

Configure Universal ZTNA for Private Resource Access on Secure Access

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[About Universal ZTNA](#)

[Network Detection](#)

[Types for Enforcement](#)

[Use Cases](#)

[Architectural Components](#)

[Packet Flow](#)

[Configure](#)

[Network Diagram](#)

[Test Cases](#)

[Test Case 1 - Remote User - Cloud Enforcement](#)

[Test Case 2 - Remote User - Local Enforcement](#)

[Test Case 3 - Local User - Local Enforcement](#)

[Test Case 4 - Local and RemoteUser - Local or Cloud Enforcement with TND](#)

[Troubleshoot](#)

[Useful Commands:](#)

Introduction

In this document we will cover the configuration for Private Resource Access via Universal ZTNA with different traffic paths.

Prerequisites

Following configuration must be completed prior to Universal ZTNA configuration

- [Identity Provider on Cisco Secure Access](#)
- [Enroll Devices in Zero Trust Access Using Certificates](#)
- [Configure Tunnels with Cisco Secure Firewall](#)
- [Remote Access Virtual Private Network](#)
- [Resource Connector on Secure Access](#)

- [FTD onboarding on Security Cloud Control](#)
- *Hybrid ZTNA* feature flag should be enabled for respective Secure Access Tenant , contact Cisco TAC to enable the flag

Requirements

Cisco recommends that you have knowledge of these topics:

- IPsec VPN configuration on Cisco Secure Access and Firewall Threat Defense
- Identity Provide (IdP) - User Provisioning from Active Directory
- Remote VPN configuration on Cisco Secure Access
- Resource Connector Deployment on Cisco Secure Access
- ZTA Certificate based Enrollment
- Certificate - OpenSSL , CSR generation , Certificate Templates etc.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall Threat Defense (Version 7.7.10)
- Cisco Secure Firepower Management Center (Version 7.7.10)
- Cisco Secure Client (ZTA Version 5.1.10.1720)
- Windows 11
- Windows 2019 Server - Certificate Authority
- Resource Connector on ESXi

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

About Universal ZTNA

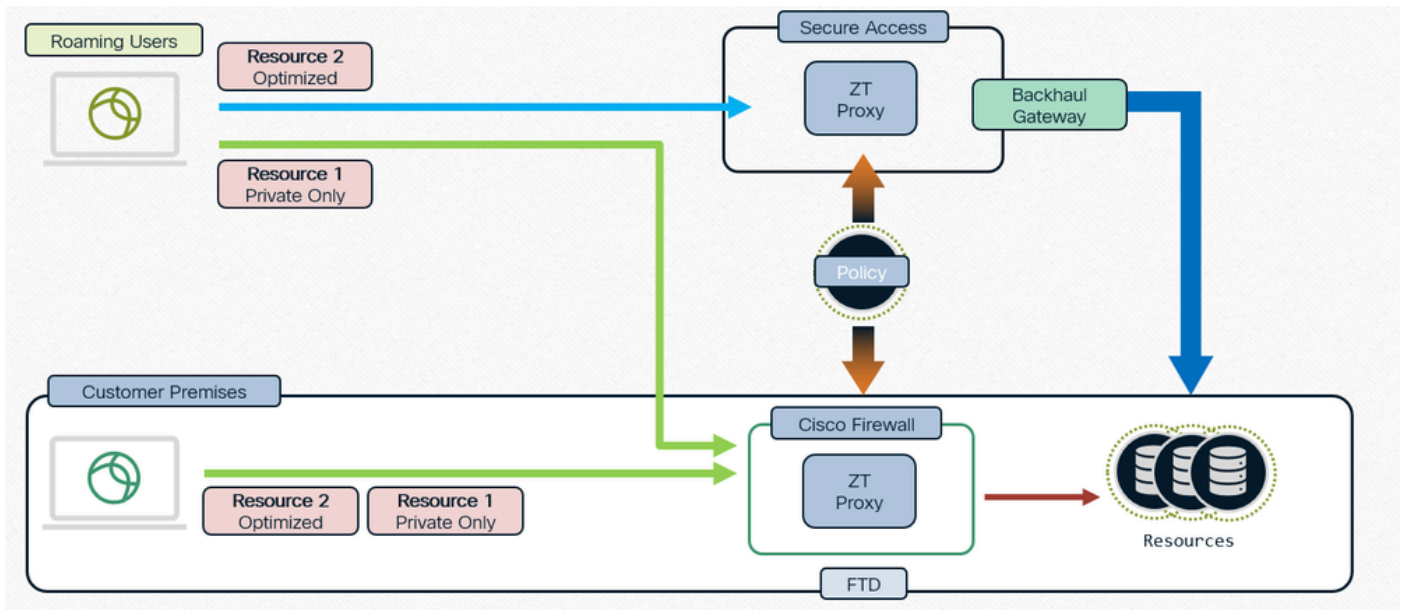
Universal zero trust network access (uZTNA) enables administrators to specifically allow access to internal network resources according to user identity (including user trust and posture), and without granting access to the entire network as with RA-VPN. uZTNA enables administrators to secure internal resources and applications for both remote and on-premises users.

Because uZTNA does not assume that access granted to one application implicitly authorizes access to other applications, the network attack surface is reduced.

Secure Access evaluates the access policy. Any access control policies deployed to devices from the Secure

Firewall Management Center are ignored.

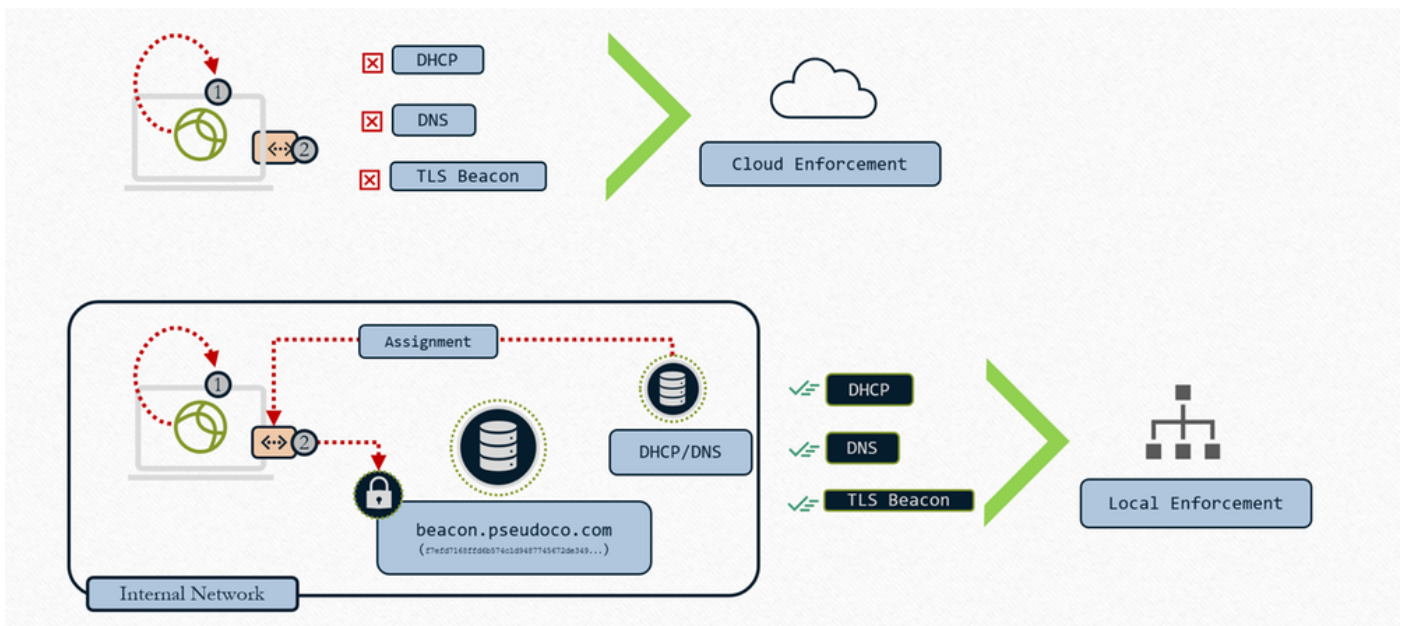
Traffic proxying, as well as IPS, file, and malware policy enforcement, is performed on the Firepower Threat Defense (FTD).



Single Policy, Distributed Enforcement

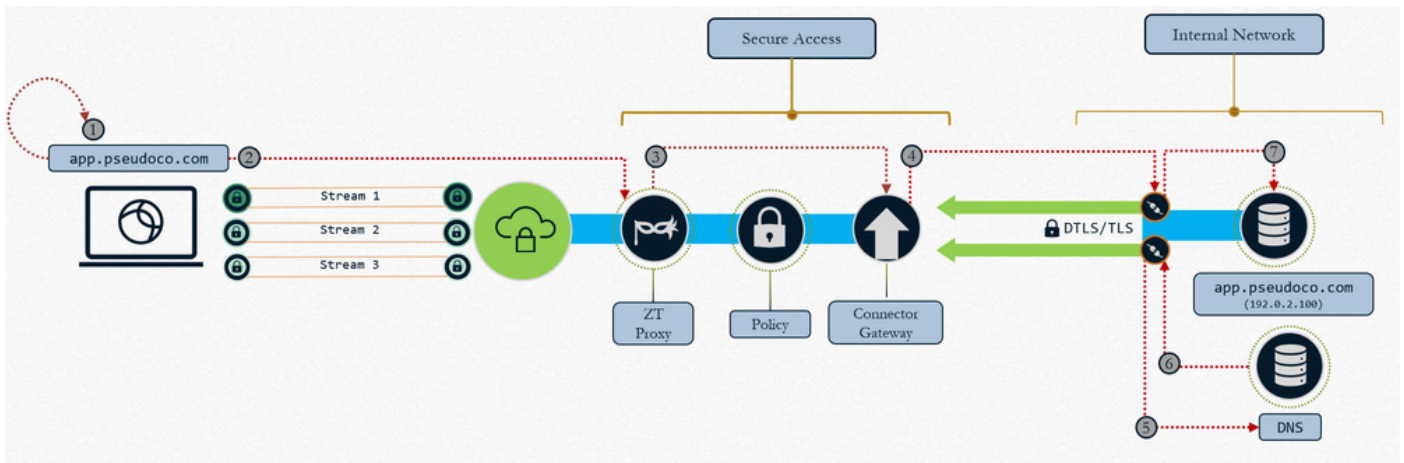
Network Detection

Determine Cloud or Local Enforcement



2. Authentication Control traffic is sent to Secure Access Cloud for policy evaluation
3. Cloud returns redirect to FTD for data plan enforcement (if policy allows)
4. Traffic steered to firewall configured headend (interface)
5. Policy defined in cloud is enforced (IPS, Malware, Decryption) using local proxy data plane
6. Event logged and duplicate shipped to cloud for consistent reporting
7. Firewall does DNS resolution on local network to route resource traffic (if allowed)
8. Firewall builds connection to resource(new connection built to resource) as the firewall behaves as a TCP proxy

- **Cloud Enforcement path : OFF Network**

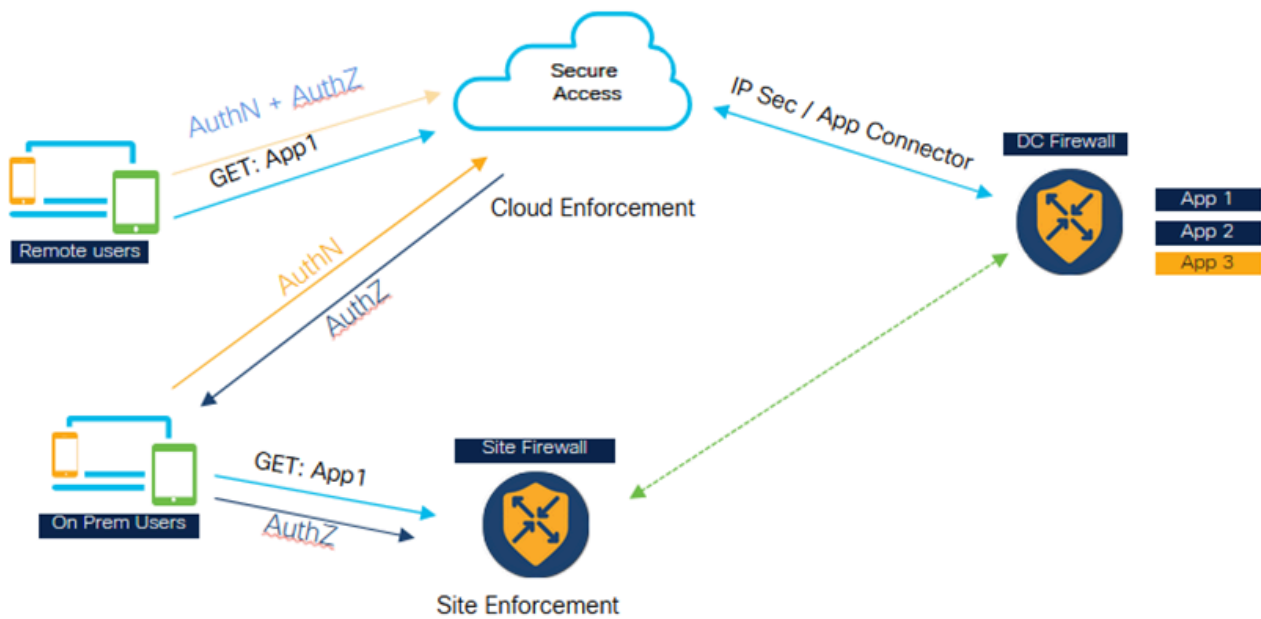


Universal ZTNA : Cloud Enforcement

1. User Requests App, client captures and resolves request to ephemeral IP (localhost range)
2. Traffic is transported to Zero Trust Proxy in Secure Access
3. TCP connection is proxied and built to the mapped resource connector, Policy is enforced on traffic
4. Gateway establishes connection to resource connector
5. Resource connector resolves resource IP
6. Local DNS responds with resource IP
7. Resource connector establishes connection to resource

Use Cases

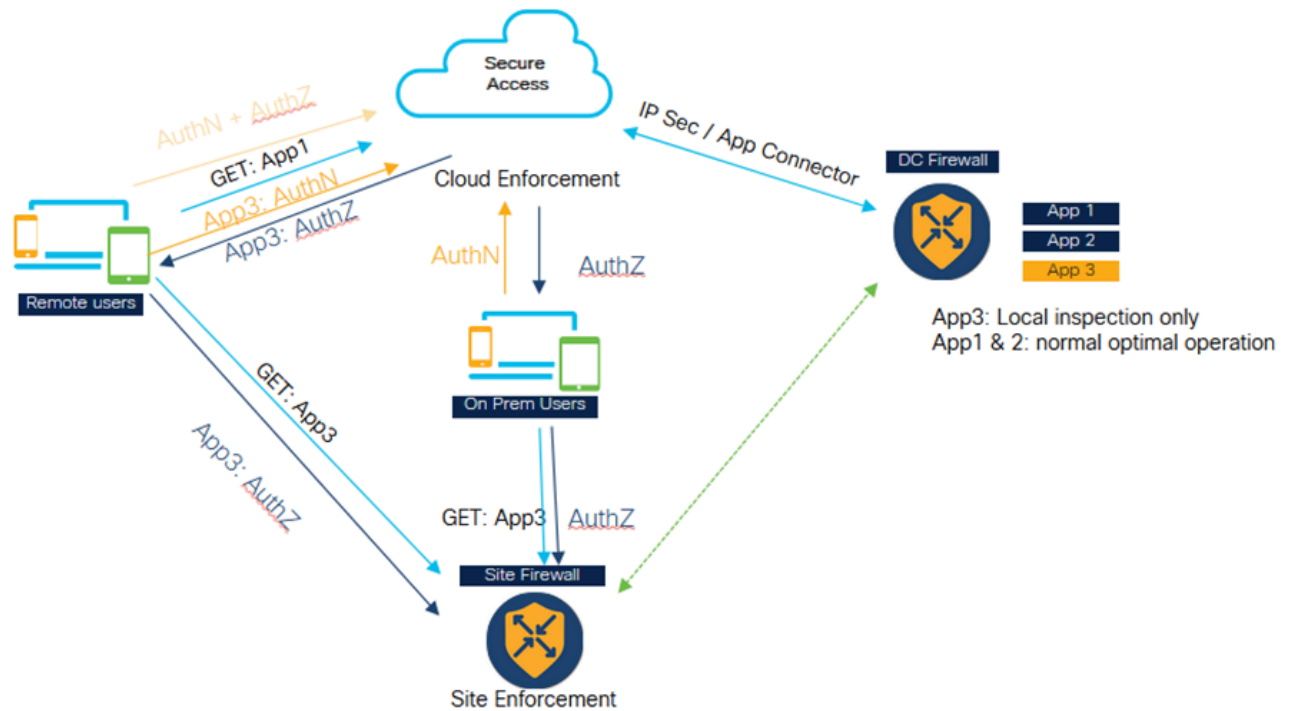
Case 1 : Consistent and Optimized ZTNA for users when on premise



Universal ZTNA - Consistent and Optimized ZTNA (On-premise user)

- Secure Access and Firewall both are configured to protect the application.
- If the user is remote, then they will go to Secure Access for policy evaluation and inspection.
- If the user is Internal/On premises then they will go to the firewall for private traffic inspection.
- On premise user can still go to Secure for authentication and evaluation just the Datapath traffic goes to the Firewall and inspected as per the policy configuration.
- The internal user accessing the application through the firewall has a performance advantage as it avoids the traffic going to cloud and then backhauling to the datacenter

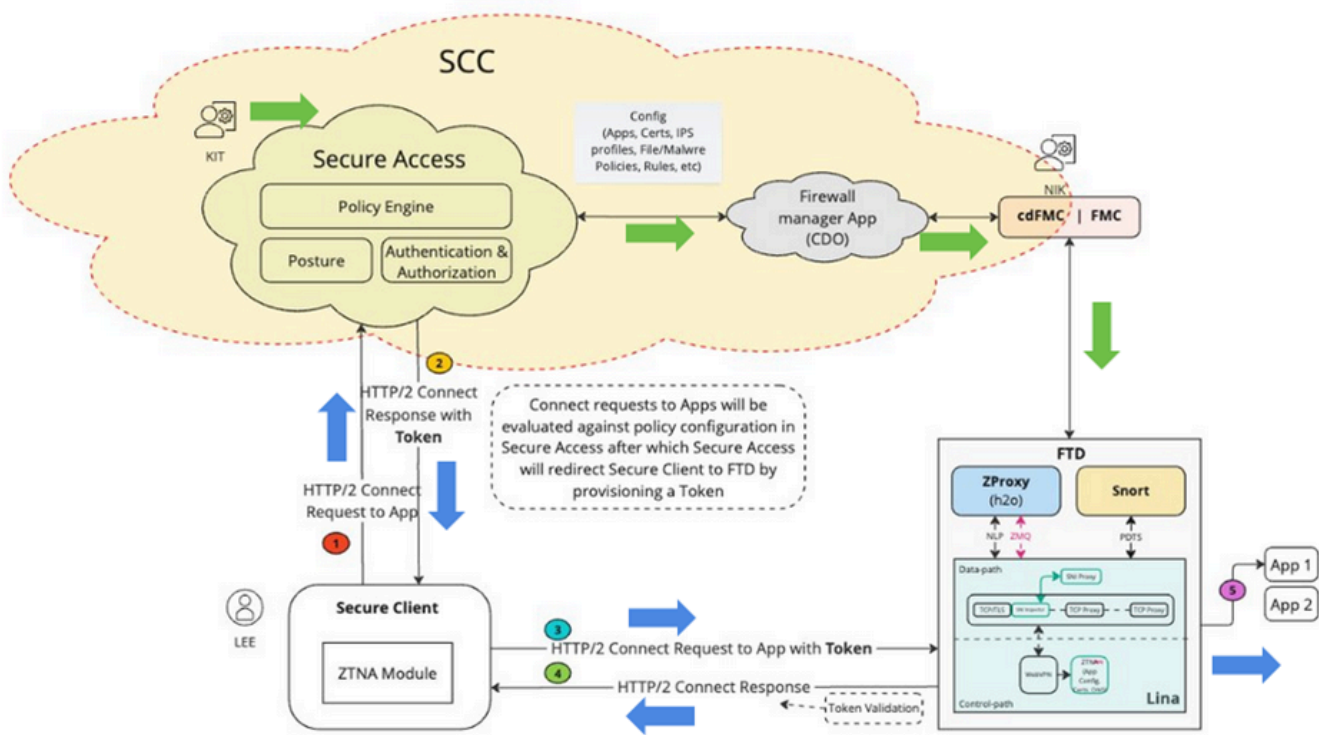
Case 2 : Private Inspection for Sensitive applications



Universal ZTNA - Private Inspection for Sensitive Applications

- Certain critical applications can be configured to always be accessed through the firewall.
- The app data traffic does not need to go to cloud. Example, there might be sensitive data application like source code, which customer doesn't want to go to cloud.
- In such scenarios, both remote and on-prem user traffic always goes through the firewall and gets inspected. However, again, in this scenario, authentication and policy evaluation is always happening in the cloud, only the data part traffic goes through the firewall.

Architectural Components



Universal ZTA - Architectural Components

Security Cloud Control (SCC) is the primary manager for uZTNA solution. uZTNA is the first feature to be built on top of SCC.

In SCC, we have two micro-applications Secure Access and Firewall. Once SCC is provisioned and the required feature flags are enabled, we will be able to see these micro-applications on the left side of the SCC panel.

Secure Client: In Secure Client we will have to enable Zero Trust Access Module (ZTNA) we need to enroll into ZTNA module to be able to access the applications.

Firewall Threat Defense: FTD protecting these applications. FTD runs a ZT proxy which is also known as H2O (same as the proxy runs in Secure Access Cloud)

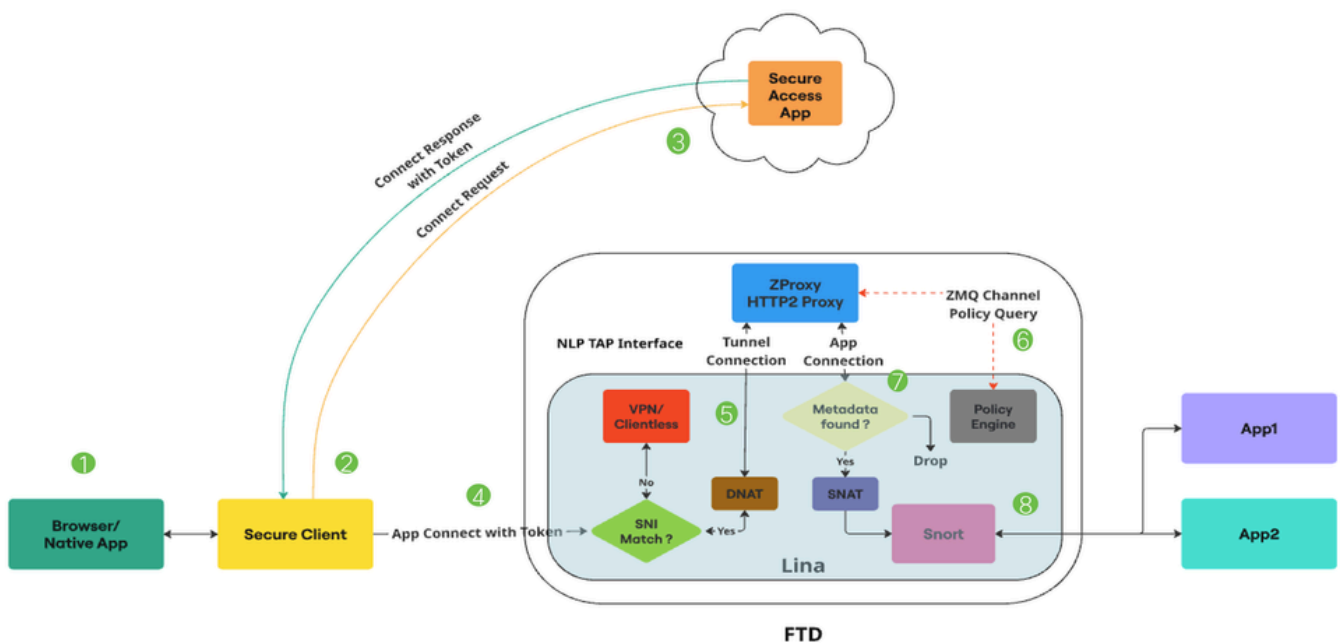
Now when a user (e.g. KIT) configures a private resource and policy on Secure Access micro-application, this configuration will be pushed to Firewall micro-application in SCC. Firewall application understands the internals of FTD, FTD configuration, how to deploy and manage the configuration on FTD. So, Firewall app validates this configuration, and it invokes the FMC APIs to push the configuration to FMC and then eventually get it deployed on FTD. FTD can have an auto deployment option enabled so that Admins (e.g. Nick) don't have to do manual deployment.

1. When a user (e.g. Lee) tries to access an application, secure client connects to Secure Access using mTLS channel. Secure Access authenticates the user using the client device certificate. It then evaluates the authorization, posture and other policies that are configured for that user and for that application.

- Secure Access ,if it finally finds that the application is being protected by Firewall then it generates an auth token , which tells the firewall that this is already authenticated and authorized. The auth token is encrypted, signed by Secure Access
- Secure Access redirects the Secure client towards FTD along with the auth token.
- Secure Client establishes another connection to FTD , it is a HTTP2 connection over mTLS channel. It sends a CONNECT request for the application being accessed along with the Token.
- FTD now validates the Token, if the Token is validated successfully then the user is allowed to access that application. FTD then sends the acknowledgment back to the Secure Client

Packet Flow

Universal ZTNA detailed packet flow



Universal ZTA - Packet flow

- User attempts to access an application through a web browser or a native application.
- The Secure Client intercepts the connection and identifies it as a user trying to access a Private Resource.
- The Secure Client establishes a mTLS connection to Secure Access, requesting access to the application. Secure Access checks the Universal ZTNA policies and posture profiles for compliance. If everything is fine, Secure Access generates an Access Token containing essential information such as user details, application details, and IPS/File policy.

4. The Access Token is encrypted and signed by Secure Access. Secure Access then redirects the Secure Client along with the token to the FTD.

5. When packet reaches the Lina Datapath, the SNI checker intercepts the connection and verifies if the Server Name (SNI Extension) in the Client Hello matches the Proxy FQDN configured on the device. If SNI matches, connection is directed to ZProxy. If SNI does not match, the connection is directed to other features which can coexist with Universal ZTNA.

