cisco Live!

Let’s go

The bridge to possible

Zero Trust Network Access (ZTNA) Demystified

What It Is, Why You Need It and the New Cisco Technologies That Make Frictionless Security Possible

Steven Chimes, Platform Security Architect
CCIE Security #35525

About Your Speaker

- Security Architect focused on global financials and global life sciences customers
- 15 years in industry including higher ed, manufacturing and 10 years at Cisco
- Author of CCNP Security Virtual Private Networks SVPN 300-730 Official Cert Guide

CISCO CERTIFIED CCIE SECURITY

CISCO CERTIFIED CCDP DESIGN

GIAC CERTIFIED INCIDENT HANDLER GCIH

GIAC CONTINUOUS MONITORING CERTIFICATION GMON

CISSP®

ISSAP®

Agenda

- Why ZTNA and it’s evolution
- ZTA w/ Cisco Secure Firewall
- ZTA w/ Cisco Secure Access

Not Covered: ISE, TrustSec or Duo

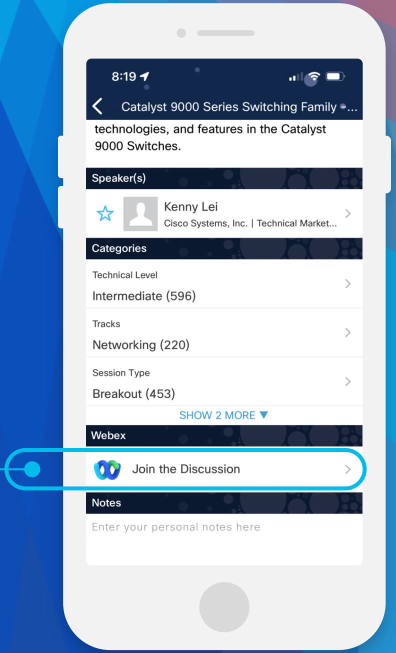
Webex App

Questions?

Use the Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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



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

Webex spaces will be moderated by the speaker until February 23, 2024.

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2079

Why ZTNA?

Why ZTNA?

49%

Employees are remote/hybrid users

53%

Remote/hybrid workers using DIA

55%

Traffic to/from off-premises, cloud-based facilities

This complexity + an increased ability of attackers to profit has made hypothetical attacks reality and pushed many organizations to the breaking point.

Reference: ESG SSE Survey, June 2023

ZTNA

Zero Trust Network Access

ZT

Zero Trust Principals

Applied To

NA

Network Access

Why ZTNA?

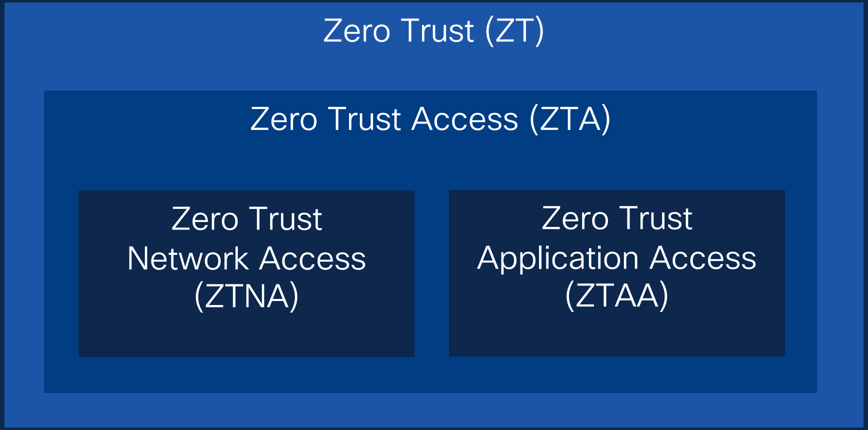
User Experience

SaaS Delivery

Zero Trust

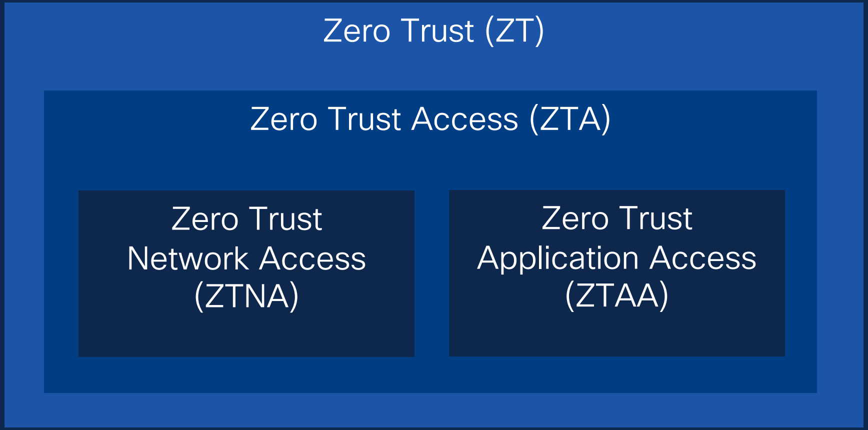
ZT vs. ZTA vs. ZTNA vs. ZTAA (Outcome View)

- 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


Zero Trust (ZT)
Zero Trust Access (ZTA)
Zero Trust Network Access (ZTNA)
Zero Trust Application Access (ZTAA)

ZT vs. ZTA vs. ZTNA vs. ZTAA (Outcome View)

- 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.


Zero Trust (ZT)
Zero Trust Access (ZTA)
Zero Trust Network Access (ZTNA)
Zero Trust Application Access (ZTAA)

ZTNA vs. ZTAA (Outcome View)

<table>
<tr><th></th><th>Zero Trust Network Access (ZTNA)</th><th>Zero Trust Application Access (ZTAA)</th></tr>
<tr><td>Allow Access To:</td><td>Corporate Network (10.0.0.0/8 or *.example.com)</td><td>Production Jira App (jira.example.com)</td></tr>
<tr><td rowspan="4">When:</td><td colspan="2">User Identity (Lee authenticated via MFA)</td></tr>
<tr><td colspan="2">Device Posture (Fully patched device)</td></tr>
<tr><td colspan="2">Location (United States)</td></tr>
<tr><td colspan="2">Continuous Monitoring (TLS decrypt and IPS inspection)</td></tr>
</table>

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

Types of Zero Trust Access

	Clientless	Client-based
General description	Lightweight method to securely access resources	More feature rich method to securely access resources
Application support	Web applications (HTTP/HTTPS) via a web browser and other select protocols (SMB/RDP/SSH/etc.) via a portal or small helper application	Broad range of applications via a software client
Partner/BYOD use	Preferred method	Yes, if desired/needed
Employee use	Yes, if desired	Preferred method

Cisco Secure Firewall Zero Trust Access (ZTA)

New Cisco Zero Trust Access Options

	Secure Firewall	Cisco Secure Access
Hosting	Hardware or VM	
Type	Clientless	
Client	Web Browser	
Supported Traffic	Client-to-server	
Supported Apps	HTTPS	
Client Protocol(s)	TLS	
Device Posture	None (Use Duo)	
Per-App Controls	TLS Decrypt, IPS, Anti-Malware	

Cisco Secure Firewall Zero Trust Access (ZTA)

Background

- Prior to Secure Firewall 7.4, organizations wanting to grant users access to private applications and implement zero trust were required to install additional software installed (like AnyConnect / Secure Client) on client devices.

What's New

- Clientless Zero Trust Access functionality added to Secure Firewall 7.4.
- SAML based authentication of users with support for Duo, Azure AD, Okta, & other Identity Providers.
- No additional network equipment needed. Simply upgrade to FTD v7.4.

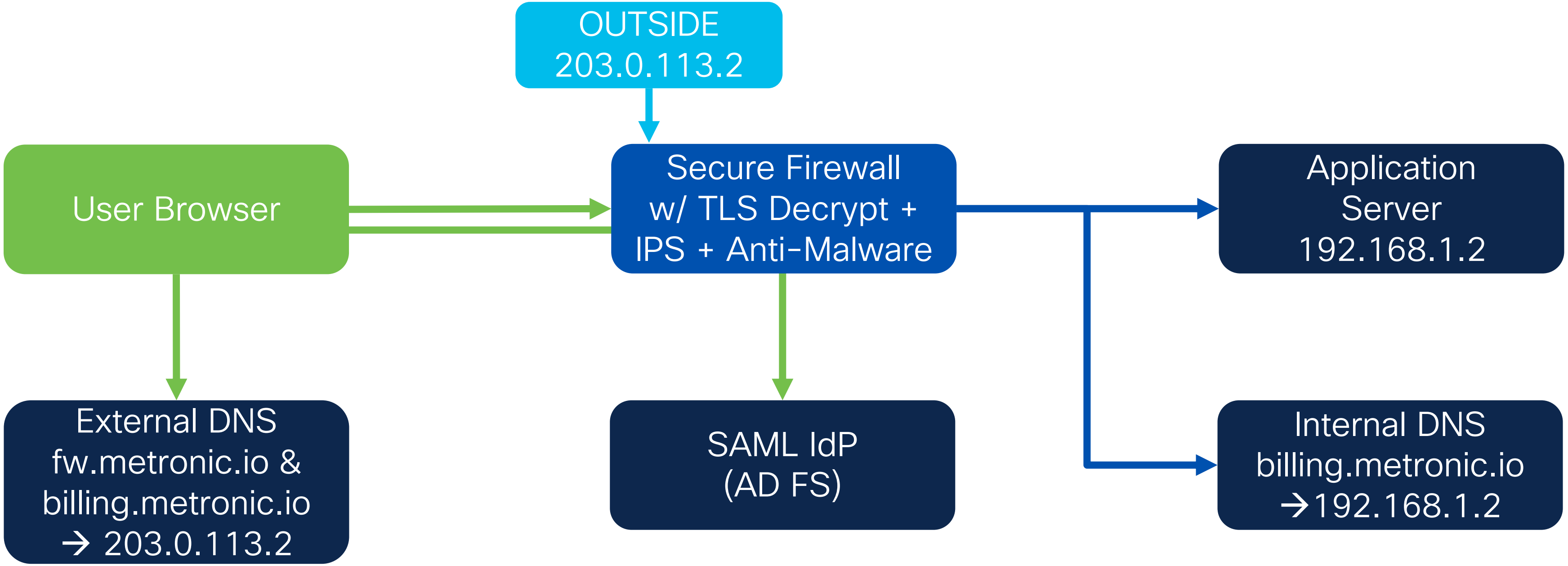
Benefits

- Enables users to access applications without requiring additional software on personal devices.

Requirements

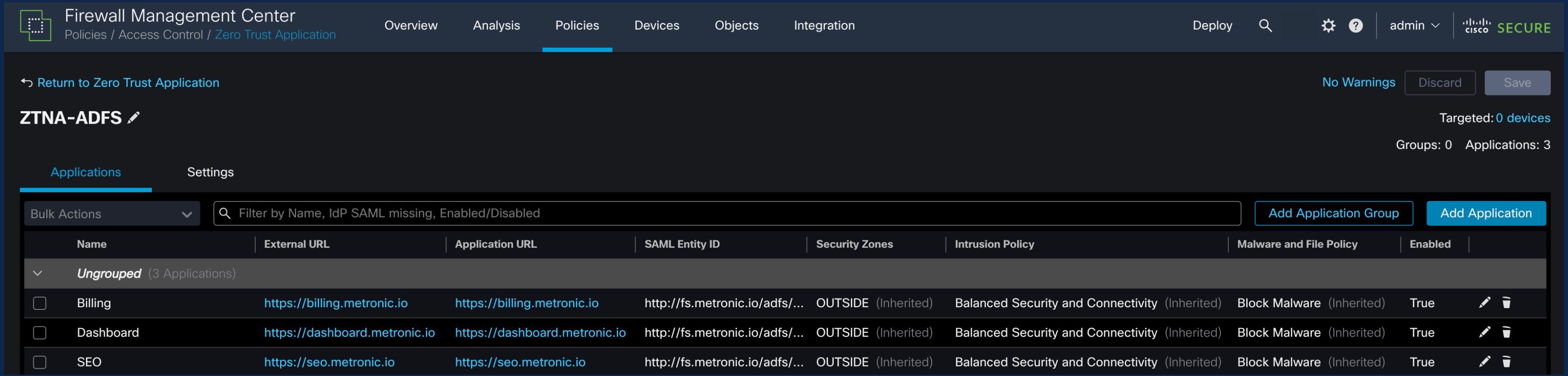
- Secure Firewall 7.4
- Snort 3
- FMC On Prem + FMC REST API or cdFMC
- Not supported on ASA
- Only Routed mode supported
- Not supported on individual mode cluster

Demo Setup: Secure Firewall ZTA w/ AD FS



Reference

Config: Secure Firewall ZTA w/ AD FS


Firewall Management Center
Policies / Access Control / Zero Trust Application
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
Return to Zero Trust Application
No Warnings
Discard
Save
Applications
Settings
Bulk Actions
Filter by Name, IdP SAML missing, Enabled/Disabled
Add Application Group
Add Application

ZTNA-ADFS

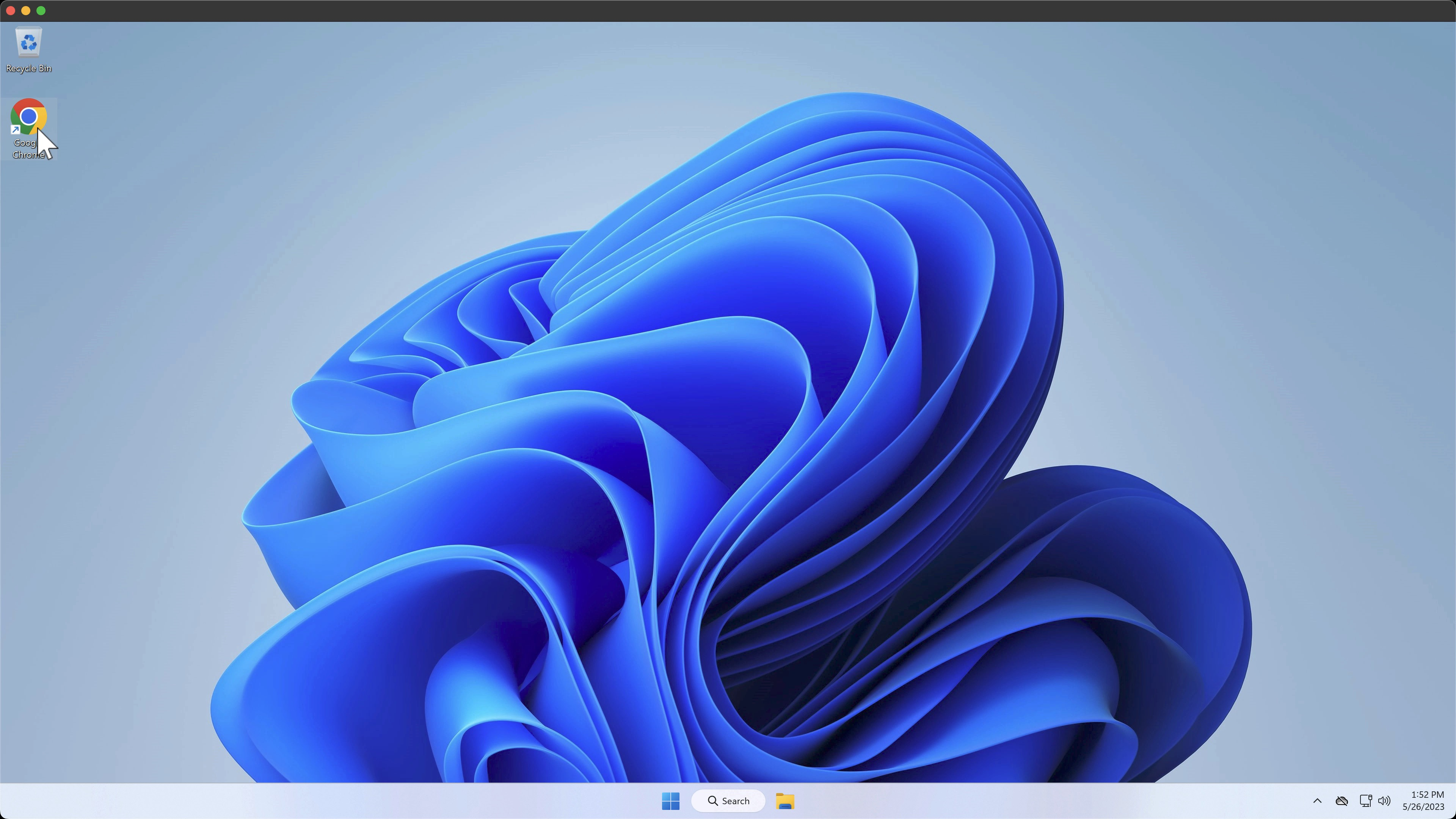
Targeted: 0 devices

Groups: 0 Applications: 3

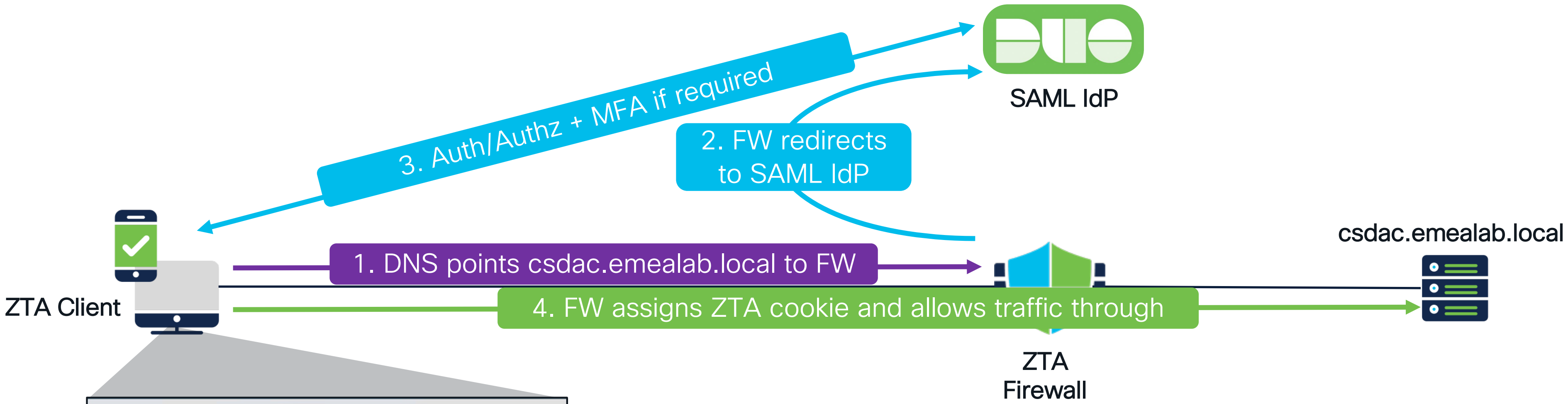
	Name	External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware and File Policy	Enabled
	Ungrouped (3 Applications)							
□	Billing	https://billing.metronic.io	https://billing.metronic.io	http://fs.metronic.io/adfs/...	OUTSIDE (Inherited)	Balanced Security and Connectivity (Inherited)	Block Malware (Inherited)	True
□	Dashboard	https://dashboard.metronic.io	https://dashboard.metronic.io	http://fs.metronic.io/adfs/...	OUTSIDE (Inherited)	Balanced Security and Connectivity (Inherited)	Block Malware (Inherited)	True
□	SEO	https://seo.metronic.io	https://seo.metronic.io	http://fs.metronic.io/adfs/...	OUTSIDE (Inherited)	Balanced Security and Connectivity (Inherited)	Block Malware (Inherited)	True

User Demo:

Cisco Secure Firewall ZTA + AD FS


Recycle Bin
Goog
Chrome
Search
1:52 PM
5/26/2023

Flow – Basic Flow

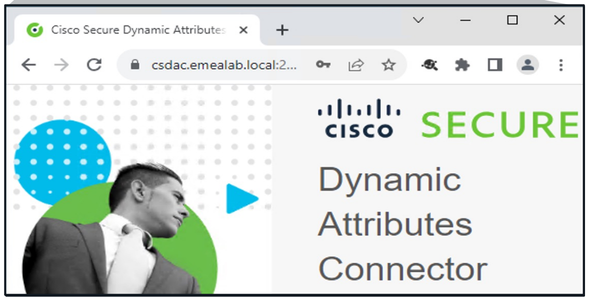


3. Auth/Authz + MFA if required

2. FW redirects to SAML IdP

1. DNS points csdac.emealab.local to FW

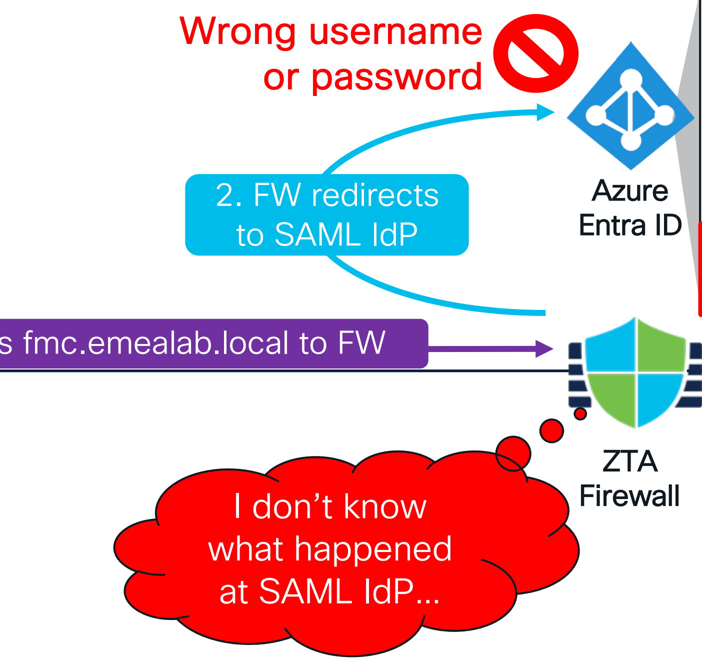
4. FW assigns ZTA cookie and allows traffic through

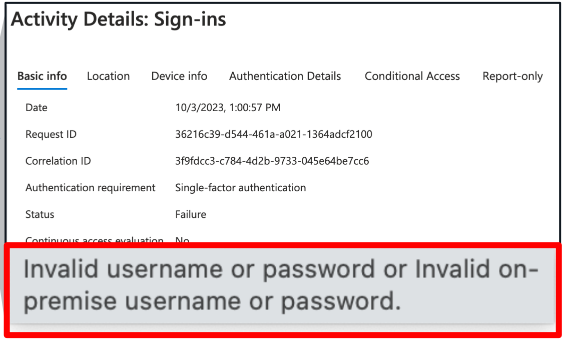


- HTTPs (Pre-Auth)
- SAML IdP AAA
- ZTA Protected Flow

Thank you to Chris Grabowski for saving me a ton of time building these ZTA Firewall slides

Flow – Failed Authentication

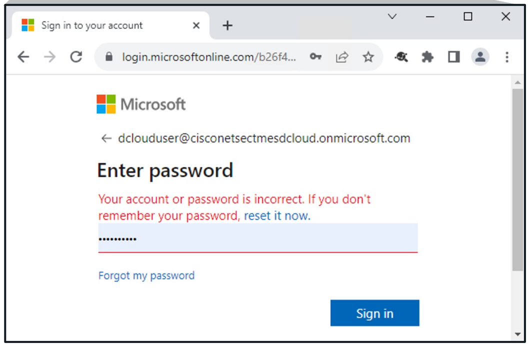

Wrong username or password
2. FW redirects to SAML IdP
Azure Entra ID
1. DNS points fmc.emealab.local to FW
ZTA Client
ZTA Firewall
I don't know what happened at SAML IdP...



Activity Details: Sign-ins

Date	10/3/2023, 1:00:57 PM
Request ID	36216c39-d544-461a-a021-1364adcf2100
Correlation ID	3f9fdcc3-c784-4d2b-9733-045e64be7cc6
Authentication requirement	Single-factor authentication
Status	Failure
Continuous access evaluation	No

Invalid username or password or Invalid on-premise username or password.



← dcloudusre@cisconetsectmesdcloud.onmicrosoft.com

Enter password

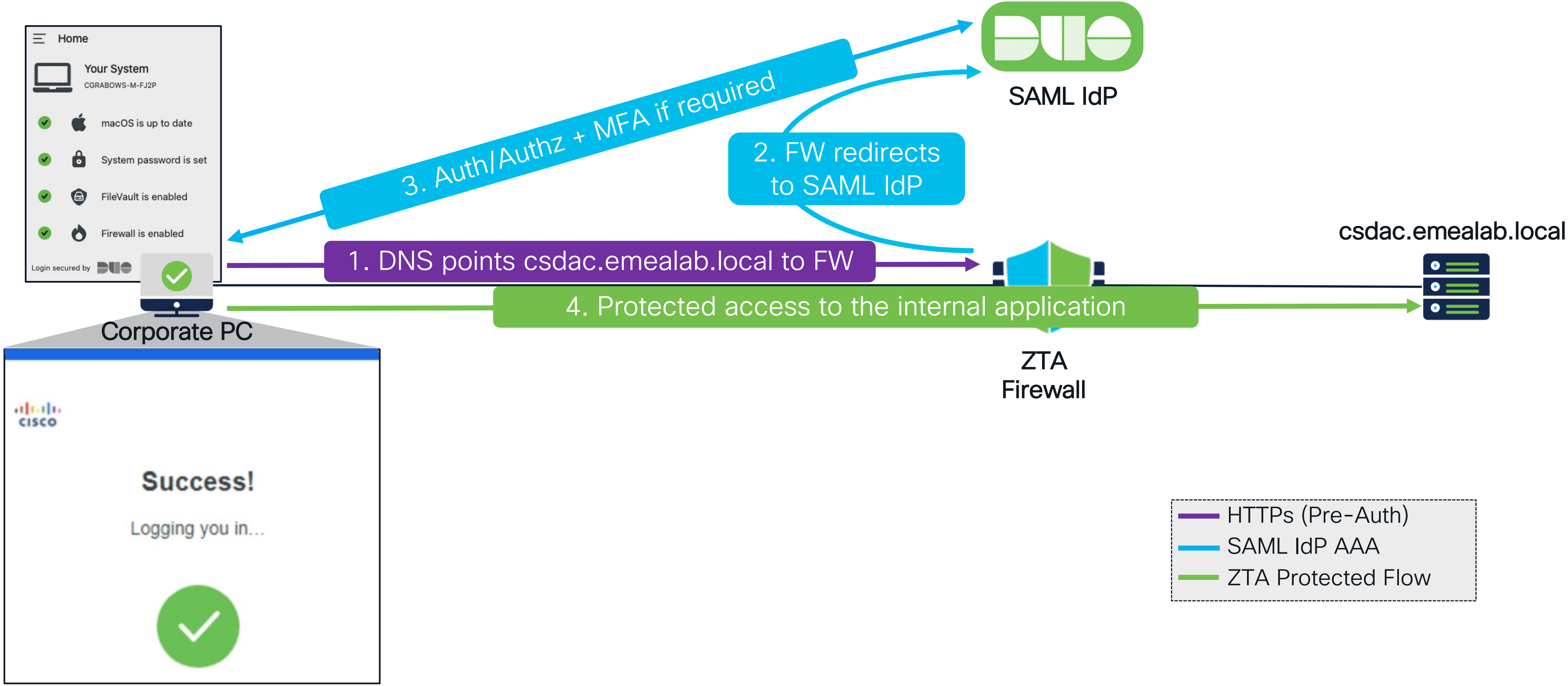
Your account or password is incorrect. If you don't remember your password, reset it now.

••••••••••

Forgot my password

🟪 HTTPs (Pre-Auth)
🟦 SAML IdP AAA
🟩 ZTA Protected Flow

Flow – Compliant Endpoint



Home

Your System
CGRABOWS-M-FJ2P

✓ macOS is up to date

✓ System password is set

✓ FileVault is enabled

✓ Firewall is enabled

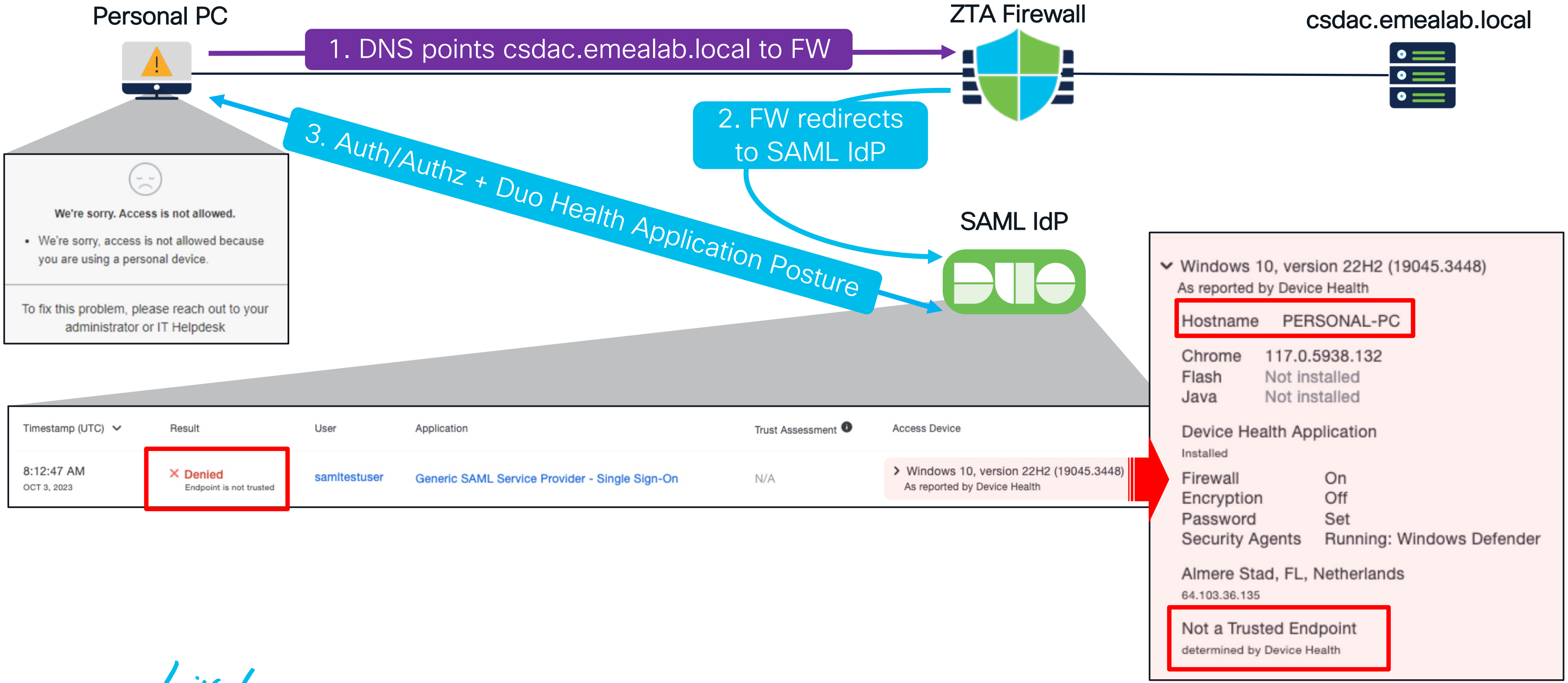
Login secured by DUO

Success!

Logging you in...

SAML IdP
3. Auth/Authz + MFA if required
2. FW redirects to SAML IdP
csdac.emealab.local
1. DNS points csdac.emealab.local to FW
4. Protected access to the internal application
Corporate PC
ZTA Firewall
cisco
HTTPs (Pre-Auth)
SAML IdP AAA
ZTA Protected Flow

Flow – Non-Compliant Endpoint



Personal PC
ZTA Firewall
csdac.emealab.local
1. DNS points csdac.emealab.local to FW
2. FW redirects to SAML IdP
3. Auth/Authz + Duo Health Application Posture
SAML IdP

We're sorry. Access is not allowed.

- We're sorry, access is not allowed because you are using a personal device.

To fix this problem, please reach out to your administrator or IT Helpdesk

Timestamp (UTC)	Result	User	Application	Trust Assessment	Access Device
8:12:47 AM OCT 3, 2023	✕ Denied Endpoint is not trusted	samltestuser	Generic SAML Service Provider - Single Sign-On	N/A	Windows 10, version 22H2 (19045.3448) As reported by Device Health

Windows 10, version 22H2 (19045.3448)
As reported by Device Health

Hostname	PERSONAL-PC
Chrome	117.0.5938.132
Flash	Not installed
Java	Not installed

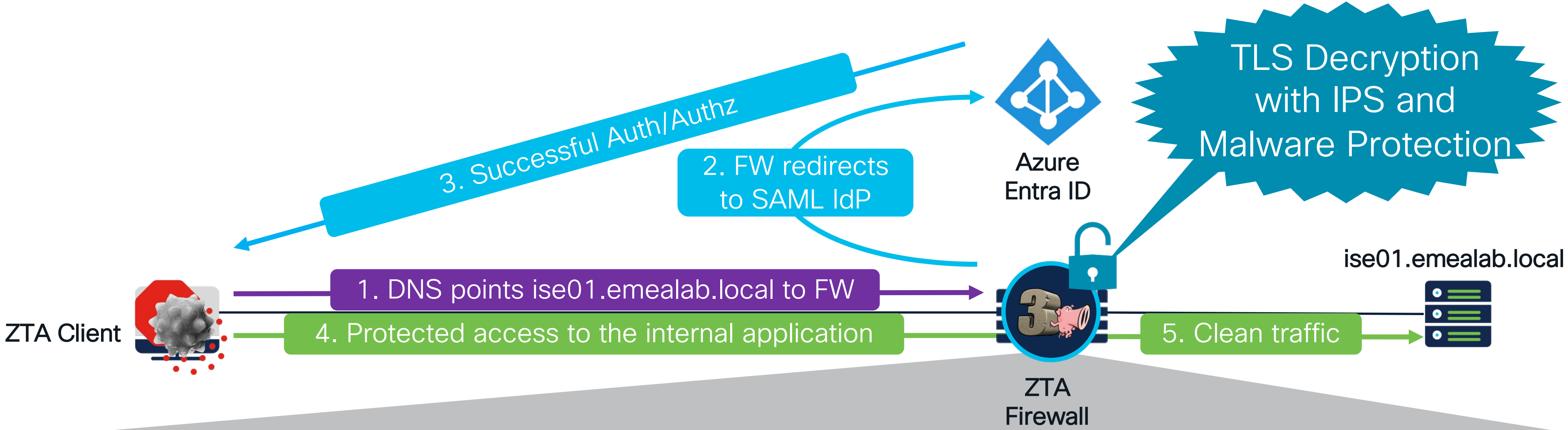
Device Health Application
Installed

Firewall	On
Encryption	Off
Password	Set
Security Agents	Running: Windows Defender

Almere Stad, FL, Netherlands
64.103.36.135

Not a Trusted Endpoint
determined by Device Health

Flow – Successful Auth/Authz w/ Inspection



1. DNS points ise01.emealab.local to FW

2. FW redirects to SAML IdP

3. Successful Auth/Authz

4. Protected access to the internal application

5. Clean traffic

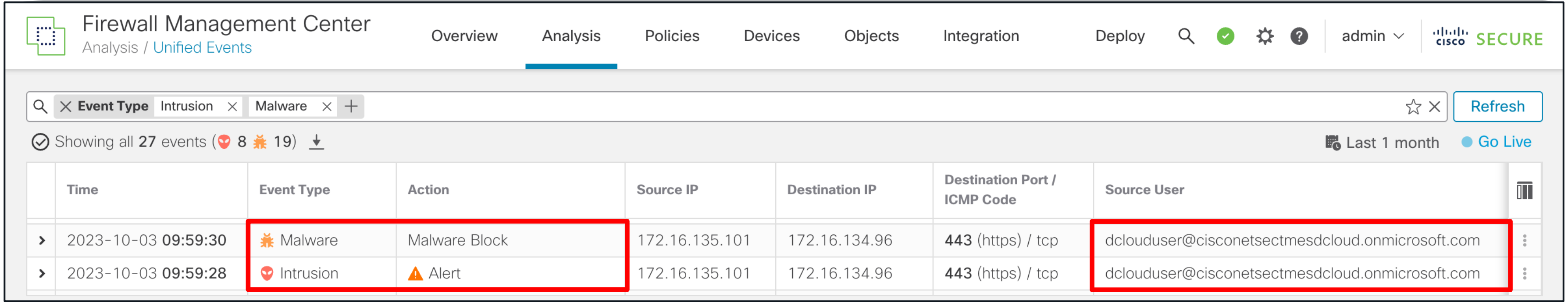
TLS Decryption with IPS and Malware Protection

ZTA Client

Azure Entra ID

ZTA Firewall

ise01.emealab.local



Firewall Management Center
Analysis / Unified Events

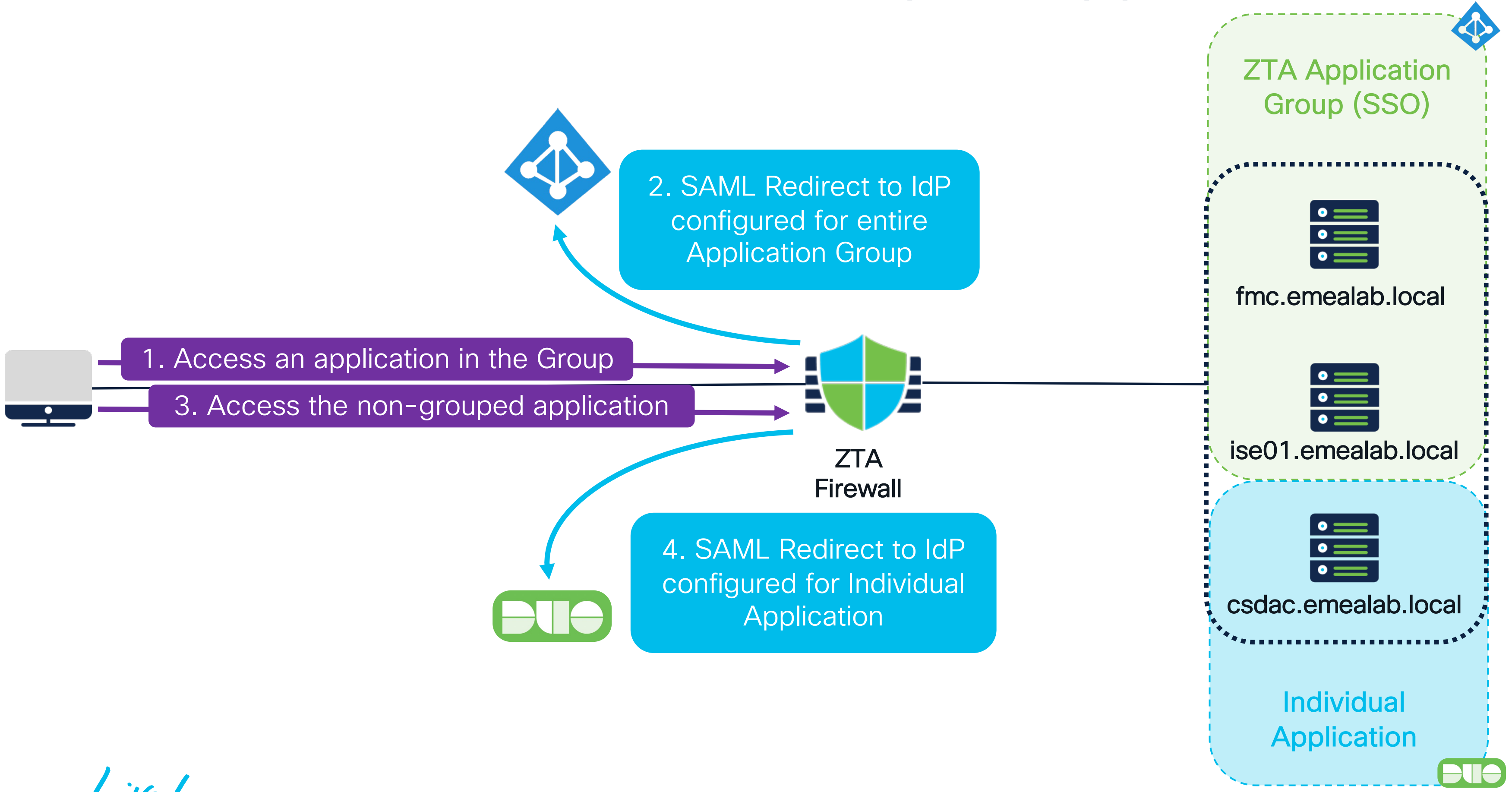
Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin | cisco SECURE

