

The background features a vibrant, abstract design with overlapping, wavy bands of color in shades of blue, green, yellow, orange, and red. On the right side, a bright white light source radiates outwards, creating a sunburst effect with sharp, colorful rays that fan across the entire image.

CISCO *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Cisco Secure Access – Deep Dive into ZTNA and Private App Access

Justin Murphy, Technical Leader, SSE

BRKSEC-2729

cisco *Live!*

#CiscoLiveAPJC

Cisco Webex App

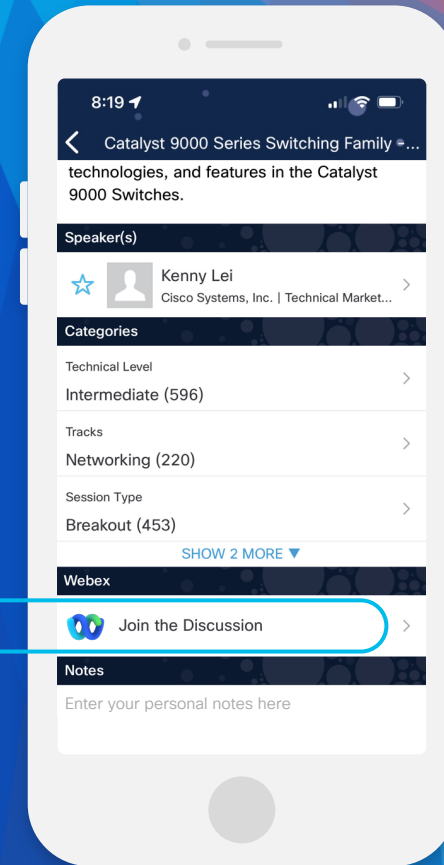
Questions?

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 December 22, 2023.



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

About Me

- Justin Murphy
- justmurp@cisco.com
- TME, CloudSec, SSE
- 7 years @ Cisco
- Father (7 & 9)
- Maker, Tech Enthusiast & Adventurer



Agenda

- Why ZTNA
- What is ZTA
- Secure Access
- Enrollment in ZTA
- ZTA User Experience
- ZTA Limitations
- Journey to Zero Trust

Why ZTNA?

Why Zero Trust?



Dissolving perimeter



Attackers actively exploiting
gaps and weaknesses



80% of organizations are
NOT prepared

[2023 Cisco's Cybersecurity Readiness Index](#)

ZTNA

Zero Trust Network Access

ZT

Zero Trust
Principals



NA

Network Access

Why ZTNA?



