



The bridge to possible

Migrate your Traditional VPN to Cloud-delivered VPNaaS with Cisco Secure Access

Viraj Nagarmunoli, Security Solutions Architect
Tim Rowley, Principal Security Architect
BRKSEC-2157

CISCO *Live!*

#CiscoLive

Cisco Secure Access *simplifies* your
hybrid worker *security* strategy

A *thoughtful migration strategy* is key

Cisco Webex App

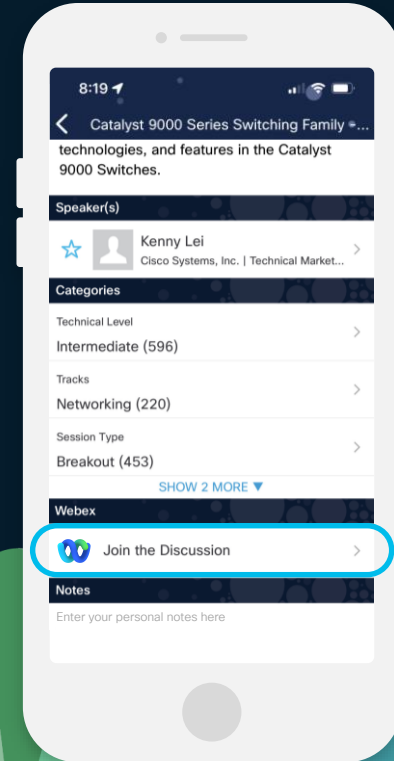
Questions?

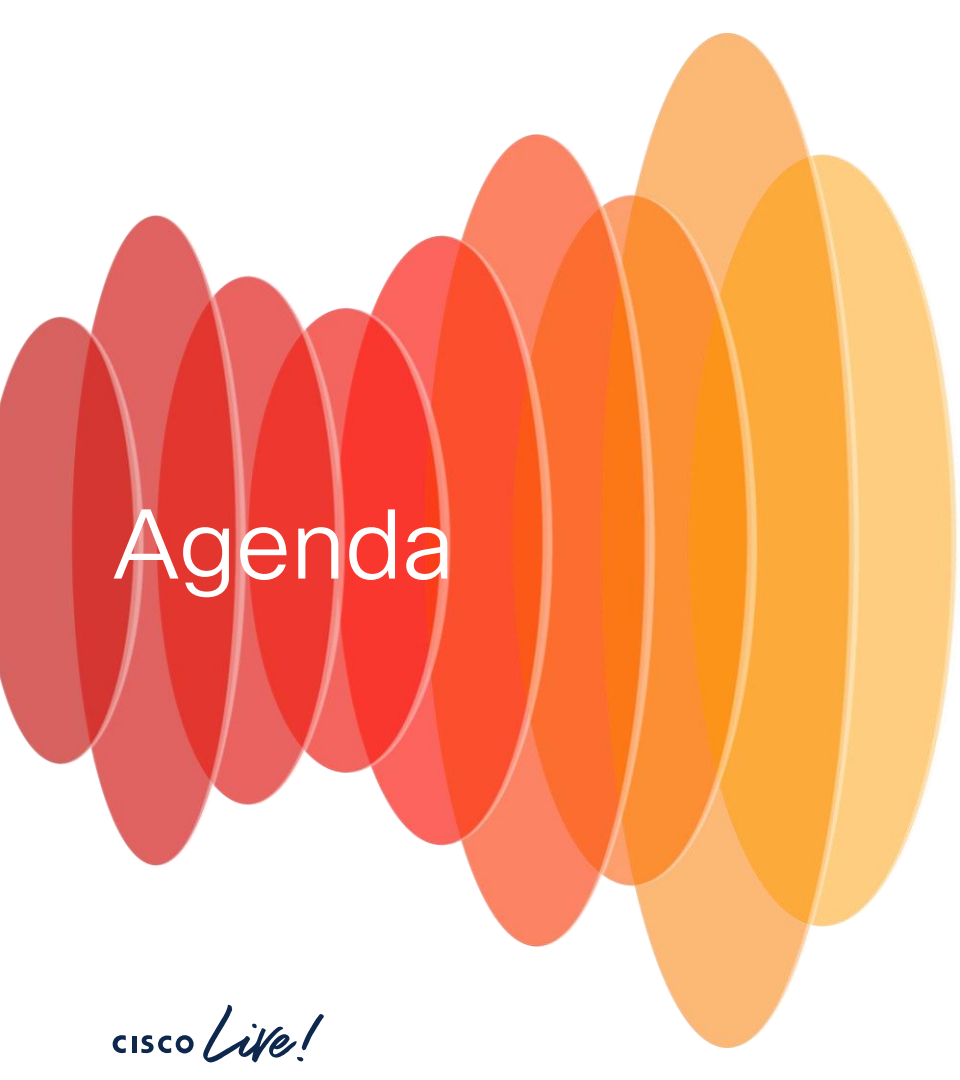
Use Cisco Webex App to chat with the speaker after the session

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 7, 2024.



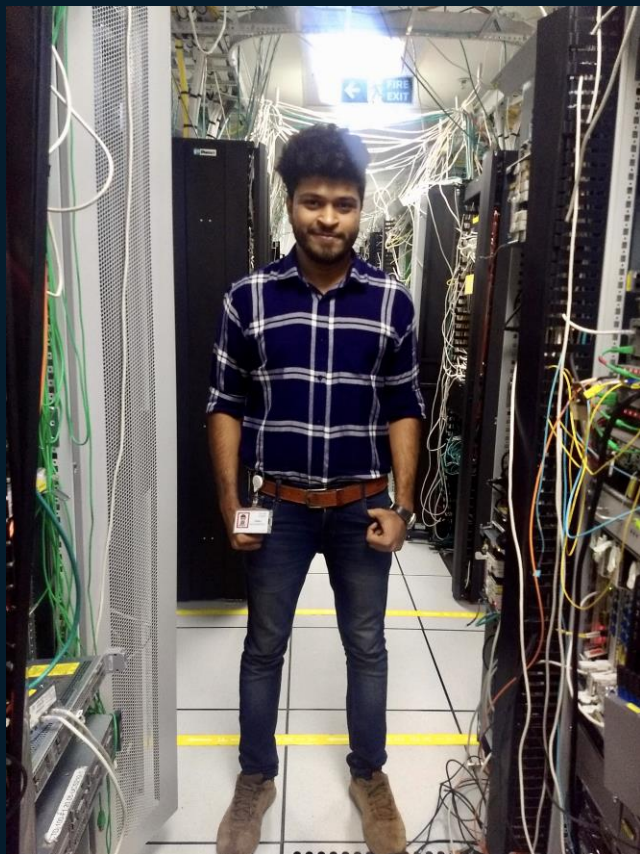


Agenda

- Traditional RAVPN vs Cisco Secure Access
- Secure Access Use Cases
- Intent-based Policy
- Migration Strategy
- Conclusion

Session Outline

- The goal for this session is to help you build a migration strategy
- The content does not cover specific configuration examples



Viraj Nagarmunoli

7 years of experience

Various roles @ Cisco

ISE / AAA TAC Escalation Engineer

Solutions Architect

Zero Trust CX Product Management

Worked in

Bangalore

Raleigh

San Jose

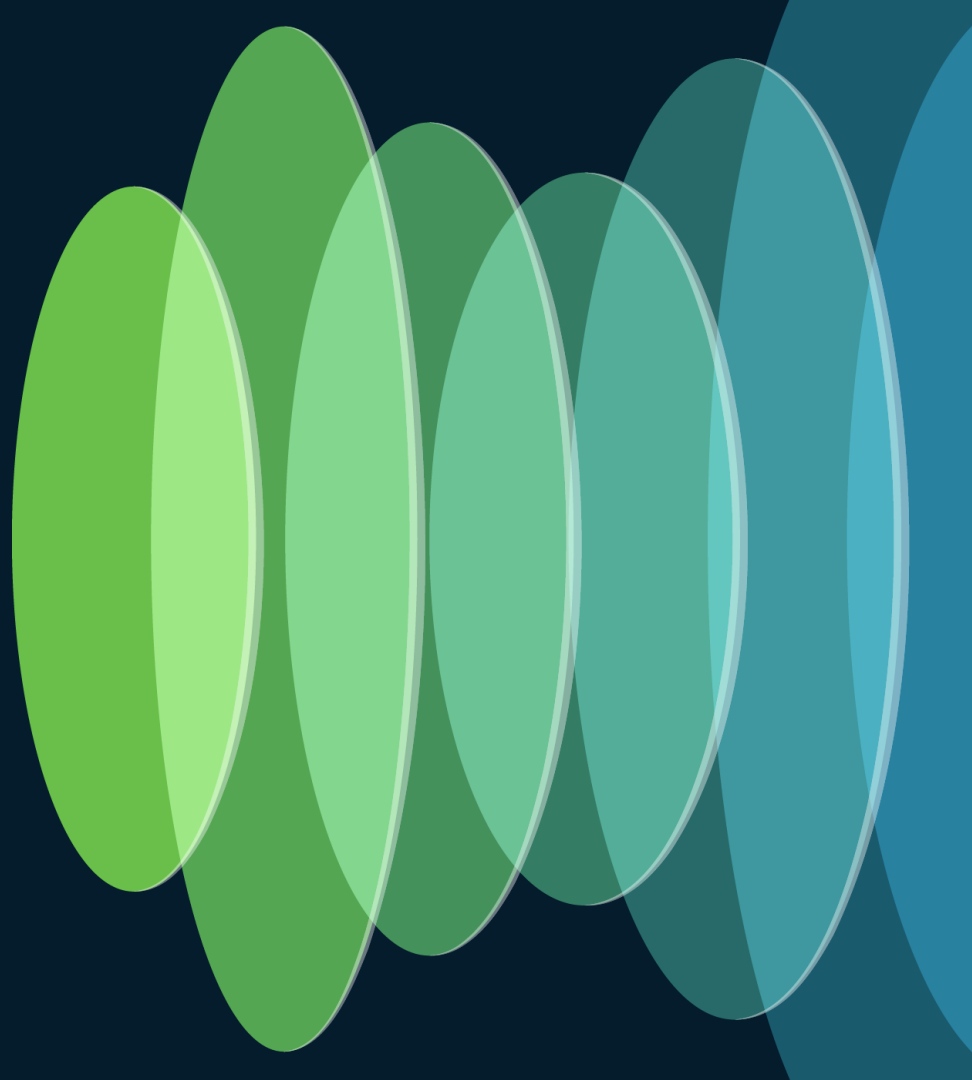
Education

Masters in Software Systems

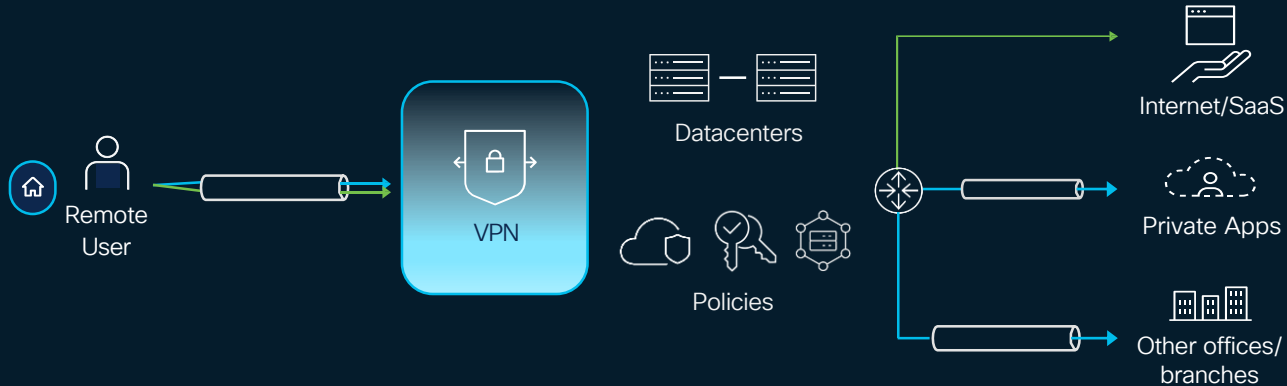
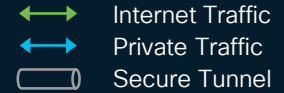
Bachelors in Electronics and Comm

6

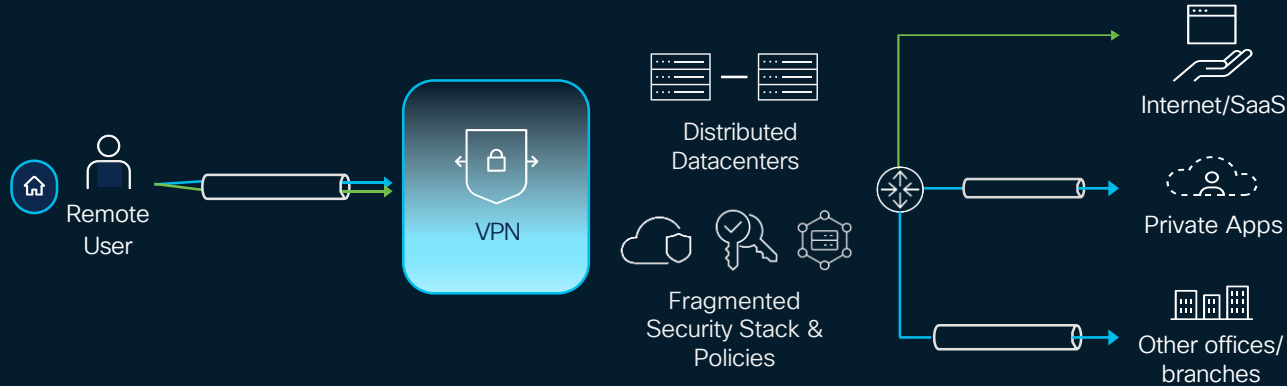
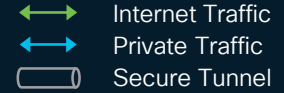
Traditional Remote Access VPN



Traditional RAVPN architecture



IT challenges increase cost and risk



Hybrid work, SaaS explosion and unabated threats

Push the limits of traditional VPNs



49%

Employees are
remote/hybrid
users



53%

Remote/hybrid
workers using
DIA



55%

Traffic to/from
off-premises,
cloud-based facilities

Capacity constraints. User frustration (opting out). Security gaps.

Why are users so frustrated?



83%

Performance issues when using the VPN



78%

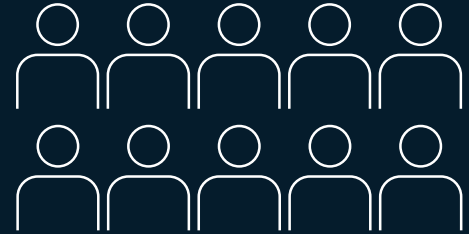
Repeatedly turning the VPN on and off



77%

Frequent and/or intrusive requests for user credentials and posture checks

User fatigue opens the door for successful attacks



40%

Of remote/hybrid users have bypassed recommended VPN use in the past

Ideal State

1 Connect to a network

2 Get to work

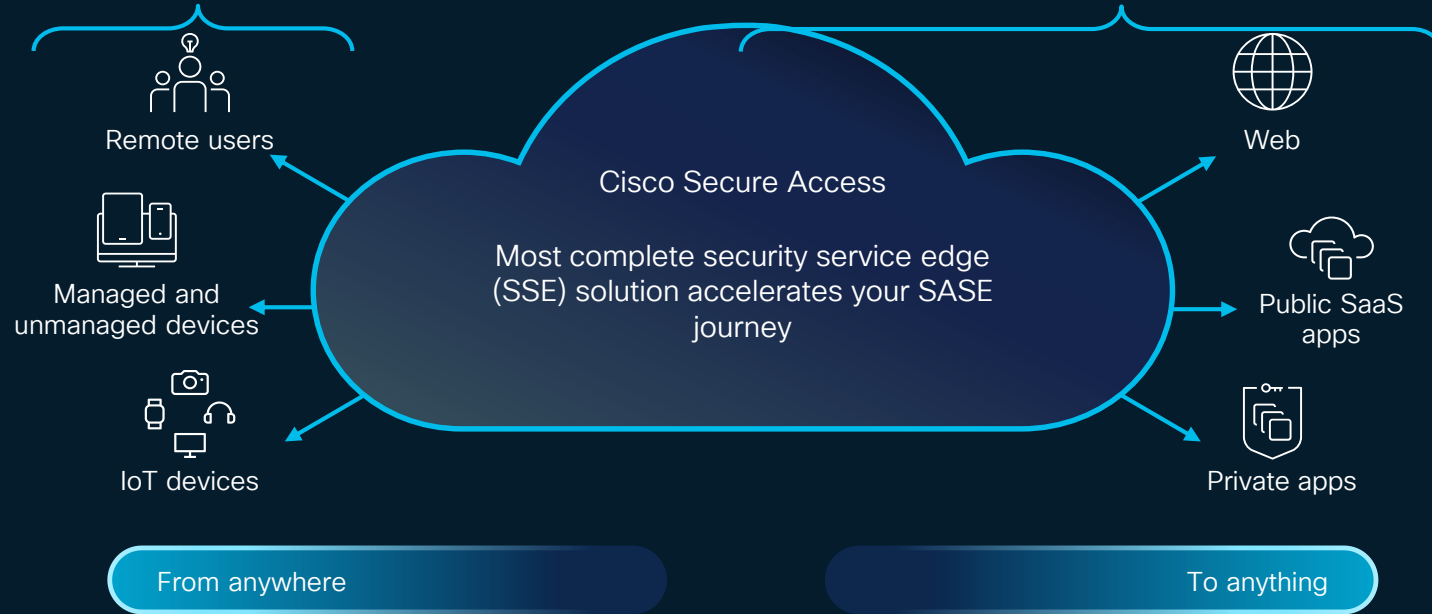


Introducing Cisco Secure Access

Modernize your defense with converged cloud security grounded in zero trust

1 Connect to a network

2 Get to work



Move your VPN to the cloud (VPNaaS)

- Deliver VPN as outsourced cloud service
- Eliminate hardware installation and maintenance
- Boost productivity with user access to all apps/resources
- Simplify operations with single console, agent, policy engine
- Enhance application access control
- Easily scale with high performance as user base grows



Secure Access Use Cases

VPNaaS and more

Use Cases



Secure Private Access

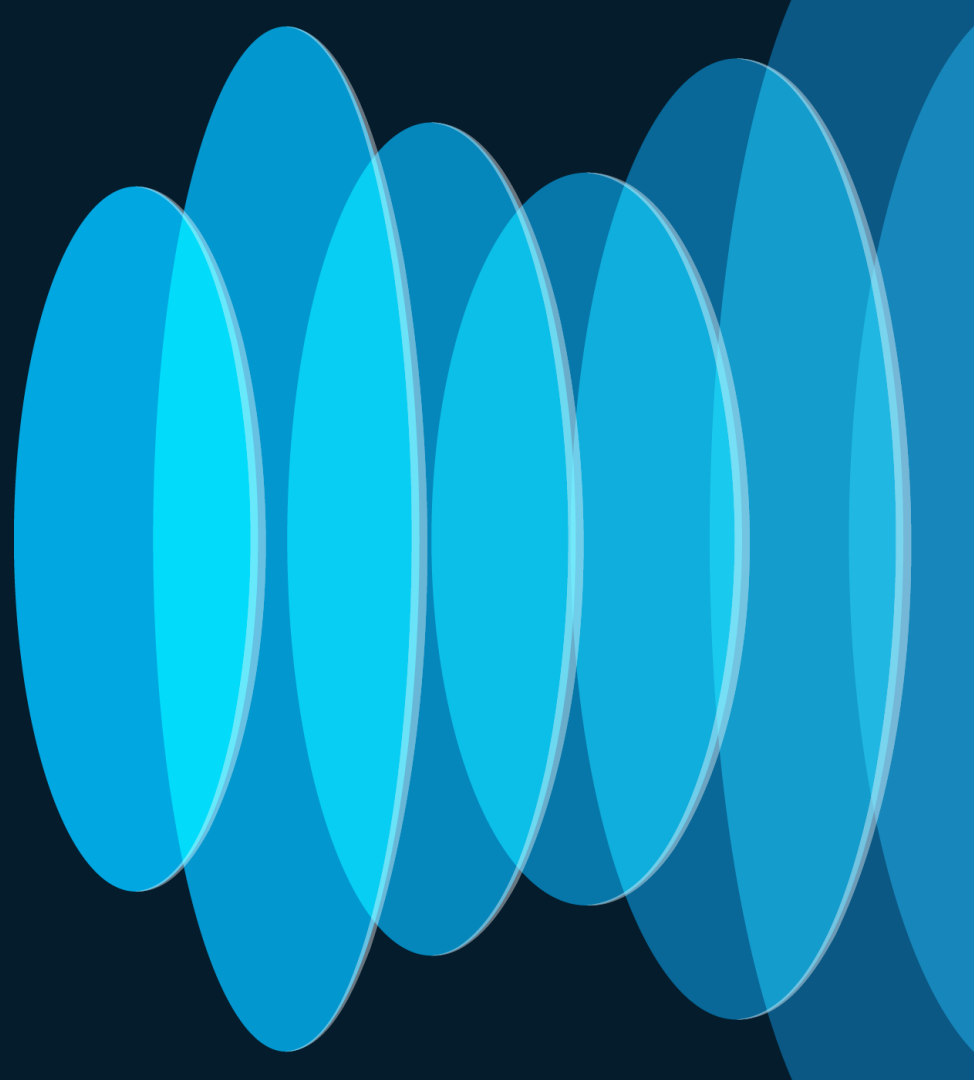
- Via VPN
- Via ZTNA (Client Based)
- Via ZTNA (Clientless)



Secure Internet Access

- VPN full tunnel
- Internet Security Module
- Branch DIA

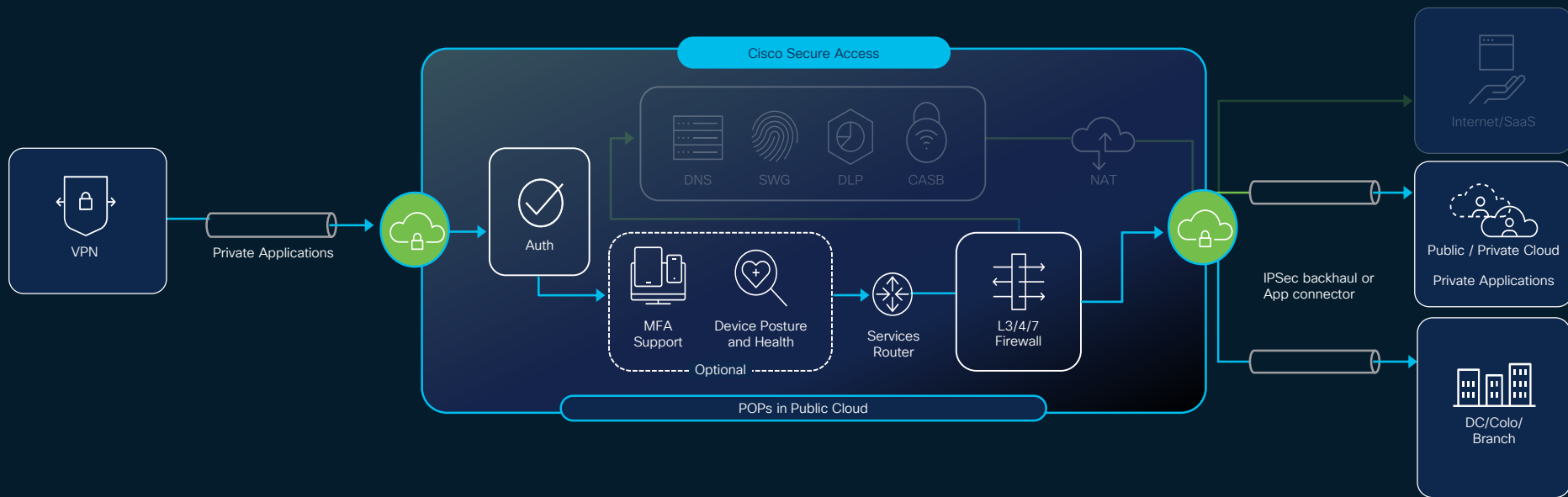
Secure Private Access



Secure Private Access (VPN)

Full or split tunnel VPNaaS

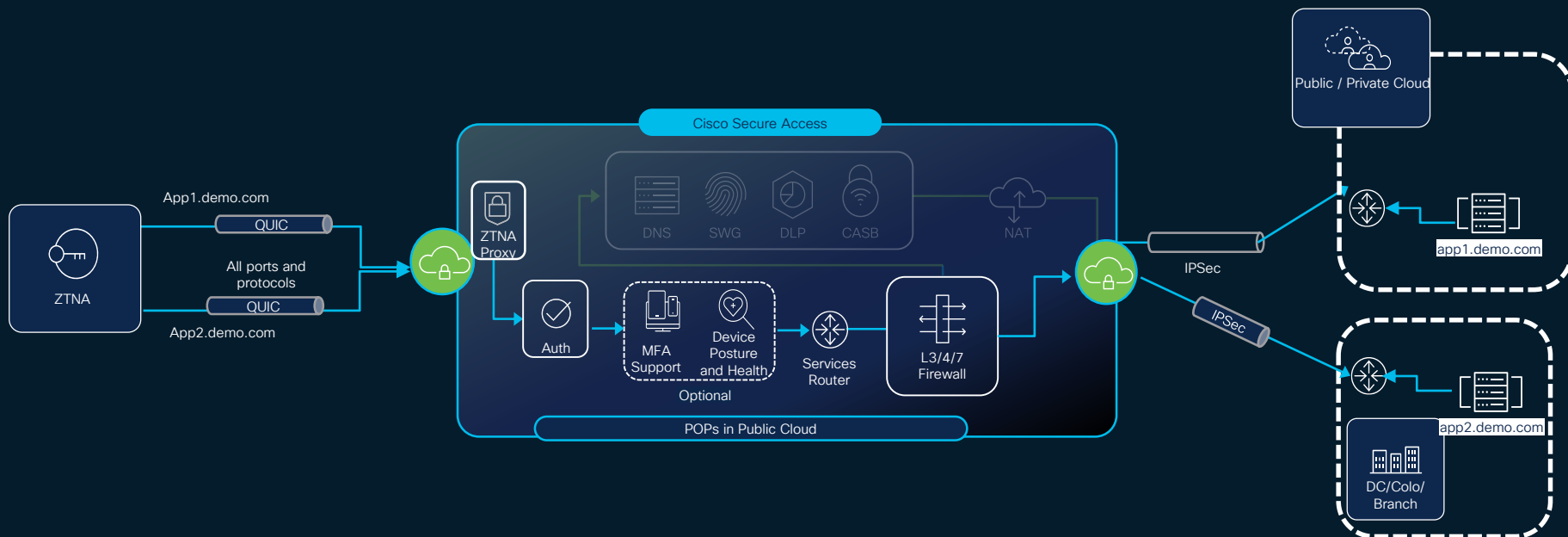
↔ Private Traffic
Secure Tunnel



Secure Private Access (Client-based ZTNA)

ZTNA supported Apps via IPSec backhaul

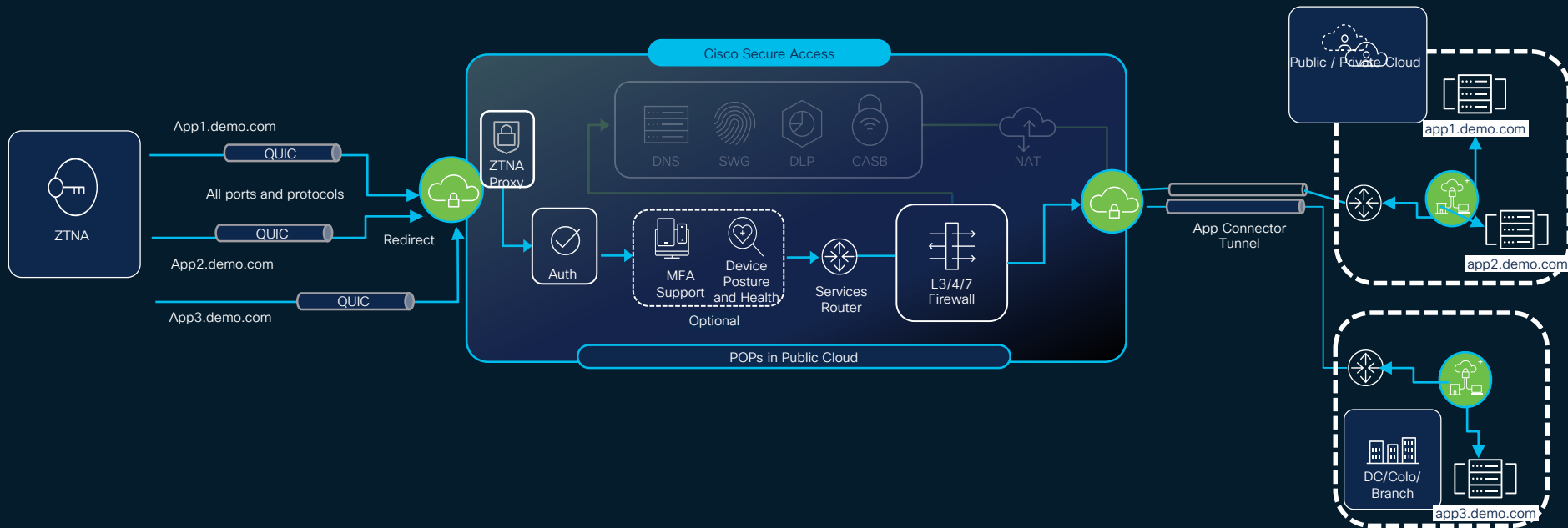
↔ Private Traffic
Secure Tunnel



Secure Private Access (Client-based ZTNA)

ZTNA supported Apps with App Connector

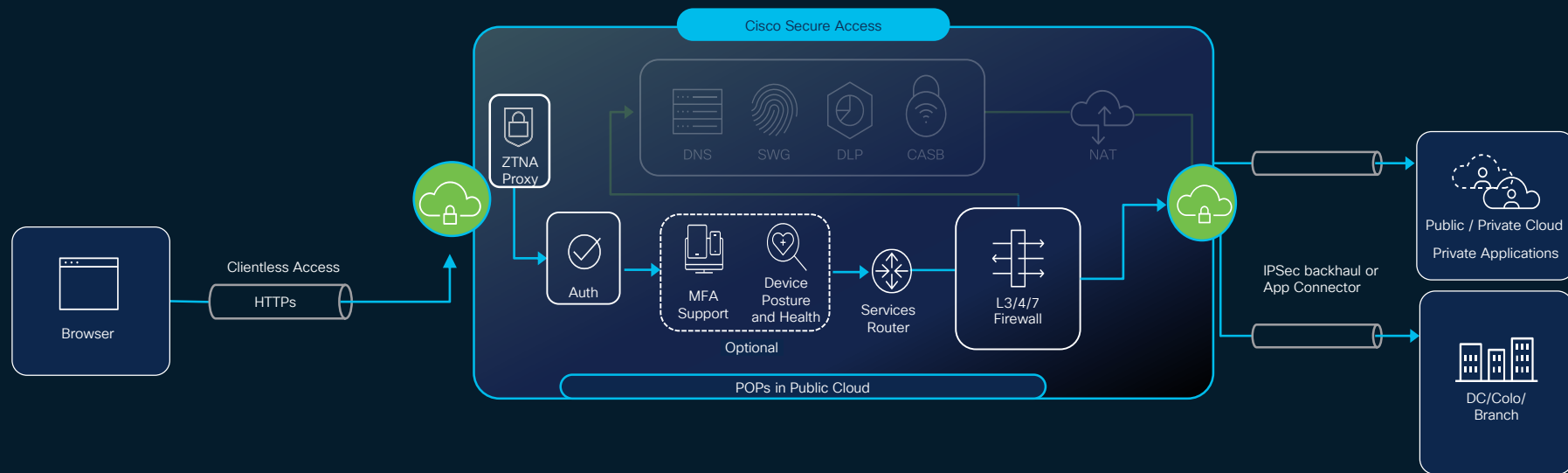
Private Traffic
Secure Tunnel



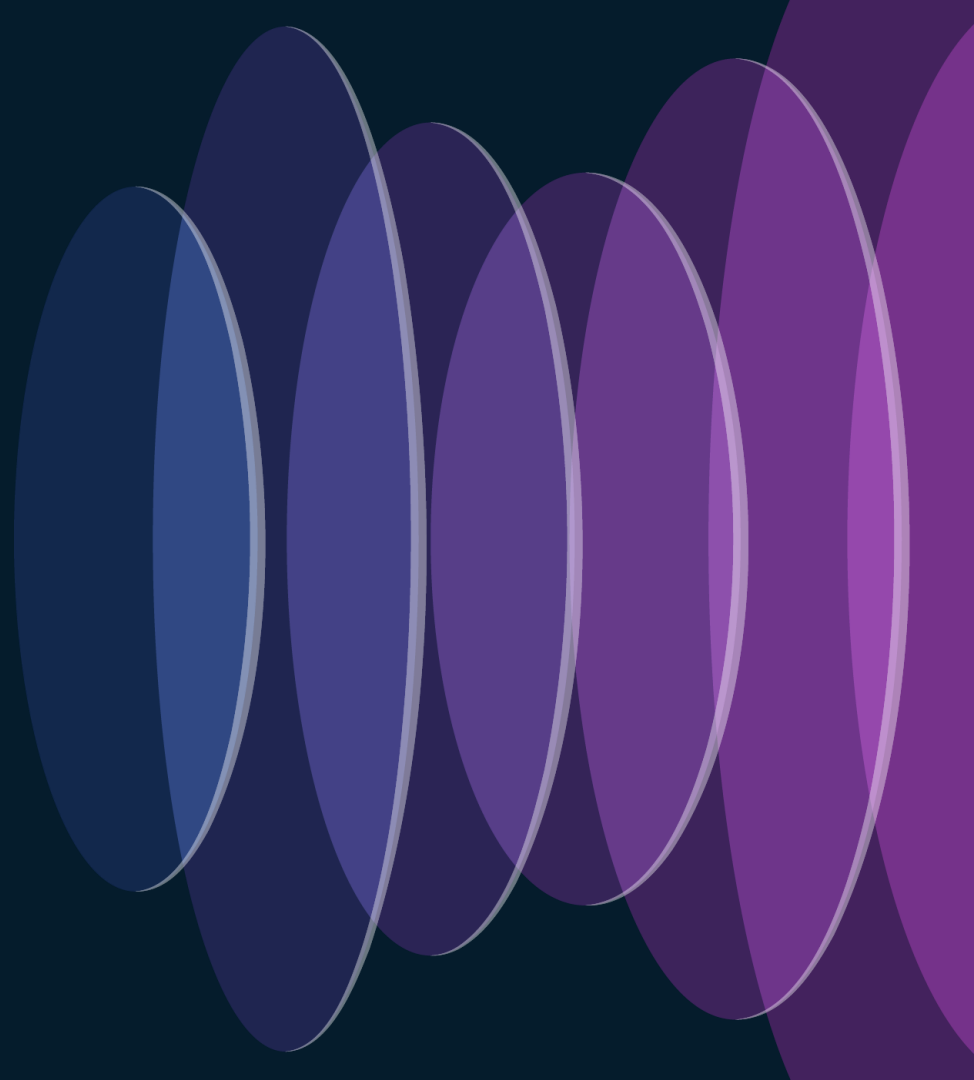
Secure Private Access (Clientless)

No VPN, No Client

↔ Clientless Access
🔒 Secure Tunnel

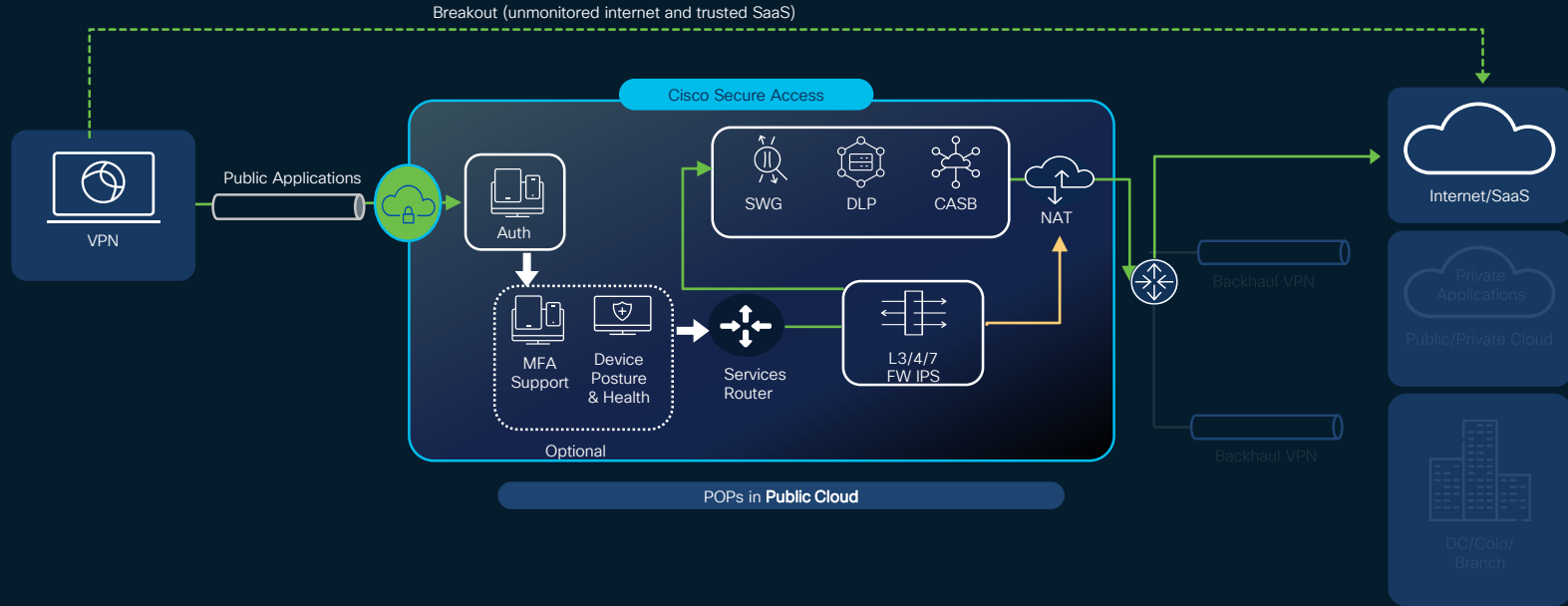
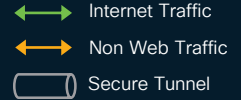


Secure Internet Access

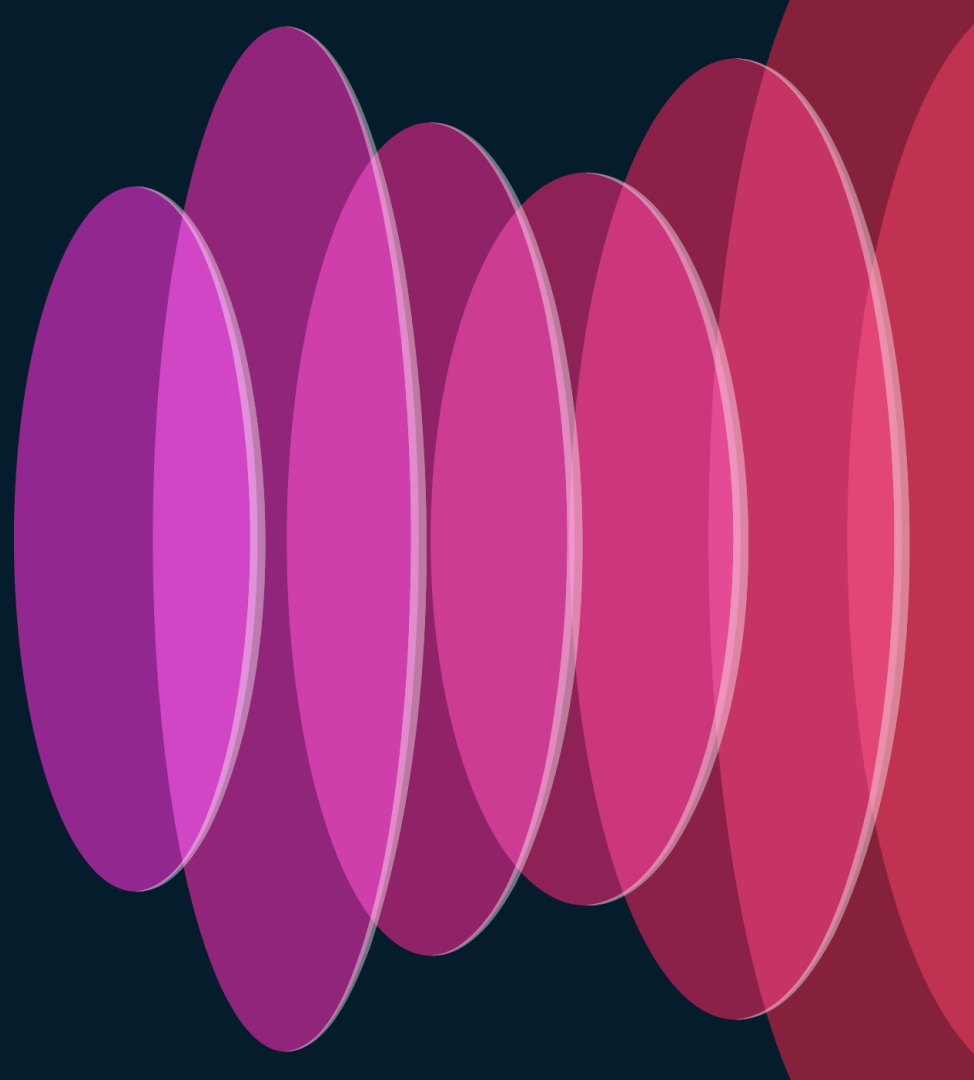


Secure Internet Access

Typically coupled with Secure Private Access via VPNaaS

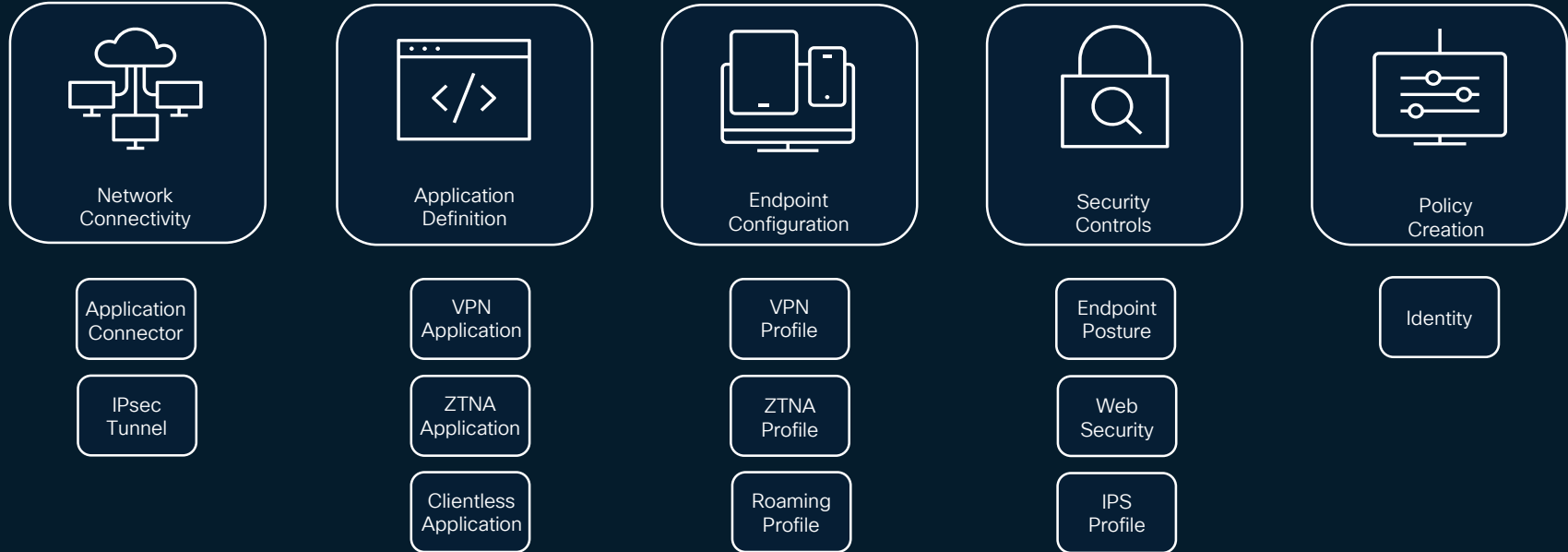


Unified Intent Based Policy



Modular Policy

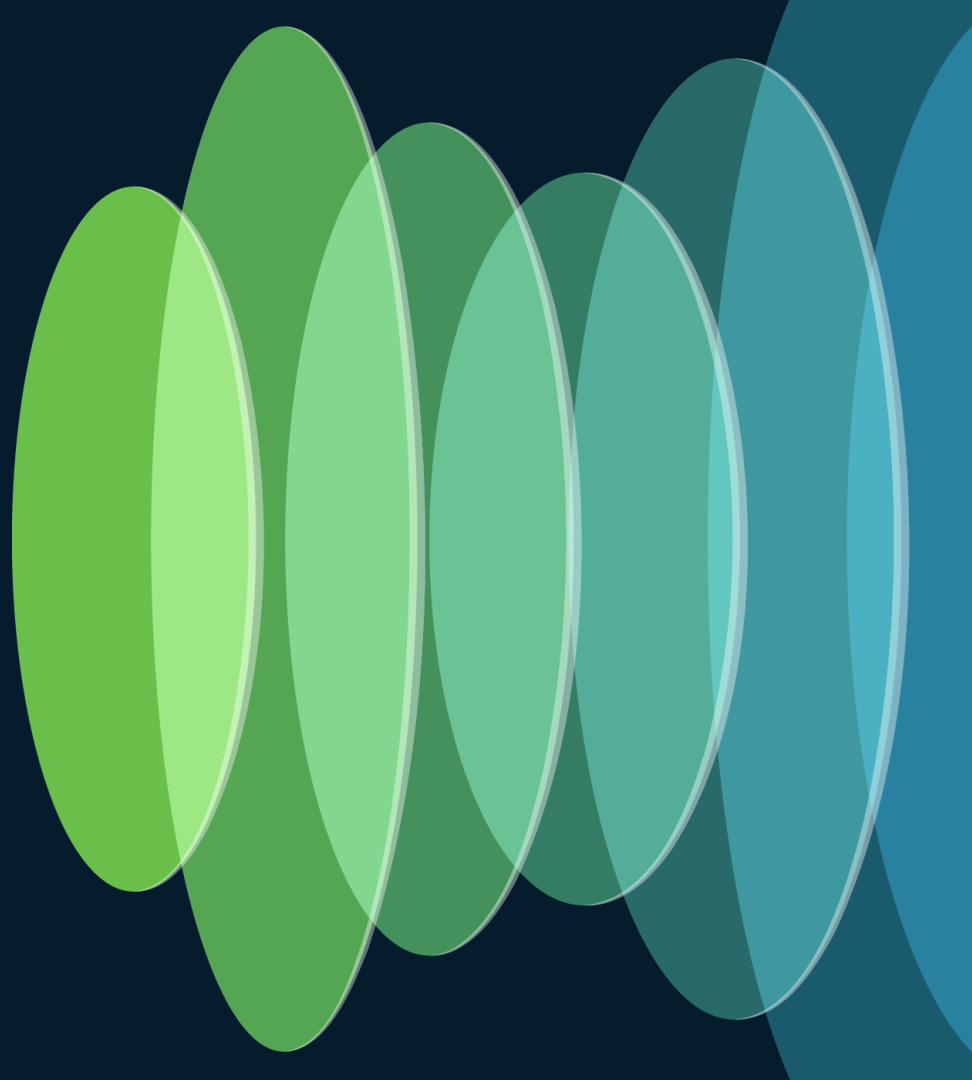
Configure Once – Use Everywhere



Cisco Secure Access *simplifies* your
hybrid worker *security* strategy

A *thoughtful migration strategy* is key

Migration Strategy





Tim Rowley

24 years of experience

Various roles @ Cisco

Solutions Architect

Principal architecture lead for CX Security product management

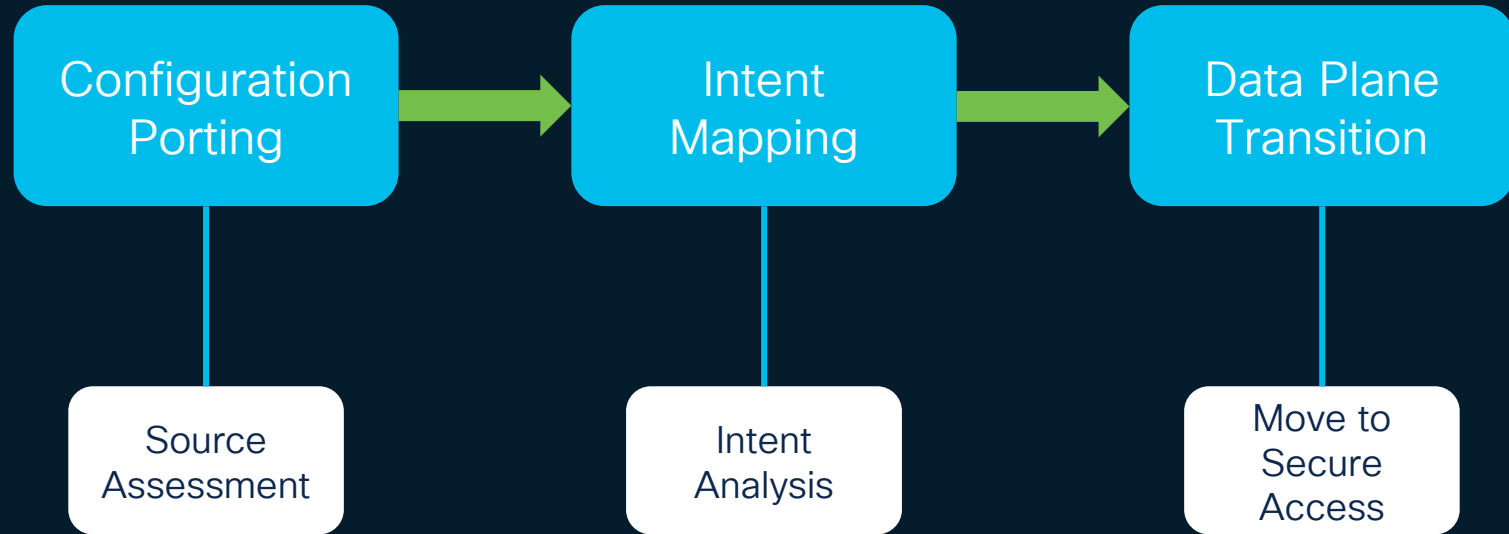
Certifications

CCIE #25960 Security and Wireless

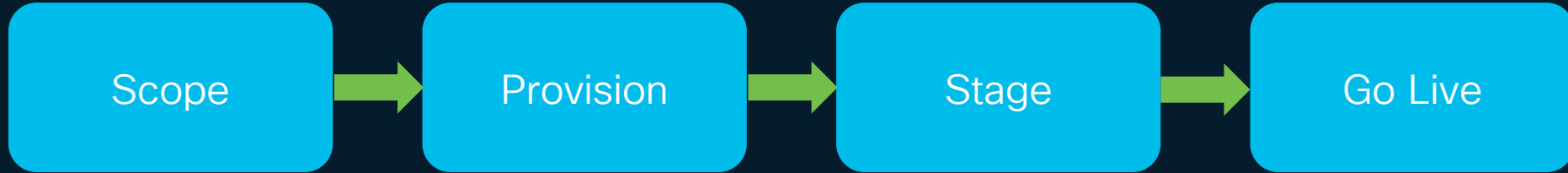
CISSP, CCSP, CWNE #124

Lives in Nashville, TN with wife, 2 kids and 2 dogs

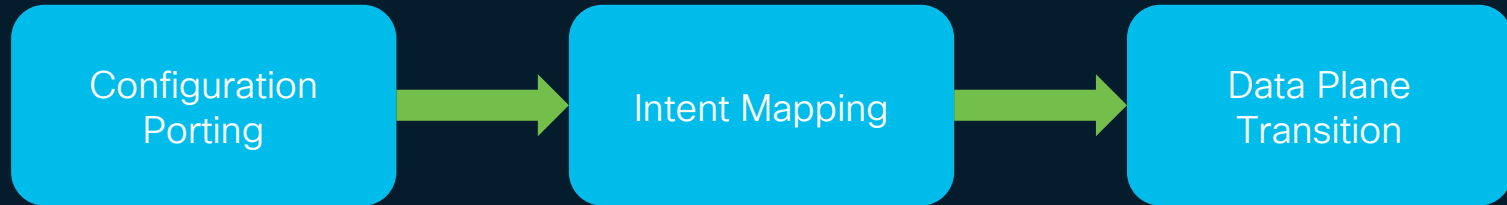
Major milestones add structure to the strategy



Migration phases support the milestones



Milestones



Map your source intent to Secure Access



On-prem RAVPN Termination

1. User connectivity
2. AAA
3. Posture
4. App reachability
5. Policy



Cisco Secure Access

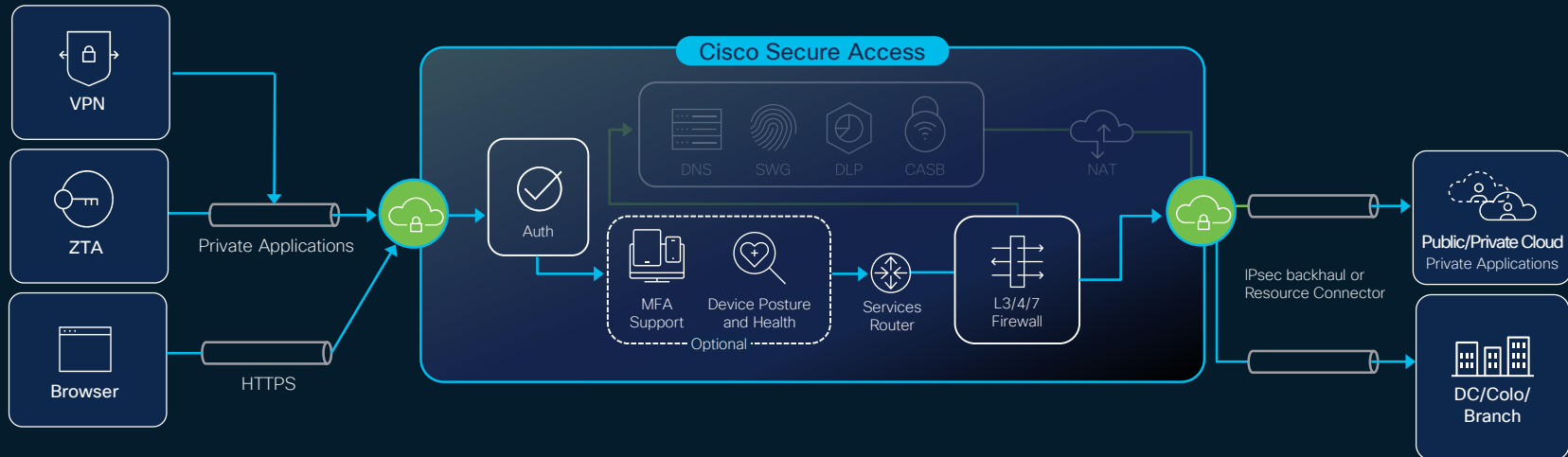
1. VPN Profiles
2. AAA within VPN Profile
3. Connect time posture
4. App reachability
 - a. IPsec backhaul
 - b. Resource Connector
5. Access Policy

Scope

Configuration
Porting

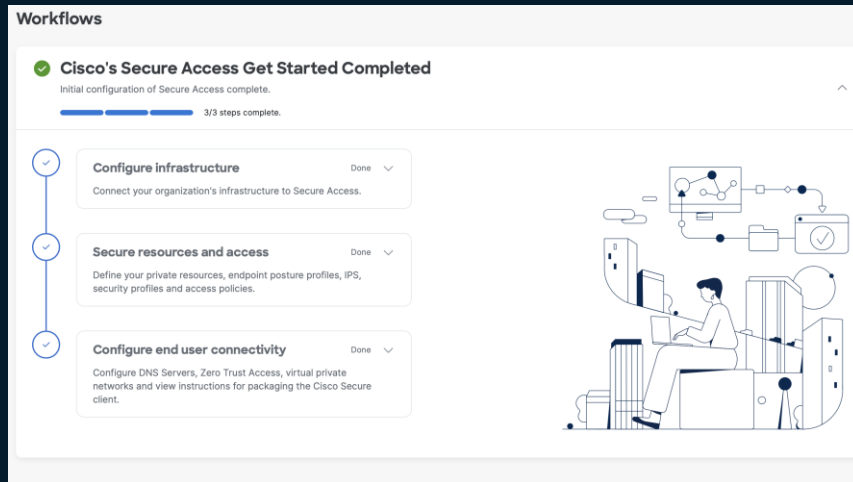
Intent
Mapping

- Requirements gathering and design
- Deep analysis of source configs and intents
- Start to document migration plan



Provision

- Bootstrap mindset
- Fundamental policy elements and system settings
- Have at it! Zero risk!

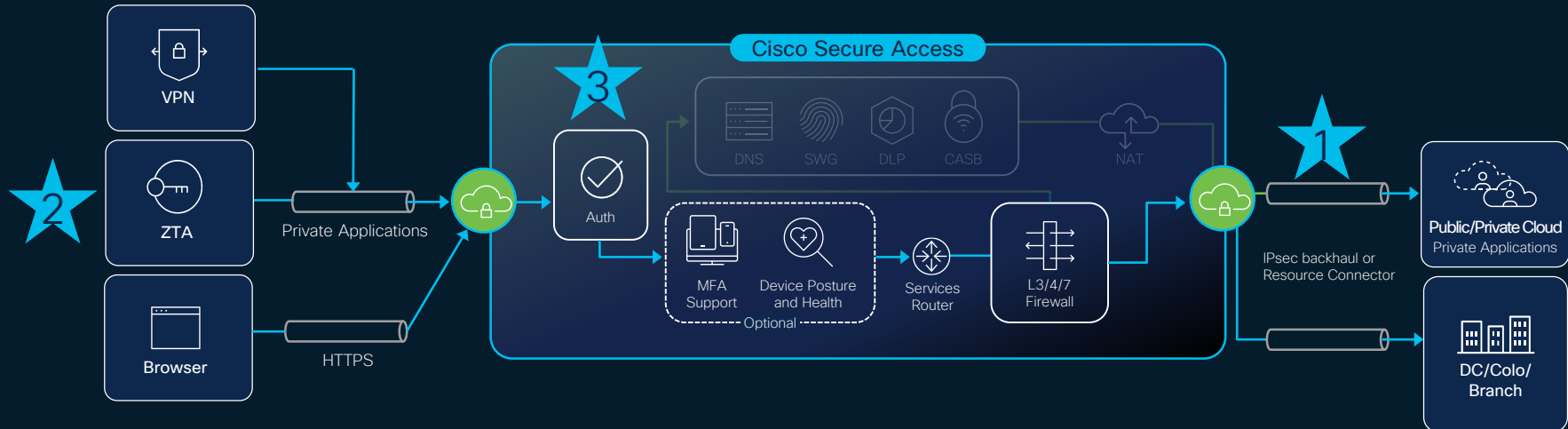


Stage

Configuration
Porting

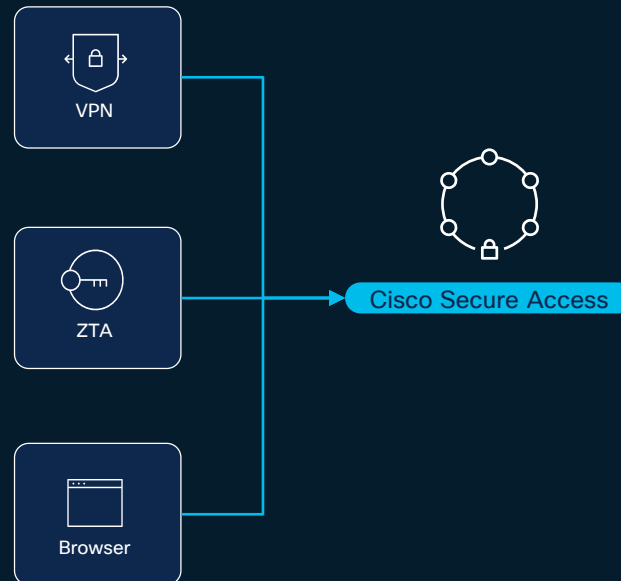
Intent
Mapping

1. Network connections (Back-end)
2. End user connectivity (Front-end)
3. Incremental policy additions with testing!



Go Live!

- Cutover occurs at your pace!
- Activate flows
- Redirect users
- Source system is still usable



Assess, plan and pace your migration



Cisco Secure Access Strategy and Implementation Services



Project Management



Solution Requirements
and Design



Implementation and
Testing



Migration Plan and
Execution



Knowledge Transfer

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 2025.



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

Continue the conversation in the session's Webex Team Space



Continue your education

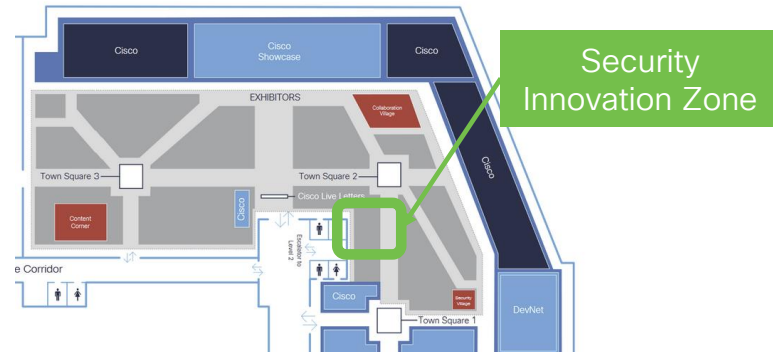
CISCO *Live!*

- Hear Tom Gillis at the Security Deep Dive Keynote KDDSEC-1000!

*Securing User to Application and
Everything in Between*

Wednesday, June 5 | 1 – 2pm

- Visit us at the Security Innovation Zone (#4435) for demos and workshops



Cisco Secure Access *simplifies* your hybrid
worker *security* strategy

A *thoughtful migration strategy* is key



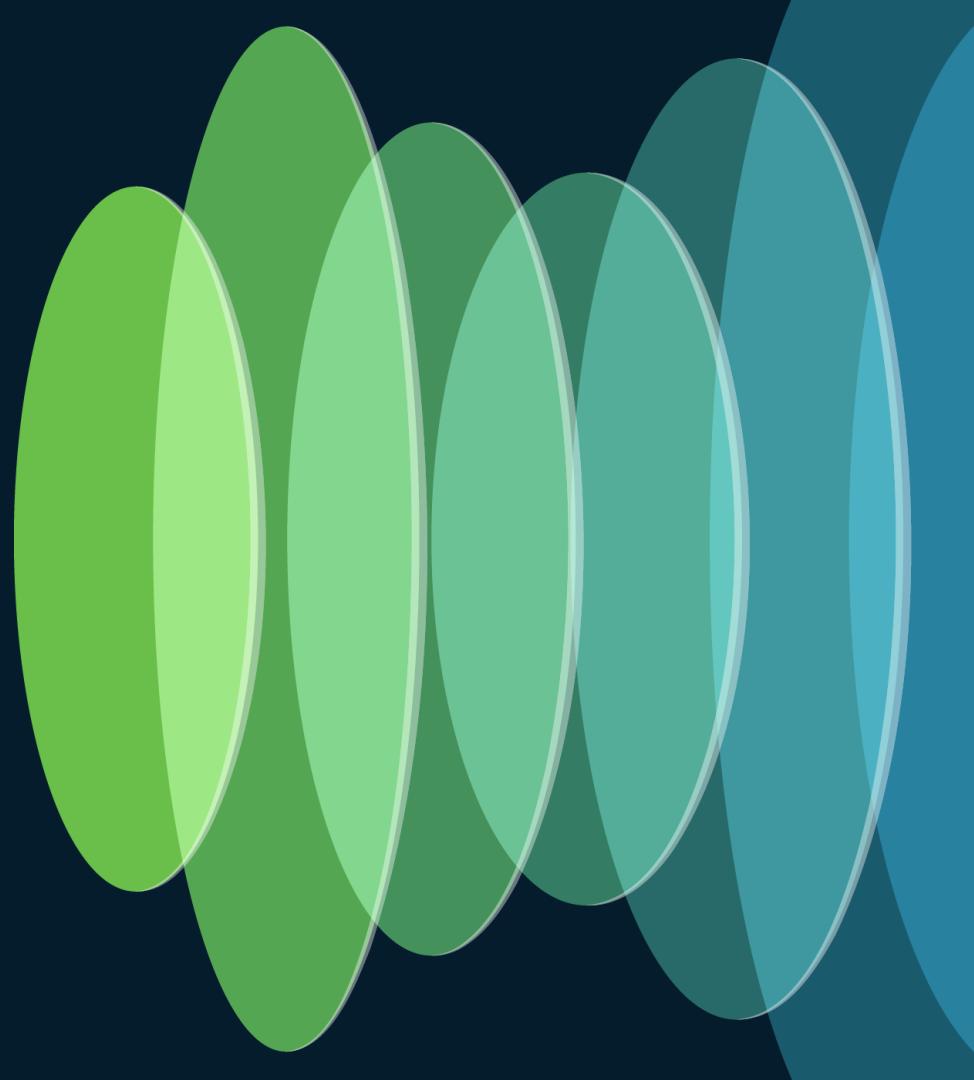
The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

Intent Mapping Appendix



VPN Profiles

Secure Access

Overview

The Overview dashboard displays

Essentials

- Network Connections
Connect data centers, tunnels, resource connectors
- Users and Groups
Provision and manage users and groups for use in access rules
- End User Connectivity**
Manage traffic steering from endpoints to Secure Access

Secure Access

End User Connectivity

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

Zero Trust **Virtual Private Network** Internet Security

FQDN [Regional FQDN's](#)

Global: ed9d.vpn.sse.cisco.com [Copy](#)

VPN Profiles

A VPN profile allows for configuration of remote user connections through a VPN. [Help](#)

AAA

Secure Access

← End User Connectivity
VPN Profile

A VPN profile allows for configuration of remote user connections through a VPN. [Help](#)

VPN Profile name
VPNProfile

General settings
Default Domain: cxsaaslab.com | DNS Server: Umbrella (208.67.222.222, 208.67.220.220) | Protocol: TLS / DTLS

2 Authentication, Authorization, and Accounting
SAML

Authentication, Authorization, and Accounting
Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication Authorization Accounting

Connect Time Posture

Secure Access

← End User Connectivity
VPN Profile
A VPN profile allows for configuration of remote user connections through a VPN. [Help](#)

VPN Profile name
VPNProfile

General settings
Default Domain: cxsaslab.com | DNS Server: Umbrella (208.67.222.222, 208.67.220.220) | Protocol: TLS / DTLS

Authentication, Authorization, and Accounting
SAML

Traffic Steering (Split Tunnel)
Connect to Secure Access | 1 Exceptions

Cisco Secure Client Configuration

Default Domain
lab.local

DNS Server
Use region configuration + New

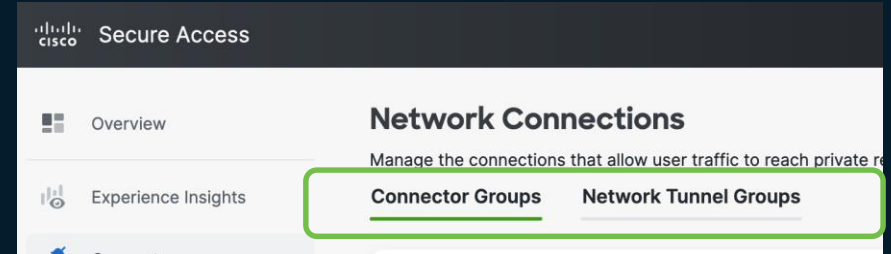
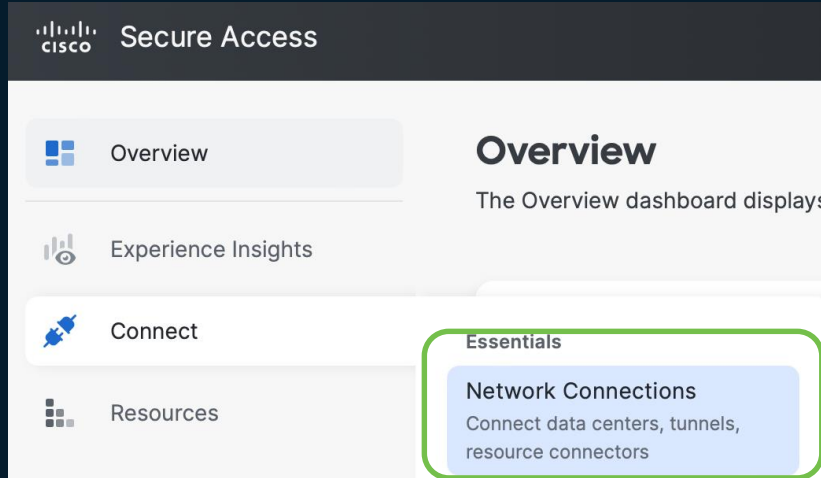
Profile Settings
☐ Include regional FQDN

Protocol
☒ TLS / DTLS
☐ IPsec (IKEv2)

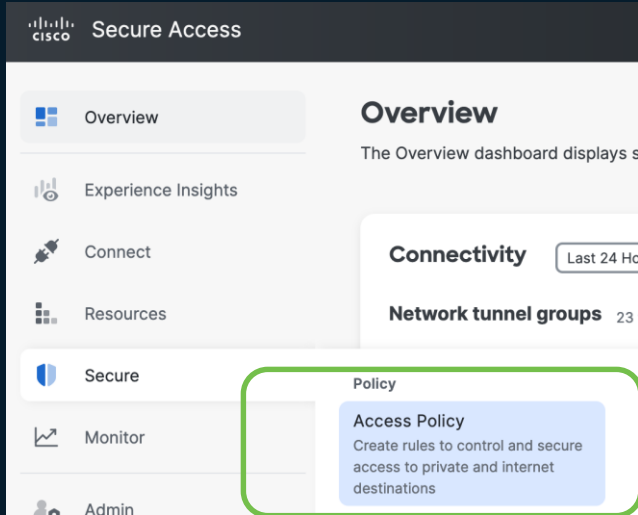
Connect time posture (optional)
None

Multiple VPN postures can be created in Posture.

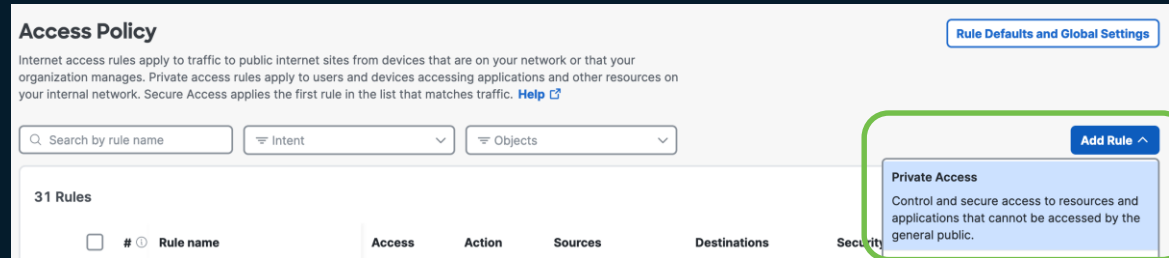
Back-end Connectivity



Access Policy



The screenshot shows the Cisco Secure Access Overview dashboard. The left sidebar contains navigation links: Overview, Experience Insights, Connect, Resources, Secure, Monitor, and Admin. The main content area is titled 'Overview' and includes a description: 'The Overview dashboard displays s'. Below this, there are sections for 'Connectivity' (with a 'Last 24 Ho' filter) and 'Network tunnel groups' (with a '23 t' filter). A green box highlights the 'Policy' section, which contains a card for 'Access Policy' with the description: 'Create rules to control and secure access to private and internet destinations'.



The screenshot shows the Cisco Access Policy configuration page. The top right has a link for 'Rule Defaults and Global Settings'. Below the header, there is a search bar and filters for 'Intent' and 'Objects'. A green box highlights the 'Add Rule ^' button. Below the filters, it says '31 Rules'. A table with columns '#', 'Rule name', 'Access', 'Action', 'Sources', 'Destinations', and 'Security' is partially visible. A green box highlights a tooltip for 'Private Access' with the description: 'Control and secure access to resources and applications that cannot be accessed by the general public.'