



CyberSec TECH DAY





CyberSec
TECH DAY

LEARN
CONNECT
WIN



Cisco Secure Access

Better for Users, Easier for IT, Safer for Everyone

Gustavo Medina, CCIE Security #51487
Technical Solutions Architect

Introducing Cisco Secure Access

Protect people and things as they seamlessly connect to anything from anywhere



Cisco Secure Access

A comprehensive Security Service Edge (SSE) solution to accelerate your SASE journey

Core SSE Capabilities



Firewall as a Service (FWaaS)



Secure Web Gateway (SWG)



Cloud Access Security Broker (CASB)



Zero Trust Network Access (ZTNA)

and so much more in one subscription...

Going beyond Core Security Service Edge

Cisco Secure Access



VPNaaS

Digital Experience Monitoring

DNS Security

Remote Browser Isolation

Data Loss Prevention

Advanced Malware Protection

Sandbox

Talos Threat Intelligence

AI-powered Platform

consolidate security into one cloud solution with a single subscription

Reimagine the user experience: Cisco Secure Access makes the connections you need

1 Connect to a network



Note: Supports both client and clientless connectivity

2 Get to work



Internet apps

Protected by Umbrella



SaaS apps

Protected by CASB



Private apps

ZTNA gives controlled access to selected applications

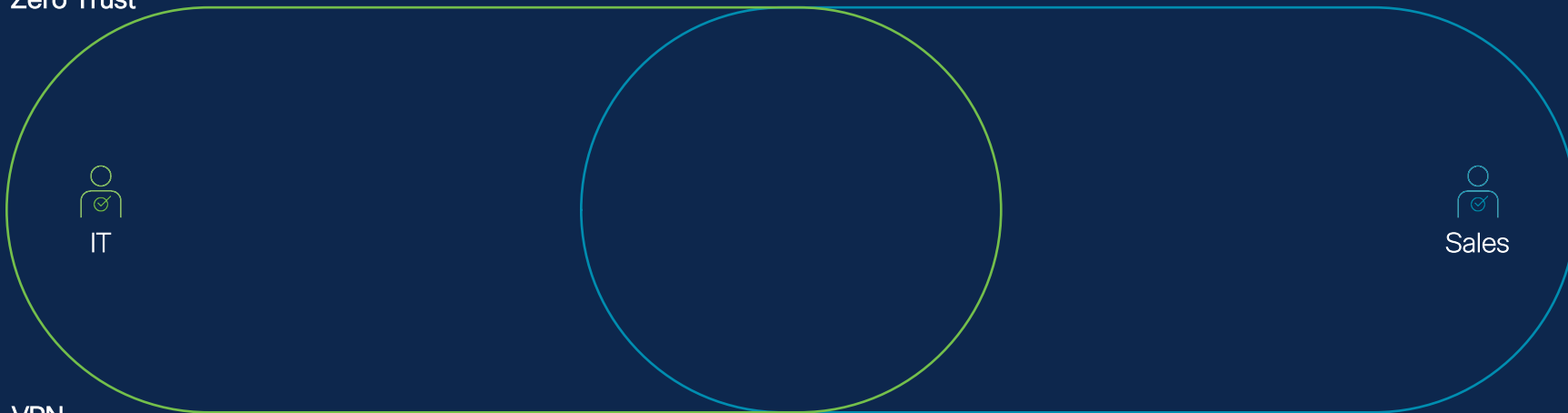


Traditional apps

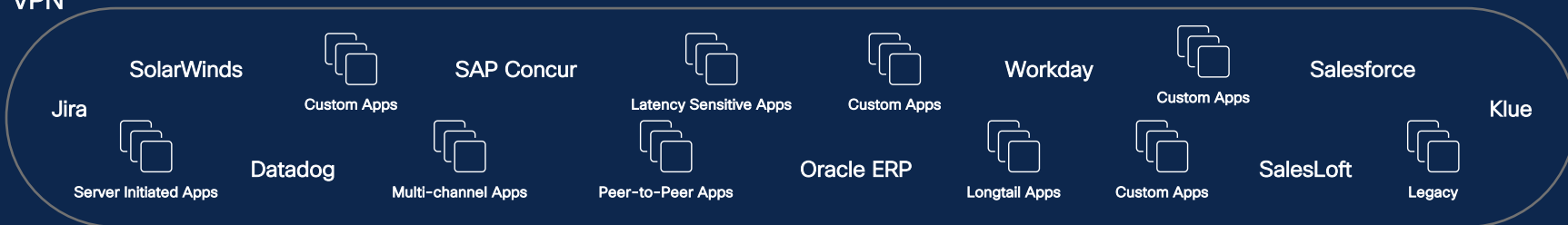
VPN gives network access for existing applications

