Secure Access Security Profiles 구성 API 고급

목차

문제

공용 API를 통해 Cisco Secure Access Security Profile을 구성하려고 할 때 기본 설정의 기본 프로필 생성만 가능한 제한 사항이 발생합니다. API에서는 다음과 같은 고급 보안 기능에 대한 세분화된 컨피그레이션 옵션을 공개하지 않습니다.

- TLS 암호 해독 설정
- 위협 범주 시행 제어
- 파일 유형 차단 및 검사
- 악성코드 검사 설정

사용자는 표준 API 호출을 통해 암호 해독 설정을 구성하려고 할 때 "403 Forbidden" 오류를 수신한다고 보고합니다. 문서화된 퍼블릭 API 엔드포인트에는 GUI 인터페이스를 통해 사용할 수 있는 세부적인 보안 프로필 컨피그레이션 매개변수가 없어 프로그래밍 가능한 관리 기능이 제한되는 것으로 보입니다.

환경

- Cisco Secure Access 플랫폼
- 보안 프로파일 API 구현
- 영향을 받는 모든 소프트웨어 버전
- 공용 API 설명서 엔드포인트

해결

고급 보안 프로파일 컨피그레이션 기능은 Cisco Secure Access API를 통해 사용할 수 있지만, 문서화된 공용 API 예와 다른 구체적인 구현 접근 방식과 필드 명명 규칙이 필요합니다. 이 해결 단계에서는 각 구성 영역을 다룹니다.

기본 보안 프로필 생성 워크플로

고급 설정으로 보안 프로파일을 생성하는 적절한 워크플로는 2단계 프로세스를 따릅니다.

1단계: POST를 사용하여 기본 보안 프로필을 생성합니다.

```
POST /api/v1/security-profiles
{
  "name": "profile_name",
  "description": "profile_description"
}
```

2단계: 프로파일 ID와 함께 PUT를 사용하여 고급 옵션을 구성합니다.

```
PUT /api/v1/security-profiles/{profile_id}
{
  "advanced_settings": {
    "decryption_settings": {...},
    "file_settings": {...},
    "threat_settings": {...}
  }
}
```

파일 검사 및 파일 유형 차단 컨피그레이션

PUT 요청 내에서 다음 API 필드 이름을 사용하여 파일 검사 및 파일 유형 차단을 구성할 수 있습니다.

- fileEngines - 파일 검사 기능을 제어합니다.
- fileTypeControlStatus - 파일 형식 차단을 활성화하거나 비활성화합니다.

파일 설정의 컨피그레이션 예:

```
{
  "fileEngines": "enabled",
  "fileTypeControlStatus": "active",
  "blockedFileTypes": ["exe", "zip", "rar"]
}
```

TLS 암호 해독 컨피그레이션

TLS 암호 해독 컨피그레이션에서는 전용 POST 엔드포인트를 사용하는 대신 Do Not Decrypt 목록 ID를 참조해야 합니다. 컨피그레이션은 다음 접근 방식을 사용하여 PUT API 요청을 통해 구현됩니다.

1단계: 기존 컨피그레이션에서 Do Not Decrypt 목록 ID를 식별합니다.

2단계: PUT API 요청에서 목록 ID를 참조합니다.

```
{
  "seetingGroupBypassInspectionGroupID": "do_not_decrypt_list_id",
  "decryptionEnabled": true
}
```

이렇게 하면 다른 API 메서드를 통해 암호 해독을 구성하려고 할 때 발생하는 "403 Forbidden" 오류가 해결됩니다.

위협 범주 컨피그레이션

위협 범주 컨피그레이션은 암호 해독 컨피그레이션이 성공한 후 액세스할 수 있는 문서화되지 않은 API 엔드포인트를 통해 사용할 수 있습니다. 엔드포인트는 세분화된 위협 범주 제어를 허용하지만 먼저 암호 해독 설정으로 보안 프로필을 올바르게 구성해야 합니다.

API 필드 이름 참조

이 표에서는 공통 보안 프로파일 기능을 해당 API 필드 이름에 매핑합니다.

기능	API 필드 이름	설명
TLS 암호 해독	그룹 우회 검사 그룹 ID 설정	참조에서 목록 ID를 해독하지 않음

파일 검사	파일 엔진	파일 검사 기능 제어
파일 형식 차단	파일 유형 제어 상태	파일 형식 제한 사용

원인

이러한 제한은 주로 실제 기능 제한이 아닌 불완전한 API 설명서 및 직관적이지 않은 필드 명명 규칙에 기인합니다. 고급 보안 프로파일 컨피그레이션 기능은 API 내에 있지만 다음을 사용하여 구현됩니다.

- GUI 용어와 다른 명확하지 않은 필드 이름
- 2단계 워크플로(생성을 위한 POST, 고급 구성을 위한 PUT)
- 기존 컨피그레이션 객체에 대한 종속성(예: Do Not Decrypt 목록)
- 특정 기능에 대한 문서화되지 않은 API 엔드포인트

공용 API 문서에서는 이러한 구현 세부사항을 명확하게 공개하지 않으므로 대체 방법을 통해 기능을 실제로 사용할 수 있는 경우 API 제한을 인식하게 됩니다.

관련 콘텐츠

- Cisco Secure Access Security Profiles API 설명서
- 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.