cisco Live!

Let’s go

#CiscoLive

The bridge to possible

Is VPN Really Dead and Replaced by Zero Trust Network Access (ZTNA)?

Tavo Medina
Technical Solutions Acrhitect
https://www.linkedin.com/in/tavo-medina/

BRKSEC-1015

Cisco Webex App

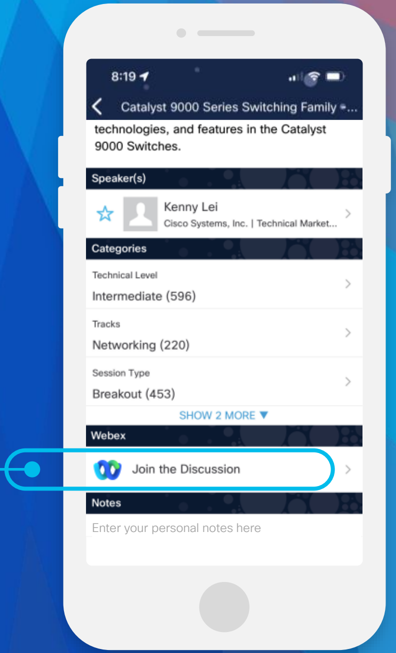
Questions?

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 9, 2023.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1015

cisco Live!

Agenda

- Introduction
- VPNs vs ZTNA
- Comprehensive Comparison
- Real-World Use Cases
- Conclusion

$ whoami

- ~~Gus~~tavo Medina
- Technical Solutions Architect
- Costa Rican CR
  - Currently living in Mexico MX
- Joined Cisco (TAC) in 2009
- CCIE Security #51487
- Football Fan

Introduction

Let’s go

What is ZTNA?

Zero Trust

VPNaaS

ZTA

ZTNA

> *“ ZTNA augments traditional VPN technologies for application access, and removes the excessive trust once required to allow employees and partners to connect and collaborate. Security and risk management leaders should pilot ZTNA projects as part of a SASE strategy or to rapidly expand remote access.”*

Gartner Market Guide for Zero Trust Network Access – June 2020

Gartner Use Cases for ZTNA

Internal-workforce remote access

- Controlled access to organizational resources for workers using managed devices.
- Full port and protocol support for proprietary, complex, or legacy applications.
- Web application, Secure Shell (SSH), or Remote Desktop Protocol (RDP) access may be sufficient in some cases.

Extended-workforce remote access and BYOD

- Includes suppliers, partners, potential acquired companies, and scenarios with less control over identity.
- Limitations on sharing applications using Zero Trust Network Access (ZTNA) due to lack of organizational control over endpoints and users
- Agents may not be an option for this use case

Privileged remote access

- Control access for privileged IT users.
- Integration with Privileged Access Management (PAM) tools.
- Access to SSH, RDP, or other IT admin tools, including legacy admin tools with nonroutable protocols in some cases.

On-premises access

- Control access to organizational resources within the local or wide-area network.
- Enforces remote access policies for other use cases on-premises.
- May require network rearchitecture to ensure security gateway enforcement.

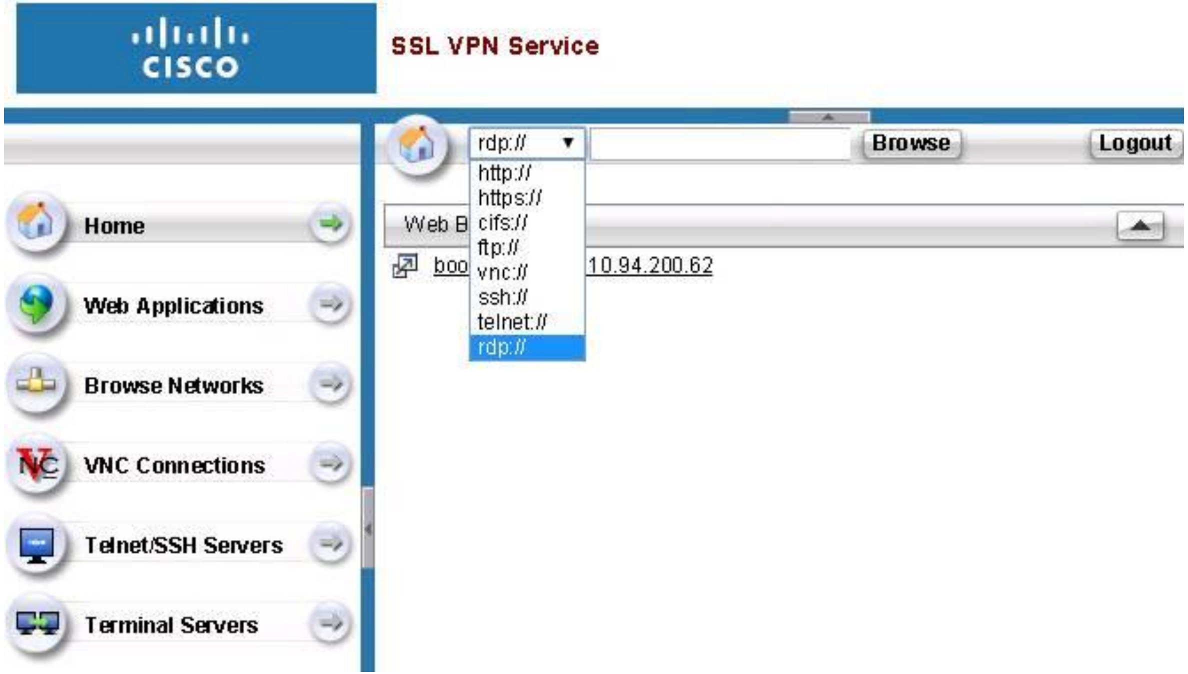
VPN vs ZTNA

VPN	ZTNA
Requires VPN client software	No client software required *
Access to full network or network segment	Access to specific applications
Posture assesed once at VPN authentication	Posture assesed at each application access
1:1 Client-to-Headend relationship	Client can connect to different headends per application

We had WebVPN Clientless before ZTNA was even a concept

Supported since ASA 7.1
*Deprecated on 9.17

VPN 3000
Series Concentrator
supported Clientless



Why Zero Trust Network Access (ZTNA)?

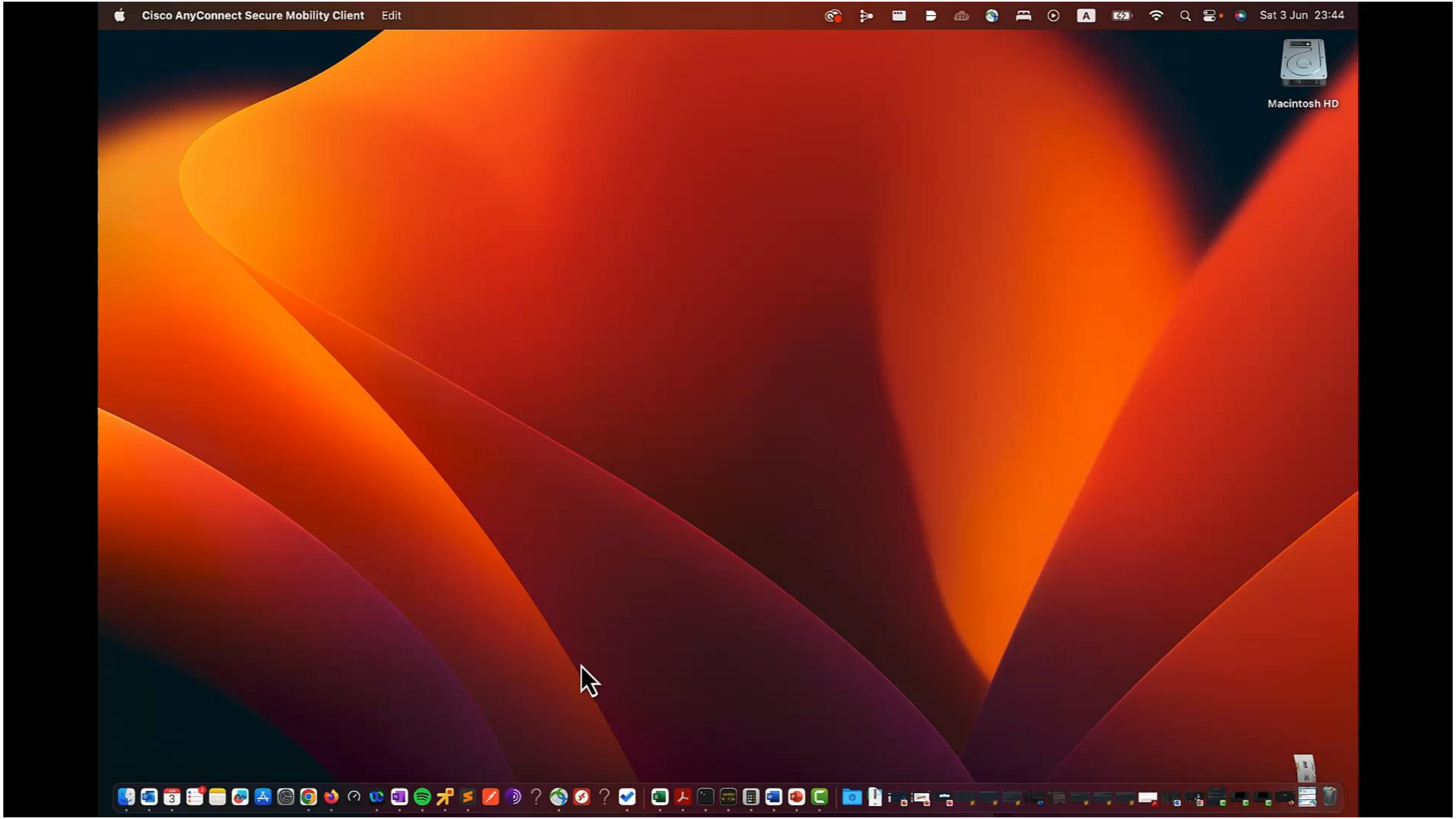
“Although traditional VPNs have been a mainstay for decades, ZTNA is the natural evolution of VPN and offers better security, more granular control, and a better user experience in light of the complexity of today’s networks, so it can be a smarter choice for securely connecting a remote workforce.”