Reimagine the journey to Zero Trust

Zero Trust



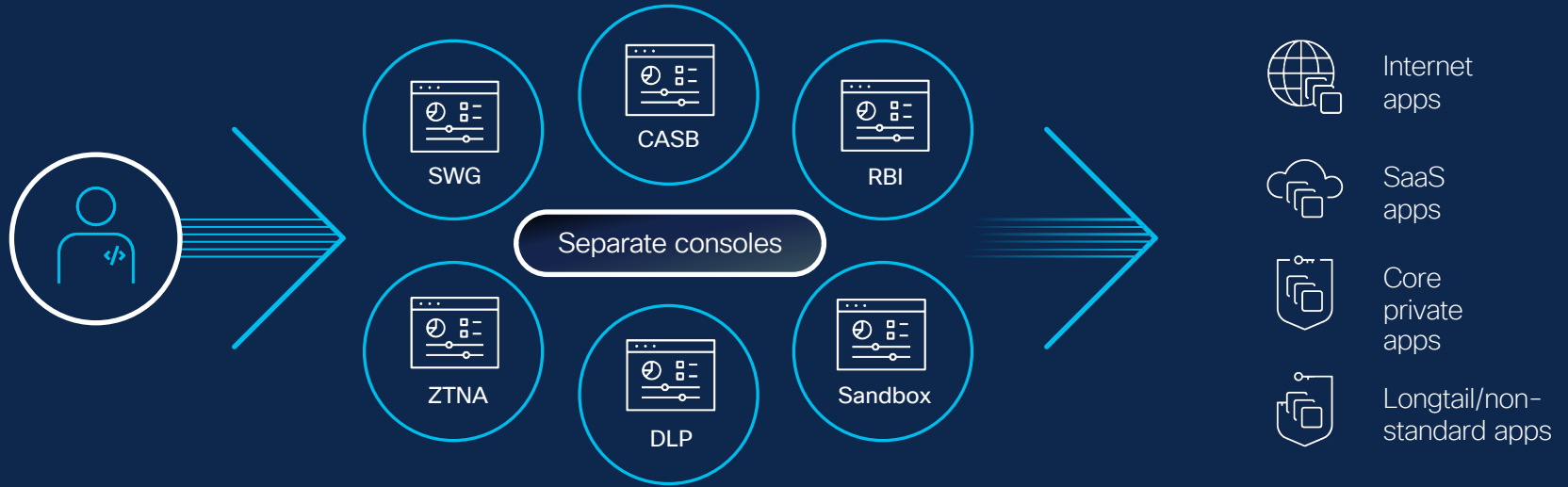
VPN



Easy migration to Zero Trust Access

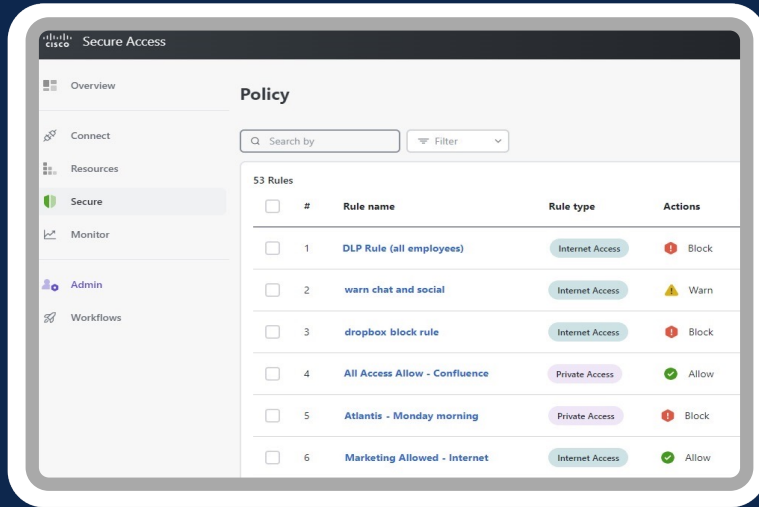


The multi-vendor approach is problematic



Easier for IT

Converged cloud security for lower cost and improved efficiencies



Higher efficiency

- Single agent
- Single console
- Single identity and posture
- Single policy management
- Single SLA

