# Kerberos 인증을 사용하여 프라이빗 리소스에 액세스하는 데 실패한 문제 해결

## 목차



## 소개

이 문서에서는 ZTNA(Secure Access Zero Trust Network Access)와 함께 사용할 때의 Kerberos 동작에 대해 설명합니다.

## 사전 요구 사항

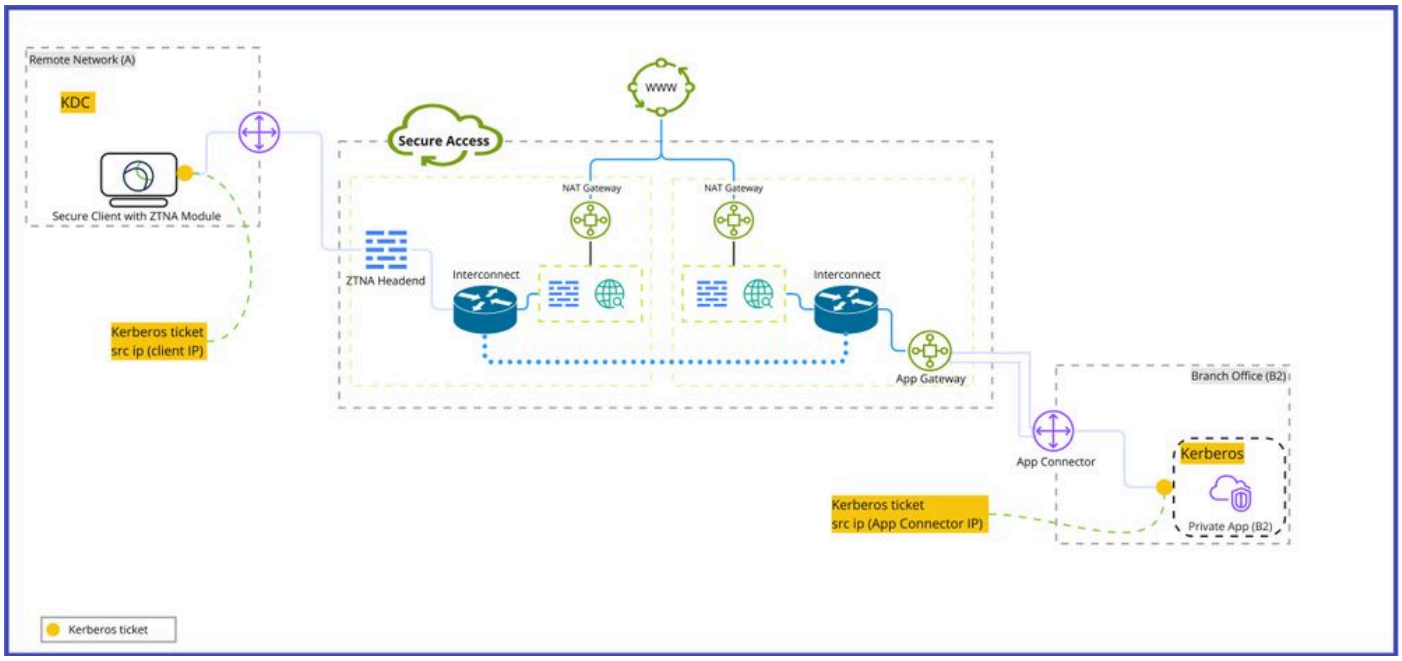
### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 보안 액세스
- Cisco 보안 클라이언트
- IPSEC(Internet Protocol Security) 터널
- RAVPN(Remote Access Virtual Private Network)
- ZTNA(Zero Trust Network Access)

## 배경 정보

보안 액세스는 보안 클라이언트의 ZTNA(Zero Trust Access Module), IPSEC 터널 또는 원격 액세스 VPN을 비롯한 여러 시나리오를 통해 프라이빗 애플리케이션에 대한 액세스를 제공하는 데 사용됩니다. 프라이빗 애플리케이션은 자체 인증 메커니즘을 제공하지만 Kerberos를 인증 메커니즘으로 사용하는 서버에는 제한이 있습니다.




