Cortex를 포함한 엔드포인트 상태 조건으로 인해 AnyConnect VPN 로그인이 거부됨

목차

문제

여러 사용자가 간헐적으로 RAVPN(Secure Client Remote Access)에 연결할 수 없으며 "AnyConnect VPN Login denied(AnyConnect VPN 로그인 거부)"라는 오류 메시지가 표시됩니다. 사용자 환경이 관리자가 정의한 액세스 기준을 충족하지 않습니다." 이 문제는 MacBook 및 Surface 노트북 모두에 영향을 미치며, 사용자는 종종 여러 번 연결을 시도하거나 시스템을 재부팅하여 정상적으로 연결해야 합니다. 연결 실패는 엔드포인트 보안 상태 검증 조건, 특히 macOS 버전 요구 사항 및 Cortex XDR 상태 검증과 관련된 것으로 보입니다.

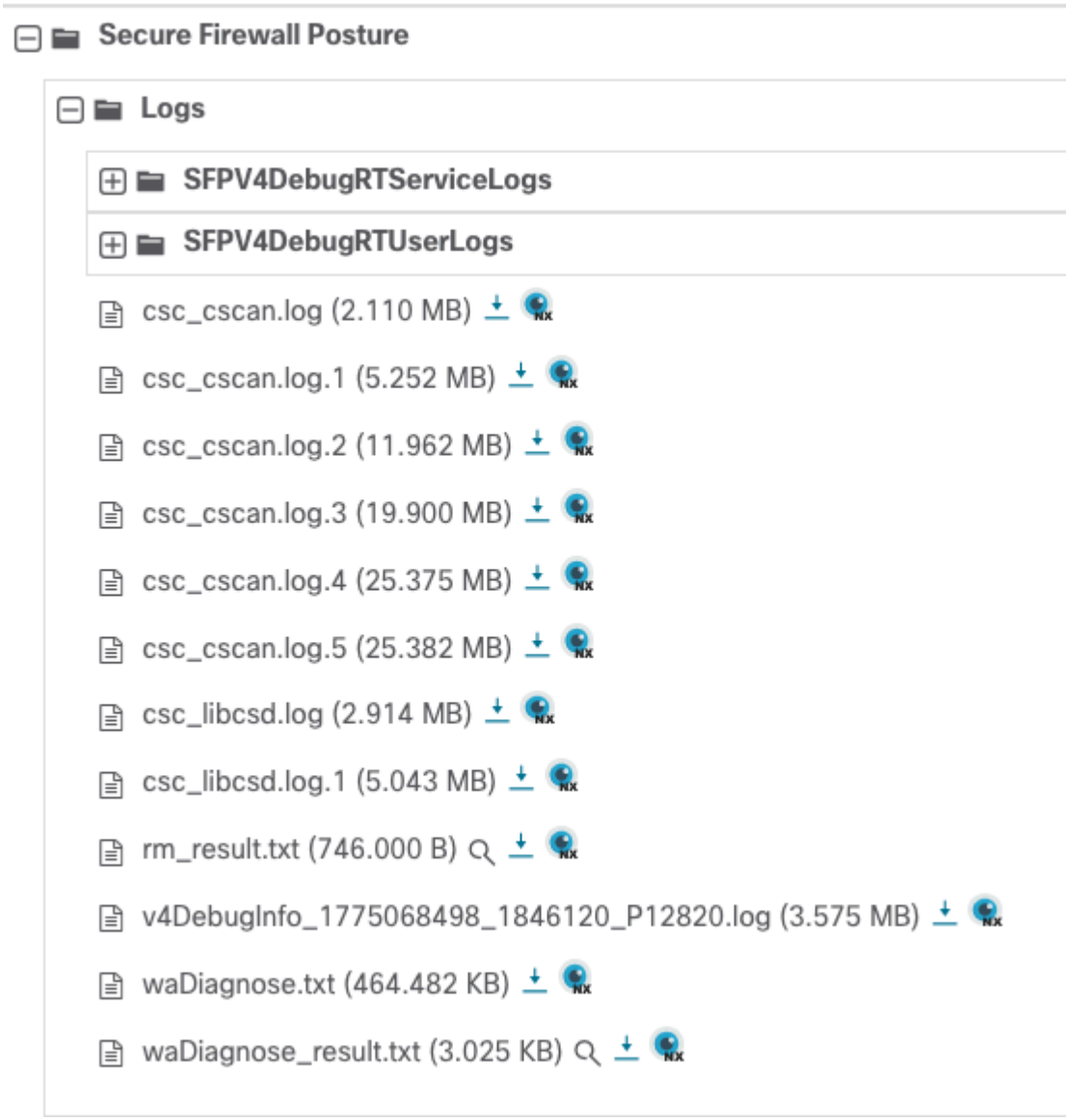
환경

- 보안 클라이언트 원격 액세스 (RAVPN) 구축 상태 평가
- MacBooks 및 Surface 랩톱을 포함한 혼합 엔드포인트 환경
- 엔드포인트 상태 요구 사항: macOS 버전 26.2 이상 및 Cortex XDR 실행
- DAP(Device Access Policy) 시행을 통한 보안 액세스 솔루션

해결

1: DART 수집

2: Secure Firewall Posture 폴더로 이동하여 csc_scan.log를 다운로드합니다.



inline_image_0.png

3: 다음 로그를 찾습니다.

