보안 액세스에서 개인 리소스 액세스를 위한 범용 ZTNA 구성

목차

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

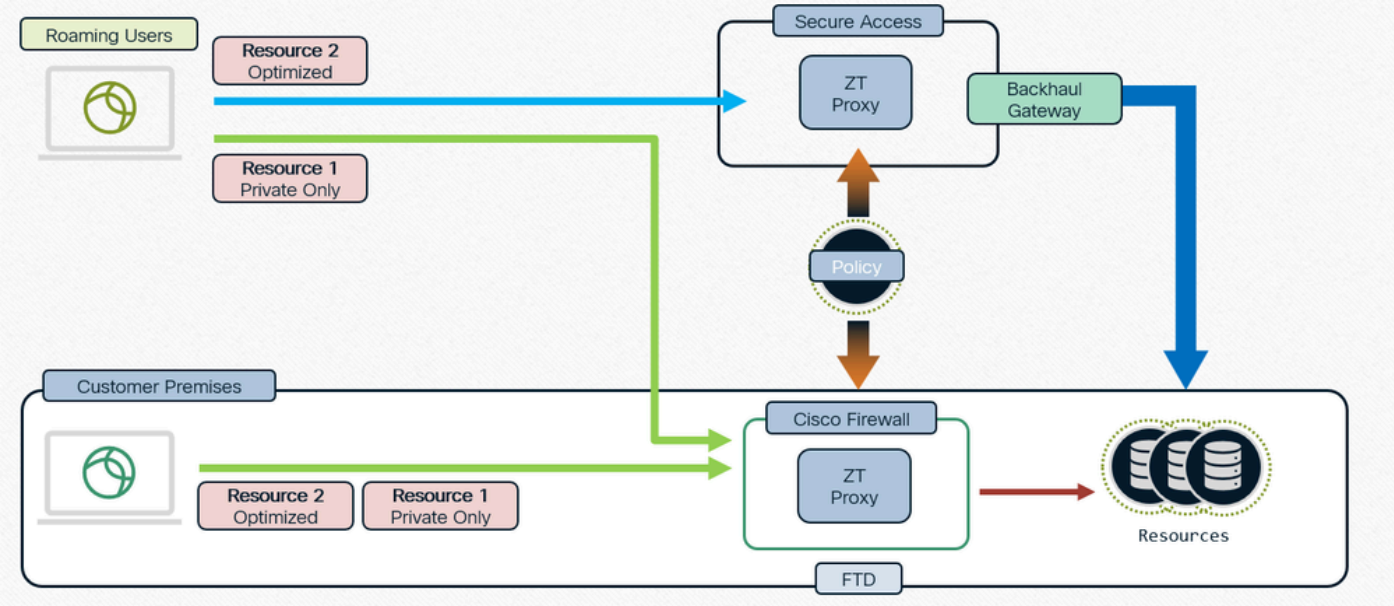
uZTNA(Universal Zero Trust Network Access)는 관리자가 사용자 ID(사용자 신뢰 및 상태 포함)에 따라, 그리고 RA-VPN에서와 같이 전체 네트워크에 대한 액세스 권한을 부여하지 않고 내부 네트워크 리소스에 대한 액세스를 구체적으로 허용할 수 있게 합니다. uZTNA를 통해 관리자는 원격 및 온

프레미스 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.

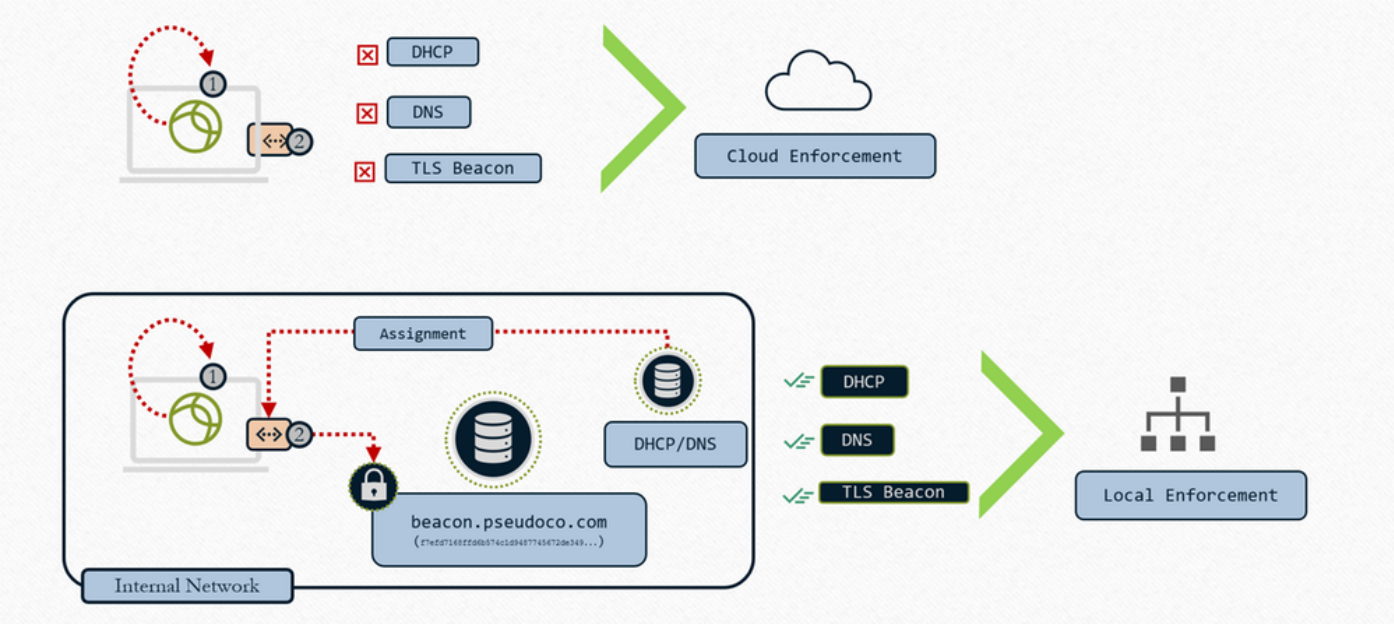
트래픽 프록시는 물론 IPS, 파일 및 악성코드 정책 시행은 FTD(Firepower Threat Defense)에서 수행됩니다.



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.

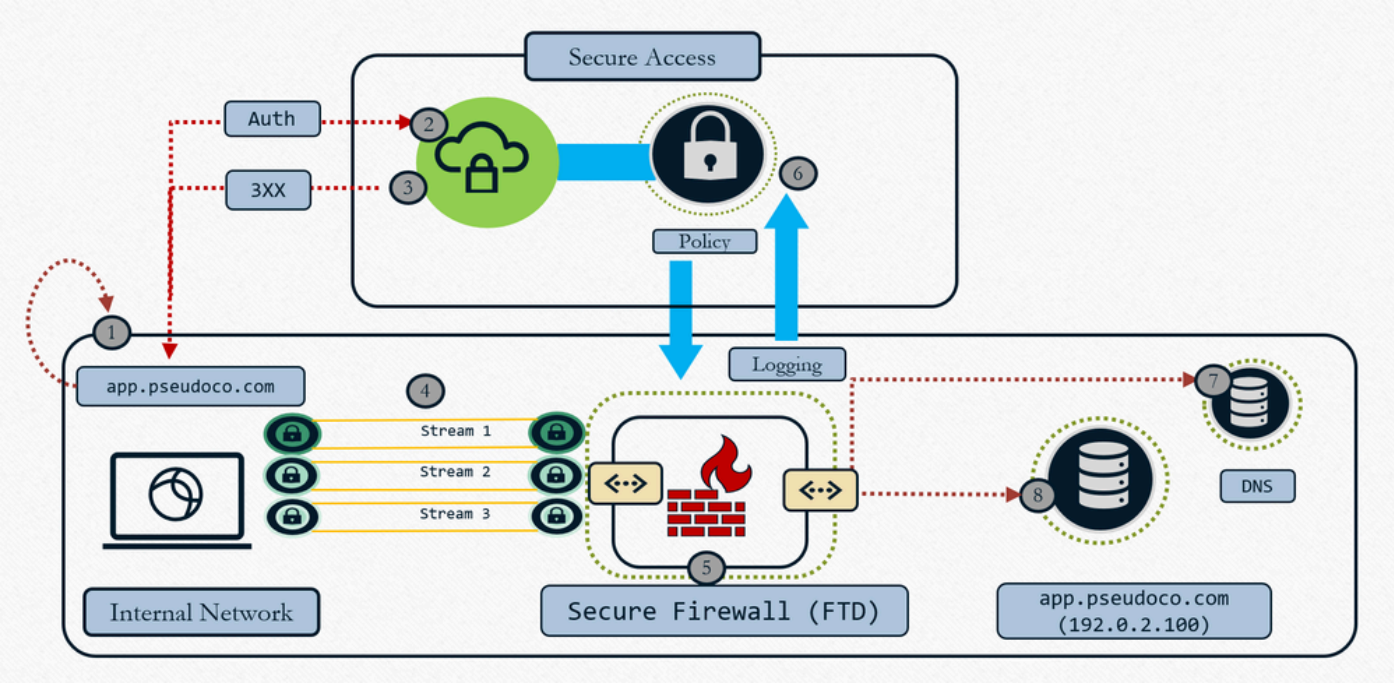
3- 조건이 일치하는 경우 - 로컬 시행

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 온펌인지 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

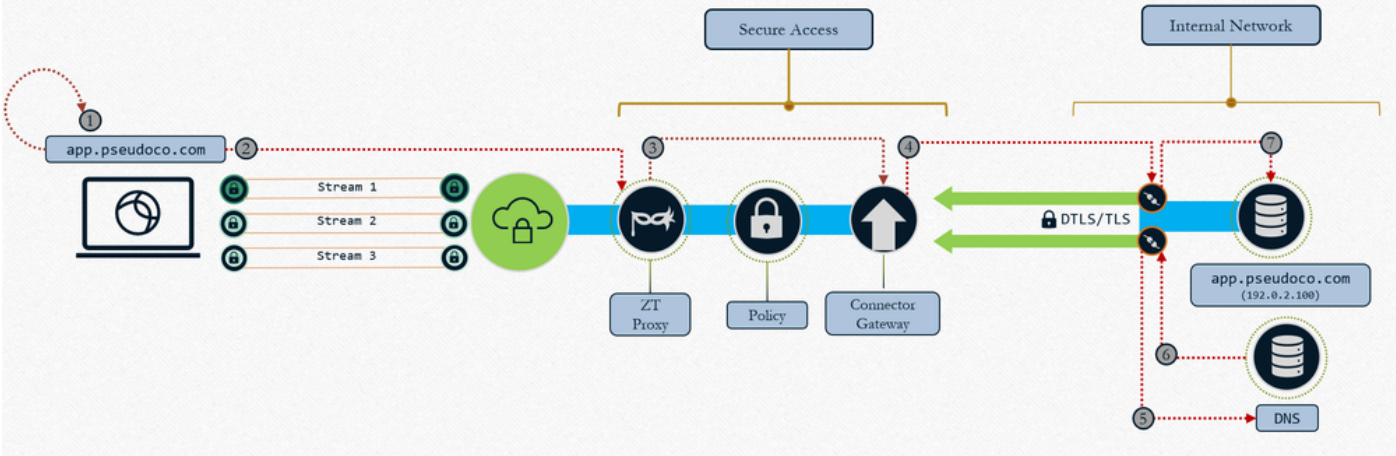
- 로컬 적용 경로: 방화벽 시행



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 클라우드에 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

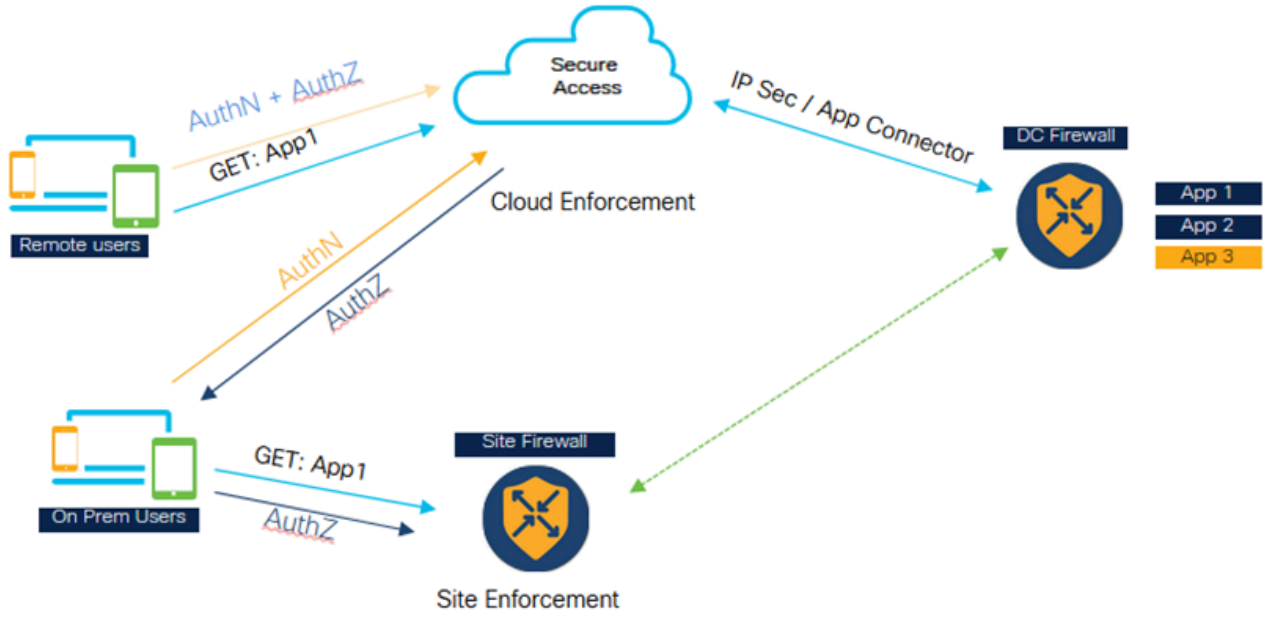


범용 ZTNA: 클라우드 시행

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

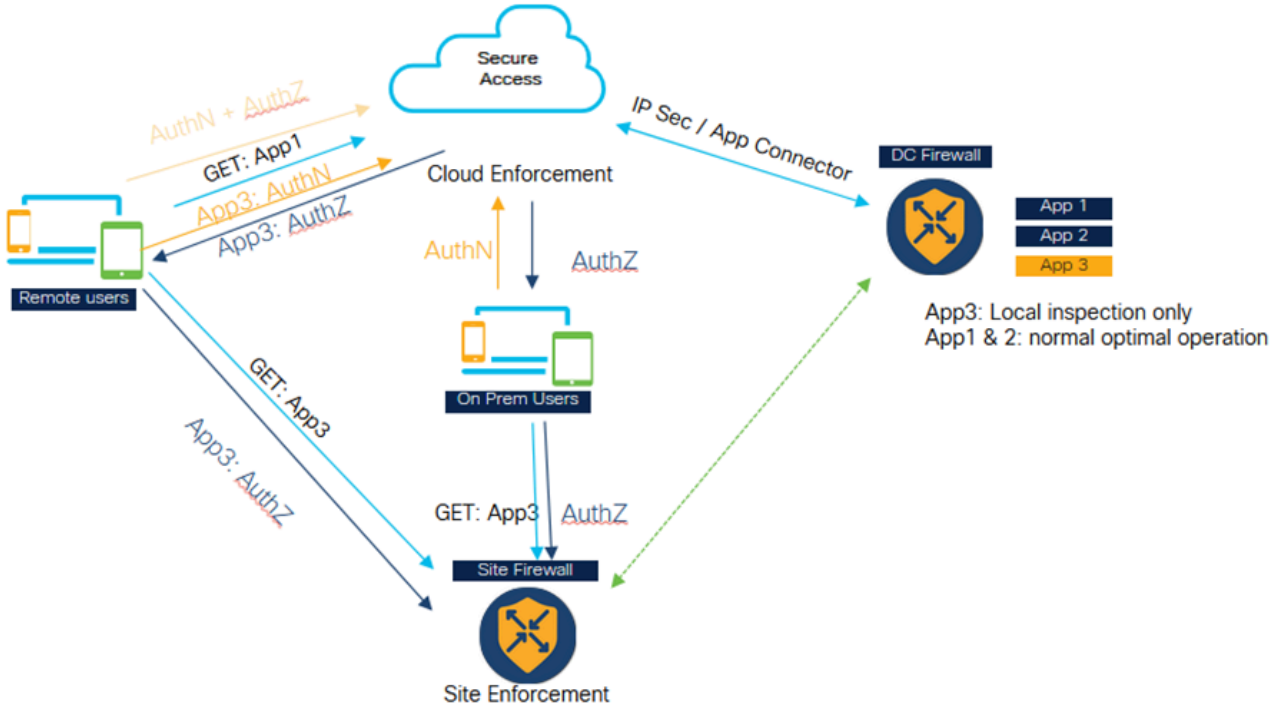
사례 1: 구내형 사용자를 위한 일관되고 최적화된 ZTNA



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

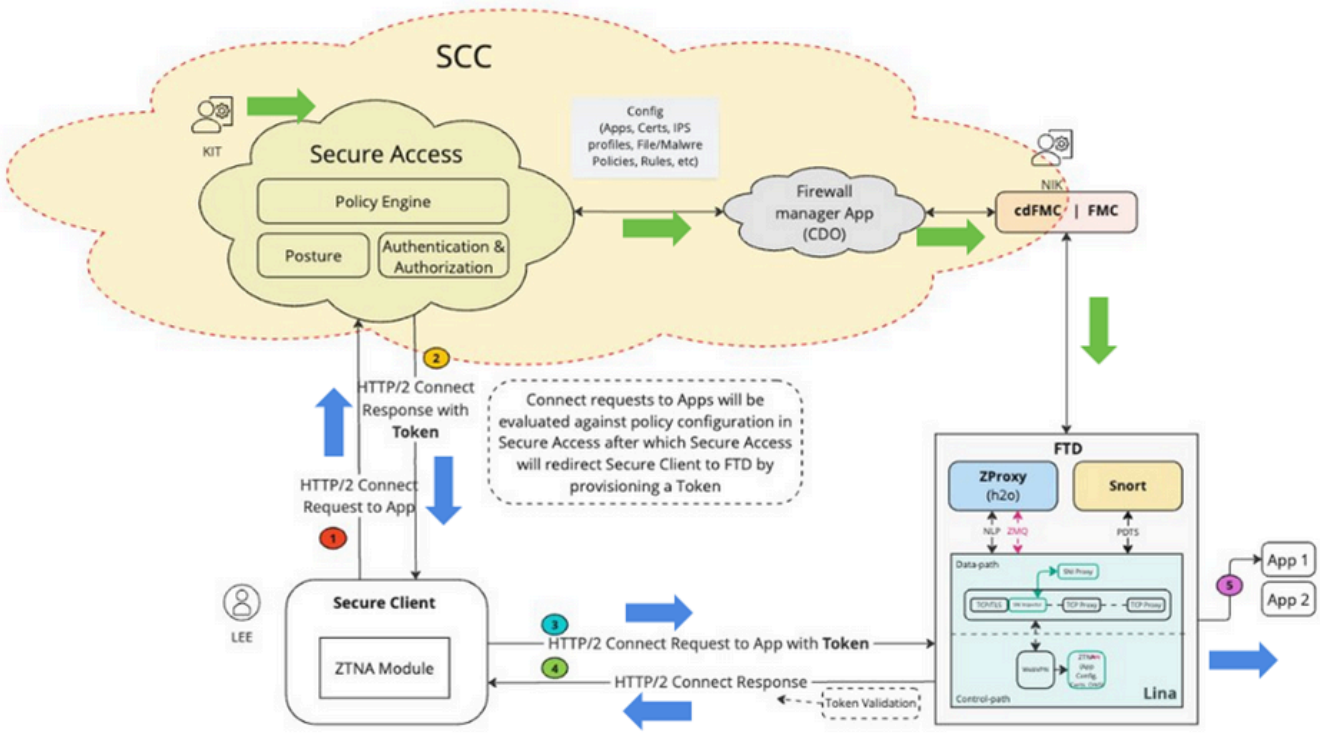
사례 2: 민감한 애플리케이션에 대한 비공개 검사



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 온펌 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

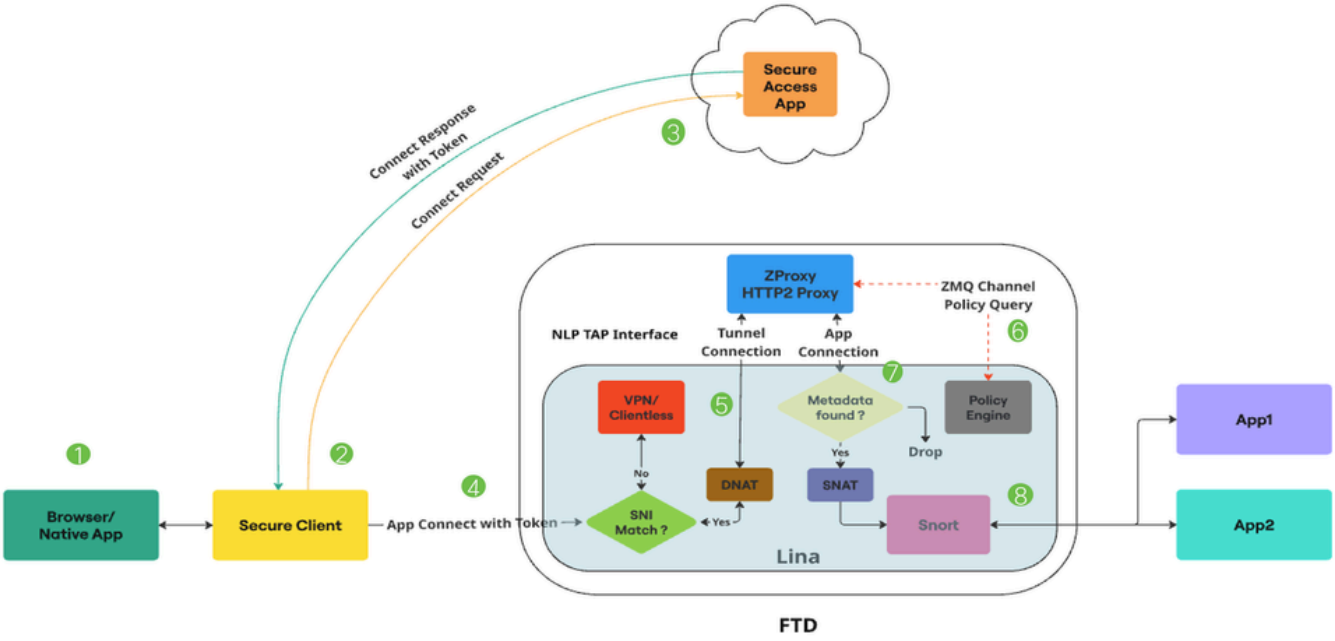
3. Secure Access는 인증 토큰과 함께 FTD로 보안 클라이언트를 리디렉션합니다.

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 플로우

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

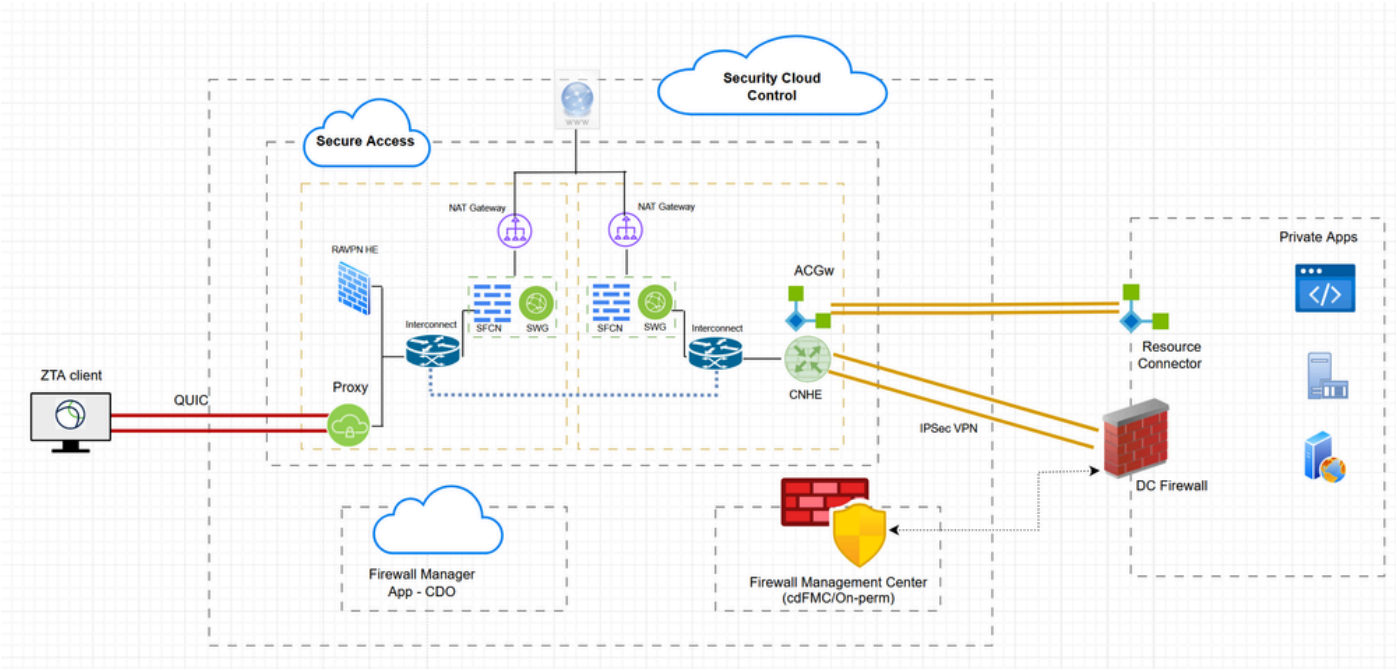
8. 앱 연결은 ZProxy에서 시작되므로 내부 IP(예:169.251.1.2)가 소스 IP로 사용됩니다. 이는 FTD 이그레스 인터페이스 IP로 변환되어 전송됩니다. 그런 다음 Lina는 파일 또는 IPS 정책이 액세스 토큰에 있는 경우에만 Snort 검사에 대해 Universal Zero Trust 흐름을 표시합니다. 액세스 토큰에서 얻은 규칙 ID는 연결 메타데이터에서 Snort로 전달됩니다.

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

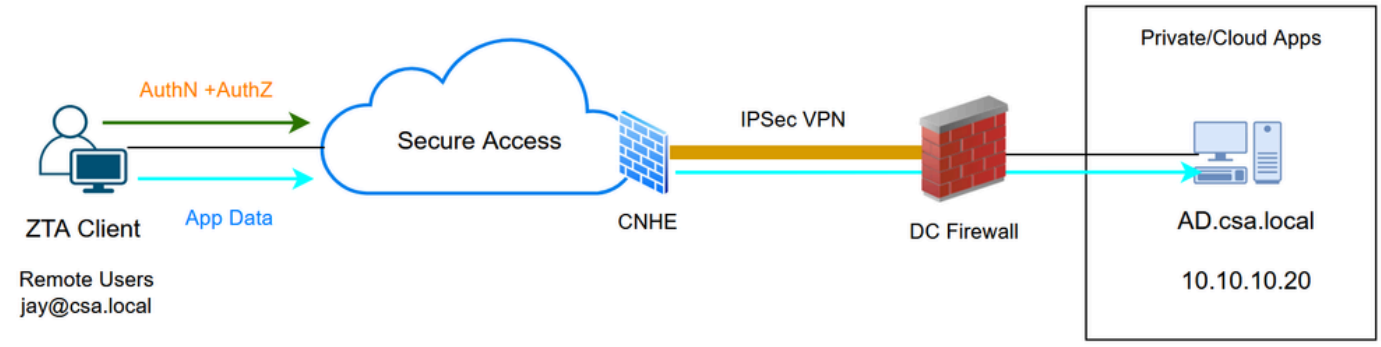


하이브리드 ZTNA - 네트워크 다이어그램

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 플로우는 ZTA 등록 클라이언트에서 Network Tunnel Group 또는 Resource Connector를 통해 사설 애플리케이션에 액세스할 수 있는 일반적인 흐름입니다

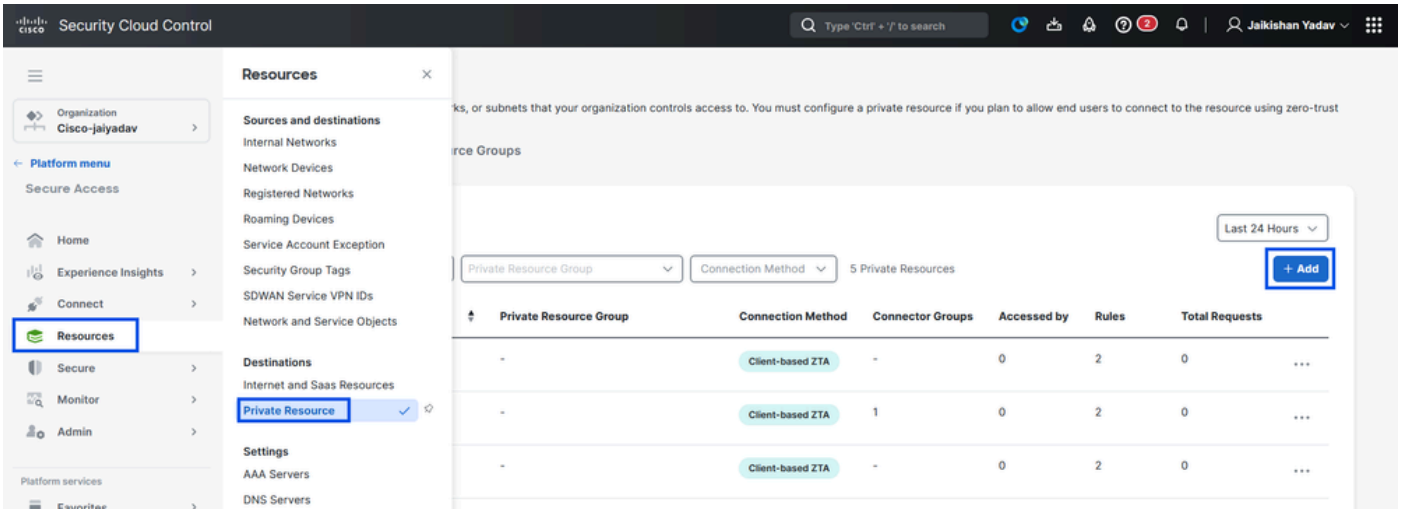


범용 ZTA - 테스트 사례 토폴로지

1단계 - Secure Access에서 프라이빗 리소스 정의

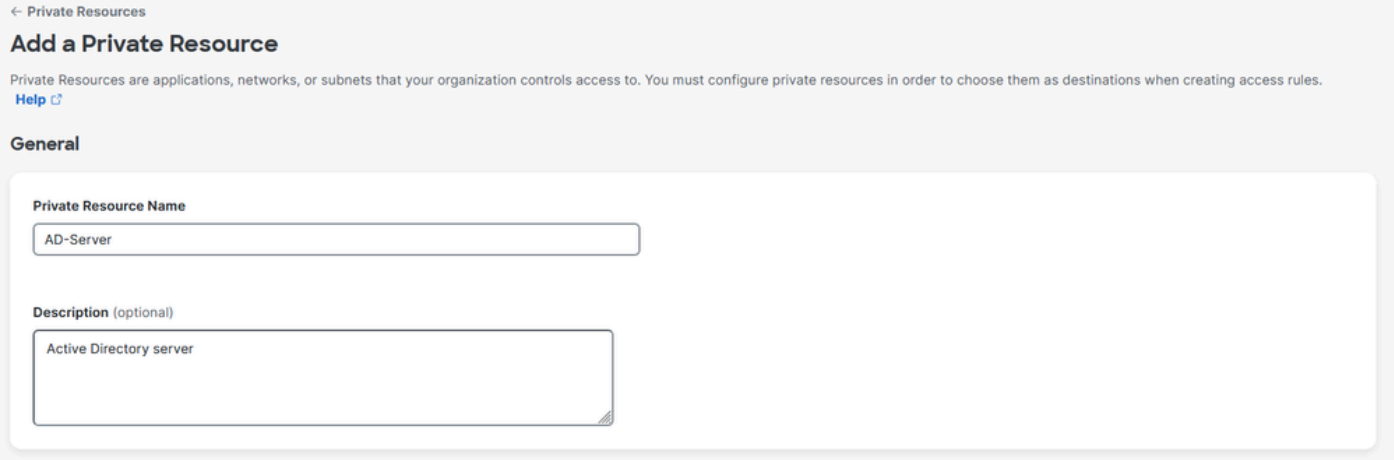
클라우드 시행으로 ZTA(Zero Trust Access) 등록된 디바이스를 통해 액세스할 수 있는 프라이빗 리소스 구성

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



보안 액세스 - 프라이빗 리소스 컨피그레이션

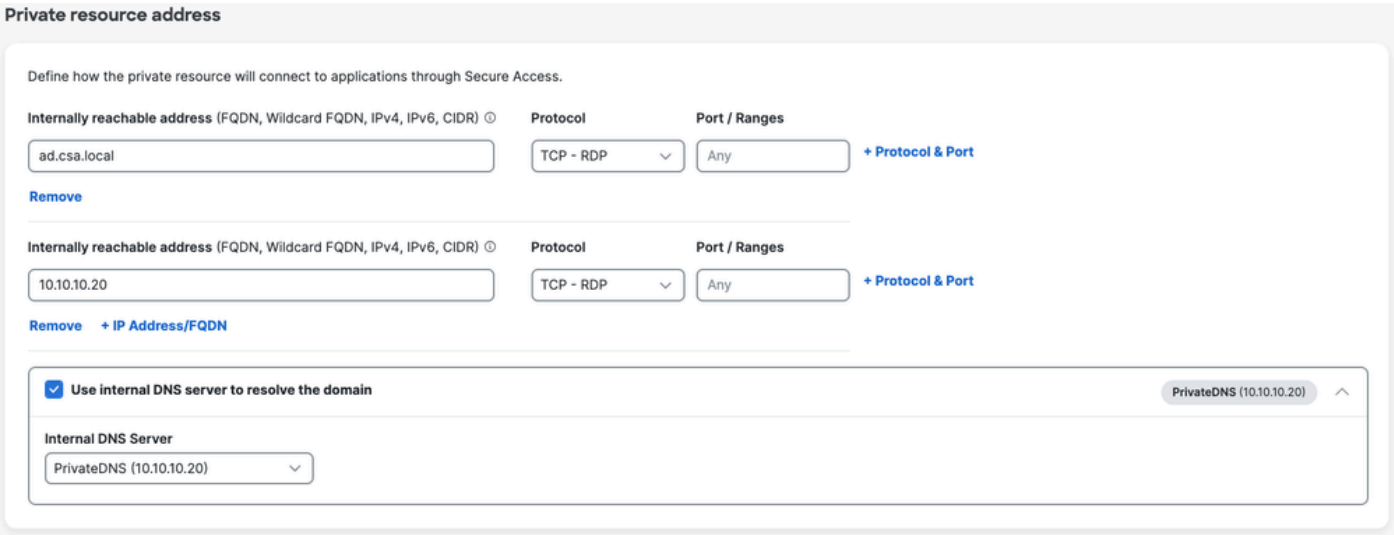
2. 개인 자원명에는 유의미한 자원명을 입력합니다. 설명의 경우, 리소스의 용도 또는 리소스 소유자의 이름과 같은 정보를 제공하는 것이 좋습니다.



보안 액세스 - 프라이빗 리소스 컨피그레이션

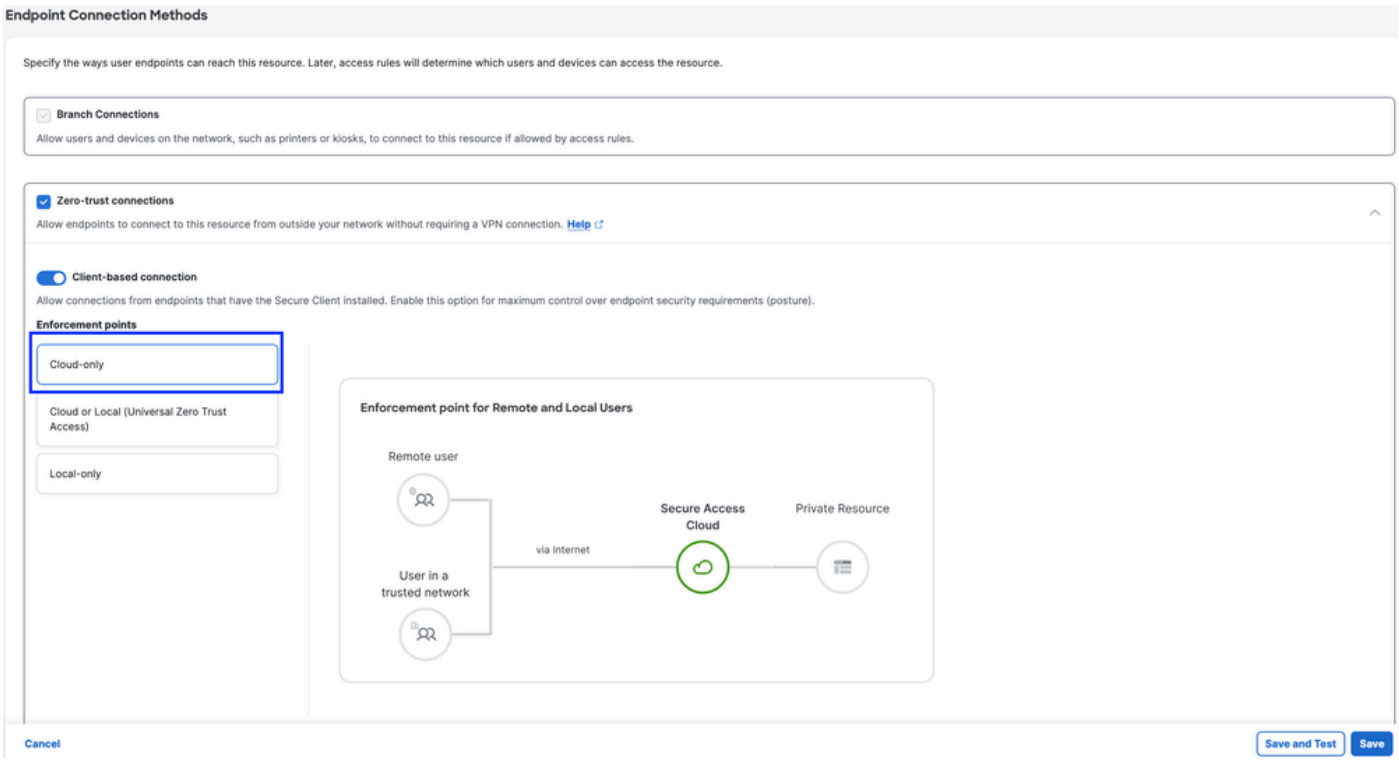
3. 액세스하려는 개인 자원의 FQDN을 입력합니다. 프라이빗 리소스의 IP 주소도 정의할 수 있습니다. 자세한 내용은 프라이빗 리소스 추가를 참조하십시오

4. 도메인을 확인할 내부 DNS 서버를 선택합니다



보안 액세스 - 프라이빗 리소스 컨피그레이션

5. 엔드포인트 연결 방법 선택



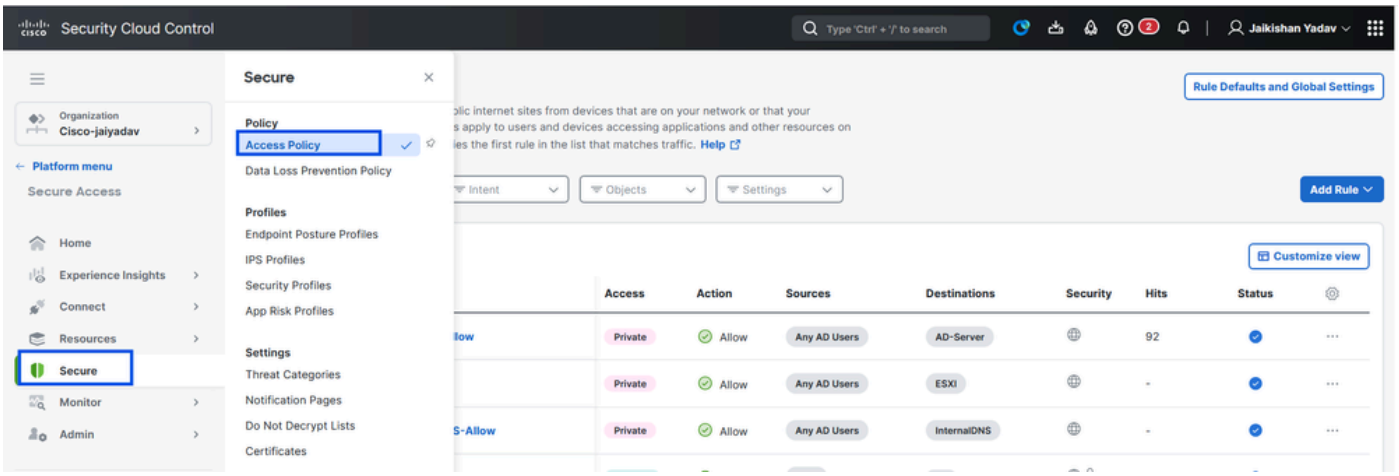
보안 액세스 - 프라이빗 리소스 컨피그레이션

6. Save(저장)를 클릭합니다.

2단계 - 개인 액세스 규칙 생성

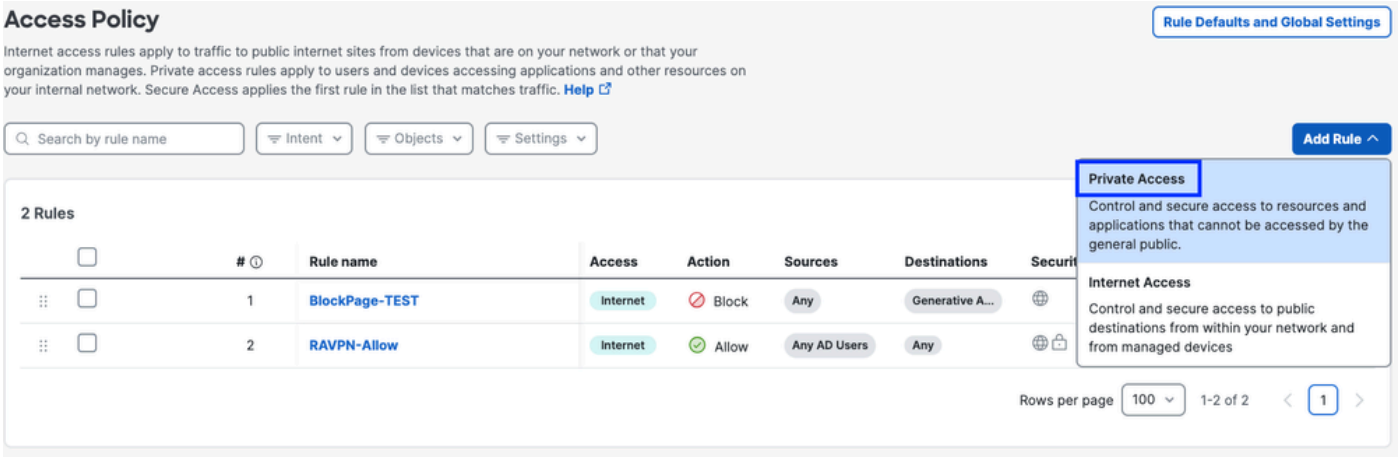
Universal ZTA 등록된 사용자가 액세스할 수 있도록 Secure Access의 비공개 액세스를 구성합니다. 자세한 내용은 개인 액세스 규칙을 참조하십시오