Kerberos 패킷 흐름

# 문제: Kerberos 인증을 사용하여 개인 리소스에 액세스하지 못했습니다.

ZTNA 모듈 뒤에 있는 클라이언트 디바이스에서 App Connector 뒤에 있는 사설 애플리케이션으로 인증 요청을 시작하면 소스 IP 주소가 Secure Access 네트워크의 경로를 따라 변경됩니다. 클라이언트 KDC(Kerberos Distribution Center)에서 시작한 kerberos 티켓을 사용할 때 인증이 실패합니다 .

# 솔루션

클라이언트 소스 IP 주소는 KDC(Kerberos Distribution Center)에서 부여된 Kerberos 티켓의 일부입니다. 일반적으로 Kerberos 티켓이 네트워크를 통과할 때 소스 IP 주소가 변경되지 않은 상태로 유지되어야 합니다. 그렇지 않으면 인증하는 대상 서버가 소스 IP와 비교하여 티켓을 승인하지 않습니다.

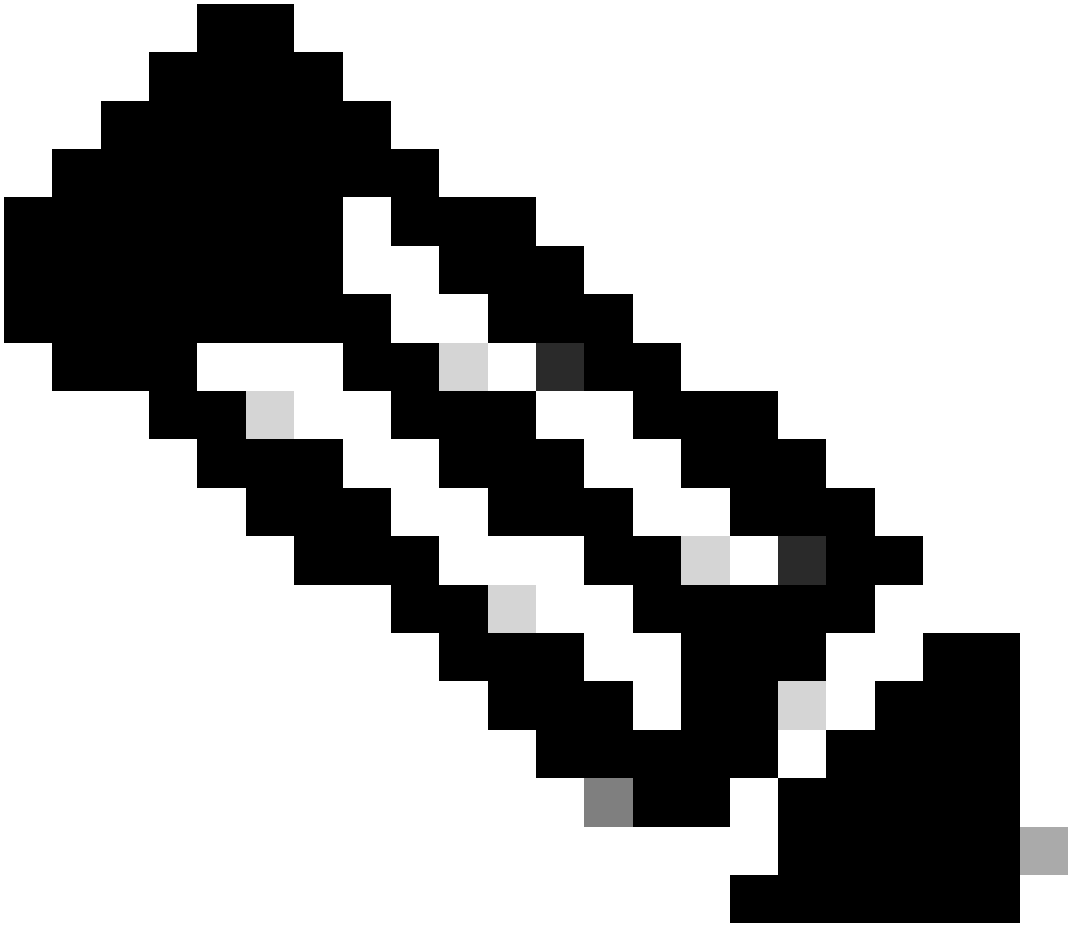
이 문제를 해결하려면 다음 옵션 중 하나를 사용하십시오.