Event Type: Intrusion, Malware | Refresh

Showing all 27 events (8 19) | Last 1 month | Go Live

	Time	Event Type	Action	Source IP	Destination IP	Destination Port / ICMP Code	Source User
›	2023-10-03 **09:59:30**	Malware	Malware Block	172.16.135.101	172.16.134.96	**443** (https) / tcp	dclouduser@cisconetsectmesdcloud.onmicrosoft.com
›	2023-10-03 **09:59:28**	Intrusion	⚠ Alert	172.16.135.101	172.16.134.96	**443** (https) / tcp	dclouduser@cisconetsectmesdcloud.onmicrosoft.com

Flow – ZTA Individual vs. Grouped Applications



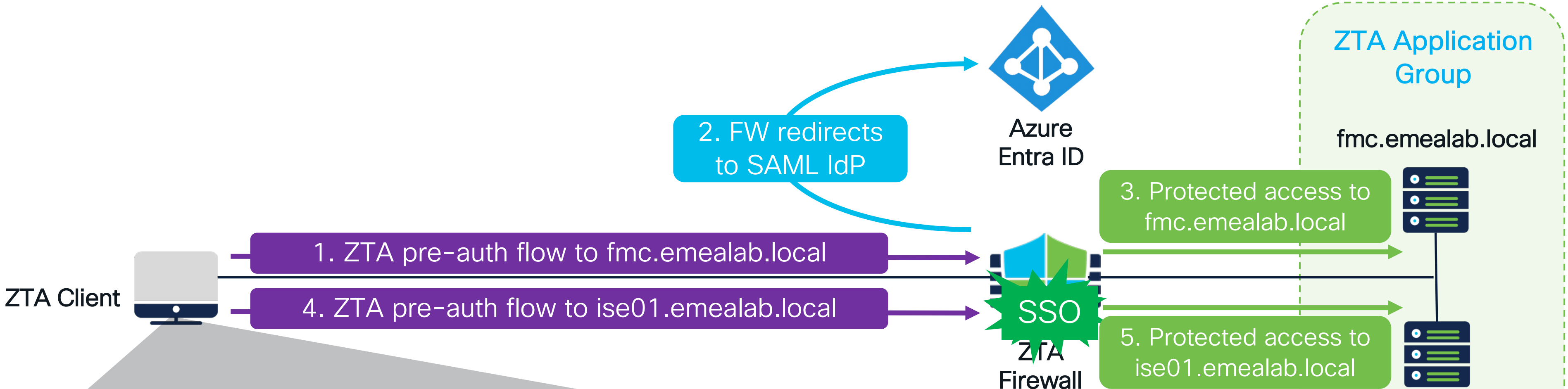
1. Access an application in the Group

2. SAML Redirect to IdP configured for entire Application Group

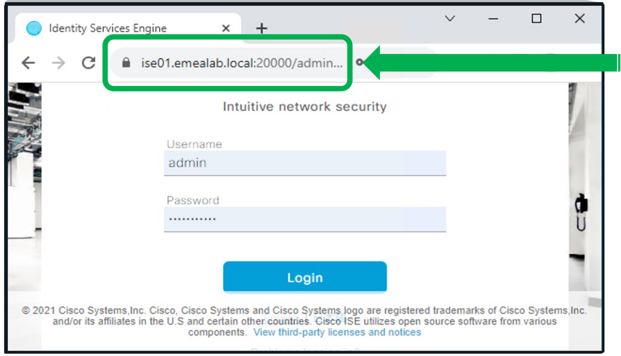
3. Access the non-grouped application

4. SAML Redirect to IdP configured for Individual Application

Flow – Grouped Applications



ZTA Application Group
fmc.emealab.local
Azure Entra ID
2. FW redirects to SAML IdP
3. Protected access to fmc.emealab.local
1. ZTA pre-auth flow to fmc.emealab.local
ZTA Client
4. ZTA pre-auth flow to ise01.emealab.local
SSO
ZTA Firewall
5. Protected access to ise01.emealab.local
ise01.emealab.local



ise01.emealab.local:20000/admin...

Intuitive network security

Username
admin

Password
···········

© 2021 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc. and/or its affiliates in the U.S and certain other countries. Cisco ISE utilizes open source software from various components. View third-party licenses and notices

Access another application in the ZTA Application Group

- ▬ HTTPs (Pre-Auth)
- ▬ SAML IdP AAA
- ▬ ZTA Protected Flow

Recommendations

- Only SAML IdPs are supported e.g. Azure AD, Duo, Ping ID, One Login, Okta
- DNS needs to be configured to direct application traffic to the ZTA firewall's interface.
- ZTA application protection supported for Internet and internal access use-case (with proper DNS configuration)
- ZTA is supported on routed mode in HA/Cluster*/Multi-Instance deployments
- License requirements:
  - Essentials license for basic ZTA access
  - IPS and/or Malware Defense for application traffic inspection
  - ZTA does not work in evaluation mode
- ZTA traffic is not subjected to Access Control Policy (ZTA policy takes precedence)

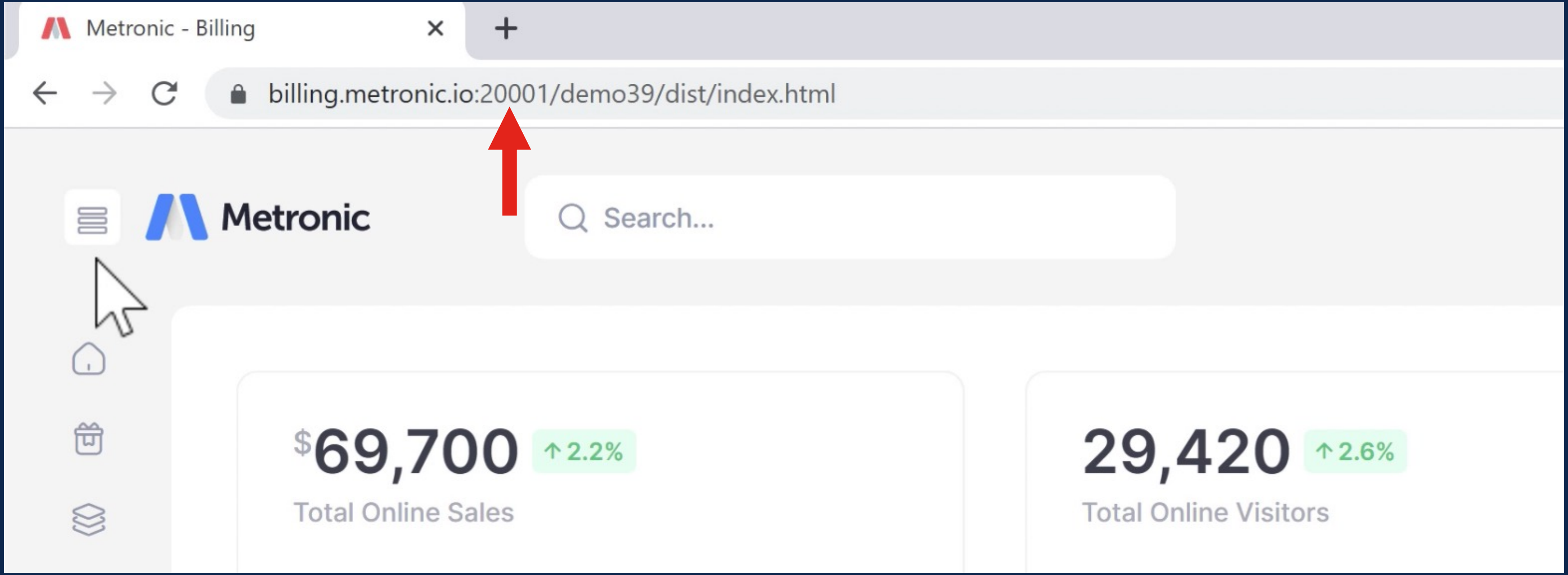
* Not supported on individual mode cluster

Recommendations

- Supports HTTPs applications only (HTTP, RDP, SSH not supported)
- ZTA supports interactive web applications (requires user SAML login)
- ZTA is not a reverse-proxy:
  - Firewall does not rewrite HTTP requests
  - The flow is based on HTTP redirects
  - TLS decryption is mandatory – Snort validates ZTA HTTP cookie in the HTTP request
- ZTA will not work for non-HTTP traffic tunneled through TCP 443 interface.
- A pre-auth certificate matching FQDNs of protected applications is required
- Not supported if protected application redirects between ports or does strict HTTP Host Header validation

Note the port at the end of the FQDN

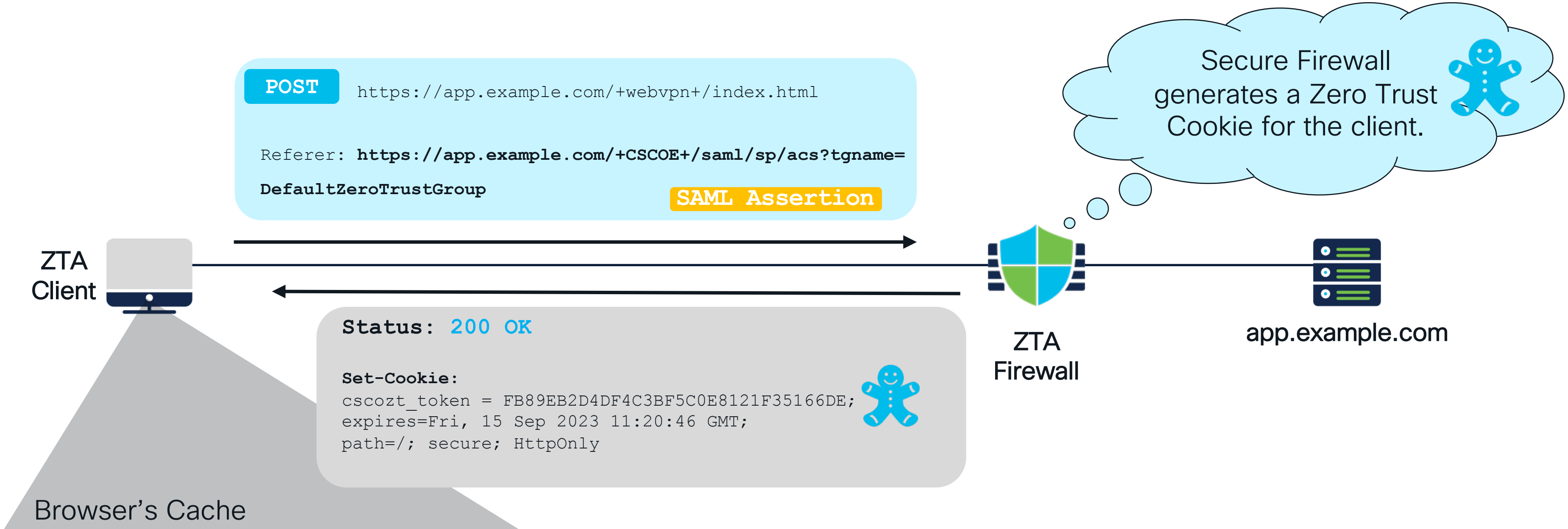
Secure Firewall redirects to a FQDN with a high port (20,000+) for each app



Metronic - Billing

billing.metronic.io:20001/demo39/dist/index.html

SAML Assertion Consumption and Setting Application Cookie



```
POST  https://app.example.com/+webvpn+/index.html

Referer: https://app.example.com/+CSCOE+/saml/sp/acs?tgname=
DefaultZeroTrustGroup                          SAML Assertion
```

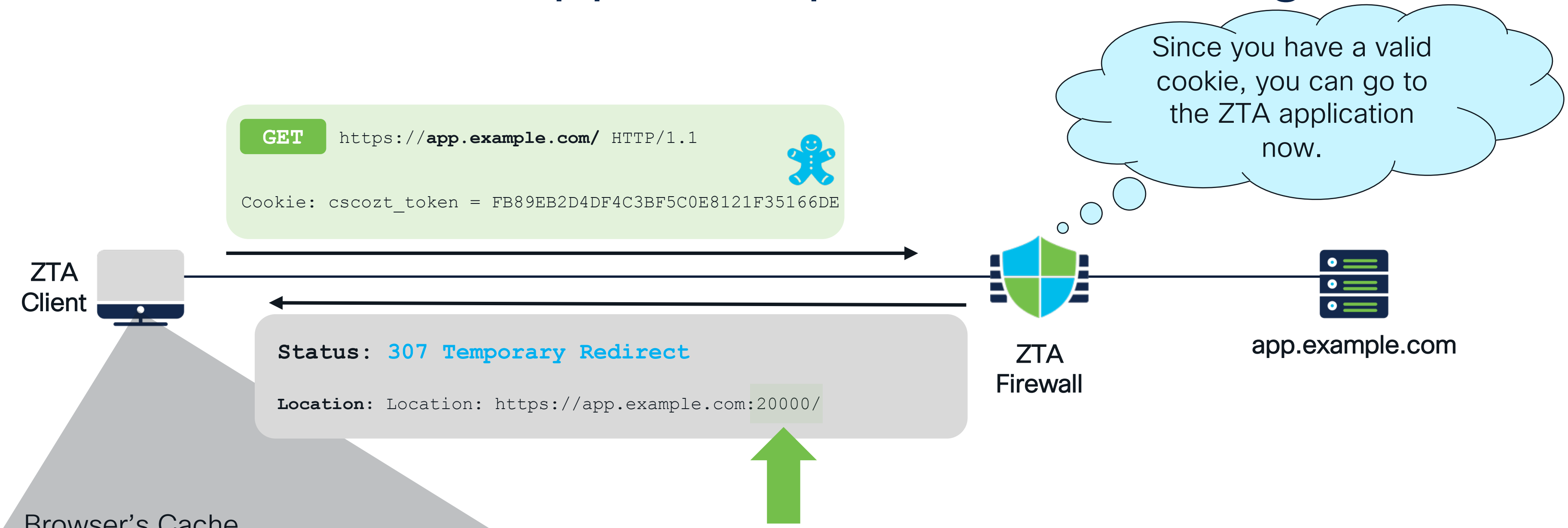
```
Status: 200 OK

Set-Cookie:
cscozt_token = FB89EB2D4DF4C3BF5C0E8121F35166DE;
expires=Fri, 15 Sep 2023 11:20:46 GMT;
path=/; secure; HttpOnly
```

Secure Firewall generates a Zero Trust Cookie for the client.

Browser's Cache

Cookie	Domain	Path	Lifetime
🍪	app.example.com	/	1 day

Redirect to ZTA app.example.com NAT High Port

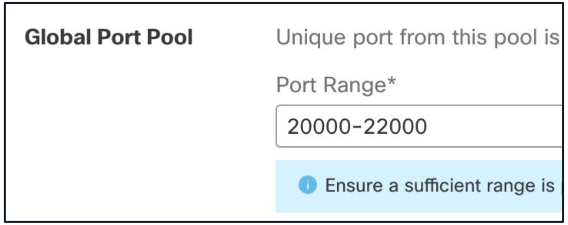

ZTA Client
ZTA Firewall
app.example.com
Since you have a valid cookie, you can go to the ZTA application now.

```
GET https://app.example.com/ HTTP/1.1

Cookie: cscozt_token = FB89EB2D4DF4C3BF5C0E8121F35166DE
```

```
Status: 307 Temporary Redirect

Location: Location: https://app.example.com:20000/
```

Browser's Cache

Cookie	Domain	Path	Lifetime
🍪	app.example.com	/	1 day



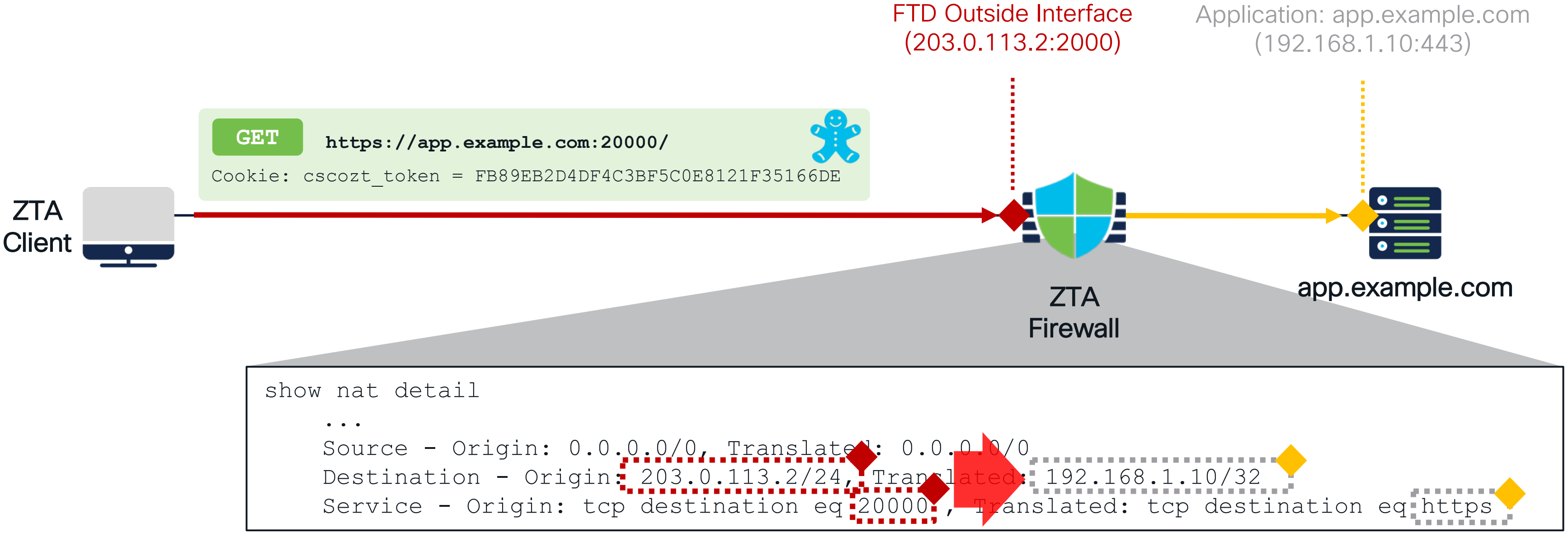
Global Port Pool Unique port from this pool is

Port Range*

20000-22000

ⓘ Ensure a sufficient range is

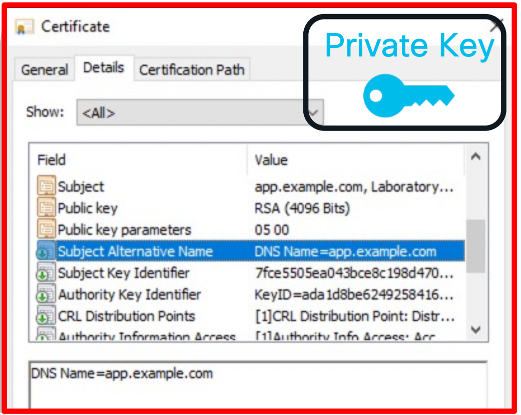
ZTA app.example.com NAT Construct



```
GET https://app.example.com:20000/
Cookie: cscozt_token = FB89EB2D4DF4C3BF5C0E8121F35166DE
```

```
show nat detail
    ...
    Source - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
    Destination - Origin: 203.0.113.2/24, Translated: 192.168.1.10/32
    Service - Origin: tcp destination eq 20000 , Translated: tcp destination eq https
```