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



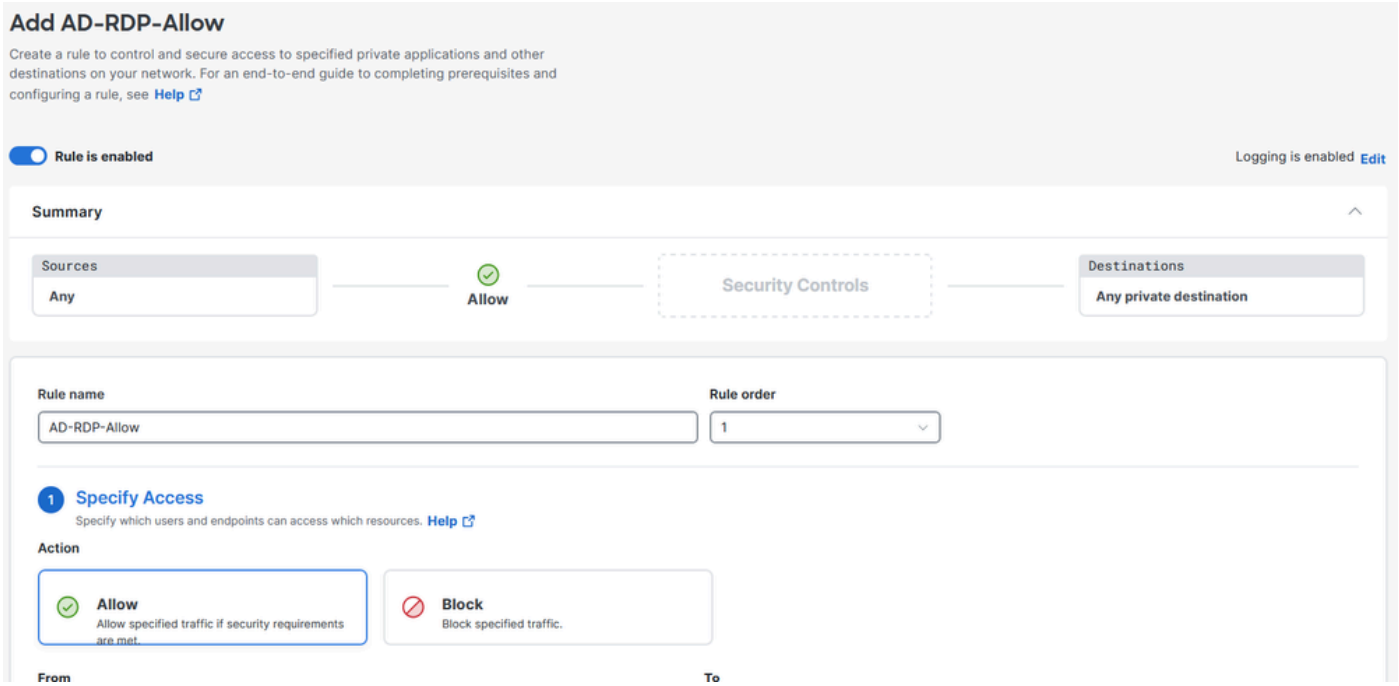
보안 액세스 - 액세스 정책 컨피그레이션

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



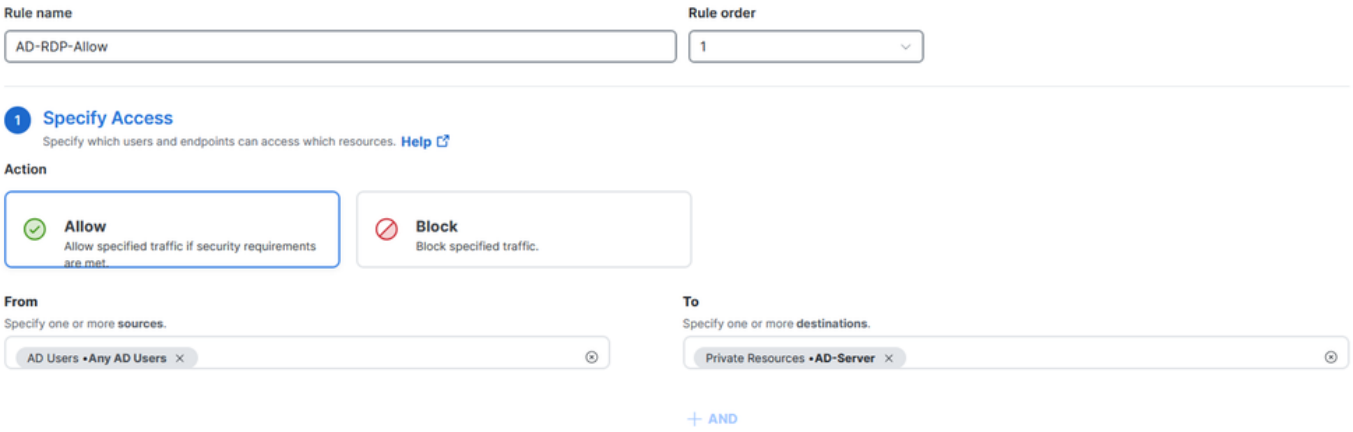
보안 액세스 - 액세스 정책 컨피그레이션

3. 규칙 이름 추가



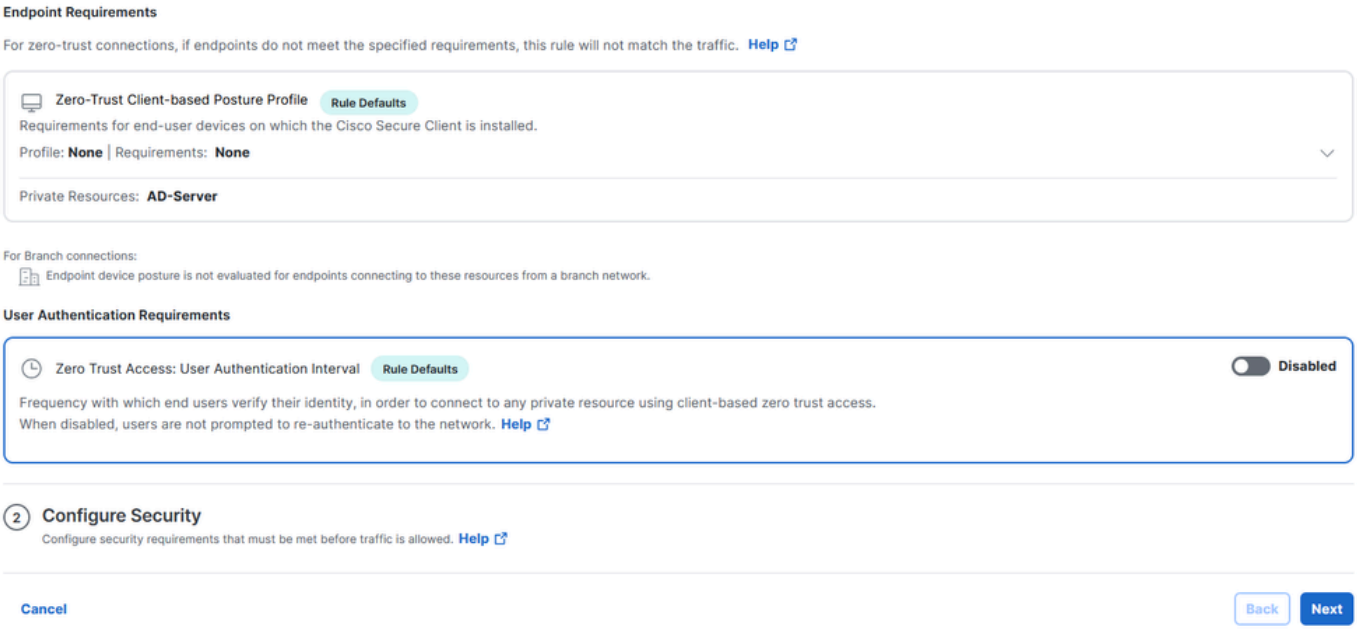
보안 액세스 - 액세스 정책 컨피그레이션

4. 규칙 조치를 선택하고 출처 및 대상을 선택합니다



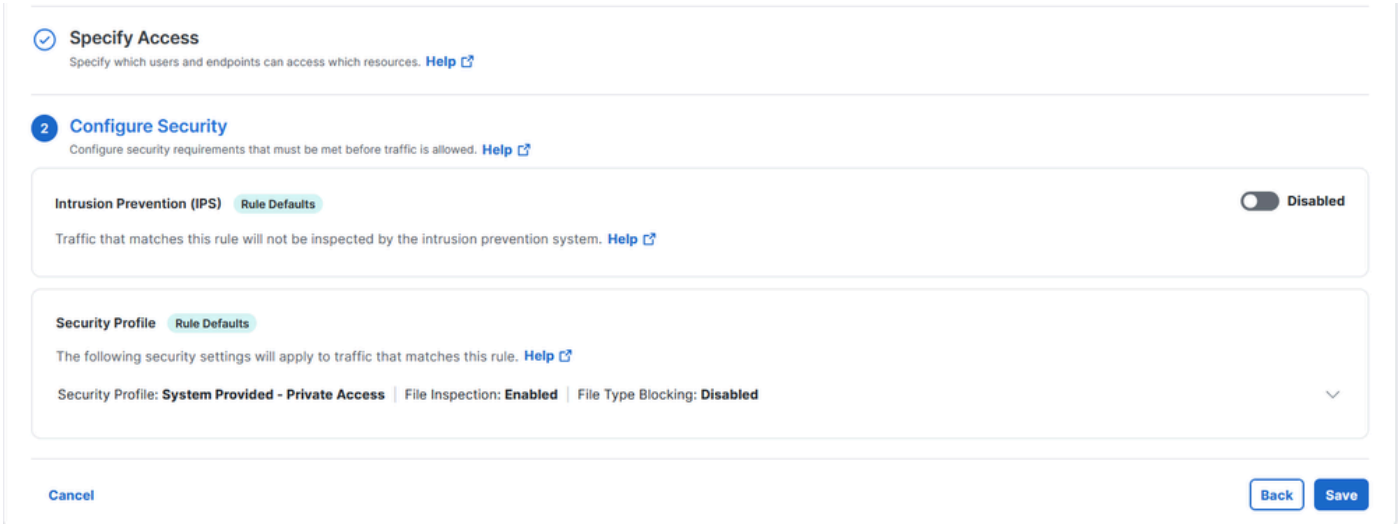
보안 액세스 - 액세스 정책 컨피그레이션

5. 엔드포인트 요구 사항 구성



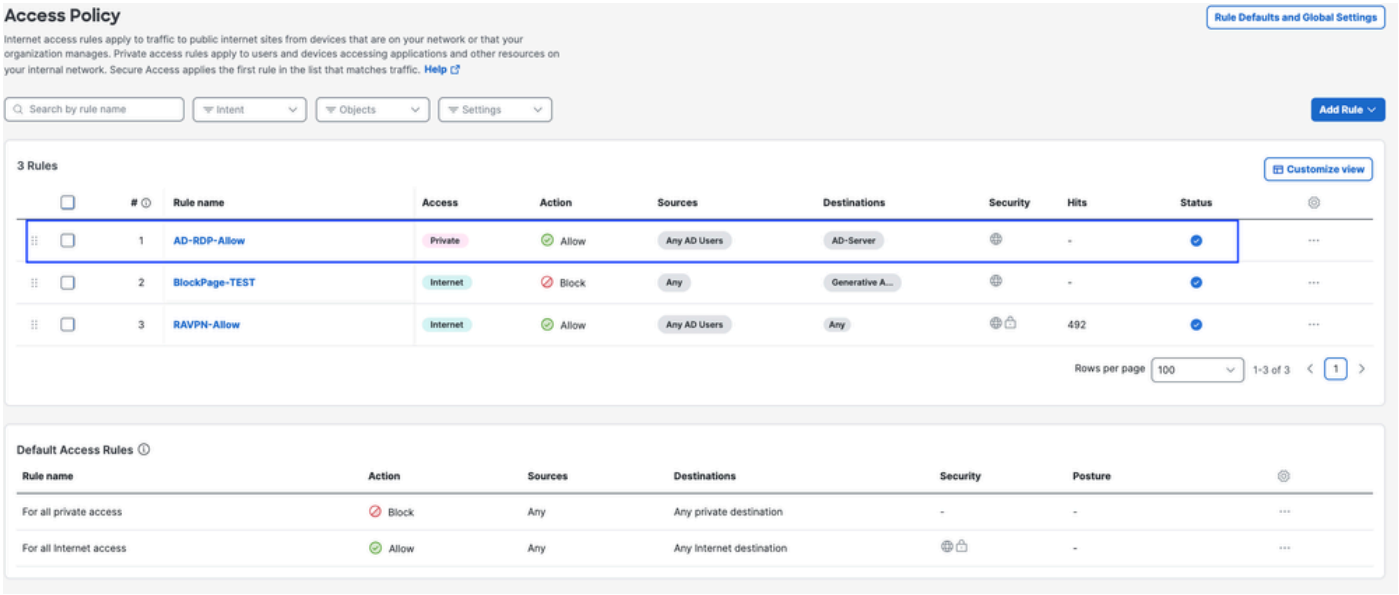
보안 액세스 - 액세스 정책 컨피그레이션

6. 보안 구성



보안 액세스 - 액세스 정책 컨피그레이션

7. 저장을 클릭합니다.

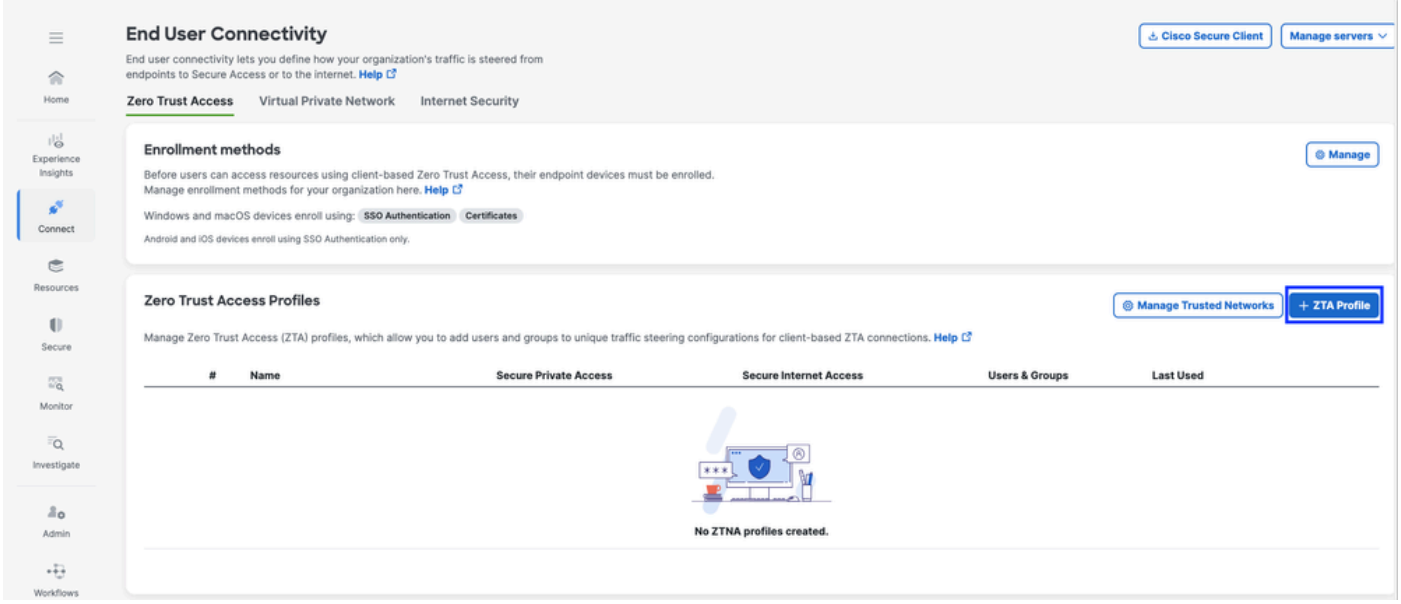


보안 액세스 - 액세스 정책 컨피그레이션

단계 - 3 ZTA 프로필에 프라이빗 리소스 추가

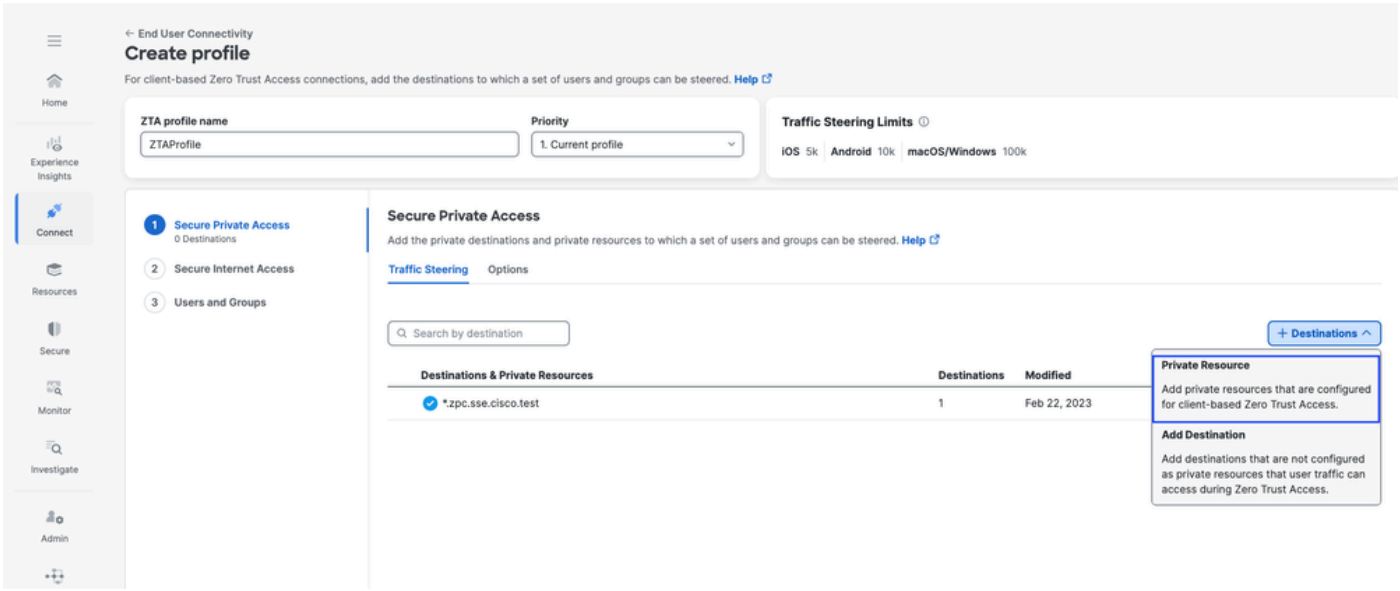
사용자 지정 ZTA 프로필을 사용 중인 경우 ZTA 프로필에 개별 개인 리소스를 추가해야 합니다

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

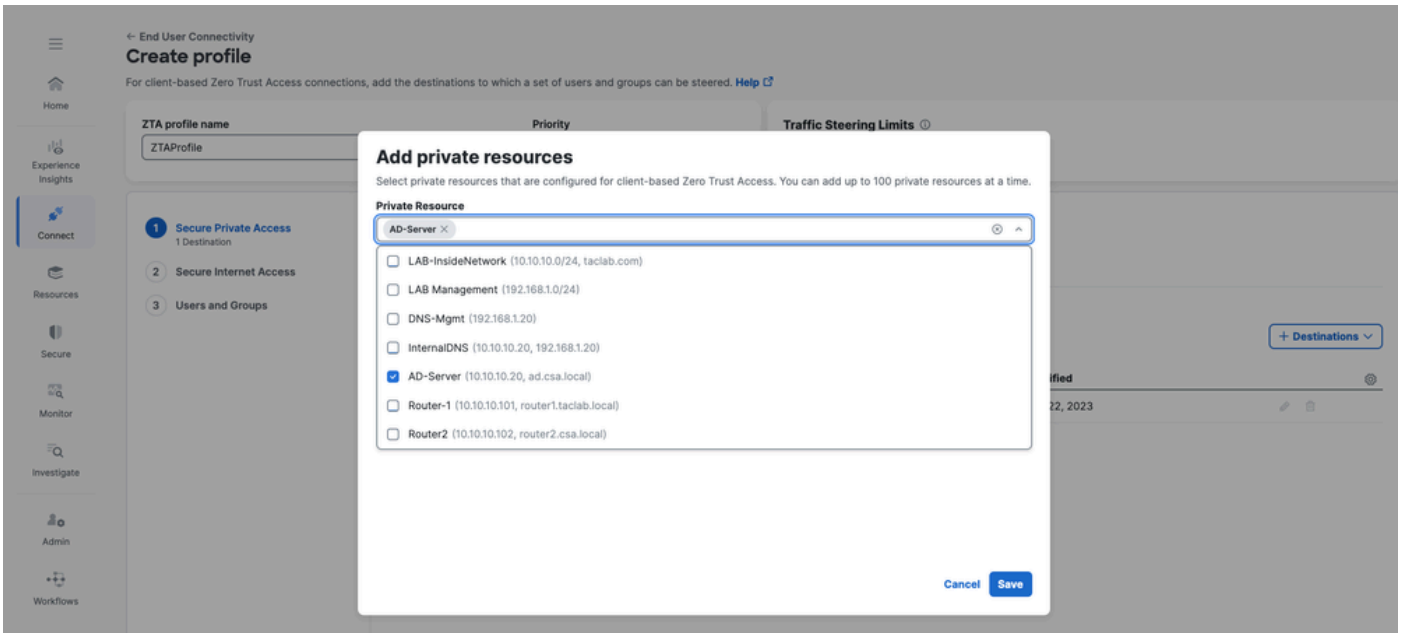


보안 액세스 - ZTA 프로필

2. 프라이빗 리소스 추가

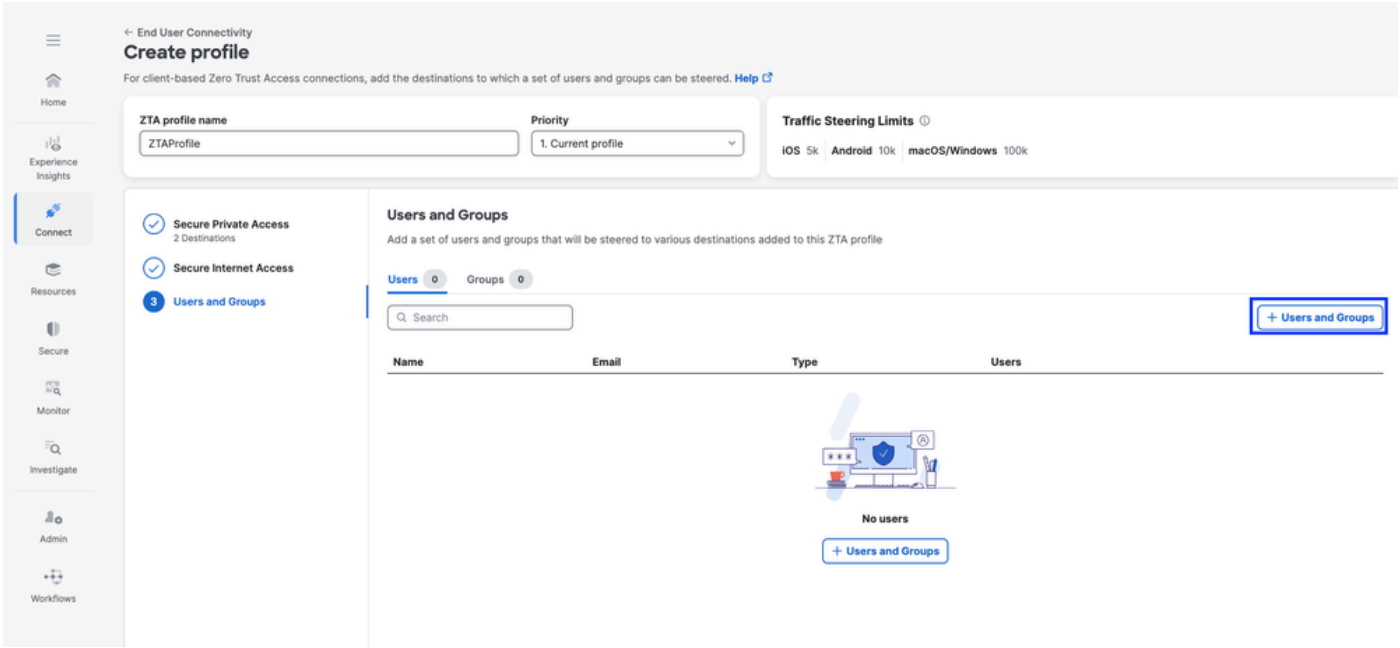


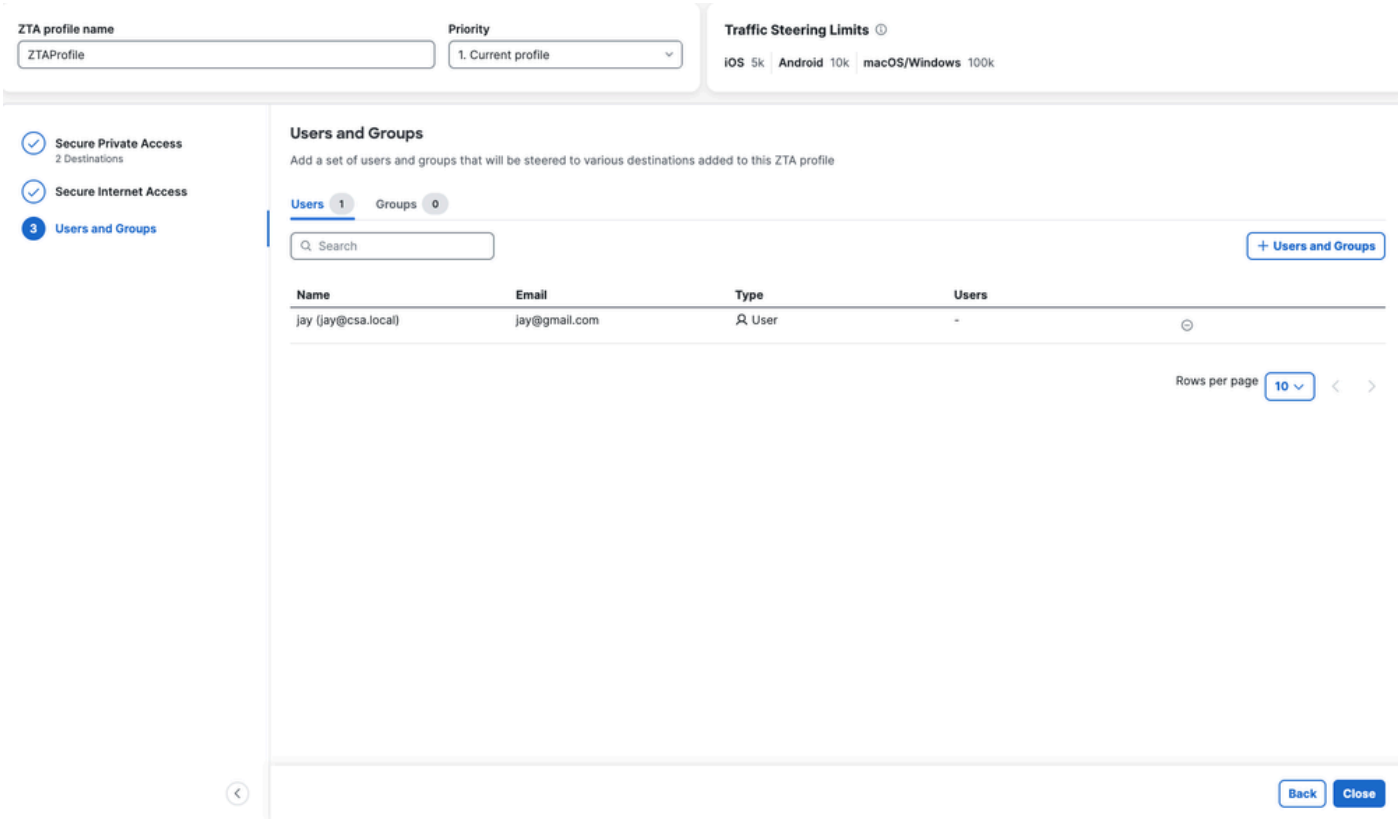
보안 액세스 - ZTA 프로필



보안 액세스 - ZTA 프로필

3 . 사용자 및 그룹 추가





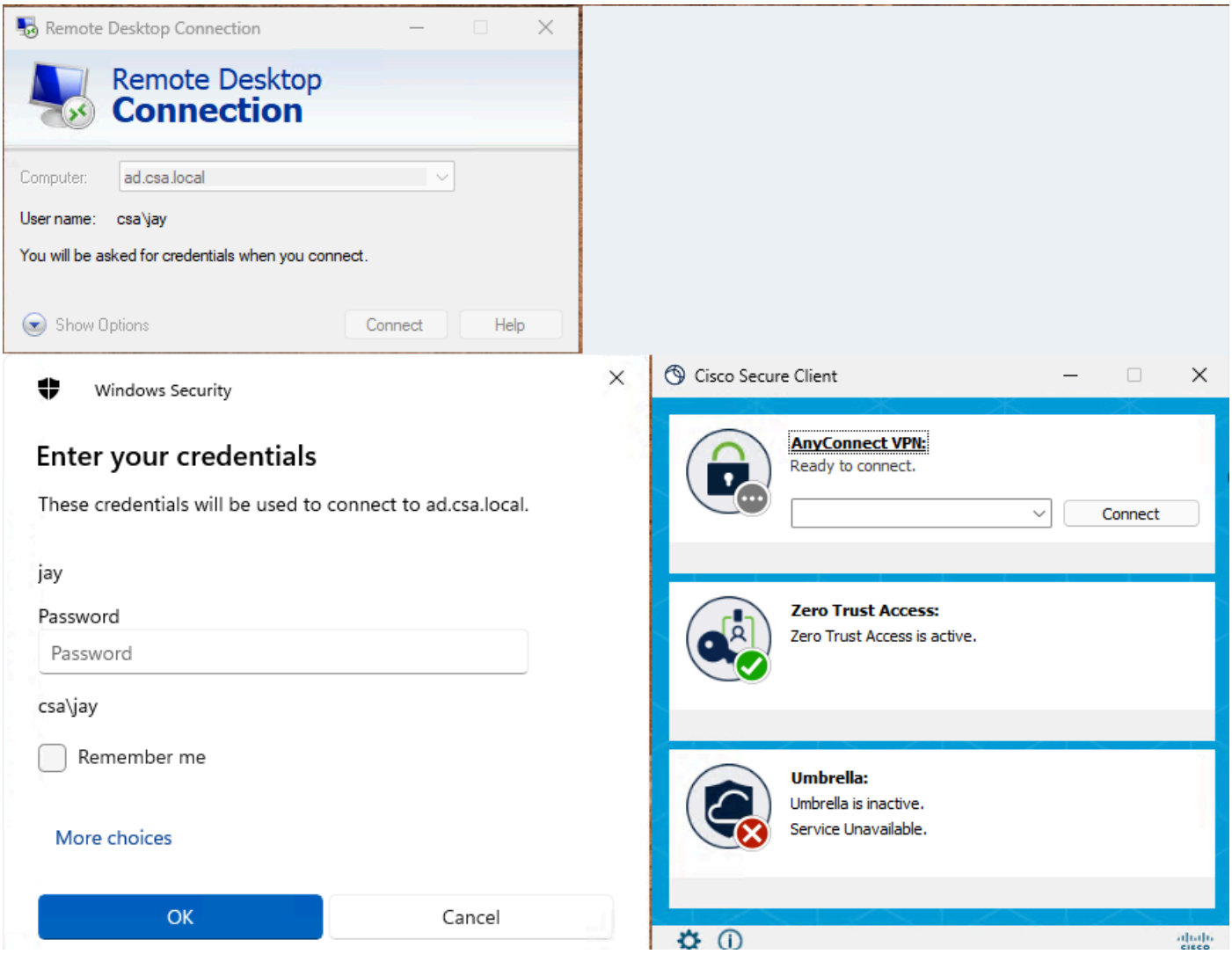
보안 액세스 - ZTA 프로필

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

단계 - 4 Private Resource에 대한 액세스 확인

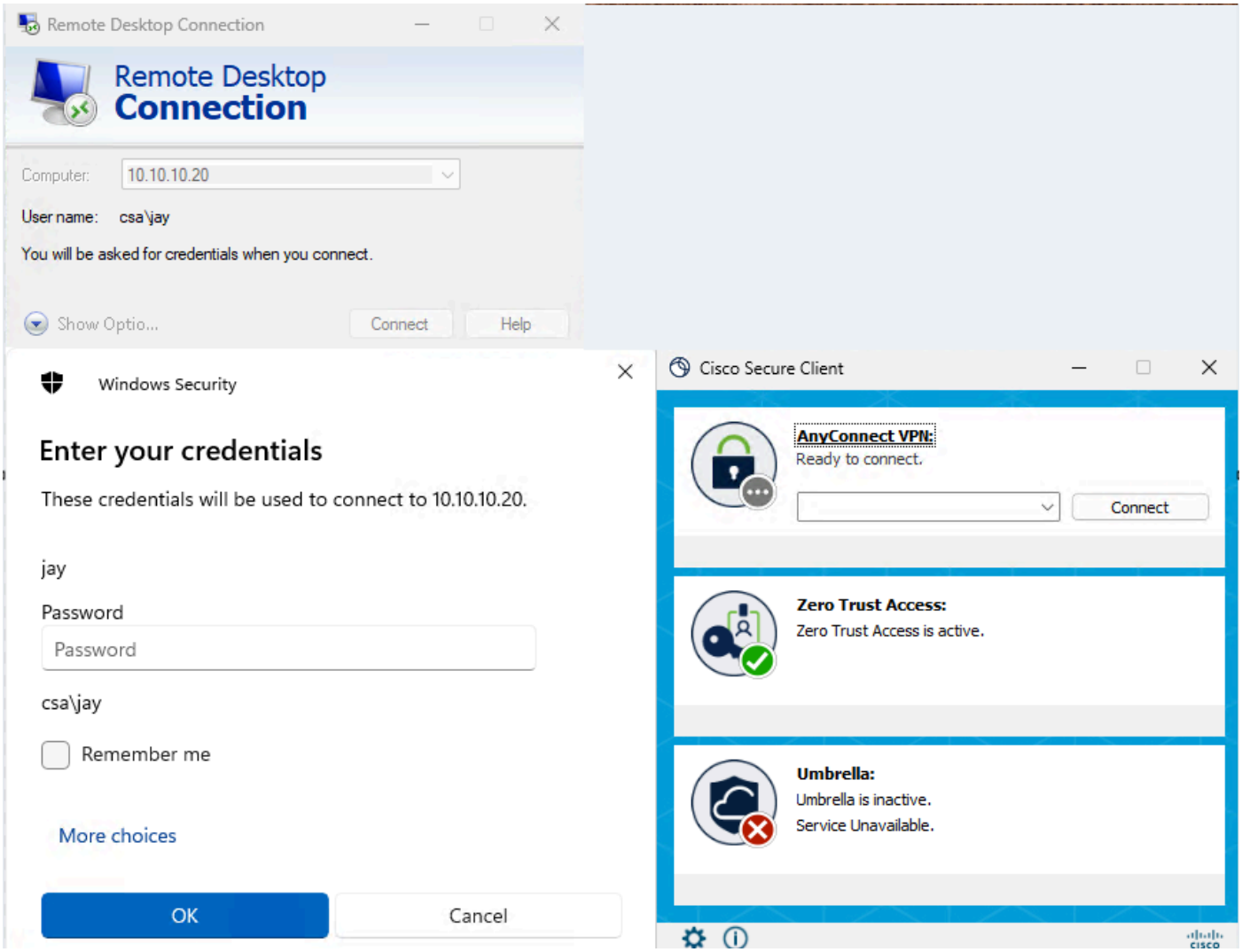
1. 프라이빗 리소스 액세스

FQDN을 사용하여 PR 액세스



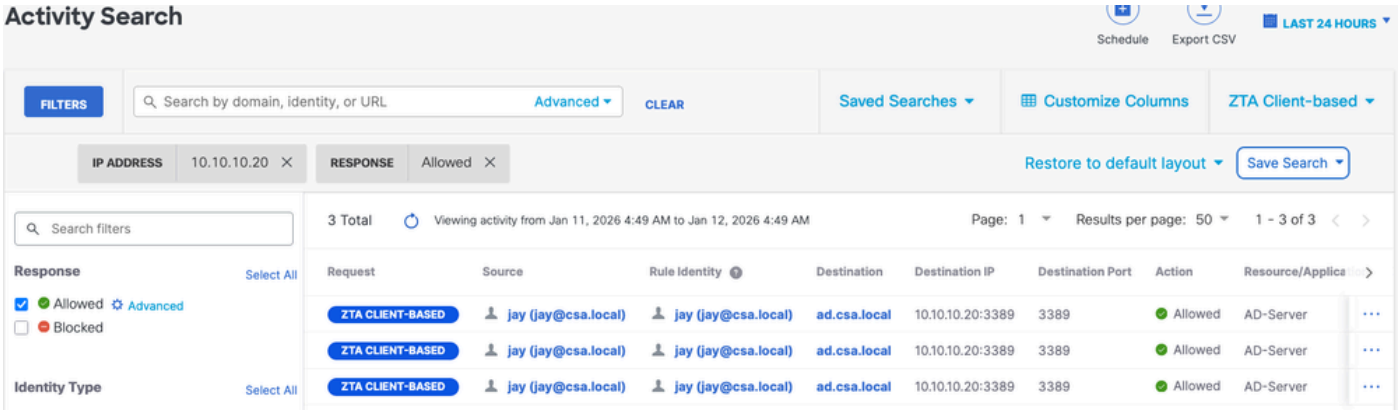
보안 액세스 - PR 테스트

IP 주소를 사용하여 PR에 액세스

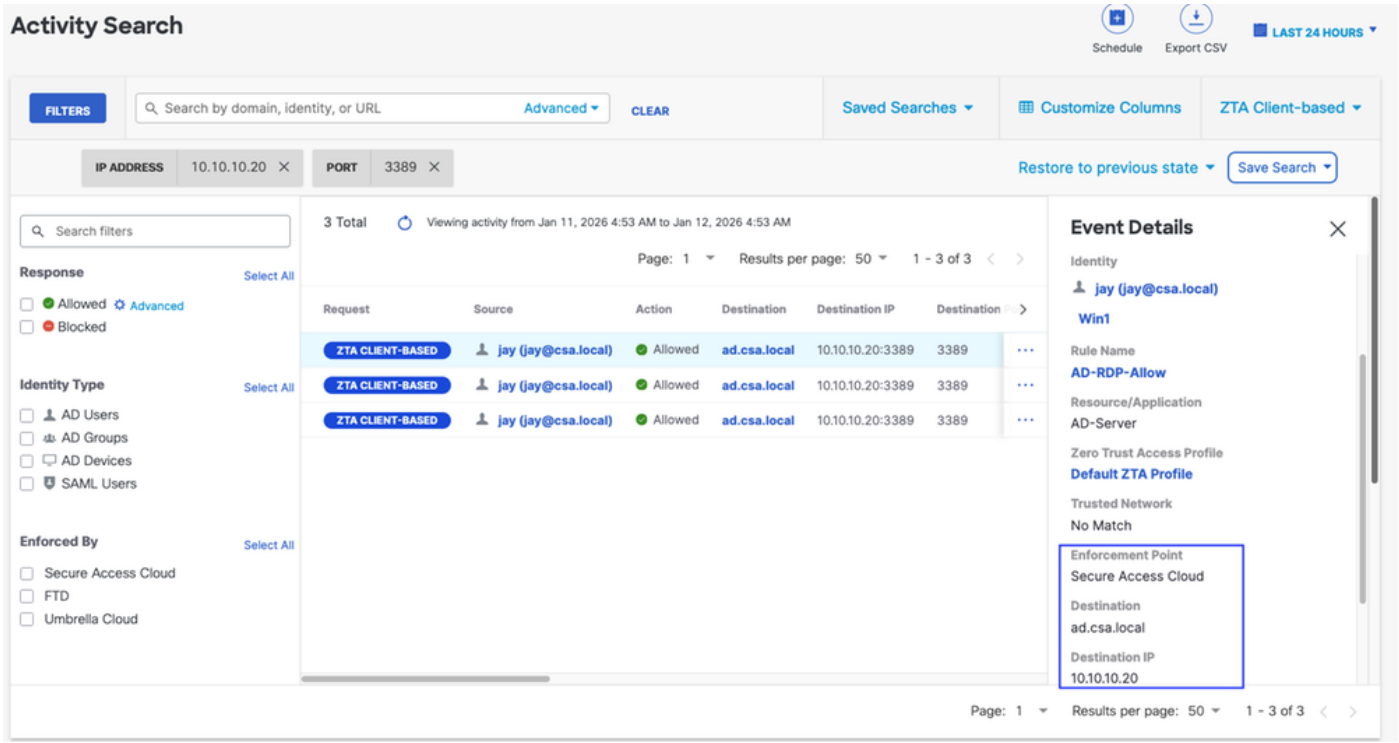


보안 액세스 - PR 테스트

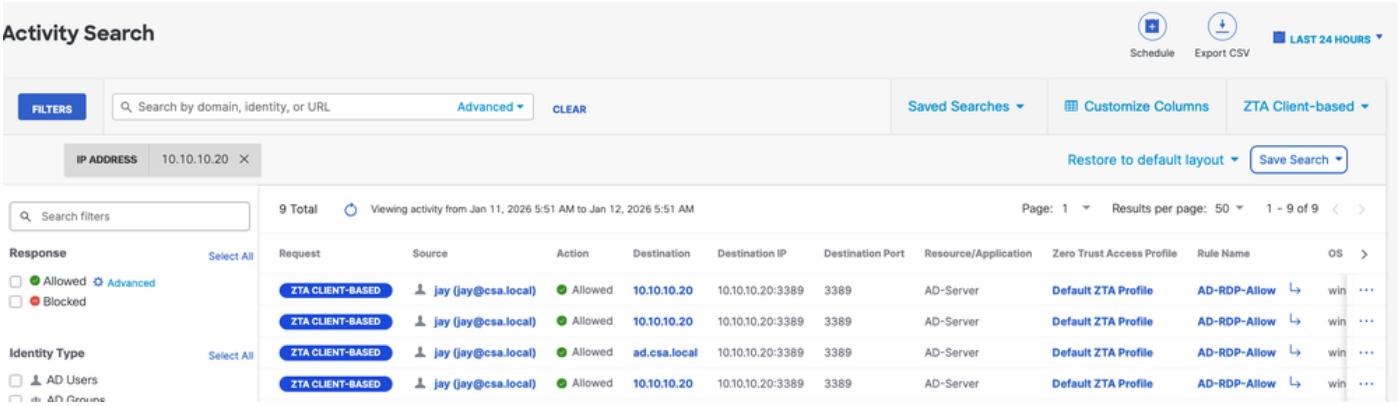
2. 활동 검색 이벤트로 확인합니다.



