

Cisco Secure Access

cisco Live !

Deep Dive Into ZTA and Private App Access

Justin Murphy
Technical Leader – Cloud Security

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 14 November 2025.



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

Who Am I?

- Father of 2 Fantastic Kids
 - Nature Enthusiast
 - Lifelong Learner
-
- 15+ years in the Information Technology Industry
 - Product focus on SSE, SASE, ZTA

Agenda

- 1 Introduction
- 2 Zero Trust Principles
- 3 What is MASQUE?
- 4 What is QUIC?
- 5 Secure Enrollment
- 6 Traffic Interception
- 7 ZTA with Secure Access
- 8 Secure Client
- 9 Secure Access Updates

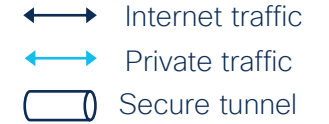
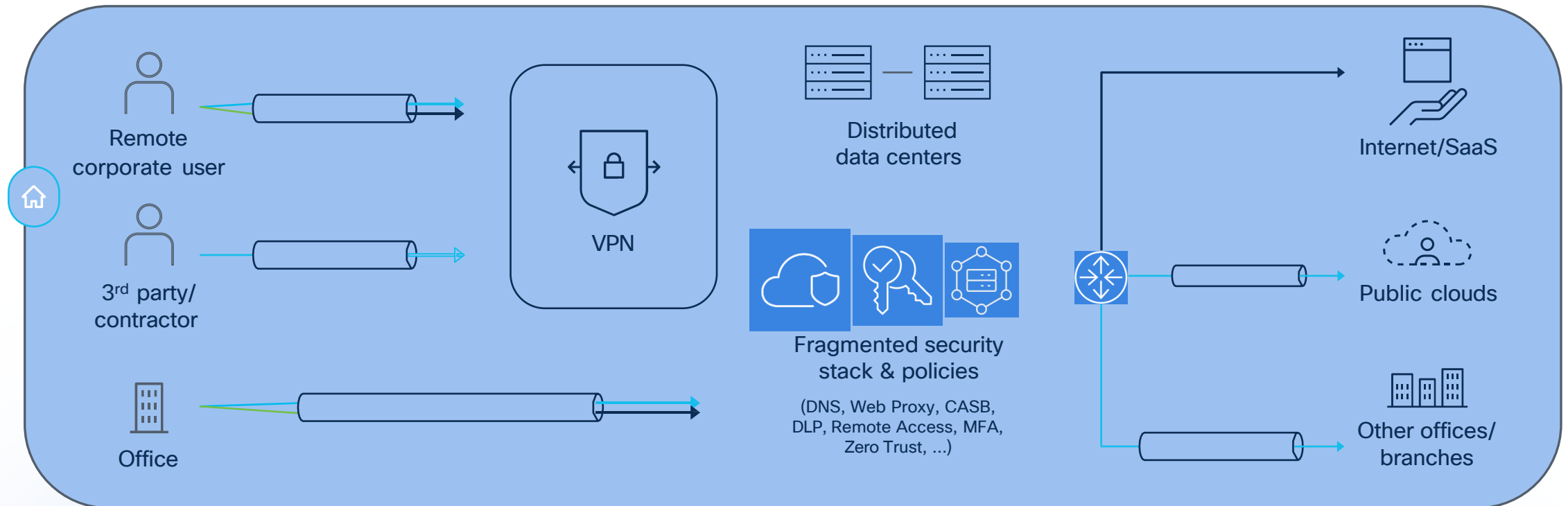


Security of network resources has been viewed traditionally as a **trade-off between security and convenience**. The lack of a network-layer security protocol suitable for use in large, administratively heterogeneous internetworks, has given rise to ad hoc security efforts, such as mailbridges, filtering routers, firewalls, application-level gateways, etc. The fundamental problem with these efforts is that, **in enforcing security, they cripple the connectivity that makes internetworking attractive in the first place.**

John Ioannidis, Matt Blaze
“The swlPe IP Security Protocol”
December 3rd, 1993

Challenge

An architecture never designed for hybrid work

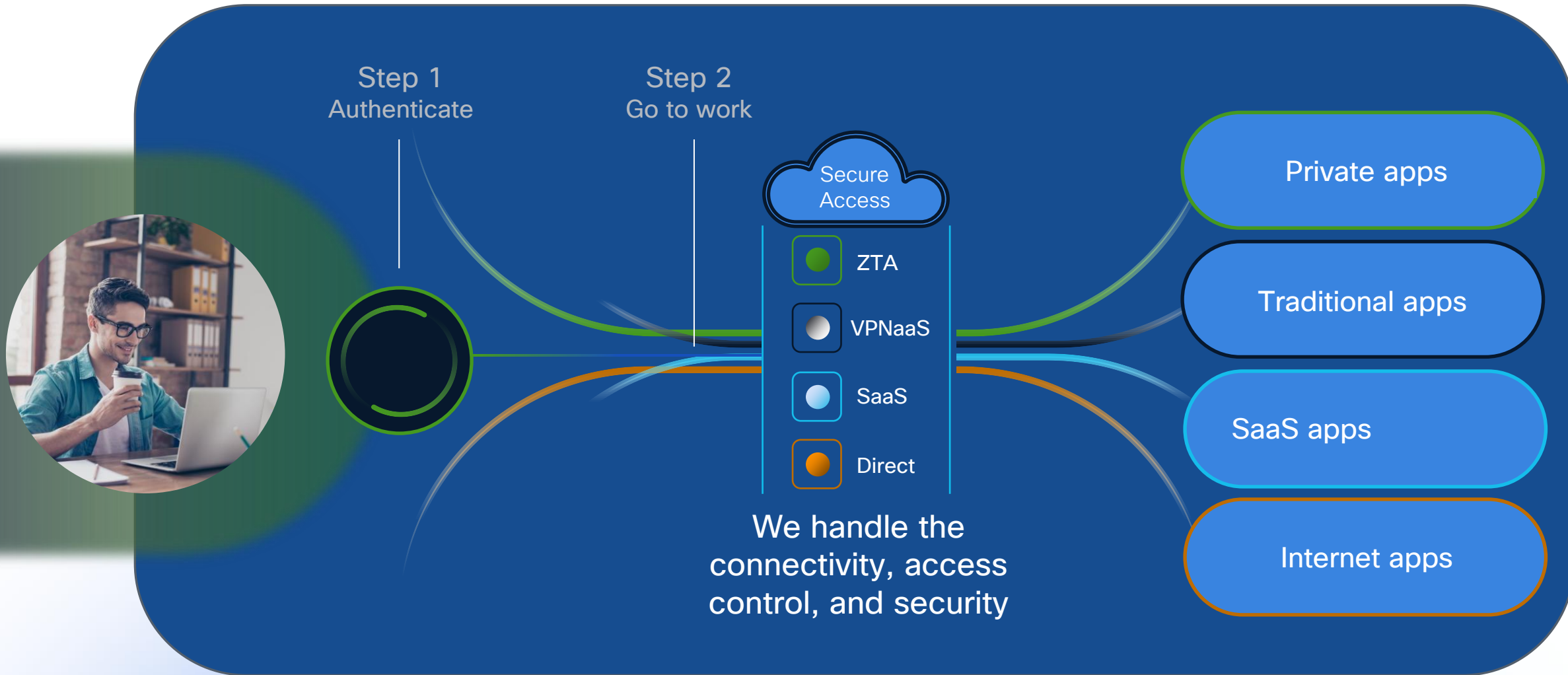


Poor user experience
Lower productivity

Large sets of individual solutions and vendors
Complexity of operations and costs

