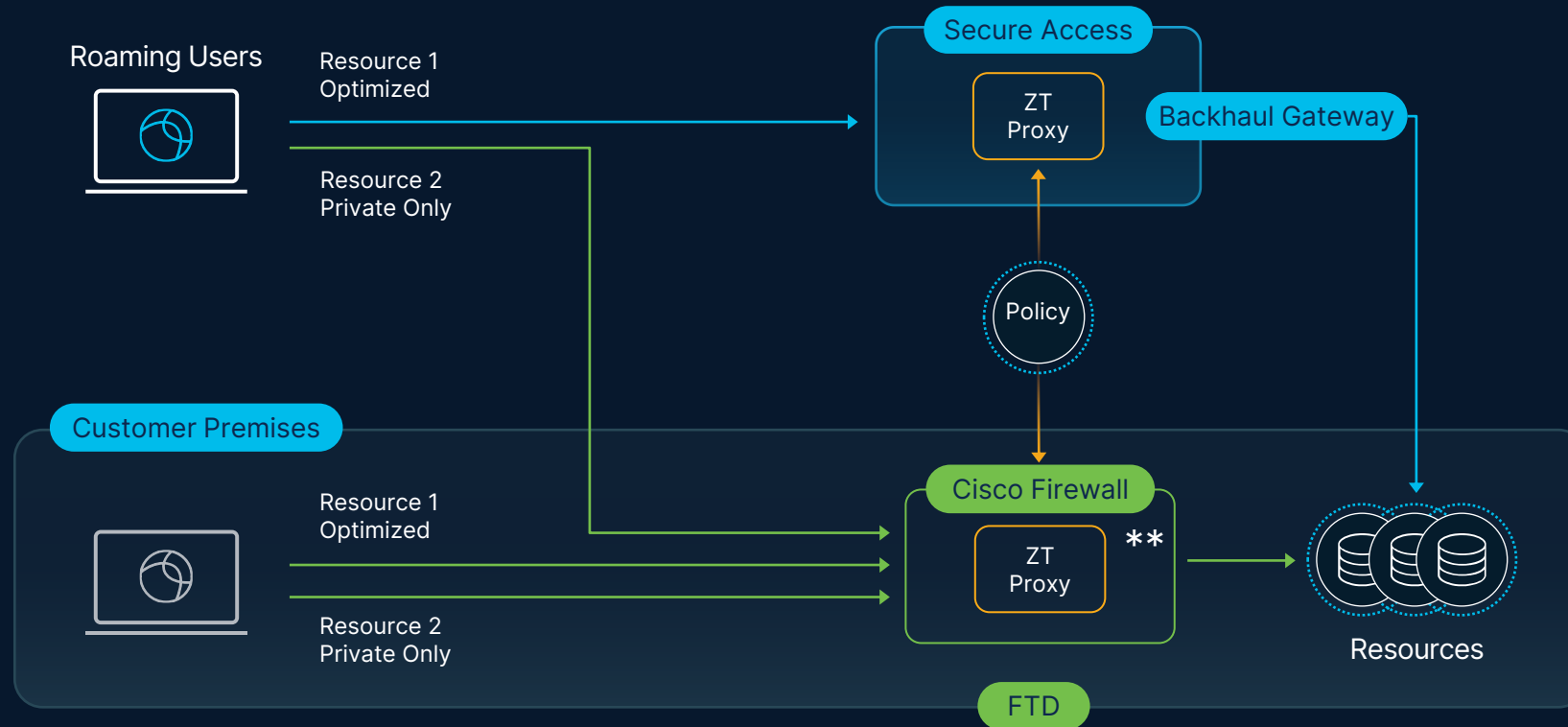


Secure Private Access (SPA)