TLS Decryption of the ZTA Flow

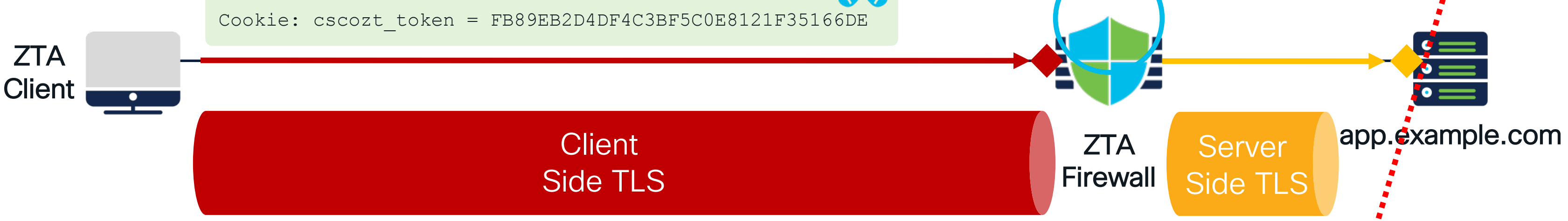


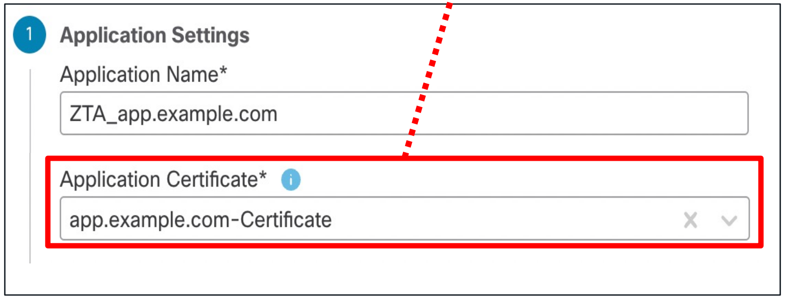
Show: <All>

Field	Value
Subject	app.example.com, Laboratory...
Public key	RSA (4096 Bits)
Public key parameters	05 00
Subject Alternative Name	DNS Name=app.example.com
Subject Key Identifier	7fce5505ea043bce8c198d470...
Authority Key Identifier	KeyID=ada1d8be6249258416...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc

DNS Name=app.example.com

```
GET https://app.example.com:20000/
Cookie: cscozt_token = FB89EB2D4DF4C3BF5C0E8121F35166DE
```



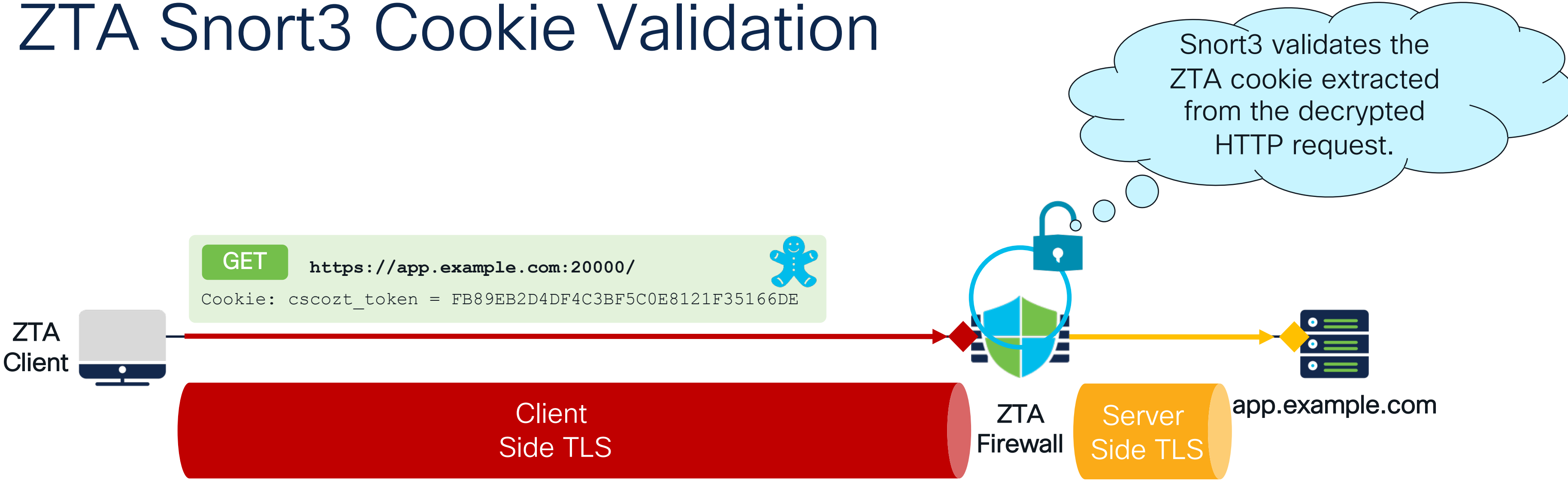


1 Application Settings

Application Name*: ZTA_app.example.com

Application Certificate*: app.example.com-Certificate

ZTA Snort3 Cookie Validation

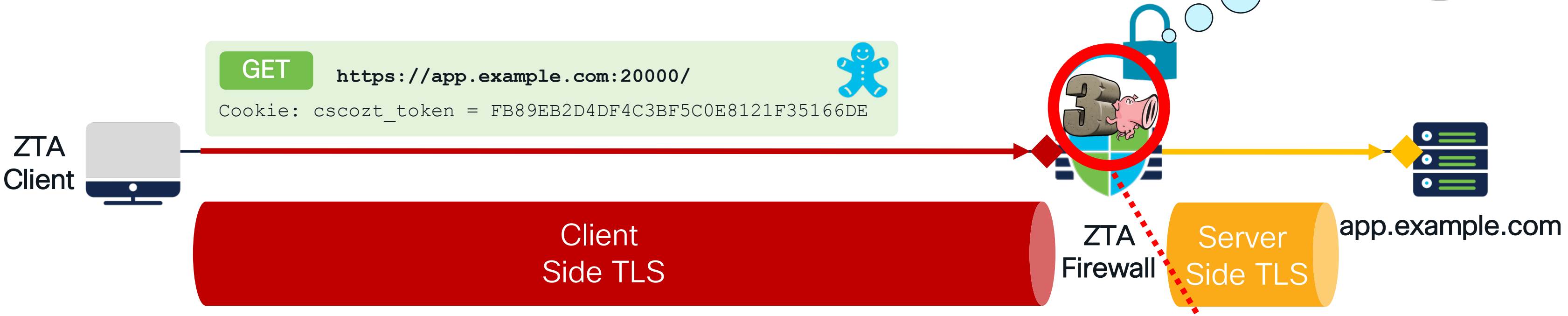


Snort3 validates the ZTA cookie extracted from the decrypted HTTP request.

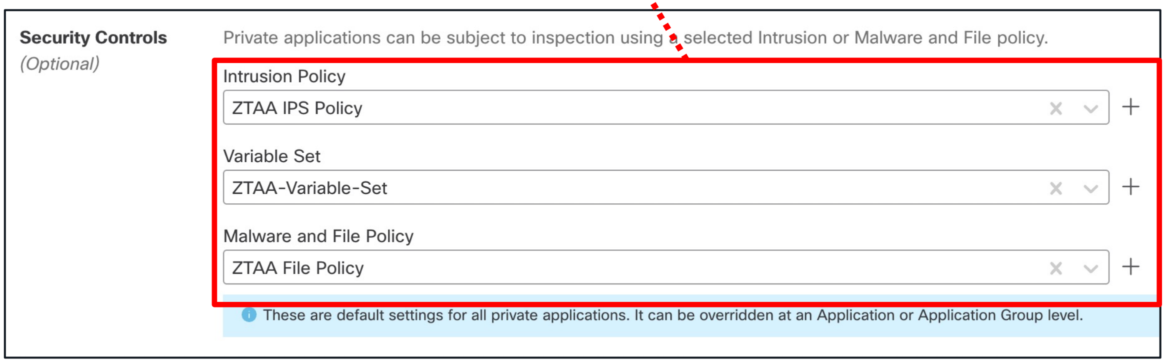
```
GET https://app.example.com:20000/
Cookie: cscozt_token = FB89EB2D4DF4C3BF5C0E8121F35166DE
```

IPS and Malware Protection

All ZTA protected application traffic is protected with IPS and/or Malware Defense policies.



```
GET https://app.example.com:20000/
Cookie: cscozt_token = FB89EB2D4DF4C3BF5C0E8121F35166DE
```



Security Controls *(Optional)*

Private applications can be subject to inspection using a selected Intrusion or Malware and File policy.

Intrusion Policy: ZTAA IPS Policy

Variable Set: ZTAA-Variable-Set

Malware and File Policy: ZTAA File Policy

These are default settings for all private applications. It can be overridden at an Application or Application Group level.

Cisco Secure Access

New Cisco Zero Trust Access Options

	Secure Firewall	Cisco Secure Access		
Hosting	Hardware or VM	SaaS		
Type	Clientless	Clientless	Client-Based	
Client	Web Browser	Web Browser	ZTA Module OS Native Clients	VPN Module
Supported Traffic	Client-to-server	Client-to-server	Client-to-server	Client-to-server, Client-to-client, Server-to-client
Supported Apps	HTTPS	HTTP, HTTPS	TCP & UDP	TCP, UDP & ICMP
Client Protocol(s)	TLS	TLS	MASQUE over QUIC or TLS	TLS, DTLS, IPSec
Device Posture	None (Use Duo)	Per-Rule	Per-Rule	On Connect
Per-App Controls	TLS Decrypt, IPS, Anti-Malware	User/Group-Based Access Control, TLS Decrypt, IPS		

Cisco Secure Access

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

Core SSE

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB) and DLP
- Zero Trust Access (ZTA)
- Firewall as a Service (FWaaS) and IPS

+

Cisco delivers the core and more in a single subscription...

- DNS Security
- Multimode DLP
- Advanced Malware protection
- Sandbox
- Talos Threat Intelligence
- VPN as a Service
- Digital Experience Monitoring*
- Remote Browser Isolation*

Add-on solutions

- SD-WAN
- XDR
- Duo MFA/ SSO
- CSPM

* Included in the unified experience / separate license (optional)

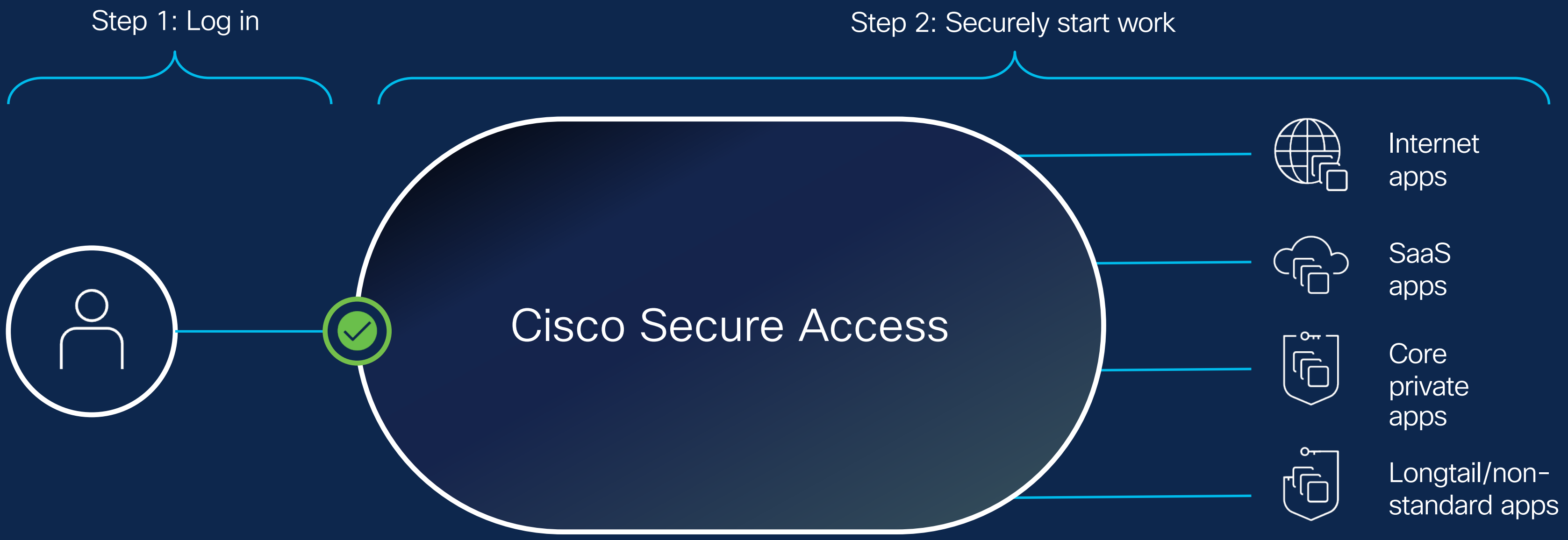
Cisco Secure Access

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

Core SSE

Zero Trust Access (ZTA)

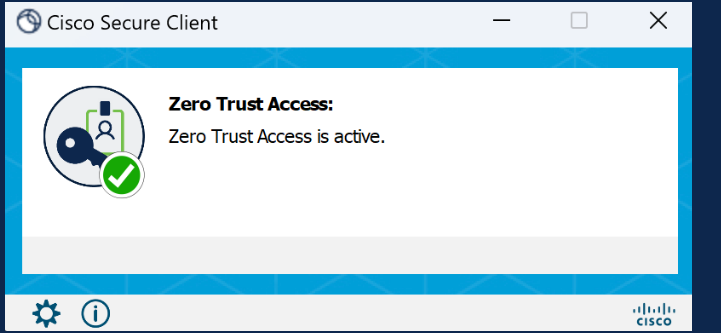
Easy, frictionless user experience



User Demo:

Cisco Secure Access
+ Client-Based Zero Trust Access

Cisco Secure Client Zero Trust Access Module



Cisco Secure Client

Zero Trust Access:

Zero Trust Access is active.

Zero Trust Access module in
Cisco Secure Client 5.1 (formerly AnyConnect)

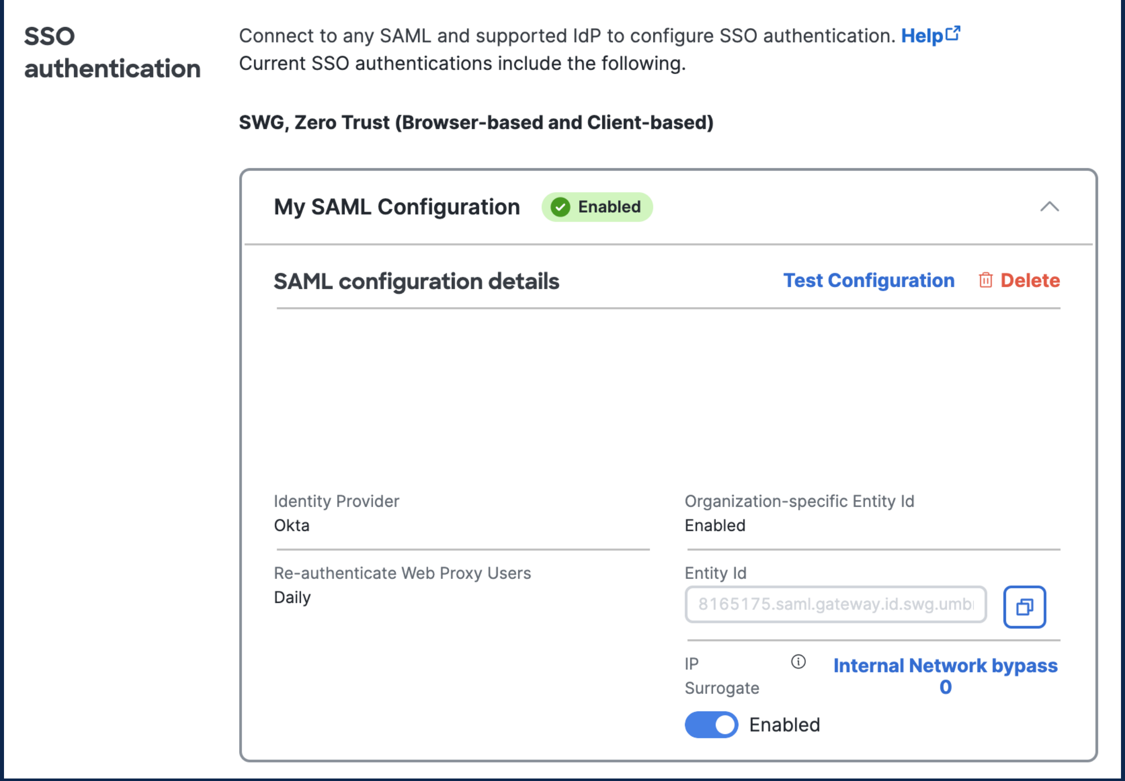
- Transparent user experience
- Forward proxied resource access with coarse-grained or fine-grained access control
- Service managed client certificates with TPM-protected key storage
- Support for TCP and UDP applications
- Cisco and third-party VPN client interop
- Next-generation protocol (MASQUE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

Why Is It Called Zero Trust Access (ZTA) Instead of Zero Trust Network Access (ZTNA)?

	ZTNA	ZTA
Multifactor Authentication	✓	✓
Device posture checks	✓	✓
Micro-segmentation	✓	✓
Complete separation between the user and the enterprise network	✗	✓
Next-generation protocols	✗	✓
Native OS support	✗	✓
Flexible backend connectivity options	✗	✓
Hardware protected credentials	✗	✓

Rule Basics: User Authentication & MFA via SAML

Use Duo or any IdP that supports SAML to strongly authenticate users



SSO authentication

Connect to any SAML and supported IdP to configure SSO authentication. **Help**
Current SSO authentications include the following.

SWG, Zero Trust (Browser-based and Client-based)

My SAML Configuration ✓ Enabled

SAML configuration details **Test Configuration** **Delete**

Identity Provider
Okta

Organization-specific Entity Id
Enabled

Re-authenticate Web Proxy Users
Daily

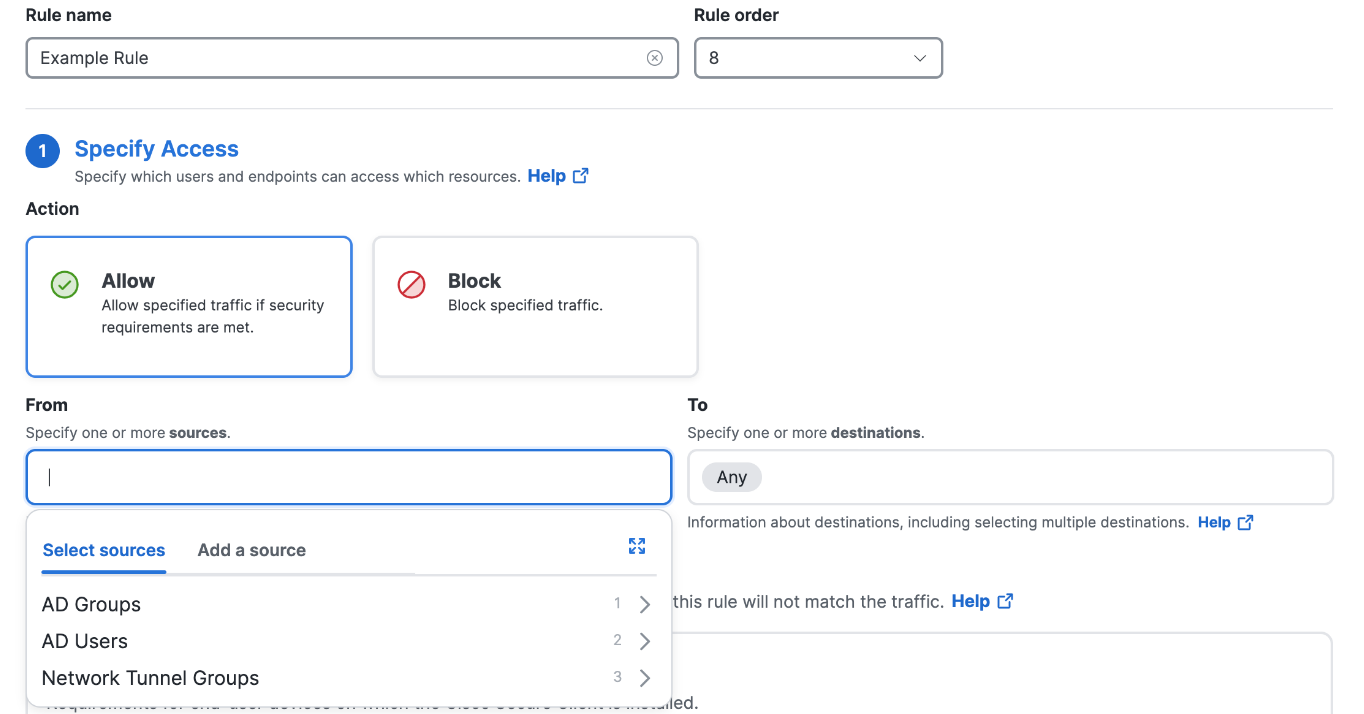
Entity Id
8165175.saml.gateway.id.swg.umb

IP Surrogate
Enabled

Internal Network bypass
0

Rule Basics: Write Policy Based on User or Group

Using user and group info loaded From Active Directory or via SCIM



Rule name: Example Rule

Rule order: 8

1 **Specify Access**

Specify which users and endpoints can access which resources. Help

Action

- ● **Allow** Allow specified traffic if security requirements are met.
- ○ **Block** Block specified traffic.