Gaps in security posture born out
of complexity and fragmentation

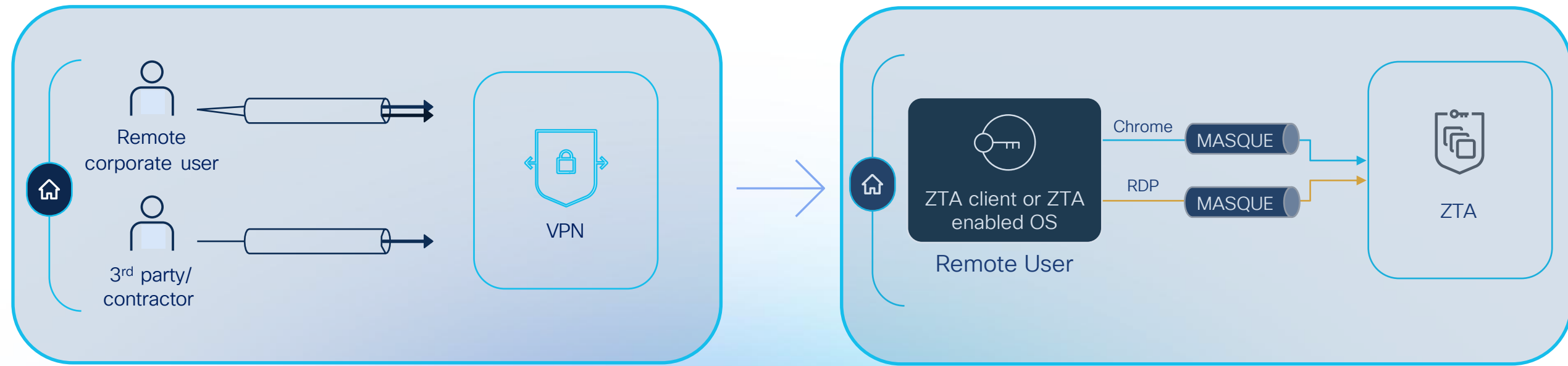
Cisco Secure Access



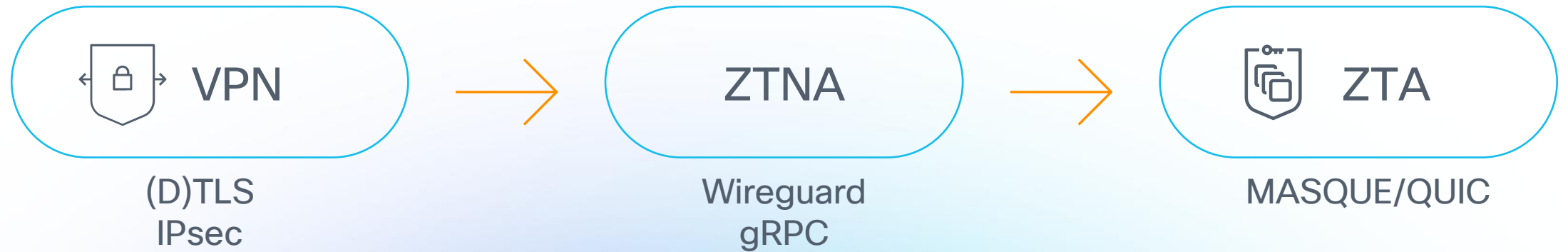
Enables Hybrid work, securely with no drama, no fuss.

Zero Trust Principles

Evolution of Remote Access



New Protocols for a New Approach



Modern Zero Trust Access Design

Architectural components



Next generation
protocols



Identity
aware proxy



Micro-
segmentation



Synthetic
addresses



Native
OS support



Network
isolation



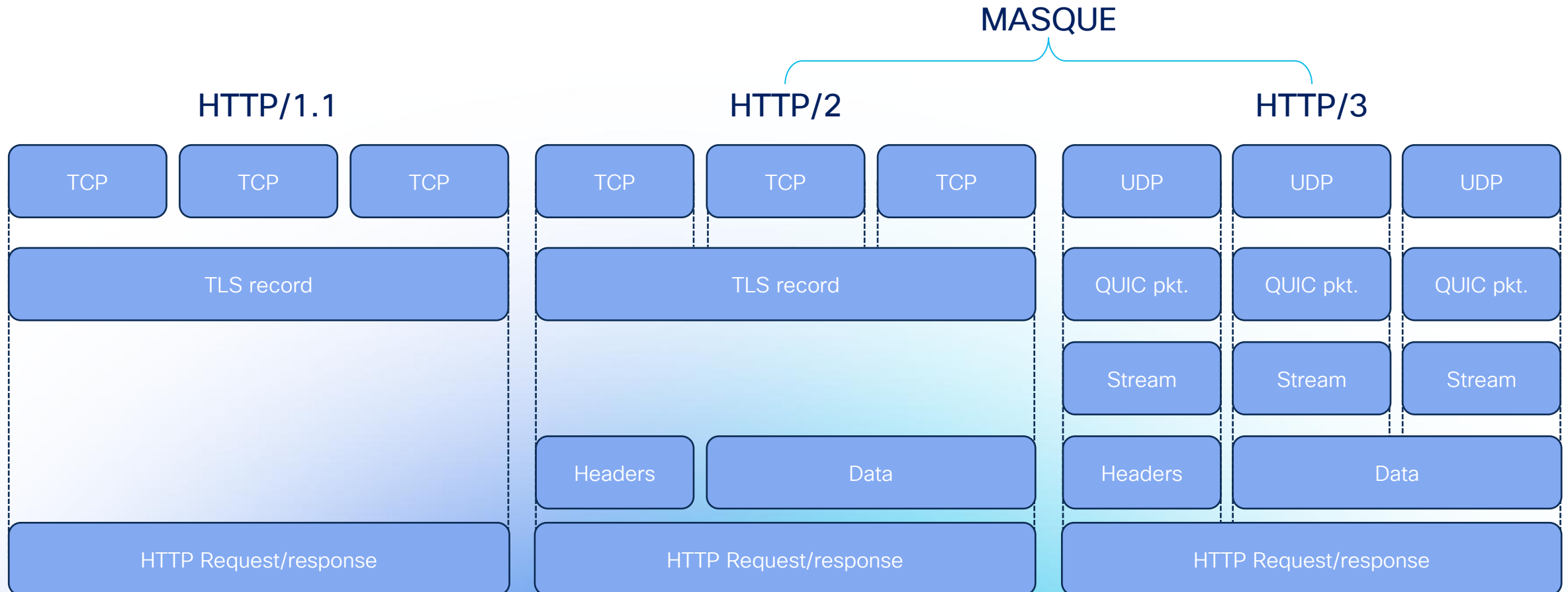
Flexible cloud/app
connectivity options



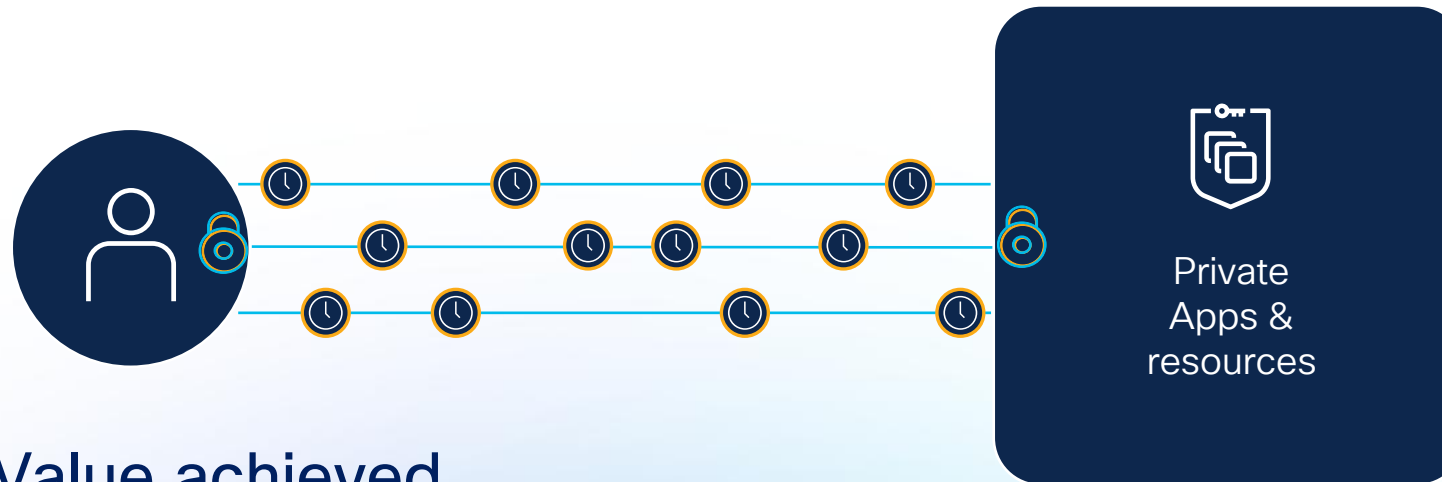
TPM certificate
protection

What is MASQUE?

HTTP Formats for Forward Proxy



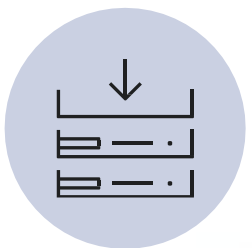
MASQUE Protocol Micro-Segmentation



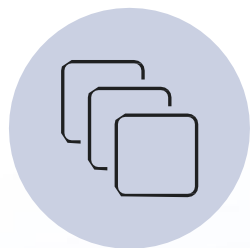
Value achieved

- Unified policy makes creating / managing user based zero trust policies easy
- Trust state is evaluated for every flow
- Least privileged access enforced for every resource
- Users only see the resources policy says they should
- Micro-segmentation directly from inside the OS at a process level

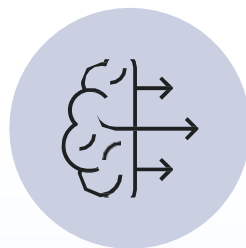
Zero Trust Access Benefits of MASQUE



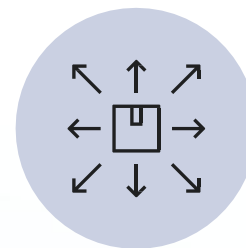
No direct resource access (forward proxy architecture)



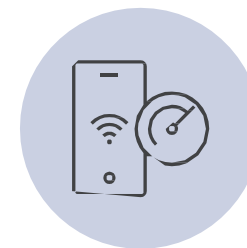
Broad application support (TCP, UDP and IP)



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)

What is QUIC?

