



Cisco Secure Access

Transforming Secure Connectivity for the Modern Enterprise

Sean Reagan
Solutions Engineer
Security Incubation
sereagan@cisco.com

Agenda

- What is Secure Access?
- Use case 1 – Secure Internet Access
- Use case 2 – VPN as a service
- Use case 3 – Zero Trust Network Access
- Use case 4 – Terminal Services replacement
- Conclusion/Q&A

Cisco Secure Access

Protect your hybrid workforce with cloud-agile security

This cloud-delivered security service edge (SSE) solution, grounded in zero trust, gives users an exceptional user experience and protected access from any device to anywhere.

Read e-book

Talk to an expert >



What's driving interest in security service edge (SSE)?

- Ongoing changes in the mix of cloud and on-premise applications/data
- Frequent changes in the mix of users/locations/device types
- Continually changing threats and attack tactics
- Shortage of cybersecurity talent/resources
- Zero trust

Tool sprawl and complexity are increasing risk and decreasing productivity

Cisco Secure Access

Converged cloud-native security grounded in zero trust



Remote

Campus

Branch

Airplane

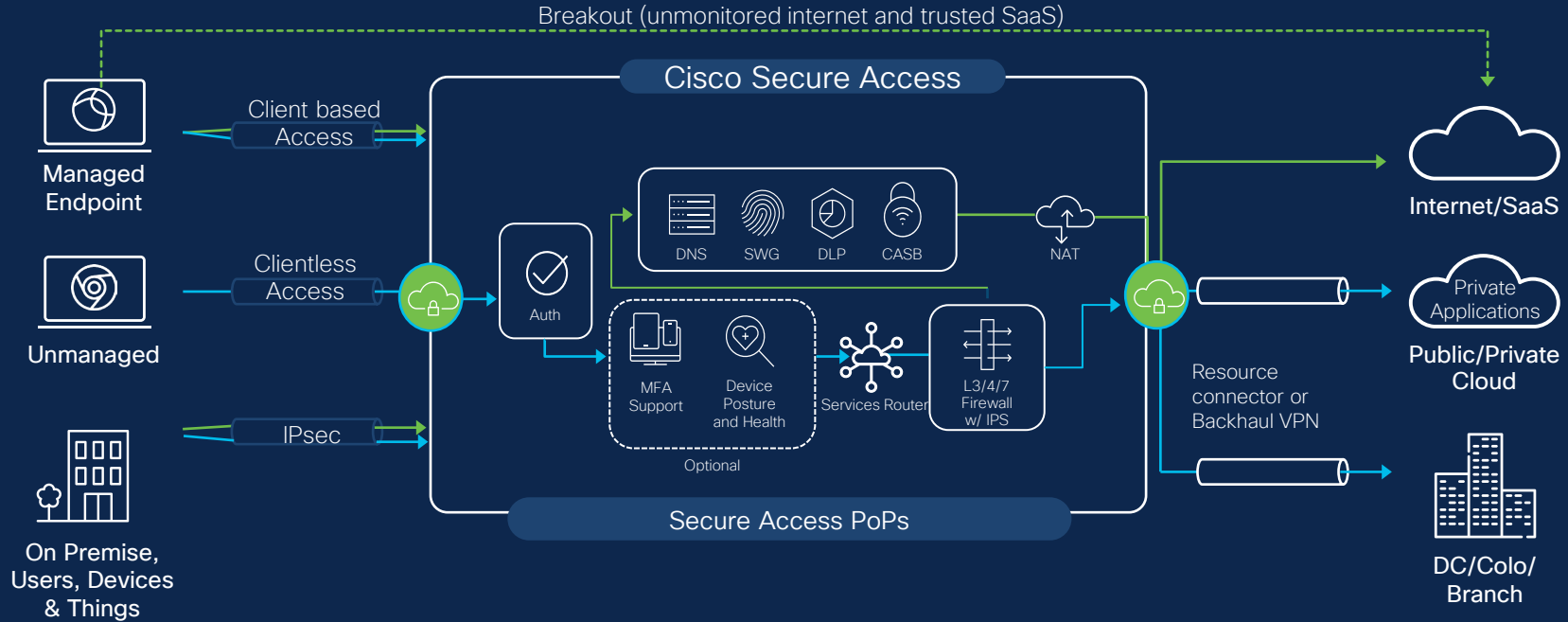
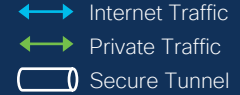
Oil rig

Stadium

Field

...

Architecture Overview



Cisco Secure Access- User Anywhere

STEP 1
Log In

STEP 2
Securely start work



Easy, frictionless user experience

Cisco Secure Client

Suite of security service enablement modules



AnyConnect VPN (Core)

ZTA Module

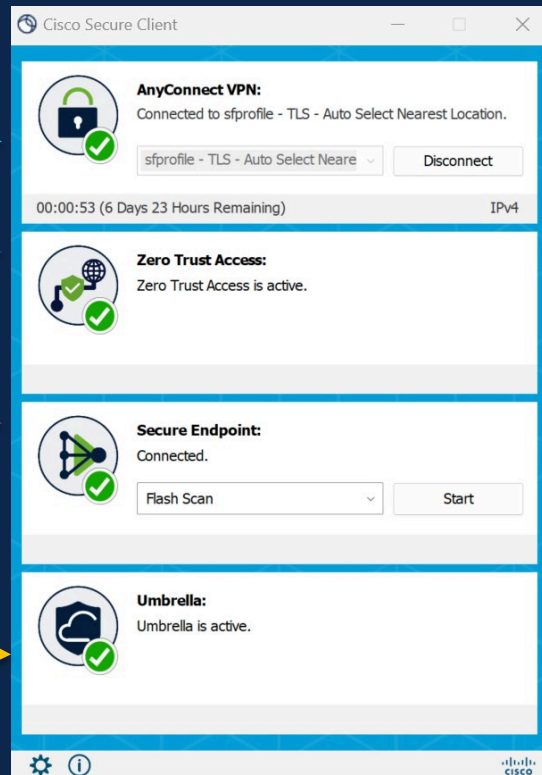
Secure Endpoint (AMP)

Roaming Module

Thousand Eyes (No UI)

Cloud Management Module (No UI)

Diagnostic and Reporting (DART)



Cisco Secure Access

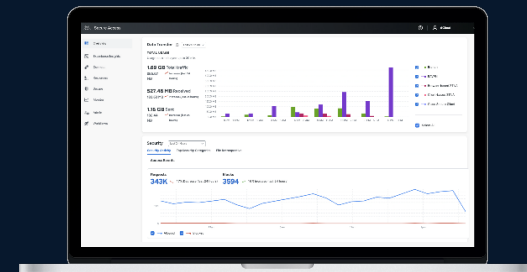
Proven cloud-native security converged into one service



Protecting 70,000+ customers

More than 220M endpoints

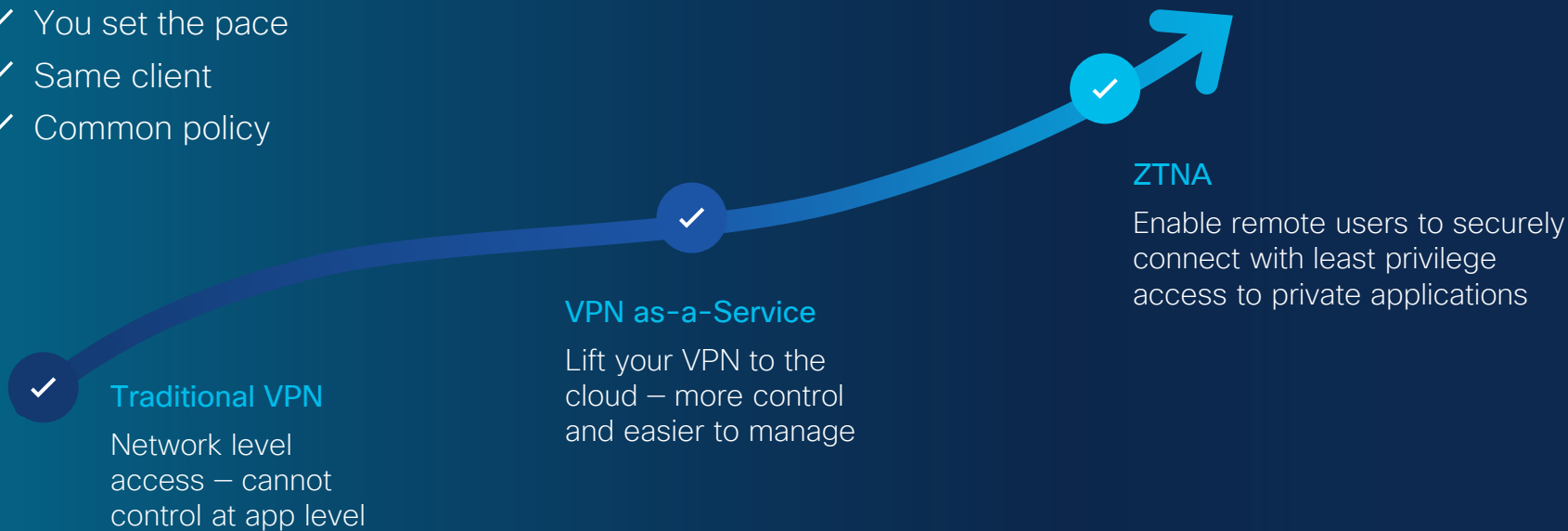
Cisco Secure Access



- Single Console
- Single Client
- Unified Policies

Flexible journey to ZTNA

- ✓ You set the pace
- ✓ Same client
- ✓ Common policy



Cisco Secure Access: Extended SSE protection



SSE core capabilities

- Secure Web Gateway
- Zero Trust Network Access
- Firewall as-a-Service
- Cloud Access Security Broker
- Data Loss Prevention
- Advanced Malware Protection
- Sandbox



So much more

- VPN as-a-Service
- AI Access and Usage Controls
- Digital Experience Monitoring
- DNS Security
- Remote Browser Isolation
- Talos Threat Intelligence
- Cloud Malware Protection

Secure Access – Features coming quickly!

- Private Resource Discovery
- Application Risk Profiles
- Resource Connectors in Docker Containers
- Virtual Appliance update
- YouTube Tenant Controls
- Realtime DLP Download Scanning
- Enhanced DLP classifications
- DLP for Private Resources
- AI-Driven Domain Generation Algorithm detection
- DLP AI Guardrails
- Enterprise Browser integration with Chrome
- Enhanced BGP controls
- Logging enhancements (Splunk)

Agenda

- What is Secure Access?
- Use case 1 – Secure Internet Access
- Use case 2 – VPN as a service
- Use case 3 – Zero Trust Network Access
- Use case 4 – Terminal Services replacement
- Conclusion/Q&A

Secure Internet Access

- 3 steps
- In about 6 minutes!

