

Learn about Cisco's Security Cloud solution: Secure Access

cisco Live !

Jim Durkin
Solutions Engineer
jdurkin@cisco.com

Cisco Webex App

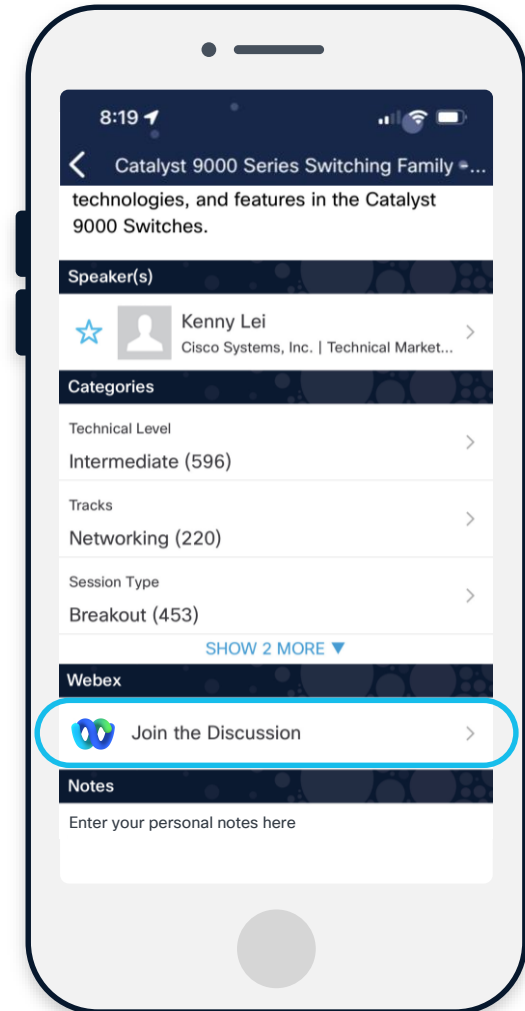
Questions?

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, 2025.



Agenda

- 01 Introduction
- 02 Use Cases
- 03 Network Connections
- 04 Conclusion

Cisco's Comprehensive SSE Solution

SSE Core Capabilities

- Secure Web Gateway
- Zero Trust Access
- Firewall as-a-Service
- Cloud Access Security Broker



So much more

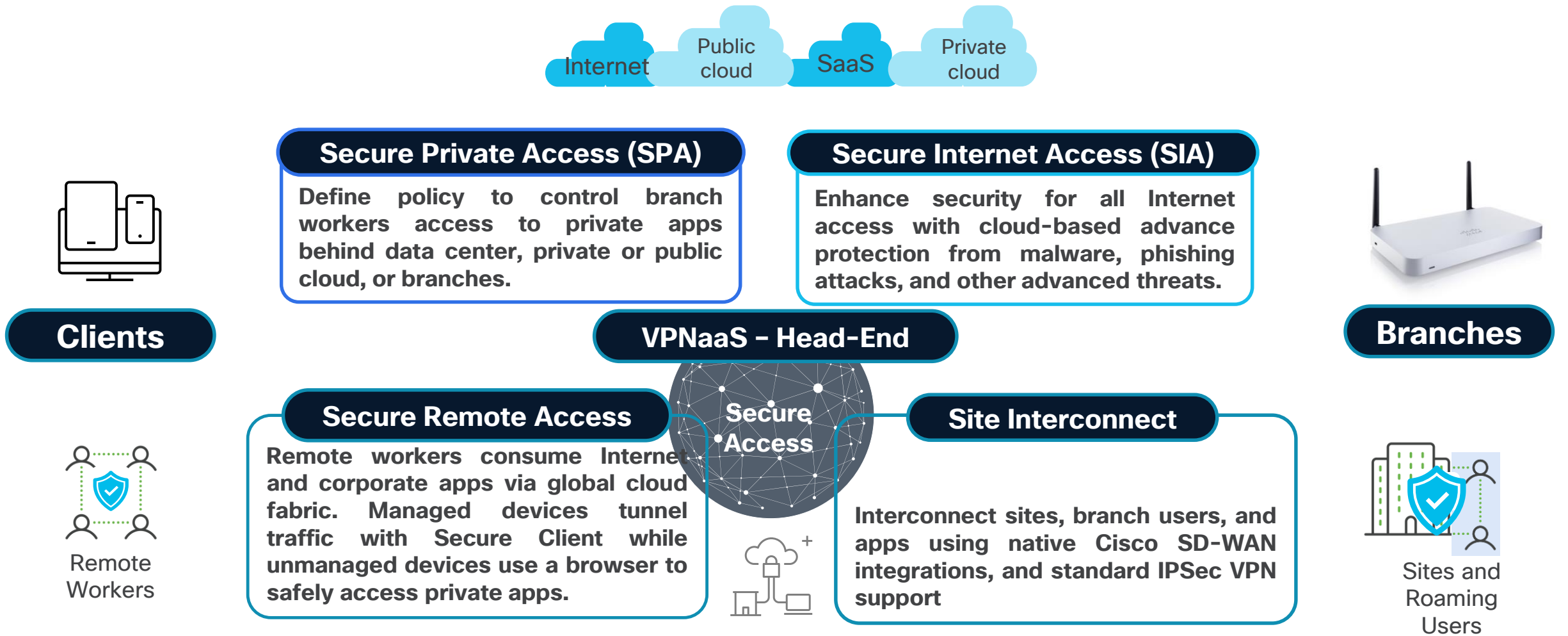
- VPN as-a-Service
- Digital Experience Monitoring
- DNS Security
- Remote Browser Isolation
- Data Loss Prevention
- Advanced Malware Protection
- Sandbox
- Talos Threat Intelligence
- AI-powered Platform

