

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Cisco Secure Access

Deep Dive into ZTNA and Private App Access

Justin Murphy, Technical Leader, SSE

BRKSEC-2729

CISCO *Live!*

#CiscoLiveAPJC

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 November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2729>





Agenda

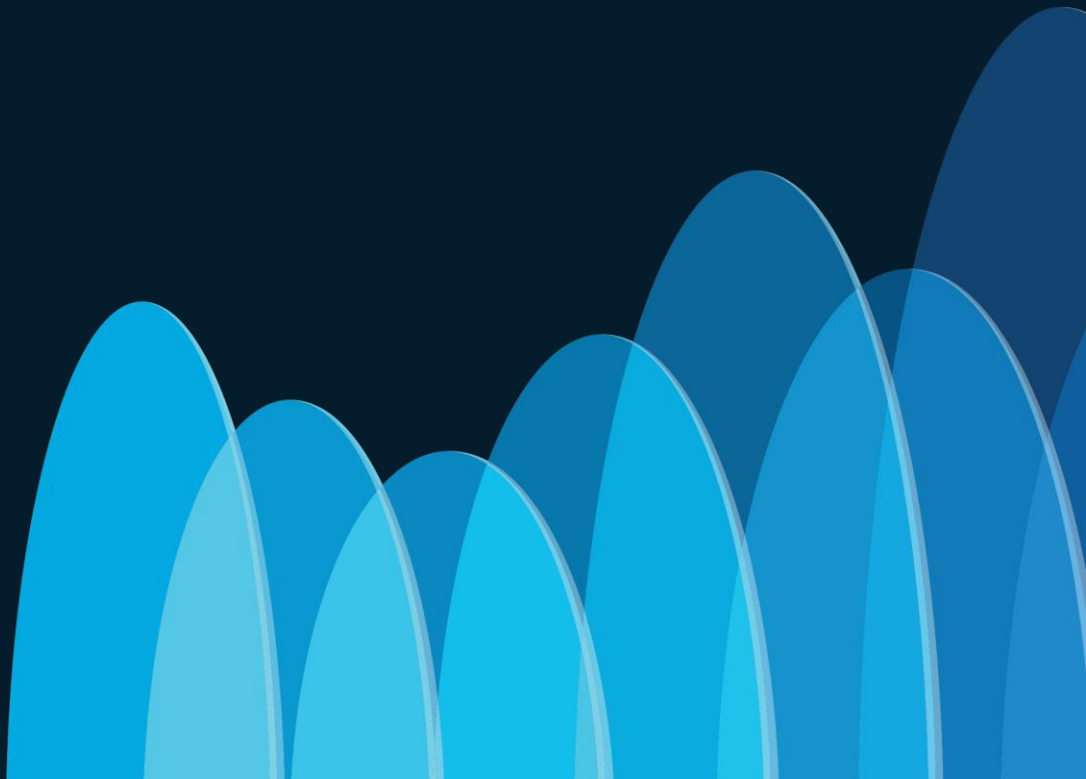
- Why ZTNA
- ZTNA w/ Secure Access

Why ZTNA?



ZTNA

Zero Trust Network Access



ZT
Zero Trust
Principals



NA
Network Access

Why ZTNA?