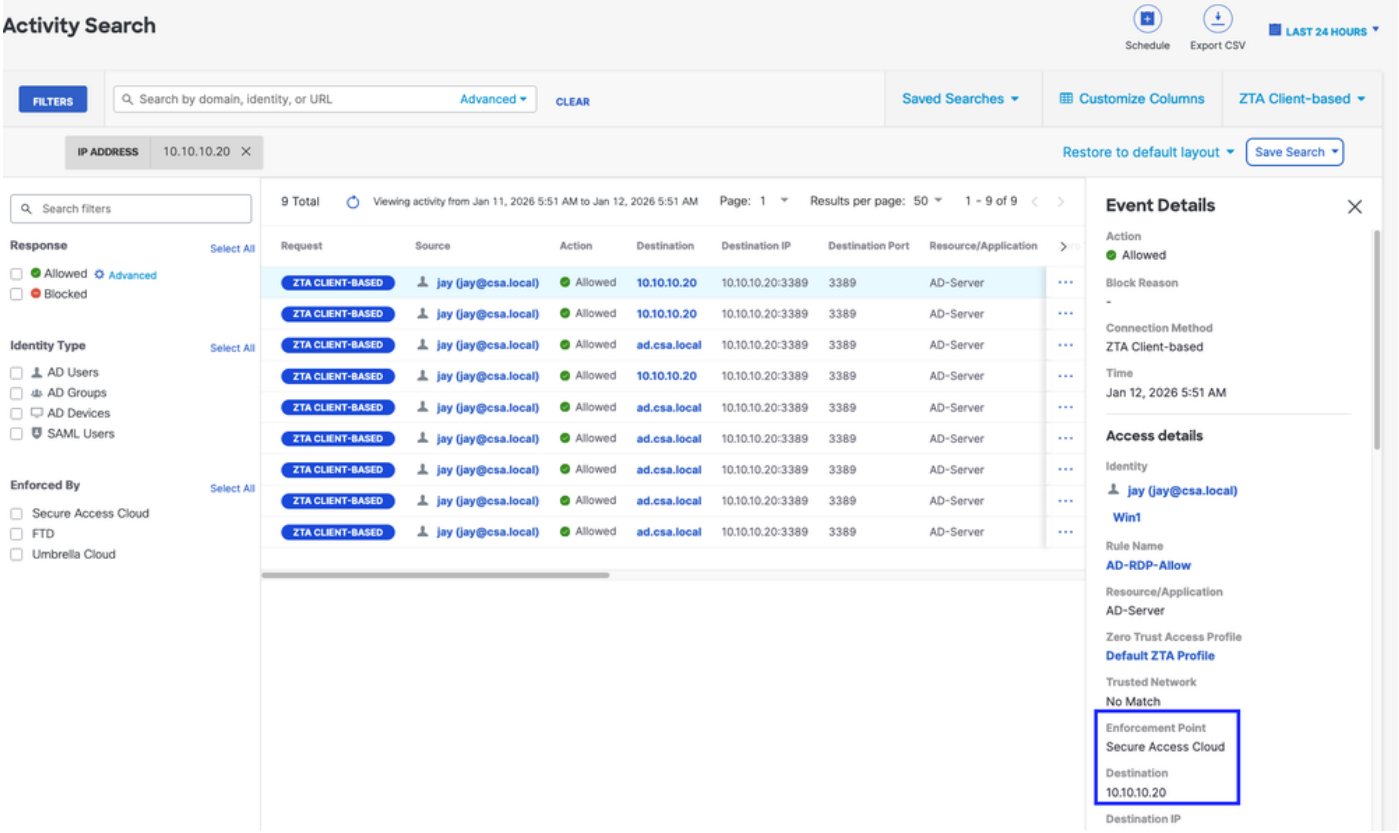
보안 액세스 - 활동 검색



보안 액세스 - 활동 검색

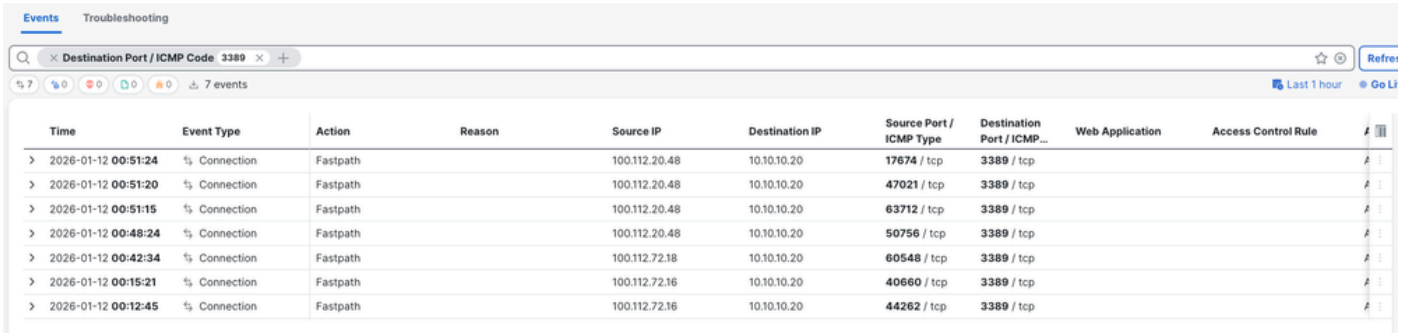


보안 액세스 - 활동 검색



보안 액세스 - 활동 검색

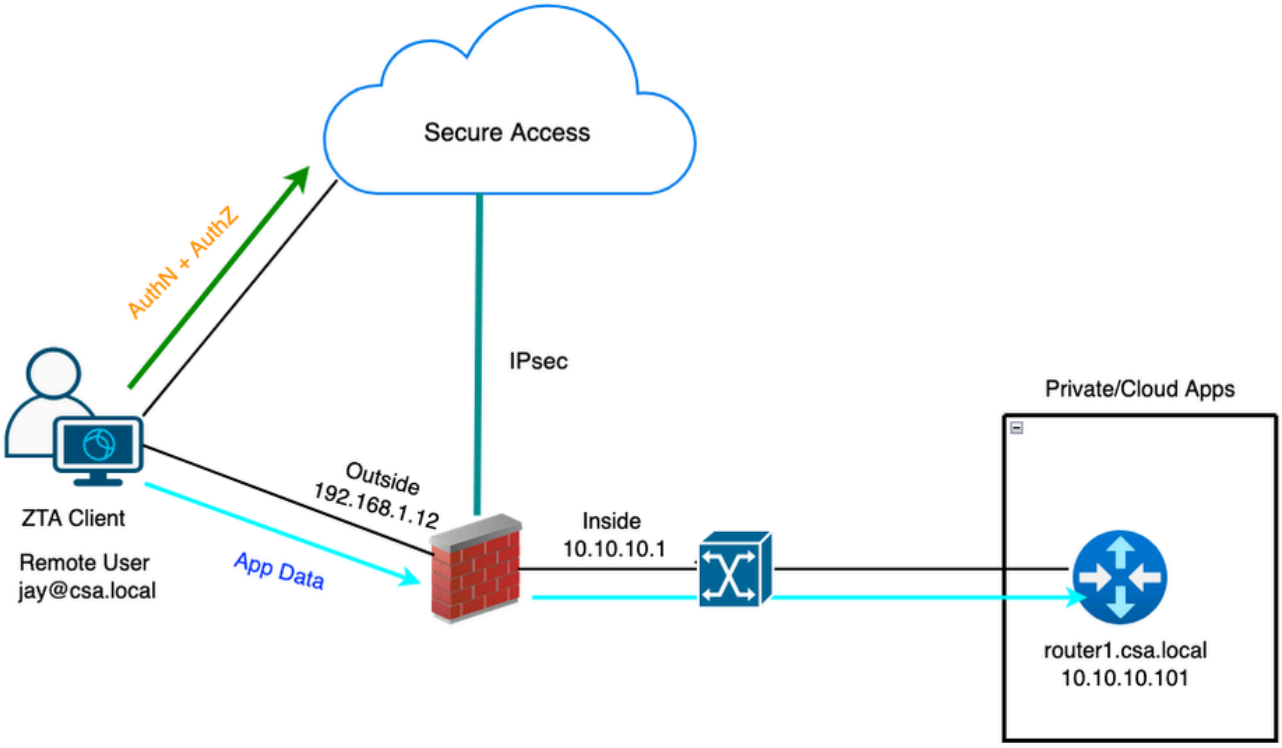
3. FMC 연결 이벤트 확인



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.

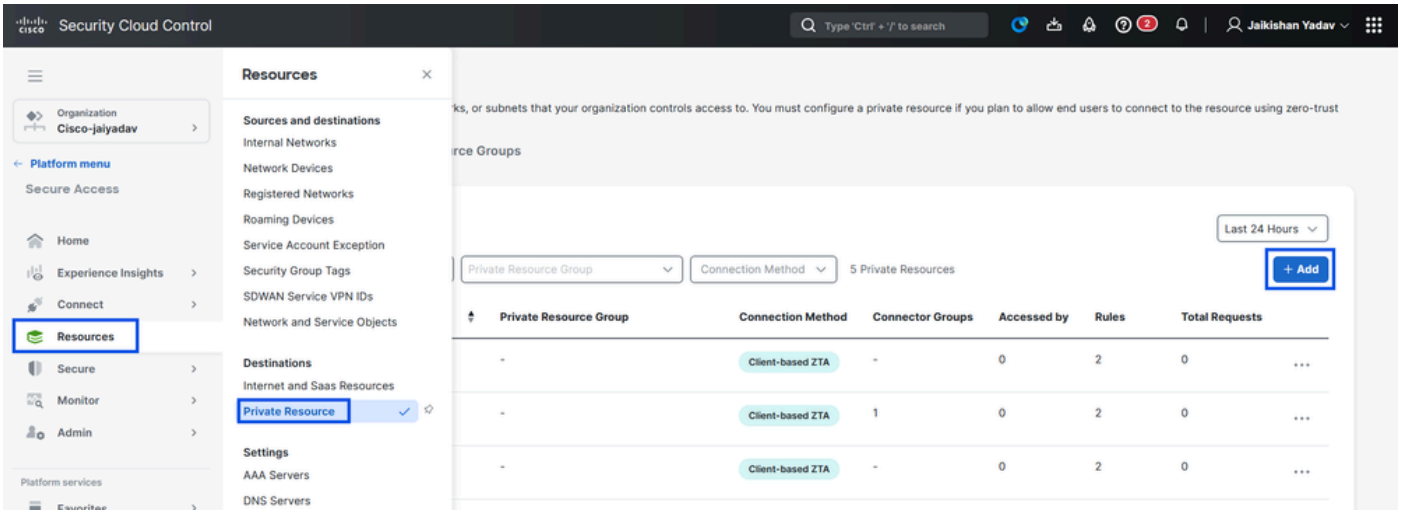


범용 ZTA - 테스트 사례 토폴로지

1단계 - Secure Access에서 프라이빗 리소스 정의

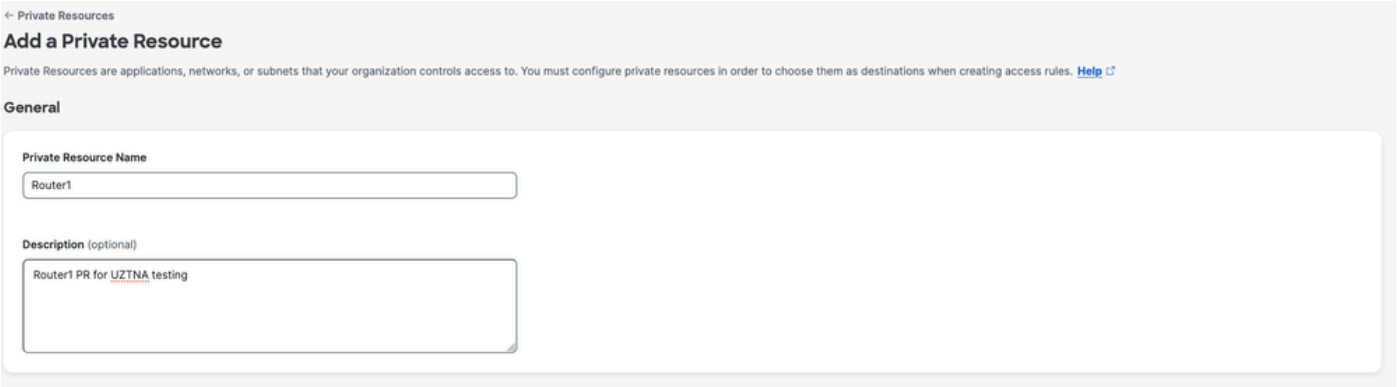
클라우드 시행으로 ZTA(Zero Trust Access) 등록된 디바이스를 통해 액세스할 수 있는 프라이빗 리소스 구성

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



보안 액세스 - 프라이빗 리소스 컨피그레이션

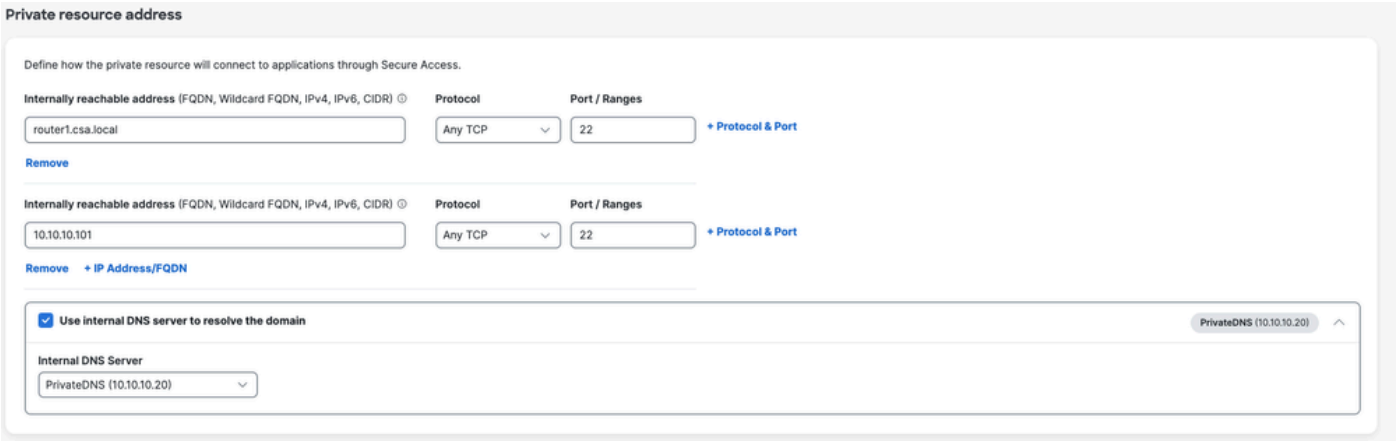
2. 개인 자원명에는 유의미한 자원명을 입력합니다. 설명의 경우, 리소스의 용도 또는 리소스 소유자의 이름과 같은 정보를 제공하는 것이 좋습니다.



보안 액세스 - 프라이빗 리소스 컨피그레이션

3. 액세스하려는 개인 자원의 FQDN을 입력합니다. 프라이빗 리소스의 IP 주소도 정의할 수 있습니다. 자세한 내용은 프라이빗 리소스 추가를 참조하십시오

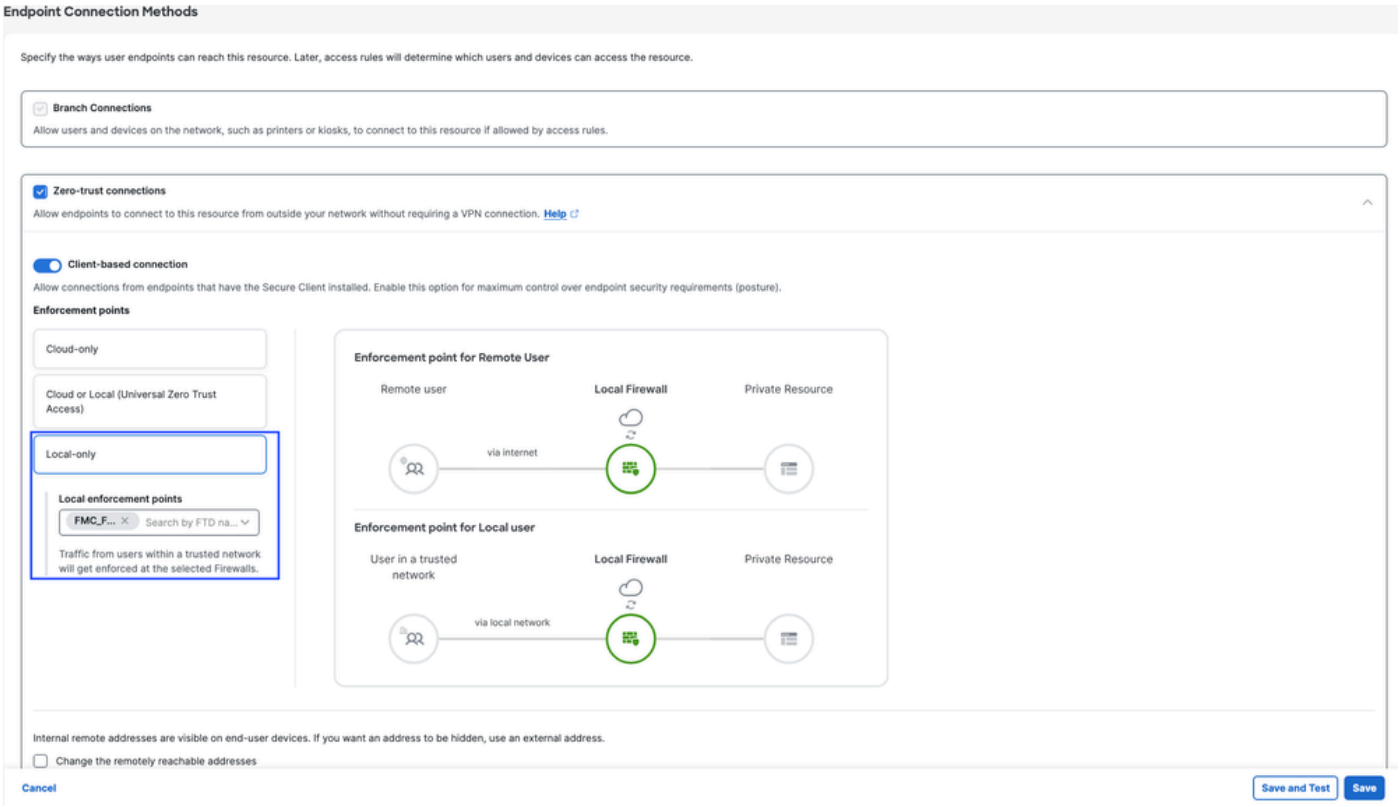
4. 도메인을 확인할 내부 DNS 서버를 선택합니다



보안 액세스 - 프라이빗 리소스 컨피그레이션

5. 엔드포인트 연결 방법 선택

6. FTD를 로컬 적용 지점으로 선택합니다



보안 액세스 - 프라이빗 리소스 컨피그레이션

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

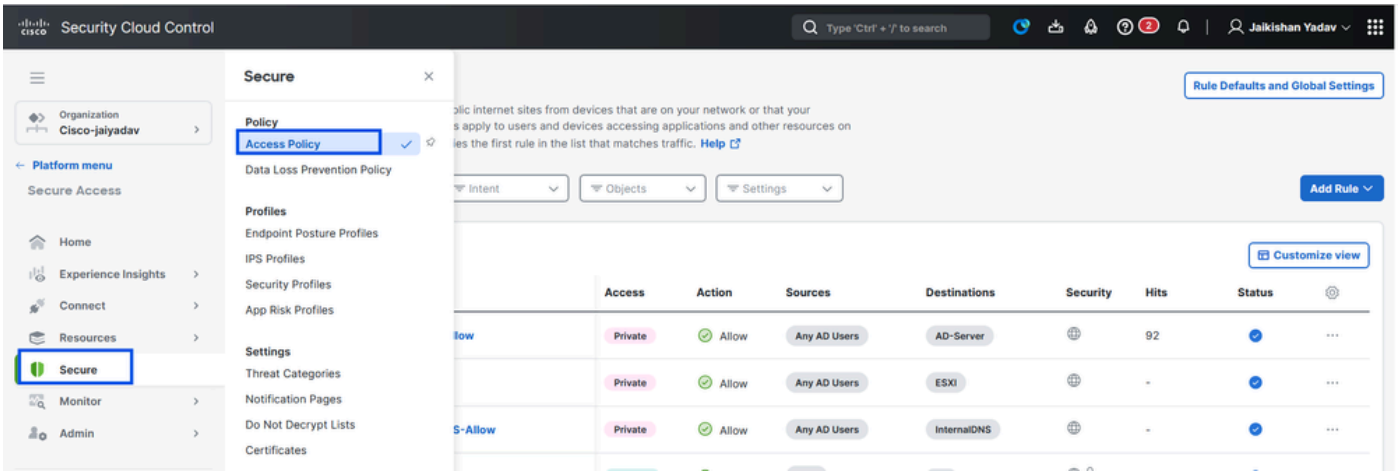
---

7 . Save(저장)를 클릭합니다.

2단계 - 개인 액세스 규칙 생성

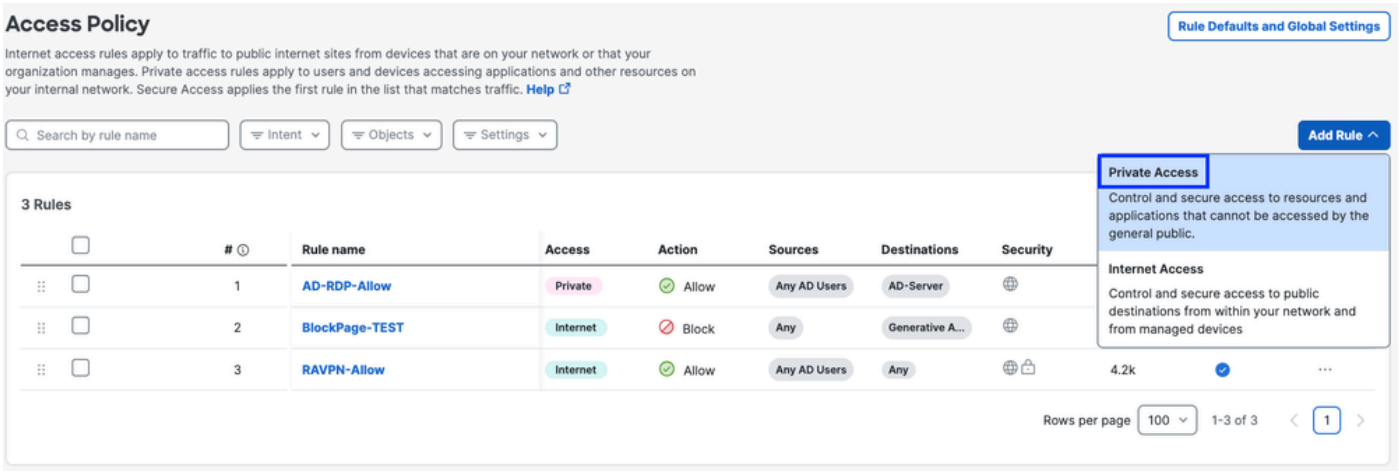
Universal ZTA 등록된 사용자가 액세스할 수 있도록 Secure Access의 비공개 액세스를 구성합니다 . 자세한 내용은 개인 액세스 규칙을 참조하십시오

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



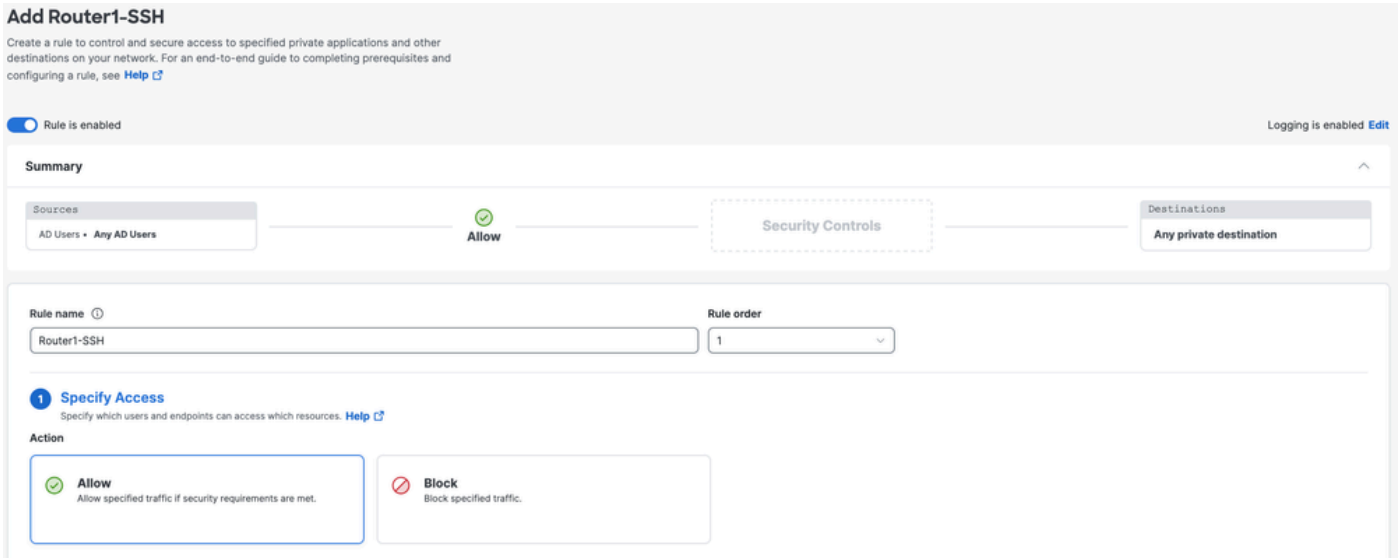
보안 액세스 - 프라이빗 리소스 컨피그레이션

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



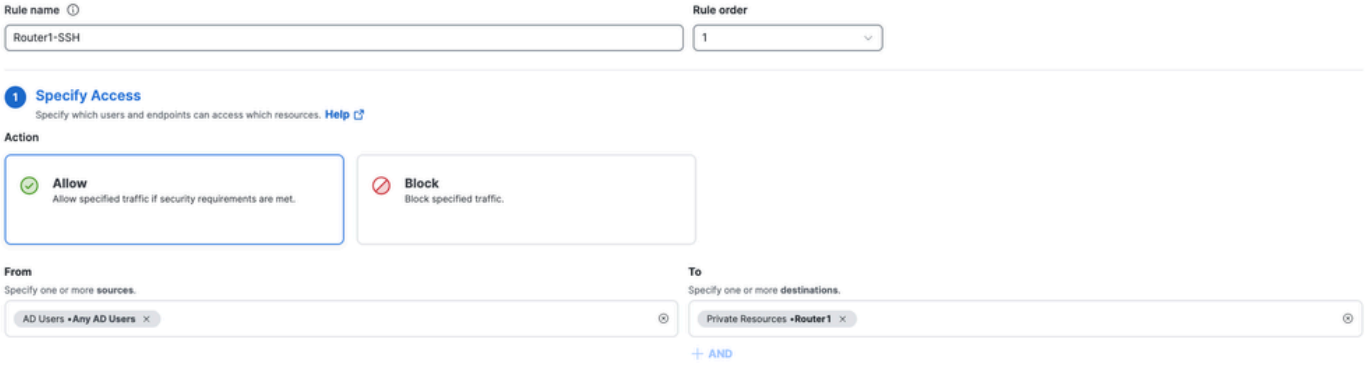
보안 액세스 - 액세스 정책 컨피그레이션

3. 규칙 이름 추가



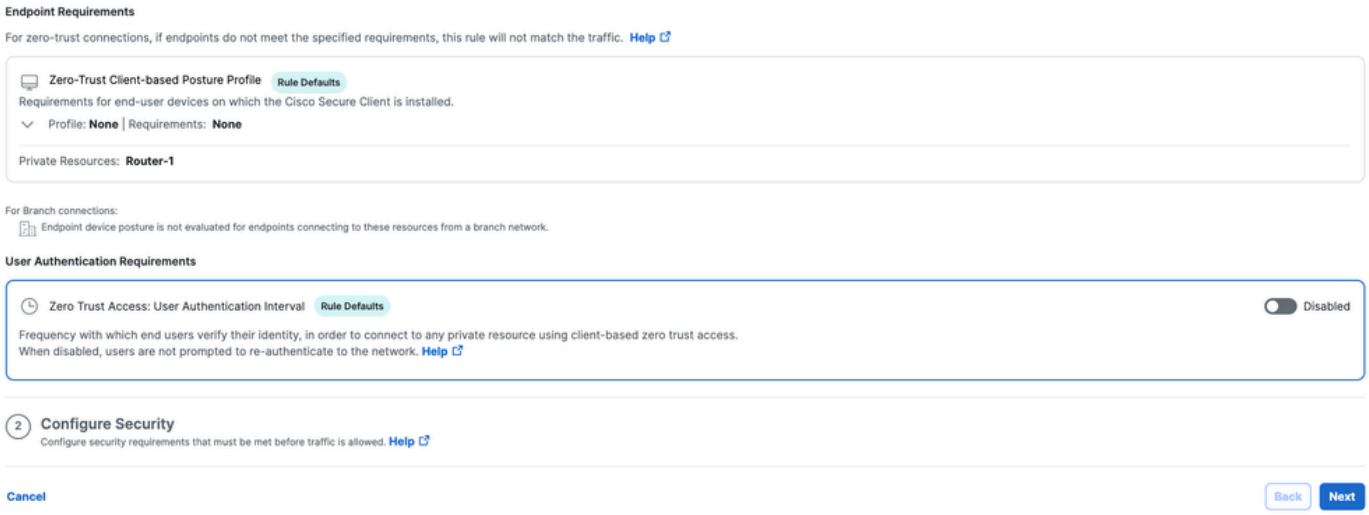
보안 액세스 - 액세스 정책 컨피그레이션

4. 규칙 조치를 선택하고 출처 및 대상을 선택합니다



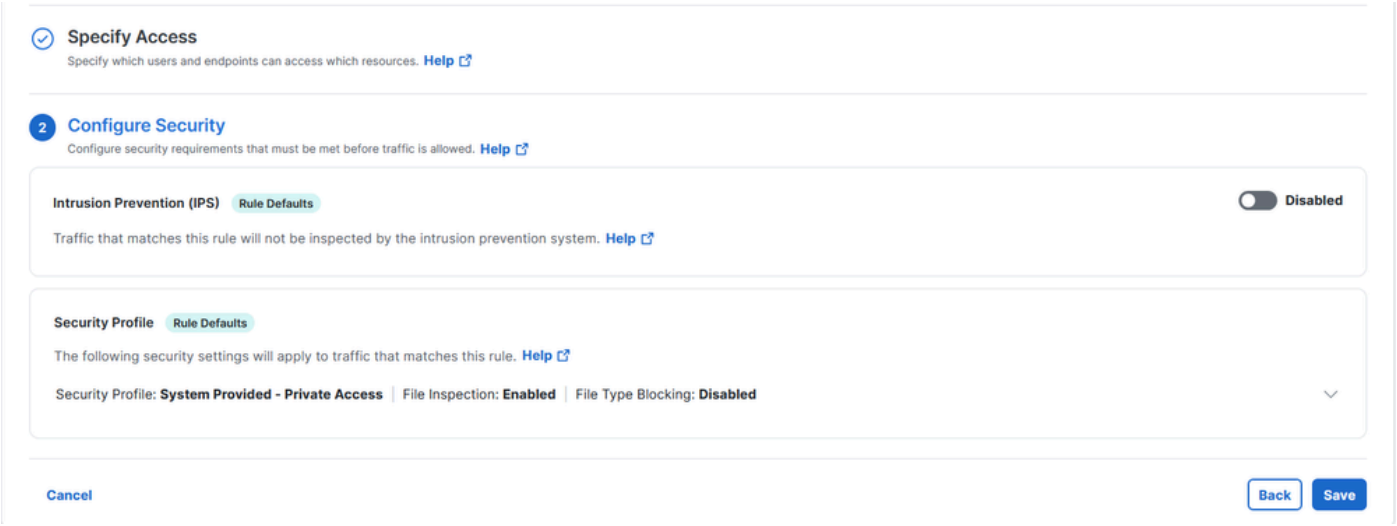
보안 액세스 - 액세스 정책 컨피그레이션

5. 엔드포인트 요구 사항 구성



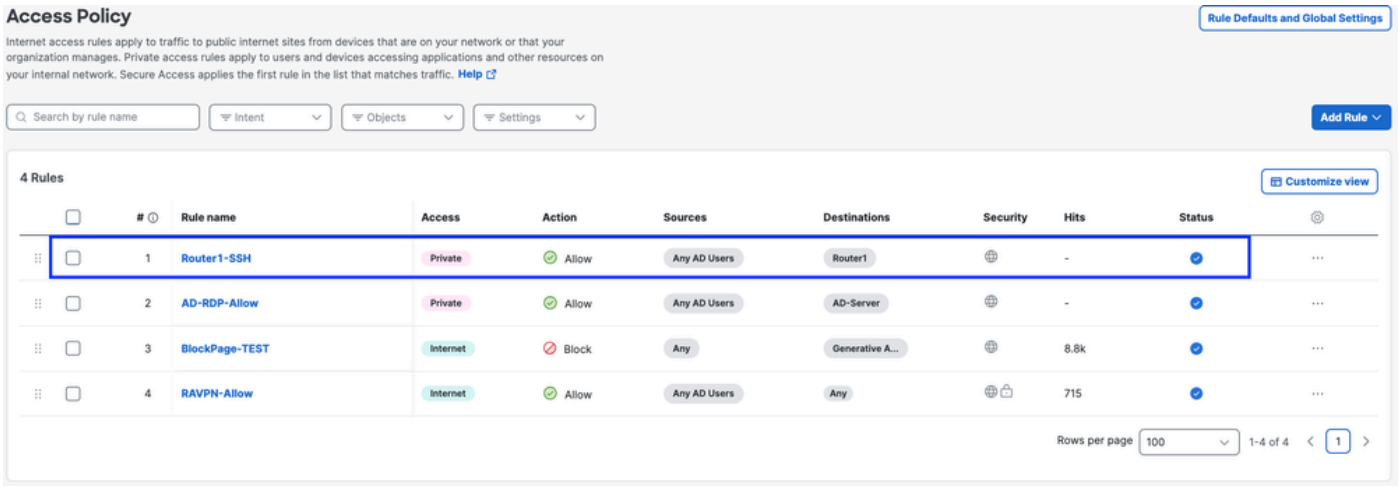
보안 액세스 - 액세스 정책 컨피그레이션

6. 보안 구성



보안 액세스 - 액세스 정책 컨피그레이션

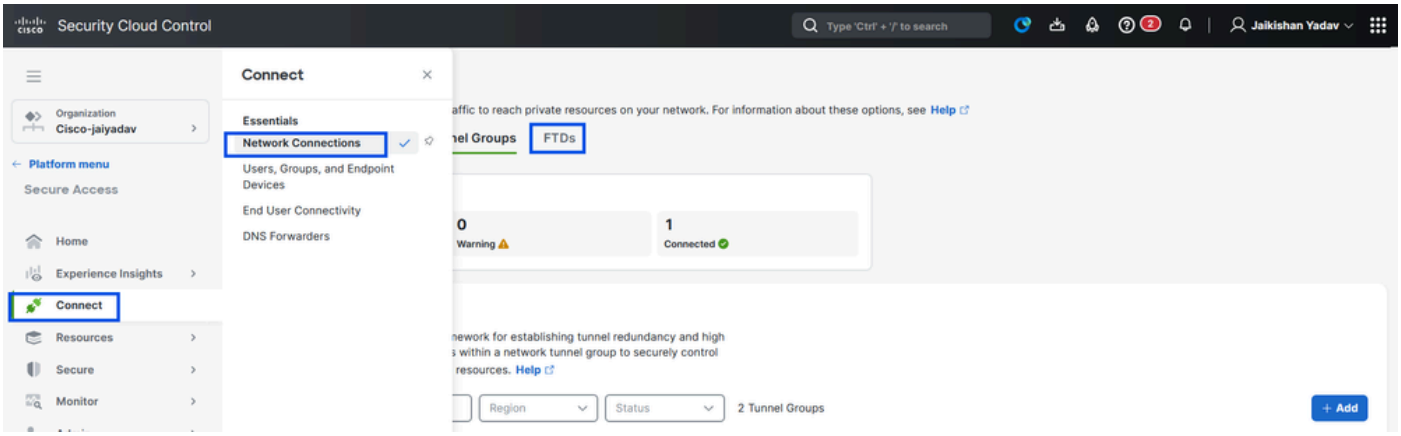
7. 저장을 클릭합니다.



보안 액세스 - 액세스 정책 컨피그레이션

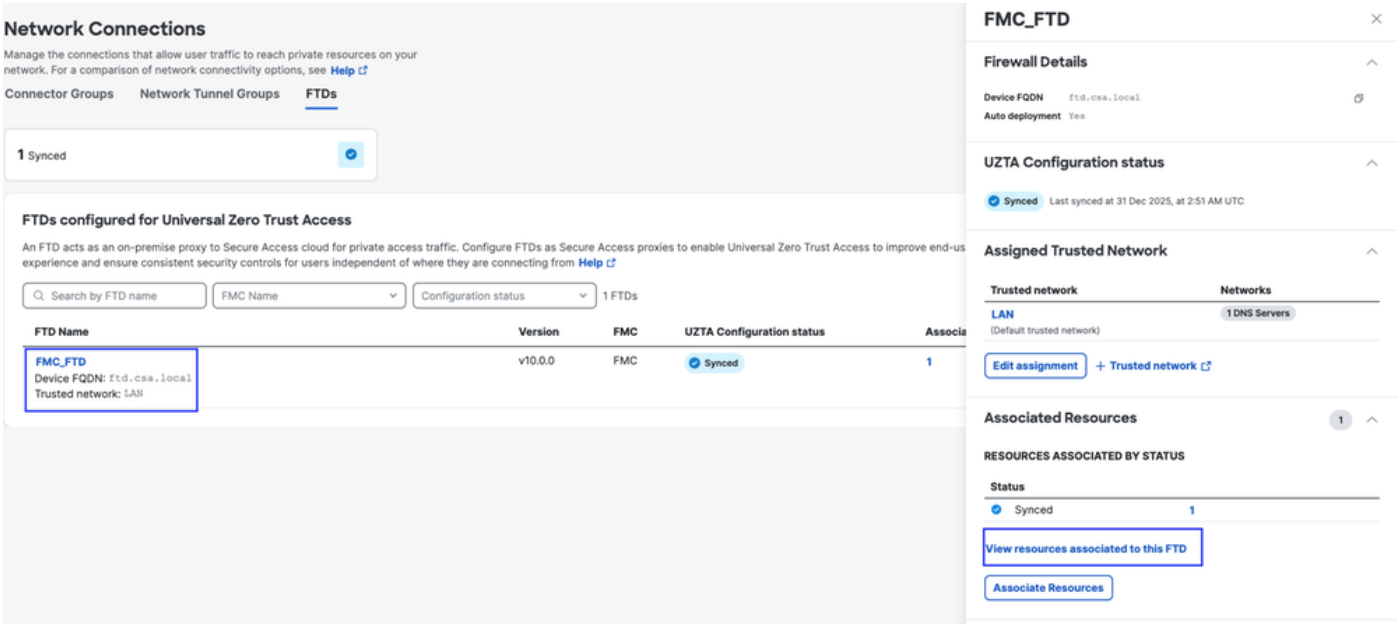
3단계 - FTD에서 PR 연결 확인

1. 연결 > 네트워크 연결 > FTDs로 이동합니다

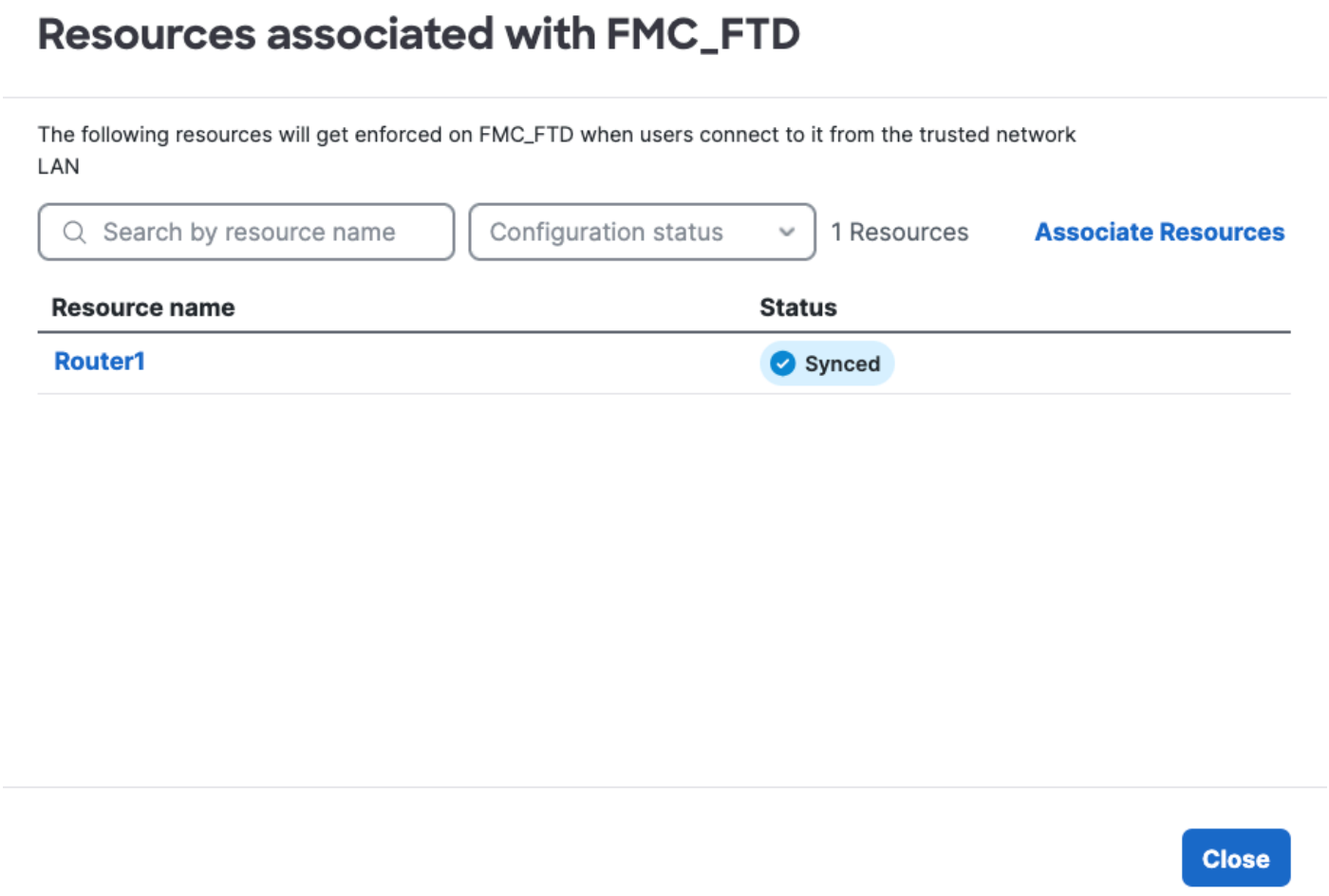


보안 액세스 - PR 확인

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



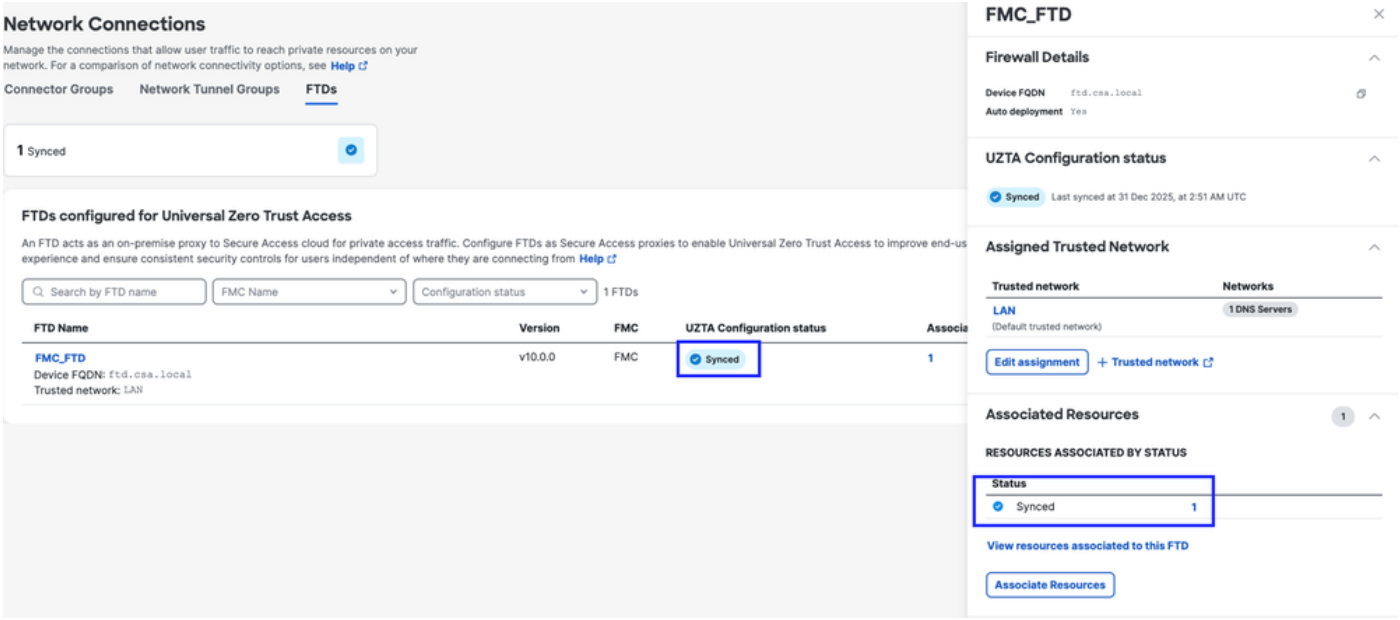
보안 액세스 - PR 확인



보안 액세스 - PR 확인

3 . Close(닫기)를 클릭합니다

4. 상태, 관련 리소스 및 구성이 동기화 상태인지 확인합니다.



보안 액세스 - PR 확인

5. 구성이 FTD로 푸시되었는지 확인합니다.

FTD cli에 로그인하고 LINA 모드로 이동합니다.