From

Specify one or more **sources**.

To

Specify one or more **destinations**.

Any

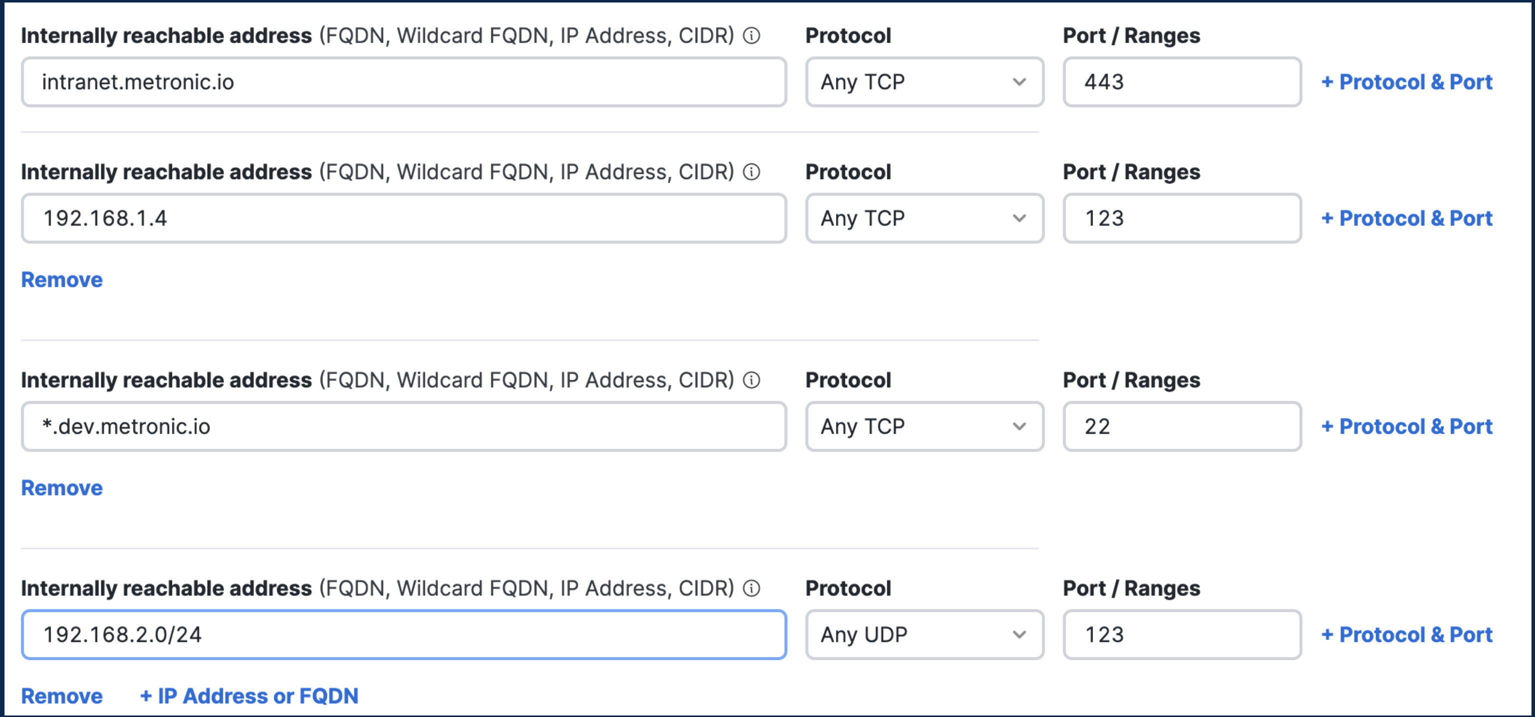
Information about destinations, including selecting multiple destinations. Help

this rule will not match the traffic. Help

Requirements for end-user devices on which the Cisco Secure Client is installed.

Rule Basics: Define Private Resources / Apps

Based on IP, FQDN, protocol and port



Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR) ⓘ	Protocol	Port / Ranges	
intranet.metronic.io	Any TCP	443	+ Protocol & Port

Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR) ⓘ	Protocol	Port / Ranges	
192.168.1.4	Any TCP	123	+ Protocol & Port

Remove

Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR) ⓘ	Protocol	Port / Ranges	
*.dev.metronic.io	Any TCP	22	+ Protocol & Port

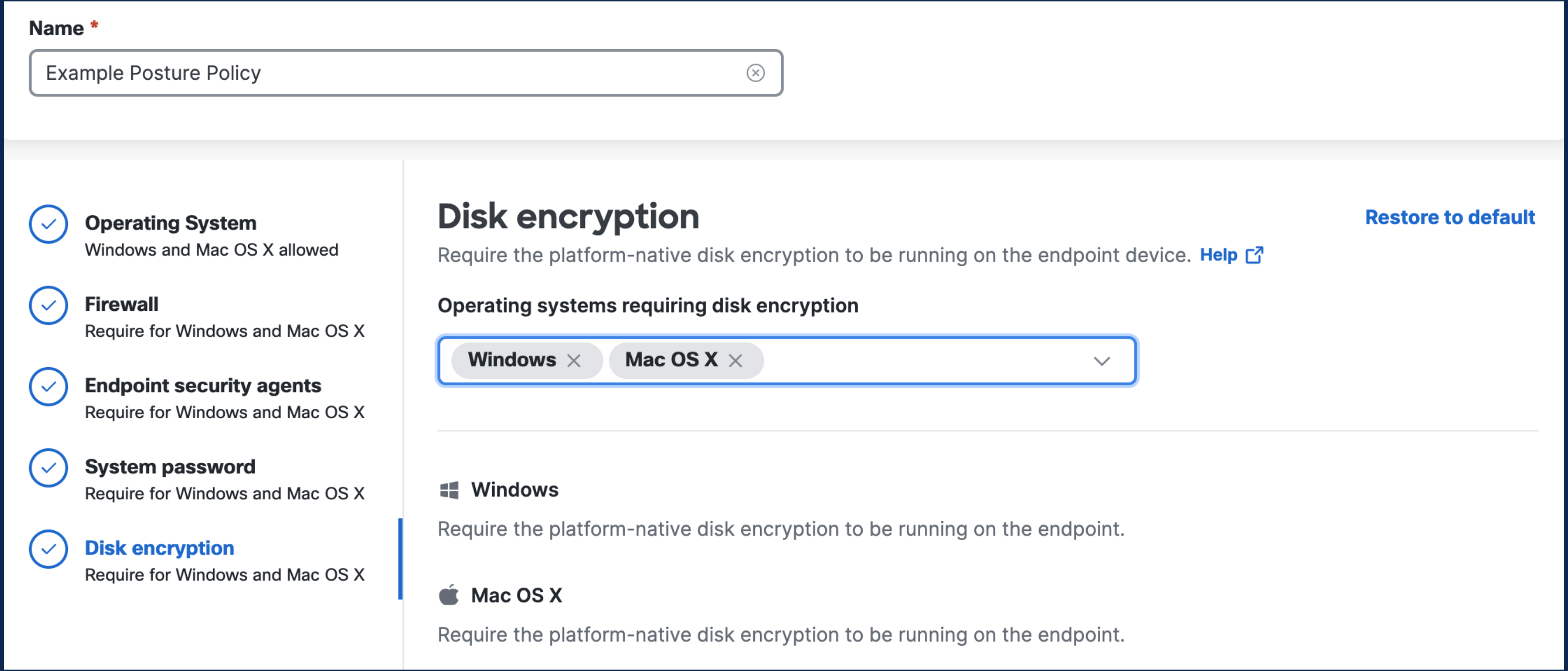
Remove

Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR) ⓘ	Protocol	Port / Ranges	
192.168.2.0/24	Any UDP	123	+ Protocol & Port

Remove + IP Address or FQDN

Rule Basics: Define and Enforce Device Posture

Posture can be enforced globally or at the rule level



Name *

Example Posture Policy

- ✓ **Operating System**
  Windows and Mac OS X allowed
- ✓ **Firewall**
  Require for Windows and Mac OS X
- ✓ **Endpoint security agents**
  Require for Windows and Mac OS X
- ✓ **System password**
  Require for Windows and Mac OS X
- ✓ **Disk encryption**
  Require for Windows and Mac OS X

Disk encryption

Restore to default

Require the platform-native disk encryption to be running on the endpoint device. Help

Operating systems requiring disk encryption

Windows × Mac OS X ×

Windows

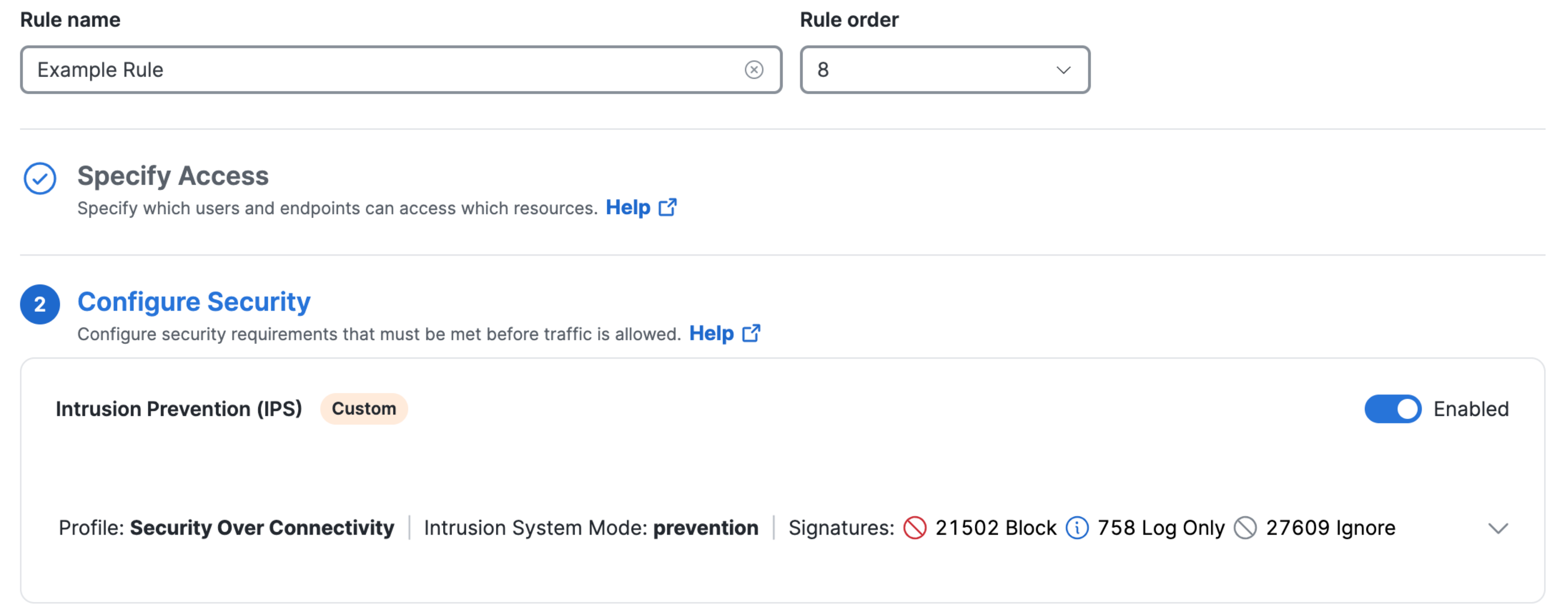
Require the platform-native disk encryption to be running on the endpoint.

Mac OS X

Require the platform-native disk encryption to be running on the endpoint.

Rule Basics: Apply TLS Decrypt and IPS

Traffic security settings can be applied globally or at a rule level



Rule name

Example Rule

Rule order

8

Specify Access

Specify which users and endpoints can access which resources. **Help**

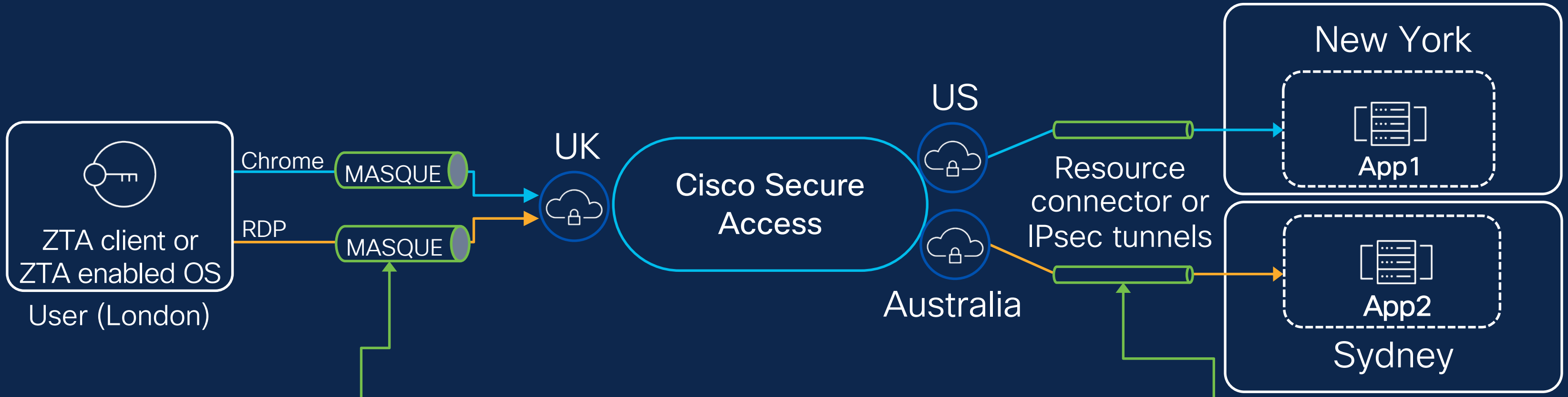
2 **Configure Security**

Configure security requirements that must be met before traffic is allowed. **Help**

Intrusion Prevention (IPS) Custom — Enabled

Profile: **Security Over Connectivity** | Intrusion System Mode: **prevention** | Signatures: 21502 Block 758 Log Only 27609 Ignore

High-Level Traffic Flow for Zero Trust Access



- ‘No click’ seamless access
- Advanced protocols reduce latency and speed content delivery

- Full separation between users and the enterprise network
- Fast deployment with no firewall setting changes

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.
  - A more technically accurate acronym would be MASQUOTE (Multiplexed Application Substrate over QUIC or TLS Encryption) as MASQUE can operate over QUIC or TLS (e.g. if QUIC is blocked).

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 Use QUIC as the Protocol?

- Less framing overhead
- 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)

Note: Not all features of QUIC as a protocol are currently used by Cisco Secure Access

Why Use MASQUE?

No direct resource access (Proxy architecture)

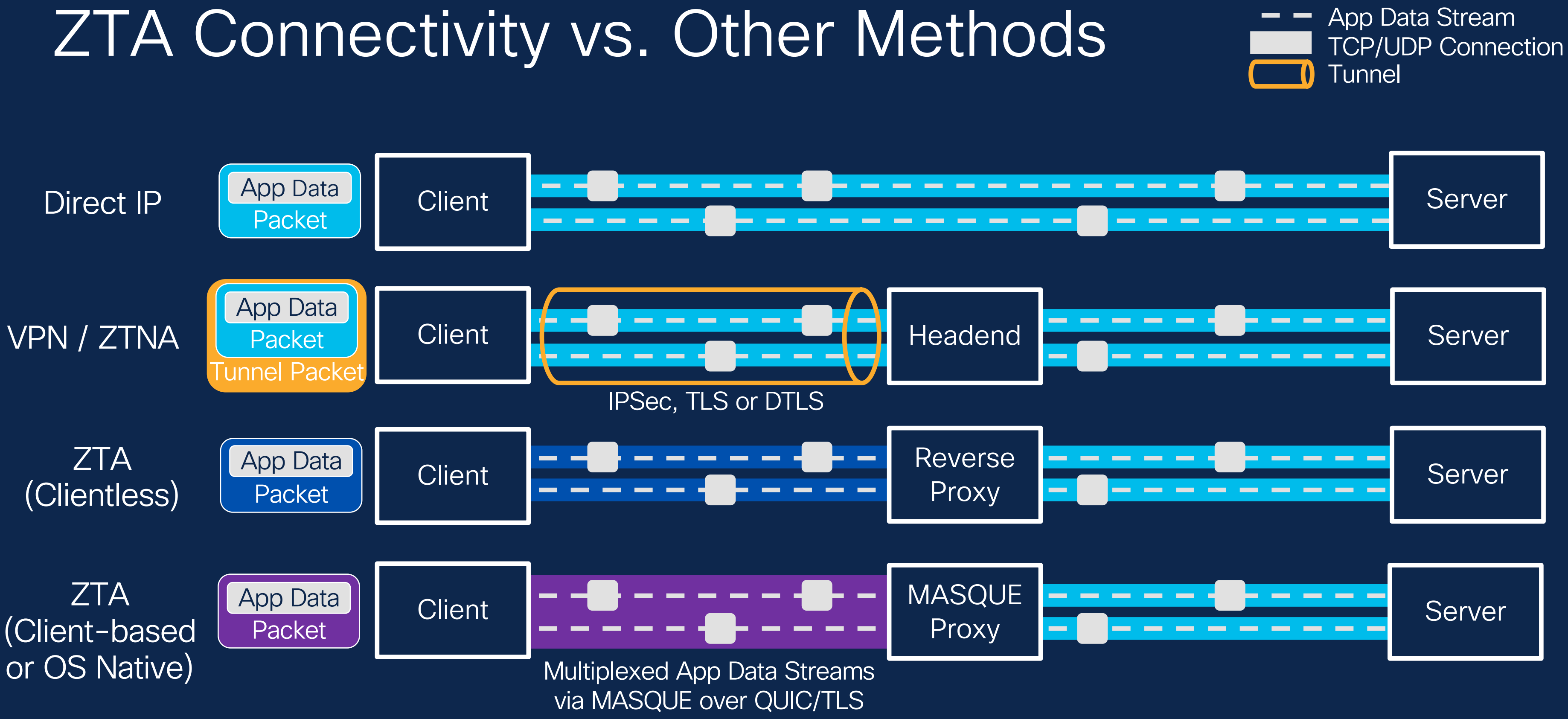
Broad application support (TCP and UDP)