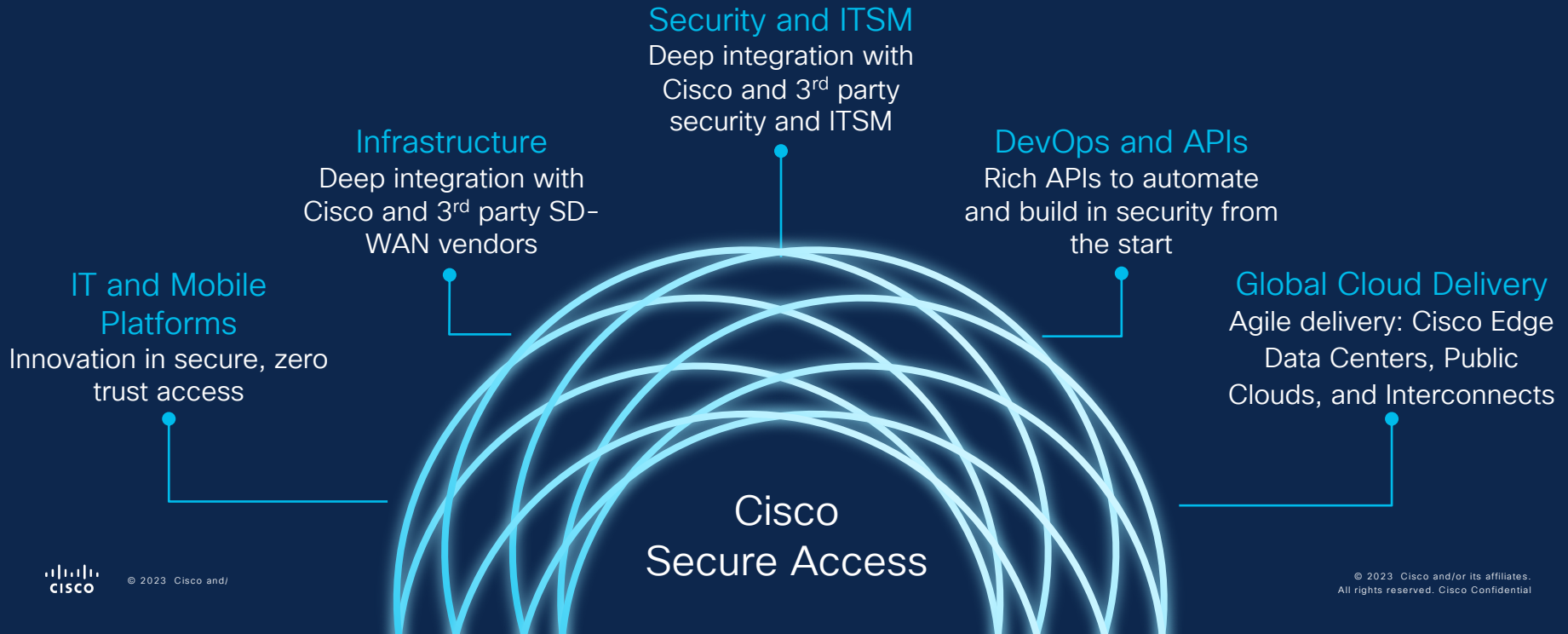
Lower costs

- Consolidated licensing
- Less hardware
- Ecosystem

One place to see traffic, set policies, and analyze risk
Built as part of the Cisco Security Cloud, an Integrated AI-powered security platform

Programmability and global ecosystem

integrates and expands your value



A great user experience everywhere

Moving the security closer to the user, not backhauling the user to the security

Extensive coverage globally

Hybrid POP approach
Cisco and public data centers

Speed. Everywhere

We target latency of ~40ms or
less for 99% of business users

End-to-end security

Cutting-edge,
comprehensive security
where you need it

Why Cisco Secure Access?

Trust and expertise at scale

Proven Expertise

70k

Cloud security customers

Proven Scale

220M

Secure endpoints

Proven Protection

600B

Requests per day



Cisco Secure Access

Announcing Accelerated General Availability!

private preview feedback is overwhelmingly positive

- More than 30 customers
- More than 200 customer meetings

Accelerated GA allows us to...

- Capture year-end budgets
- Build our pipeline for H1FY24

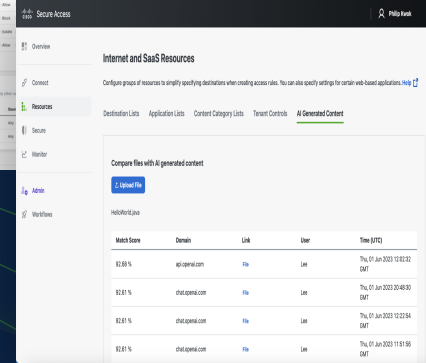
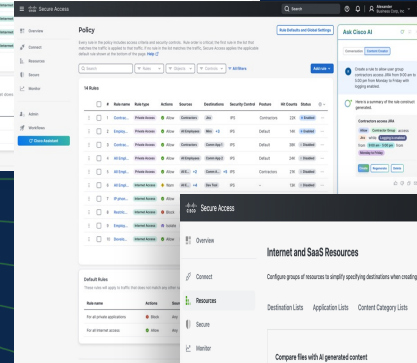
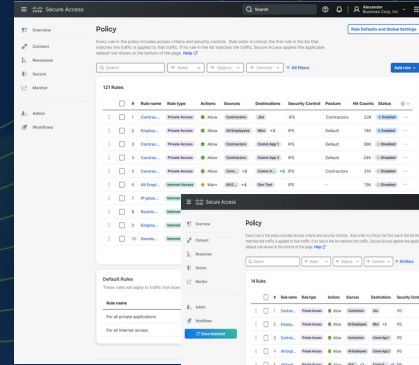
Security Service Edge is Fundamental to your Security Strategy

Converged set of cloud security



SSE

65% plan on adopting SSE in next 2 years



Why ZTNA?



ZTNA

Zero Trust Network Access



ZT

Zero Trust

Principals



NA

Network Access

Why ZTNA?