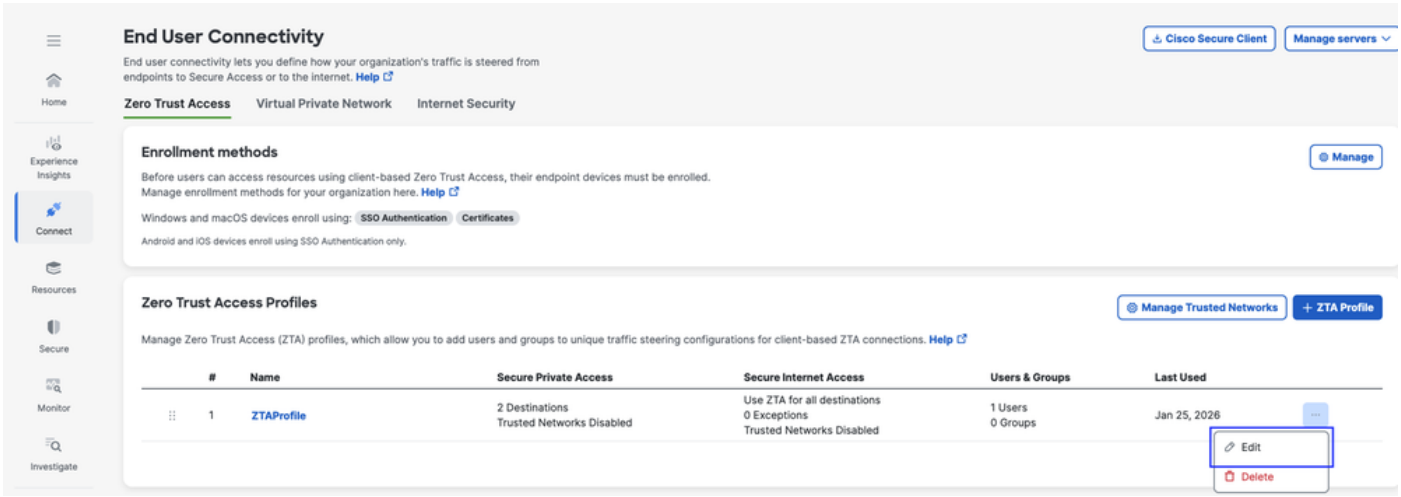
show running-config object application

```
> 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

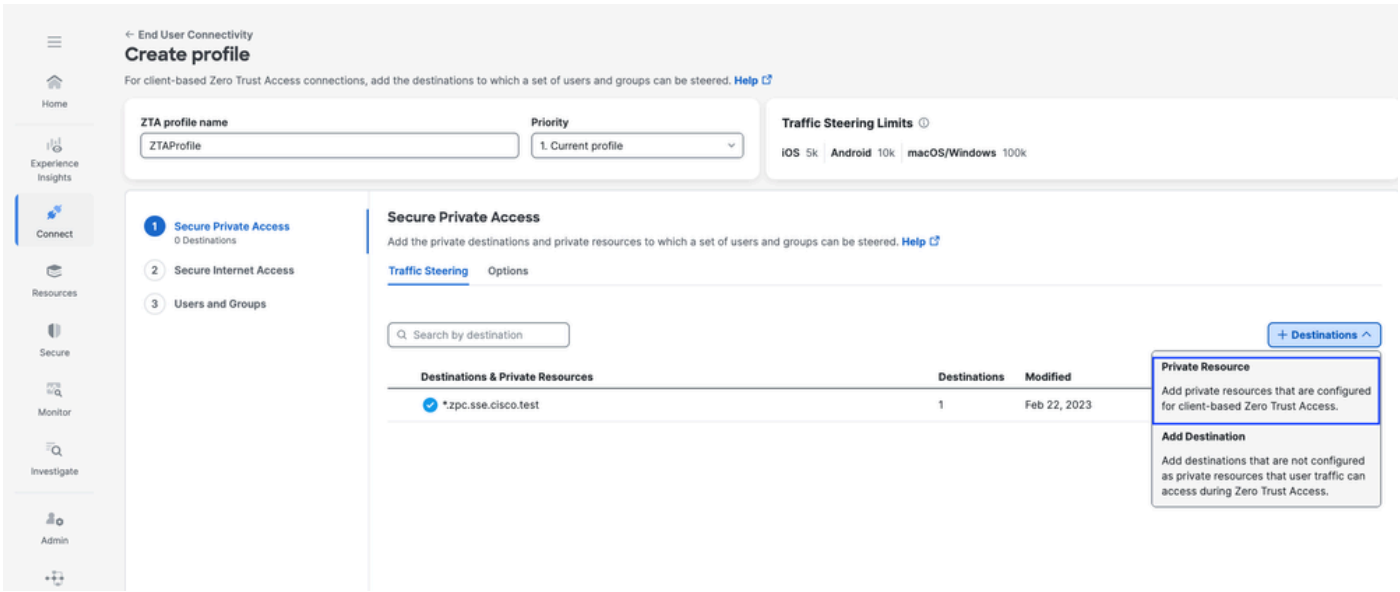
단계 - 4 ZTA 프로필에 프라이빗 리소스 추가

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

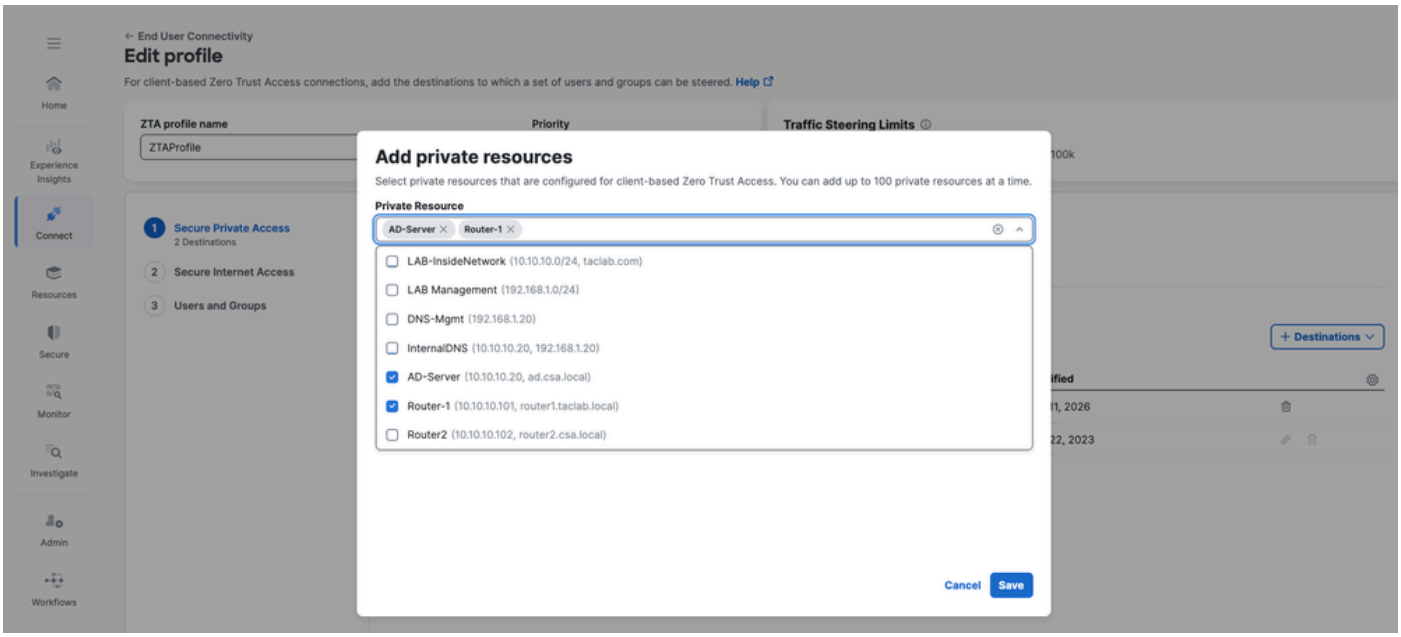


보안 액세스 - ZTA 프로필

2. 프라이빗 리소스 추가

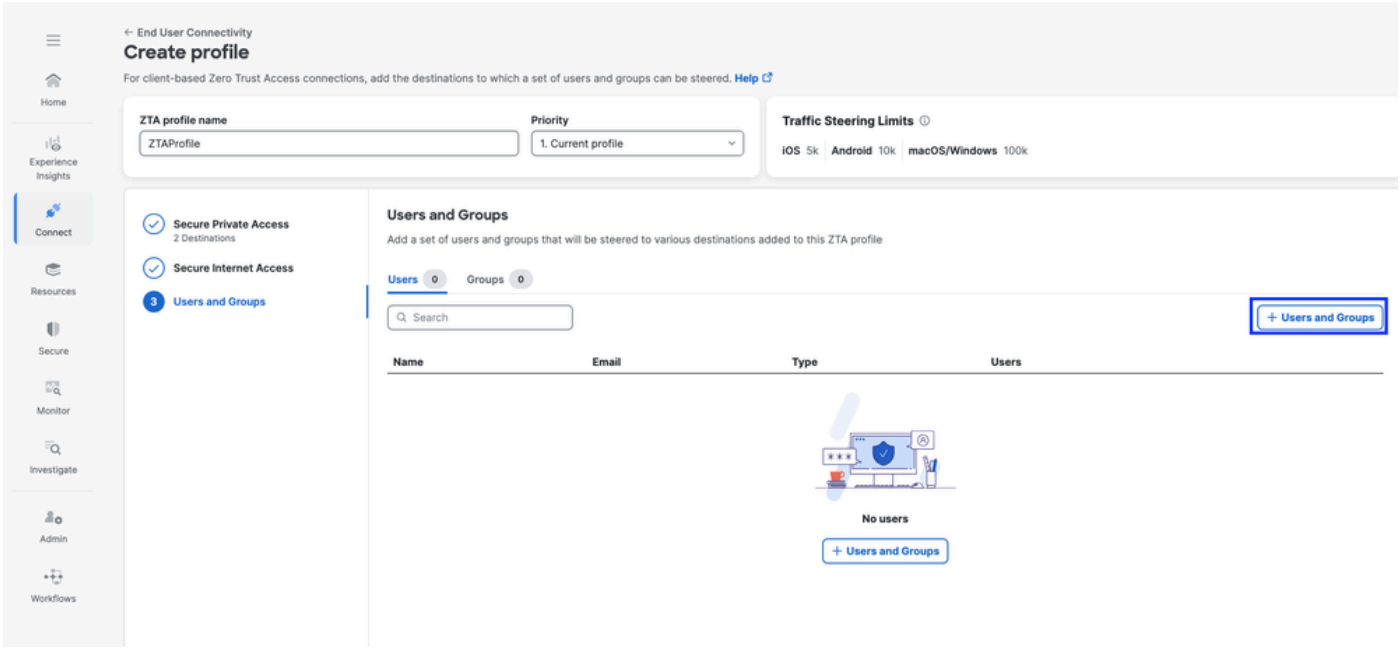


보안 액세스 - ZTA 프로필

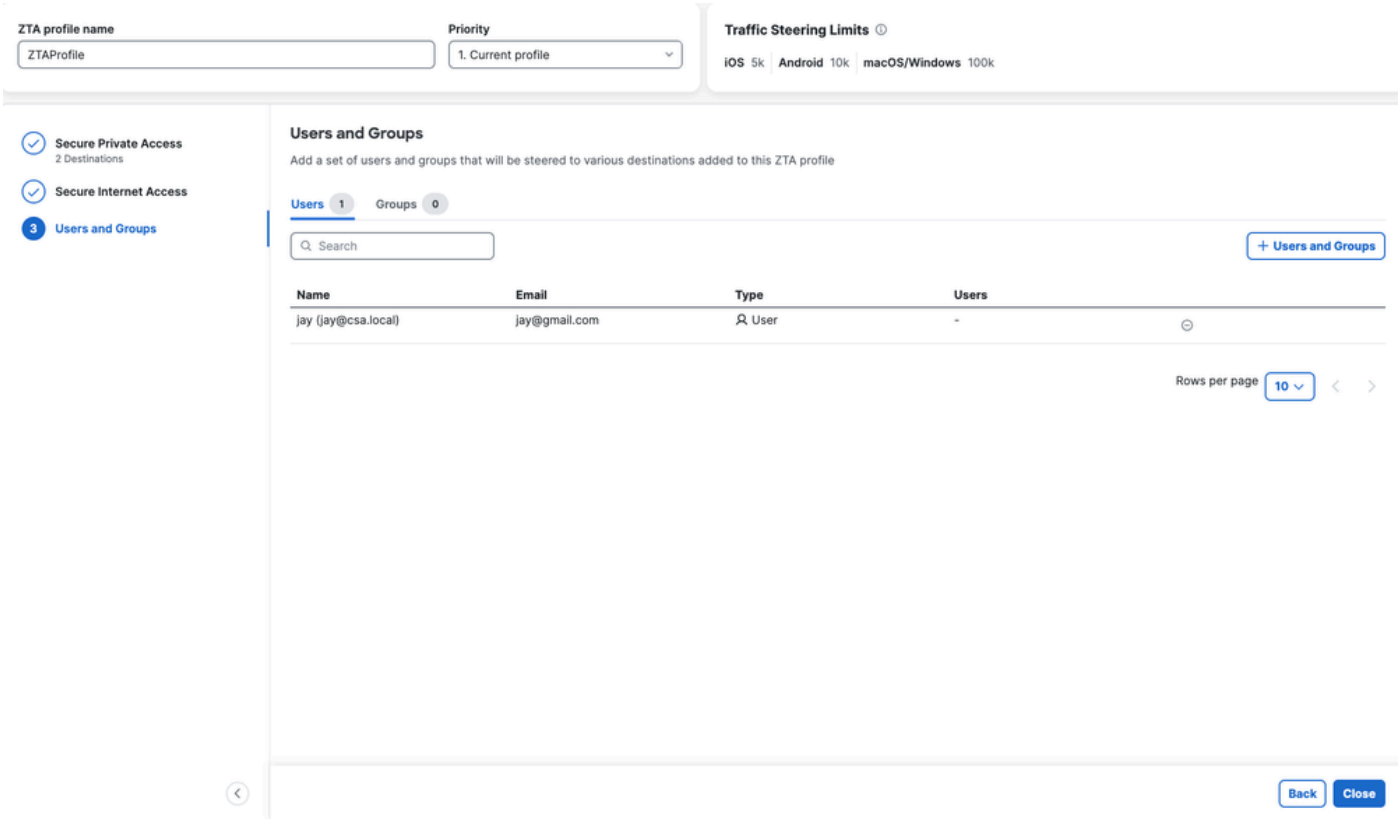


보안 액세스 - ZTA 프로필

3 . 사용자 및 그룹 추가



보안 액세스 - ZTA 프로필



보안 액세스 - ZTA 프로필

단계 - 5 Private Resource에 대한 액세스 확인

1. 원격 사용자가 FTD FQDN을 확인할 수 있는지 확인

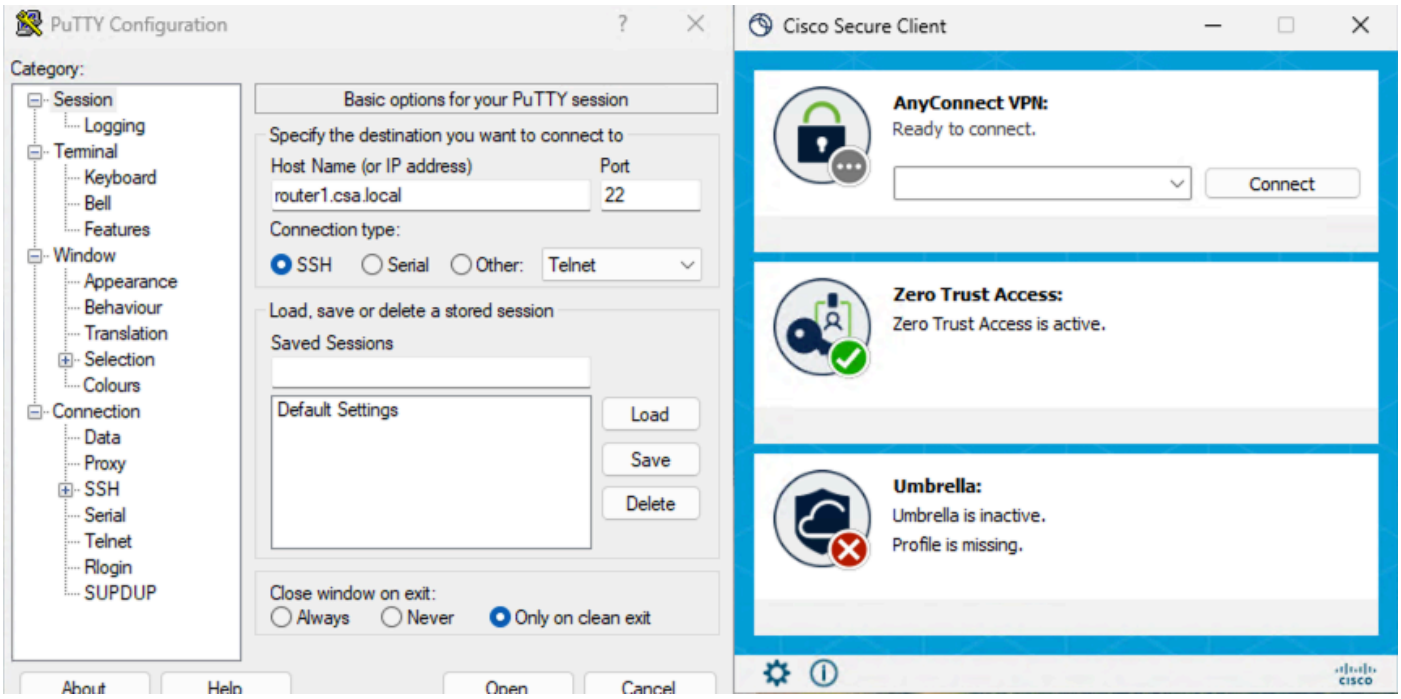
```
PS C:\Users\jay> ping ftd.csa.local

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
```

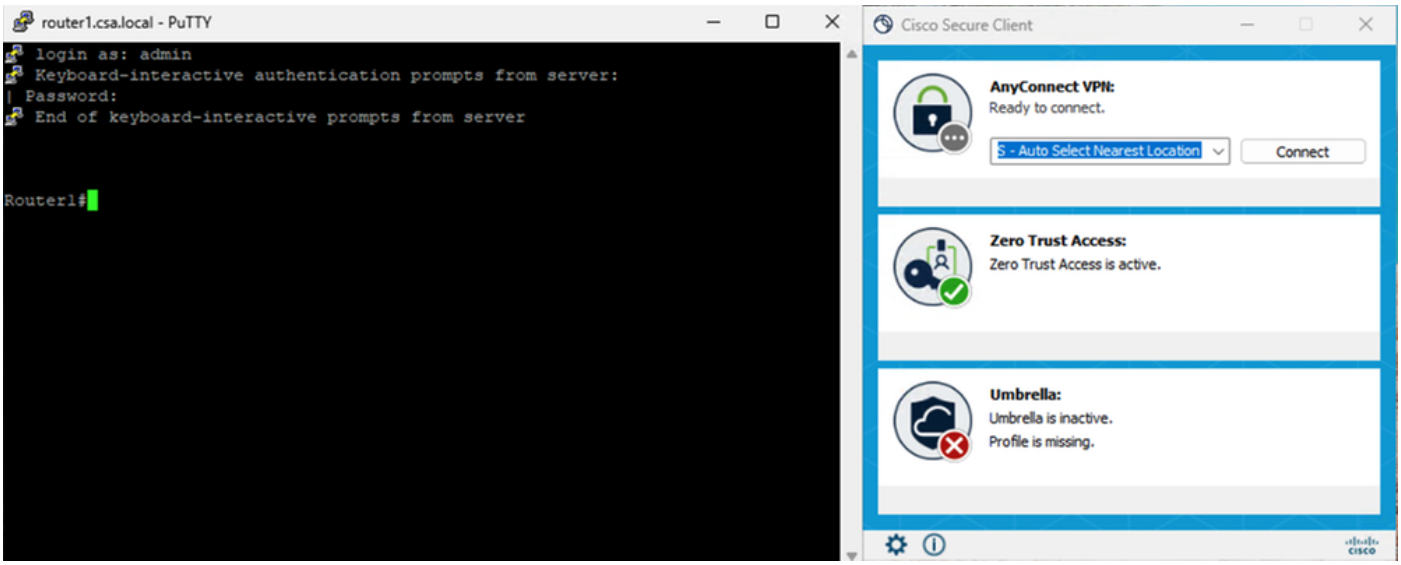
2. FQDN을 사용하여 FTD가 전용 리소스에 연결할 수 있는지 확인합니다.