Benefits of the QUIC Protocol



Fast

Better user experience than TCP/TLS for HTTP/2



Secure

Always-encrypted end-to-end security



Evolvable

Not set in stone, new versions deployed quickly



Compatible

Supports all TCP content while avoiding known TCP issues

UDP



CC



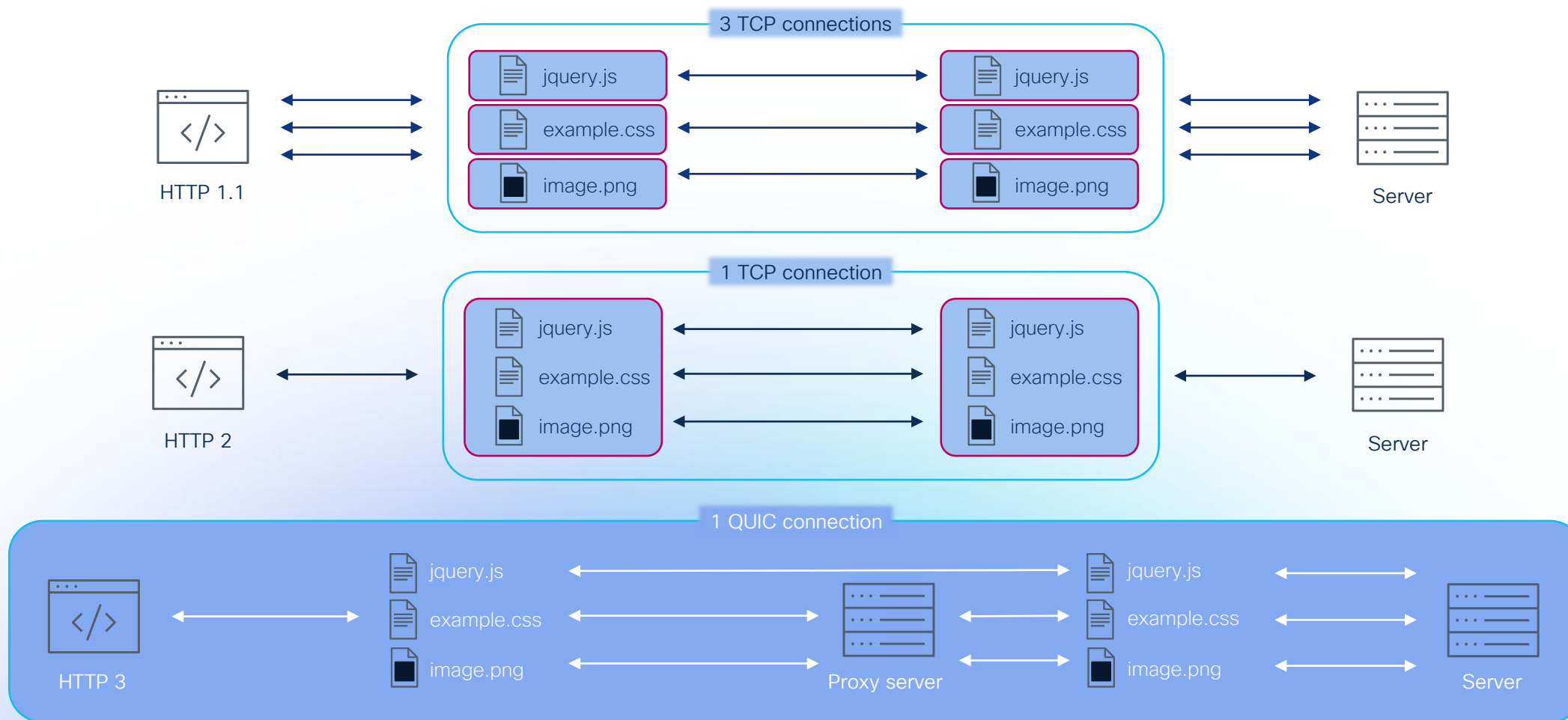
TLS



HTTP



From TCP to QUIC



Zero Trust Access Benefits of 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)

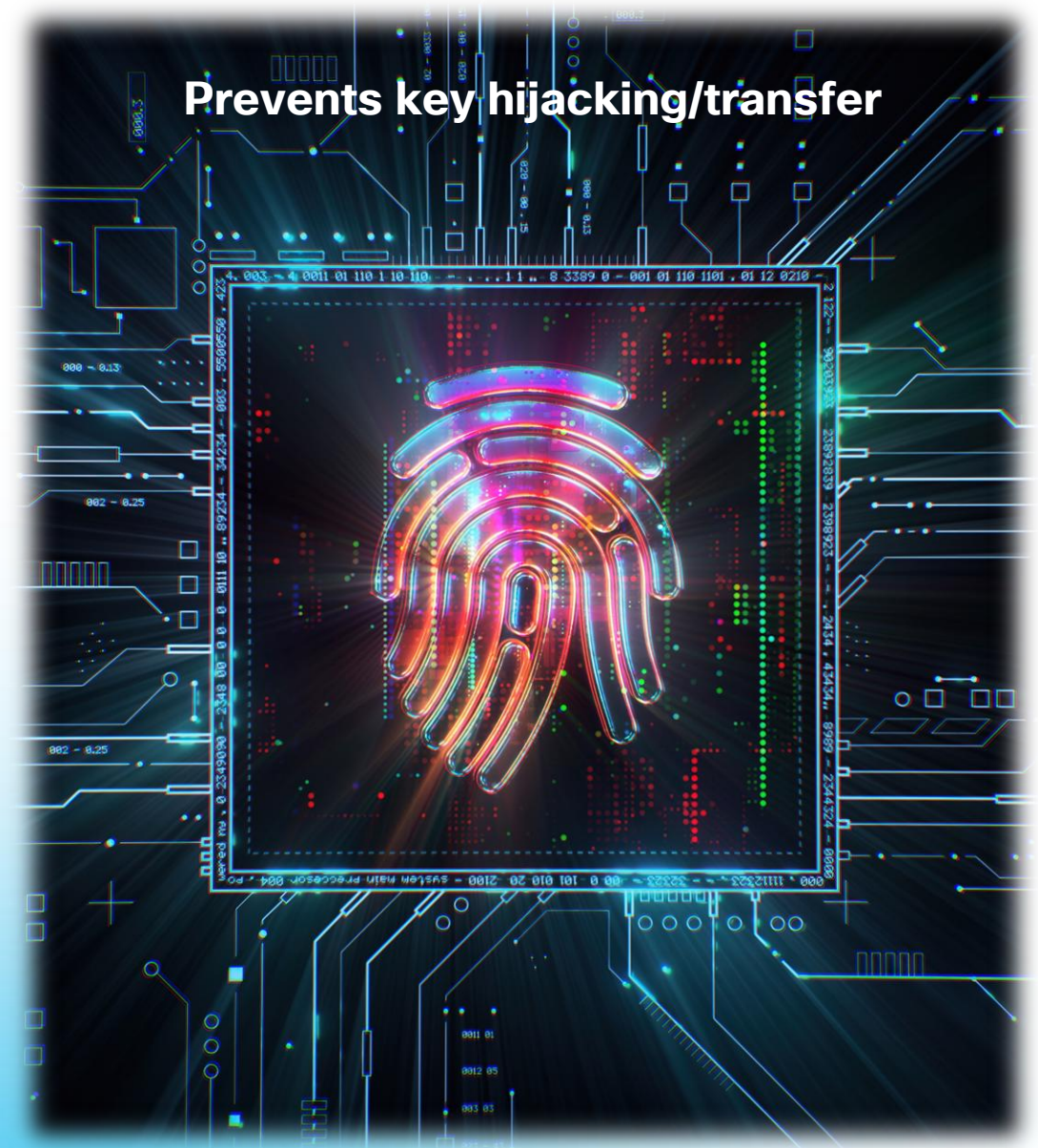


Can simultaneously use multiple interfaces (Multipath)

Secure Enrollment

What is a TPM?

- TPM is a hardware enclave that protects private keys
- Most TPMs do not store private keys directly, but instead key-wrap them so that they can't be accessed without the root TPM key stored in hardware
- On Windows this is known as a TPM 2.0 device
- On macOS and iOS this is called the “Secure Enclave”
- On Samsung devices this is called Knox TPM
- Ensure private key can't be extracted, preventing certificates from being stolen and reused
- Different than the software feature ‘non-exportable’ flag, which is easily defeated in most OSes