Step 1 – Define the network

Resources

Home

Experience Insights

Connect

Resources

Secure

Monitor

Admin

Workflows

Sources and destinations

Internal Networks

Registered Networks

Roaming Devices

Security Group Tags

SDWAN Service VPN IDs

Network and Service Objects

Destinations

Internet and SaaS Resources

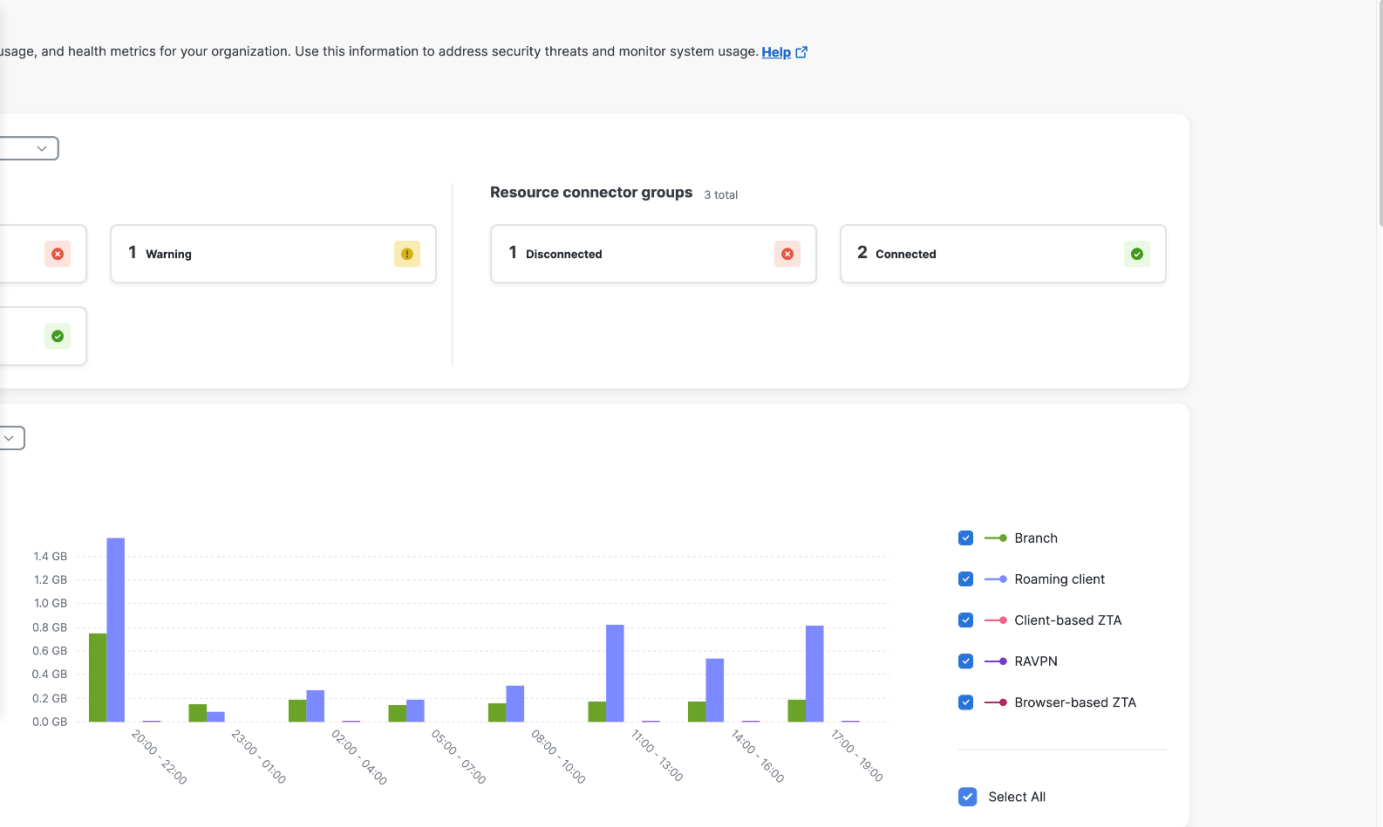
Private Resources

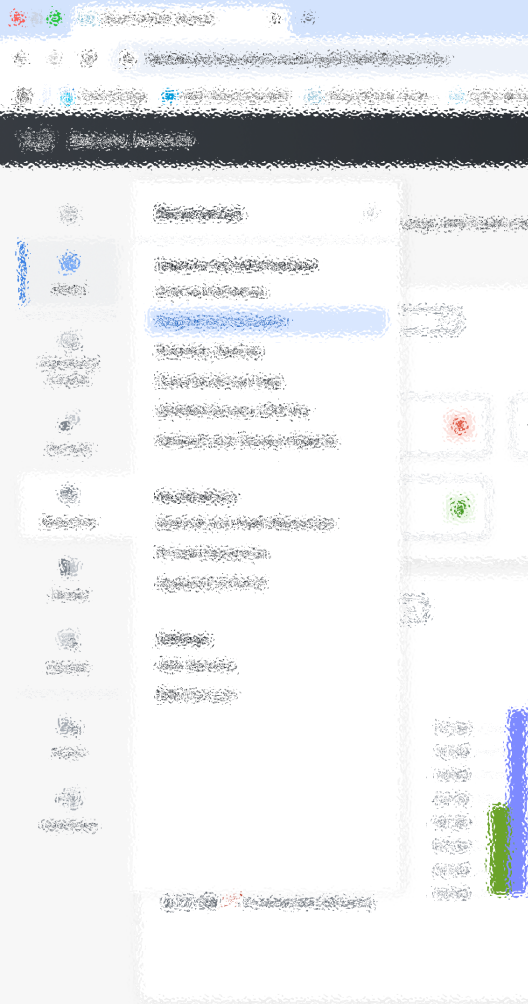
Application Portal

Settings

AAA Servers

DNS Servers








dashboardsse.cisco.com/org/82064


Cisco Bridge S&C Salesforce S&C Cisco Se


Secure Access


Home


Experience
Insights


Connect


Resources


Secure

Resources

Sources and destinations

Internal Networks

Registered Networks

Roaming Devices

Security Group Tags

SDWAN Service VPN IDs

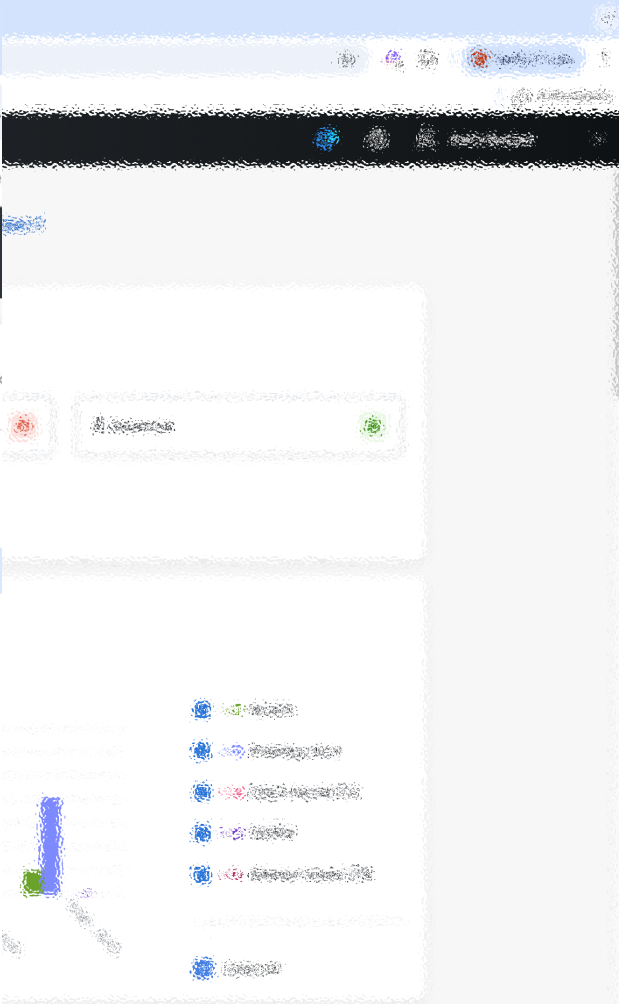
Network and Service Objects

Destinations

Internet and SaaS Resources

Private Resources

Application Portal



Workflow

10

Save

Add network

Start by pointing your networks DNS to our servers [Help](#) 

IPv4: 208.67.220.220 and 208.67.222.222

IPv6: 2620:119:35::35 and 2620:119:53::53

Network Name

Lab Network 162 Test - SEan

IP version



IPv4



IPv6

IPv4 address

70.99.78.162

32 (1 address)



This network has a dynamic IP address.

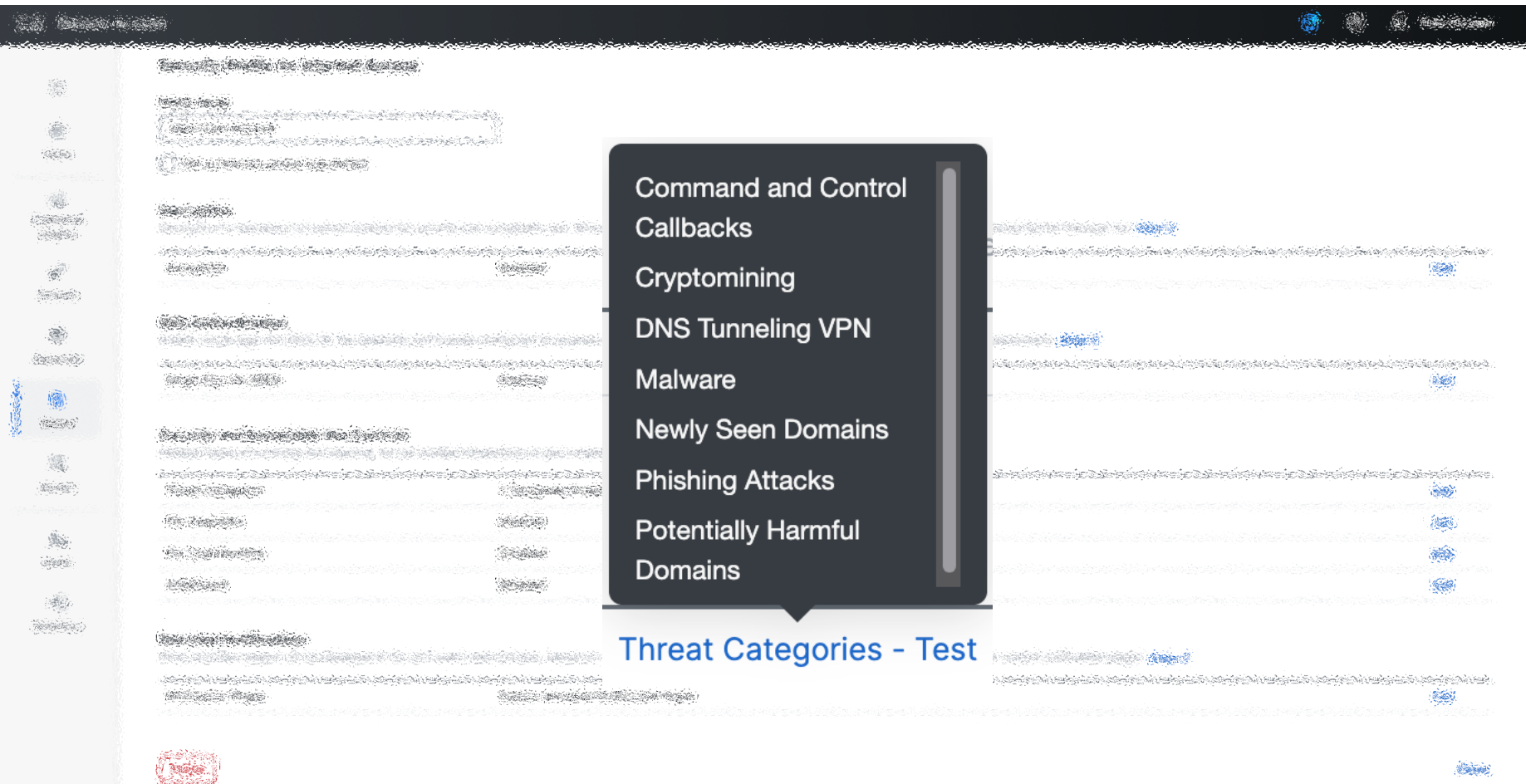
Cancel

Save

Step 2 – Create a Security Profile



Workflows



Step 3 – Create a rule



Home



Experience
Insights



Connect



Resources



Secure



Monitor



Admin



Workflows

Access Policy

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. [Help](#)

[Rule Defaults and Global Settings](#)

Q Sean

Intent

Objects

[Reset all](#)

[Add Rule](#)

6 Results

[Customize view](#)

	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	
	7	Sean 161 Internet	Internet	Allow	Sean-W11-Okt... +1	Any		57.8k		
	8	Sean VPN Access Rule	Private	Allow	Sean Reagan ...	OneSASE Webs...		-		
	9	Sean-RBI	Internet	Isolate	Sean-W11-SAS... +1	Generative A... +2		-		
	10	Sean-Test-Web	Internet	Allow	Sean-W11-SAS... +2	Any		333.8k		
	11	Sean - Test Vcenter	Private	Allow	Sean Reagan ... +1	vcenter +1		-		
	12	Sean- Test-RDP	Private	Allow	Sean-W11-SAS... +1	Boston-OnPre...		-		

Rows per page 100 < 1 >



Home



Experience
Insights



Connect



Resources



Secure



Monitor



Admin



Workflows

Rule name

Sean 161 Internet

Rule order

7

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.



Warn

Allow access but display a warning.



Isolate

Allow access to specified destinations, but isolate the traffic.

From

Specify one or more **sources**.

