

# Cisco Secure Access

Gerard van Bon  
gvanbon@cisco.com



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Security | 1

Cisco Confidential

# SASE/SSE approach is the technology foundation

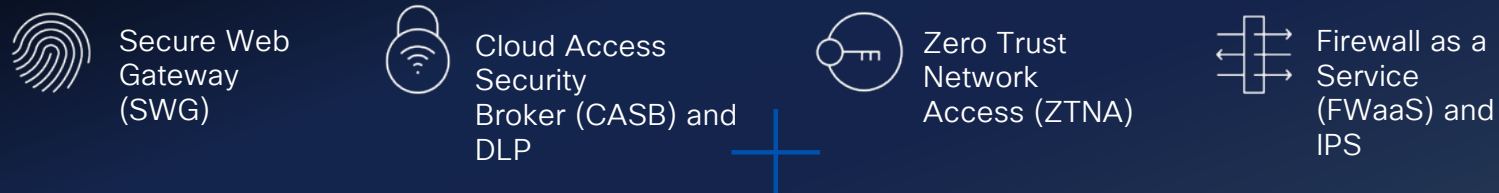
Fundamental to your security strategy for a hyper-distributed world



# Cisco Secure Access

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

## Core SSE



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

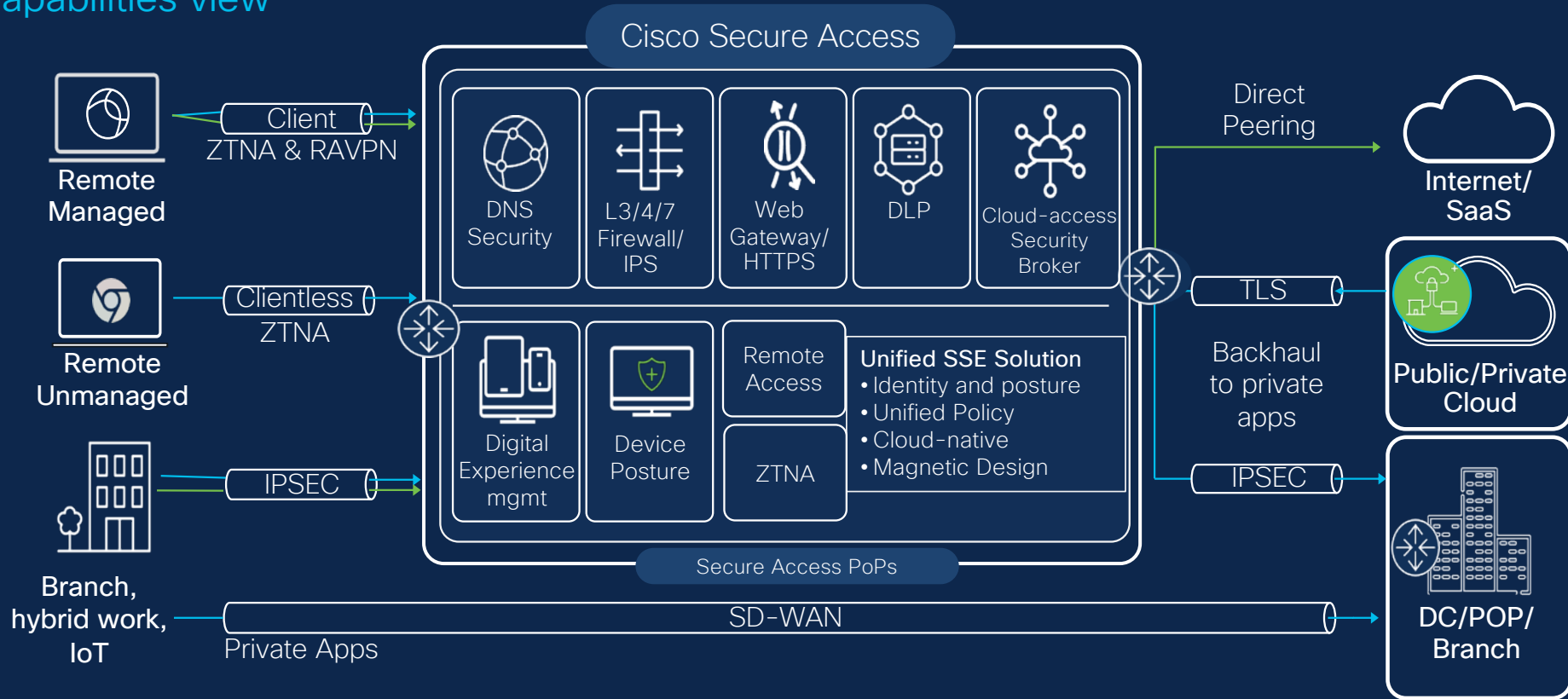


## Add-on solutions



# Cisco Secure Access

## Capabilities view



Users

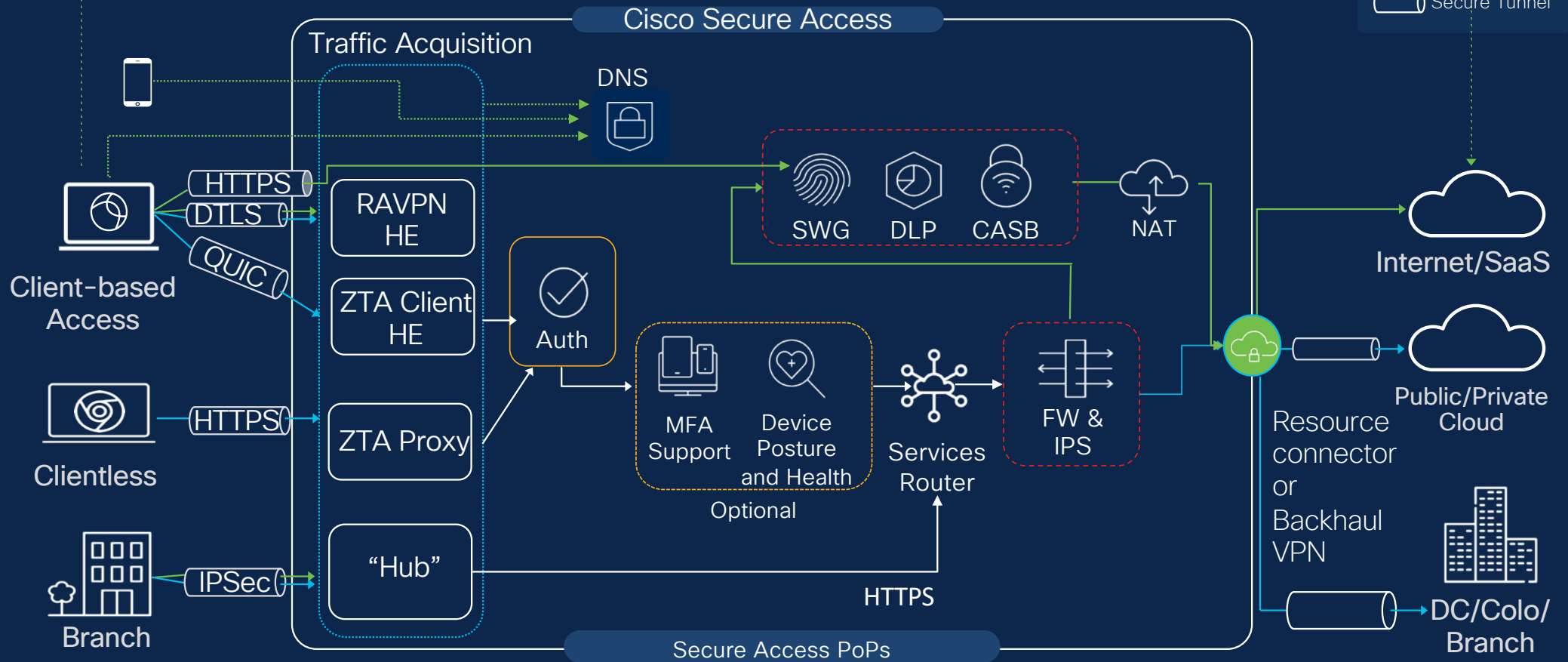
Secure Access

Apps



# Secure Access Architecture Overview

Breakout (unmonitored internet and trusted SaaS)



Users

How

Apps



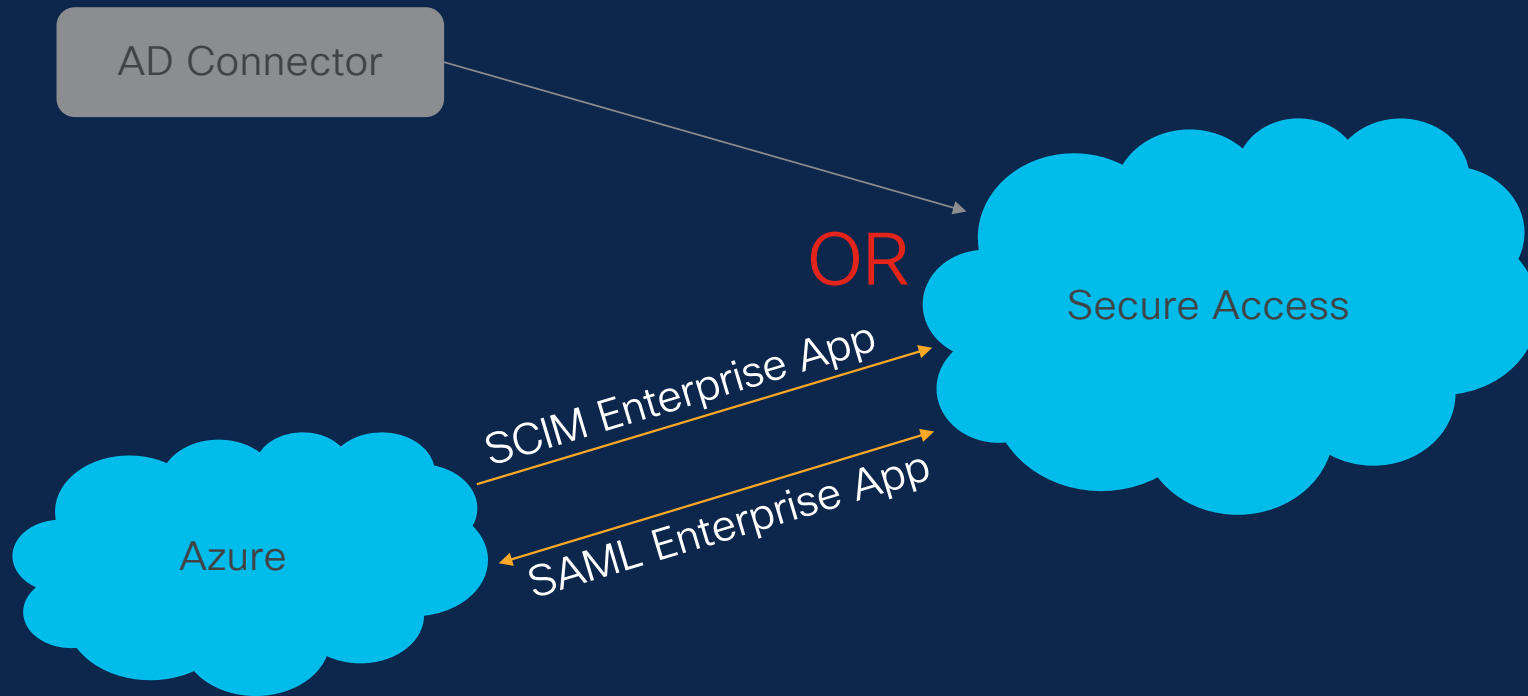
# Secure Private Access



# User provisioning



# User provisioning and authentication





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

### Users and User Groups

Manage your organization's users and user groups. To add new users and user groups, provision them through a supported identity provider. Once added, users and user groups can then be added to an access rule. [Help](#)

Users Groups

Configuration management

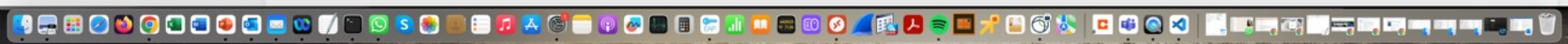
#### Users

Manage your organization's users and their devices connections and enrollments. To add new users, click Provision Users. At anytime, you can disconnect or unenroll a user's device. [Help](#)

21 results

Provision Users

Name	Email	Source	Connected(VPN)	Enrolled(ZTNA)	Associated Rules
Administrator	Administrator@lab.netcope.ch	onprem	0	0	0
Bart Van Hoecke	bart@24g6q3.onmicrosoft.com	azure	0	0	2
Cyrrill Meier	cymeier@lab.netcope.ch	onprem	0	0	0
Cyrrill Meier	cyrrill@24g6q3.onmicrosoft.com	azure	0	0	1
Gerard Van Bon	gerard@24g6q3.onmicrosoft.com	azure	0	0	2
Gerard van Bon	gvanbon@lab.netcope.ch	onprem	0	0	1
Gert Tilburgs	gert@24g6q3.onmicrosoft.com	azure	0	0	2
Hans Mathys	hans@24g6q3.onmicrosoft.com	azure	0	0	1
Hans Mathys	hmathys@lab.netcope.ch	onprem	0	0	0
HR	hr@lab.netcope.ch	onprem	0	0	0



Chrome File Edit View History Bookmarks Profiles Tab Window Help Tue 18 Jun 11:49

Cisco Secure Access

dashboard.sse.cisco.com/org/8219751/connect/users-and-groups/provisioning

Secure Access Gerard Van Bon (...)

← Users and Groups

### Provision Users and Groups

To add users to Secure Access, provision users through one of Secure Access's supported methods. [Help](#)

#### Provisioning Method

Select a provisioning method to add users to Secure Access.

#### Methods

- Identity provider (IdP)**  
Provision Users and Groups through a supported identity provider (IdP) service.
- Manual Upload**  
Manually upload users and groups exported from Active Directory.
- Active Directory**  
Connect Secure Access to your Active Directory and import your users and groups.

#### Choose Identity Provider

Select

- Azure
- Okta
- Other

Cancel Back Next

# Backhaul Connections

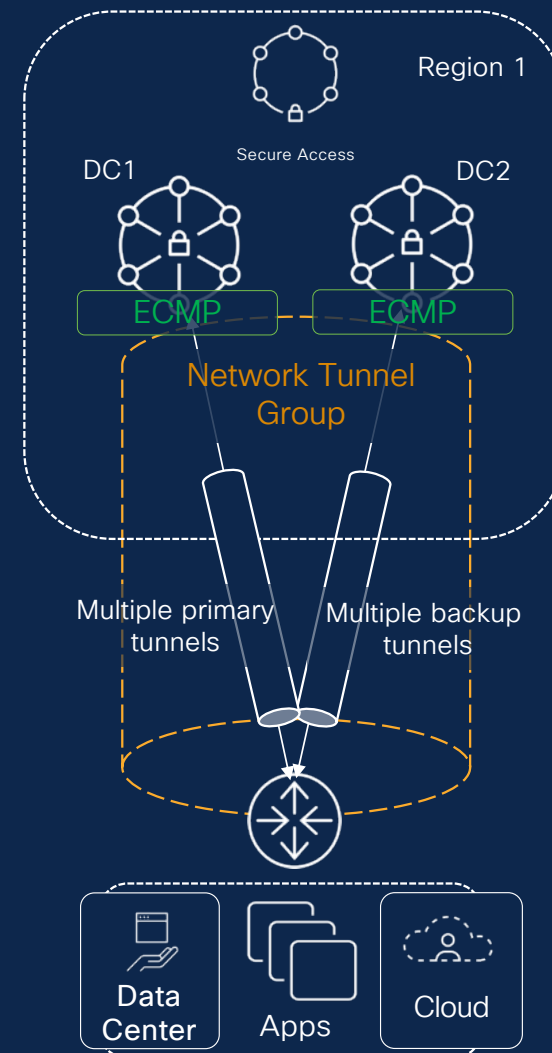


# IPsec

- Any IPsec capable device
- Network Tunnel Groups (NTGs)
  - A pair of IPsec tunnels
  - Connected to different pre-defined DCs
  - Within the same region
  - Provide intra-DC failover

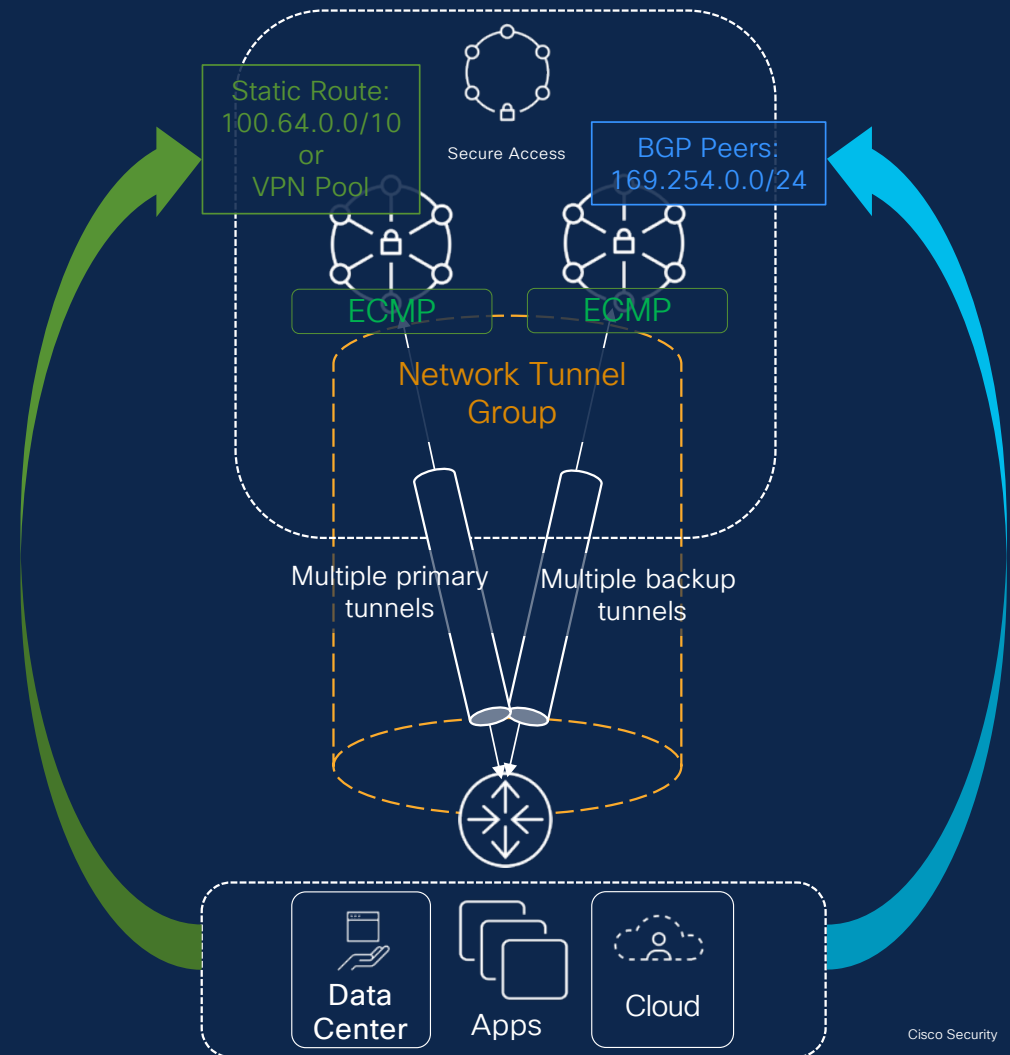
Platform	Support Version
Cisco ASA	v9.8
Cisco ISR-G2	15.4M3
Cisco FTD	6.4+ (6.7 when using VTI)
Cisco Meraki MX	15.3

