

# 보안 액세스에서 개인 리소스 액세스를 위한 범용 ZTNA 구성

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[유니버설 ZTNA 정보](#)

[네트워크 탐지](#)

[시행 유형](#)

[활용 사례](#)

[아키텍처 구성 요소](#)

[패킷 플로우](#)

### [구성](#)

[네트워크 다이어그램](#)

[테스트 사례](#)

[테스트 사례 1: 원격 사용자 - 클라우드 시행](#)

[테스트 사례 2 - 원격 사용자 - 로컬 시행](#)

[테스트 사례 3 - 로컬 사용자 - 로컬 시행](#)

[테스트 사례 4 - 로컬 및 원격 사용자 - TND를 통한 로컬 또는 클라우드 시행](#)

### [문제 해결](#)

[유용한 명령:](#)

---

## 소개

이 문서에서는 서로 다른 트래픽 경로를 사용하는 Universal ZTNA를 통한 Private Resource Access에 대한 컨피그레이션을 다룹니다.

## 사전 요구 사항

범용 ZTNA 구성에 앞서 다음 구성을 완료해야 합니다.

- [Cisco Secure Access의 ID 공급자](#)
- [인증서를 사용하여 제로 트러스트 액세스에 디바이스 등록](#)
- [Cisco Secure Firewall로 터널 구성](#)

- [원격 액세스 가상 사설망](#)
- [보안 액세스의 리소스 커넥터](#)
- [보안 클라우드 제어에서 FTD 온보딩](#)
- 하이브리드 ZTNA 기능 플래그는 각 보안 액세스 테넌트에 대해 활성화되어야 합니다. 플래그를 활성화하려면 Cisco TAC에 문의하십시오.

## 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Access 및 Firewall Threat Defense의 IPsec VPN 구성
- IdP(ID 제공) - Active Directory에서 사용자 프로비저닝
- Cisco Secure Access의 원격 VPN 구성
- Cisco Secure Access에 리소스 커넥터 구축
- ZTA 인증서 기반 등록
- 인증서 - OpenSSL, CSR 생성, 인증서 템플릿 등

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure Firewall Threat Defense( 버전 7.7.10 )
- Cisco Secure Firepower Management Center(버전 7.7.10)
- Cisco Secure Client(ZTA 버전 5.1.10.1720)
- Windows 11
- Windows 2019 Server - 인증 기관
- ESXi의 리소스 커넥터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

### 유니버설 ZTNA 정보

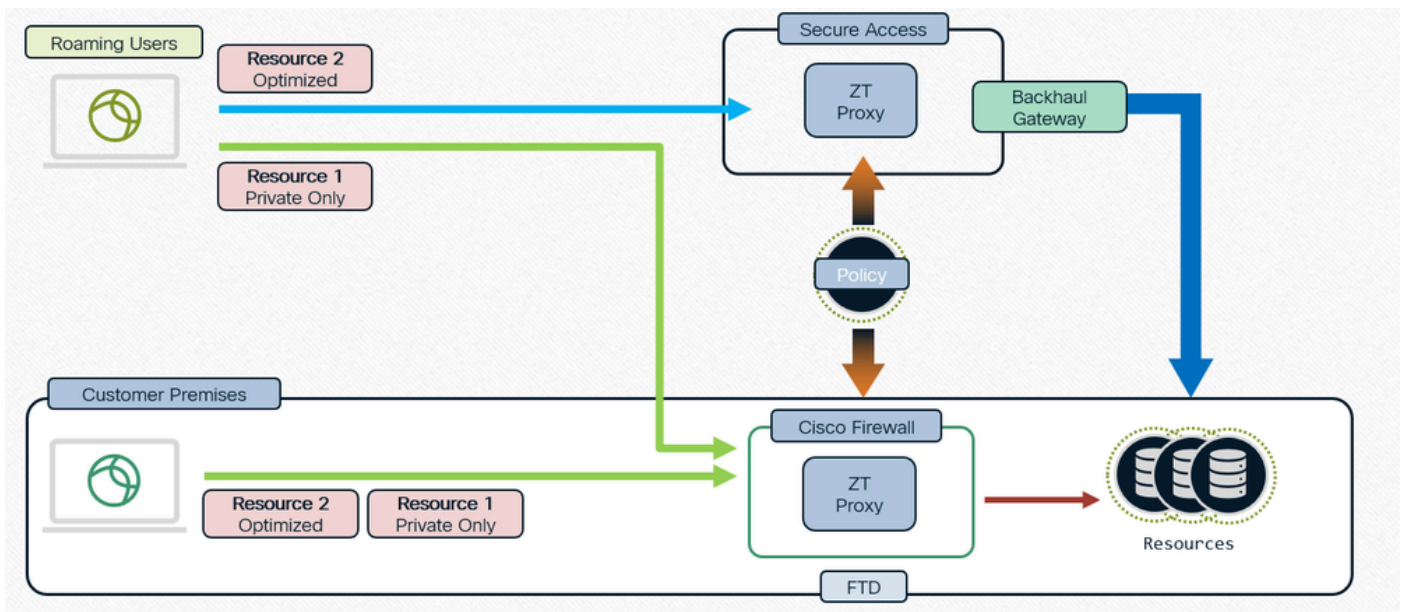
uZTNA(Universal Zero Trust Network Access)는 관리자가 사용자 ID(사용자 신뢰 및 상태 포함)에 따라, 그리고 RA-VPN에서와 같이 전체 네트워크에 대한 액세스 권한을 부여하지 않고 내부 네트워크 리소스에 대한 액세스를 구체적으로 허용할 수 있게 합니다. uZTNA를 통해 관리자는 원격 및 온

프리미스 사용자 모두를 위한 내부 리소스 및 애플리케이션을 보호할 수 있습니다.

uZTNA는 한 애플리케이션에 부여된 액세스가 다른 애플리케이션에 대한 액세스를 암시적으로 승인한다고 가정하지 않으므로 네트워크 공격 표면이 줄어듭니다.

보안 액세스는 액세스 정책을 평가합니다. Secure Firewall Management Center에서 디바이스에 배포된 모든 액세스 제어 정책은 무시됩니다.

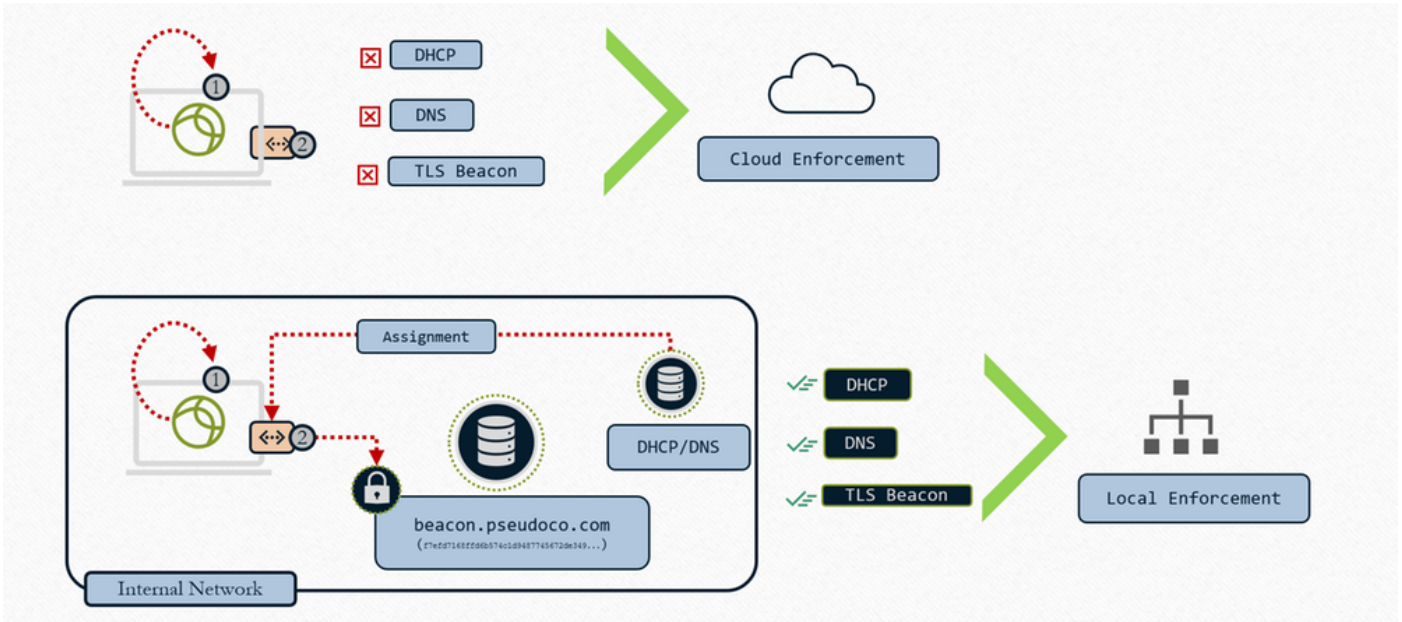
트래픽 프록시는 물론 IPS, 파일 및 악성코드 정책 시행은 FTD(Firepower Threat Defense)에서 수행됩니다.



단일 정책, 분산 시행

네트워크 탐지

클라우드 또는 로컬 적용 결정



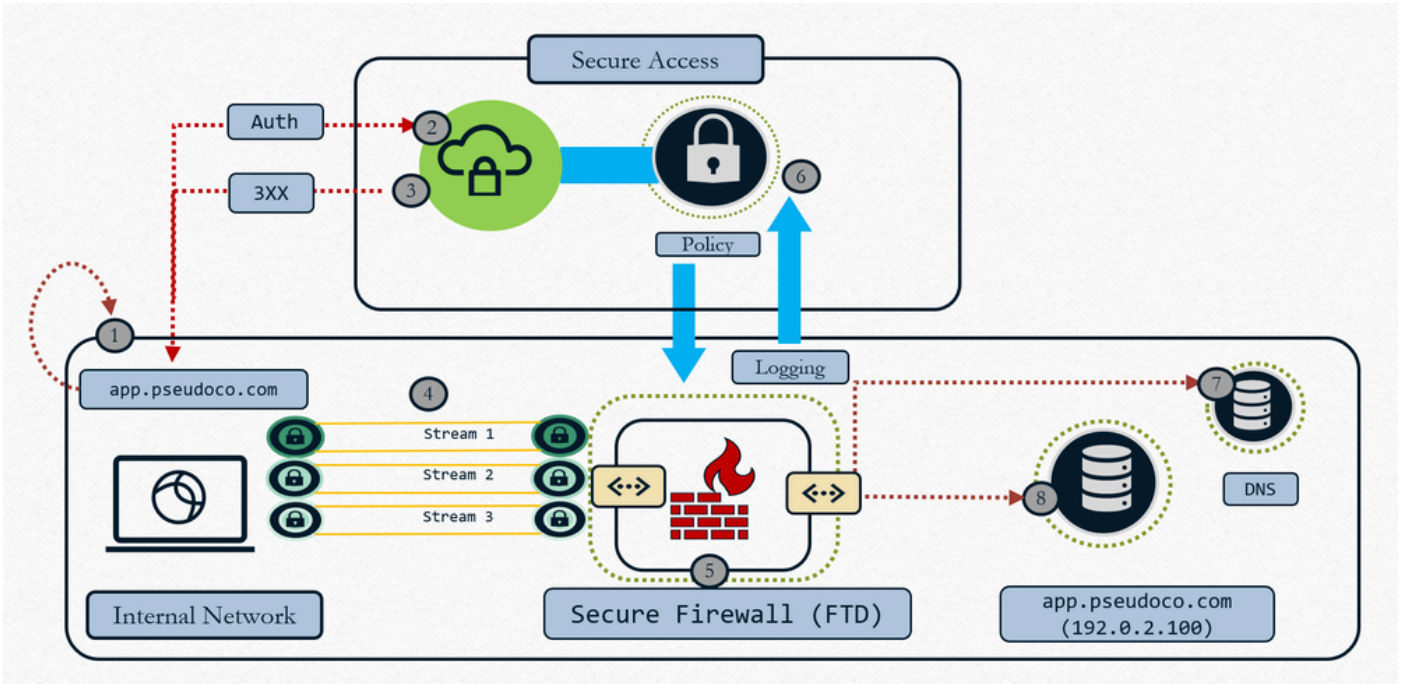
## 범용 ZTNA - 클라우드 또는 로컬 시행 결정

- 1- 클라이언트가 네트워크 컨피그레이션을 위해 로컬 인터페이스 문의
- 2- 클라이언트가 TLS 신호를 검색합니다.
- 3- 조건이 일치하는 경우 - 로컬 시행
- 4- 조건이 일치하지 않는 경우 - 클라우드 시행

리소스를 "클라우드 또는 로컬 시행"으로 구성하고 TND 규칙을 FTD와 연결할 때, 실제로 수행하는 작업은 클라이언트에 전송되는 인터셉트 규칙 집합으로, TND 규칙 평가를 포함합니다. 따라서 해당 클라이언트는 클라우드에서 TND 규칙을 평가하라는 안내를 받게 됩니다. 연결을 전송할 때 TND - 네트워크 지문 평가 결과를 HTTP 헤더에 입력하여 프록시에 온팜인지 신뢰할 수 없는 네트워크인지를 알려준 다음 프록시에서 해당 정보를 사용하고 그에 따라 트래픽을 리디렉션합니다. 핑거프린트가 일치하는 경우, Zproxy는 클라이언트에게 트래픽을 FTD로 리디렉션하도록 지시하며, 핑거프린트가 일치하지 않으면 트래픽을 클라우드로 리디렉션합니다. 신뢰할 [수 있는 네트워크 탐지를 사용하여 제로 트러스트 네트워크 액세스 구성을 참조하십시오.](#)

## 시행 유형

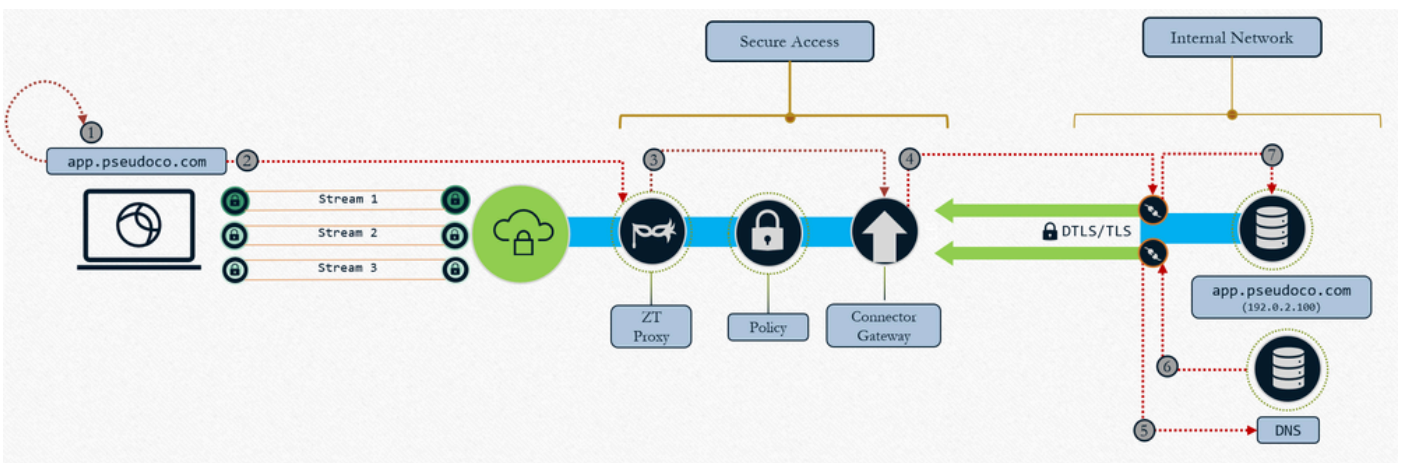
- 로컬 적용 경로: 방화벽 시행



## Universal ZTNA - 로컬 시행

1. 사용자 요청 앱, 클라이언트가 임시 IP(localhost range)에 대한 요청을 캡처 및 확인
2. 인증 제어 트래픽은 정책 평가를 위해 Secure Access Cloud로 전송됩니다.
3. 클라우드는 데이터 계획 시행을 위해 FTD로 리디렉션 반환(정책이 허용하는 경우)
4. 방화벽으로 구성된 헤드엔드(인터페이스)로 트래픽 조정
5. 로컬 프록시 데이터 플레인을 사용하여 클라우드에 정의된 정책 적용(IPS, 악성코드, 암호 해독)
6. 일관된 보고를 위해 이벤트가 기록되고 중복 이벤트가 클라우드로 제공됨
7. 방화벽은 리소스 트래픽을 라우팅하기 위해 로컬 네트워크에서 DNS 확인을 수행합니다(허용된 경우).
8. 방화벽은 방화벽이 TCP 프록시로 작동함에 따라 리소스에 대한 연결을 구축합니다(리소스에 대한 새 연결 구축).

- 클라우드 시행 경로: 네트워크 외부

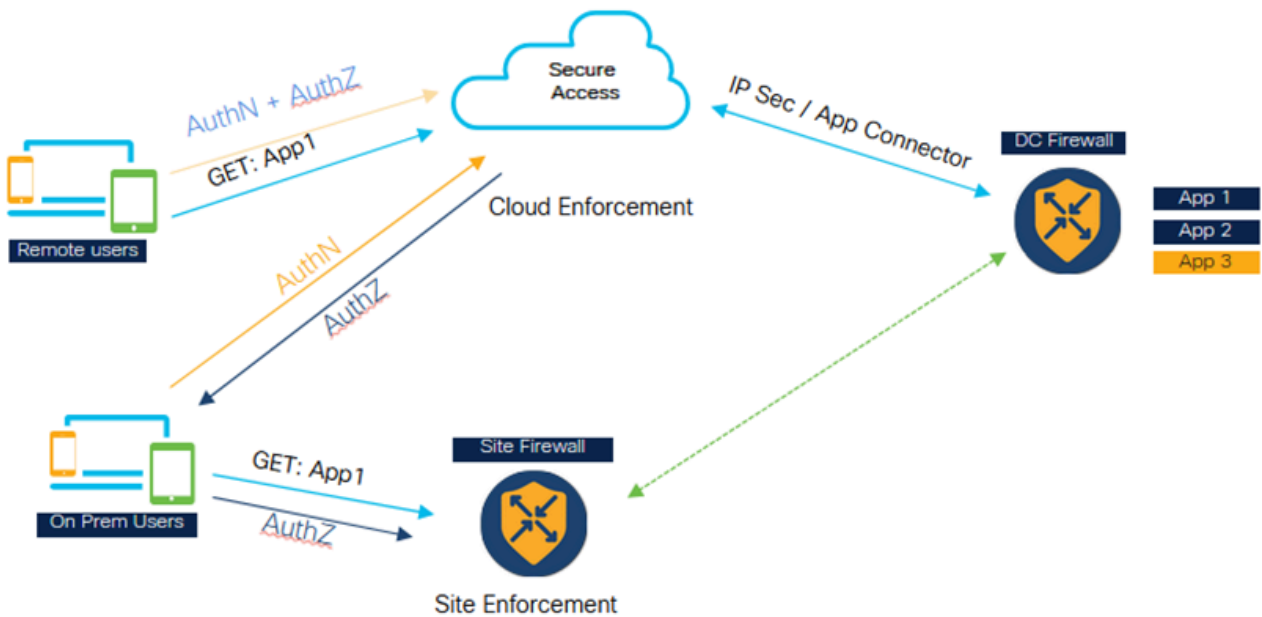


## 범용 ZTNA: 클라우드 시행

1. 사용자 요청 앱, 클라이언트가 임시 IP(localhost range)에 대한 요청을 캡처 및 확인
2. 트래픽은 보안 액세스에서 제로 트러스트 프록시로 전송됨
3. TCP 연결이 프록시되고 매핑된 리소스 커넥터에 구축되며, 트래픽에 정책이 적용됩니다.
4. 게이트웨이가 리소스 커넥터에 대한 연결을 설정합니다.
5. 리소스 커넥터에서 리소스 IP 확인
6. 로컬 DNS는 리소스 IP로 응답함
7. 리소스 커넥터가 리소스에 대한 연결을 설정합니다.

## 활용 사례

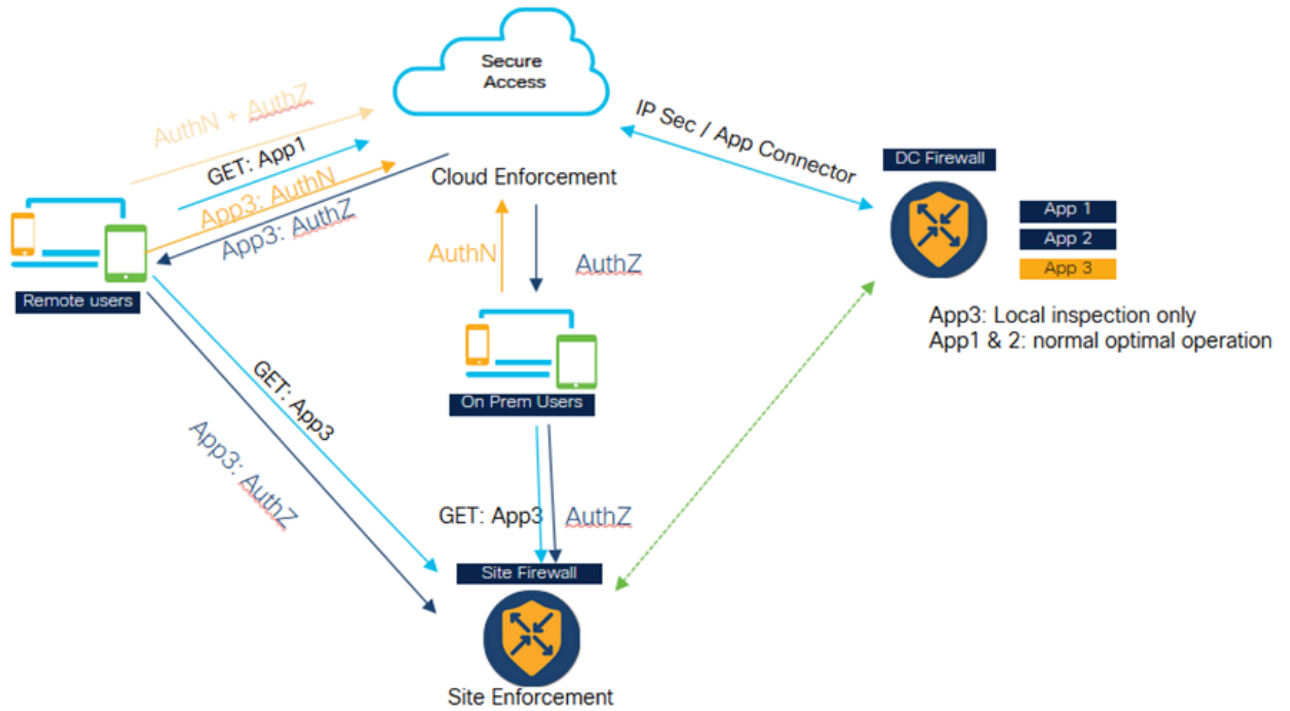
### 사례 1: 구내형 사용자를 위한 일관되고 최적화된 ZTNA



### 범용 ZTNA - 일관되고 최적화된 ZTNA(온프레미스 사용자)

- 보안 액세스와 방화벽 모두 애플리케이션을 보호하도록 구성됩니다.
- 사용자가 원격인 경우 정책 평가 및 검사를 위해 Secure Access(보안 액세스)로 이동합니다.
- 사용자가 내부/온프레미스인 경우 프라이빗 트래픽 검사를 위해 방화벽으로 이동합니다.
- 온프레미스 사용자는 Secure for authentication and evaluation(인증 및 평가를 위해 보안)으로 계속 이동할 수 있습니다. Datapath 트래픽이 방화벽으로 이동하고 정책 컨피그레이션에 따라 검사됩니다.
- 방화벽을 통해 애플리케이션에 액세스하는 내부 사용자는 클라우드로 이동한 후 데이터 센터로 백홀되는 트래픽을 피할 수 있으므로 성능 면에서 이점이 있습니다

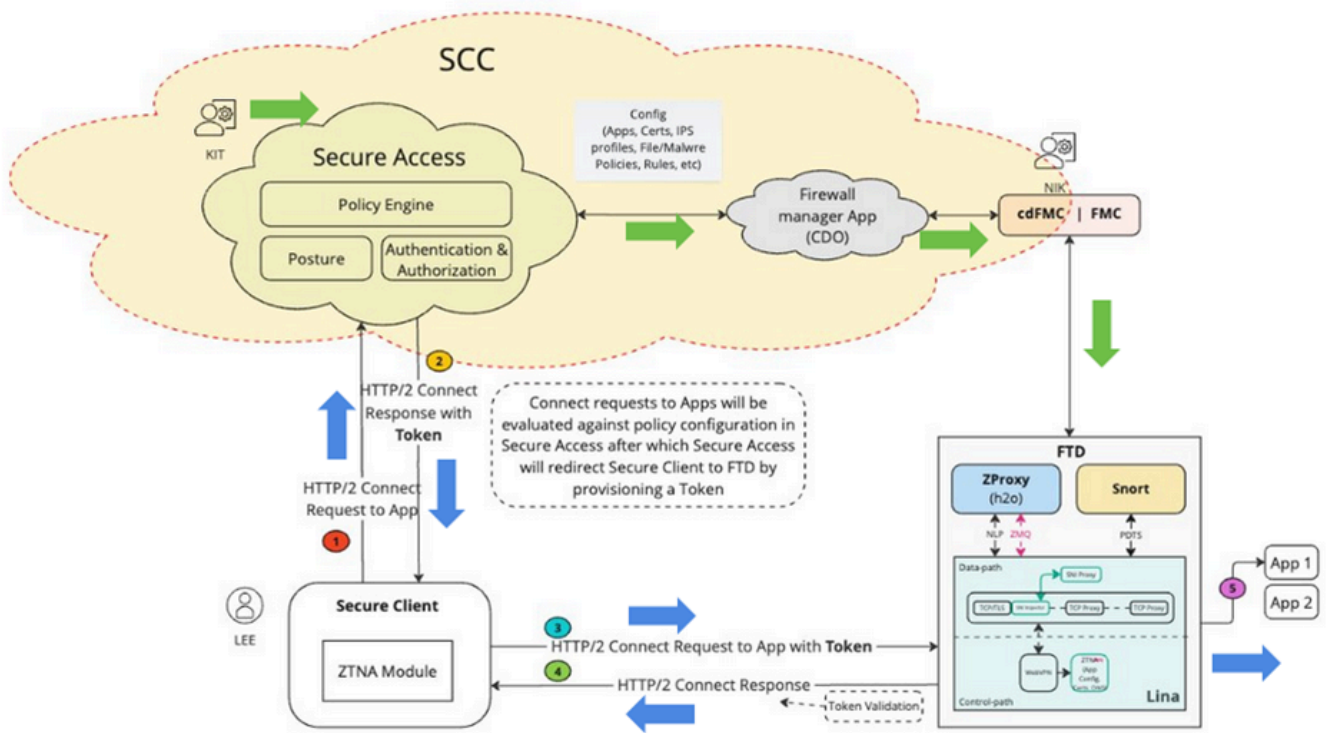
## 사례 2: 민감한 애플리케이션에 대한 비공개 검사



## 범용 ZTNA - 민감한 애플리케이션에 대한 비공개 검사

- 특정 중요 애플리케이션은 방화벽을 통해 항상 액세스하도록 구성할 수 있습니다.
- 앱 데이터 트래픽은 클라우드로 이동할 필요가 없습니다. 예를 들어 소스 코드와 같은 민감한 데이터 애플리케이션이 있을 수 있는데, 고객은 클라우드로 이동하지 않으려 합니다.
- 이러한 시나리오에서는 원격 및 온prem 사용자 트래픽이 항상 방화벽을 통과하여 검사됩니다. 그러나 이 시나리오에서도 역시 인증 및 정책 평가가 클라우드에서 항상 이루어지므로 데이터 부분 트래픽만 방화벽을 통과합니다.

## 아키텍처 구성 요소



## Universal ZTA - 아키텍처 구성 요소

SCC(Security Cloud Control)는 ZTNA 솔루션의 기본 관리자입니다. uZTNA는 SCC에 처음 구축된 기능입니다.

SCC에서는 두 개의 마이크로 애플리케이션 Secure Access와 방화벽이 있습니다. SCC가 프로비저닝되고 필수 기능 플래그가 활성화되면 SCC 패널의 왼쪽에 이러한 마이크로 애플리케이션을 볼 수 있습니다.

보안 클라이언트: Secure Client에서는 ZTNA(Zero Trust Access Module)를 활성화해야 애플리케이션에 액세스할 수 있습니다.

방화벽 위협 방어: 이러한 애플리케이션을 보호하는 FTD. FTD는 H2O라고도 하는 ZT 프록시를 실행합니다(프록시가 Secure Access Cloud에서 실행되는 것과 동일).

이제 사용자(예: KIT)가 Secure Access 마이크로-애플리케이션에서 프라이빗 리소스 및 정책을 구성하면 이 컨피그레이션이 SCC의 방화벽 마이크로-애플리케이션으로 푸시됩니다. 방화벽 애플리케이션은 FTD, FTD 컨피그레이션의 내부 내용, FTD에서 컨피그레이션을 구축하고 관리하는 방법을 이해합니다. 따라서 방화벽 앱은 이 컨피그레이션을 검증하고 FMC API를 호출하여 컨피그레이션을 FMC에 푸시한 다음 결국 FTD에 구축합니다. FTD는 자동 구축 옵션을 활성화하여 관리자(예: Nick)가 수동 구축을 수행할 필요가 없도록 할 수 있습니다.

1. 사용자(예: Lee)가 애플리케이션에 액세스를 시도하는 경우 보안 클라이언트는 mTLS 채널을 사

용하여 Secure Access에 연결합니다. Secure Access는 클라이언트 디바이스 인증서를 사용하여 사용자를 인증합니다. 그런 다음 해당 사용자 및 해당 애플리케이션에 대해 구성된 권한 부여, 상태 및 기타 정책을 평가합니다.

2. Secure Access(보안 액세스). 애플리케이션이 방화벽에 의해 보호되고 있음을 마지막으로 발견하면 인증 토큰을 생성합니다. 그러면 방화벽에 이 토큰이 이미 인증되고 권한이 부여되었음을 알립니다. 인증 토큰은 암호화되고 보안 액세스에 의해 서명됩니다

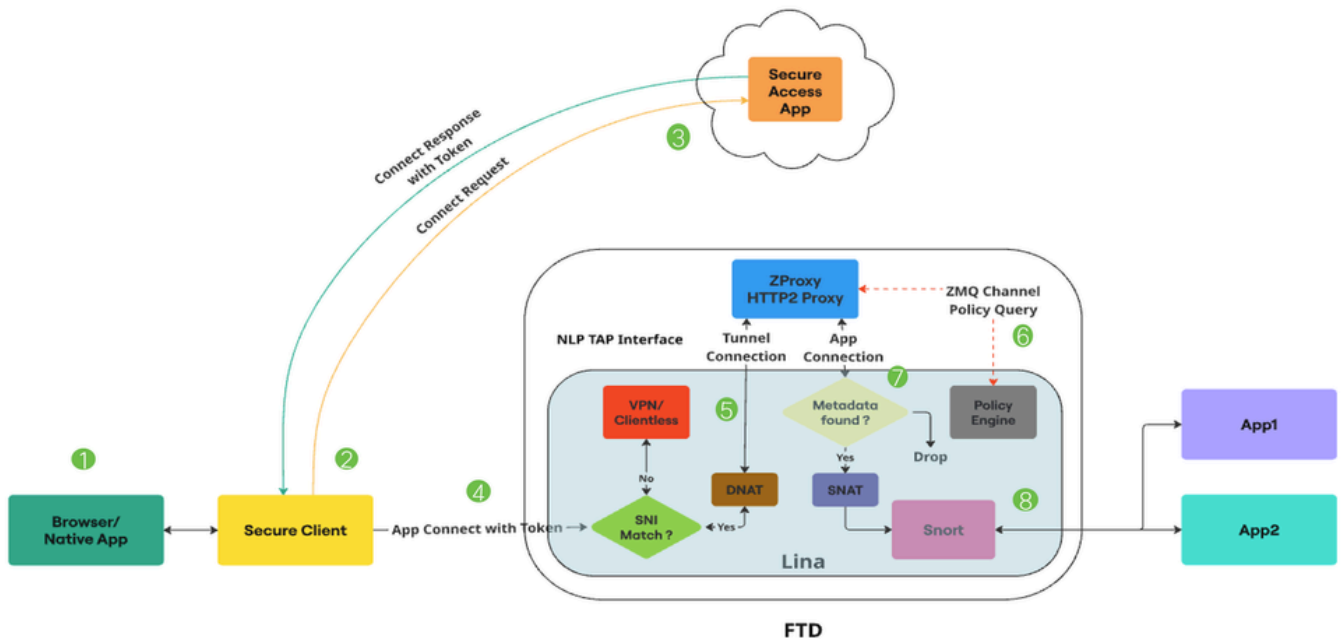
3. Secure Access는 인증 토큰과 함께 FTD로 보안 클라이언트를 리디렉션합니다.

4. Secure Client는 FTD에 대한 또 다른 연결을 설정합니다. 이는 mTLS 채널을 통한 HTTP2 연결입니다. 토큰과 함께 액세스 중인 애플리케이션에 대한 CONNECT 요청을 보냅니다.

5. 이제 FTD가 토큰을 검증합니다. 토큰이 성공적으로 검증되면 사용자가 해당 애플리케이션에 액세스할 수 있습니다. 그런 다음 FTD는 승인을 Secure Client로 다시 전송합니다

## 패킷 흐름

### 범용 ZTNA 상세 패킷 흐름



### 범용 ZTA - 패킷 흐름

1. 사용자가 웹 브라우저 또는 네이티브 애플리케이션을 통해 애플리케이션에 액세스하려고 시도합니다.

2. Secure Client가 연결을 인터셉트하여 Private Resource에 액세스하려는 사용자로 식별합니다.

3. Secure Client가 Secure Access에 대한 mTLS 연결을 설정하여 애플리케이션에 대한 액세스를 요청합니다. Secure Access는 범용 ZTNA 정책 및 상태 프로필에서 규정 준수를 확인합니다. 모든 것이 정상인 경우 Secure Access는 사용자 세부 정보, 애플리케이션 세부 정보 및 IPS/File 정책과 같은 필수 정보를 포함하는 액세스 토큰을 생성합니다.

4. 액세스 토큰은 Secure Access에서 암호화되고 서명됩니다. 그러면 Secure Access가 토큰과 함께 Secure Client를 FTD로 리디렉션합니다.

5. 패킷이 Lina Datapath에 도달하면 SNI 검사기가 연결을 인터셉트하고 클라이언트 Hello의 서버 이름(SNI 확장)이 장치에 구성된 프록시 FQDN과 일치하는지 확인합니다. SNI가 일치하면 연결은 ZProxy로 연결됩니다. SNI가 일치하지 않으면 Universal ZTNA와 공존할 수 있는 다른 기능으로 연결됩니다.

예를 들면 다음과 같습니다. VPN, 종속 포털 또는 클라이언트리스 ZTNA. HTTP/2 프로토콜을 통한 MASQUE를 지원하는 ZProxy는 전용 코어에서 Non-Lina 프로세스로 FTD에서 실행됩니다. Lina와 ZProxy 간의 통신은 데이터 트래픽 처리를 위해 NLP Tap 인터페이스를 사용합니다. 연결의 대상 IP는 SNI 검사기에서 TAP 인터페이스 IP로 변환됩니다.

6. ZProxy가 보안 클라이언트로부터 mTLS 터널 연결을 수신하면 보안 클라이언트에서 보낸 클라이언트 장치 인증서를 확인합니다. 또한 APP Connect와 함께 전송된 액세스 토큰을 확인합니다. Lina와 ZProxy 사이에 Zero MQ 채널이 있습니다. 주로 제어 메시지를 교환하는 데 사용됩니다. ZProxy는 Lina와 통신하여 Private 리소스의 FQDN 확인에 이 채널을 사용합니다.

제로 MQ 채널은 액세스 토큰에 있는 정보를 Lina에게 전달하는 데에도 사용됩니다(예: Lina는 액세스 토큰 정보를 수신하여 메타데이터 DB에 저장한다).

7. 제어 메시지가 교환되면 ZProxy는 전용 리소스에 대한 새 연결을 시작합니다. TCP 또는 UDP일 수 있습니다. 그런 다음 Lina는 이 앱 연결에 대해 메타데이터 DB 조회를 수행합니다. 메타데이터를 찾을 수 없는 경우 연결이 삭제됩니다.

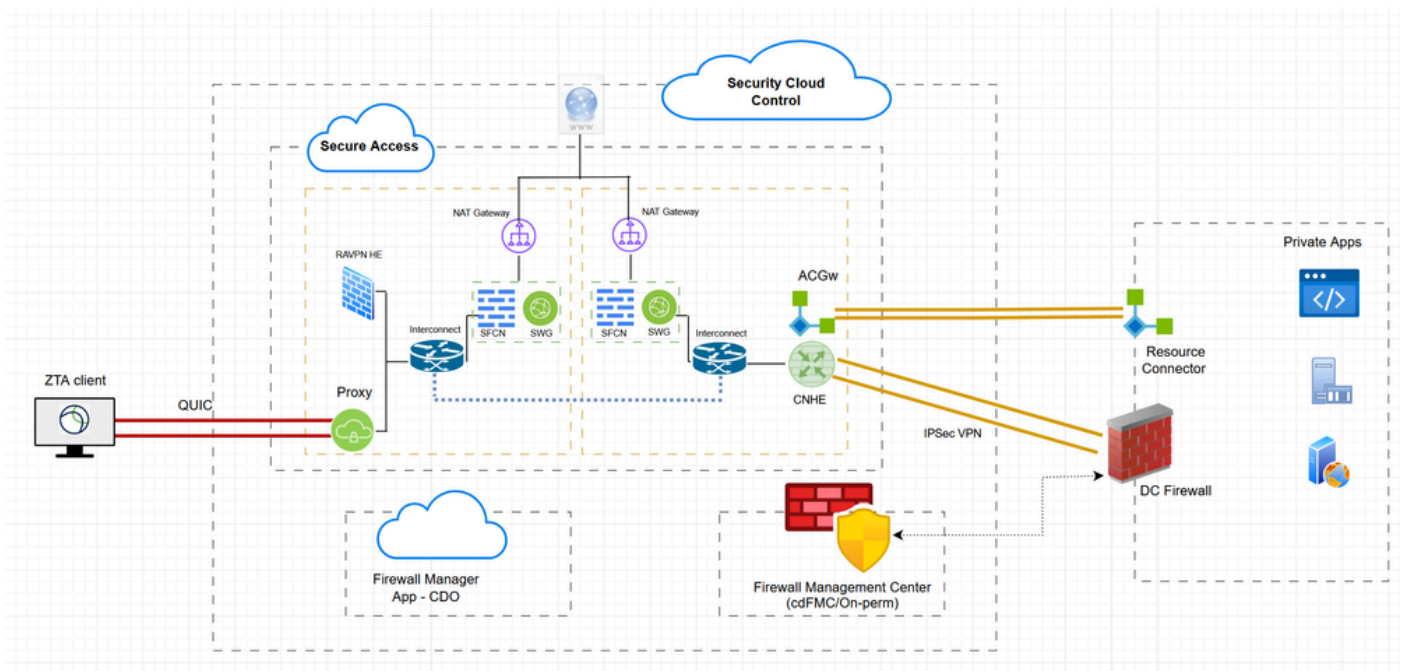
8. 앱 연결은 ZProxy에서 시작되므로 내부 IP(예:169.251.1.2)가 소스 IP로 사용됩니다. 이는 FTD 이그레스 인터페이스 IP로 변환되어 전송됩니다. 그런 다음 Lina는 파일 또는 IPS 정책이 액세스 토큰에 있는 경우에만 Snort 검사에 대해 Universal Zero Trust 흐름을 표시합니다. 액세스 토큰에서 얻은 규칙 ID는 연결 메타데이터에서 Snort로 전달됩니다.

9. Universal Zero Trust 규칙 및 해당 파일 및 IPS 정책 매핑이 FMC를 통해 FTD에 푸시됩니다. Snort의 Zero Trust 플러그인은 초기화 중에 이러한 규칙을 로드합니다. Lina는 Secure Access에서 얻은 Private Resource 액세스를 위한 액세스 토큰에 파일 또는 IPS 정책이 언급되어 있는 경우에만 Snort 검사를 위한 Universal Zero Trust 스트림 흐름을 표시합니다.

액세스 토큰에서 얻은 규칙 ID는 Conn Meta를 통해 Snort로 전달됩니다. 모든 Universal Zero Trust 스트림 흐름에 대해 Snort의 Zero Trust 플러그인은 Conn Meta에서 얻은 규칙 ID에 대한 규칙 조회를 수행합니다. 규칙 일치가 발견되면 흐름이 허용되며 해당 규칙과 관련된 IPS 및 파일 정책이 흐름에 적용됩니다. 규칙 일치가 발견되지 않으면 Snort의 Zero Trust 플러그인이 흐름을 차단합니다.

## 구성

### 네트워크 다이어그램

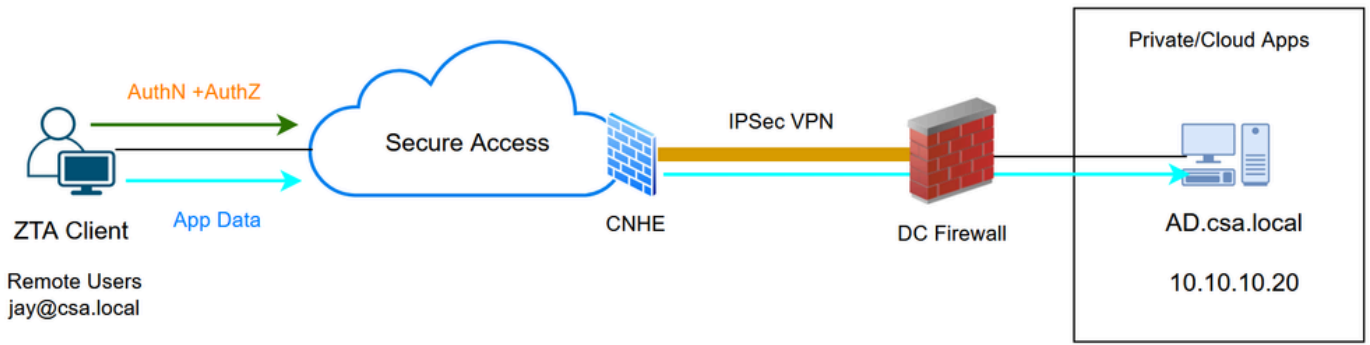


### 하이브리드 ZTNA - 네트워크 다이어그램

## 테스트 사례

### 테스트 사례 1: 원격 사용자 - 클라우드 시행

이 테스트 사례에서는 Cloud Enforcement(클라우드 시행)를 통해 Network Tunnel Group(네트워크 터널 그룹)을 통해 프라이빗 리소스에 액세스합니다. 이 경우 정책 평가와 애플리케이션 데이터 모두 ZTA 모듈을 통한 Secure Access에 의해 차단됩니다. 이 플로는 ZTA 등록 클라이언트에서 Network Tunnel Group 또는 Resource Connector를 통해 사설 애플리케이션에 액세스할 수 있는 일반적인 흐름입니다.

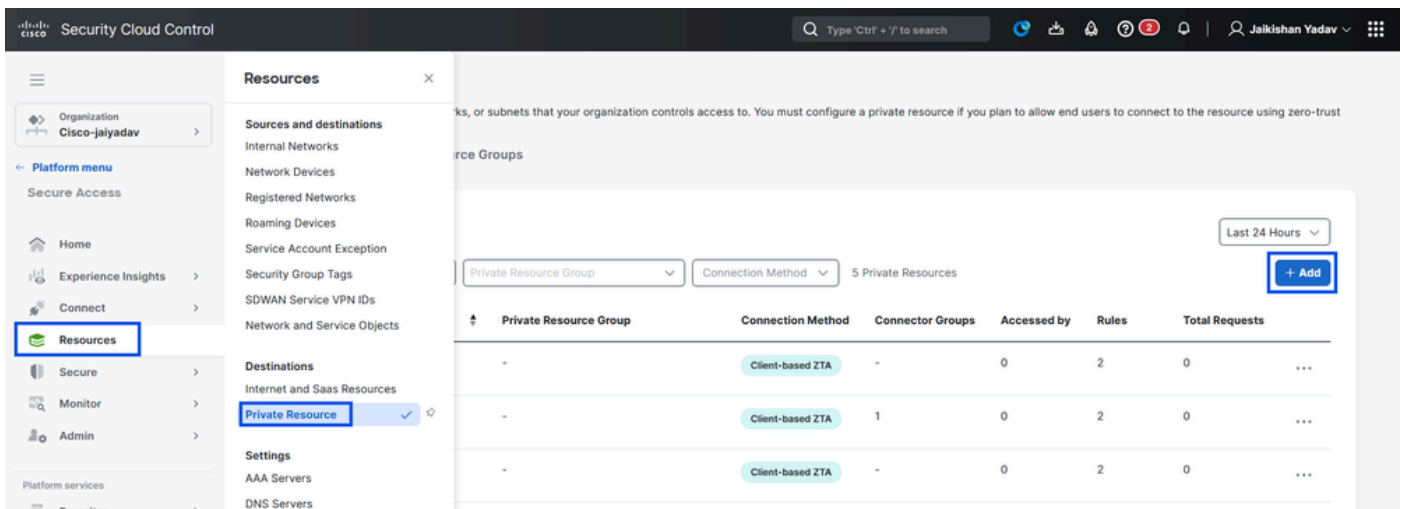


## 범용 ZTA - 테스트 사례 토폴로지

### 1단계 - Secure Access에서 프라이빗 리소스 정의

클라우드 시행으로 ZTA(Zero Trust Access) 등록된 디바이스를 통해 액세스할 수 있는 프라이빗 리소스 구성

1. Resources > Destinations > Private Resources > Click on +Add로 이동합니다.



## 보안 액세스 - 프라이빗 리소스 컨피그레이션

2. 개인 자원명에는 유의미한 자원명을 입력합니다. 설명의 경우, 리소스의 용도 또는 리소스 소유자의 이름과 같은 정보를 제공하는 것이 좋습니다.

## 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

AD-Server

Description (optional)

Active Directory server

### 보안 액세스 - 프라이빗 리소스 컨피그레이션

3. 액세스하려는 개인 자원의 FQDN을 입력합니다. 프라이빗 리소스의 IP 주소도 정의할 수 있습니다. 자세한 내용은 프라이빗 [리소스 추가를 참조하십시오](#)

4. 도메인을 확인할 내부 DNS 서버를 선택합니다

### Private resource address

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

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ

ad.csa.local

Protocol

Port / Ranges

TCP - RDP

▼

Any

+ Protocol & Port

Remove

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ

10.10.10.20

Protocol

Port / Ranges

TCP - RDP

▼

Any

+ 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) ▼

### 보안 액세스 - 프라이빗 리소스 컨피그레이션

5. 엔드포인트 연결 방법 선택

## 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**

Remote user

User in a trusted network

via Internet

Secure Access Cloud

Private Resource

Cancel Save and Test Save

## 보안 액세스 - 프라이빗 리소스 컨피그레이션

6. Save(저장)를 클릭합니다.

## 2단계 - 개인 액세스 규칙 생성

Universal ZTA 등록된 사용자가 액세스할 수 있도록 Secure Access의 비공개 액세스를 구성합니다 . 자세한 내용은 [개인 액세스 규칙을 참조하십시오](#)

1. Secure(보안) > Access Policy(액세스 정책)로 이동합니다

Organization: Cisco-jaiyadav

Platform menu: Secure Access

Secure

Policy: Access Policy

Data Loss Prevention Policy

Profiles: Endpoint Posture Profiles, IPS Profiles, Security Profiles, App Risk Profiles

Settings: Threat Categories, Notification Pages, Do Not Decrypt Lists, Certificates

Intent: [Dropdown] Objects: [Dropdown] Settings: [Dropdown]

Add Rule

Access	Action	Sources	Destinations	Security	Hits	Status
low	Private	Allow	Any AD Users	AD-Server	92	...
	Private	Allow	Any AD Users	ESXI	-	...
S-Allow	Private	Allow	Any AD Users	InternalDNS	-	...

## 보안 액세스 - 액세스 정책 컨피그레이션

2. 규칙 추가를 클릭한 다음 개인 액세스를 선택합니다.

규칙의 맨 위에는 규칙의 구성된 구성 요소를 설명하는 요약이 있습니다.

**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 ^

	#	Rule name	Access	Action	Sources	Destinations	Security
<input type="checkbox"/>	1	BlockPage-TEST	Internet	Block	Any	Generative A...	🌐
<input type="checkbox"/>	2	RAVPN-Allow	Internet	Allow	Any AD Users	Any	🌐🔒

Rows per page  1-2 of 2 < 1 >

**Private Access**  
Control and secure access to resources and applications that cannot be accessed by the general public.

**Internet Access**  
Control and secure access to public destinations from within your network and from managed devices

## 보안 액세스 - 액세스 정책 컨피그레이션

3. 규칙 이름 추가

**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**

Sources: Any — Allow — Security Controls — Destinations: Any private 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 To

## 보안 액세스 - 액세스 정책 컨피그레이션

4. 규칙 조치를 선택하고 출처 및 대상을 선택합니다

Rule name:  Rule order:

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

**Action**

**Allow**  
Allow specified traffic if security requirements are met.

**Block**  
Block specified traffic.

**From**  
Specify one or more sources.

**To**  
Specify one or more destinations.

+ AND

## 보안 액세스 - 액세스 정책 컨피그레이션

### 5. 엔드포인트 요구 사항 구성

**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](#)

## 보안 액세스 - 액세스 정책 컨피그레이션

### 6. 보안 구성

✓ **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](#)

## 보안 액세스 - 액세스 정책 컨피그레이션

### 7. 저장을 클릭합니다.

**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](#)

3 Rules [Customize view](#)

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

Rows per page: 100 | 1-3 of 3 | [1](#)

---

**Default Access Rules**

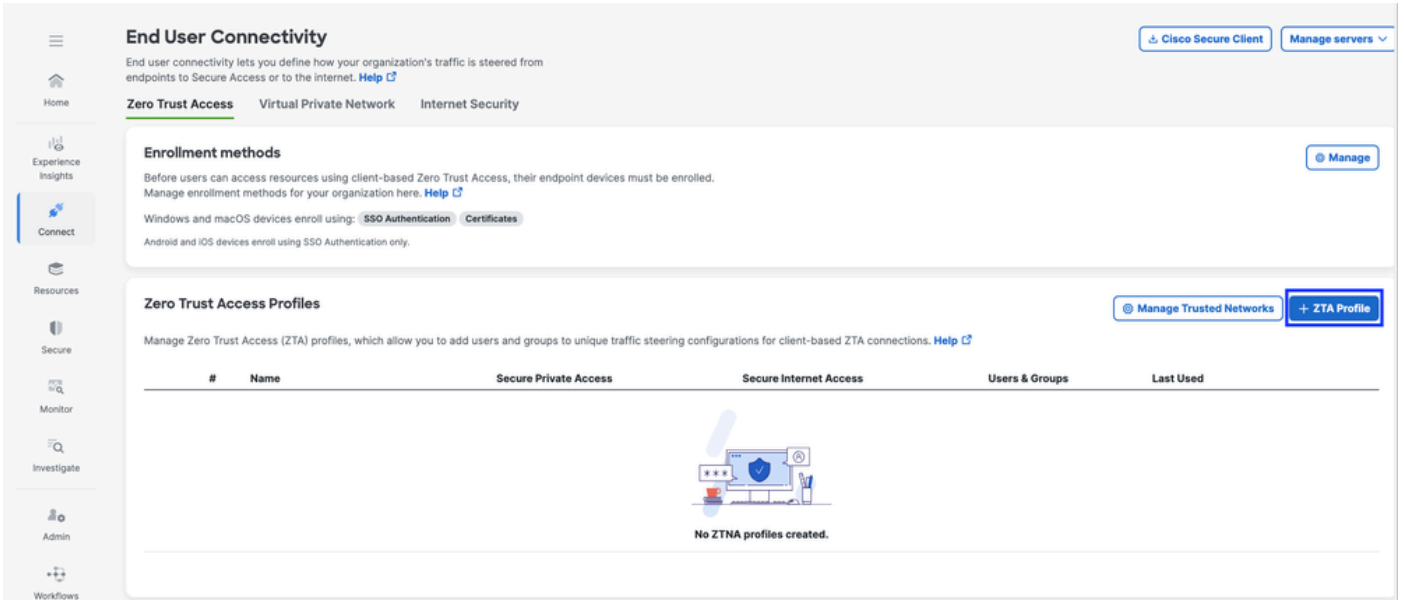
Rule name	Action	Sources	Destinations	Security	Posture
For all private access	Block	Any	Any private destination	-	-
For all Internet access	Allow	Any	Any Internet destination	🌐🔒	-

## 보안 액세스 - 액세스 정책 컨피그레이션

### 단계 - 3 ZTA 프로필에 프라이빗 리소스 추가

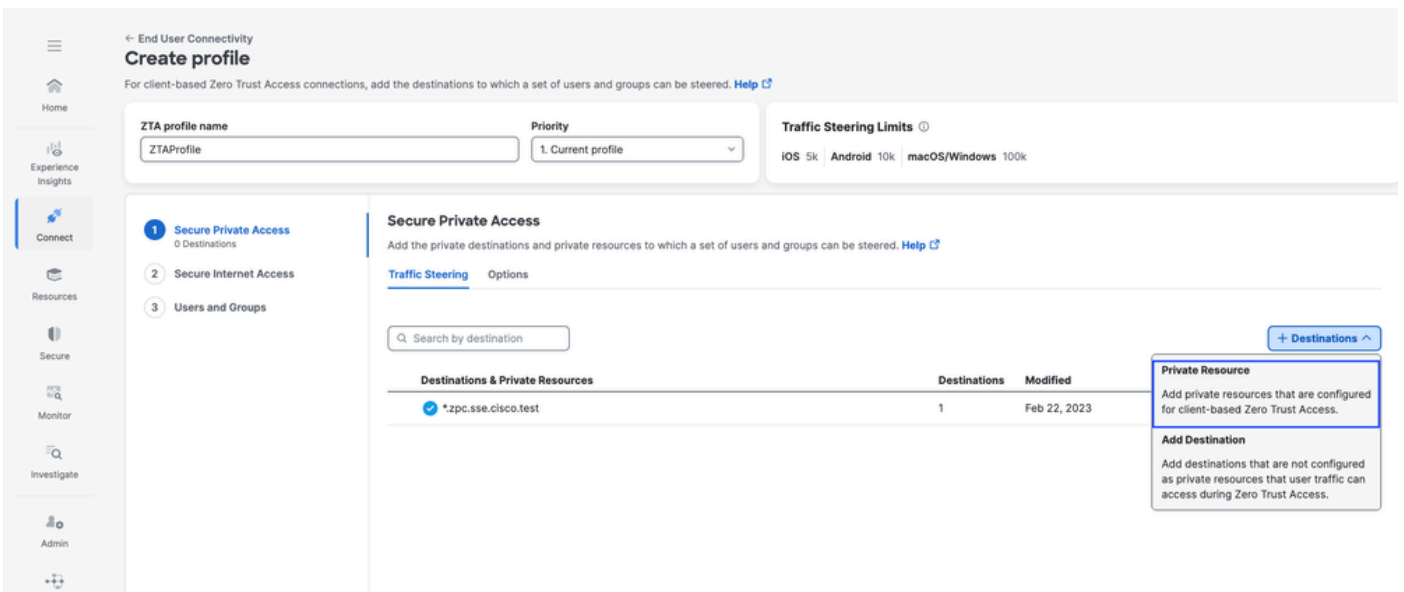
사용자 지정 ZTA 프로필을 사용 중인 경우 ZTA 프로필에 개별 개인 리소스를 추가해야 합니다

1. Connect(연결) > End User Connectivity(최종 사용자 연결) > Zero Trust Access(제로 트러스트 액세스)로 이동하고 +ZTA Profile(ZTA 프로파일)을 클릭합니다.

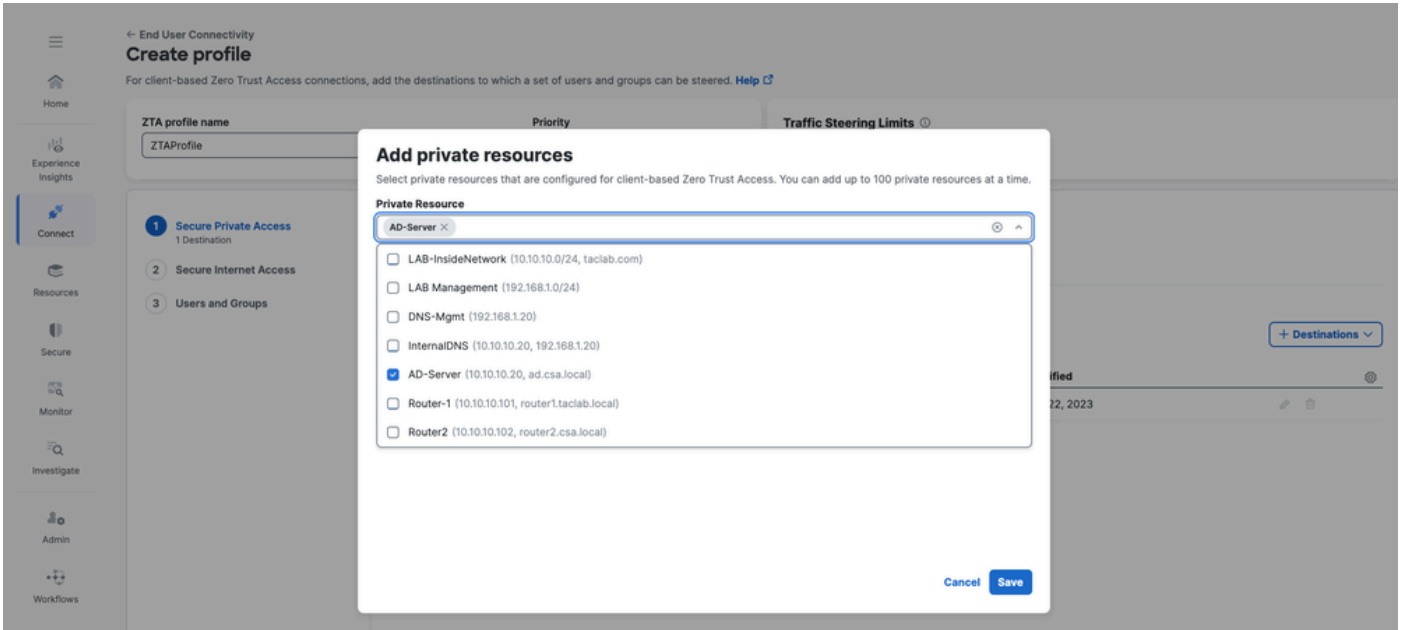


## 보안 액세스 - ZTA 프로필

### 2. 프라이빗 리소스 추가

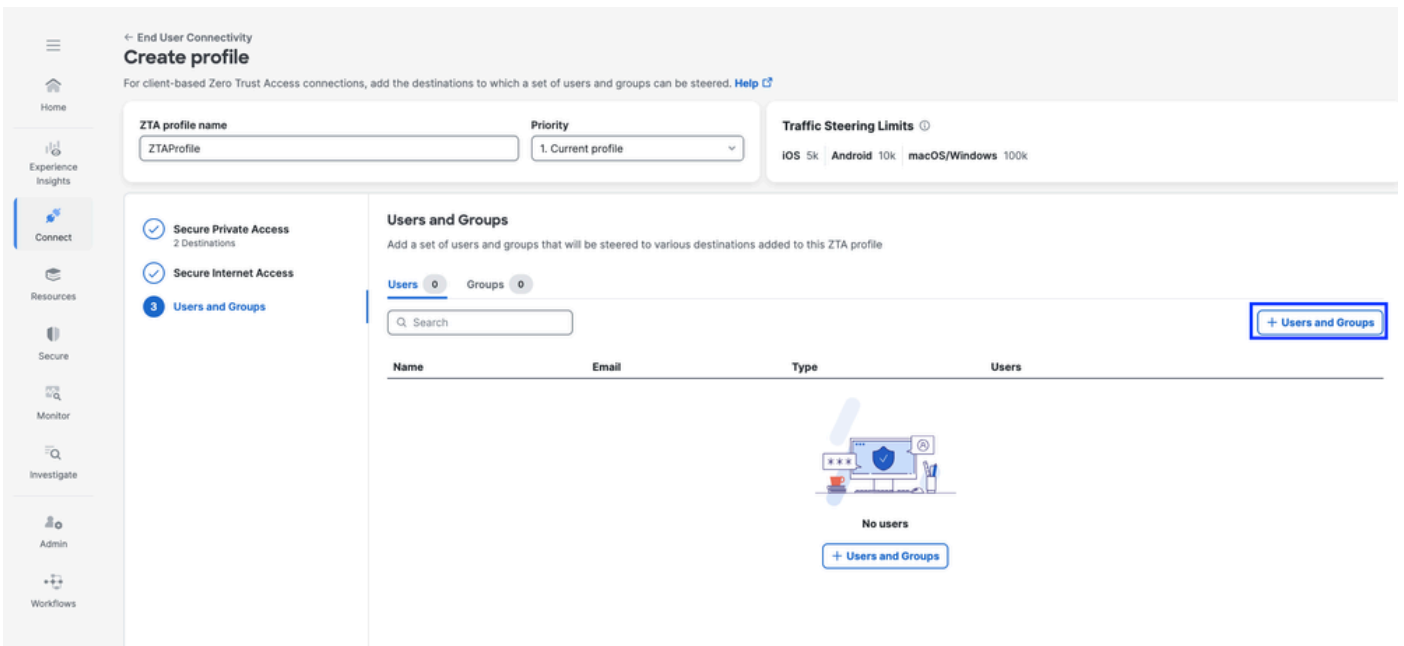


## 보안 액세스 - ZTA 프로필



## 보안 액세스 - ZTA 프로필

### 3. 사용자 및 그룹 추가



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

## 보안 액세스 - ZTA 프로파일

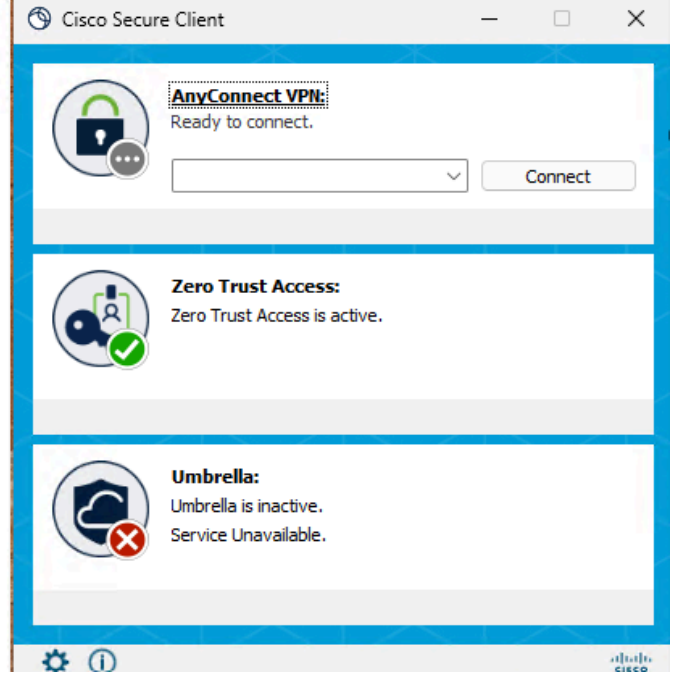
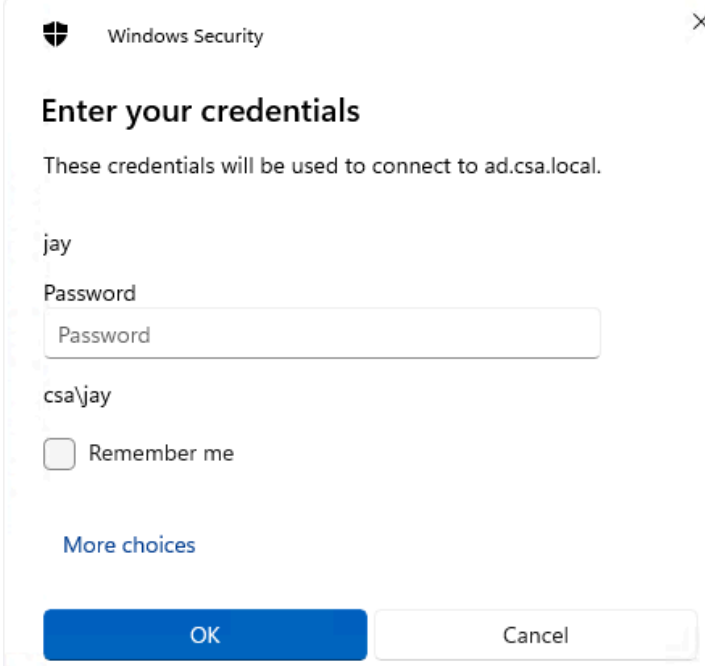
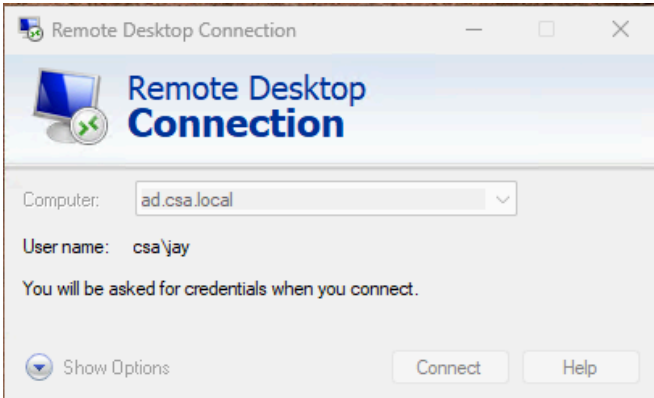


참고: 할당된 개인 리소스에 대해 컨피그레이션을 클라이언트에 푸시하고 동기화하는 데 최대 15-20분이 소요될 수 있습니다

### 단계 - 4 Private Resource에 대한 액세스 확인

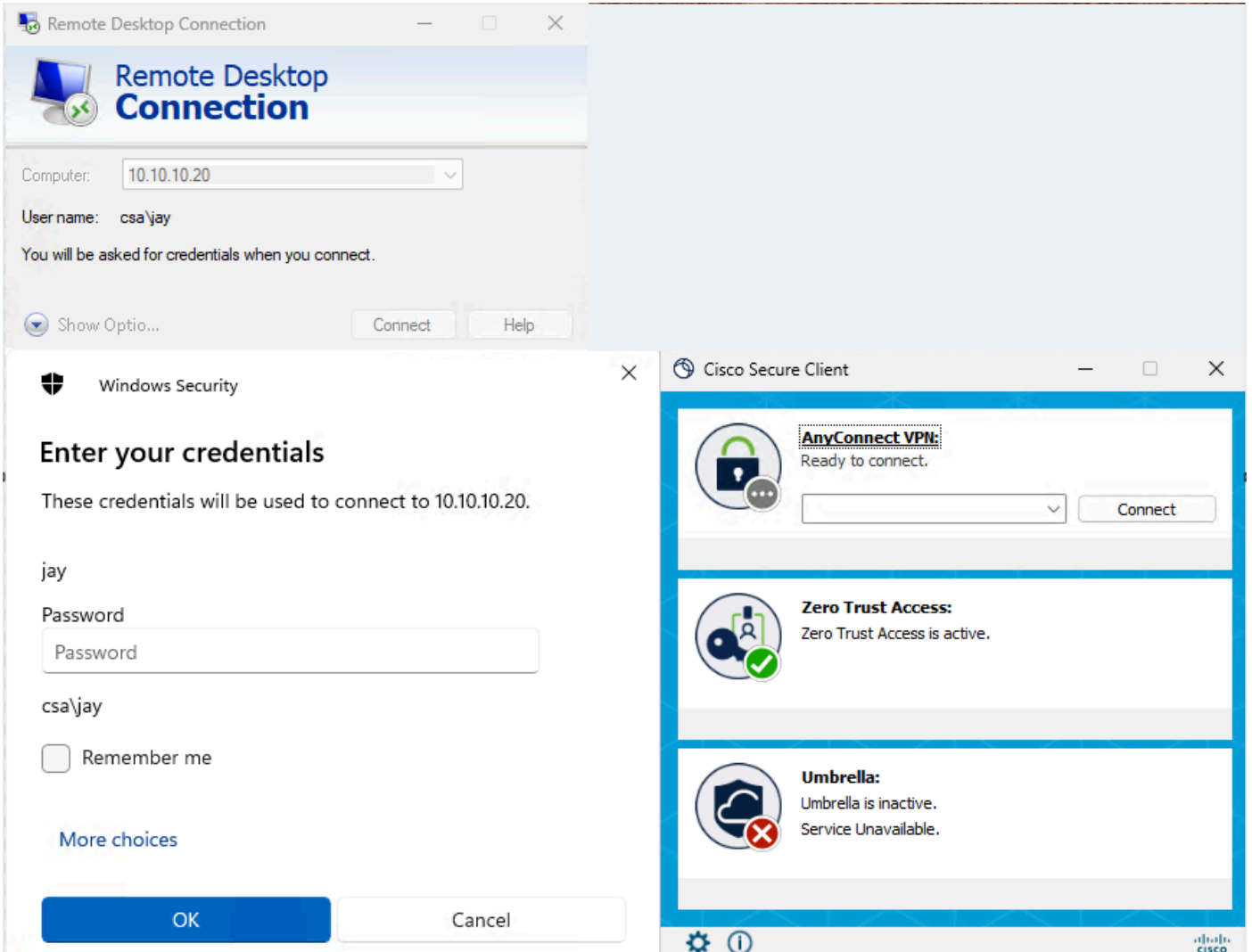
#### 1. 프라이빗 리소스 액세스

FQDN을 사용하여 PR 액세스



보안 액세스 - PR 테스트

IP 주소를 사용하여 PR에 액세스



보안 액세스 - PR 테스트

2. 활동 검색 이벤트로 확인합니다.

**Activity Search**

Filters: IP ADDRESS 10.10.10.20, RESPONSE Allowed

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

보안 액세스 - 활동 검색

# 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 PORT 3389 Restore to previous state Save Search

3 Total Viewing activity from Jan 11, 2026 4:53 AM to Jan 12, 2026 4:53 AM Page: 1 Results per page: 50 1 - 3 of 3

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

보안 액세스 - 활동 검색

**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 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	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

보안 액세스 - 활동 검색

### Activity Search

Schedule Export CSV LAST 24 HOURS

Search by domain, identity, or URL Advanced CLEAR

Filters: IP ADDRESS 10.10.10.20 X Saved Searches Customize Columns ZTA Client-based 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

#### 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

## 보안 액세스 - 활동 검색

### 3. FMC 연결 이벤트 확인

Events Troubleshooting

Destination Port / ICMP Code 3389

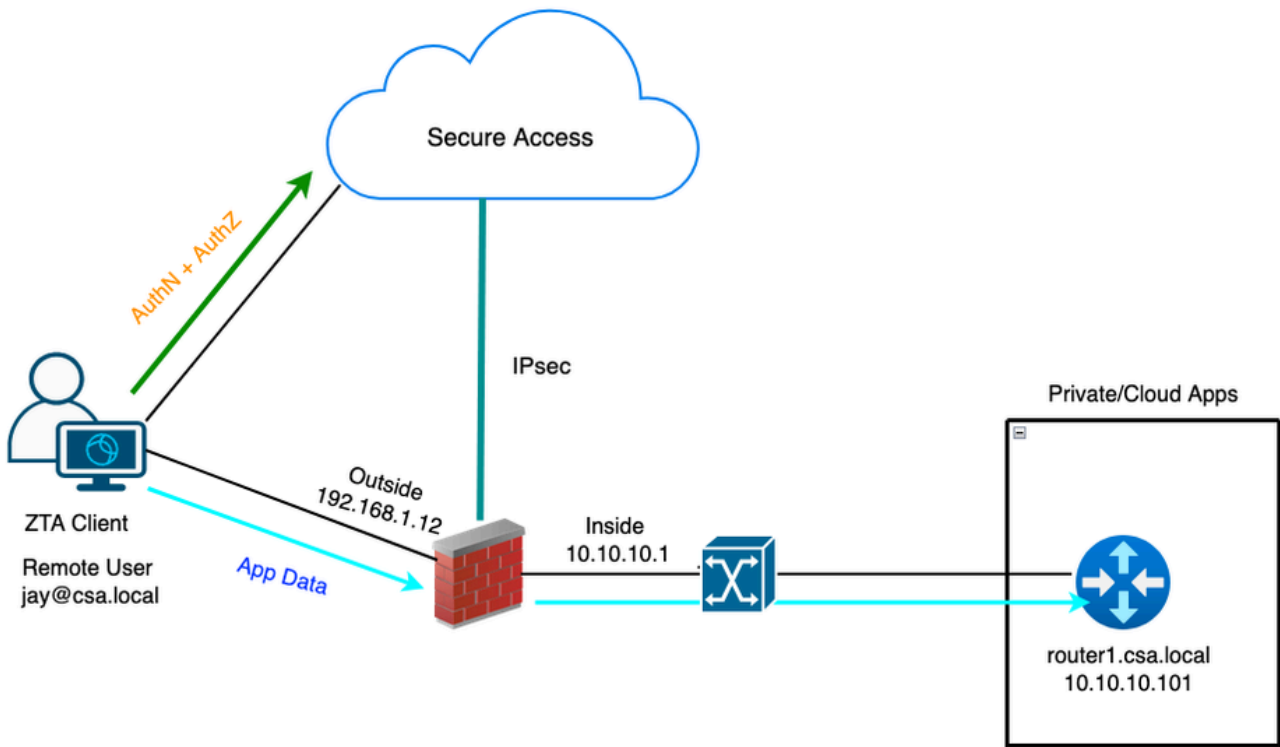
7 events Last 1 hour

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 연결 이벤트

### 테스트 사례 2 - 원격 사용자 - 로컬 시행

로컬 시행을 통해 프라이빗 리소스에 액세스, 이 유형의 시행 정책 평가는 보안 액세스에서 수행되지만 애플리케이션 데이터는 FTD에 로컬로 유지됩니다. 예를 들어 ZTA가 홈 네트워크에 연결된 클라이언트 또는 사용자를 등록하고 FTD 내부 인터페이스 뒤에 있는 전용 리소스에 액세스하려고 했습니다.



## 범용 ZTA - 테스트 사례 토폴로지

### 1단계 - Secure Access에서 프라이빗 리소스 정의

클라우드 시행으로 ZTA(Zero Trust Access) 등록된 디바이스를 통해 액세스할 수 있는 프라이빗 리소스 구성

1. Resources > Destinations > Private Resources > Click on +Add로 이동합니다.

The screenshot shows the Cisco Security Cloud Control interface. The 'Resources' section is expanded, showing 'Destinations' > 'Private Resource'. A table displays the configured Private Resources:

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

## 보안 액세스 - 프라이빗 리소스 컨피그레이션

2. 개인 자원명에는 유의미한 자원명을 입력합니다. 설명의 경우, 리소스의 용도 또는 리소스 소유자의 이름과 같은 정보를 제공하는 것이 좋습니다.

← 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

### 보안 액세스 - 프라이빗 리소스 컨피그레이션

3. 액세스하려는 개인 자원의 FQDN을 입력합니다. 프라이빗 리소스의 IP 주소도 정의할 수 있습니다. 자세한 내용은 프라이빗 [리소스 추가를 참조하십시오](#)

4. 도메인을 확인할 내부 DNS 서버를 선택합니다

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)

### 보안 액세스 - 프라이빗 리소스 컨피그레이션

5. 엔드포인트 연결 방법 선택

6. FTD를 로컬 적용 지점으로 선택합니다

## 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

## 보안 액세스 - 프라이빗 리소스 컨피그레이션



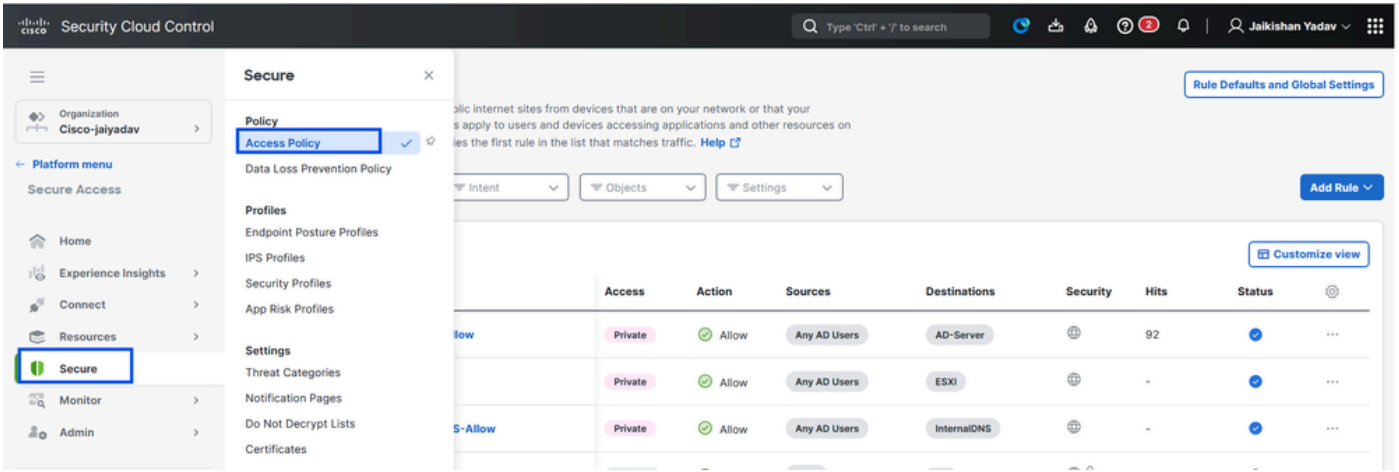
참고: 선택하는 등록 유형에 따라 이 변경 사항은 PR을 FTD에 자동으로 연결하고 정책 구축을 트리거합니다

7. Save(저장)를 클릭합니다.

2단계 - 개인 액세스 규칙 생성

Universal ZTA 등록된 사용자가 액세스할 수 있도록 Secure Access의 비공개 액세스를 구성합니다. 자세한 내용은 [개인 액세스 규칙을 참조하십시오](#)

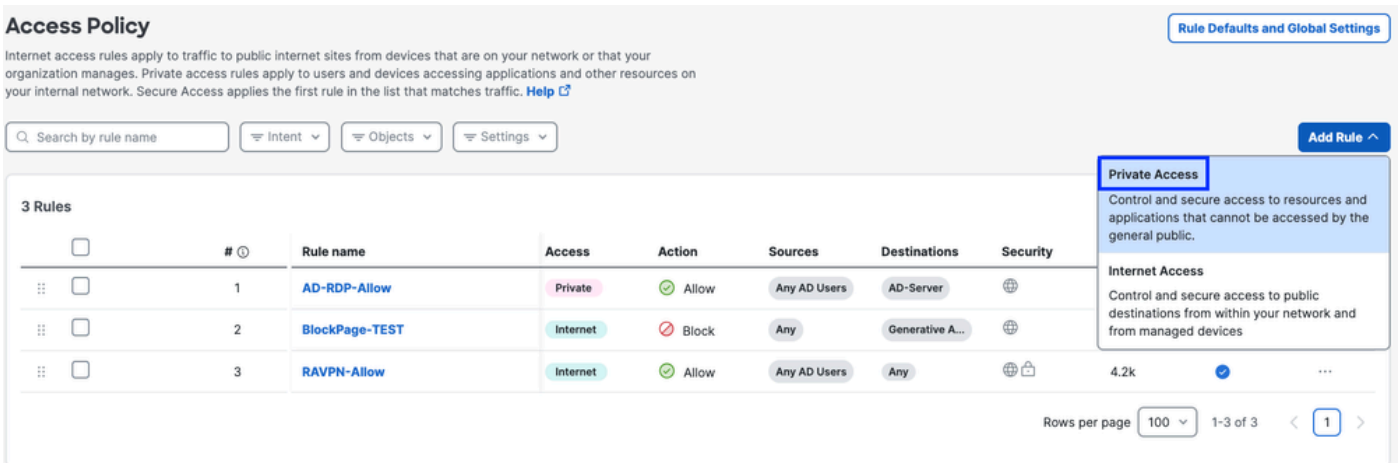
1. Secure(보안) > Access Policy(액세스 정책)로 이동합니다



## 보안 액세스 - 프라이빗 리소스 컨피그레이션

2. 규칙 추가를 클릭한 다음 개인 액세스를 선택합니다.

규칙의 맨 위에는 규칙의 구성된 구성 요소를 설명하는 요약이 있습니다.



## 보안 액세스 - 액세스 정책 컨피그레이션

3. 규칙 이름 추가

## 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



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.

## 보안 액세스 - 액세스 정책 컨피그레이션

### 4. 규칙 조치를 선택하고 출처 및 대상을 선택합니다

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

#### To

Specify one or more destinations.

Private Resources - Router1

+ AND

## 보안 액세스 - 액세스 정책 컨피그레이션

### 5. 엔드포인트 요구 사항 구성

### 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](#)

보안 액세스 - 액세스 정책 컨피그레이션

## 6. 보안 구성

**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](#)

보안 액세스 - 액세스 정책 컨피그레이션

7. 저장을 클릭합니다.

## 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

#	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 >

## 보안 액세스 - 액세스 정책 컨피그레이션

### 3단계 - FTD에서 PR 연결 확인

#### 1. 연결 > 네트워크 연결 > FTDs로 이동합니다

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar has a 'Connect' menu item highlighted. The main content area shows a 'Connect' panel with a 'Network Connections' section. Under 'Network Connections', there are two items: '0 Warning' and '1 Connected'. The '1 Connected' item is highlighted, and a 'FTDs' link is visible in the top right of the panel. The interface also shows a search bar at the top and a user profile 'Jaikishan Yadav'.

## 보안 액세스 - PR 확인

#### 2. FTD(FTD) > 이 FTD와 연관된 리소스 보기를 클릭합니다.

## 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
<b>FMC_FTD</b> Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	<span>Synced</span>	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
<b>LAN</b> (Default trusted network)	1 DNS Servers

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

### Associated Resources

#### RESOURCES ASSOCIATED BY STATUS

Status
<span>Synced</span> 1

[View resources associated to this FTD](#)

[Associate Resources](#)

보안 액세스 - PR 확인

## 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](#)

보안 액세스 - PR 확인

3. Close(닫기)를 클릭합니다

4. 상태, 관련 리소스 및 구성이 동기화 상태인지 확인합니다.

The screenshot displays the Palo Alto Networks management console. On the left, the 'Network Connections' page shows a table of FTDs configured for Universal Zero Trust Access. The table has columns for FTD Name, Version, FMC, UZTA Configuration status, and Associated Resources. One entry, 'FMC\_FTD', is shown with a 'Synced' status, which is highlighted with a blue box. On the right, a detailed view for 'FMC\_FTD' is open, showing '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 Synced resource).

보안 액세스 - PR 확인

5. 구성이 FTD로 푸시되었는지 확인합니다.

FTD cli에 로그인하고 LINA 모드로 이동합니다.

# show running-config object application

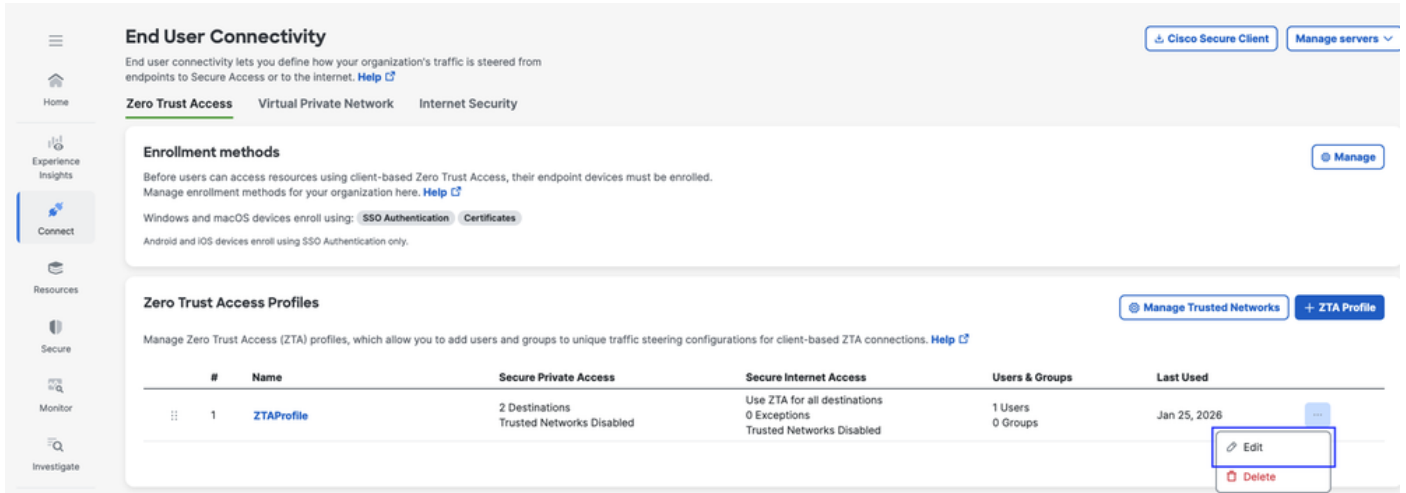
```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

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 확인

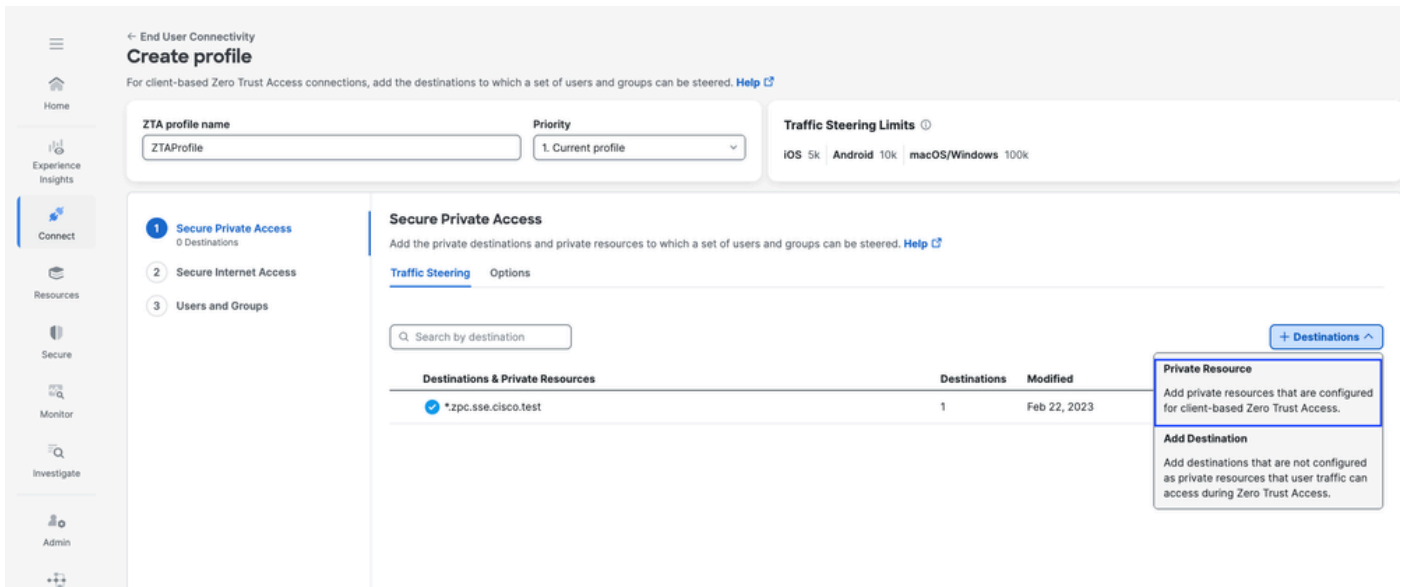
## 단계 - 4 ZTA 프로필에 프라이빗 리소스 추가

1. Connect(연결) > End User Connectivity(최종 사용자 연결) > Zero Trust Access(Zero Trust 액세스)로 이동하고 3개의 점을 클릭하여 ZTA 프로파일을 편집합니다

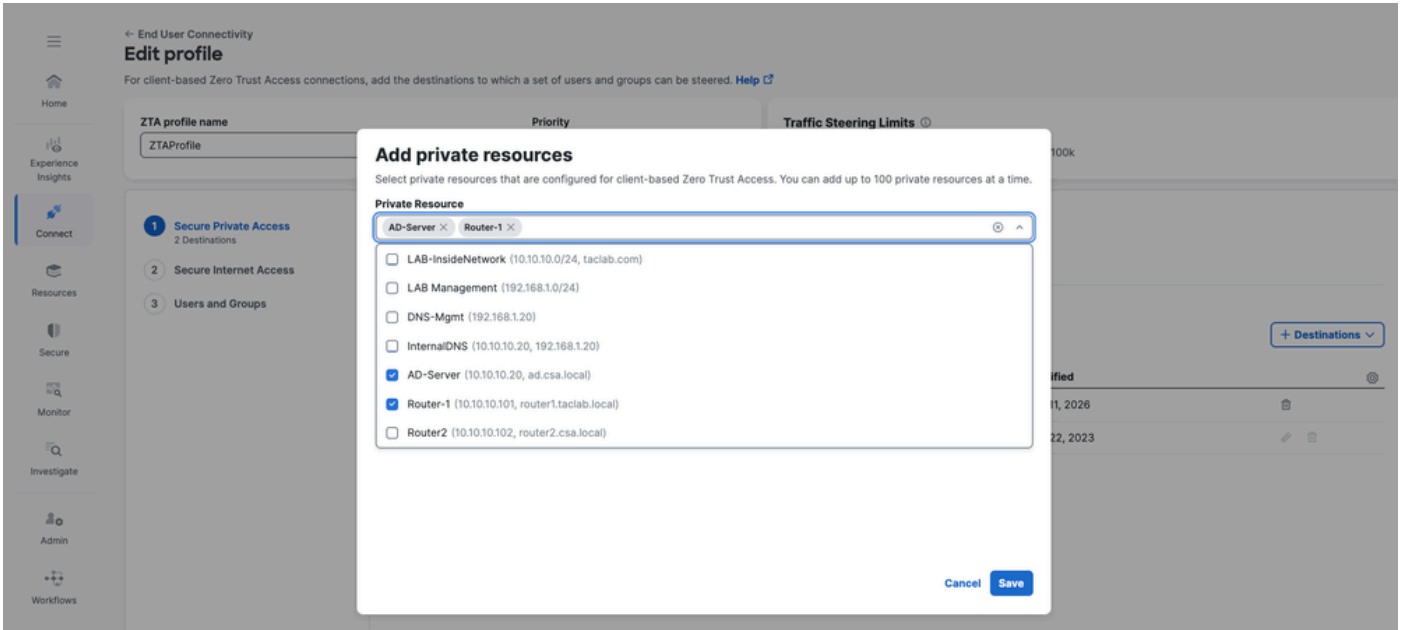


## 보안 액세스 - ZTA 프로필

## 2. 프라이빗 리소스 추가

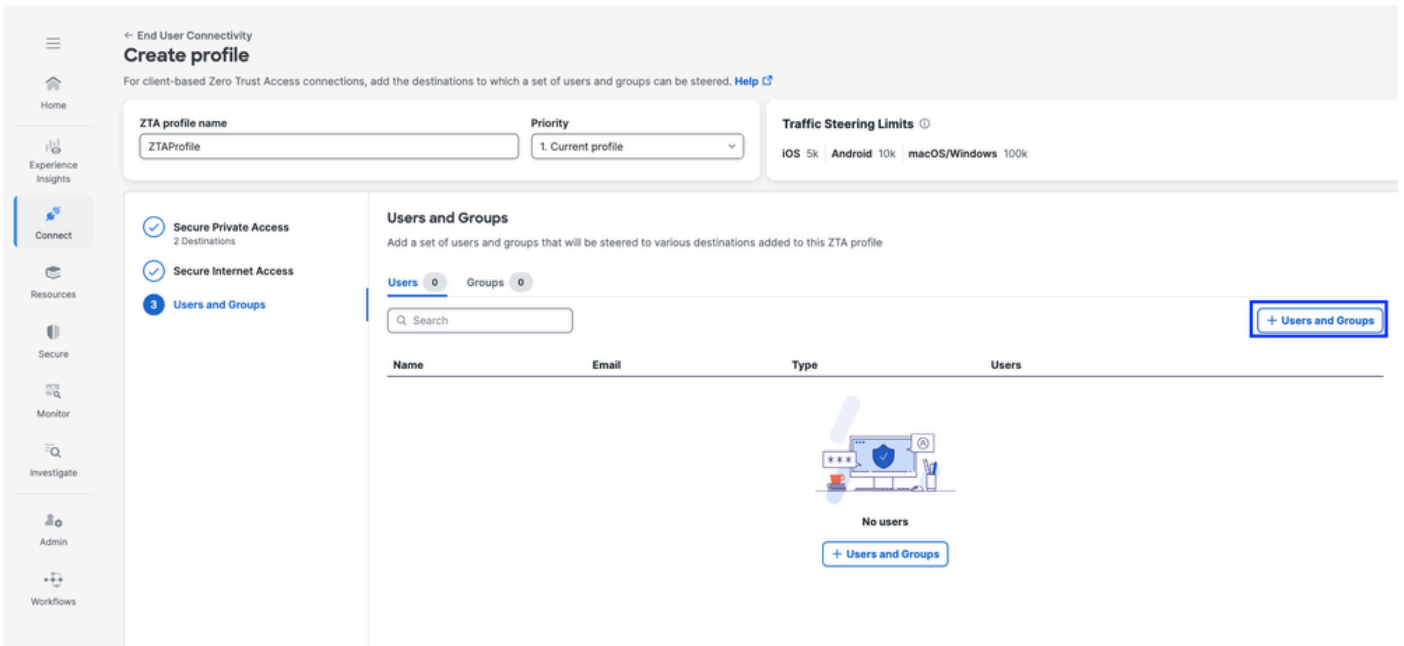


## 보안 액세스 - ZTA 프로필



## 보안 액세스 - ZTA 프로필

### 3. 사용자 및 그룹 추가



## 보안 액세스 - ZTA 프로필

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

## 보안 액세스 - ZTA 프로필

### 단계 - 5 Private Resource에 대한 액세스 확인

#### 1. 원격 사용자가 FTD FQDN을 확인할 수 있는지 확인

```
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
```

보안 액세스 - PR 테스트

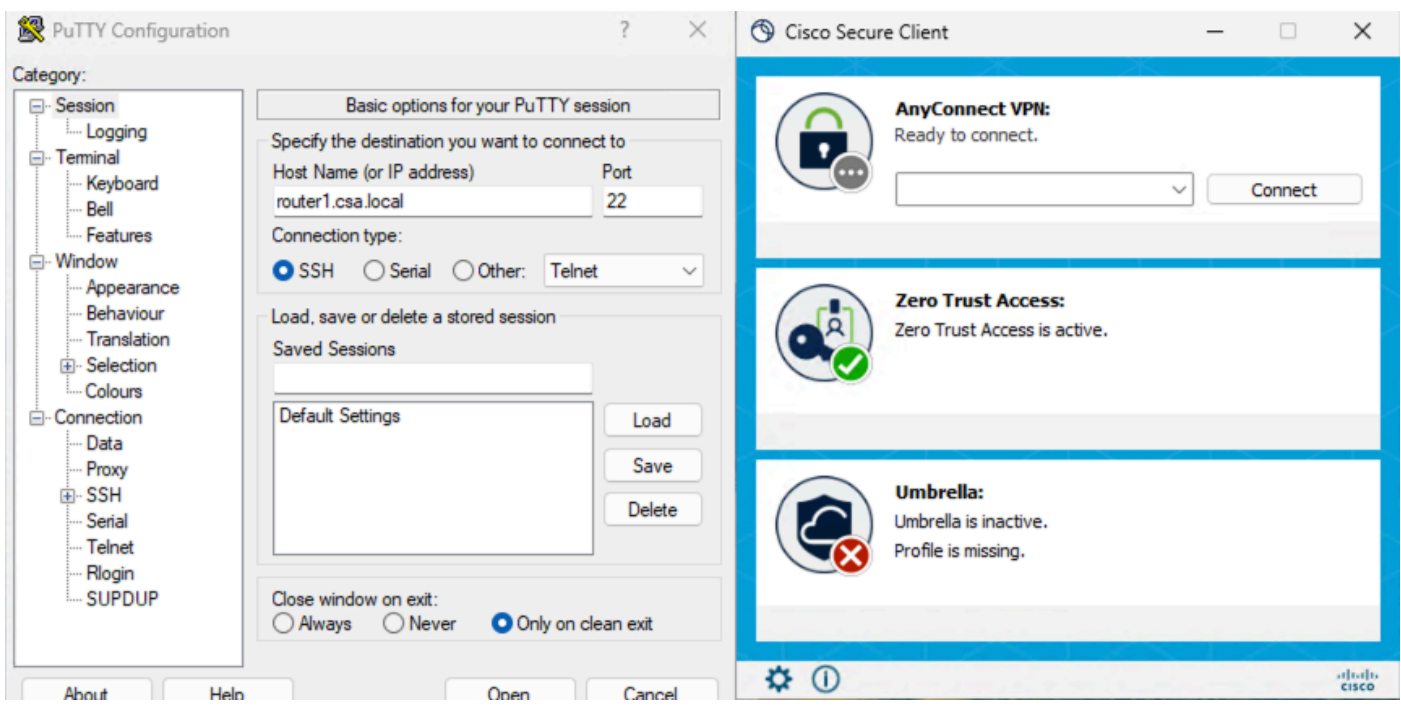
2. FQDN을 사용하여 FTD가 전용 리소스에 연결할 수 있는지 확인합니다.

```
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#
```

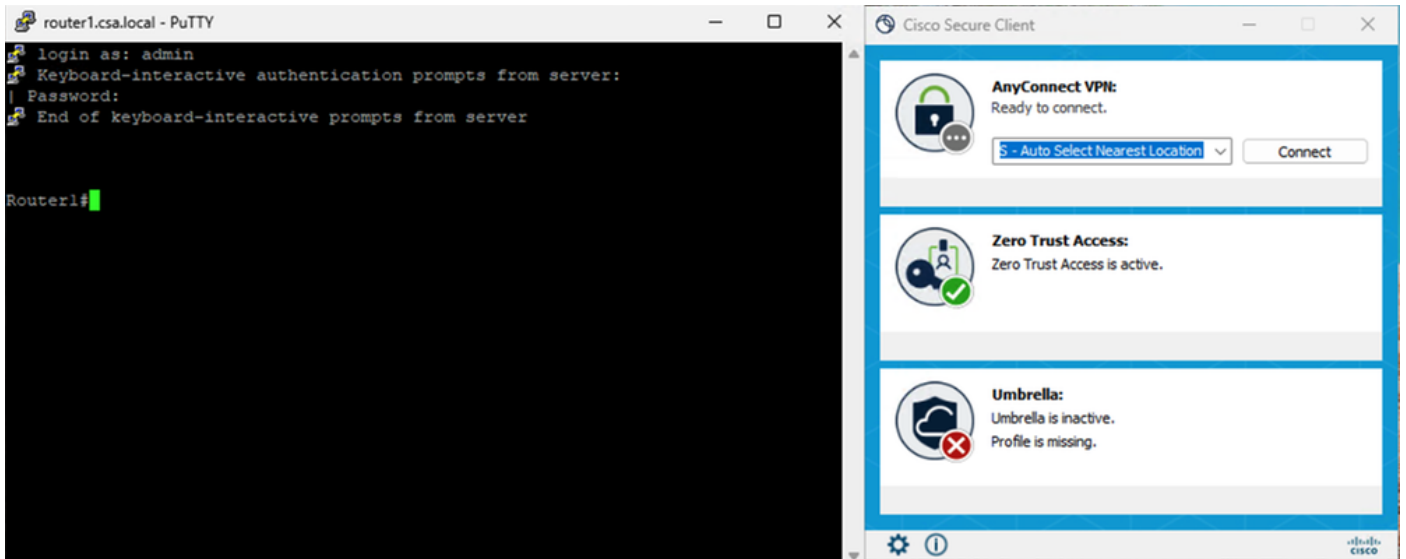
보안 액세스 - PR 테스트

3. 프라이빗 리소스에 대한 SSH 연결 테스트

FQDN을 사용하여 PR 액세스

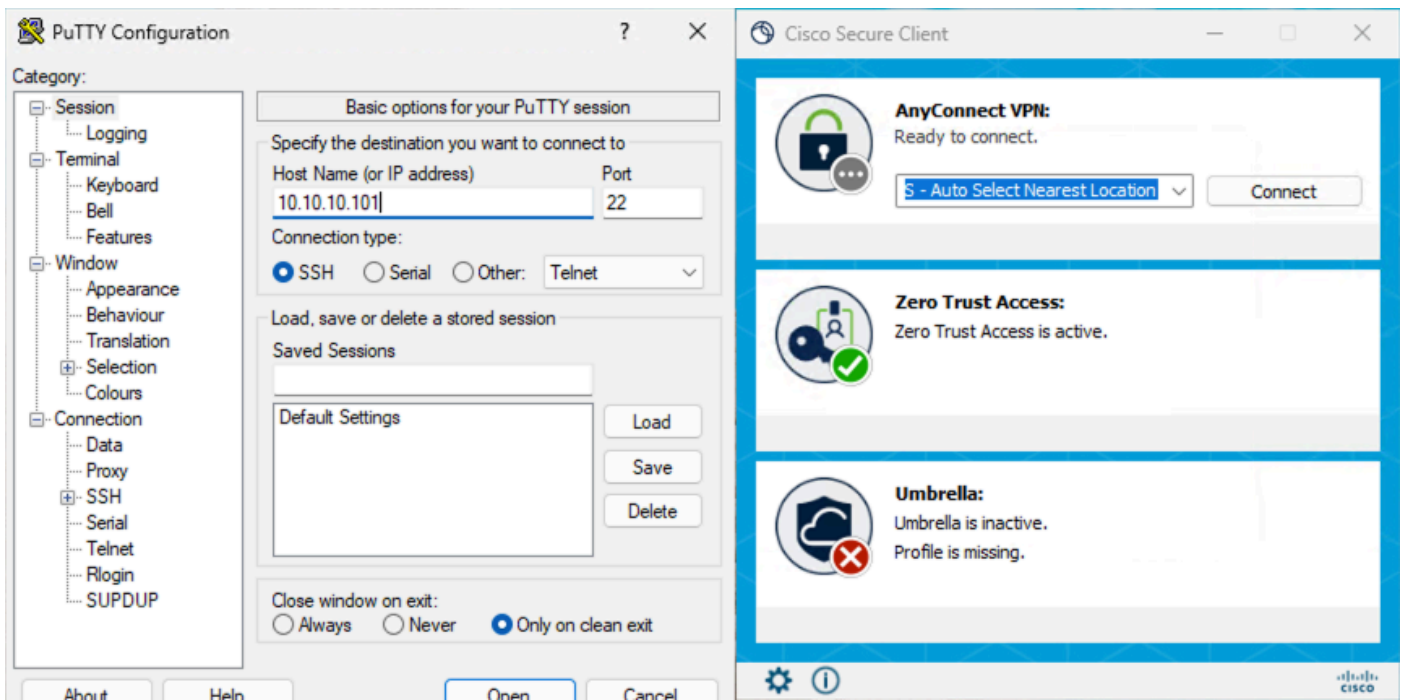


보안 액세스 - PR 테스트

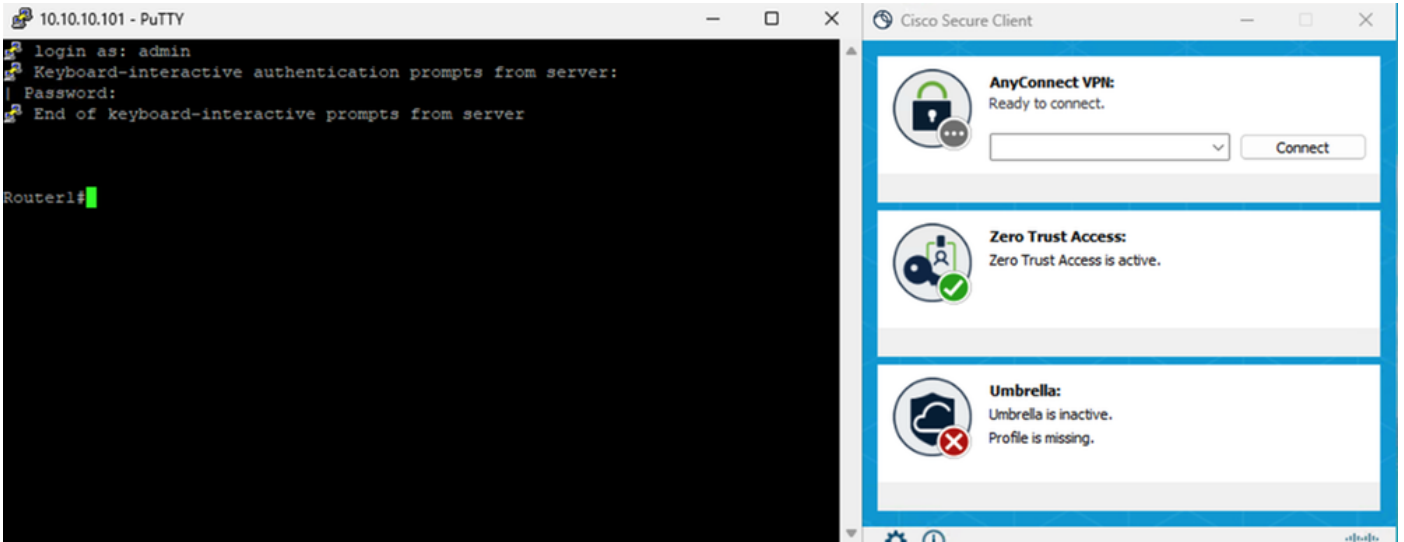


보안 액세스 - PR 테스트

IP 주소를 사용하여 PR에 액세스



보안 액세스 - PR 테스트



## 보안 액세스 - PR 테스트

### 4. 보안 액세스 활동 검색 로그 확인

Activity Search

Filters: Search by domain, identity, or URL. Domain: router1.csa.local, Response: Allowed. 4 Total results.

Response	Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Browser	Location
Allowed	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
Allowed	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
Allowed	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
Allowed	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

## 보안 액세스 - 활동 검색

4 Total results. 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)

WinT: WinT

Rule Name: Router1-SSH

Resource/Application: Router1

Zero Trust Access Profile: Default ZTA Profile

Trusted Network: No Match

Enforcement Point: FTD > FMC\_FTD

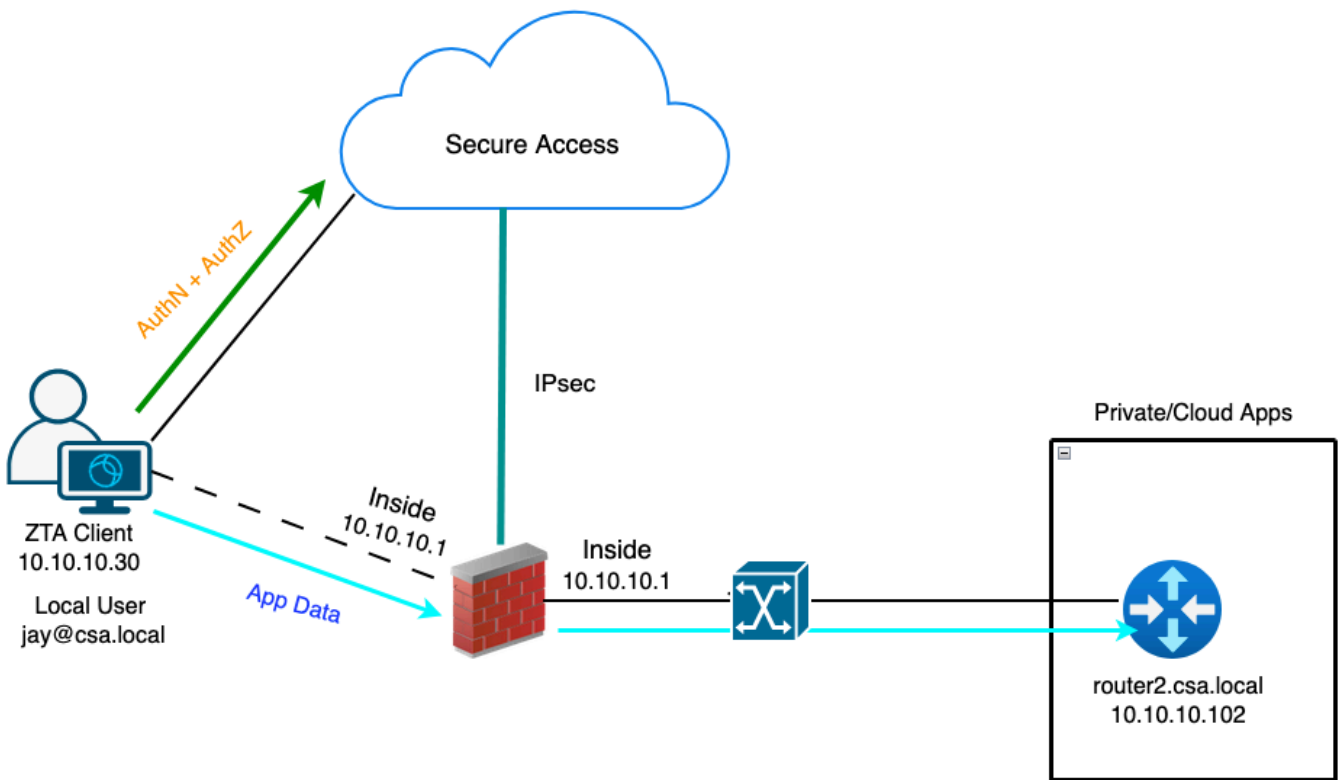
Destination: router1.csa.local

Destination IP: -



### 테스트 사례 3 - 로컬 사용자 - 로컬 시행

로컬 사용자로서 로컬 시행을 통해 프라이빗 리소스에 액세스하는 이 유형의 시행 정책 평가는 보안 액세스에서 수행되지만 애플리케이션 데이터는 FTD에 로컬로 유지됩니다. 예를 들어 ZTA가 홈 네트워크에 연결된 클라이언트 또는 사용자를 등록하고 FTD 내부 인터페이스 뒤에 있는 전용 리소스에 액세스하려고 했습니다. 프라이빗 리소스가 DMZ 또는 FTD의 다른 인터페이스 뒤에 있는 경우 클라이언트 IP 또는 네트워크와 프라이빗 리소스 간의 트래픽을 허용하기 위해 FTD에 대한 액세스 규칙을 생성해야 합니다.

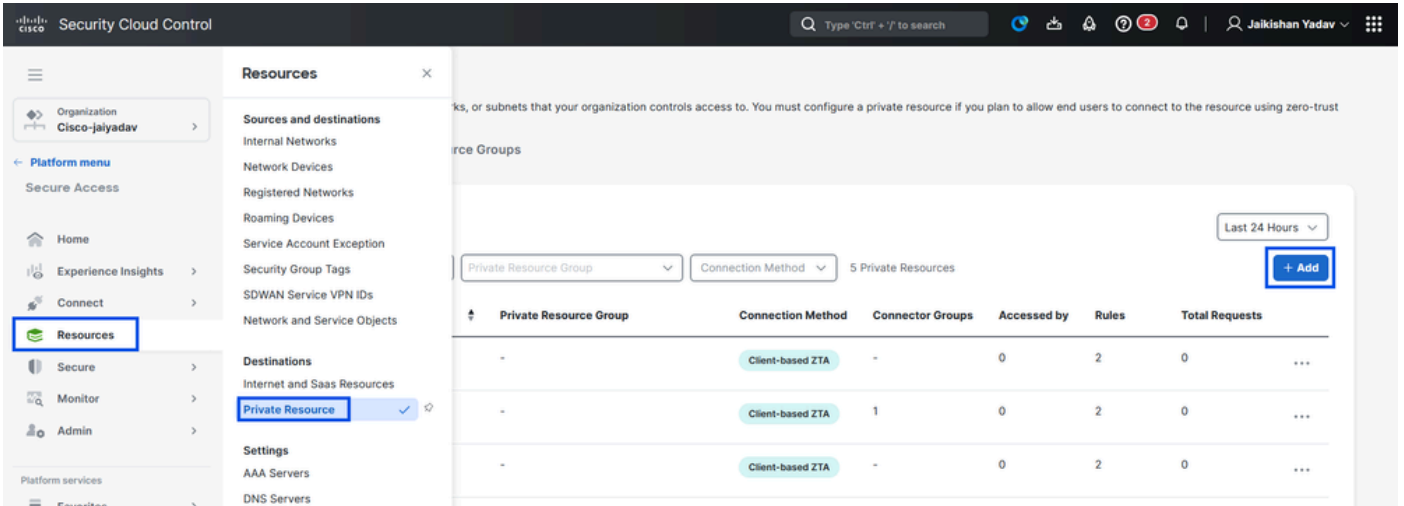


### 범용 ZTA - 테스트 사례 토폴로지

#### 1단계 - Secure Access에서 프라이빗 리소스 정의

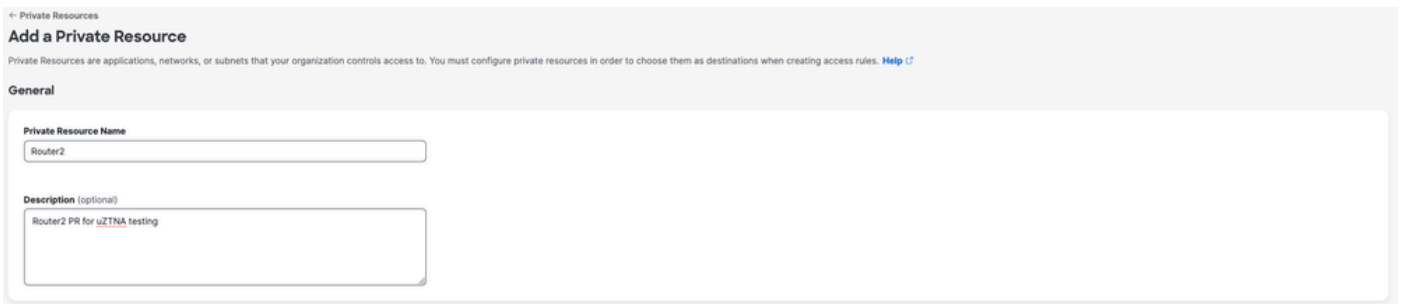
클라우드 시행으로 ZTA(Zero Trust Access) 등록된 디바이스를 통해 액세스할 수 있는 프라이빗 리소스 구성

1. Resources > Destinations > Private Resources > Click on +Add로 이동합니다.



## 보안 액세스 - 프라이빗 리소스 컨피그레이션

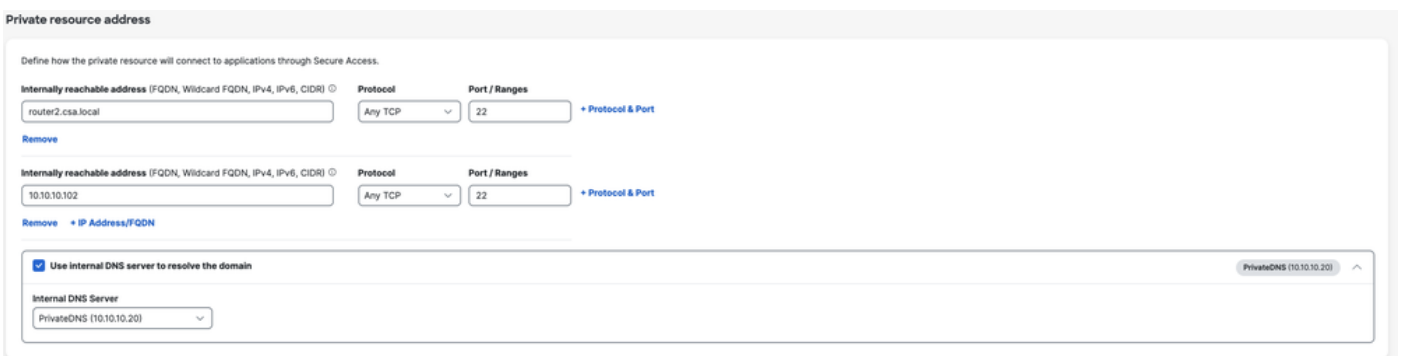
2. 개인 자원명에는 유의미한 자원명을 입력합니다. 설명의 경우, 리소스의 용도 또는 리소스 소유자의 이름과 같은 정보를 제공하는 것이 좋습니다.



## 보안 액세스 - 프라이빗 리소스 컨피그레이션

3. 액세스하려는 개인 자원의 FQDN을 입력합니다. 프라이빗 리소스의 IP 주소도 정의할 수 있습니다. 자세한 내용은 프라이빗 [리소스 추가를 참조하십시오](#)

4. 도메인을 확인할 내부 DNS 서버를 선택합니다



5. 엔드포인트 연결 방법 선택

6. FTD를 로컬 적용 지점으로 선택합니다

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**

Remote user via internet Local Firewall Private Resource

**Enforcement point for Local user**

User in a trusted network via local network Local Firewall Private Resource

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



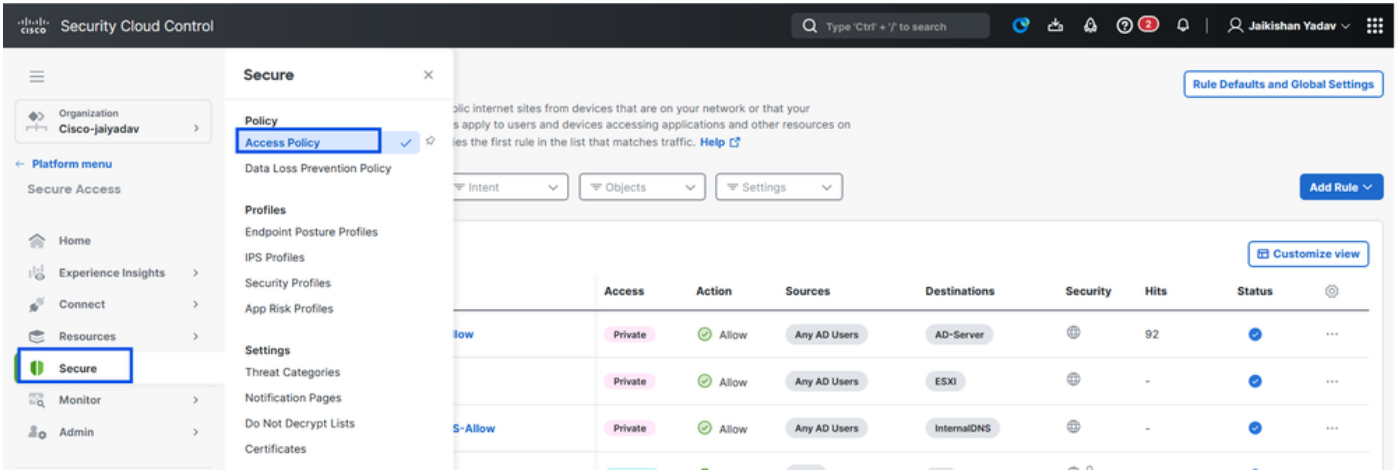
참고: 선택하는 등록 유형에 따라 이 변경 사항은 PR을 FTD에 자동으로 연결하고 정책 구축을 트리거합니다

7. Save(저장)를 클릭합니다.

2단계 - 개인 액세스 규칙 생성

Universal ZTA 등록된 사용자가 액세스할 수 있도록 Secure Access의 비공개 액세스를 구성합니다 . 자세한 내용은 [개인 액세스 규칙을 참조하십시오](#)

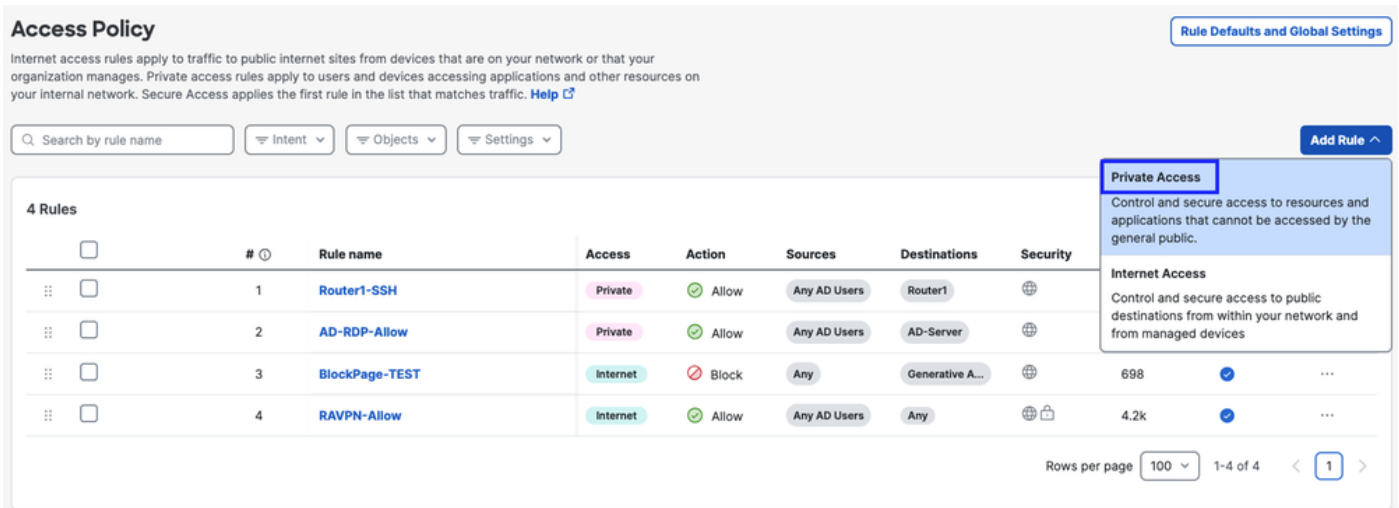
1. Secure(보안) > Access Policy(액세스 정책)로 이동합니다



## 보안 액세스 - 액세스 정책 컨피그레이션

2. 규칙 추가를 클릭한 다음 개인 액세스를 선택합니다.

규칙의 맨 위에는 규칙의 구성된 구성 요소를 설명하는 요약이 있습니다.



## 보안 액세스 - 액세스 정책 컨피그레이션

3. 규칙 이름 추가

## 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.

## 보안 액세스 - 액세스 정책 컨피그레이션

### 4. 규칙 조치를 선택하고 출처 및 대상을 선택합니다

Rule name <sup>ⓘ</sup>  Rule order

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

**Action**

**Allow**  
Allow specified traffic if security requirements are met.

**Block**  
Block specified traffic.

**From**  
Specify one or more sources

**To**  
Specify one or more destinations

+ AND

## 보안 액세스 - 액세스 정책 컨피그레이션

### 5. 엔드포인트 요구 사항 구성

### 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](#)

## 보안 액세스 - 액세스 정책 컨피그레이션

### 6. 보안 구성

#### 1 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](#)

## 보안 액세스 - 액세스 정책 컨피그레이션

### 7. 저장을 클릭합니다.

## 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 >

보안 액세스 - 액세스 정책 컨피그레이션

3단계 - FTD에서 PR 연결 확인

1. connect(연결) > Network Connections(네트워크 연결) > FTDs(FTD)로 이동합니다

The screenshot shows the Cisco Security Cloud Control interface. The 'Connect' menu is open, showing 'Network Connections' as the selected option. The main content area displays 'Network Connections' with a 'FTDs' tab selected. A summary card shows '0 Warning' and '1 Connected'. Below this, there are filters for 'Region' and 'Status', and a '+ Add' button.

보안 액세스 - PR 확인

2. FTD(FTD) > View resources associated to this FTD(이 FTD와 연결된 리소스 보기)를 클릭합니다.

## 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
<b>FMC_FTD</b> 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 (Default trusted network)	1 DNS Servers

Edit assignment + Trusted network

### Associated Resources

#### RESOURCES ASSOCIATED BY STATUS

Status
Synced 2

View resources associated to this FTD

Associate Resources

보안 액세스 - PR 확인

## 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
<b>Router1</b>	Synced
<b>Router2</b>	Synced

Close

3. Close(닫기)를 클릭합니다

4. 상태, 관련 리소스 및 구성이 동기화 상태인지 확인합니다.

The screenshot displays the 'Network Connections' page in the Palo Alto Networks management console. The 'FTDs' tab is selected, showing a table of configured FTDs. The 'FMC\_FTD' entry is highlighted, with its 'UZTA Configuration status' set to 'Synced'. A right-hand sidebar provides detailed information for 'FMC\_FTD', 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).

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

5. 구성이 FTD로 푸시되었는지 확인합니다.

FTD cli에 로그인하고 LINA 모드로 이동합니다.

# show running-config object application

```

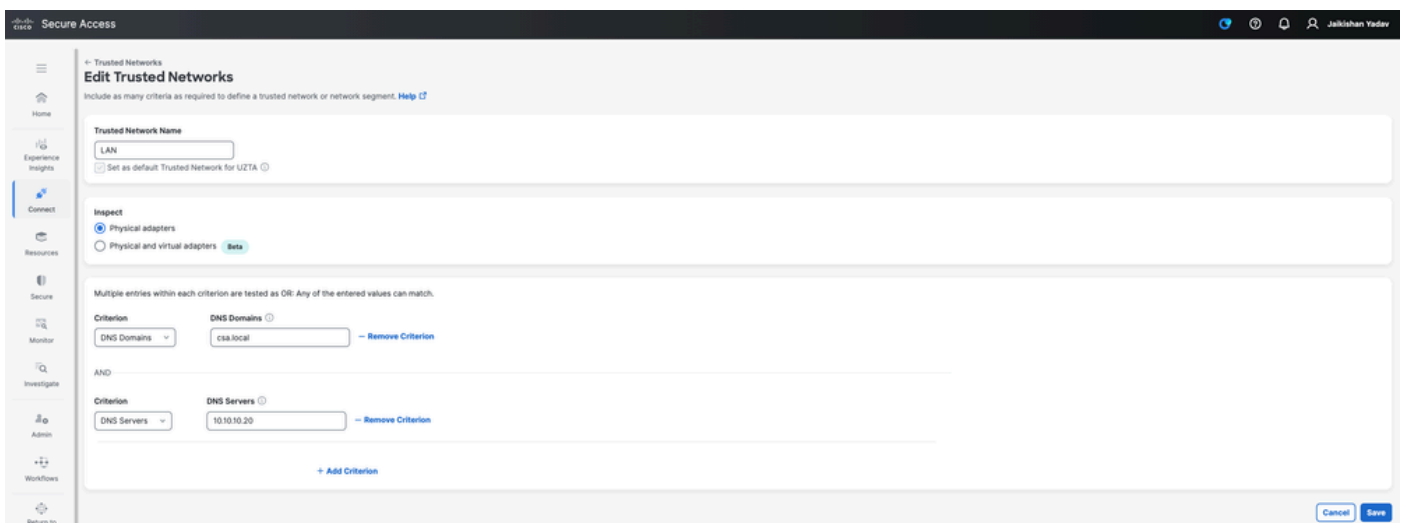
ftd# sh run ob application
object application PR_Router1
  id 427221
  internal domain router1.csa.local tcp eq 22
  internal subnet 10.10.10.101 255.255.255.255 tcp eq 22
  external domain router1.csa.local
  external subnet 10.10.10.101 255.255.255.255
object application PR_Router2
  id 434482
  internal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

```

보안 액세스 - PR 확인

4단계 " 신뢰할 수 있는 네트워크 또는 ZTA 설정 관리" 구성

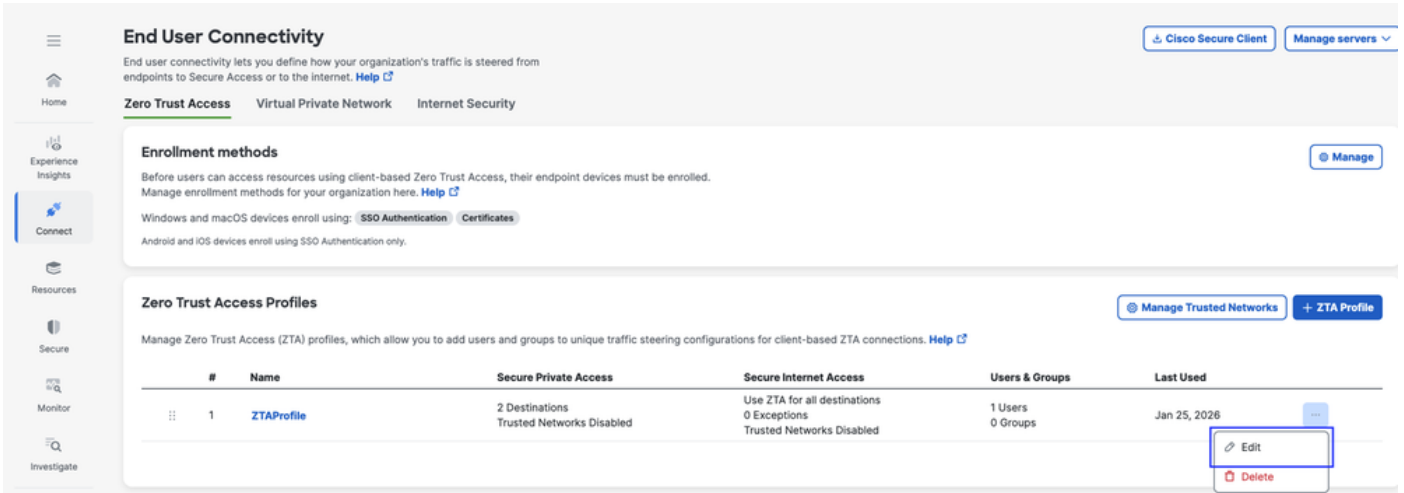
Connect(연결) > End User Connectivity(최종 사용자 연결) > Zero Trust Access(제로 트러스트 액세스) > ZTA Settings(ZTA 설정)로 이동하고 신뢰할 수 있는 네트워크를 구성합니다



보안 액세스 - TND 컨피그레이션

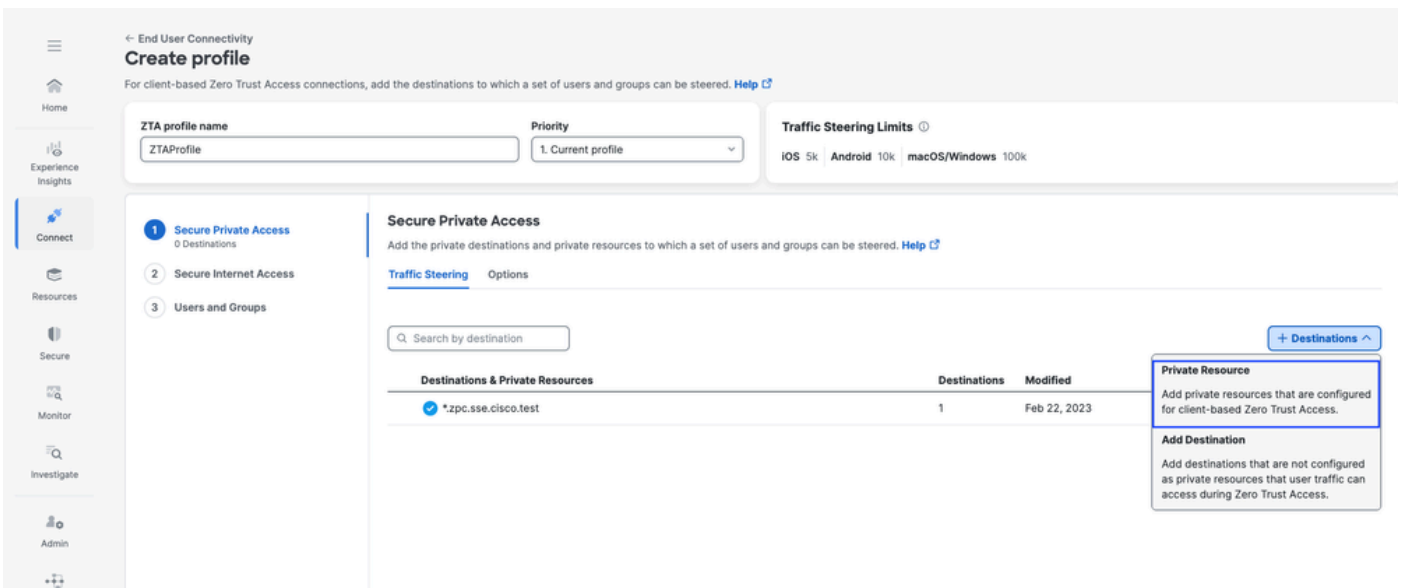
-5단계 ZTA 프로필에 프라이빗 리소스 추가

1. Connect(연결) > End User Connectivity(최종 사용자 연결) > Zero Trust Access(Zero Trust 액세스)로 이동하고 3개의 점을 클릭하여 ZTA 프로파일을 편집합니다

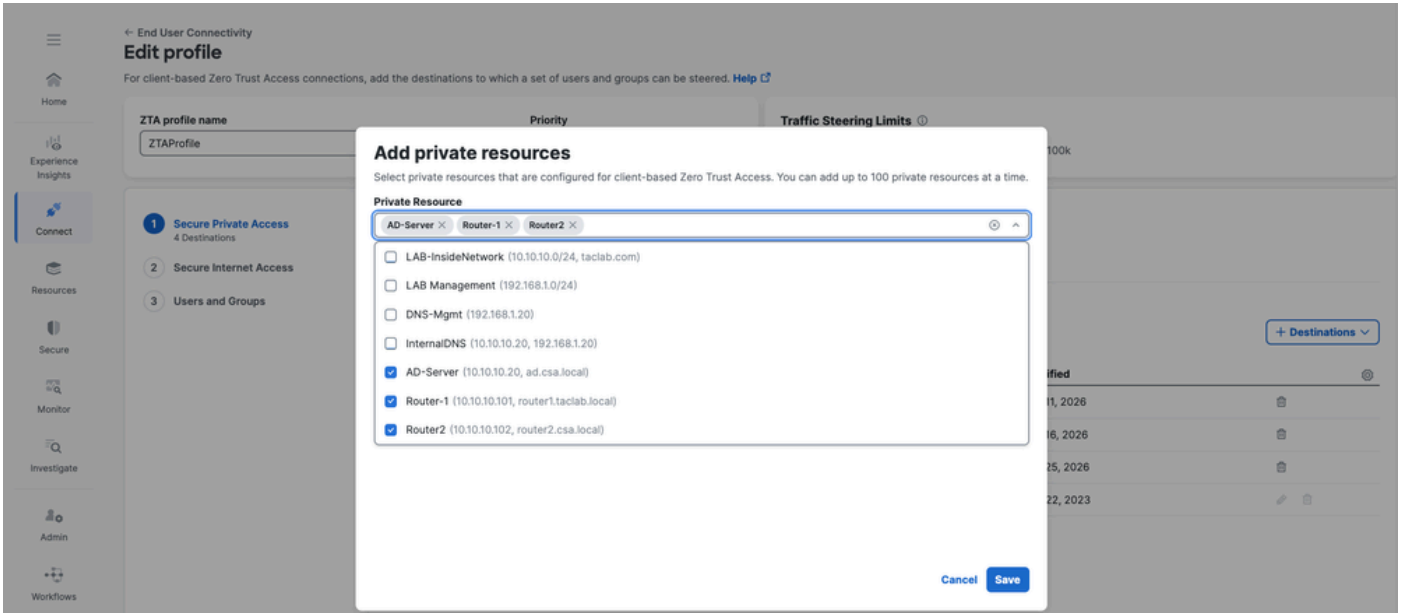


## 보안 액세스 - ZTA 프로필

### 2. 프라이빗 리소스 추가

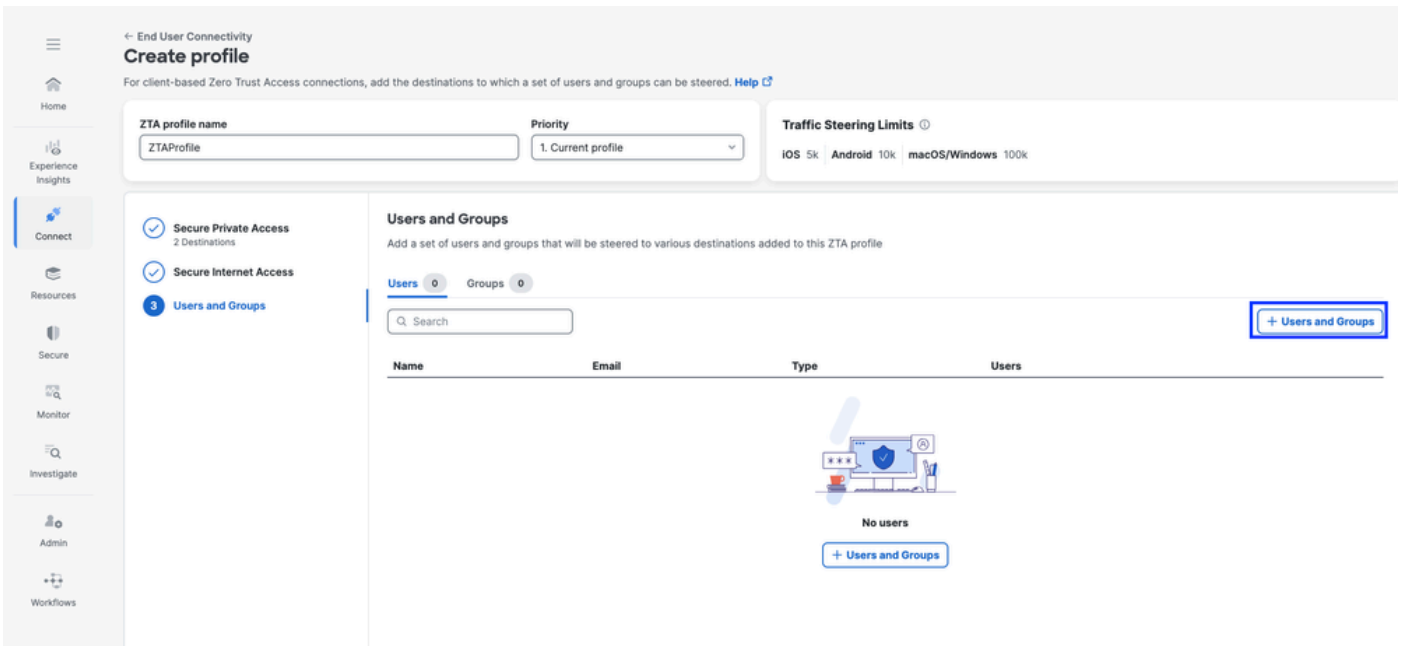


## 보안 액세스 - ZTA 프로필



## 보안 액세스 - ZTA 프로파일

### 3. 사용자 및 그룹 추가



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	-

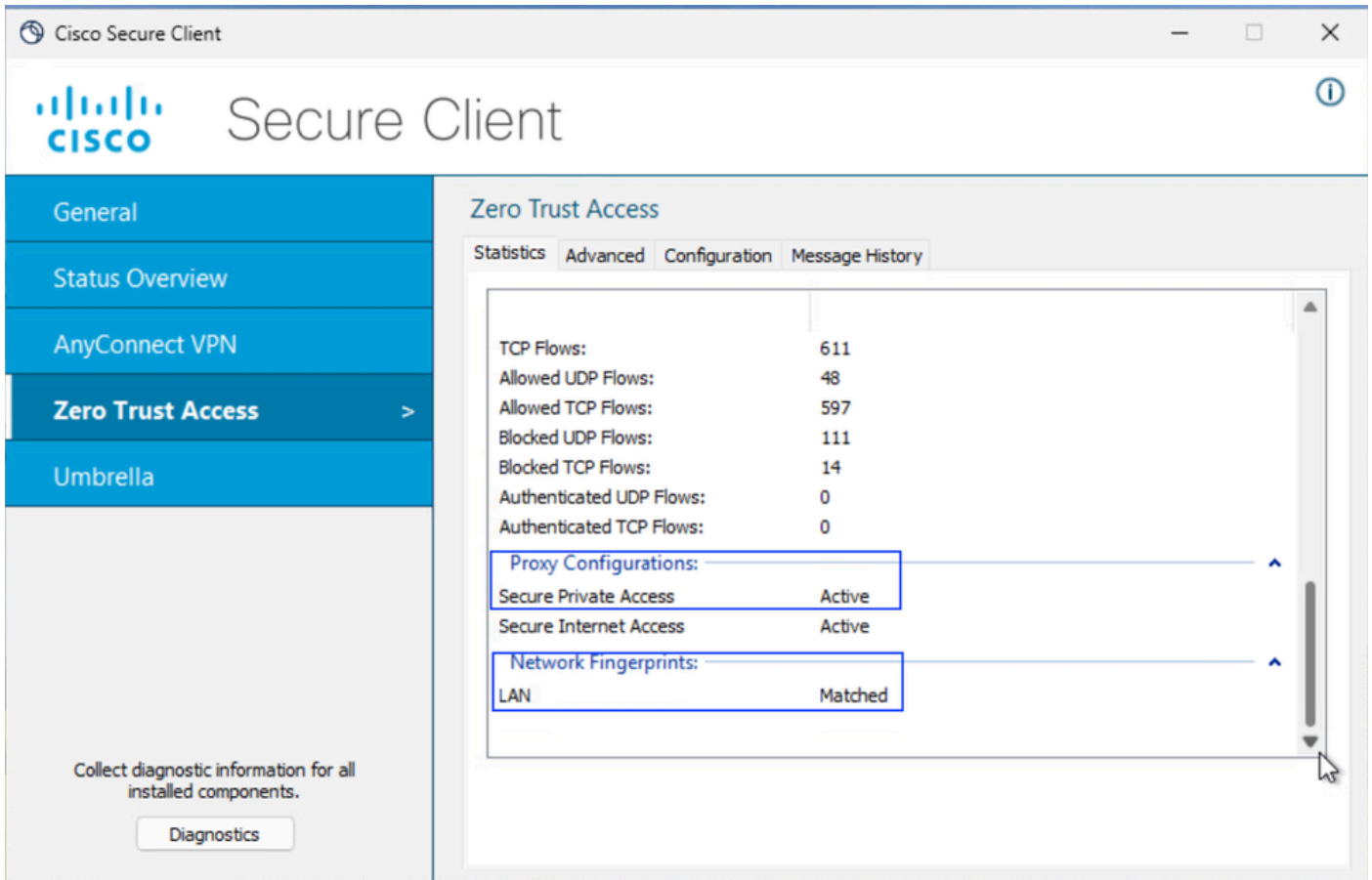
Rows per page: 10 < >

Back Close

## 보안 액세스 - ZTA 프로필

### 단계 - 6 프라이빗 리소스에 대한 액세스 확인

#### 1. ZTA TND에 대한 네트워크 핑거프린트 확인



보안 액세스 - PR 테스트

2. 원격 사용자가 FTD FQDN을 확인할 수 있는지 확인

```
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
```

보안 액세스 - PR 테스트

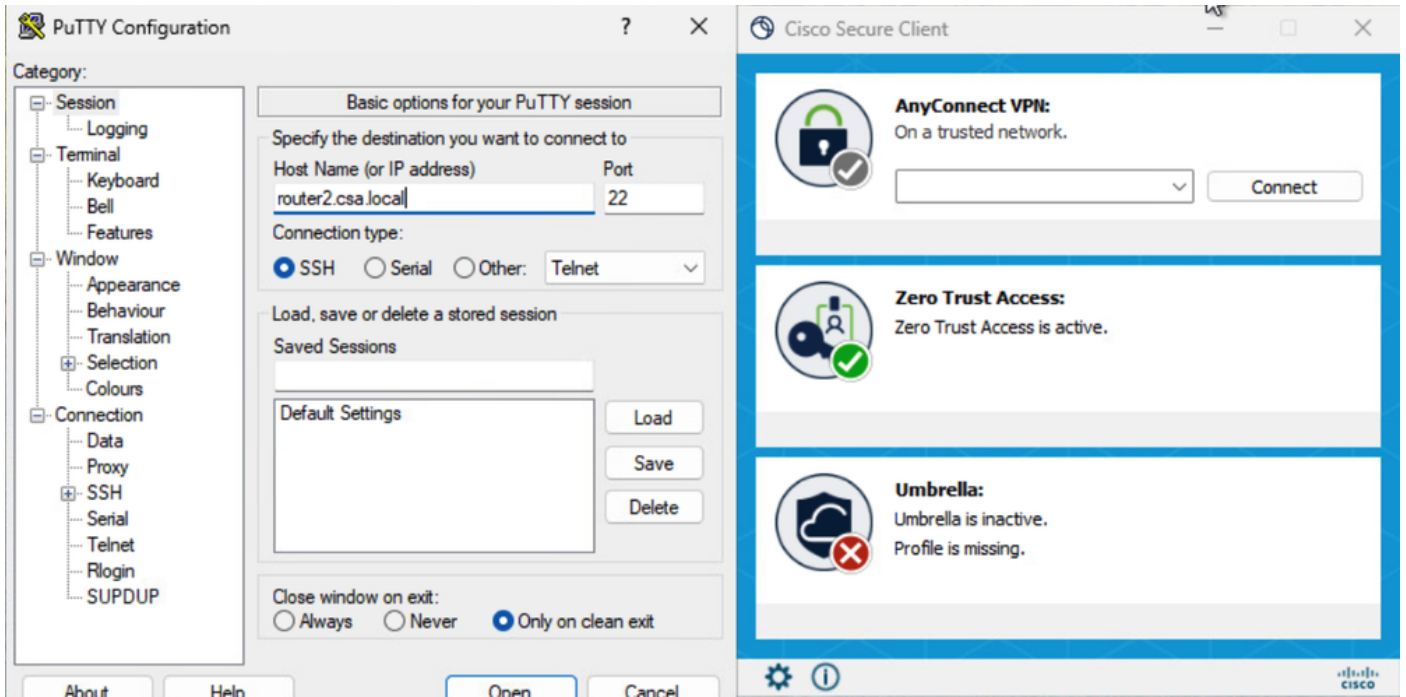
3. FQDN을 사용하여 FTD가 전용 리소스에 연결할 수 있는지 확인합니다.

```
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# █
```

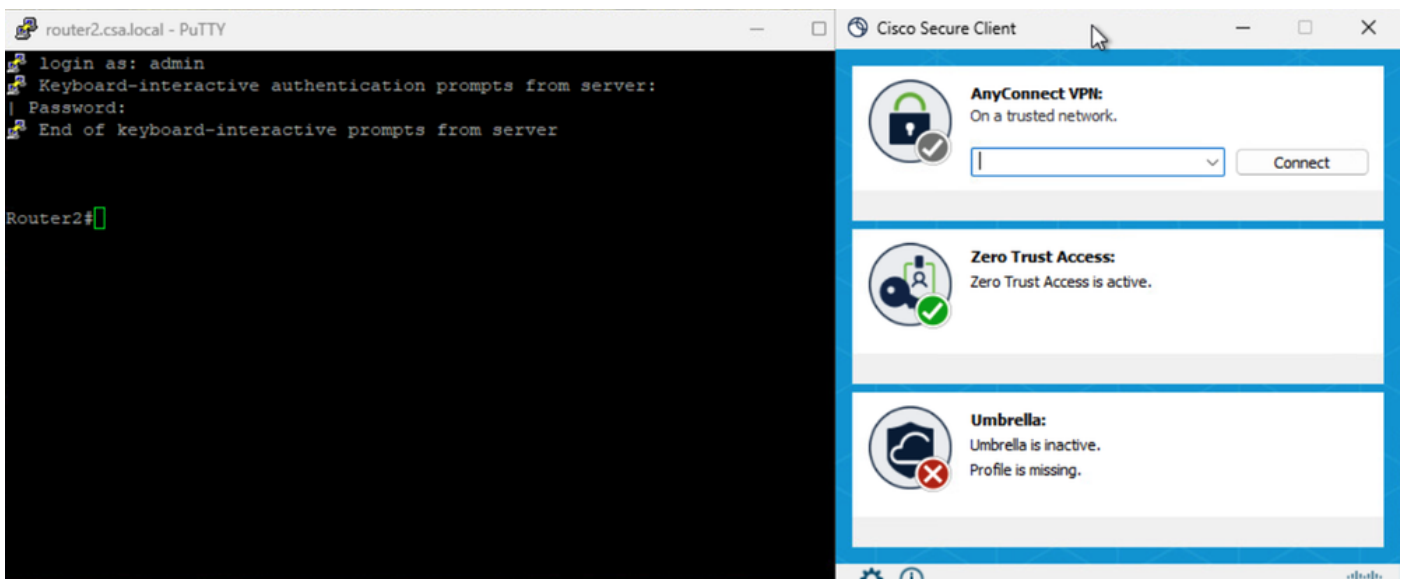
보안 액세스 - PR 테스트

4. 프라이빗 리소스에 대한 SSH 연결 테스트

FQDN을 사용하여 PR 액세스

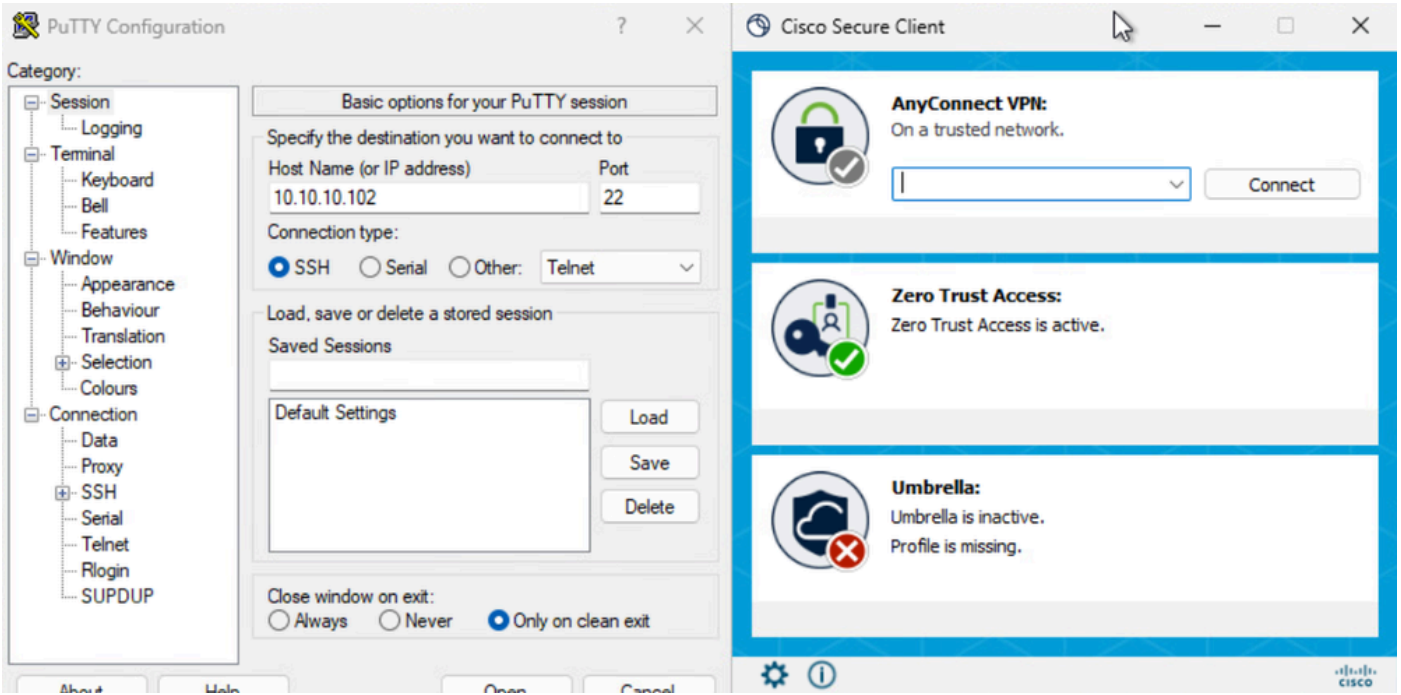


보안 액세스 - PR 테스트

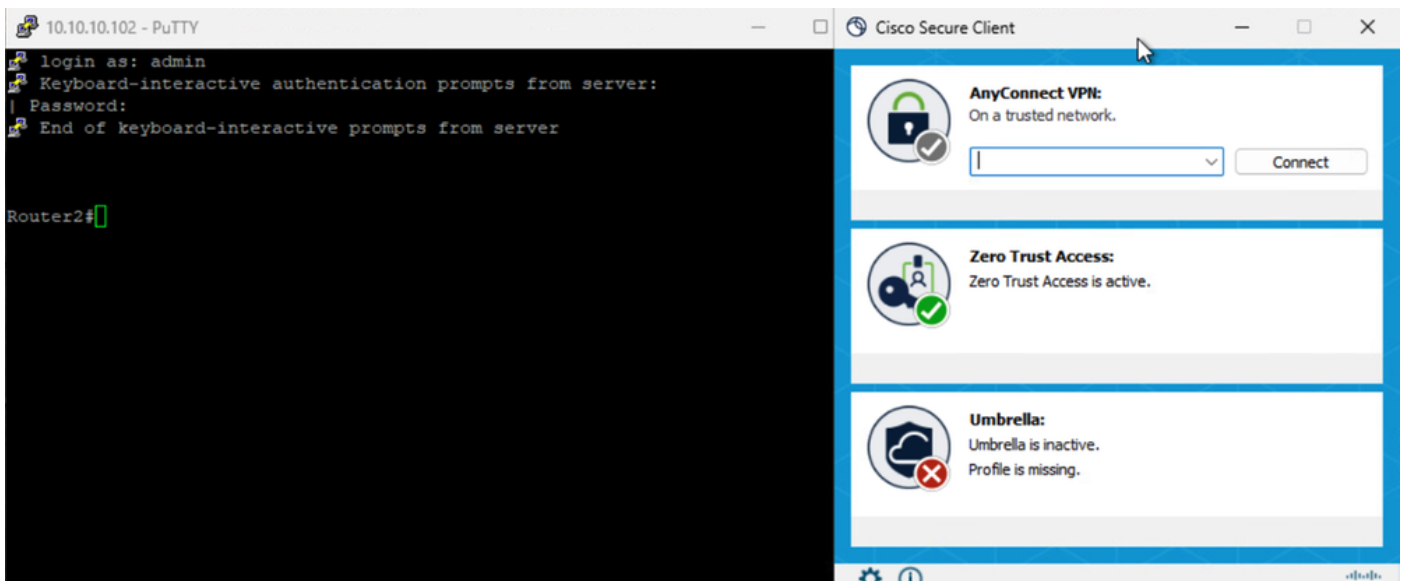


보안 액세스 - PR 테스트

IP 주소를 사용하여 PR에 액세스



보안 액세스 - PR 테스트



보안 액세스 - PR 테스트

5. 보안 액세스 활동 검색 로그 확인

### Activity Search

Activity Search interface showing search filters and results. The search criteria is set to 'DOMAIN router2.csa.local'. The results table shows 8 total results, all with a response of 'Allowed'. The table columns include Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Action, Resource/Application, Zero Trust Access Profile, Rule Name, OS, and Bro.

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	OS	Bro
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	win 10.0.26200.7840	...

### 보안 액세스 - 활동 검색

### Activity Search

Activity Search interface showing search filters and results. The search criteria is set to 'RESPONSE Allowed'. The results table shows 17 total results. An 'Event Details' sidebar is open, showing details for a specific event, including Action (Allowed), Block Reason, Connection Method (ZTA Client-based), Time (Feb 23, 2026 3:33 AM), Access details (Identity: jay (jay@csa.local), Rule Name: Router2-SSH-Allow, Resource/Application: Router2, Zero Trust Access Profile: ZTAProfile, Trusted Network: No Match), and Enforcement Point (FTD > FMC\_FTD). The destination router2.csa.local is highlighted in a blue box.

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/App
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	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
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	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
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.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)	router2.csa.local	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
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	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
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	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
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	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
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	router2.csa.local	10.10.10.102	22	Allowed	Router2
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	192.168.1.64	192.168.1.64	7680	Allowed	LAB Manager
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	192.168.1.23	192.168.1.23	7680	Allowed	LAB Manager

### 보안 액세스 - 활동 검색

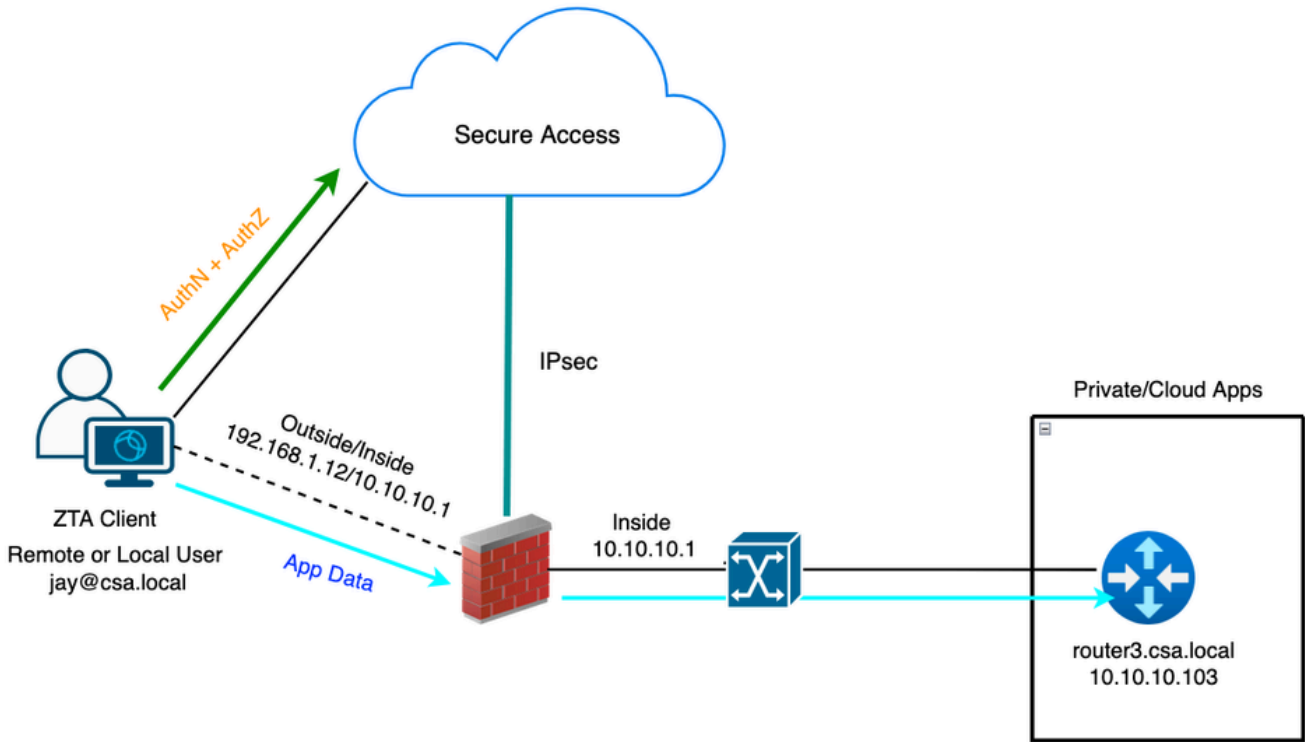
### Activity Search

Activity Search interface showing search filters and results. The search criteria is set to 'IP ADDRESS 10.10.10.102' and 'RESPONSE Allowed'. The results table shows 19 total results, all with a response of 'Allowed'. The table columns include Request, Source, Rule Identity, Destination, Destination IP, Destination Port, Action, Resource/Application, Zero Trust Access Profile, Rule Name, and Bro.

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name	Bro
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	...
ZTA CLIENT-BASED	jay (jay@csa.local)	jay (jay@csa.local)	10.10.10.102	10.10.10.102	22	Allowed	Router2	ZTAProfile	Router2-SSH-Allow	...

### 보안 액세스 - 활동 검색





## 범용 ZTA - 테스트 사례 토폴로지

### 1단계 - Secure Access에서 프라이빗 리소스 정의

클라우드 시행으로 ZTA(Zero Trust Access) 등록된 디바이스를 통해 액세스할 수 있는 프라이빗 리소스 구성

1. Resources > Destinations > Private Resources > Click on +Add로 이동합니다.

The screenshot shows the Cisco Security Cloud Control interface. The 'Resources' section is active, and the 'Private Resource' tab is selected. The interface displays a table of Private Resources with the following data:

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

## 보안 액세스 - 프라이빗 리소스 컨피그레이션

2. 개인 자원명에는 유의미한 자원명을 입력합니다. 설명의 경우, 리소스의 용도 또는 리소스 소유자의 이름과 같은 정보를 제공하는 것이 좋습니다.

← 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

보안 액세스 - 프라이빗 리소스 컨피그레이션

3. 액세스하려는 개인 자원의 FQDN을 입력합니다. 프라이빗 리소스의 IP 주소도 정의할 수 있습니다. 자세한 내용은 프라이빗 [리소스 추가를 참조하십시오](#)

4. 도메인을 확인할 DNS 서버를 선택합니다

**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
192.168.1.103	Any TCP	22
10.10.10.103	Any TCP	22

Use internal DNS server to resolve the domain

LabDNS (192.168.1.20, 10.10.10.20)

보안 액세스 - 프라이빗 리소스 컨피그레이션

5. 엔드포인트 연결 방법 선택

6. FTD를 로컬 적용 지점으로 선택합니다

## 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... 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

## 보안 액세스 - 프라이빗 리소스 컨피그레이션

RC를 통해 개인 리소스에 액세스할 수 있는 경우 RC를 선택하고, 그렇지 않은 경우 IPsec 터널 그룹(Network Tunnel Group)을 통해 개인 리소스에 액세스할 수 있는 경우 비워둡니다.

## Resource Connector Groups

Secure Access can forward Zero Trust Access traffic to this private resource using resource connectors. ⓘ

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. ⓘ

## 보안 액세스 - 프라이빗 리소스 컨피그레이션



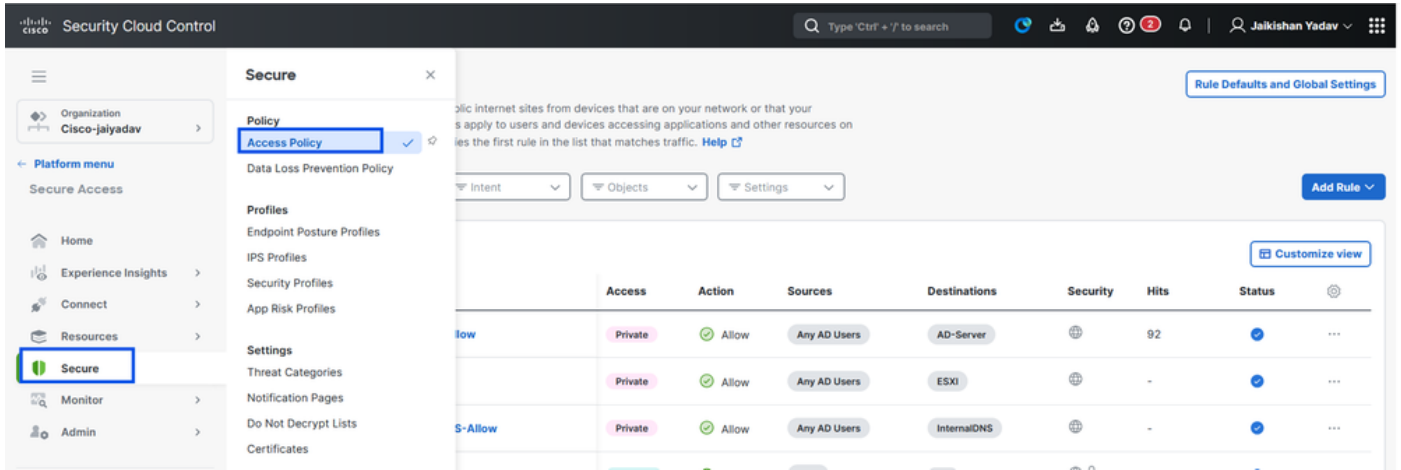
참고: 선택하는 등록 유형에 따라 이 변경 사항은 PR을 FTD에 자동으로 연결하고 정책 구축을 트리거합니다

7. Save(저장)를 클릭합니다.

2단계 - 개인 액세스 규칙 생성

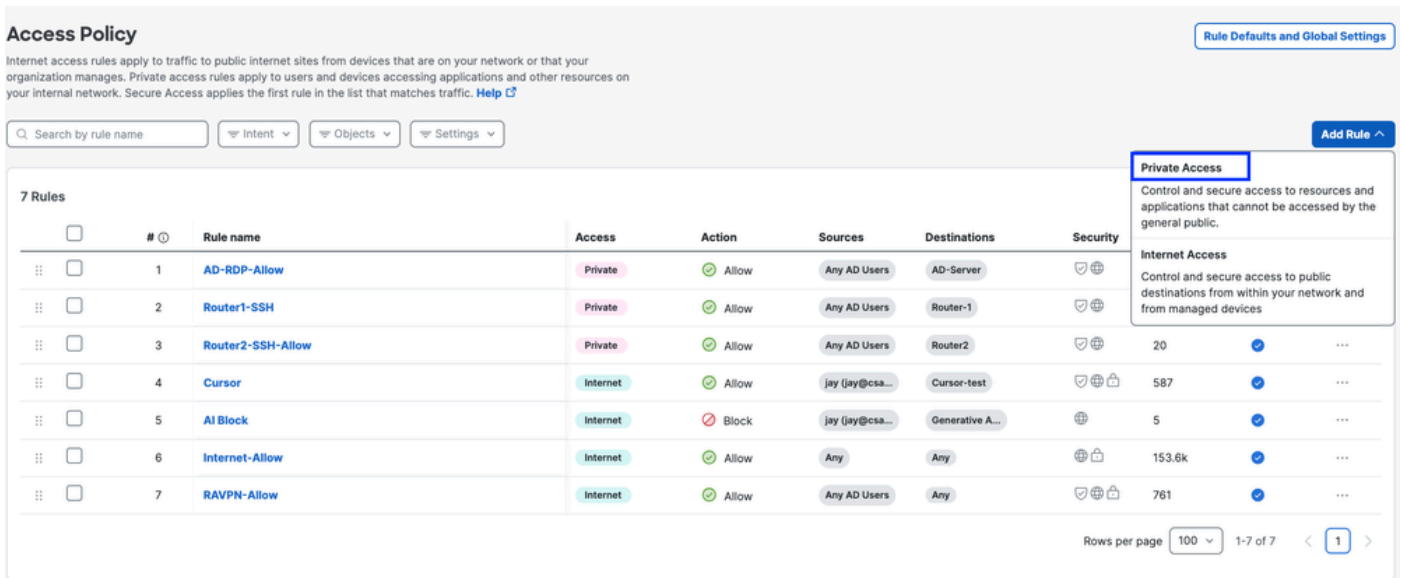
Universal ZTA 등록된 사용자가 액세스할 수 있도록 Secure Access의 비공개 액세스를 구성합니다 . 자세한 내용은 [개인 액세스 규칙을 참조하십시오](#)

1. Secure(보안) > Access Policy(액세스 정책)로 이동합니다



보안 액세스 - 액세스 정책 컨피그레이션

2. 규칙 추가를 클릭한 다음 개인 액세스를 선택합니다.  
 규칙의 맨 위에는 규칙의 구성된 구성 요소를 설명하는 요약이 있습니다.



보안 액세스 - 액세스 정책 컨피그레이션

3. 규칙 이름 추가

## 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

**Allow**  
Allow specified traffic if security requirements are met.

**Block**  
Block specified traffic.

## 보안 액세스 - 액세스 정책 컨피그레이션

### 4. 규칙 조치를 선택하고 출처 및 대상을 선택합니다

Rule name  Rule order

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

Action

**Allow**  
Allow specified traffic if security requirements are met.

**Block**  
Block specified traffic.

From  To

+ AND

## 보안 액세스 - 액세스 정책 컨피그레이션

### 5. 엔드포인트 요구 사항 구성

### 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](#)

## 보안 액세스 - 액세스 정책 컨피그레이션

### 6. 보안 구성

**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](#)

## 보안 액세스 - 액세스 정책 컨피그레이션

### 7. 저장을 클릭합니다.

### 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](#)

Search by rule name:  Intent:  Objects:  Settings:  Add Rule

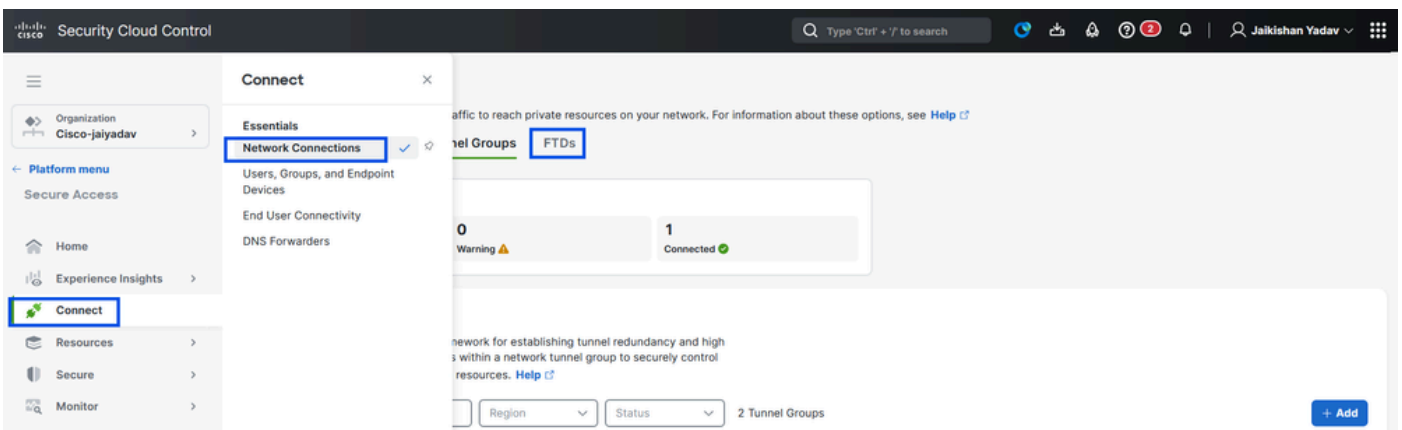
#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
1	Router3-SSH-Allow	Private	Allow	Any AD Users	Router3	Shield	-	On
2	AD-RDP-Allow	Private	Allow	Any AD Users	AD-Server	Shield	-	On
3	Router1-SSH	Private	Allow	Any AD Users	Router-1	Shield	-	On
4	Router2-SSH-Allow	Private	Allow	Any AD Users	Router2	Shield	20	On
5	Cursor	Internet	Allow	jay (jay@csa...)	Cursor-test	Shield, Lock	587	On
6	AI Block	Internet	Block	jay (jay@csa...)	Generative A...	Shield	5	On
7	Internet-Allow	Internet	Allow	Any	Any	Shield, Lock	154.8k	On
8	RAVPN-Allow	Internet	Allow	Any AD Users	Any	Shield, Lock	761	On

Rows per page: 100 1-8 of 8 1

## 보안 액세스 - 액세스 정책 컨피그레이션

### 3단계 - FTD에서 PR 연결 확인

1. connect(연결) > Network Connections(네트워크 연결) > FTDs(FTD)로 이동합니다



## 보안 액세스 - PR 확인

2. FTD(FTD) > View resources associated to this FTD(이 FTD와 연결된 리소스 보기)를 클릭합니다.

```

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

```

보안 액세스 - PR 확인

### 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.

FMC Name

Configuration status

1 FTDs

FTD Name	Version	FMC	UZTA Configuration status	Associated
<b>FMC_FTD</b> 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>	<span style="border: 1px solid #ccc; padding: 2px;">1 DNS Domains</span> <span style="border: 1px solid #ccc; padding: 2px;">1 DNS Servers</span>

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

**Associated Resources** 3

**RESOURCES ASSOCIATED BY STATUS**

Status	Count
● Synced	3

[View resources associated to this FTD](#)

[Associate Resources](#)

보안 액세스 - PR 확인

```
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
```

보안 액세스 - PR 확인

## Resources associated with FMC\_FTD

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

<input type="text" value="Search by resource name"/>	<input type="text" value="Configuration status"/>	3 Resources	<a href="#">Associate Resources</a>
Resource name	Status		
Router-1	<input checked="" type="checkbox"/> Synced		
Router2	<input checked="" type="checkbox"/> Synced		
Router3	<input checked="" type="checkbox"/> Synced		

Close

보안 액세스 - PR 확인

3 . Close(닫기)를 클릭합니다

4. 상태, 관련 리소스 및 구성이 동기화 상태인지 확인합니다.

**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
<b>FMC_FTD</b> Device FQDN: ftd.csa.local Trusted network: LAN	v10.0.0	FMC	<b>Synced</b>	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)  
 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

보안 액세스 - PR 확인

5. 구성이 FTD로 푸시되었는지 확인합니다.

FTD cli에 로그인하고 LINA 모드로 이동합니다.

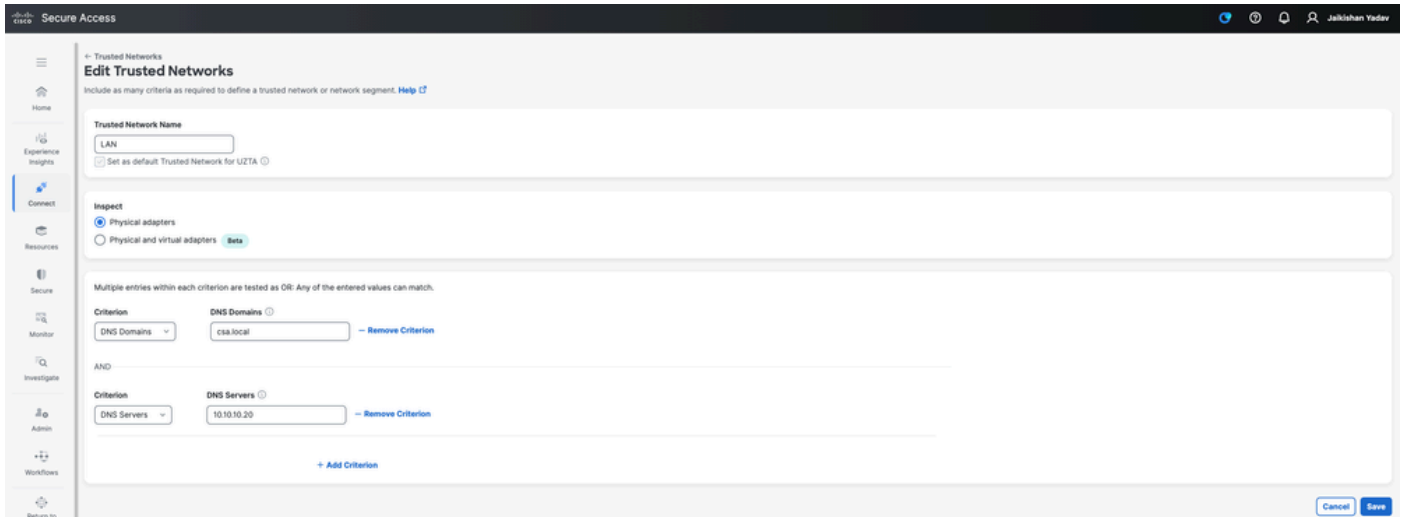
# show running-config object application

```
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
```

## 보안 액세스 - PR 확인

4단계 " 신뢰할 수 있는 네트워크 또는 ZTA 설정 관리" 구성 또는 확인

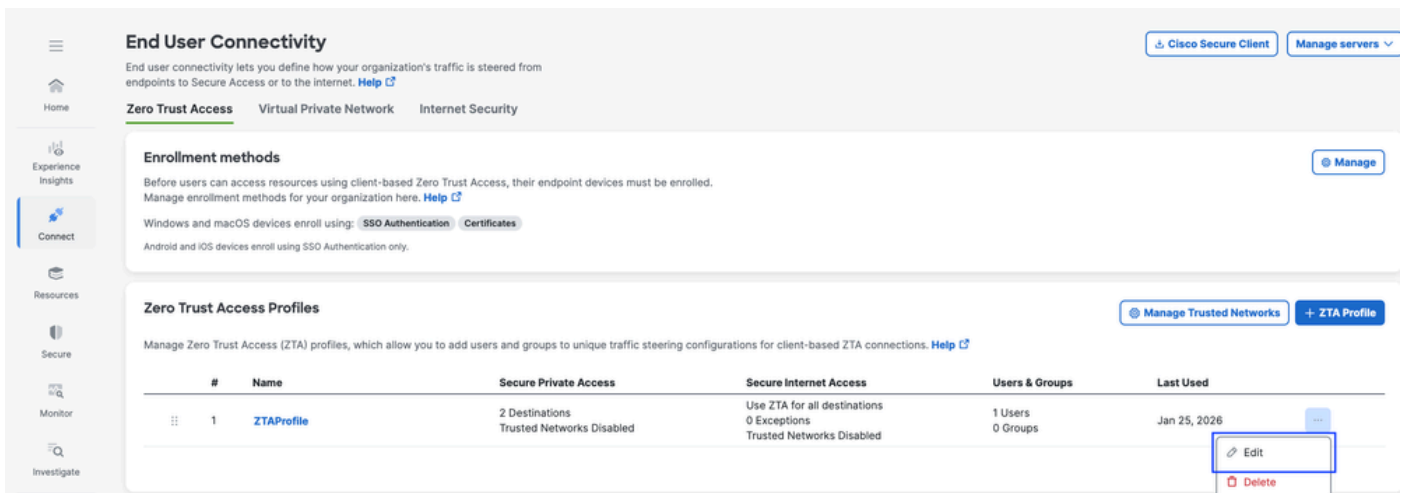
Connect(연결) > End User Connectivity(최종 사용자 연결) > Zero Trust Access(제로 트러스트 액세스) > ZTA Settings(ZTA 설정)로 이동하고 신뢰할 수 있는 네트워크를 구성합니다



## 보안 액세스 - ZTA TND 컨피그레이션

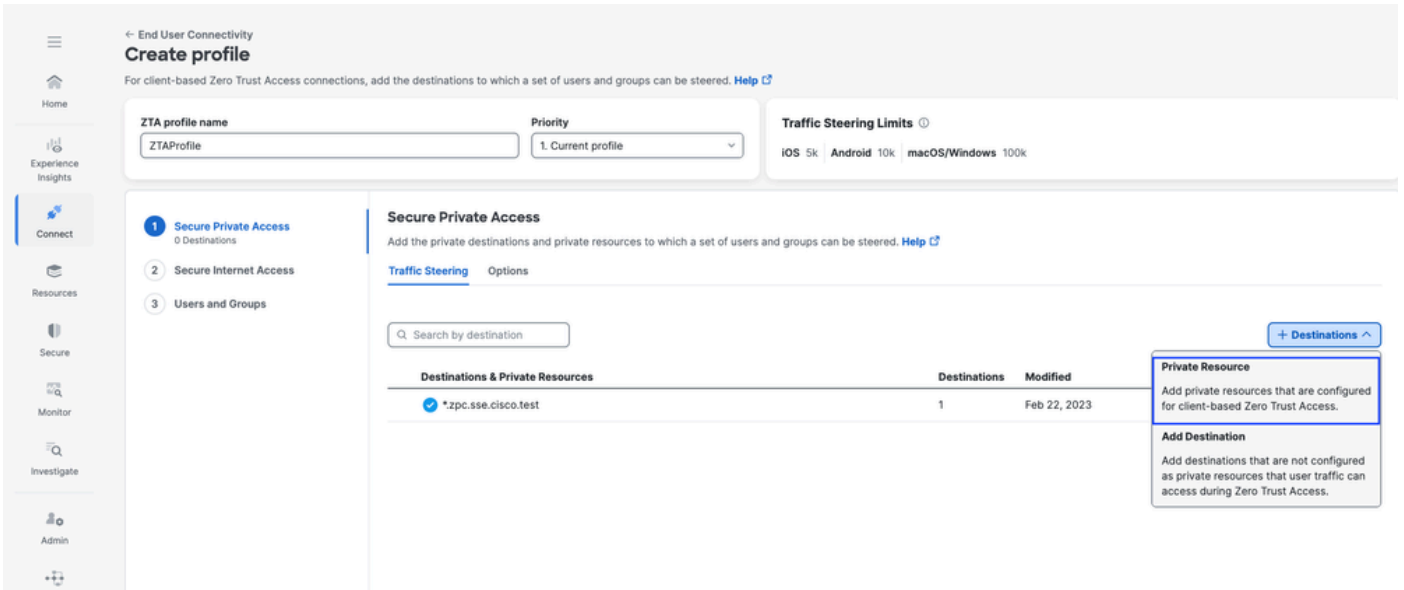
단계 - 5 ZTA 프로필에 프라이빗 리소스 추가

1. Connect(연결) > End User Connectivity(최종 사용자 연결) > Zero Trust Access(Zero Trust 액세스)로 이동하고 3개의 점을 클릭하여 ZTA 프로파일을 편집합니다

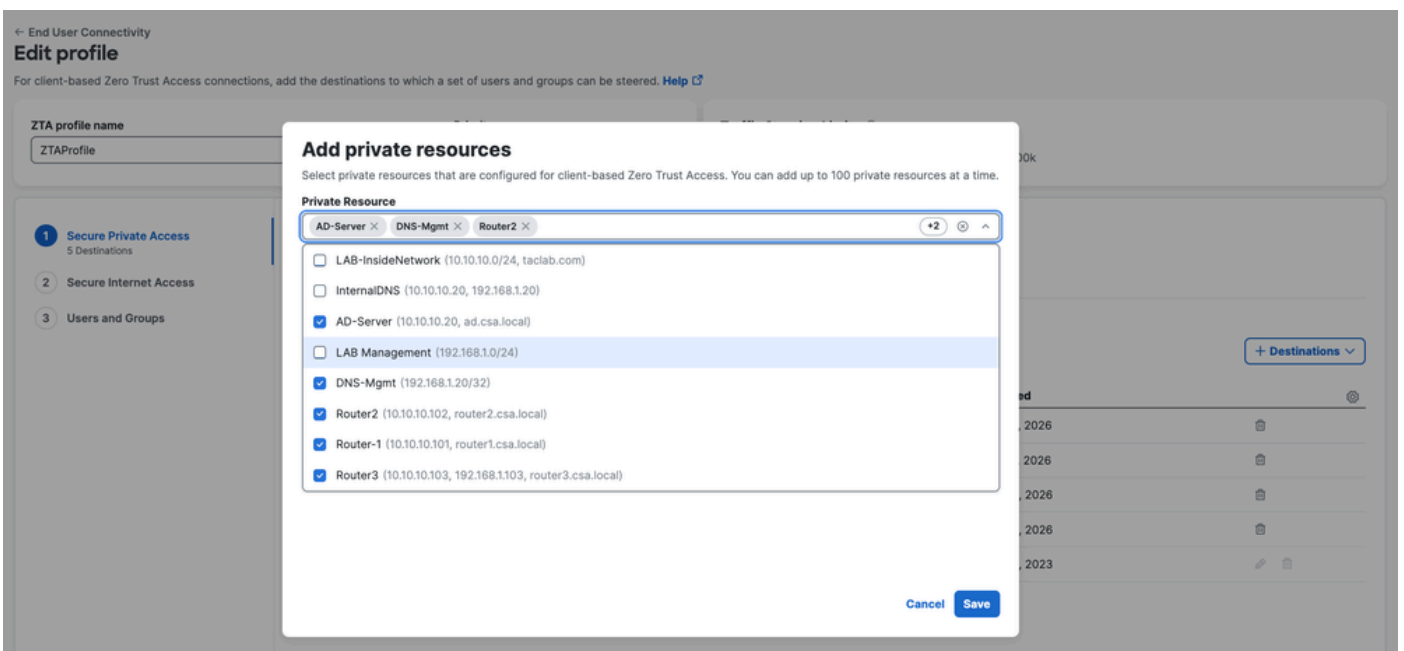


## 보안 액세스 - ZTA 프로필

## 2. 프라이빗 리소스 추가

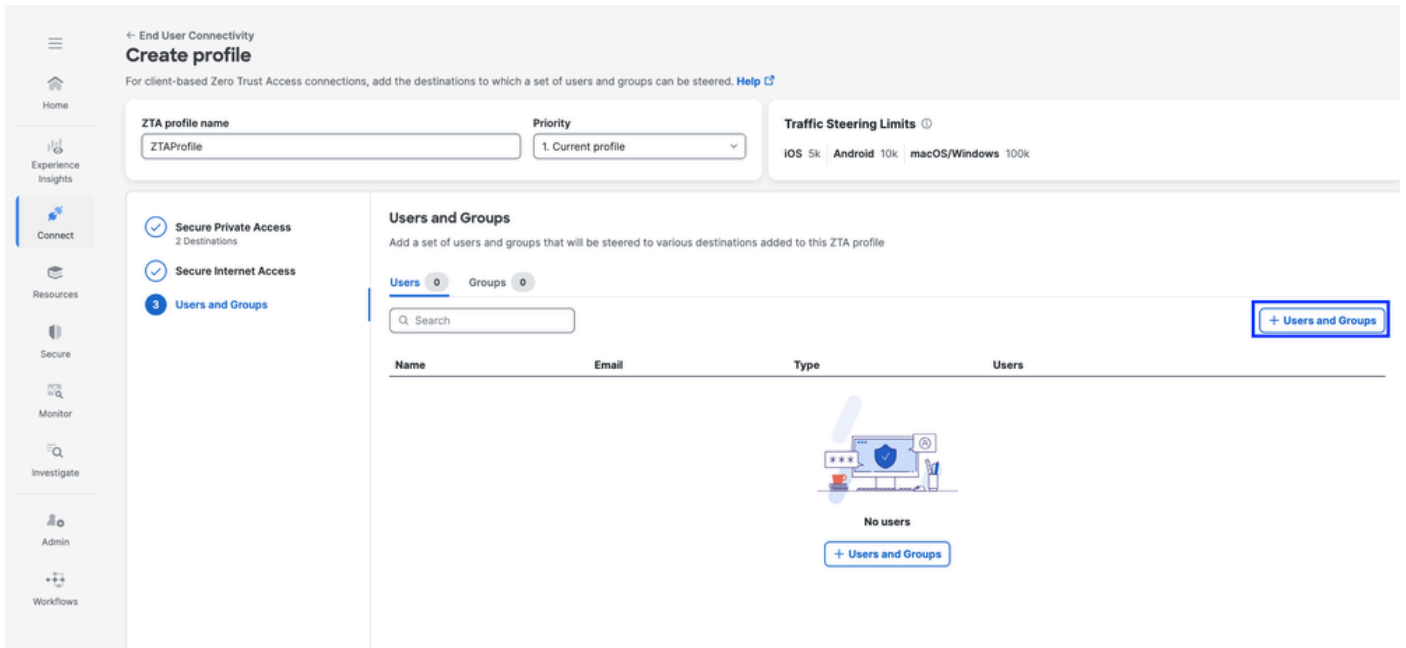


## 보안 액세스 - ZTA 프로필

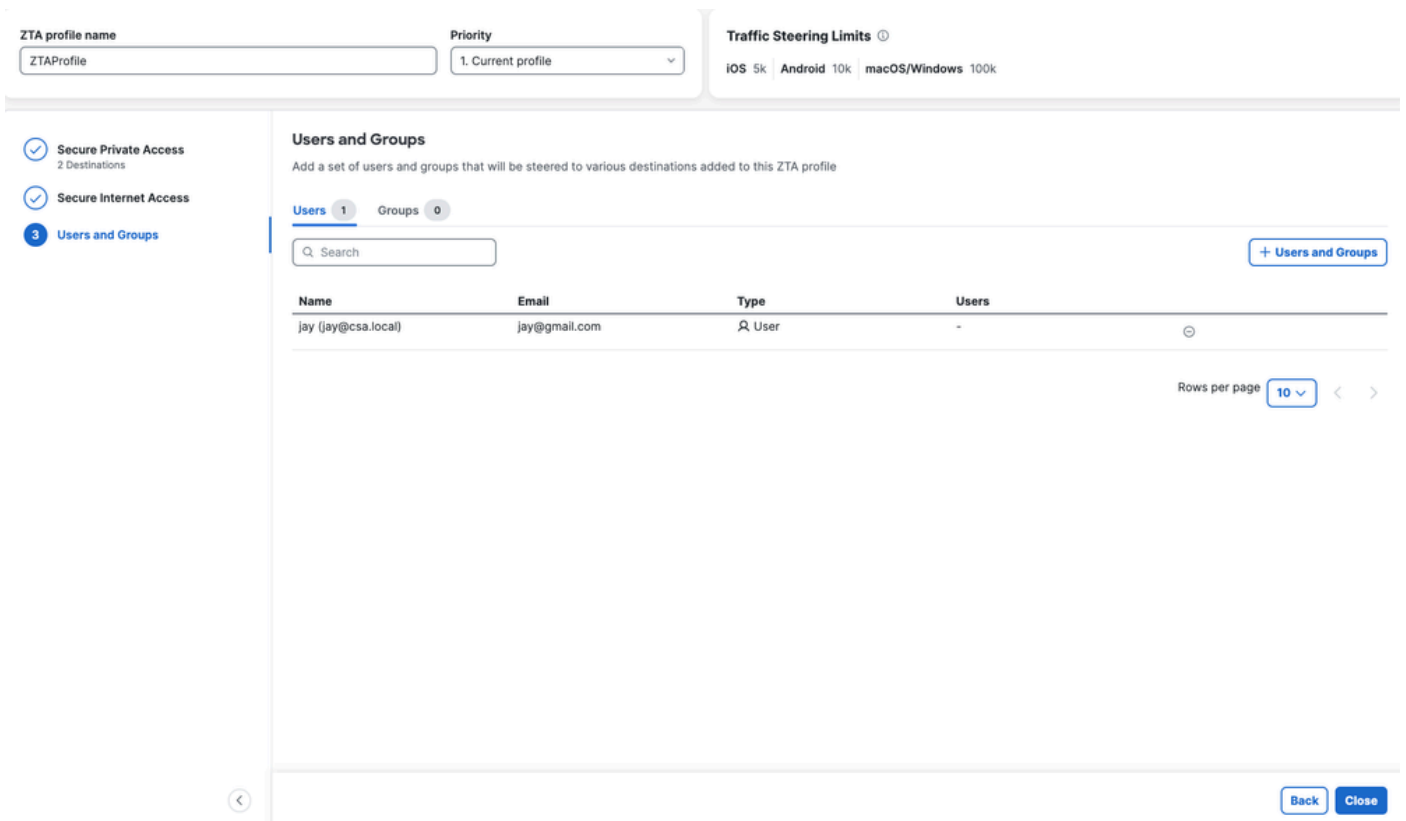


## 보안 액세스 - ZTA 프로필

## 3. 사용자 및 그룹 추가



## 보안 액세스 - ZTA 프로필

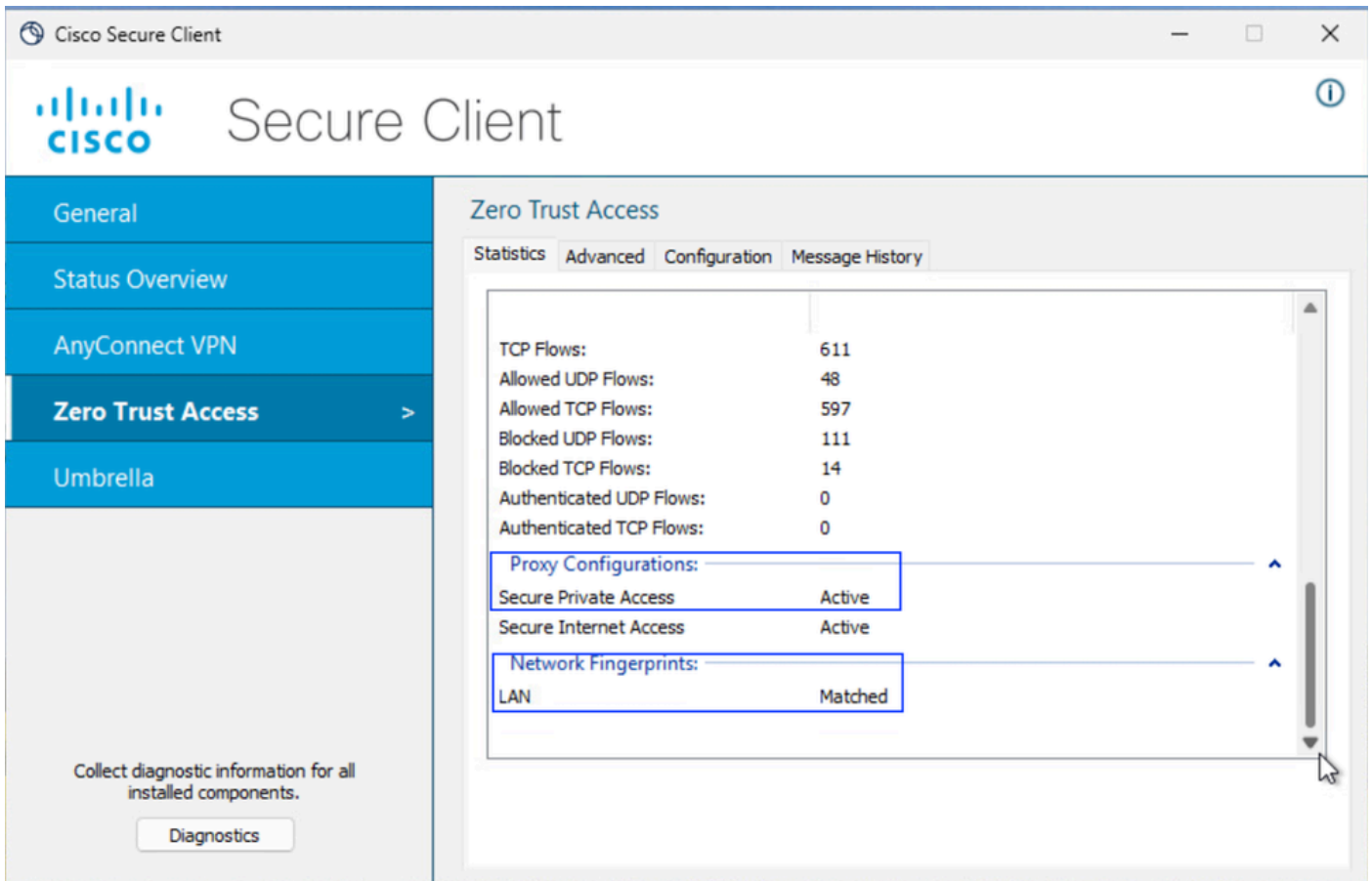


## 보안 액세스 - ZTA 프로필

### 단계 - 6 프라이빗 리소스에 대한 액세스 확인

사용자가 로컬인 경우

1. ZTA TND에 대한 네트워크 핑거프린트를 확인합니다. 사용자가 로컬이고 Secure Private Access를 활성화해야 하는 경우 일치해야 합니다.



보안 액세스 - PR 테스트

2. 원격 사용자가 FTD FQDN을 확인할 수 있는지 확인

```
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
```

보안 액세스 - PR 테스트

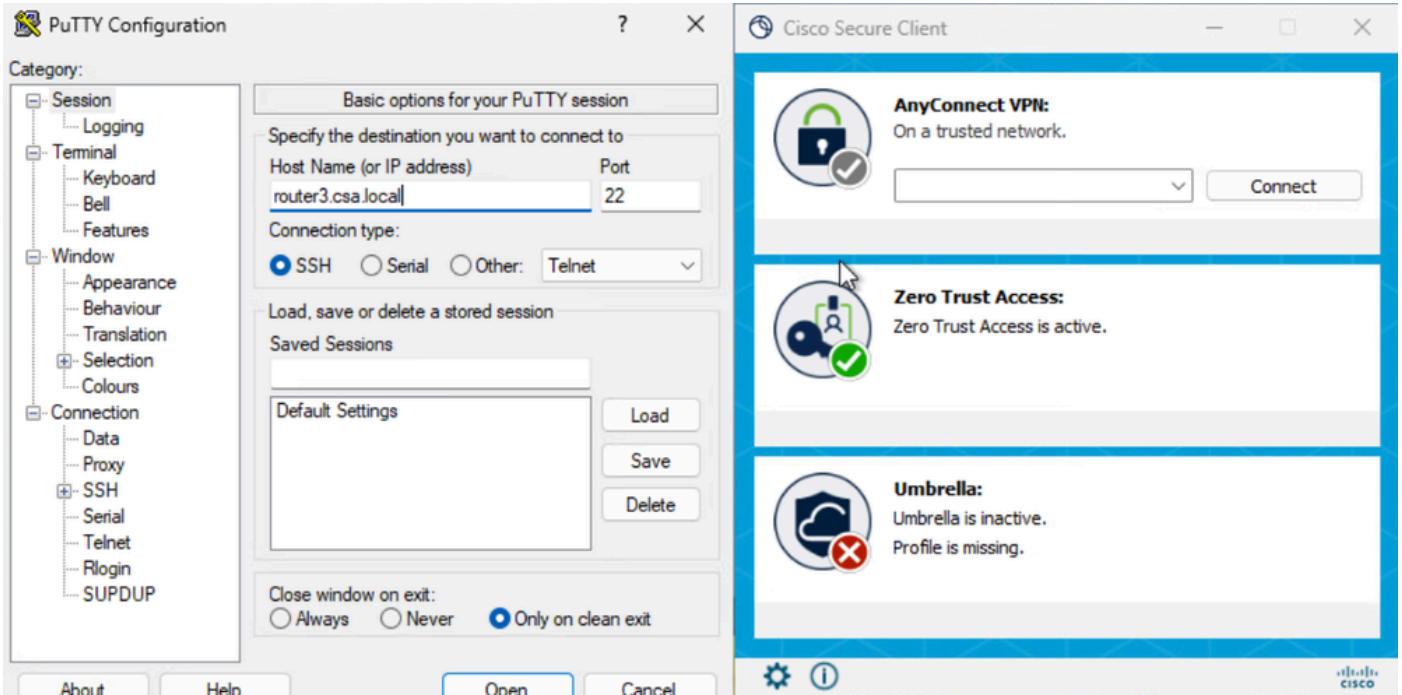
3. FQDN을 사용하여 FTD가 전용 리소스에 연결할 수 있는지 확인합니다.

```
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# █
```

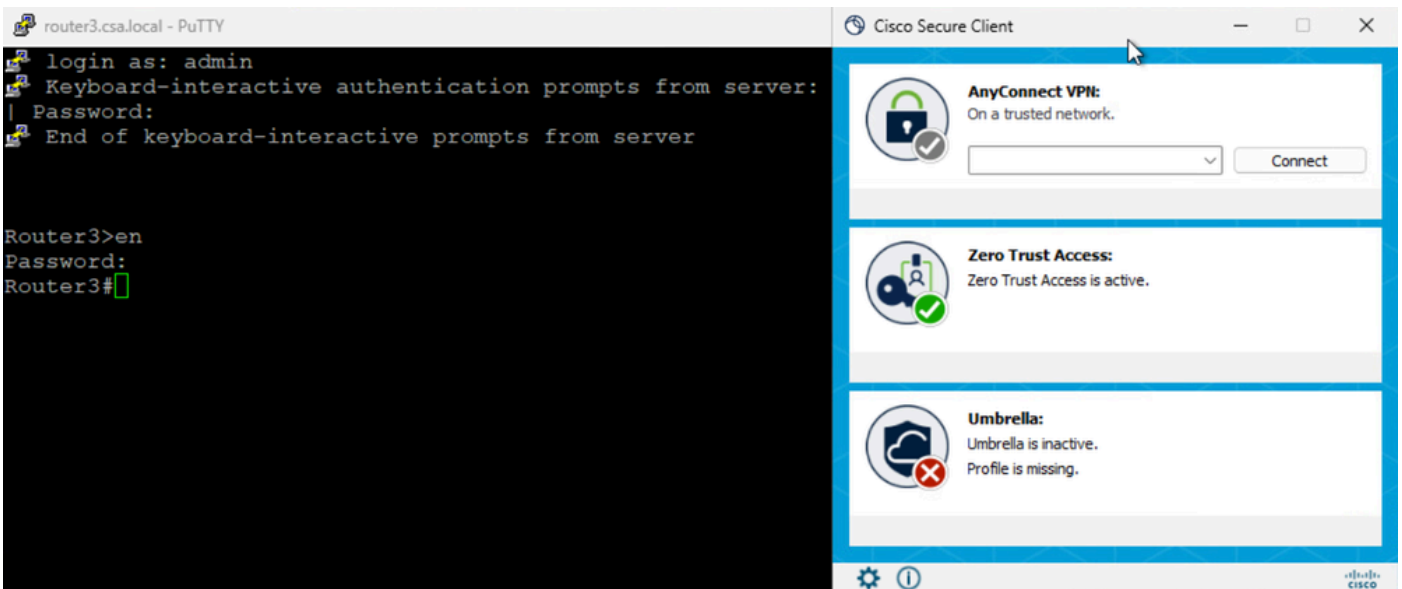
보안 액세스 - PR 테스트

4. 프라이빗 리소스에 대한 SSH 연결 테스트

FQDN을 사용하여 PR 액세스

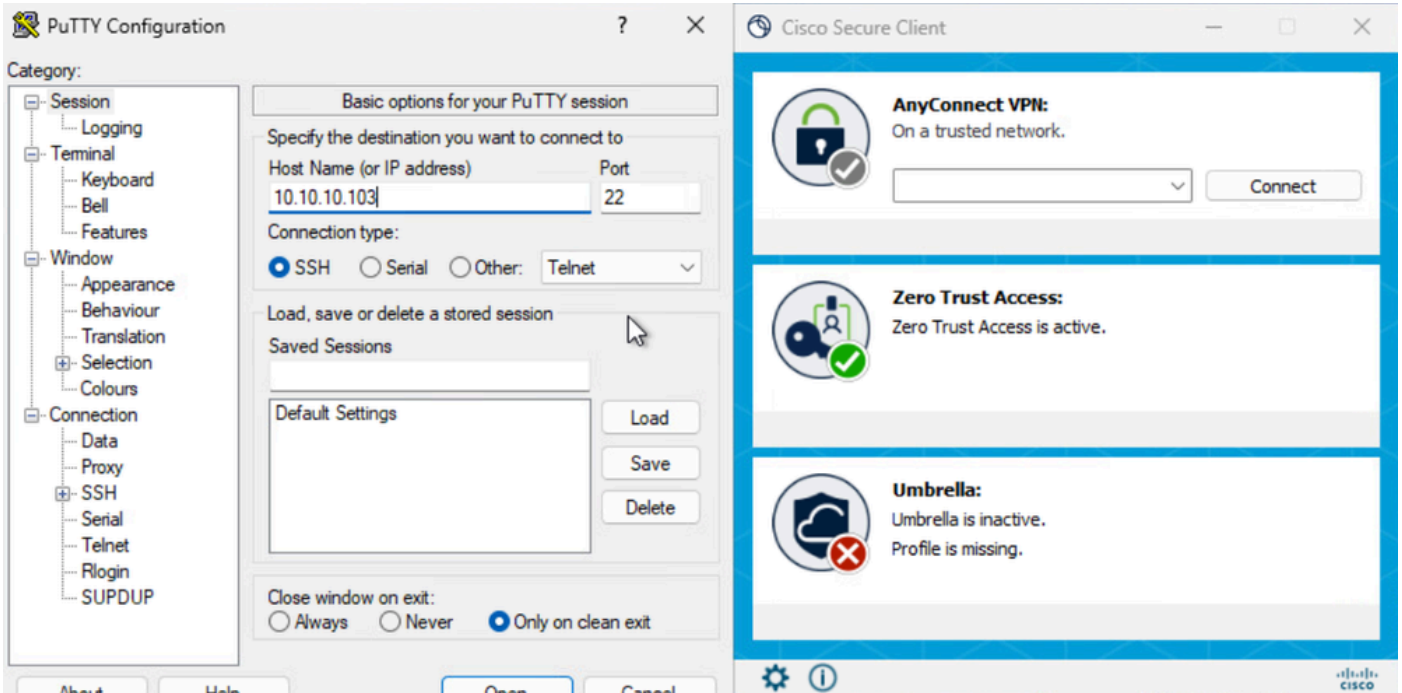


보안 액세스 - PR 테스트

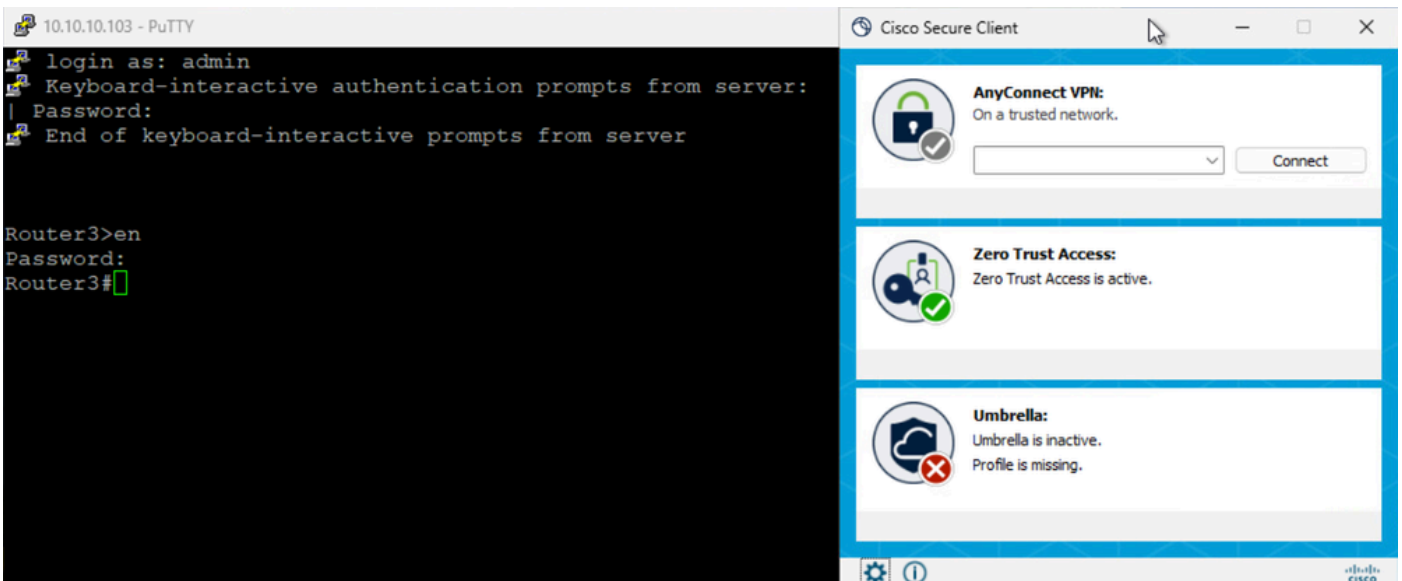


보안 액세스 - PR 테스트

IP 주소를 사용하여 PR에 액세스



## 보안 액세스 - PR 테스트



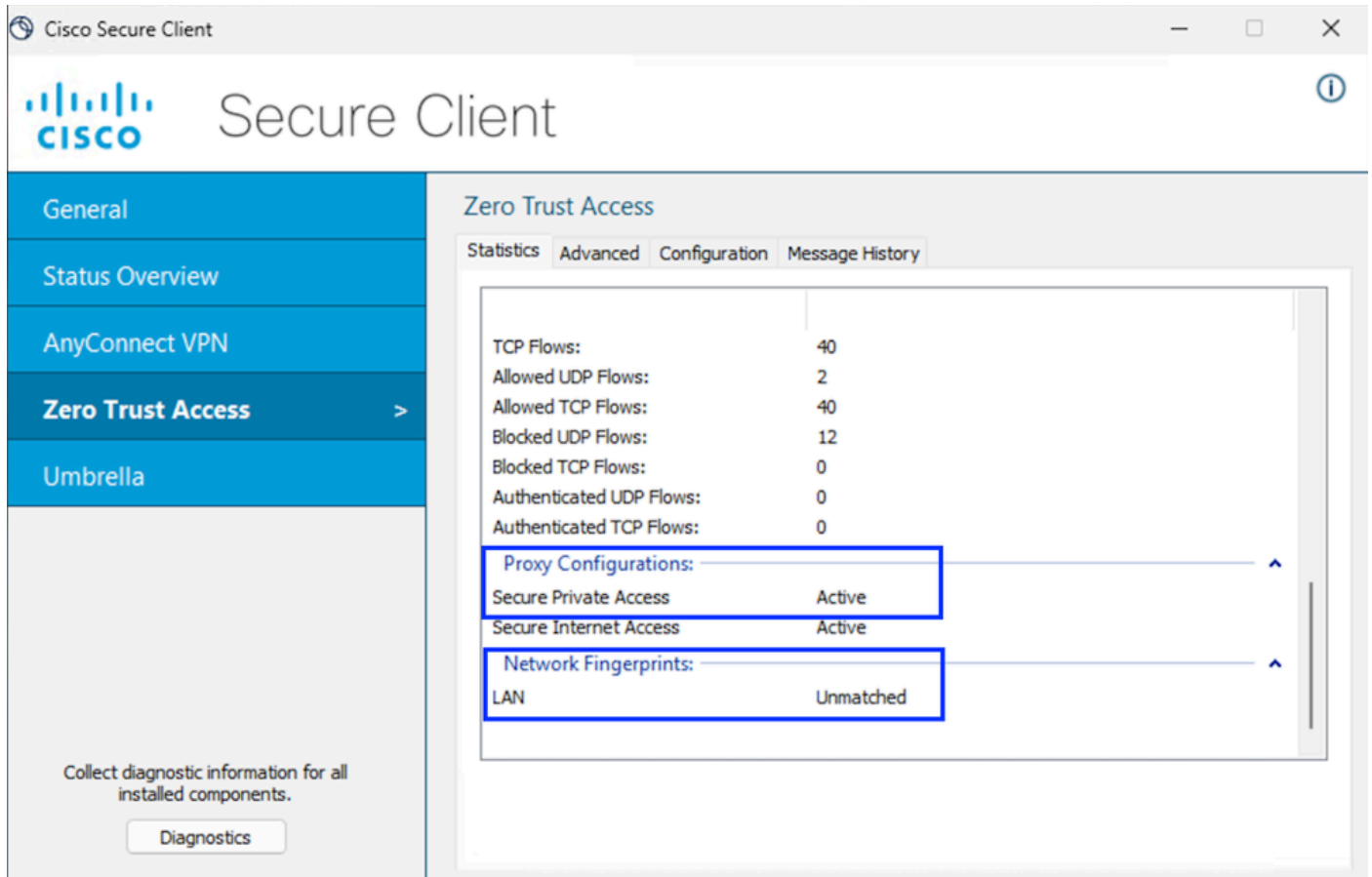
## 보안 액세스 - PR 테스트

### 5. 보안 액세스 활동 검색 로그 확인



사용자가 원격인 경우

1. ZTA TND에 대한 네트워크 핑거프린트를 확인합니다. 사용자가 원격인 경우 일치하지 않아야 합니다.



보안 액세스 - PR 테스트

2. 원격 사용자가 FTD FQDN을 확인할 수 있는지 확인

```

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

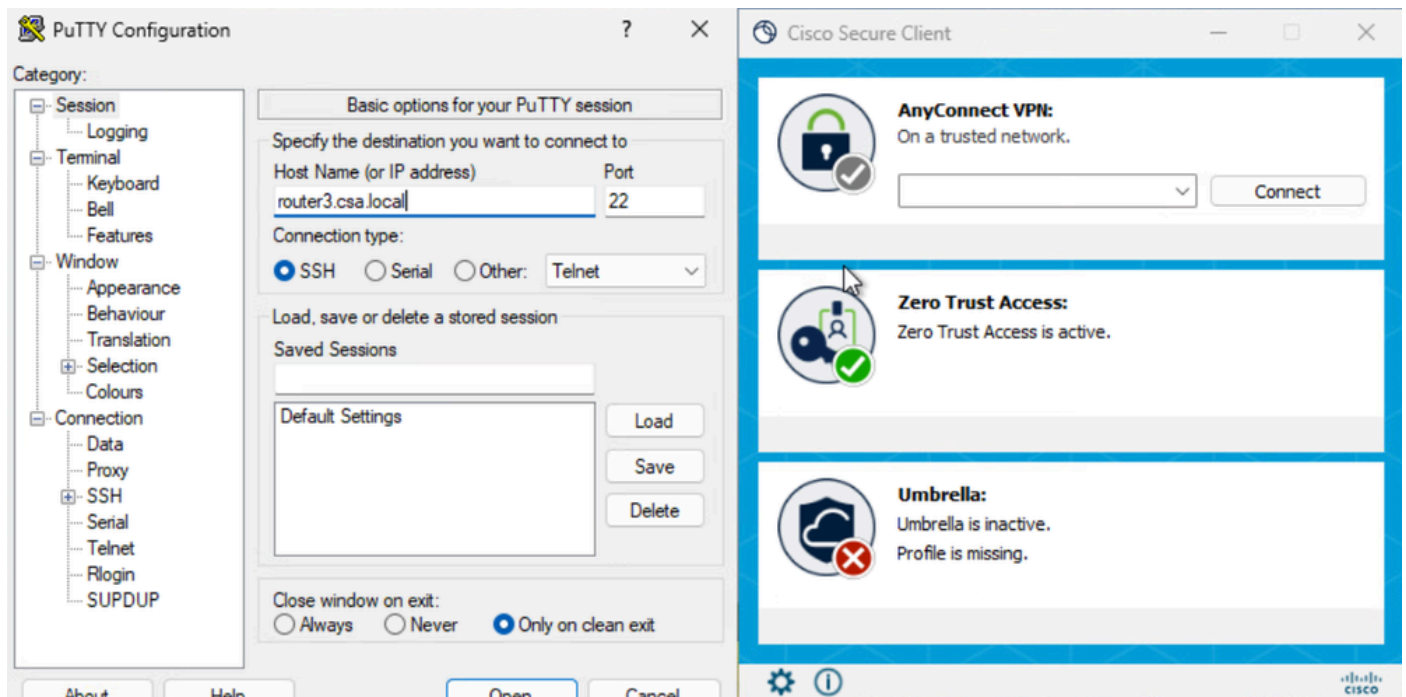
Name: ftd.csa.local
Addresses: 192.168.1.12

```

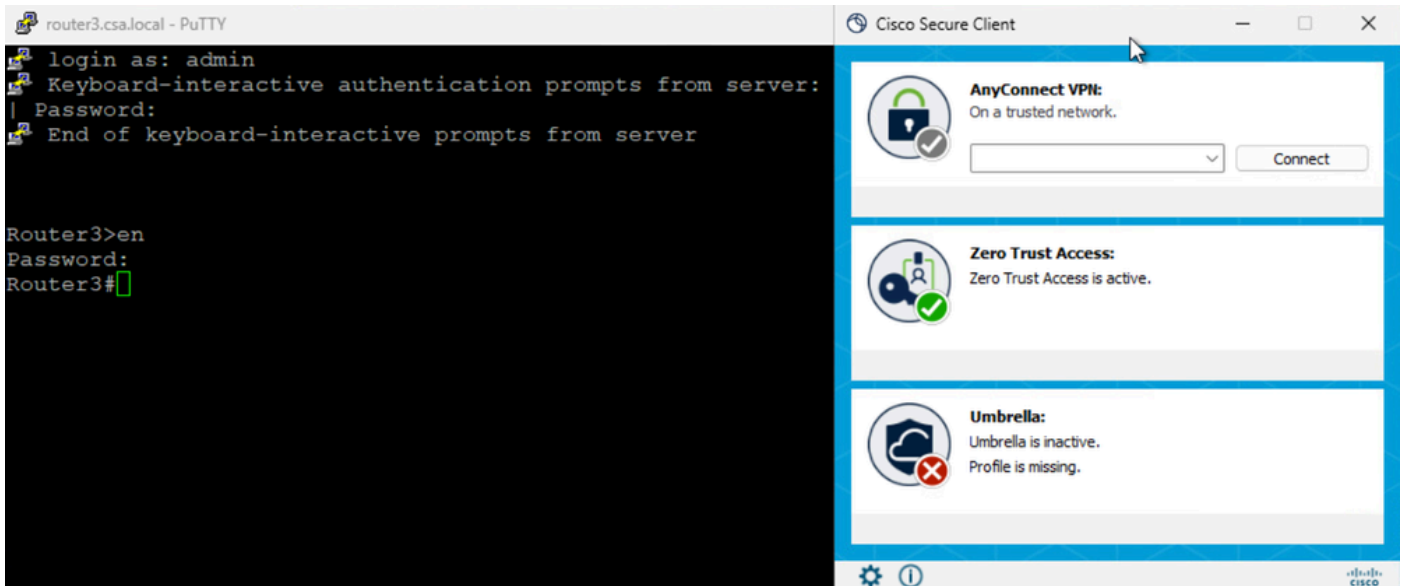
보안 액세스 - PR 테스트

### 3. 프라이빗 리소스에 대한 SSH 연결 테스트

FQDN을 사용하여 PR 액세스

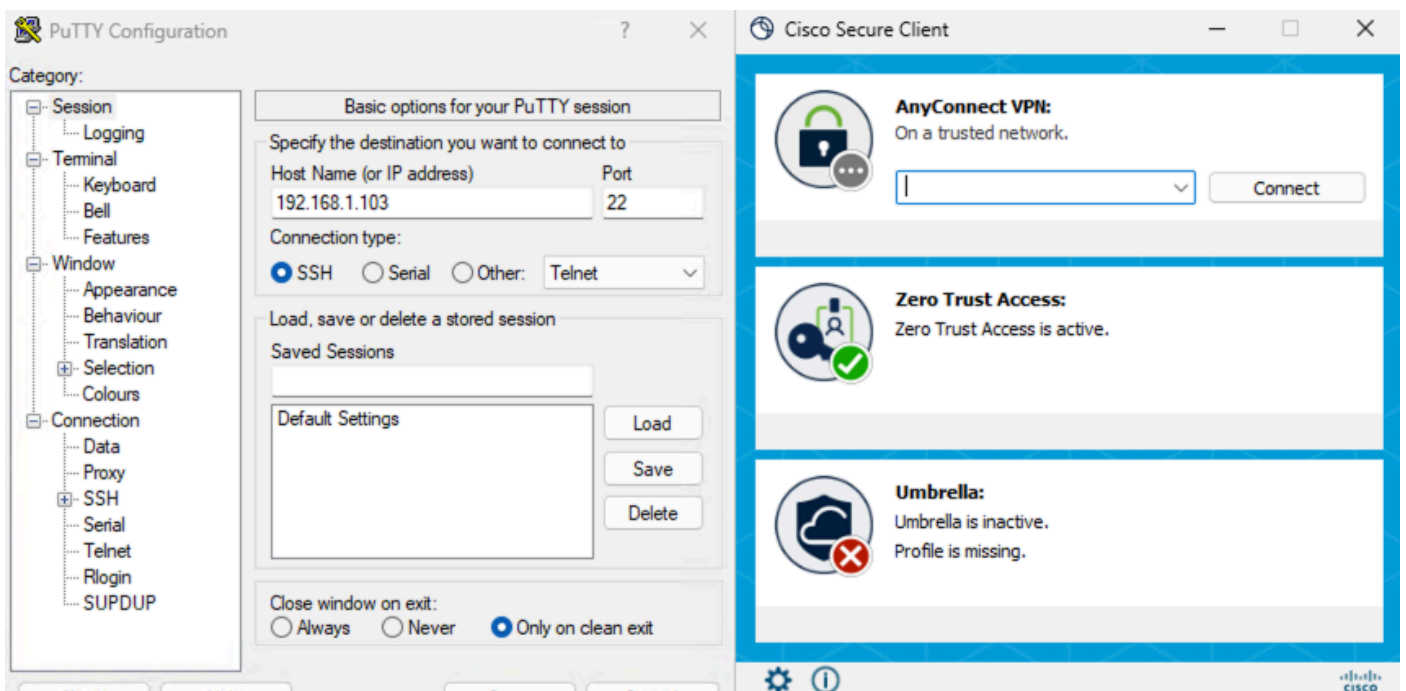


보안 액세스 - PR 테스트

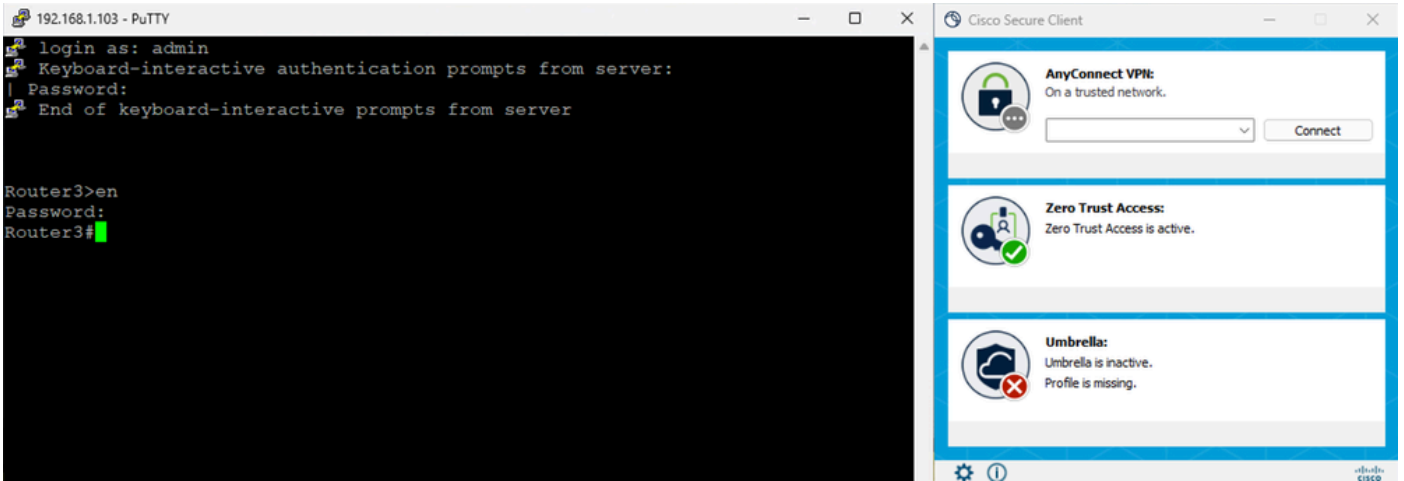


보안 액세스 - PR 테스트

IP 주소를 사용하여 PR에 액세스



보안 액세스 - PR 테스트



## 보안 액세스 - PR 테스트

### 5. 보안 액세스 활동 검색 로그 확인

**Activity Search** Filters  Advanced CLEAR Saved Searches Customize Columns ZTA Client-based Restore to default layout Save Search LAST 24 HOURS

**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

Response	Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Action	Resource/Application	Zero Trust Access Profile	Rule Name
Allowed	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
Allowed	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
Allowed	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
Allowed	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
Allowed	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
Allowed	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
Allowed	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
Allowed	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
Allowed	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
Allowed	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
Allowed	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

## 보안 액세스 - 활동 검색

**Activity Search** Filters  Advanced CLEAR Saved Searches Customize Columns ZTA Client-based Restore to default layout Save Search LAST 24 HOURS

**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

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

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

## 문제 해결

### 유용한 명령:

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

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

```
! expert 모드로 전환하여
```

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

```
# show conn all
```

```
# nat 세부사항 표시
```

```
# asp 테이블 소켓 표시
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.