```
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#
```


3 . 프라이빗 리소스에 대한 SSH 연결 테스트

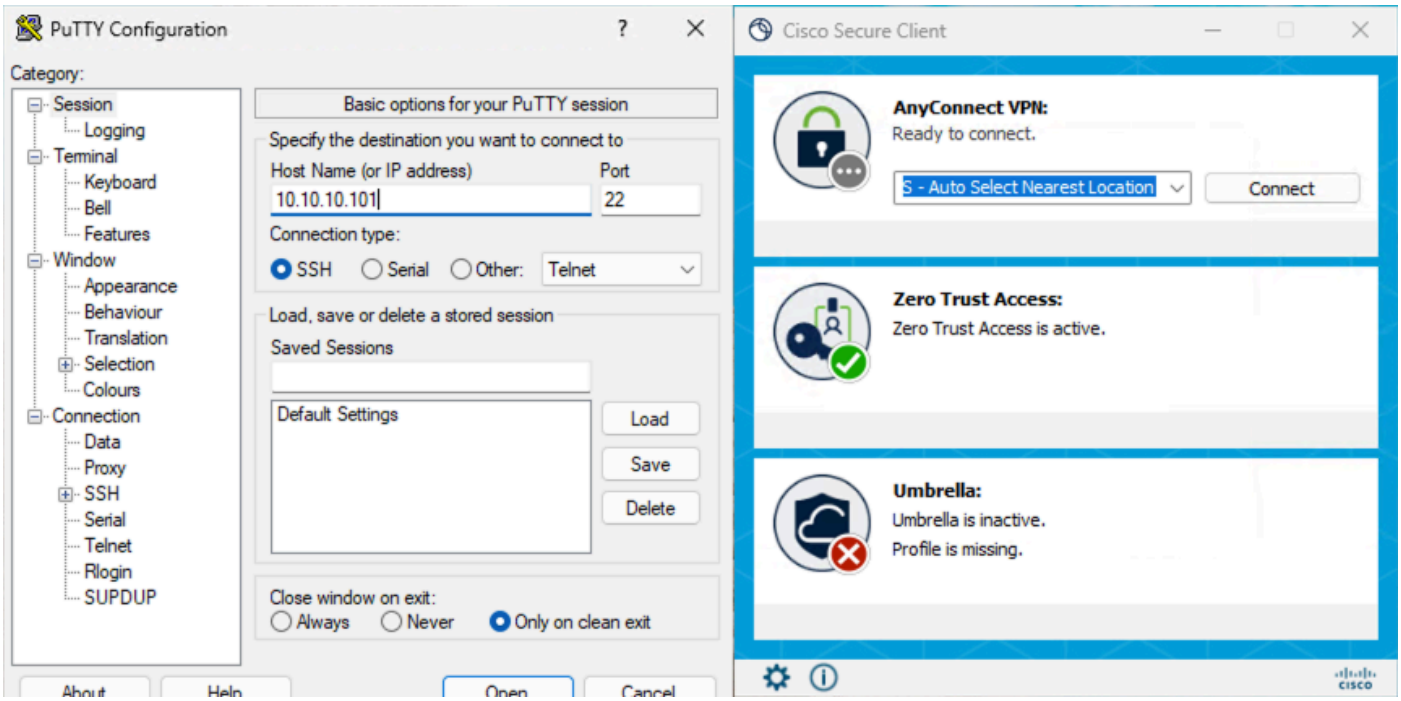
FQDN을 사용하여 PR 액세스



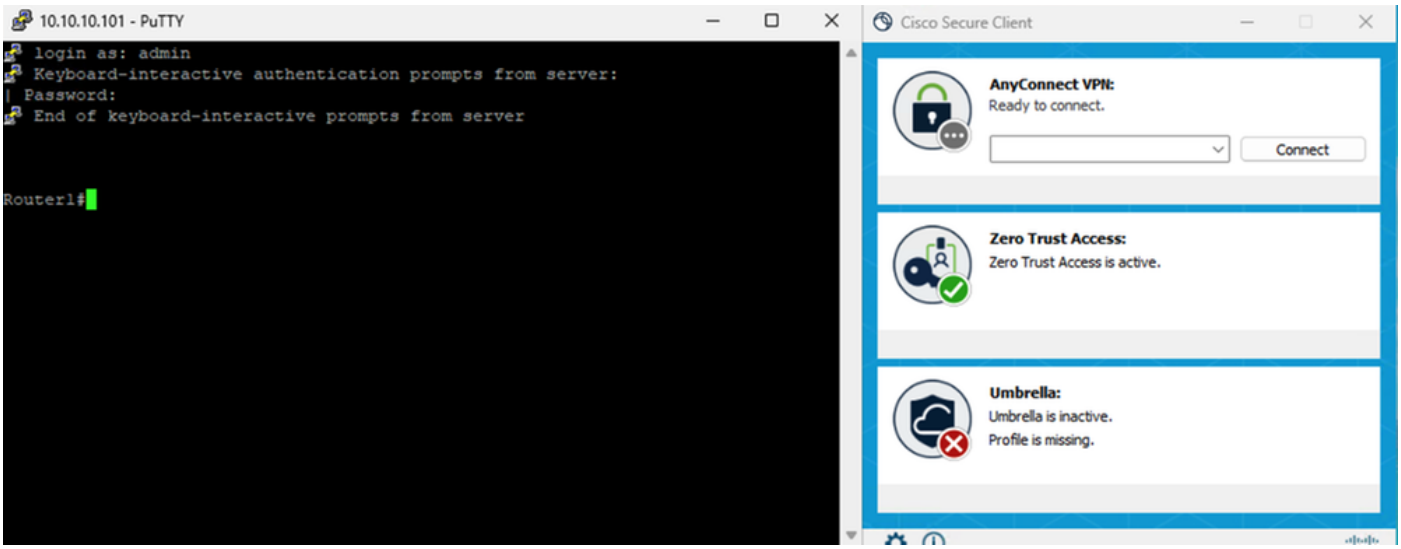


보안 액세스 - PR 테스트

IP 주소를 사용하여 PR에 액세스

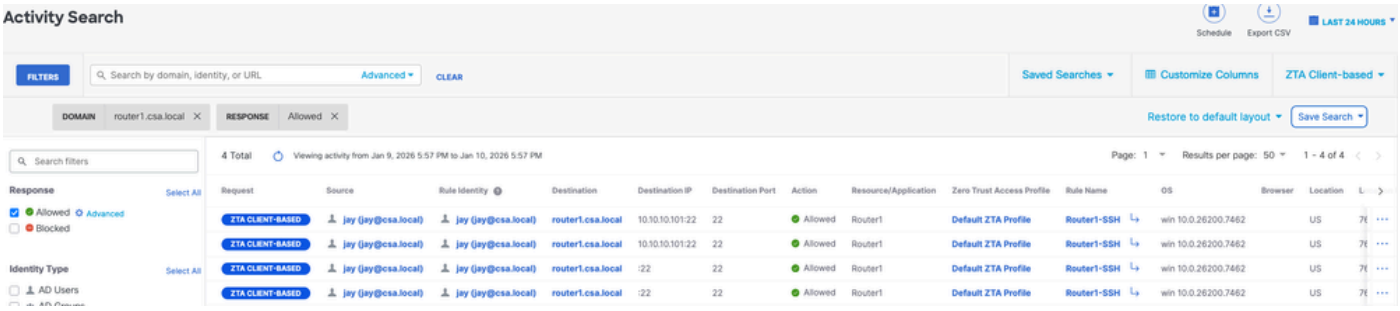


보안 액세스 - PR 테스트

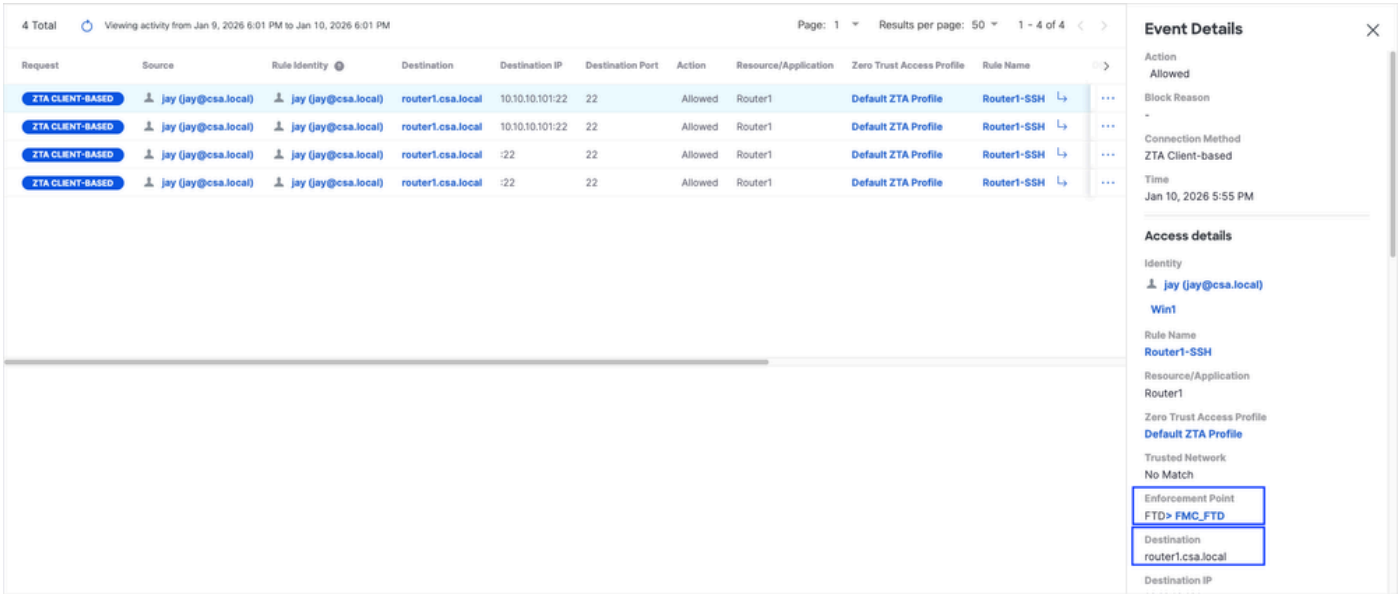


보안 액세스 - PR 테스트

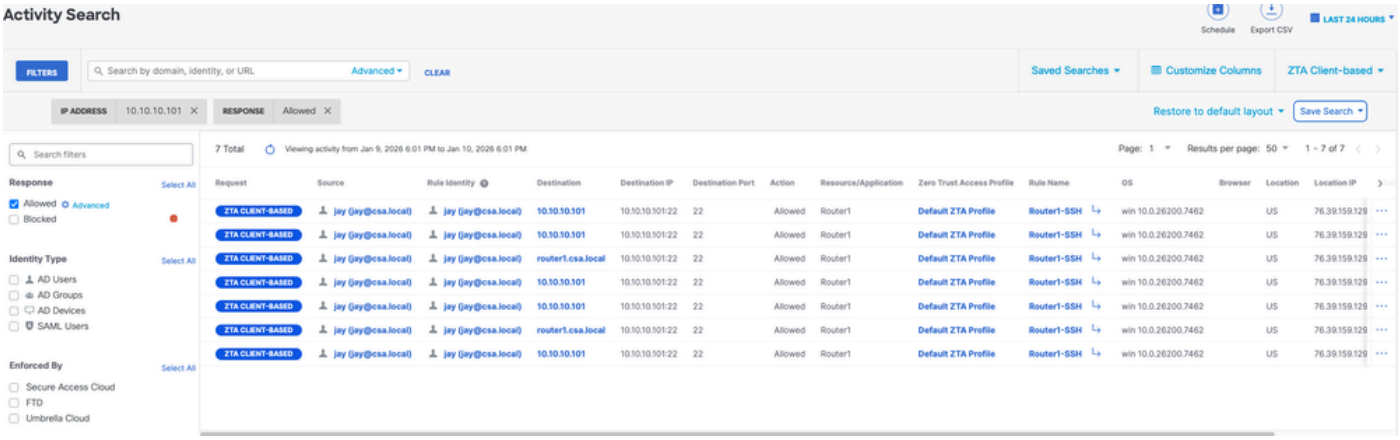
4. 보안 액세스 활동 검색 로그 확인



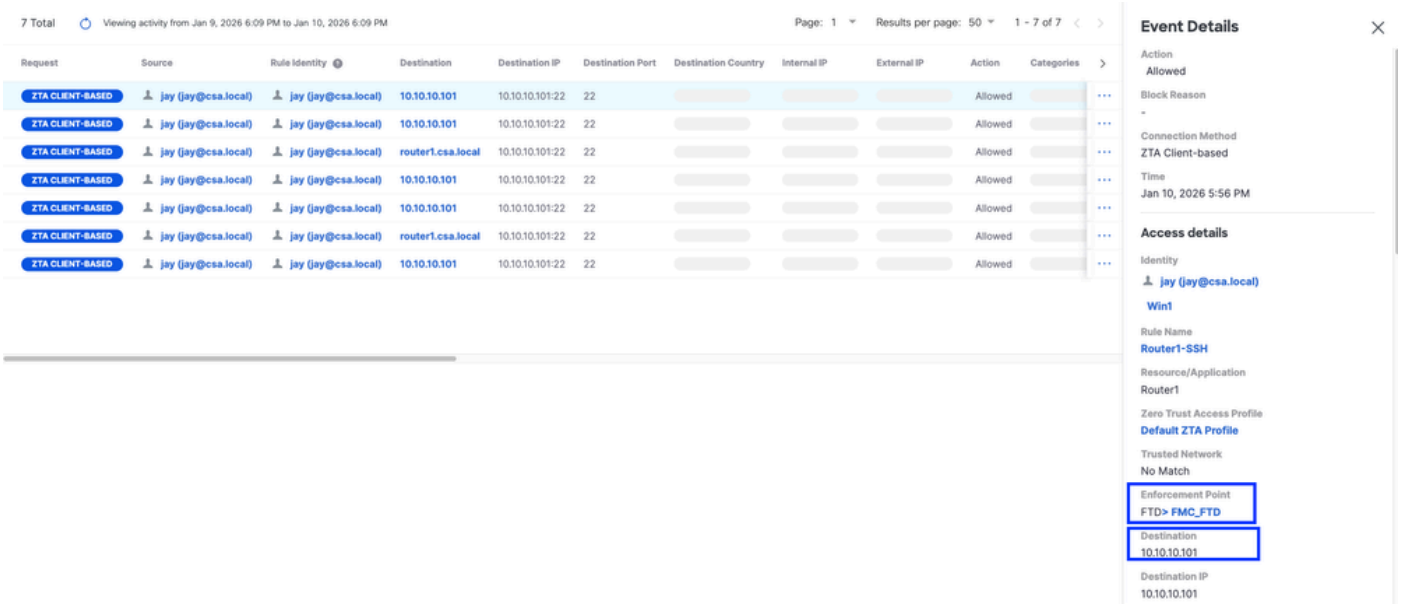
보안 액세스 - 활동 검색



보안 액세스 - 활동 검색

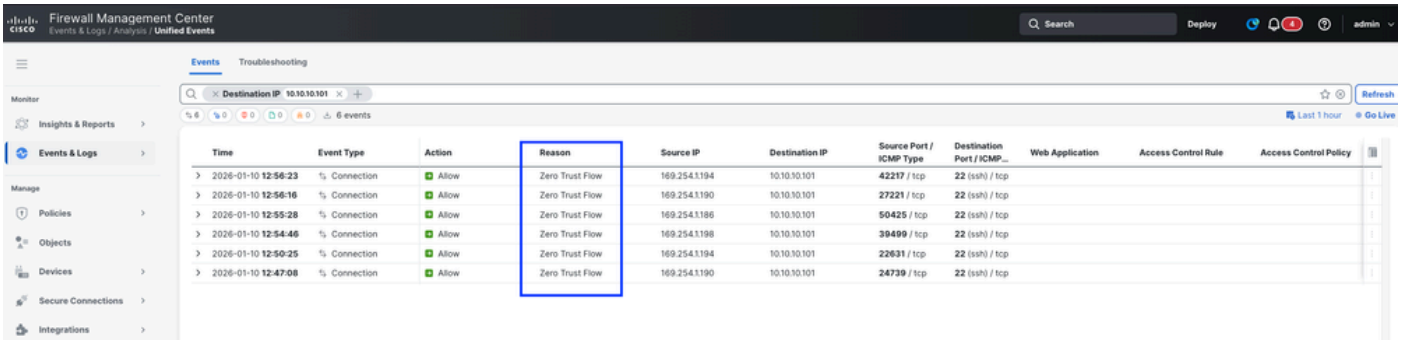


보안 액세스 - 활동 검색



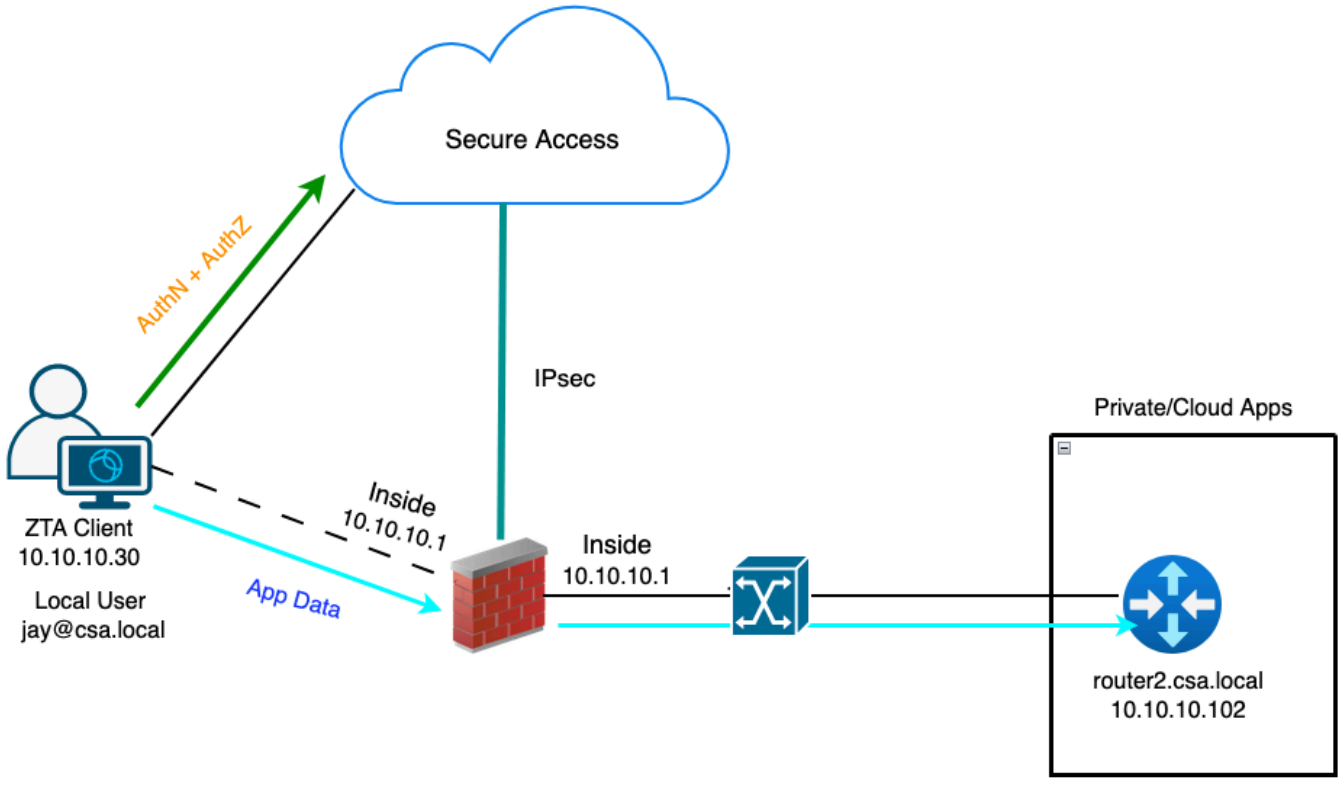
보안 액세스 - 활동 검색

5. FMC 연결 이벤트 확인



테스트 사례 3 - 로컬 사용자 - 로컬 시행

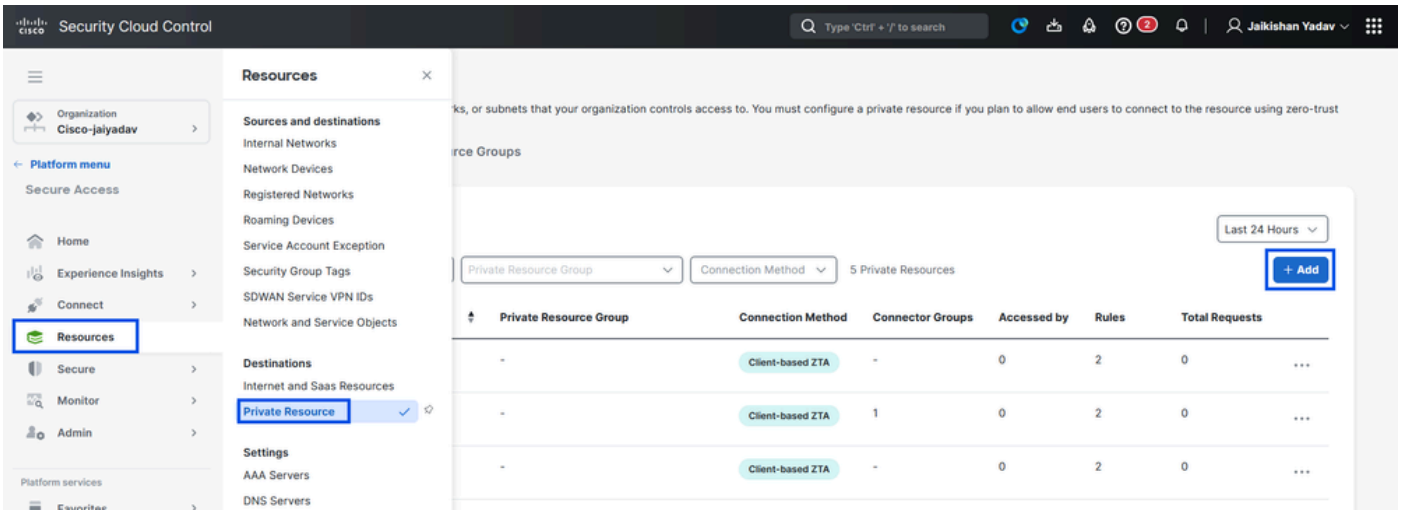
로컬 사용자로서 로컬 시행을 통해 프라이빗 리소스에 액세스하는 이 유형의 시행 정책 평가는 보안 액세스에서 수행되지만 애플리케이션 데이터는 FTD에 로컬로 유지됩니다. 예를 들어 ZTA가 홈 네트워크에 연결된 클라이언트 또는 사용자를 등록하고 FTD 내부 인터페이스 뒤에 있는 전용 리소스에 액세스하려고 했습니다. 프라이빗 리소스가 DMZ 또는 FTD의 다른 인터페이스 뒤에 있는 경우 클라이언트 IP 또는 네트워크와 프라이빗 리소스 간의 트래픽을 허용하기 위해 FTD에 대한 액세스 규칙을 생성해야 합니다.



1단계 - Secure Access에서 프라이빗 리소스 정의

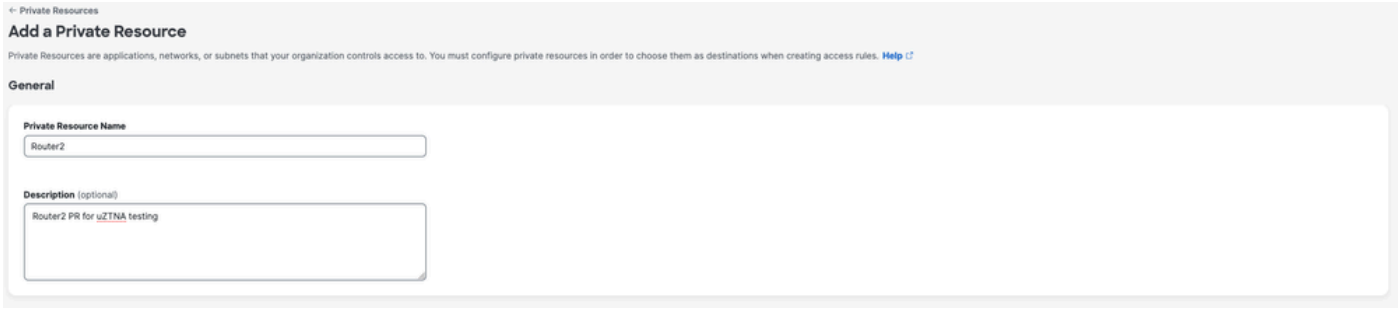
클라우드 시행으로 ZTA(Zero Trust Access) 등록된 디바이스를 통해 액세스할 수 있는 프라이빗 리소스 구성

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



보안 액세스 - 프라이빗 리소스 컨피그레이션

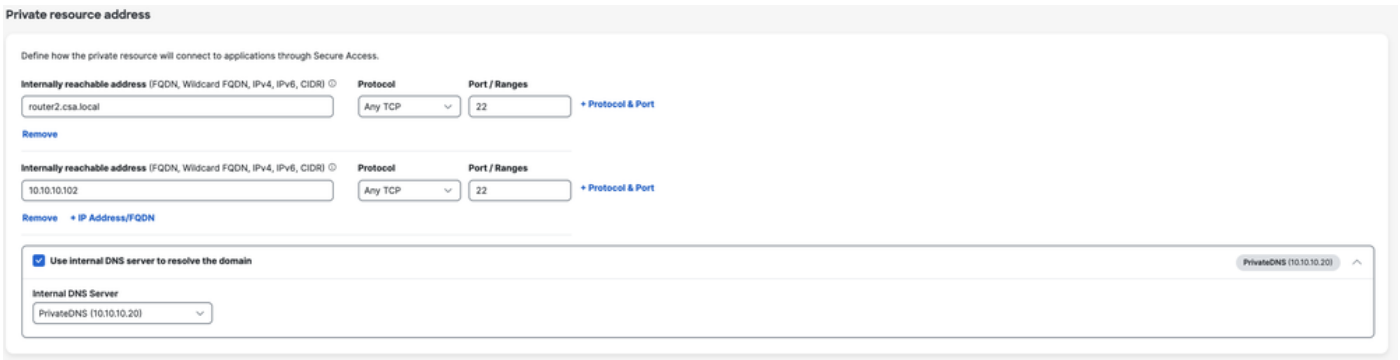
2. 개인 자원명에는 유의미한 자원명을 입력합니다. 설명의 경우, 리소스의 용도 또는 리소스 소유자의 이름과 같은 정보를 제공하는 것이 좋습니다.



보안 액세스 - 프라이빗 리소스 컨피그레이션

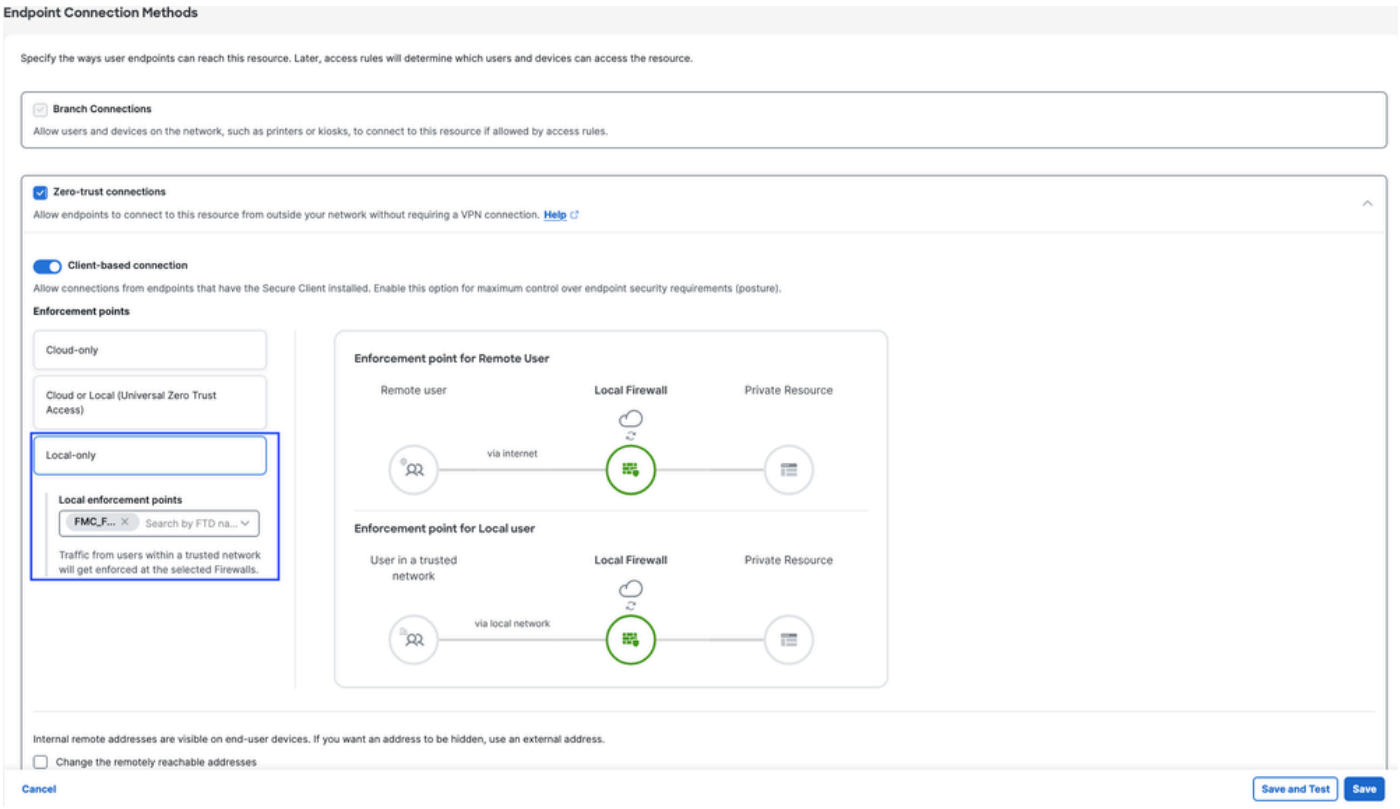
3. 액세스하려는 개인 자원의 FQDN을 입력합니다. 프라이빗 리소스의 IP 주소도 정의할 수 있습니다. 자세한 내용은 프라이빗 [리소스 추가를 참조하십시오]

4. 도메인을 확인할 내부 DNS 서버를 선택합니다



5. 엔드포인트 연결 방법 선택

6. FTD를 로컬 적용 지점으로 선택합니다



보안 액세스 - 프라이빗 리소스 컨피그레이션

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

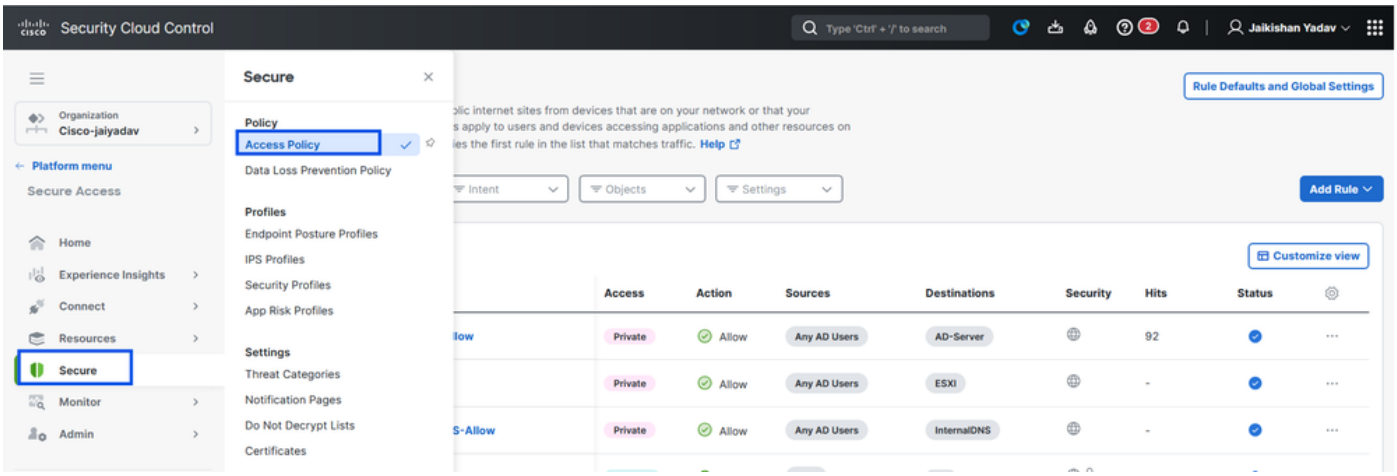
---

7 . Save(저장)를 클릭합니다.

2단계 - 개인 액세스 규칙 생성

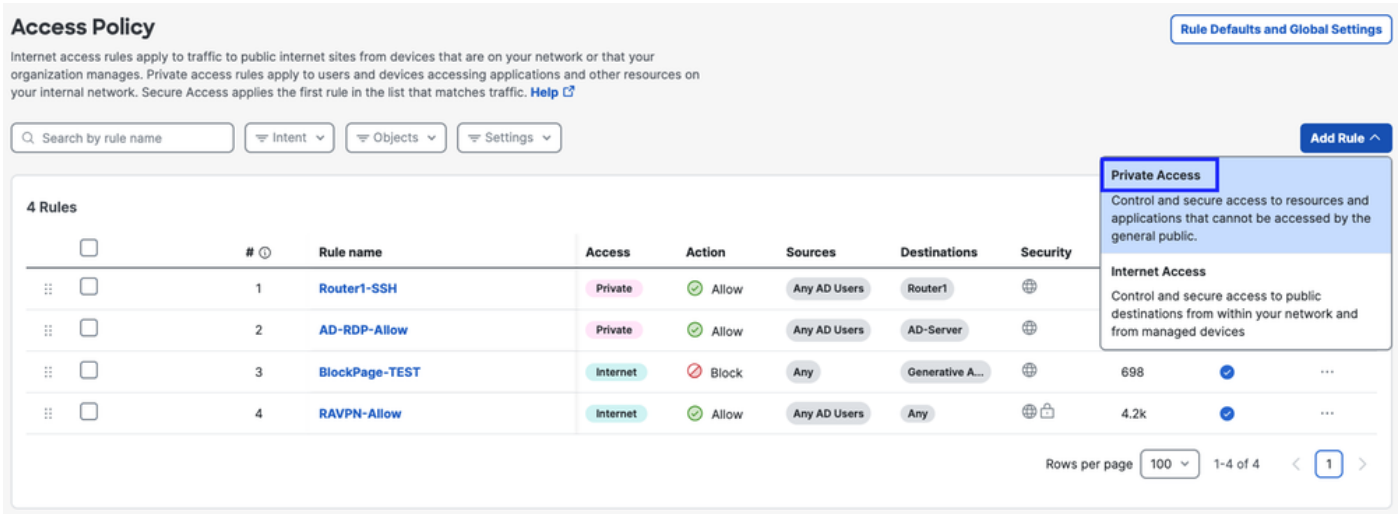
Universal ZTA 등록된 사용자가 액세스할 수 있도록 Secure Access의 비공개 액세스를 구성합니다 . 자세한 내용은 개인 액세스 규칙을 참조하십시오

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



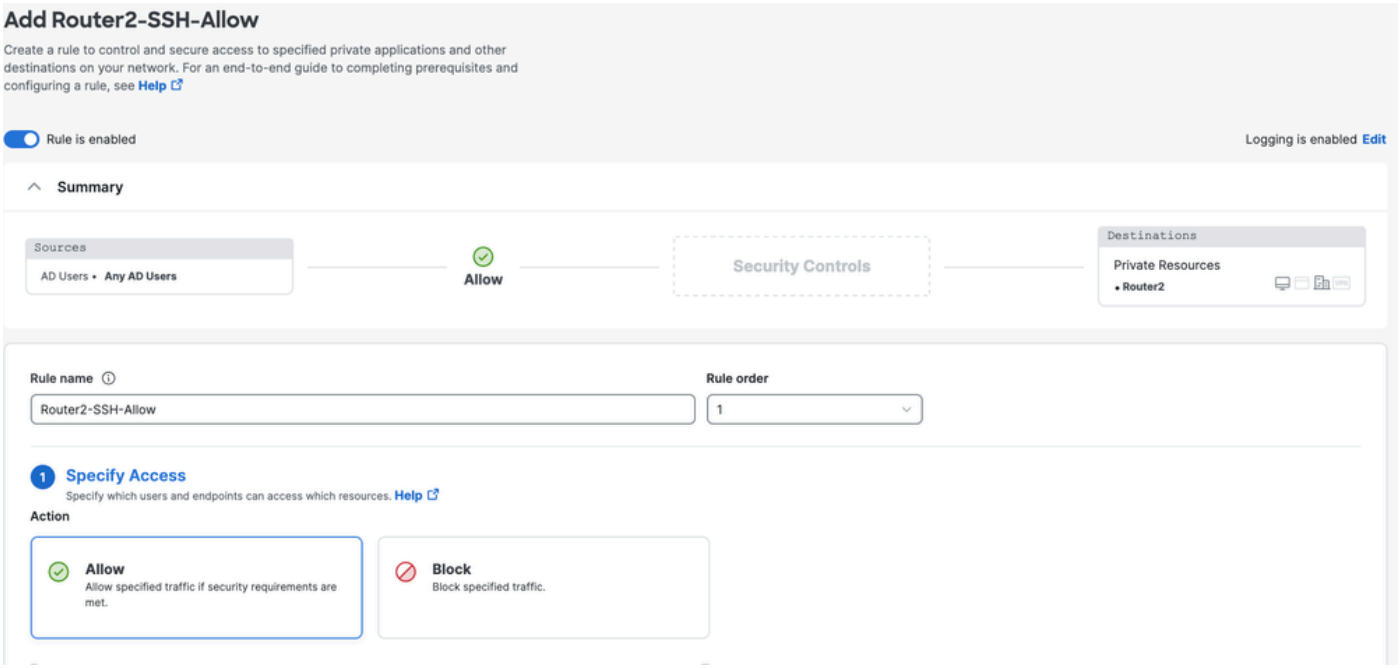
보안 액세스 - 액세스 정책 컨피그레이션

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



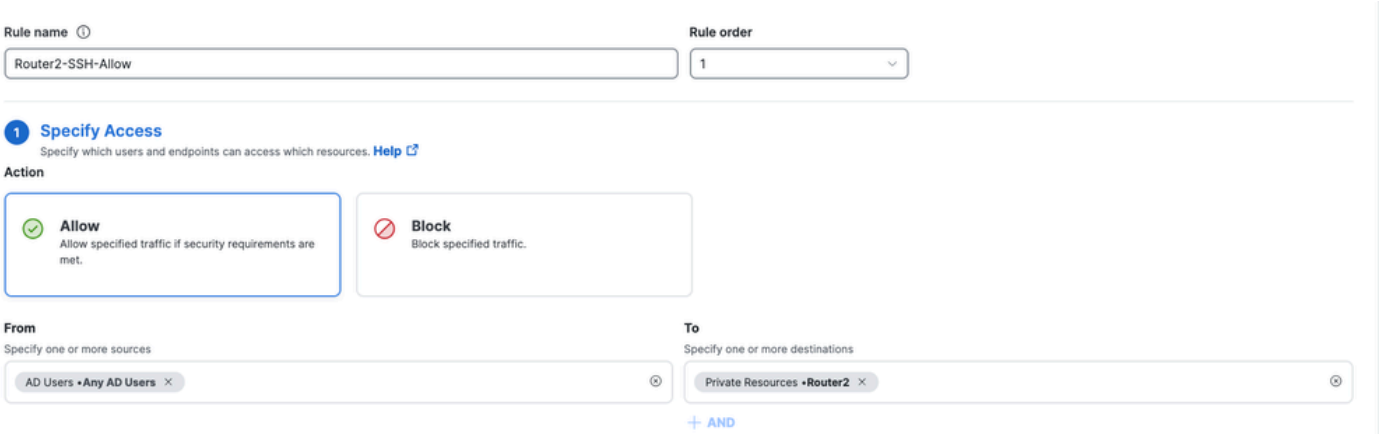
보안 액세스 - 액세스 정책 컨피그레이션

3. 규칙 이름 추가



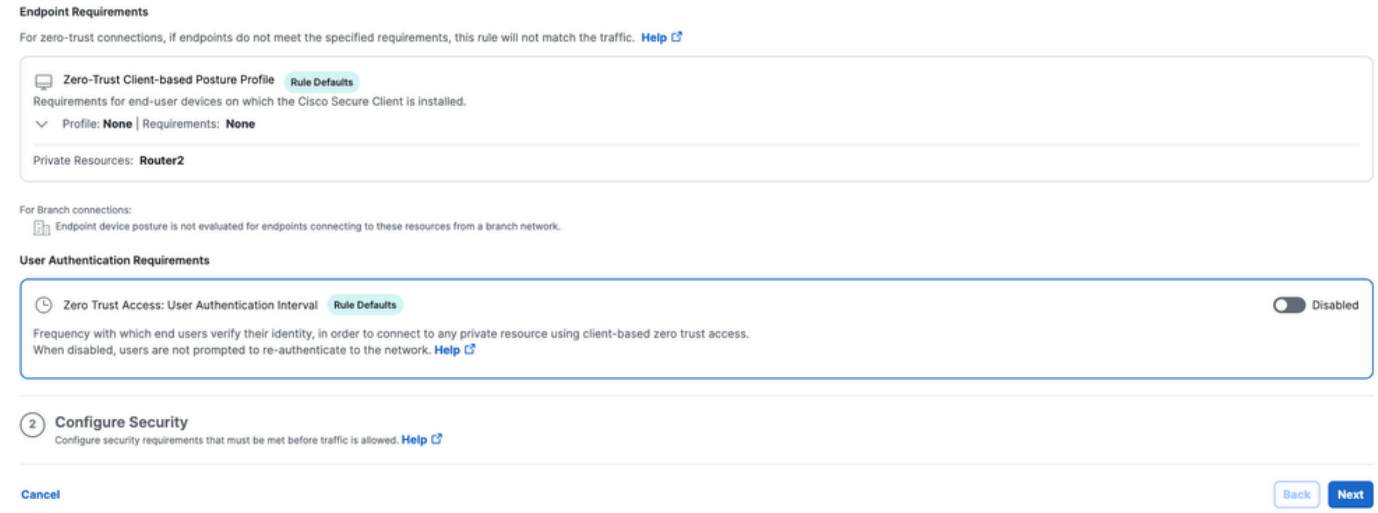
보안 액세스 - 액세스 정책 컨피그레이션

4. 규칙 조치를 선택하고 출처 및 대상을 선택합니다



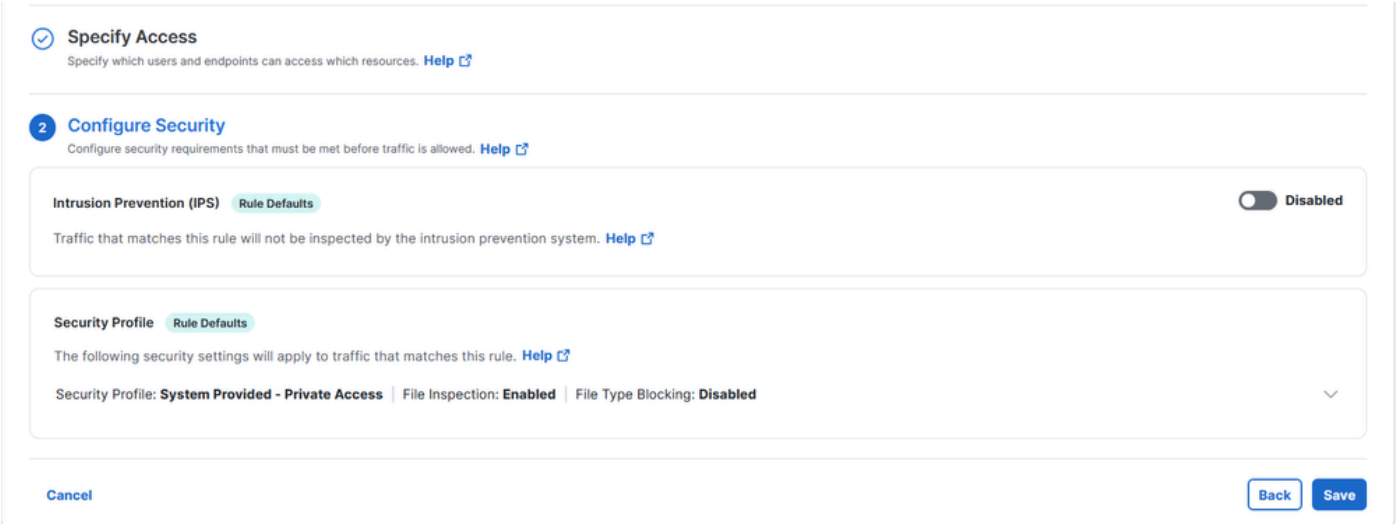
보안 액세스 - 액세스 정책 컨피그레이션

5. 엔드포인트 요구 사항 구성



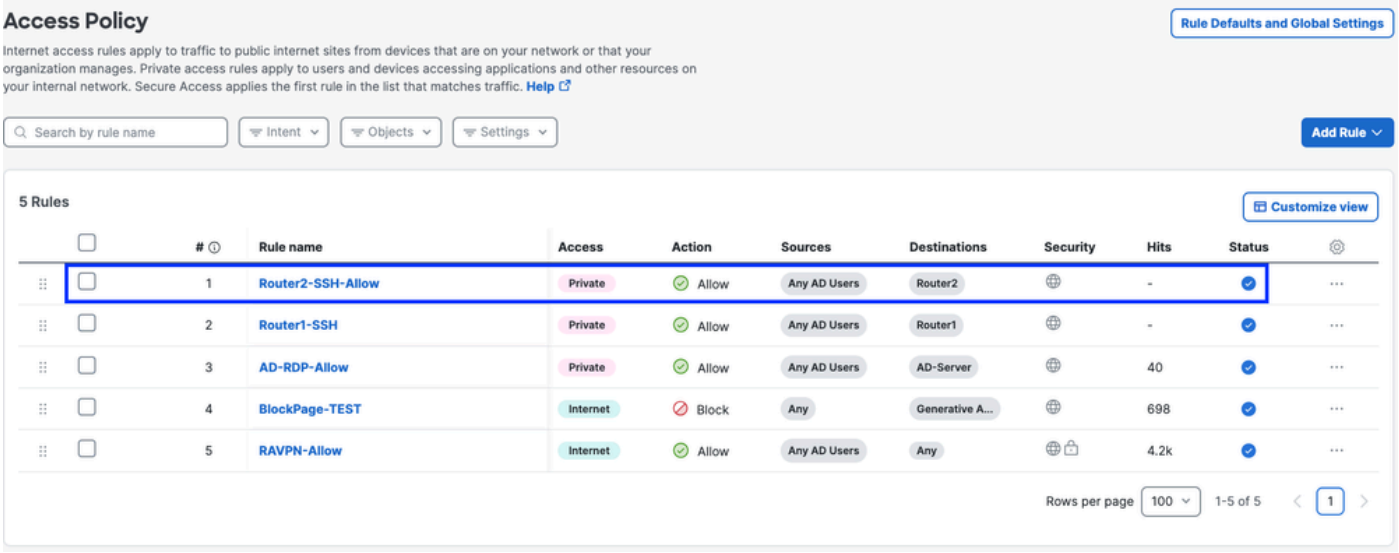
보안 액세스 - 액세스 정책 컨피그레이션

6. 보안 구성



보안 액세스 - 액세스 정책 컨피그레이션

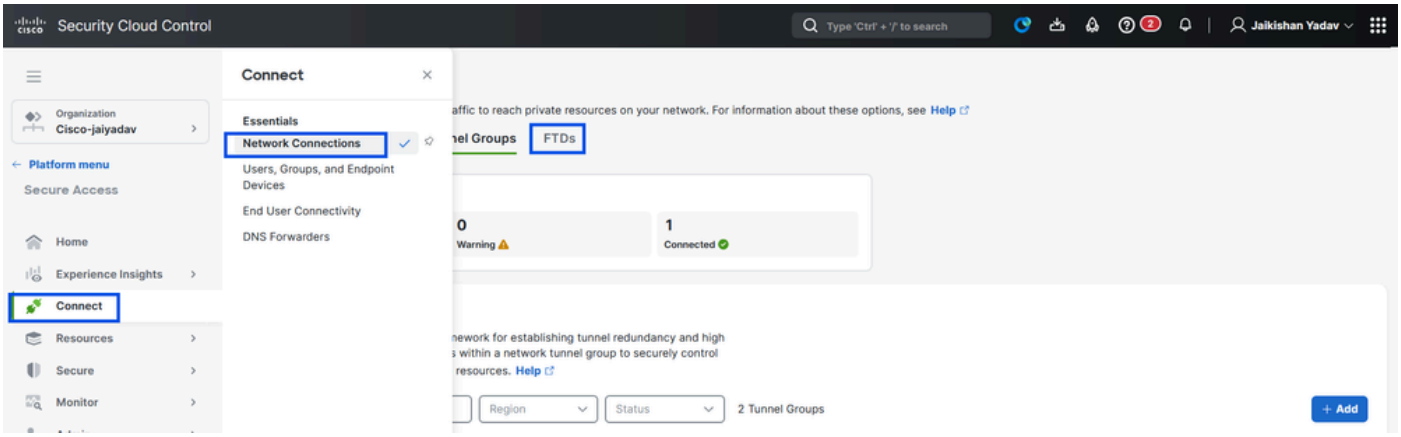
7. 저장을 클릭합니다.



보안 액세스 - 액세스 정책 컨피그레이션

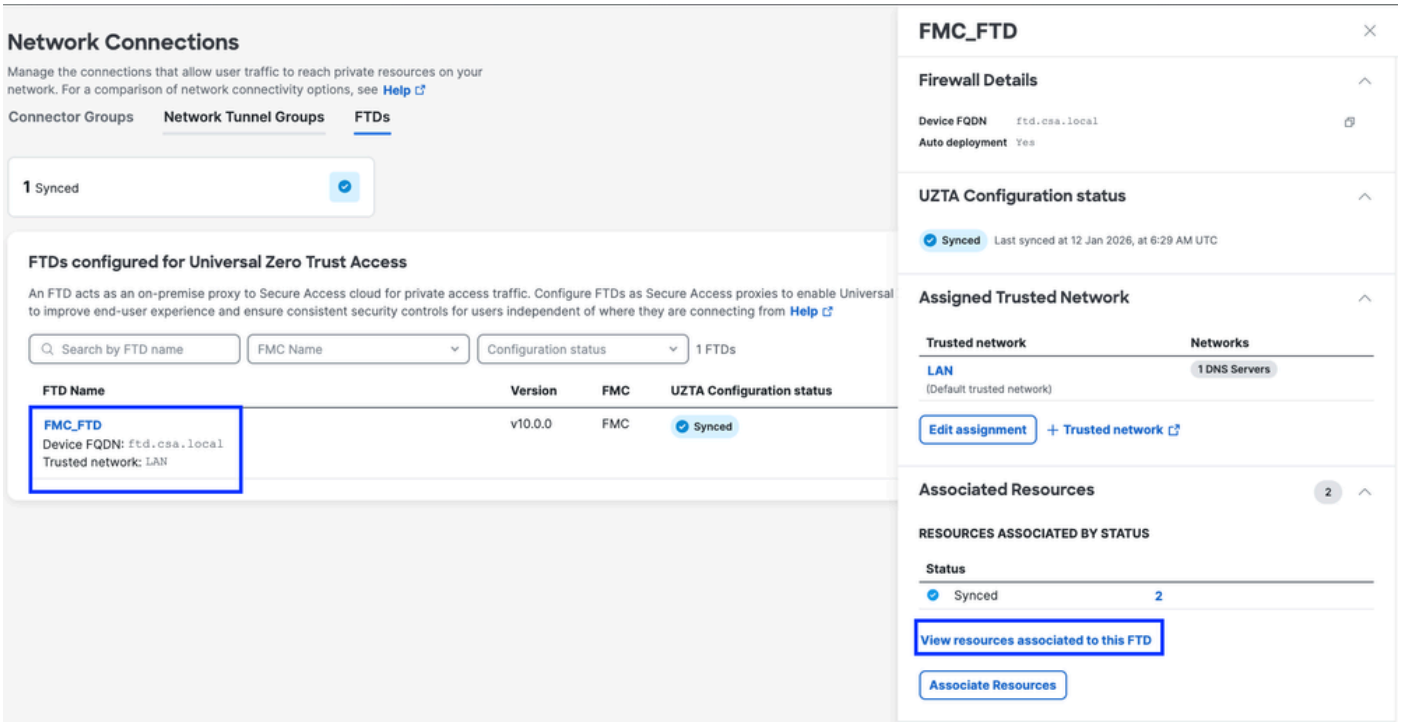
3단계 - FTD에서 PR 연결 확인

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

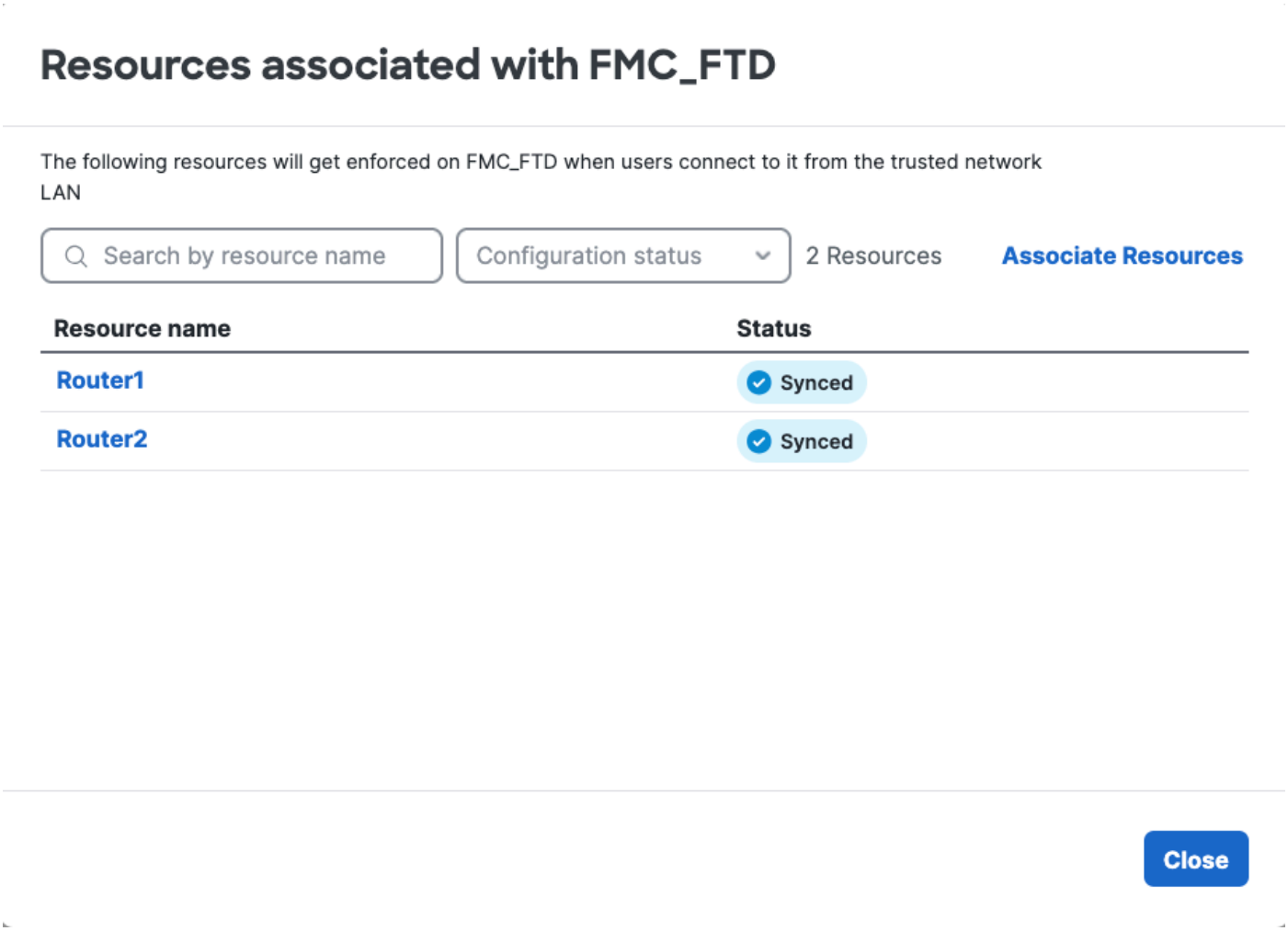


보안 액세스 - PR 확인

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

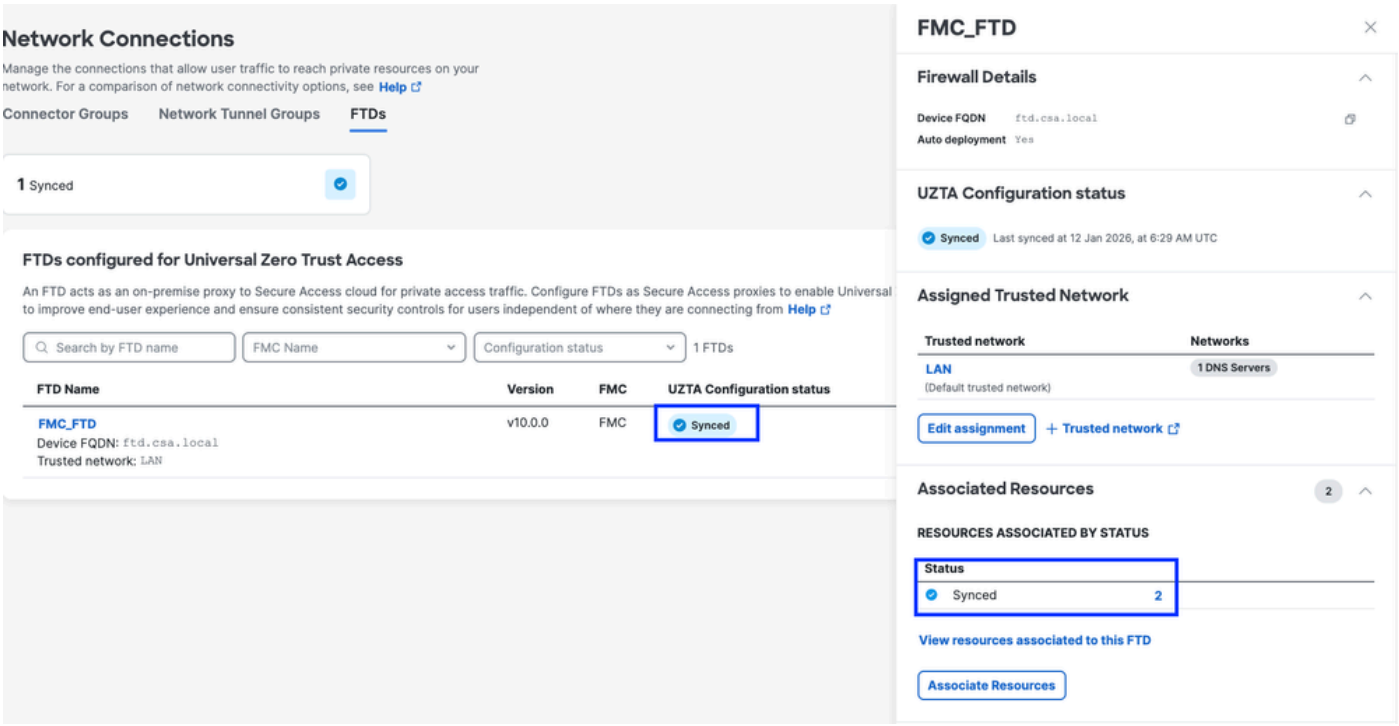

Network Connections
Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see Help
Connector Groups
Network Tunnel Groups
FTDs
1 Synced
FTDs configured for Universal Zero Trust Access
An FTD acts as an on-premise proxy 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
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
(Default trusted network)
1 DNS Servers
Edit assignment
+ Trusted network
Associated Resources
2
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
Search by resource name
Configuration status
2 Resources
Associate Resources
Resource name
Status
Router1
Synced
Router2
Synced
Close

3 . Close(닫기)를 클릭합니다

4. 상태, 관련 리소스 및 구성이 동기화 상태인지 확인합니다.



보안 액세스 - PR 확인

5. 구성이 FTD로 푸시되었는지 확인합니다.

FTD cli에 로그인하고 LINA 모드로 이동합니다.

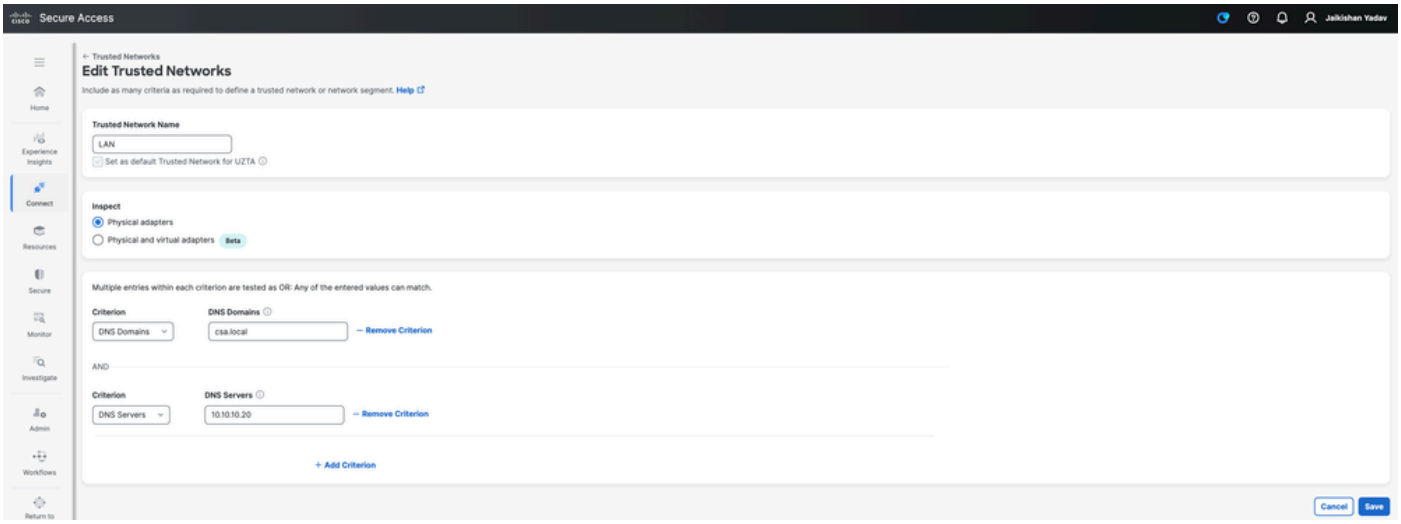
show running-config object application

```
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

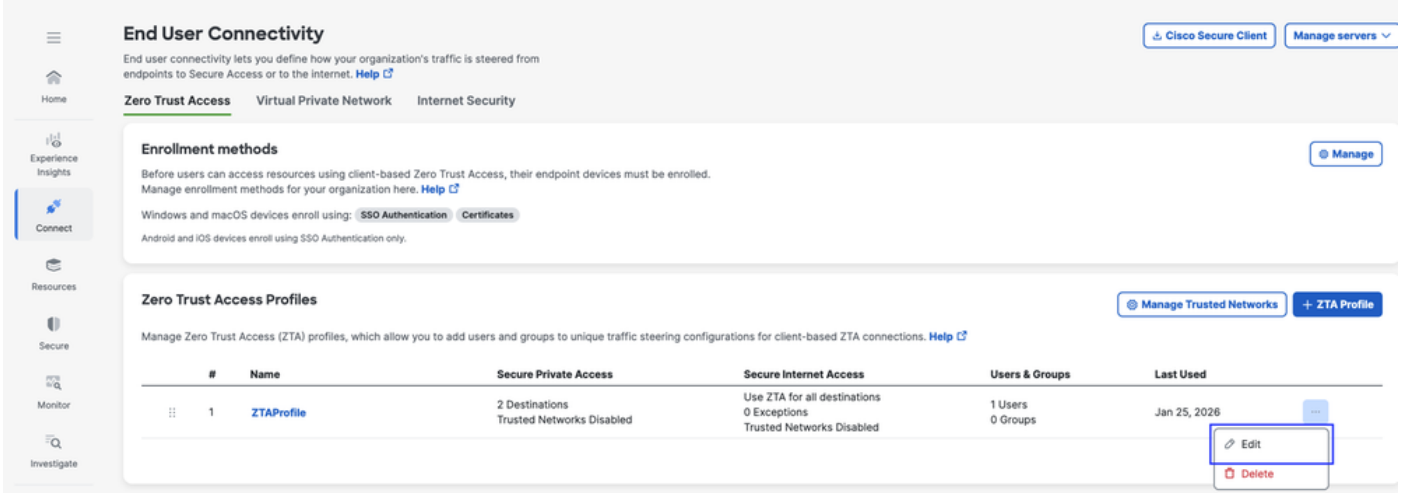
Connect(연결) > End User Connectivity(최종 사용자 연결) > Zero Trust Access(제로 트러스트 액세스) > ZTA Settings(ZTA 설정)로 이동하고 신뢰할 수 있는 네트워크를 구성합니다