Zero Trust



User Experience

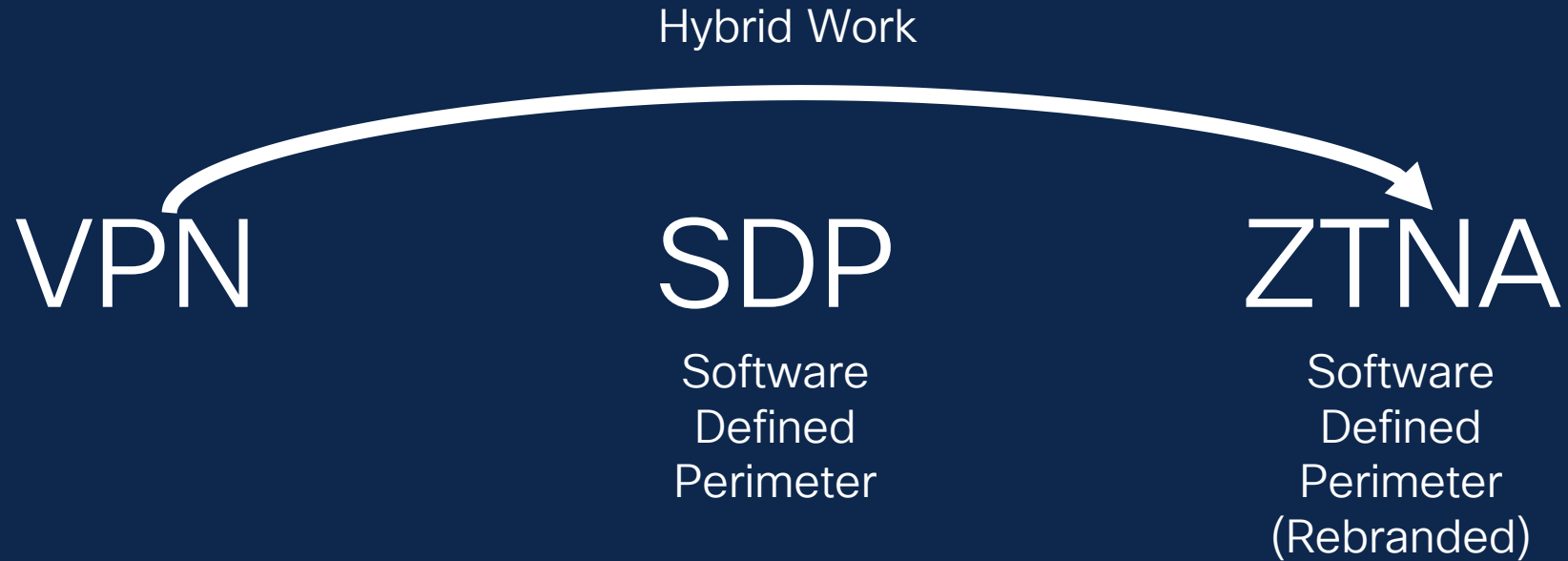


SaaS Delivery

Evolution of ZTNA



Evolution of ZTNA: Organization Adoption



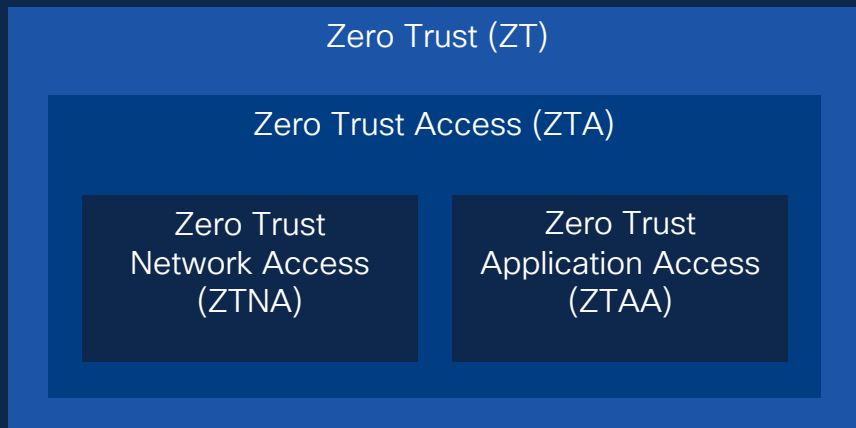
ZT vs. ZTA vs. ZTNA vs. ZTAA

- **Zero Trust**

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

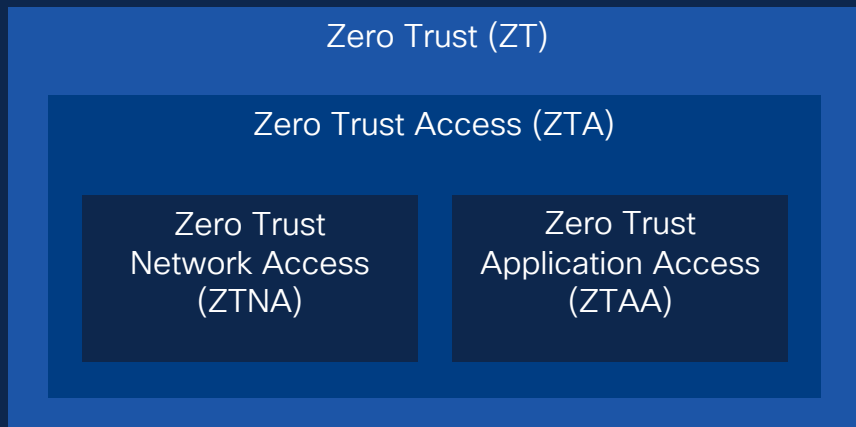
- **Zero Trust Access**

- 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

Cisco Secure Access

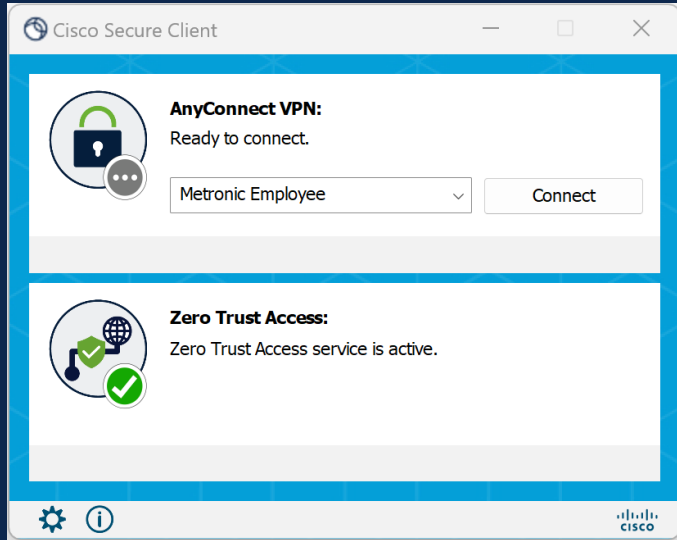




User Demo:

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?

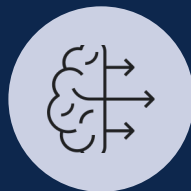


No direct
resource
access
(forward
proxy