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

Cisco SASE

Secure Access

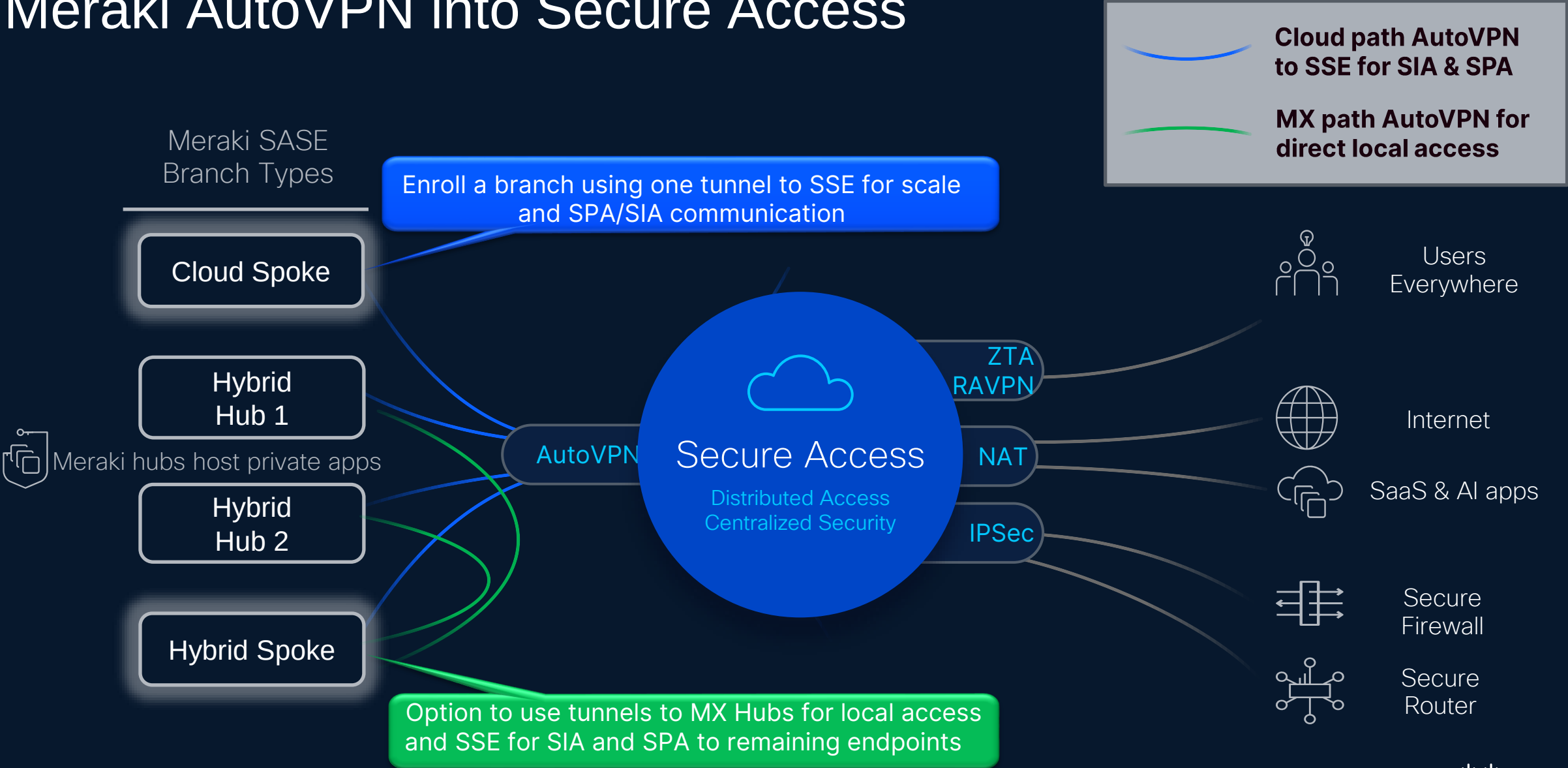
Meraki SD-WAN

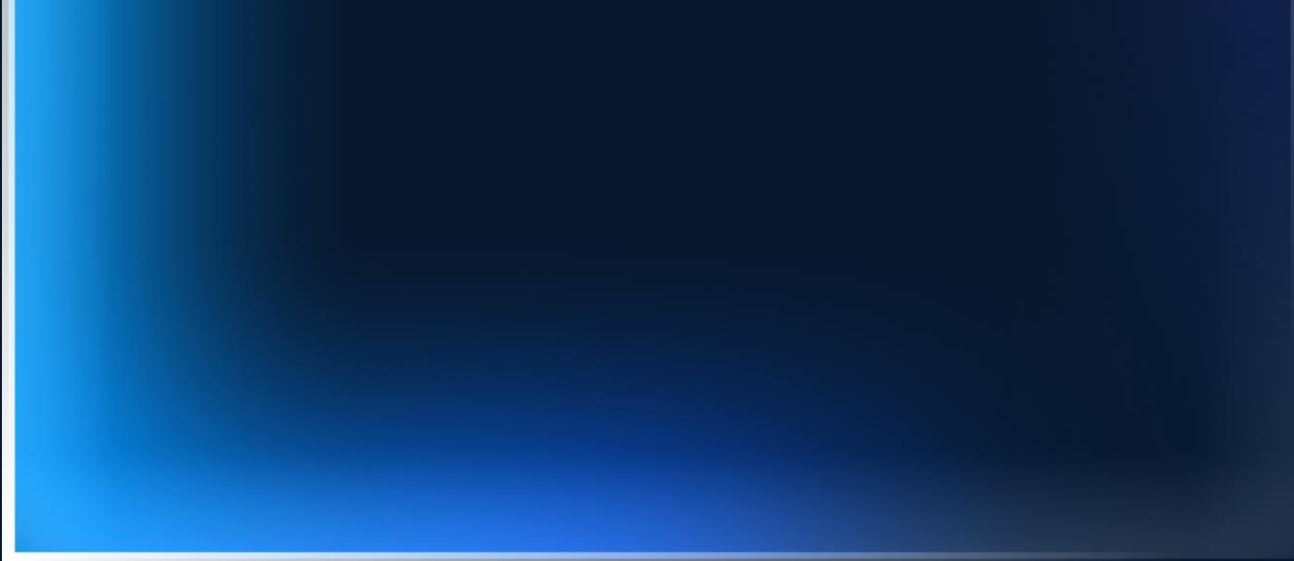
Catalyst SD-WAN

FTD SD-WAN

Mix and Match Components | Single Policy | Flexible Enforcement

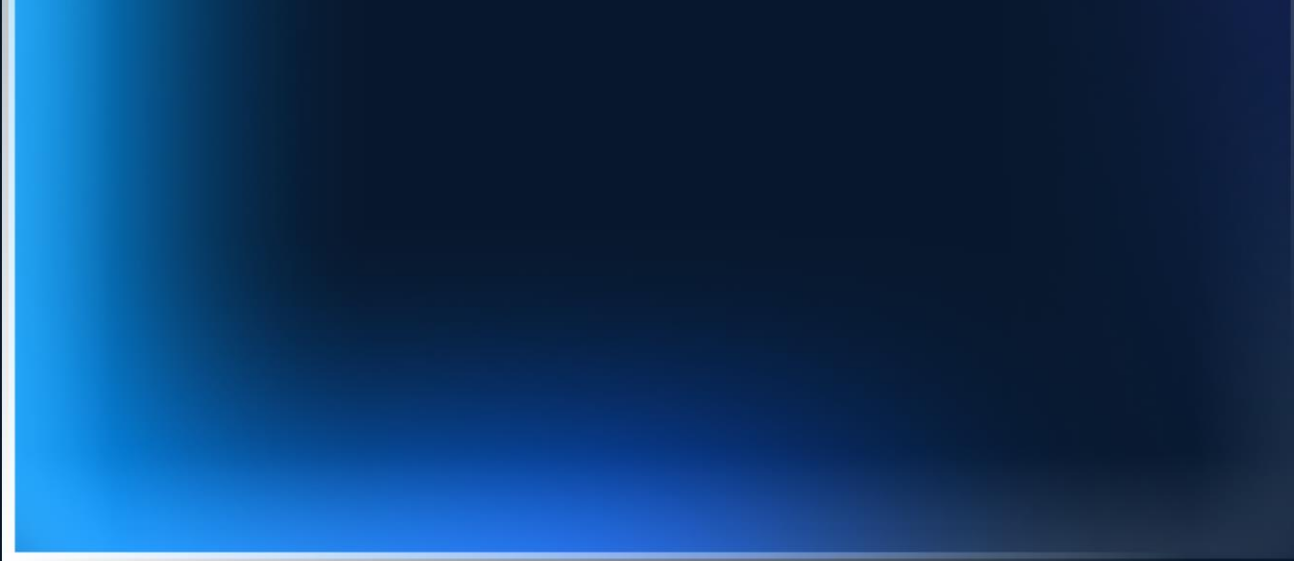
Meraki AutoVPN into Secure Access





Cisco SASE with Meraki





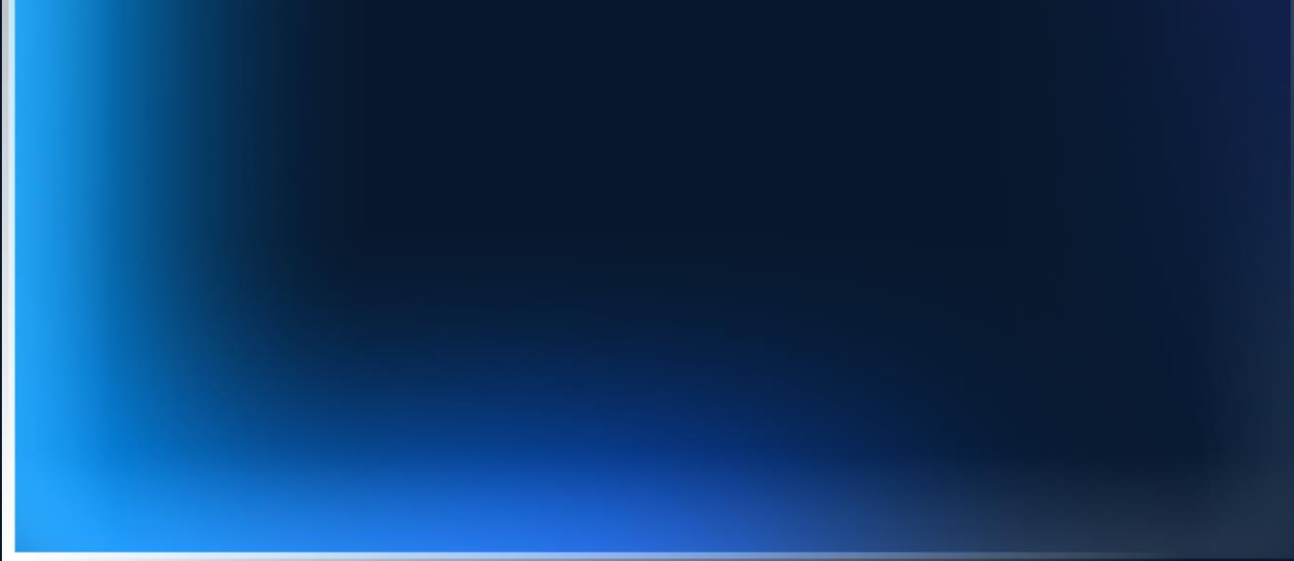
SDWAN integration with LAN switches and access points