Product Features + Integrations



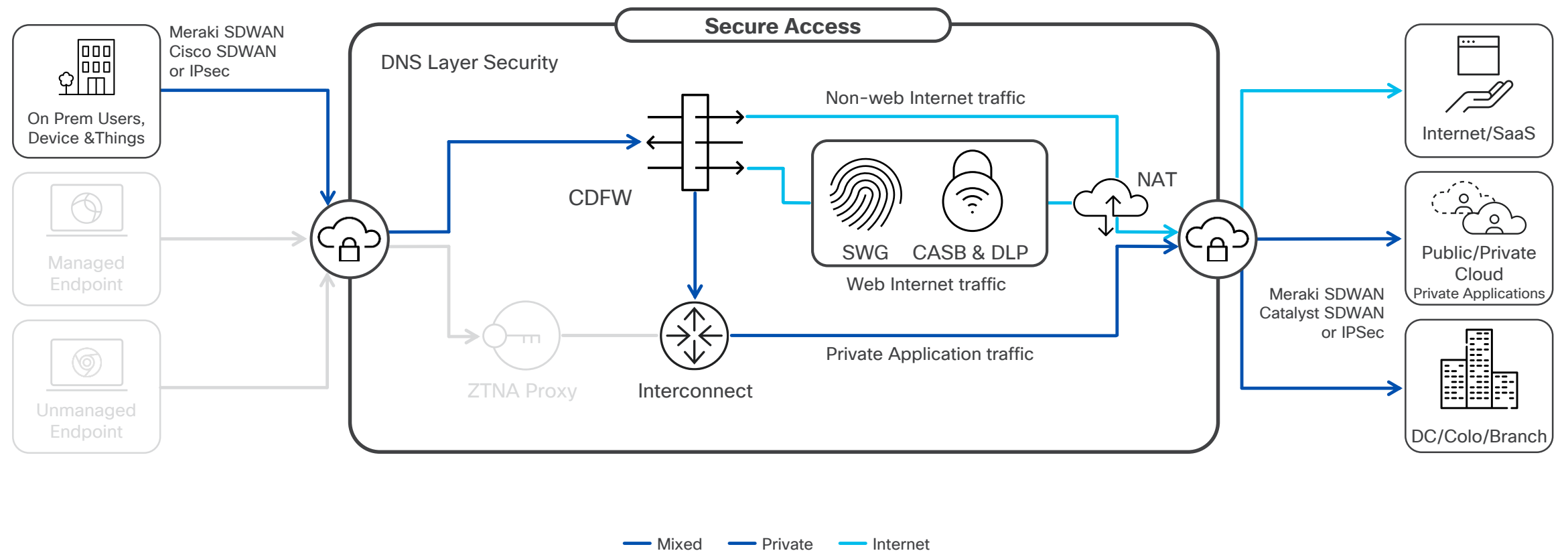
Use Cases

Cisco Secure Access Use Cases



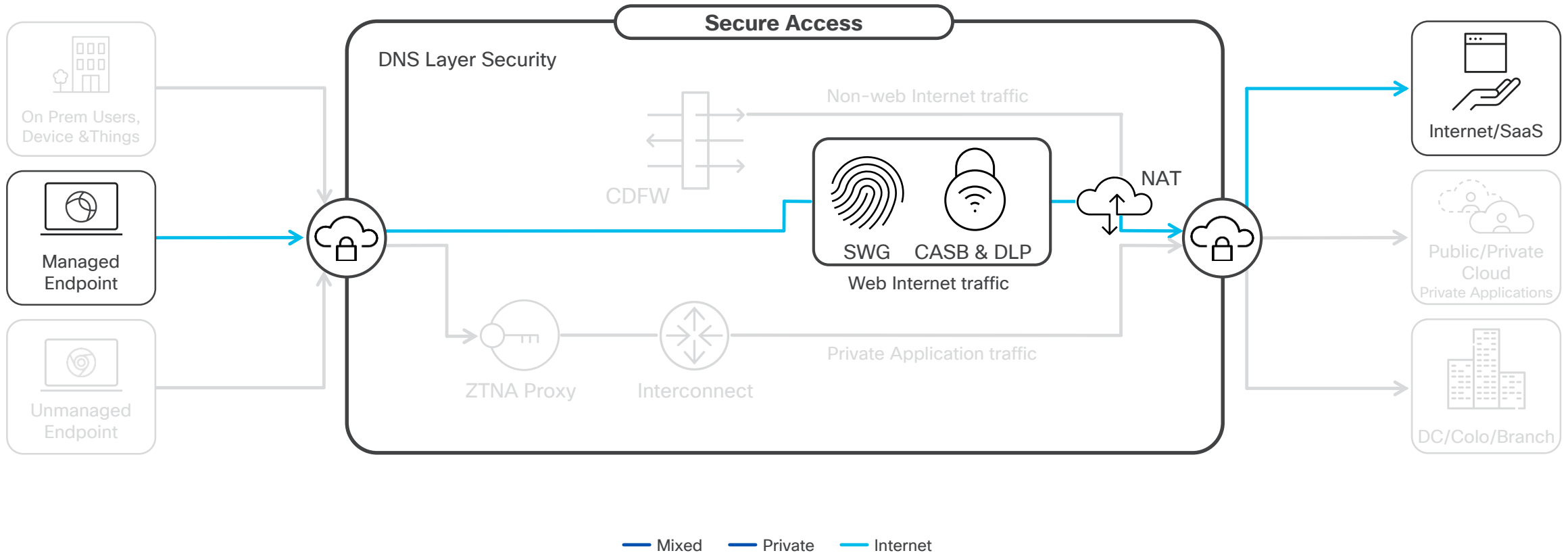
Secure Branch Traffic

- SIA
- SPA

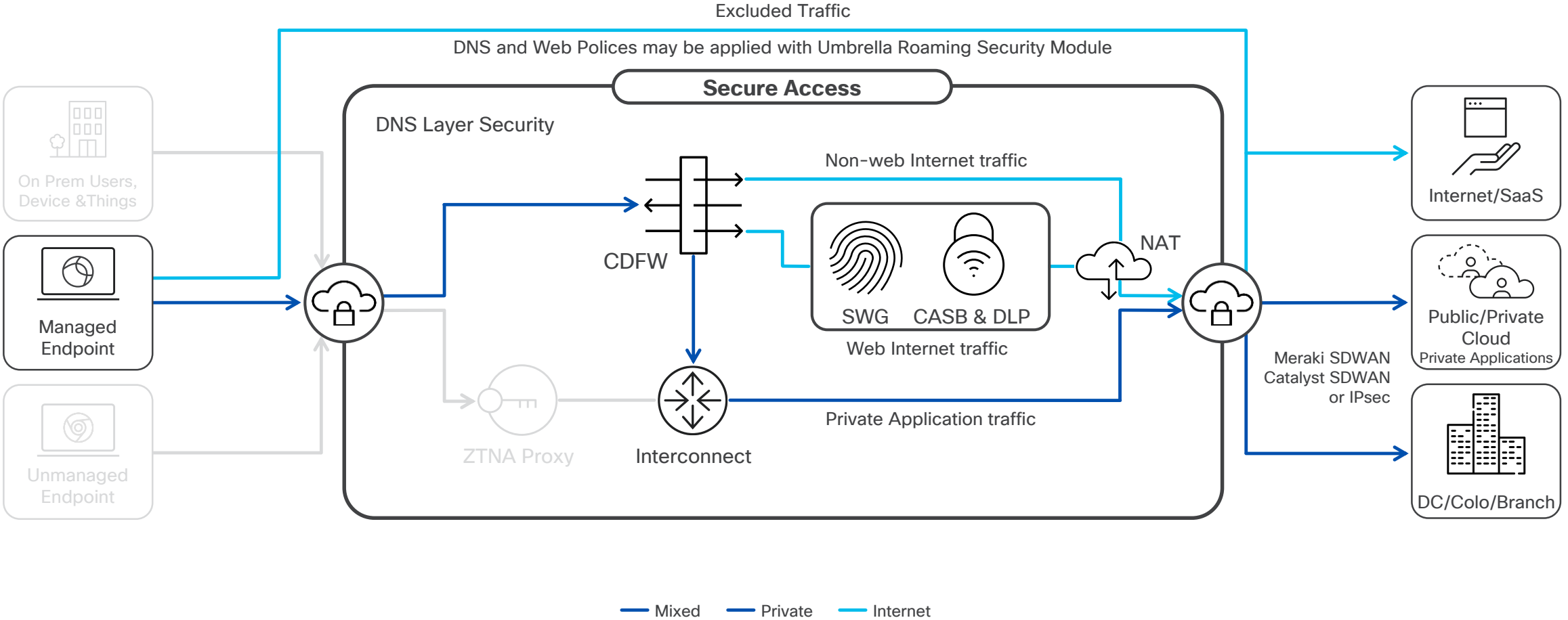


Umbrella Roaming Module with Secure Client

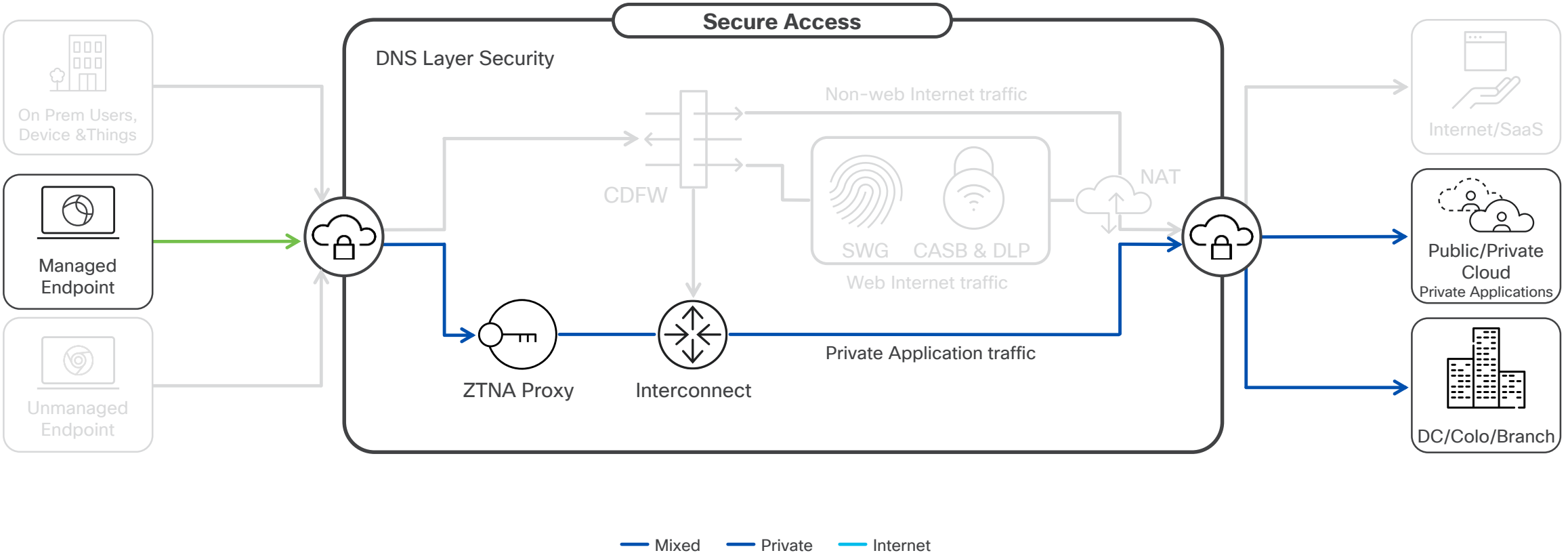
SIA



RAVPNN Client with Traffic Steering



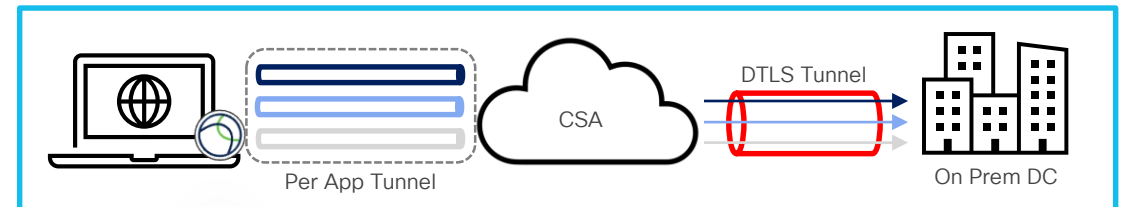
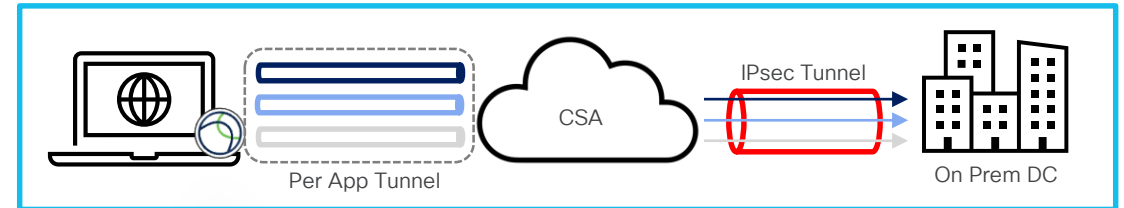
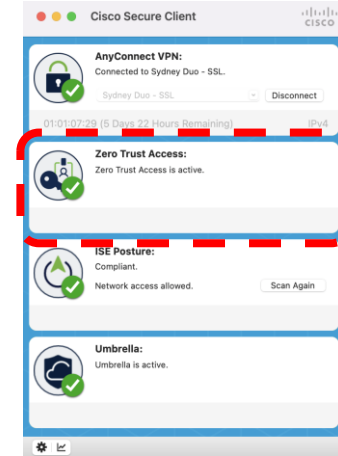
Zero Trust Access – Client-based



Secure Private Access – Cisco Secure Client

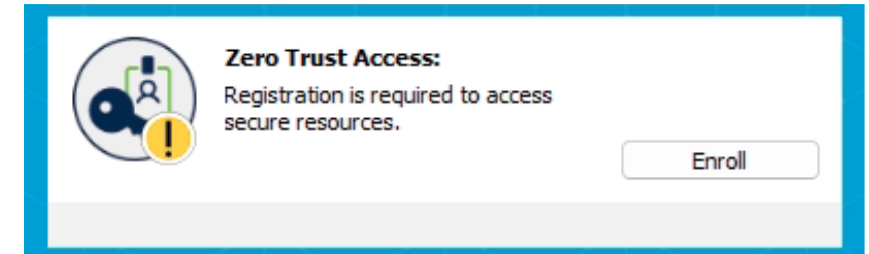
ZTNA Client Based

- Alternative to VPNaaS.
- Micro tunnels per application, allowing for stepping up/down:
 - Authentication
 - Posture requirements.
- QUIC/MASQUE tunnel.
- Supports all TCP/UDP protocols.
- Backhaul can use:
 - IPSec tunnel from an IPSec IKEv2 capable device.
 - Resource Connector.



Client-based ZTA: Enrollment

- New users are prompted to enroll by the Secure Client
 - User input email address as username
 - IdP must be pre-configured in Secure Access
 - User must be in the list of imported users
- User is presented with a list of their tenants
 - One IdP per tenant is supported
 - One enrollment per local user is supported
 - SAML redirection to configured IdP
- Once enrolled, a certificate is pushed to the client
 - Saved in the TPM (required)
 - Auto-renewal occurs within two weeks of expiration
 - Re-enrollment is required if the device is offline during renewal period



Cisco Secure Access

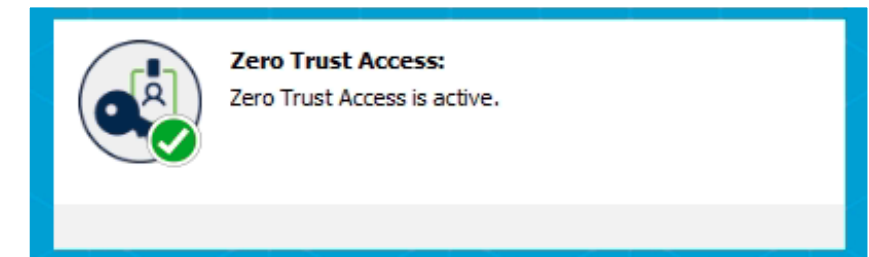
Sign In to Enroll

Use your company email address and continue.

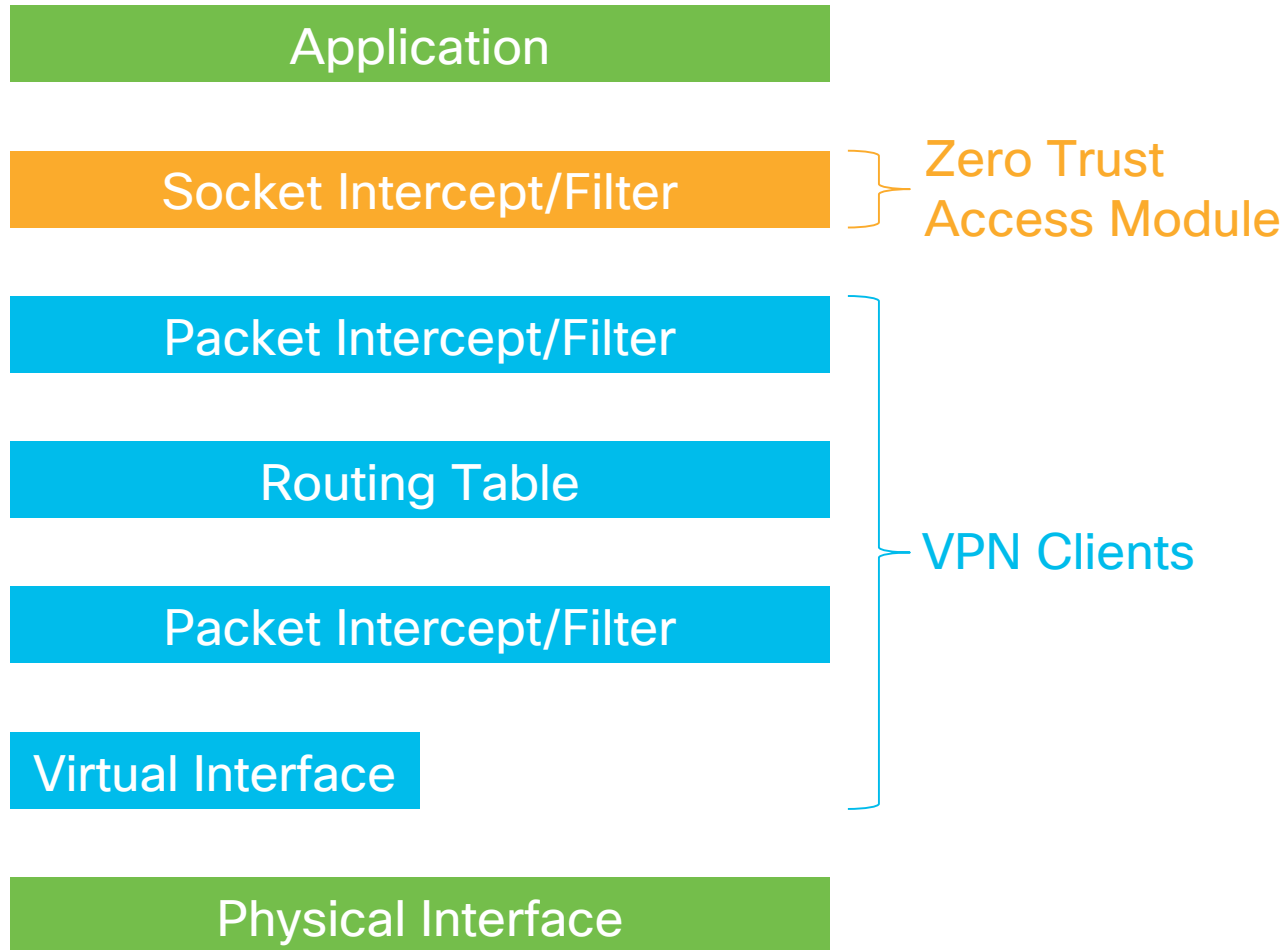
Email Address

miles@lab.christianclasen.com

Continue



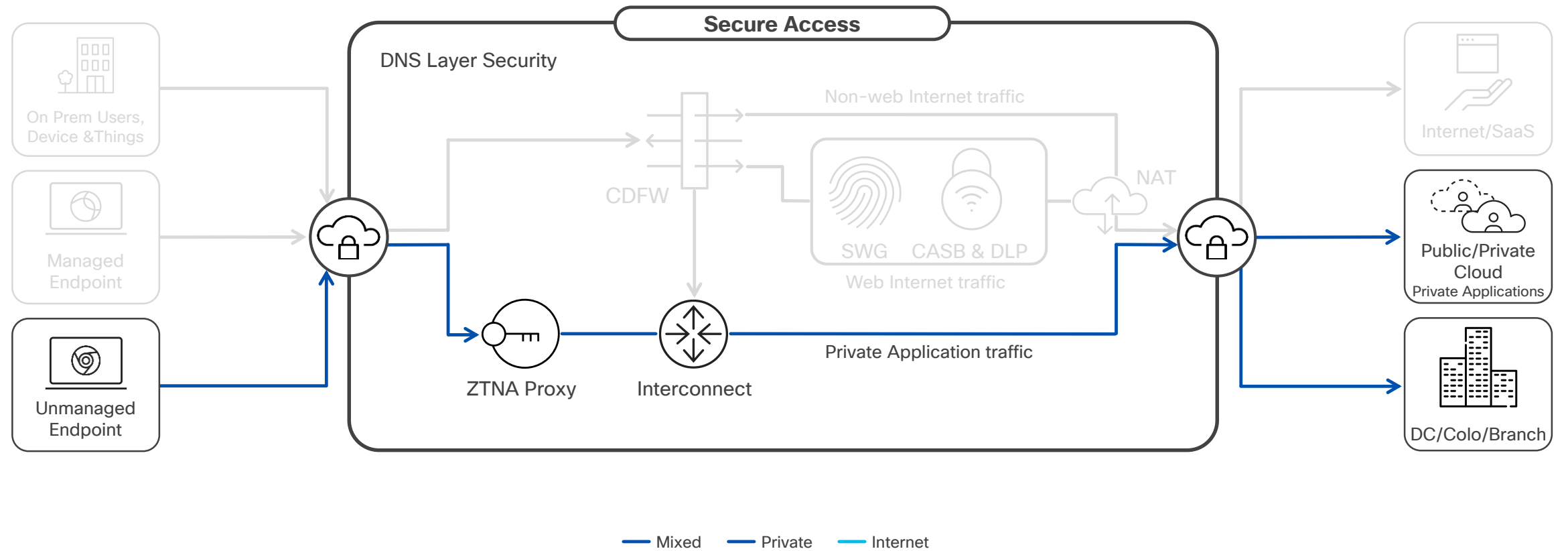
Secure Client ZTA Module: Socket Intercept



Why Socket Intercept?

- Control of DNS and application traffic before VPN clients
- No route table manipulation
- Ability to capture traffic by IP, IP subnet, FQDN and FQDN wildcard
- Interoperability with Cisco and non-Cisco VPNs

Zero Trust Access – Browser-based



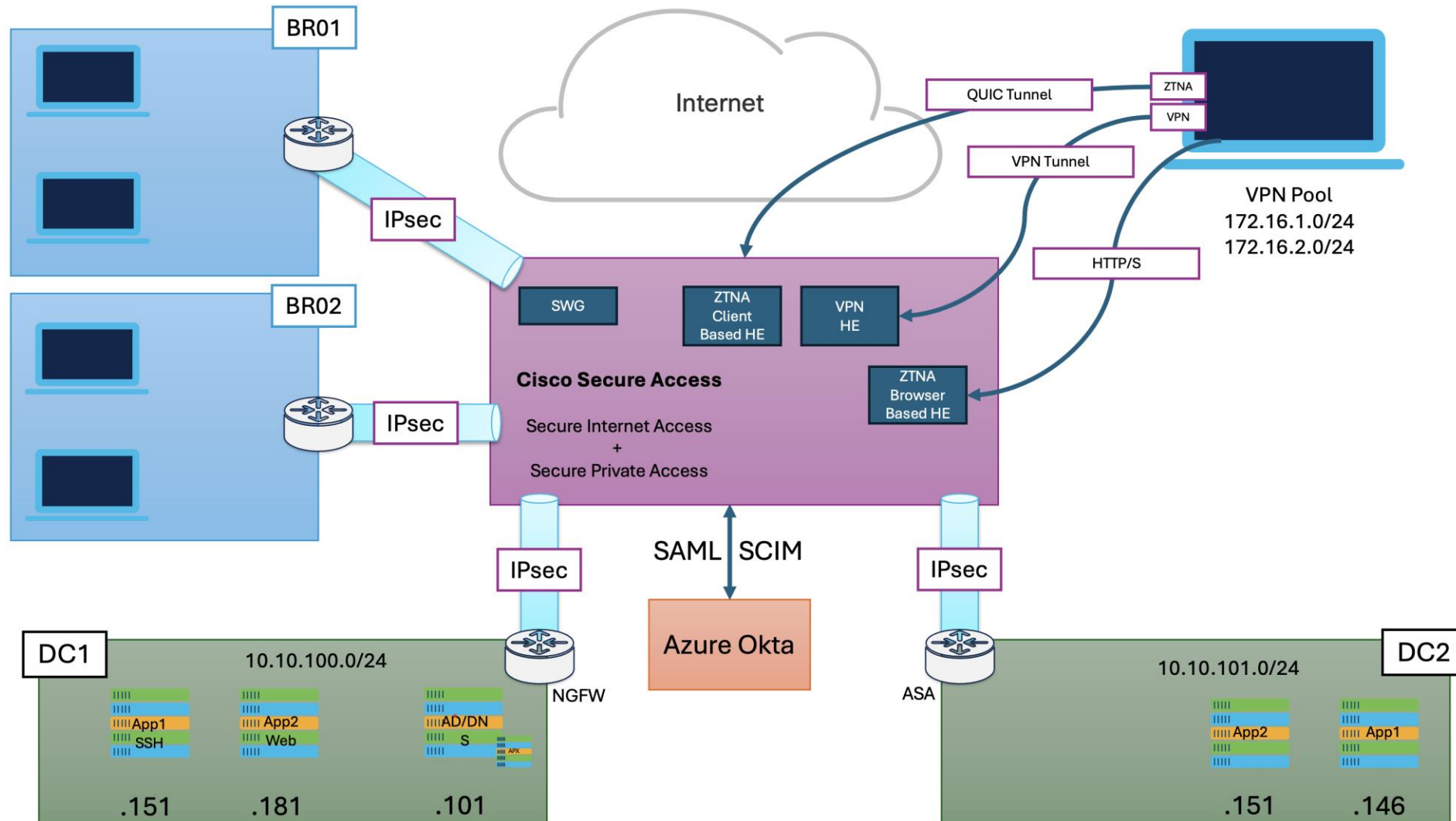
Posture Check Profiles

Authorization check prior
to application access

Authorization and access check
per session

	 VPNaaS	 ZTA Client-based	 ZTA Browser
Operating System	✓	✓	✓
Anti-Malware	✓	✓	
Firewall	✓	✓	
Disk Encryption	✓	✓	
Certificate Check	✓		
Browser Check	✓		✓
System Password		✓	
File Check	✓		
Registry Check (windows only)	✓		
Process Check	✓		

High Level Deployment Topology



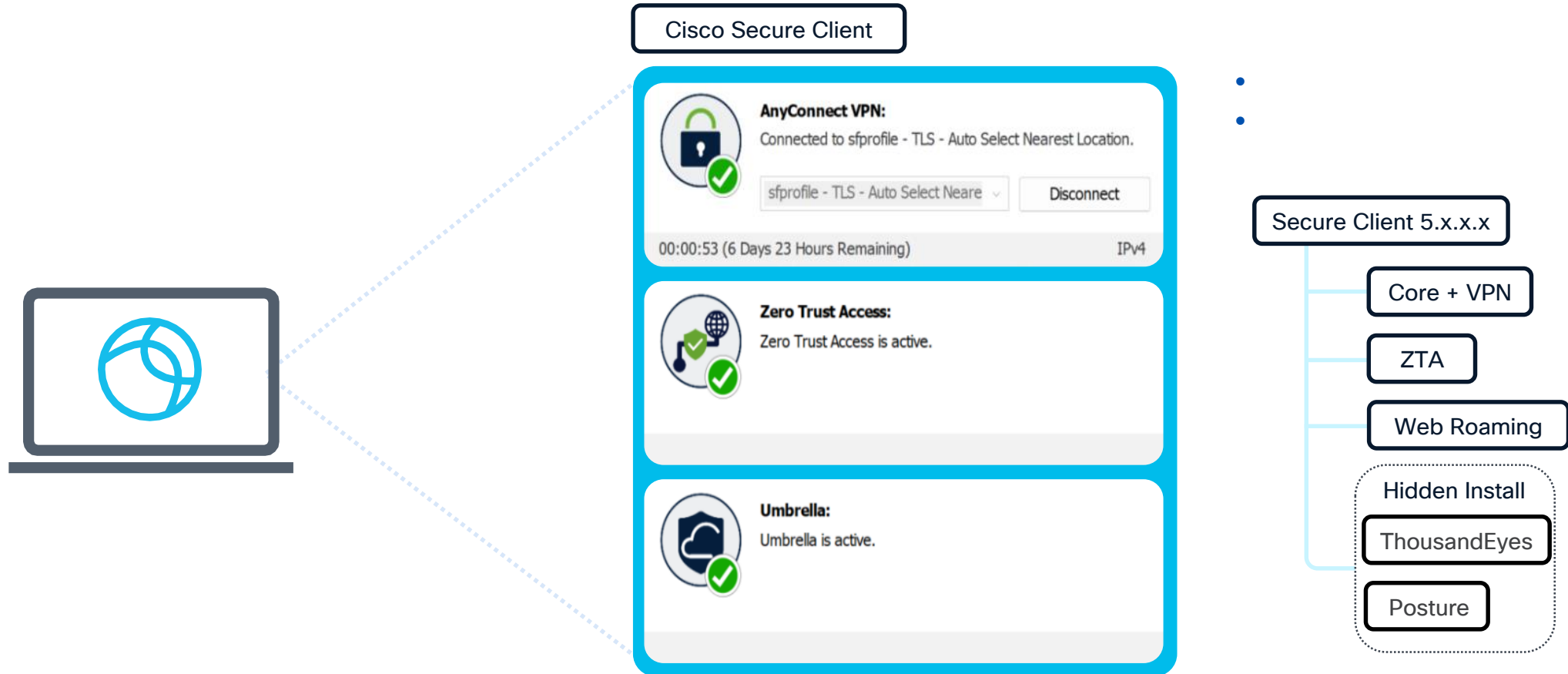
Network Connections

Cisco Secure Client

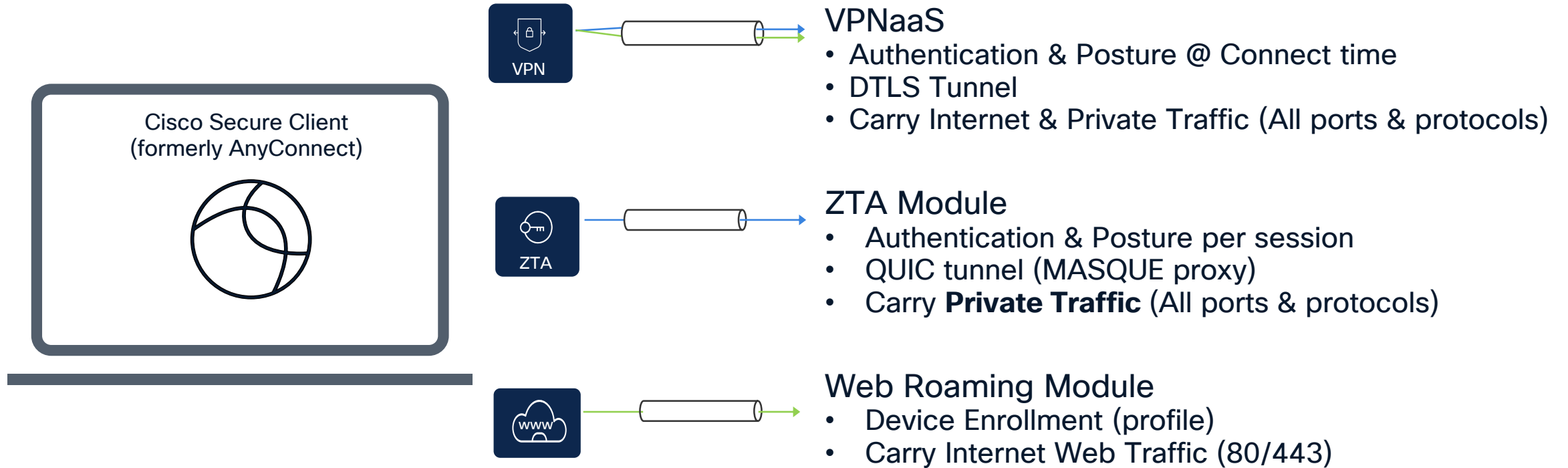
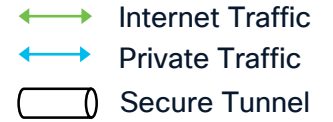
Enable Remote User Connectivity

End User Connectivity

Remote User Client Software



End User Connectivity



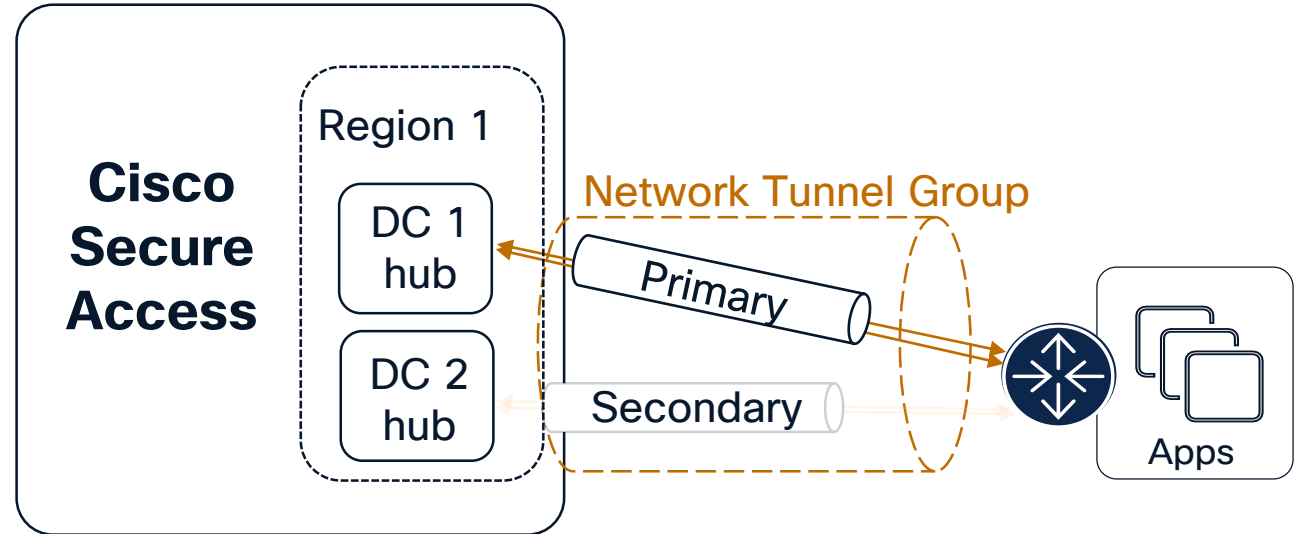
Network Tunnel Groups

Enable Branch Connectivity
Enable Access to Private Applications (IPSec Backhaul)

Network Tunnel Group

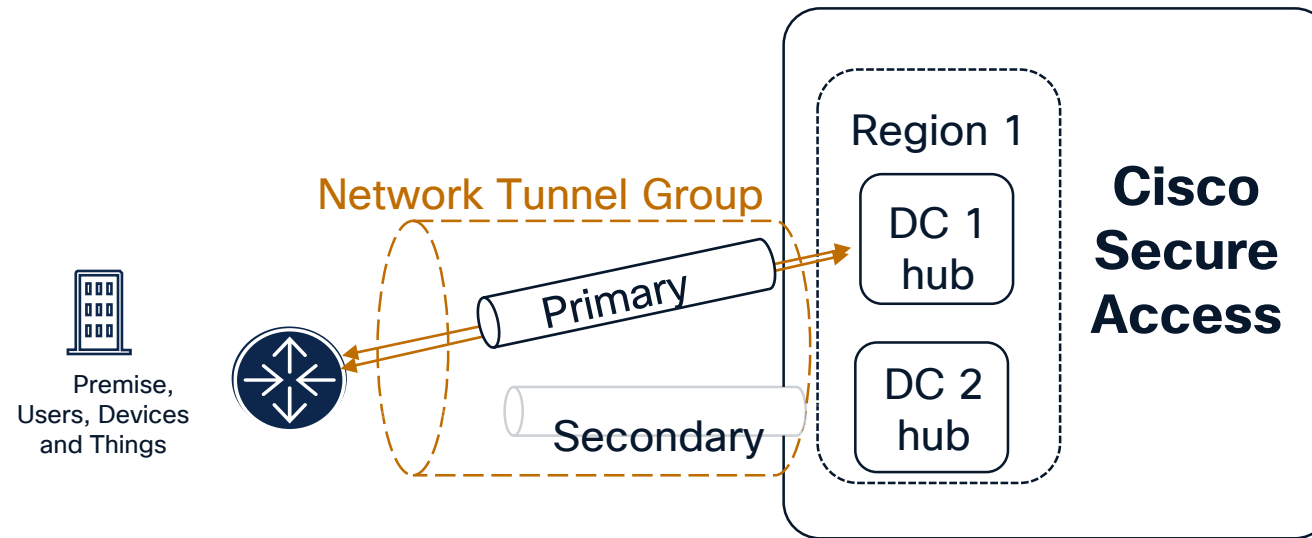
Private App Backhaul

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



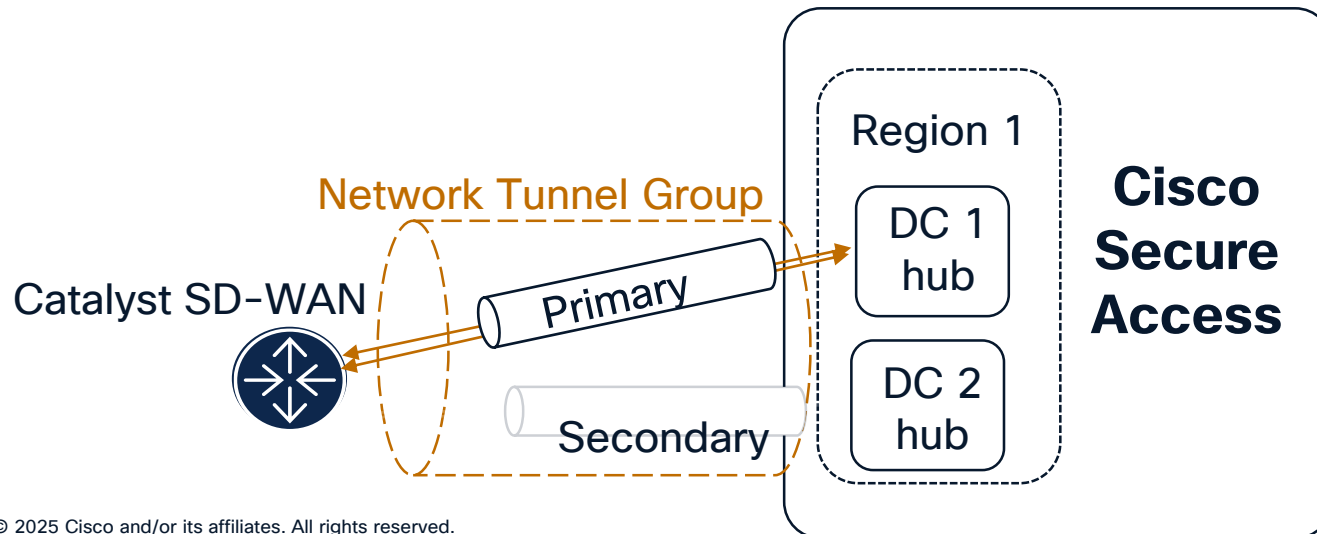
Branch

Secure Internet Access



Site-to-site Tunnels with IPsec

- Standards-based IPsec connection
- Single tunnel for Internet and private application access
- Static or BGP routing support
- Auto failover for redundancy + ECMP for scale
- Regional redundancy
- Outbound NAT support for internet only tunnels



Catalyst SD-WAN

- Auto tunnel creation from Catalyst SD-WAN manager (version 20.13/17.13)
- 1GB per tunnel
- Up to 8 active, 8 backup per tunnel group
- Tunnels for Internet access only
- Outbound NAT
- VPNID & SGT based policy