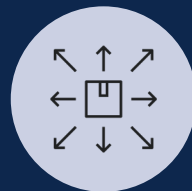
architecture)



Broad
application
support
(TCP, UDP
and IP)



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

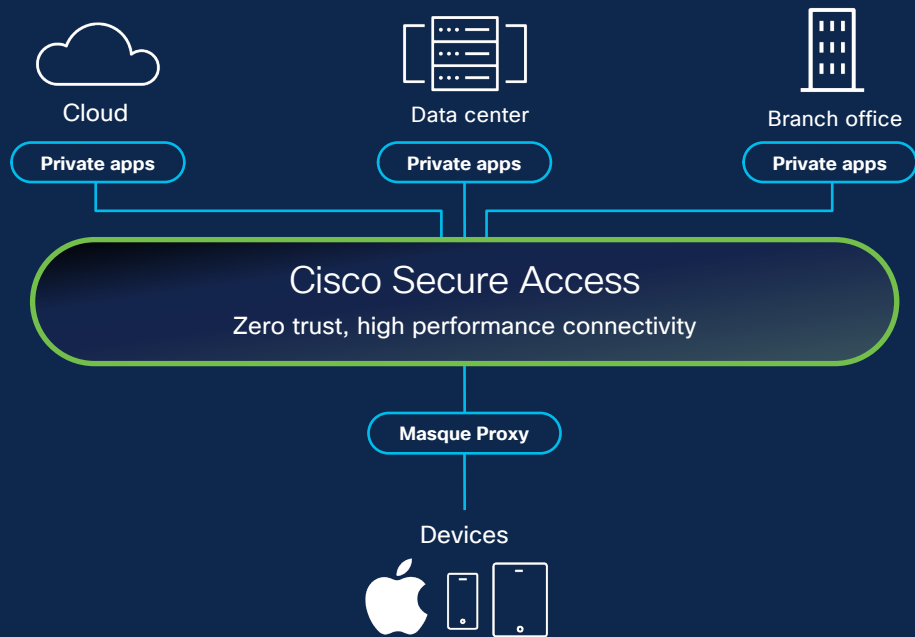


Flexibility to support
per-connection,
per-app or per-
device tunnels



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

COMING
SOON

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





User Demo:

Zero Trust Access
on Apple iOS





AnyConnect



Duo Mobile



Okta Verify



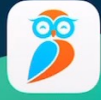
Billing



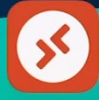
Dashboard



SEO



Owlfiles



RD Client



Billing (PWL)



Dashboard (PWL)