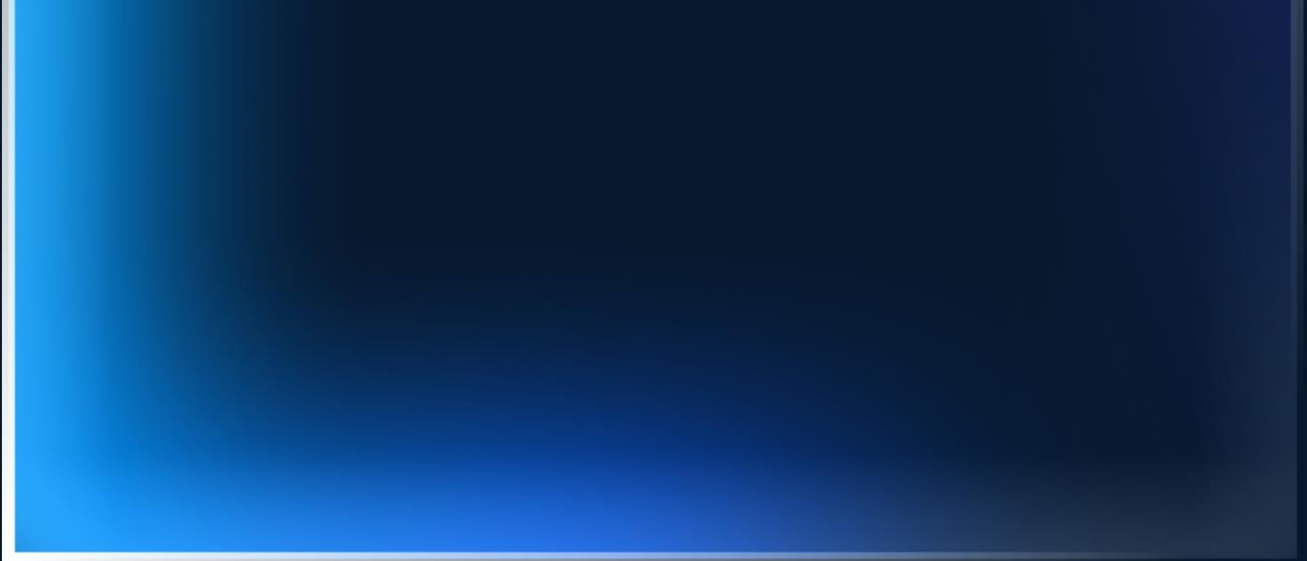
Secure Firewall into Secure Access

- 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

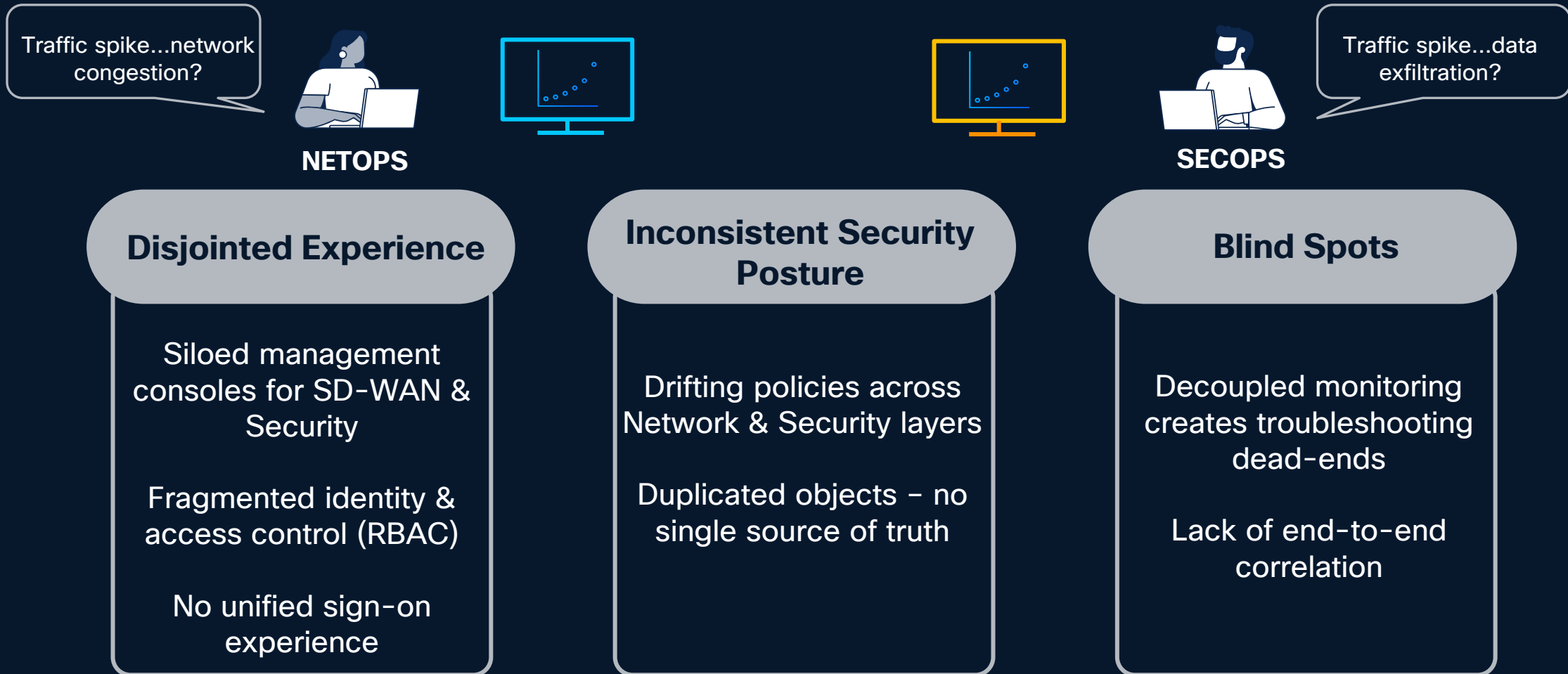


Cisco SASE with Catalyst



The high cost of fragmented operations

Challenges of managing SASE



Rich, centralized management for SecOps

Security Cloud Control

SSO

Security policy

Monitoring

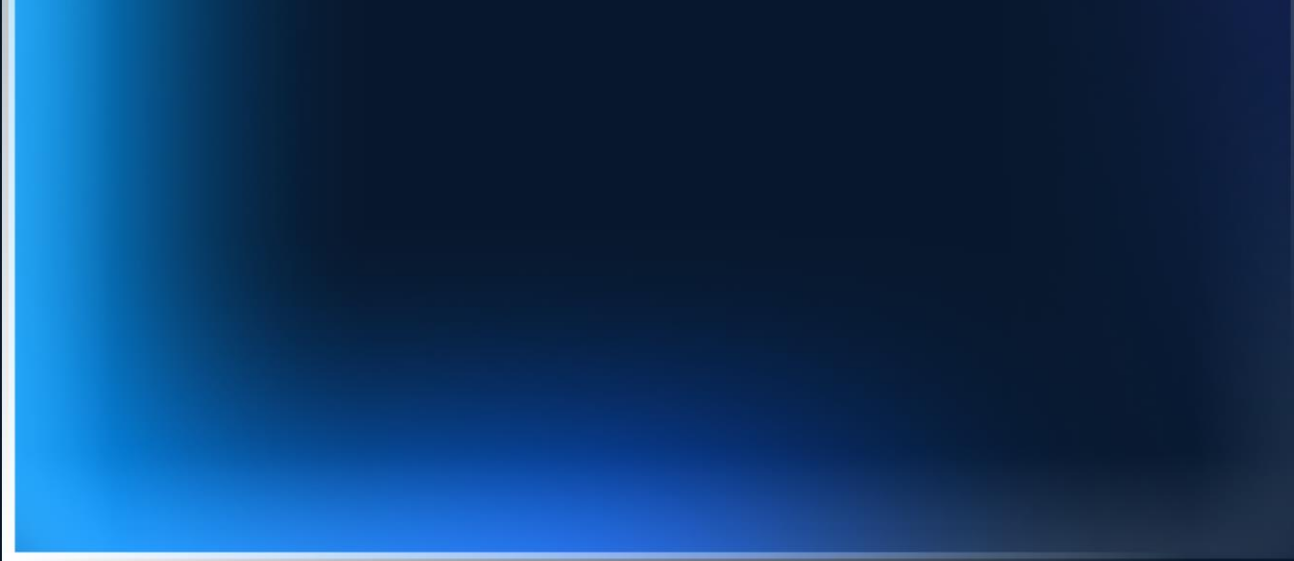
Troubleshooting

**SD-WAN
Manager**

**Firewall
Management
Console**

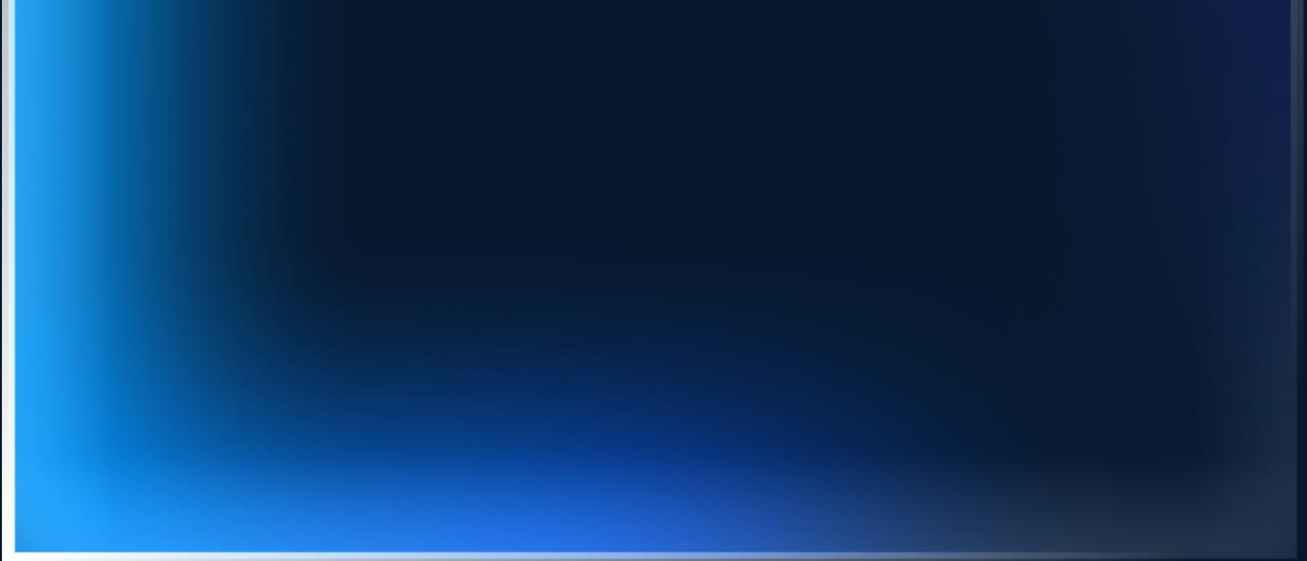
**Multicloud
Defense**

**Secure
Access**



SASE with Catalyst SD-WAN Demo



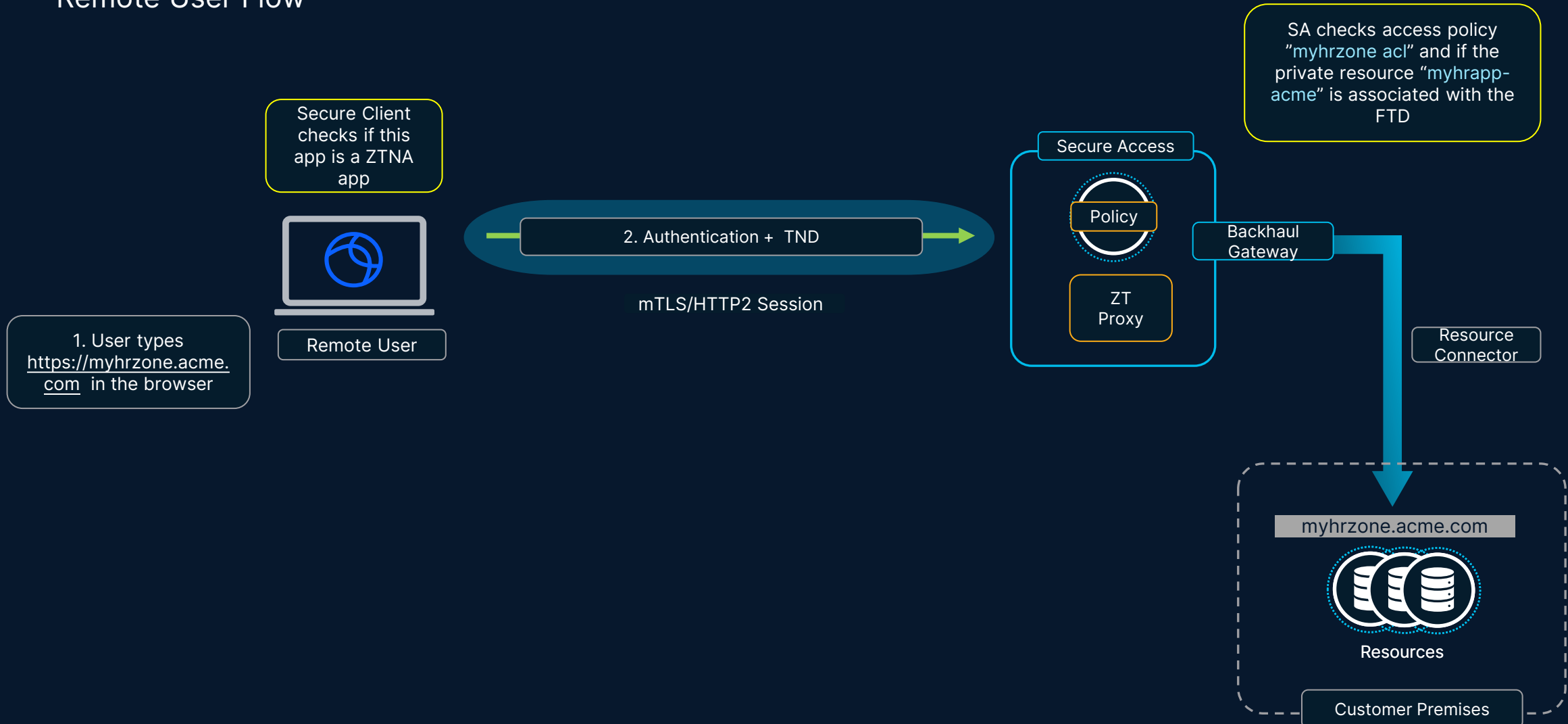


Cisco Hybrid Private Access with Firepower Threat Defense



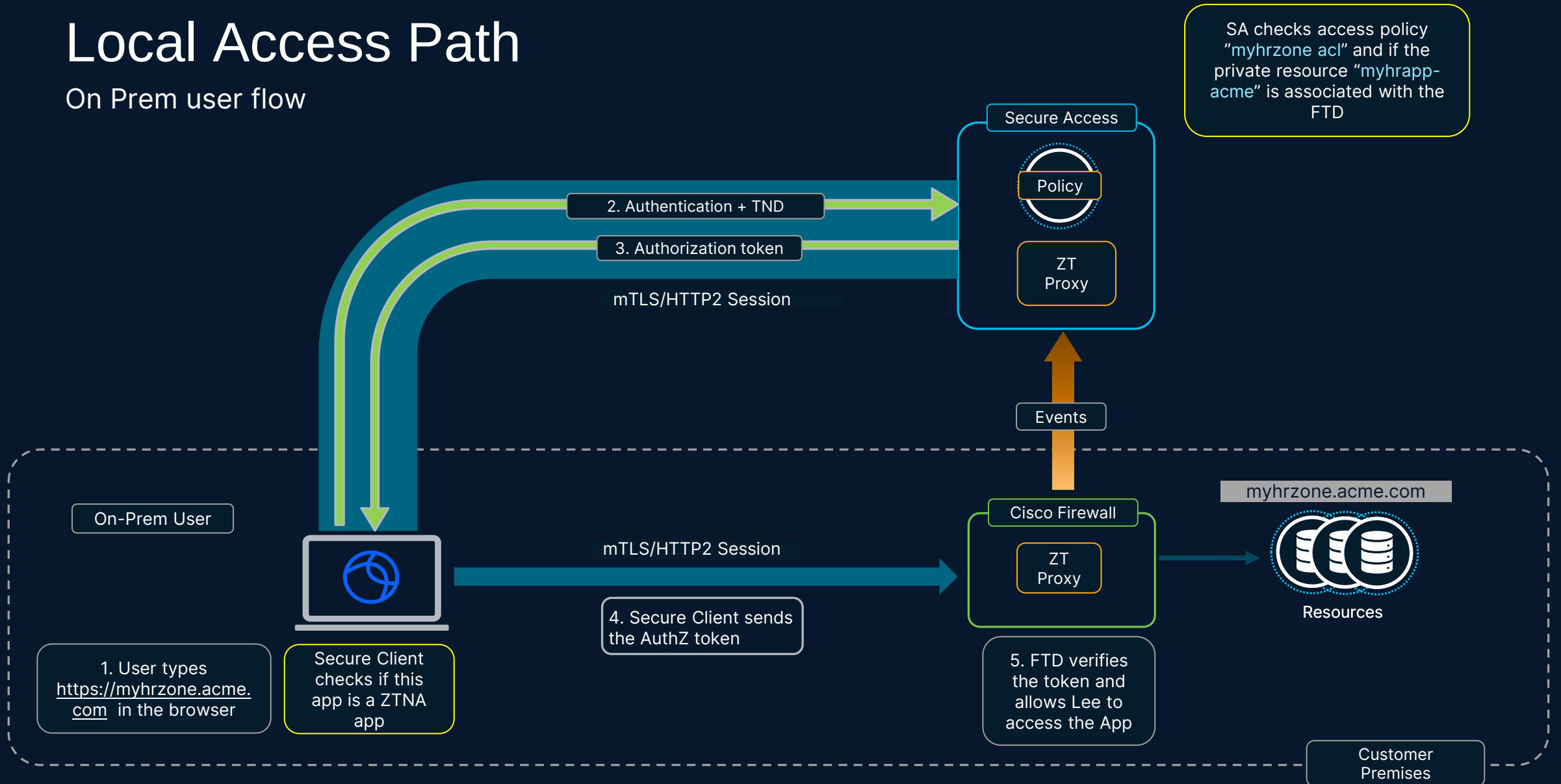
Cloud Access Path

Remote User Flow

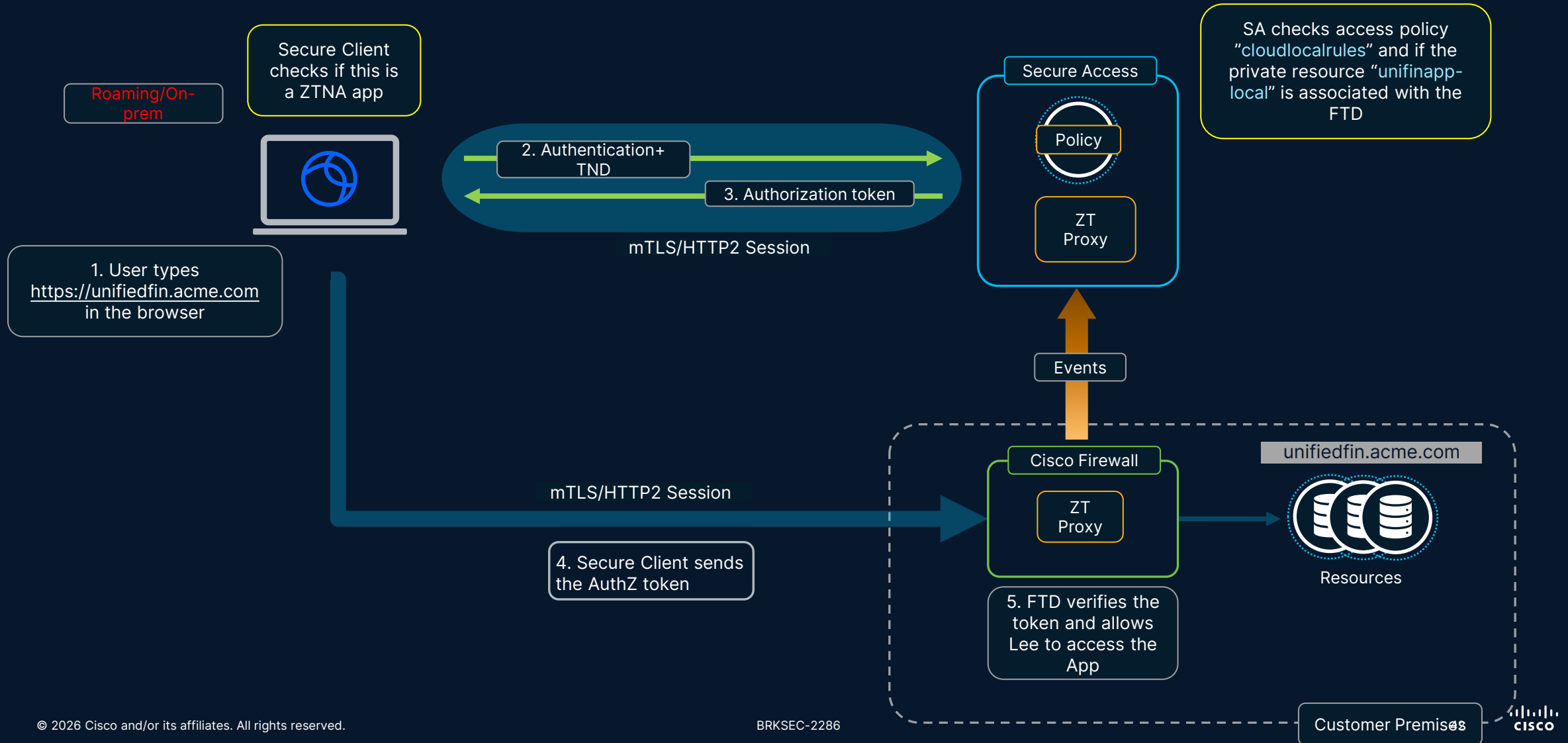


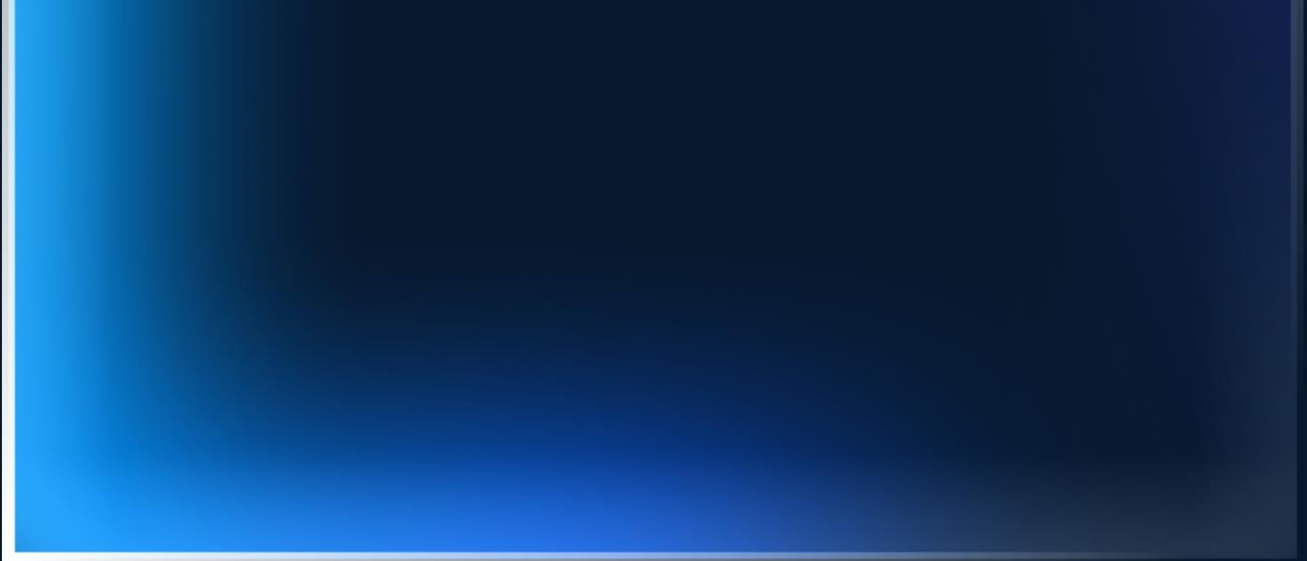
Local Access Path

On Prem user flow



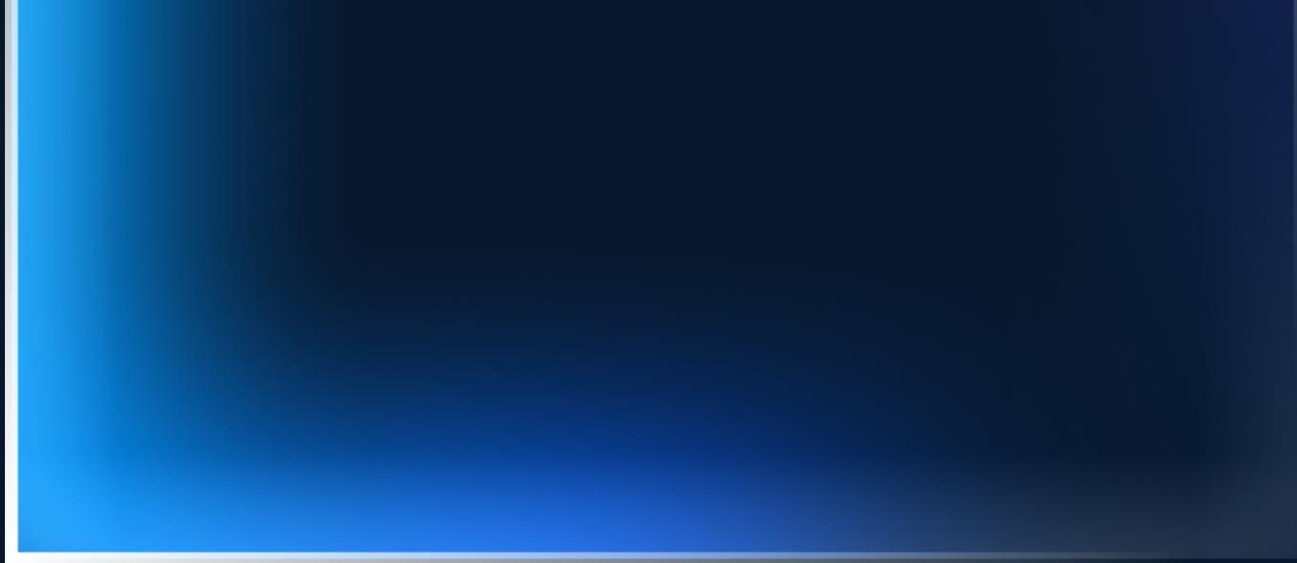
Something





Hybrid Private Access Demo





Configuration



Sharing Context-Aware Identity to Secure Access

1

2

3

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The main navigation menu on the left is highlighted with a blue circle and the number 1. The top navigation bar is highlighted with a blue circle and the number 2. The Integrations section content is highlighted with a blue circle and the number 3.

Integrations

Secure Access supports the integration of various Cisco solutions, which allow you to enhance Secure Access network management and security. [Help](#)

My Integrations Integration Hub

My Integrations 1

Search Integration Type 1 module As of: May 30, 2025, 5:00 PM [Add Integration Module](#)

Module name	Integration	Created	Status
SGTDemosISE2Connector	Identity Service Engine (ISE)	May 14, 2025 by faylee@cisco.com	...

Rows per page 10 < 1 >

1 Sharing Context-Aware Identity to Secure Access

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Help. The top navigation bar includes tabs for Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, Admin Access, and Settings. The main content area shows the pxGrid configuration page. It features a toggle switch for 'Administration' (enabled), a toggle for 'Monitoring' (disabled), and a toggle for 'Policy Service' (disabled). The 'pxGrid' section is expanded, showing a toggle for 'Enable pxGrid Cloud' (checked). Below this, a message states: 'To enable pxGrid Cloud application, please go to the [Integration Catalog](#).' A table displays the configuration details:

Cisco DNA Portal account	Status
SecureAccessTME	Connected
ISE deployment name	Registered region
ISEContextSharing	us-west-2
Description	Mode
--	Active

A red 'Deregister' button is located at the bottom of the configuration section.

Sharing Context-Aware Identity to Secure Access

2