옵션 1:

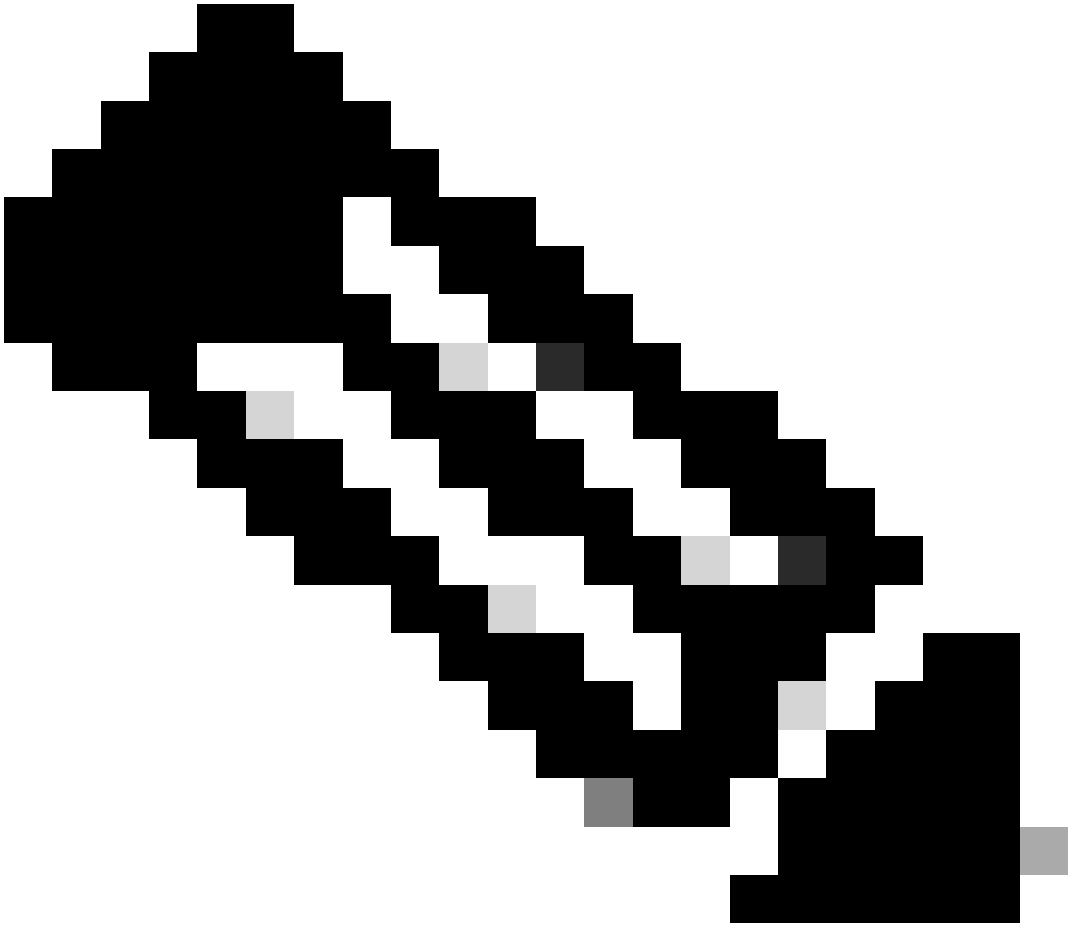
클라이언트 Kerberos 티켓에 소스 IP 주소를 포함하려면 이 옵션을 비활성화합니다.

옵션 2:

App Connector 뒤의 프라이빗 애플리케이션 대신 IPSEC 터널 뒤의 프라이빗 리소스로 보안 액세스 VPN을 사용합니다.



참고: 이 동작은 App Connector 뒤에 구축된 프라이빗 애플리케이션에만 영향을 미치며, 트래픽은 VPN 없이 ZTNA 모듈을 사용하는 클라이언트에서 발생합니다.



주: 보안 액세스 활동 검색은 보안 액세스가 아닌 프라이빗 애플리케이션 측에서 차단되므로 트랜잭션에 대해 허용된 작업을 표시합니다.

## 관련 정보

- Secure Access 사용 설명서
- 기술 지원 및 문서 – Cisco Systems

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.