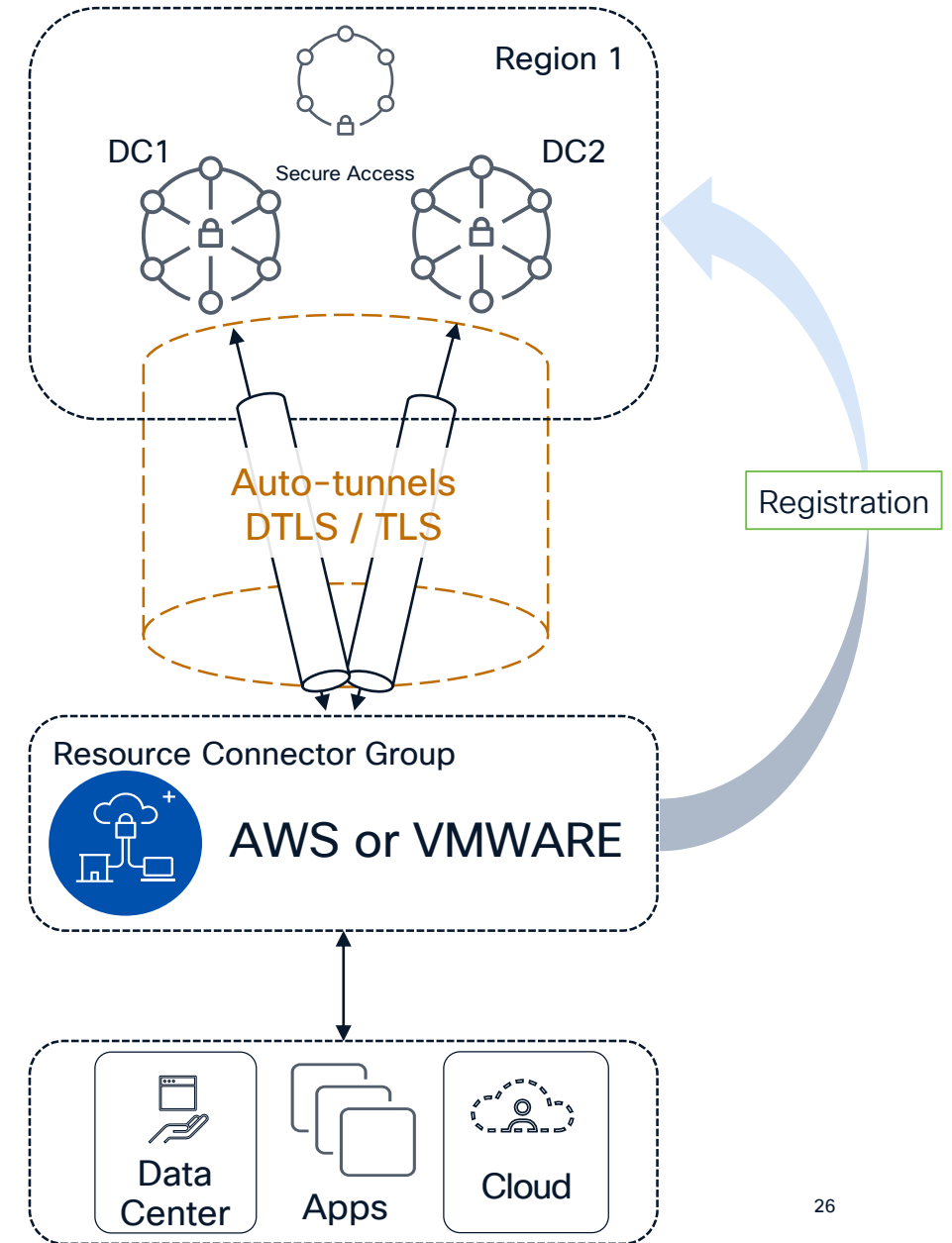
Resource Connectors

Enable Access to Private Applications (ZTNA)

Resource Connector

Secure Private Access

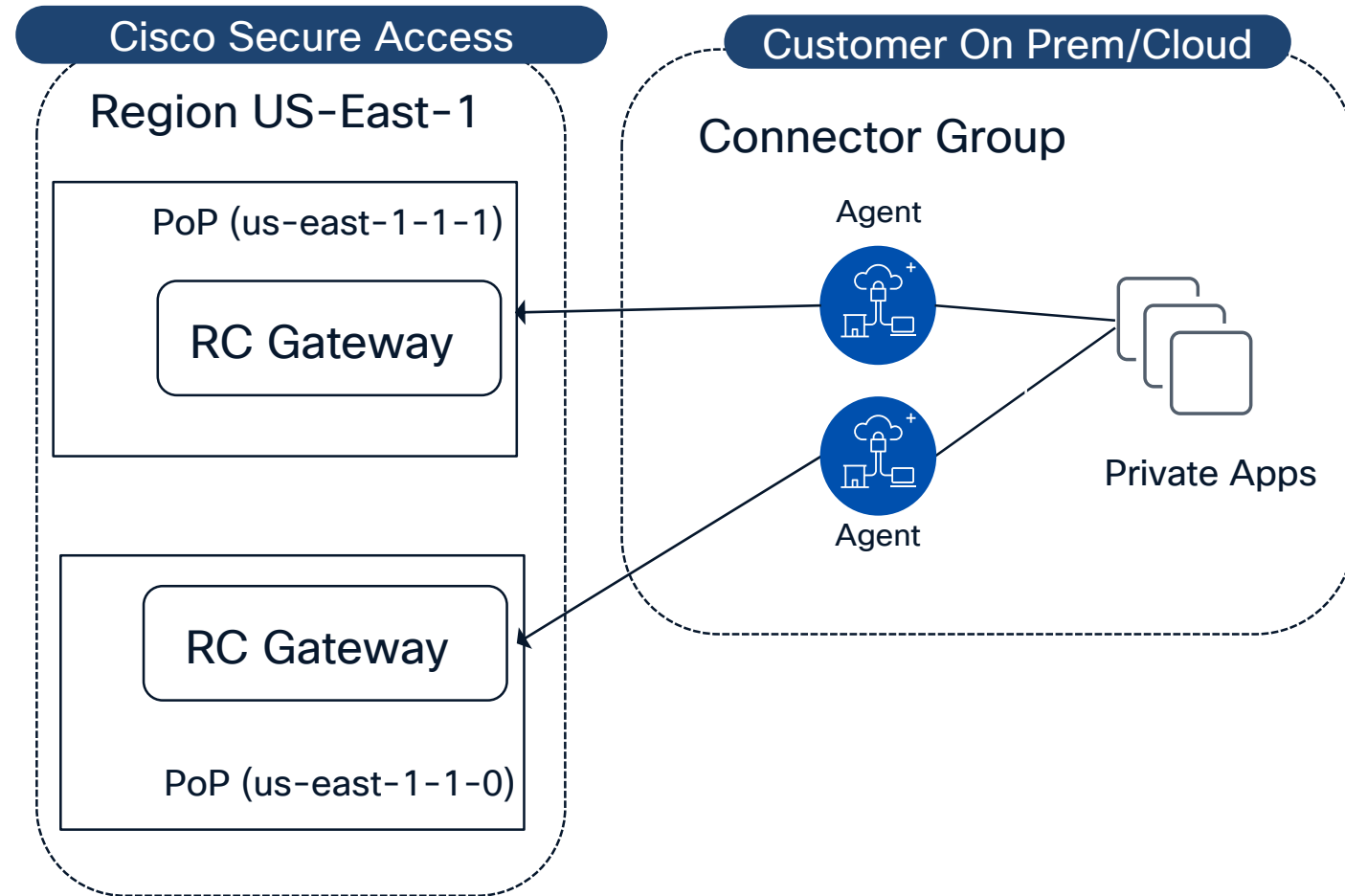
- Deployed in a group
 - Can be deployed with one member
- Virtual machines
 - AWS Marketplace (c5.xlarge only)
 - VMWare image (OVA)
 - Intel x86_64/AMD64 only
 - IPv4 only
- Registers with dashboard
 - Provisioning key
 - Manual confirmation
- Load balancing
 - Automatic across all in a group
 - Must be same instance type
 - Must be in same region



