IPS 및 SWG 암호 해독 우회에 대해 SSE Do Not Decrypt 구성

목차

문제

재무 카테고리 또는 특정 도메인을 DND(Do Not Decrypt) 목록에 추가하고 관련 액세스 규칙을 적용한 후에도 재무 카테고리 대상에 대한 HTTPS 트래픽은 계속해서 원본 웹 사이트 인증서 대신 Cisco SSE 인증서를 제공합니다. 이 동작은 TIA(Zero Trust Access Client)를 통해 사이트에 액세스할 때 관찰되며, 특히 엔드 투 엔드 인증서 가시성이 필요한 https://onlinesbi.sbi.bank.in/과 같은 금융 관련 웹 사이트에 대한 액세스에 영향을 미칩니다.

예상된 동작은 사이트 또는 콘텐츠 카테고리가 DND 목록에 추가될 때 Cisco SSE 인증서 대신 원본 웹 사이트 인증서를 브라우저에 제공할 수 있다는 것입니다. 그러나 Cisco SSE 인증서는 계속 표시되며, 이는 DND 컨피그레이션에도 불구하고 트래픽 해독이 여전히 진행 중임을 나타냅니다.

환경

- Cisco SSE(Secure Service Edge)
- TIA(Zero Trust Access Client) 연결
- 전역 IPS 암호 해독 사용
- 액세스 정책에서 활성화된 IPS
- 보안 프로필 내의 Do Not Decrypt 목록에 구성된 재무 범주
- 해당 보안 프로필과 함께 적용된 액세스 규칙

해결

해결 방법에는 Cisco SSE가 두 가지 유형의 해독을 수행한다는 점을 이해하고 두 가지 해독 유형 모두에 대해 적절한 Do Not Decrypt 설정을 구성하는 것이 포함됩니다.

SSE 암호 해독 유형 이해

Cisco SSE는 두 가지 별도의 암호 해독 프로세스를 수행합니다.

- SWG(Secure Web Gateway) 암호 해독 - 웹 프록시 암호 해독
- IPS 암호 해독 - 침입 방지 시스템 암호 해독

보안 프로파일 내에 구성된 항목을 Do Not Decrypt는 SWG 해독에만 적용되며 IPS 해독을 방지하지 않습니다. 전역 IPS 암호 해독이 활성화되고 모든 액세스 정책에서 IPS가 활성화된 경우에도 IPS 암호 해독이 수행되므로 Cisco SSE 인증서가 브라우저에 표시됩니다.

컨피그레이션 단계

1단계: 제공된 System Provided Do Not Decrypt 목록에 사이트 또는 콘텐츠 범주를 추가합니다.

제공된 시스템 Do Not Decrypt 목록이 모든 IPS 프로필에 적용됩니다. 이 시스템 제공 목록에 사이트 또는 콘텐츠 카테고리를 추가하면 원본 웹 사이트 인증서가 표시되므로 IPS 암호 해독을 효과적으로 우회할 수 있습니다.

2단계: 추가 정책 변경이 필요하지 않은지 확인합니다.

액세스 정책 내에서 제공된 시스템 Do Not Decrypt List를 참조할 필요가 없습니다. 목록은 모든 IPS 프로파일에 자동으로 적용됩니다.

검증 테스트

이러한 유효성 검사 방법은 올바른 구성을 확인하는 데 사용할 수 있습니다.

방법 1: 제공된 시스템에 도메인 추가 Do Not Decrypt 목록

특정 도메인을 System Provided Do Not Decrypt List에 추가하면 Cisco SSE 인증서 대신 원본 웹 사이트 인증서가 제공될 수 있습니다.

방법 2: 일시적으로 전역 IPS 암호 해독 비활성화(테스트 전용)

전역 IPS 암호 해독을 일시적으로 비활성화하면 테스트한 사이트에 대해 원본 인증서가 표시되므로 IPS 암호 해독이 Cisco SSE 인증서 표시의 원인임을 확인할 수 있습니다.

예상 결과

적절한 컨피그레이션 후:

- 제공된 System Provided Do Not Decrypt List에 추가된 사이트 또는 콘텐츠 범주는 원래 웹 사이트 인증서를 제공합니다.
- SWG 및 IPS 암호 해독 모두 지정된 사이트 또는 범주에 대해 우회됩니다.
- 브라우저에 Cisco SSE 인증서 대신 실제 웹 사이트 인증서가 표시됩니다.

원인

이 문제는 Cisco SSE가 두 가지 암호 해독 프로세스를 수행하기 때문에 발생합니다. SWG 암호 해독 및 IPS 암호 해독 Do Not Decrypt 보안 프로필 내에 구성된 항목은 SWG 해독만 우회합니다. 전역 IPS 암호 해독이 활성화되고 액세스 정책에서 IPS가 활성화된 경우, IPS 암호 해독이 계속 독립적으로 수행되므로 보안 프로파일 DND 목록에 사이트가 포함된 경우에도 Cisco SSE 인증서가 브라우저에 표시됩니다.

두 암호 해독 유형을 완전히 우회하려면 사이트 또는 콘텐츠 카테고리를 System Provided Do Not Decrypt List에 추가해야 합니다. 이 목록은 모든 IPS 프로필에 적용되며 SWG 및 IPS 암호 해독 작업이 모두 발생하지 않도록 합니다.

관련 콘텐츠

- 보안 액세스를 위한 유효한 Do Not Decrypt 목록 생성
- 보안 액세스를 위한 문제 해결 및 기본 정보 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.