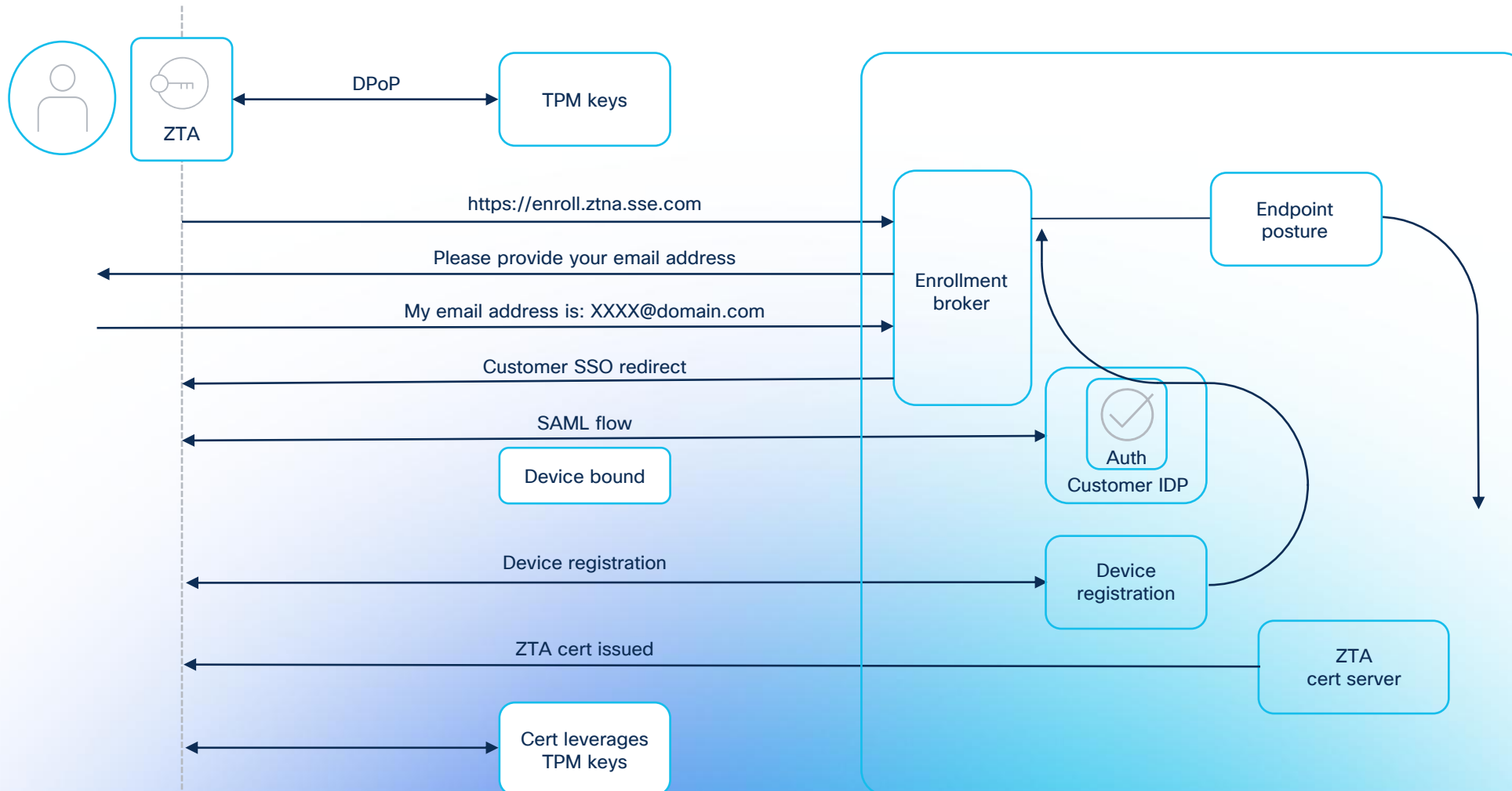


How does ACME work in ZTA?

- Users enroll using Biometric Identity via SAML
- DPoP is a new IETF OAuth standard for token binding
- DPoP key pairs can be generated in hardware
- User and device identity attributes are bound to a device during enrollment
- An ACME certificate challenge is completed, and an identity certificate is issued to that user/device pair with TPM-bound private keys
- Certificate renewal is automatic every 3 to 5 weeks and uses the previously issued TPM-bound certificate to verify identity



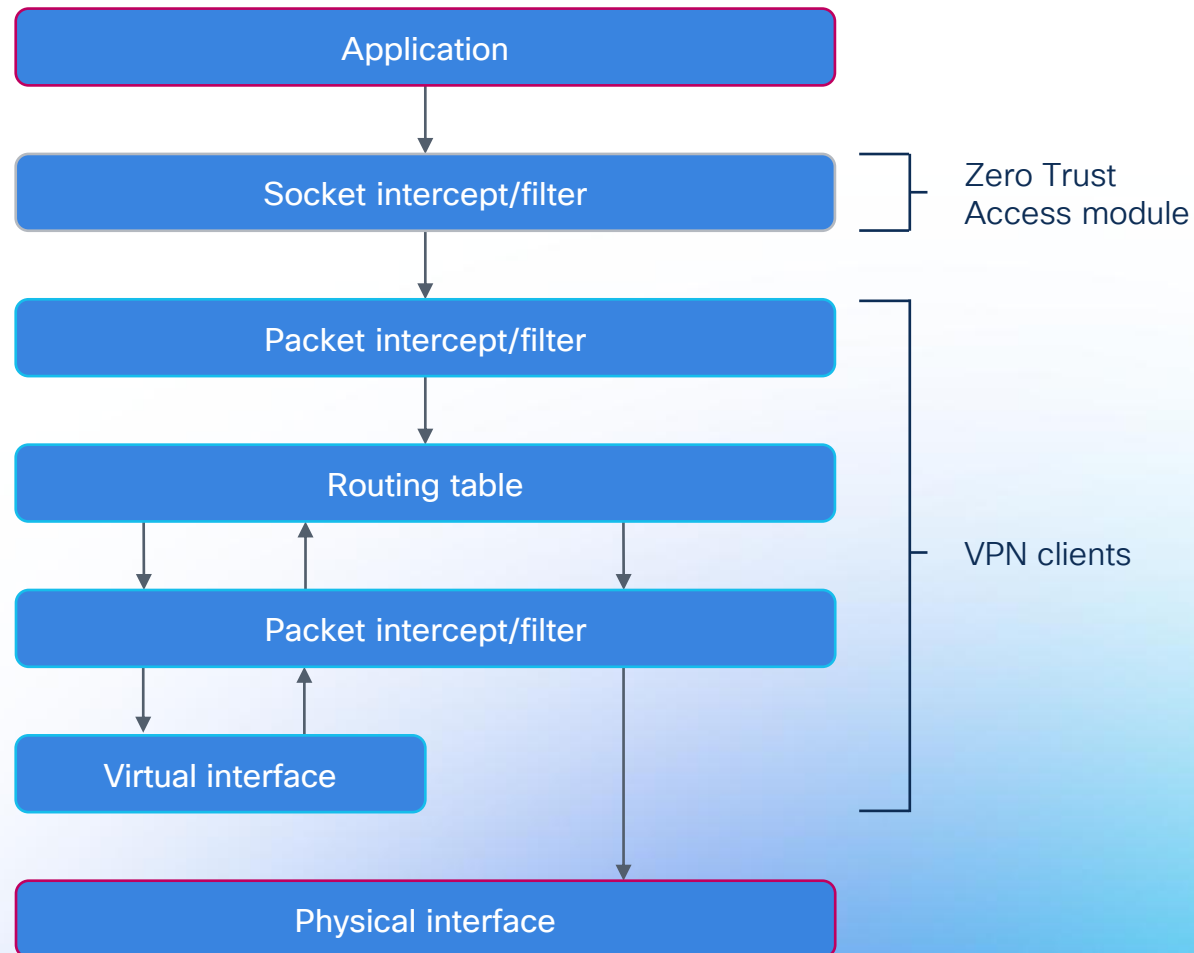
Enrollment Procedure



- Simple for user
- Advanced level of security

Traffic Interception

Zero Trust Access – Socket Intercept



Why socket intercept?

- No DNS on the wire
- 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

IP Packet vs Socket Streaming

Packet approach

VPNs and legacy ZTNA use packets



CGNAT is obfuscation not security



Firewalls and NATs rely on timing for IP protocols other than TCP, often 30 seconds or more



Attackers can piggyback on UDP flows to continue them in IP packet systems

Streaming approach

modern ZTA uses socket streams

010110
110010
001011

Socket streaming allows any protocol to be tracked by socket call and terminated at the instance the socket is closed



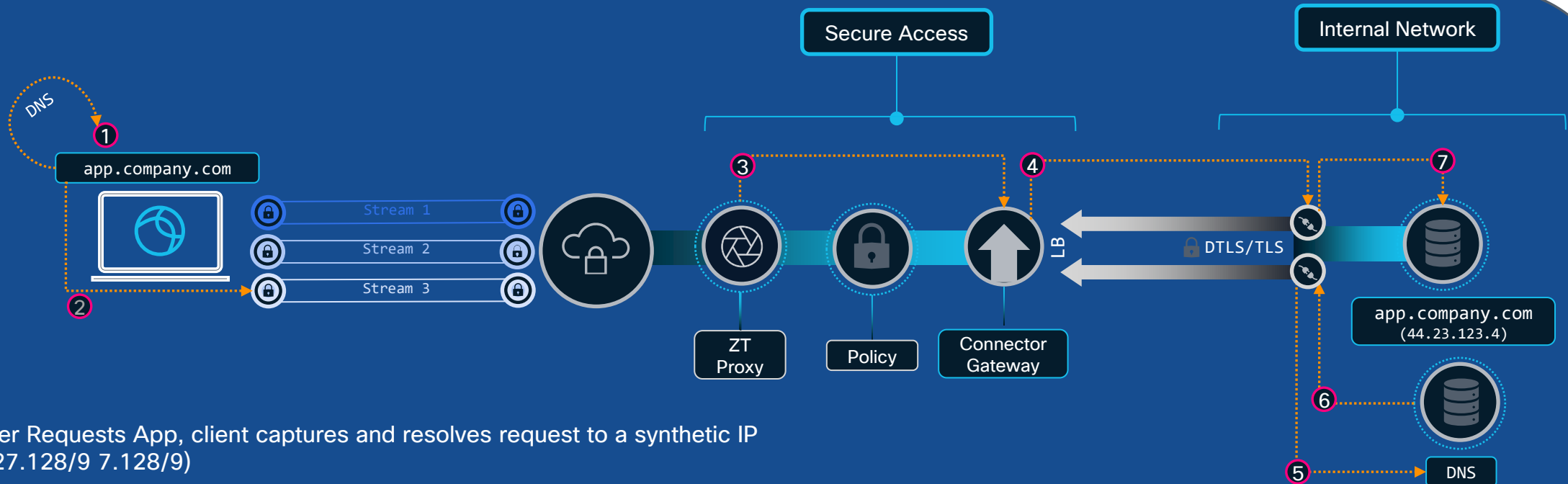
Socket streaming eliminates timers and is deterministic