Lab Network 161 Test - Sean

+1

To

Specify one or more **destinations**.

Any

+ AND

Access Criteria

Additional criteria that apply to this traffic:

App Risk Profile

Application risk criteria will not be applied to destinations in this rule. [Help](#)

Disabled

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)



Home



Experience
Insights



Connect



Resources



Secure



Monitor



Admin



Workflows



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

☐ Disabled

Traffic that matches this rule will not be inspected by the intrusion prevention system. [Help](#)

Security Profile Custom

The following web-related settings will apply to traffic that matches this rule. [Help](#)

Security Profile: **Sean-Test-Network** | Decryption: **Disabled** | SAML Authentication: **Disabled** | Threat Categories: **Enabled** | [+3 More](#)

Tenant Control Profile Rule Defaults

Limit access to your organization's tenant for certain SaaS applications. [Help](#)

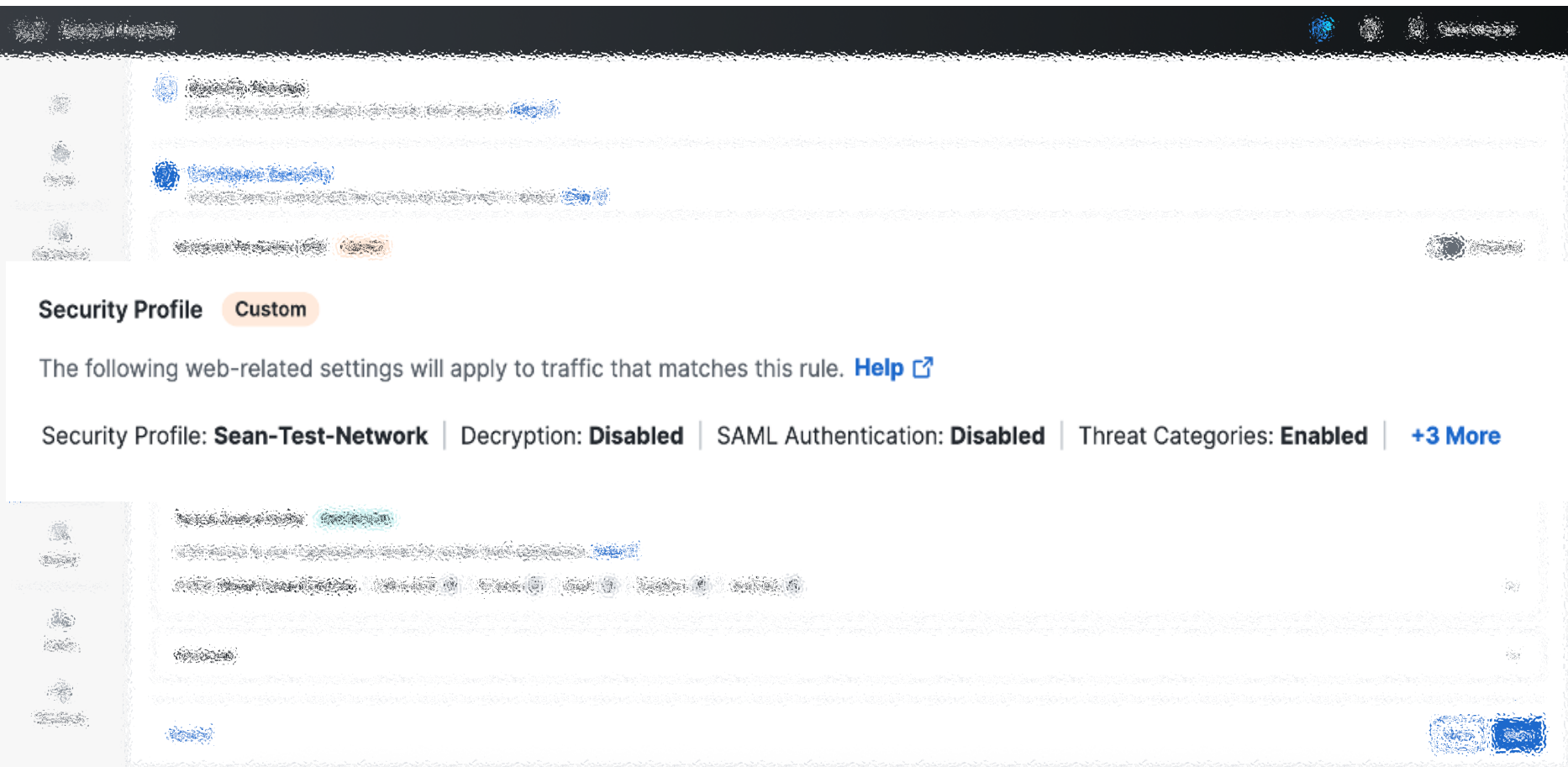
Profile: **Global Tenant Controls** | Office 365 0 | G Suite 0 | Slack 0 | Dropbox 0 | YouTube 0

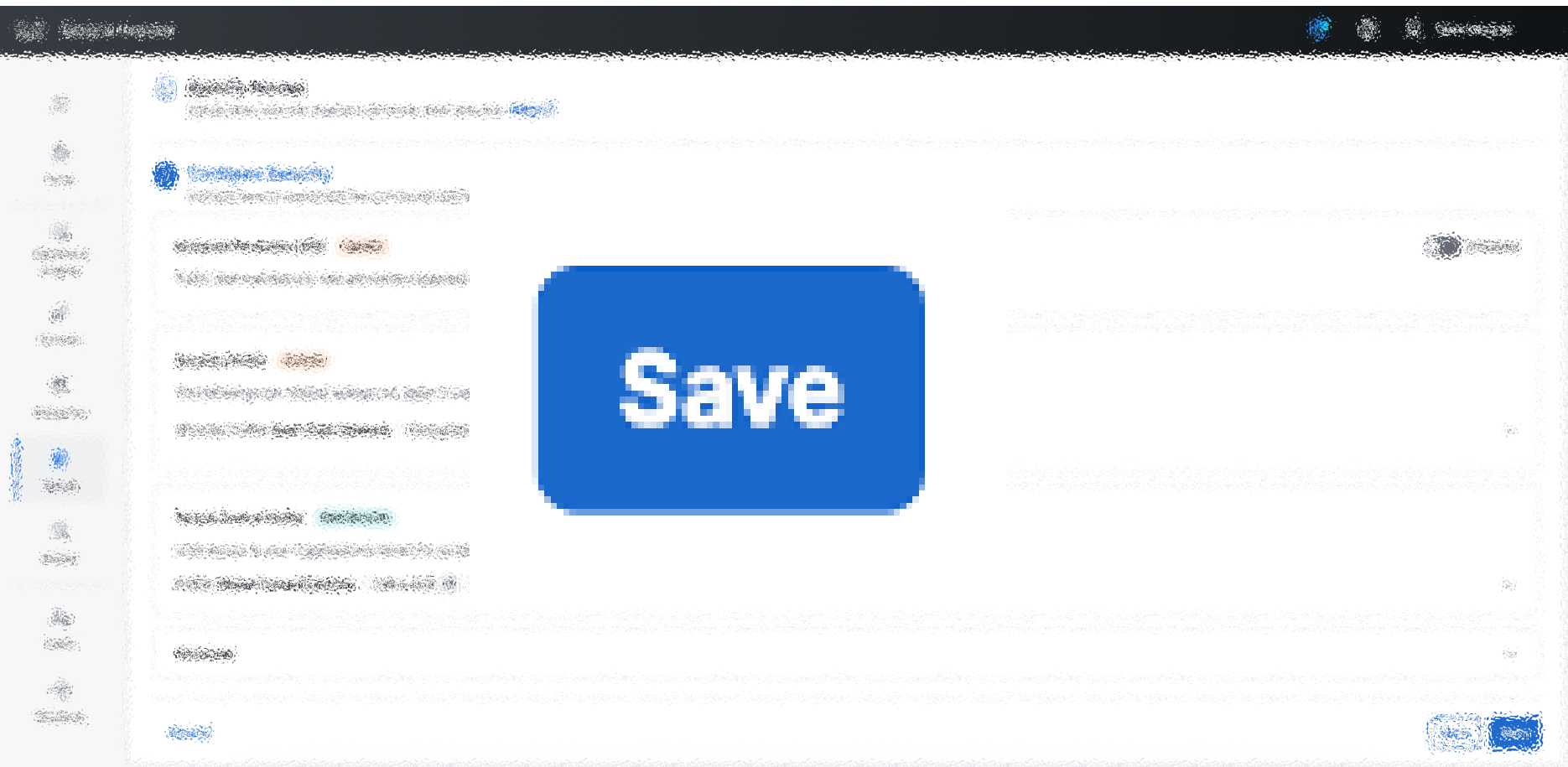
Advanced

[Cancel](#)

[Back](#)

[Save](#)







Cisco Secure Access



This site is blocked.

examplemalwaredomain.com

Sorry, examplemalwaredomain.com has been blocked by your network administrator.

This site was blocked due to the following categories: **Enterprise Malware**

[> Diagnostic Info](#)

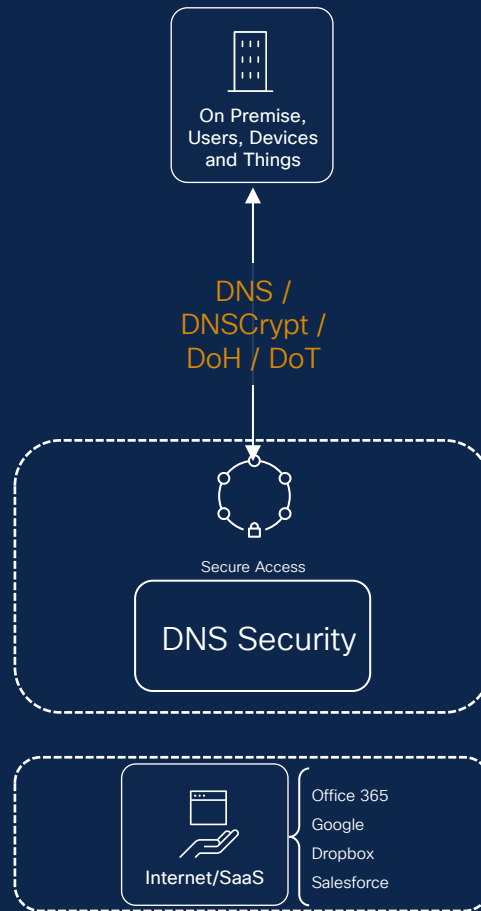
[Contact](#)

It really is that simple.