보안 액세스 - TND 컨피그레이션

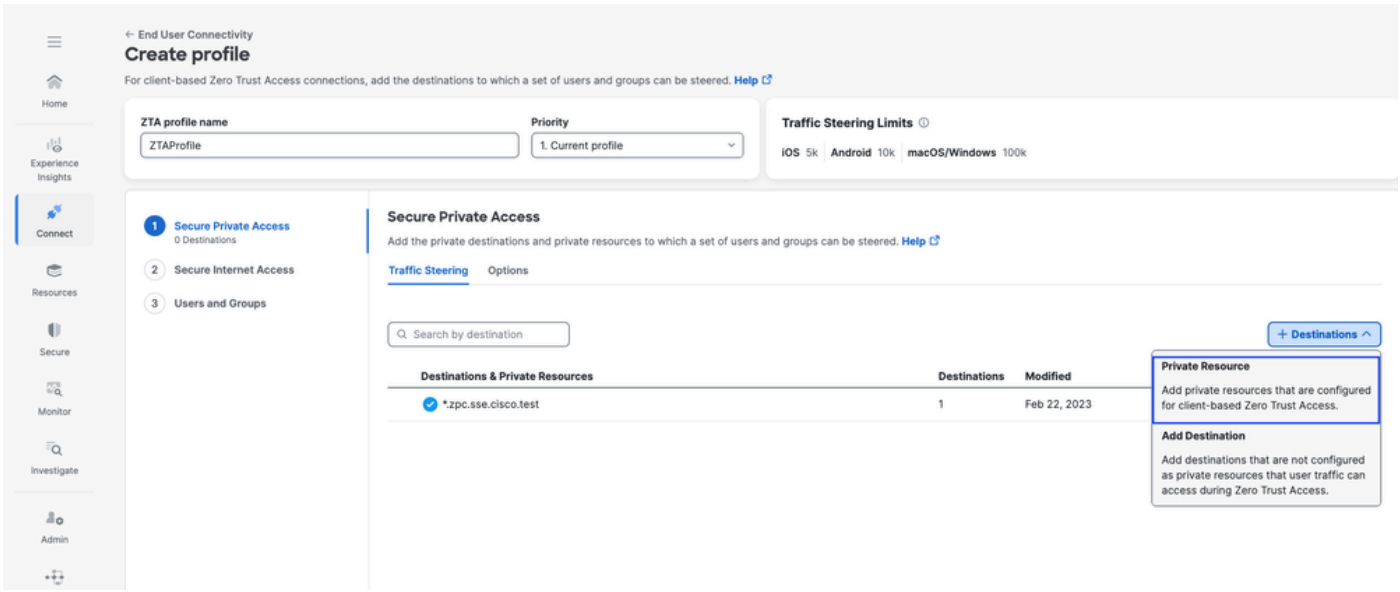
-5단계 ZTA 프로필에 프라이빗 리소스 추가

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

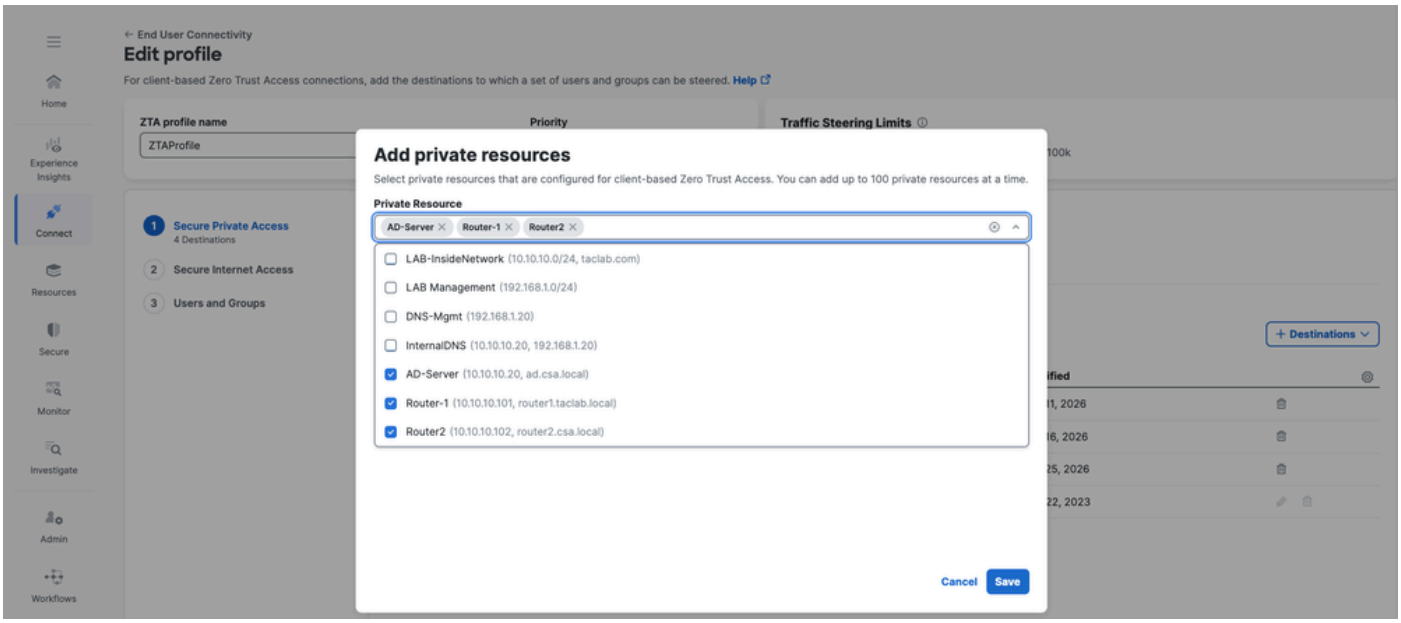


보안 액세스 - ZTA 프로필

2. 프라이빗 리소스 추가

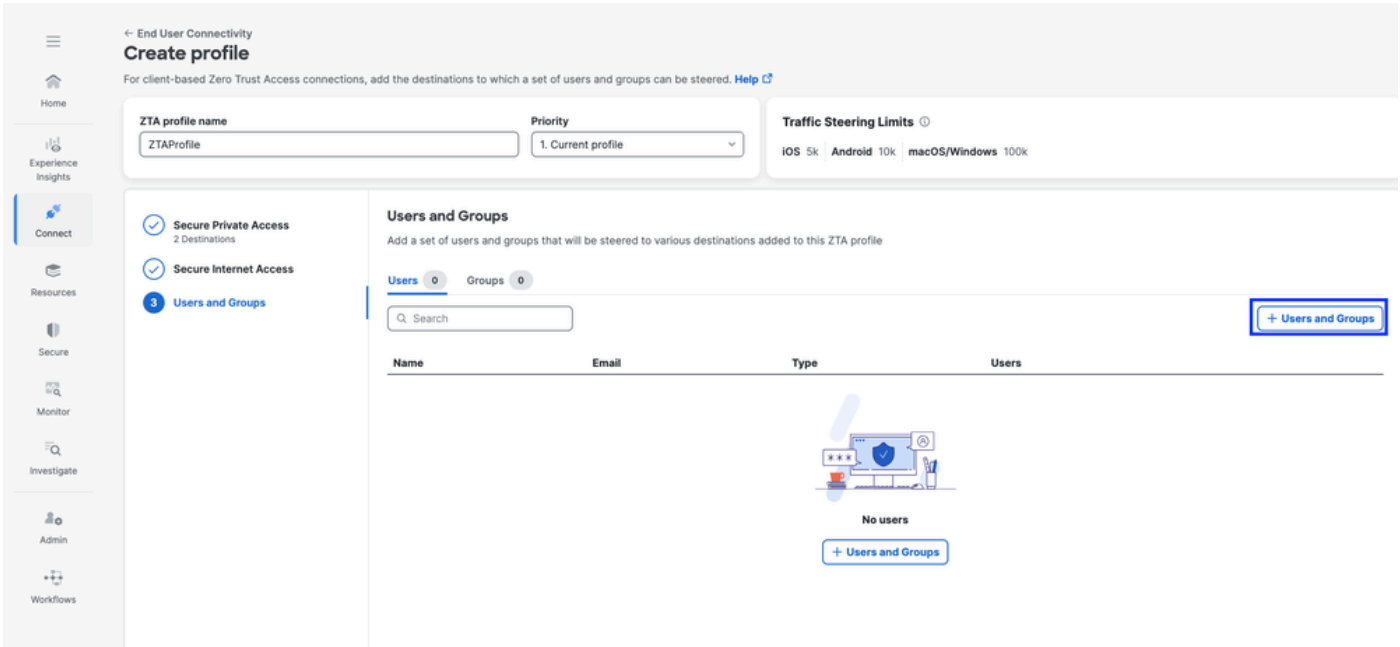


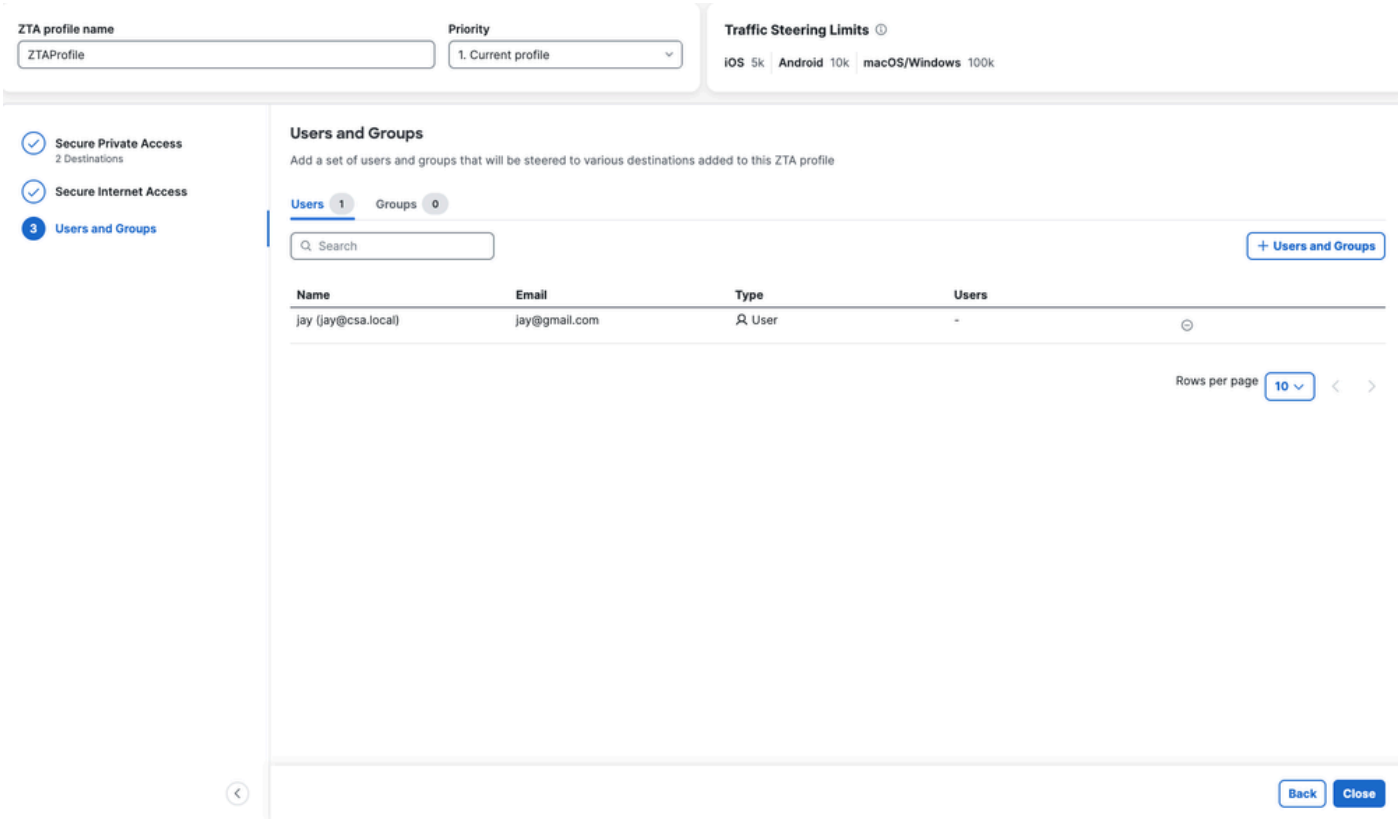
보안 액세스 - ZTA 프로필



보안 액세스 - ZTA 프로필

3 . 사용자 및 그룹 추가

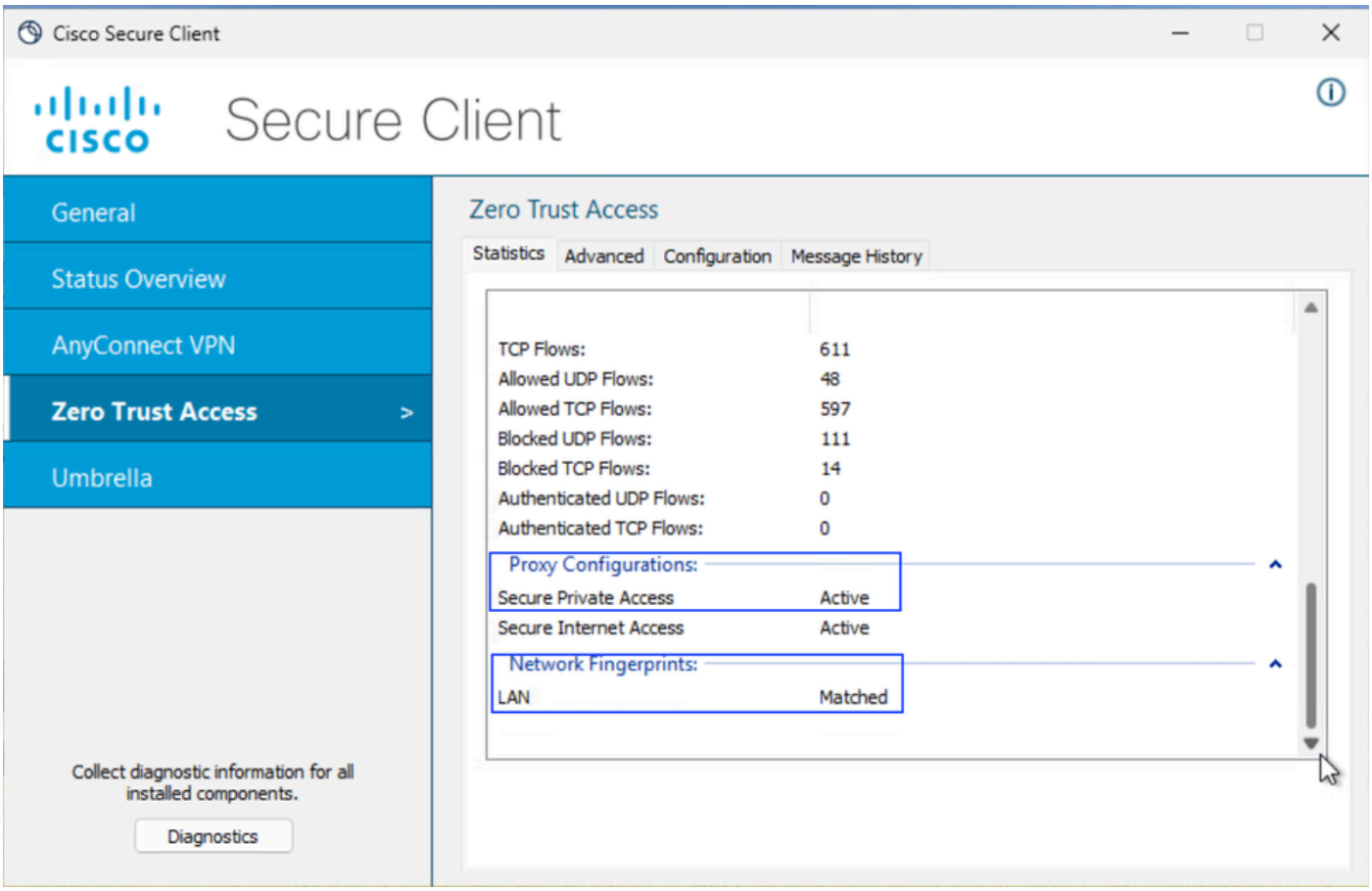




보안 액세스 - ZTA 프로필

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

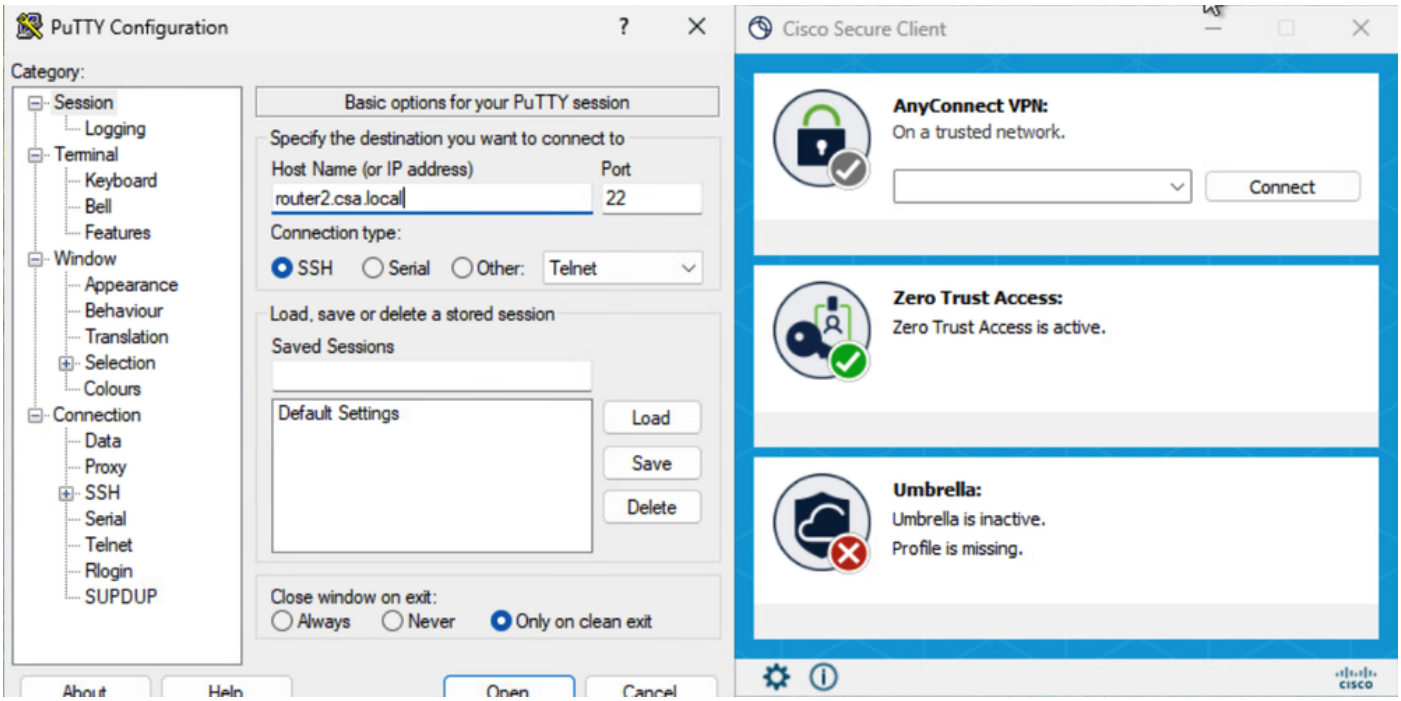
3. FQDN을 사용하여 FTD가 전용 리소스에 연결할 수 있는지 확인합니다.

```
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#
```

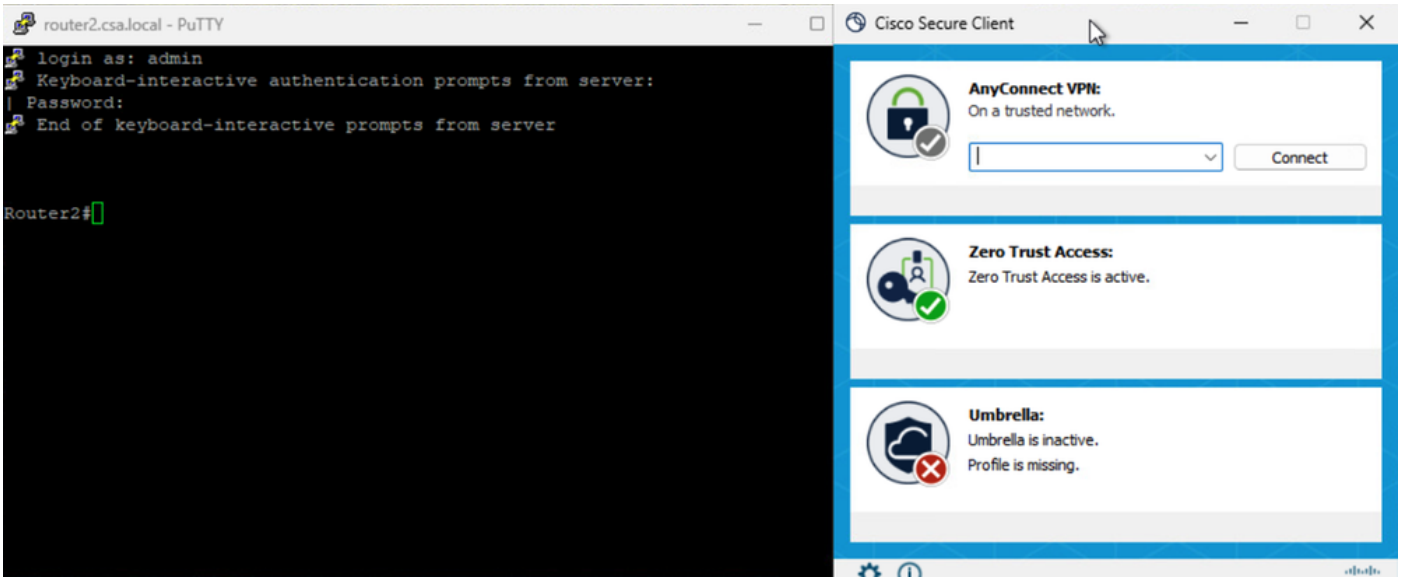
보안 액세스 - PR 테스트

4. 프라이빗 리소스에 대한 SSH 연결 테스트

FQDN을 사용하여 PR 액세스

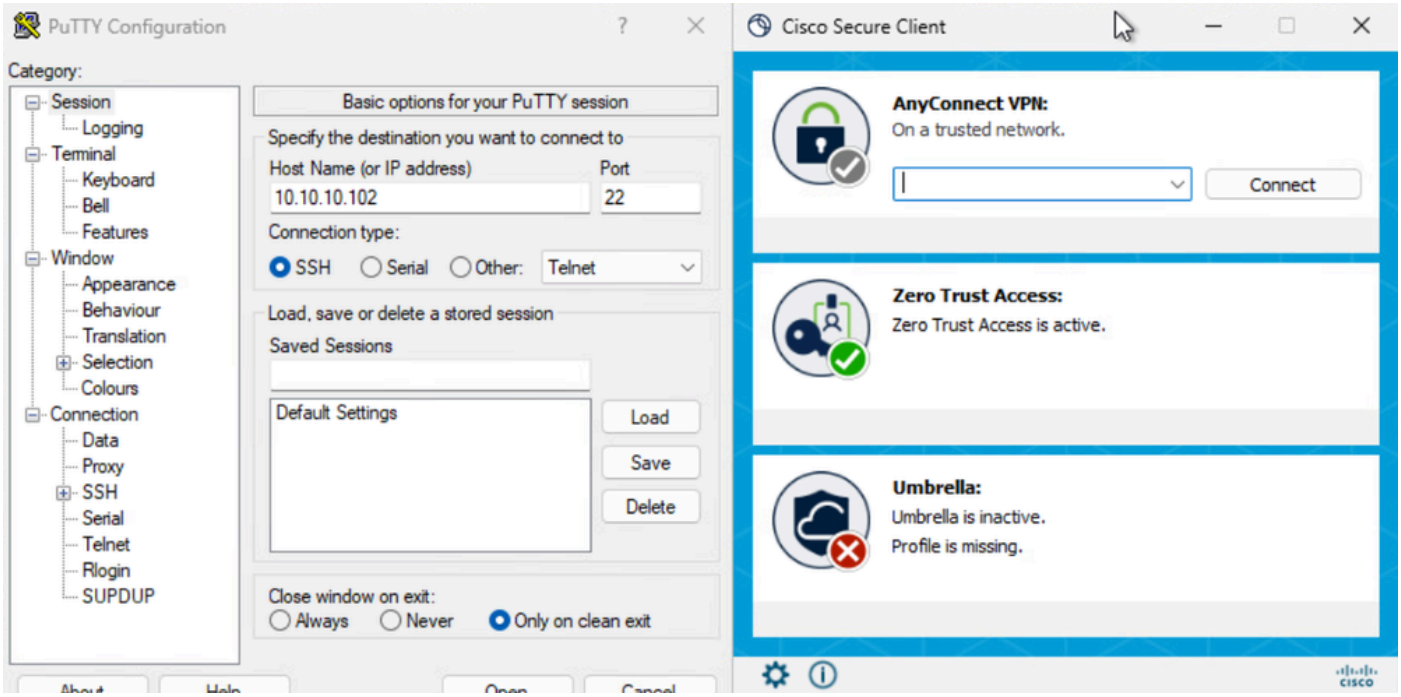


보안 액세스 - PR 테스트

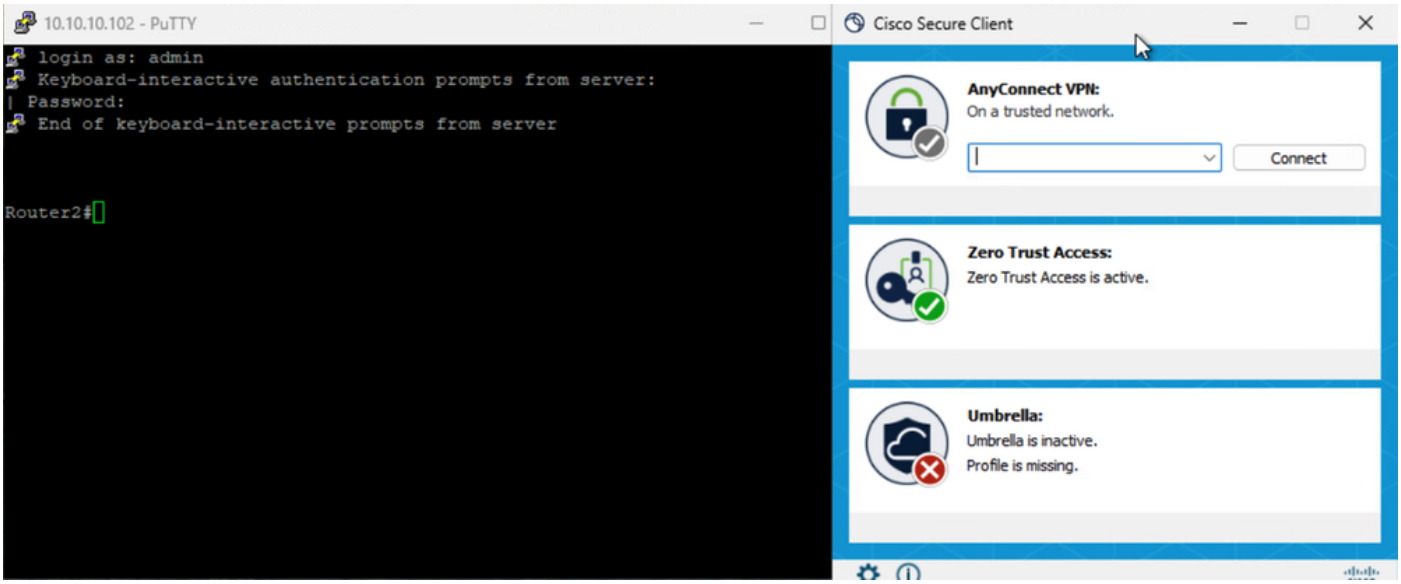


보안 액세스 - PR 테스트

IP 주소를 사용하여 PR에 액세스

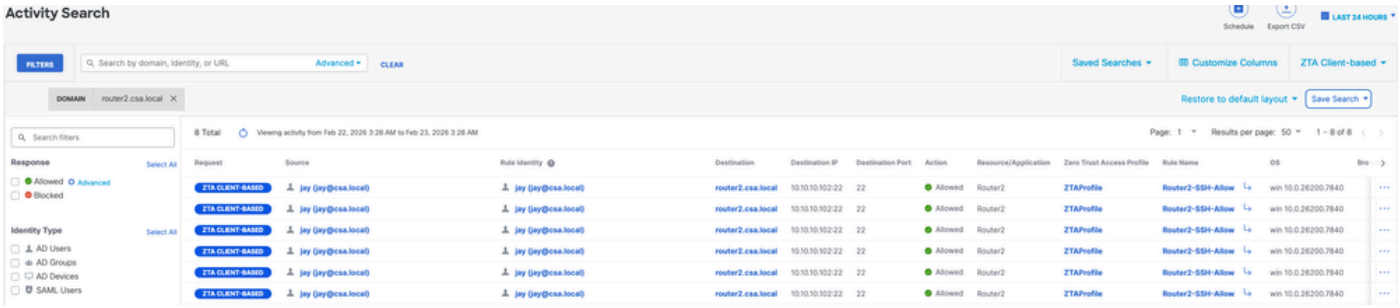


보안 액세스 - PR 테스트

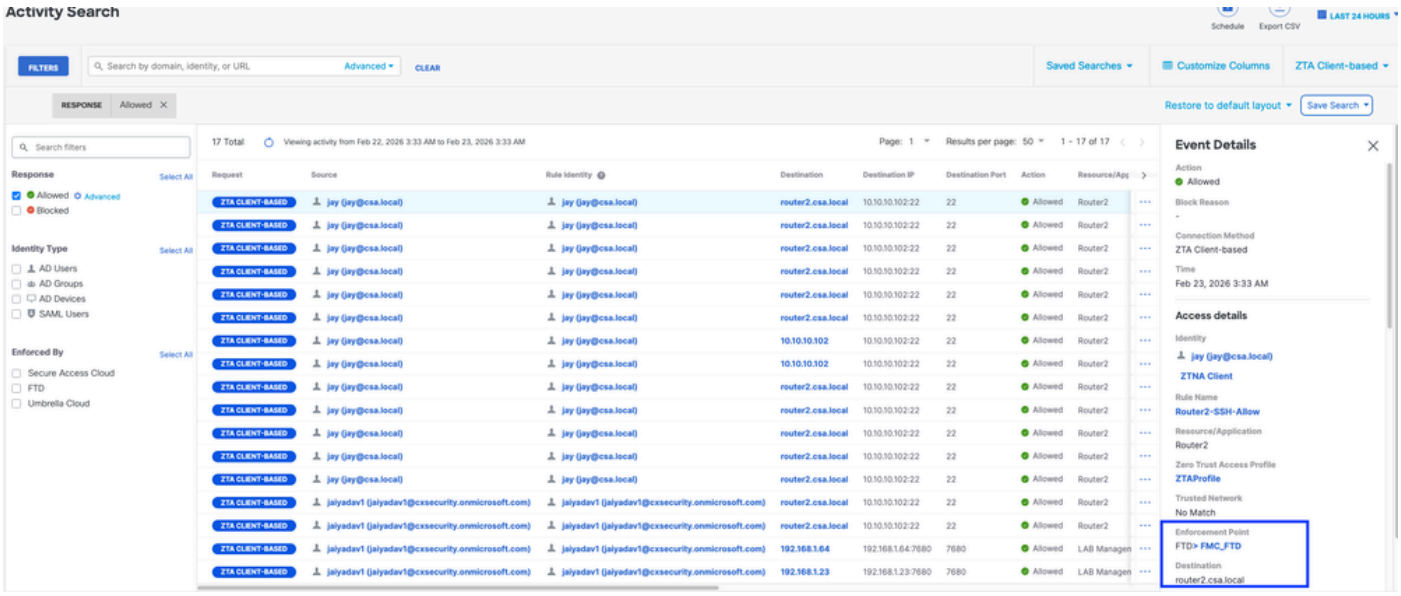


보안 액세스 - PR 테스트

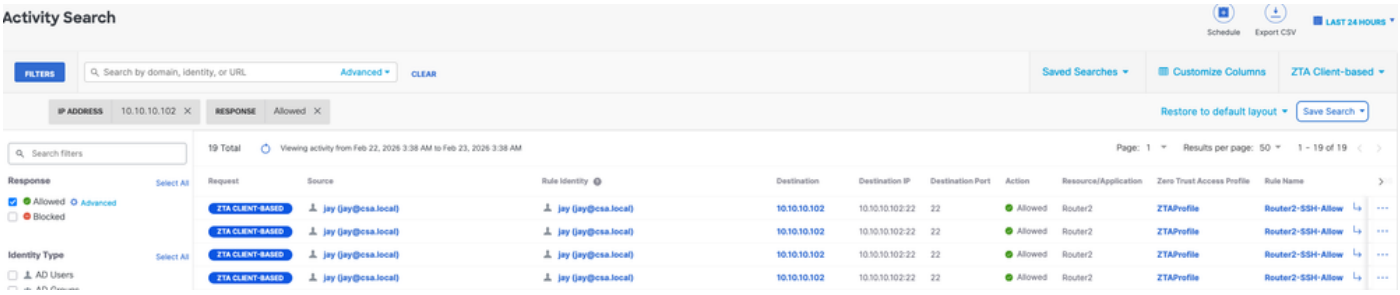
5. 보안 액세스 활동 검색 로그 확인



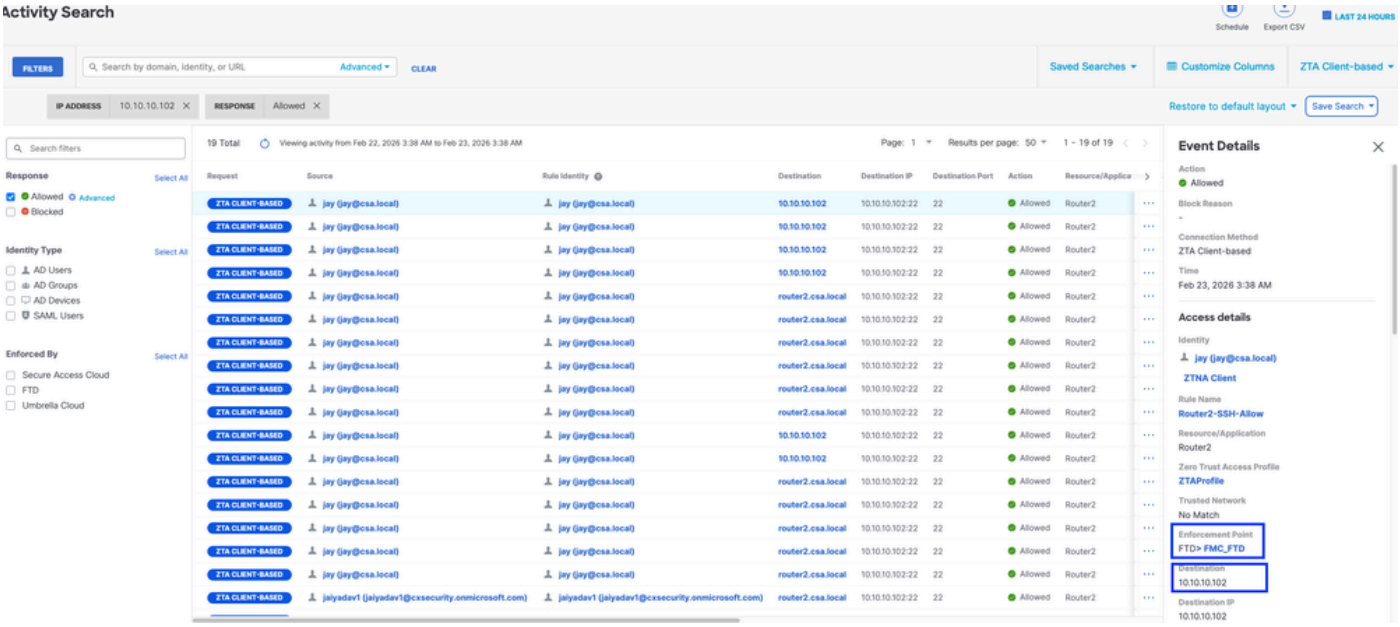
보안 액세스 - 활동 검색



보안 액세스 - 활동 검색

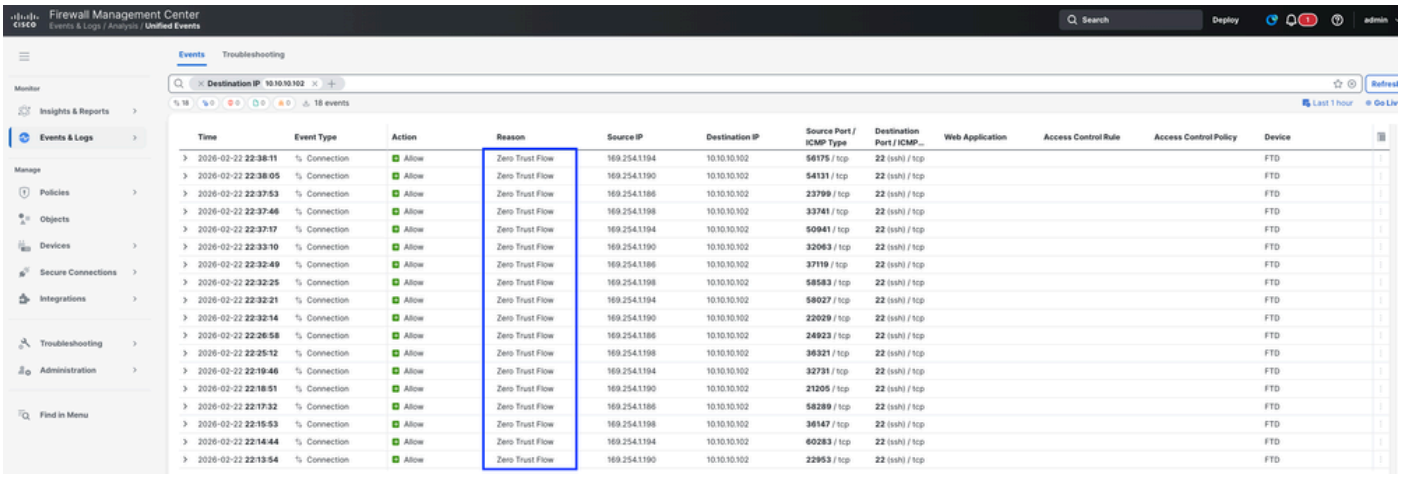


보안 액세스 - 활동 검색



보안 액세스 - 활동 검색

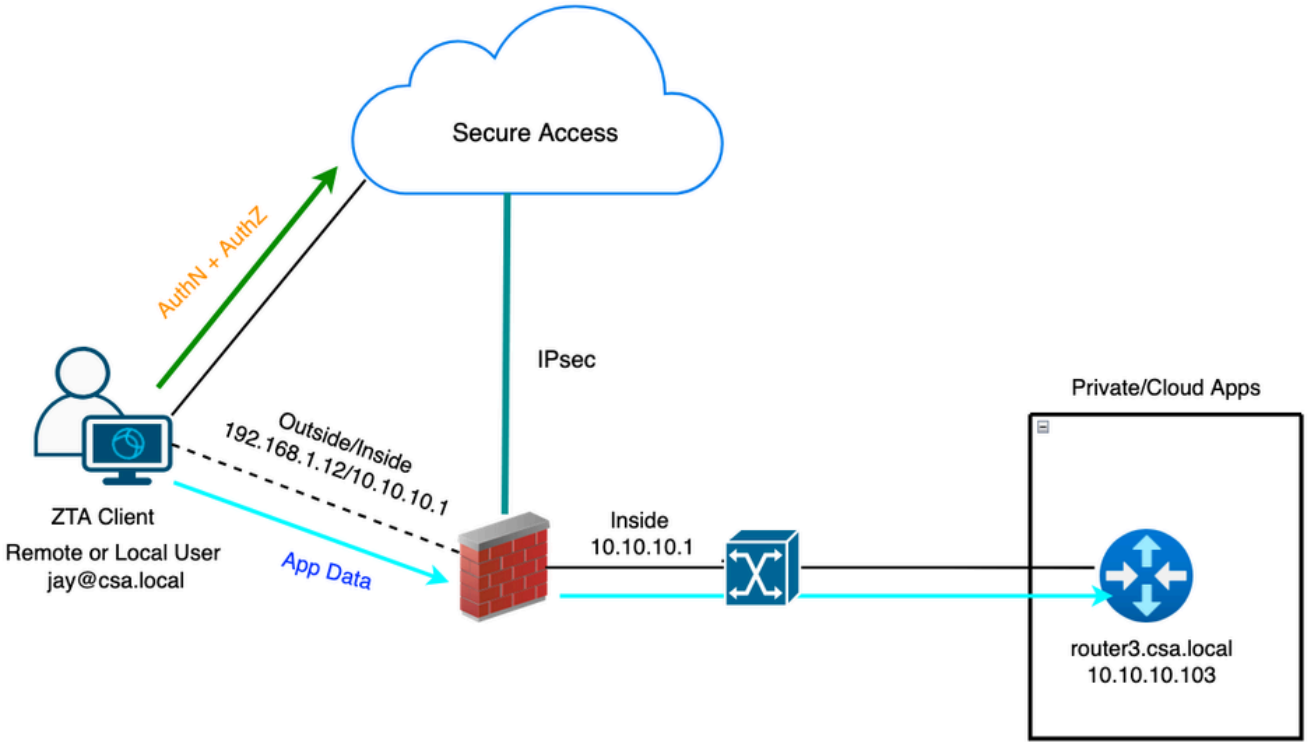
6. FMC 연결 이벤트 확인



FMC 연결 이벤트

테스트 사례 4 - 로컬 및 원격 사용자 - TND를 통한 로컬 또는 클라우드 시행

이 경우 시행 유형은 사용자 위치에 따라 다르며, 사용자가 로컬이거나 신뢰할 수 있는 FTD 영역(내부, DMZ 등) 뒤에 있으면 시행은 로컬이 됩니다(테스트 사례 3). 마찬가지로, 사용자가 원격이면 시행은 클라우드(테스트 사례 1)가 됩니다. 사용자 위치는 네트워크 핑거프린트 또는 TND 설정에 따라 결정되며, 네트워크 핑거프린트가 일치하면 사용자의 로컬이 로컬이 되고 일치하지 않으면 사용자 로컬이 원격으로 간주됩니다.

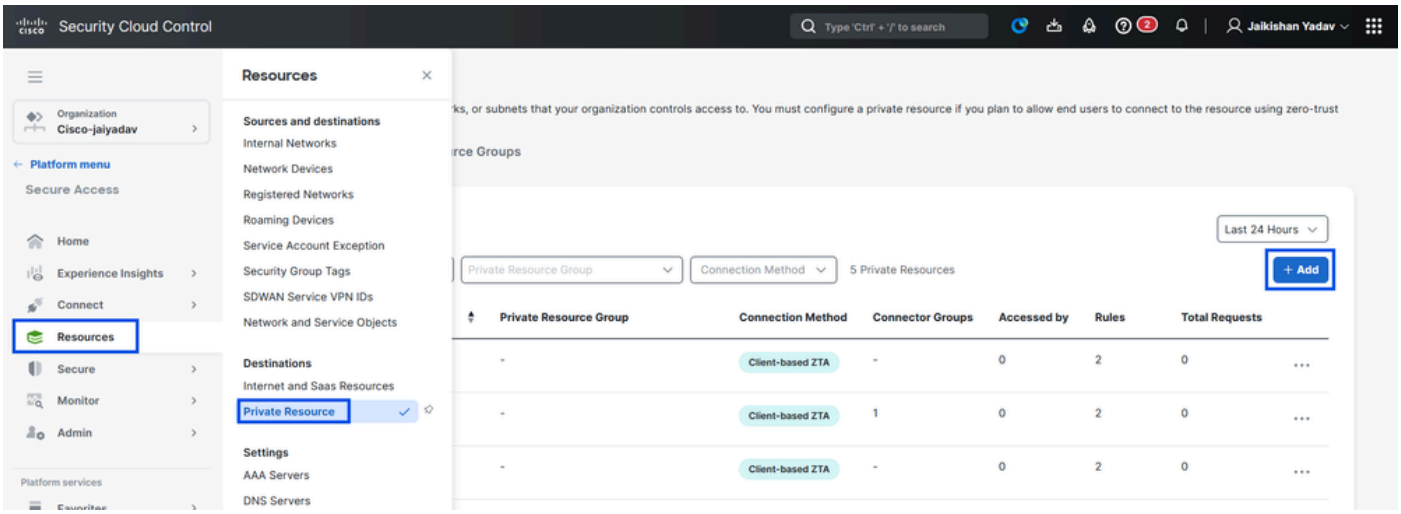


범용 ZTA - 테스트 사례 토폴로지

1단계 - Secure Access에서 프라이빗 리소스 정의

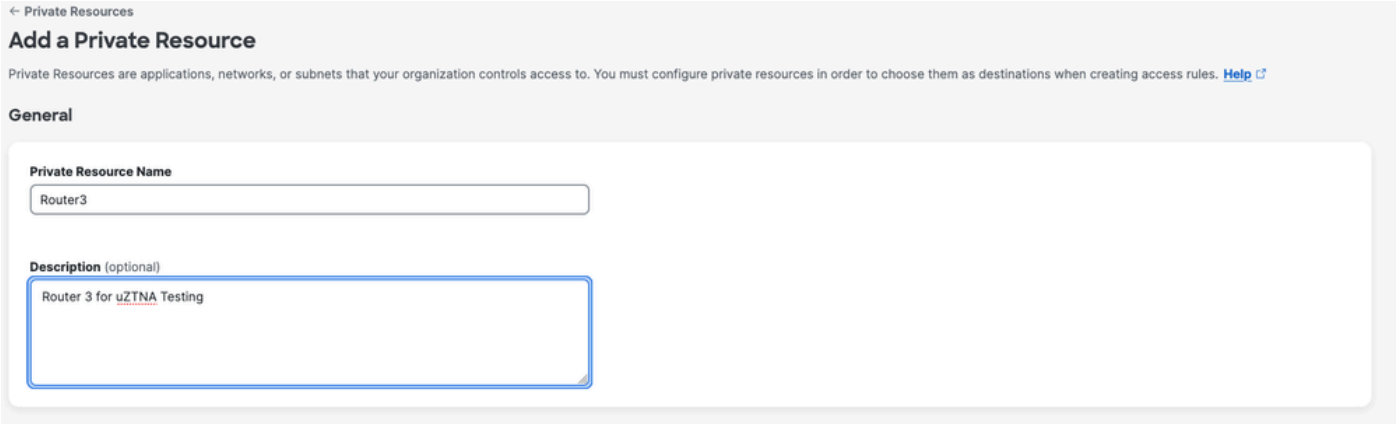
클라우드 시행으로 ZTA(Zero Trust Access) 등록된 디바이스를 통해 액세스할 수 있는 프라이빗 리소스 구성

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



보안 액세스 - 프라이빗 리소스 컨피그레이션

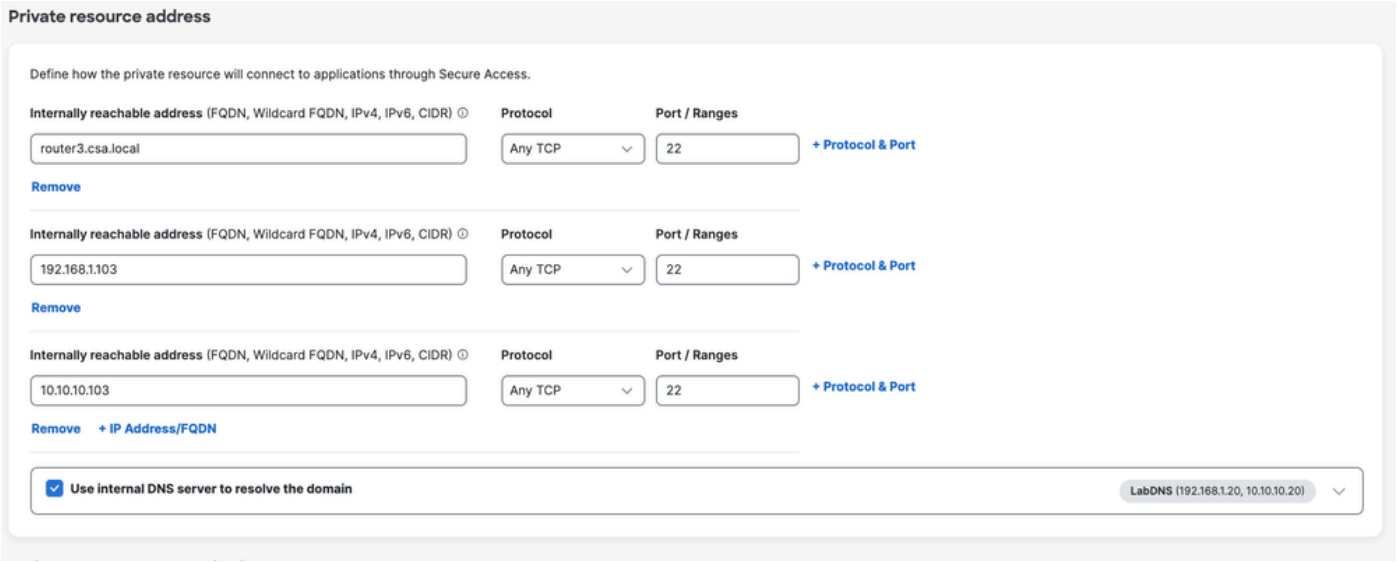
2. 개인 자원명에는 유의미한 자원명을 입력합니다. 설명의 경우, 리소스의 용도 또는 리소스 소유자의 이름과 같은 정보를 제공하는 것이 좋습니다.



보안 액세스 - 프라이빗 리소스 컨피그레이션

3. 액세스하려는 개인 자원의 FQDN을 입력합니다. 프라이빗 리소스의 IP 주소도 정의할 수 있습니다. 자세한 내용은 프라이빗 리소스 추가를 참조하십시오

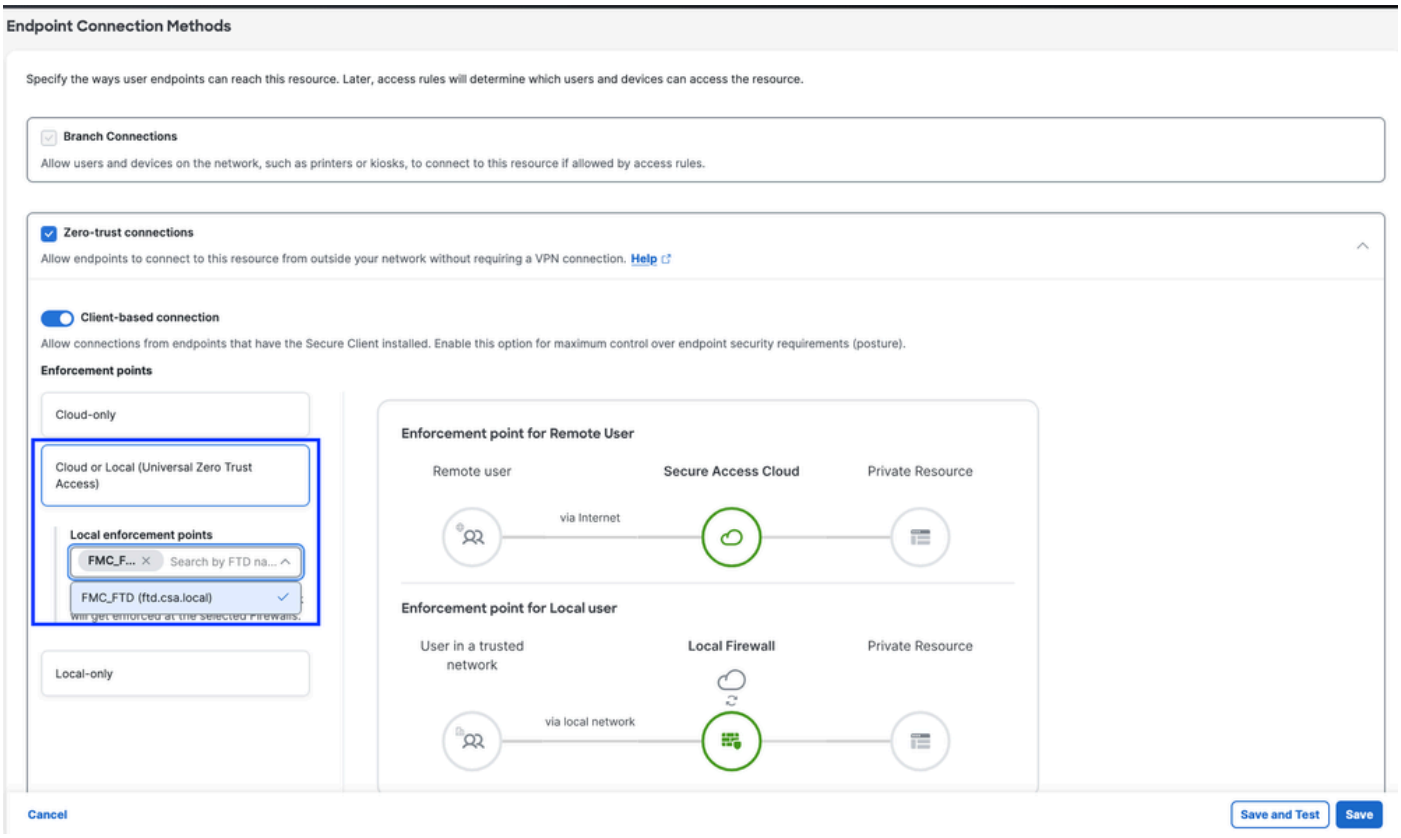
4. 도메인을 확인할 DNS 서버를 선택합니다



보안 액세스 - 프라이빗 리소스 컨피그레이션

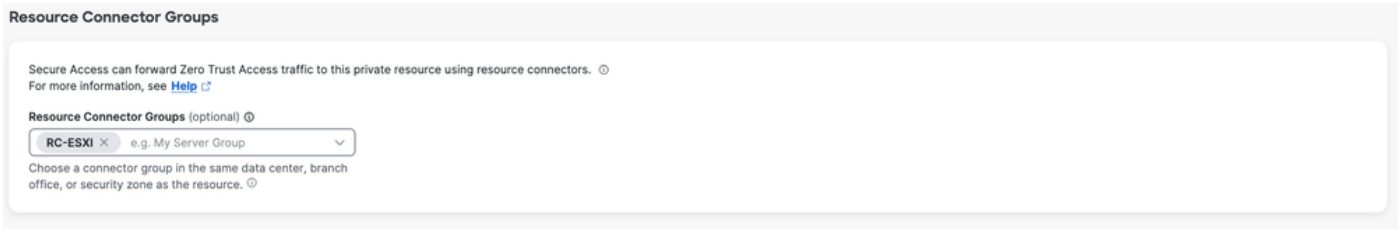
5. 엔드포인트 연결 방법 선택

6. FTD를 로컬 적용 지점으로 선택합니다



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.