Flows can't be continued or hijacked

ZTA with Secure Access

Seamless and Secure Access for Everyone



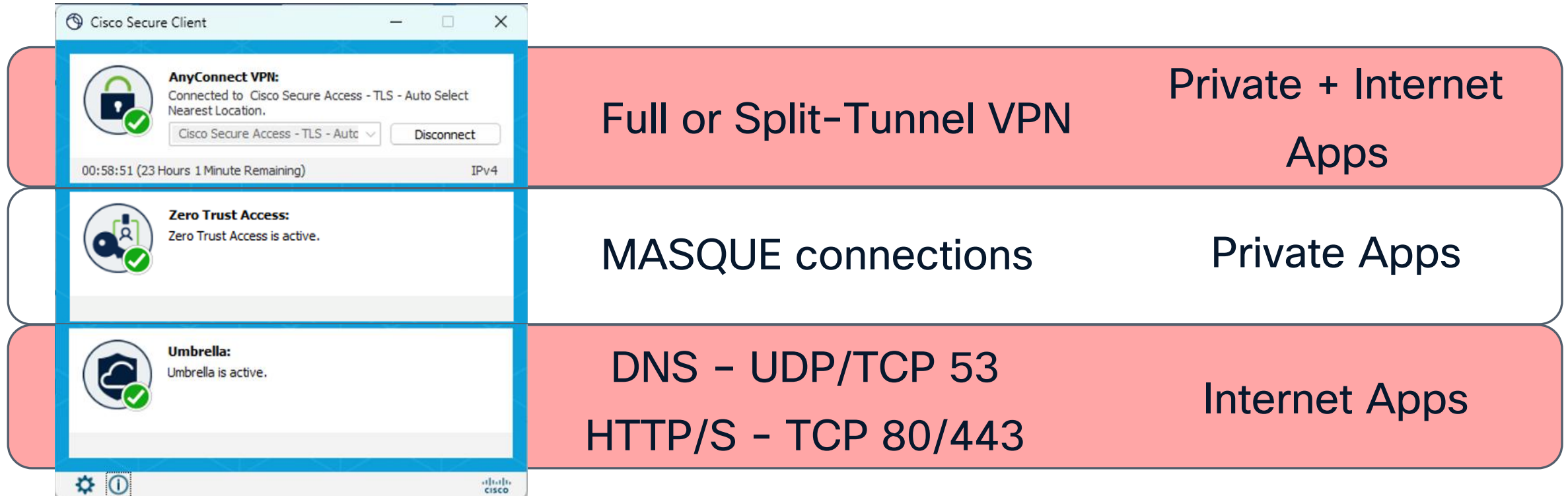
- 1 User Requests App, client captures and resolves request to a synthetic IP (127.128/9 7.128/9)
- 2 Traffic is transported to ZT Proxy in Secure Access via a stream in MASQUE
- 3 TCP connection is proxied and built to the mapped resource connector, Policy is enforced on traffic
- 4 Gateway establishes connection to resource connector
- 5 Resource connector resolves APP IP
- 6 Local DNS responds with App IP
- 7 Resource connector establishes connection to App

- Seamless In Office Experience
- Full separation between user's network and enterprise network

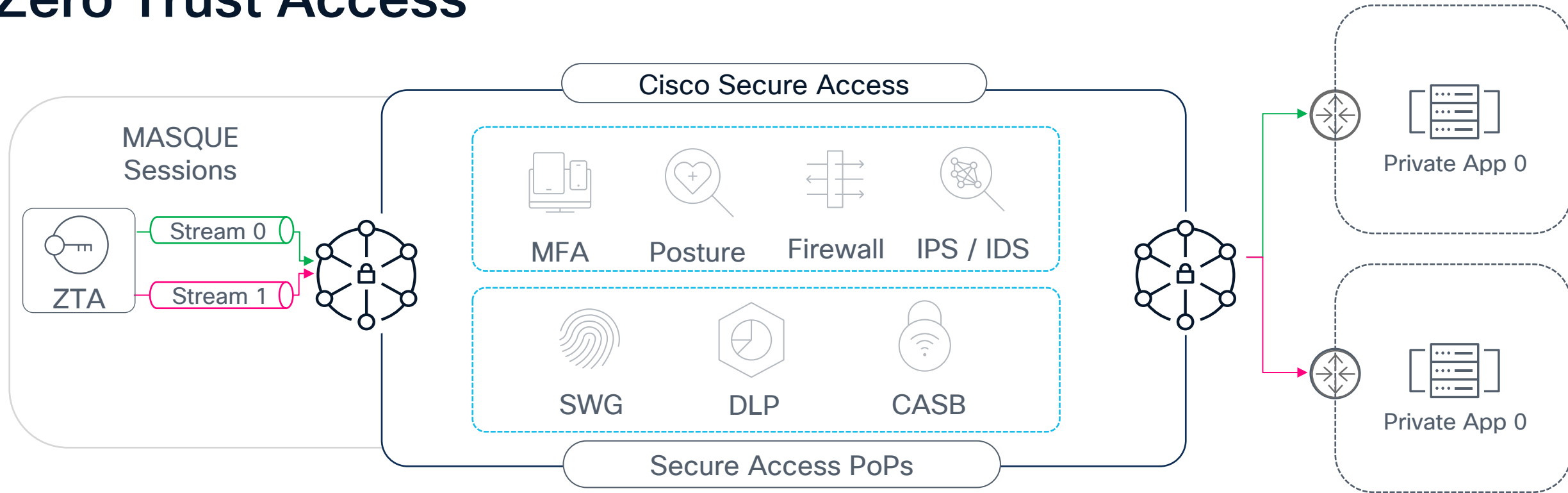
Secure Client

Secure Client Modules

[Previous](#) public and private app connectivity



Zero Trust Access



- Transparent user experience
- Forward proxied resource access with coarse or fine-grained access control
- Service managed client certificates with TPM-protected key storage
- Inside to out L4-7 tunnels from RCs
- No routing complexities
- Apps are hidden, supports overlapping subnets
- Easy to scale with high availability