Zero Trust



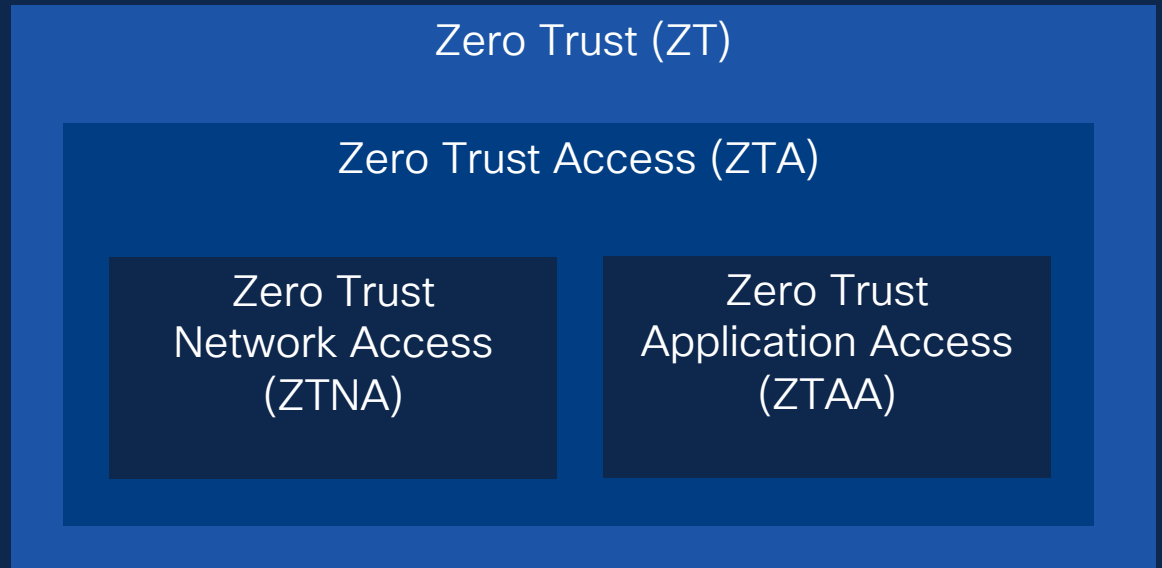
User Experience



SaaS Delivery

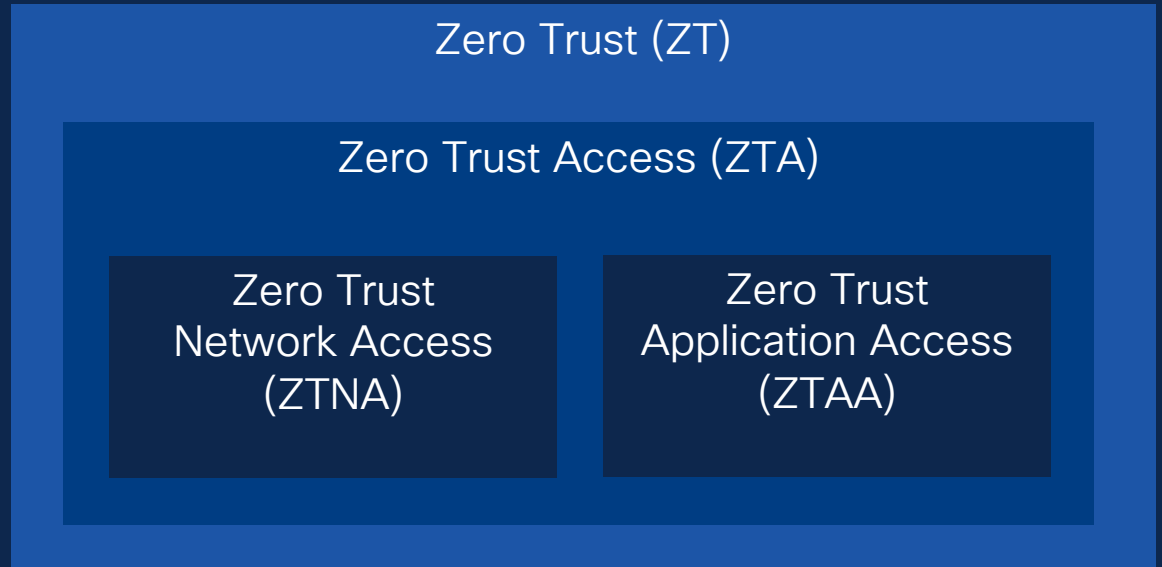
ZT vs. ZTA vs. ZTNA vs. ZTAA

- **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)

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

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.

Cisco Secure Access

Cisco Secure Access

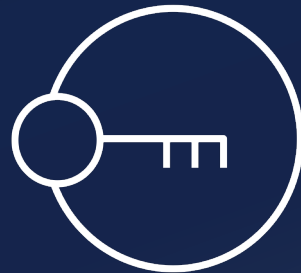
- Go beyond core Security Service Edge (SSE) to better connect and protect your business



Cisco Secure Access

Go beyond core Security Service Edge (SSE) to better connect and protect your business

Core SSE

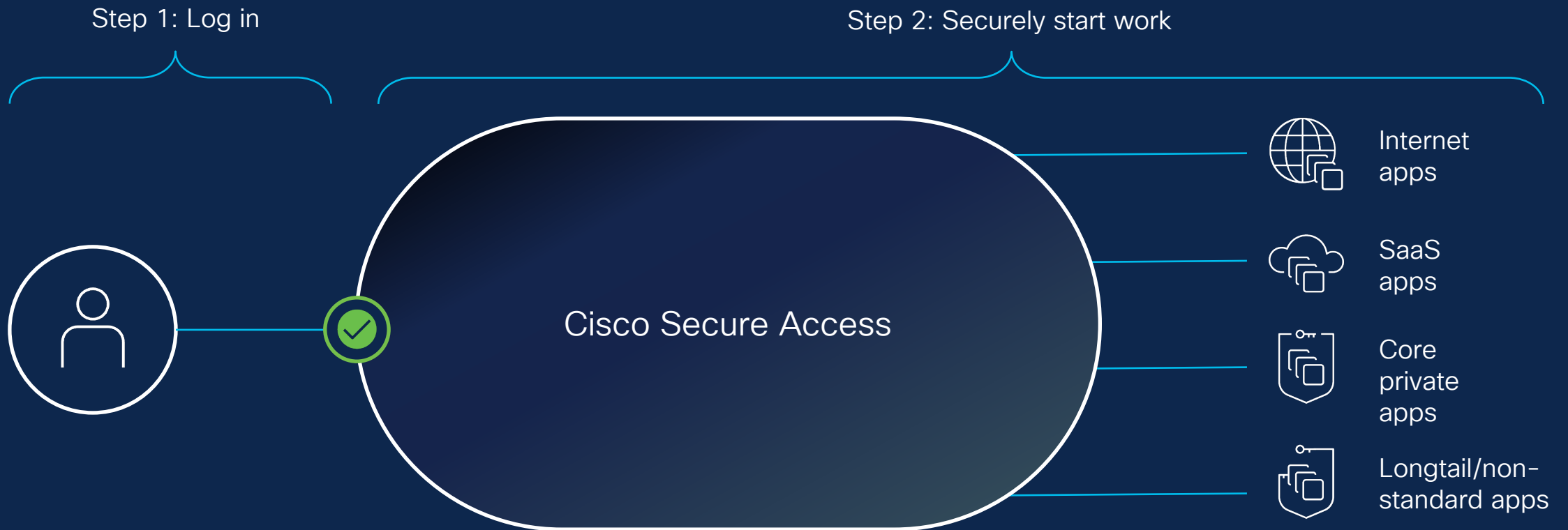


Zero Trust Access
(ZTA)

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		

Easy, frictionless user experience



User Demo:

Cisco Secure Access
+ ZTA Enrollment



Recycle Bin



Git Bash



Google Chrome



Microsoft Edge



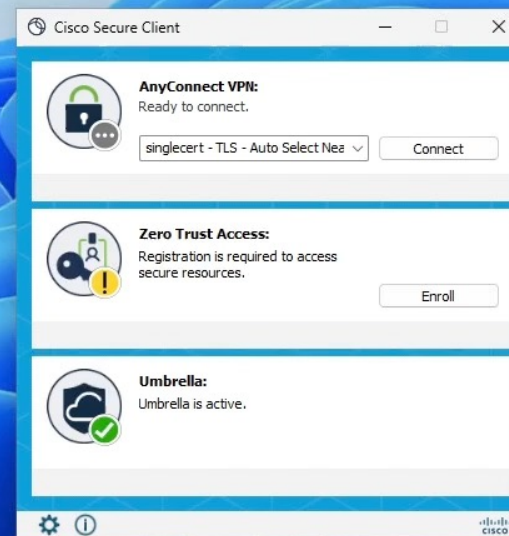
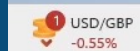
Console



Webex



PuTTY (64-bit)

USD/GBP
-0.55%

Search



File Explorer



Microsoft Edge



Google Chrome



File Explorer



Microsoft Edge



Google Chrome



File Explorer



Microsoft Edge



Google Chrome



File Explorer



Microsoft Edge



Google Chrome



File Explorer



Microsoft Edge



Google Chrome



File Explorer



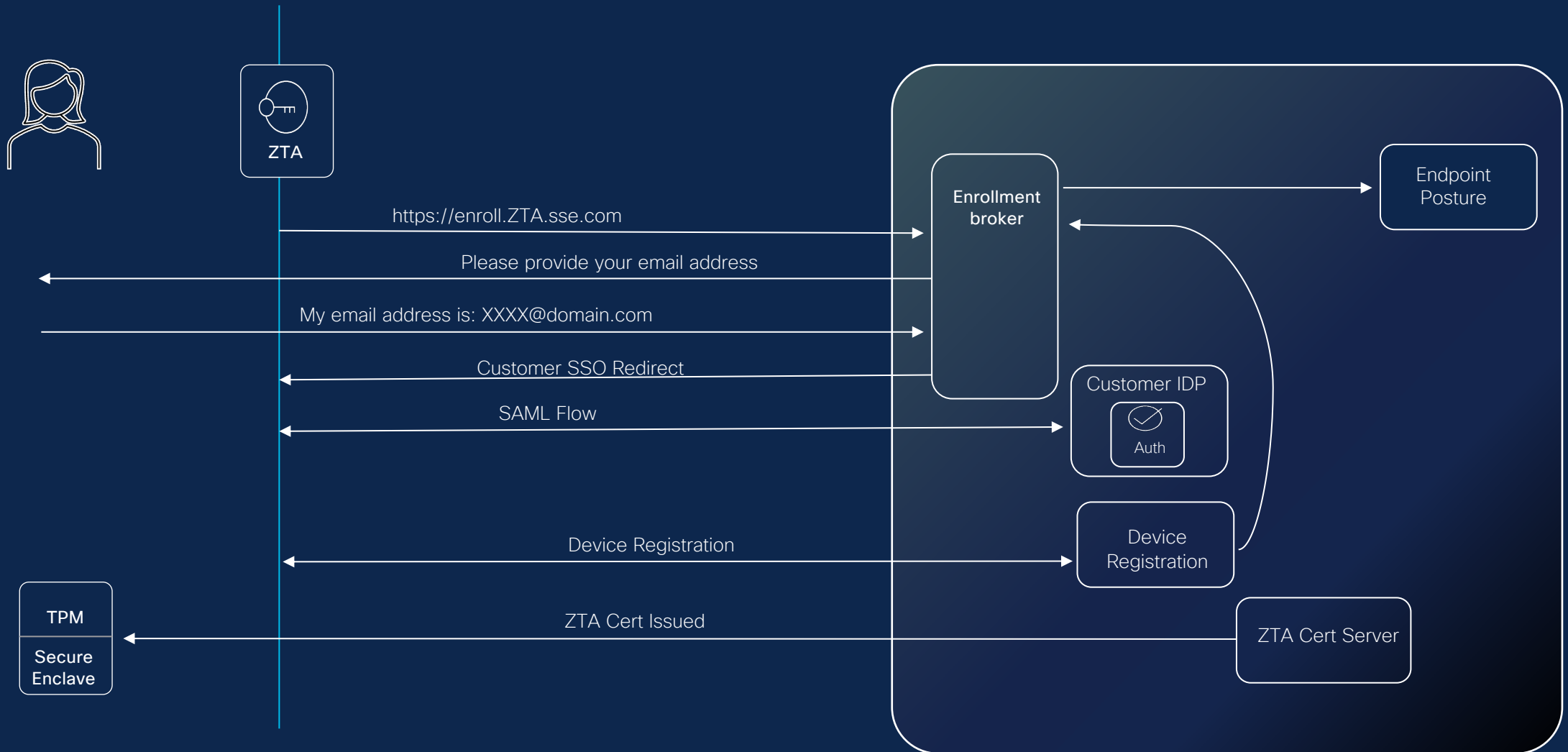
