원격 액세스 VPN용 iOS에서 Cisco Secure Client를 사용한 DNS 로깅 및 디바이스 등록 동작

목차

문제

iPad(iOS)에서 Cisco Secure Client를 사용하여 Microsoft Entra ID를 통한 SAML 인증을 사용하여 Cisco Secure Access와의 원격 액세스 VPN을 설정할 경우, 방화벽 및 웹 로그가 올바르게 생성되더라도 VPN 연결이 성공한 후 DNS 로그가 Secure Access에 표시되지 않습니다. 또한 iPad는 VPN 연결을 설정한 후 Secure Access 대시보드에서 Roaming Devices(로밍 디바이스) > Mobile Devices(모바일 디바이스) 아래에 나타나지 않습니다.

관찰된 특정 증상은 다음과 같습니다.

- 원격 액세스 로그에 Secure Access에서 성공한 "연결" 이벤트 표시
- 방화벽 및 웹 로그가 생성되고 SAML 인증 사용자 ID가 표시됩니다
- DNS 로그는 Secure Access 로깅에 전혀 없습니다.
- iPad 디바이스 정보가 Secure Access roaming devices 섹션에 입력되지 않습니다
- 모든 트래픽은 VPN 터널을 통해 이동합니다(구성된 스플릿 터널링 없음).

환경

- iOS 26.2를 실행하는 iPad
- Cisco 보안 클라이언트
- ID 공급자: Microsoft Entra ID
- 보안 커넥터: 설치되지 않음
- SSO 인증이 구성된 Cisco Secure Access

- SAML 인증 구현
- DNS 모드가 기본값으로 설정된 VPN 프로파일
- 구성된 스플릿 터널링 없음(모든 트래픽이 VPN을 통해 라우팅됨)
- 프로필 배포에 사용되는 MDM(Mobile Device Management)

해결

관찰된 동작은 문서화된 컨피그레이션에 필요합니다. iOS의 Cisco Secure Client는 VPN 클라이언트로 작동하며(AnyConnect와 동일) 기본적으로 RSM과 동등한 기능을 포함하지 않습니다. 보안 커넥터는 엔드포인트 ID 채우기 및 Umbrella 스타일 DNS 제어에 필요한 iOS의 RSM과 동등한 구성 요소입니다.

아키텍처 이해

DNS 로그 및 디바이스 등록이 없는 이유는 다음과 같습니다.

- Cisco Secure Client에서만 VPN 연결을 제공하지만 DNS 가시성에 필요한 엔드포인트 에이전트 기능이 없음
- Secure Access에서 DNS 제어 및 디바이스 등록을 위해서는 보안 커넥터(Windows의 RSM과 동일)가 필요합니다.
- 보안 커넥터가 없으면 Umbrella/Secure Access에 대한 가시성 없이 VPN에서 얻은 DNS 서버에서 DNS 쿼리를 처리합니다

트래픽 스티어링을 통한 DNS 로깅 솔루션

보안 커넥터를 설치하지 않고 DNS 로깅을 활성화하려면 DNS 쿼리를 Umbrella DNS 서버로 보내도록 트래픽 스티어링을 구성합니다.

1단계: 보안 액세스에서 트래픽 조정 구성

Traffic Steering(트래픽 스티어링) > Add(추가) > Add a source(소스 추가)로 이동하고 DNS 서버

IP를 소스로 지정합니다.

2단계: Umbrella 서버에 DNS 트래픽 직접 전송

DNS 쿼리가 보안 액세스에 표시되도록 하려면 Umbrella DNS 서버(208.67.222.222 및 208.67.220.220)를 사용하도록 VPN 프로필을 구성합니다.

3단계: DNS 로깅 유효성 검사

트래픽 스티어링 컨피그레이션을 구현한 후 DNS 로그는 VPN 세션용 Secure Access 대시보드에 표시되어야 합니다.

VPN 프로필 DNS 모드 설정

VPN 프로필의 "DNS 모드" 설정은 이 컨피그레이션에 DNS 로그가 없는 것과 관련이 없습니다. RAVPN(Remote Access VPN) 세션은 이 설정과 상관없이 VPN에서 얻은 DNS 서버를 사용하며 로깅 가시성은 DNS 트래픽이 모니터링되는 DNS 인프라로 향하는지 여부에 따라 달라집니다.

보안 커넥터 설치 옵션

iOS에 보안 커넥터를 설치하면 다음을 사용할 수 있습니다.

- 보안 액세스에서 DNS 로깅 가시성
- 엔드포인트 ID 및 디바이스 등록 기능 향상
- Umbrella 방식 DNS 제어 및 보호

보안 커넥터는 Secure Client와 함께 사용할 수 있지만 두 구성 요소 간의 충돌을 방지하기 위해 적절한 트래픽 제외 및 설계 고려 사항이 필요합니다.

원인

그 근본 원인은 다음과 같습니다. iOS의 Cisco Secure Client는 VPN 연결을 제공하지만 Secure Access에서 DNS 가시성 및 디바이스 등록에 필요한 엔드포인트 에이전트 기능은 포함하지 않습니다. 이 기능을 사용하려면 보안 커넥터 설치 또는 트래픽 스티어링 컨피그레이션이 모니터링되는 인프라를 통해 DNS 쿼리를 전달해야 합니다. 이러한 구성 요소가 없으면 DNS 쿼리는 보안 액세스 모니터링을 우회하고, 디바이스 ID 정보는 로밍 디바이스 섹션에 채워지지 않습니다.

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.