Settings



Zero Trust



RD Client



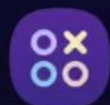
Boxborough
Fair



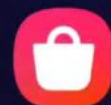
Gallery



Clock



Gaming Hub



Store



Play Store



Google



Enterprise Browser

Cisco and Google Enhance Zero Trust Access

Google Chrome Enterprise



Browser-based security for web apps



Cisco Secure Access



Cloud-based security for Private apps and more

DEVICE TRUST



SECURE ACCESS TO ALL APPS



EXPANSIVE TELEMETRY

Unmanaged Devices

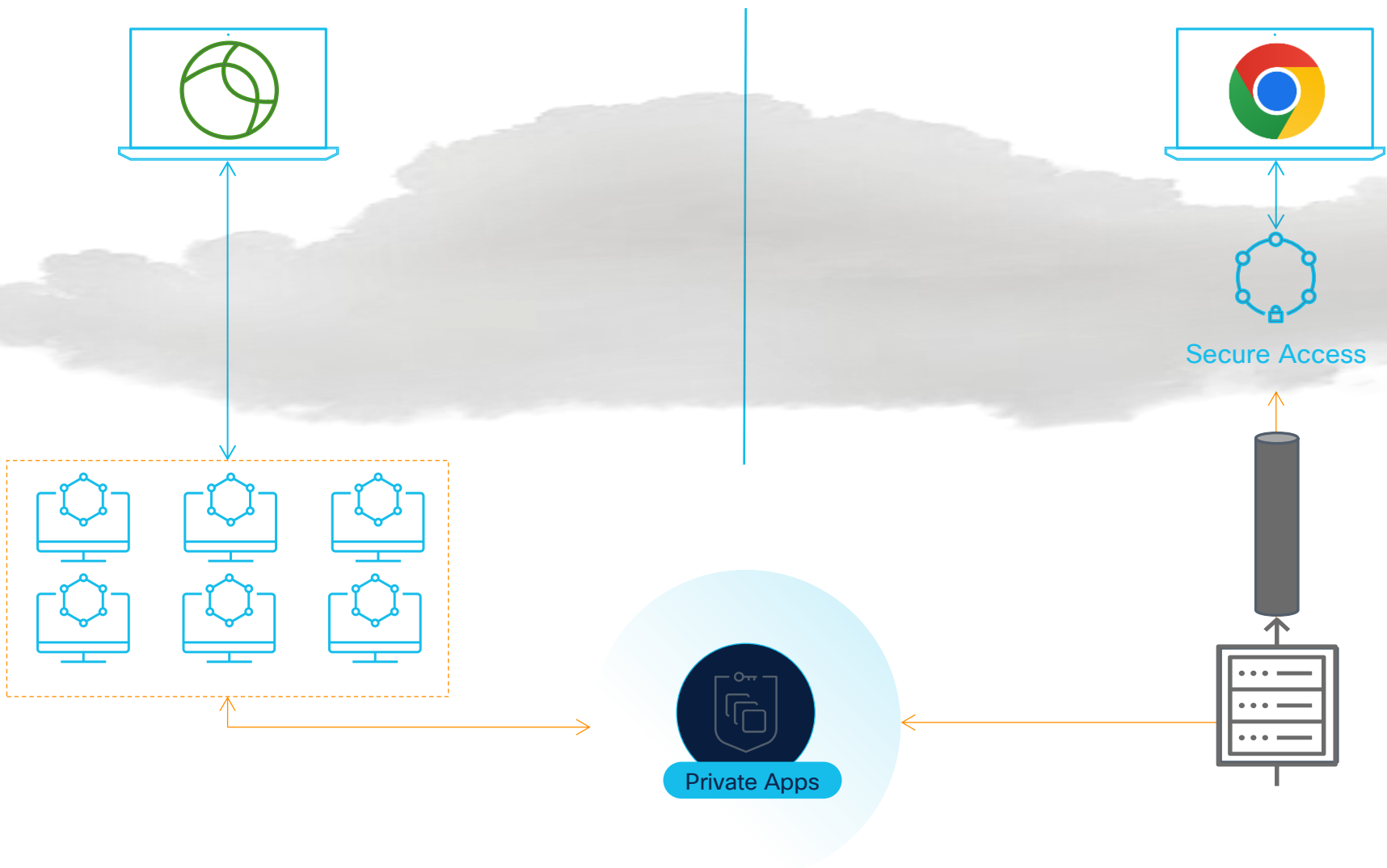
Extend ZTNA to BYOD

Private application access for

- Partners
- Contractors
- No software to deploy

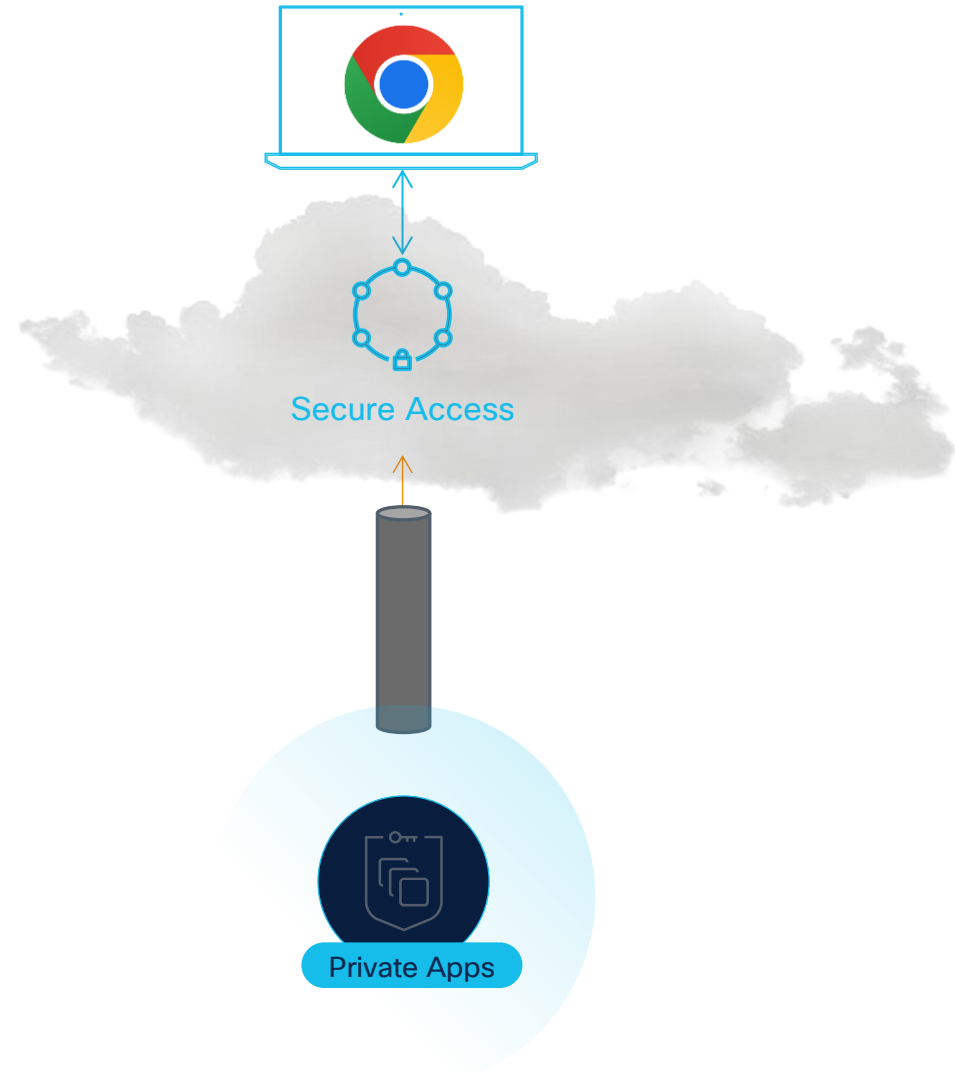


VDI Replacement



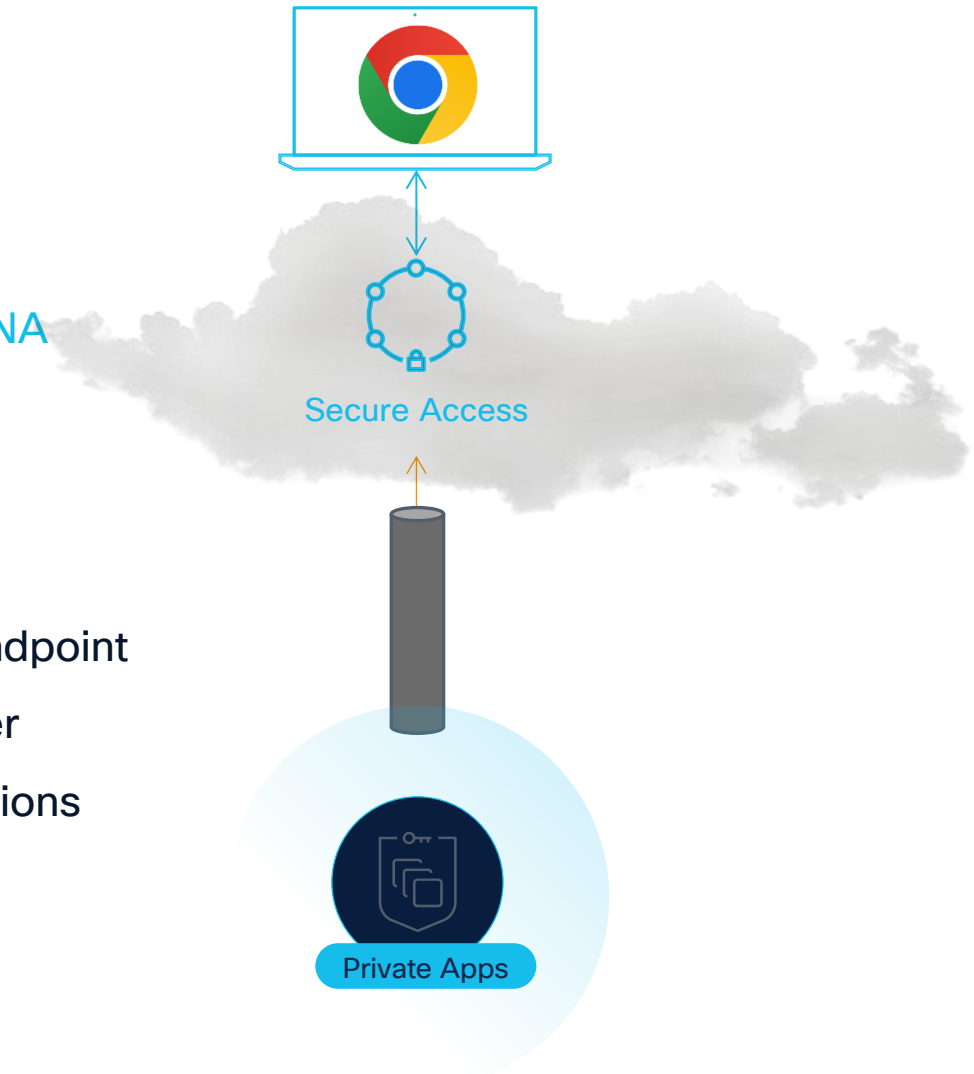
VDI Replacement

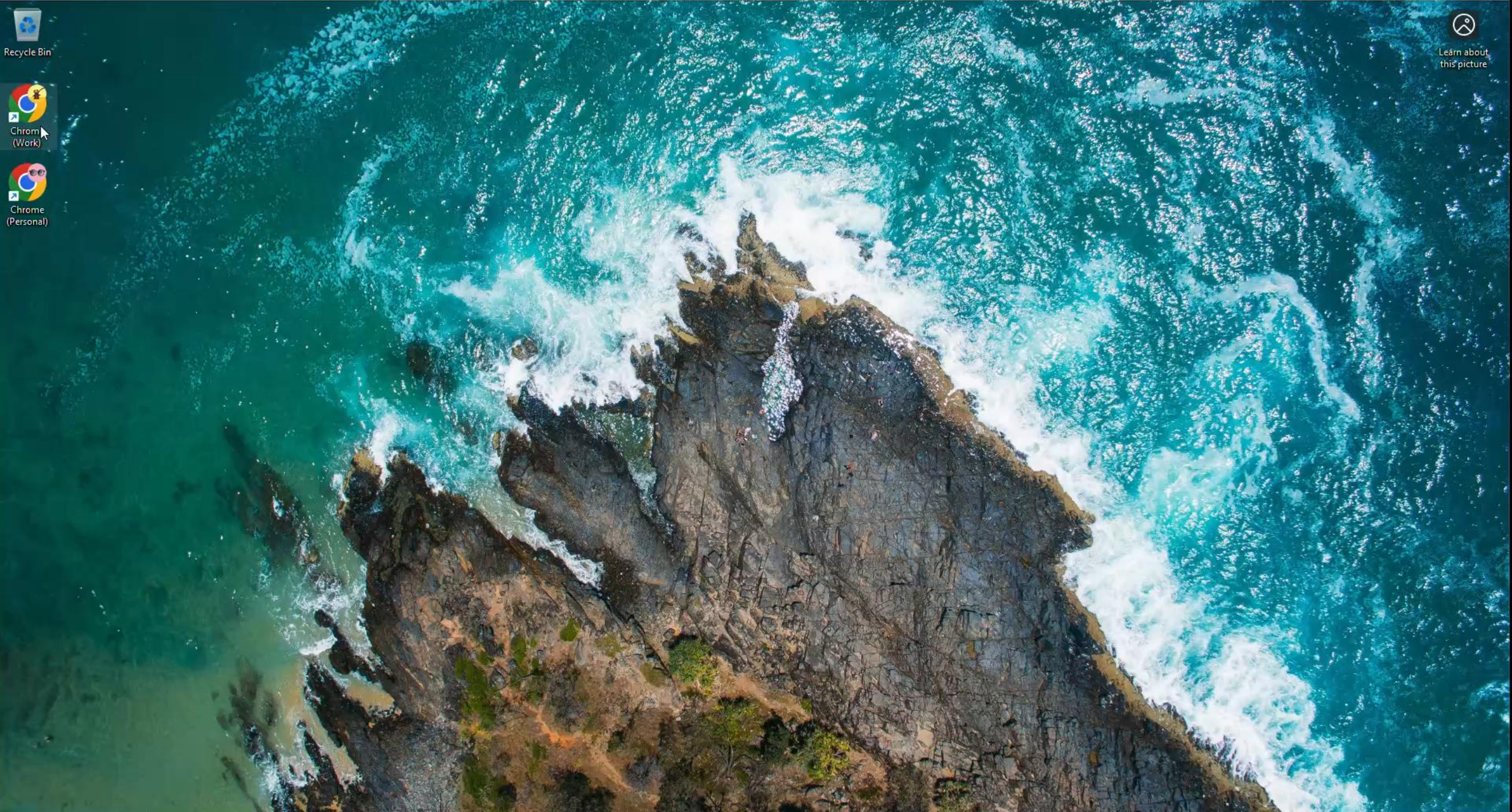
- Simplified Infrastructure
- Cost Efficiency
- Lightweight and Streamlined
- Built-in Security Features
- Improved User Experience
- Modernized Security Approach
- Bandwidth Efficiency
- Scalability



Separation of Duties

- **Network Security with SSE:**
 - Provides secure and optimized connectivity to cloud resources via ZTNA
 - Enforces centralized policies
 - Ensures consistent security for both remote and hybrid workforces
- **Endpoint Security with Enterprise Browser:**
 - Delivers session isolation to protect against malicious activity at the endpoint
 - Implements local data loss prevention (DLP) directly within the browser
 - Enables granular, context-aware access controls for sensitive applications