Zero Trust



User Experience

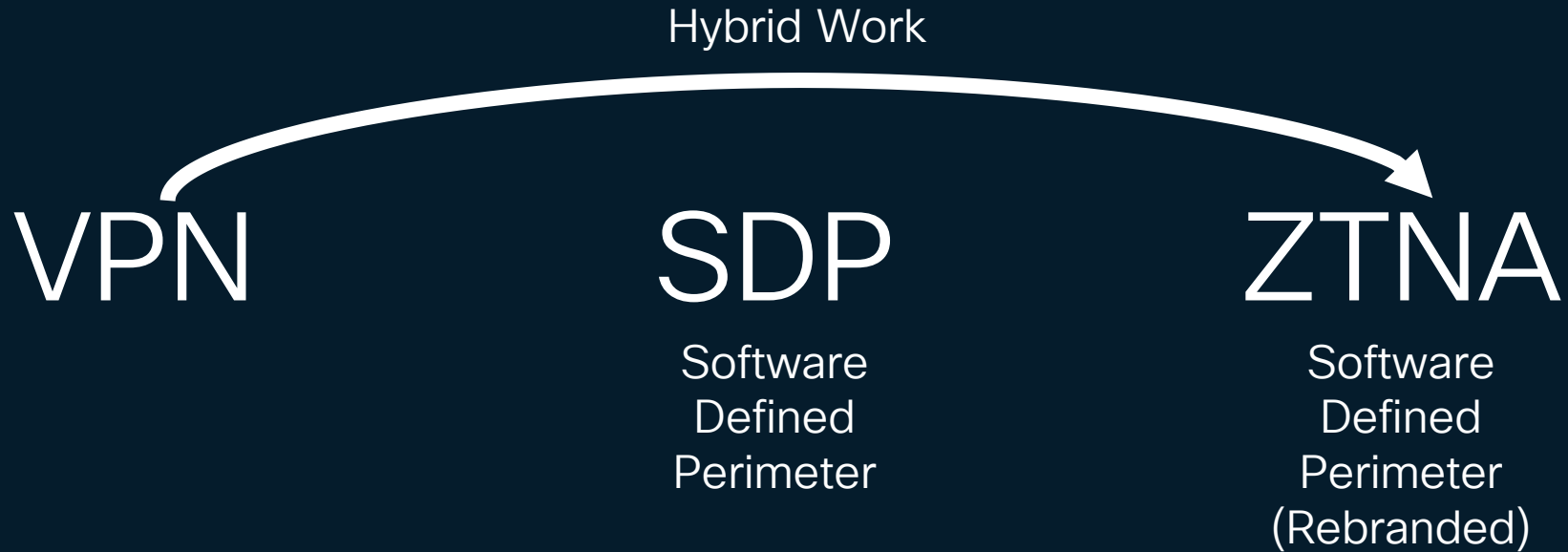


SaaS Delivery

Evolution of ZTNA



Evolution of ZTNA: Organization Adoption



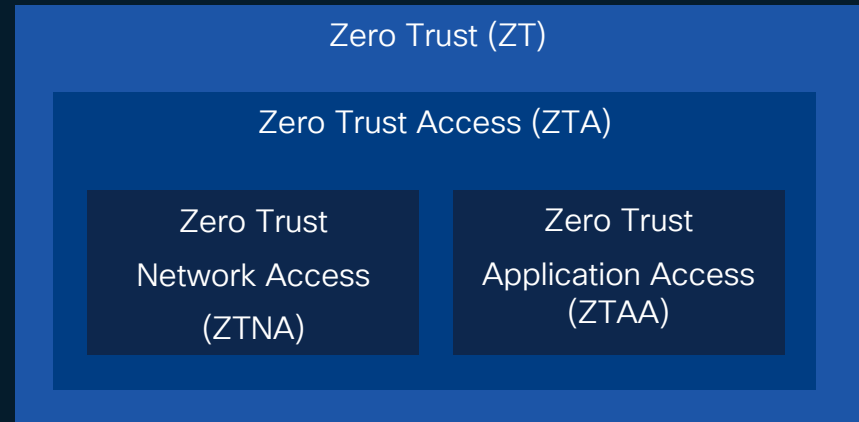
ZT vs. ZTA vs. ZTNA vs. ZTAA

Zero Trust

- A comprehensive security framework that prioritizes least privilege, strict access controls, and continuous monitoring to mitigate risks and protect resources.

Zero Trust Access

- A specific aspect of Zero Trust that focuses on managing and enforcing access to resources



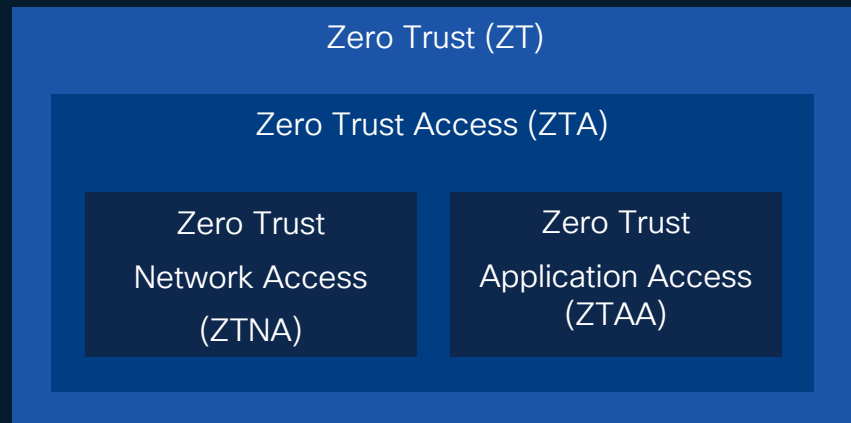
ZT vs. ZTA vs. ZTNA vs. ZTAA

Zero Trust Network Access (ZTNA)

- A subset of Zero Trust Access that focuses on secure access to networks.

Zero Trust Application Access (ZTAA)

- A subset of Zero Trust Access that focuses on secure access to individual applications.



ZTNA vs. ZTAA

	Zero Trust Network Access (ZTNA)	Zero Trust Application Access (ZTAA)
Allow Access To:	Corporate Network (10.0.0.0/8 or *.example.com)	Production Jira App (jira.example.com)
When:	User Identity (Lee authenticated via MFA)	
	Device Posture (Fully patched device)	
	Location (United States)	
	Continuous Monitoring (TLS decrypt and IPS inspection)	

The primary difference between ZTNA and ZTAA is the granularity of access in the policy

Types of Zero Trust Access

	Clientless Zero Trust Access	Client-Based Zero Trust Access
General Description	A lightweight method of securely accessing resources.	A more feature rich method of securely accessing resource.
Application Support	Supports web applications (HTTP/HTTPS) without any software and other select protocols (SMB/RDP/SSH/etc.) via a portal or small helper application.	Broad application support via client software on the user's device.
Partner/BYOD Use	Preferred method	Yes, if desired/needed
Employee Use	Yes, if desired	Preferred method

Zero Trust Networking (ZTN)

Are ZTN and ZTNA the same?

- No, ZTN is an implementation. ZTNA (in Gartner's view) is a product market.

Is Network Access Control ZTN?

- Probably not. Most NAC implementations fail to address requirements #2 and #3.

Is Microsegmentation ZTN?

- Probably not. Many microsegmentation implementations fail to address requirements #1 and #3.