Microsoft Edge



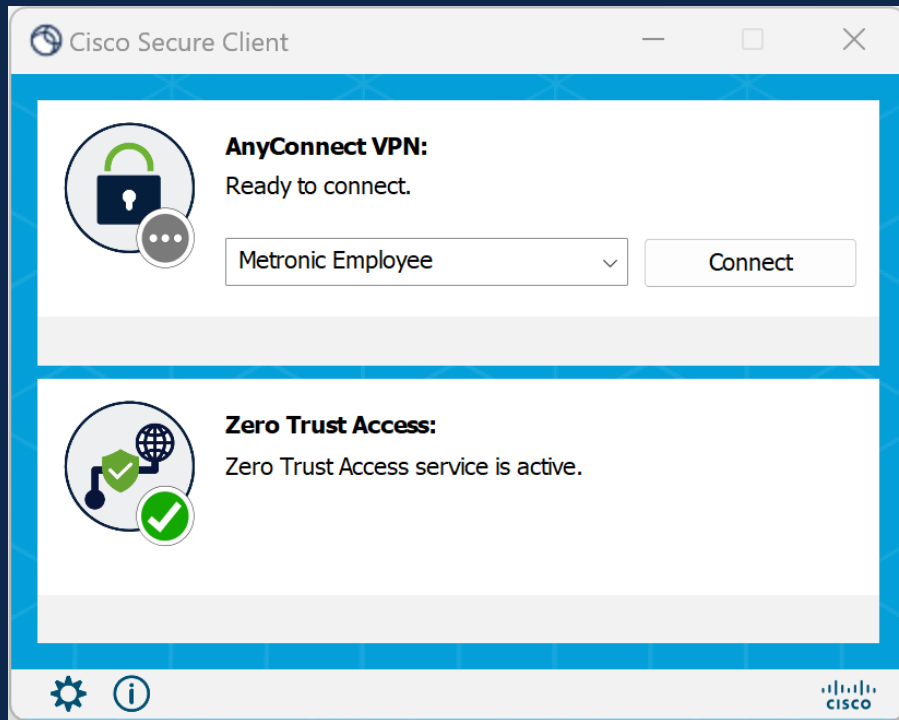
Google Chrome

6:28 AM
11/25/202312:28 PM
11/25/2023

Enrollment Procedure



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/Secure 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)

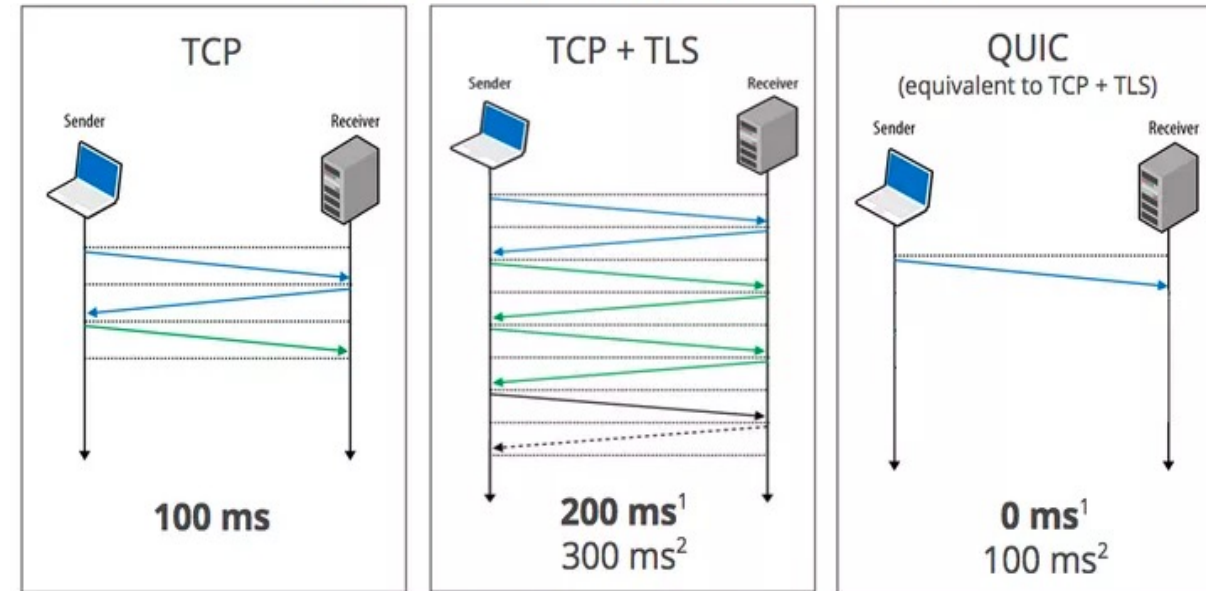


No head-of-line blocking (Stream multiplexing)



Can simultaneously use multiple interfaces (Multipath)

Zero RTT Connection Establishment



1. Repeat connection
2. Never talked to server before

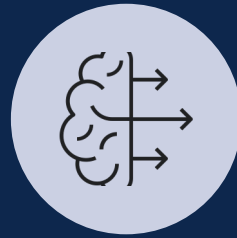
Why MASQUE?