Learn about
this picture

-  Recycle Bin
-  Chrom
(Work)
-  Chrome
(Personal)

Google Chrome Enterprise Browser

Summary

- Google Device Connector establishes trust with Secure Access
- Posture signals shared from Chrome to Secure Access
- Chrome provides local security enforcement
- Secure Access provides:
 - Back-end application connectivity
 - Additional security features
 - Digital Experience Management
- User Cases:
 - VDI Replacement
 - Contractors / Third Party Application access
 - BYOD

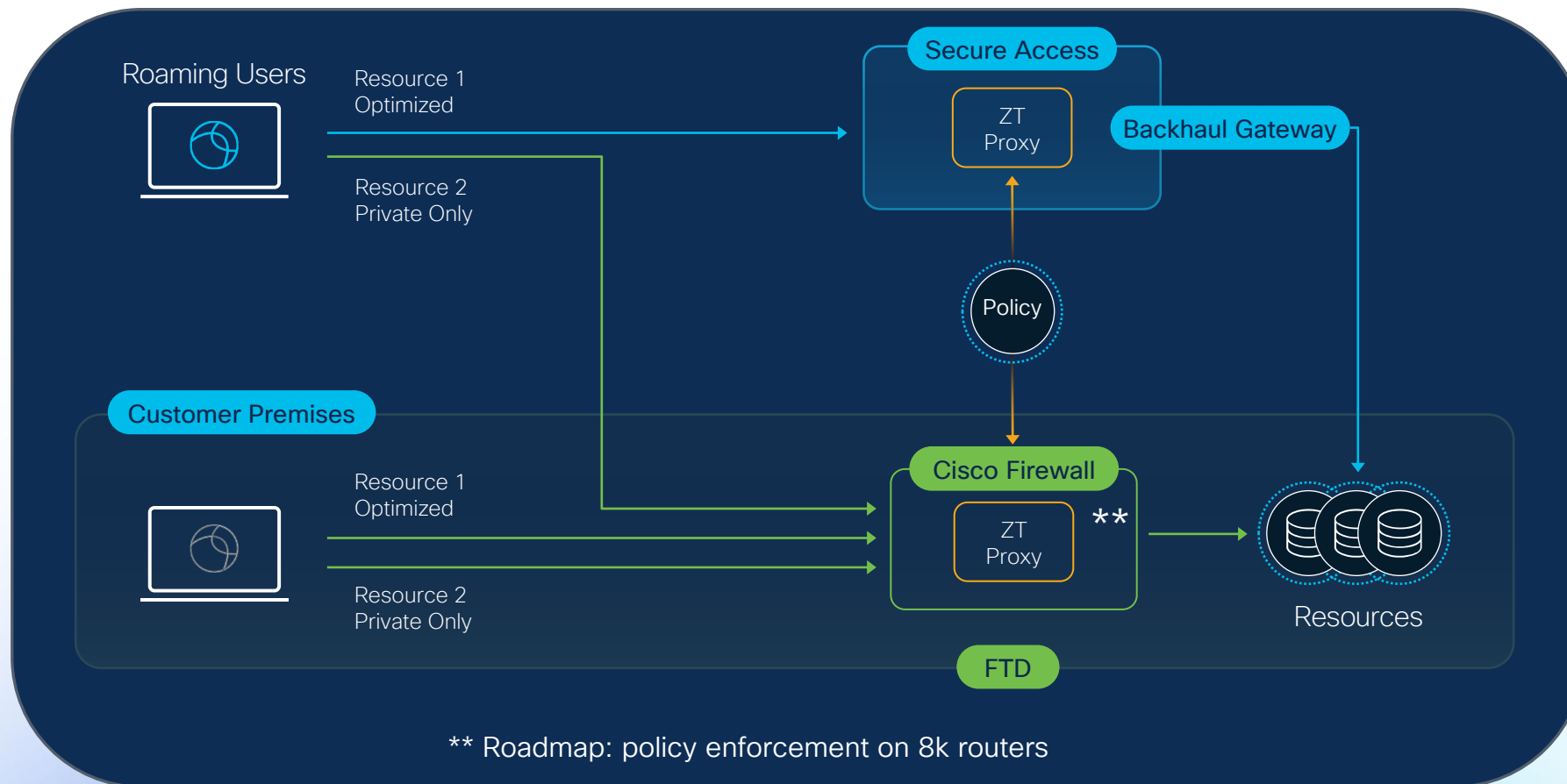
Resources

- Enterprise Browser:
 - <https://www.cisco.com/c/en/us/products/collateral/security/secure-access/chrome-enterprise-integration-aag.html>
 - <https://services.google.com/fh/files/misc/cisco-secure-access-chrome-enterprise-recommended.pdf>
 - <https://www.cisco.com/c/en/us/products/collateral/security/secure-access/sec-access-chrome-enterprise-sg.html>
 - <https://docs.sse.cisco.com/sse-user-guide/docs/chrome-enterprise-browser>

Hybrid ZTA

Hybrid ZTA with FTD

Flexible Steering, Consistent Enforcement



ZTA Module Updates

Zero Trust Network Access Module

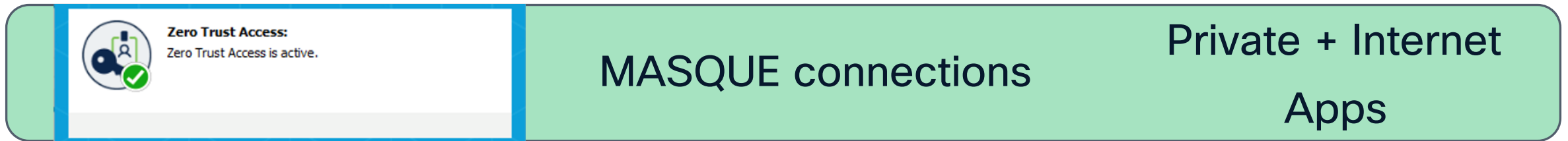
New and Upcoming Features

- ZT Internet Access
 - Lite version – Based on Destination List
 - Full – Split Include / Exclude
- ZT Network Access Profiles
 - Steering rules per user / group
 - Posture for Internet access
- ZT Network Access Trusted Network Detection
 - Trusted DNS resolver
 - Trusted DNS search domain
 - Trusted HTTPS server