<https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters>



# Routing and Failover

- Static routing
  - Secure Access uses CGNAT
  - 100.64.0.0/10 for ZTNA
  - VPN pool for AnyConnect
- Border Gateway Protocol (BGP)
  - Peers are 169.254.0.0/24
- ECMP enable by default
  - Equal cost across NTG
  - No dashboard config
  - No flow stickiness
- 1G per tunnel capacity
  - Use multiple tunnels to increase
- Failover
  - IKE Dead Peer Detection
  - BGP keepalive/hold-down timers



# Network Tunnel Group Example

## AWSWest2

Review and edit this network tunnel group. Details for each IPsec tunnel added to this group are listed including which tunnel hub it is a member of. [Help](#)

### Summary

<span>Connected</span>	
Region	US (Virginia)
Device Type	ISR
Routing Type	Dynamic Routing (BGP)
Device BGP AS	65003
Peer (Secure Access) BGP AS	64512
BGP Peer (Secure Access) IP Addresses	169.254.0.9, 169.254.0.5
Last Status Update	Mar 10, 2024 8:41 PM

### Primary Hub

<span>Hub Up</span>	
1 Active Tunnels	
Tunnel Group ID	awswest2@8174213-616864291-sse.cisco.com
Data Center	sse-use-1-1-1
IP Address	44.217.195.188

### Secondary Hub

<span>Hub Up</span>	
1 Active Tunnels	
Tunnel Group ID	awswest2@8174213-616864292-sse.cisco.com
Data Center	sse-use-1-1-0
IP Address	35.171.214.188

### Network Tunnels

Review this network tunnel group's IPsec tunnels. [Help](#)

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update
<a href="#">Primary 1</a>	327681	54.203.107.49	sse-use-1-1-1	44.217.195.188	<span>Connected</span>	Mar 10, 2024 8:41 PM
<a href="#">Secondary 1</a>	196612	54.203.107.49	sse-use-1-1-0	35.171.214.188	<span>Connected</span>	Mar 10, 2024 8:41 PM

## Primary 1 (327683)

Connected

Data Center	Data Center IP Address	Peer Device IP Address
sse-use-1-1-1	44.217.195.188	52.39.130.113
Last Status Update		
Mar 21, 2024 3:29 PM		

### Traffic

Packets In	Bytes In
5.21 K	694.37 KB
Packets Out	Bytes Out
4.95 K	509.67 KB

### IPSec

State	Age	Integrity Algorithm
INSTALLED	2027 sec	—
Encryption Algorithm	Key Size	
AES-CBC-128	16	
SPI In	SPI Out	
1181648113	2206108016	

### IKE

State	Age	PRF Algorithm
ESTABLISHED	328886 sec	HMAC-SHA2-256
Encryption Algorithm	DH Group	
AES-CBC-256	ECP-384	
Initiator SPI In	Responder SPI In	
1084022175269336492	18348602232954430461	

### Routing

Routing Type

BGP

Client Routes

10.1.204.0/24, 10.1.205.0/24, 2.2.2.8/32, 173.37.58.32/27

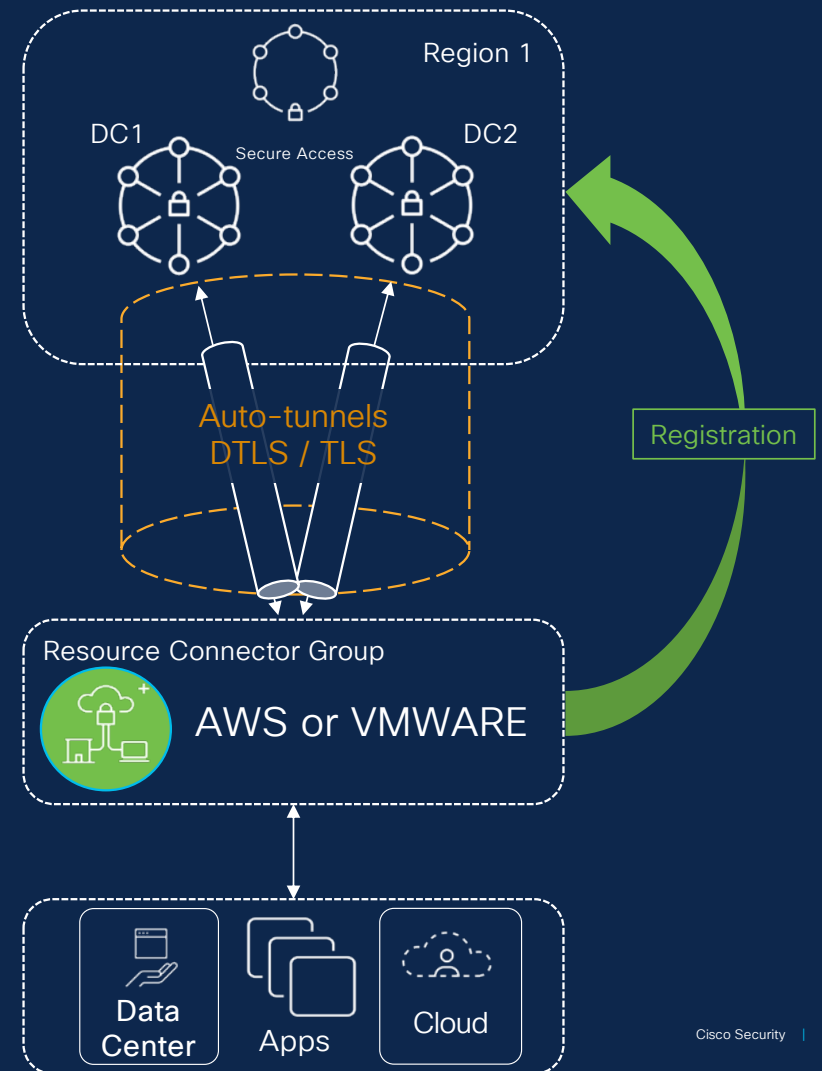
Cloud Routes

172.16.1.0/25, 100.122.8.2/32, 100.81.16.4/31, 100.96.3.16/28, 172.16.128.0/24, 10.1.202.0/24, 100.81.13.2/31, 100.96.11.0/28, 100.81.16.2/31, 172.17.0.1/32, 100.81.8.4/31, 0.0.0.0/0, 100.122.4.6/32, 100.96.3.0/28, 100.122.4.7/32, 100.81.13.4/31, 100.81.15.4/31, 172.17.0.10/32, 100.72.160.0/20, 100.81.9.2/31, 100.81.14.2/31, 100.96.2.16/28, 100.122.4.2/32, 100.96.11.16/28, 100.81.8.2/31, 100.96.5.0/28, 2.2.2.7/32, 100.81.15.2/31, 100.96.2.0/28, 100.96.15.16/28, 100.96.15.0/28, 100.122.8.7/32, 100.122.8.6/32, 100.96.10.0/28, 100.96.10.16/28, 10.1.200.0/24, 100.81.14.4/31, 100.81.9.4/31, 172.16.1.128/25, 100.96.5.16/28, 100.96.4.0/28, 100.96.4.16/28



# Resource Connector

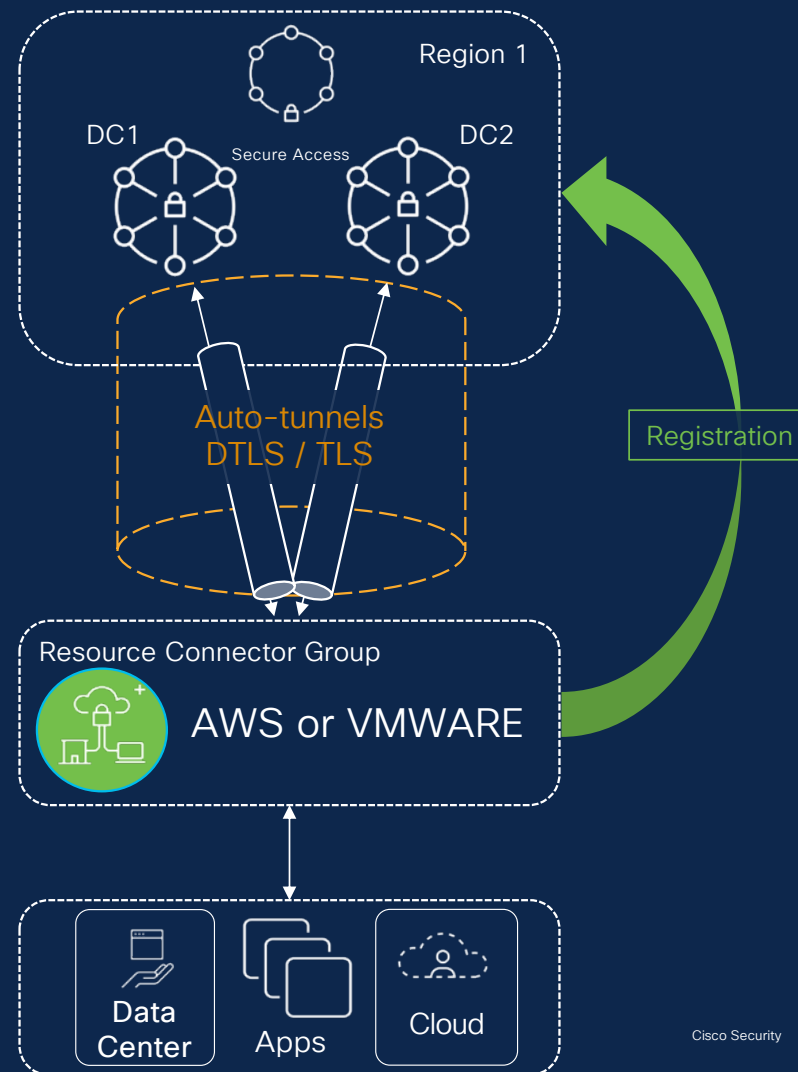
- Deployed in a group
  - Can be deployed with one member
- Virtual machines
  - AWS Marketplace (c5.xlarge only)
  - VMWare image (OVA)
  - Azure nearby roadmap
  - Intel x86\_64/AMD64 only
  - IPv4 only
- Registers with dashboard
  - Provisioning key
  - Manual confirmation
- Load balancing
  - Automatic across all in a group
  - Must be same instance type
  - Must be in same region



<https://docs.sse.cisco.com/sse-user-guide/docs/allow-resource-connector-traffic-to-secure-access>

# Resource Connector

- Scaling and Redundancy
  - Dashboard provides calculator
  - Based on 70% CPU and DTLS
  - 500 Mb/s at full capacity
  - 400 Mb/s at 70% load
  - With TLS 250 Mb/s throughput



**Scaling calculator**

For planning purposes, estimate the maximum volume of traffic that connectors in this group must handle:

0 2 4 6 8 10 12 14 16 18 20  
Throughput in Gbps

Estimated number of connectors to deploy in this connector group:

**11 x** instances (each with 2 CPU's and 4 GB RAM)

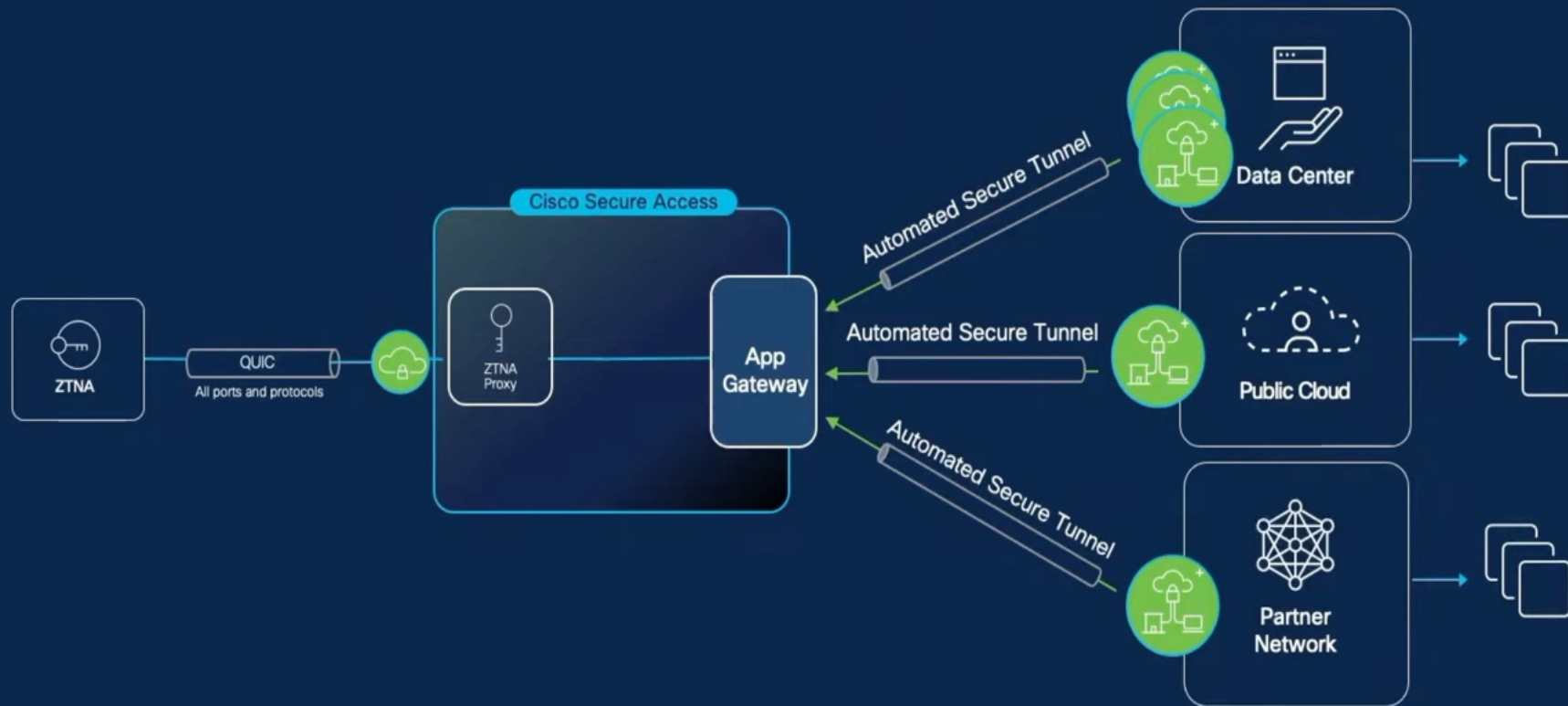
**Note:** This recommendation is based on 75% CPU load, includes 1 connector for redundancy, and assumes adequate network capacity.

You can deploy additional connectors at any time.

<https://docs.sse.cisco.com/sse-user-guide/docs/limitations-and-range-limits>



# Resource connector



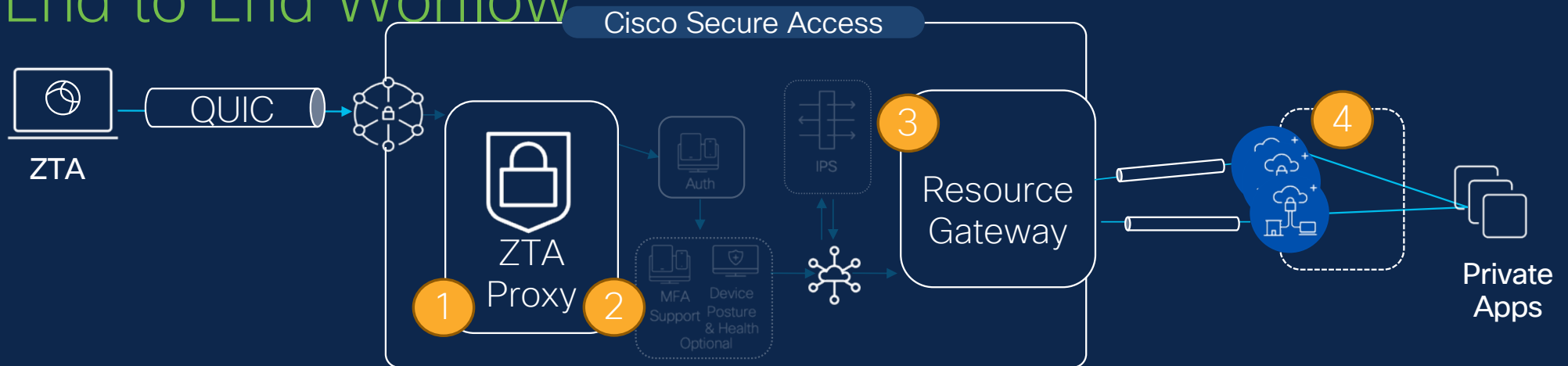
## Benefits

- Overlapping IPs support
- Intelligent connectivity
- Latency aware (future)
- Load aware (future)
- On demand authorization
- Cloud managed connectors

## Select Cisco Innovations

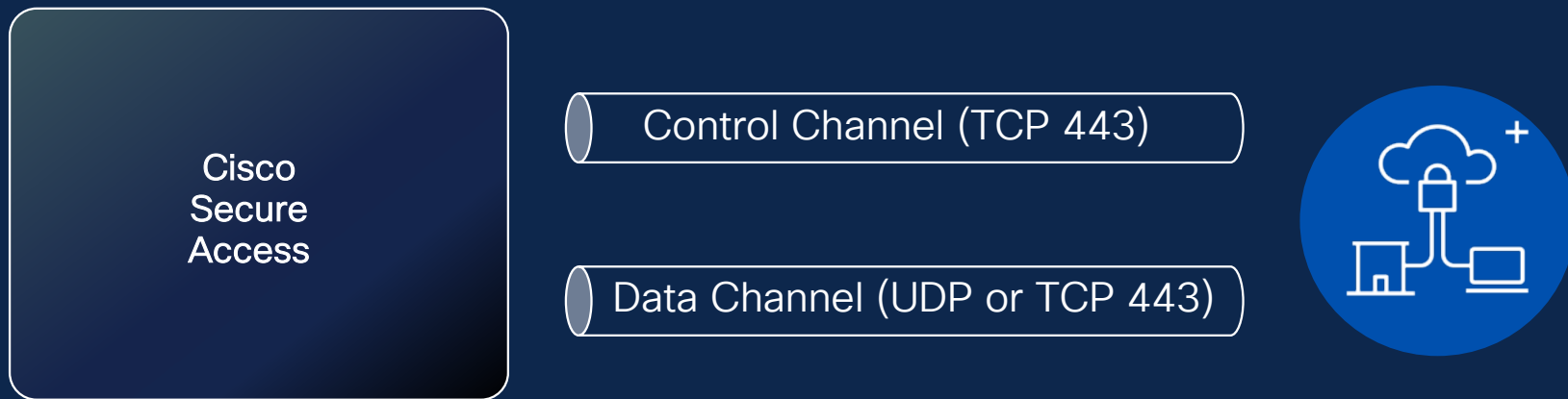
- Network isolation
- Invisible operations- no exposed IP, no over-the-internet DNS queries, no breadcrumbs or system leaks
- Standards-based, compatible with forthcoming mobile ZTNA clients

# End to End Workflow



1. Map destination to resource
2. Query resource gateway to see which connector group is serving traffic for the resource (latency based selection)
3. ZT Proxy forwards connection to app gateway which in turn load balances traffic to the selected connector in the group
4. Resource connector forwards traffic to the resource

# Resource Connector Communication Channels



Inside-out, Always On

Data: D(TLS) tunnels for application traffic

Control: MQTT over TLS

on-demand messages from controller to agent: upgrade, revoke, troubleshooting

Metrics: basic system and networks statistics, monitor status

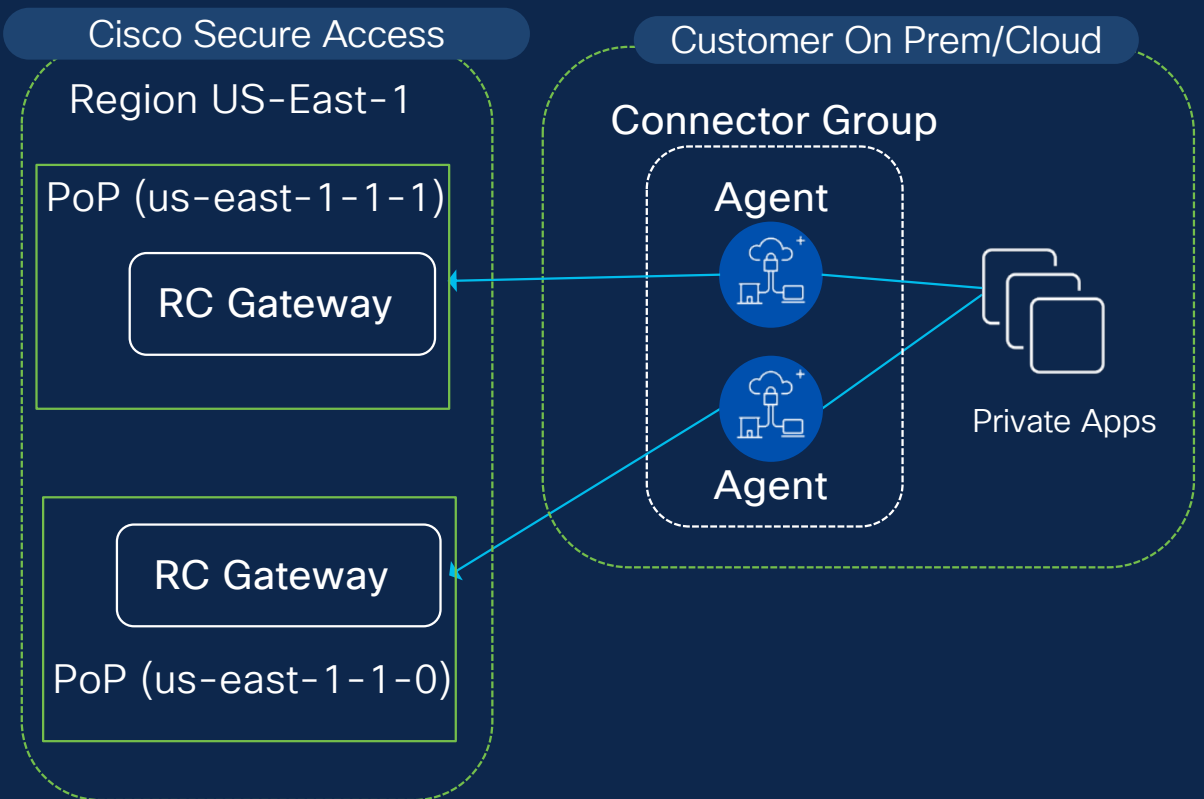
# Access rules for resource connectors to work

## Customer edge firewall rules

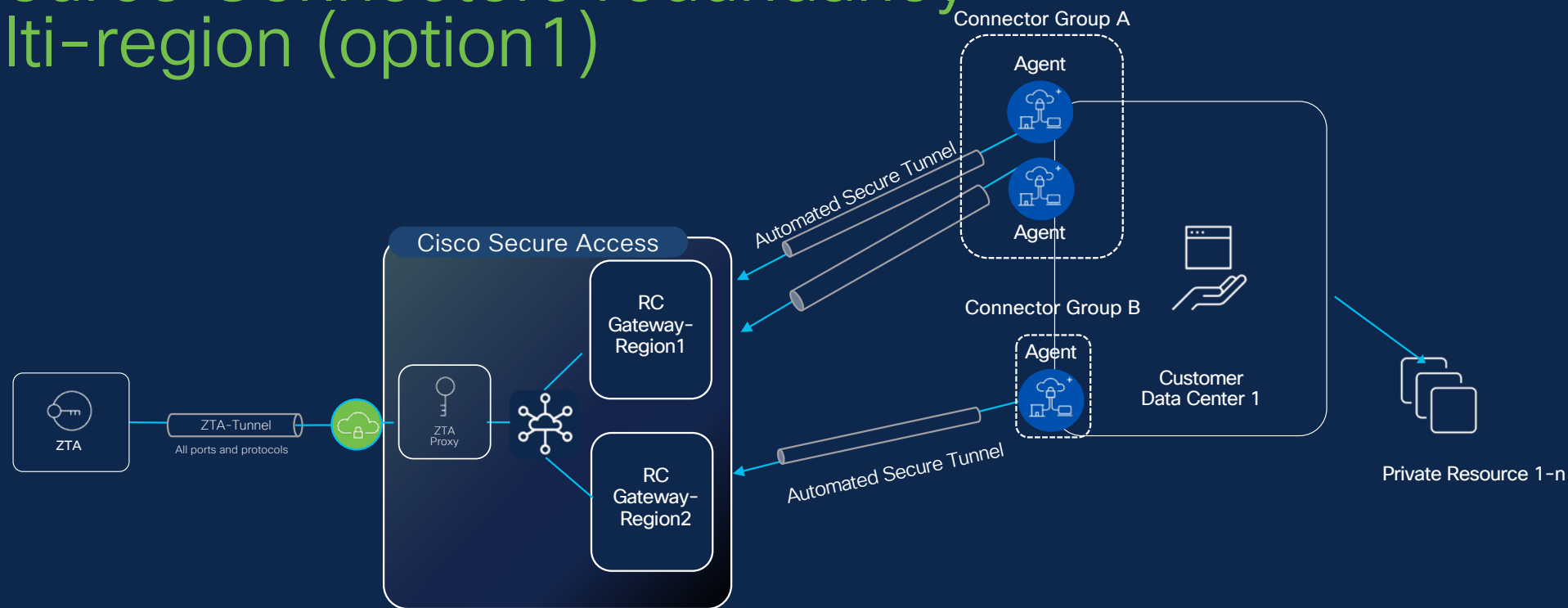
Secure Access Services	FQDN for Whitelisting	Port/Protocol
Gateway	Cisco IP Space	TCP/UDP 443
Controller	Us.controller.acgw.sse.cisco.com Eu.controller.acgw.sse.cisco.com Ap.controller.acgw.sse.cisco.com  Will resolve to AWS Static IPs	TCP 443
Repo (Auto upgrades)	Us.repo.acgw.sse.cisco.com Eu.repo.acgw.sse.cisco.com Ap.repo.acgw.sse.cisco.com	TCP 443
ACME	Prod.acme.sse.cisco.com	TCP 443
API Gateway	Api.sse.cisco.com	TCP 443
PKI	Ssepki.cryptosvcs.cisco.com	TCP 80

# Resource Connector Redundancy-single Region

- Recommended minimum of 2 agents per connector group
- All agents within a group should be identical and connect to the same region
  - Tunnel URL returned during registration (based on group location)
  - All agents have same connectivity to apps



# Resource Connectors redundancy multi-region (option 1)

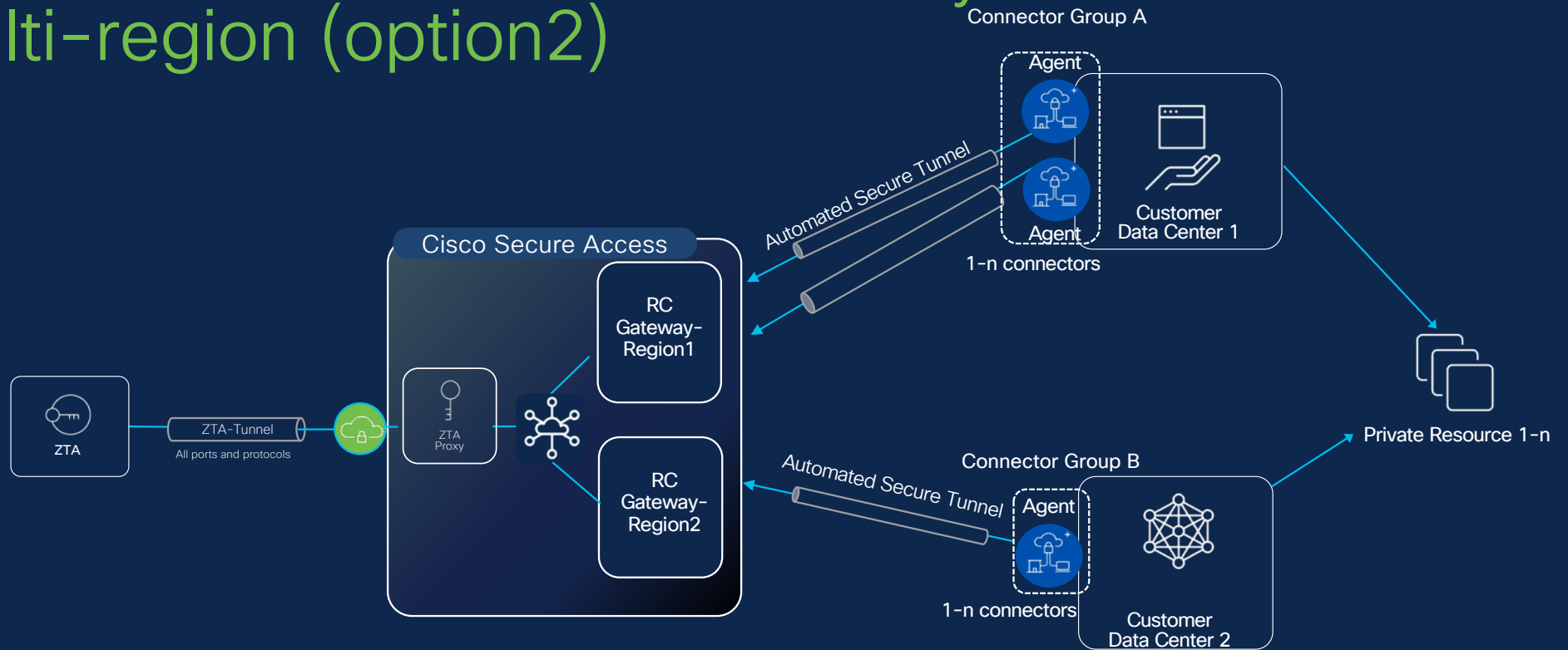


## Resource Connector HA Design

- All RC-Gateways are redundant nodes per region
- RC-Group should be created in the region closest to your private resources
- Traffic will be load-balanced across connectors in RC-Group
- optional:  
Create RC-Group to secondary region. Secure access will steer traffic to RC-Group closest to user by Geo-Proximity

- All connectors in a group must be of the same type e.g., AWS, ESX, Azure
- The instance type (or HW resources) must be identical for accurate load-balancing
- Each connector must be able to reach all the resources assigned to RC-Group

# Resource Connectors redundancy- multi-region (option2)



## Resource Connector HA Design

- All RC-Gateways are redundant nodes per region
- RC-Group should be created in the region closest to your private resources
- Traffic will be load-balanced across connectors in RC-Group
- optional:  
Create RC-Group to secondary region. Secure access will steer traffic to RC-Group closest to user by Geo-Proximity

- All connectors in a group must be of the same type e.g., AWS, ESX, Azure
- The instance type (or HW resources) must be identical for accurate load-balancing
- Each connector must be able to reach all the resources assigned to RC-Group

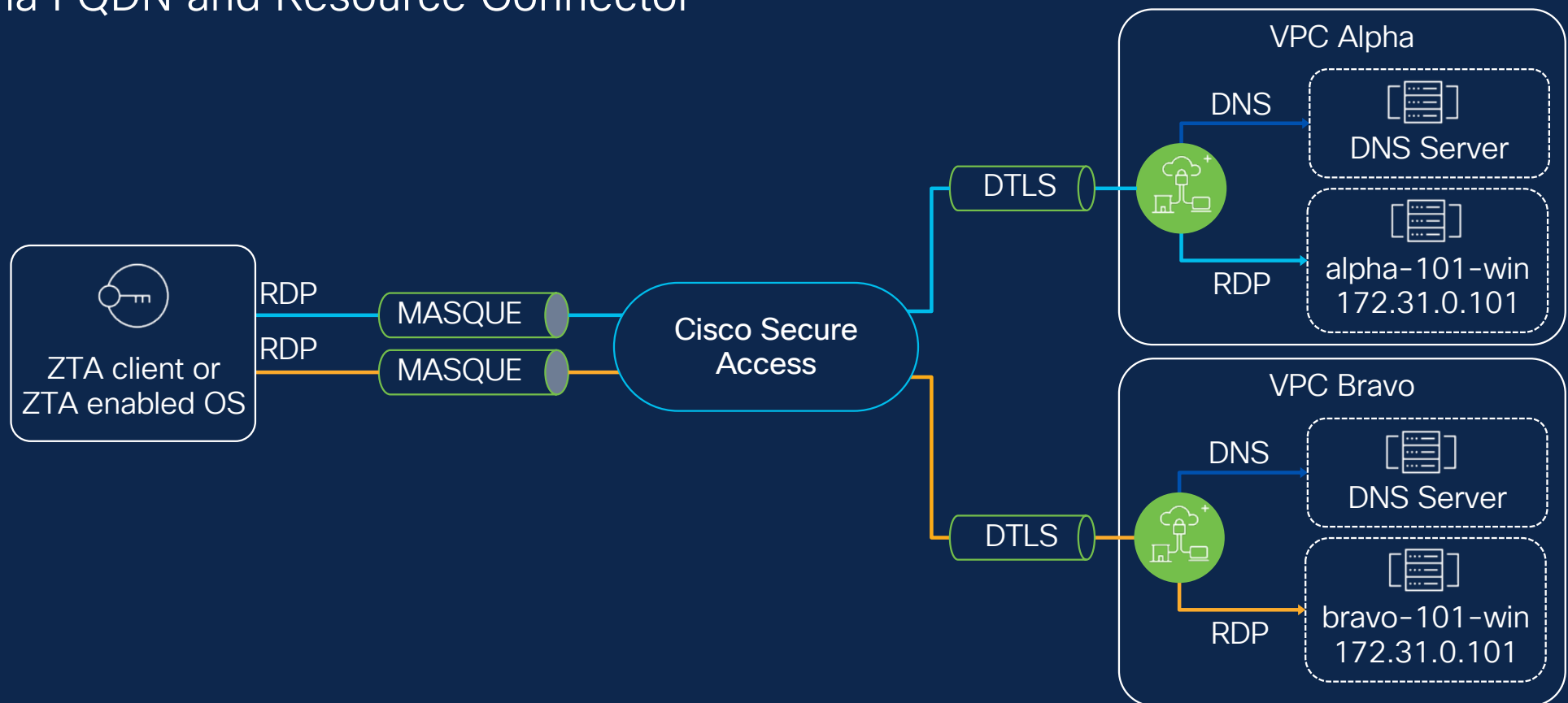
## Resource Connector Benefits

- Resource connectors can be quickly deployed in AWS and VMWare without any additional infrastructure.
- Resource connectors typically do not require any additional route configuration on the network, nor do they require any changes to firewall rules in most environments.
- Resource connectors can provide connectivity to applications on overlapping IP space. This is very beneficial for mergers and acquisitions where applications in the acquired DC may be on overlapping IP space.
- They are deployed in groups for load balancing and redundancy purposes. Providing the necessary bandwidth and high availability for mission critical applications.



# Access Overlapping IPs Simultaneously

via FQDN and Resource Connector



Next steps

1 Deploy your Connectors

We recommend deploying connectors in multiples. Each connector must have connectivity to the same resources. To deploy the connectors:

- Copy the provisioning key below.
- Head to the AWS marketplace and set up the SSE Connector instances using the provisioning key. Connectors deployed using the same key will be part of the same group.

Connector Group	Provisioning Key		
AWS	.....	<a href="#">Copy</a> <a href="#">Regenerate</a>	Key expires on May 30, 2023 5:00 PM
US-DC	.....	<a href="#">Copy</a> <a href="#">Regenerate</a>	Key expires on Jun 2, 2023 5:00 PM
US-EAST	.....	<a href="#">Copy</a> <a href="#">Regenerate</a>	Key expires on Jun 8, 2023 5:00 PM
US-WEST	.....	<a href="#">Copy</a> <a href="#">Regenerate</a>	Key expires on Jun 11, 2023 5:00 PM
APJC	.....	<a href="#">Copy</a> <a href="#">Regenerate</a>	Key expires on May 30, 2023 5:00 PM
EMEA	.....	<a href="#">Copy</a> <a href="#">Regenerate</a>	Key expires on Jun 2, 2023 5:00 PM

Refer to the step by step guide for setting up connectors in your environment. [Help](#)

2 Confirm Connectors

3 Map Private Resources to Connector Group

Connector Groups

Connector groups allow the SSE cloud to communicate securely with your private resources without requiring open inbound ports on your network. [Help](#)

Q Search SSE Region Status 6 Connector Groups [Add a Connector Group](#)

Connector Group	SSE Region	Status	Connectors	Resources	Total Requests	Total Traffic
AWS	US East (N. Virginia)	Waiting	3	1	TBD	TBD
US-DC	US East (N. Virginia)	Connected	0	2	TBD	TBD
US-EAST	US East (N. Virginia)	Connected	0	0	TBD	TBD
US-WEST	US West (Oregon)	Connected	0	0	TBD	TBD
APJC	Asia Pacific (Singapore)	Connected	0	1	TBD	TBD
EMEA	Europe (Frankfurt)	Connected	0	2	TBD	TBD

## Add a Connector Group

Connector groups allow you to securely connect the Private resources in your servers to the SSE cloud without needing to open inbound ports in your environment.

**i** We recommend creating a connector group for each network segment in your organization that contains private resources.

**1** Select nearest SSE cloud instance

**2** Review environment

### Select nearest SSE cloud instance

Connector Group name

Nearest SSE cloud instance

The SSE cloud instance that is closest to the data center in which connect to the SSE Cloud in this region. [Help](#)



Cancel

Next

## Add a Connector Group

Connector groups allow you to securely connect the Private resources in your servers to the SSE cloud without needing to open inbound ports in your environment.

**1** We recommend creating a connector group for each network segment in your organization that contains private resources.

**1** Select nearest SSE cloud instance  
DataCenter Connector, US East (N. Virginia)

**2** Review environment

### Review environment

SSE provides the connectors as a virtual machine (VM) image that is auto-enrolled and the lifecycle of the connector is managed by SSE. [Help](#)

 Amazon Web Services

#### Prerequisites

- Intel x86\_64/AMD64 based architecture
- Root or sudo access to the system in order to configure a new package repository and install packages
- Prerequisite 3
- Prerequisite n

#### Throughput requirements

Select the required throughput for a group



Throughput in Gbps

**Recommendation:** To achieve the above throughput we recommend a set of

**3 x  EC2 instances**

To learn more about best practices in scalability refer to [Scalability Considerations](#)



Cancel

Back

Save

# Network Connections

Manage connections between your data centers and SSE.

**Connector Groups** | Network Tunnels

## Next steps

### 1 Deploy your Connectors

We recommend deploying connectors in multiples. Each connector must have connectivity to the same resources. To deploy the connectors:

- Copy the provisioning key below.
- Head to the AWS marketplace and set up the SSE Connector instances using the provisioning key. Connectors deployed using the same key will be part of the same group.

Connector Group	Provisioning Key		
AWS	.....	<a href="#">Copy</a>	<a href="#">Regenerate</a> Key expires on May 30, 2023 5:00 PM
DataCenter Connector	.....	<a href="#">Copy</a>	<a href="#">Regenerate</a> Key expires on Jun 12, 2023 5:00 PM
US-DC	.....	<a href="#">Copy</a>	<a href="#">Regenerate</a> Key expires on Jun 2, 2023 5:00 PM
US-EAST	.....	<a href="#">Copy</a>	<a href="#">Regenerate</a> Key expires on Jun 8, 2023 5:00 PM
US-WEST	.....	<a href="#">Copy</a>	<a href="#">Regenerate</a> Key expires on Jun 11, 2023 5:00 PM
APJC	.....	<a href="#">Copy</a>	<a href="#">Regenerate</a> Key expires on May 30, 2023 5:00 PM
EMEA	.....	<a href="#">Copy</a>	<a href="#">Regenerate</a> Key expires on Jun 2, 2023 5:00 PM

Refer to the step by step guide for setting up connectors in your environment. [Help](#)

### 2 Confirm Connectors

### 3 Map Private Resources to Connector Group

## Connector Groups

Connector groups allow the SSE cloud to communicate securely with your private resources without requiring open inbound ports on your network. [Help](#)

Search:  SSE Region:  Status:  7 Connector Groups Add a Connector Group

Connector Group	SSE Region	Status	Connectors	Resources	Total Requests	Total Traffic
AWS	US East (N. Virginia)	<span>Connected</span>	3	1	TBD	TBD
DataCenter Connector	US East (N. Virginia)	<span>Connected</span>	0	0	TBD	TBD
US-DC	US East (N. Virginia)	<span>Connected</span>	0	2	TBD	TBD
US-EAST	US East (N. Virginia)	<span>Connected</span>	0	0	TBD	TBD

## Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

### Name and tags Info

Name  
 [Add additional tags](#)

### Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

[AMI from catalog](#) | [Recents](#) | [My AMIs](#) | [Quick Start](#)

Amazon Machine Image (AMI)

appconnector-v1.0.1  
ami-067eac00aea8667e



[Browse more AMIs](#)  
Including AMIs from  
AWS, Marketplace and  
the Community

Published	Architecture	Virtualization	Root device type	ENA Enabled
2023-05-15T20:48:19.000Z	x86_64	hvm	ebs	Yes

### Instance type Info

Instance type  
**t2.micro** Free tier eligible  
Family: t2 | 1 vCPU | 1 GiB Memory | Current generation: true  
On-Demand RHEL pricing: 0.0738 USD per Hour  
On-Demand SUSE pricing: 0.0138 USD per Hour  
On-Demand Windows pricing: 0.0184 USD per Hour  
On-Demand Linux pricing: 0.0138 USD per Hour

All generations [Compare instance types](#)

### Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

### Number of instances Info

### Software Image (AMI)

[Copied ami-02d2ce0af550f6420 ...read more  
ami-067eac00aea8667e

### Virtual server type (instance type)

t2.micro

### Firewall (security group)

New security group

### Storage (volumes)

1 volume(s) - 32 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#)

[Launch instance](#)

[Review commands](#)



Disable

Capacity reservation [Info](#)

Select

Tenancy [Info](#)

Select

RAM disk ID [Info](#)

Select

Kernel ID [Info](#)

Select

Nitro Enclave [Info](#)

Select

Nitro Enclaves are not compatible with instance types that have less than 2 vCPUs.

Specify CPU options

The selected instance type does not support CPU options.

Metadata accessible [Info](#)

Select

Metadata transport

Select

Metadata version [Info](#)

Select

Metadata response hop limit [Info](#)

Select

Allow tags in metadata [Info](#)

Select

User data - optional [Info](#)

Enter user data in the field.

Enter user data in the field.

```
#!/bin/bash  
yum install -y awscli  
aws configure  
aws s3 cp /usr/share/doc/awscli/awscli-1.16.130.tar.gz s3://my-bucket/
```

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

[Copied ami-02d2ce0af550fd420 ...read more  
ami-067eac00aea8667e

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 32 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Launch instance

Review commands



EC2 &gt; Instances &gt; Launch an Instance

## Launching instance

Please wait while we launch your instance.

Do not close your browser while this is loading.

Launch initiation

69%

Details



- Overview
- Connect**
- Resources
- Secure
- Monitor
- Admin
- Workflows

## Network Connections

Manage connections between your data centers and SSE.

**Connector Groups** Network Tunnels

### Next steps

1 Deploy your Connectors

2 Confirm Connectors

**3 Map Private Resources to Connector Group**

In order to route traffic, Connector Groups must be associated with the resources that they are capable of reaching. [Help](#)

#### Connector Group

DataCenter Connector	<a href="#">Map Private Resources</a>
APJC	<a href="#">Map Private Resources</a>
EMEA	<a href="#">Map Private Resources</a>

You can always map resources later from the corresponding connector group page or associate a resource to the connector group while defining the resource.

[Map Resources Later](#) [Define a Private Resource](#)

### Connector Groups

Connector groups allow the SSE cloud to communicate securely with your private resources without requiring open inbound ports on your network. [Help](#)

Search SSE Region Status 7 Connector Groups

[Add a Connector Group](#)

Connector Group	SSE Region	Status	Connectors	Resources	Total Requests	Total Traffic
AWS	US East (N. Virginia)	Waiting	3	1	TBD	TBD
US-DC	US East (N. Virginia)	Waiting	0	0	TBD	TBD
US-EAST	US East (N. Virginia)	Waiting	0	2	TBD	TBD
US-WEST	US West (Oregon)	Waiting	0	0	TBD	TBD
APJC	Asia Pacific (Singapore)	Waiting	0	0	TBD	TBD
EMEA	Europe (Frankfurt)	Waiting	0	1	TBD	TBD
AZURE	US East (N. Virginia)	Waiting	0	2	TBD	TBD

Overview

Connect

Resources

Secure

Monitor

Admin

Workflows New

## Resource Groups

Applications, networks, or subnets that your organization controls access to. The login page for these resources is visible only to the users and devices that you specify.

Private Resources Resource Groups

### 3 Resource Groups

Q Search

Add a Private Resource Group

Resource Group	Resources	Rules	Description	Last Modified
<a href="#">Atlassian Tools</a>	3	0		May 22, 2023
<a href="#">BLDG4 Servers</a>	2	0		May 25, 2023
<a href="#">Secure Access Data Center</a>	3	0		May 29, 2023

Rows per page 10 < 1 >

Overview

← Resource Groups

Connect

Resources

Secure

Monitor

Admin

Workflows New

### Add Resource Group

Group resources to simplify rule creation, apply rules consistently to all resources in the group, and avoid updating multiple rules when resources change.

#### General

Resource Group Name \*

Secure Access Data Center

Description (optional)

#### Choose Resources

Copy from Existing Group

Resource Group

#### Choose Resources

11 available

- U2EMU-Private-APP
- Jira TMElabs
- Jira-AWS
- MedicalHomePage
- My Confluence Instance
- My Jira Instance
- My SAP Instance
- New Application
- VSCode-Server
- ZTNA Client based

3 selected

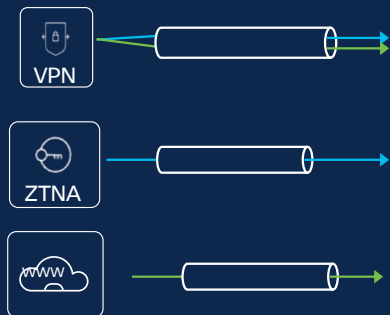
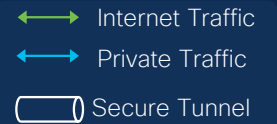
- Jira - Dev
- Portainer
- Postgres DB

Save Cancel

Remote User



# Users: Remote Connectivity



## AnyConnect VPN

- Authentication & Posture @ Connect time
- DTLS Tunnel
- Carry **Internet & Private Traffic** (All ports & protocols)
- SAML, (+) Cert, & (+) Multi-Cert Authentication

## ZTNA Module

- Authentication & Posture per session
- QUIC tunnel (MASQUE proxy)
- Carry **Private Traffic** (All TCP/UDP ports)
- SAML Auth + Auto re-new

## Security Roaming Module

- Device Enrollment (profile)
- Carry DNS & Internet Web Traffic (80/443)

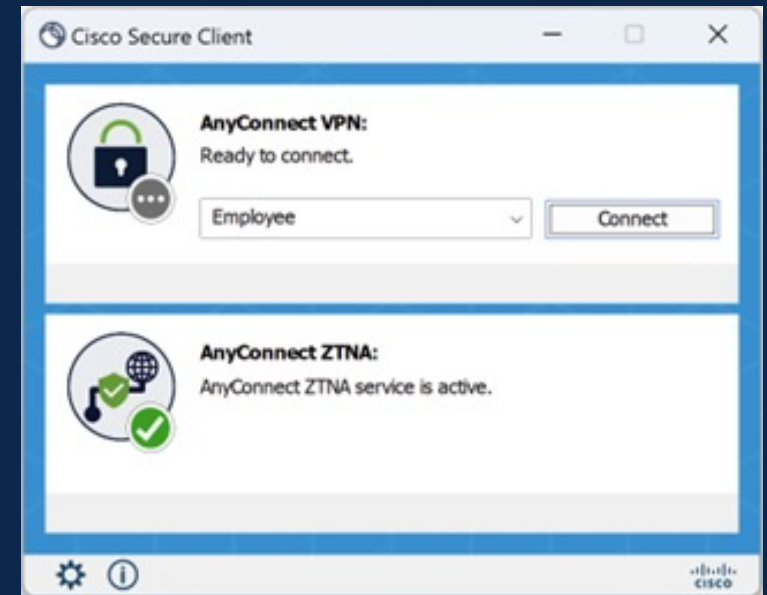


## Clientless ZTNA

- Accessible from any browser that supports SAML/Cookies
- Request based posture (geolocation, browser version, OS)
- Web Apps Only (RDP, SSH roadmap)

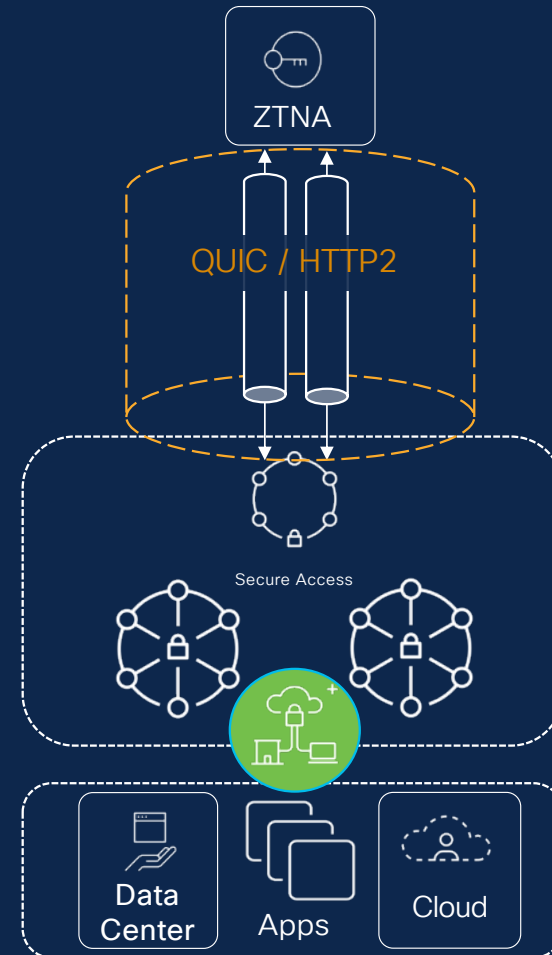
# Zero Trust Access Module

- Transparent user experience
- Proxied resource access with coarse-grained or fine-grained access control
- Service managed client certificates with TPM/hardware enclave key storage
- Support for both TCP and UDP applications
- Cisco and third-party VPN client interop
- Next-generation protocol (QUIC & MASQUE)
- Apple and Samsung native Masque client



# Client-based ZTNA

- Zero Trust Network Access (ZTNA)
  - New module in Secure Client 5.0+
  - Deploy using MDM / SCCM, etc.
  - Pre-deploy MSI available
- Private Application Access
  - Traffic is routed based on app IP/FQDN
  - QUIC tunnels created on demand
  - Sent through MASQUE proxy in Secure Access
  - No need to connect VPN
  - Falls back to HTTP2 when QUIC is blocked
- Traffic steering rules are added automatically
  - In most cases should not be modified
  - Can be used to narrow wildcard FQDNs



# 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)

# 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

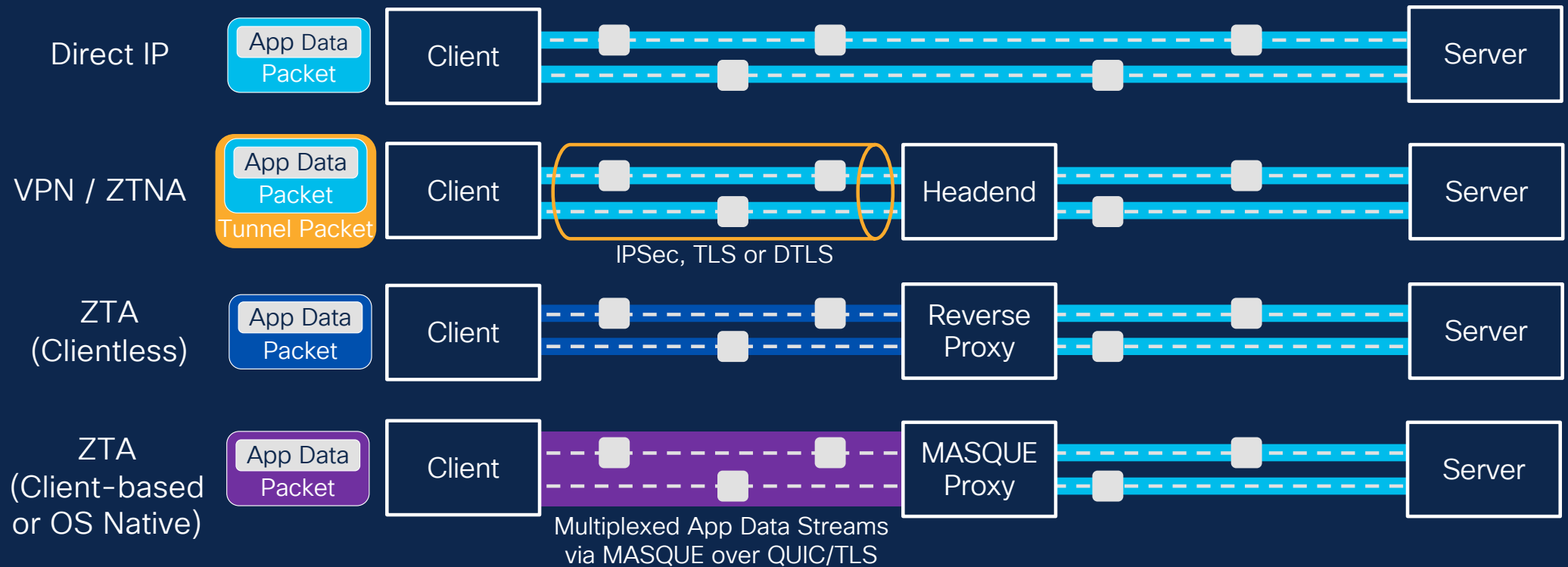


Flexibility to support per-connection, per-app or per-device tunnels



Native OS support

# ZTA Connectivity vs. Other Methods

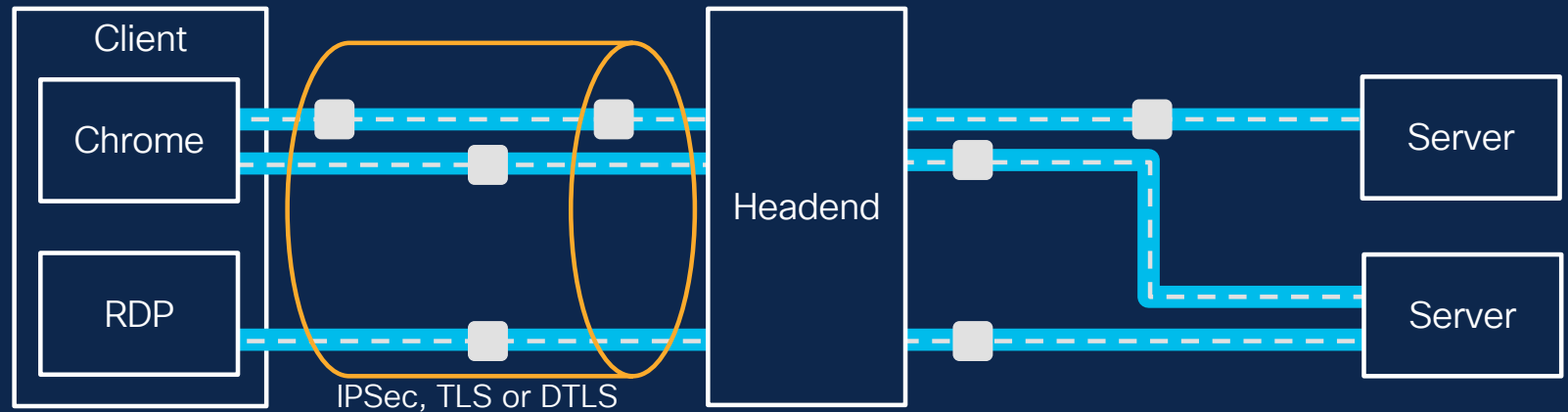


ZTA eliminates the overhead of VPN tunnels and improves security with full separation between users and the enterprise network

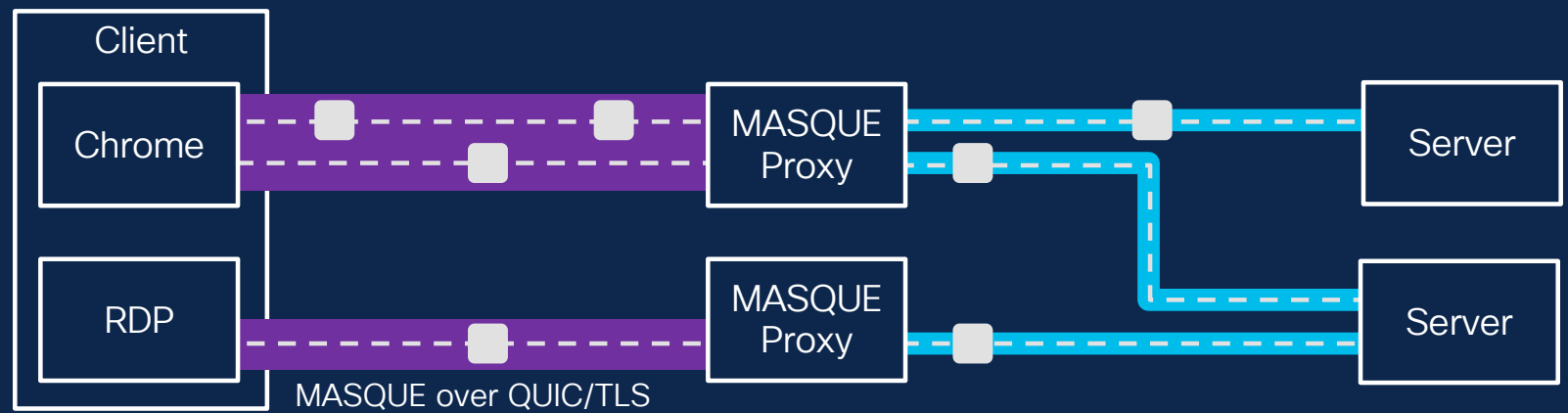
# ZTA Connectivity vs. Other Methods

- - - App Data Stream
- TCP/UDP Connection
- Tunnel

VPN / ZTNA

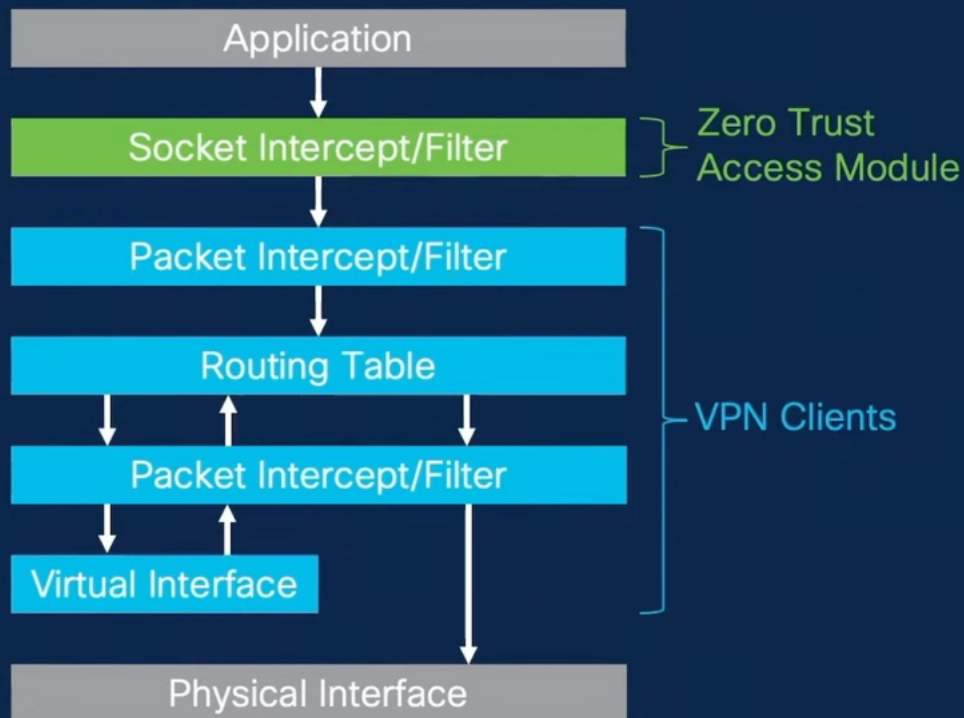


ZTA  
(Client-based  
or OS Native)



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

# Zero Trust Access Module - Socket Intercept

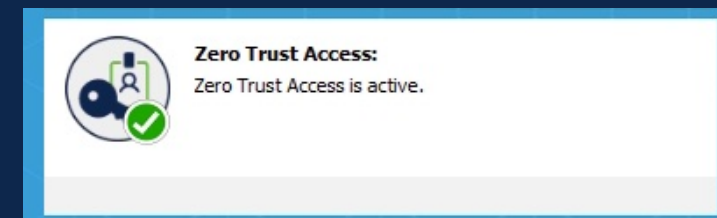
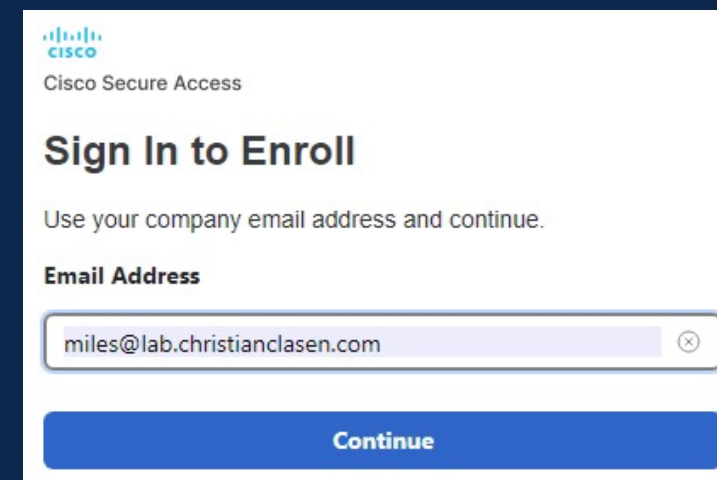
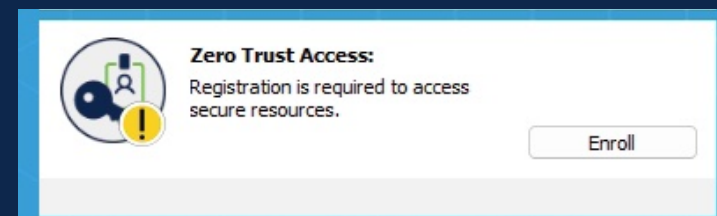


## Why use socket intercept?

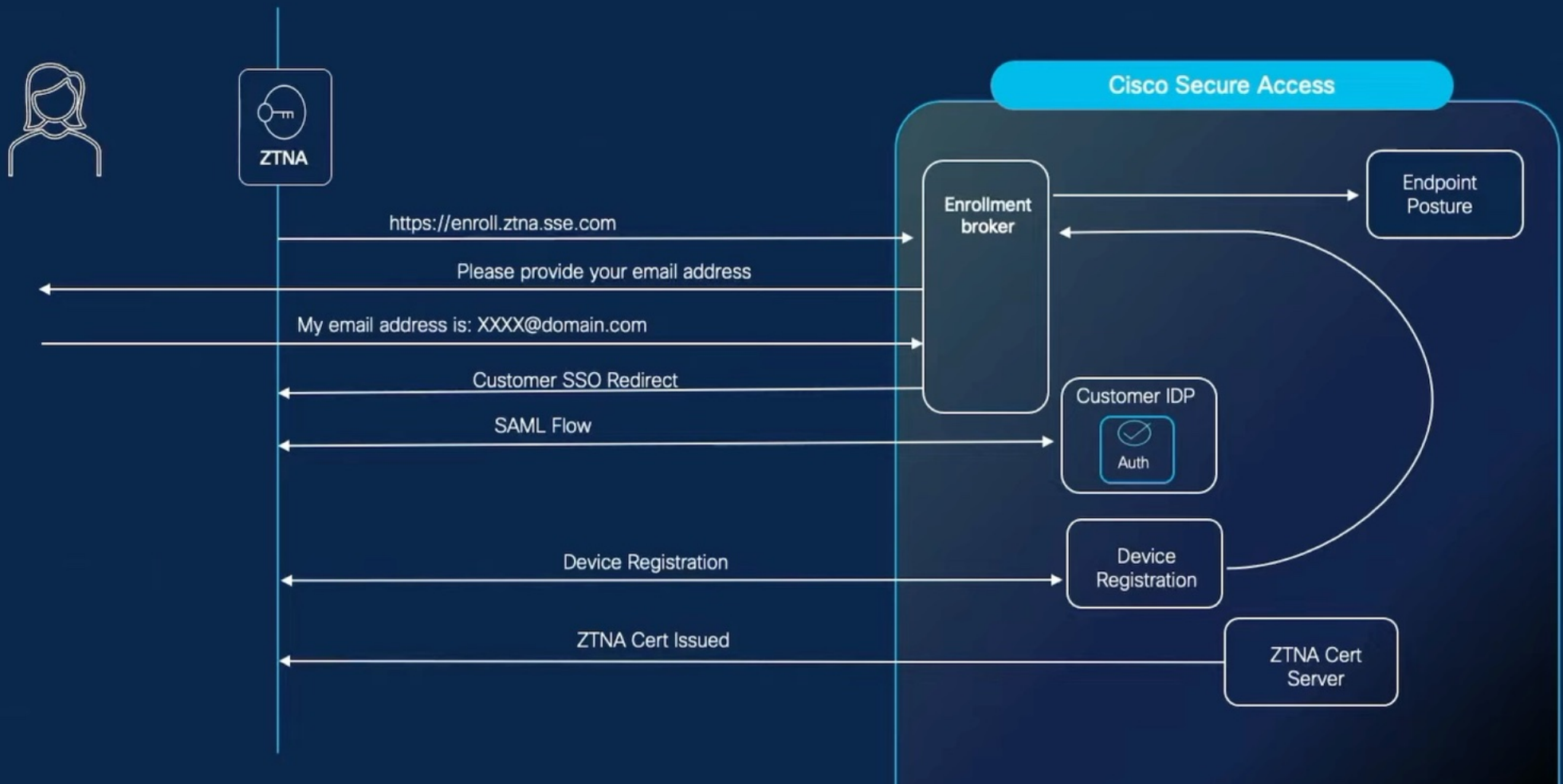
- Control of DNS and application traffic *before* VPN clients
- No route table manipulation
- Ability to capture traffic by IP, IP subnet, FQDN and FQDN wildcard
- Interoperability with Cisco and non-Cisco VPNs

# Client-based ZTNA: Enrollment

- New users are prompted to enroll by the Secure Client
  - User input email address as username
  - IdP must be pre-configured in Secure Access
  - User must be in the list of imported users
- User is presented with a list of their tenants
  - One IdP per tenant is supported
  - One enrollment per local user is supported
  - SAML redirection to configured IdP
- Once enrolled, a certificate is pushed to the client
  - Saved in the TPM (required)
  - Auto-renewal occurs within two weeks of expiration
  - Re-enrollment is required if the device is offline during renewal period

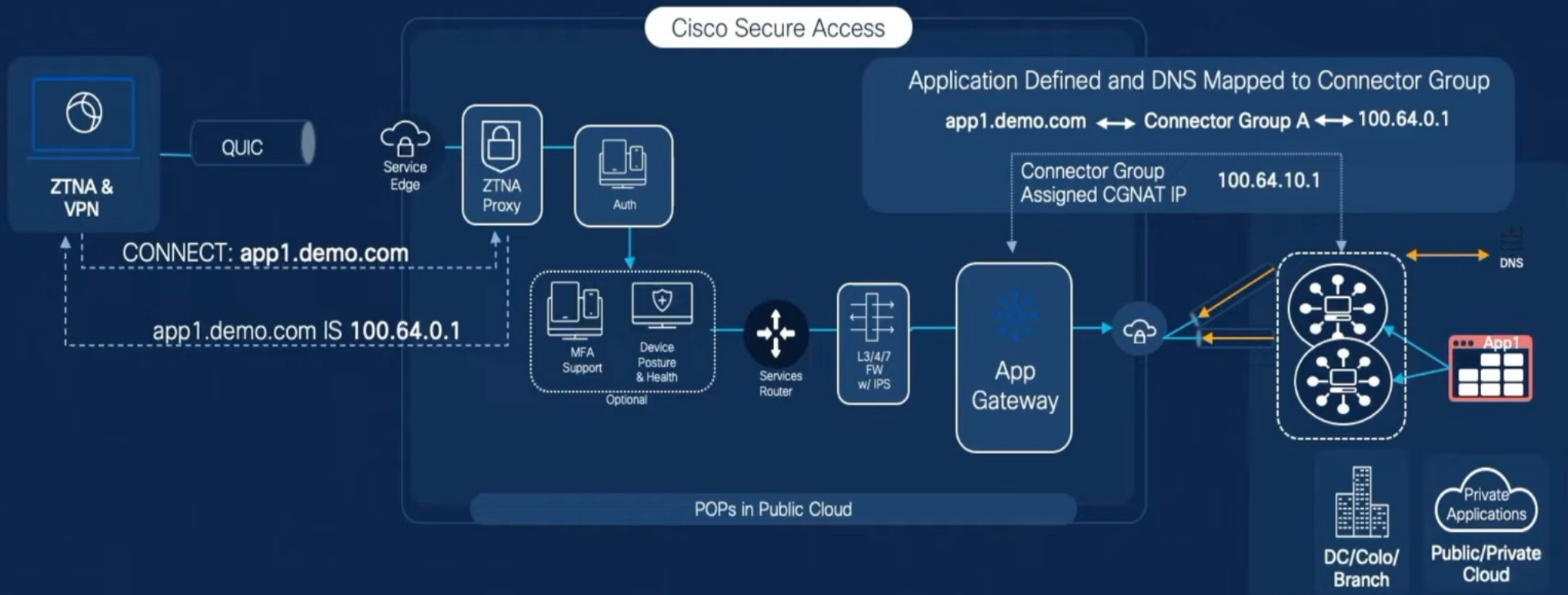


# Enrollment Procedure



# End to End Workflow

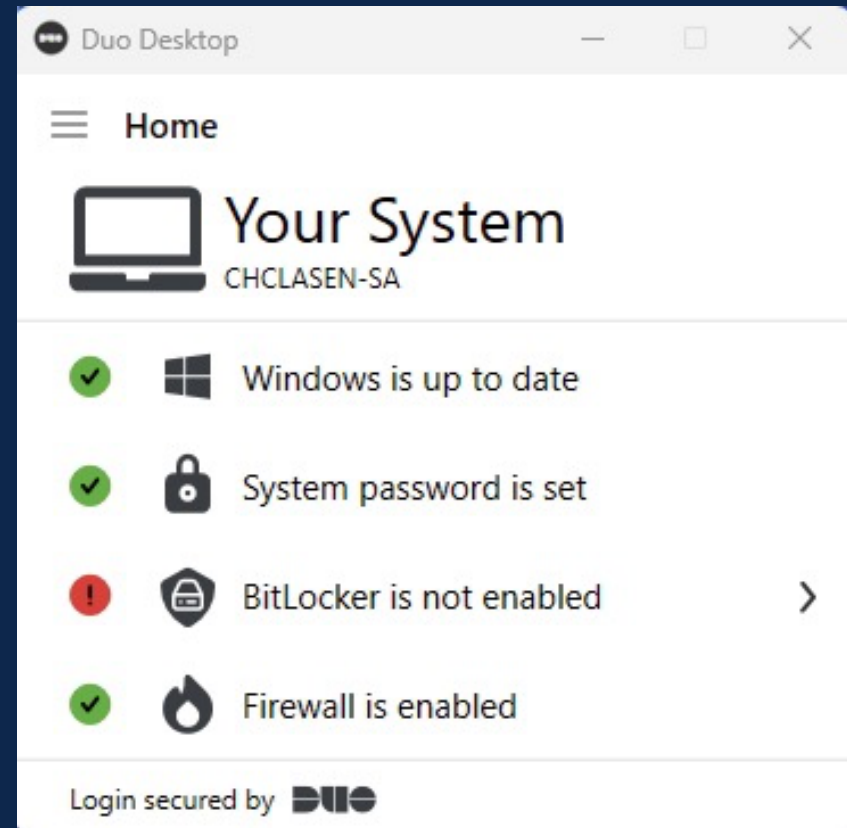
↔ Client based Access  
Secure Tunnel



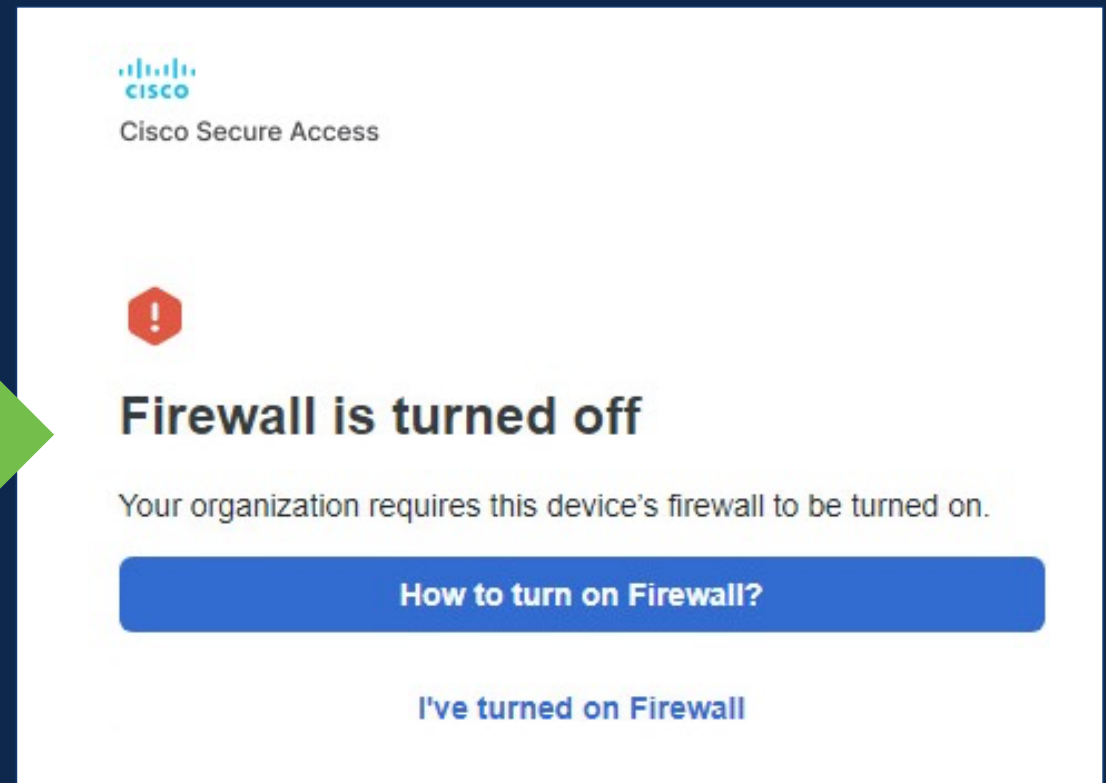
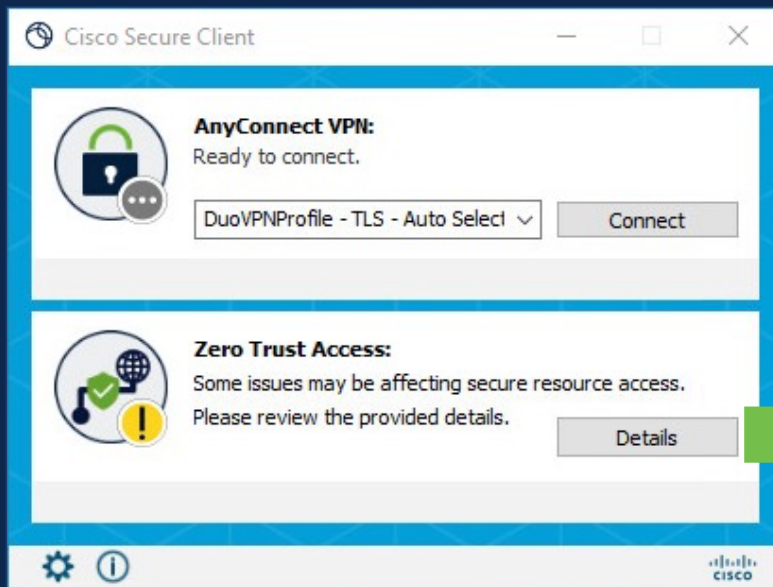


# Client-based ZTNA: Posture

- Posture checks provided by Duo Health Agent
  - Packaged with the client installer
  - Updated every 30 minutes
- Supports the following attributes:
  - Operating system
  - Firewall
  - Endpoint security agent
  - System password
  - Disk encryption
  - Browser

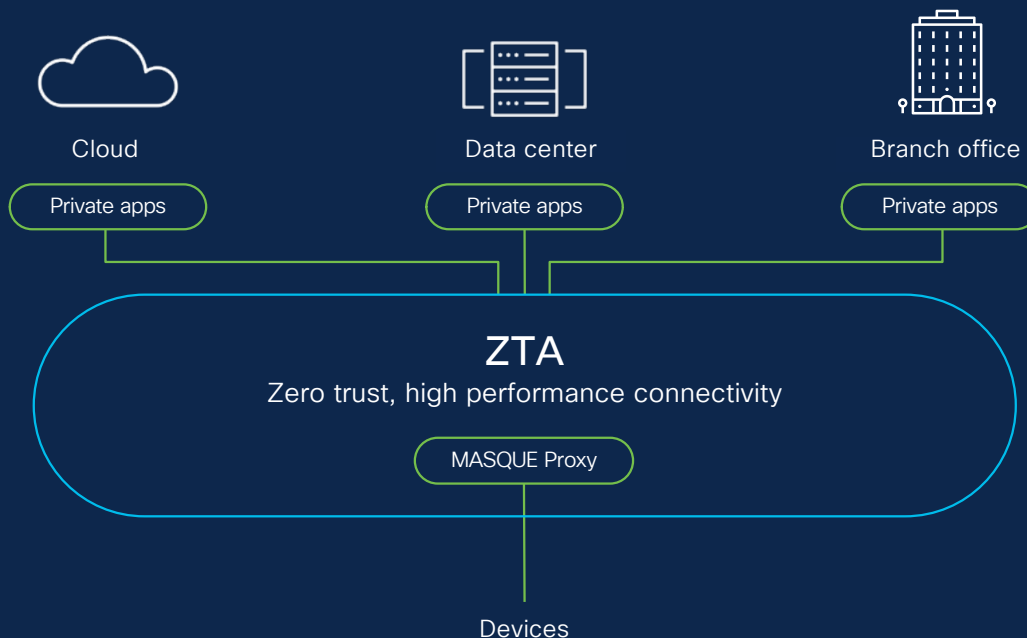


# Client-based ZTNA: Posture



Mobile ZTA

# 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 (iOS)
- 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 iOS

## OS Native ZTA with Apple Enterprise Relay



Single layer of encryption for lightning-fast, secure access and compatible with iCloud Private Relay

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

Traffic Flow w/ Enterprise Relay Enabled:  
Device → Enterprise Relay → Secure Access → Application

# Settings

Search

**SC Steven Chimes**  
Apple ID, iCloud+, Media & Purchases

SC AC Family

- Airplane Mode
- Wi-Fi Omni Guest
- Bluetooth On
- VPN & Relays** On

- Notifications
- Sounds
- Focus

## < VPN & Relays

### Cisco Enterprise Relay (SYN H2)

Type Relay

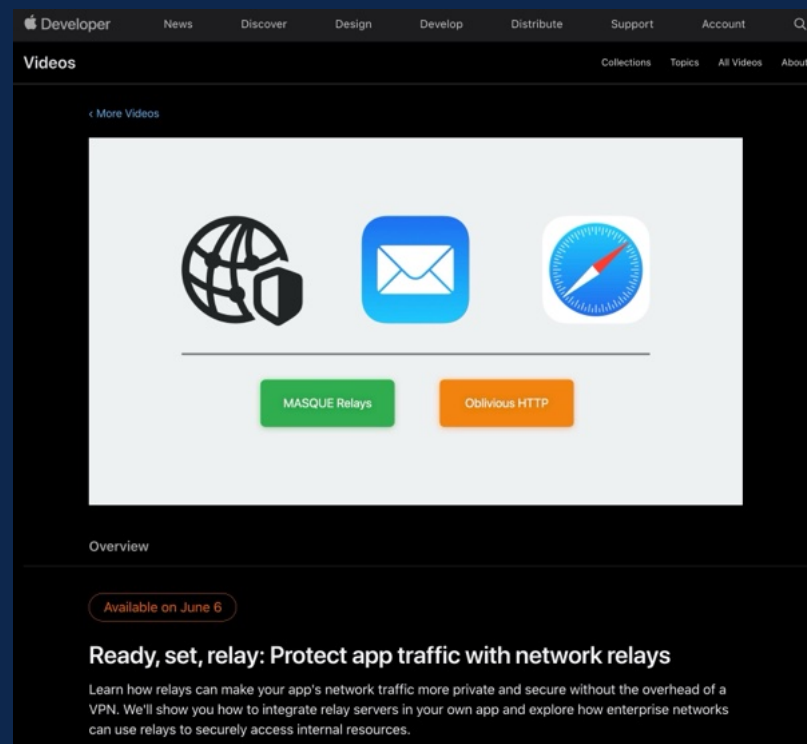
Server <https://proxy-8165175.zpc.sse.cisco.com:443/>

#### DOMAINS

- rdp.metronic.io
- smb.metronic.io
- nfs.metronic.io
- ntp.metronic.io
- snmp.metronic.io
- iis.metronic.io
- billing.metronic.io
- dashboard.metronic.io
- seo.metronic.io
- speedtest.metronic.io
- iwa.metronic.io

# More on Apple's Native OS Support of MASQUE

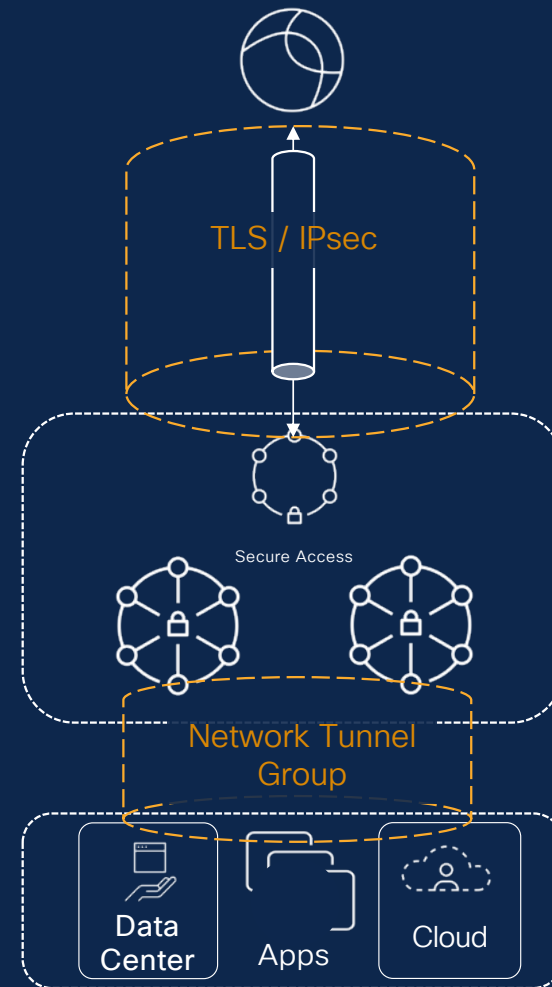
*“Learn how relays can make your app's network traffic **more private and secure** without the overhead of a VPN. We'll show you how to integrate relay servers in your own app and **explore how enterprise networks can use relays to securely access internal resources.**”*



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

# Remote Access VPN

- Secure Client VPN (formerly AnyConnect)
  - Terminates at cloud head-ends
  - No on-premises VPN devices for client-side
- Cloud-side VPN configuration
  - DNS server assigned to clients
  - IP pool for client addressing (per region)
- SAML authentication
  - IdP must be pre-configured in Secure Access
  - User must be imported into Secure Access
- Certificate authentication
  - Can be used alone or with SAML
  - PKI is client-managed and must be pre-deployed





# Remote Access VPN: Posture

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

The screenshot displays the Hostscan posture configuration interface. On the left, a list of eight posture checks is shown, each with a status of 'Not required':

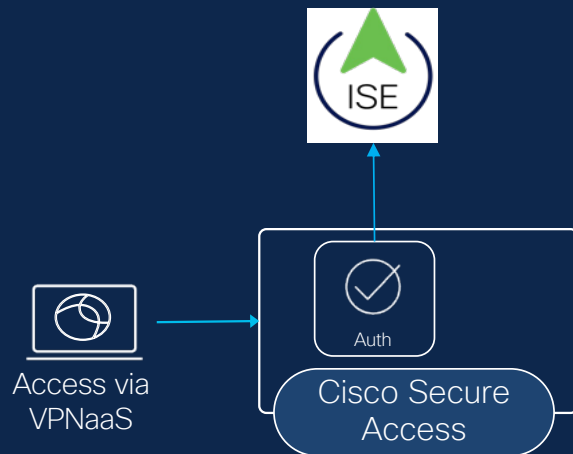
- 1 **Operating System** Any
- 2 **Endpoint security agent** Not required
- 3 **Windows registry entries** Not required
- 4 **Firewall** Not required
- 5 **Disk encryption** Not required
- 6 **File** Not required
- 7 **Processes** Not required
- 8 **Certificate** Not required

On the right, a detailed view for the 'Operating System' check is shown. It includes the title 'Operating System', the requirement 'Require specific operating systems', and a dropdown menu for 'Operating system'. The dropdown menu is currently open, showing 'Windows' as the selected option, with other options 'Mac OS X' and 'Linux' visible below it.

# ISE integration with Secure Access VPNaaS

RADIUS authentication, in addition to SAML authentication

- Simplifies IT operations: RADIUS is already widely used for identity-based access, includes COA support
- Foster consistency: Radius to manage identity for remotely connected users (VPNaaS) and on-premises users.

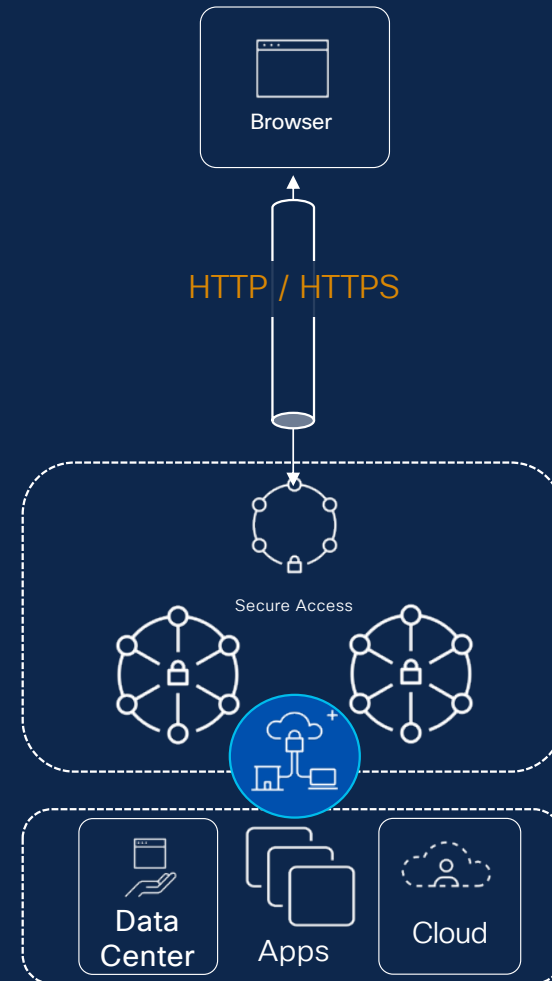


## Essential foundation

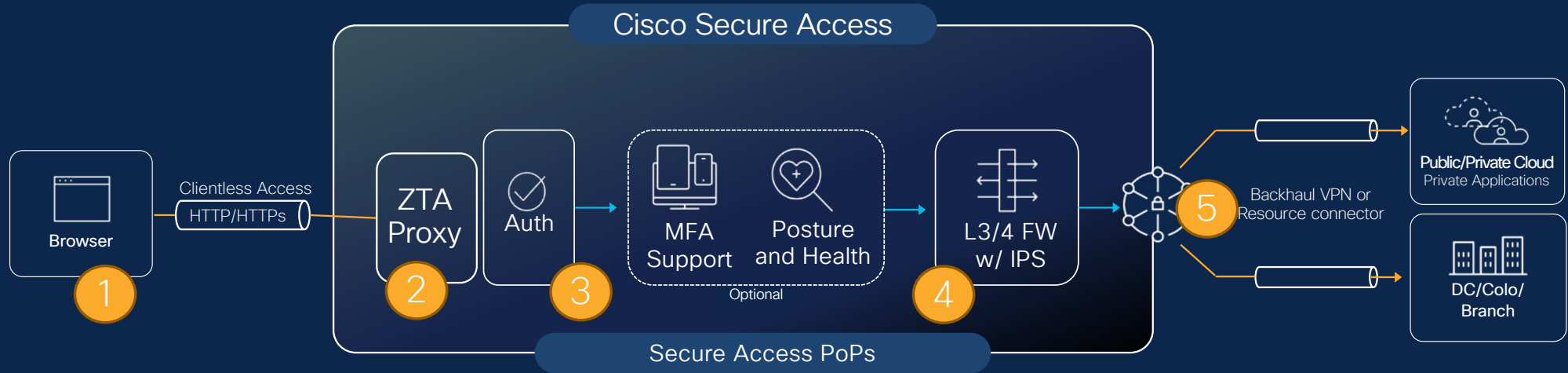
- **End state:** Leverage ISE identity and posture context to deepen Secure Access's visibility into what users are doing, when, and how
- **Coming soon:** Secure Access will ingest the identity and posture context from ISE to inform security policy creation and enforcement
- **In the future:** AI analytics will be able to detect anomalies in device posture and automatically apply the correct policy.

# Browser-based Clientless ZTNA

- Unmanaged and BYOD use-cases
- Secure Access generates a publicly resolvable FQDN
  - Must be shared OOB to users
  - IdP landing pages are best option (e.g., Duo Central)
- SAML authentication
  - IdP must be pre-configured in Secure Access
  - User must be imported into Secure Access
- Basic posture is available based on HTTP headers
  - Browser type
  - Pulled from user-agent string



# Clientless/Browser based Access



1. Client initiates a browser connection to the application specific URL. The request gets resolved and redirected to the nearest Datacenter based upon Anycast DNS.
2. The ZTA Proxy changes the traffic source to an address within 100.64.0.0/16.
3. The request is sent for authentication and posture check
4. Once authenticated and authorized, it will redirect the request to the policy engine, where the decision is made to let the request in or not based on your set policies
5. Once decided, it will be sent to our routing engine to deliver traffic to the application correctly

# Posture




Authorization check prior to application access

Authorization and access check per session

Supported AV vendors:

[Client-based ZTA](#)

[VPN-as-a-service](#)

	 VPNaaS	 ZTA Client-based	 ZTA Browser
Operating System	✓	✓	✓
Anti-Malware	✓	✓	
Firewall	✓	✓	
Disk Encryption	✓	✓	
Certificate Check	✓		
Browser Check	✓		✓
System Password		✓	
File Check	✓		
Registry Check (windows only)	✓		
Process Check	✓		

# Private Resources



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

## Private Resources

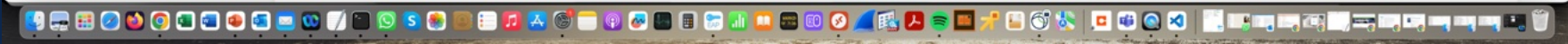
Private Resources are applications, networks, or subnets that your organization controls access to. You must configure a private resource if you plan to allow end users to connect to the resource using zero-trust access. [Help](#)

Private Resources Private Resource Groups

Private Resources Last 24 Hou...

Search by resource name Private Resource Group Connection Method 12 Private Resources + Add

Private Resource	Private Resource Group	Connection Method	Connector Groups	Accessed by	Rules	Total Requests
<a href="#">cymeier-fmc2-lab-netcope-ch</a>	cymeier-wlsn01-lab-resource-group	Browser-based ZTA Client-based ZTA	1	0	2	0
<a href="#">cymeier-ISE Netcope</a>	cymeier-wlsn01-lab-resource-group	Browser-based ZTA Client-based ZTA	1	0	2	0
<a href="#">cymeier-ISE-GUI</a>	cymeier-wlsn01-lab-resource-group	Browser-based ZTA	1	0	2	0
<a href="#">cymeier-sna-fc</a>	cymeier-wlsn01-lab-resource-group	Browser-based ZTA Client-based ZTA	1	0	2	0
<a href="#">cymeier-windows-server</a>	cymeier-wlsn01-lab-resource-group	Browser-based ZTA Client-based ZTA	1	0	2	0



- Overview
- 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 access. [Help](#)

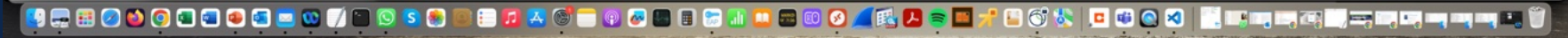
Private Resources Private Resource Groups

#### Private Resource Groups

Group resources to apply rules easily and consistently to all resources in the group. [Help](#)

5 Private Resource Groups + Add

Private Resource Group	Private Resources	Associated Rules	Description	Last Modified
<a href="#">cymeier-wlsn01-lab-resource-group</a>	5	2	-	Mar 8, 2024
<a href="#">gtilburg-beluxlab</a>	2	1	-	Feb 9, 2024
<a href="#">gvanbon-amslab1-philips</a>	1	2	Philips resources in amslab demo	Apr 8, 2024
<a href="#">gvanbon-resource-Group</a>	1	2	-	Mar 14, 2024
<a href="#">vscriban-aws</a>	1	1	-	Jan 9, 2024





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

← Private Resources

### Add a Private Resource

Private Resources are applications, networks, or subnets that your organization controls access to. You must configure private resources in order to choose them as destinations when creating access rules. [Help](#)

#### General

Private Resource Name  
gvanbon-ISE02

Description (optional)  
ISE02 server in AMS lab, gvanbon

#### Communication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address. [Help](#)

Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)	Protocol	Port / Ranges
192.168.61.23	TCP - (HTTP/H...	443 + Protocol & Port

+ IP Address or FQDN  
 Use internal DNS server to resolve the domain

Save Cancel



Chrome File Edit View History Bookmarks Profiles Tab Window Help Tue 18 Jun 11:00

Cisco Secure Access x +

dashboard.sse.cisco.com/org/B219751/resources/privateresources

Secure Access Gerard Van Bon (...)

### Endpoint Connection Methods

Specify the ways user endpoints can reach this resource. Later, access rules will determine which users and devices can access the resource.

- Branch Connections**  
Allow users and devices on the network, such as printers or kiosks, to connect to this resource if allowed by access rules.
- Zero-trust connections**  
Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)
- 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) ⓘ  
192.168.61.23  
[+ 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** ⓘ  
https:// gvanbon-ise02 -8219751.ztna.sse.cisco.io ⓘ

Protocol Custom host header (optional) ⓘ Server Name Indication (SNI) (optional) ⓘ

Save Cancel

Chrome File Edit View History Bookmarks Profiles Tab Window Help

Cisco Secure Access

dashboard.sse.cisco.com/org/8219751/resources/privateresources

Secure Access Gerard Van Bon (...)

**VPN connections**  
Allow endpoints to connect to this resource when connected to the network using VPN.

**Resource Connector Groups**

Secure Access can forward Zero Trust Access traffic to this private resource using resource connectors. [Help](#)

For more information, see [Help](#)

**Resource Connector Groups** (optional) ⓘ

gvanbon-AMS5-CCC-LAB X e.g. My Server G... ▾

Choose a connector group in the same data center, branch office, or security zone as the resource. ⓘ

**Decryption**

**Decrypt Traffic**  
Decrypt traffic to this resource to allow inspection by the intrusion prevention system (IPS)

**Associated Rules**

**Private Resource Group** (optional)

gvanbon-resource-Group

Group similar resources to simplify creating access rules. [Help](#)

**Used in 5 Rules**

This resource is specified as a destination in the following private access rules:

Rule Order	Rule name	Action	Sources	Destinations
<p><a href="#">Save</a> <a href="#">Cancel</a></p>				

Mac OS dock with various application icons.

Chrome File Edit View History Bookmarks Profiles Tab Window Help Tue 18 Jun 11:00

Cisco Secure Access dashboard.sse.cisco.com/org/8219751/resources/privateresources

Secure Access Gerard Van Bon (...)

### Associated Rules

Private Resource Group (optional)

gvanbon-resource-Group

Group similar resources to simplify creating access rules. [Help](#)

Used in 5 Rules

This resource is specified as a destination in the following private access rules:

Rule Order	Rule name	Action	Sources	Destinations
3	<a href="#">bvanhoec-private-access</a>	✓ Allow	Bart Van Hoecke (bart@24g6q3.onmicrosoft.com)	gvanbon-ISE02
10	<a href="#">gtilburg-private_ZTNA</a>	✓ Allow	Gert Tilburgs (gert@24g6q3.onmicrosoft.com)	gvanbon-ISE02
14	<a href="#">gvanbon-ISE02-lab-access</a>	✓ Allow	Gerard van Bon (gvanbon@lab.netcope.ch) +2	gvanbon-resource-Group
16	<a href="#">joschwei-private access</a>	✓ Allow	Jonas Schweigert (jonas@24g6q3.onmicrosoft.com)	gvanbon-ISE02 +1
17	Default Rule	⚠ Block	Any	Any

**Save** Cancel



# Unified Policy



# Unified Policy, easy to manage

- SSE policies are structured as
  - Public Internet/SaaS access control policy
  - Private Access control policy
- “Unified view” of separate policies with explicit “Rule type” tagged on each rule
- Policy Translation Layer responsible for policy rule rendering and distribution logic to various PDP/PEP services based on the “Rule type” tag
- Rules evaluated in order in each enforcement engine
- **AI assistant to create rules**

The screenshot displays the Cisco Policy management interface. At the top, there is a search bar and a filter dropdown. Below this, a table lists 16 rules. The 'Rule type' column is highlighted with green dashed boxes and arrows pointing to two green callout boxes. The first callout box, labeled 'DNS, FWaaS, SWG', points to the 'Internet Access' rule types of rules 1, 2, and 3. The second callout box, labeled 'ZTNA & RAVPN, Private Access', points to the 'Private Access' rule types of rules 4, 5, 6, 7, and 8. Below the main table, there is a section for 'Default Rules' with two entries: 'Block' and 'Allow'.

#	Rule name	Rule type	Actions	Sources	Destinations	Security Control	Status
1	Eng2Internet-Allow	Internet Access	Allow	Engineering (tmelabs.com)Engineering	News +1	IPS, Web, Tenant	Enabled
2	Eng2Internet-Warn	Internet Access	Warn	Engineering (tmelabs.com)Engineering	BH-Warn	IPS, Web	Enabled
3	Eng2Internet-Block	Internet Access	Block	Engineering (tmelabs.com)Engineering	BH-Block	Web	Enabled
4	Health App	Private Access	Allow	Eng1 (eng1@tmelabs.com)	Health DB	-	Disabled
5	Finance To Finance Resources	Private Access	Allow	Finance (tmelabs.com)Finance	Finance Portal	-	Enabled
6	Eng to Eng Resources	Private Access	Allow		AWS-Jira	-	Enabled
7	BH-Jira-ZTA	Private Access	Allow		AWS-Jira	-	Enabled
8	BH-BAP	Private Access	Allow		Jira-BAP	IPS	Enabled
9	Test SaML	Internet Access	Block		Internet destination	Web	Disabled
10	block IP App	Private Access	Block		IP-VPN	-	Disabled

- Overview
- Experience Insights
- Connect
- Resources
- Secure**
- Monitor
- Admin
- Workflows

## Access Policy

[Rule Defaults and Global Settings](#)

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](#)

**Add Rule**

16 Rules

[Customize view](#)

<input type="checkbox"/>	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
<input type="checkbox"/>	1	<a href="#">gvanbon-amslab-philips-mri</a>	Private	Allow	Gerard Van B... +1	gvanbon-amsl...	-	-	✓
<input type="checkbox"/>	2	<a href="#">cymeier-wlsn01-lab</a>	Private	Allow	Cyrill Meier... +3	cymeier-wlsn...	-	-	✓
<input type="checkbox"/>	3	<a href="#">bvanhoec-private-access</a>	Private	Allow	Bart Van Hoe...	gvanbon-ISE0...	-	-	✓
<input type="checkbox"/>	4	<a href="#">bvanhoec-internet-access</a>	Internet	Allow	bvanhoec-be...	Any	🌐	-	✓
<input type="checkbox"/>	5	<a href="#">bvanhoec-internet-access-rem...</a>	Internet	Isolate	Bart Van Hoe...	News	🌐	-	✓
<input type="checkbox"/>	6	<a href="#">prodiono_Internet Access</a>	Internet	Allow	None	Any	🌐	-	✓
<input type="checkbox"/>	7	<a href="#">joschwei-Internet Access</a>	Internet	Allow	Jonas Schwei... +1	Any	🌐	-	✓
<input type="checkbox"/>	8	<a href="#">vscriban-TECSEC-2780</a>	Internet	Allow	C6385286146	Any	🌐🛡️	-	✓
<input type="checkbox"/>	9	<a href="#">vscriban-aws</a>	Private	Allow	Jonas Schwei... +1	vscriban-aws...	🛡️	51	✓
<input type="checkbox"/>	10	<a href="#">gtilburg-private_ZTNA</a>	Private	Allow	Gert Tilburg...	gvanbon-ISE0...	-	-	✓



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

### Edit gvanbon-ISE02-lab-access

For information about configuring a private access rule, see [Help](#)

Rule is enabled

Logging is enabled [Edit](#)

#### Summary



Rule name:  Rule order:

#### 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.

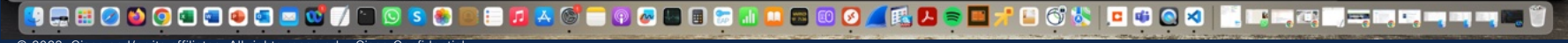
From: Specify one or more sources.

To: Specify one or more destinations.

Information about sources, including selecting multiple sources. [Help](#)

Information about destinations, including selecting multiple destinations. [Help](#)

#### Endpoint Requirements





Chrome File Edit View History Bookmarks Profiles Tab Window Help

Cisco Secure Access

dashboard.sse.cisco.com/org/8219751/secure/policy/editRule?trafficType=private&ruleId=565106

Secure Access Gerard Van Bon (...)

Specify one or more sources. Gerard Van Bon (gerard@24g6q3.onmicrosoft.com) +2 More

Specify one or more destinations. gvanbon-resource-Group

Information about sources, including selecting multiple sources. [Help](#)

Information about destinations, including selecting multiple destinations. [Help](#)

**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: **None** | Requirements: **None**

Private Resources: **gvanbon-resource-Group** 1

**Zero Trust Browser-based Posture Profile** Rule Defaults

Requirements for end-user devices on which the Cisco Secure Client is NOT installed.

Profile: **None** | Requirements: **None**

Private Resources: **gvanbon-resource-Group** 1

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.

**User Authentication Requirements**

**Zero Trust Access: User Authentication Interval** Custom  Enabled

Frequency with which end users verify their identity, in order to connect to any private resource using client-based zero trust access. When disabled, users are not prompted to re-authenticate to the network. [Help](#)

Require users to authenticate again after: Days 0 | Hours 0 | Minutes 0



Chrome File Edit View History Bookmarks Profiles Tab Window Help

dashboard.sse.cisco.com/org/B219751/secure/policy/editRule?trafficType=private&ruleId=565106

Secure Access Gerard Van Bon (...)

## Edit gvanbon-ISE02-lab-access

For information about configuring a private access rule, see [Help](#)

Rule is enabled Logging is enabled [Edit](#)

**Summary**

Sources

Gerard Van Bon  
(gerard@24g6q3.onmicrosoft.com)

[+ 2 More](#)

Allow

Security Controls

IPS Profile is disabled for Global Settings

Destinations

Private Resource Groups

- gvanbon-resource-Gro...