Zero Trust, ZTA, and ZTNA: What’s the difference? - CSO

VPN objections

- VPNs provide a bad user experience.
- VPN assumes that anyone or anything passing network perimeter controls can be trusted.
- ZTNA (Zero Trust Network Access) takes the opposite approach by not trusting any user or device until proven otherwise.
- ZTNA extends the zero-trust model beyond the network.
- ZTNA reduces the attack surface by hiding applications from the internet.

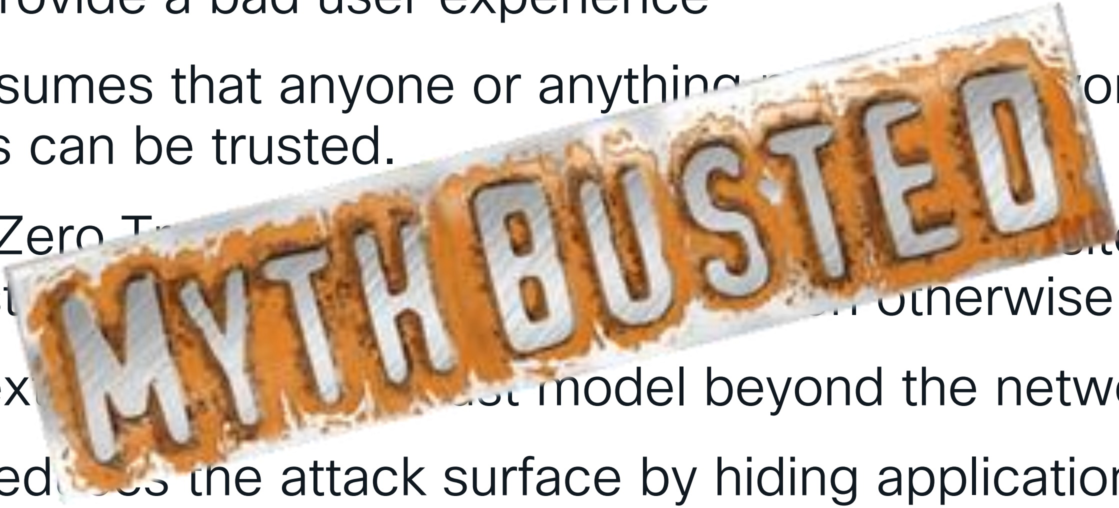
AnyConnect Demo



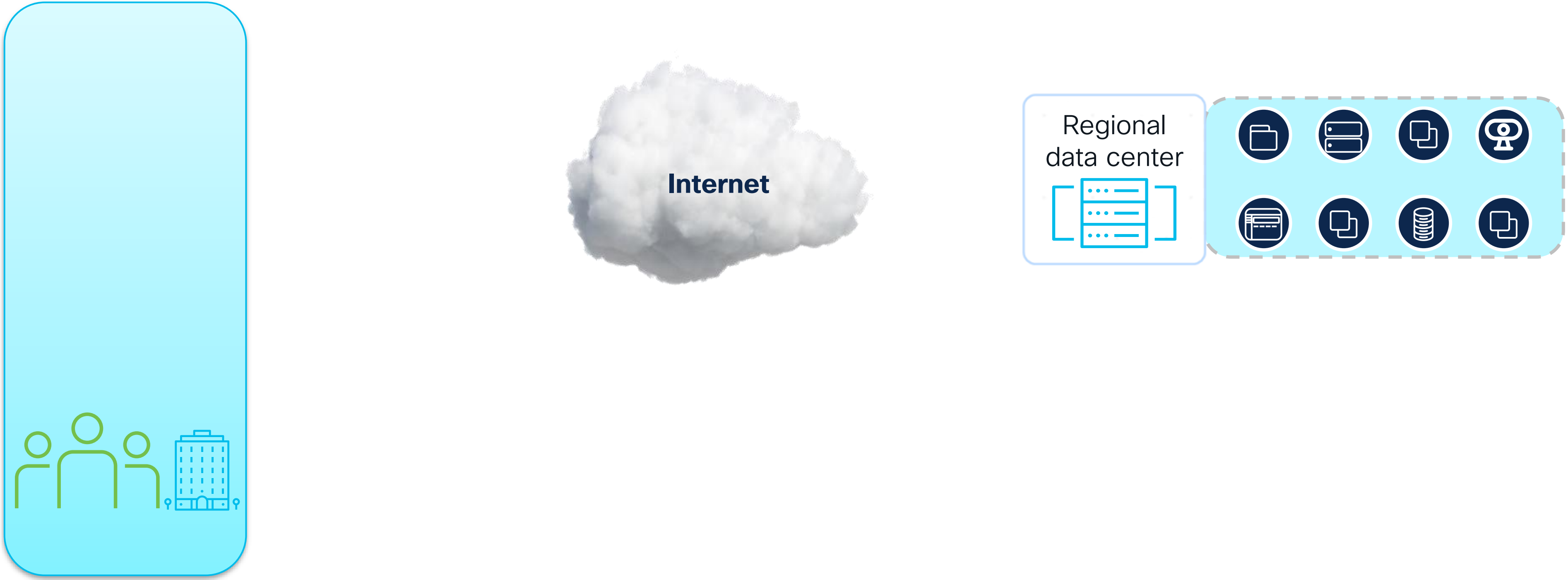
Cisco AnyConnect Secure Mobility Client
Edit
Sat 3 Jun 23:44
Macintosh HD