The screenshot displays the Cisco Secure Access web interface. The top navigation bar includes the Cisco logo, the text 'Secure Access', and user information 'Fay Ann Lee'. A left-hand sidebar contains navigation icons for Home, Experience Insights, Connect, Resources, Secure, Monitor, Admin (highlighted), and Workflows. The main content area is titled 'Integrations' and includes a sub-header 'Cisco Identity Services Engine – Security Group Tag (SGT) Integration'. Below this, a paragraph explains that the integration streamlines the deployment of Security Group Tags (SGTs) for dynamic network segmentation. The workflow is presented in three sequential steps, each with a title, icon, and a list of required actions:

- Configure Cisco Identity Services Engine**
 - In ISE you must:
 - 1 Enable PxGrid.
 - 2 Select the PxGrid Services for your integration.
 - 3 Connect ISE and PxGrid Cloud.
- Configure DNA Portal**
 - In DNA Portal you must:
 - 1 Register an ISE module.
 - 2 Generate a One-Time Password (OTP).
 - 3 Activate Firewall Management Center.
- Configure Secure Access**
 - In Secure Access you must:
 - 1 Connect ISE instance using the OTP.
 - 2 Click save to connect the integration.

An 'Integrate' button is located at the bottom right of the workflow area.

Sharing Context-Aware Identity to Secure Access

3

 Secure Access

 Fay-Ann Lee

☰

Home

Experience Insights

Connect

Resources

Secure

Monitor

Integrations

Secure Access supports the integration of various Cisco solutions, which allow you to enhance Secure Access network management and security. [Help](#)

My Integrations

Integration Hub

My Integrations 1

Integration Type

▼

1 module

As of: May 30, 2025, 5:00 PM 

Add Integration Module

Module name	Integration	Created	Status
SGTDemosISE2Connector	 Identity Service Engine (ISE)	May 14, 2025 by faylee@cisco.com	

Rows per page

10 ▼

 <

1

 >

© 2026 Cisco and/or its affiliates. All rights reserved.

BRKSEC-2286

48



Leveraging SGTs in Cloud based policy enforcement

The screenshot displays the Cisco Secure Access interface. On the left, a sidebar menu includes options like Home, Experience Insights, Connect, Resources, Secure, Monitor, Admin, and Workflows. The main content area is divided into two sections. The top section, titled 'Security Group Tags', shows a list of tags with columns for Rule name, Rule order, and a search bar. The bottom section, titled 'Activity Search', displays a table of activity results. The table has columns for Request, Source, Rule Identity, Destination IP, Destination Country, Internal IP, External IP, Action, and Category. The 'Source' column is highlighted in pink, showing the value '*IOT_OT (VPN-154)'. The 'Action' column shows 'Allowed'. The 'Event Details' panel on the right shows the 'Source' as '*IOT_OT (VPN-154)' and 'Cell1 (SGT-28)'. The 'Source IP' is 192.168.25.3 and the 'Destination IP' is 108.139.3.127. The interface also includes a 'Filters' section with a search bar and a 'Save Search' button.