Fallback to HTTP/2 (TCP 443) if QUIC (UDP 443) is blocked

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

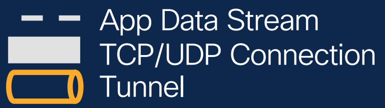
Native OS support

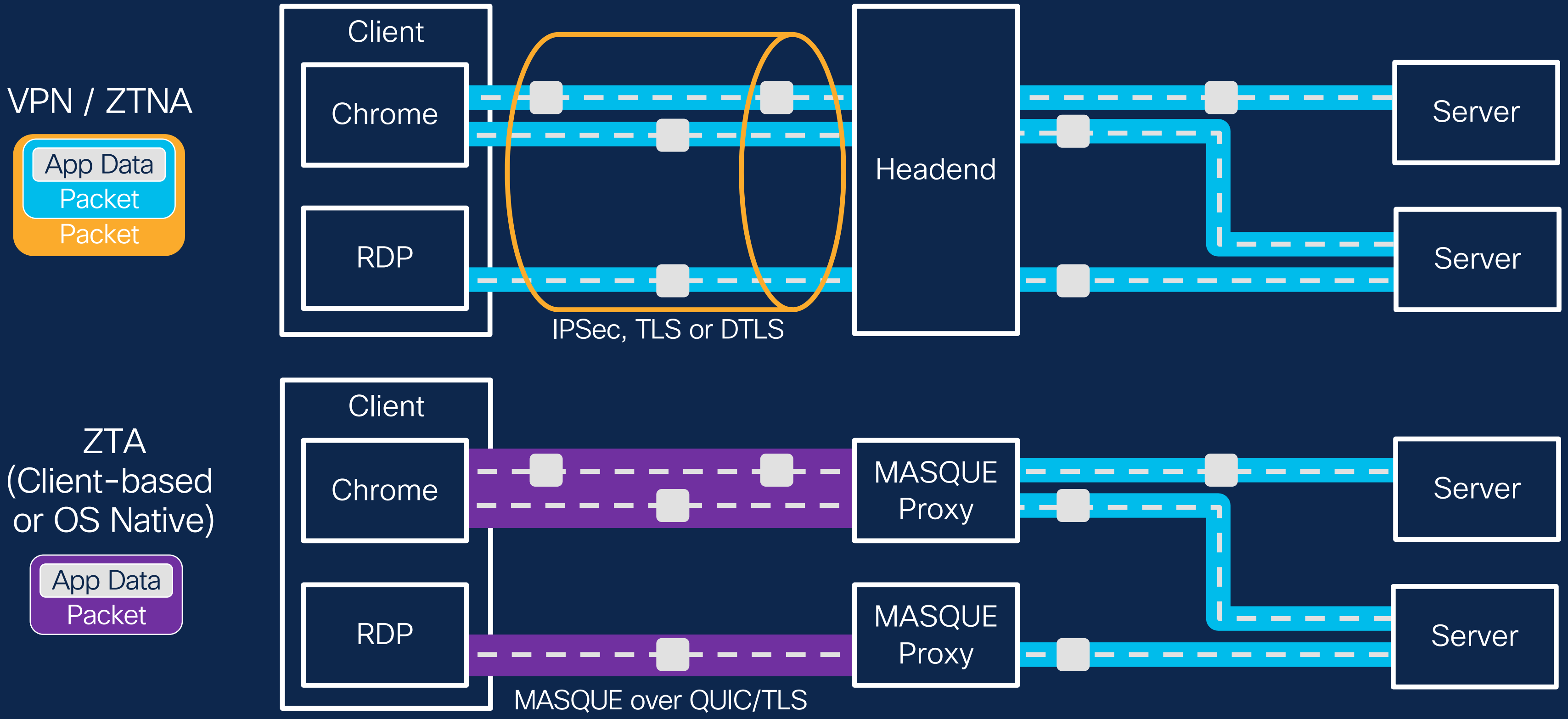
ZTA Connectivity vs. Other Methods



ZTA eliminates the overhead of VPN tunnels and improves security with full separation between users and the enterprise network

ZTA Connectivity vs. Other Methods

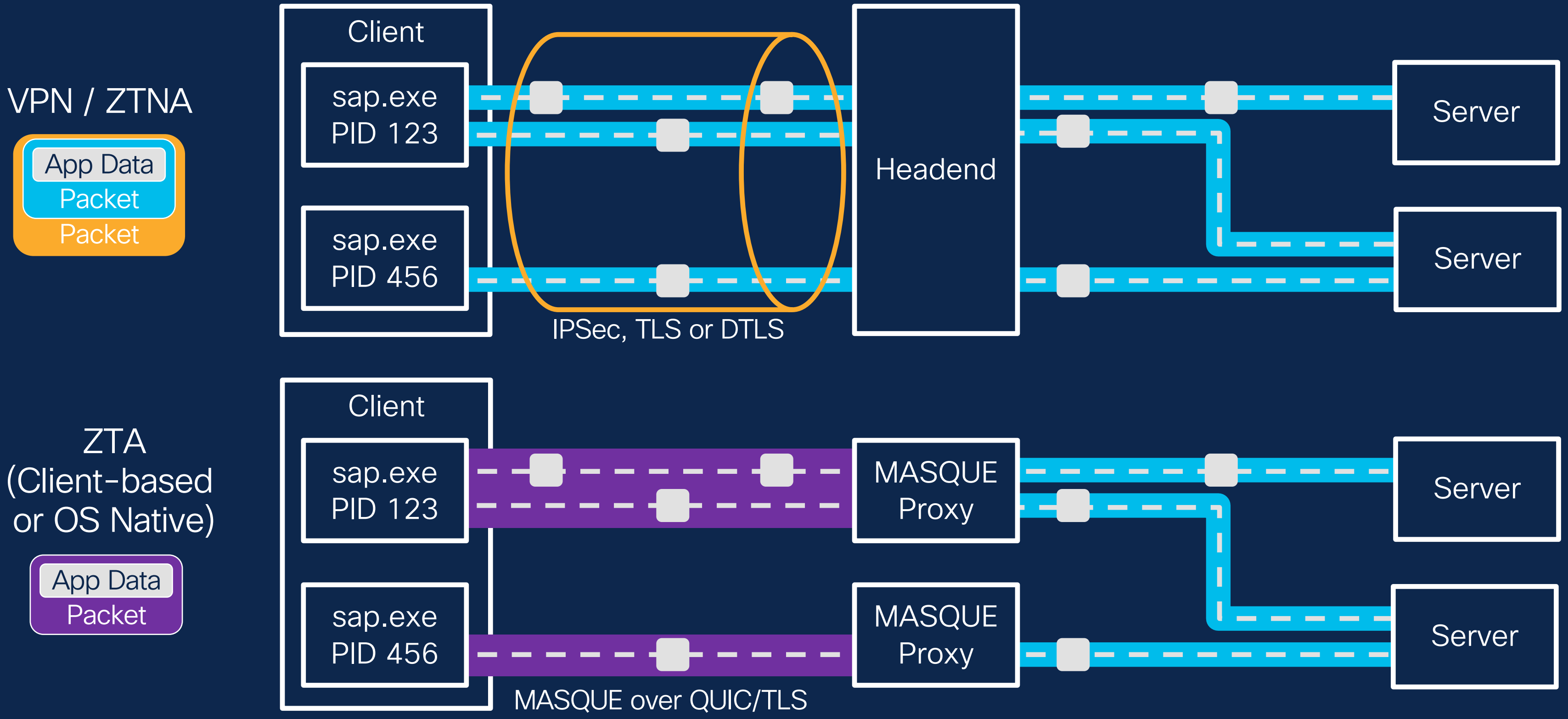




With ZTA, each process uses a unique MASQUE connection, even if the data streams are destined to different servers

ZTA Connectivity vs. Other Methods

App Data Stream
TCP/UDP Connection
Tunnel



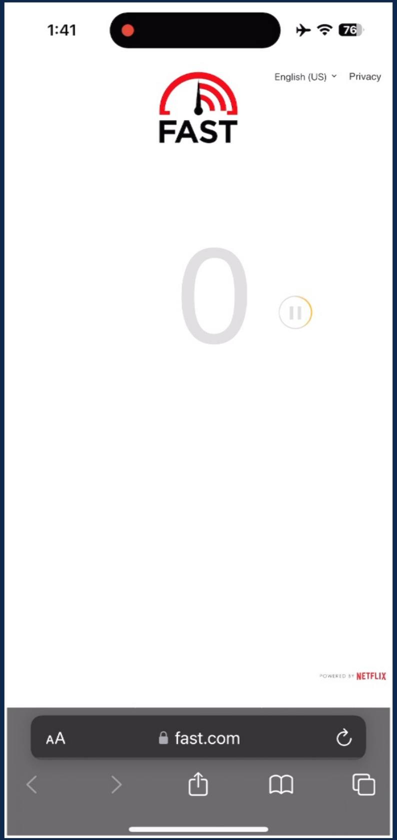
With ZTA, each process uses a unique MASQUE connection, even if the data streams are destined to different servers

Connectivity is sometimes really bad…

…but the user experience doesn’t have to be

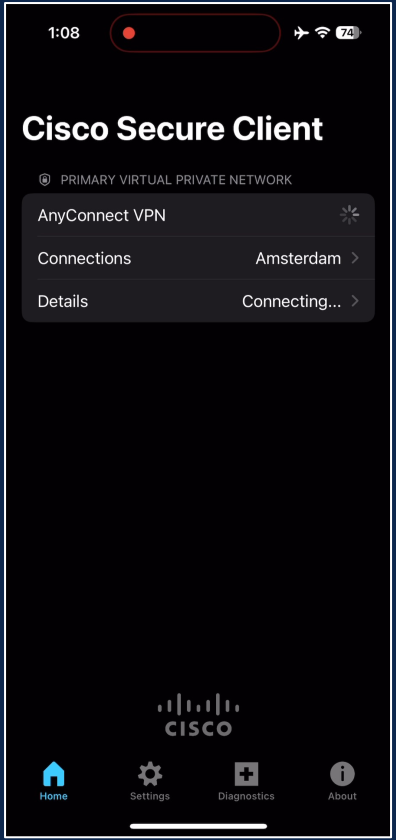
User Demo:

OS Native Zero Trust Access on iOS vs. VPN on Extremely Slow Airplane Wi-Fi



fast.com Speedtest

Connectivity was bad...



Cisco Secure Client

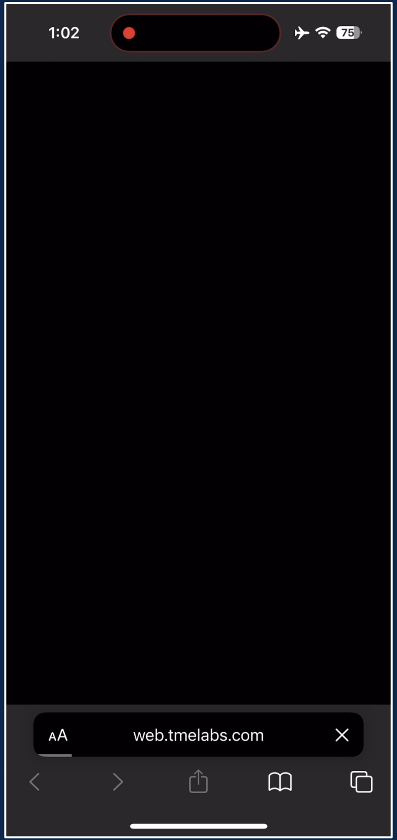
PRIMARY VIRTUAL PRIVATE NETWORK

AnyConnect VPN

Connections Amsterdam

Details Connecting...

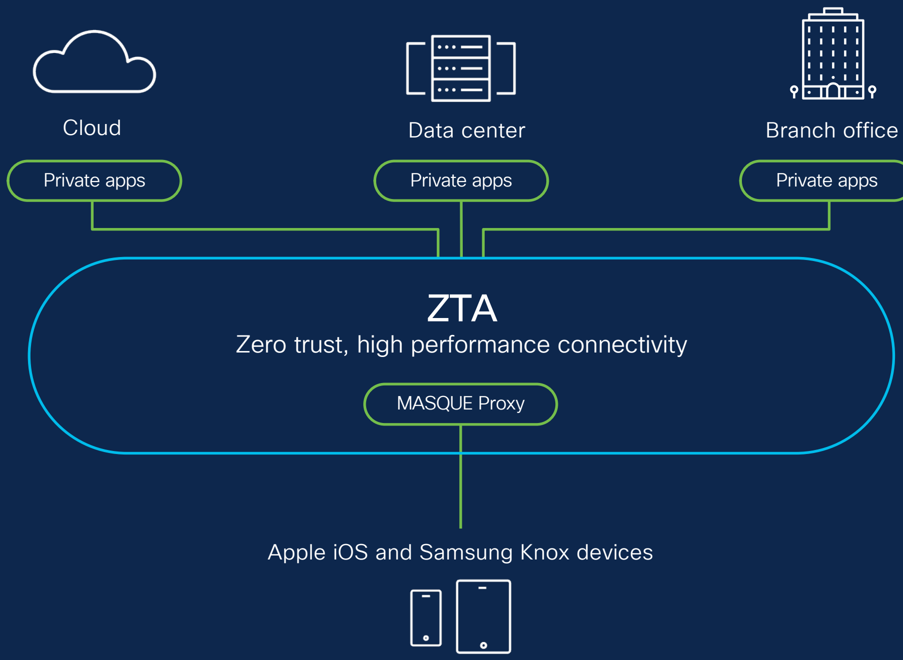
VPN



OS Native ZTA on iOS 17

ZTA connects + loads a site faster than VPN can even connect

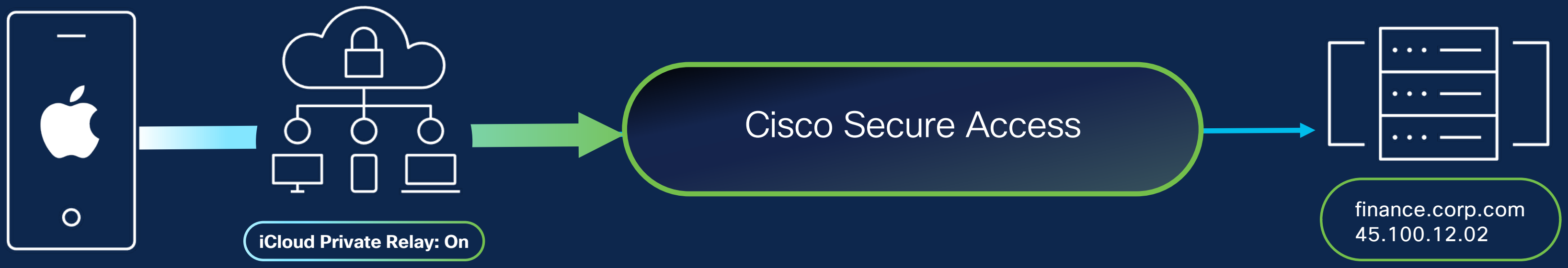
OS Native ZTA: Apple iOS and Samsung Knox



- New OS native ZTA functionality built into Apple iOS 17 and Samsung Knox 3.10
- Transparent user experience for users – no need to start or wait for VPN
- Delivers low latency and high throughput connectivity by directly intercepting traffic within the application
- Preserves battery life by eliminating the need for device-wide, continuously running VPN connections
- iCloud Private Relay compatible (iOS)
- Built on industry leading technologies: MASQUE and QUIC
- Supports all applications, ports and protocols - not just web applications

Cisco Secure Access traffic optimization with Apple iCloud Private Relay

OS Native ZTA with Apple iCloud Private Relay On



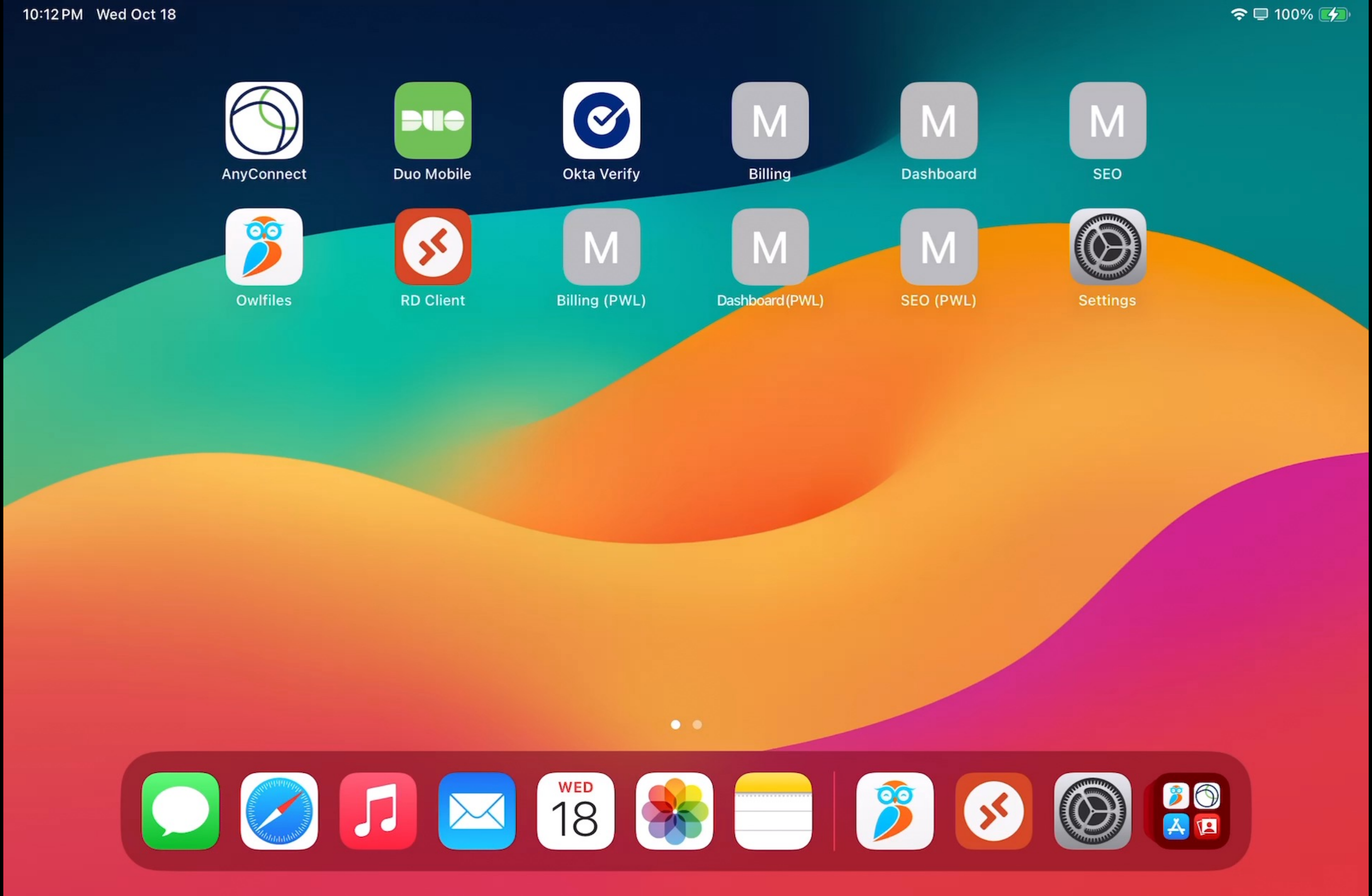
Single layer of encryption for lightning-fast, secure access

Traffic Flow w/o iCloud Private Relay Enabled:
Device → Secure Access → Application

Traffic Flow w/ iCloud Private Relay Enabled:
Device → Apple Relay → Secure Access → Application

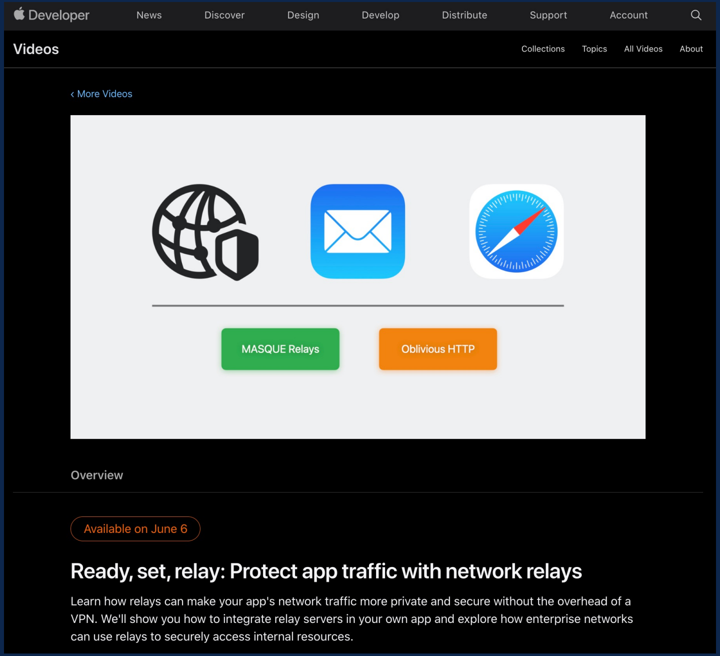
User Demo:

Zero Trust Access on Apple iOS


10:12 PM Wed Oct 18
100%
AnyConnect
Duo Mobile
Okta Verify
Billing
Dashboard
SEO
Owlfiles
RD Client
Billing (PWL)
Dashboard(PWL)
SEO (PWL)
Settings
WED
18

More on Apple’s Native OS Support of MASQUE

“Learn how relays can make your app's network traffic more private and secure without the overhead of a VPN. We'll show you how to integrate relay servers in your own app and explore how enterprise networks can use relays to securely access internal resources.”