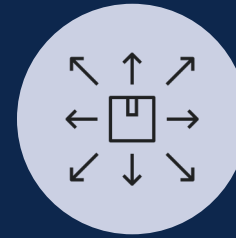
No direct
resource access
(forward proxy
architecture)



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

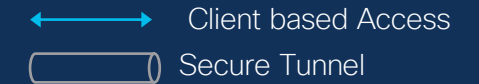
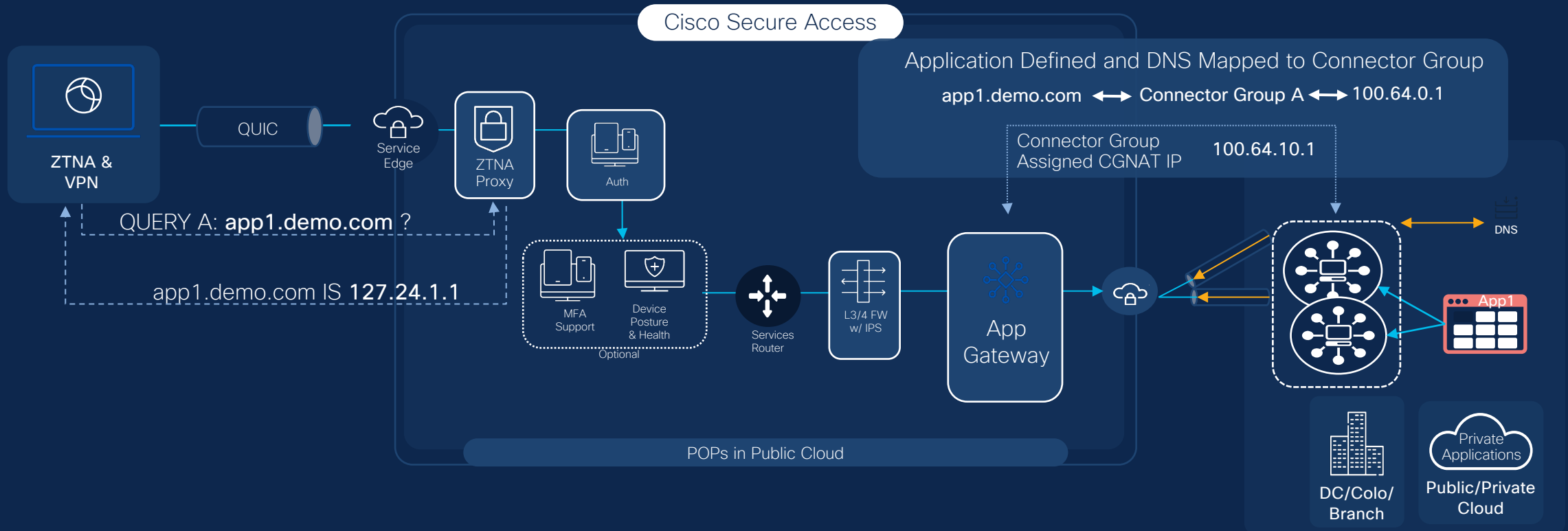


Native OS support
(macOS, iOS,
Samsung Knox)

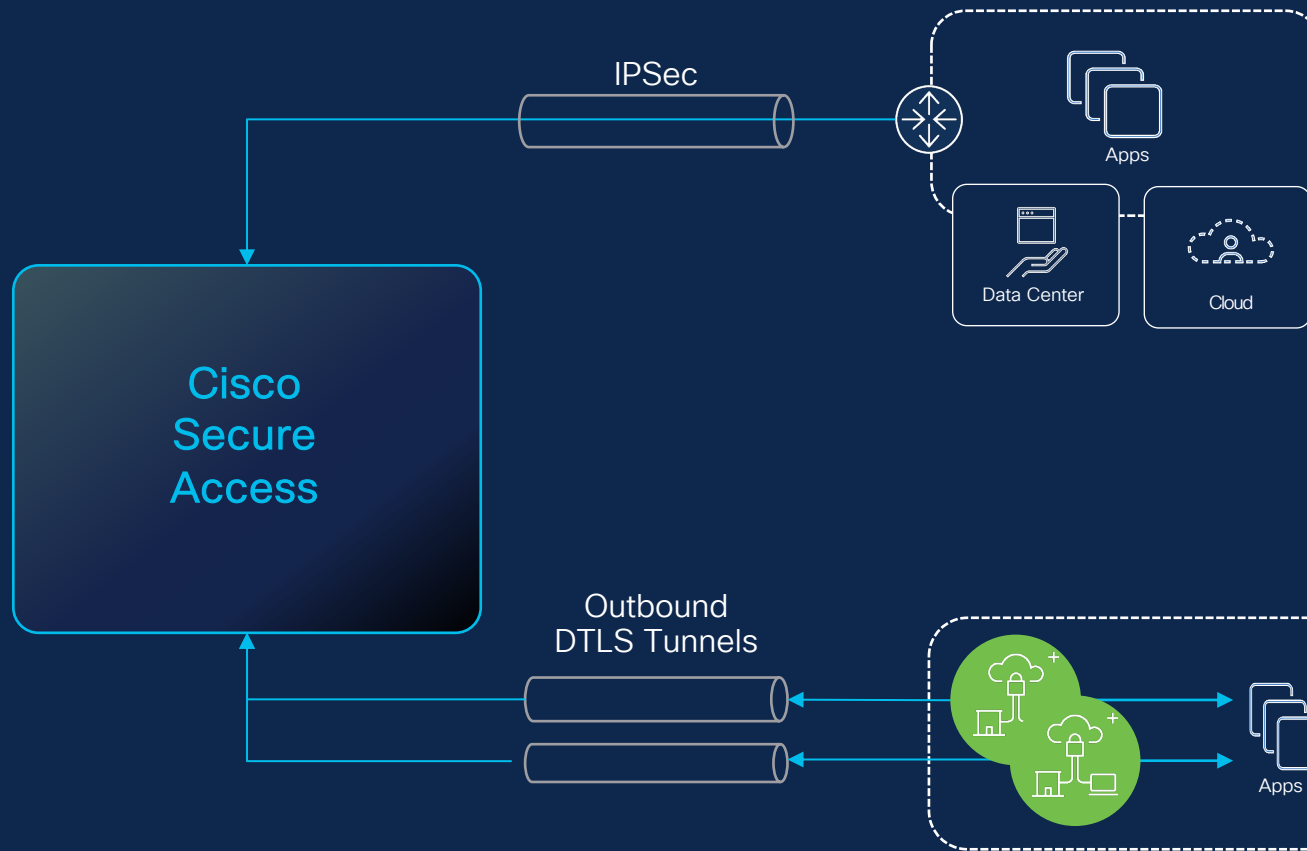
User Demo:

Cisco Secure Access
+ Client-Based ZTA

End to End Workflow



Zero Trust Access App Connections (Deploy Both)



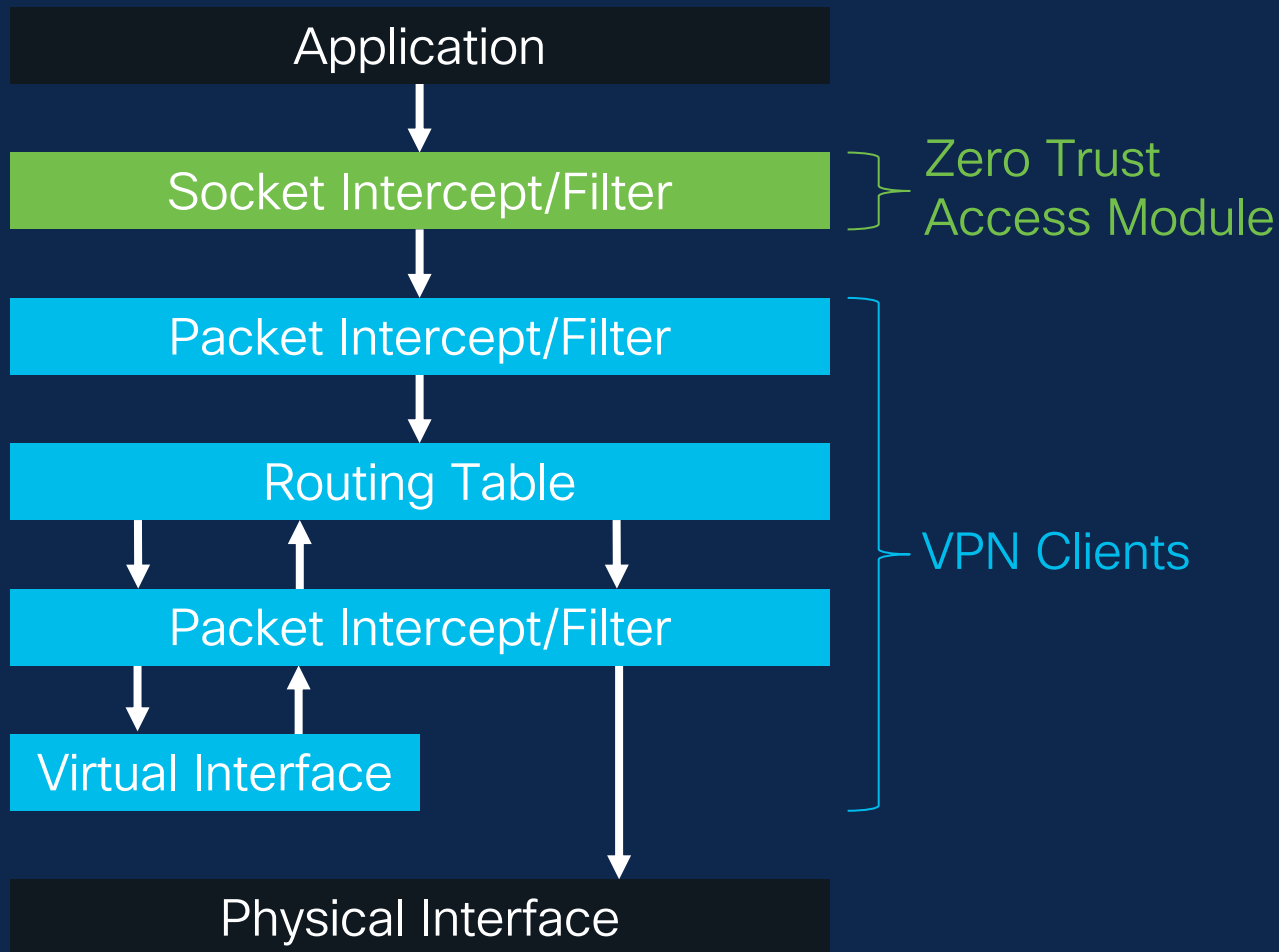
Network Tunnel

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

Resource Connector (RC)

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

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

- Recycle Bin
- RDP (Via OpenVPN)
- Portaliner (Via ZTNA)

Cisco Secure Client

AnyConnect VPN:

Ready to connect.