보안 액세스 - 프라이빗 리소스 컨피그레이션

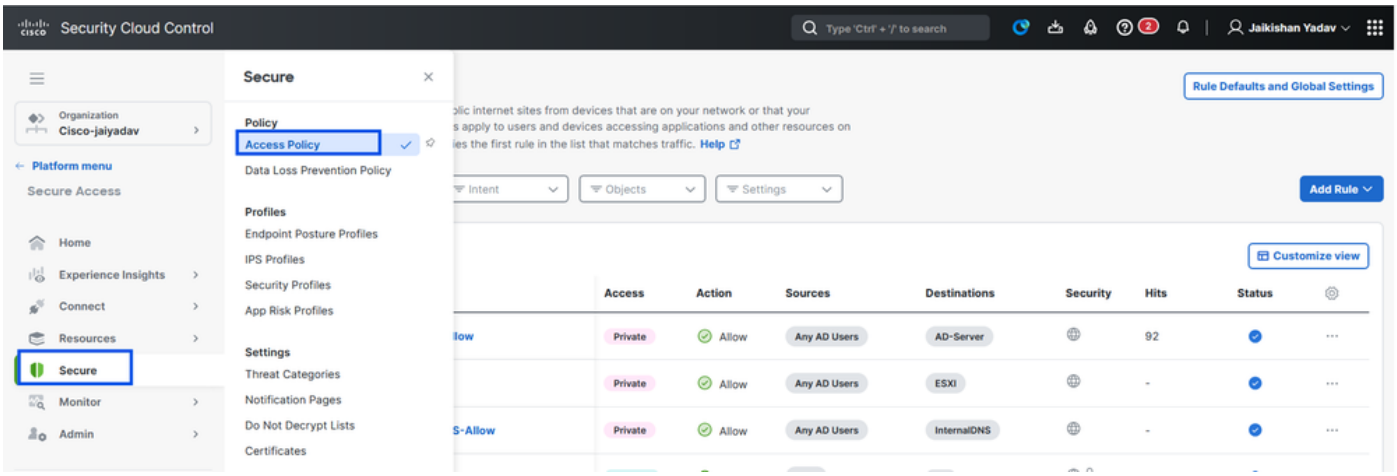
참고: 선택하는 등록 유형에 따라 이 변경 사항은 PR을 FTD에 자동으로 연결하고 정책 구축을 트리거합니다

7 . Save(저장)를 클릭합니다.

2단계 - 개인 액세스 규칙 생성

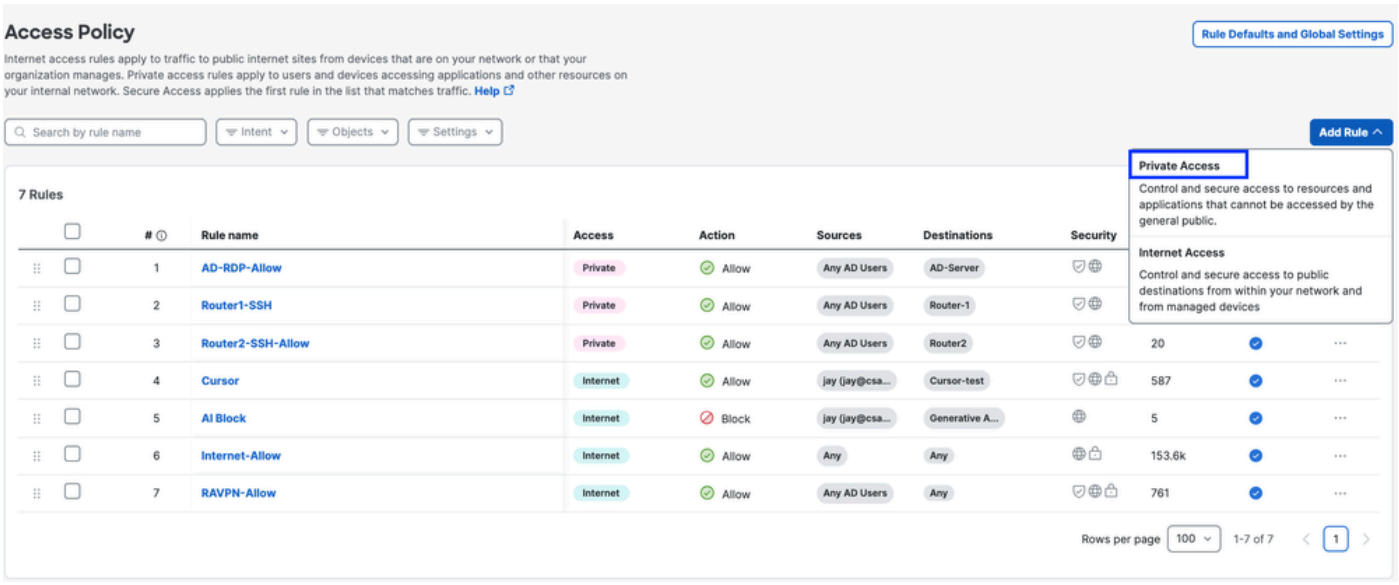
Universal ZTA 등록된 사용자가 액세스할 수 있도록 Secure Access의 비공개 액세스를 구성합니다 . 자세한 내용은 [개인 액세스 규칙을 참조하십시오]

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



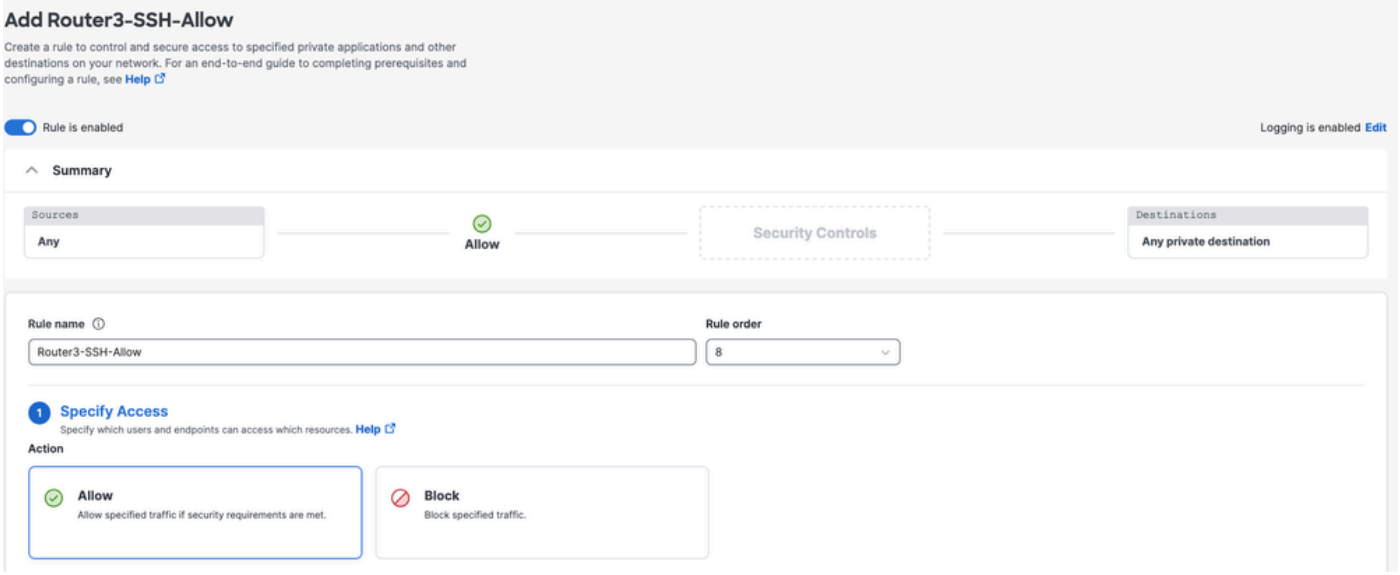
보안 액세스 - 액세스 정책 컨피그레이션

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



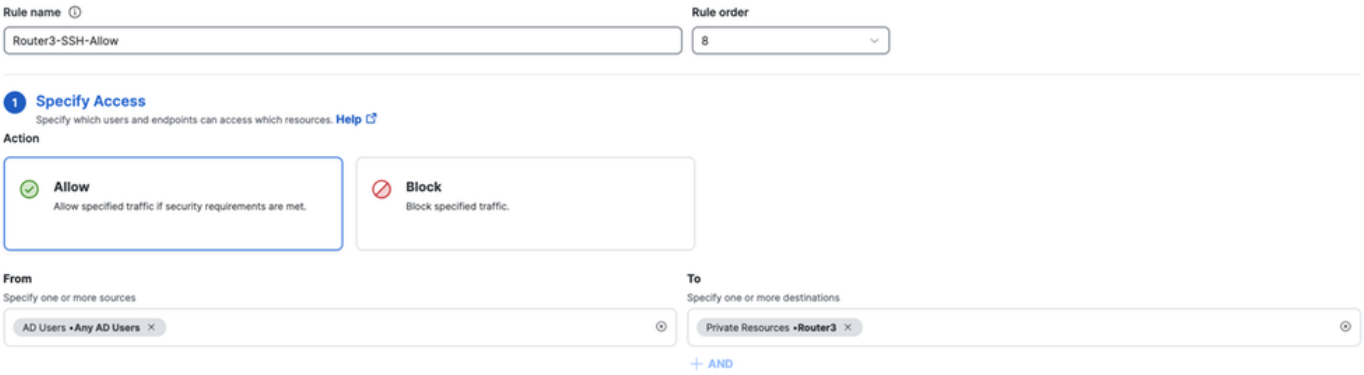
보안 액세스 - 액세스 정책 컨피그레이션

3. 규칙 이름 추가



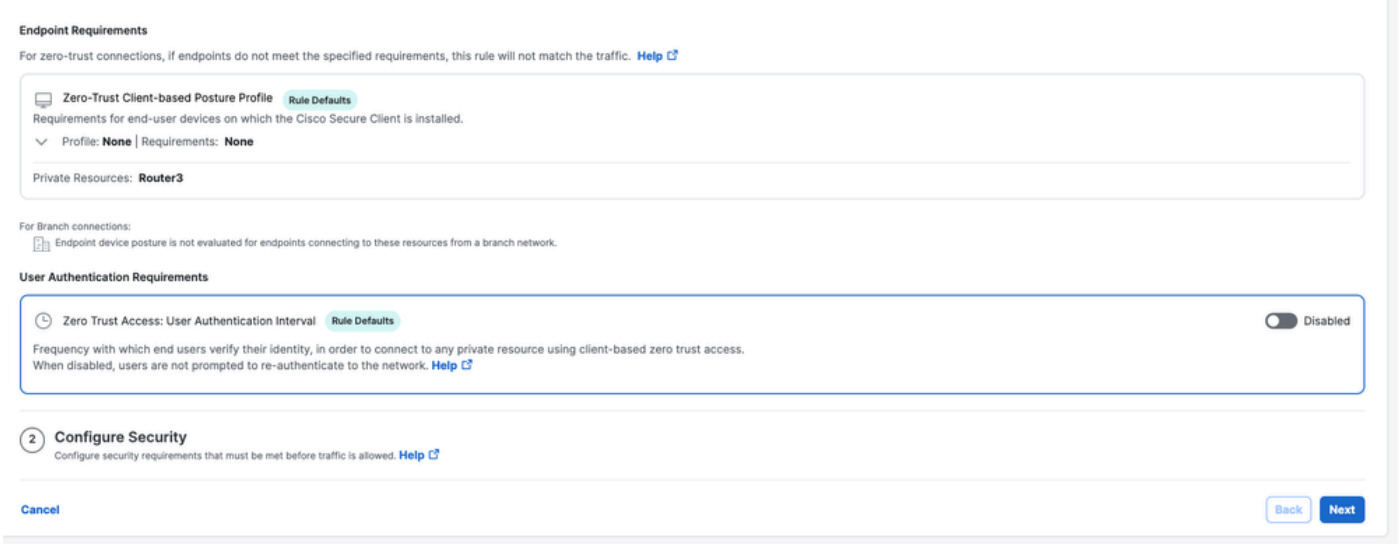
보안 액세스 - 액세스 정책 컨피그레이션

4. 규칙 조치를 선택하고 출처 및 대상을 선택합니다



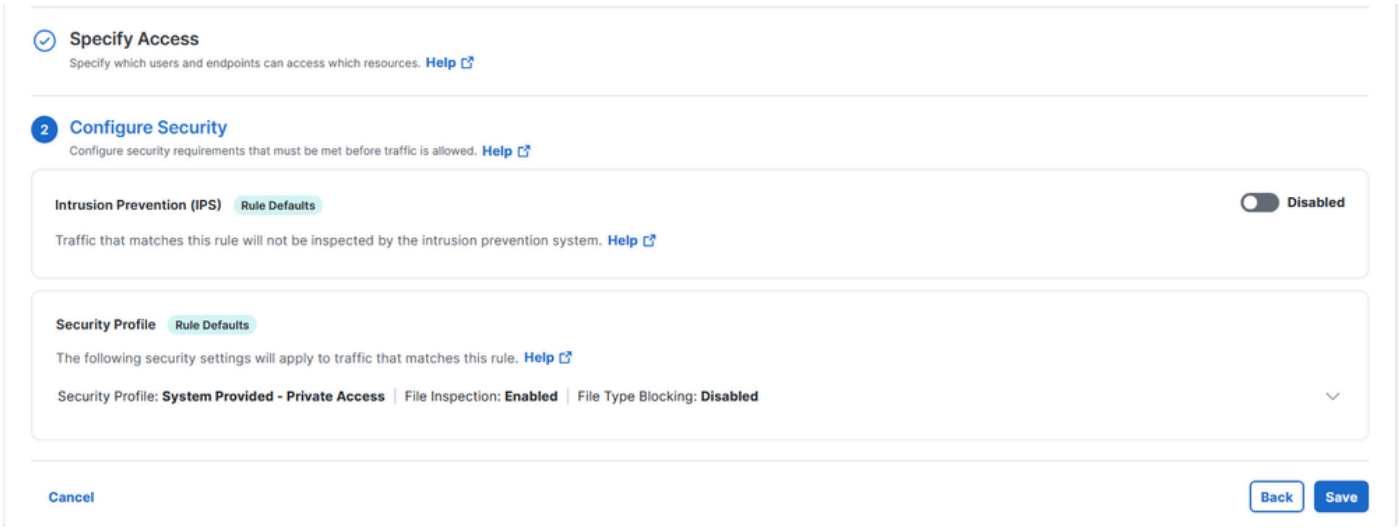
보안 액세스 - 액세스 정책 컨피그레이션

5. 엔드포인트 요구 사항 구성



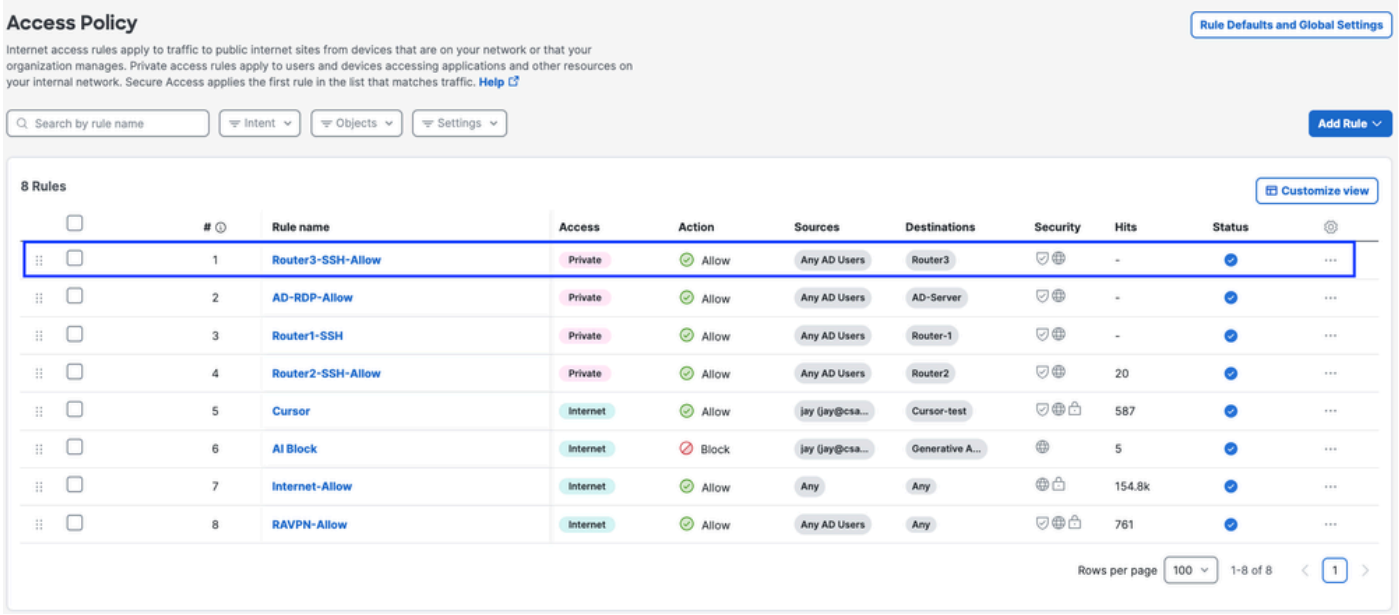
보안 액세스 - 액세스 정책 컨피그레이션

6. 보안 구성



보안 액세스 - 액세스 정책 컨피그레이션

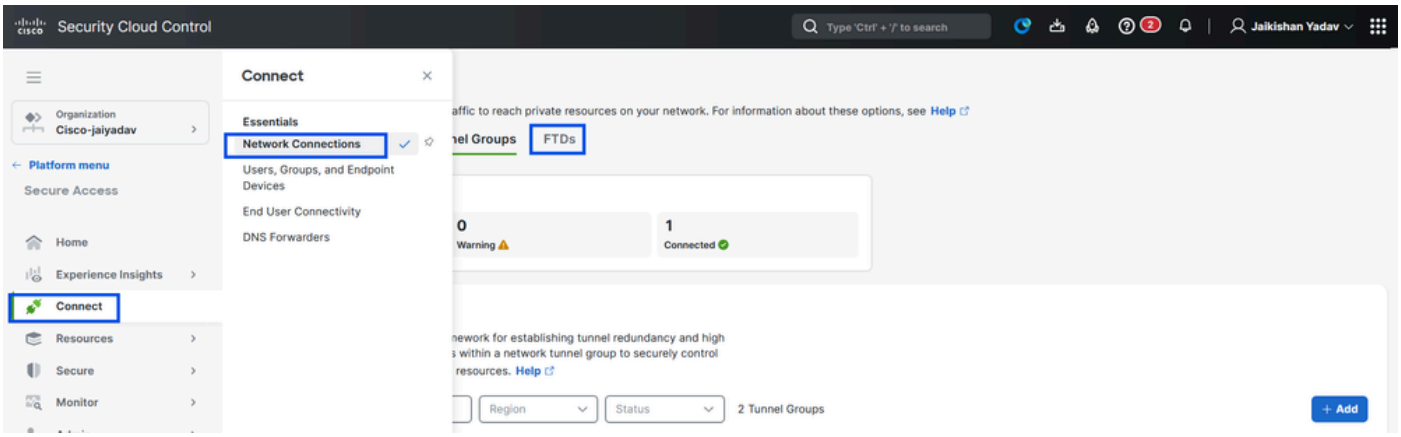
7. 저장을 클릭합니다.



보안 액세스 - 액세스 정책 컨피그레이션

3단계 - FTD에서 PR 연결 확인

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

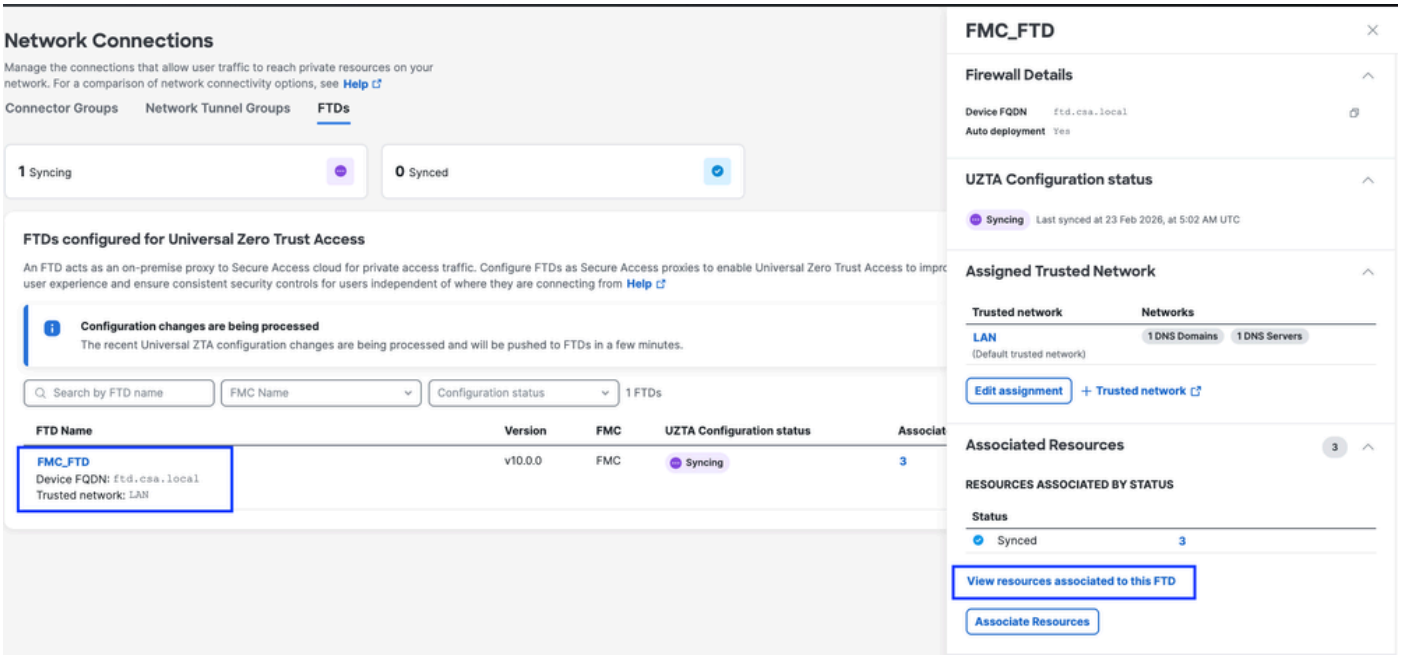


보안 액세스 - PR 확인

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
```

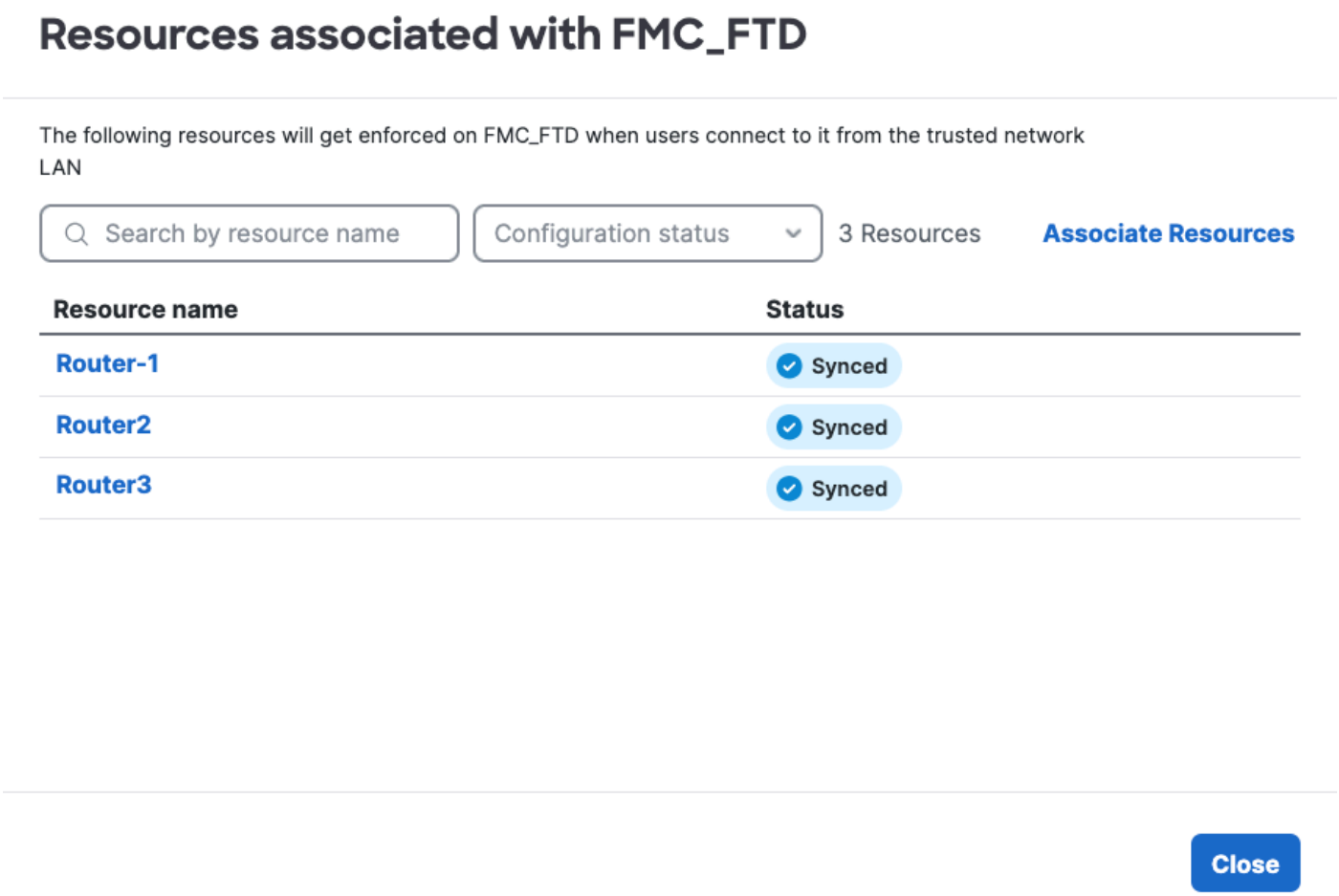
보안 액세스 - PR 확인



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
```

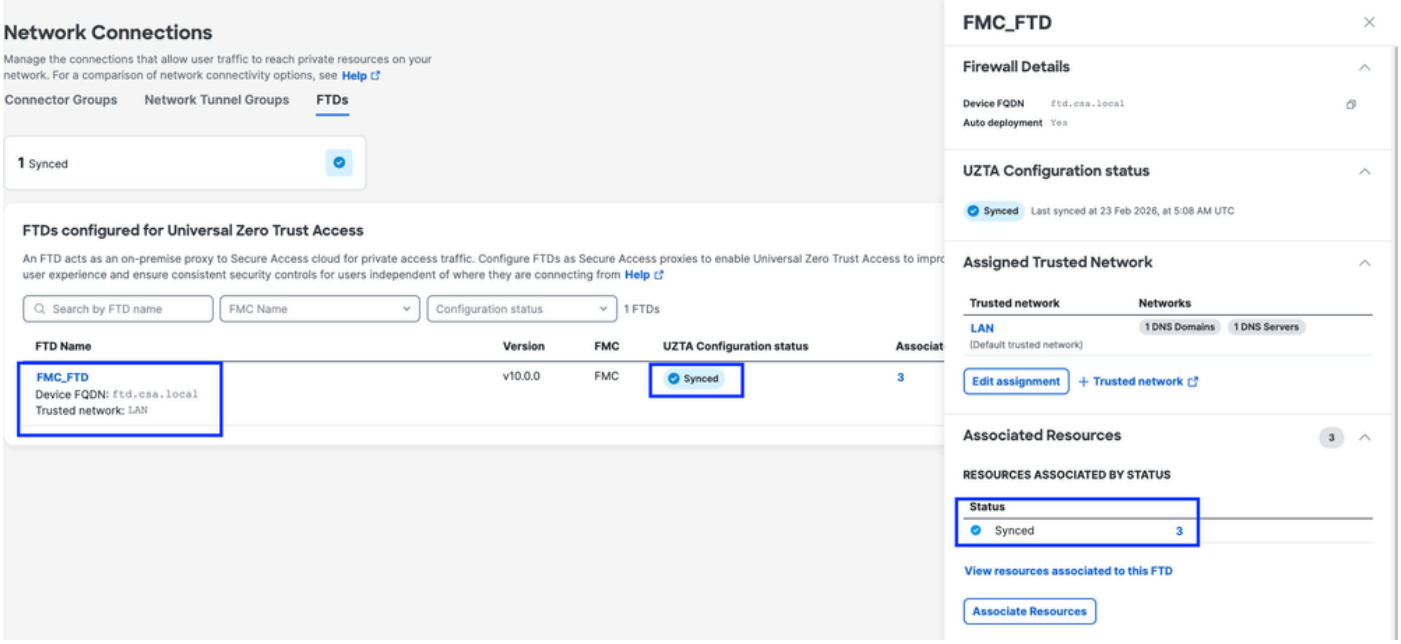
보안 액세스 - PR 확인



보안 액세스 - PR 확인

3 . Close(닫기)를 클릭합니다

4. 상태, 관련 리소스 및 구성이 동기화 상태인지 확인합니다.



보안 액세스 - PR 확인

5. 구성이 FTD로 푸시되었는지 확인합니다.

FTD cli에 로그인하고 LINA 모드로 이동합니다.

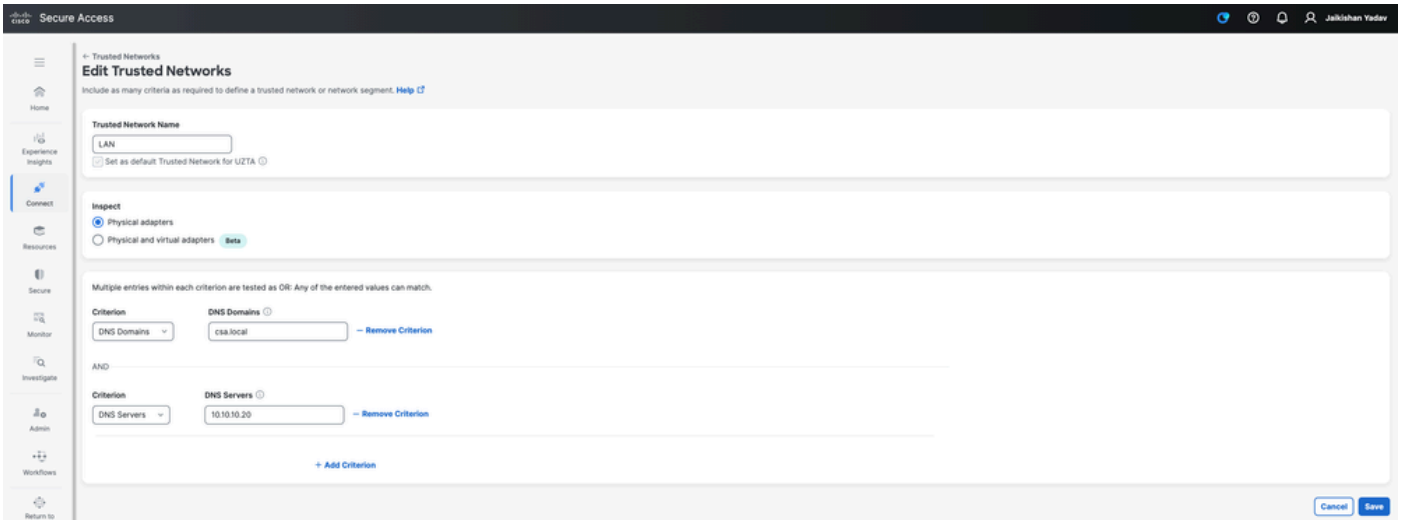
show running-config object application

```
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

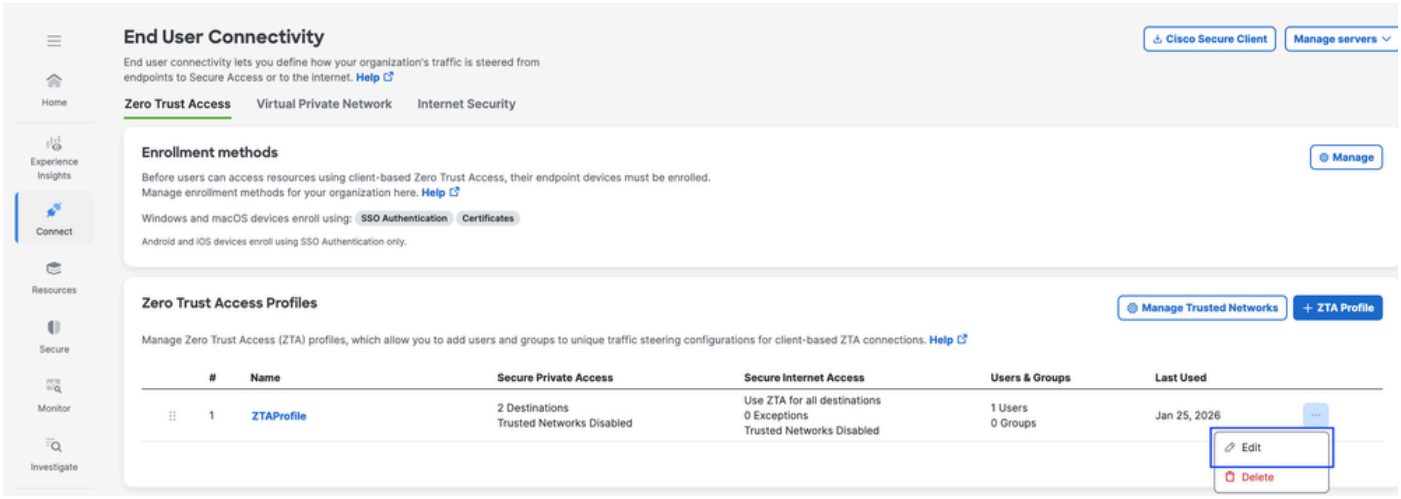
Connect(연결) > End User Connectivity(최종 사용자 연결) > Zero Trust Access(제로 트러스트 액세스) > ZTA Settings(ZTA 설정)로 이동하고 신뢰할 수 있는 네트워크를 구성합니다



보안 액세스 - ZTA TND 컨피그레이션

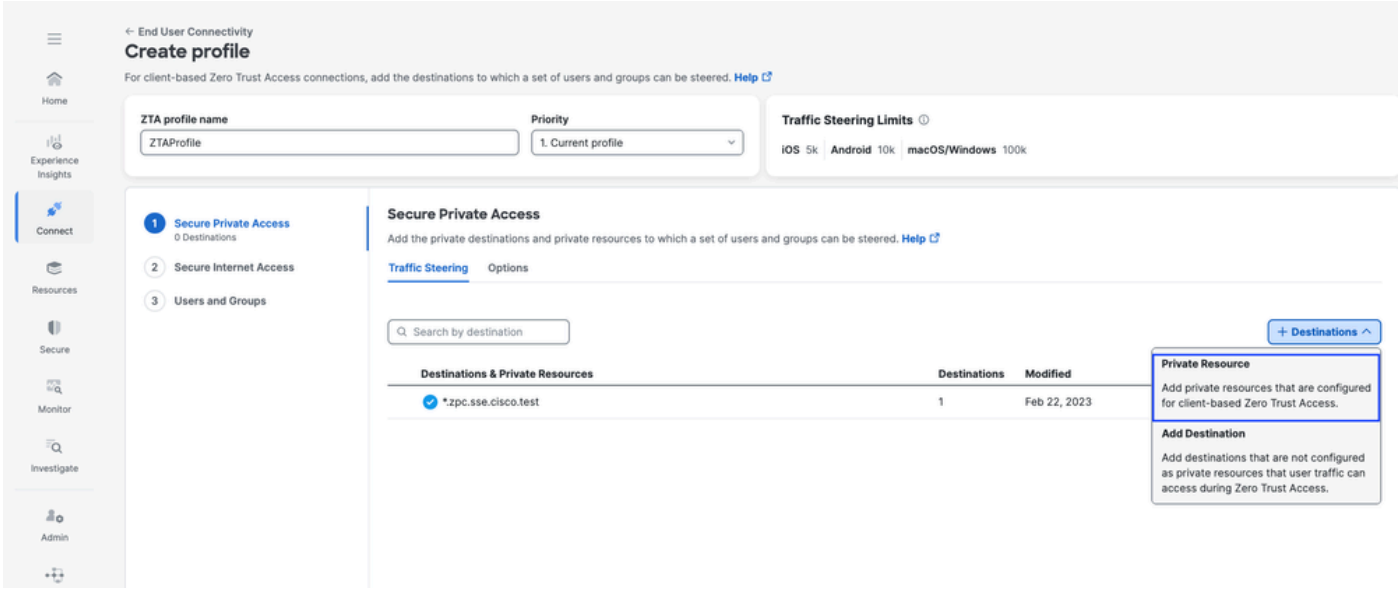
단계 - 5 ZTA 프로필에 프라이빗 리소스 추가

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

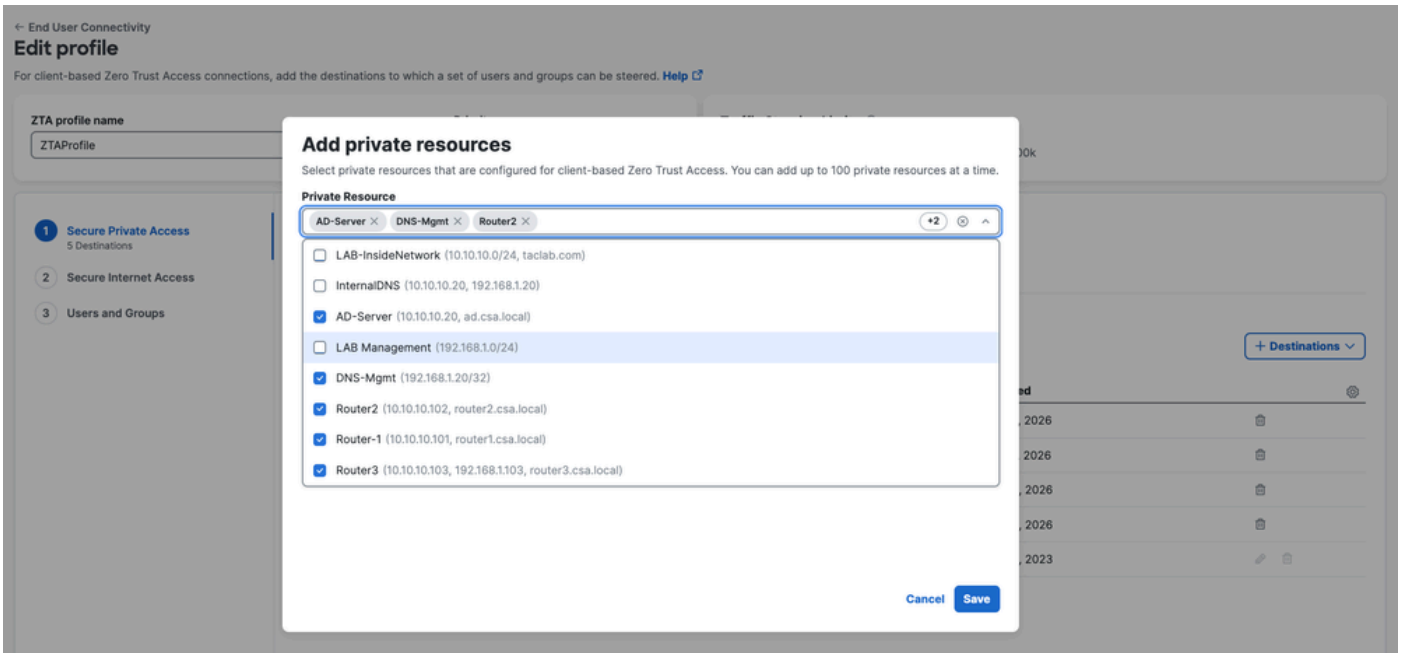


보안 액세스 - ZTA 프로필

2. 프라이빗 리소스 추가

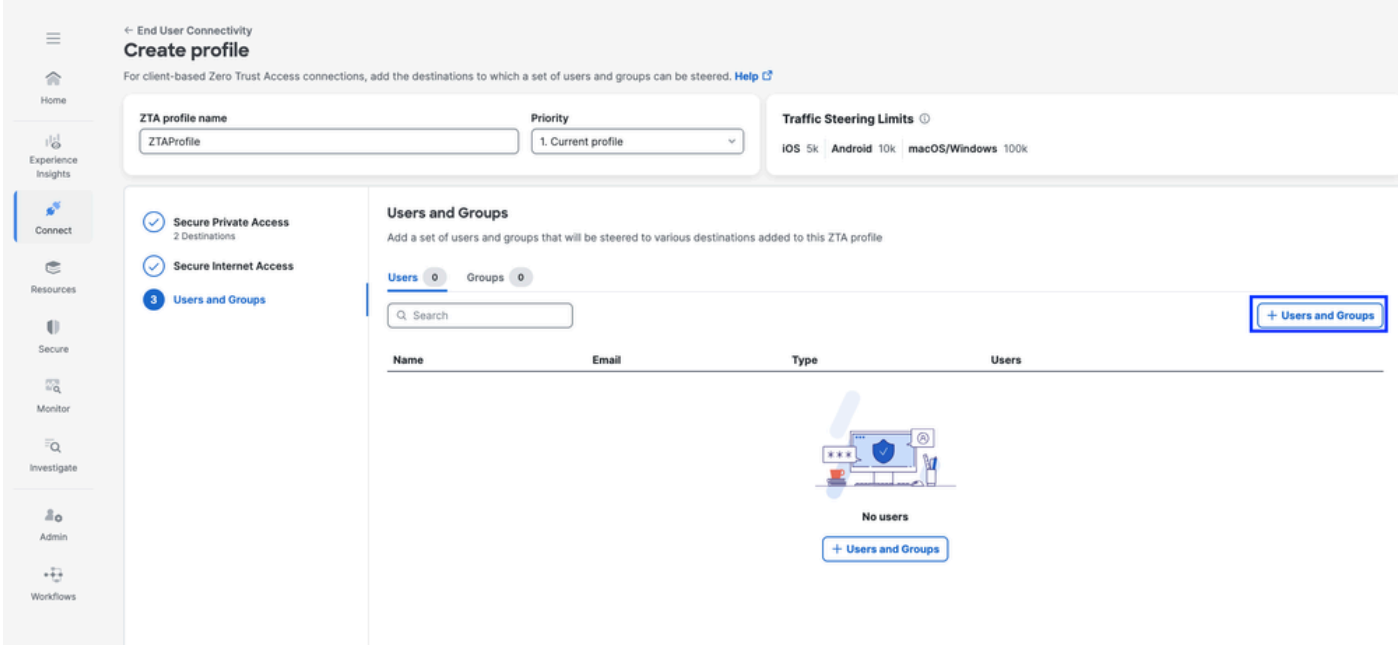


보안 액세스 - ZTA 프로필

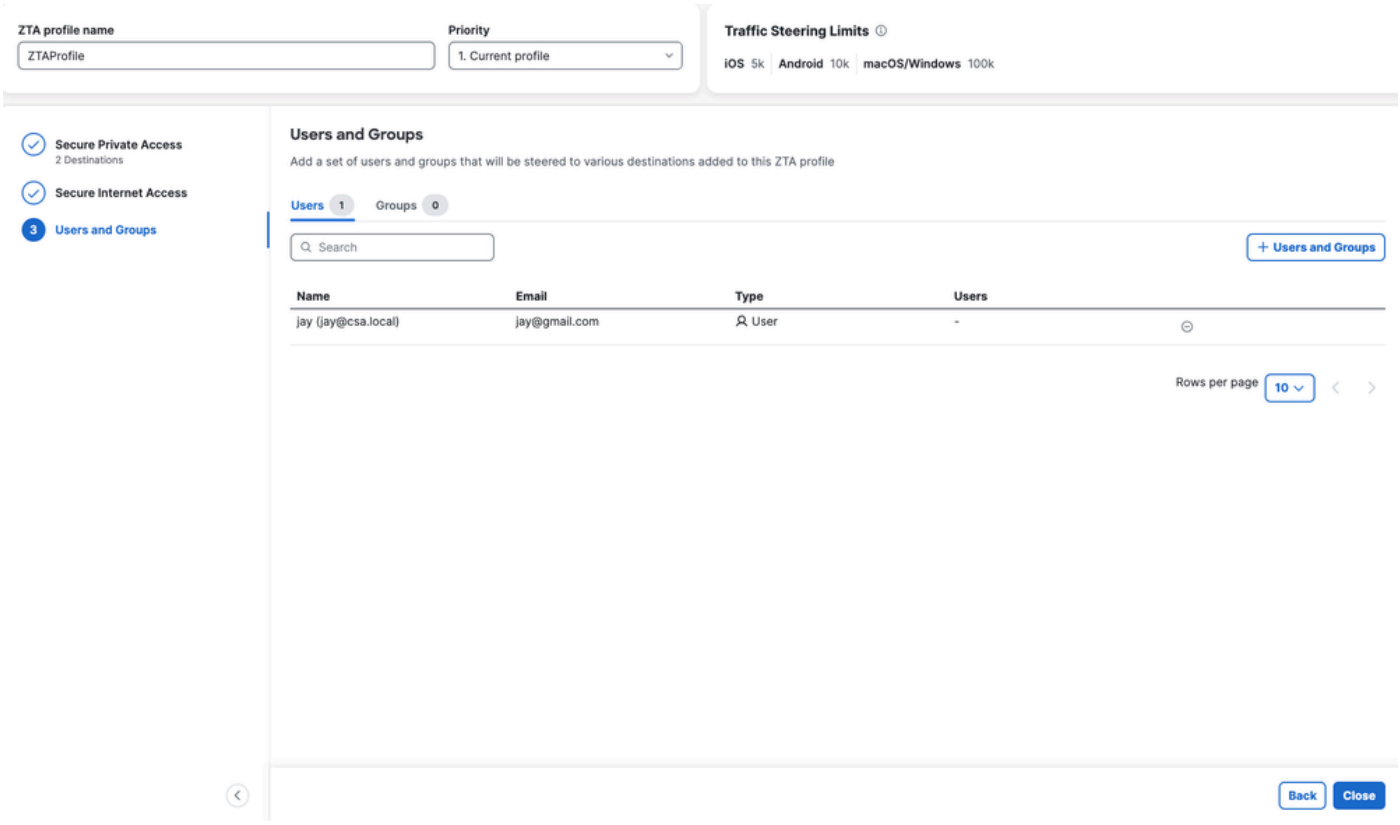


보안 액세스 - ZTA 프로필

3 . 사용자 및 그룹 추가



보안 액세스 - ZTA 프로필

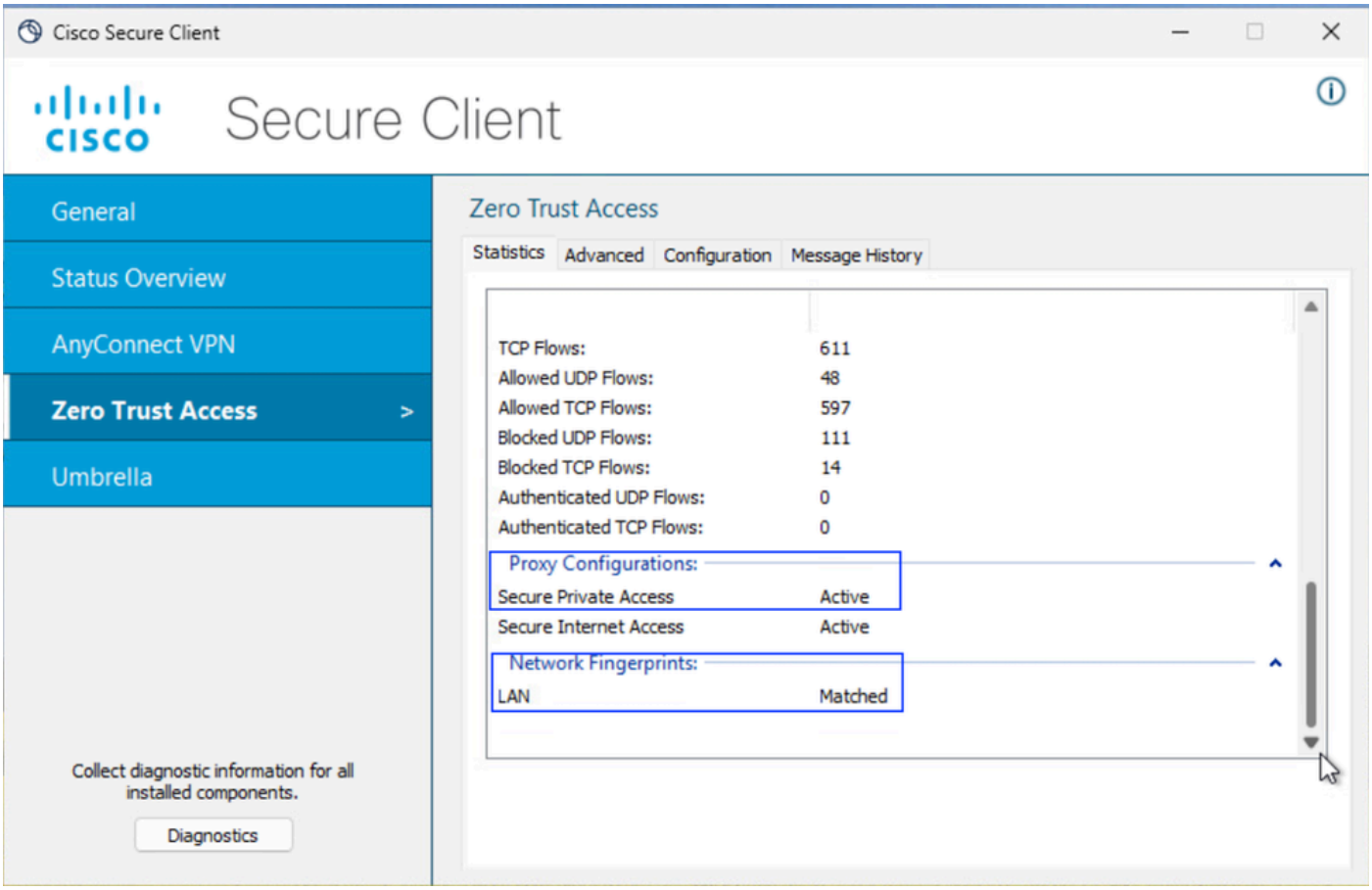


보안 액세스 - ZTA 프로필

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

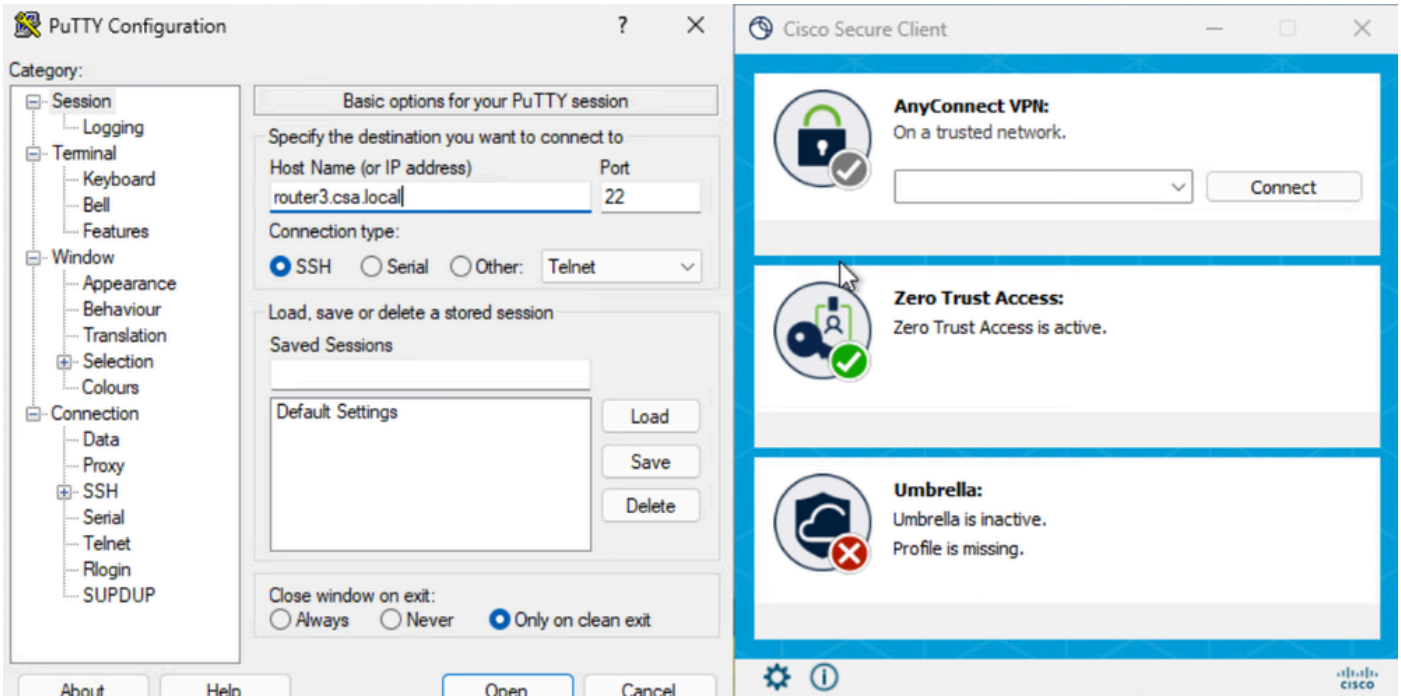
3. FQDN을 사용하여 FTD가 전용 리소스에 연결할 수 있는지 확인합니다.