Network infrastructure implementation that adheres to three principals:

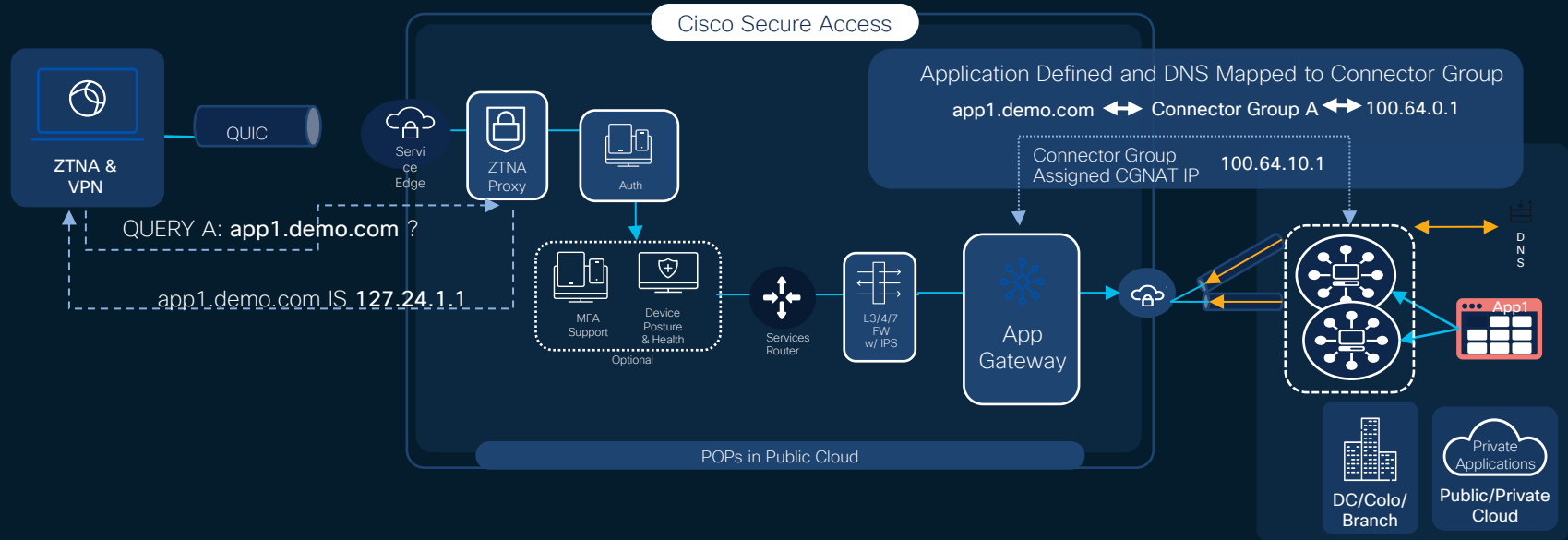
1. Grants network access only after identity is authenticated and authorized
2. Limits network access only to necessary resource/applications
3. Continuously adjusts network access in near real time, based on device/user context