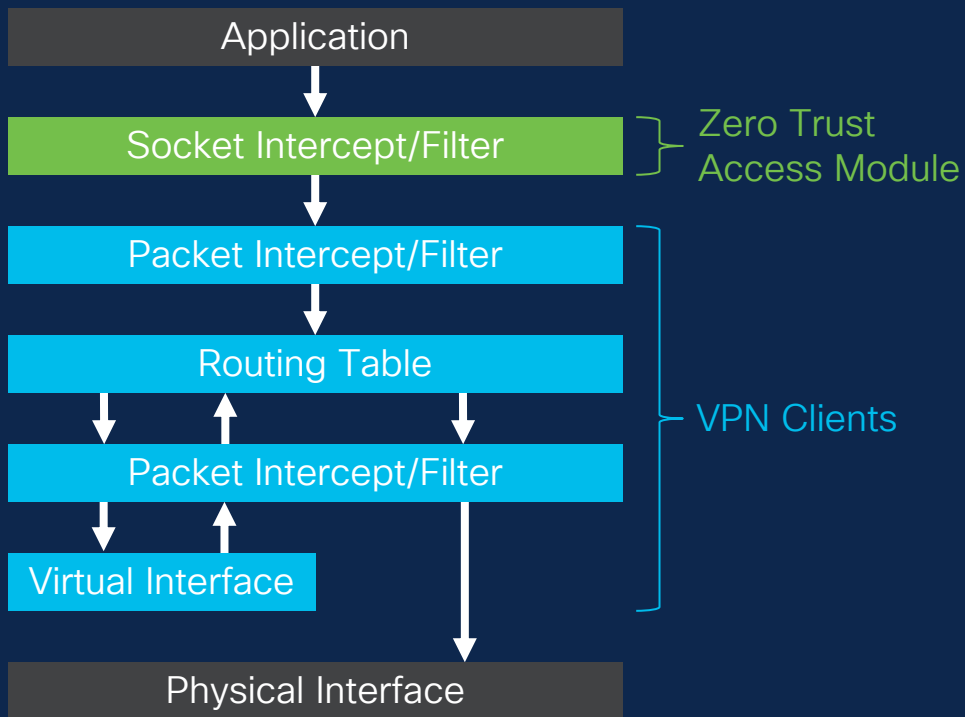
SEO (PWL)



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



ZTNA Module: All your ZTNA traffic belongs to me



User Demo:

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



Recycle Bin



RDP (Via OpenVPN)



Perimeter (Via ZTNA)

Cisco Secure Client

AnyConnect VPN:
Ready to connect.

Metronic Employee

AnyConnect ZTNA:
AnyConnect ZTNA service is active.

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' 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

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

Take control of all your private apps with precision

Traditional VPN

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

VPN as-a-Service

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

Unified Zero Trust Access + VPNaaS

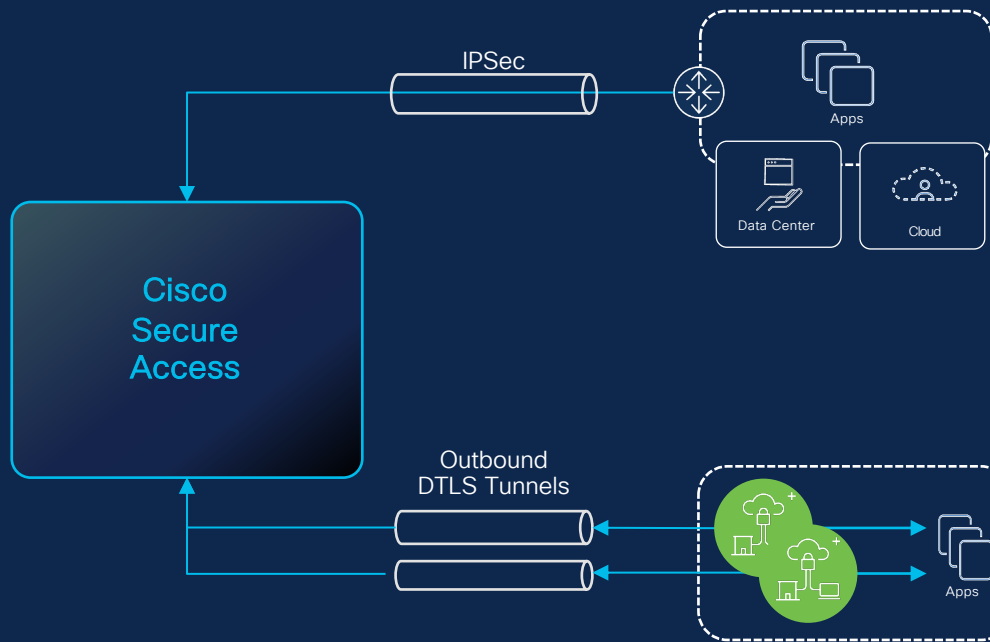
Granular controls at the application level. VPNaaS for non-standard apps

Success

Benefits

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

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



The bridge to possible