**Rule name** **Rule order**

gvanbon-ISE02-lab-access 14

---

**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  Disabled

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

[Cancel](#)

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



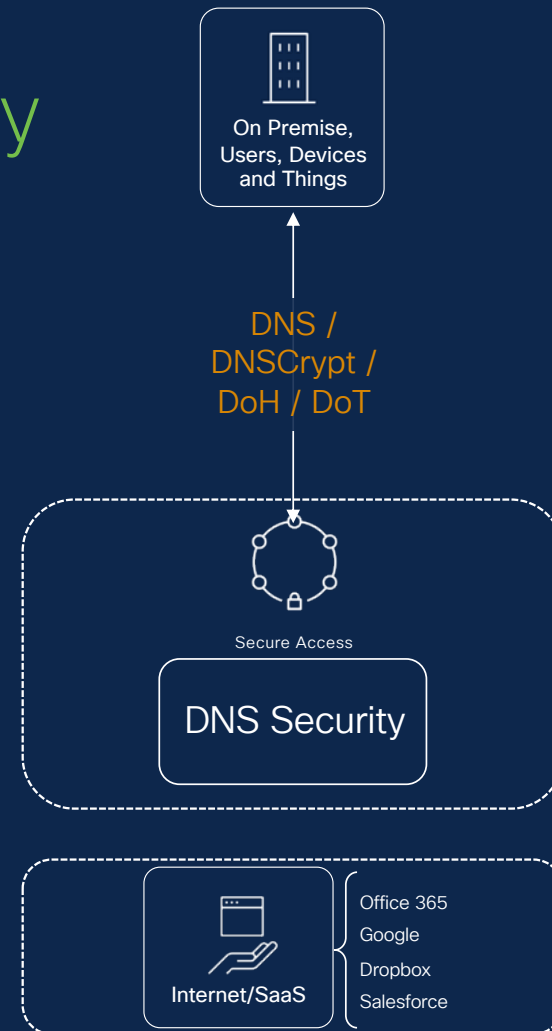


# Secure Internet Access



# Registered Network DNS security

- 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 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

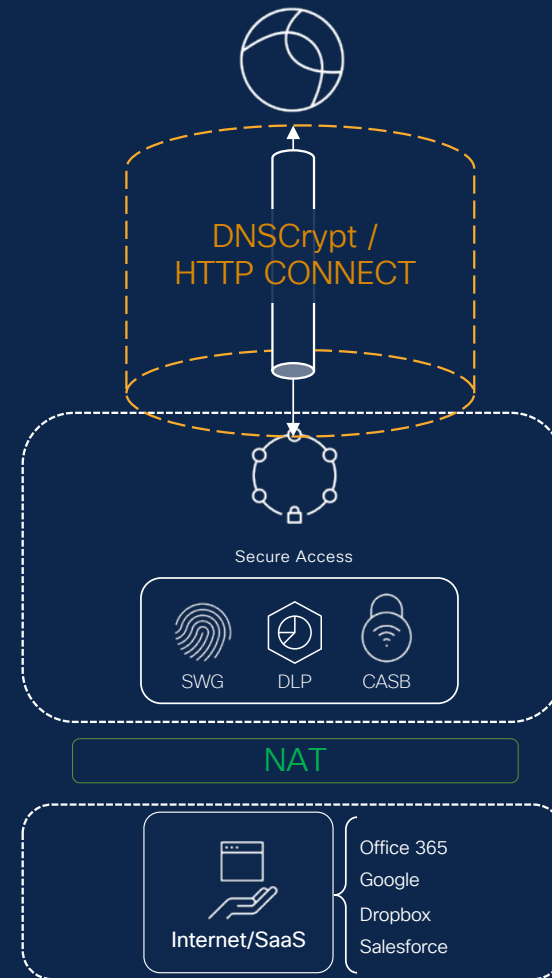


# Roaming Security Module

- Redirects DNS and HTTP/S from the local machine
  - DNS is sent over DNSCrypt
  - HTTP/S is converted to explicit proxy requests
  - HTTP only redirected on TCP 80/443
- OS version support
  - Windows 8.1 or newer (.NET framework 4.6.2+)
  - Windows 10 or 11 on ARM-64
  - macOS 10.14 or newer
- Exceptions for destinations added in dashboard
  - Local domain suffix is excluded
  - Same exceptions apply to PAC file deployment
- Download and deploy OrgInfo file from dashboard
- Dual stack is supported but not native IPv6
- Authentication occurs using the UPN of the logged-in user on the local machine

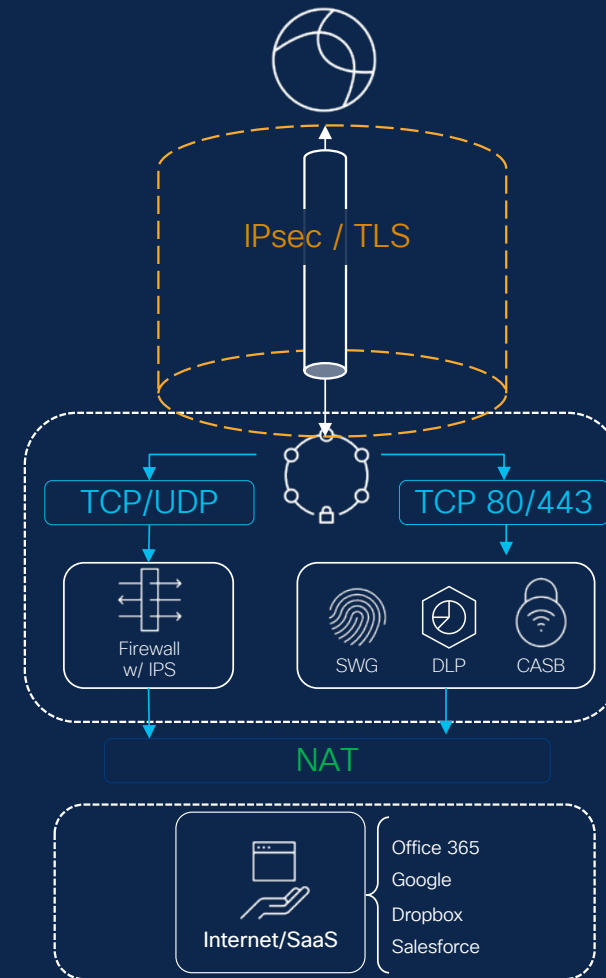
<https://docs.sse.cisco.com/sse-user-guide/docs/roaming-security-module-requirements>

<https://docs.sse.cisco.com/sse-user-guide/docs/download-the-orginfo-json>



# Remote Access VPN

- Full or split-tunnel options are available
- Same deployment as the SPA use-case
- Web traffic is evaluated by Cloud Firewall and Secure Web Gateway
  - Snort IDP/IPS
  - Layer 3-7 firewall rules
  - Data Loss Prevention
  - Anti-malware
  - Tenant controls
  - CASB
- Non-web traffic is evaluated by Cloud Firewall
  - Snort IDP/IPS
  - Layer 3-7 firewall rules





# Secure Access Experience Insights



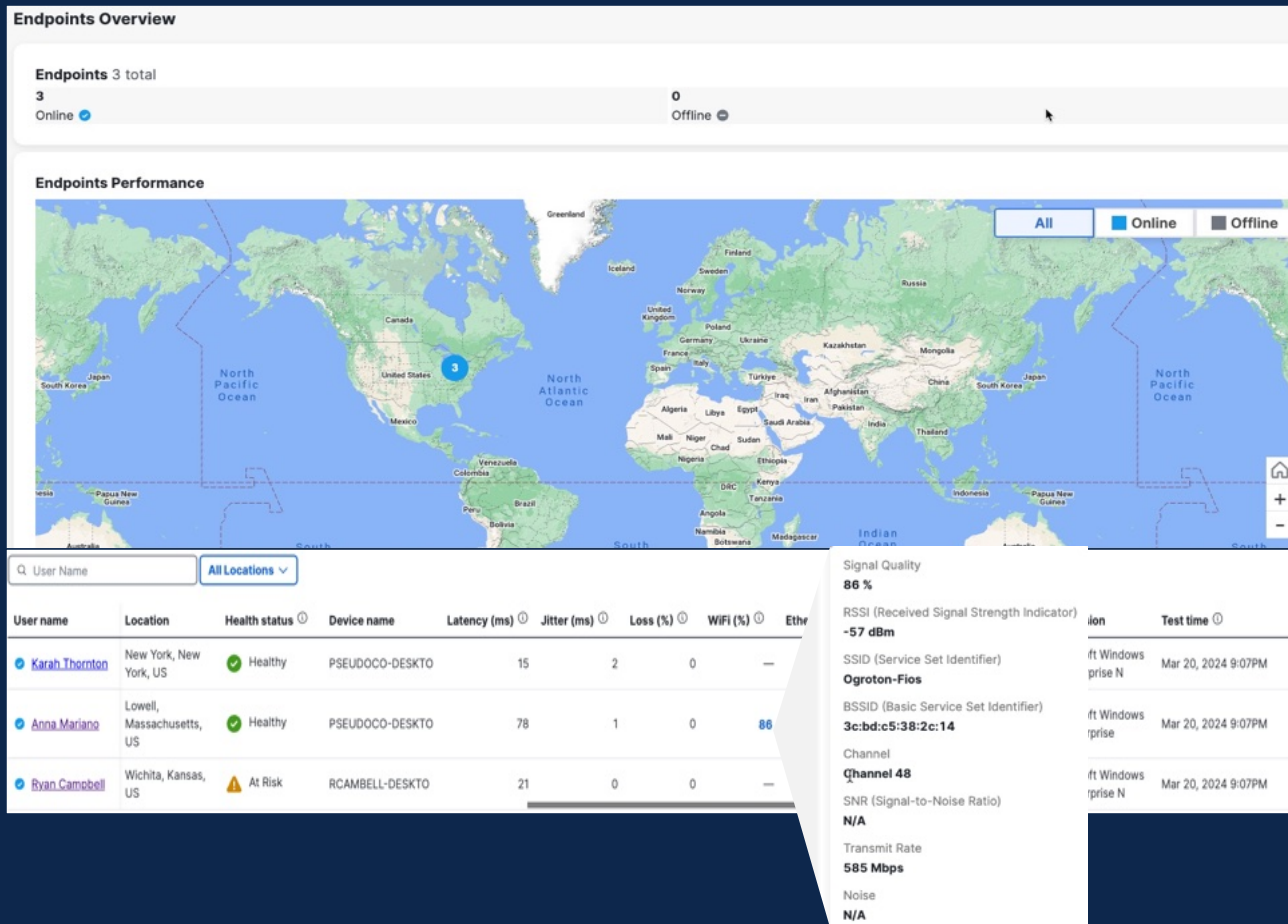
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Confidential

# Secure Access Experience Insights

POWERED BY  
**ThousandEyes**

Monitor user digital experience **without separate agents or management portals**



- Global visibility of registered endpoint status
- Is part of the Cisco Secure Access dashboard
- Includes ThousandEyes Embedded Endpoint Agent(EPA) as a module in Cisco Secure Client





# Proactive Monitoring of Workforce Productivity

**Ryan Campbell (ryan.campbell@d1.pseudoco.org)**  
Explore device performance metrics, connection quality to application cloud and collaboration tools. Monitor real-time CPU, memory, Wi-Fi strength, and view summarized security and application events for user safety. [Help](#)  
Last updated Mar 20, 2024, 21:51

← Experience Insights

**User Details**

User: Ryan Campbell (ryan.campbell@d1.pseudoco.org)  
Username: Ryan Campbell  
Region: Wichita, Kansas, US  
Hostname: RCAMBELL-DESKTO

**Device Details**

Device name: RCAMBELL-DESKTO  
Public IP address: 173.37.58.43  
Client version: 1.191.2  
OS Version: VMware7.1 Microsoft Windows 10 Enterprise N

**Performance**

CPU Usage: 100.00 %  
System, CPU Level

Memory Usage: 79.61 %  
System, Memory

Ethernet Link: 1000 Mbps  
Network

**Endpoint Agent to Cisco Secure Access Cloud**

Endpoint: RCAMBELL-DESKTO  
Local Network: ethernet: Intel(R) 82574L Gigabit Network Connection  
Destination: Secure Access

Avg Latency (ms)	Max Latency (ms)	Min Latency (ms)	Jitter (ms)	Loss (%)	Destination IP Address
21	22	21	0	0	44.239.28.172

**Suggested Remediation**

- Close any unnecessary or background applications and browser tabs to improve the device's performance
- Restart your computer to allow system components to be flushed and for the cleanup of temporary files and processes.

**Collaboration Application Summary** (Last 24 hours)

**WEBEX APPLICATION SCORE**  
Visited Pages - Application Score: 99.9 (0.0% mean)

**LATENCY**  
54.0 ms (Expected > 60 ms)

**JITTER**  
0.7 ms (Expected < 60 ms)

**LOSS**  
0.0% (No change, Expected 3% - 5%)

Connected user details

Identify local wifi, CPU, memory errors that influence connectivity to apps

Connection quality from endpoint to Secure Access

Suggested remediation tips to help reduce mean time to resolution

UcaaS monitoring

# What does Secure Access call Healthy?

Here are the threshold values that establish the health status of endpoints and your network.

## Endpoint thresholds

Metric	Green	Yellow	Red
CPU	<80	80 < value < 95	>95
Memory	<80	80 < value < 95	>95
Wifi signal	>40	40 > value > 20	<20

## Network thresholds to data center destination

Metric	Green	Yellow	Red
Jitter	<30	30 < value < 40	>40
Packet loss	<10	10 < value < 20	>20
Average latency	<100	100 < value < 150	>150

# Correlate App and Network Performance

Common SaaS applications Performance ⓘ

Search  Israel (Tel Aviv) Status  20 applications

Status	Application	URL (Domain)	Response Time ⓘ	Response Code	Description	Time	Location
✓	AWS	aws.amazon.com	319 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Bing	www.bing.com	253 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Box	www.box.com	228 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Confluence	confluence.atlassian.com	152 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	DocuSign	www.docusign.com	425 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Dropbox	www.dropbox.com	945 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Figma	www.figma.com	719 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Gmail	mail.google.com	212 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Google Docs	docs.google.com	248 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Google Drive	drive.google.com	239 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Google Workspace	workspace.google.com	142 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Jira	jira.atlassian.com	465 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Microsoft 365	www.office.com	531 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Monday.com	monday.com	191 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Outlook	outlook.office.com	290 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Salesforce	www.salesforce.com	167 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	SharePoint	sharepoint.com	856 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Smartsheet	www.smartsheet.com	182 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Splunk	www.splunk.com	218 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Workday	www.workday.com	109 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)

- This view provides quick dashboard access to the top 20 SaaS apps and their performance from every Secure Access DC
- Quickly diagnose regional performance issues
- Measured using ThousandEyes Enterprise Agents (not configurable)



# New and roadmap



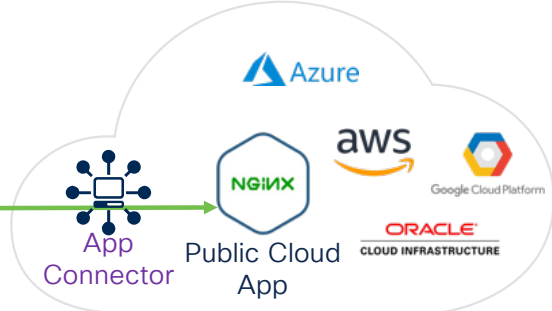
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Confidential

# Hybrid Zero Trust Network Access (ZTNA)



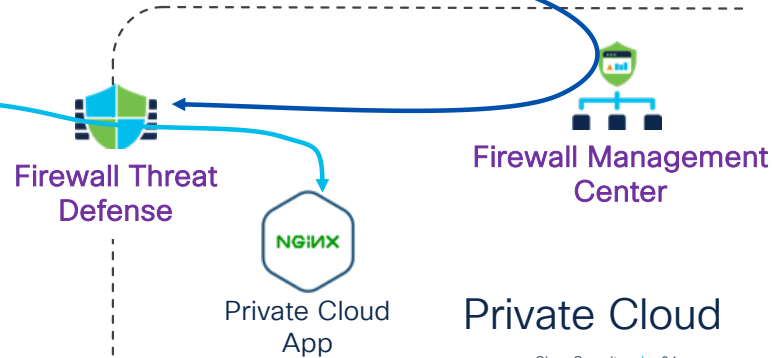
2. **Secure Client** creates a control connection to **Secure Access**. It is used to authenticate and authorize application access and select the appropriate edge device based on policy or proximity.



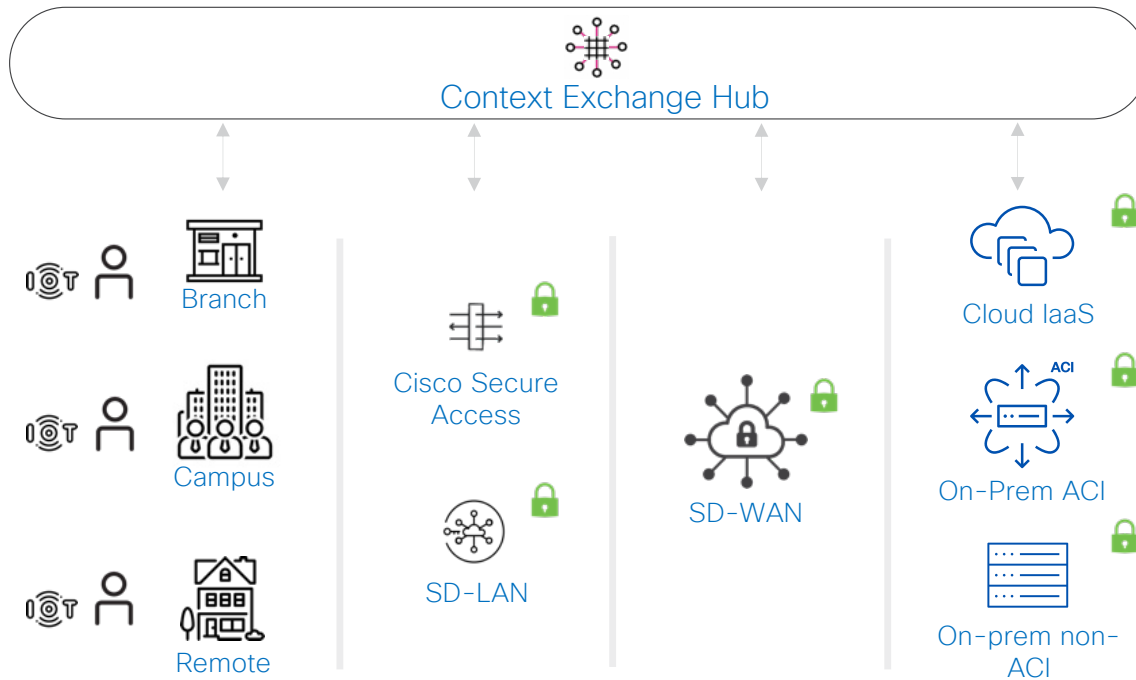
1. **Secure Access** provisions private Firewall instances with appropriate private application access policies.

3. Per-application tunnels to public apps or private apps requiring advanced inspection features (e.g. DLP) go through **Secure Access** and **App Connectors**.

4. Eligible per-application tunnels to private apps are automatically directed to closest edge **Firewall Threat Defense** instance for full threat inspection.



# Common Policy



- ✔ Build context in its local domain and store it as standard security group tags (SGT)
- ✔ Share context everywhere, across networking and security domains
- ✔ Enforce consistent SGT based policies, enable simple and unified policy experience

✔ Context-aware policies for on-prem app and cloud workloads for multiple enforcement points

# Cisco's flexible approach simplifies migration

Accelerate your SSE and SASE journey with zero trust

- ✓ You set the pace of ZTNA adoption
- ✓ Same client
- ✓ Common policy



## Traditional VPN

Network level access –  
cannot control at app level



## VPN as-a-Service

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



## Unified ZTNA

Granular controls at the  
application level + VPNaaS and  
Digital Experience Monitoring



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

CISCO *Live!*

BRKSEC-2079





[Demo on youtube](#)