Cisco Secure Access

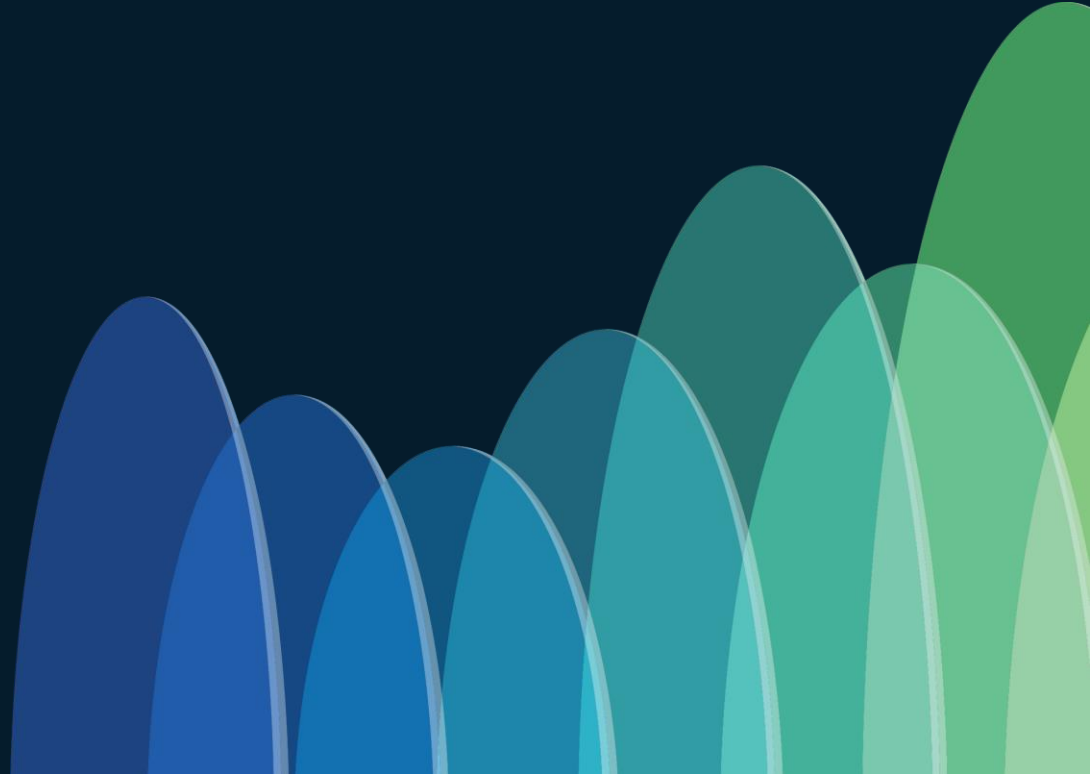
Cisco Zero Trust Access

	Cisco Secure Access		
Hosting	SaaS		
Type	Clientless	Client-Based	
Client	Web Browser	ZTA Module OS Native Clients	VPN Module
Supported Traffic	Client-to-server	Client-to-server	Client-to-server, Client-to-client, Server-to-client
Supported Apps	HTTP, HTTPS	Most TCP, UDP	All TCP, UDP, ICMP
Client Protocol(s)	TLS	MASQUE over QUIC or TLS	TLS, DTLS, IPSec
Device Posture	Per-App	Per-App	On Connect
Per-App Controls	Access Control, TLS Decrypt, IPS		

End to End Workflow

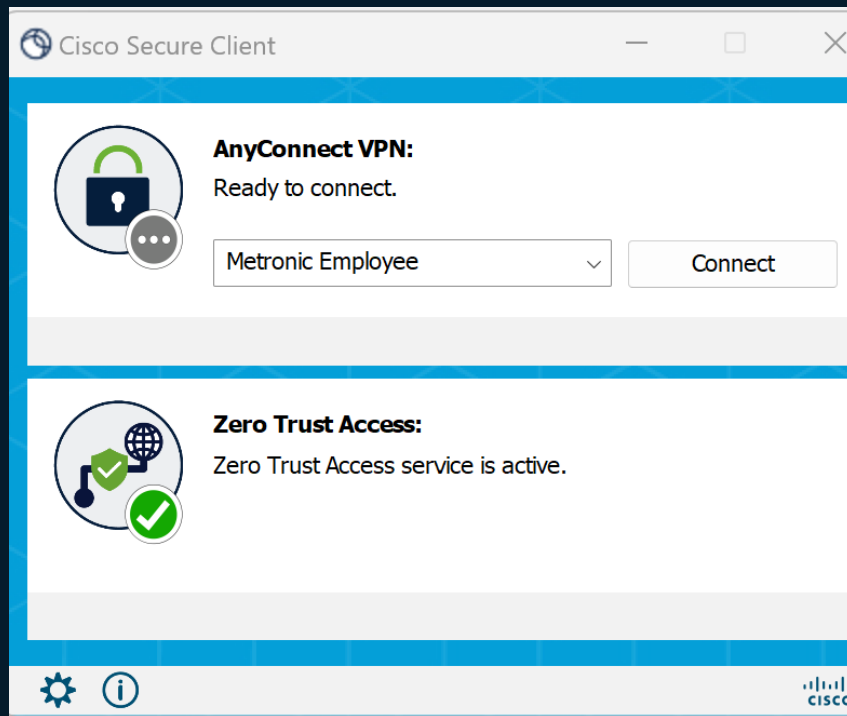


User Demo: Cisco Secure Access + Client-Based ZTA



Cisco Secure Client Zero Trust Access Module

- Transparent user experience
- Forward proxied resource access with coarse-grained or fine-grained access control
- Service managed client certificates with TPM/hardware enclave key storage
- Support for most TCP and UDP applications
- Cisco and third-party VPN client interop
- Next-generation protocol (MASQUE + QUIC)



What is QUIC and MASQUE?

QUIC (not an acronym):

- UDP-based, stream-multiplexing, encrypted transport protocol.
- First used in Google Chrome in 2012.
- Used for HTTP/3, iCloud Private Relay, SMB over QUIC, DNS over QUIC, etc.
- Optimized for the next generation of internet traffic with reduced latency compared to TLS over TCP.

MASQUE (Multiplexed Application Substrate over QUIC Encryption):

- IETF working group focused on next generation proxying technologies on top of the QUIC protocol.
- Provides the mechanisms for multiple proxied stream and datagram-based flows inside HTTP/2 and HTTP/3.
- Used by iCloud Private Relay since 2021.
- HTTP/2 and HTTP/3 extensions allow for the signaling and encapsulation of UDP and IP traffic.

When combined, MASQUE + QUIC provides an efficient and secure transport mechanism for TCP, UDP and IP traffic for both web and non-web protocols.

Why QUIC?



Fast connection establishment (0-RTT)



Ability to change IPs without renegotiation (Connection migration)



No waiting for partially delivered packets (Individually encrypted packets)



Not vulnerable to TCP meltdown (UDP transport)



No head-of-line blocking (Stream multiplexing)



Can simultaneously use multiple interfaces (Multipath)

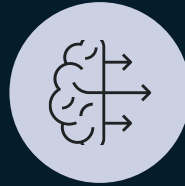
Why MASQUE?