1. Register a network
2. Create a Security Profile
3. Create a Rule

Registered Network

- Register the branch public IP with Secure Access
 - Single static IPv4 or IPv6 address
 - Single dynamic IPv4 address
 - Range of IP addresses
 - IPv4 ranges larger than /29 must be approved by support
 - IPv6 ranges larger than /56 must be approved by support
- Forward queries to the DNS AnyCast resolvers
 - 208.67.220.220
 - 208.67.222.222
 - 2620:119:35::35
 - 2620:119:53::53
- Dynamic updater is available
 - Available for Mac and Windows



Flexible connection methods



IPsec
tunnel*
FW & Web



HQ & Branch



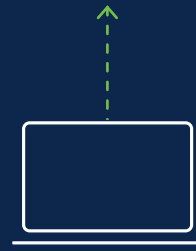
Proxy chain or
Cloud PAC File
Web only



HQ & Branch



Cisco Secure Client
Web & DNS

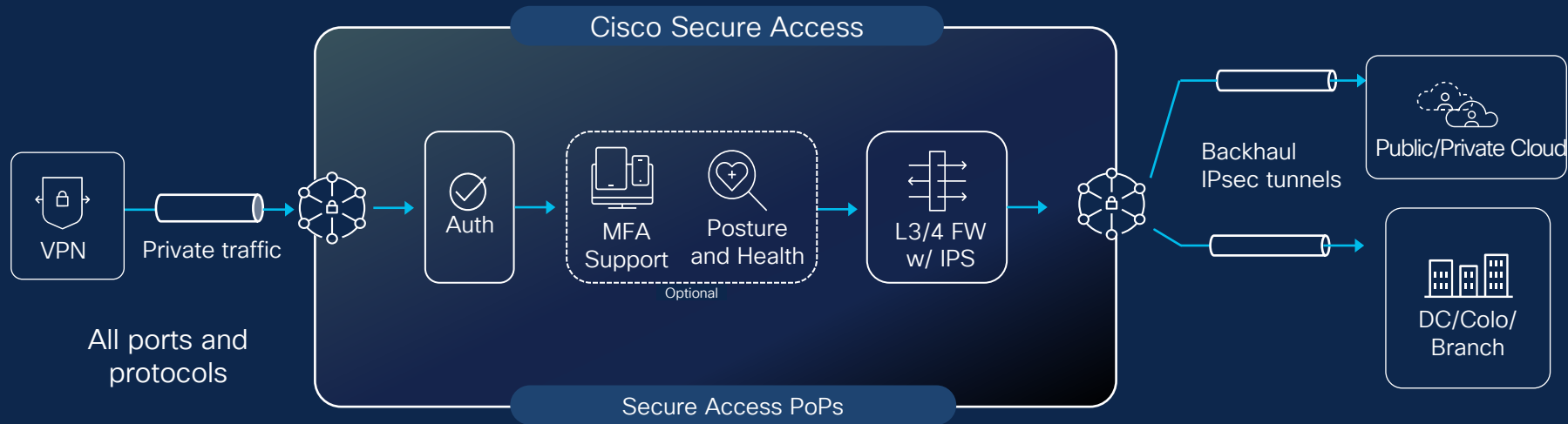


Roaming

Agenda

- What is Secure Access?
- Use case 1 – Secure Internet Access
- Use case 2 – VPN as a service
- Use case 3 – Zero Trust Network Access
- Use case 4 – Terminal Services replacement
- Conclusion/Q&A

VPN-as-a-Service



- Authentication Methods:
SAML 2.0, SAML+ certificate, Certificate, RADIUS
- Identity based access
- Region specific IP pool for client addressing

- Posture Verification: (optional)
Secure Firewall (formerly hostscan) or ISE with RADIUS
- IPS (optional)
- Connection profiles

Posture

Hostscan

- Packaged with the client installer
- Supports the following attributes:
 - Operating system
 - Firewall
 - Endpoint security agent
 - System password
 - Disk encryption
 - Browser
 - Files
 - Processes
 - Certificates

ISE

- Packaged with the client installer
- [ISE Posture Prescriptive Deployment Guide](#)

The screenshot displays a configuration interface for the ISE Posture Prescriptive Deployment Guide. On the left, a vertical list of eight steps is shown, each with a numbered circle icon. Step 1, 'Operating System', is highlighted in blue. The other steps are: 2. Endpoint security agent (Not required), 3. Windows registry entries (Not required), 4. Firewall (Not required), 5. Disk encryption (Not required), 6. File (Not required), 7. Processes (Not required), and 8. Certificate (Not required). The main content area on the right is titled 'Operating System' and includes the instruction 'Require specific operating systems'. Below this, there is a section labeled 'Operating system' with a dropdown menu. The dropdown is currently open, showing a search bar with 'Windows' and a close button (X). Below the search bar, three options are listed: 'Windows' (highlighted in light blue), 'Mac OS X', and 'Linux'.

Step	Attribute	Requirement
1	Operating System	Any
2	Endpoint security agent	Not required
3	Windows registry entries	Not required
4	Firewall	Not required
5	Disk encryption	Not required
6	File	Not required
7	Processes	Not required
8	Certificate	Not required

Operating System
Require specific operating systems

Operating system

Windows X

Windows

Mac OS X

Linux



Recycle Bin



Microsoft
Edge



csc-deploy...



Cisco Secu...
(1)



cisco-secu...



Google
Chrome



seanwllsa...



USD/EUR
+0.84%



3:43 PM
4/22/2025

Cisco Secure Client

AnyConnect VPN:
Ready to connect.
SASE4ALL-SAML - IPSec - Auto Si ▼ Connect

Zero Trust Access:
Zero Trust Access is active.

Secure Endpoint:
Connected.
Flash Scan ▼ Start

Umbrella:
Umbrella is active.

cisco *Connect*



Sign in

sean@sase4all.com

[Can't access your account?](#)

Next



Sign-in options

[Terms of use](#) [Privacy & cookies](#) ...



about
Cisco





Enter code in Duo Mobile

Verify it's you by entering this verification code
in the Duo Mobile app...

311

Sent to "iOS" (*****7172)



Waiting for approval...

[Other options](#)



Remember me

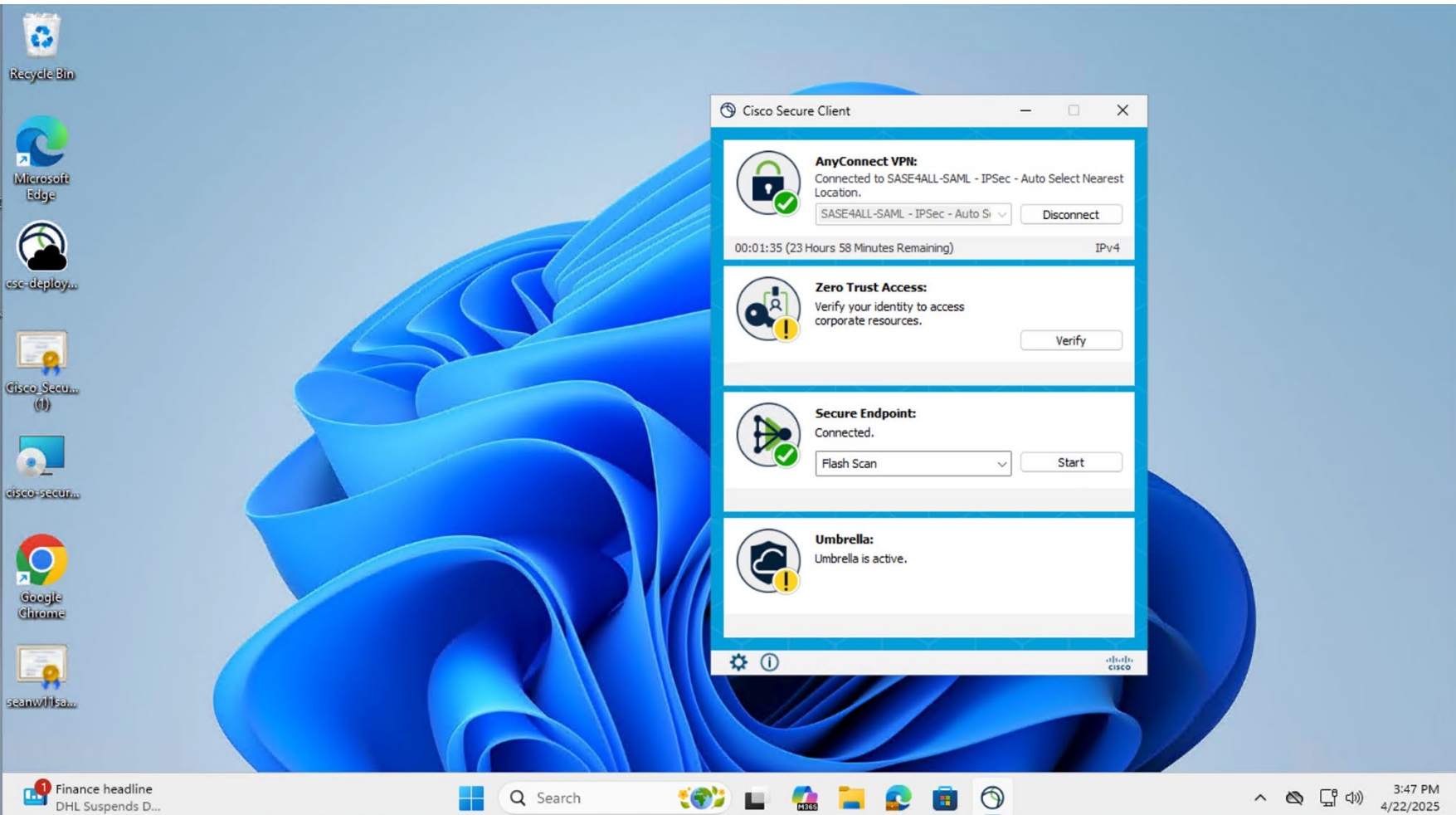


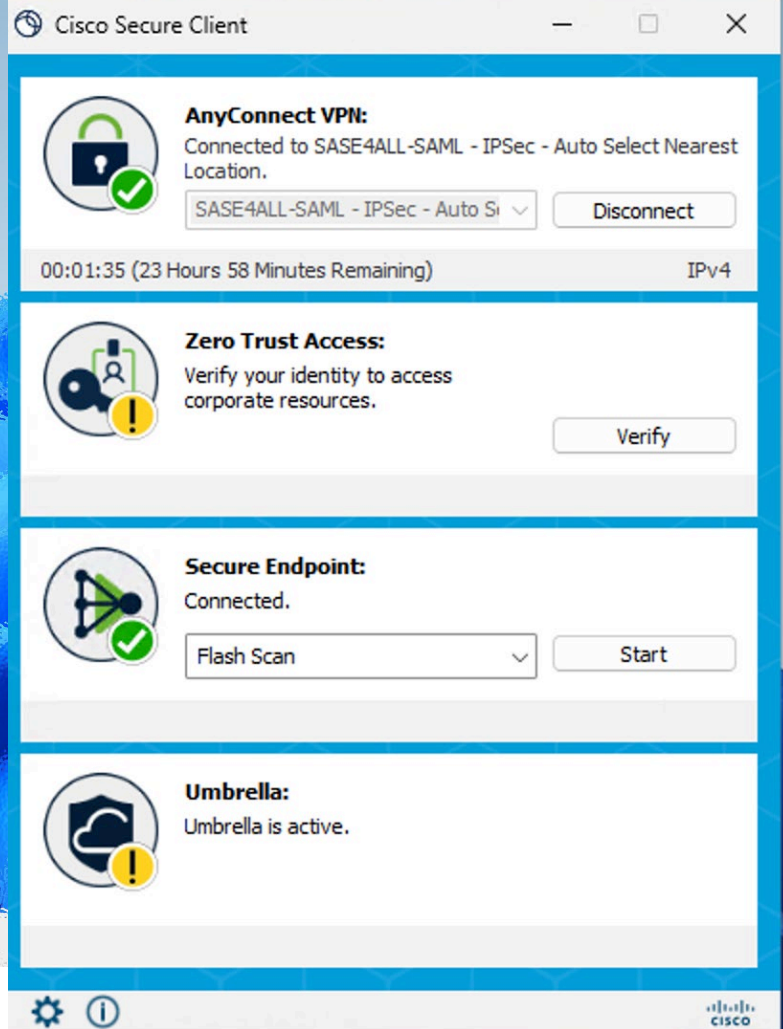
cisco











seanwilliams







Step 1. Create VPN components

- ☰
-  Home
-  Experience Insights
-  Connect
-  Resources
-  Secure
-  Monitor
-  Admin
-  Workflows

End User Connectivity

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

 Cisco Secure Client

Manage servers ▾

- Zero Trust
- Virtual Private Network
- Internet Security

FQDN

Use the FQDN listed here to configure VPN access to Secure Access. [Help](#)

Global: 0b00.vpn.sse.cisco.com  [Copy](#) [View Regional FQDN's](#)

VPN Headend: list-0b00.vpn.sse.cisco.com  [Copy](#)


Regions and IP Pools


Click manage to add and edit IP pools that can be used when configuring your VPN profiles. [Help](#)


Regions mapped 3 [Manage](#)



VPN Profiles

A VPN profile is a configuration that provides your remote devices with the means to securely connect to your network through a VPN. This configuration includes options for custom attributes and a machine tunnel. [Help](#)

 A region has been added to or deleted from IP Pool Configurations. Download the XML files associated with each VPN profile, which contain updated region information.




 Settings ▾ [+ VPN profile](#)

Name	Display name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL	Download XML
SASE-Certificate-Standard	SASE-Certificate-No-Mgmt-Tunnel-No-AlwaysOn	sase4all.com 3 IP Pools TLS / DTLS	Certificates	Connect to Secure Access 1 Exception(s)	12 Settings	0b00.vpn.sse.cisco.com/SASE-Certificate-Standard 	 ...


