Secure Access Password-Protected ZIP 파일 다운로드 구성

목차

문제

Cisco Secure Access로 마이그레이션한 후에는 비밀번호로 보호된(암호화된) ZIP 파일을 다운로드할 수 없습니다. Secure Access 서비스를 통해 암호화된 파일 콘텐츠에 액세스하려고 하면 다운로드가 일관되게 실패합니다. 이 문제는 카테고리 기반 차단, SSL 검사 제어, 샌드박스 기능 등 여러 보안 규칙을 사용하여 C8200 디바이스에서 인터넷 바인딩 트래픽 정책을 구성했음에도 불구하고 발생합니다.

사용자는 Secure Access 마이그레이션 전에 이전에 액세스할 수 있었던 비밀번호로 보호된 ZIP 파일에 액세스를 시도할 때 완전한 다운로드 실패를 경험합니다. 이 문제는 여러 터널 그룹에서 지속되며 구성된 15개 위치 모두에 영향을 미칩니다.

환경

- Cisco Secure Access(보안 액세스 조직ID: 8320925)
- 인터넷 바인딩 트래픽 정책을 관리하는 C8200 디바이스
- 15개 위치에 여러 터널 그룹(TK-TG 및 기타)
- 활성화된 컨피그레이션과 비활성화된 컨피그레이션이 모두 포함된 SSL 검사 정책
- 특정 정책에서 활성화된 샌드박스 보안 프로파일
- 특정 액세스 규칙에 구성된 IPS 프로파일

해결

Cisco Secure Access에서 비밀번호로 보호되는 ZIP 파일 다운로드를 허용하기 위한 해결책에는 암호화된 파일에 대한 액세스 허용 설정을 구성하고 필요한 경우 적절한 해결 방법을 구현하는 것이 포함됩니다.

기본 컨피그레이션 방법

1단계: Cisco 보안 액세스 정책 컨피그레이션에 액세스

Cisco Secure Access 대시보드에서 영향을 받는 트래픽을 처리하는 특정 액세스 정책으로 이동합니다.

2단계: 암호화된 파일 액세스 사용

정책 Advanced Settings(고급 설정)에서 Allow access to encrypted files(암호화된 파일에 대한 액세스 허용) 옵션을 찾아 활성화합니다. 이 설정은 규칙별로 구성되며, 해당 특정 정책을 통해 암호화된 콘텐츠에 액세스할 수 있는지 여부를 제어합니다.

3단계: 컨피그레이션 적용

정책 변경 사항을 저장하고 적용하여 사용자 트래픽에 대해 활성화하십시오.

대체 해결 방법

기본 방법으로 문제가 해결되지 않으면 다음 섹션에서 설명하는 해결 방법을 구현합니다.

1단계: 영향을 받는 URL 식별

비밀번호로 보호된 ZIP 파일이 호스팅되어 다운로드 오류를 일으키는 특정 URL 또는 도메인을 확인합니다.

2단계: Do Not Decrypt 목록 구성

식별된 URL을 Cisco Secure Access 컨피그레이션의 Do Not Decrypt 목록에 추가합니다. 이렇게 하면 이러한 특정 URL에 대한 SSL 검사가 방지됩니다.

3단계: SSL 검사 우회 정책 생성

SSL 검사가 비활성화된 액세스 정책이 이러한 URL에 대한 트래픽을 처리하도록 구성되어 있는지 확인합니다.

이 정책에는 다음이 있어야 합니다.

- SSL 검사 사용 안 함
- 모든 보안 프로파일 사용 안 함
- SSL 검사 지원 정책보다 우선 순위가 높음

정책 컨피그레이션 참조

다음 하위 섹션에 설명된 정책 순서 및 각 컨피그레이션을 적절한 트래픽 처리를 위한 참조로 사용할 수 있습니다.

정책 1: 카테고리 기반 차단 규칙

- 정책 이름: IA-To-InternetContent블록
- IPS 프로필: 없음

- 목적: 특정 콘텐츠 범주 차단
- 대상: 모든 터널 그룹

정책 2: SSL 검사 사용 안 함 규칙

- 정책 이름: IA-SSL-Inspection-MUKOU
- IPS 프로필: 비활성화됨
- 보안 프로파일: 모두 사용 안 함
- 대상: 모든 터널 그룹

정책 3: SSL 검사 사용 규칙

- 정책 이름: IA-SSL-검사
- IPS 프로필: 활성화됨
- 보안 프로파일: 샌드박스 기능 사용
- 대상: 모든 터널 그룹

중요 구성 참고 사항

암호화된 파일에 대한 액세스 허용 기능에 해당하는 전역 설정이 없습니다. 이 설정은 필요에 따라 개별 액세스 정책에 구성해야 합니다. 암호화된 파일 액세스가 필요한 각 정책에는 고급 설정 컨피그레이션에서 이 설정을 명시적으로 사용하도록 설정해야 합니다.

컨피그레이션 변경 사항을 테스트할 때는 기능을 검증하기 전에 Cisco Secure Access 인프라 전반에 정책 전파에 충분한 시간을 할애해야 합니다. 서비스 인시던트 또는 유지 관리 기간은 테스트 결과에 영향을 미칠 수 있으며 트러블슈팅 시 고려해야 합니다.

원인

이 문제는 Cisco Secure Access가 기본적으로 보안 조치로 암호화된 파일에 대한 액세스를 차단하기 때문에 발생합니다. SSL 검사가 활성화되고 비밀번호로 보호되거나 암호화된 콘텐츠가 발견되면, 이러한 액세스를 허용하도록 명시적으로 구성되지 않는 한 서비스는 다운로드를 차단합니다. 액세스 정책의 고급 설정에서 암호화된 파일에 대한 액세스 허용 설정은 이 동작을 제어하며, 이 설정을 사용하지 않으면 암호화된 ZIP 파일 및 유사한 콘텐츠가 다운로드 프로세스 동안 차단됩니다.

또한 SSL 검사 정책은 검사 프로세스에서 암호화된 콘텐츠를 제대로 처리할 수 없을 때 암호화된 파일 다운로드를 방해할 수 있으므로, 영향을 받는 URL에 대해 암호화된 파일 액세스 설정 또는 SSL 검사 우회가 필요합니다.

관련 콘텐츠

- 고급 보안 제어
- 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.