보안 액세스 IdleTimeout 오류로 인해 회사 방화벽 뒤의 연결이 간헐적으로 끊김

목차

- 문제
- 환경
- 해결
  - 1단계: MX TTL 버퍼 구성 구현
  - 2단계: 필수 도메인 제외 구성
  - 3단계: 포트 및 프로토콜 허용 확인
  - 4단계: 해결 모니터링 및 검증
- 원인
- 관련 콘텐츠

문제

Cisco Secure Access 클라이언트는 엔드포인트가 기업 네트워크에 연결될 때 간헐적으로 연결이 끊기고 즉시 다시 연결됩니다. 연결이 끊기는 무작위로 발생하며, 클라이언트는 약 5초 후에 자동으로 다시 연결됩니다. 이 동작은 Cisco Firepower 및 Meraki MX 디바이스 뒤에 위치한 엔드포인트에서 보안 액세스를 위해 ZTA(Zero Trust Access)를 통해 인터넷 트래픽이 프록시될 때 관찰됩니다.

Windows 이벤트 로그는 이러한 연결 끊기 이벤트 동안 특정 "idleTimeout" 오류를 캡처합니다. 사용자가 홈 인터넷 연결에서 연결할 때 연결 끊기 패턴은 발생하지 않으므로 특히 이 문제가 기업 네트워크 인프라와 관련이 있음을 나타냅니다.

이러한 증상으로 인해 기업 네트워크 환경 내에서 작동하는 사용자의 보안 원격 액세스 연결이 업

무에 차질을 빚는 반면, 원격 사용자는 이 연결 문제의 영향을 받지 않습니다.

환경

- Cisco Secure Access - Advantage 구축
- Cisco SIA(Secure Internet Access) 클라이언트 소프트웨어
- Cisco Firepower 보안 어플라이언스를 사용하는 기업 네트워크 인프라
- 네트워크 경로에 있는 Meraki MX 보안 어플라이언스
- ZTA(Zero Trust Access) 컨피그레이션으로 인터넷 트래픽을 보안 액세스로 프록시
- 이벤트 로깅 기능이 있는 Windows 엔드포인트
- 혼합 연결 시나리오: 기업 네트워크(영향 받음) 및 홈 인터넷 연결(영향 받지 않음)

해결

해결책에는 Meraki MX 디바이스에서 컨피그레이션 변경을 구현하고 Secure Access 통합을 위한 올바른 도메인 제외 및 포트 허용을 확인하는 작업이 포함되었습니다.

1단계: MX TTL 버퍼 구성 구현

간헐적인 연결 끊김 문제를 일으키는 DNS TTL 캐싱 동작을 해결하도록 Meraki MX 디바이스에서 MX TTL 버퍼를 구성합니다. 이 컨피그레이션 변경은 DNS 확인 캐싱과 Secure Access 클라이언트 연결 기대 간의 시간 충돌을 해결합니다.

2단계: 필수 도메인 제외 구성

다음 Firepower이 인터셉션에서 올바르게 제외되고 Cisco 도메인과 Meraki MX 디바이스 모두에서 암호 해독 목록에 추가되었는지 확인합니다.

- ztna.sse.cisco.com
- zpc.sse.cisco.com
- 정책 컨피그레이션에서 식별된 추가 Secure Access 서비스 도메인

3단계: 포트 및 프로토콜 허용 확인

firepower 및 Meraki MX 디바이스를 통해 필요한 보안 액세스 포트 및 프로토콜을 허용하도록 기업 방화벽 인프라를 구성합니다. Secure Access 서비스 엔드포인트용 포트 443에 대한 트래픽이 시간 초과 조건의 원인이 될 수 있는 보안 검사의 간섭 없이 올바르게 처리되는지 확인합니다.

4단계: 해결 모니터링 및 검증

MX TTL 버퍼 컨피그레이션을 구현한 후 며칠 동안 Secure Access 클라이언트 동작을 모니터링하여 간헐적인 연결 끊김 및 재연결 패턴이 중지되었는지 확인합니다.

원인

간헐적인 연결 끊기는 기업 네트워크 인프라와 Secure Access 서비스 기대 간의 DNS TTL(Time To Live) 캐싱 동작 충돌로 인해 발생했습니다. Cisco 엔지니어링 분석에 따르면 DNS TTL 값은 확인자 캐싱 동작으로 인해 달라지며, Secure Access 서비스 아키텍처의 로드 밸런싱 메커니즘으로 인해 대체 IP 주소가 예상된 동작입니다.

기업 네트워크 디바이스(Cisco Firepower 및 Meraki MX)가 보안 액세스 엔드포인트에 대한 DNS 응답을 처리하면 캐싱 및 TTL이 타이밍 불일치를 생성하여 "idleTimeout" 조건이 발생합니다. 이 타이밍 충돌로 인해 Secure Access 클라이언트가 연결을 유휴 상태로 해석하고 연결 끊기/다시 연결 주기를 시작했습니다.

홈 인터넷 연결이 일반적으로 Secure Access 클라이언트 연결 상태 관리에 방해가 될 수 있는 동일한 수준의 DNS 캐싱 및 트래픽 검사를 구현하지 않기 때문에 이 문제는 기업 네트워크 환경에서만 발생했습니다.

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.