Secure Web Gateway SWG 웹 사이트 액세스 문제 해결

목차

소개

이 문서에서는 클라우드 기반 프록시(Secure Web Gateway/SWG)를 통해 라우팅될 때 DIA(Direct Internet Access)를 사용할 때가 아닌 웹 사이트 액세스 문제를 진단하기 위한 체계적인 방법론에 대해 설명합니다.

- 범위: Cisco Umbrella SIG 및 Cisco Secure Access 모두에 적용됩니다.

전제 조건 및 중요 경고

- 재현 가능한 문제에 대해 모든 트러블슈팅이 수행되었는지 확인합니다.
- 분석을 위한 정확한 데이터를 제공하기 위해 HAR(HTTP Archive) 파일 및 PCAP(Simultaneous Packet Capture)를 수집합니다.
- 프록시 정책을 변경하면(예: 암호 해독 또는 검사를 우회하는 경우) 보안 상태에 영향을 줄 수 있습니다. 문제 해결 또는 권장 사항에만 적용합니다.

프록시 레벨 오류 식별

일반적인 프록시 간섭 지표는 다음과 같습니다.

- 502 불량 게이트웨이
- 515 업스트림 인증서를 신뢰할 수 없음
- 517 업스트림 인증서가 해지됨
- 403 금지
- 폐기된 인증서
- 암호 그룹 불일치
- 웹 사이트 연결 시간 초과

문제 해결 방법론

1단계: 트래픽이 프록시를 통과하는지 확인

- 데이터 수집: 문제가 발생하면 HAR 파일 및 PCAP를 생성합니다.
- 헤더 분석: HTTP 응답에서 Via 헤더를 검사합니다. `s_proxy`(Nginx proxy) 또는 `m_proxy`(Modular Proxy Service/MPS)가 있으면 트래픽이 프록시되었음을 확인합니다.
- TCP 스트림: Wireshark에서 TCP 스트림을 따라 대상 IP가 아닌 프록시 IP에 연결합니다.

2단계: TLS 암호 해독 상태 확인

- 브라우저 검사: 브라우저 주소 표시줄에서 잠금 아이콘을 클릭합니다. Cisco Secure Access Root Certificate가 인증서 체인에 나타나면 HTTPS 검사가 활성화됩니다.
- 검증: HAR/PCAP 파일에서 Via 헤더를 상호 참조합니다.
- OpenSSL 명령: 인증서 체인을 검사하려면
  `openssl s_client -connect www.example.com:443 -showcerts`
  이 명령은 서버에서 제공하는 인증서 체인을 확인합니다. 직접 검증을 위해 프록시를 통과하는 시스템에서 실행합니다.

3단계: 격리 및 제거 과정

1. A단계 - 테스트 HTTPS 검사(Nginx 계층):
   - 문제가 있는 도메인을 SWG "Do Not Decrypt" 목록에 추가합니다.
   - 파일 검사를 활성화한 상태로 유지합니다.
   - 문제가 해결된 경우 근본 원인은 Nginx SSL/TLS 검사일 가능성이 높습니다. PCAP에서 암호화 불일치 또는 SNI 문제를 분석합니다. 동작을 비교하려면 프록시와 함께 또는 없이 curl을 사용합니다.
   - 문제가 지속되는 경우: 단계 B로 진행합니다.
2. B단계 - 파일 검사 테스트(스캐닝 레이어):
   - 특정 트래픽에 대해 파일 검사를 비활성화합니다.
   - 문제가 해결된 경우 근본 원인은 파일 검사 엔진에 있습니다. PCAP 및 HAR을 검토하고, Lab에서 재현한 다음 특정 파일 또는 스캔 시그니처로 인해 문제가 발생하는지 확인합니다.
   - 해결되지 않는 경우: 종합 로그 및 결과를 지원 부서에 문의하십시오.

일반적인 문제 및 오류 코드

515 업스트림 인증서를 신뢰할 수 없음

이 오류는 SWG 프록시가 대상 서버의 인증서를 검증할 수 없을 때 발생합니다. 원인은 만료, 자체 서명 또는 불완전한 인증서 체인이 있습니다.

- HTTPS 검사 대상 + 파일 검사 대상: 웹 사이트 작업; 인증서 오류가 없습니다.
- HTTPS 검사 켜기 + 파일 검사 끄기: 515 오류가 발견되어 사용자 보고서와 일치합니다.
- HTTPS 검사 OFF + 파일 검사 OFF(Do Not Decrypt 목록의 도메인): 문제가 관찰되지 않았습니다.

기술 세부사항: 업스트림 서버가 AIA(Authority Information Access) 가져오기를 사용하여 중간 인증서를 누락하는 경우 Nginx 프록시가 실패할 수 있습니다. Nginx는 AIA를 파일 검사 프록시 서비스처럼 정상적으로 처리하지 않기 때문입니다. TLS 핸드셰이크 중 SNI 및 SAN 불일치는 실패를 트리거할 수도 있습니다.

517 업스트림 인증서가 해지됨

517 오류는 SWG 프록시의 CRL 또는 OCSP 검사에서 업스트림 서버의 인증서가 폐기되었음을 의미합니다.

- 문제 해결: SSL Labs 또는 OpenSSL과 같은 외부 툴을 사용하여 폐기 상태를 확인합니다.
- 설명서:
  - Cisco 트러블슈팅 오류 517 - 업스트림 인증서가 해지됨
  - 일반 인증서 및 프로토콜 오류 이해

인증서 오류 처리 옵션

Cisco Secure Access는 암호 해독을 완전히 비활성화하지 않고 세분화된 오류 우회를 위해 "인증서 오류 처리 옵션"이라는 새로운 기능을 도입할 예정입니다. 검사로 인해 인증서 오류가 발생하는 도메인은 광범위한 "Do Not Decrypt" 목록 대신 이 기능을 사용하여 관리할 수 있습니다.
이 기능은 오늘부로 Umbrella SIG에 존재합니다. CSA에 대한 기능 요청 세부 정보

502 불량 게이트웨이

502 오류는 SWG 프록시가 중재자 역할을 하면서 업스트림 서버로부터 잘못된 응답을 받았음을 나타냅니다.

- 다운스트림: 클라이언트에서 SWG로의 프록시

- 업스트림: 대상 서버에 대한 SWG 프록시

프로토콜 오류, TCP 재설정 또는 헤더 형식이 잘못되어 오류가 항상 업스트림 연결에 있습니다.

일반적인 502 원인

- 지원되지 않는 SWG 암호 그룹
- 클라이언트 인증서 인증 요청
- SWG 프록시에서 추가된 헤더

지원되지 않는 암호 그룹

원인: 서버에 SWG에서 지원하지 않는 암호가 필요합니다(예: TLS_CHACHA20_POLY1305_SHA256).
해결 방법: 선택적 암호 해독 목록에 도메인을 추가합니다.

테스트 명령:
프록시 사용:

```
curl -x proxy.sig.umbrella.com:80 -v xyz.com:80
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k "https://www.cnn.com" >> null
```

프록시 없음:

```
curl -v www.xyz.com:80
```

Mac/Linux:

```
curl -vvv -o /dev/null -k -L www.cnn.com
```

창:

```
curl -vvv -o null -k -L www.cnn.com
```

클라이언트 인증서 인증 요청

원인: 업스트림 서버에는 SWG가 지원하지 않는 클라이언트측 인증서가 필요합니다.
해결 방법: 외부 도메인 관리 목록(Umbrella SIG) 또는 보안 프록시 우회(Cisco Secure Access)를 사용하여 프록시에서 도메인을 우회합니다. HTTPS 검사만 우회하는 것은 충분하지 않습니다.

프록시에서 추가된 헤더

원인: 일부 서버는 HTTPS 검사가 활성화된 경우 SWG에서 추가한 XFF(X-Forwarded-For) 헤더가 있는 요청을 거부합니다.

해결 방법: HTTPS 및 파일 검사와 동작 비교 XFF가 있는 경우에만 오류가 발생하면 웹 서버가 잘못 구성되었을 수 있습니다.

예:

```
curl https://www.xyz.com -k –헤더 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "상태 코드: %{http_code}" -s
```

상태 코드: 502

```
curl https://www.xyz.com -k -o /dev/null -w "상태 코드: %{http_code}" -s
```

상태 코드: 200

지오로케이션에 대한 XFF 헤더가 추가됩니다. 서버에서 처리할 수 없는 경우 502 오류가 발생합니다.

잠재적으로 원치 않는 PUA 또는 손상된 파일

SWG가 파일 검사(예: 보호, 범위 요청 또는 손상된 파일)를 사용하여 파일을 스캔할 수 없는 경우 다운로드 및 보고서 - 차단됨 - 잠재적으로 원치 않는 응용 프로그램(보호된 파일)을 차단합니다

- 문제 해결: 차단 이벤트 중에 HAR을 캡처합니다. 임시 해결 방법으로 Override Security를 사용합니다. 파일이 손상되었거나 악의적인 경우 소스에서 수정해야 합니다.

잠재적으로 유해한 카테고리 및 평판 블록

- Talos를 사용하여 웹 평판(WBRS)을 확인합니다. 도메인이 잘못 분류된 경우 COG Jira 요청을 Talos에 제출하여 검토하십시오. Talos는 안전하거나 우호적이지만 여전히 SWG 블록으로 분류되었으며, SWG의 Beaker 서비스에서 확인이 필요합니다.

SWG 이그레스 IP에 대한 Akamai의 액세스 거부

- SWG는 공유 이그레스 IP를 사용합니다. IP 평판 서비스(예: Brightcloud)에 의해 블랙리스트에 추가된 경우 특정 사이트에 대한 액세스가 거부될 수 있습니다.

알려진 문제: Youtube 로그인 봇 및 비디오를 사용할 수 없음

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.