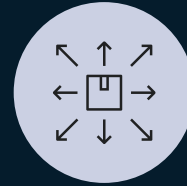
No direct
resource
access
(forward
proxy
architecture)



Broad
application
support
(TCP, UDP
and IP)



Fallback to
TLS (TCP
443) if QUIC
(UDP 443) is
blocked

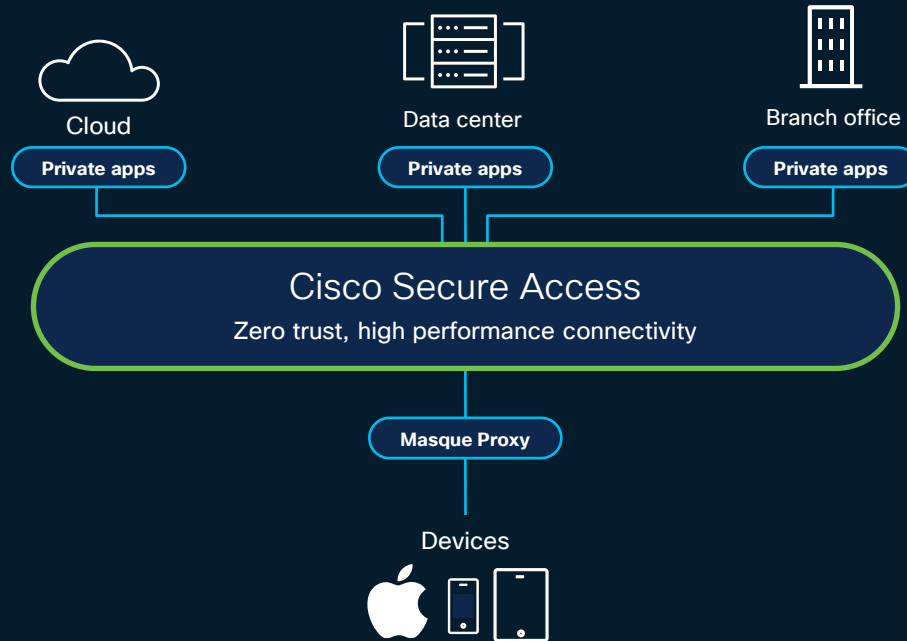


Flexibility to
support per-
connection,
per-app or
per-device
tunnels



Native OS
support
(macOS,
iOS,
Samsung
Knox)

Extend easy, zero trust access from Apple iOS



- Enterprise Relay, not last generation ZTNA
- Per application and per domain proxying done directly within the application, not device-wide, continuous VPN
- Enterprise privacy with “direct to workload” connectivity, iCloud Private Relay compatible
- 100% Standards-based. Built on industry leading technologies: MASQUE and QUIC
- All Applications, Ports, and Protocols, not just web applications

Cisco Secure Access traffic optimization with Apple iCloud Private Relay

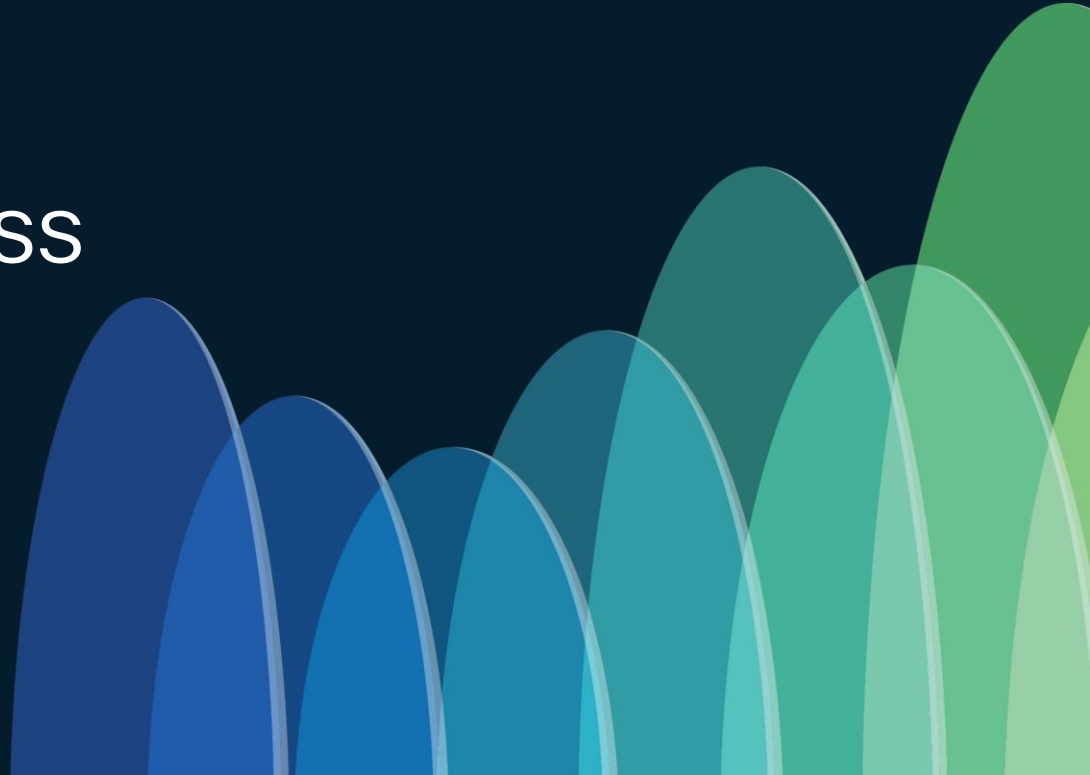
Enterprise Relay with Apple iCloud Private Relay On



Single layer of encryption for lightning-fast, secure access

Vision Demo:

Zero Trust Access Enrollment on Apple iOS

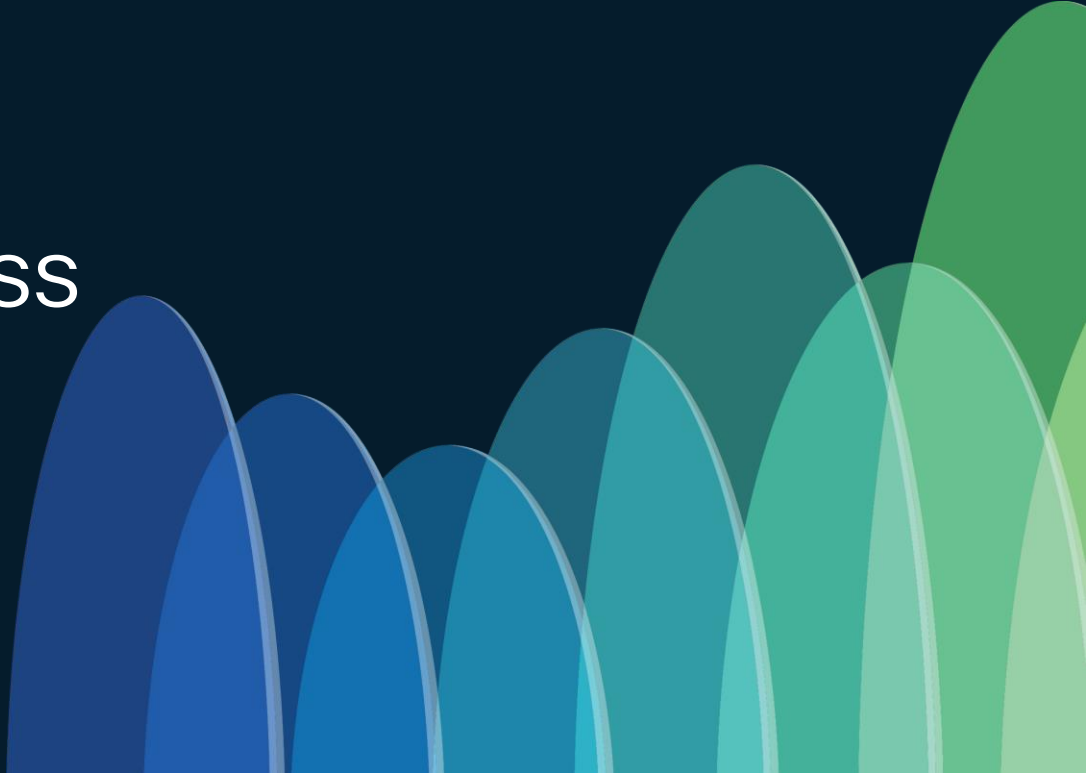




Vision Demo

User Demo:

Zero Trust Access
on Apple iOS





AnyConnect



Duo Mobile



Okta Verify



Billing



Dashboard



SEO



Owlfiles



RD Client



Billing (PWL)



Dashboard (PWL)



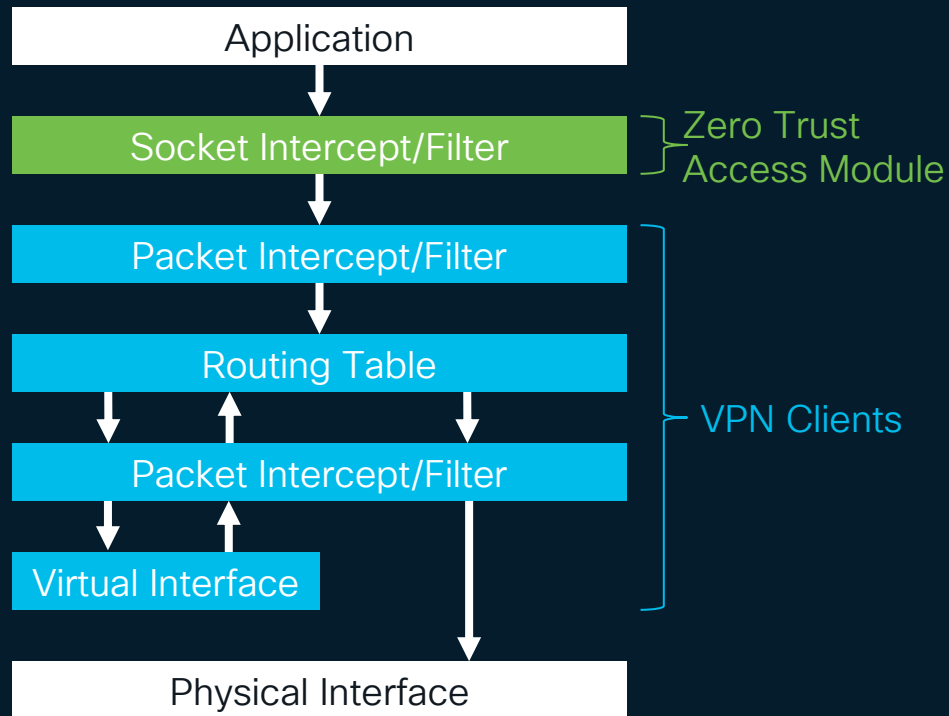
SEO (PWL)