1

2

3

Activity Search

Filters

Search by domain, identity, or URL

Advanced

CLEAR

Saved Searches

Customize Columns

All

SAVE SEARCH

1,304,977 Total

Viewing activity from May 1, 2025 12:00 AM to May 30, 2025 10:03 PM

Page: 1

Results per page: 50

1 - 50

Event Details

Action

Allowed

Time

May 30, 2025 10:03 PM

Rule Name

IOT branch (952085)

Source

*IOT_OT (VPN-154)

Cell1 (SGT-28)

Source IP

192.168.25.3

Destination IP

108.139.3.127

Leveraging SGTs in Cloud based policy enforcement

1

 Secure Access

 Fay Ann Lee

☰

Home

Experience Insights

Connect

Resources

Secure

Monitor

Admin

Workflows

Security Group Tags

Security Group Tags (SGT) specify the privileges of a traffic source within a trusted network. When you enable an Identity Services Engine integration, SGTs become available for use in access rules. [Help](#)

29 total

As of: Sep 25, 2024, 09:13 AM

Name	Tag
ANY	65535
AP_EMR_EPG	503
AP_Services_EPG	501
AP_Test_EPG	502
Auditors	9
BYOD	15
Cameras	24
Contractors	5
Developers	8
Development_Servers	12

Rows per page 10 < 1 2 3 >

Leveraging SGTs in Cloud based policy enforcement

2

Rule name

VideoEquipmentAccess

Rule order

15

1

Specify Access

Specify which users and endpoints can access which resources. [Help](#)

Action

✓

Allow

Allow specified traffic if security requirements are met.