VPN Profiles

A VPN profile is a configuration that provides your remote devices with the means to securely connect to your network through a VPN. This configuration includes options for custom attributes and a machine tunnel. [Help](#)

 A region has been added to or deleted from IP Pool Configurations. Download the XML files associated with each VPN profile, which contain updated region information.

 Settings ▾

+ VPN profile

Name	Display name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL	Download XML
SASE-Certificate-Standard	SASE-Certificate-No-Mgmt-Tunnel-No-AlwaysOn	sase4all.com 3 IP Pools TLS / DTLS	Certificates	Connect to Secure Access 1 Exception(s)	12 Settings	0b00.vpn.sse.cisco.com/SASE-Certificate-Standard	 ...



General settings

Default Domain: sase4all.com | DNS
Server: 0 | Protocol: TLS / DTLS



Authentication, Authorization, and Accounting

Single Certificate



Traffic Steering (Split Tunnel)

Connect to Secure Access | 1
Exceptions



Cisco Secure Client Configuration

Step 2. Configure Private Resources



Home



Experience
Insights



Connect



Resources



Secure



Monitor



Admin



Workflows

Private Resources

Private Resources are applications, networks, or subnets that your organization controls access to. You must configure a private resource if you plan to allow end users to connect to the resource using zero-trust.

[Private Resources](#) [Private Resource Groups](#)

Private Resources

1 Private Resource

Private Resource	Private Resource Group	Connection Method	Connector Groups	Accessed by	Rules
OneSASE Webserver 1	-	VPN	-	0	4

OneSASE Webserver 1

VPN

Resource Address

Internally reachable address 10.60.50.180

Protocol Any

Port Any

DNS Server -

Endpoint Connection Method

Client-based ZTA

State OFF

Browser-based ZTA

State Unavailable

VPN

State ON

[Edit Private Resource](#)

OneSASE Webserver 1

VPN

Resource Address

Internally
reachable address

10.60.50.180



Protocol

Any

Port

Any

DNS Server

-

Endpoint Connection Method

Client-based ZTA

State OFF

Browser-based ZTA










State Unavailable

VPN

State ON

Edit Private Resource >


Step 3. Create a rule for VPN traffic

- 
-  Home
-  Experience Insights
-  Connect
-  Resources
-  Secure
-  Monitor
-  Admin
-  Workflows

Access Policy

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. [Help](#)














[Rule Defaults and Global Settings](#)

 Filters 1 [Reset all](#)

[Add Rule](#)

3 Results

[Customize view](#)

<input type="checkbox"/>	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	
<input type="checkbox"/>	8	Sean VPN Access Rule	Private	 Allow	Sean Reagan ...	OneSASE Webs...		-		
<input type="checkbox"/>	11	Sean - Test Vcenter	Private	 Allow	Sean Reagan ... +1	vcenter +1		-		
<input type="checkbox"/>	12	Sean- Test-RDP	Private	 Allow	Sean-W11-SAS... +1	Boston-OnPre...		-		

Rows per page 100 < 1 >

0 result from Default Access Rules ⓘ

Rule name	Action	Sources	Destinations	Security	Posture	
-----------	--------	---------	--------------	----------	---------	---



Rule name

Sean VPN 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**.

Sean Reagan (sean@sase4all.com) ×

To

Specify one or more **destinations**.

OneSASE Webserver 1 ×

Endpoint Requirements

For VPN connections:



End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. ⓘ

Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#)

For Branch connections:



Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

Rule name

Sean VPN 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) Rule Defaults

☒ Enabled

Traffic will be decrypted and inspected based on the selected IPS profile. [Help](#)

Profile: **Balanced Security And Connectivity** | Intrusion System Mode: **Prevention** | Signatures: 9490 Block 488 Log Only 41358 Ignore

Security Profile Rule Defaults

The following security settings will apply to traffic that matches this rule. [Help](#)

Security Profile: **None** | File Inspection: **Disabled** | File Type Blocking: **Disabled**

[Cancel](#)

[Back](#) [Save](#)

Summary



Sources

Sean Reagan (sean@sase4all.com)

Allow

Security Controls

Destinations

Private Resources

- OneSASE Webserver 1

Cisco Secure Access- User Anywhere

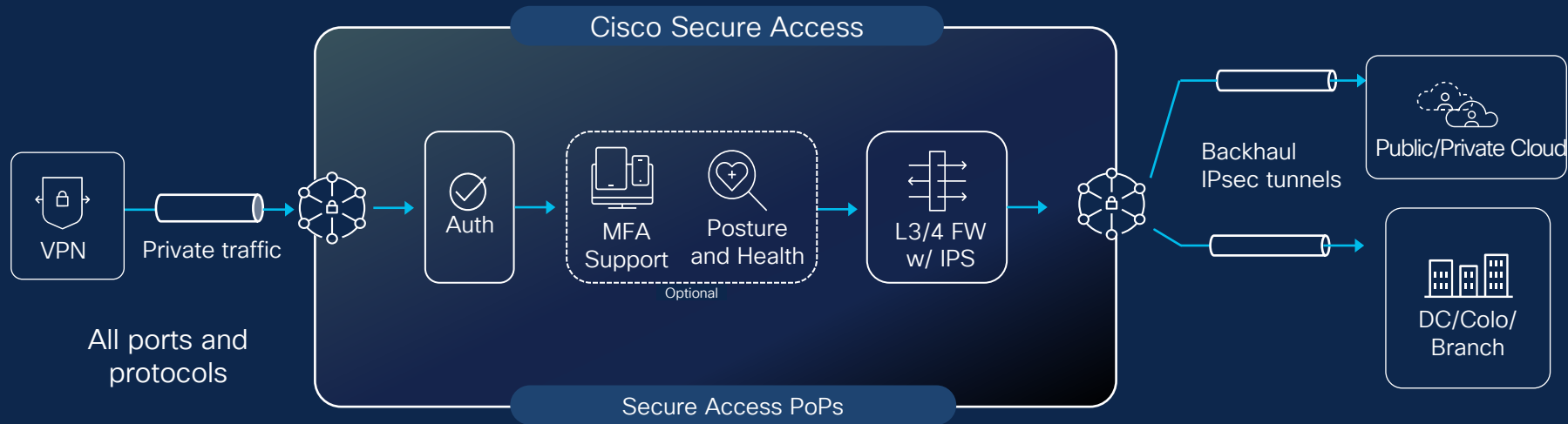
STEP 1
Log In

STEP 2
Securely start work



Easy, frictionless user experience

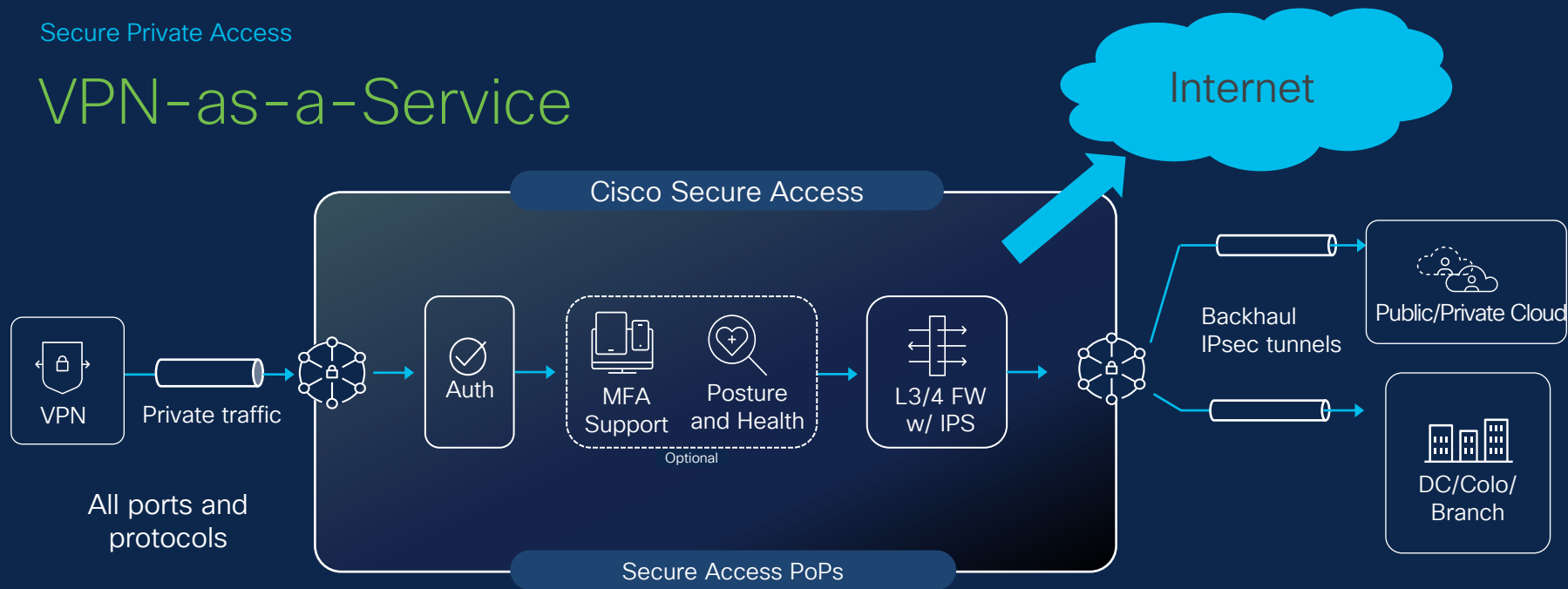
VPN-as-a-Service



- Authentication Methods:
SAML 2.0, SAML+ certificate, Certificate, RADIUS
- Identity based access
- Region specific IP pool for client addressing

- Posture Verification: (optional)
Secure Firewall (formerly hostscan) or ISE with RADIUS
- IPS (optional)
- Connection profiles

VPN-as-a-Service



- Authentication Methods:
SAML 2.0, SAML+ certificate, Certificate, RADIUS
- Identity based access
- Region specific IP pool for client addressing

- Posture Verification: (optional)
Secure Firewall (formerly hostscan) or ISE with RADIUS
- IPS (optional)
- Connection profiles

Agenda

- What is Secure Access?
- Use case 1 – Secure Internet Access
- Use case 2 – VPN as a service
- Use case 3 – Zero Trust Network Access
- Use case 4 – Terminal Services replacement
- Conclusion/Q&A

Cisco Secure Access- User Anywhere

STEP 1
Log In

STEP 2
Securely start work



Easy, frictionless user experience

Cisco Secure Client

Suite of security service enablement modules



AnyConnect VPN (Core)

ZTA Module

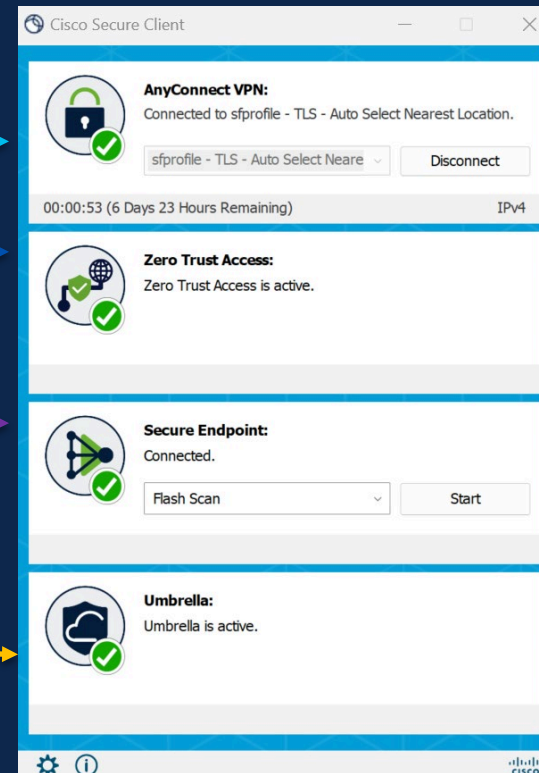
Secure Endpoint (AMP)