VPN objections

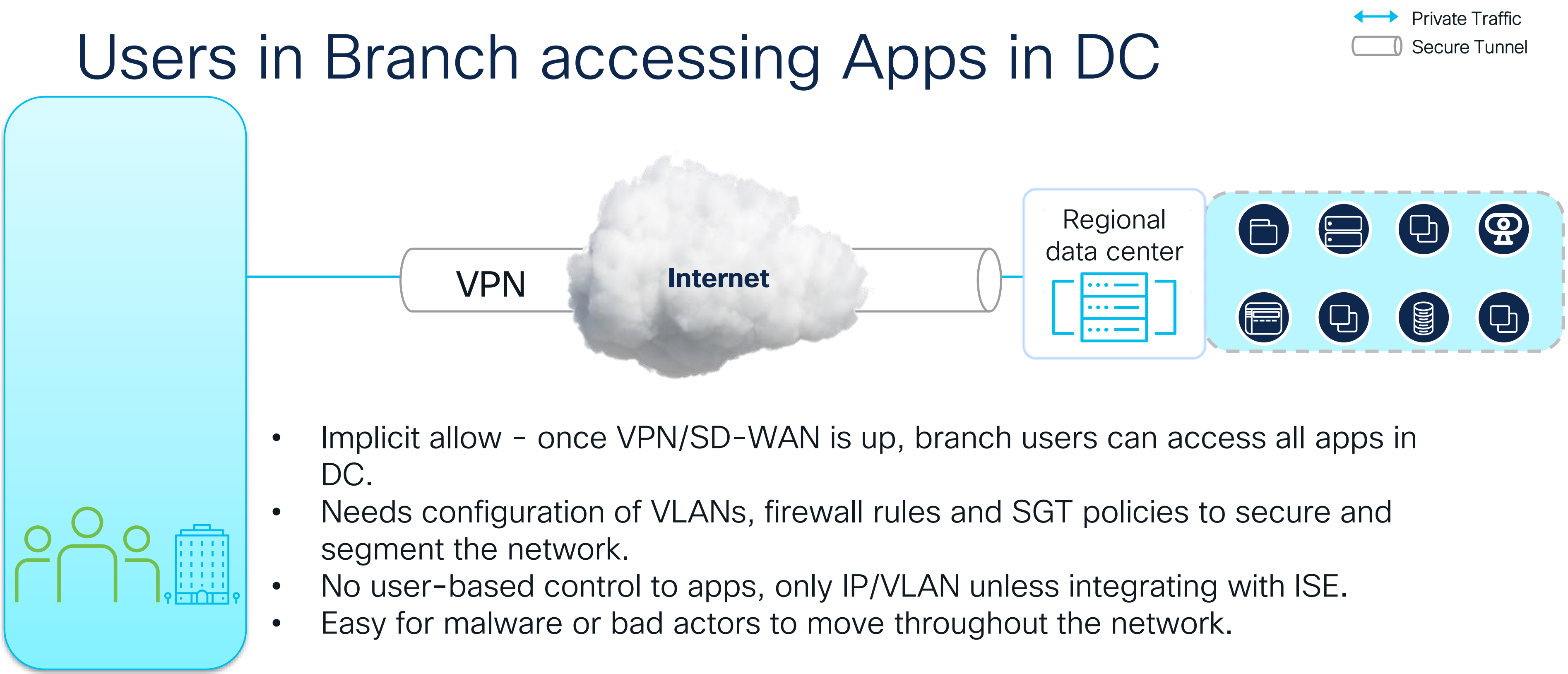
- VPNs provide a bad user experience
- VPN assumes that anyone or anythin[illegible]ork perimeter controls can be trusted.
- ZTNA (Zero T[illegible]ite approach by not trust[illegible] otherwise.
- ZTNA ex[illegible] model beyond the network.
- ZTNA red[illegible] the attack surface by hiding applications from the internet



Users in Branch accessing Apps in DC

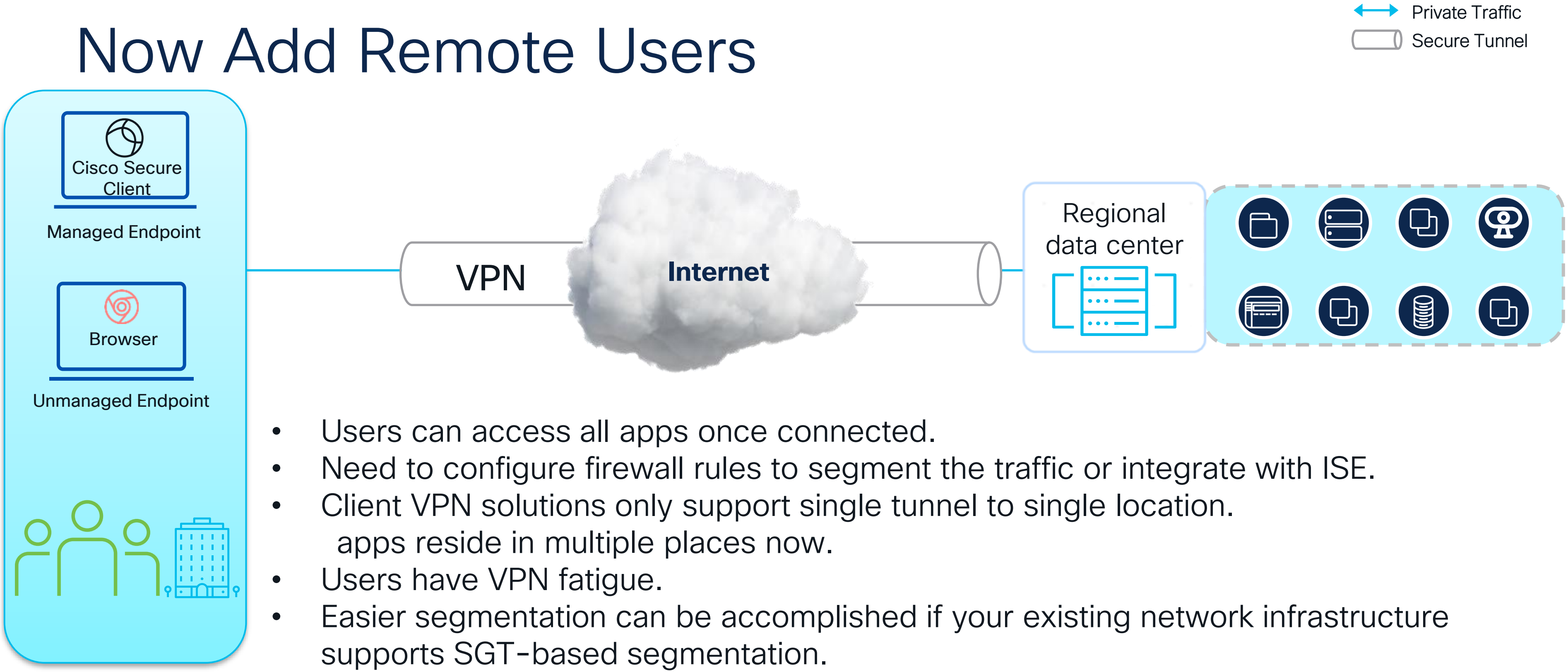


Users in Branch accessing Apps in DC



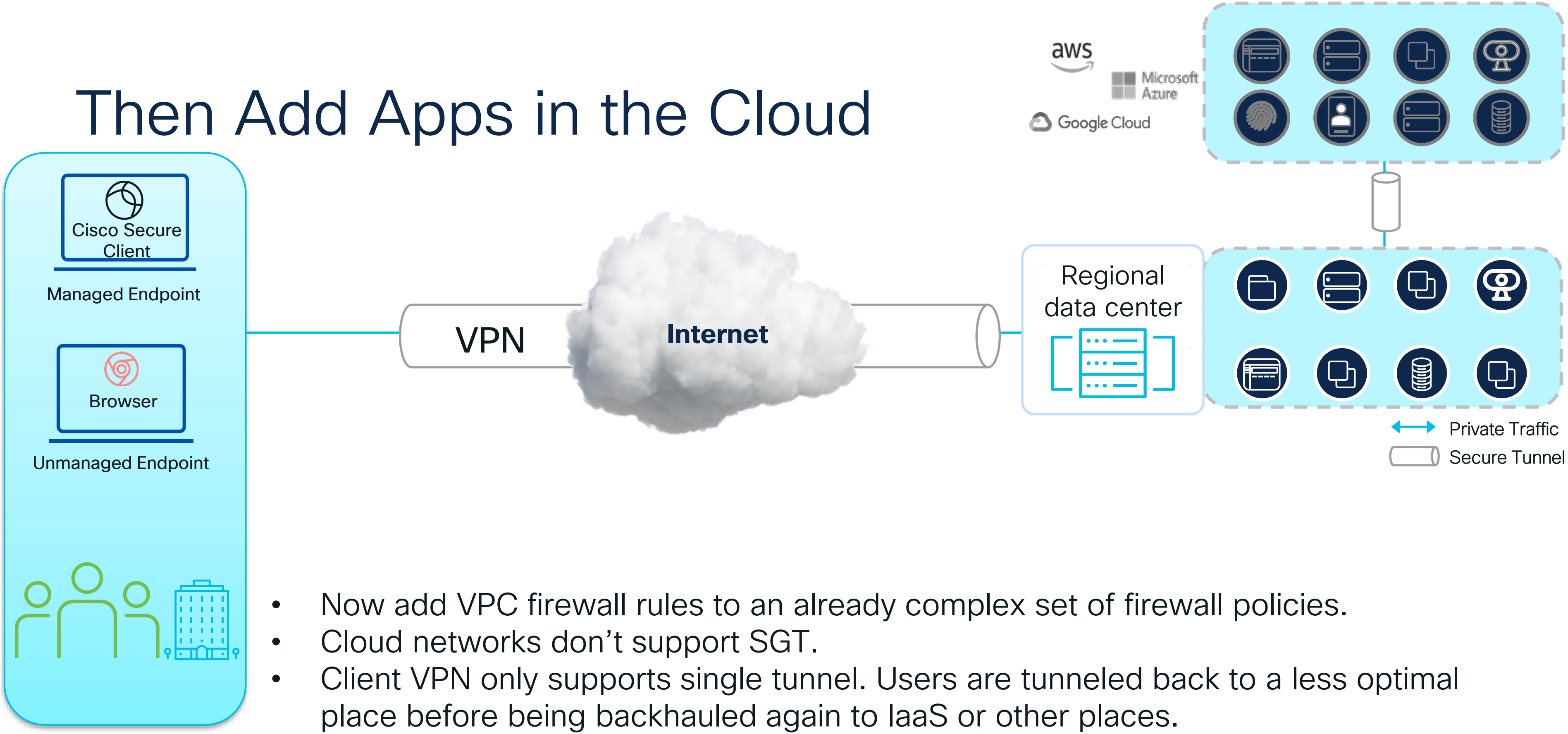
- Implicit allow - once VPN/SD-WAN is up, branch users can access all apps in DC.
- Needs configuration of VLANs, firewall rules and SGT policies to secure and segment the network.
- No user-based control to apps, only IP/VLAN unless integrating with ISE.
- Easy for malware or bad actors to move throughout the network.