```
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#
```

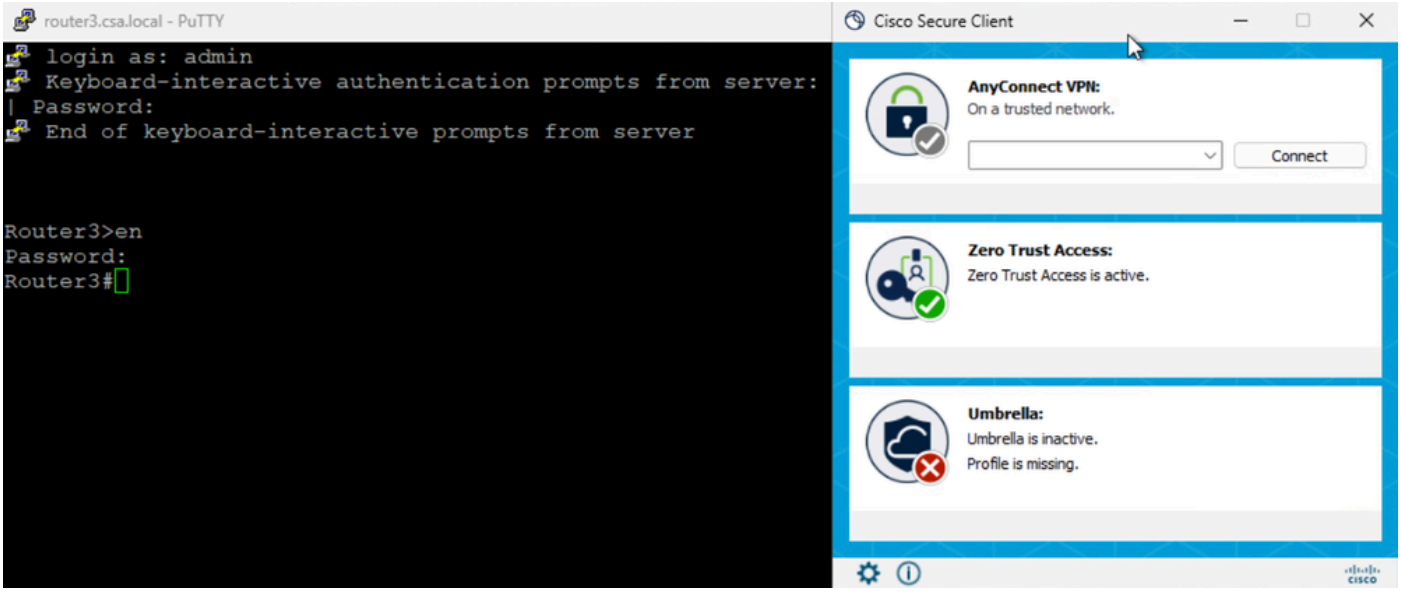
보안 액세스 - PR 테스트

4. 프라이빗 리소스에 대한 SSH 연결 테스트

FQDN을 사용하여 PR 액세스

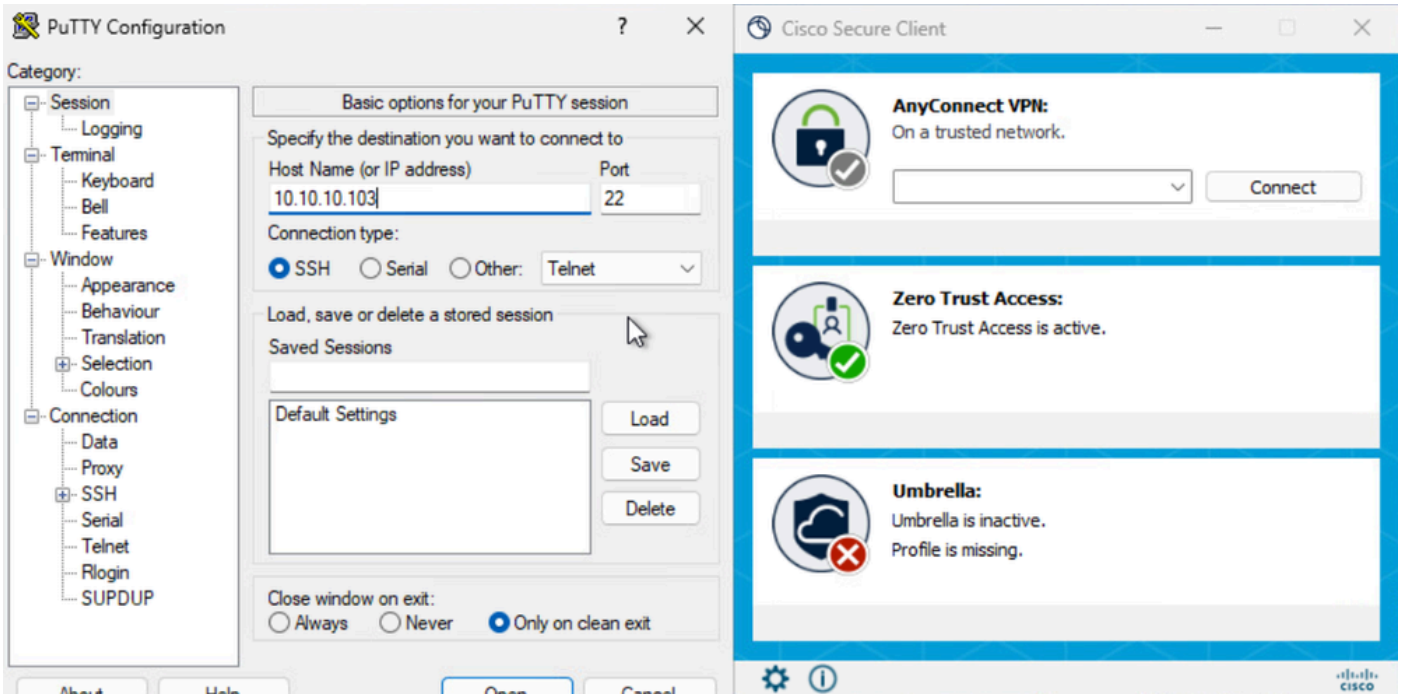


보안 액세스 - PR 테스트

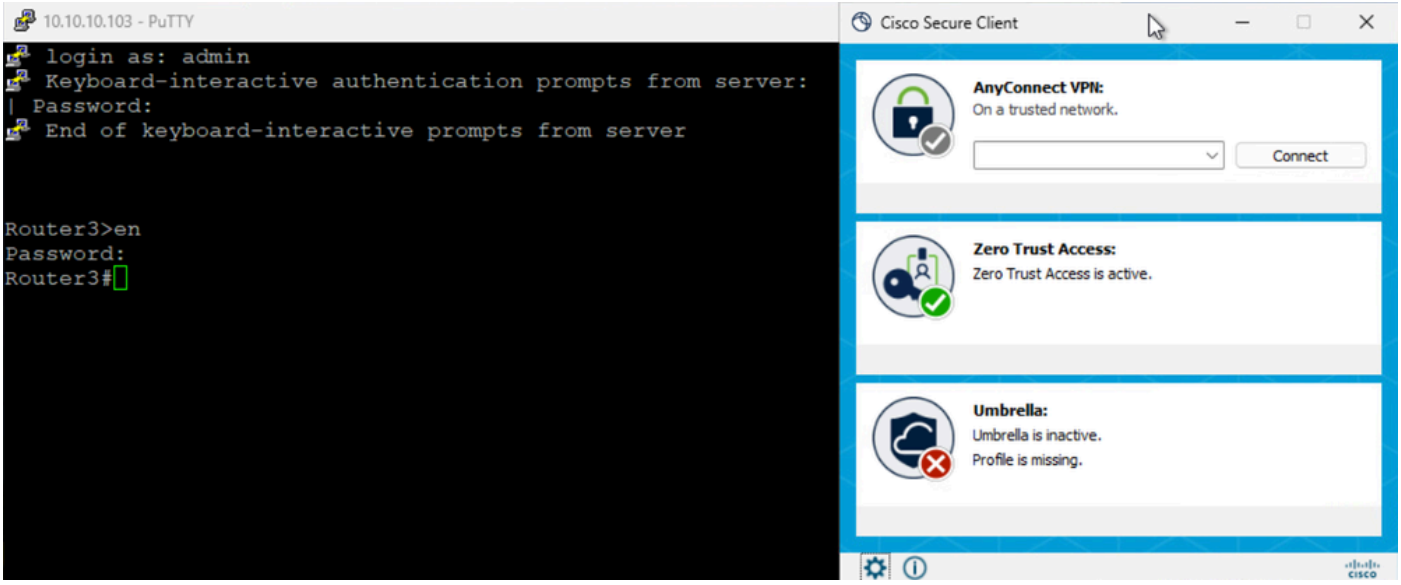


보안 액세스 - PR 테스트

IP 주소를 사용하여 PR에 액세스

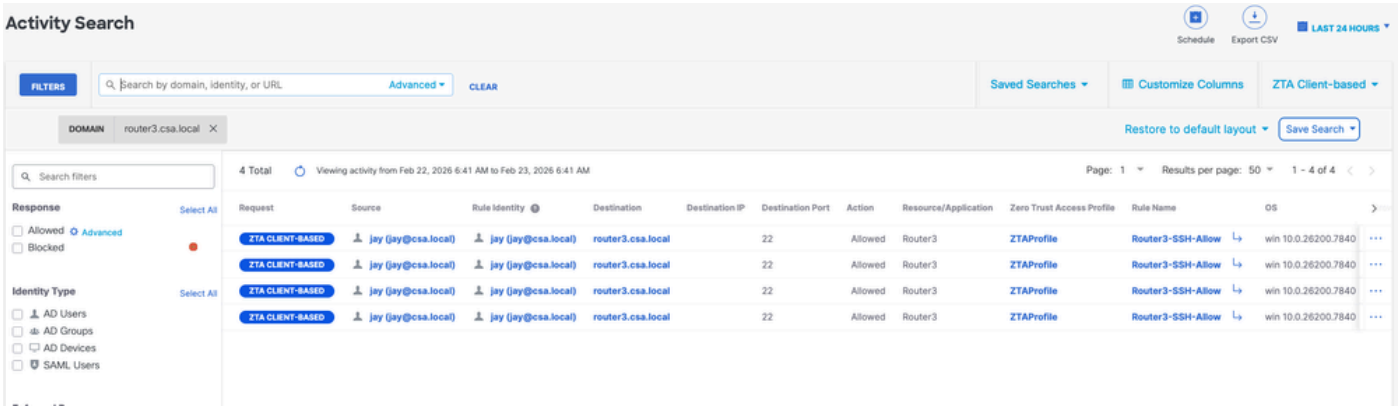


보안 액세스 - PR 테스트

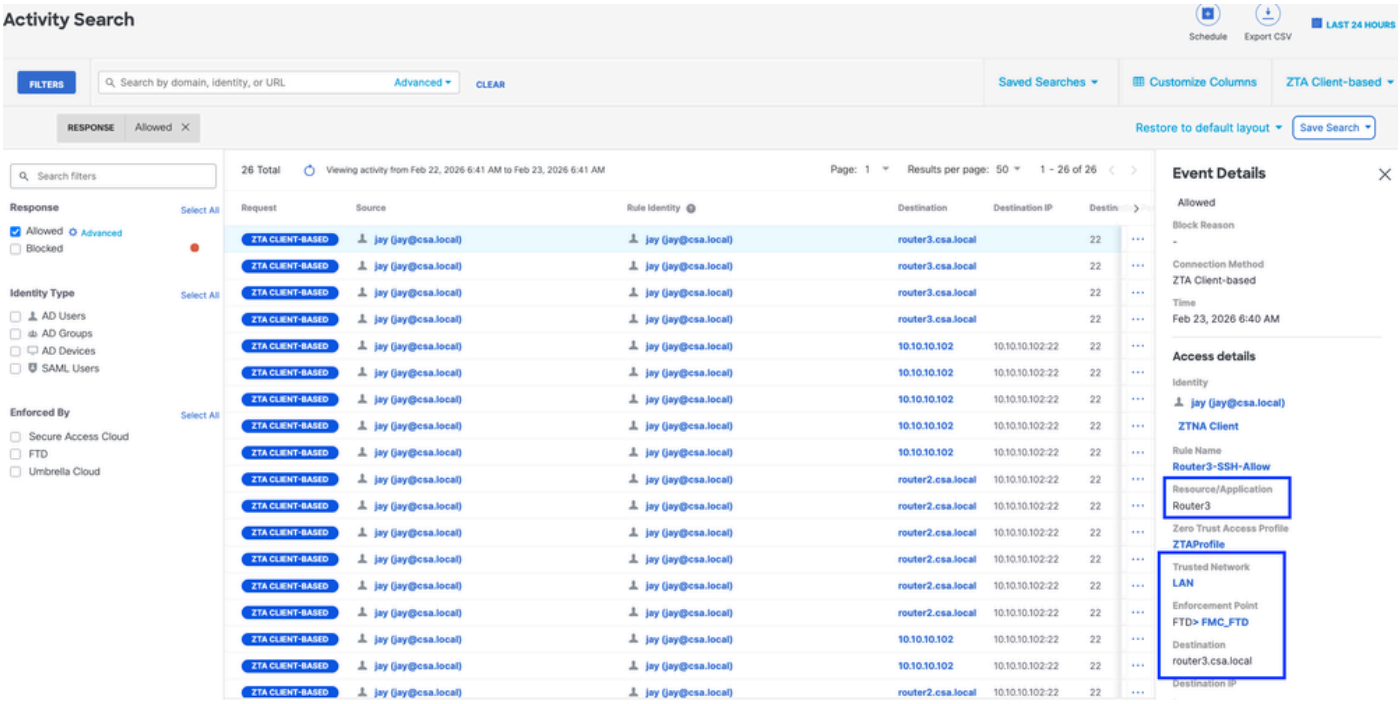


보안 액세스 - PR 테스트

5. 보안 액세스 활동 검색 로그 확인

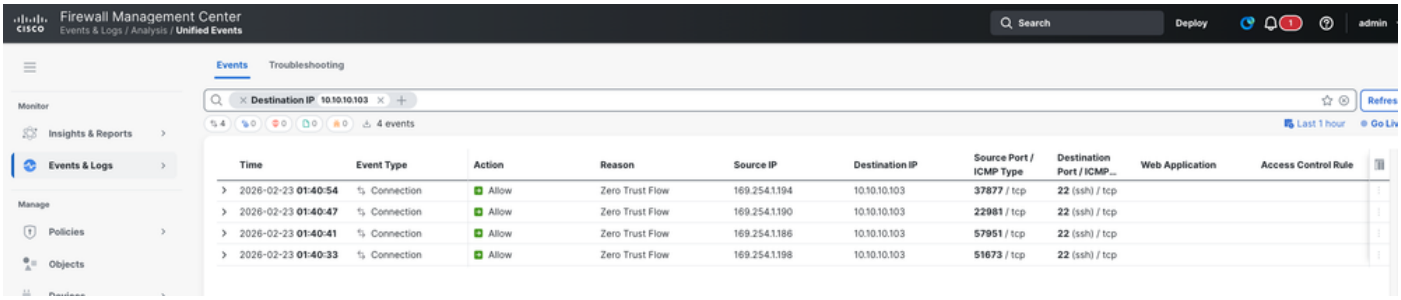


보안 액세스 - 활동 검색



보안 액세스 - 활동 검색

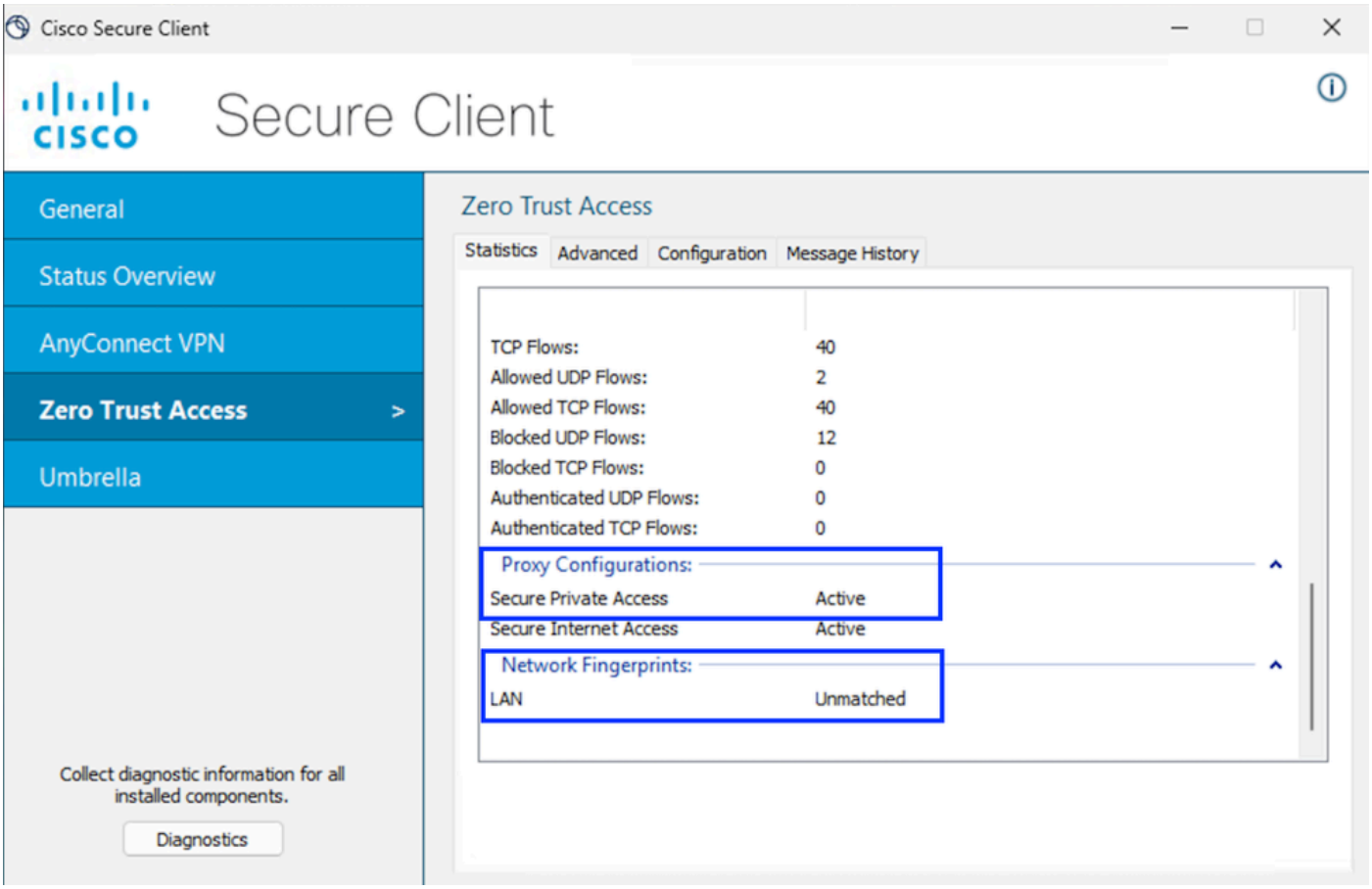
6. FMC 연결 이벤트 확인



FMC 연결 이벤트

사용자가 원격인 경우

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



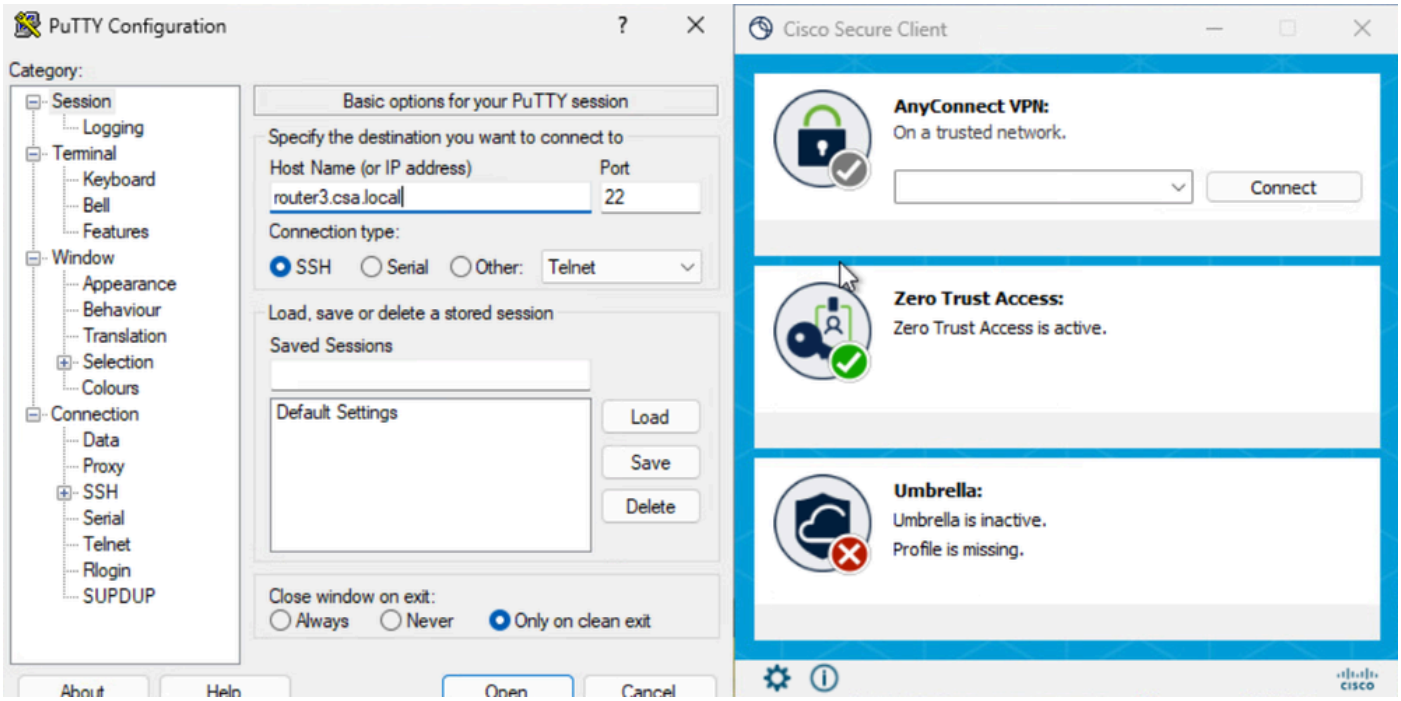
보안 액세스 - PR 테스트

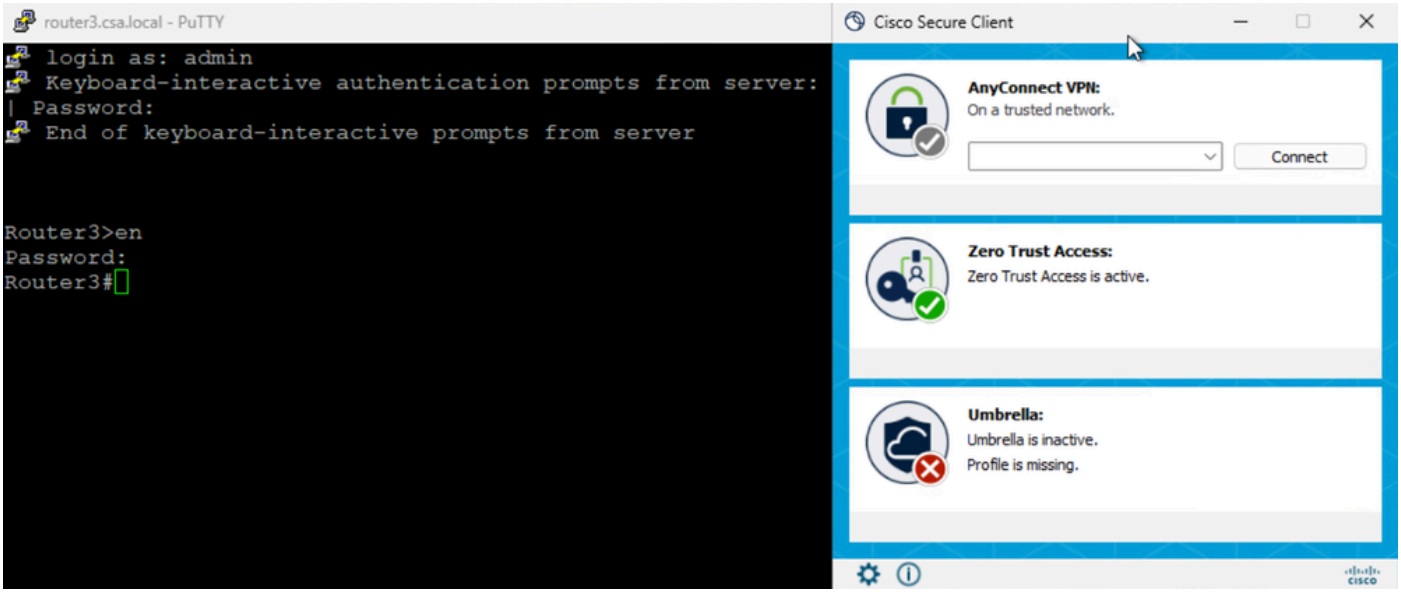
2 . 원격 사용자가 FTD FQDN을 확인할 수 있는지 확인

```
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
```


3 . 프라이빗 리소스에 대한 SSH 연결 테스트

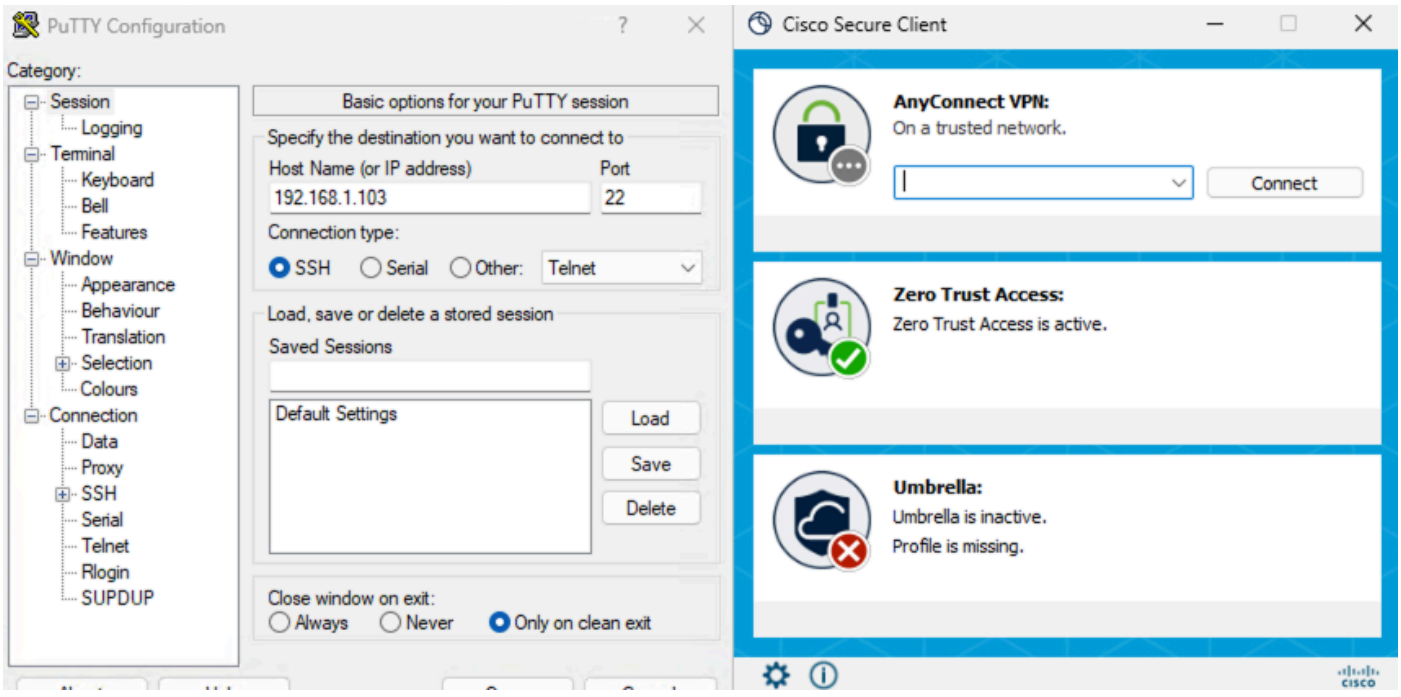
FQDN을 사용하여 PR 액세스



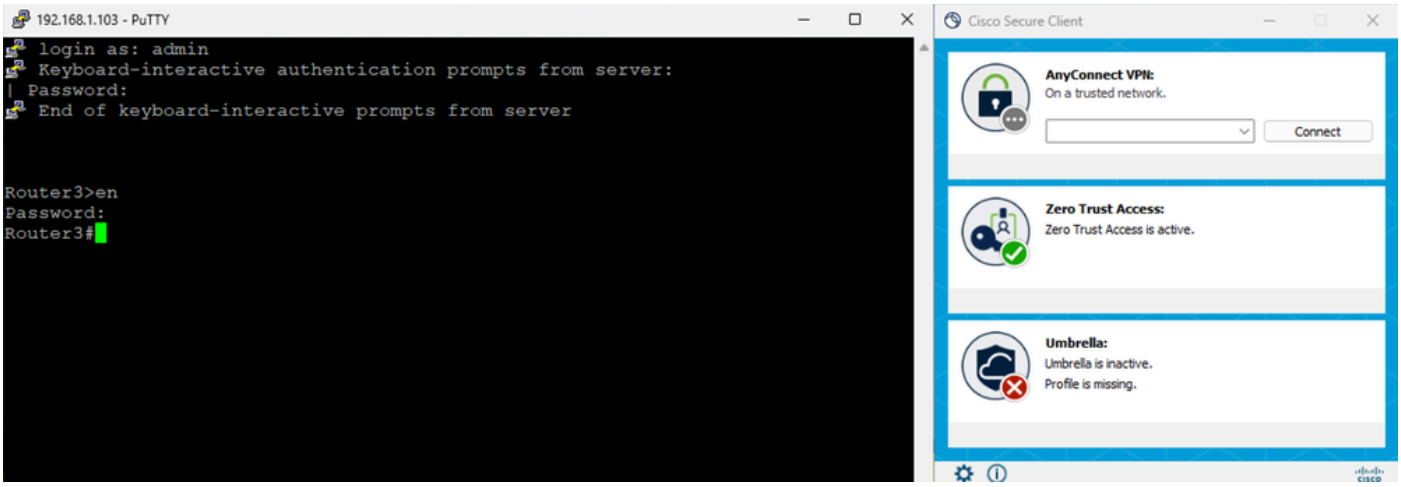


보안 액세스 - PR 테스트

IP 주소를 사용하여 PR에 액세스

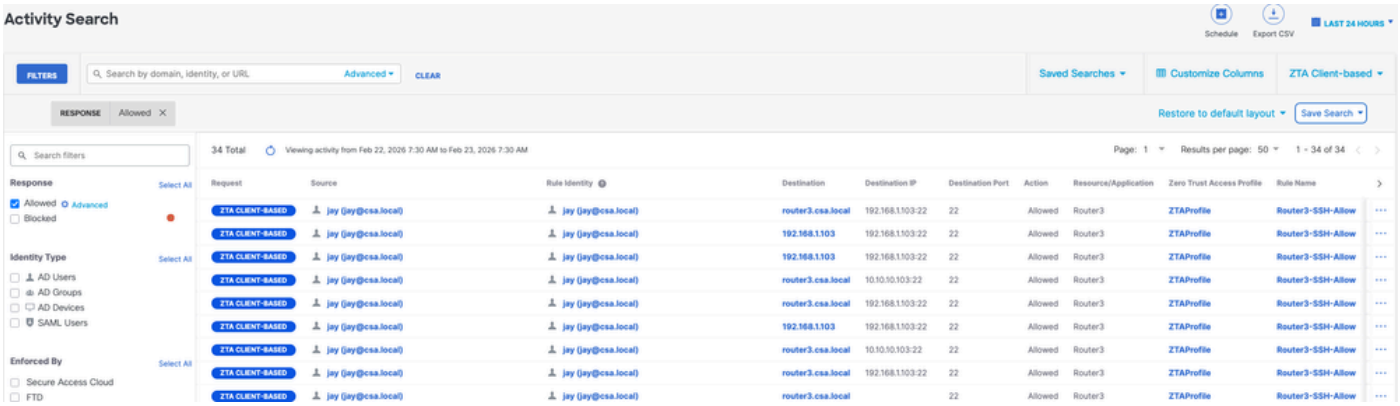


보안 액세스 - PR 테스트

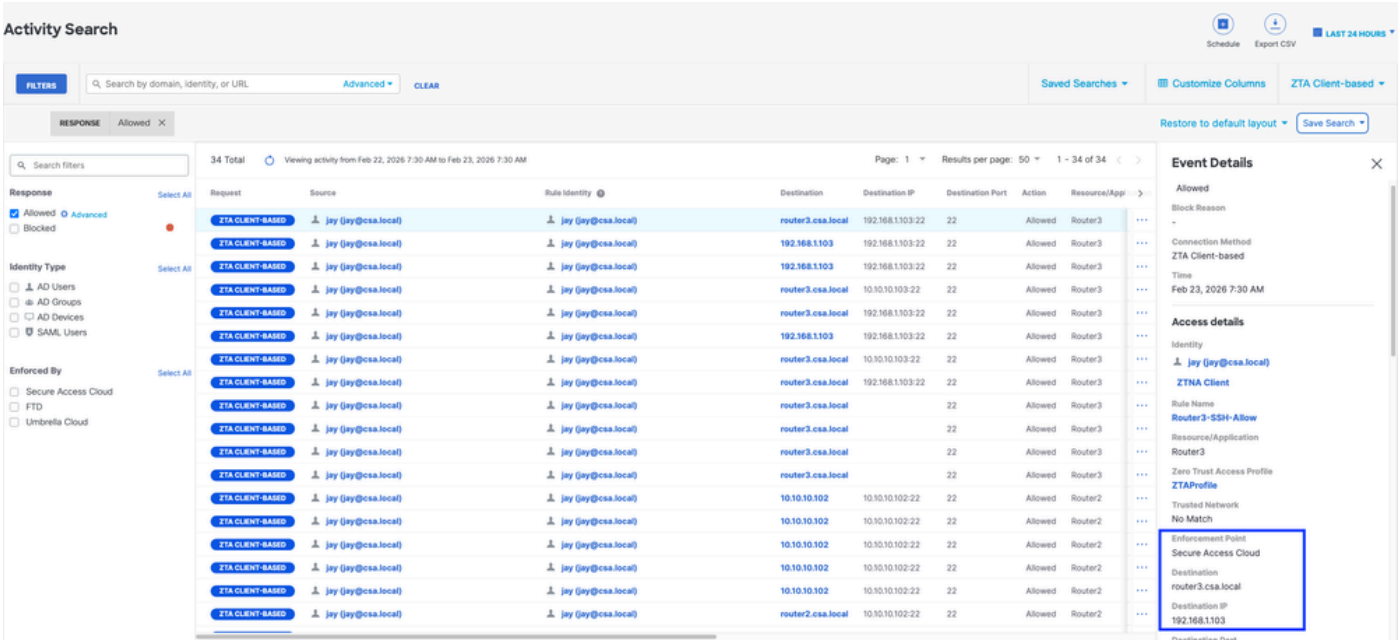


보안 액세스 - PR 테스트

5. 보안 액세스 활동 검색 로그 확인



보안 액세스 - 활동 검색



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.