SSL 암호 해독 및 네트워크 터널의 보안 액세스 ZTNA 구성 동기화 오류

목차

문제

Cisco ZTA(Secure Client Zero Trust Access)가 성공적으로 등록되었지만 HTTP 502 응답 및 "BadResponse" 서버 연결 상태와의 컨피그레이션 동기화 중에 실패합니다. Windows 11 엔드포인트의 DART 로그에는 성공적인 등록이 표시되지만 컨피그레이션 동기화 실패가 반복됩니다. 이 문제는 엔드포인트가 Meraki AutoVPN 터널과 함께 Secure Access/Umbrella 프록시를 사용하여 기업 네트워크 경로에 연결된 경우에만 발생하며, 동일한 엔드포인트가 프록시 또는 터널 인프라 없이 홈 네트워크에서 컨피그레이션 동기화를 성공적으로 완료한 경우에 발생합니다.

환경

- Cisco Secure Client ZTA 버전 5.1.16.4434
- Windows 11 Enterprise 끝점
- Meraki MX 어플라이언스와 AutoVPN 통합
- NTG(Network Tunnels Gateway)를 사용하는 SSE(Secure Access)
- Umbrella DNS 및 Secure Access 웹 보안
- 회사 네트워크 경로에서 SSL 암호 해독 및 HTTPS 검사 사용
- 제공된 DND(System Provided Do Decrypt List)가 초기에 구성되지 않음

해결

보안 액세스가 있는 네트워크 터널을 사용할 때 ZTA 관련 도메인에 대해 적절한 SSL 암호 해독 우

회를 구현하여 구성 동기화 실패를 해결했습니다.

1단계: SSL 암호 해독 영향 식별

Secure Access에서 ZTA 도메인과 관련된 암호 해독 이벤트에 대한 작업 검색 로그를 검토하여 SSL 암호 해독으로 인해 구성 동기화 오류가 발생하는지 확인합니다.

2단계: 시스템 제공 DND 목록 구성

보안 액세스로 NTG(Network Tunnels Gateway)를 사용하는 경우 SSL 검사에서 ZTA 관련 트래픽을 제대로 우회하려면 시스템 제공 DND를 활성화해야 합니다.

Secure Access Dashboard(보안 액세스 대시보드) > Secure(보안) > Do Not Decrypt Lists(목록 해독 안 함)로 이동하고 제공된 System Provided Do Not Decrypt(시스템 제공 Do Decrypt) 목록을 수정합니다.

3단계: ZTA 도메인에 대한 보안 프로파일 생성

System Provided DND List(시스템 제공 DND 목록)를 사용하여 필요한 ZTA 관련 도메인을 새 보안 프로파일에 추가합니다.

- zpc.sse.cisco.com
- *.zpc.sse.cisco.com
- ztna.sse.cisco.com
- acme.sse.cisco.com
- devices.api.umbrella.com

4단계: 테스트 규칙에 보안 프로필 적용

ZTA 도메인이 우회하는 새로 생성된 보안 프로파일을 테스트 규칙에 할당하여 컨피그레이션을 검증합니다.

5단계: 구성 동기화 확인

기업 네트워크에서 ZTA 등록 및 컨피그레이션 동기화를 테스트합니다. 이제 HTTP 502 오류 없이 동기화를 완료할 수 있습니다.

6단계: Meraki 팀과 협력

포괄적 커버리지를 위해 Meraki 지원과 협력하여 Secure Access 검사에서 우회할 수 있는 공식 ZTA 관련 URL 및 도메인을 검증합니다. 다음 Meraki 문서를 참조하십시오.

- 클라우드 연결을 위한 업스트림 방화벽 규칙
- Meraki 대시보드 URL 업데이트 - PCI 규정 준수

원인

회사 네트워크에서 SSL 암호 해독 및 제로 트러스트 액세스 트래픽의 프록시로 인해 구성 동기화 오류가 발생했습니다. NTG(Network Tunnels Gateway)가 보안 액세스와 함께 사용되는 경우 ZTA 관련 도메인은 DND(System Provided Do Decrypt List)를 사용하여 우회해야 합니다. 이러한 우회 컨피그레이션이 없으면 SSL 검사는 인증서 체인을 수정하고 ZTA 제어 평면 통신을 방해하여 클라이언트가 컨피그레이션 동기화 시도 중에 HTTP 502 응답을 수신하게 합니다.

관련 콘텐츠

- 보안 액세스 암호 해독 및 SSL 문제 해결
- Secure Access Zero Trust 클라이언트 기반 등록 서비스
- 보안 액세스를 위한 ZTA 도메인 요구 사항

- 보안 액세스 오류 등록 문제 해결
- 보안 클라이언트 구성 동기화 오류 트러블슈팅
- 문제 해결을 위한 자세한 ZTNA 로그 수집
- 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.