Cisco Secure Access에서 IPS 암호 해독 확인

목차

문제

Secure Client를 통해 RAVPN(Remote Access VPN)과 함께 Cisco Secure Access를 사용하는 경우, 조직은 특정 웹 사이트로 이동하는 트래픽에 대해 IPS(Intrusion Prevention System) 암호 해독 및 검사가 올바르게 수행되고 있는지 확인해야 합니다. 주요 과제는 액티비티 검색과 같은 표준 관리 UI 로그 이외의 방법을 통해 TLS 해독 및 검사 프로세스가 제대로 작동하고 있는지 확인하는 것이다. 특정 확인 요구 사항에는 테스트 검증을 지원하고 관리 인터페이스 이외의 IPS 작업에 대한 추가 확인을 제공할 수 있는 클라이언트측 인증서 확인 또는 디버그/보고 메커니즘 식별이 포함됩니다.

환경

- RAVPN 기능이 있는 CSA(Cisco Secure Access)
- 원격 액세스 VPN 연결을 위한 Cisco Secure Client
- IPS 해독 및 검사 기능 활성화
- 보안 검사를 위해 해독이 필요한 TLS/SSL 트래픽
- RAVPN 클라이언트에서 외부 웹 사이트로 이동하는 웹 트래픽

해결

Cisco Secure Access에서 원격 액세스 VPN 트래픽에 대해 IPS 암호 해독 및 검사가 올바르게 작동하는지 확인하는 두 가지 방법이 있습니다.

방법 1: 관리 UI 활동 검색(기본 방법)

Cisco Secure Access 관리 인터페이스의 활동 검색 기능은 IPS 해독 및 검사 작업을 확인하는 가장 안정적인 방법을 제공합니다. 이 인터페이스에는 보안 서비스에서 트래픽을 해독하고 검사한 시기를 보여주는 자세한 로그와 분석이 표시됩니다.

활동 검색에 액세스하려면

Cisco Secure Access 관리 대시보드로 이동하고 활동 검색 기능을 찾아 특정 사용자 세션 및 대상 웹 사이트에 대한 트래픽 검사 로그 및 암호 해독 상태를 검토합니다.

암호 해독 로그를 사용하려면 전역 설정에서 이 설정을 사용하도록 설정할 수 있습니다.

대시보드 -> 보안 -> 액세스 정책 -> 규칙 기본값 및 전역 설정 -> 전역 설정 -> 암호 해독 로깅.

방법 2: 클라이언트측 인증서 확인

추가 확인 방법으로 클라이언트 측 인증서 확인을 수행하여 트래픽 해독이 발생하는지 확인할 수 있습니다.

Cisco Secure Access가 성공적으로 TLS 트래픽을 해독 및 검사하면 원래 웹 사이트 인증서 대신 자체 인증서를 클라이언트에 표시합니다.

인증서 검사를 통해 암호 해독을 확인하려면

1. 웹 사이트 인증서 확인
브라우저에서 인증서 세부사항을 열고 발급자 및 유효 기간을 검토합니다.

유효 기간이 ~10일인 Cisco Secure Access Root CA에서 인증서를 발급한 경우, 방화벽 레벨에서 Intrusion Prevention System 암호 해독을 나타냅니다.

인증서 유효기간이 약 5일인 경우 Secure Web Gateway 기반 암호 해독을 나타냅니다.

2. 인증서 발급자(DC 이름 지정) 확인

이 클라이언트 측 인증서 검증 방법은 기본 활동 검색 방법과 함께 보조 확인 기법의 역할을 하며, IPS 해독 프로세스가 예상대로 작동하고 있다는 추가적인 보장을 제공합니다.

Intrusion Prevention System Do Decrypt:

다음과 같은 경우 침입 방지 시스템에 대한 암호 해독이 수행됩니다.

· 전역 설정 및

· Intrusion Prevention System은 하나 이상의 액세스 정책 규칙에 대해 활성화되어 있습니다(규칙이 비활성화되어 있더라도 이 조건은 여전히 적용된다고 생각함).

Intrusion Prevention System 암호 해독에서 도메인 우회

제공된 시스템 암호 해독 목록 사용 및 제공된 시스템 암호 해독 목록에 도메인 추가

또는

Cisco Secure Access의 전역 설정에서 소스 기반 암호 해독 활용 -

참고:보안 액세스의 네트워크 터널 컨피그레이션에 구성된 아웃바운드 NAT가 없는 경우 이 기능이 작동합니다.

원인

엔터프라이즈 환경에서 보안 정책 시행을 검증하기 위한 요구 사항에서 여러 검증 방법이 필요합니다. 관리 UI 로그가 포괄적인 가시성을 제공하는 반면, 클라이언트측 확인 방법은 규정 준수 테스트, 문제 해결 및 관리 인터페이스에 대한 직접 액세스가 제한될 수 있거나 철저한 테스트 절차를 위해 여러 확인 지점이 필요한 확인 시나리오에 유용할 수 있는 추가 확인 지점을 제공합니다.

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.