보안 액세스에서 MX75 네트워크 터널의 보안 클라이언트 ID 가시성 문제

목차

문제

Secure Client가 있는 엔드포인트가 Secure Access에 연결된 MX75 네트워크 터널 뒤에 구축된 경우 시스템에 로밍 클라이언트 및 사용자 ID가 제대로 표시되지 않습니다. 다음과 같은 특정 동작이 관찰됩니다.

- 엔드포인트가 MX75 뒤에 있을 때 네트워크 터널 연결을 통해 보안 클라이언트의 우선 순위를 지정하도록 구성된 백오프 설정이 예상대로 작동하지 않습니다
- 트래픽이 로밍 클라이언트가 아닌 네트워크 터널 ID에만 기인하므로 도메인을 기반으로 하는 트래픽 조정 규칙은 적용되지 않습니다
- 활동 검색은 불완전한 소스 위치 정보를 표시하며, 사용자 및 로밍 클라이언트 ID를 생략한 채 네트워크 터널 ID만 표시합니다
- ID 기반 트래픽 조정 규칙(예: Active Directory 사용자 또는 로밍 클라이언트 ID 기반)은 MX75 터널을 통과하는 트래픽에 적용되지 않습니다

이러한 동작으로 인해 네트워크 터널 인프라를 통해 연결하는 엔드포인트에 대한 올바른 ID 분리 및 정책 적용이 방지됩니다.

환경

- Cisco Secure Access 구축
- 보안 액세스에 대한 네트워크 터널 컨피그레이션이 포함된 MX75 어플라이언스
- 모든 엔드포인트에 설치된 보안 클라이언트 에이전트
- 네트워크 터널 연결을 통해 보안 클라이언트의 우선 순위를 지정하기 위해 로밍 클라이언트에서 백오프 설정이 비활성화됨
- 도메인 기반 라우팅을 위해 구성된 트래픽 조정 규칙
- Active Directory 사용자 및 로밍 클라이언트에 대해 구성된 ID 기반 정책

해결

MX75 네트워크 터널을 통해 로밍 ID 가시성에 의존하는 대신 등록된 네트워크 접근 방식을 사용하여 해결 컨피그레이션을 구현하여 문제를 해결했습니다.

해결 방법 구현

1단계: 등록된 네트워크로 RSM(Roaming Security Module) 구성

기존 네트워크 터널 컨피그레이션을 등록된 네트워크 설정과 결합된 RSM 구축으로 교체합니다. 이 컨피그레이션을 통해 적절한 ID 속성 및 정책 적용이 가능합니다.

2단계: ID 가시성 검증

등록된 네트워크 컨피그레이션을 구현한 후 다음을 확인합니다.

- 사용자 ID가 활동 검색에 올바르게 표시됨
- 로밍 클라이언트 ID가 올바르게 표시되고 사용됩니다.
- 사용자 및 클라이언트 ID 기능을 기반으로 한 트래픽 조정 규칙

3단계: 트래픽 조정 기능 테스트

도메인 기반 트래픽 조정 규칙 및 ID 기반 정책이 새 컨피그레이션에 올바르게 적용되는지 확인합니다.

대안적 접근 방식

프라이빗 네트워크를 통한 ID 분리가 필요하지 않은 환경에서는 RSM - 인터넷 컨피그레이션 구현을 고려하십시오. 이 접근 방식은 RSM 트래픽을 사설 네트워크 터널이 아닌 인터넷으로 직접 전송합니다. 그러면 보안 제어를 유지하면서 적절한 ID 가시성을 제공할 수 있습니다.

기술 분석

트러블슈팅 중에 엔드포인트가 MX75 터널 뒤에 있을 때 ID 속성 동작을 입증하기 위해 policy.test.sse.cisco.com을 사용하여 진단 출력을 수집했습니다. 분석 결과, 네트워크 터널을 통해

로밍 ID를 라우팅하는 것이 기술적으로 가능하지만, 이 특정 구축 시나리오에서는 권장되거나 지원되는 운영 흐름이 아닌 것으로 확인되었습니다.

원인

근본 원인은 트래픽이 네트워크 터널 인프라를 통과할 때 Secure Access에서 ID 특성을 처리하는 방식과 관련이 있습니다. 엔드포인트가 MX75 네트워크 터널을 통해 연결되면 시스템은 개별 로밍 클라이언트 및 사용자 ID를 유지하는 대신 터널 ID에 모든 트래픽을 특성화합니다. 이 동작은 네트워크 터널 연결을 위해 설계되었지만 개별 ID 가시성 및 정책 애플리케이션에 대한 요구 사항과 충돌합니다.

기술적으로 네트워크 터널을 통해 로밍 ID를 라우팅하는 것이 가능하지만, 위에서 설명한 ID 특성 제한 때문에 이 컨피그레이션은 표준 운영 흐름으로 권장되거나 지원되지 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.