For Example : VPN, Captive Portal or Clientless ZTNA. ZProxy, which supports MASQUE over HTTP/2 protocol will be running on the FTD as a Non-Lina Process on dedicated cores. The communication between Lina and ZProxy utilizes the NLP Tap Interface, for handling data traffic. The destination IP of the connection is translated to the TAP interface IP by the SNI checker.

6. When the ZProxy receives the mTLS Tunnel Connection from Secure Client, it verifies the Client Device Certificate sent by Secure Client. It also verifies the Access Token sent with the APP Connect. There is a Zero MQ channel between Lina and ZProxy. It is primarily used to exchange control messages. ZProxy uses this channel for FQDN resolution of Private resources by communicating with Lina.

Zero MQ Channel is also used to propagate information present in the access token to Lina. (Example : Rule ID, Policy ID etc) Lina receives the access token information and stores it in a metadata db.

7. Once the control messages are exchanged, ZProxy initiates a new connection towards the private resource. This can be TCP or UDP. Lina then performs a metadata db lookup for this app connection. If the metadata is not found, Connection is dropped

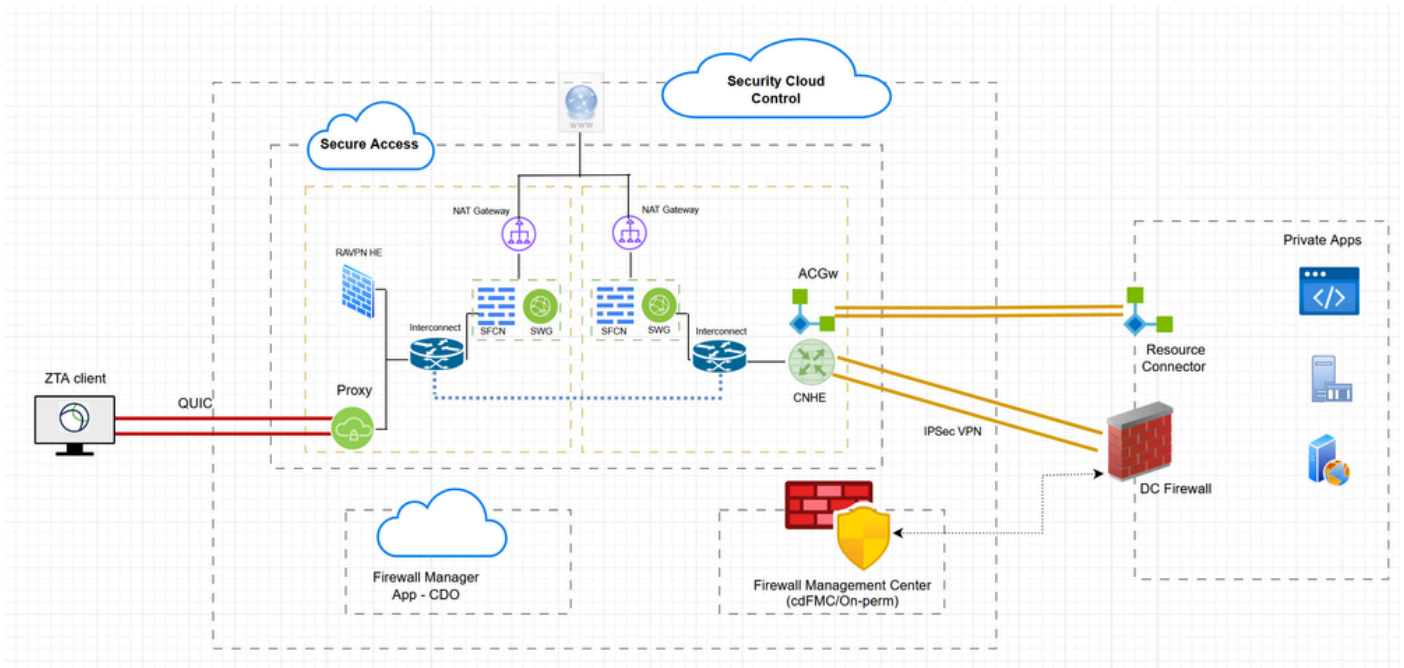
8. Since the app connection is originating from ZProxy, it will have an Internal IP (example: 169.251.1.2) as Source IP. This will be translated to the FTD egress interface IP, before sending it out. Lina then marks Universal Zero Trust flows for Snort inspection only if a File or IPS policy is present in the access token. The Rule ID obtained from the access token is passed to Snort in the connection metadata.

9. Universal Zero Trust rules and corresponding File and IPS policy mappings are pushed to the FTD via the FMC. The Zero Trust plugin in Snort will load these rules during initialization. Lina will mark the Universal Zero Trust stream flows for Snort inspection only if a File or IPS policy is mentioned in the access token obtained from Secure Access for accessing that Private Resource.

Rule ID obtained from the access token is passed to Snort via Conn Meta. For all Universal Zero Trust stream flows, the Zero Trust plugin in Snort will perform a rule lookup for the rule ID obtained from the Conn Meta. If a rule match is found, the flow will be allowed, and the IPS and File policies specific to that rule will be applied to the flow. If no rule match is found, the Zero Trust plugin in Snort will block the flow.

Configure

Network Diagram

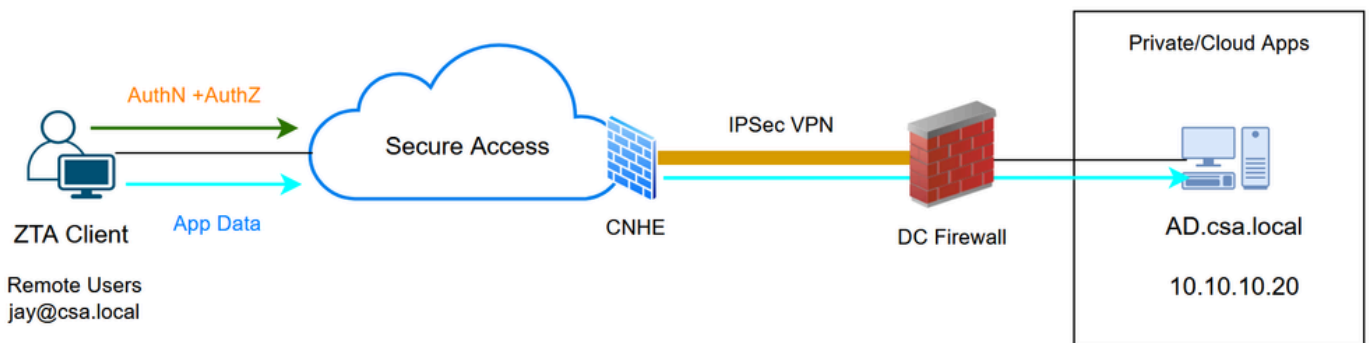


Hybrid ZTNA - Network Diagram

Test Cases

Test Case 1 : Remote User - Cloud Enforcement

In this test case, we will be accessing a private resource over Network Tunnel Group via Cloud Enforcement. In this case both policy evaluation and application data will be intercepted by Secure Access via ZTA module. This is a traditional flow where private application can be accessed from ZTA enrolled client via Network Tunnel Group or Resource Connector

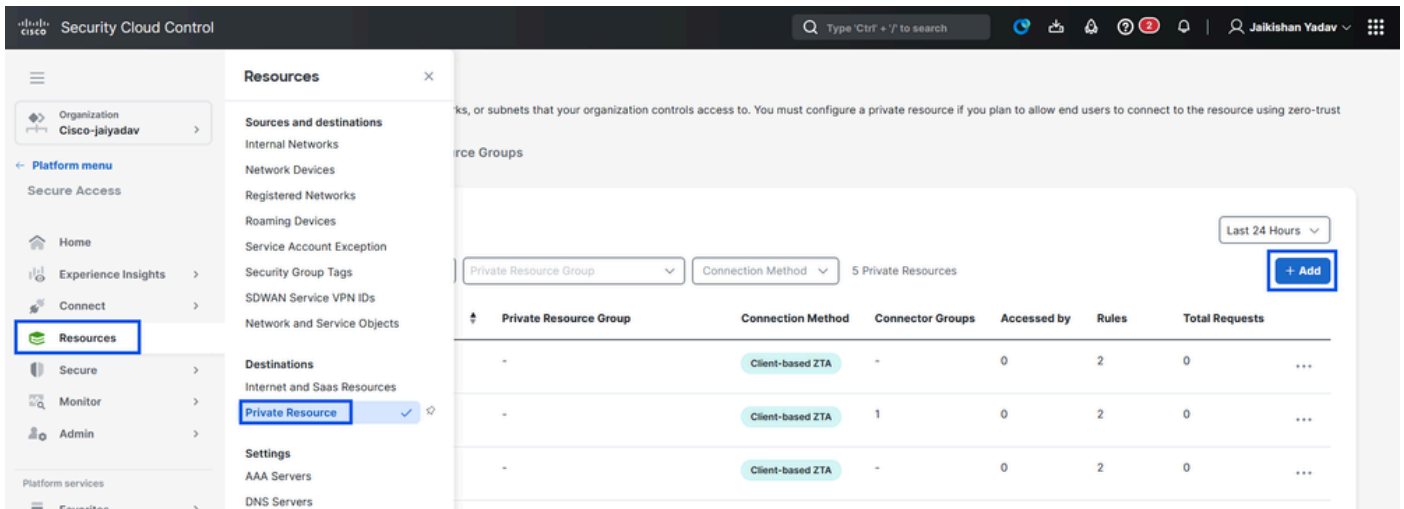


Universal ZTA - Test case topology

Step 1 - Define a Private Resource on Secure Access

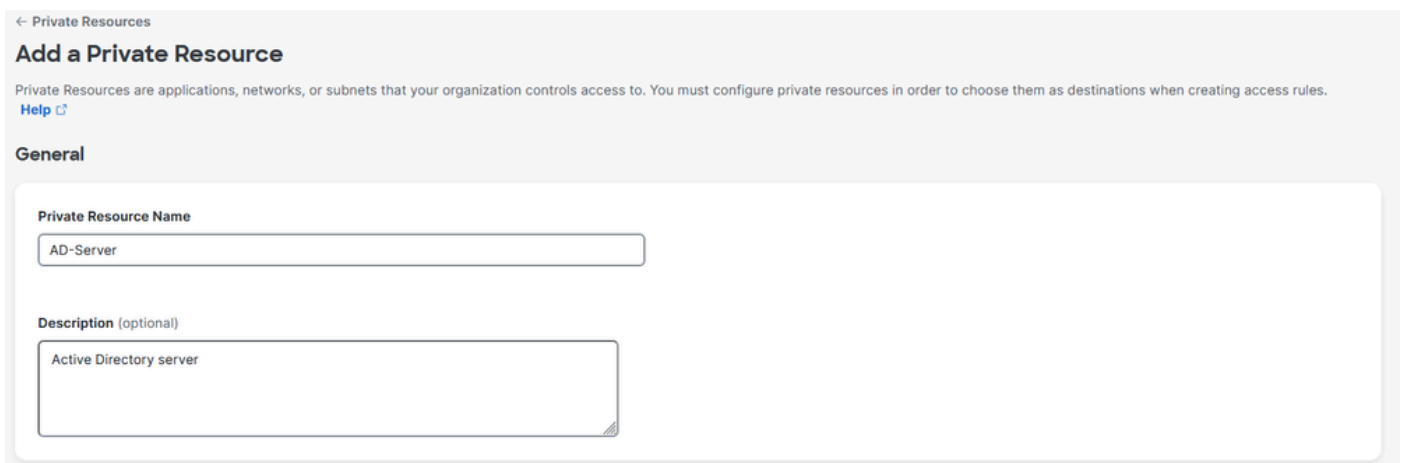
Configure a private resource to be accessible via Zero Trust Access (ZTA) enrolled device with cloud enforcement

1. Navigate to **Resources > Destinations > Private Resources > Click on +Add**



Secure Access - Private Resource Configuration

2. For **Private Resource Name**, enter a meaningful name for the resource. For **Description**, we recommend that you provide information such as the purpose of the resource or the name of the resource owner.



Secure Access - Private Resource Configuration

3. Enter the FQDN of the private resource you want to access . We can also define the IP address of the private resource . For more information see [Add a Private Resource](#)

4. Select the internal DNS server to resolve the domain

Private resource address

Define how the private resource will connect to applications through Secure Access.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges	
<input type="text" value="ad.csa.local"/>	TCP - RDP ▾	<input type="text" value="Any"/>	+ Protocol & Port
Remove			
<input type="text" value="10.10.10.20"/>	TCP - RDP ▾	<input type="text" value="Any"/>	+ Protocol & Port
Remove + IP Address/FQDN			

Use internal DNS server to resolve the domain PrivateDNS (10.10.10.20) ^

Internal DNS Server

Secure Access - Private Resource Configuration

5. Select Endpoint Connection Methods

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).

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Enforcement point for Remote and Local Users

```
graph LR; RemoteUser[Remote user] --- Internet[via Internet]; TrustedUser[User in a trusted network] --- Internet; Internet --- SecureAccessCloud[Secure Access Cloud]; SecureAccessCloud --- PrivateResource[Private Resource]
```

[Cancel](#) [Save and Test](#) [Save](#)

Secure Access - Private Resource Configuration

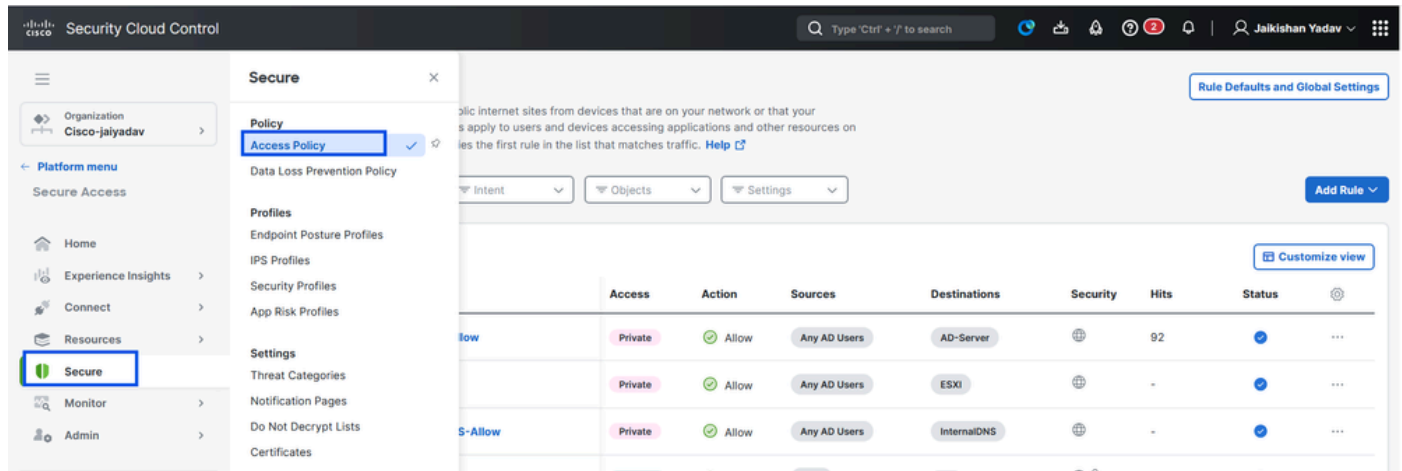
6. Click Save

Step 2 - Create Private Access Rule

Configure a private access on Secure Access to be access by Universal ZTA enrolled users . For more

information see [Private Access Rule](#)

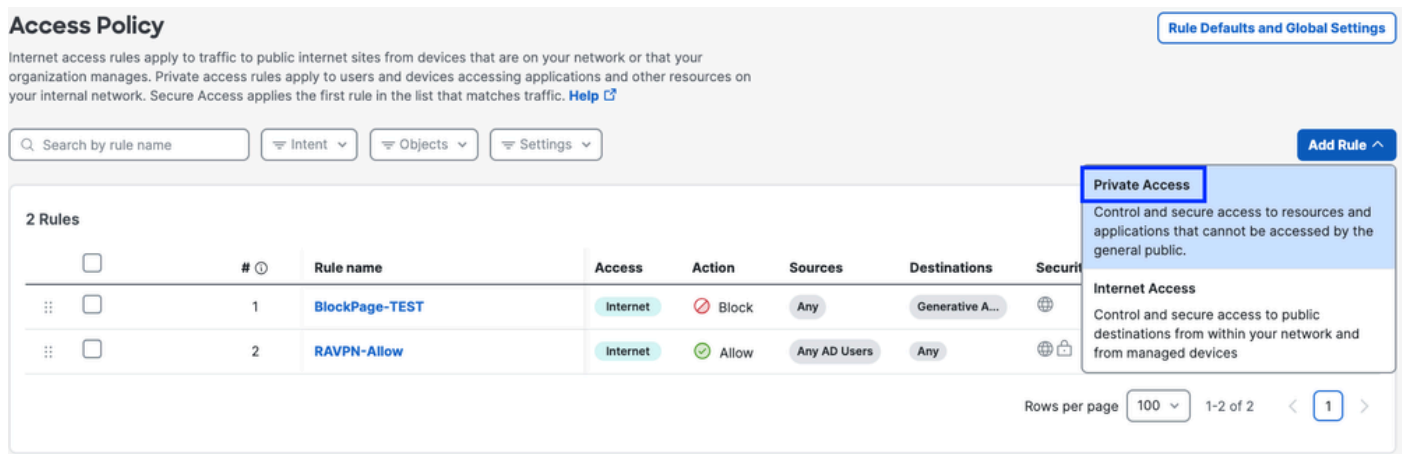
1. Navigate to **Secure > Access Policy**



Secure Access - Access Policy Configuration

2. Click **Add Rule**, and then choose **Private Access**.

At the top of the rule is a summary that describes the configured components of your rule.



Secure Access - Access Policy Configuration

3. Add a Rule Name

Add AD-RDP-Allow

Create a rule to control and secure access to specified private applications and other destinations on your network. For an end-to-end guide to completing prerequisites and configuring a rule, see [Help](#)

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

AD-RDP-Allow

Rule order

1

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

To

Secure Access - Access Policy Configuration

4. Select the rule action and select source and destination

Rule name

AD-RDP-Allow

Rule order

1

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.

AD Users • Any AD Users

To

Specify one or more destinations.

Private Resources • AD-Server

+ AND

Secure Access - Access Policy Configuration

5. Configure Endpoint Requirements

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: **AD-Server**

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 [Rule Defaults](#) Disabled

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](#)

2 Configure Security

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

[Cancel](#)

[Back](#)

[Next](#)

Secure Access - Access Policy Configuration

6. Configure Security

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](#)

Security Profile [Rule Defaults](#)

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

Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**

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

Secure Access - Access Policy Configuration

7. Click on Save

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](#)

Search by rule name Intent Objects Settings

[Add Rule](#)

3 Rules [Customize view](#)

#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
1	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server		-	On
2	BlockPage-TEST	Internet	Block	Any	Generative A...		-	On
3	RAVPN-Allow	Internet	Allow	Any AD Users	Any		492	On

Rows per page: 100 1-3 of 3 < 1 >

Default Access Rules

Rule name	Action	Sources	Destinations	Security	Posture
For all private access	Block	Any	Any private destination	-	-
For all Internet access	Allow	Any	Any Internet destination		-

Secure Access - Access Policy Configuration

Step - 3 Add Private Resource to the ZTA Profile

If you are using a custom ZTA profile then you need to add the respective private resource to the ZTA profile

1. Navigate to **Connect > End User Connectivity > Zero Trust Access** and Click on **+ZTA Profile**

End User Connectivity [Cisco Secure Client](#) [Manage servers](#)

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

Zero Trust Access Virtual Private Network Internet Security

Enrollment methods [Manage](#)

Before users can access resources using client-based Zero Trust Access, their endpoint devices must be enrolled. Manage enrollment methods for your organization here. [Help](#)

Windows and macOS devices enroll using: [SSO Authentication](#) [Certificates](#)

Android and iOS devices enroll using SSO Authentication only.

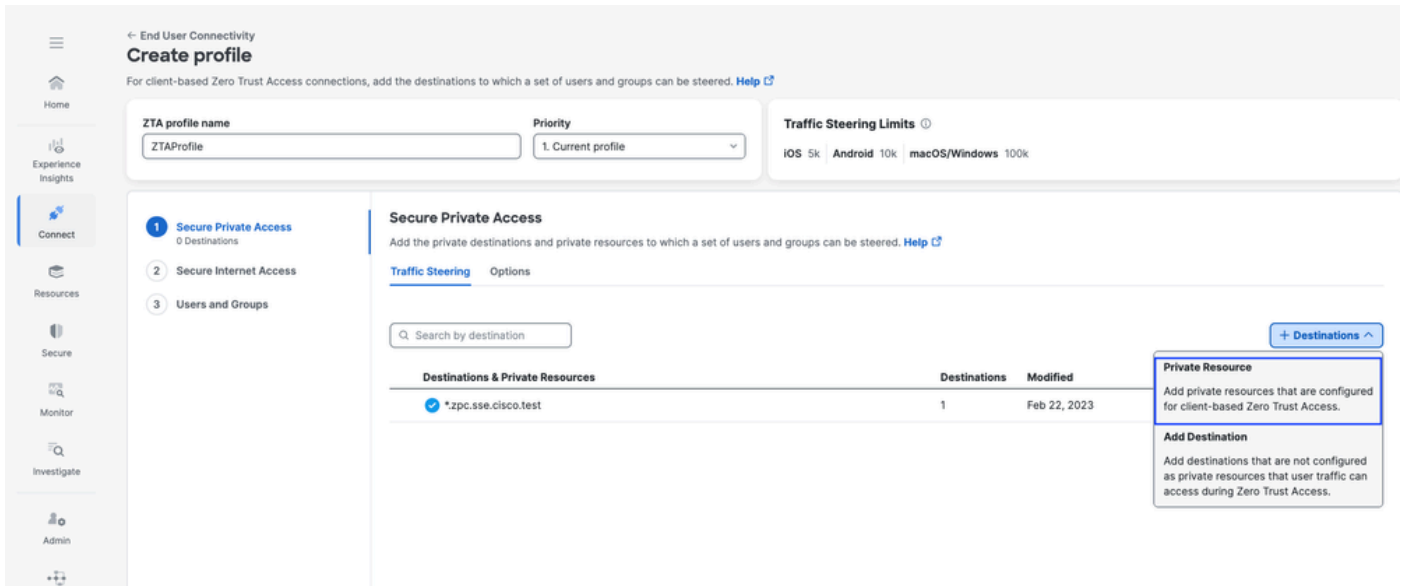
Zero Trust Access Profiles [Manage Trusted Networks](#) [+ ZTA Profile](#)

Manage Zero Trust Access (ZTA) profiles, which allow you to add users and groups to unique traffic steering configurations for client-based ZTA connections. [Help](#)

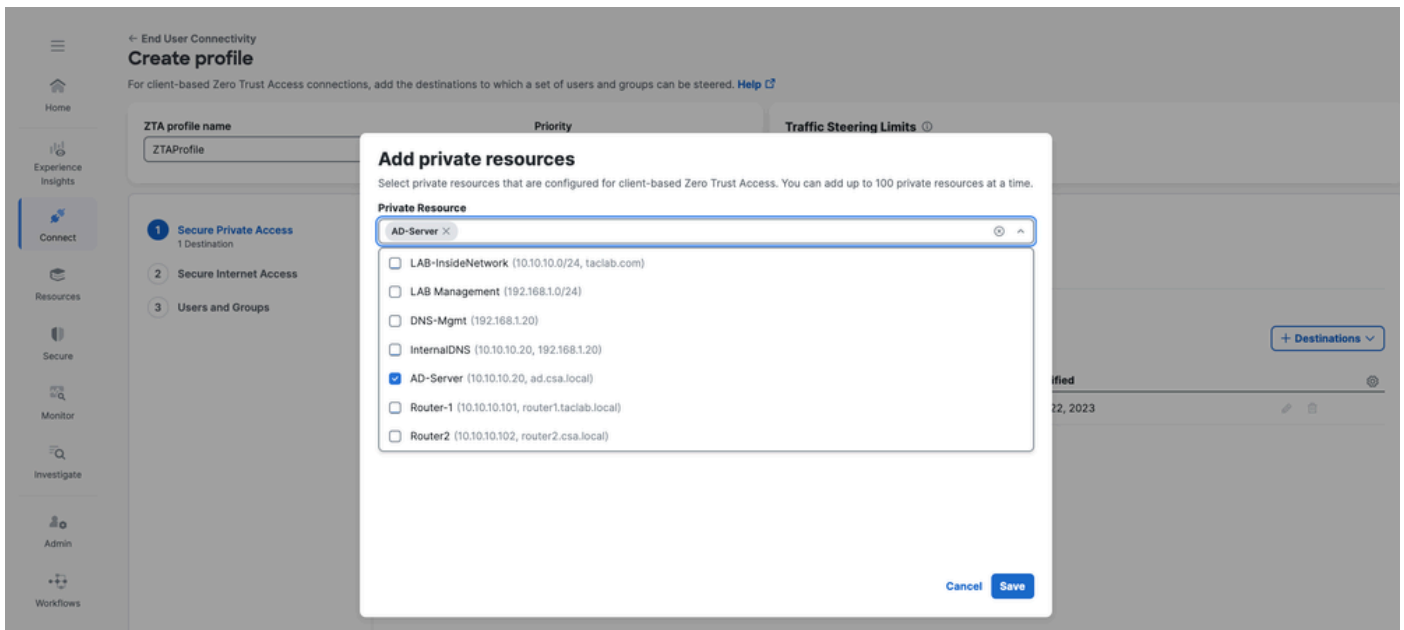
#	Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
<p>No ZTNA profiles created.</p>					

Secure Access - ZTA Profile

2. Add the Private Resource



Secure Access - ZTA Profile



Secure Access - ZTA Profile

3 . Add Users and Groups

← End User Connectivity
Create profile
 For client-based Zero Trust Access connections, add the destinations to which a set of users and groups can be steered. [Help](#)


ZTA profile name: ZTAProfile | Priority: 1. Current profile | Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

- Secure Private Access (2 Destinations)
- Secure Internet Access
- Users and Groups**

Users and Groups
 Add a set of users and groups that will be steered to various destinations added to this ZTA profile

Users: 0 | Groups: 0

Q Search + Users and Groups

Name	Email	Type	Users
 No users + Users and Groups			

ZTA profile name: ZTAProfile | Priority: 1. Current profile | Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

- Secure Private Access (2 Destinations)
- Secure Internet Access
- Users and Groups**

Users and Groups
 Add a set of users and groups that will be steered to various destinations added to this ZTA profile

Users: 1 | Groups: 0

Q Search + Users and Groups

Name	Email	Type	Users
jay (jay@csa.local)	jay@gmail.com	User	-

Rows per page: 10 < >

Back Close

Secure Access - ZTA Profile

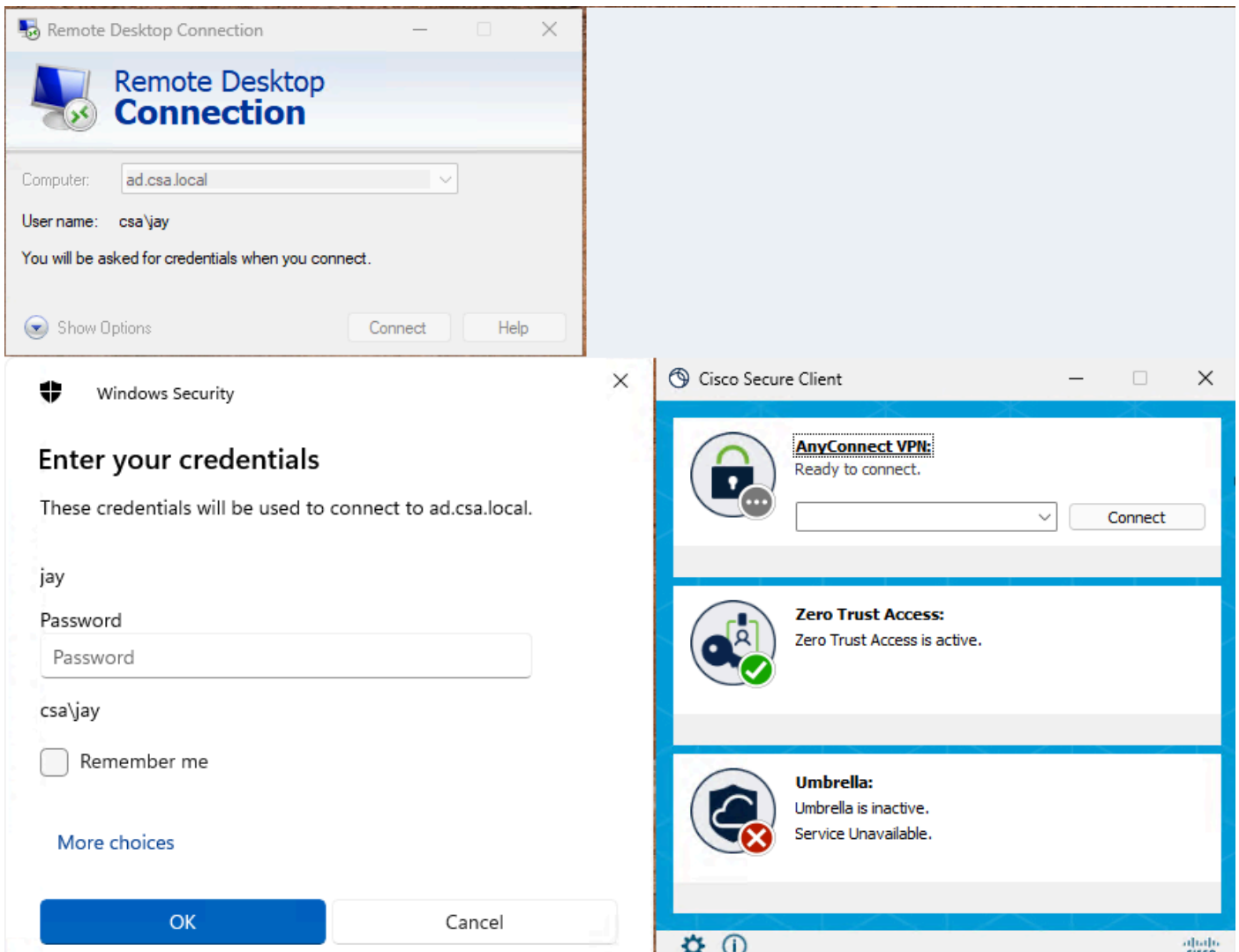


Note: It may take upto 15-20 minutes push and sync the configuration to the client for the assigned Private Resource

Step - 4 Verify access to the Private Resource

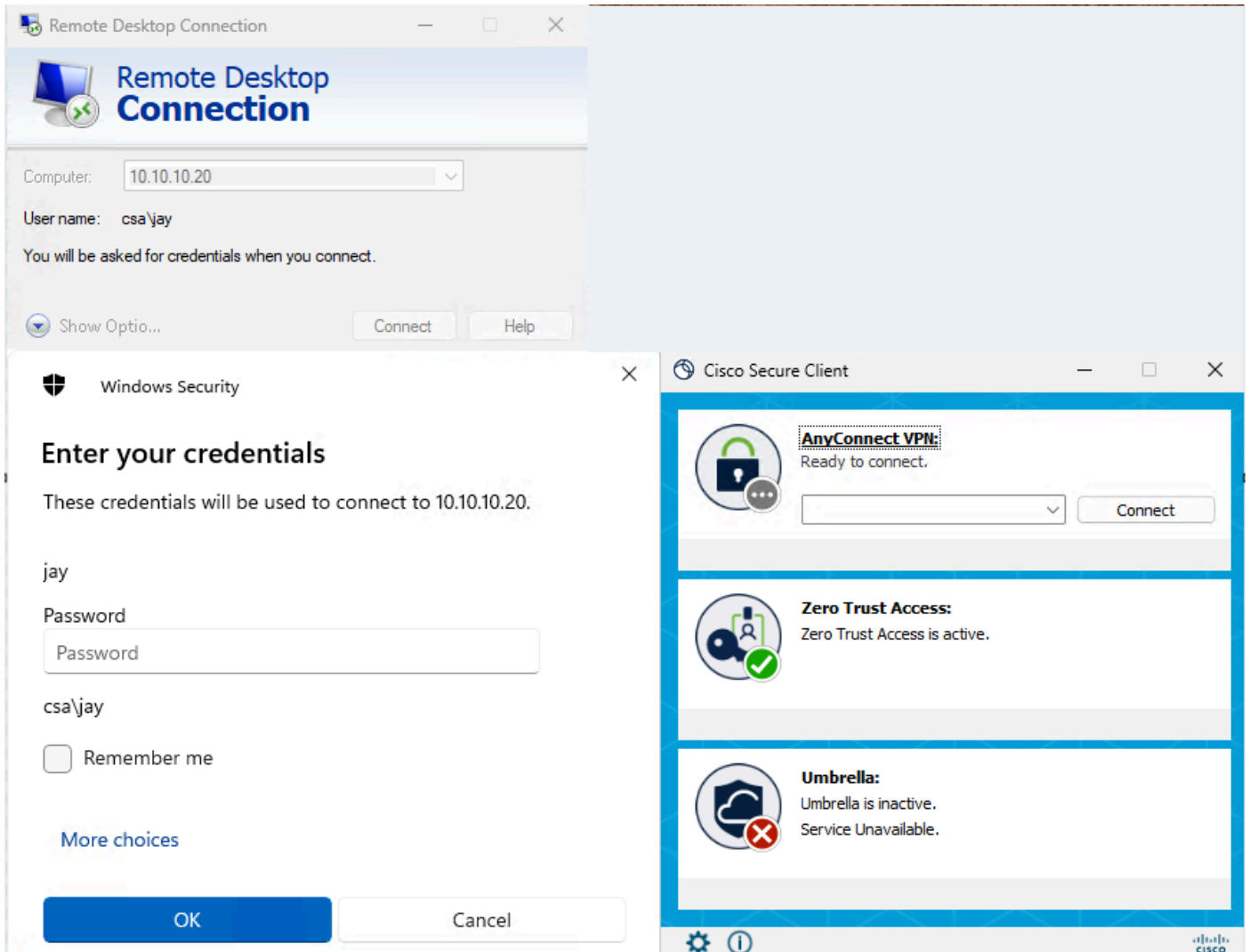
1. Access the Private Resource

Access the PR using FQDN



Secure Access - PR Testing

Access the PR using IP address



Secure Access - PR Testing

2. Verify with the Activity Search events

Activity Search

Schedule Export CSV LAST 24 HOURS

FILTERS Search by domain, identity, or URL Advanced CLEAR Saved Searches Customize Columns ZTA Client-based

IP ADDRESS 10.10.10.20 RESPONSE Allowed Restore to default layout Save Search

3 Total Viewing activity from Jan 11, 2026 4:49 AM to Jan 12, 2026 4:49 AM Page: 1 Results per page: 50 1 - 3 of 3

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Applica
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	ad.csa.local	10.10.10.20:3389	3389	Allowed	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	ad.csa.local	10.10.10.20:3389	3389	Allowed	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	ad.csa.local	10.10.10.20:3389	3389	Allowed	AD-Server

Secure Access - Activity Search

Activity Search

10.10.10.20
 3389

3 Total
Viewing activity from Jan 11, 2026 4:53 AM to Jan 12, 2026 4:53 AM

Allowed Advanced Blocked

AD Users AD Groups AD Devices SAML Users

Secure Access Cloud FTD Umbrella Cloud

Request	Source	Action	Destination	Destination IP	Destination Port
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389

Event Details

Identity: jay (jay@csa.local)

Win1

Rule Name: AD-RDP-Allow

Resource/Application: AD-Server

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: ad.csa.local

Destination IP: 10.10.10.20

Page: 1 Results per page: 50 1 - 3 of 3

Secure Access - Activity Search

10.10.10.20

9 Total
Viewing activity from Jan 11, 2026 5:51 AM to Jan 12, 2026 5:51 AM

Allowed Advanced Blocked

AD Users AD Groups

Request	Source	Action	Destination	Destination IP	Destination Port	Resource/Application	Zero Trust Access Profile	Rule Name	OS
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server	Default ZTA Profile	AD-RDP-Allow	win
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server	Default ZTA Profile	AD-RDP-Allow	win
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server	Default ZTA Profile	AD-RDP-Allow	win
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server	Default ZTA Profile	AD-RDP-Allow	win

Page: 1 Results per page: 50 1 - 9 of 9

Secure Access - Activity Search

Activity Search

Schedule Export CSV LAST 24 HOURS

Search by domain, identity, or URL Advanced CLEAR

Filters: IP ADDRESS 10.10.10.20 X Restore to default layout Save Search

9 Total Viewing activity from Jan 11, 2026 5:51 AM to Jan 12, 2026 5:51 AM Page: 1 Results per page: 50 1 - 9 of 9

Request	Source	Action	Destination	Destination IP	Destination Port	Resource/Application
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	10.10.10.20	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server
ZTA CLIENT-BASED	jay (jay@csa.local)	Allowed	ad.csa.local	10.10.10.20:3389	3389	AD-Server

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 12, 2026 5:51 AM

Access details

Identity: jay (jay@csa.local)

Win1

Rule Name: AD-RDP-Allow

Resource/Application: AD-Server

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: 10.10.10.20

Destination IP

Secure Access - Activity Search

3. Verify FMC connection events

Events Troubleshooting

Destination Port / ICMP Code 3389

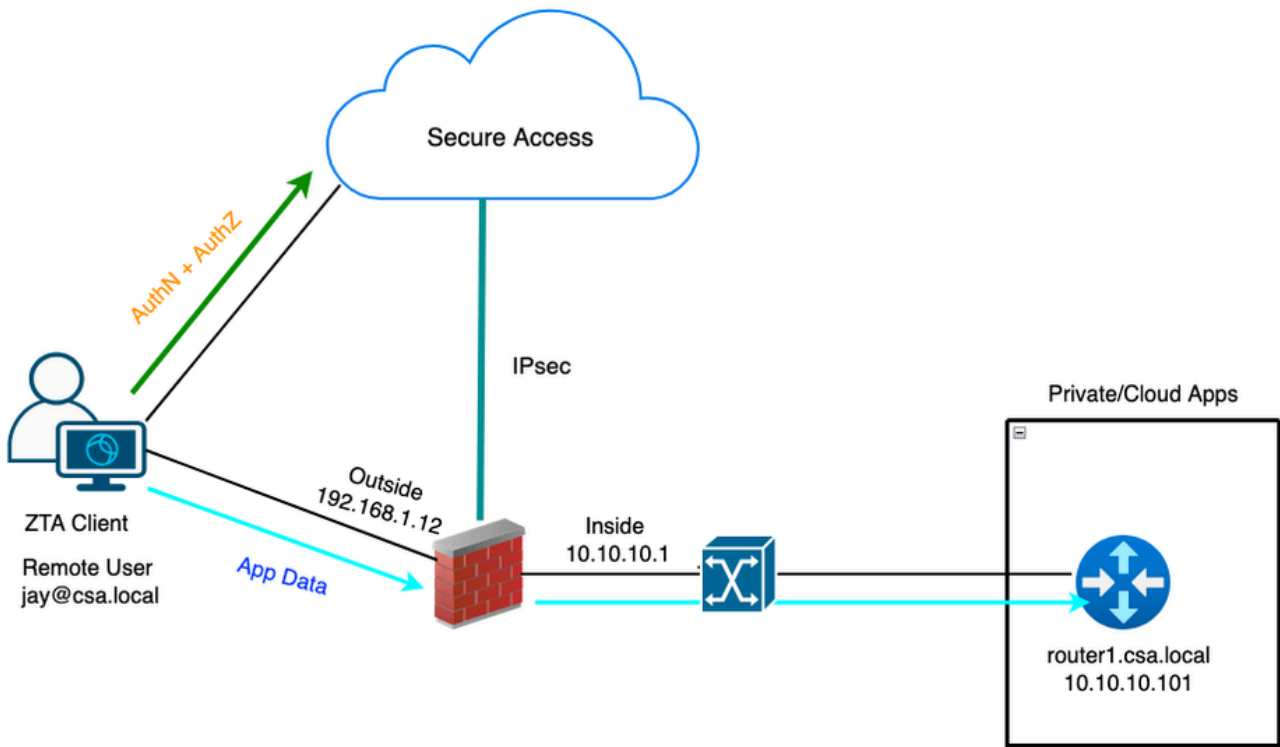
7 events

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP...	Web Application	Access Control Rule
2026-01-12 00:51:24	Connection	Fastpath		100.112.20.48	10.10.10.20	17674 / tcp	3389 / tcp		
2026-01-12 00:51:20	Connection	Fastpath		100.112.20.48	10.10.10.20	47021 / tcp	3389 / tcp		
2026-01-12 00:51:15	Connection	Fastpath		100.112.20.48	10.10.10.20	63712 / tcp	3389 / tcp		
2026-01-12 00:48:24	Connection	Fastpath		100.112.20.48	10.10.10.20	50756 / tcp	3389 / tcp		
2026-01-12 00:42:34	Connection	Fastpath		100.112.72.18	10.10.10.20	60548 / tcp	3389 / tcp		
2026-01-12 00:15:21	Connection	Fastpath		100.112.72.16	10.10.10.20	40660 / tcp	3389 / tcp		
2026-01-12 00:12:45	Connection	Fastpath		100.112.72.16	10.10.10.20	44262 / tcp	3389 / tcp		

FMC Connection Events

Test Case 2 - Remote User - Local Enforcement

Accessing a Private Resource via Local enforcement, in this type of enforcement policy evaluation happens on Secure Access but the application data stays local to FTD. For example, a ZTA enrolled client or user connected to home network and trying to access a private resource which is behind FTD inside interface.



Universal ZTA - Test case topology

Step 1 - Define a Private Resource on Secure Access

Configure a private resource to be accessible via Zero Trust Access (ZTA) enrolled device with cloud enforcement

1. Navigate to **Resources > Destinations > Private Resources > Click on +Add**

Private Resource Group	Connection Method	Connector Groups	Accessed by	Rules	Total Requests	
-	Client-based ZTA	-	0	2	0	...
-	Client-based ZTA	1	0	2	0	...
-	Client-based ZTA	-	0	2	0	...

Secure Access - Private Resource Configuration

2. For **Private Resource Name**, enter a meaningful name for the resource. For **Description**, we recommend that you provide information such as the purpose of the resource or the name of the resource owner.

← 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
Router1

Description (optional)
Router1 PR for UZTNA testing

Secure Access - Private Resource Configuration

3. Enter the FQDN of the private resource you want to access . We can also define the IP address of the private resource . For more information see [Add a Private Resource](#)

4. Select the internal DNS server to resolve the domain

Private resource address

Define how the private resource will connect to applications through Secure Access.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR)	Protocol	Port / Ranges	
router1.csa.local	Any TCP	22	+ Protocol & Port
Remove			
10.10.10.101	Any TCP	22	+ Protocol & Port
Remove + IP Address/FQDN			

Use internal DNS server to resolve the domain PrivateDNS (10.10.10.20) ^

Internal DNS Server
PrivateDNS (10.10.10.20)

Secure Access - Private Resource Configuration

5. Select Endpoint Connection Methods

6. Select FTD as Local enforcement points

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).

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

FMC_F... Search by FTD na...

Traffic from users within a trusted network will get enforced at the selected Firewalls.

Enforcement point for Remote User



Enforcement point for Local user



Internal remote addresses are visible on end-user devices. If you want an address to be hidden, use an external address.

Change the remotely reachable addresses

Cancel

Save and Test Save

Secure Access - Private Resource Configuration



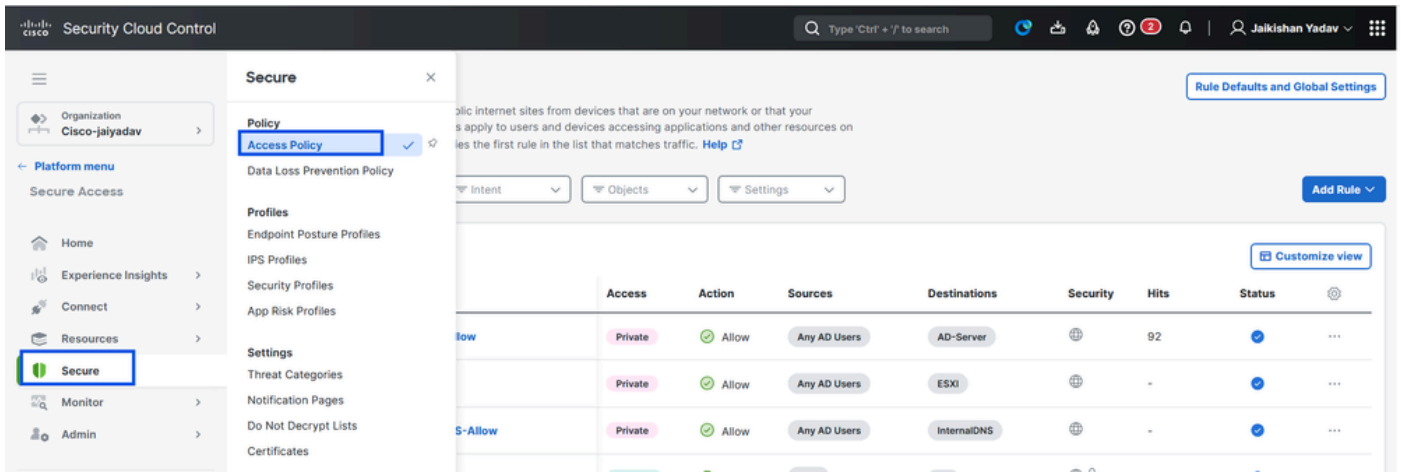
Note: Depending on the type of enrollment you select, this change will automatically associate the PR to the FTD and will trigger a policy deployment

7. Click Save

Step 2 - Create Private Access Rule

Configure a private access on Secure Access to be accessed by Universal ZTA enrolled users. For more information see [Private Access Rule](#)

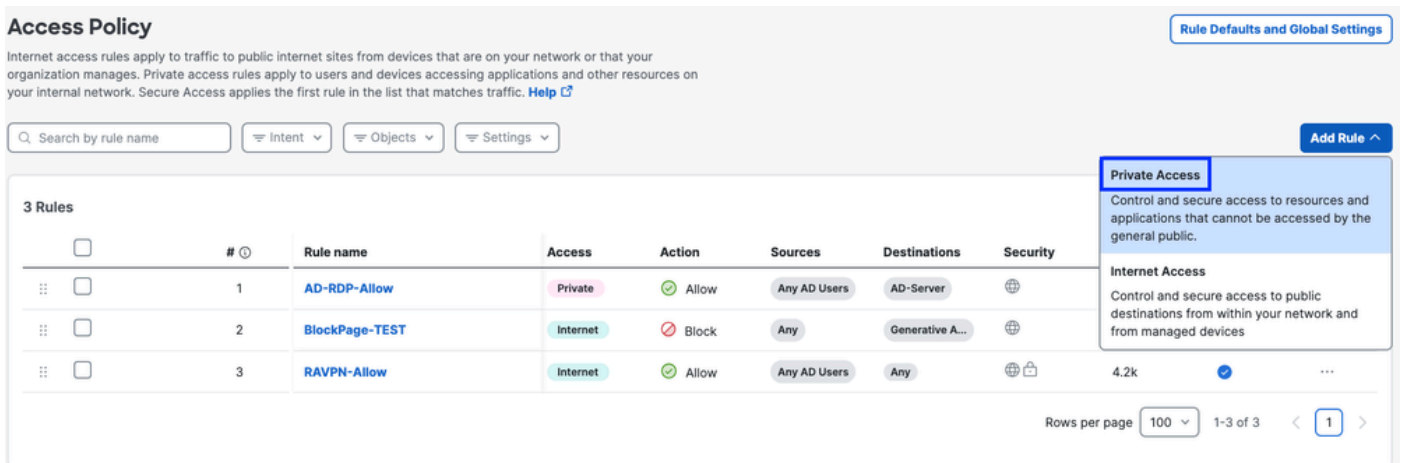
1. Navigate to **Secure > Access Policy**



Secure Access - Private Resource Configuration

2. Click **Add Rule**, and then choose **Private Access**.

At the top of the rule is a summary that describes the configured components of your rule.



Secure Access - Access Policy Configuration

3. Add a Rule Name

Add Router1-SSH

Create a rule to control and secure access to specified private applications and other destinations on your network. For an end-to-end guide to completing prerequisites and configuring a rule, see [Help](#)

Rule is enabled

Logging is enabled [Edit](#)

Summary

Sources

AD Users • Any AD Users



Allow

Security Controls

Destinations

Any private destination

Rule name ⓘ

Router1-SSH

Rule order

1

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.

Secure Access - Access Policy Configuration

4. Select the rule action and select source and destination

Rule name ⓘ

Router1-SSH

Rule order

1

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.

AD Users • Any AD Users



+ AND

To

Specify one or more destinations.

Private Resources • Router 1



Secure Access - Access Policy Configuration

5. Configure Endpoint Requirements

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: **Router-1**

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 [Rule Defaults](#)

Disabled

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](#)

2 Configure Security

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

[Cancel](#)

[Back](#) [Next](#)

Secure Access - Access Policy Configuration

6. Configure Security

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](#)

Security Profile [Rule Defaults](#)

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

Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**

[Cancel](#)

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

Secure Access - Access Policy Configuration

7. Click on Save

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](#)

Search by rule name Intent Objects Settings Add Rule

4 Rules Customize view

#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
1	Router1-SSH	Private	Allow	Any AD Users	Router1		-	✓
2	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server		-	✓
3	BlockPage-TEST	Internet	Block	Any	Generative A...		8.8k	✓
4	RAVPN-Allow	Internet	Allow	Any AD Users	Any		715	✓

Rows per page: 100 1-4 of 4 < 1 >

Secure Access - Access Policy Configuration

Step 3 - Verify the association of PR on the FTD

1. Navigate to **Connect > Network Connections > FTDs**

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has a 'Connect' menu item highlighted. The main content area shows the 'Connect' section with 'Network Connections' and 'FTDs' highlighted. The 'FTDs' section shows a status of '1 Connected' and a 'Warning' icon. Below this, there are filters for 'Region' and 'Status' and a '+ Add' button.

Secure Access - PR Verification

2. Click on the **FTD > View resources associated to this FTD**

Network Connections

Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see [Help](#)

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access

An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal Zero Trust Access to improve end-user experience and ensure consistent security controls for users independent of where they are connecting from [Help](#)

Q Search by FTD name FMC Name Configuration status 1 FTDs

FTD Name	Version	FMC	UZTA Configuration status	Associa
FMC_FTD Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	Synced	1

FMC_FTD

Firewall Details

Device FQDN ftd.csa.local
Auto deployment Yes

UZTA Configuration status

Synced Last synced at 31 Dec 2025, at 2:51 AM UTC

Assigned Trusted Network

Trusted network	Networks
LAN (Default trusted network)	1 DNS Servers

[Edit assignment](#) + [Trusted network](#)

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status
Synced 1

[View resources associated to this FTD](#)

[Associate Resources](#)

Secure Access - PR Verification

Resources associated with FMC_FTD

The following resources will get enforced on FMC_FTD when users connect to it from the trusted network LAN

Q Search by resource name

Configuration status

1 Resources

[Associate Resources](#)

Resource name

Status

Router1

Synced

[Close](#)

Secure Access - PR Verification

3. Click close

4. Verify the status , Associated Resource and Configuration should be in Synced state

The screenshot displays the Palo Alto Networks management console. On the left, the 'Network Connections' page shows a summary of '1 Synced' connections. Below this, a table lists 'FTDs configured for Universal Zero Trust Access'. The table has columns for 'FTD Name', 'Version', 'FMC', 'UZTA Configuration status', and 'Associated Resources'. The entry for 'FMC_FTD' shows a version of 'v10.0.0', FMC as 'FMC', a 'Synced' status (highlighted with a blue box), and 1 associated resource. On the right, a detailed view for 'FMC_FTD' is shown. It includes 'Firewall Details' (Device FQDN: ftd.csa.local, Auto deployment: Yes), 'UZTA Configuration status' (Synced, Last synced at 31 Dec 2025, at 2:51 AM UTC), 'Assigned Trusted Network' (LAN, 1 DNS Servers), and 'Associated Resources' (1 resource, Synced status highlighted with a blue box).

Secure Access - PR Verification

5. Verify the configuration has been pushed to FTD

Login to FTD cli and navigate to LINA mode

show running-config object application

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftd# sh run object application
object application PR_Router1
  id 427221
  internal domain router1.csa.local tcp eq 22
  internal subnet 10.10.10.101 255.255.255.255 tcp eq 22
  external domain router1.csa.local
  external subnet 10.10.10.101 255.255.255.255
ftd#
```

FTD - PR Verification

Step - 4 Add Private Resource to the ZTA Profile

1. Navigate to **Connect > End User Connectivity > Zero Trust Access** and click 3 dots to edit ZTA profile

The screenshot shows the 'Zero Trust Access Profiles' page. At the top, there are buttons for 'Cisco Secure Client' and 'Manage servers'. Below this, the 'Enrollment methods' section is visible, followed by the 'Zero Trust Access Profiles' section. A table lists the profiles, with one profile named 'ZTAPProfile' highlighted. A context menu is open over the 'ZTAPProfile' row, showing 'Edit' and 'Delete' options.

#	Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
1	ZTAPProfile	2 Destinations Trusted Networks Disabled	Use ZTA for all destinations 0 Exceptions Trusted Networks Disabled	1 Users 0 Groups	Jan 25, 2026

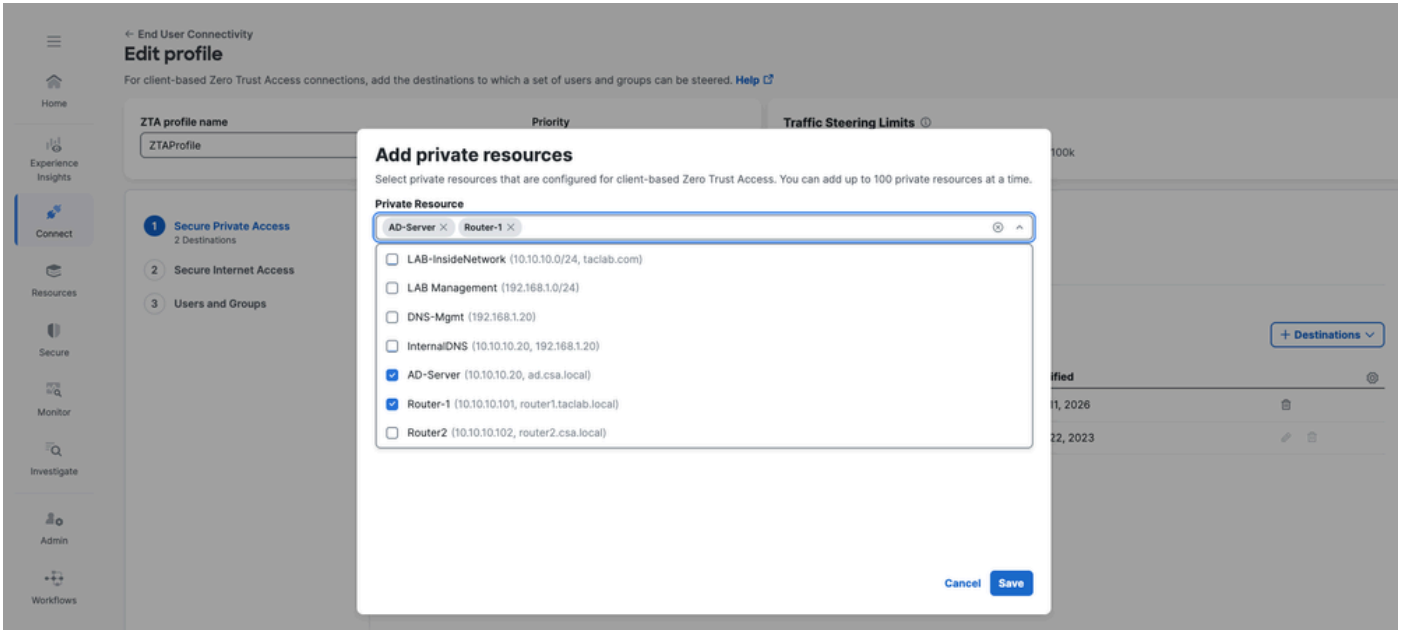
Secure Access - ZTA Profile

2. Add the Private Resource

The screenshot shows the 'Create profile' page. It includes a 'ZTA profile name' field with 'ZTAPProfile' and a 'Priority' dropdown set to '1. Current profile'. There are also 'Traffic Steering Limits' for iOS (5k), Android (10k), and macOS/Windows (100k). The 'Secure Private Access' section is active, showing a search bar and a table of destinations. A 'Destinations' button is visible, and a tooltip for 'Private Resource' is shown.

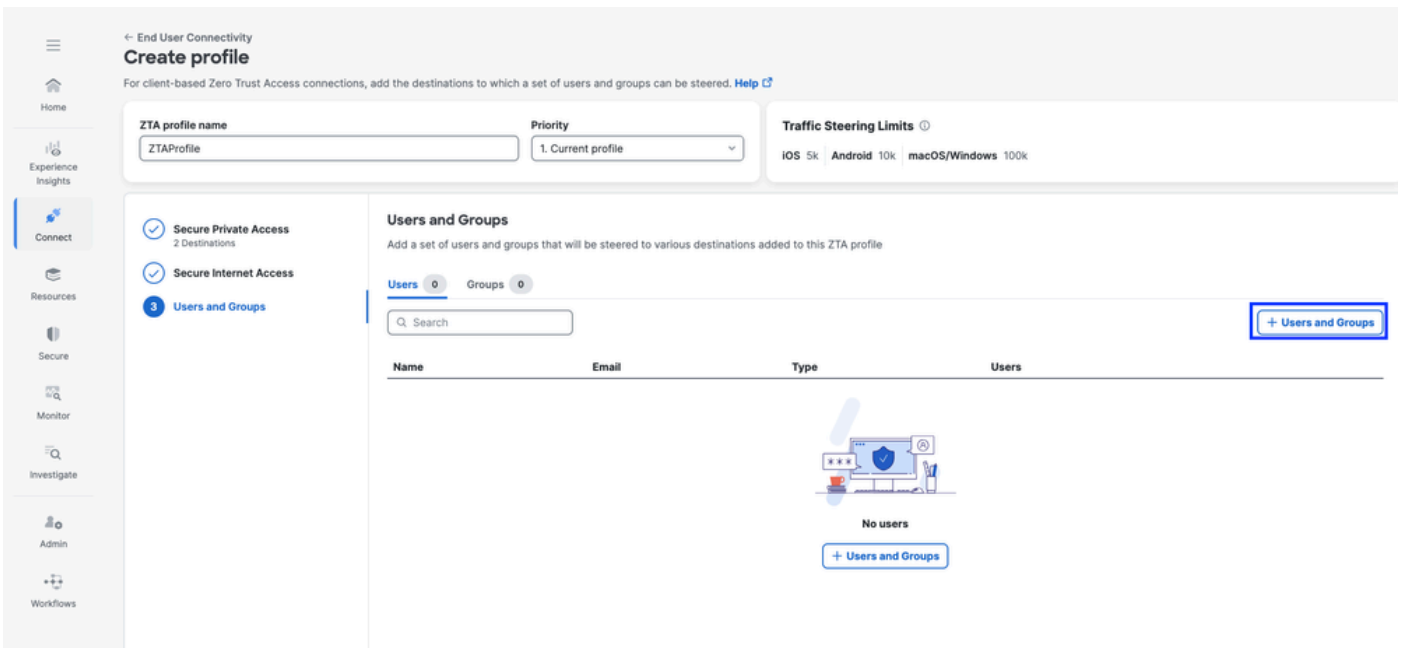
Destinations & Private Resources	Destinations	Modified
*zpc.sse.cisco.test	1	Feb 22, 2023

Secure Access - ZTA Profile



Secure Access - ZTA Profile

3 . Add Users and Groups



Secure Access - ZTA Profile

ZTA profile name: ZTAProfile | Priority: 1. Current profile | Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

- Secure Private Access (2 Destinations)
- Secure Internet Access
- Users and Groups**

Users and Groups
Add a set of users and groups that will be steered to various destinations added to this ZTA profile

Users: 1 | Groups: 0

Q Search + Users and Groups

Name	Email	Type	Users
jay (jay@csa.local)	jay@gmail.com	User	-

Rows per page: 10

Back Close

Secure Access - ZTA Profile

Step - 5 Verify access to the Private Resource

1. Verify the remote user can resolve FTD FQDN

```
PS C:\Users\jay> ping ftd.csa.local

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
PS C:\Users\jay> nslookup ftd.csa.local
Server: UnKnown
Address: 192.168.1.20

Name:     ftd.csa.local
Addresses: 192.168.1.12
```

Secure Access - PR Testing

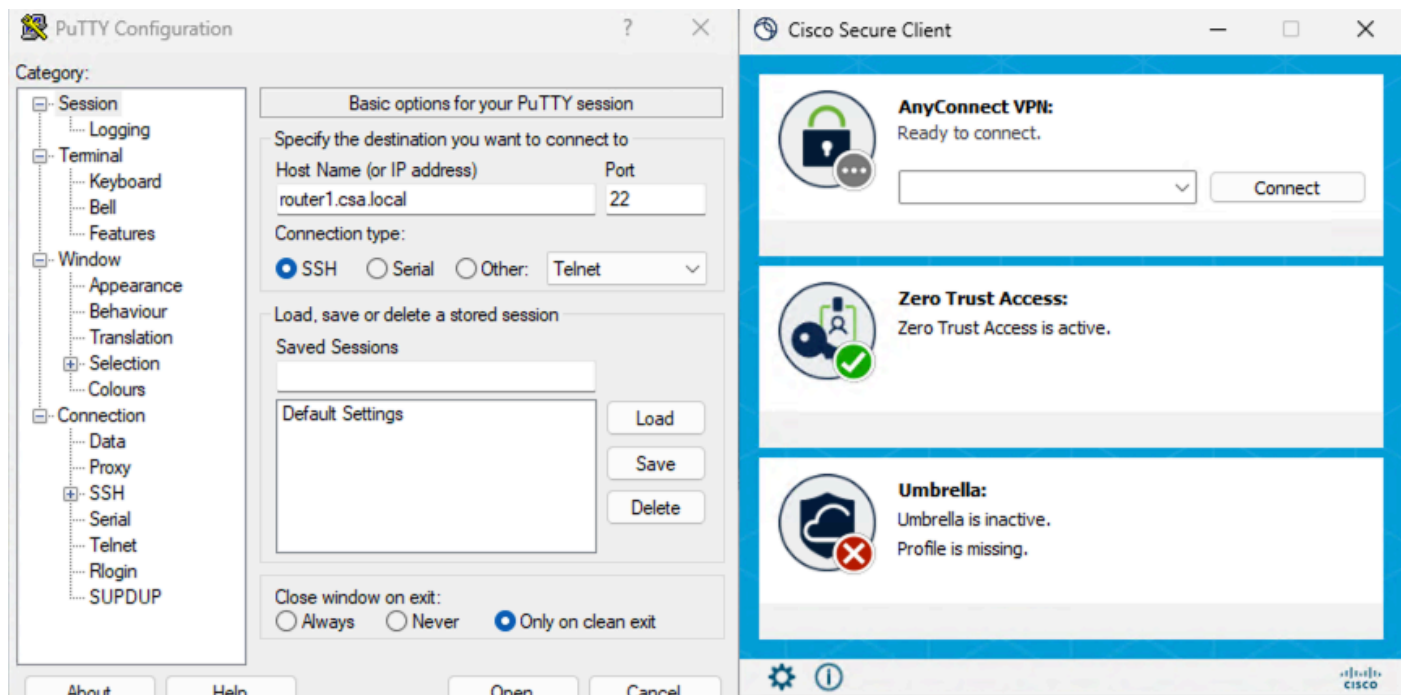
2. Verify FTD can reach to private resource using FQDN

```
ftd> en
Password:
ftd# ping router1.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.101, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ftd# █
```

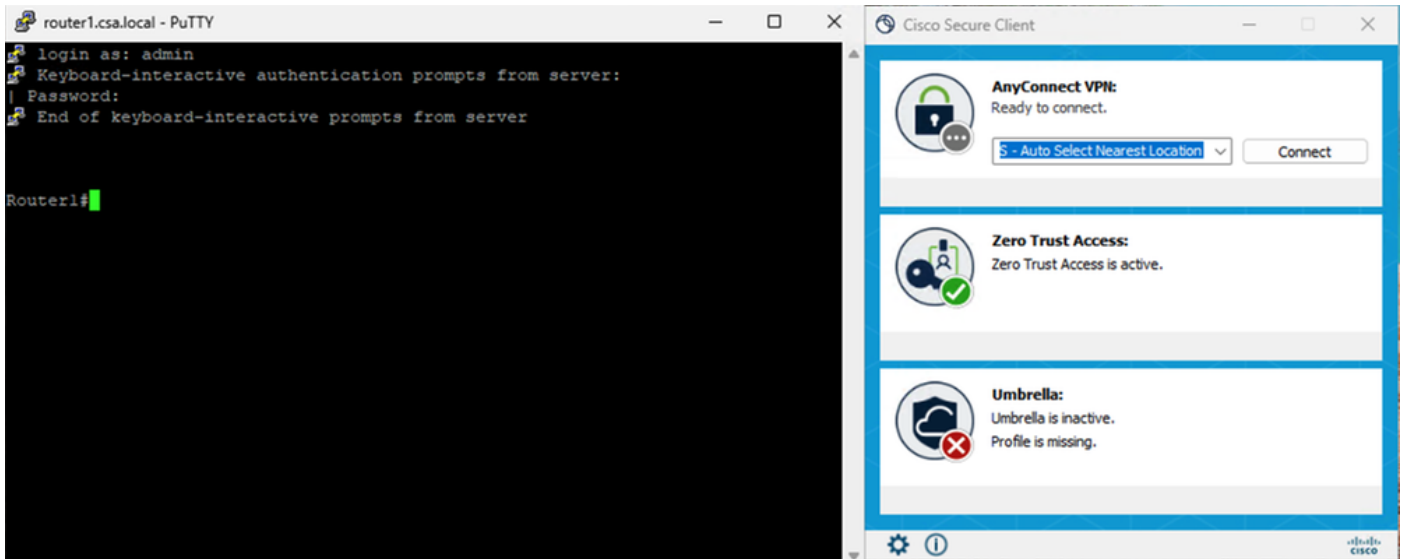
Secure Access - PR Testing

3. Test the SSH connection to the Private Resource

Access the PR using FQDN

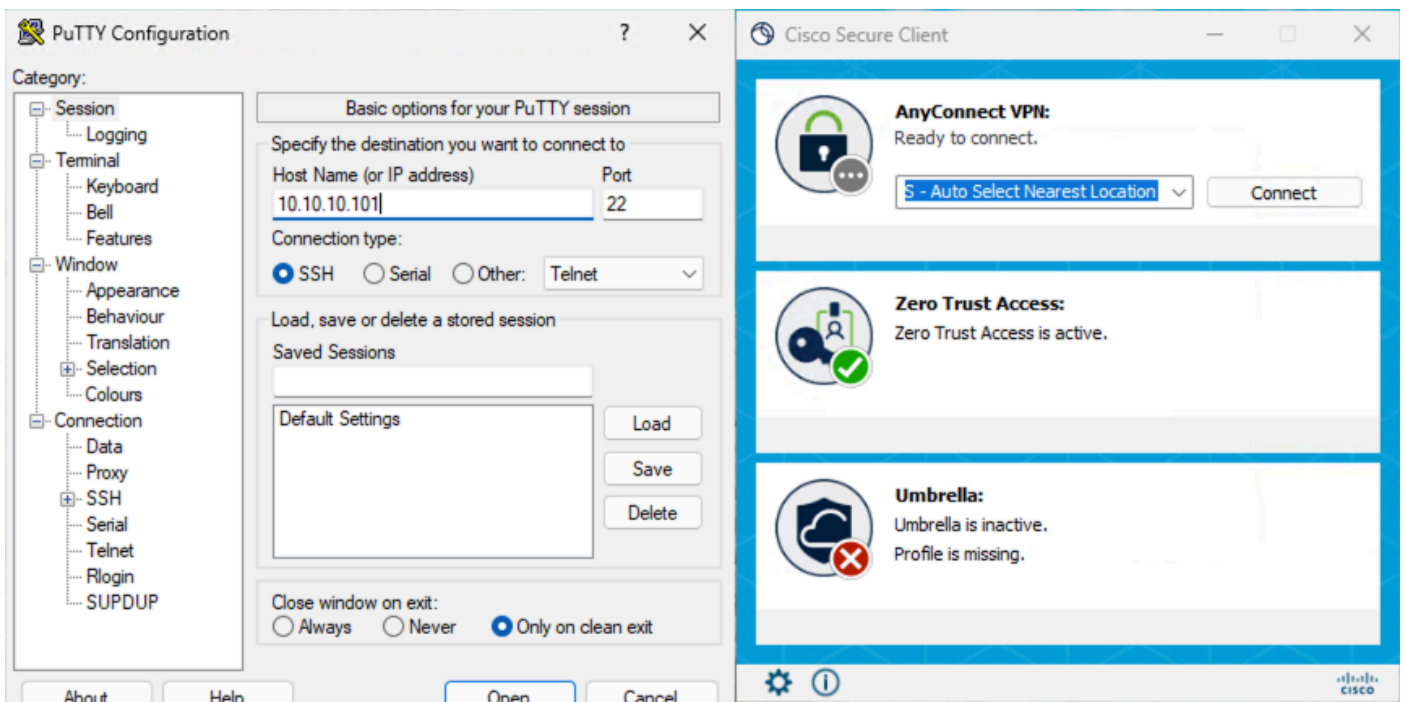


Secure Access - PR Testing

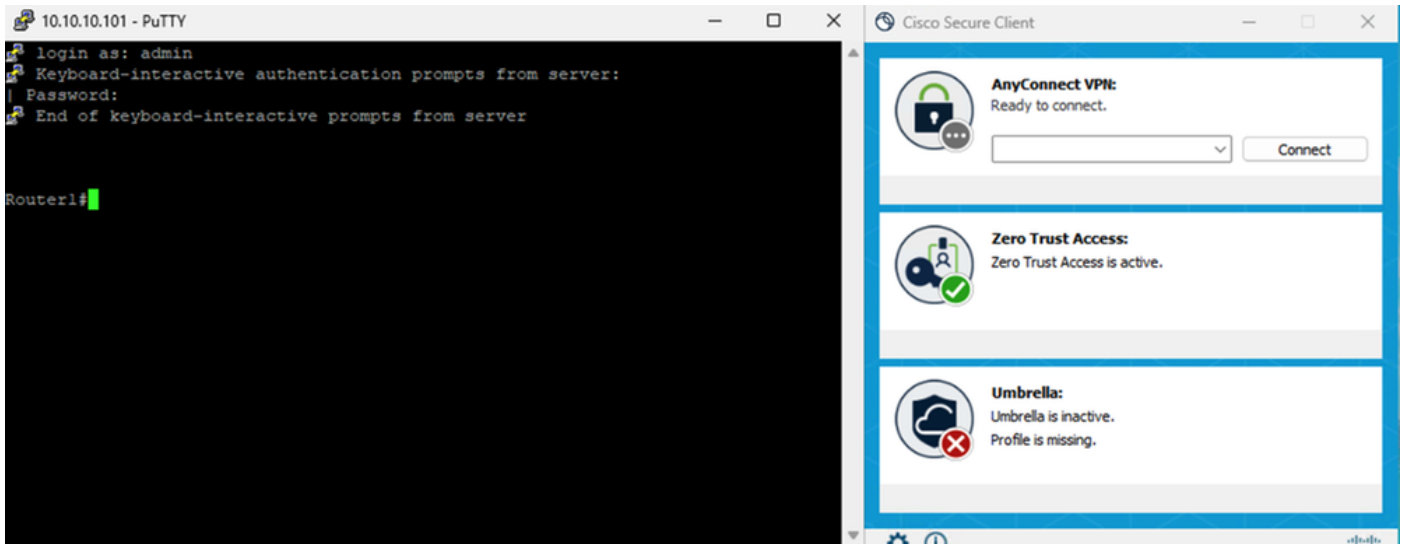


Secure Access - PR Testing

Access the PR using IP address



Secure Access - PR Testing



Secure Access - PR Testing

4. Verify Secure Access Activity Search logs

Activity Search

4 Total Viewing activity from Jan 9, 2026 5:57 PM to Jan 10, 2026 5:57 PM

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Browser	Location
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76

Secure Access - Activity Search

4 Total Viewing activity from Jan 9, 2026 6:01 PM to Jan 10, 2026 6:01 PM

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	:22	22	Allowed	Router1	Default ZTA Profile	Router1-SSH

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 10, 2026 5:55 PM

Access details

Identity: jay (jay@csa.local)

Win1

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: FTD> FMC_FTD

Destination: router1.csa.local

Destination IP:

Secure Access - Activity Search

Activity Search

Filters: Search by domain, identity, or URL. IP ADDRESS: 10.10.10.101. RESPONSE: Allowed.

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Browser	Location	Location IP
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22	Allowed	Router1	Default ZTA Profile	Router1-SSH	win 10.0.26200.7462	US	76.38.159.129	...

Secure Access - Activity Search

7 Total. Viewing activity from Jan 9, 2026 6:09 PM to Jan 10, 2026 6:09 PM.

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Destination Country	Internal IP	External IP	Action	Categories
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22				Allowed	
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22				Allowed	
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101	22				Allowed	
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22				Allowed	
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22				Allowed	
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router1.csa.local	10.10.10.101	22				Allowed	
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.101	10.10.10.101	22				Allowed	

Event Details

Action: Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Jan 10, 2026 5:56 PM

Access details

Identity: jay (jay@csa.local)

Win1

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: FTD> FMC_FTD

Destination: 10.10.10.101

Destination IP: 10.10.10.101

Secure Access - Activity Search

5. Verify FMC connection events

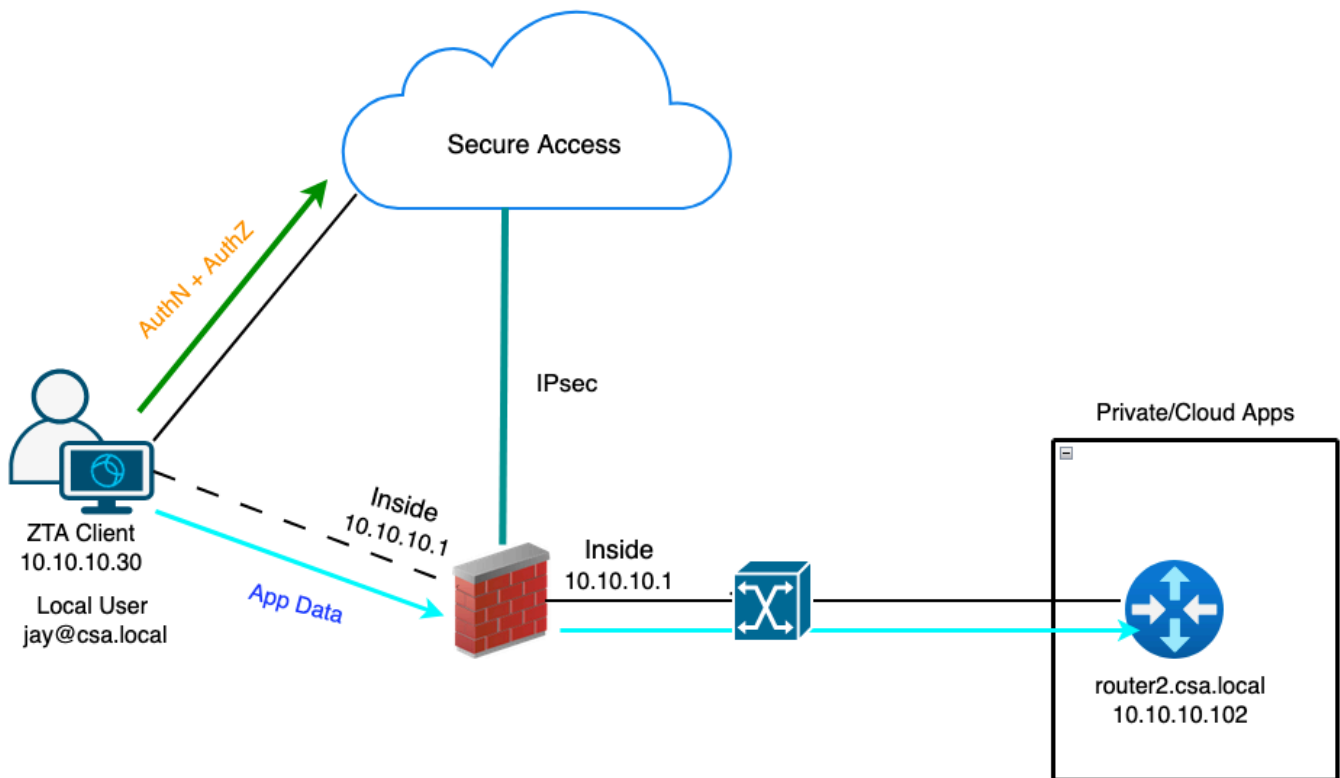
Firewall Management Center - Events & Logs / Analysis / Unified Events

Monitor: Destination IP: 10.10.10.101. 6 events.

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP...	Web Application	Access Control Rule	Access Control Policy
2026-01-10 12:56:23	Connection	Allow	Zero Trust Flow	169.254.1194	10.10.10.101	42217 / tcp	22 (ssh) / tcp			
2026-01-10 12:56:16	Connection	Allow	Zero Trust Flow	169.254.1190	10.10.10.101	27221 / tcp	22 (ssh) / tcp			
2026-01-10 12:55:28	Connection	Allow	Zero Trust Flow	169.254.1196	10.10.10.101	50425 / tcp	22 (ssh) / tcp			
2026-01-10 12:54:46	Connection	Allow	Zero Trust Flow	169.254.1198	10.10.10.101	38499 / tcp	22 (ssh) / tcp			
2026-01-10 12:50:25	Connection	Allow	Zero Trust Flow	169.254.1194	10.10.10.101	22631 / tcp	22 (ssh) / tcp			
2026-01-10 12:47:08	Connection	Allow	Zero Trust Flow	169.254.1190	10.10.10.101	24739 / tcp	22 (ssh) / tcp			

Test Case 3 - Local User - Local Enforcement

Accessing a Private Resource via Local enforcement as a local user, in this type of enforcement policy evaluation happens on Secure Access but the application data stays local to FTD. For example , a ZTA enrolled client or user connected to home network and trying to access a private resource which is behind FTD inside interface . If the private resource is behind DMZ or any other interface of the FTD then we would have to create a access rule on the FTD to permit the traffic between Client IP or network and Private Resource.

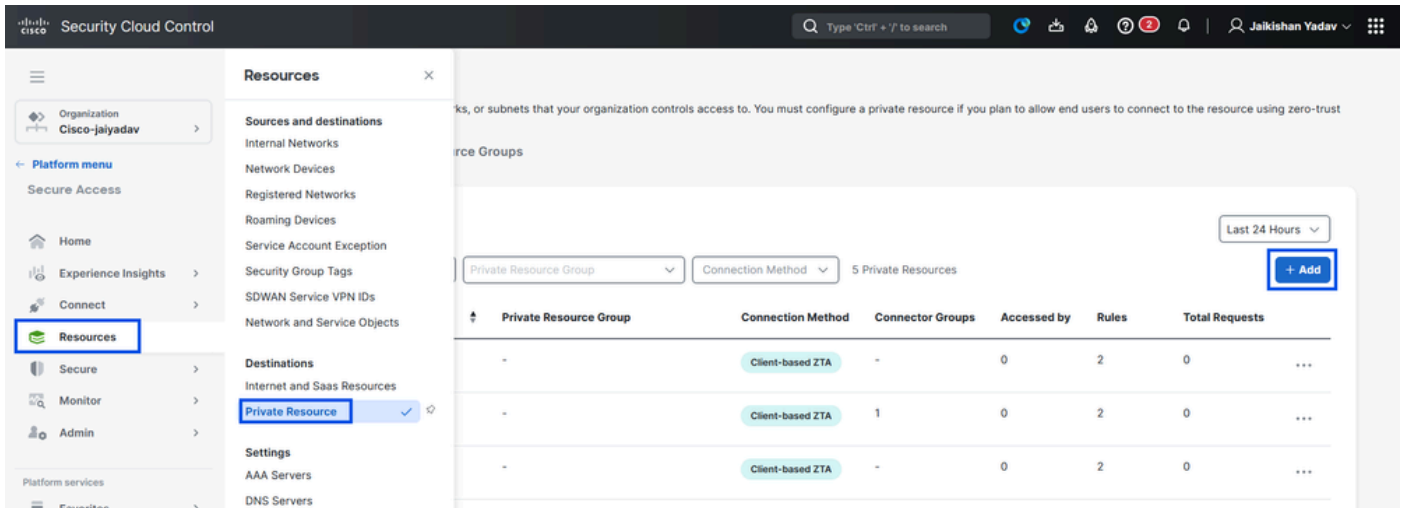


Universal ZTA - Test Case Topology

Step 1 - Define a Private Resource on Secure Access

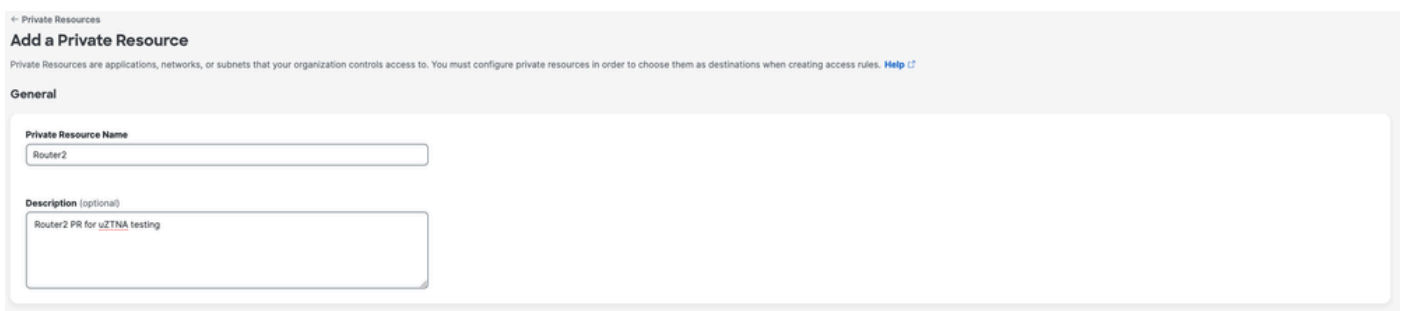
Configure a private resource to be accessible via Zero Trust Access (ZTA) enrolled device with cloud enforcement

1. Navigate to **Resources > Destinations > Private Resources > Click on +Add**



Secure Access - Private Resource Configuration

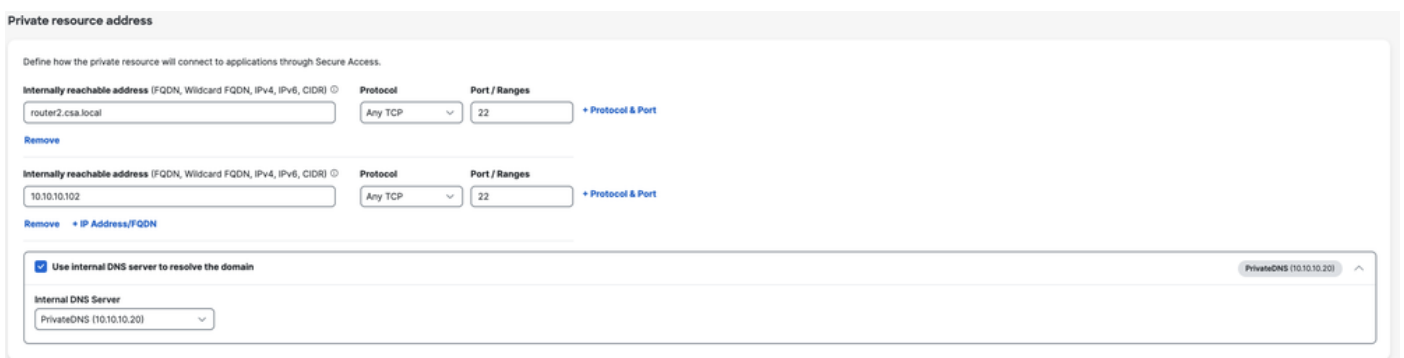
2. For **Private Resource Name**, enter a meaningful name for the resource. For **Description**, we recommend that you provide information such as the purpose of the resource or the name of the resource owner.



Secure Access - Private Resource Configuration

3. Enter the FQDN of the private resource you want to access . We can also define the IP address of the private resource . For more information see [Add a Private Resource](#)

4. Select the internal DNS server to resolve the domain



5. Select Endpoint Connection Methods

6. Select FTD as Local enforcement points

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).

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local-only

Local enforcement points

FMC_F... X Search by FTD na... v

Traffic from users within a trusted network will get enforced at the selected Firewalls.

Enforcement point for Remote User

Remote user Local Firewall Private Resource

via internet

Enforcement point for Local user

User in a trusted network Local Firewall Private Resource

via local network

Internal remote addresses are visible on end-user devices. If you want an address to be hidden, use an external address.

Change the remotely reachable addresses

Cancel Save and Test Save



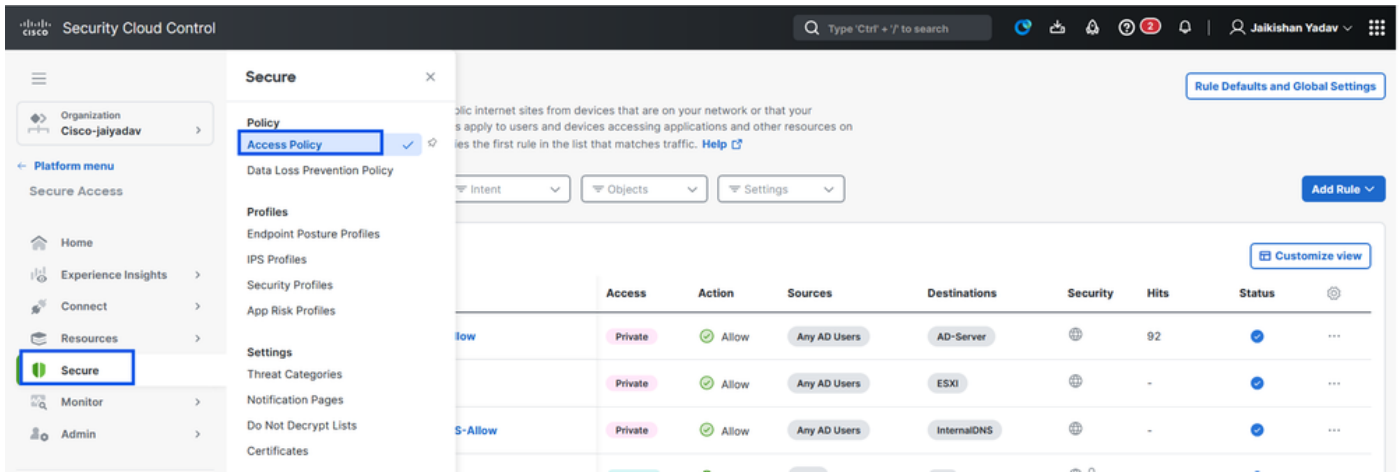
Note: Depending on the type of enrollment you select , this change will automatically associate the PR to the FTD and will trigger a policy deployment

7. Click **Save**

Step 2 - Create Private Access Rule

Configure a private access on Secure Access to be access by Universal ZTA enrolled users . For more information see [Private Access Rule](#)

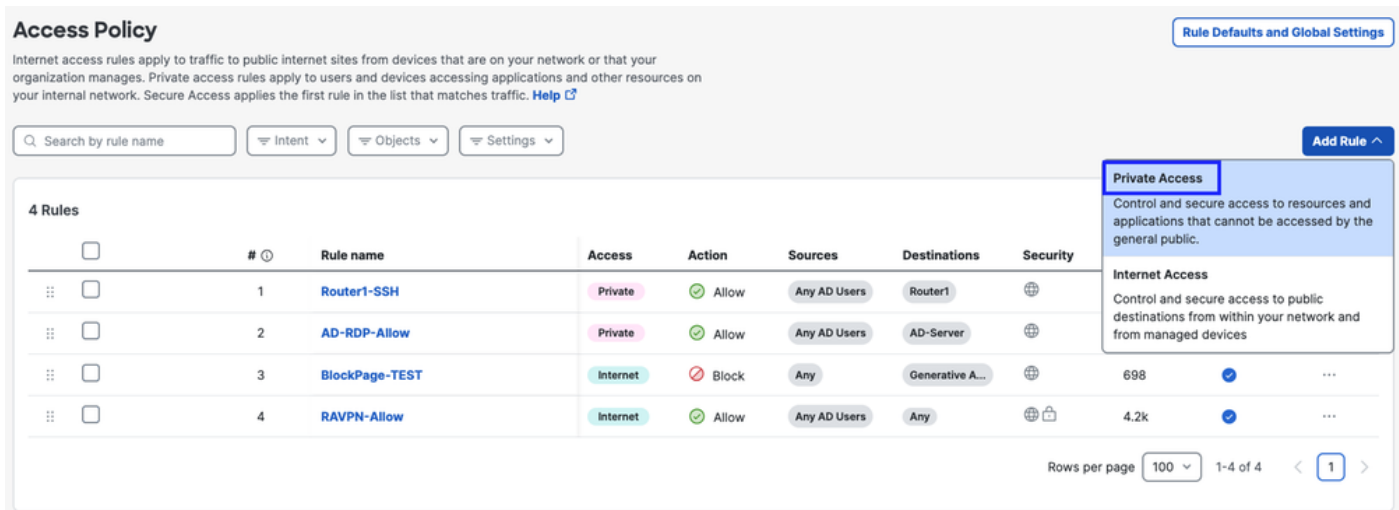
1. Navigate to **Secure > Access Policy**



Secure Access - Access Policy Configuration

2. Click **Add Rule**, and then choose **Private Access**.

At the top of the rule is a summary that describes the configured components of your rule.



Secure Access - Access Policy Configuration

3. Add a Rule Name

Add Router2-SSH-Allow

Create a rule to control and secure access to specified private applications and other destinations on your network. For an end-to-end guide to completing prerequisites and configuring a rule, see [Help](#)

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

Router2-SSH-Allow

Rule order

1

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.

Secure Access - Access Policy Configuration

4. Select the rule action and select source and destination

Rule name

Router2-SSH-Allow

Rule order

1

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

AD Users - Any AD Users

To

Specify one or more destinations

Private Resources - Router2

+ AND

Secure Access - Access Policy Configuration

5. Configure Endpoint Requirements

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: **Router2**

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 Rule Defaults

Disabled

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](#)

2 Configure Security

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

Cancel

Back Next

Secure Access - Access Policy Configuration

6. Configure Security

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](#)

Security Profile Rule Defaults

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

Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**



Cancel

Back Save

Secure Access - Access Policy Configuration

7. Click on Save

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](#)

Search by rule name Intent Objects Settings

Add Rule

5 Rules

Customize view

	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	
<input type="checkbox"/>	1	Router2-SSH-Allow	Private	Allow	Any AD Users	Router2		-		
<input type="checkbox"/>	2	Router1-SSH	Private	Allow	Any AD Users	Router1		-		
<input type="checkbox"/>	3	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server		40		
<input type="checkbox"/>	4	BlockPage-TEST	Internet	Block	Any	Generative A...		698		
<input type="checkbox"/>	5	RAVPN-Allow	Internet	Allow	Any AD Users	Any		4.2k		

Rows per page 100 1-5 of 5 1

Secure Access - Access Policy Configuration

Step 3 - Verify the association of PR on the FTD

1. Navigate to connect > Network Connections > FTDs

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar contains a 'Platform menu' with 'Connect' highlighted. A 'Connect' dialog box is open, showing 'Essentials' with 'Network Connections' selected. The main content area displays 'FTDs' with a status indicator showing '1 Connected' and '0 Warning'. The interface includes a search bar, user profile 'Jalkishan Yadav', and various navigation icons.

Secure Access - PR Verification

2. Click on the FTD > View resources associated to this FTD

Network Connections

Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see [Help](#)

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access

An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal to improve end-user experience and ensure consistent security controls for users independent of where they are connecting from [Help](#)

Q Search by FTD name FMC Name Configuration status 1 FTDs

FTD Name	Version	FMC	UZTA Configuration status
FMC_FTD Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	Synced

FMC_FTD

Firewall Details

Device FQDN: ftd.csa.local

Auto deployment: Yes

UZTA Configuration status

Synced Last synced at 12 Jan 2026, at 6:29 AM UTC

Assigned Trusted Network

Trusted network	Networks
LAN <small>(Default trusted network)</small>	1 DNS Servers

[Edit assignment](#) [+ Trusted network](#)

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status	Count
Synced	2

[View resources associated to this FTD](#)

[Associate Resources](#)

Secure Access - PR Verification

Resources associated with FMC_FTD

The following resources will get enforced on FMC_FTD when users connect to it from the trusted network LAN

Q Search by resource name Configuration status 2 Resources [Associate Resources](#)

Resource name	Status
Router1	Synced
Router2	Synced

[Close](#)

Secure Access - PR Verification

3. Click **close**

4. Verify the status , Associated Resource and Configuration should be in Synced state

The screenshot displays the 'Network Connections' page in the Palo Alto Networks management console. The 'FTDs' tab is active, showing a summary of '1 Synced' FTDs. Below this, a table lists FTDs configured for Universal Zero Trust Access. The table has columns for 'FTD Name', 'Version', 'FMC', and 'UZTA Configuration status'. One entry is shown: 'FMC_FTD' with version 'v10.0.0', FMC 'FMC', and a 'Synced' status. A blue box highlights the 'Synced' status in the table. To the right, a detailed view for 'FMC_FTD' is shown, including 'Firewall Details' (Device FQDN: ftd.csa.local, Auto deployment: Yes), 'UZTA Configuration status' (Synced, last synced at 12 Jan 2026, 6:29 AM UTC), 'Assigned Trusted Network' (LAN, 1 DNS Servers), and 'Associated Resources' (2 resources associated by status). A blue box highlights the 'Synced' status in the 'Associated Resources' section.

FTD Name	Version	FMC	UZTA Configuration status
FMC_FTD Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	Synced

Secure Access - PR Verification

5. Verify the configuration has been pushed to FTD

Login to FTD cli and navigate to LINA mode

show running-config object application

```

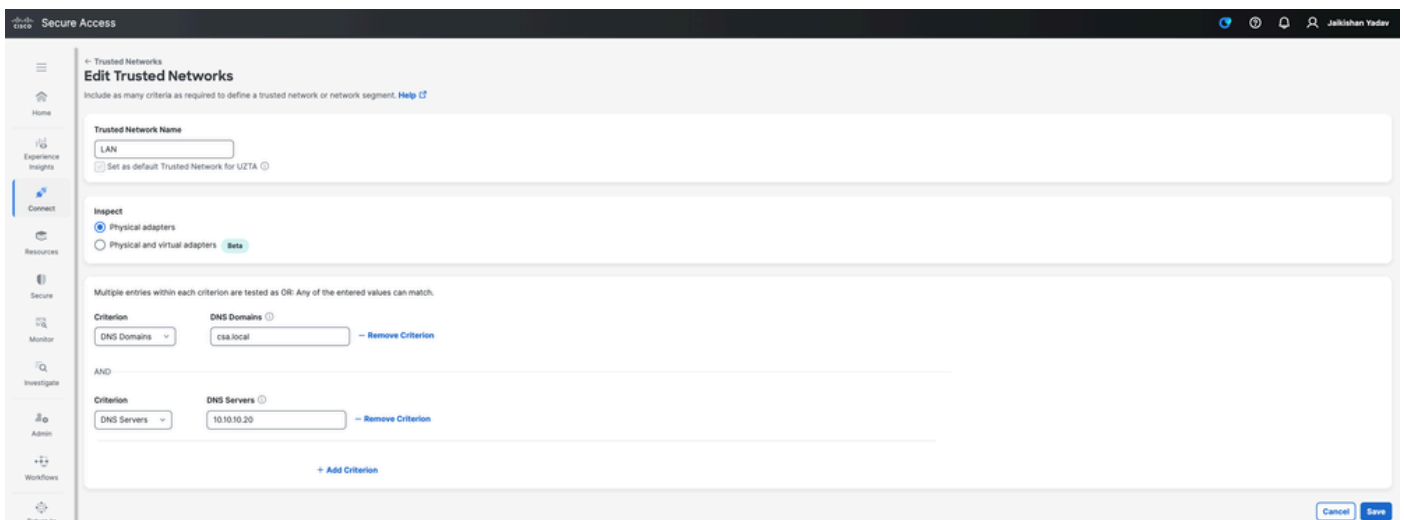
ftd# sh run ob application
object application PR_Router1
  id 427221
  internal domain router1.csa.local tcp eq 22
  internal subnet 10.10.10.101 255.255.255.255 tcp eq 22
  external domain router1.csa.local
  external subnet 10.10.10.101 255.255.255.255
object application PR_Router2
  id 434482
  internal domain router2.csa.local tcp eq 22
  internal subnet 10.10.10.102 255.255.255.255 tcp eq 22
  external domain router2.csa.local
  external subnet 10.10.10.102 255.255.255.255

```

Secure Access - PR Verification

Step - 4 Configure " Manage Trusted Networks or ZTA Settings"

Navigate to **Connect > End User Connectivity > Zero Trust Access > ZTA Settings** and configure **Trusted Networks**



Secure Access - TND Configuration

Step -5 Add Private Resource to the ZTA Profile

1. Navigate to **Connect > End User Connectivity > Zero Trust Access** and click 3 dots to edit ZTA profile

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](#)

Enrollment methods

Before users can access resources using client-based Zero Trust Access, their endpoint devices must be enrolled. Manage enrollment methods for your organization here. [Help](#)

Windows and macOS devices enroll using: **SSO Authentication** **Certificates**

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles

Manage Zero Trust Access (ZTA) profiles, which allow you to add users and groups to unique traffic steering configurations for client-based ZTA connections. [Help](#)

#	Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
1	ZTAProfile	2 Destinations Trusted Networks Disabled	Use ZTA for all destinations 0 Exceptions Trusted Networks Disabled	1 Users 0 Groups	Jan 25, 2026

Secure Access - ZTA Profile

2. Add the Private Resource

Create profile

For client-based Zero Trust Access connections, add the destinations to which a set of users and groups can be steered. [Help](#)

ZTA profile name: Priority:

Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

Secure Private Access

Add the private destinations and private resources to which a set of users and groups can be steered. [Help](#)

Destinations & Private Resources

Destinations & Private Resources	Destinations	Modified
<input checked="" type="checkbox"/> *zpc.sse.cisco.test	1	Feb 22, 2023

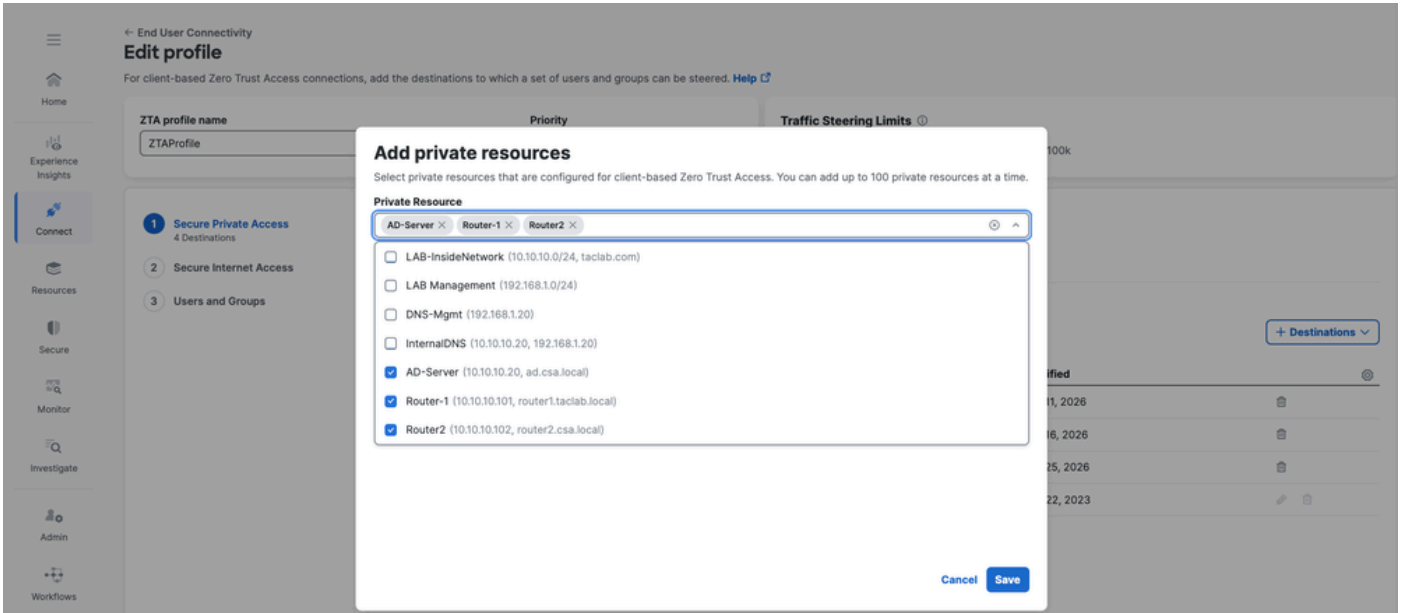
Private Resource

Add private resources that are configured for client-based Zero Trust Access.

Add Destination

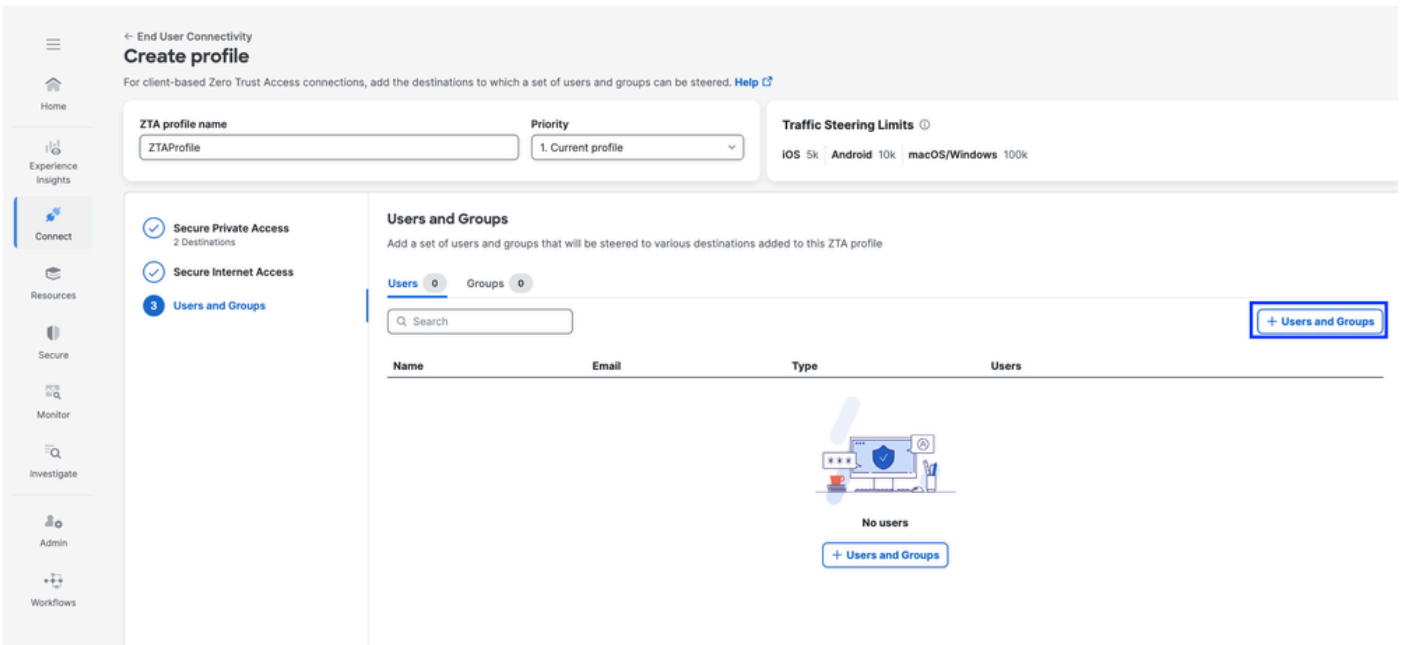
Add destinations that are not configured as private resources that user traffic can access during Zero Trust Access.

Secure Access - ZTA Profile



Secure Access - ZTA Profile

3 . Add Users and Groups



ZTA profile name: ZTAProfile | Priority: 1. Current profile | Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

Secure Private Access (2 Destinations)
Secure Internet Access
Users and Groups

Users and Groups

Add a set of users and groups that will be steered to various destinations added to this ZTA profile

Users 1 | Groups 0

Q Search + Users and Groups

Name	Email	Type	Users
jay (jay@csa.local)	jay@gmail.com	User	-

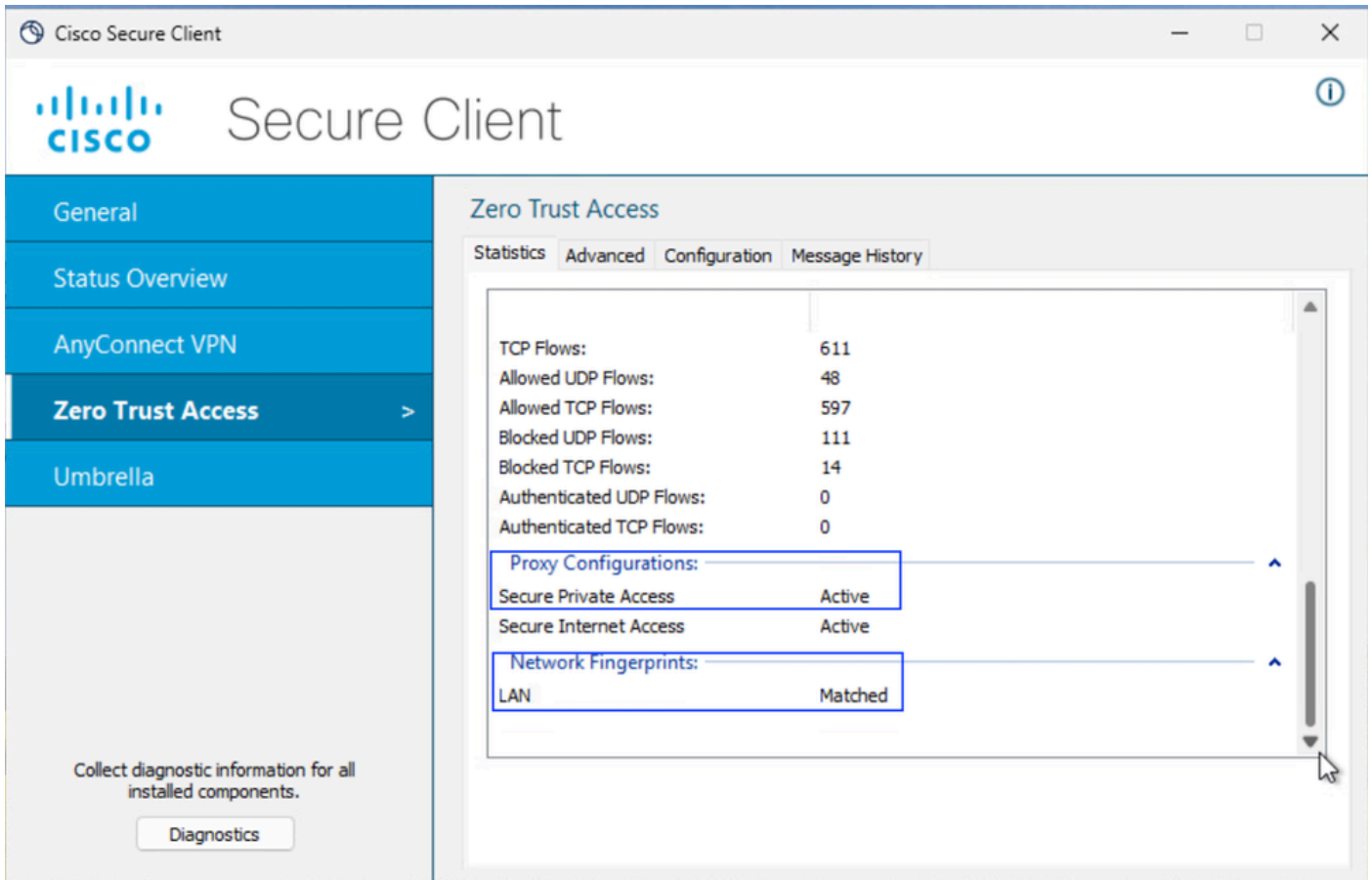
Rows per page: 10

Back Close

Secure Access - ZTA Profile

Step - 6 Verify access to the Private Resource

1. Verify the Network Fingerprint for ZTA TND



Secure Access - PR Testing

2. Verify the remote user can resolve FTD FQDN

```
C:\Users\jay>ping ftd.csa.local

Pinging ftd.csa.local [10.10.10.1] with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\jay>nslookup ftd.csa.local
Server: AD.csa.local
Address: 10.10.10.20

Name: ftd.csa.local
Addresses: 10.10.10.1
```

Secure Access - PR Testing

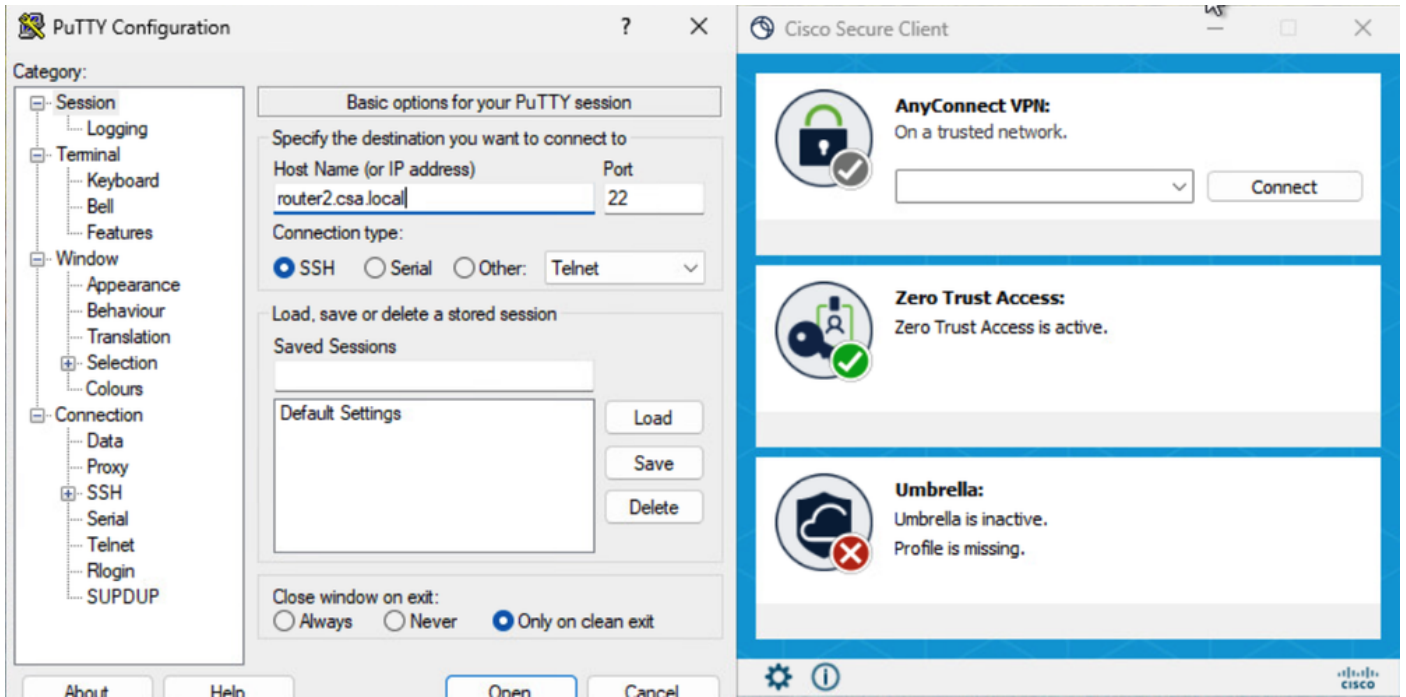
3. Verify FTD can reach to private resource using FQDN

```
ftd# ping router2.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.102, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/12/60 ms
ftd# █
```

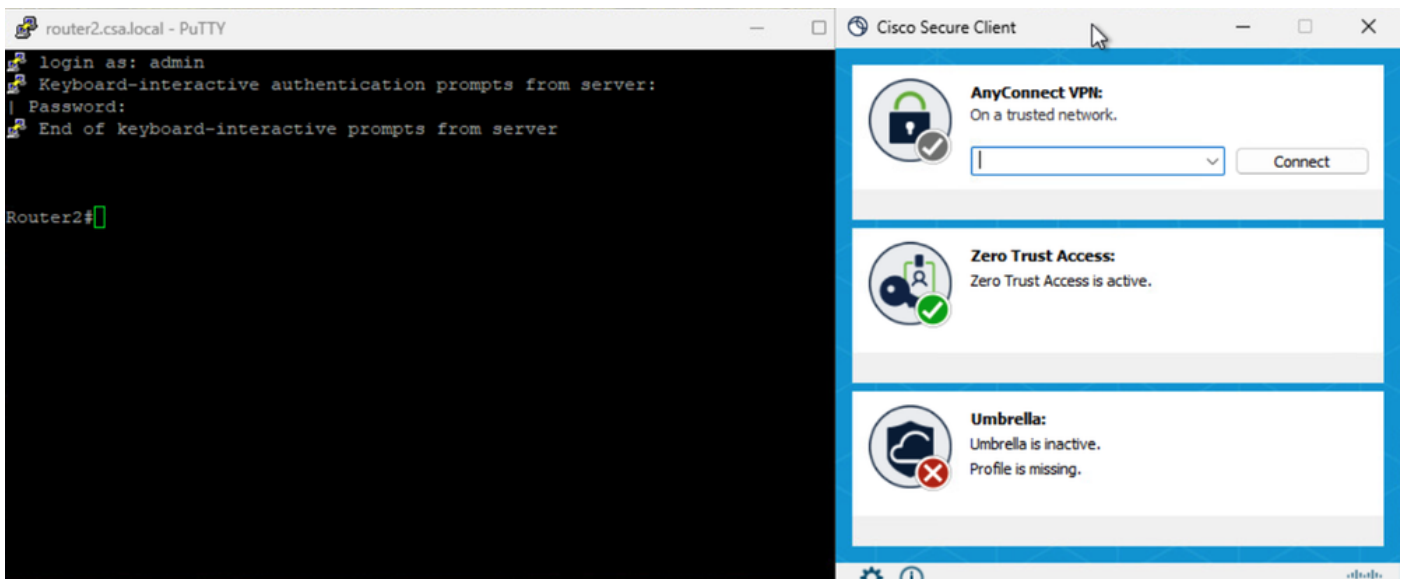
Secure Access - PR Testing

4. Test the SSH connection to the Private Resource

Access the PR using FQDN

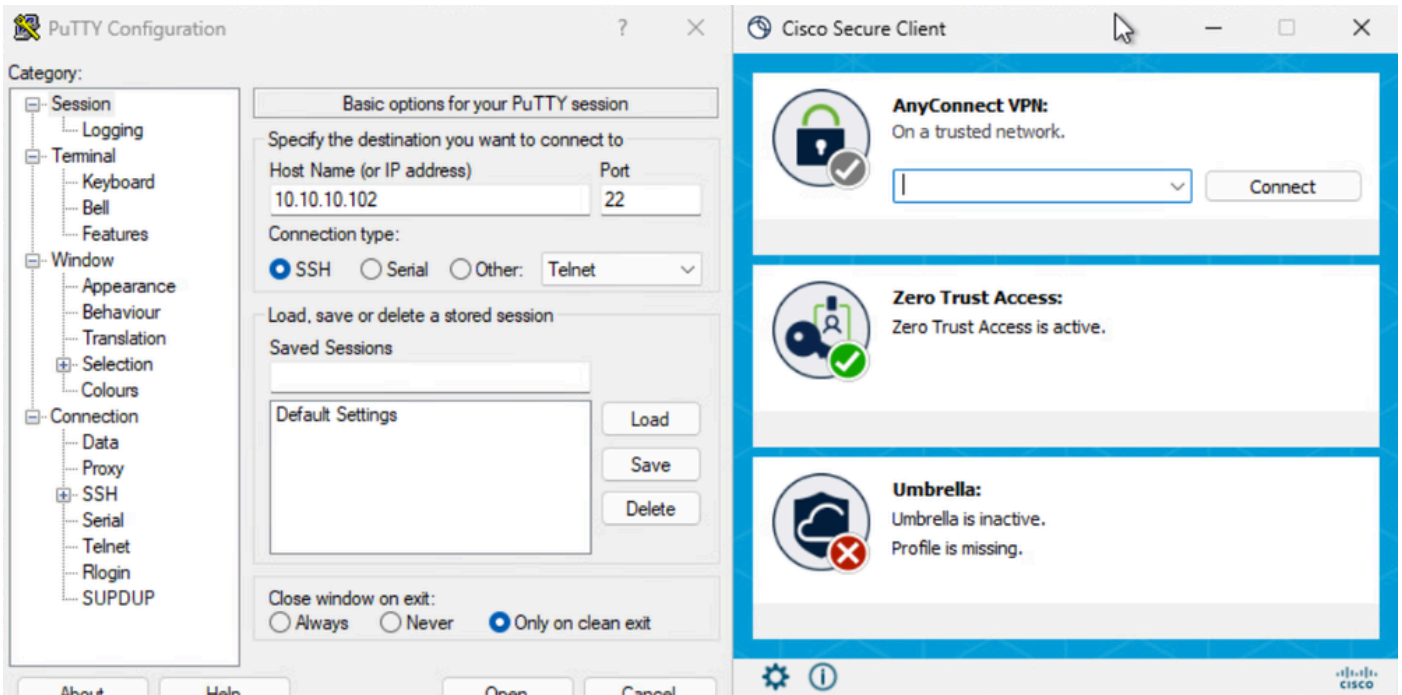


Secure Access - PR Testing

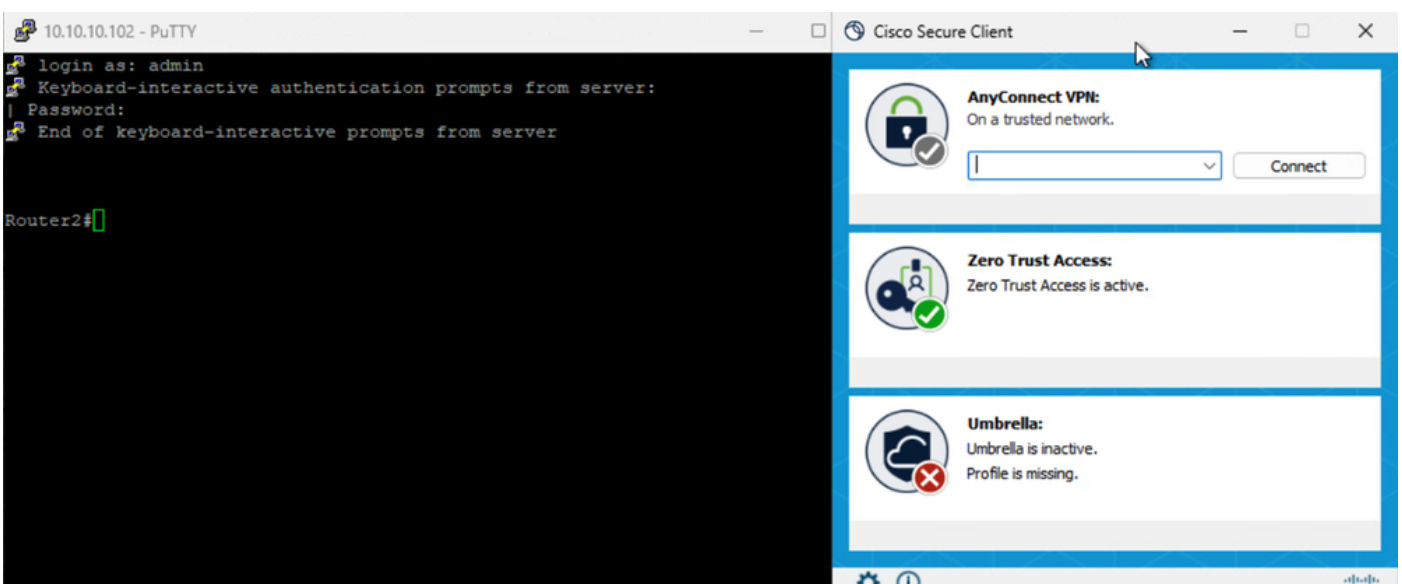


Secure Access - PR Testing

Access the PR using IP address

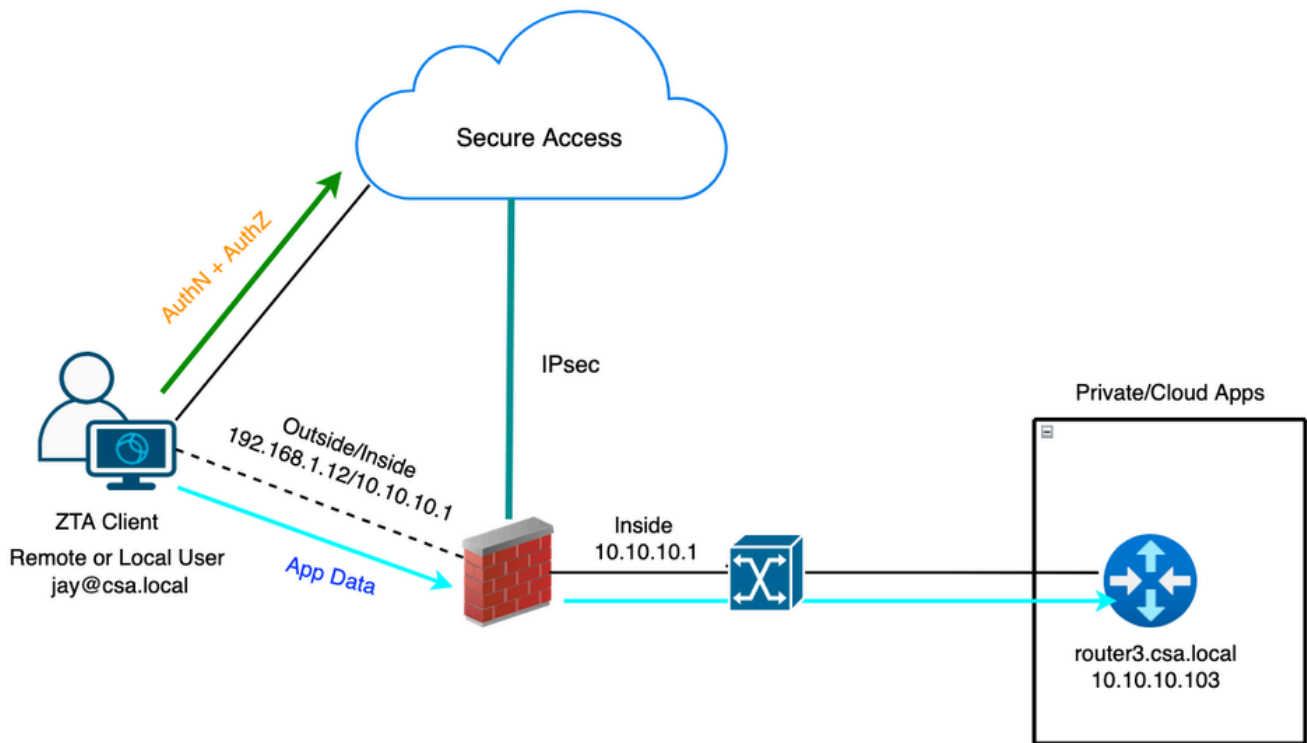


Secure Access - PR Testing



Secure Access - PR Testing

5. Verify Secure Access Activity Serach logs



Universal ZTA - Test Case Topology

Step 1 - Define a Private Resource on Secure Access

Configure a private resource to be accessible via Zero Trust Access (ZTA) enrolled device with cloud enforcement

1. Navigate to **Resources > Destinations > Private Resources > Click on +Add**

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has 'Resources' highlighted. The main content area shows the 'Resources' configuration page. Under 'Destinations', 'Private Resource' is selected. The main area displays a table of Private Resource Groups. The table has the following columns: Private Resource Group, Connection Method, Connector Groups, Accessed by, Rules, and Total Requests. There are three rows of data, all with 'Client-based ZTA' as the Connection Method. A '+ Add' button is visible in the top right corner of the table area.

Private Resource Group	Connection Method	Connector Groups	Accessed by	Rules	Total Requests
-	Client-based ZTA	-	0	2	0
-	Client-based ZTA	1	0	2	0
-	Client-based ZTA	-	0	2	0

Secure Access - Private Resource Configuration

2. For **Private Resource Name**, enter a meaningful name for the resource. For **Description**, we recommend that you provide information such as the purpose of the resource or the name of the resource owner.

← 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

Router3

Description (optional)

Router 3 for uZTNA Testing

Secure Access - Private Resource Configuration

3. Enter the FQDN of the private resource you want to access . We can also define the IP address of the private resource . For more information see [Add a Private Resource](#)

4. Select the DNS server to resolve the domain

Private resource address

Define how the private resource will connect to applications through Secure Access.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR)	Protocol	Port / Ranges	
router3.csa.local	Any TCP	22	+ Protocol & Port
Remove			
192.168.1.103	Any TCP	22	+ Protocol & Port
Remove			
10.10.10.103	Any TCP	22	+ Protocol & Port
Remove + IP Address/FQDN			

Use internal DNS server to resolve the domain LabDNS (192.168.1.20, 10.10.10.20)

Secure Access - Private Resource Configuration

5. Select Endpoint Connection Methods

6. Select FTD as Local enforcement points

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).

Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

Local enforcement points

FMC_F... x Search by FTD na... ^

FMC_FTD (ftd.csa.local) ✓
Will get enforced at the selected firewalls.

Local-only

Enforcement point for Remote User

Remote user Secure Access Cloud Private Resource

via Internet

Enforcement point for Local user

User in a trusted network Local Firewall Private Resource

via local network

Cancel Save and Test Save

Secure Access - Private Resource Configuration

Select RC if the Private Resource is accessible over RC , otherwise leave it blank if the Private Resource is accessible over Network Tunnel Group (IPsec Tunnel).

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) [?](#)

RC-ESXI x e.g. My Server Group v

Choose a connector group in the same data center, branch office, or security zone as the resource. [?](#)

Secure Access - Private Resource Configuration



Note: Depending on the type of enrollment you select , this change will automatically associate the PR to the FTD and will trigger a policy deployment

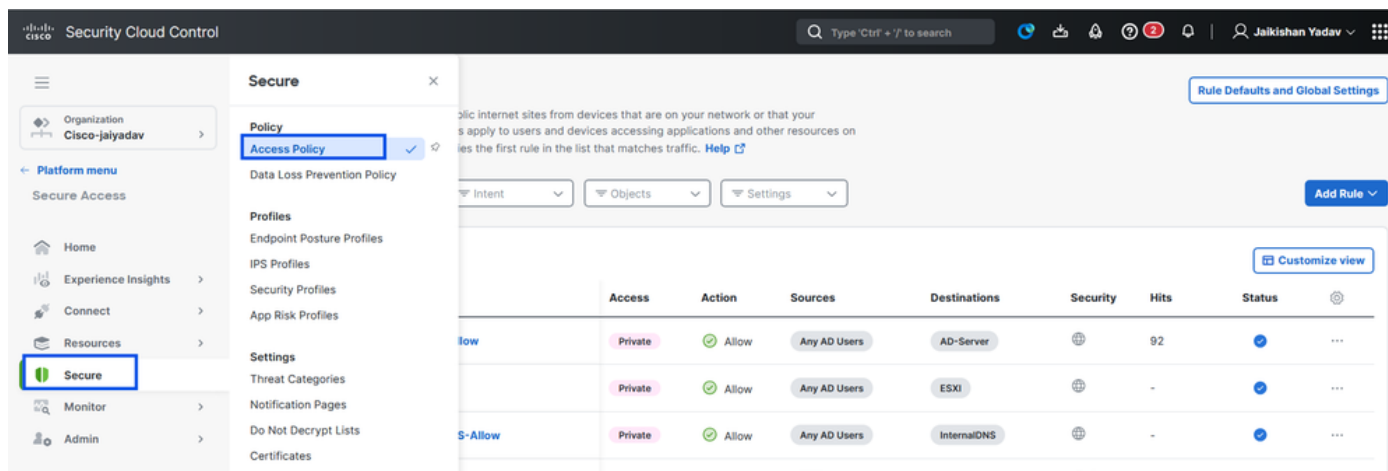
7. Click **Save**

Step 2 - Create Private Access Rule

Configure a private access on Secure Access to be access by Universal ZTA enrolled users . For more

information see [Private Access Rule](#)

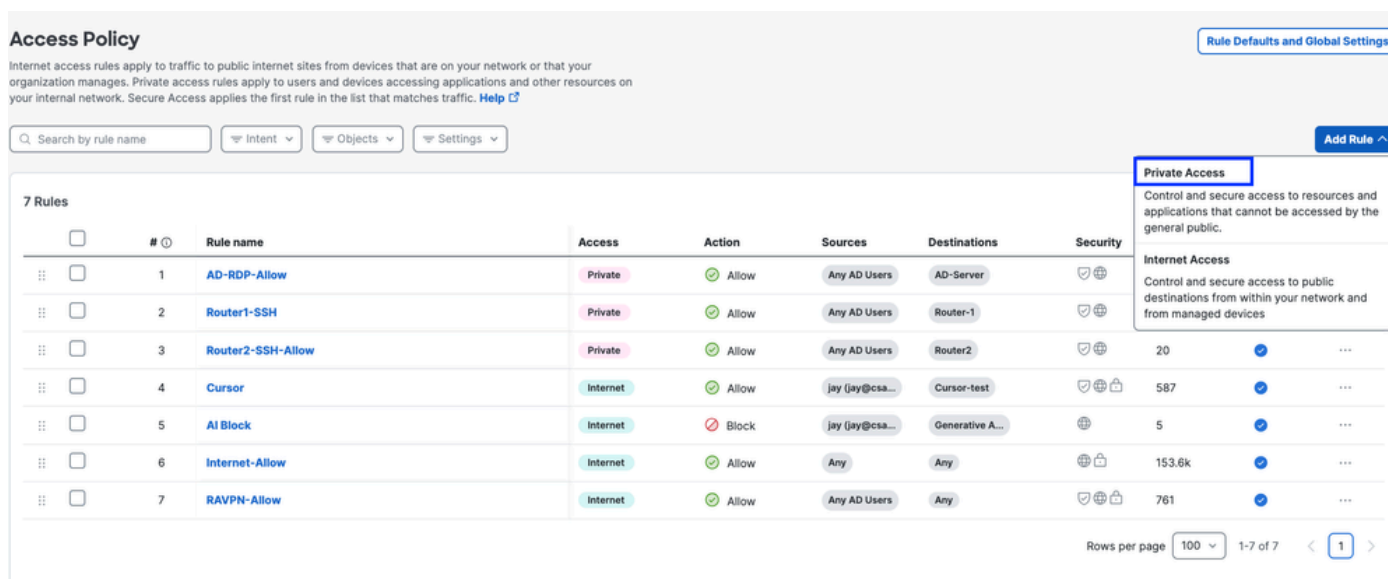
1. Navigate to **Secure > Access Policy**



Secure Access - Access Policy Configuration

2. Click **Add Rule**, and then choose **Private Access**.

At the top of the rule is a summary that describes the configured components of your rule.



Secure Access - Access Policy Configuration

3. Add a Rule Name

Add Router3-SSH-Allow

Create a rule to control and secure access to specified private applications and other destinations on your network. For an end-to-end guide to completing prerequisites and configuring a rule, see [Help](#)

Rule is enabled

Logging is enabled [Edit](#)

Summary



Rule name

Router3-SSH-Allow

Rule order

8

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

Action

Two action options are shown:

- Allow** (selected): Allow specified traffic if security requirements are met.
- Block**: Block specified traffic.

Secure Access - Access Policy Configuration

4. Select the rule action and select source and destination

The configuration page shows the following details:

- Rule name:** Router3-SSH-Allow
- Rule order:** 8
- Action:** 'Allow' is selected.
- From:** AD Users • Any AD Users
- To:** Private Resources • Router3

Secure Access - Access Policy Configuration

5. Configure Endpoint Requirements

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: **Router3**

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 [Rule Defaults](#) Disabled
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](#)

2 Configure Security

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

Cancel

[Back](#) [Next](#)

Secure Access - Access Policy Configuration

6. Configure Security

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](#)

Security Profile [Rule Defaults](#)
The following security settings will apply to traffic that matches this rule. [Help](#)
Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**

Cancel

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

Secure Access - Access Policy Configuration

7. Click on **Save**

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](#)

Search by rule name Intent Objects Settings Add Rule

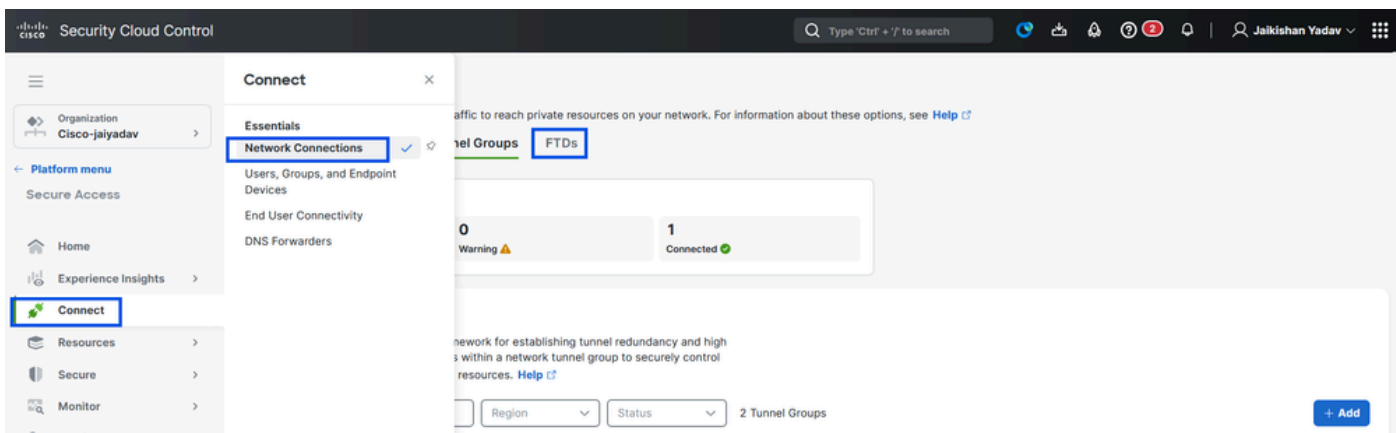
8 Rules Customize view										
	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	
<input type="checkbox"/>	1	Router3-SSH-Allow	Private	Allow	Any AD Users	Router3	Shield	-	On	...
<input type="checkbox"/>	2	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server	Shield	-	On	...
<input type="checkbox"/>	3	Router1-SSH	Private	Allow	Any AD Users	Router-1	Shield	-	On	...
<input type="checkbox"/>	4	Router2-SSH-Allow	Private	Allow	Any AD Users	Router2	Shield	20	On	...
<input type="checkbox"/>	5	Cursor	Internet	Allow	jay (jay@csa...	Cursor-test	Shield	587	On	...
<input type="checkbox"/>	6	AI Block	Internet	Block	jay (jay@csa...	Generative A...	Shield	5	On	...
<input type="checkbox"/>	7	Internet-Allow	Internet	Allow	Any	Any	Shield	154.8k	On	...
<input type="checkbox"/>	8	RAVPN-Allow	Internet	Allow	Any AD Users	Any	Shield	761	On	...

Rows per page: 100 | 1-8 of 8 | Page 1

Secure Access - Access Policy Configuration

Step 3 - Verify the association of PR on the FTD

1. Navigate to connect > Network Connections > FTDs



Secure Access - PR Verification

2. Click on the FTD > View resources associated to this FTD

```

C:\Users\jay>ping ftd.csa.local

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\jay>

C:\Users\jay>nslookup ftd.csa.local
Server: AD.csa.local
Address: 192.168.1.20

Name:     ftd.csa.local
Addresses: 192.168.1.12

```

Secure Access - PR Verification

Network Connections

Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see [Help](#)

Connector Groups Network Tunnel Groups **FTDs**

1 Syncing

0 Synced

FTDs configured for Universal Zero Trust Access

An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal Zero Trust Access to improve user experience and ensure consistent security controls for users independent of where they are connecting from [Help](#)

Configuration changes are being processed
The recent Universal ZTA configuration changes are being processed and will be pushed to FTDs in a few minutes.

1 FTDs

FTD Name	Version	FMC	UZTA Configuration status	Associat
FMC_FTD Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	Syncing	3

FMC_FTD

Firewall Details

Device FQDN: ftd.csa.local
Auto deployment: Yes

UZTA Configuration status

Syncing Last synced at 23 Feb 2026, at 5:02 AM UTC

Assigned Trusted Network

Trusted network	Networks
LAN <small>(Default trusted network)</small>	1 DNS Domains 1 DNS Servers

[Edit assignment](#) [+ Trusted network](#)

Associated Resources

RESOURCES ASSOCIATED BY STATUS

Status

Synced 3

[View resources associated to this FTD](#)

[Associate Resources](#)

Secure Access - PR Verification

```
C:\Users\jay>ping ftd.csa.local

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\jay>

C:\Users\jay>nslookup ftd.csa.local
Server: AD.csa.local
Address: 192.168.1.20

Name: ftd.csa.local
Addresses: 192.168.1.12
```

Secure Access - PR Verification

Resources associated with FMC_FTD

The following resources will get enforced on FMC_FTD when users connect to it from the trusted network LAN

3 Resources [Associate Resources](#)

Resource name	Status
Router-1	<input checked="" type="checkbox"/> Synced
Router2	<input checked="" type="checkbox"/> Synced
Router3	<input checked="" type="checkbox"/> Synced

[Close](#)

Secure Access - PR Verification

3. Click **close**

4. Verify the status , Associated Resource and Configuration should be in Synced state

Network Connections
 Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see [Help](#)

Connector Groups Network Tunnel Groups **FTDs**

1 Synced

FTDs configured for Universal Zero Trust Access
 An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal Zero Trust Access to improve user experience and ensure consistent security controls for users independent of where they are connecting from [Help](#)

Q Search by FTD name FMC Name Configuration status 1 FTDs

FTD Name	Version	FMC	UZTA Configuration status	Associated
FMC_FTD Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	Synced	3

FMC_FTD

Firewall Details

Device FQDN: ftd.csa.local
Auto deployment: Yes

UZTA Configuration status

Synced Last synced at 23 Feb 2026, at 5:08 AM UTC

Assigned Trusted Network

Trusted network: **LAN** (Default trusted network)
 Networks: 1 DNS Domains, 1 DNS Servers

Edit assignment + Trusted network

Associated Resources (3)

RESOURCES ASSOCIATED BY STATUS

Status: **Synced** (3)

View resources associated to this FTD

Associate Resources

Secure Access - PR Verification

5. Verify the configuration has been pushed to FTD

Login to FTD cli and navigate to LINA mode

show running-config object application

```

ftd# sh run object application
object application PR_Router2
  id 443200
  internal domain router2.csa.local tcp eq 22
  internal subnet 10.10.10.102 255.255.255.255 tcp eq 22
  external domain router2.csa.local
  external subnet 10.10.10.102 255.255.255.255
object application PR_Router-1
  id 438025
  internal domain router1.csa.local tcp range 1 65535
  internal subnet 10.10.10.101 255.255.255.255 tcp range 1 65535
  external domain router1.csa.local
  external subnet 10.10.10.101 255.255.255.255
object application PR_Router3
  id 468677
  internal domain router3.csa.local tcp eq 22
  internal subnet 192.168.1.103 255.255.255.255 tcp eq 22
  internal subnet 10.10.10.103 255.255.255.255 tcp eq 22
  external domain router3.csa.local
  external subnet 10.10.10.103 255.255.255.255
  external subnet 192.168.1.103 255.255.255.255
  
```

Secure Access - PR Verification

Step - 4 Configure or verify " Manage Trusted Networks or ZTA Settings"

Navigate to **Connect > End User Connectivity > Zero Trust Access > ZTA Settings** and configure **Trusted Networks**

The screenshot shows the 'Edit Trusted Networks' configuration page in the Cisco Secure Access interface. The page title is 'Edit Trusted Networks' and it includes a sub-header 'Include as many criteria as required to define a trusted network or network segment. Help'. The configuration is divided into several sections:

- Trusted Network Name:** A text input field containing 'LAN'. Below it is a checkbox labeled 'Set as default Trusted Network for UZTA'.
- Inspect:** Two radio button options: 'Physical adapters' (selected) and 'Physical and virtual adapters' (with a 'Beta' tag).
- Criteria:** A section for defining criteria with the note 'Multiple entries within each criterion are tested as OR: Any of the entered values can match.' It contains two criteria:
 - DNS Domains:** A dropdown menu set to 'DNS Domains' and a text input field containing 'csa.local'. A '- Remove Criterion' link is next to it.
 - DNS Servers:** A dropdown menu set to 'DNS Servers' and a text input field containing '10.10.10.20'. A '- Remove Criterion' link is next to it.

At the bottom of the criteria section is a '+ Add Criterion' button. The page also features a 'Cancel' button and a 'Save' button in the bottom right corner.

Secure Access - ZTA TND Configuration

Step - 5 Add Private Resource to the ZTA Profile

1. Navigate to **Connect > End User Connectivity > Zero Trust Access** and click 3 dots to edit ZTA profile

The screenshot shows the 'End User Connectivity' page in the Cisco Secure Access interface. The page title is 'End User Connectivity' and it includes a sub-header 'End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. Help'. The page is divided into several sections:

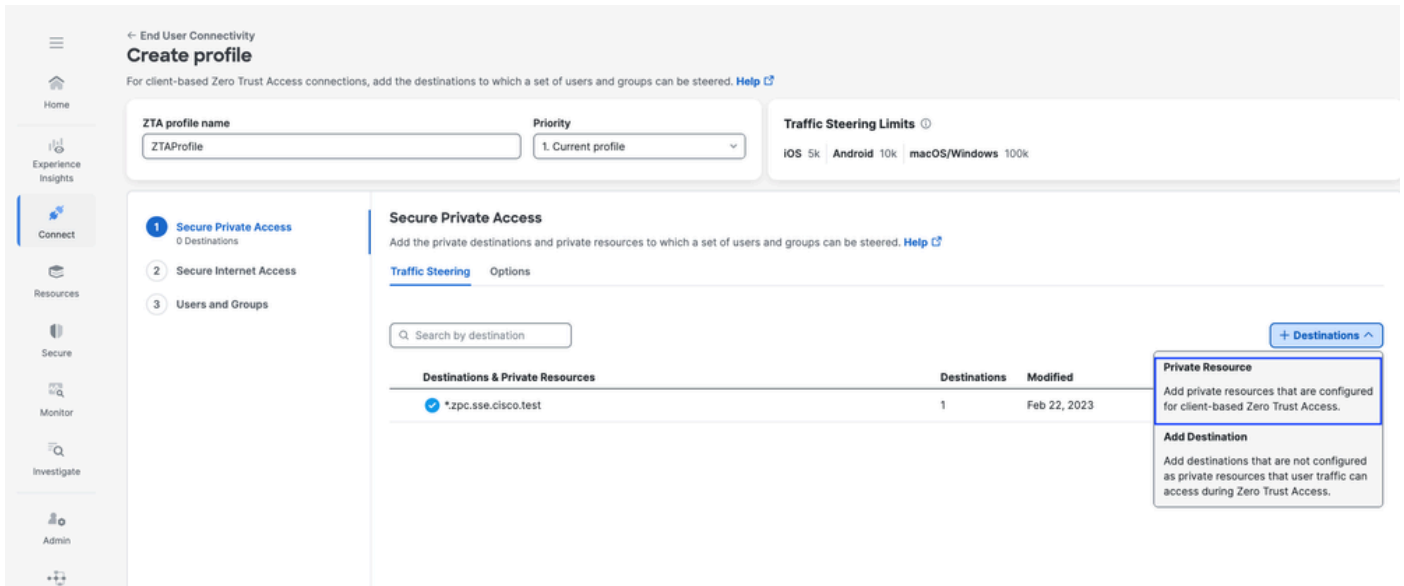
- Enrollment methods:** A section with a 'Manage' button. It contains text about enrollment methods for Windows, macOS, Android, and iOS devices.
- Zero Trust Access Profiles:** A section with a 'Manage Trusted Networks' button and a '+ ZTA Profile' button. It contains a table of Zero Trust Access profiles.

#	Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
1	ZTAProfile	2 Destinations Trusted Networks Disabled	Use ZTA for all destinations 0 Exceptions Trusted Networks Disabled	1 Users 0 Groups	Jan 25, 2026

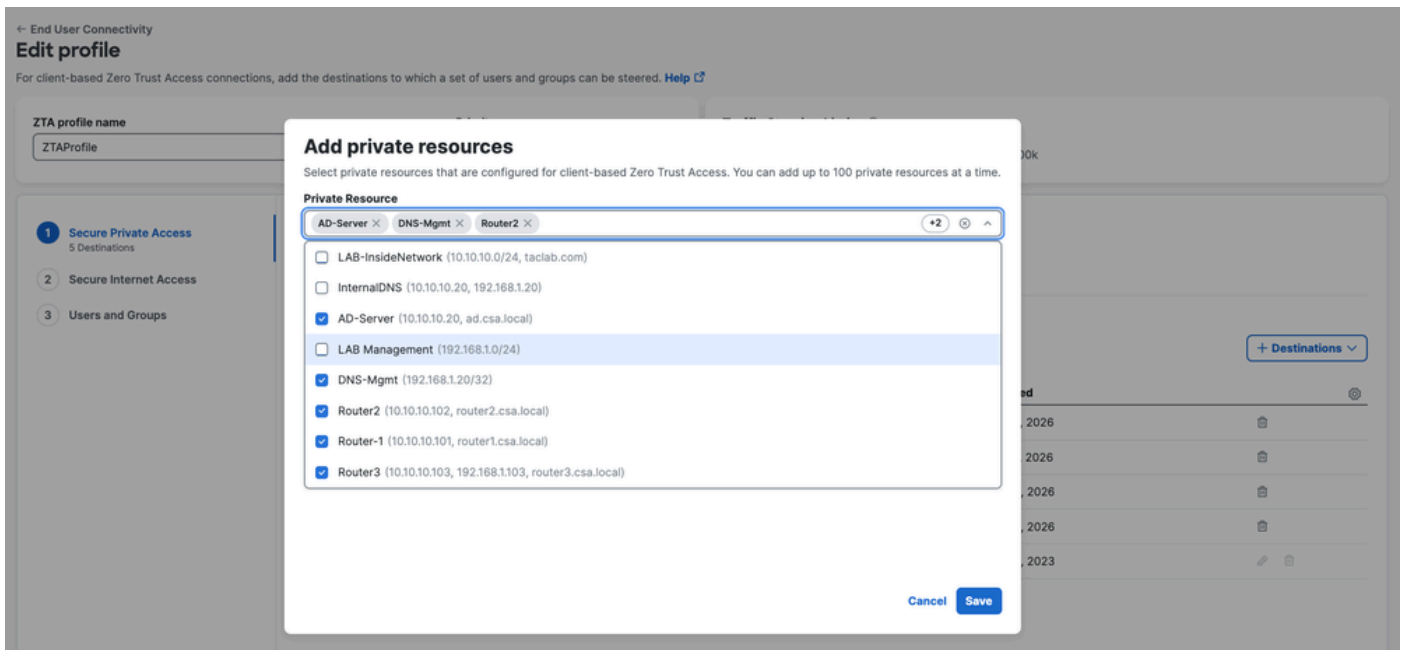
Below the table, there are 'Edit' and 'Delete' buttons for the profile.

Secure Access - ZTA Profile

2. Add the Private Resource



Secure Access - ZTA Profile



Secure Access - ZTA Profile

3 . Add Users and Groups

← End User Connectivity
Create profile
 For client-based Zero Trust Access connections, add the destinations to which a set of users and groups can be steered. [Help](#)


ZTA profile name: ZTAProfile | Priority: 1. Current profile | Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

- Secure Private Access (2 Destinations)
- Secure Internet Access
- Users and Groups**

Users and Groups
 Add a set of users and groups that will be steered to various destinations added to this ZTA profile

Users 0 | Groups 0

Q Search + Users and Groups

Name	Email	Type	Users
 No users + Users and Groups			

Secure Access - ZTA Profile

ZTA profile name: ZTAProfile | Priority: 1. Current profile | Traffic Steering Limits: iOS 5k | Android 10k | macOS/Windows 100k

- Secure Private Access (2 Destinations)
- Secure Internet Access
- Users and Groups**

Users and Groups
 Add a set of users and groups that will be steered to various destinations added to this ZTA profile

Users 1 | Groups 0

Q Search + Users and Groups

Name	Email	Type	Users
jay (jay@csa.local)	jay@gmail.com	User	-

Rows per page 10 < >

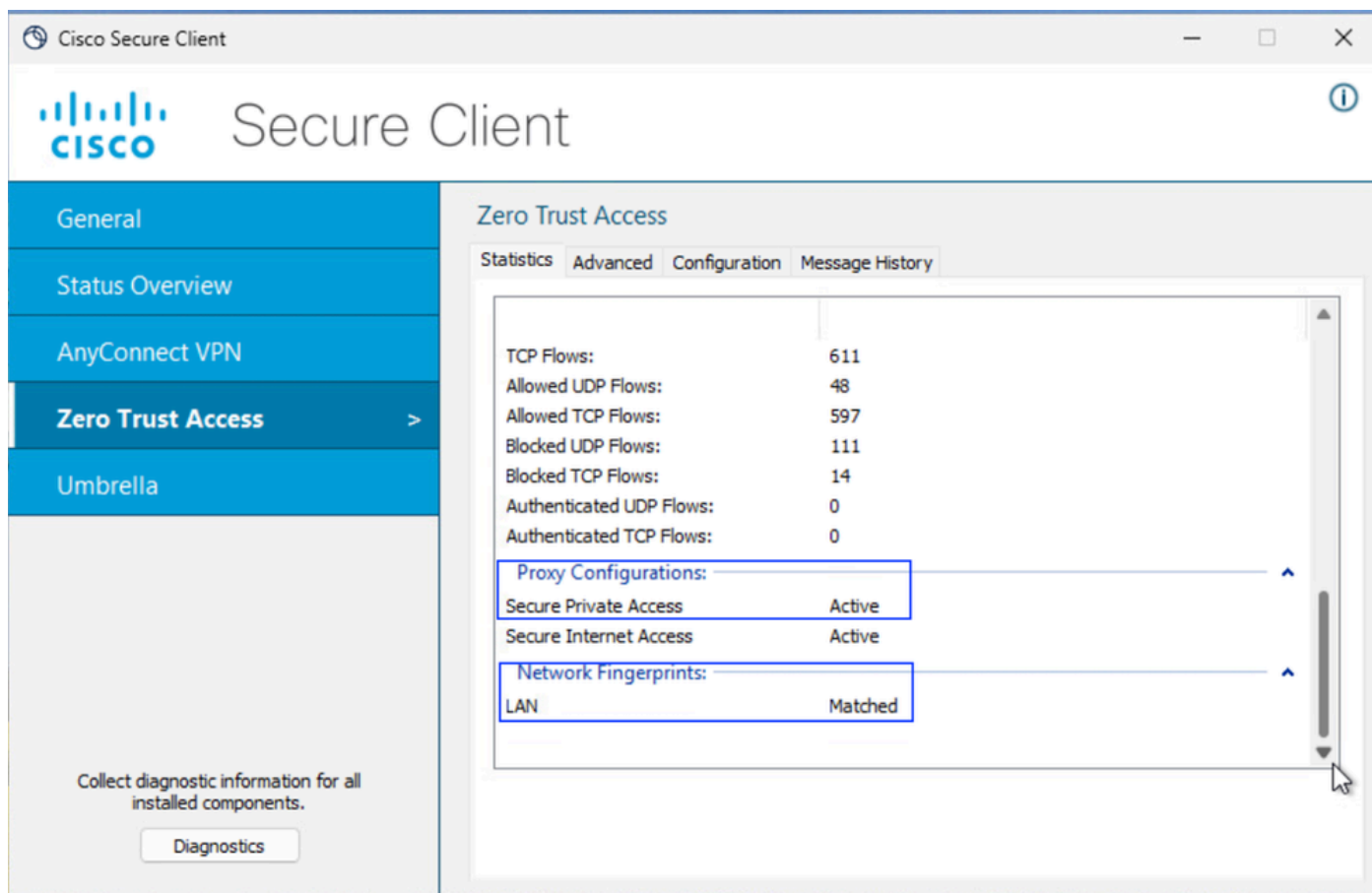
Back Close

Secure Access - ZTA Profile

Step - 6 Verify access to the Private Resource

When the user is Local

1. Verify the Network Fingerprint for ZTA TND, it should match if the user is Local and Secure Private Access should be Active



Secure Access - PR Testing

2. Verify the remote user can resolve FTD FQDN

```
C:\Users\jay>ping ftd.csa.local

Pinging ftd.csa.local [10.10.10.1] with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\jay>nslookup ftd.csa.local
Server: AD.csa.local
Address: 10.10.10.20

Name: ftd.csa.local
Addresses: 10.10.10.1
```

Secure Access - PR Testing

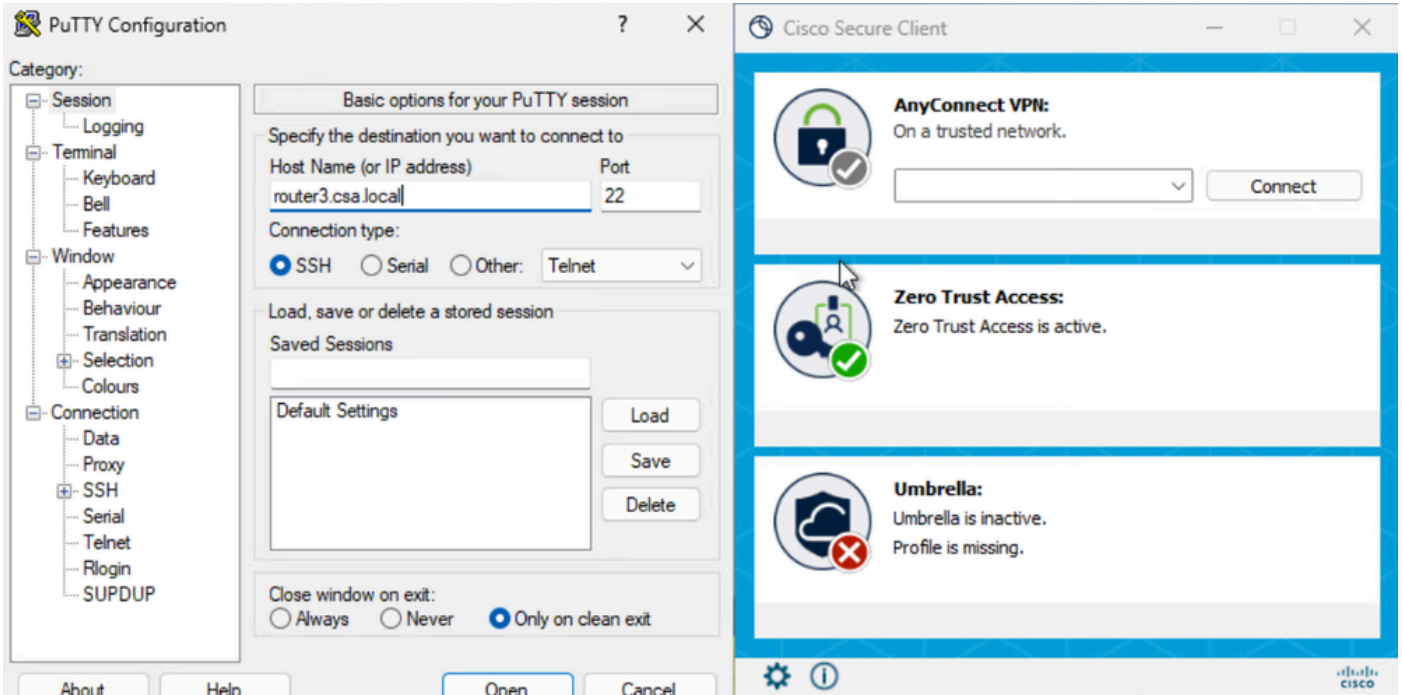
3. Verify FTD can reach to private resource using FQDN

```
ftd# ping router3.csa.local
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.103, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd# █
```

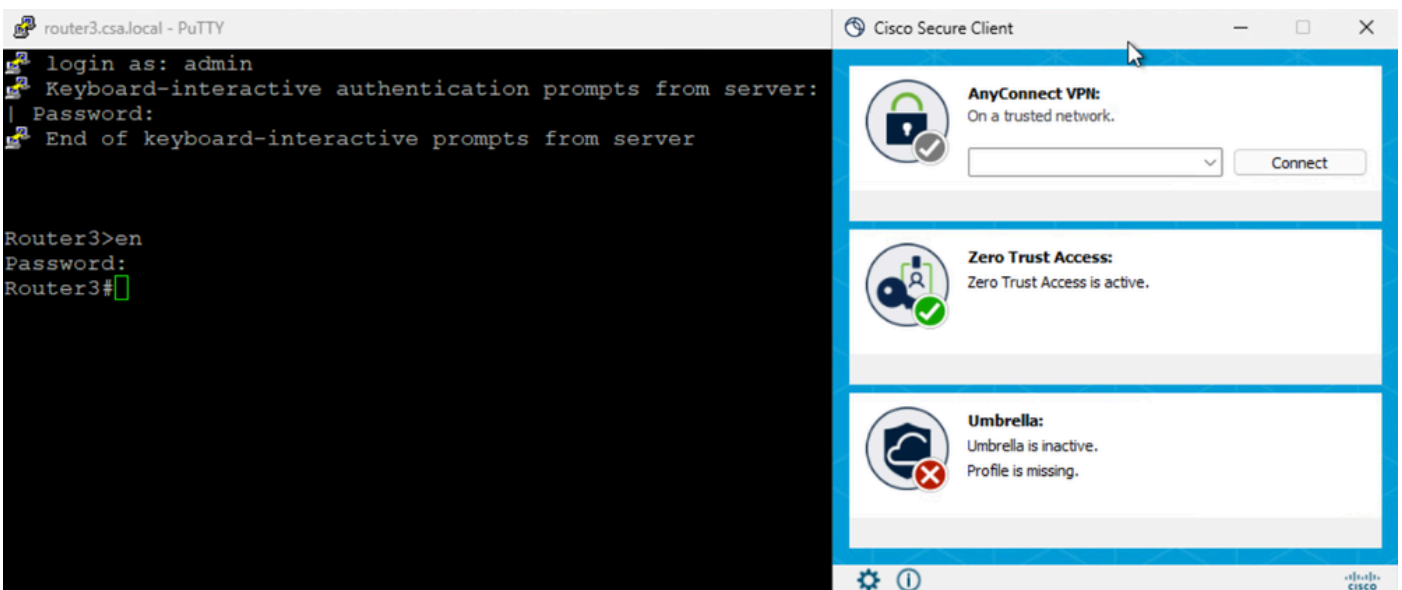
Secure Access - PR Testing

4. Test the SSH connection to the Private Resource

Access the PR using FQDN

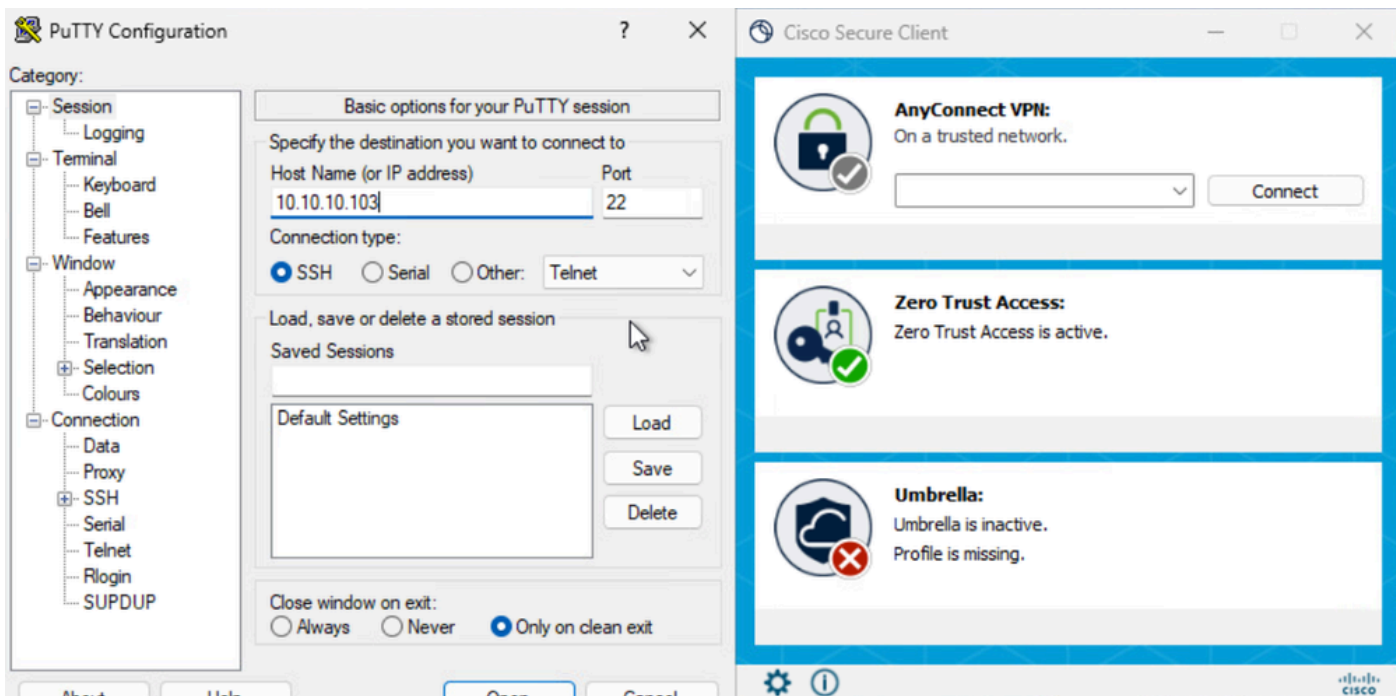


Secure Access - PR Testing

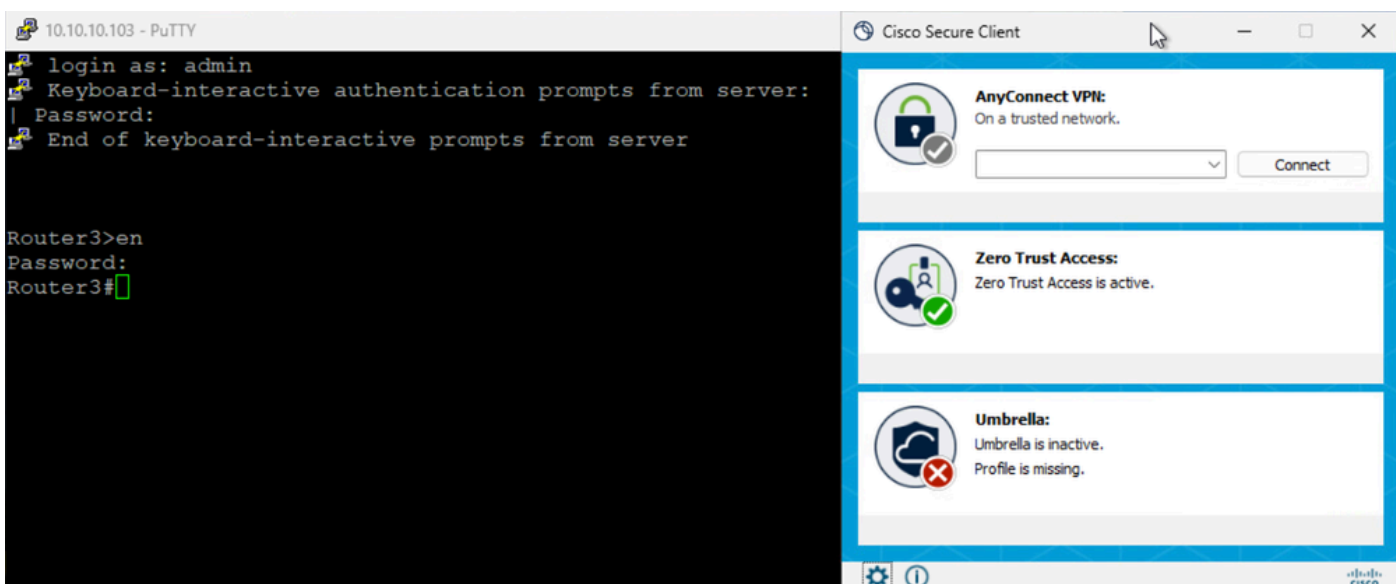


Secure Access - PR Testing

Access the PR using IP address



Secure Access - PR Testing

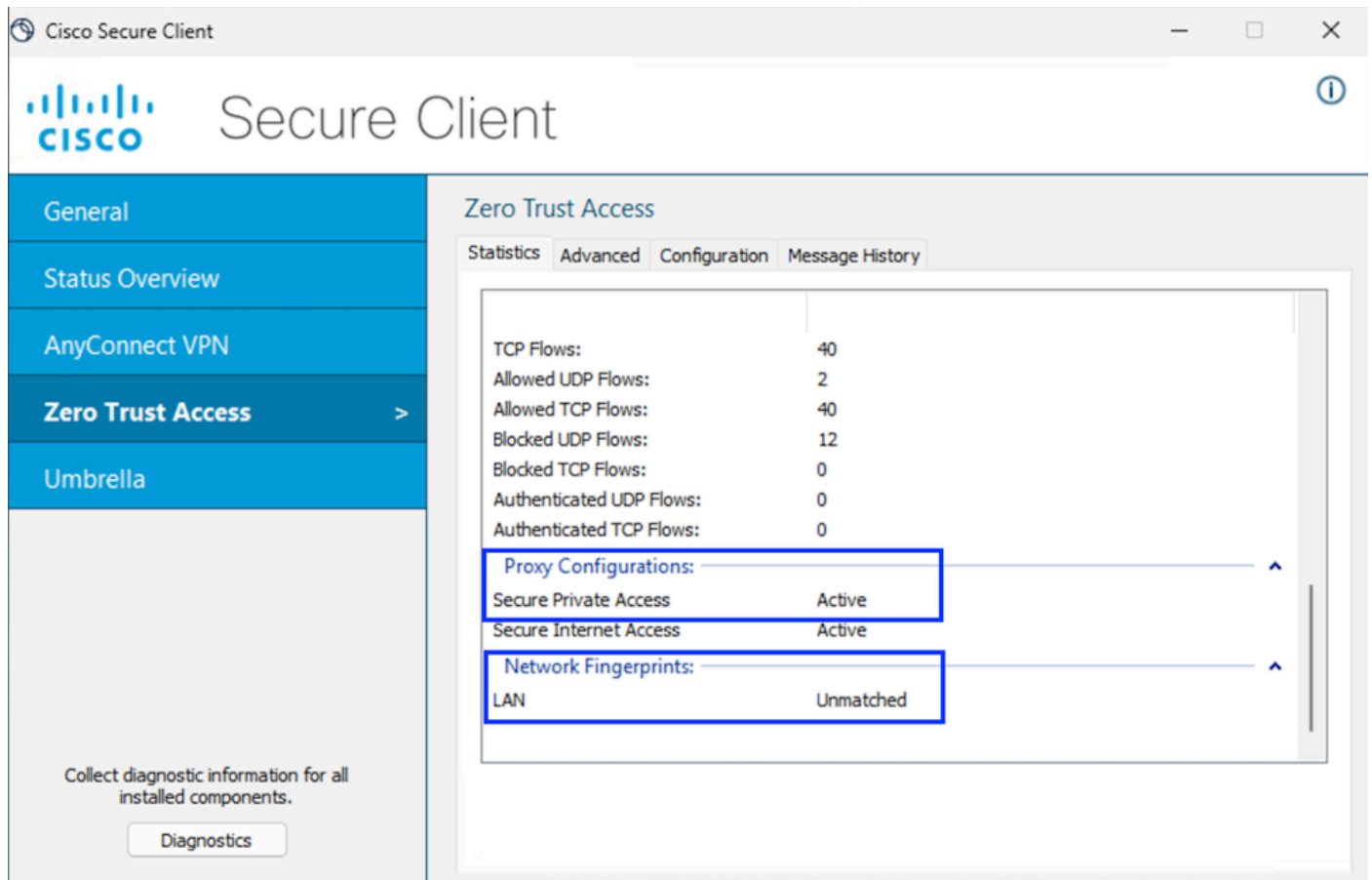


Secure Access - PR Testing

5. Verify Secure Access Activity Serach logs

When the user is Remote

1. Verify the Network Fingerprint for ZTA TND, it should unmatched if the user is remote



The screenshot shows the Cisco Secure Client interface. The left sidebar contains navigation options: General, Status Overview, AnyConnect VPN, Zero Trust Access (selected), and Umbrella. The main content area is titled 'Zero Trust Access' and has tabs for Statistics, Advanced, Configuration, and Message History. The Statistics tab is active, displaying a table of network flow statistics. Two sections are highlighted with blue boxes: 'Proxy Configurations' and 'Network Fingerprints'.

Category	Value
TCP Flows:	40
Allowed UDP Flows:	2
Allowed TCP Flows:	40
Blocked UDP Flows:	12
Blocked TCP Flows:	0
Authenticated UDP Flows:	0
Authenticated TCP Flows:	0

Category	Status
Proxy Configurations:	
Secure Private Access	Active
Secure Internet Access	Active

Category	Status
Network Fingerprints:	
LAN	Unmatched

At the bottom of the sidebar, there is a button labeled 'Diagnostics' with the text 'Collect diagnostic information for all installed components.'

Secure Access - PR Testing

2. Verify the remote user can resolve FTD FQDN

```
C:\Users\jay>ping ftd.csa.local

Pinging ftd.csa.local [192.168.1.12] with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\jay>

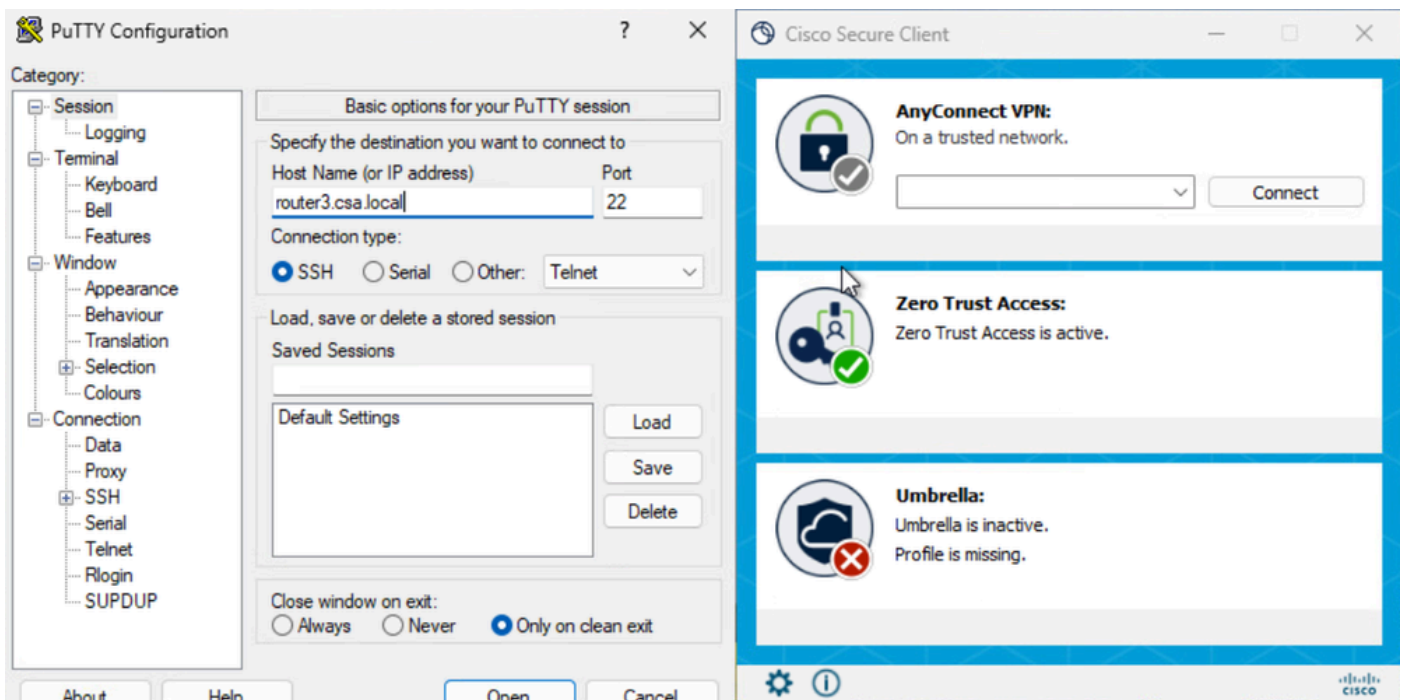
C:\Users\jay>nslookup ftd.csa.local
Server: AD.csa.local
Address: 192.168.1.20

Name: ftd.csa.local
Addresses: 192.168.1.12
```

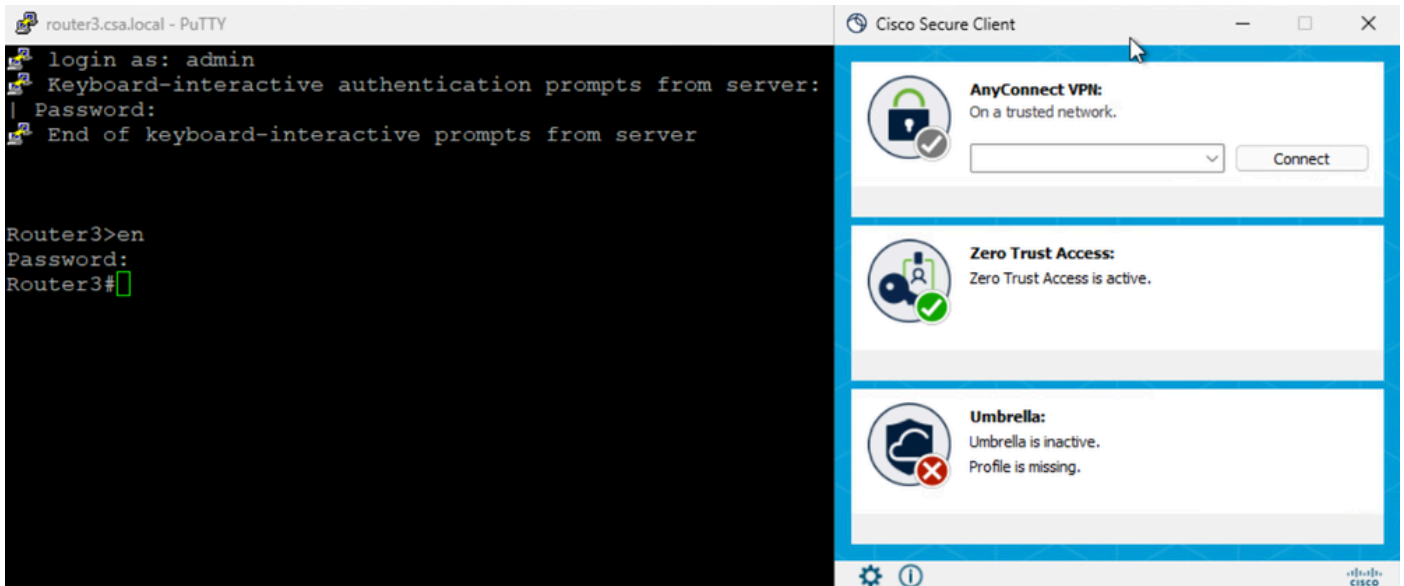
Secure Access - PR Testing

3. Test the SSH connection to the Private Resource

Access the PR using FQDN

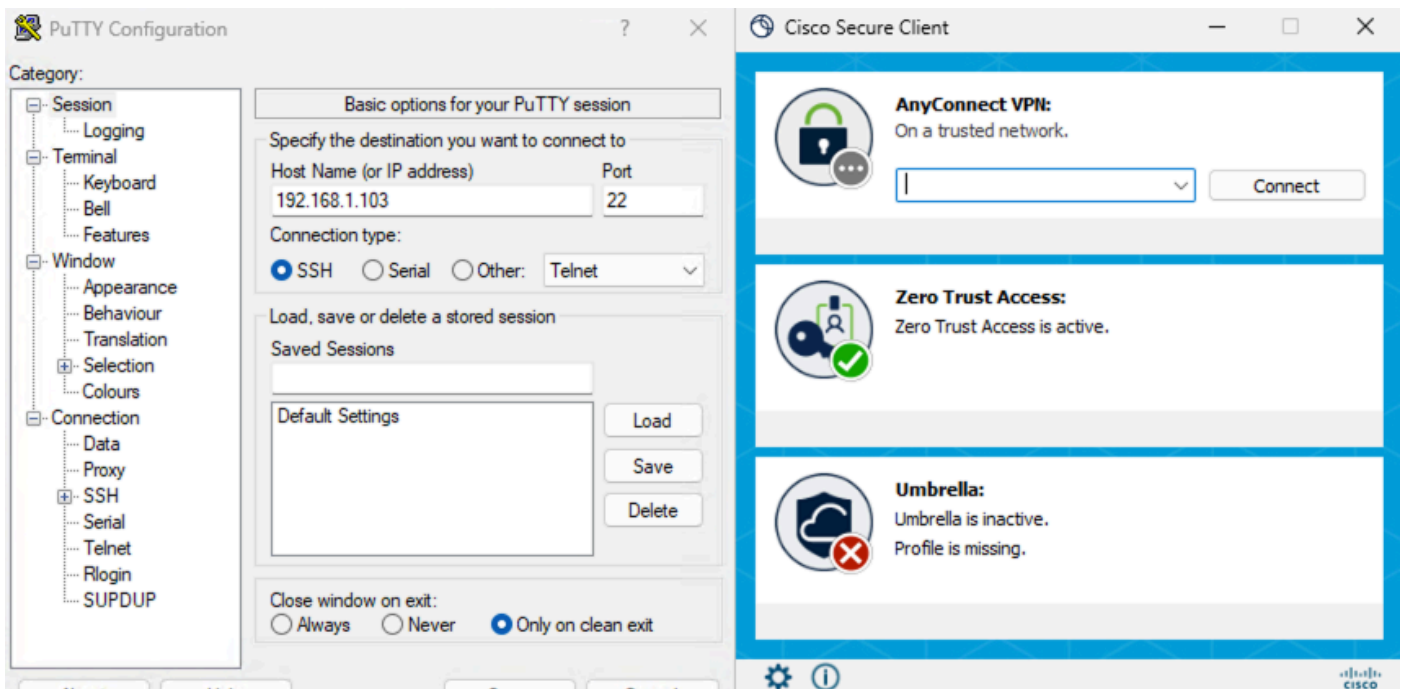


Secure Access - PR Testing

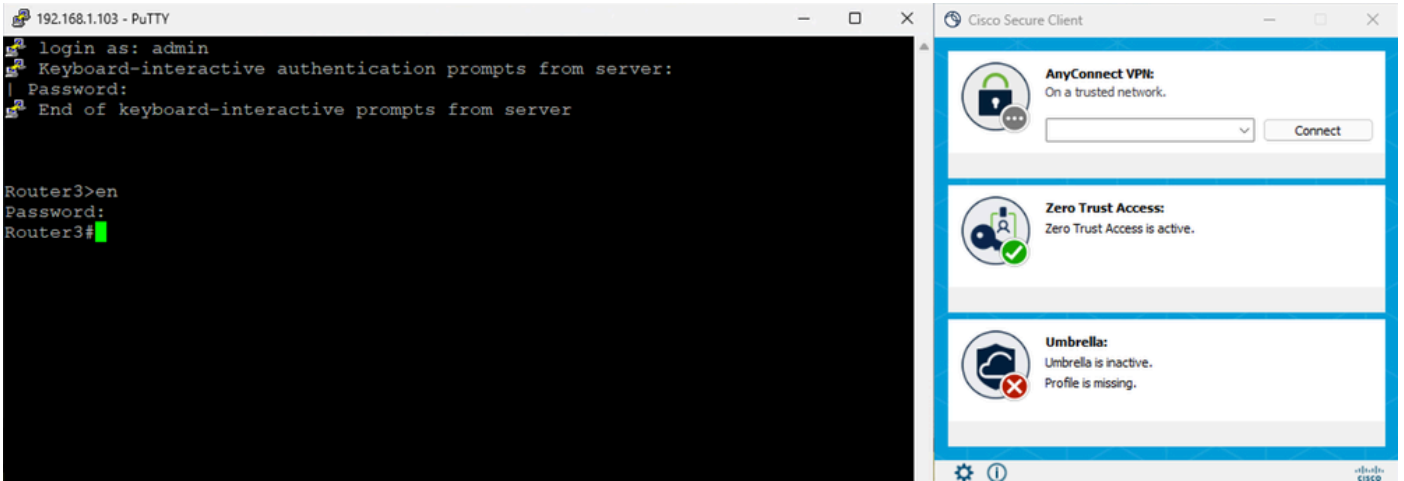


Secure Access - PR Testing

Access the PR using IP address



Secure Access - PR Testing



Secure Access - PR Testing

5. Verify Secure Access Activity Serach logs

Activity Search

Filters: Search by domain, identity, or URL. Advanced. CLEAR

Response: Allowed X

34 Total. Viewing activity from Feb 22, 2026 7:30 AM to Feb 23, 2026 7:30 AM. Page: 1. Results per page: 50. 1 - 34 of 34

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3	ZTAProfile	Router3-SSH-Allow

Secure Access - Activity Search

Activity Search

Filters: Search by domain, identity, or URL. Advanced. CLEAR

Response: Allowed X

34 Total. Viewing activity from Feb 22, 2026 7:30 AM to Feb 23, 2026 7:30 AM. Page: 1. Results per page: 50. 1 - 34 of 34

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/App
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	192.168.1.103	192.168.1.103	22	Allowed	Router3
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.103	22	Allowed	Router3
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	192.168.1.103	22	Allowed	Router3
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router3.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	Jay (jay@csa.local)	Jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2

Event Details

Allowed

Block Reason: -

Connection Method: ZTA Client-based

Time: Feb 23, 2026 7:30 AM

Access details

Identity: Jay (jay@csa.local)

Rule Name: ZTNA Client

Rule Name: Router3-SSH-Allow

Resource/Application: Router3

Zero Trust Access Profile: ZTAProfile

Trusted Network: No Match

Enforcement Point: Secure Access Cloud

Destination: router3.csa.local

Destination IP: 192.168.1.103

Troubleshoot

Useful Commands:

```
> show allocate-core profile  
> show asp inspect-dp snort  
> sh running-config universal-zero-trust  
> show interface ip brief
```

```
> debug universal-zero-trust zproxy 7
```

! and then go to expert mode

```
# tail -f /ngfw/var/log/messages
```

```
# show conn all
```

```
# show nat detail
```

```
# show asp table socket
```