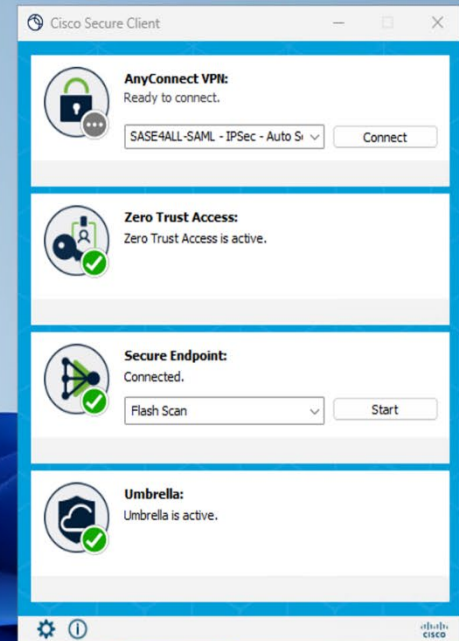
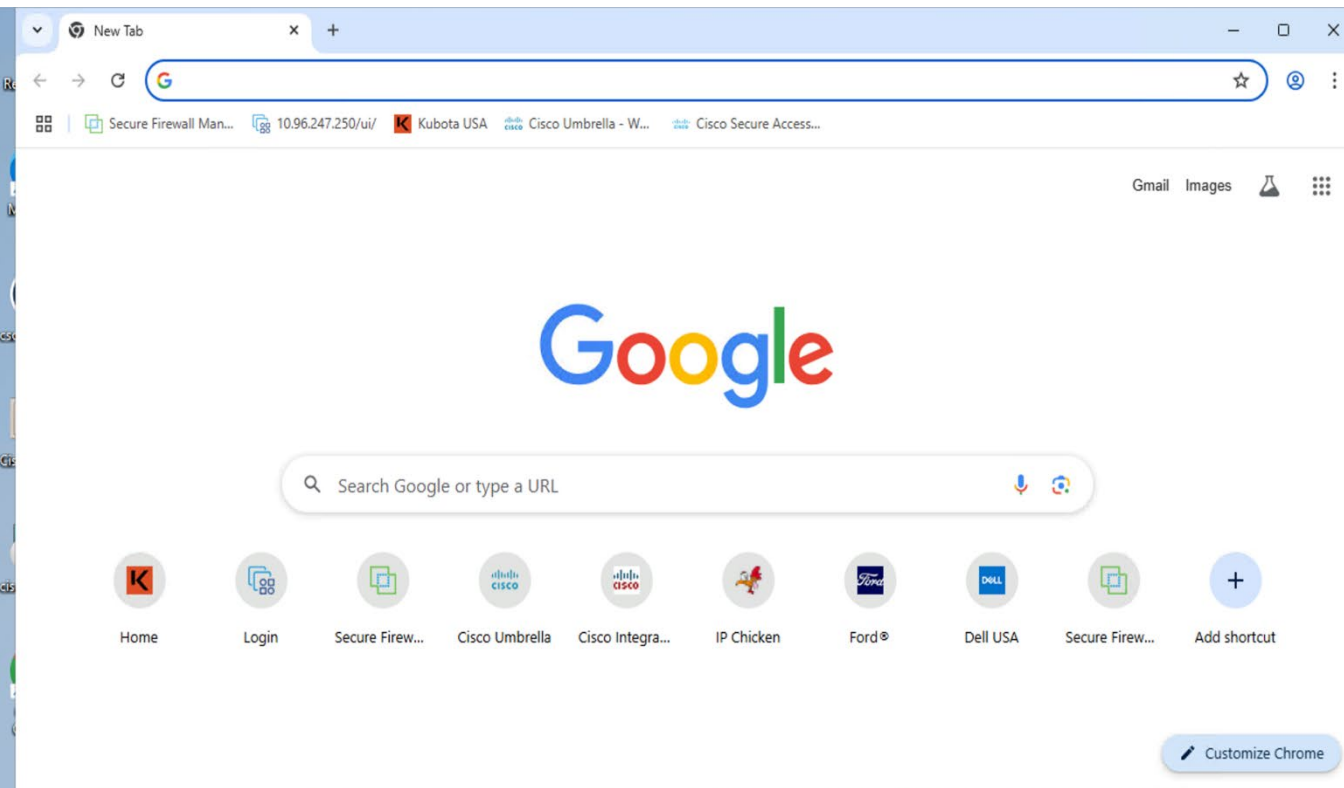
Roaming Module

Thousand Eyes (No UI)

Cloud Management Module (No UI)

Diagnostic and Reporting (DART)





66°F
Partly sunny



Search



1:17 PM
4/23/2025

Status: Running

cisco *Connect*



Zero Trust Access:
Zero Trust Access is active.

<https://fmc-1234567.ztna.sse.cisco.io>





Google

<https://fmc-1234567.ztna.sse.cisco.io>

Secure Proxy Management Center

Username:

Password:

-  **John Doe**
john.doe@company.com
-  **Jane Smith**
jane.smith@company.com
-  **Mike Johnson**
mike.johnson@company.com
-  **Sarah Lee**
sarah.lee@company.com



Secure Firewall Management Center

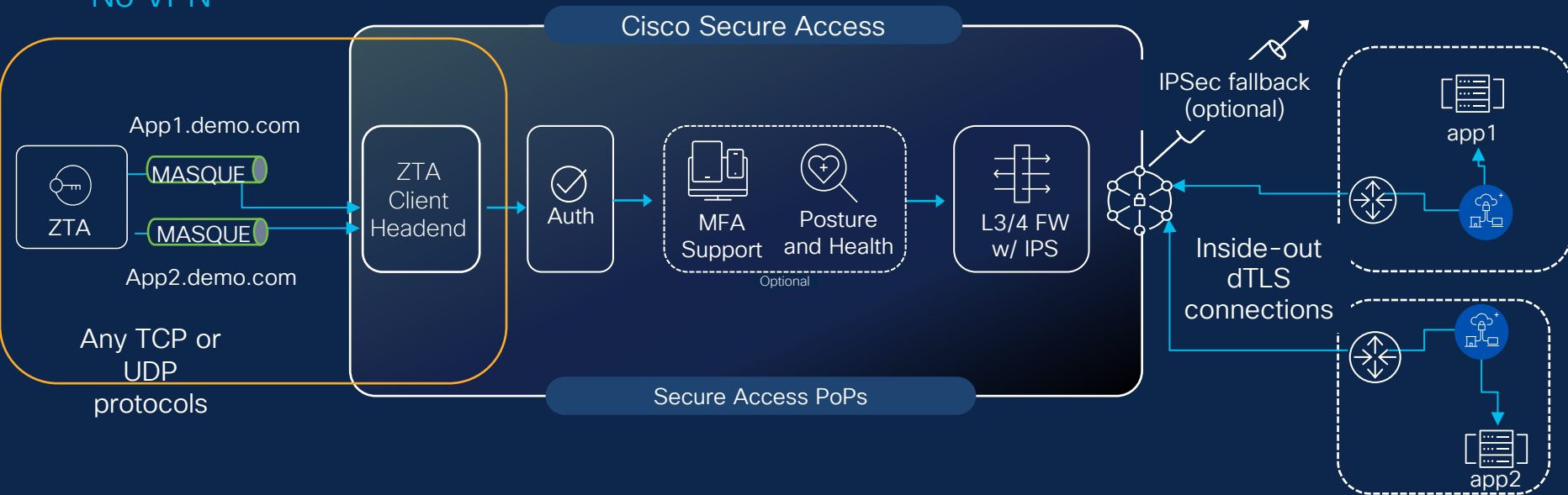
Username

Password

[Single Sign-On \(SSO\)](#)

Client-based Zero Trust Access

No VPN



- 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

Step 1 – Define the Private Resource

Secure Access

Home

Experience Insights

Connect

Resources

Secure

Monitor

Admin

Workflows

Private Resources

Private Resources are applications, networks, or subnets that your organization controls access to. You must configure a private resource if you plan to allow end users to connect to the resource using zero-trust.

Private Resources

Private Resource Groups

Private Resources

FMC

Private Resource Group

Client-based ZTA

1 Private Resource

Private Resource	Private Resource Group	Connection Method	Connector Groups	Accessed by	Rules
FMC	CHICAGO-APPS	<div>Client-based ZTA</div> <div>Browser-based ZTA</div>	2	2	3

FMC

Client-based ZTA

Browser-based ZTA

Internally reachable address

fmc.sase4all.local

Protocol

http/https

Port

443

DNS Server

Route53 A (10.60.0.2)

Endpoint Connection Method

Client-based ZTA

State

ON

User Reachable Address

fmc.sase4all.local

Browser-based ZTA

State

ON

External URL

https://fmc-8...

Protocol

https

Server Name Indication

-

Test Reachability

Edit Private Resource

CISCO Connect

Resource Address

**Internally
reachable address**

fmc.sase4all.local



Protocol

http/https

Port

443

DNS Server

Route53 A (10.60.0.2)

Endpoint Connection Method

Client-based ZTA

State

ON

**User Reachable
Address**

fmc.sase4all.local



Step 2 – Create a rule

Rule name

Sean test FMC 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**.

Sean Reagan (sean@sase4all.com) ×



To

Specify one or more **destinations**.

FMC ×

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)



Zero-Trust Client-based Posture Profile

Rule Defaults

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

Profile: **System provided (Client-based)** | Requirements: **Operating System, Firewall, Endpoint security agent, Disk encryption**

Private Resources: **FMC**

Rule name

Rule order

Sean test FMC rule

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)

Rule Defaults

Traffic will be decrypted and inspected based on the selected IPS profile. [Help](#)

Profile: **Balanced Security And Connectivity** | Intrusion System Mode: **Prevention** | Signatures: 9490 Block 488 Log Only 41358 Ignore

Security Profile

Rule Defaults

The following security settings will apply to traffic that matches this rule. [Help](#)



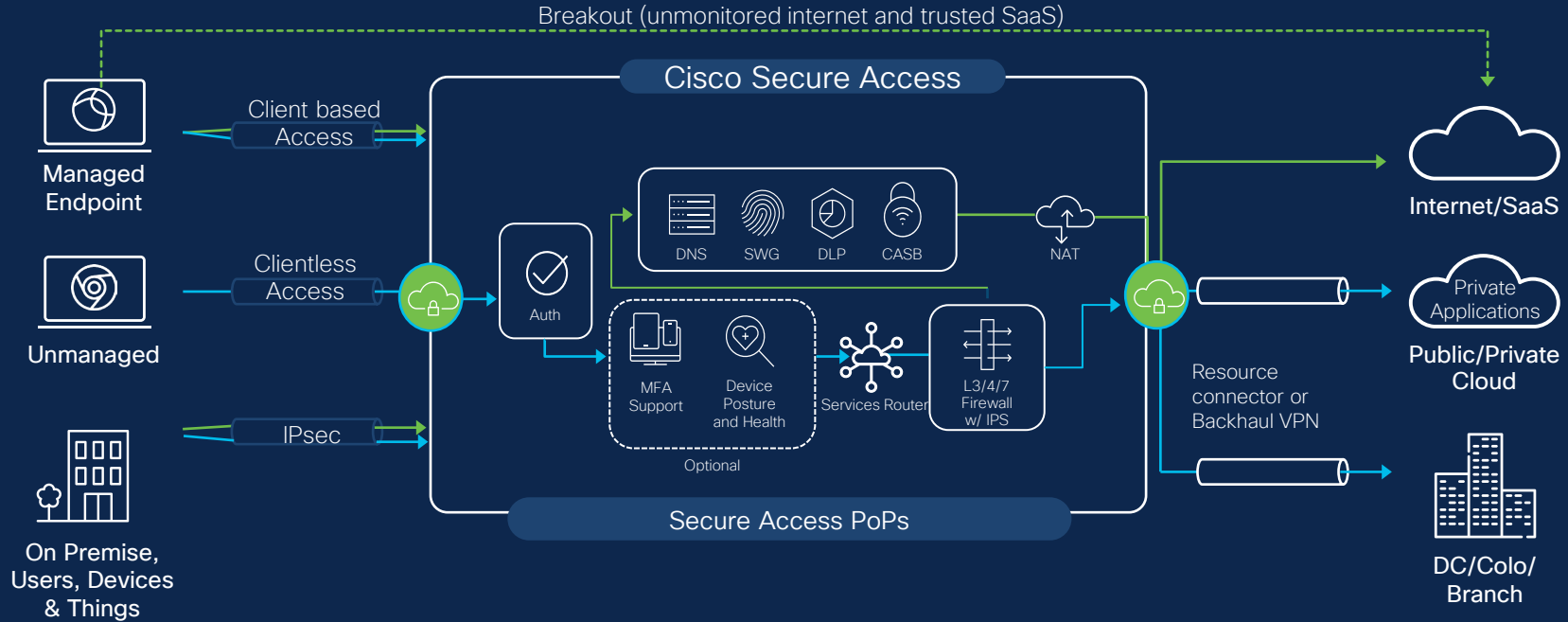
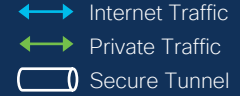
<input type="checkbox"/>	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	
	<input type="checkbox"/> Sean test block	Internet	Block	Sean Reagan ... +1	2 IP Address/CIDR AND 1 Services ⓘ		334		...
	<input type="checkbox"/> Sean test FMC rule	Private	Allow	Sean Reagan ...	FMC		-		...
	<input type="checkbox"/> Sean VPN Rule	Private	Allow	Sean Reagan ...	OneSASE Webs...		-		...
	<input type="checkbox"/> Sean 161 Internet	Internet	Allow	Sean-W11-Okt... +1	Any		932.4k		...
	<input type="checkbox"/> Sean-RBI	Internet	Isolate	Sean-W11-SAS... +1	Generative A... +2		-		...
	<input type="checkbox"/> Sean-Test-Web	Internet	Allow	Sean-W11-SAS... +2	Any		302		...
	<input type="checkbox"/> Sean - Test ZTA Apps	Private	Allow	Sean Reagan ... +1	vcenter +1		-		...
	<input type="checkbox"/> Sean- Test-RDP	Private	Allow	Sean-W11-SAS... +1	Boston-OnPre...		-		...

The user connects to their application.
They have no idea how, it just works!

Do I always need that Zero-Trust Client module to do these kind of things?

NO!

Architecture Overview



☒ **Client-based connection**

Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

fmc.sase4all.local

[+ FQDN or IP Address](#)

☒ **Browser-based connection**

Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when devices that your organization does not manage must connect to this resource. Fewer endpoint security checks are possible.

Public URL for this resource ⓘ

You will give the selected address to browser-based users.

☒ Use a URL in a Cisco domain

https:// fmc -8206406.ztna.sse.cisco.io

Provide a URL prefix that uniquely identifies this resource.

☐ Use a URL in your domain

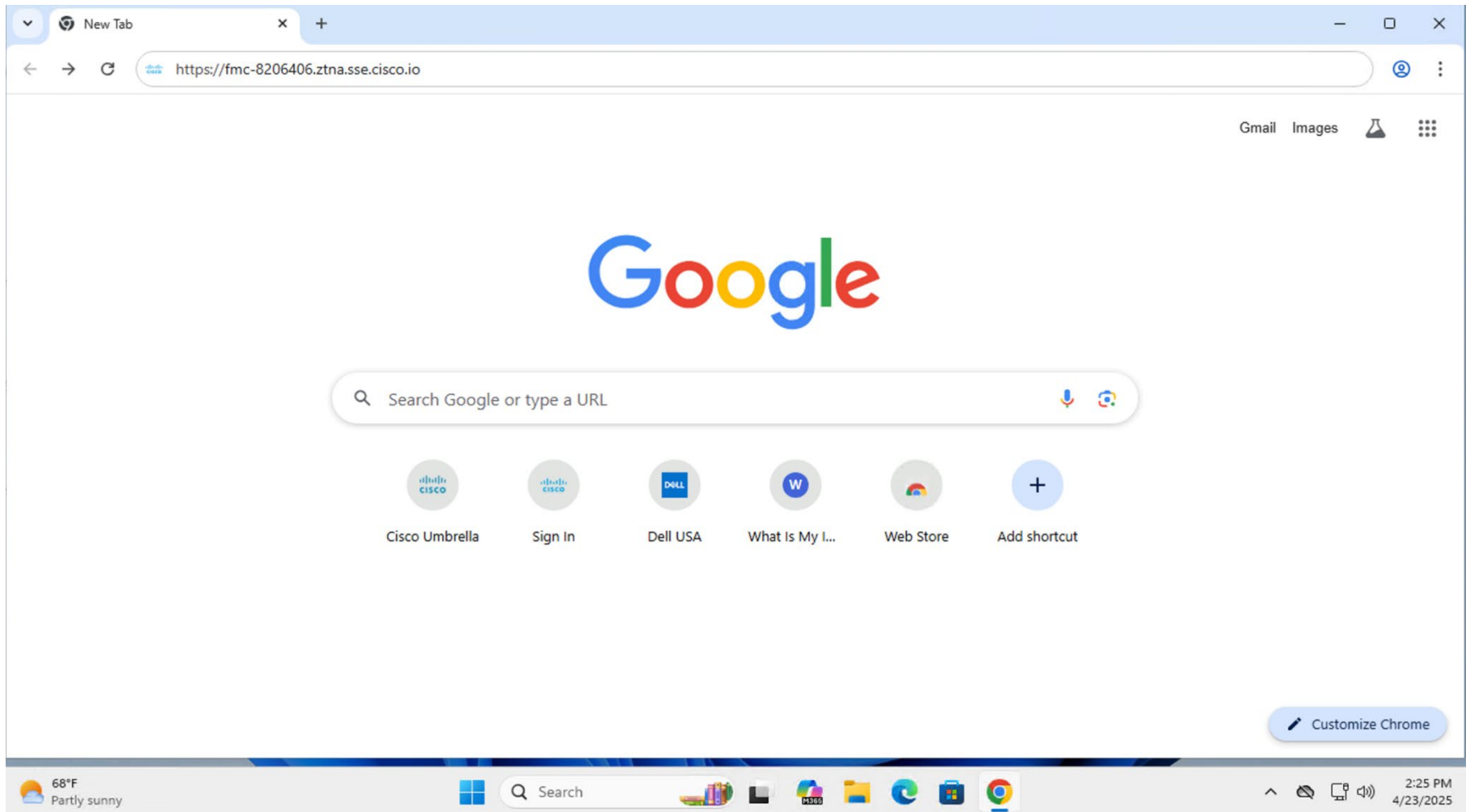
Protocol

Custom host header (optional) ⓘ

Server Name Indication (SNI) (optional) ⓘ

HTTPS ▾

☐ **Validate Application Certificate** ⓘ





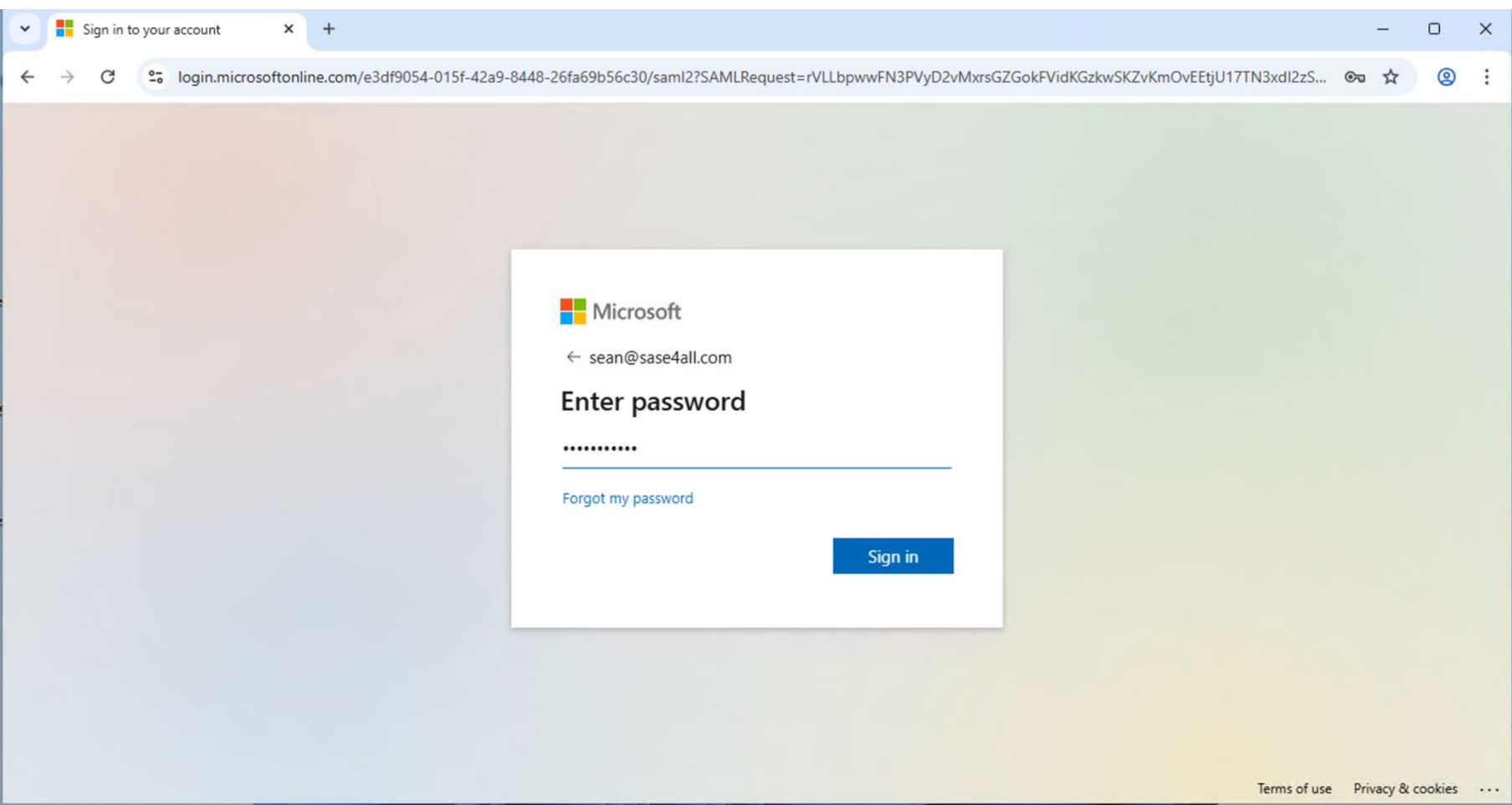
Cisco Secure Access

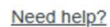
Sign In

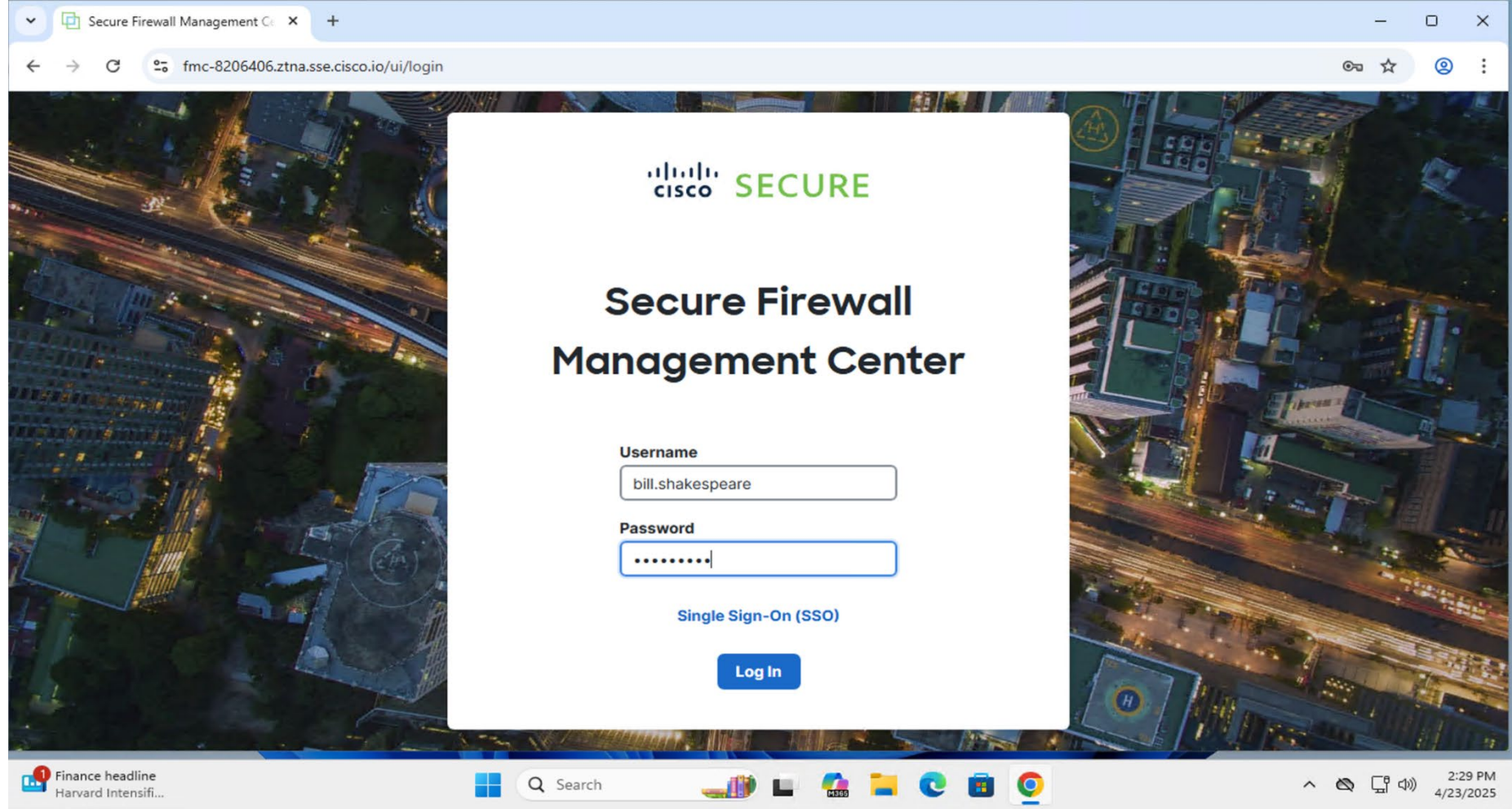
Use the username provided by your organization to sign in.