Metronic Employee

Connect

AnyConnect ZTNA:

AnyConnect ZTNA service is active.

1

CISCO

OpenVPN Connection (client)

Current State: Connected

Wed May 31 21:31:48 2023 TAP: DHCP address renewal succeeded

Wed May 31 21:31:48 2023 MANAGEMENT: >STATE:1685593908,ASSIGN_IP,,172.27.232.4,,,

Wed May 31 21:31:48 2023 IPv4 MTU set to 1500 on interface 20 using service

Wed May 31 21:31:48 2023 Data Channel: cipher 'AES-256-GCM', peer-id: 0, compression: 'stubv2'

Wed May 31 21:31:48 2023 Timers: ping 12, ping-restart 50

Wed May 31 21:31:48 2023 Protocol options: explicit-exit-notify 1

Wed May 31 21:31:53 2023 TEST ROUTES: 1/1 succeeded len=0 ret=1 a=0 u/d=up

Wed May 31 21:31:53 2023 C:\Windows\system32\route.exe ADD 0.0.0.0 MASK 128.0.0.0 172.27.232.1

Wed May 31 21:31:53 2023 Route addition via service succeeded

Wed May 31 21:31:53 2023 C:\Windows\system32\route.exe ADD 128.0.0.0 MASK 128.0.0.0 172.27.232.1

Wed May 31 21:31:53 2023 Route addition via service succeeded

Wed May 31 21:31:53 2023 Initialization Sequence Completed

Wed May 31 21:31:53 2023 Register_dns request sent to the service

Wed May 31 21:31:53 2023 MANAGEMENT: >STATE:1685593913,CONNECTED,SUCCESS,172.27.232.4

Assigned IP: 172.27.232.4

Bytes in: 10726241 (10.2 MiB) out: 8216528 (7.8 MiB)

OpenVPN GUI 11.42.0.0/2.6.4

Disconnect

Reconnect

Hide

CISCO Live!