Settings



Zero Trust Access Module – Socket Intercept

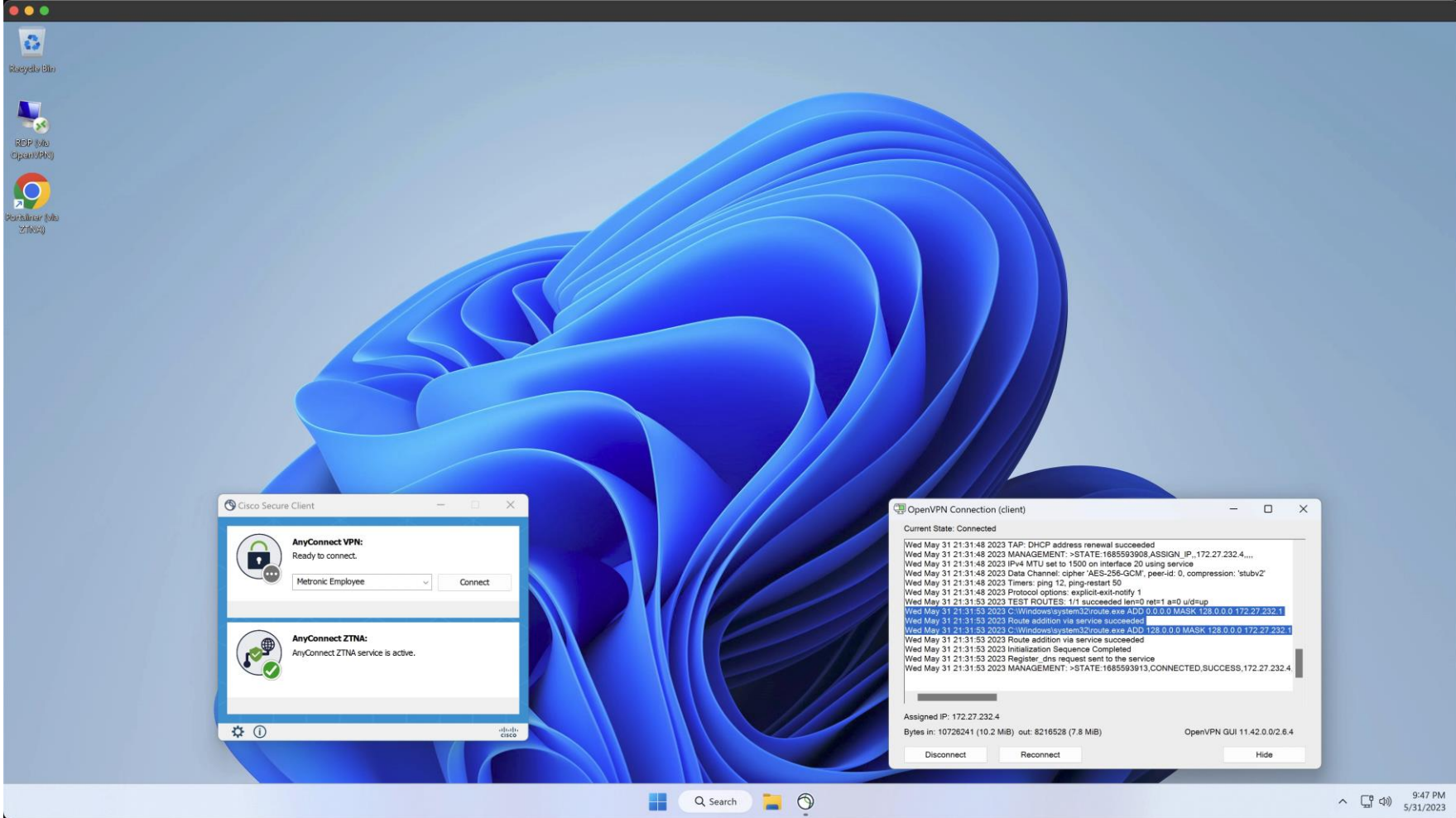


Why Socket Intercept?

- 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

User Demo:

Cisco Secure Access
+ Client-Based ZTA
+ Third-Party VPN



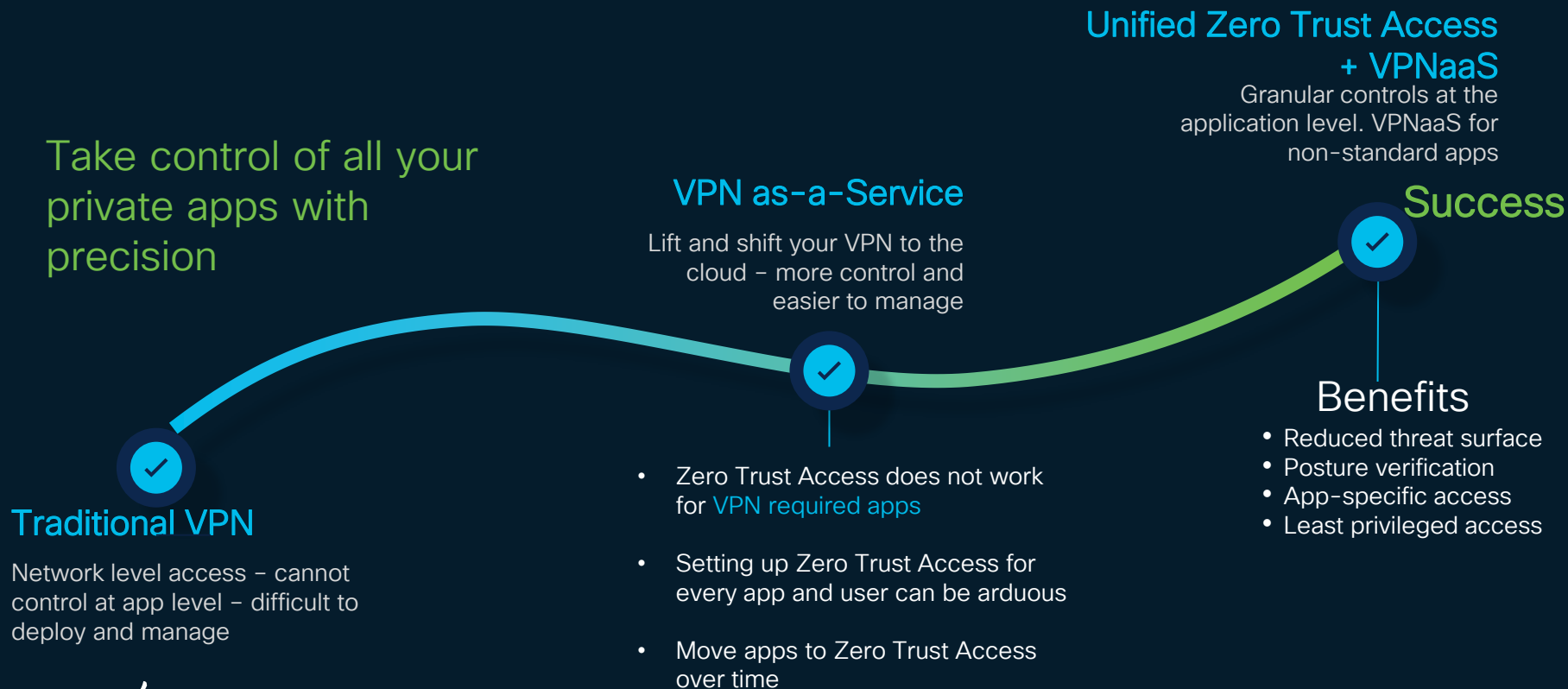
Not Every App Works with Zero Trust Access

- Apps that don't work with via Zero Trust Access
- Client-to-client traffic (e.g. peer-to-peer VoIP)
- Server-to-client traffic (e.g. remote desktop, remote assistance)
- Applications that require a unique client IP (e.g. SMBv1)
- Applications that require SRV DNS records (e.g. Active Directory, Kerberos, SCCM)
- Applications that require the server to send the first data payload after the TCP 3-way handshake (e.g. MySQL Studio)

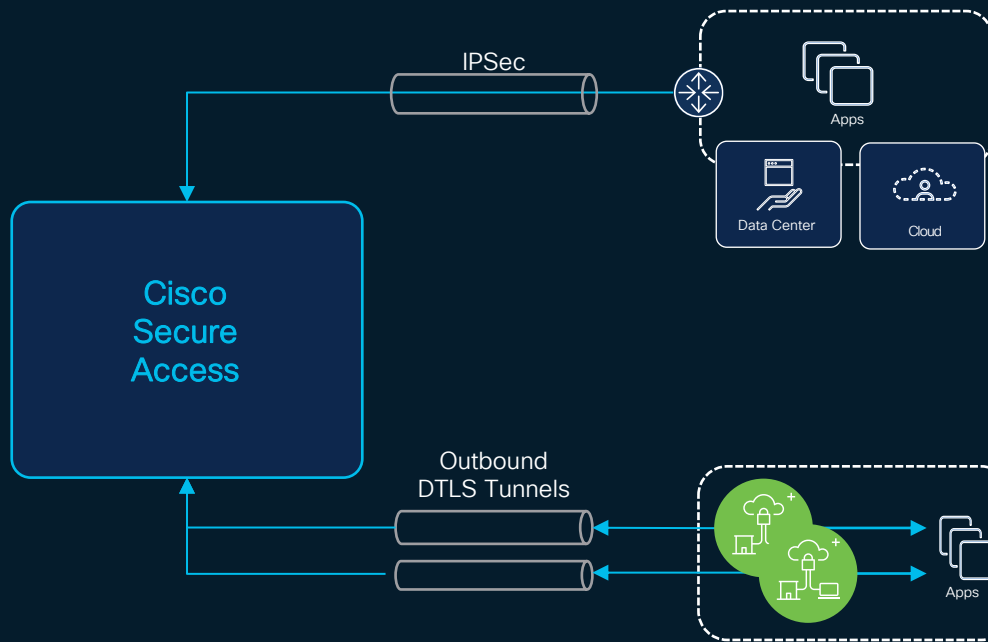
We Have the Solution! → Cisco Secure Access VPN

Zero Trust Access Journey

Pragmatic migration to more control – direct to private apps



Zero Trust Access App Connections (Deploy Both)



Network Tunnel

- IPsec Backhaul
- Static or BGP based routing
- Auto Failover/ Redundancy

Application Connector (AC)

- Software deployment (VM or Cloud Instance)
- Deploy closest to application
- Outbound connectivity (no holes in firewall)
- Auto failover / load balancing

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert 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



Thank you



#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC