

보안 클라이언트의 클라이언트 기반 ZTNA 트래픽 조정 문제

목차

문제

클라이언트 기반 ZTNA(Zero Trust Network Access)는 FQDN 또는 직접 IP 주소로 액세스할 때 내부 애플리케이션에 대한 액세스를 제공하지 못하는 반면, 동일한 애플리케이션은 VPN 연결을 통해 연결 가능합니다.

관찰된 특정 증상은 다음과 같습니다.

- VPN 연결이 끊어진 경우 FQDN 또는 직접 IP를 사용하여 보안 클라이언트 ZTNA가 내부 애플리케이션에 연결할 수 없습니다.
- 브라우저 기반 ZTNA 액세스는 동일한 애플리케이션에서 올바르게 작동합니다.
- VPN이 다운된 경우 작업 로그에 ZTNA 이벤트가 표시되지 않으며, 이는 클라이언트 트래픽이 ZTNA 경로를 통해 라우팅되지 않음을 나타냅니다.
- 프라이빗 앱 정의가 올바른 IP/포트/FQDN 컨피그레이션과 VPN 라우팅 가능 리소스와 일치하는지 검증되었습니다.
- ZTNA 정책이 테스트 사용자 및 그룹 할당과 일치하는 것으로 확인되었습니다.

이 문제는 특히 Secure Client ZTNA 트래픽 조정 또는 시행 메커니즘과 관련이 없습니다. 브라우저 기반 ZTNA가 백엔드 게시 및 시행이 제대로 작동하는지 검증하기 때문입니다.

환경

- 기술: 보안 액세스 - ZTNA(Zero Trust Network Access)
- 구성요소: 클라이언트 기반 ZTNA, 상태, 등록, 개인 리소스 액세스

- 공존하는 VPN 프로파일을 사용하는 보안 클라이언트
- FQDN 및 직접 IP 주소 지정을 통해 액세스할 수 있는 전용 애플리케이션
- 브라우저 기반 ZTNA 기능 작동 확인
- 가장 구체적인 일치 적용 모드에서 구성된 정책 적용

해결

해결에는 ZTA 프로필에 대한 컨피그레이션 조정 및 정책 검증이 포함되었습니다. 클라이언트 기반 ZTNA 기능을 복원하기 위해 다음 섹션에 설명된 단계를 수행했습니다.

1단계: ZTA 프로필에 개인 리소스 추가

개인 리소스가 ZTA 프로필 구성에 추가되었습니다. 이 변경 후 차단된 이벤트가 작업 로그와 스크린샷에 나타나기 시작했으며, 이는 클라이언트 트래픽이 이제 ZTNA 경로를 통해 제대로 라우팅되고 있음을 나타냅니다.

2단계: 정책 확인 및 테스트

트래픽 흐름을 검증하기 위해 임시 "permit any" 규칙이 추가되었습니다. 이 규칙이 활성화된 동안 클라이언트 기반 ZTNA 액세스가 올바르게 작동하여 트래픽 조정 메커니즘은 작동하지만 정책 시행에는 조정이 필요함을 확인했습니다.

3단계: 정책 구체화

임시 permit-any 규칙이 제거되고 특정 액세스 정책이 검증되었습니다. 비공개 리소스가 플랫폼의 Most Specific Match Enforcement Mode를 사용하여 Private Resources_Cyril이라는 액세스 정책에서 액세스 가능한 것으로 확인되었습니다.

4단계: 구성 검증

사용자가 컨피그레이션 변경 후 클라이언트 기반 ZTNA 액세스가 지속적으로 작동하기 시작했음을 확인했습니다. 추가 정책 수정 또는 시스템 변경 없이 문제가 해결되었습니다.

원인

근본 원인은 ZTA 프로필의 비공개 리소스 구성이 불완전합니다. ZTA 프로필에 정의된 적절한 프라이빗 리소스가 없으면 클라이언트 트래픽이 ZTNA 시행 경로를 통해 조정되지 않아 로컬 라우팅 메커니즘으로 다시 이동했습니다. 이로 인해 트래픽이 ZTNA 정책을 완전히 우회하게 되었으며, VPN 연결이 끊길 때 작업 로그에 ZTNA 이벤트가 표시되지 않은 이유를 설명했습니다.

이 문제는 클라이언트 기반 ZTNA 트래픽 스티어링 컨피그레이션에만 해당하는 반면, 브라우저 기반 ZTNA는 올바르게 구성된 다른 트래픽 처리 메커니즘을 사용하므로 계속 작동합니다.

관련 콘텐츠

- [Cisco 기술 지원 및 다운로드](#)

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.