✗

Block

Block specified traffic.

From

Specify one or more **sources**.

Select sources

Add a source

Source > Security Group Tags

☐ BYOD (15)

☐ Cameras (24)

☐ Contractors (5)

☐ Developers (8)

To

Specify one or more **destinations**.

Select destinations

Add a destination

Private Resources 5 >

Private Resource Groups 2 >

Save

Leveraging SGTs in Cloud based policy enforcement

3

Secure Access

Fay-Ann Lee

Activity Search

Schedule

Export CSV

LAST 30 DAYS

Home

Experience Insights

Connect

Resources

Secure

Monitor

Admin

FILTERS

Search by domain, identity, or URL

Advanced

CLEAR

Saved Searches

Customize Columns

All

SAVE SEARCH

IDENTITY TYPE

Security Group Tags

Search filters

Response

Select All

☐

☒ Allowed

☒ Blocked

Warn Page Behavior

Select All

☐

☐ Warned

☐ Accessed After Warn

Isolate

☐ Isolated

IPS Signature

Select All

1,304,977 Total

Viewing activity from May 1, 2025 12:00 AM to May 30, 2025 10:03 PM

Page: 1

Results per page: 50

1 - 50

Request	Source	Rule Identity	Destination IP	Destination Country	Internal IP	External IP	Action	Category
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	108.139.3.127	United States	192.168.25.3		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	108.139.3.127	United States	192.168.25.3		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	151.101.195.5	United States	192.168.25.2		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	151.101.195.5	United States	192.168.25.2		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	108.139.3.127	United States	192.168.25.3		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	108.139.3.127	United States	192.168.25.3		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	151.101.195.5	United States	192.168.25.2		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	151.101.195.5	United States	192.168.25.2		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	108.139.3.127	United States	192.168.25.3		Allowed	Uncat

Event Details

Action

Allowed

Time

May 30, 2025 10:03 PM

Rule Name

IOT branch (952085)

Source

*IOT_OT (VPN-154)

Cell1 (SGT-28)

Source IP

192.168.25.3

Destination IP

108.139.3.127

Extending SDWAN Identity Context to Secure Access

1

2

3

Catalyst SD-WAN

Monitor

Configuration

Analytics

Workflows

Tools

Reports

Maintenance

Administration

SSE Provider

Cisco Secure Access

Context Sharing

VPN

Tracker

Configuration

Region

Source IP address

Name

Interface Name

ipsec10

ipsec10

Network Tunnel Groups

C8K-3D1A8960-6E76-532C-DA93-50626FC5797E

Review and edit this network tunnel group. Details for each IPsec tunnel added to this group are listed including which tunnel hub it is a member of.

Summary

Connected

RegionUS (Virginia)

Routing TypeNAT / Outbound Only

Device TypeCatalyst SDWAN

Last Status UpdateMay 20, 2025 10:45 AM

Primary Hub

Hub Up

1 Active Tunnels

Tunnel Group ID

Data Center

IP Address

C8K-3D1A8960-6E76-532C-DA93-50626FC5797E@8323651-651797504-sse.cisco.com

sse-use-1-1-1

44.217.195.188

Secondary Hub

Hub Up

1 Active Tunnels

Tunnel Group ID

Data Center

IP Address

C8K-3D1A8960-6E76-532C-DA93-50626FC5797E@8323651-651797506-sse.cisco.com

sse-use-1-1-0

35.171.214.188

Network Tunnels

Review this network tunnel group's IPsec tunnels.

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update
Primary 1	65539	128.107.222.147	sse-use-1-1-1	44.217.195.188	Connected	May 20, 2025 10:45 AM
Secondary 1	131073	128.107.222.147	sse-use-1-1-0	35.171.214.188	Connected	May 20, 2025 10:44 AM

Extending SDWAN Identity Context to Secure Access

The screenshot displays the Cisco Catalyst SD-WAN web interface. The left sidebar contains navigation links: Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, and Administration. The main content area is titled 'Settings' and includes a search bar. Under the 'Settings / External Services' section, the 'Cloud Credentials' tab is active. It features two sub-sections: 'Cloud Provider Credentials' and 'Umbrella DNS Certificate'. The 'Cloud Provider Credentials' section includes a description, a toggle for 'Umbrella' (which is off), and a highlighted area containing a 'Cisco SSE' toggle (on), an 'Organization Id' field (8323651), an 'Api Key' field (6a58188199504b9b83bc4441bcf03bf5), a 'Secret' field, and a 'Context Sharing' toggle (on).

2 Extending SDWAN Identity Context to Secure Access

The screenshot displays the Cisco Catalyst SD-WAN configuration interface. The left sidebar contains navigation icons for Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, Administration, and Explore. The main content area is titled 'Catalyst SD-WAN' and includes a top navigation bar with icons for search, menu, help, notifications (99+), and user profile.

SSE Provider

☒ Cisco Secure Access ☐ Zscaler

Context Sharing

☒ VPN ☒ SGT

Tracker

Source IP address

Name	Threshold	Interval	Multiplier	API URL Of Endpoint	Action
Tracker	300	60	3	http://www.cisco.com	

Configuration

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec101		false		1400	
ipsec102		false		1400	

Region

Extending SDWAN Identity Context to Secure Access

3

[← Network Tunnel Groups](#)

C8K-3D1A8960-6E76-532C-DA93-50626FC5797E 

Review and edit this network tunnel group. Details for each IPsec tunnel added to this group are listed including which tunnel hub it is a member of. [Help](#) 

Summary

Last Status Update May 20, 2025 10:45 AM

 Connected

Region US (Virginia) Routing Type NAT / Outbound Only
Device Type Catalyst SDWAN

Primary Hub

 Hub Up

1

Active Tunnels 

Tunnel Group ID C8K-3D1A8960-6E76-532C-DA93-50626FC5797E@8323651-651797504-sse.cisco.com
Data Center sse-use-1-1-1
IP Address 44.217.195.188

Secondary Hub

 Hub Up

1

Active Tunnels 

Tunnel Group ID C8K-3D1A8960-6E76-532C-DA93-50626FC5797E@8323651-651797506-sse.cisco.com
Data Center sse-use-1-1-0
IP Address 35.171.214.188

Network Tunnels

Review this network tunnel group's IPsec tunnels. [Help](#) 

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update
Primary 1	65539	128.107.222.147	sse-use-1-1-1	44.217.195.188	 Connected	May 20, 2025 10:45 AM
Secondary 1	131073	128.107.222.147	sse-use-1-1-0	35.171.214.188	 Connected	May 20, 2025 10:44 AM

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