[Fri Mar 27 13:53:10.419 2026] 디버그: {"input":{"method":1000,"signature":}} 형식의 JSON

[Fri Mar 27 13:53:10.420 2026] 오류: Opswat에서 오류를 반환했습니다. -22 및 다음으로 변환: 6

[Fri Mar 27 13:53:10.420 2026] 오류: 조건에서 실패: opSuccess != 상태

[Fri Mar 27 13:53:10.420 2026] 디버그: Opswat 반환 상태가 액세스 거부됨

[Fri Mar 27 13:53:10.420 2026] 디버그: 서비스를 사용하여 안티멀웨어의 rtp 상태를 확인합니다.

[Fri Mar 27 13:53:10.420 2026] 추적:: TCP/IP 상태 Ipv4(1),Ipv6(1)

[Fri Mar 27 13:53:10.420 2026] 추적:: TCP/IP 상태 Ipv4(1),Ipv6(1)

[Fri Mar 27 13:53:10.420 2026] 추적:: TCP/IP 상태 Ipv4(1),Ipv6(1)

[Fri Mar 27 13:53:10.420 2026] 추적:: TCP/IP 상태 Ipv4(1),Ipv6(1)

[Fri Mar 27 13:53:15.060 2026] 오류: 응답 수신.

[Fri Mar 27 13:53:15.060 2026] 디버그: am 검사 rtp를 수행할 수 없습니다.<<<<--------

[Fri Mar 27 13:53:15.060 2026] 정보: 반환된 RTP 상태가 실패했습니다.

[Fri Mar 27 13:53:15.060 2026] 정보: Opswat 반환 정의 날짜는 1입니다.

[Fri Mar 27 13:53:15.060 2026] 디버그: 서비스를 사용하여 안티 멀웨어의 정의 날짜를 가져옵니다.

[Fri Mar 27 13:53:15.060 2026] 추적:: TCP/IP 상태 Ipv4(1),Ipv6(1)

[Fri Mar 27 13:53:15.060 2026] 추적:: TCP/IP 상태 Ipv4(1),Ipv6(1)

[Fri Mar 27 13:53:15.060 2026] 추적:: TCP/IP 상태 Ipv4(1),Ipv6(1)

[Fri Mar 27 13:53:15.060 2026] 추적:: TCP/IP 상태 Ipv4(1),Ipv6(1)

[Fri Mar 27 13:53:20.079 2026] 오류: 응답 수신.

[Fri Mar 27 13:53:20.079 2026] 디버그: 맬웨어 방지 정의 날짜 작업을 수행할 수 없습니다.
<<<<<—

[Fri Mar 27 13:53:20.079 2026] 디버그: 안티멀웨어 ==> ()(Cortex XDR(Mac))(9.1.0) () ()(실패)를 찾았습니다.

[Fri Mar 27 13:53:20.084 2026] 디버그: 일치 실패: 프로세스 이름은 'ciscod' 및 'cscan'입니다.

[Fri Mar 27 13:53:20.084 2026] 디버그: edr 인터넷 연결 확인 상태(1)

참고: 이를 근거로 우리 공정에 대한 피질의 제약 또는 인터넷 접속에 대한 제약 그리고 피질이 공정을 방해하지 않는지 확인할 수 있는 다른 것으로 보인다. 스캔을 악성코드로 처리할 수 있으므로 Secure Firewall Posture를 차단할 수 있습니다.

안티멀웨어에서 제외 목록

CSC(Cisco Secure Client): 모든 모듈 - 시스템

1. Windows: C:\Program Files (x86)\Cisco\Cisco Secure Client*
2. macOS: /opt/cisco/secureclient/*
3. Linux: /opt/cisco/secureclient/*

CSC(Cisco Secure Client): 모든 모듈 - 사용자

1. Windows: %localappdata%\\Cisco\Cisco Secure Client*
2. macOS: ~/.cisco/secureclient/*
3. Linux: ~/.cisco/secureclient/*

원인

이 문제는 특히 macOS 버전 요구 사항 및 Cortex XDR 상태의 검증과 관련된 엔드포인트 상태 평가 프로세스에서 간헐적인 실패로 인해 발생합니다. 상태 평가 시스템이 필수 보안 조건(macOS 26.2 이상 및 Cortex XDR 실행 상태)을 일관성 없이 탐지하거나 검증하므로, 엔드포인트가 지정된 기준을 충족하더라도 연결이 거부됩니다. 따라서 사용자는 성공적인 상태 평가 및 VPN 연결을 위해 여러 연결 시도 또는 시스템 재부팅이 필요합니다.

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.