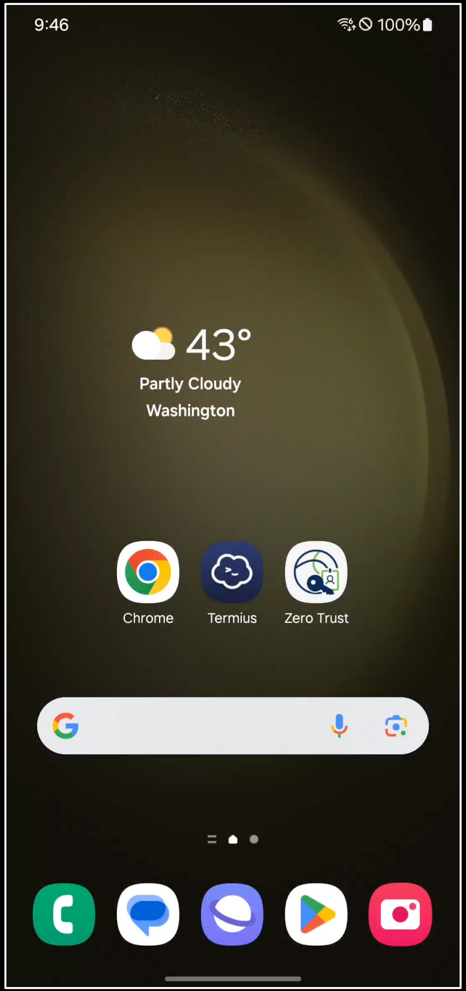
Ready, set, relay: Protect app traffic with network relays

Learn how relays can make your app's network traffic more private and secure without the overhead of a VPN. We'll show you how to integrate relay servers in your own app and explore how enterprise networks can use relays to securely access internal resources.

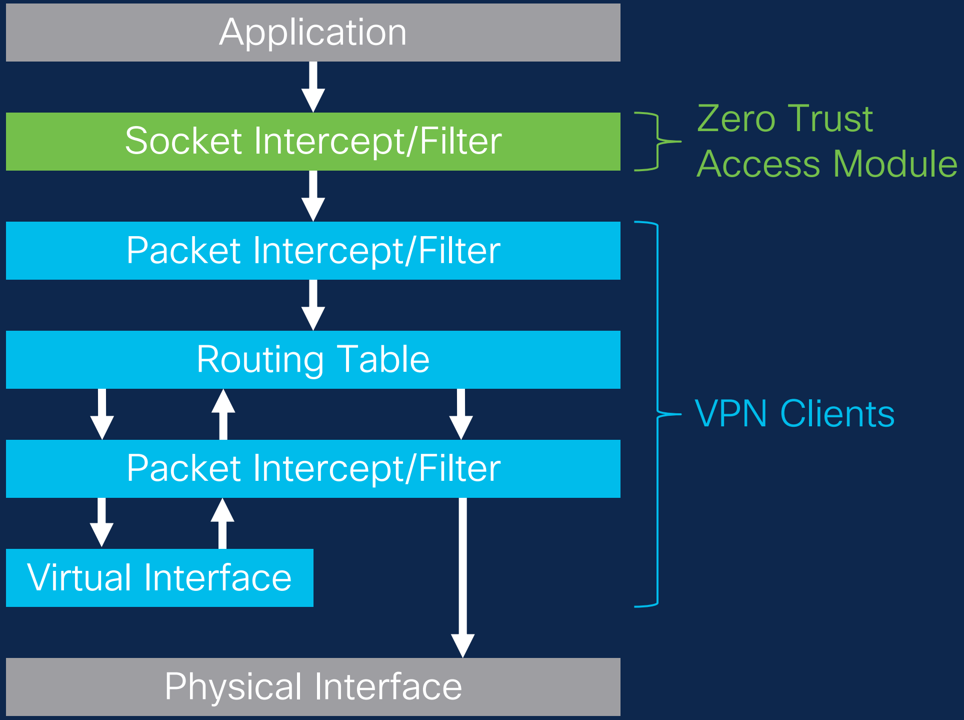
https://developer.apple.com/videos/play/wwdc2023/10002/

User Demo:

Cisco ZTA Enrollment on Samsung Knox


9:46
100%
43°
Partly Cloudy
Washington
Chrome
Termius
Zero Trust

Secure Client ZTA Module - Socket Intercept

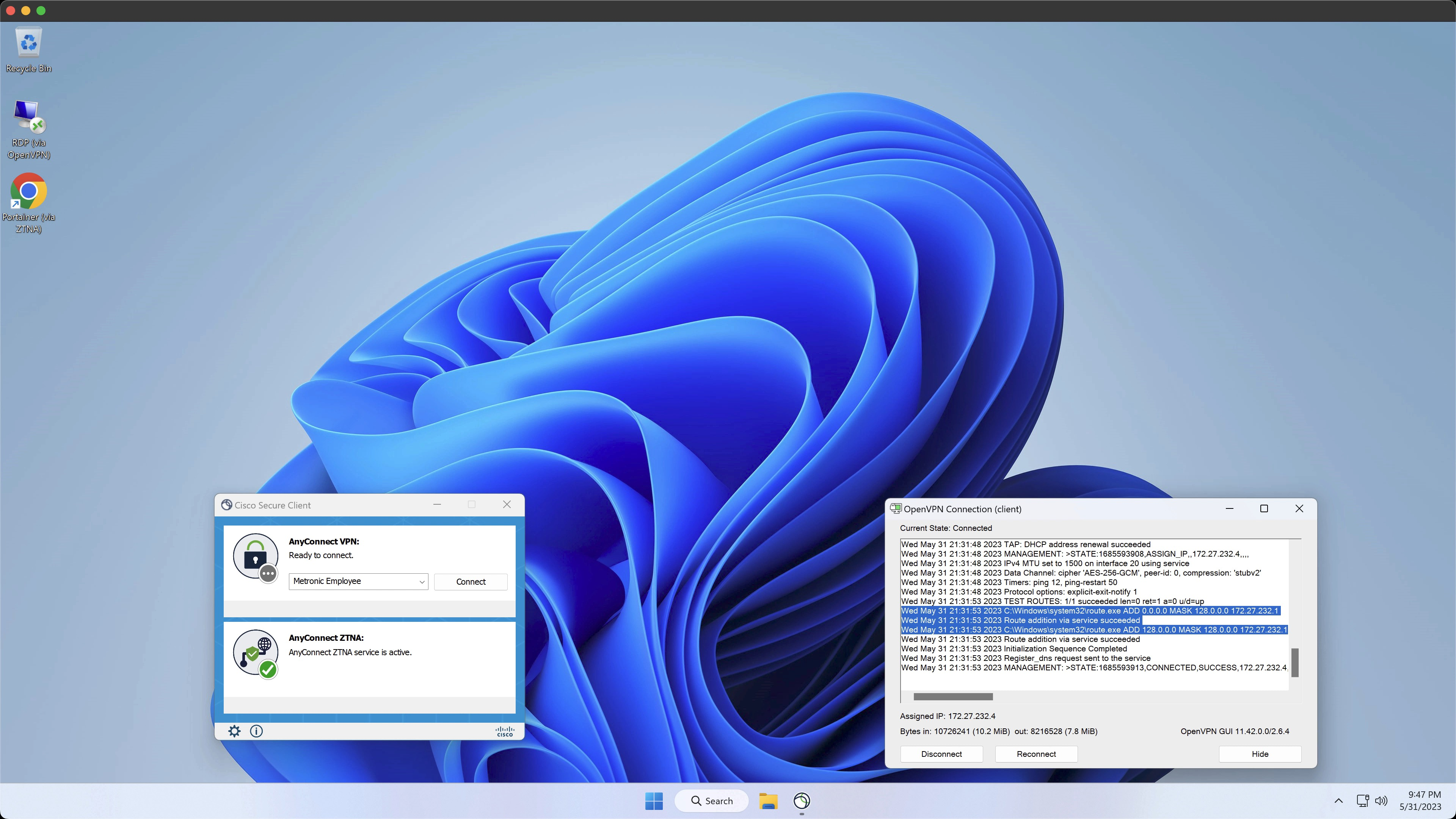


Why Socket Intercept?

- 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 Zero Trust Access
+ Third-Party VPN (OpenVPN)



Cisco Secure Client

AnyConnect VPN:
Ready to connect.

Metronic Employee

AnyConnect ZTNA:
AnyConnect ZTNA service is active.

OpenVPN Connection (client)