Zero Trust Profiles

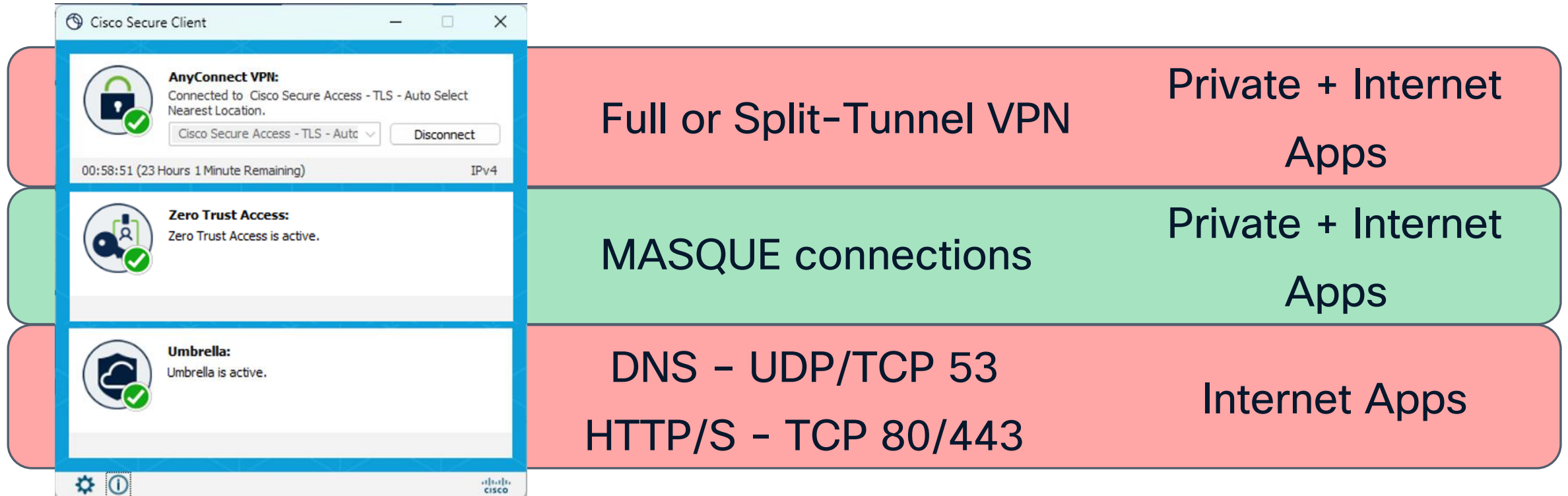
- **Previous** behavior was to push all app steering to **all clients**
- Even if they did not have access to the app
- Synced to the client in a **JSON configuration** file
- **KDF filter** intercepts based on FQDN or IP address
- **New** behavior will allow for **steering** rules per **user/group**
- Push configuration to client based on who needs access
- Fully **compatible** with **Reserved IP**



Zero Trust Internet Access

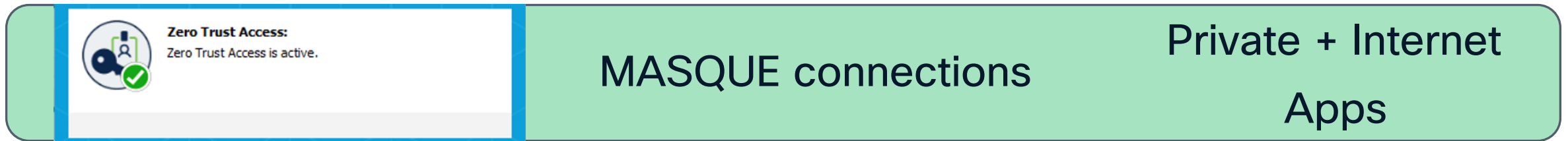
Secure Client Modules

New public and private app connectivity



Zero Trust Internet Access

- All ports and protocols security for roaming users
- Seamless in-office user experience
- No need to connect VPN profiles
- Native mobile support for iOS and Samsung Android
- Unified client for both private and Internet access
- Client enrollment for identity aware access
- Compatible with VPN



Zero Trust Internet Access

C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments\cached_configs

Destination List	Destinations	Excluded Destinations
Internet ZTA	8	+ Add
<div><div>Destination</div><div><div>youtube.com</div><div>facebook.com</div><div>yahoo.com</div><div>gambling.com</div><div>instagram.com</div><div>browserleaks.com</div><div>ssh.christianclasen.com</div><div>web.christianclasen.com</div></div></div>		



```
{
  "fqdn": {
    "include": [
      "*.browserleaks.com",
      "*.facebook.com",
      "*.gambling.com",
      "*.instagram.com",
      "*.ssh.christianclasen.com",
      "*.web.christianclasen.com",
      "*.yahoo.com",
      "*.youtube.com",
      "browserleaks.com",
      "facebook.com",
      "gambling.com",
      "instagram.com",
      "ssh.christianclasen.com",
      "web.christianclasen.com",
      "yahoo.com",
      "youtube.com"
    ]
  },
  "id": "tia_steering_config",
  "label": "TIA Steering Config"
}
```

Zero Trust Internet Access

- DNS queries for resources **resolve** to a **local** listener
- Requests **forwarded** to the **MASQUE** proxy in the cloud

```
PS C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments\cached_configs> Resolve-DnsName youtube.com
```

Name	Type	TTL	Section	IPAddress
----	----	---	-----	-----
youtube.com	AAAA	15	Answer	100::eb11:df24:fd8:4d26
youtube.com	A	15	Answer	127.145.127.117
youtube.com	A	15	Answer	7.145.127.117



Recycle Bin



Google Chrome



Microsoft Edge



Webex

Cisco Secure Client

**Zero Trust Access:**
Registration is required to access secure resources.

Enroll

**Umbrella:**
Umbrella is active.





Zero Trust Internet Access

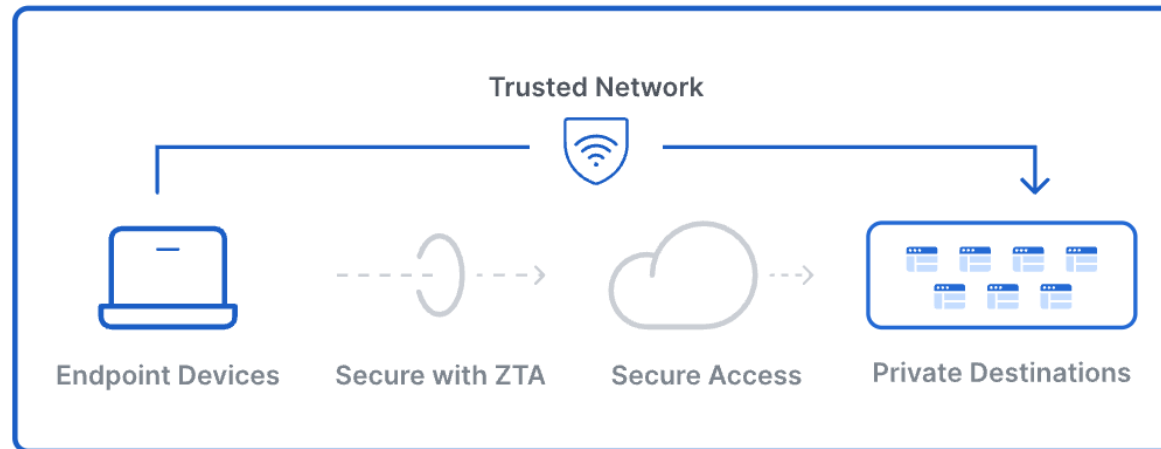
Summary

- All ports and protocols intercepted at the socket layer
- Same module used for Private Application interception
- Native Mobile Support for iOS and Android
- Client enrollment provides SAML auth for identity
- TPM is used for storing client certificate
- Posture coming soon

Trusted Network Detection

Trusted Network Detection

- **Improved** network **performance** and reduced latency provide a smoother user experience
- **Local** security **enforcement** in the trusted network offers flexible and optimized resource utilization
- End users can leverage the benefits **without** any **prompts** or actions
- **Independent** control of TND for **Private** access and **Internet** access provide admin flexibility to handle different operational and security concerns



TND Configuration

DNS Servers – Comma separated values of all DNS server addresses that a network interface may have when the client is in trusted network.

DNS Domains – Comma separated values of DNS suffixes that a network interface may have when the client is in trusted network.

Trusted Server – Add one or more servers on the network that will present a TLS certificate with a hash that matches the hash you provide

Certificate Public Key Hash – Certificate to check against configured web server

← Trusted Networks

Edit Trusted Networks

Include as many criteria as required to define a trusted network or network segment

[Help](#)

Trusted Network Name

Blizzard Demo

Multiple entries within each criterion are tested as OR: Any of the entered values can match.

Criterion

DNS Domains

DNS Domains ⓘ

cisco.com

— Remove Criterion

AND

Criterion

DNS Servers

DNS Servers ⓘ

72.113.47.11, 123.36.131.10

— Remove Criterion

AND

Criterion

Trusted Servers

Trusted Servers ⓘ

Certificate Hash ⓘ (optional)

1

https://demo.secureaccess.com

3c5239098eccc5d4eac29d038a

— Remove Criterion

Trusted Network Detection

Summary

- Options are **DNS Server**, **DNS domain**, **HTTPS Server**
 - Implicit **Or** when multiple options are configured
 - Virtual interfaces coming soon
- **Trusted Servers** configured in any TND profile are implicitly **excluded** from **ZTA interception**
- DNS Server and Domain are **supersets** of the **NIC configuration**
 - If NIC has multiple entries, **all** must be in a TND configuration
 - Each **NIC** is evaluated **independently**
- Secure Client version **5.1.10** and later

Complete your session evaluations



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



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events 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 Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: Insert preferred comms method

Thank you!

cisco Live !