Username

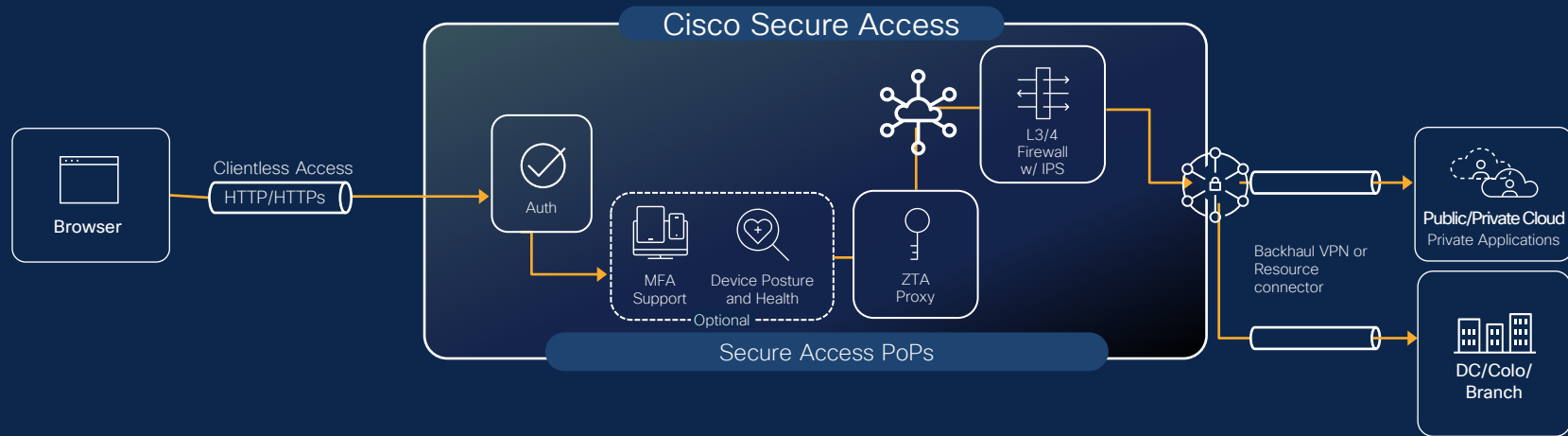
Sign In







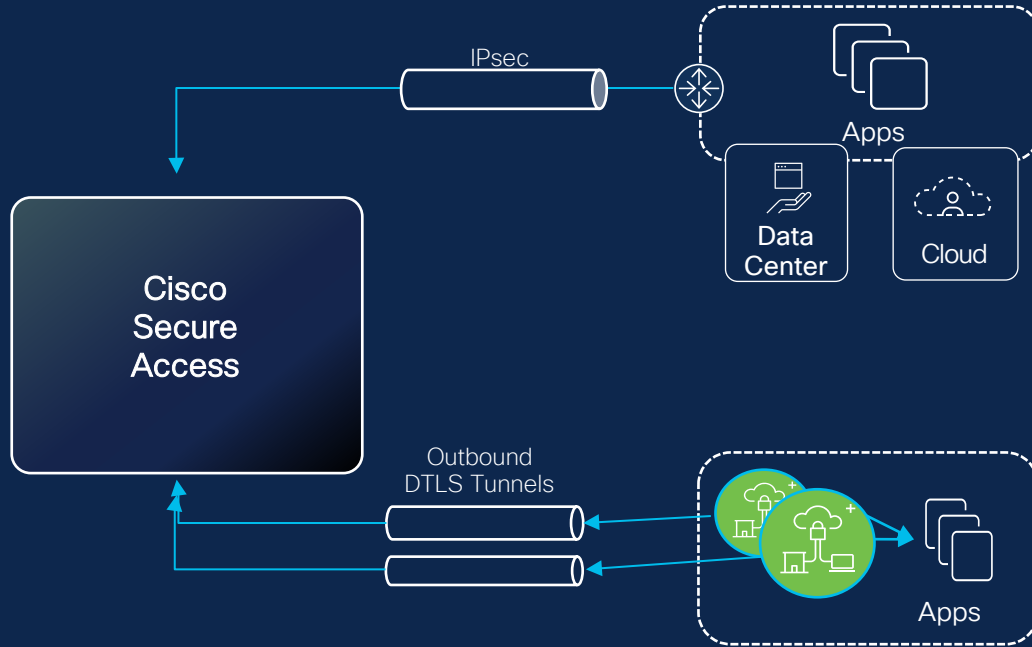
Clientless Zero Trust Access



- Ideal for unmanaged devices and BYOD use-cases
- Automatically generated publicly resolvable FQDN for per app access

- Posture (optional) verification based on HTTP headers
- SAML authentication

Apps: Private Applications



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
- Supported in AWS, Azure, Docker and VMWare

Agenda

- What is Secure Access?
- Use case 1 – Secure Internet Access
- Use case 2 – VPN as a service
- Use case 3 – Zero Trust Network Access
- Use case 4 – Terminal Services replacement
- Conclusion/Q&A

Why do we use VDI / Terminal Services?

Industry's most comprehensive SSE solution

SSE Core Capabilities

So much more

Enterprise Browser Integration

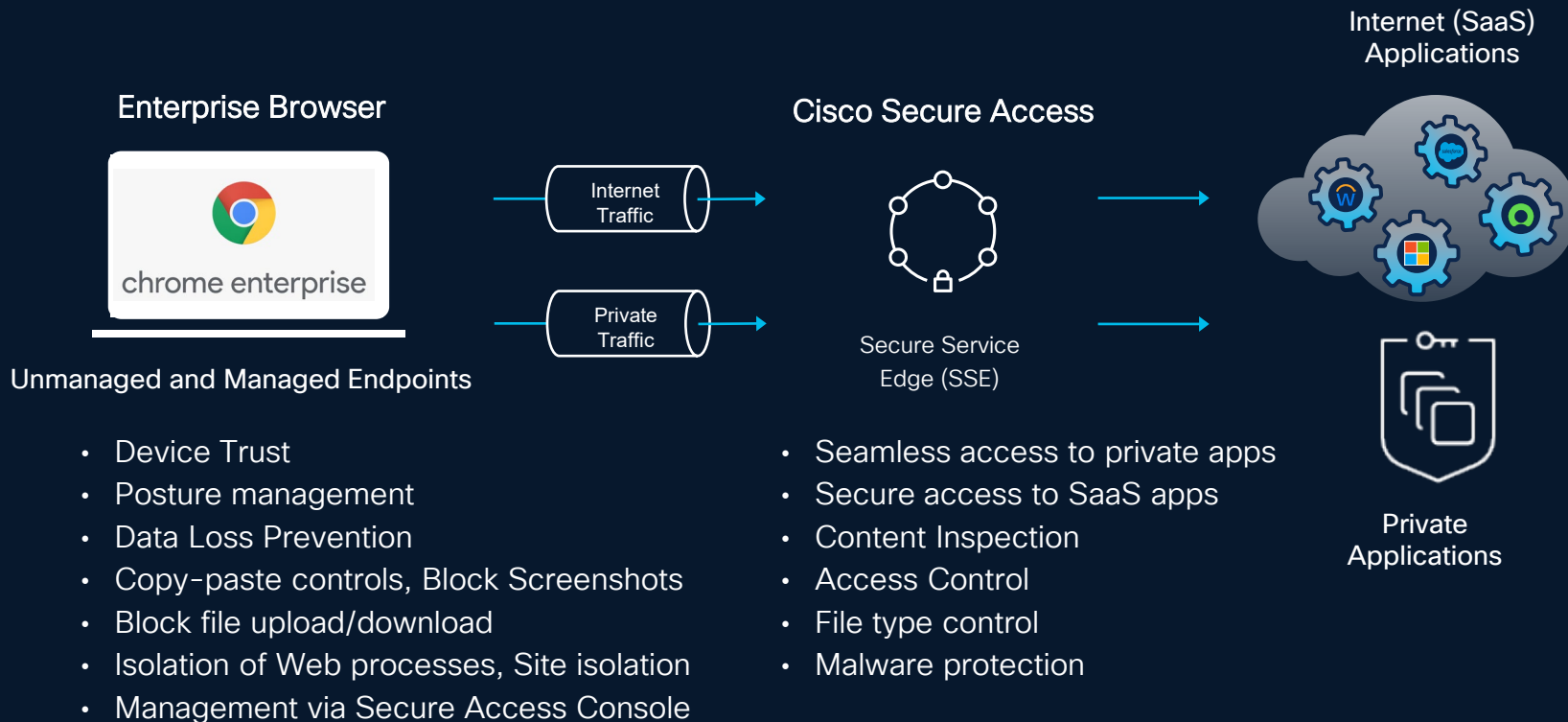
AI-powered Platform

Enterprise Browser Use cases

- Unmanaged device with managed profile based on identity
- VDI replacement using Enterprise Browser and Secure Access
- 3rd party/consultant/contractor/partner access to private apps
- Corporate approved browser controls

Secure Access with Enterprise Browser






Zero Trust Access to Private Apps and Internet Apps



Cisco and Google Enhance Zero Trust Access



Chrome

-  Google Safe Browsing
-  Extension Security
-  Sandboxing & Auto Updates
-  Password Manager
-  Local policy controls

Chrome Enterprise Core

-  Extension Management
-  Compliance & Data Regions
-  Fleet risk management
-  Managed profiles and BYOD
-  Reporting and Insights
-  Centralized policy controls
-  Enterprise integrations

Chrome Enterprise Premium

-  Data Loss Prevention
 -   Print
 -  File Uploads & Downloads
 -  Copy & Paste Controls
-  Threat Protection
 -   URL Filtering
 -  Evidence Locker
 -  Phishing
 -  Malware
-  Security Insights and reporting
 -   Security Events
 -  Sensitive Data Loss
 -  Content Transfer
-  Access Control
 -   30+ Device Signals
 -  Zero Trust
 -  Partner Signals
 -  Context Aware Access for SaaS & Private Web Apps

Joint Solution Use Cases

Copy/Paste Controls
Local File Download/Upload Controls
Print Control
Screenshot Control
Watermark Control
Sanctioned/Unsanctioned Application control
Site/Tab Browser Isolation
And more

Enterprise Browser – User experience



Agenda

- What is Secure Access?
- Use case 1 – Secure Internet Access
- Use case 2 – VPN as a service
- Use case 3 – Zero Trust Network Access
- Use case 4 – Terminal Services replacement
- Conclusion/Q&A

Cisco Secure Access

Converged cloud-native security grounded in zero trust



Remote

Campus

Branch

Airplane

Oil rig

Stadium

Field

...



Thank you!

Sean Reagan
Solutions Engineer
Security Incubation
sereagan@cisco.com

CISCO *Connect*

#CiscoConnect