Resource Connector Redundancy

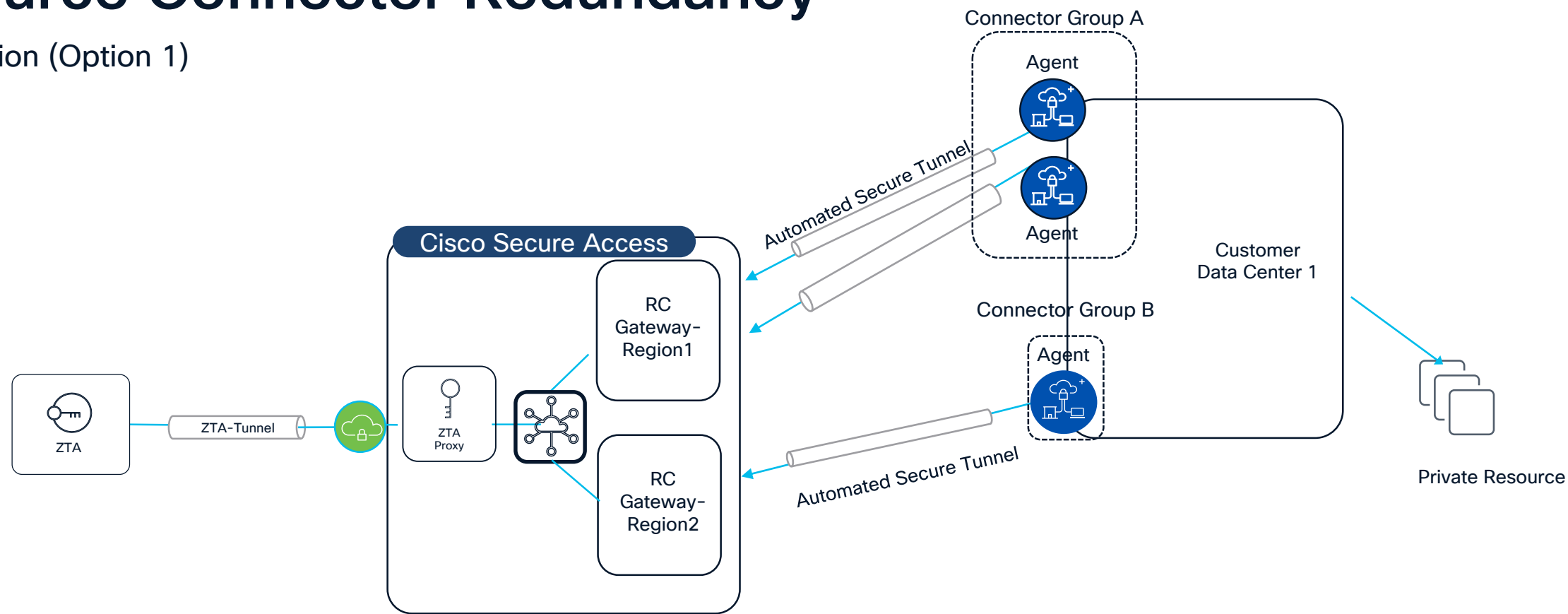
Single Region

- Recommended minimum of 2 agents per connector group
- All agents within a group should be identical and connect to the same region
 - Tunnel URL returned during registration (based on group location)
 - All agents have same connectivity to apps



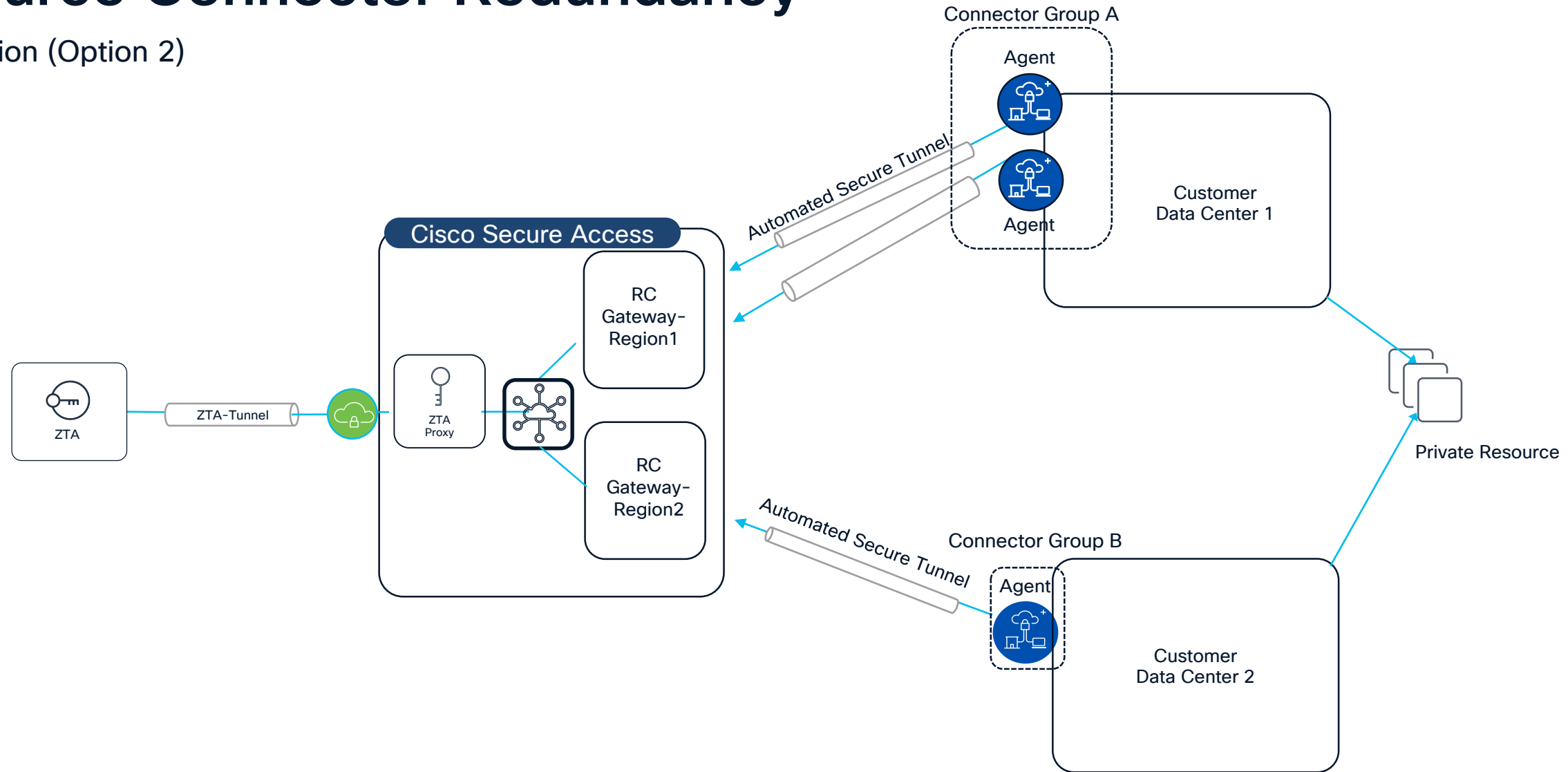
Resource Connector Redundancy

Multi-Region (Option 1)



Resource Connector Redundancy

Multi-Region (Option 2)



Other Secure Access Topics

- Digital Experience Monitoring for End-to-End Visibility
- VPNID based policy across both Catalyst SD-WAN and Secure Access
- SGT based policy across network and Secure Access using Identify Services Engine (ISE)
- Secure Access APIs
- Universal ZTNA – Single Policy across Secure Access and Cisco Secure Firewall

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 2026.



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

Contact me at: jdurkin@cisco.com

Thank you

CISCO Live !