#CiscoLiveAPJC

BRKSEC-2729

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

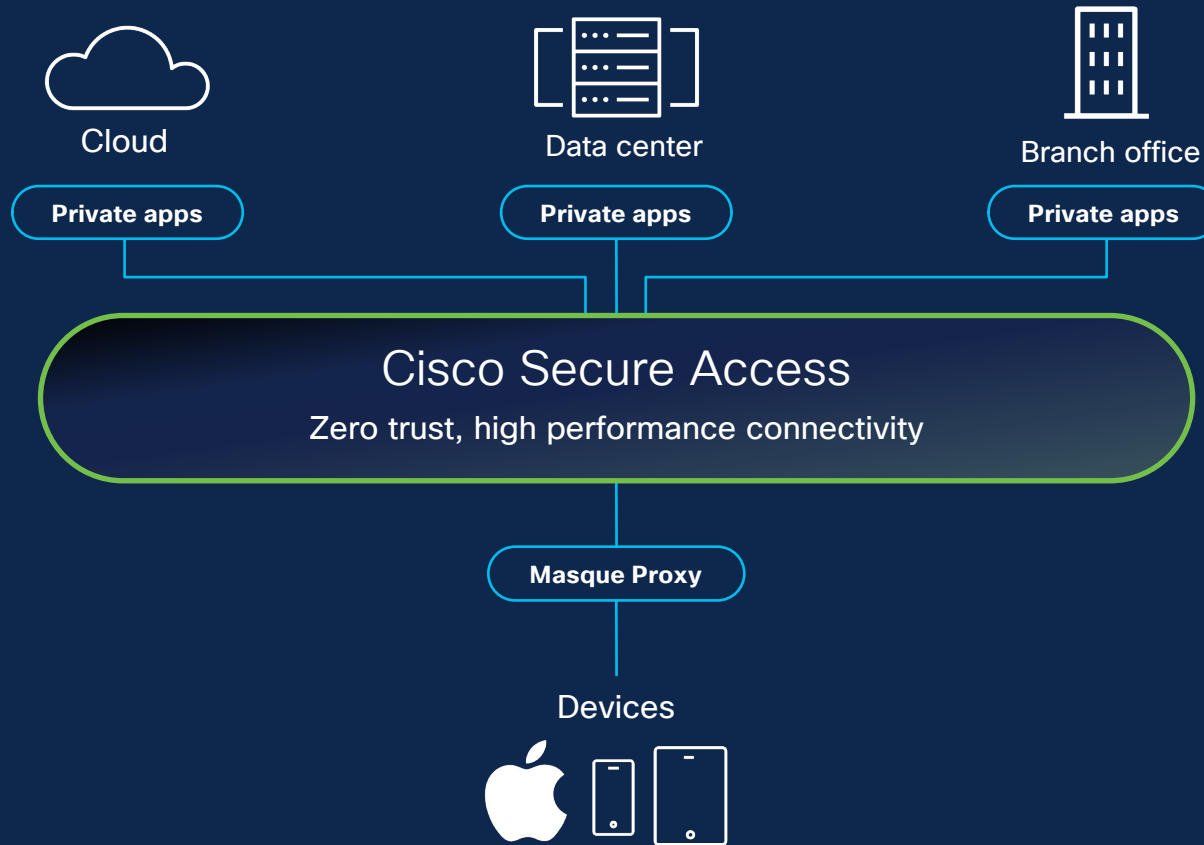
36

9:47 PM

5/31/2023

Extend easy, zero trust access from Apple iOS

COMING
SOON



- 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

COMING
SOON

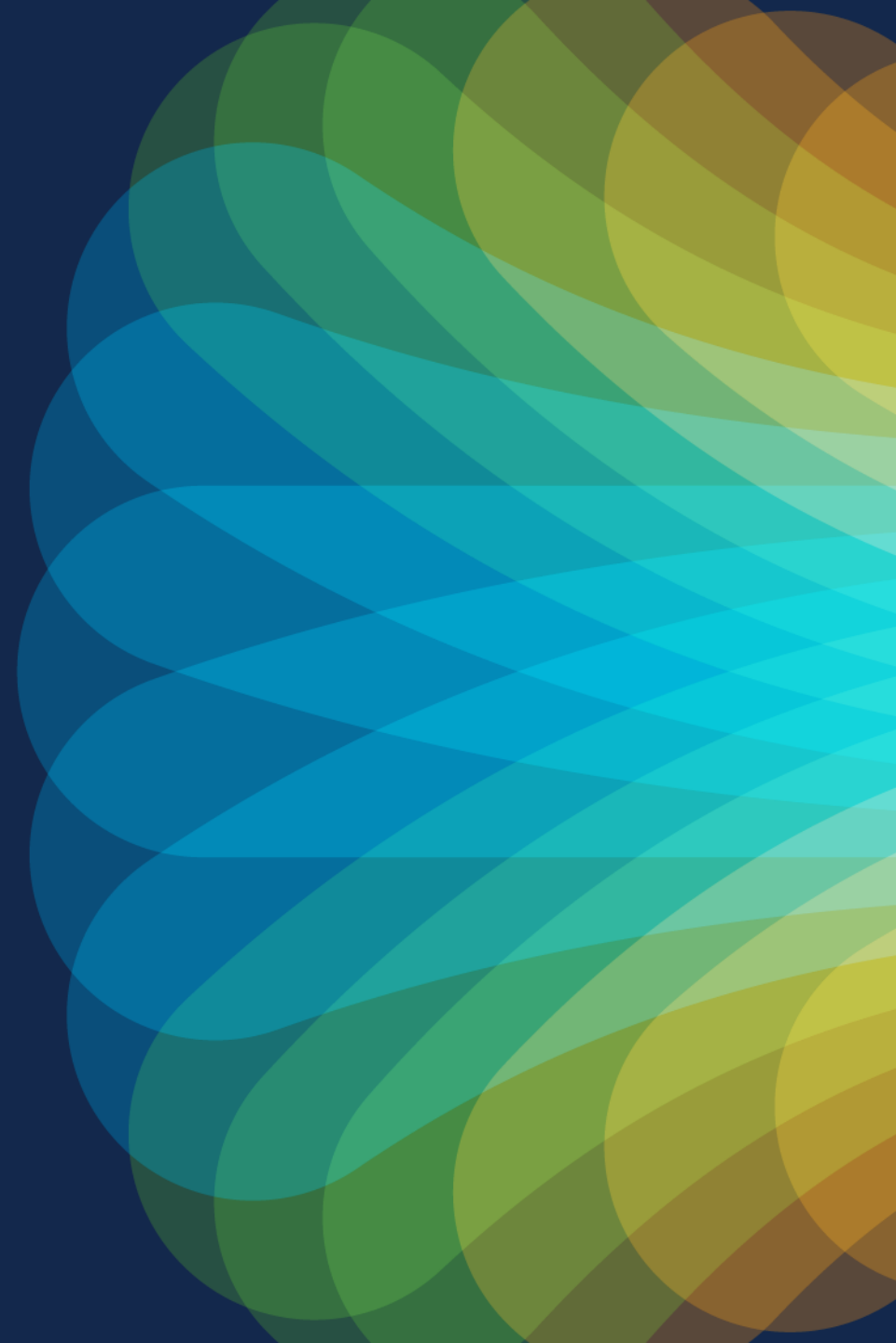
Enterprise Relay with Apple iCloud Private Relay On



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)



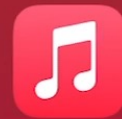
Dashboard (PWL)



SEO (PWL)



Settings



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

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		

Zero Trust Access Journey

Pragmatic migration to more control – direct to private apps

Take control of all your private apps
with precision

Unified Zero Trust Access + VPNaaS

Granular controls at the
application level. VPNaaS for
non-standard apps

Success

VPN as-a-Service

Lift and shift your VPN to the
cloud – more control and
easier to manage

Benefits

- Reduced threat surface
- Posture verification
- App-specific access
- Least privileged access

Traditional VPN

Network level access – cannot
control at app level – difficult to
deploy and manage

- Zero Trust Access does not work for
VPN required apps
- Setting up Zero Trust Access for
every app and user can be arduous
- Move apps to Zero Trust Access
over time

CISCO *Live!*

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase 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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of orange, red, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect.

CISCO *Live!*

Let's go

#CiscoLiveAPJC