Now Add Remote Users



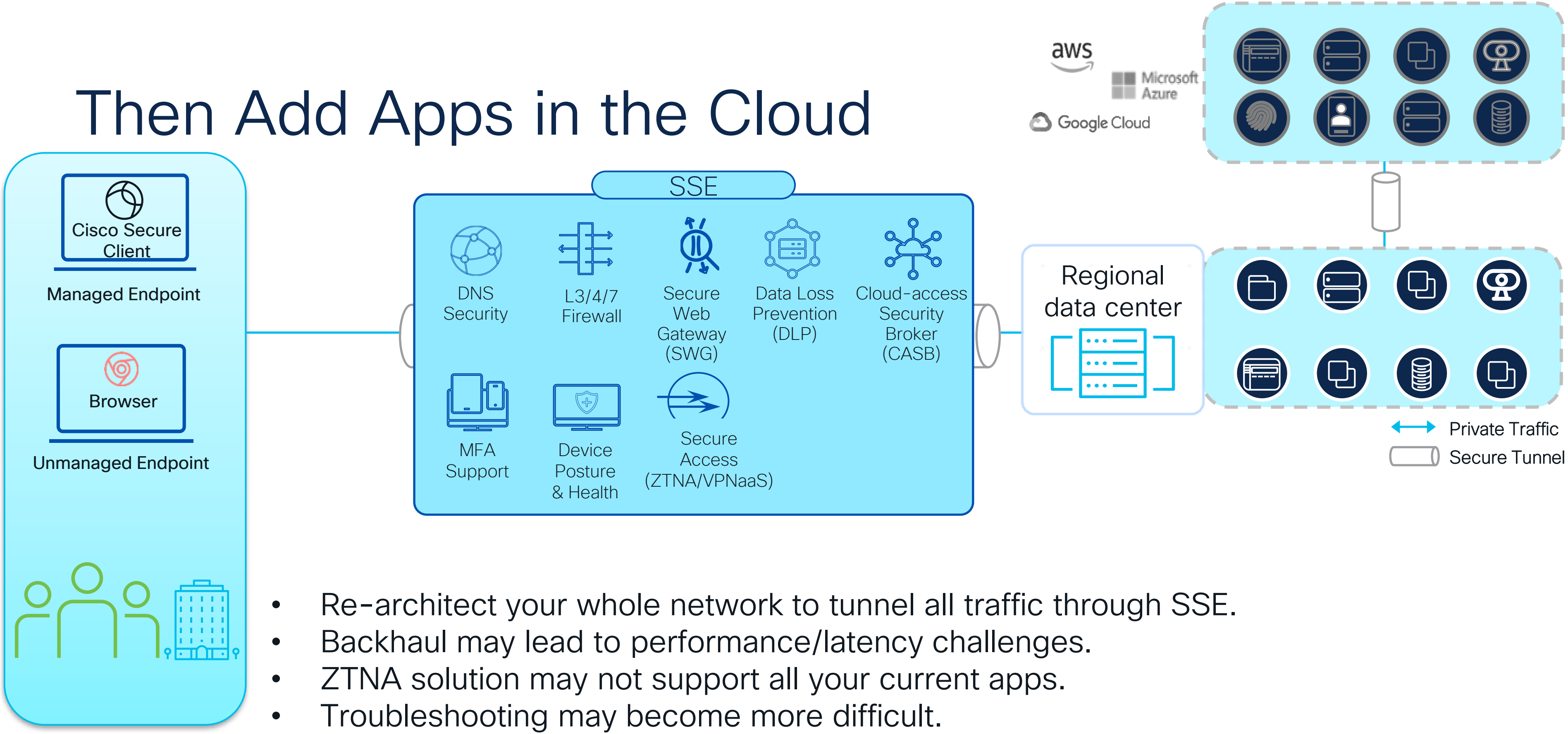
- Users can access all apps once connected.
- Need to configure firewall rules to segment the traffic or integrate with ISE.
- Client VPN solutions only support single tunnel to single location.
  apps reside in multiple places now.
- Users have VPN fatigue.
- Easier segmentation can be accomplished if your existing network infrastructure supports SGT-based segmentation.

Then Add Apps in the Cloud



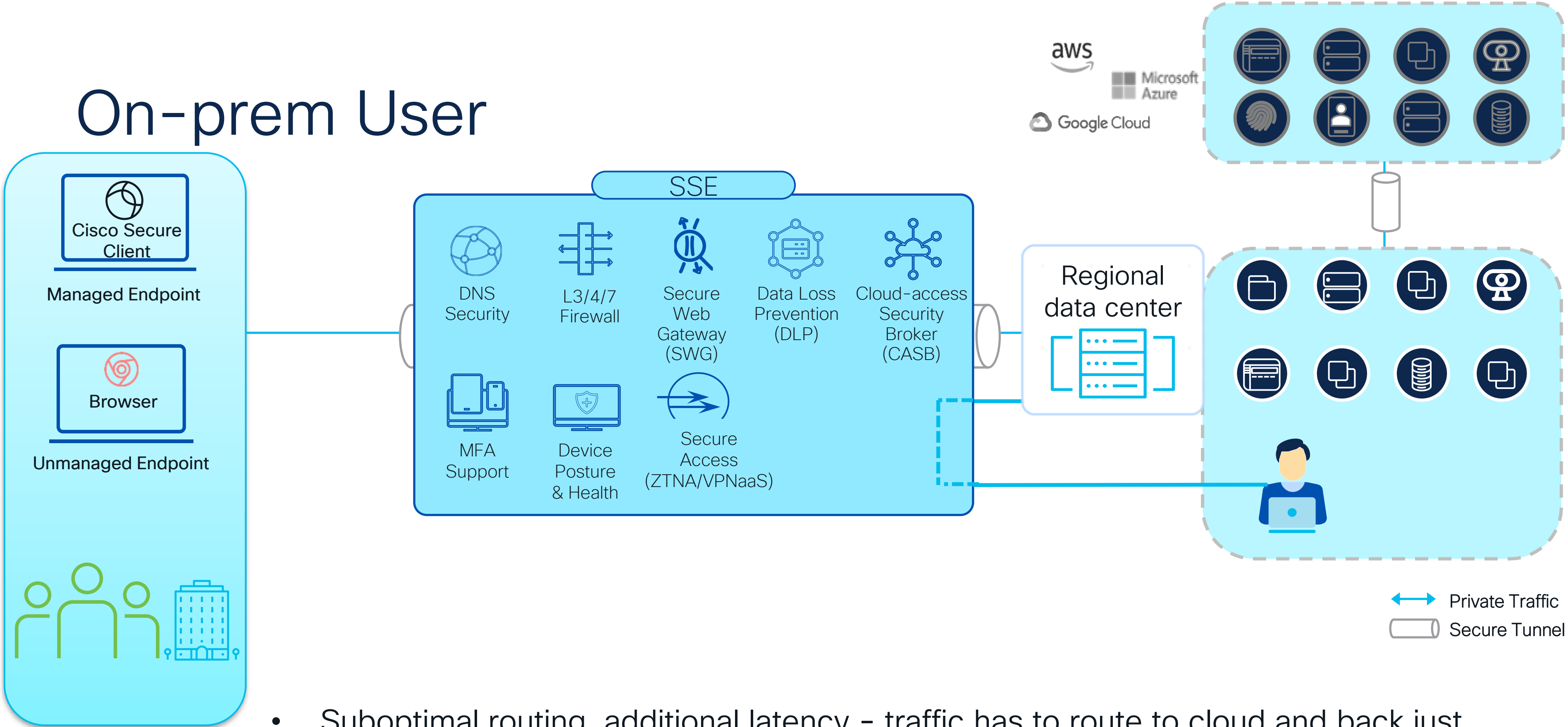
- Now add VPC firewall rules to an already complex set of firewall policies.
- Cloud networks don’t support SGT.
- Client VPN only supports single tunnel. Users are tunneled back to a less optimal place before being backhauled again to IaaS or other places.

Then Add Apps in the Cloud



- Re-architect your whole network to tunnel all traffic through SSE.
- Backhaul may lead to performance/latency challenges.
- ZTNA solution may not support all your current apps.
- Troubleshooting may become more difficult.

On-prem User



- Suboptimal routing, additional latency - traffic has to route to cloud and back just to traverse inter-vlan.
- Unnecessary WAN utilization just for local routing within a site.

Cisco ZTNA Options

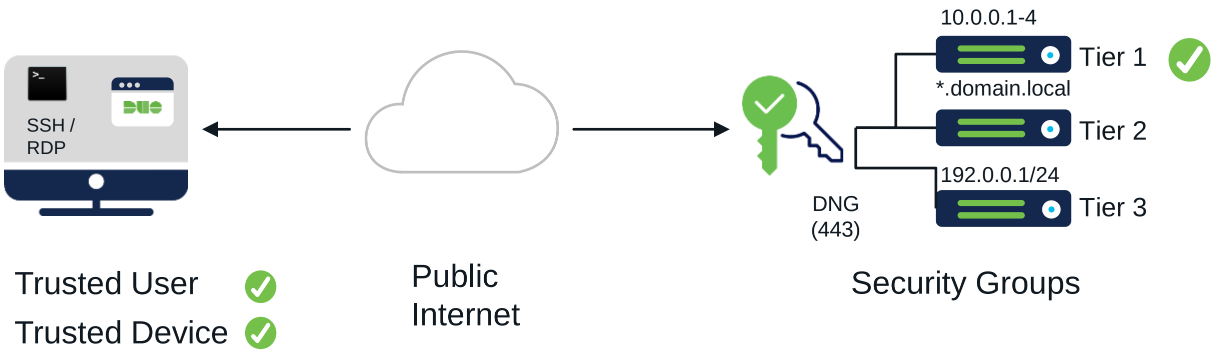
Cisco ZTNA Options

- ✓ Duo DNG
- ✓ FTD ZTNA 7.4
- ✓ Cisco Secure Access

Duo DNG

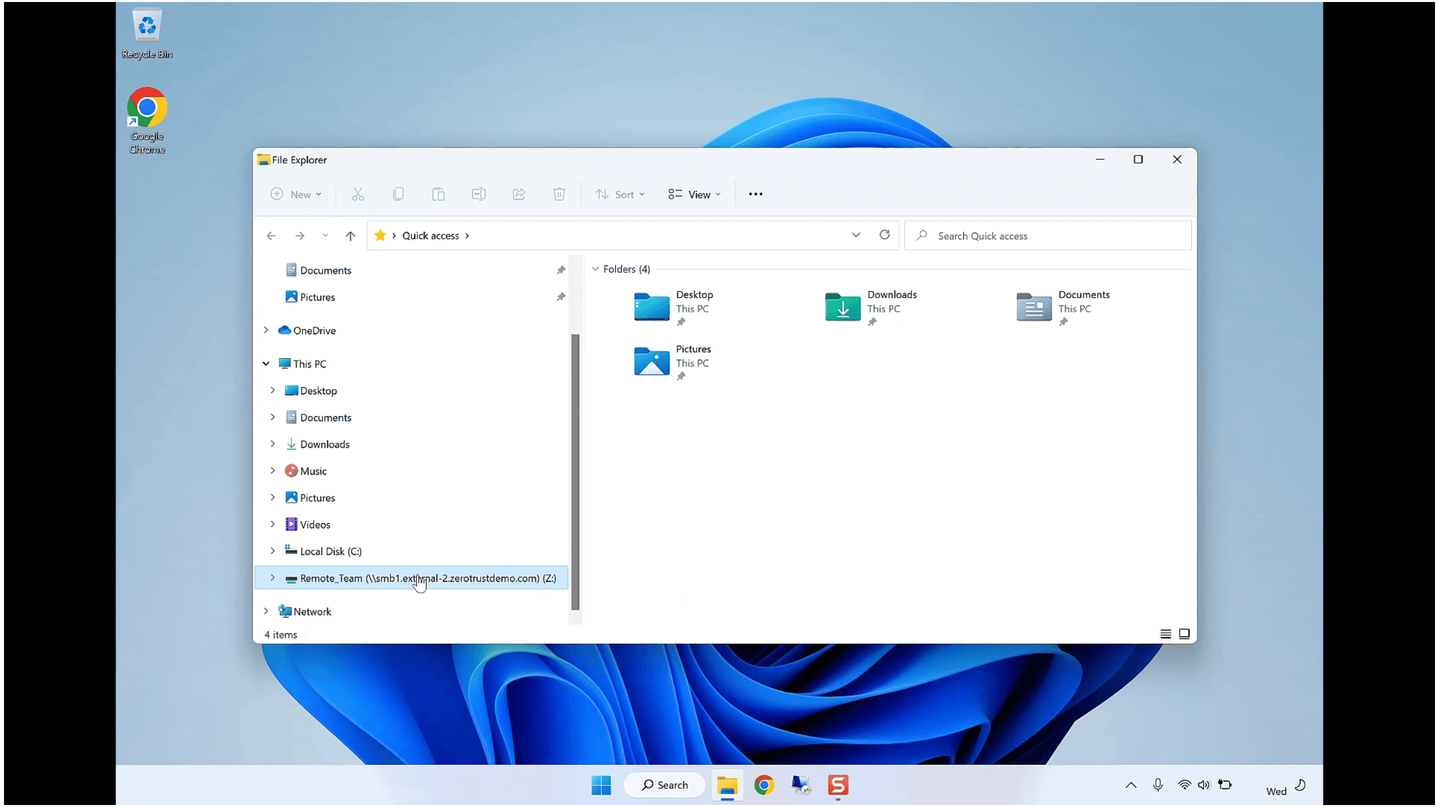
VPN-less Remote Access to Private Applications

Detect user & device context for internal apps with the Duo Network Gateway

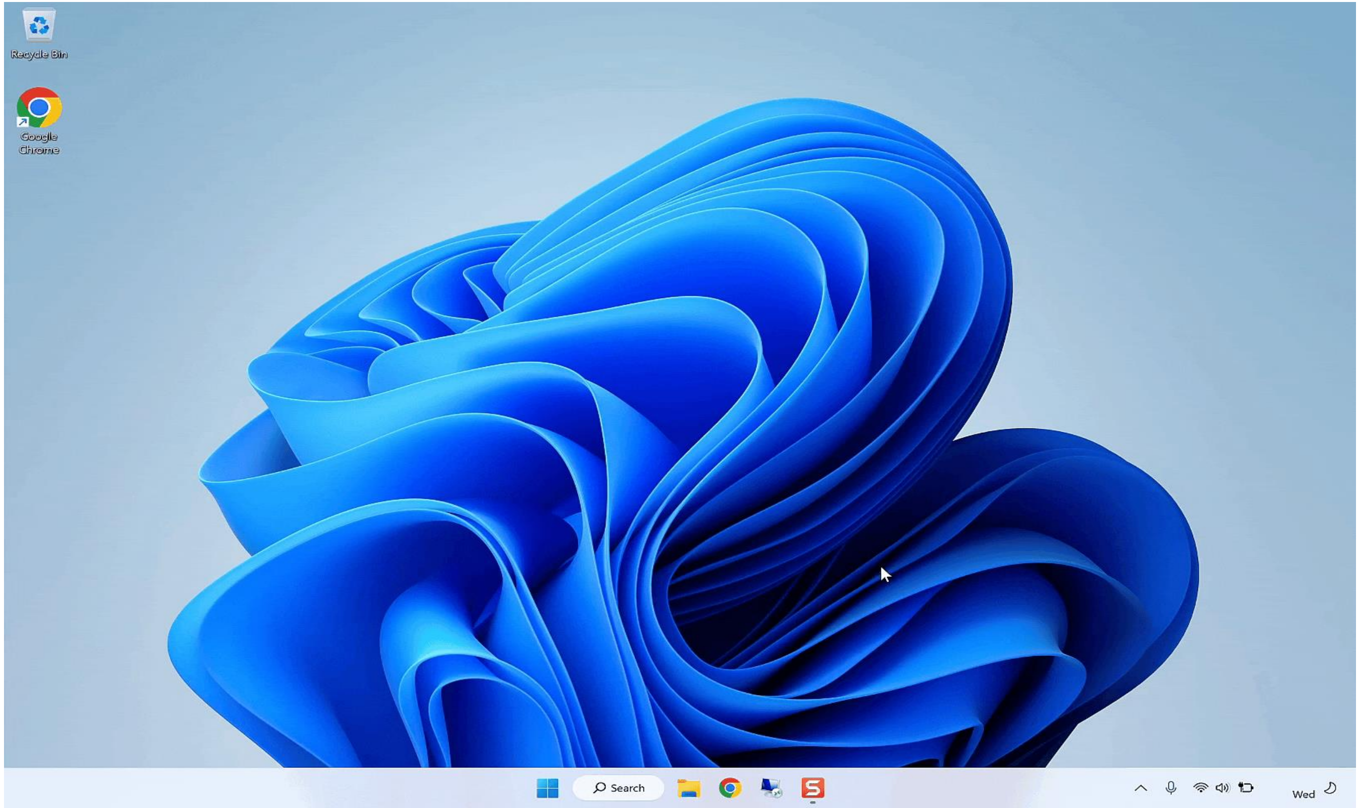


Supports: HTTP/S SSH RDP SMB

Demo: Shared Drive Access (SMB)



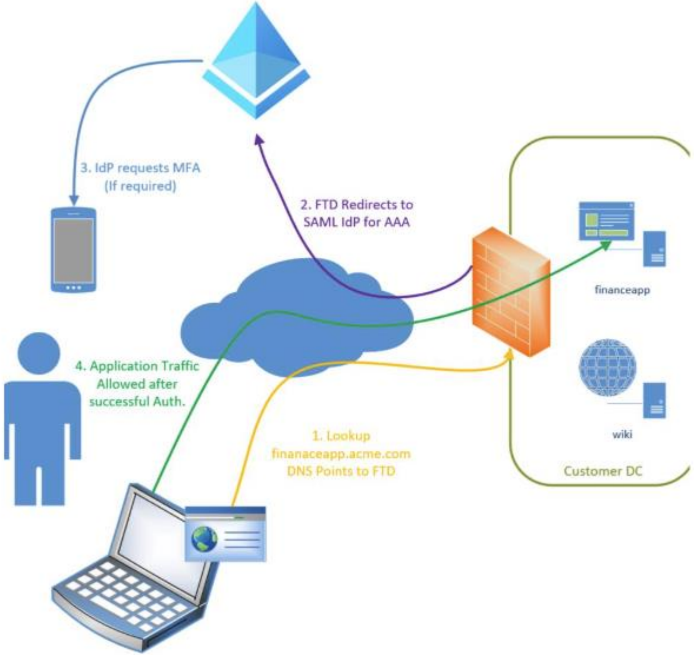
Demo: Remote Desktop Access



Cisco Secure Firewall ZTNA

Clientless ZTNA 7.4

- Allows HTTPS Browser-Based apps to be published through Secure Firewall.
- Requires DNS entry to point to Secure Firewall interface.
- Similar user experience to Duo Network Gateway.



Clientless (7.4) and Client-Based ZTNA

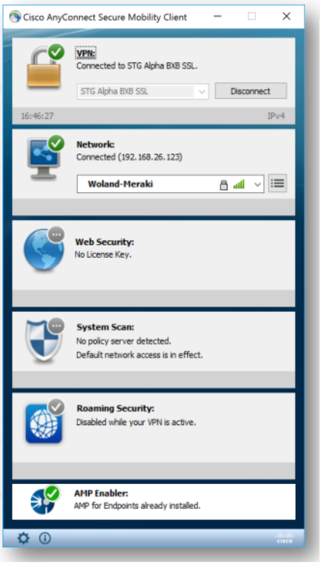
	Clientless ZTNA	Client-Based ZTNA
Endpoint Presence	No client application required on endpoint device	Client software required to be installed on endpoint device
Access Type	Can only be accessed through a web browser	Client software handles traffic transparent to the user
Application Type	Posture only available through authentication flow (e.g., Duo Health or Intune)	Client software handles posture based on policy (similar to HostScan or ISE Posture)
User Types	1:1 Client-to-Headend relationship	Client can connect to different headends per application

Cisco Secure Client ZTNA Module

Cisco AnyConnect

Suite of Security Service Enablement Modules

- VPN Module (Core)
- Network Access Manager (NAM)
- ~~Web Security (CWS)~~
- Posture
- Umbrella Module
- HostScan (aka: ASA posture) (No UI)
- Network Visibility Module (NVM) (No UI)
- ~~AMP Enabler Module~~
- Diagnostics and Reporting Tool (DART)



VPN:
Connected to STG Alpha BXB SSL.
16:46:27 IPv4

Network:
Connected (192.168.26.123)

Web Security:
No License Key.

System Scan:
No policy server detected.
Default network access is in effect.

Roaming Security:
Disabled while your VPN is active.

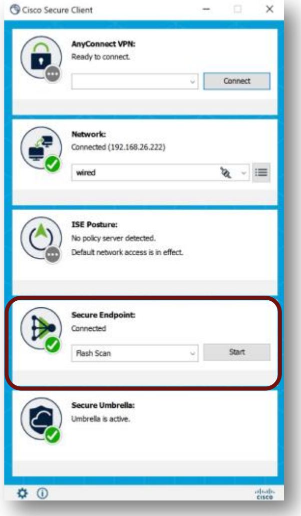
AMP Enabler:
AMP for Endpoints already installed.

SECURE © 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Secure Client

Suite of Security Service Enablement Modules

- AnyConnect VPN (Core)
- Network Access Manager (NAM)
- ISE Posture
- HostScan (aka: ASA posture) (No UI)
- Secure Endpoint (AMP)
- Umbrella Module
- Cloud Management Module (No UI)
- Network Visibility Module (NVM) (No UI)
- Diagnostics and Reporting Tool (DART)



AnyConnect VPN:
Ready to connect.

Network:
Connected (192.168.26.222)

ISE Posture:
No policy server detected.
Default network access is in effect.

Secure Endpoint:
Connected

Secure Umbrella:
Umbrella is active.

SECURE © 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

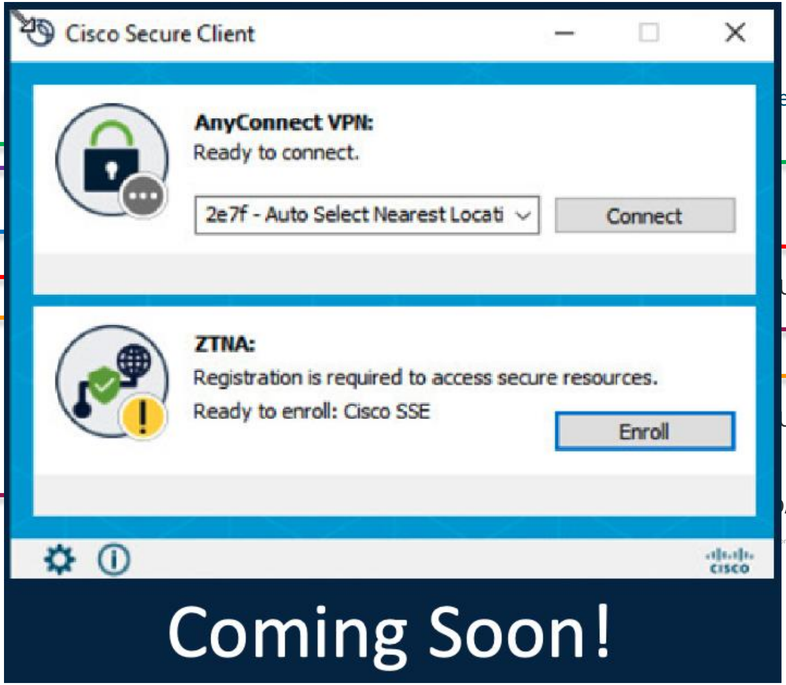
Cisco Secure Client ZTNA Module

Cisco AnyConnect

Suite of Security Service Enablement Modules

- VPN Module (Core)
- Network Access Manager (NAM)
- ~~Web Security (CWS)~~
- Posture
- Umbrella Module
- HostScan (aka: ASA posture) (No UI)
- Network Visibility Module (NVM) (No UI)
- ~~AMP Enabler Module~~
- Diagnostics and Reporting Tool (DART)

SECURE



Cisco Secure Client

AnyConnect VPN:
Ready to connect.

2e7f - Auto Select Nearest Locati

ZTNA:
Registration is required to access secure resources.
Ready to enroll: Cisco SSE

Coming Soon!

ent Modules

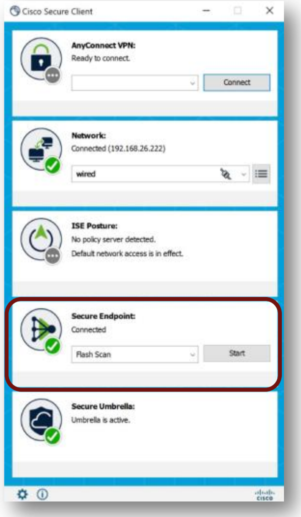
UI)

UI)

(No UI)

ART)

nfidential



Cisco Secure Client

AnyConnect VPN:
Ready to connect.

Network:
Connected (192.168.26.222)
wired

ISE Posture:
No policy server detected.
Default network access is in effect.

Secure Endpoint:
Connected
Flash Scan

Secure Umbrella:
Umbrella is active.

Cisco Secure Access

Secure Private Access Use Cases

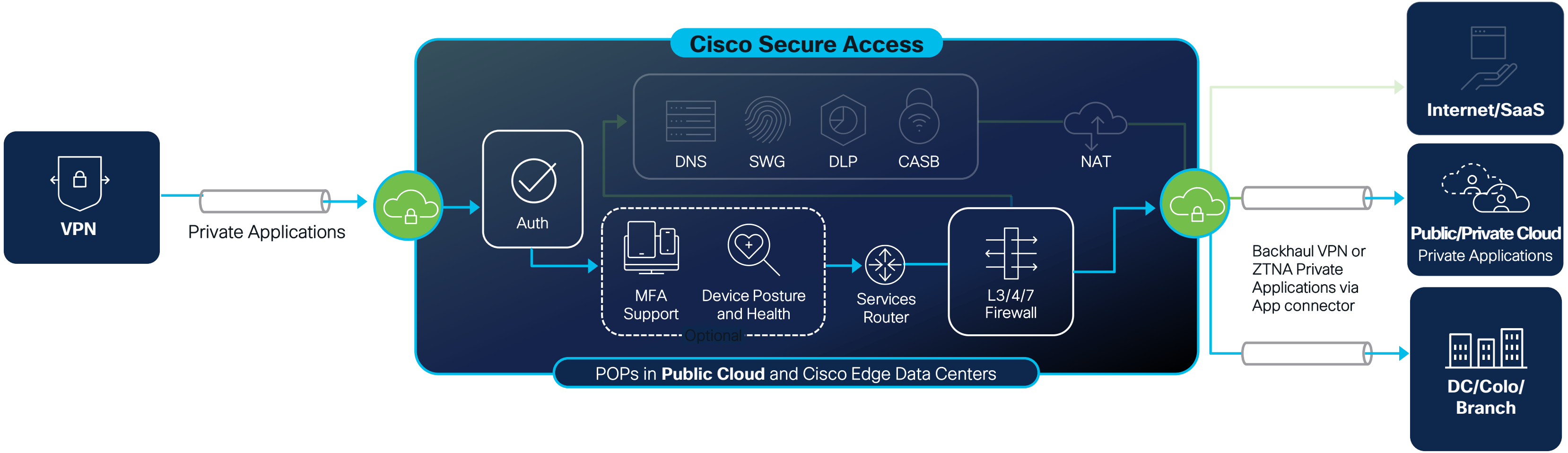
- Secure Private Access
  - Via VPN
  - Via ZTNA (Client Based)
  - Via ZTNA (Clientless)

Secure Private Access

via VPN

⟷ Private Traffic

▭ Secure Tunnel



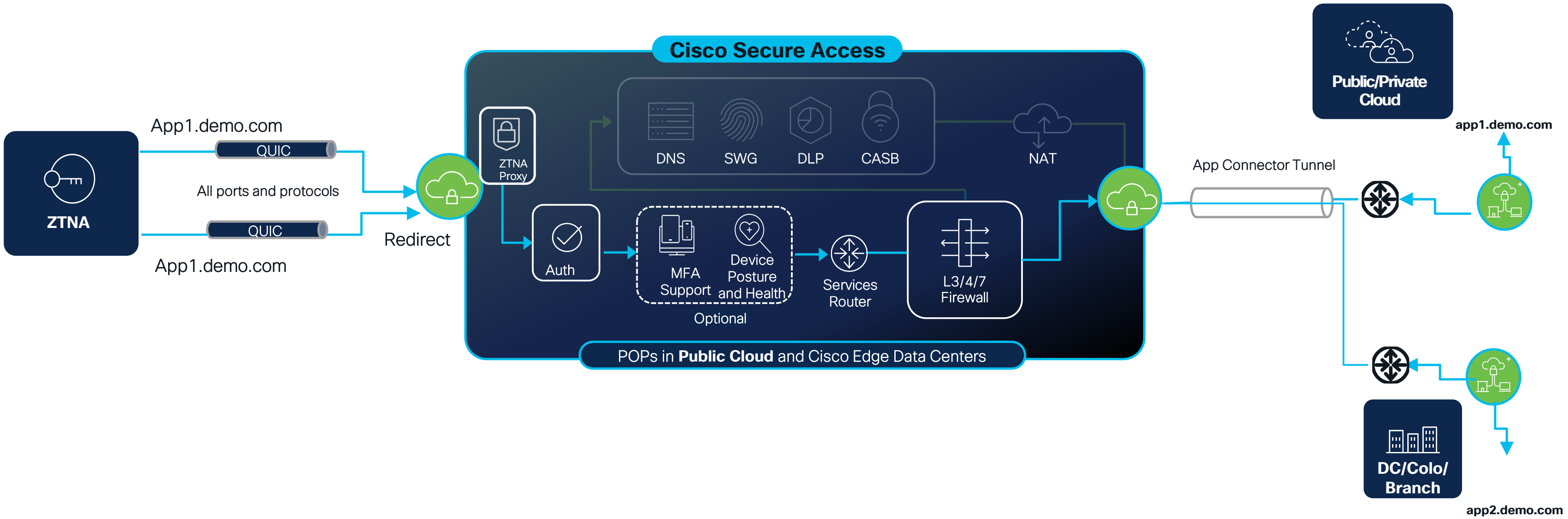
Benefits

- SAML 2.0 + cert-based authentication
- Posture verification (optional)
- Trusted Network Detection
- Start before logon
- IPS
- Granular context-based control

Secure Private Access (Client-based ZTNA)

↔ Private Traffic
▭ Secure Tunnel

No VPN



Benefits

- Improved end-user experience
- Improved Security step up auth
- Always on access

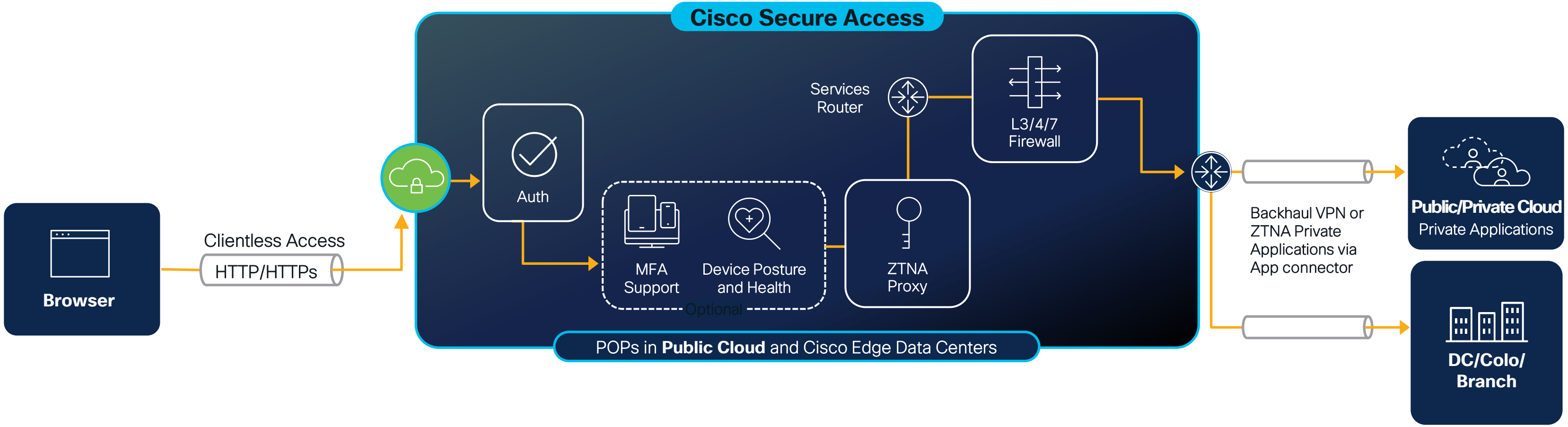
- Performance benefits QUIC & MASQUE
- Per App tunnels
- Cloud bypass for sensitive apps

- No client based VPN
- No routing/network modification on client
- App specific access

Secure Private Access

No VPN, No Client

⟷ Clientless Access
▭ Secure Tunnel

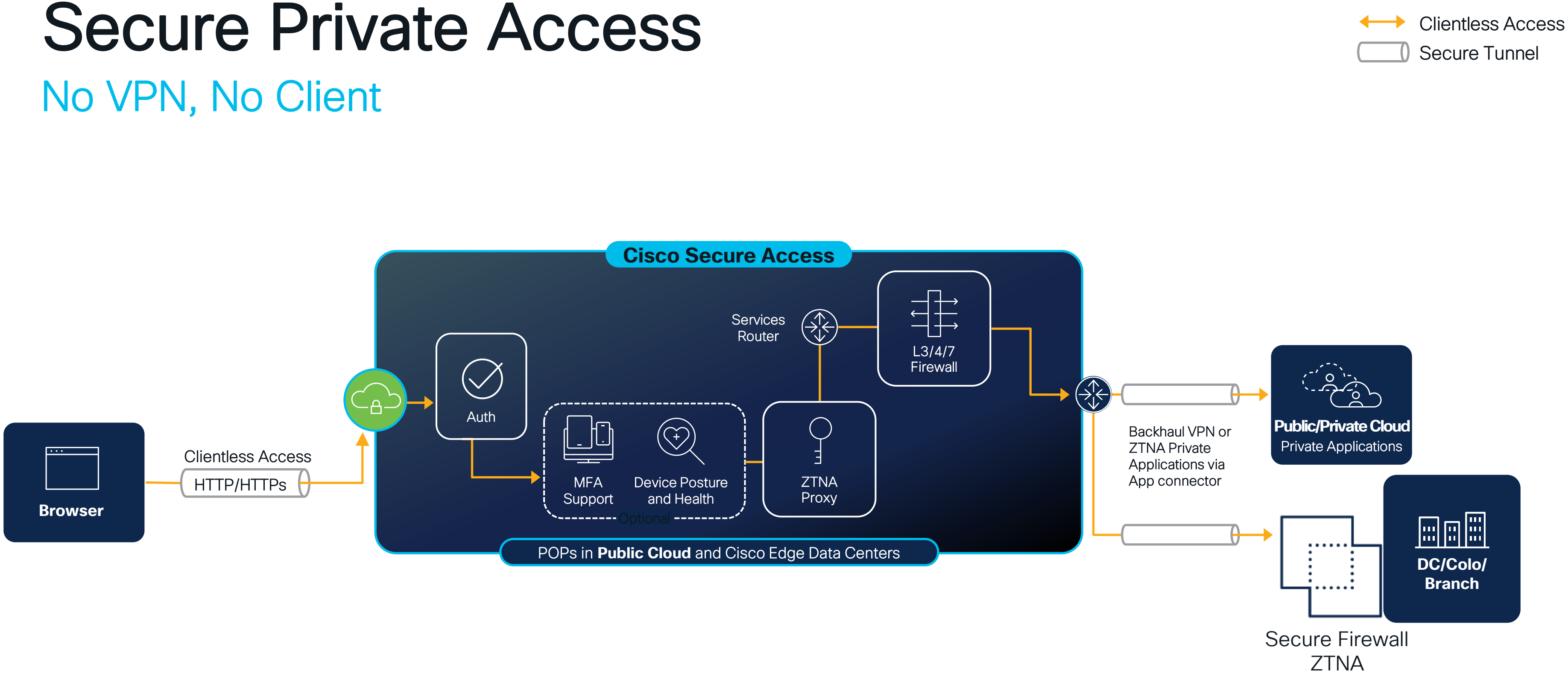


Capabilities

- Clientless
- App-specific access
- Undiscoverable IP address
- Least privileged user access
- Reduced threat surface

Secure Private Access

No VPN, No Client



Capabilities

- Clientless
- App-specific access
- Undiscoverable IP address
- Least privileged user access
- Reduced threat surface

Key takeaways

Key takeaways

- ✓ Both VPN and ZTNA have their strengths and weaknesses. Despite claims of VPN obsolescence.
- ✓ Both technologies can be effectively utilized to establish a secure architecture with Zero Trust Principles.
- ✓ Evaluate and select the most suitable solution for your organization.
- ✓ Contextualize the technologies and consider their implementation based on your organization's specific requirements and objectives.

Slido

“The design of the network, where our applications live, and the security infrastructure is a speed bump and adds unnecessary complexity burden on our users. We need to to provide security, availability, performance and do it in a way that is completely transparent to our users.”

Jay Young – VPN Technical Leader

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Fill out your session surveys!

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

The bridge to possible

Thank you

#CiscoLive

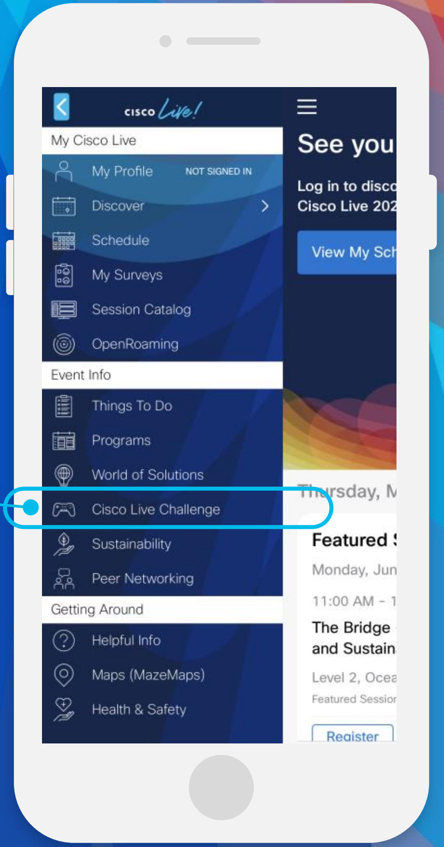
Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

cisco Live!

Let’s go

#CiscoLive