Current State: Connected

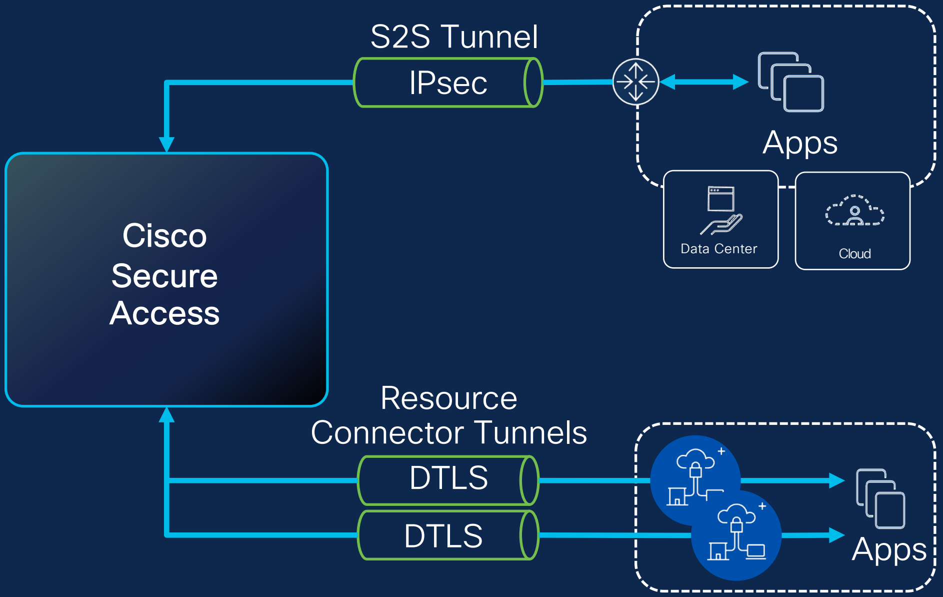
```
Wed May 31 21:31:48 2023 TAP: DHCP address renewal succeeded
Wed May 31 21:31:48 2023 MANAGEMENT: >STATE:1685593908,ASSIGN_IP,,172.27.232.4,,,,
Wed May 31 21:31:48 2023 IPv4 MTU set to 1500 on interface 20 using service
Wed May 31 21:31:48 2023 Data Channel: cipher 'AES-256-GCM', peer-id: 0, compression: '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: 1/1 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

Flexible private application connectivity options



Site-to-site Tunnels with IPsec

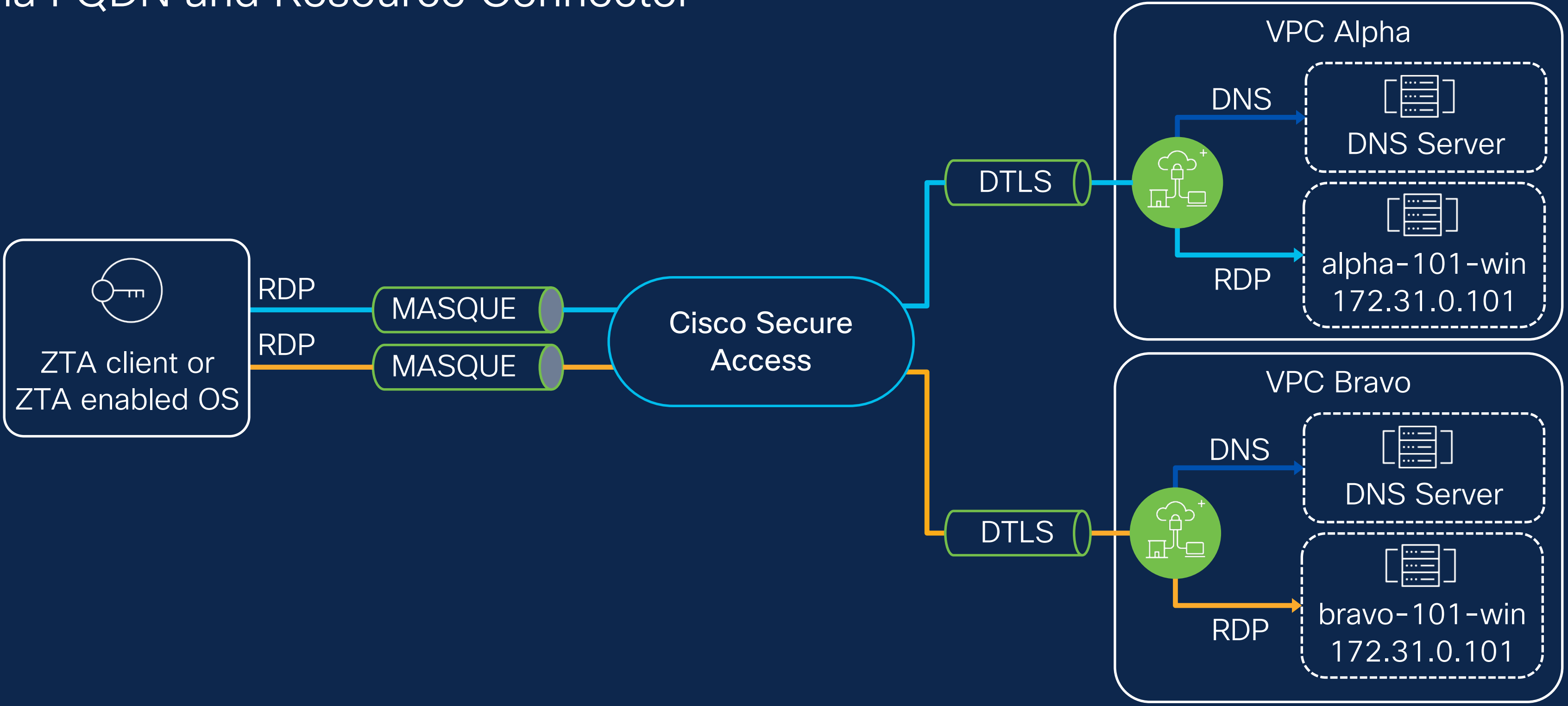
- Standards-based IPsec connection
- Connect with (nearly) any brand router or firewall
- Single tunnel for Internet and private application access
- Outbound connection / no firewall holes required
- Static or BGP routing support
- Auto failover for redundancy + ECMP for scale

Resource Connectors

- Lightweight VM for AWS and ESXi (today)
- All traffic egresses from Resource Connector IP
- Access applications with overlapping IPs
- Outbound connection / no firewall holes required
- No routing configuration required
- Auto failover / load balancing

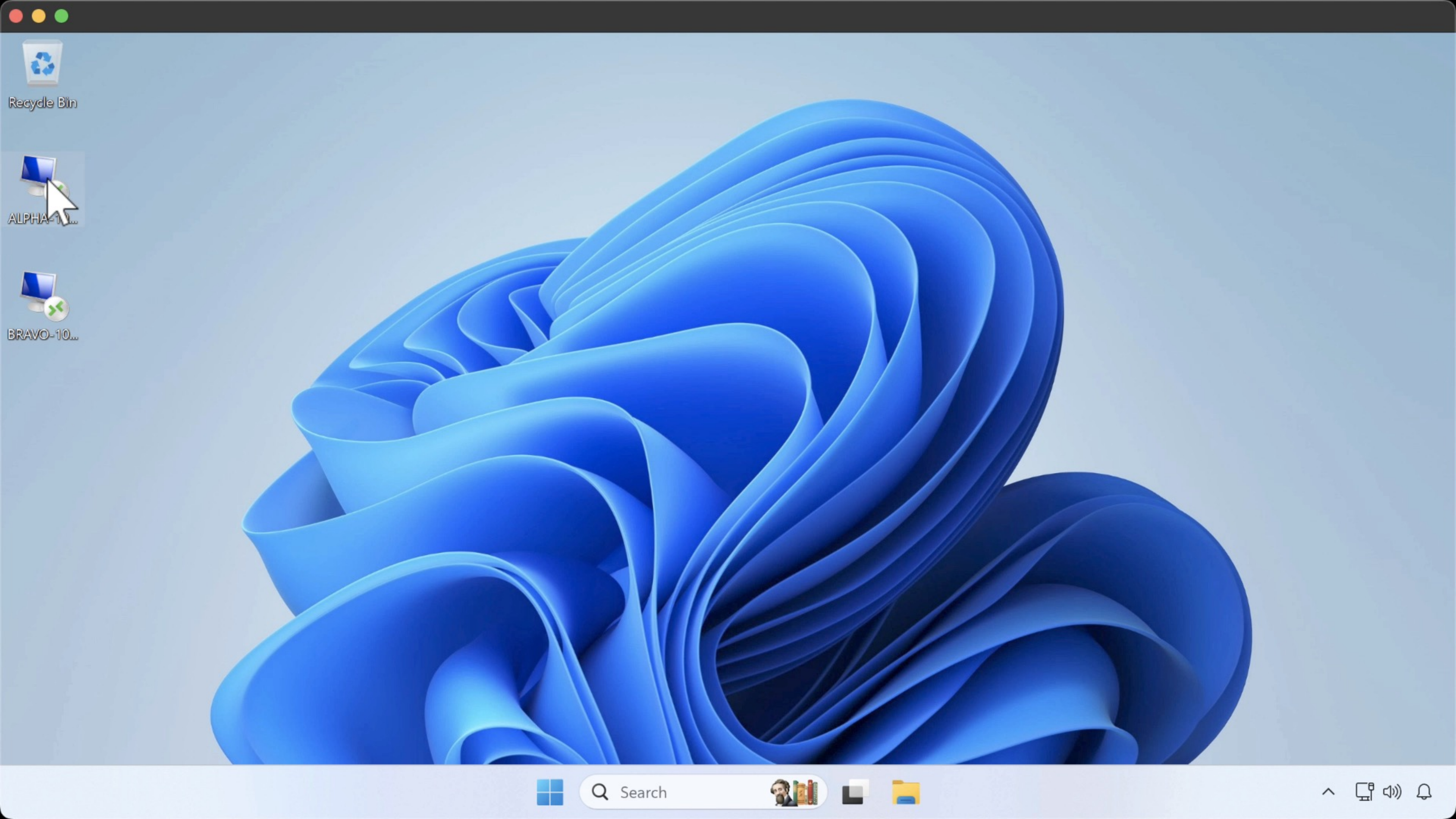
Access Overlapping IPs Simultaneously

via FQDN and Resource Connector

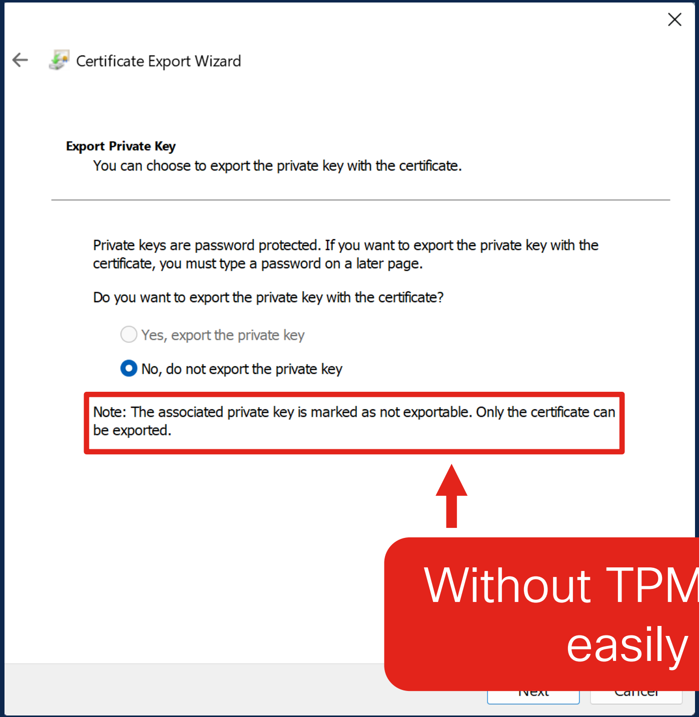


User Demo:

Accessing Servers with Overlapping IP Addresses


Recycle Bin
ALPHA-1...
BRAVO-10...
Search

Background: Marking Keys as Non-Exportable



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

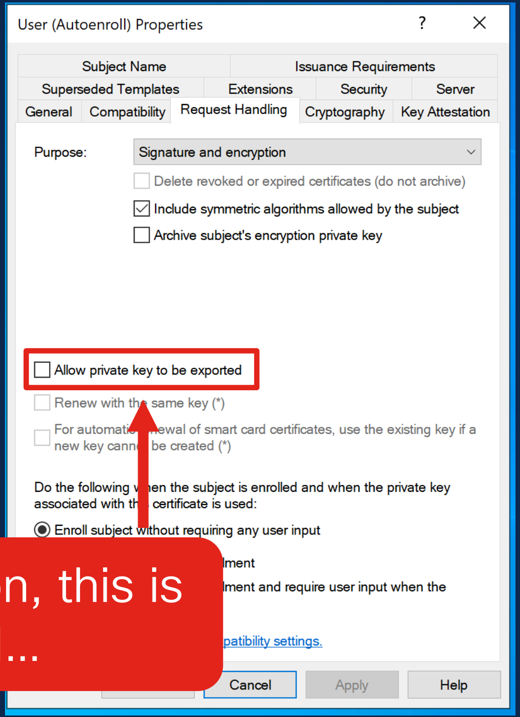
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

Note: The associated private key is marked as not exportable. Only the certificate can be exported.



User (Autoenroll) Properties

Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)

☑ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Allow private key to be exported

□ Renew with the same key (*)

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

lment

lment and require user input when the

patibility settings.

Without TPM protection, this is easily bypassed…

Exporting “Non-Exportable” Private Keys from non-TPM Protected Storage

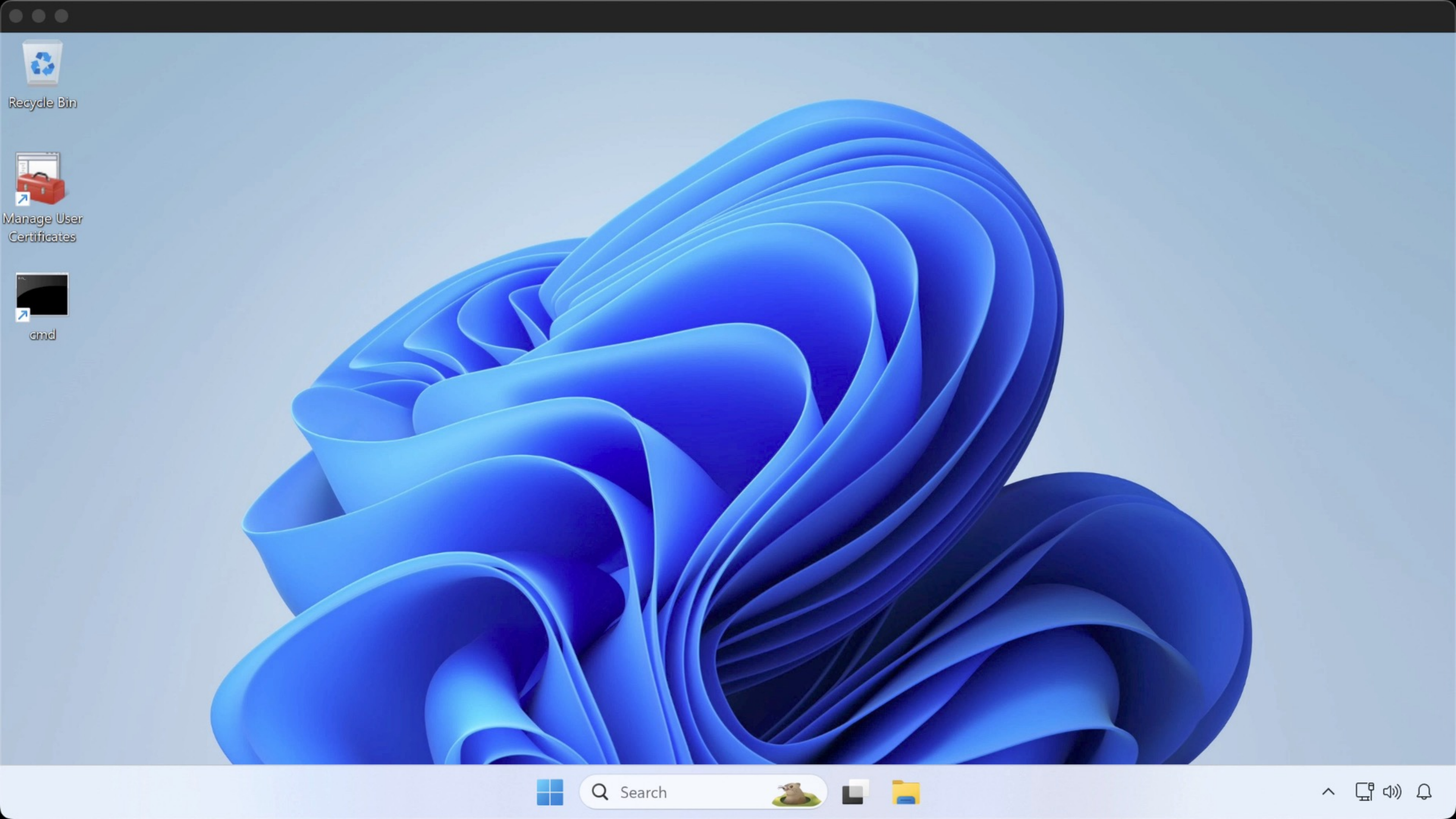
- Paper published in *2011* by Jason Geffner of NGS Secure outlined how to export non-exportable private keys without code injection or function hooking:
  - https://research.nccgroup.com/wp-content/uploads/2020/07/exporting_non-exportable_rsa_keys.pdf
- Code turned into a tool called exportrsa in *2016*:
  - https://github.com/luipir/ExportNotExportablePrivateKey
- Other tools such as Mimikatz and Jailbreak have existed for similarly long using code injection and/or function hooking
- TL;DR “Non-Exportable” is an obfuscated bit flag

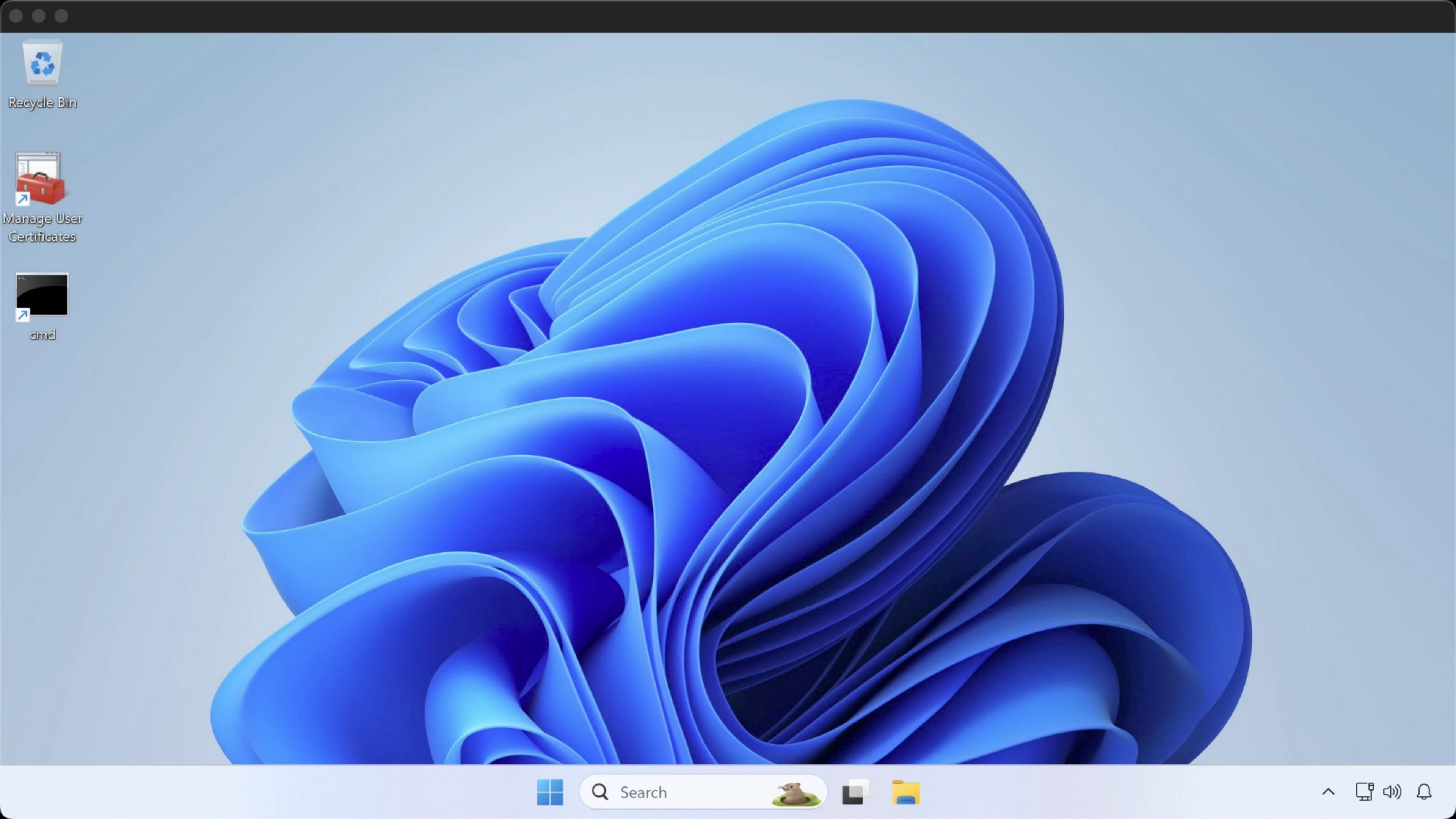
Attacker Demo:

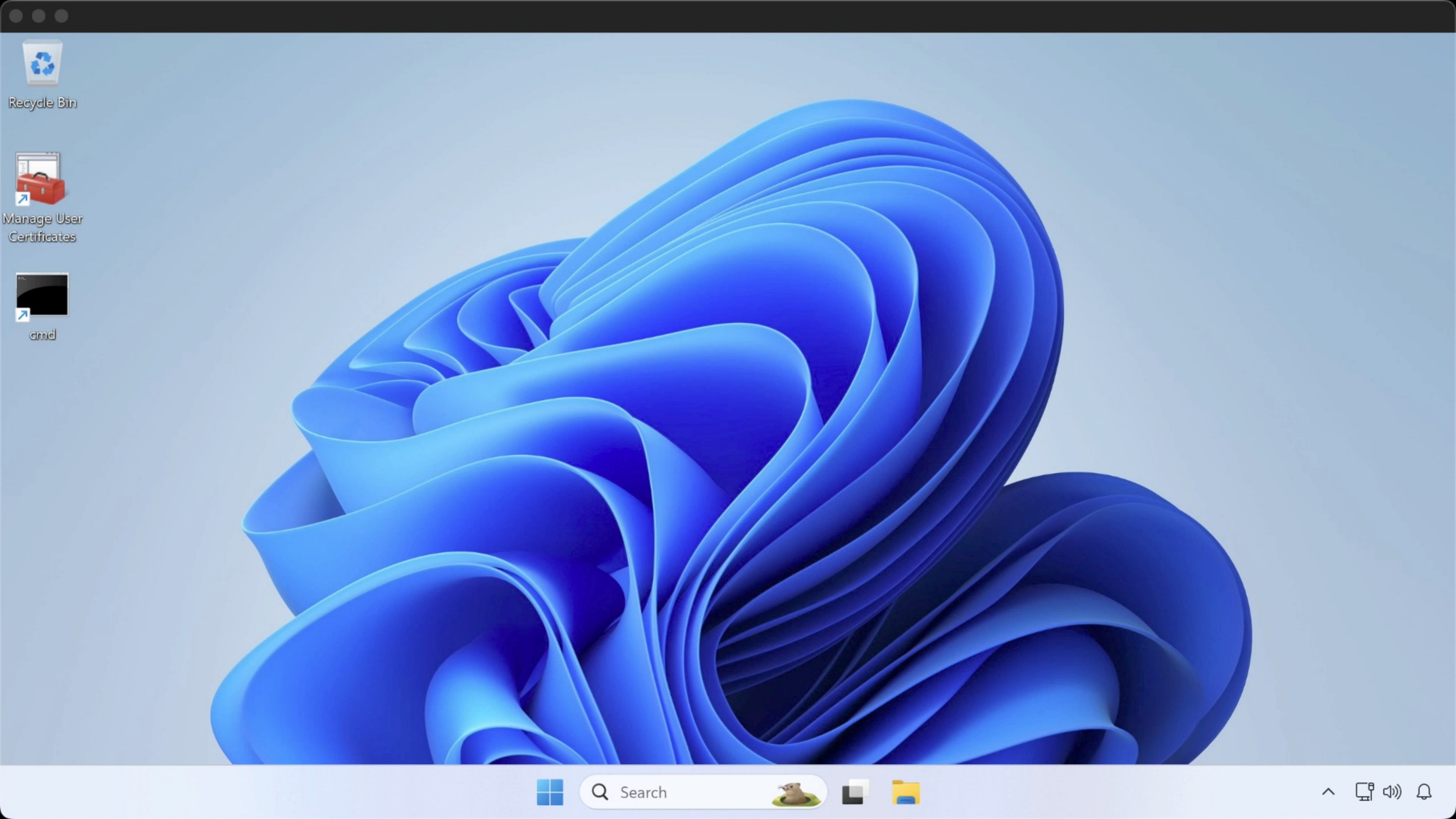
Exporting a “Non-Exportable” Private Key from a Fully Patched Windows 11 Enterprise System

The Demo Environment

- New Active Directory Forest on Windows Server 2022
- New Certificate Services on Windows Server 2022
- User certificates deployed via Active Directory autoenrollment with "Allow private key to be exported" disabled in the template.
- Demo workstation running Windows 11 Enterprise, fully patched
- Microsoft Defender is enabled with default protections
- User running with standard user privileges


Recycle Bin
Manage User Certificates
cmd
Search


Recycle Bin
Manage User Certificates
cmd
Search


Recycle Bin
Manage User Certificates
cmd
Search

Commands Used in the Demo

```
ECHO ### 1. Change to the directory where the exported user certificates should be saved ###
cd C:\Tools\UserCerts
ECHO ### 2. Export users certificates with private keys via exportrsa.exe ###
C:\Tools\exportrsa.exe
ECHO ### 3. Copy exported certificates to the desktop ###
COPY *.pfx %USERPROFILE%\Desktop
```

```
ECHO ### 1. Extract the certificate from the PFX file ###
openssl pkcs12 -in 1.pfx -nokeys -out 1-pfx-certificate.cer
ECHO ### 2. Extract the certificate public key from the certificate ###
openssl x509 -in 1-pfx-certificate.cer -noout -pubkey > 1-pfx-certificate-public.key
ECHO ### 3. Create hello-world.txt file to be encrypted ###
ECHO "Hello, World!" > hello-world.txt
ECHO ### 4. Encrypt hello-world.txt with the certificate public key ###
openssl pkeyutl -encrypt -in hello-world.txt -pubin -inkey 1-pfx-certificate-public.key -out ciphertext.txt
ECHO ### 5. Verify ciphertext.txt contents ###
more ciphertext.txt
ECHO ### 6. Extract the private key from the PFX file ###
openssl pkcs12 -in 1.pfx -nocerts -nodes -out 1-pfx-private.key
ECHO ### 7. Decrypt ciphertext.txt with the private key###
openssl pkeyutl -decrypt -in ciphertext.txt -inkey 1-pfx-private.key
```

Solution for ZTA: TPM Key Storage and ACME Certificates

TPM

- Trusted Platform Module
- Hardware storage of cryptographic material
- Even with a complete and total compromise of the OS, the certificate private key can not be exported/moved to another device

ACME

- Automated Certificate Management Environment
- Protocol to automate the issuance and renewal of certificates
- Eliminates user interaction for certificate renewal and private key rotation, allowing extremely short certificate lifetimes which drastically reduces certificate compromise risks

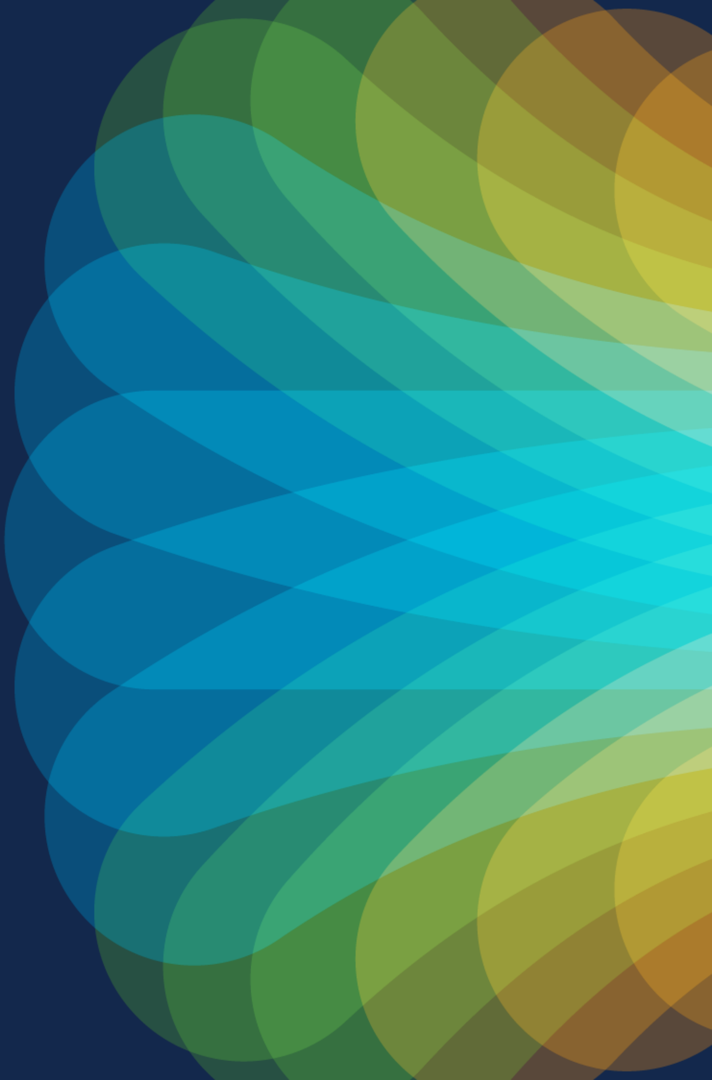
Fill out your session surveys!

Participants who fill out a minimum of **four session surveys and the overall event survey** will get a Cisco Live t-shirt (from 11:30 on Thursday, while supplies last)!

All surveys can be taken in the Cisco Events Mobile App or by logging into the Session Catalog and clicking the 'Participant Resource Center' link at https://www.ciscolive.com/emea/learn/session-catalog.html.

The bridge to possible

Thank you



cisco Live!

Let’s go