인증 후 은행 사이트에 대한 보안 액세스 502 오류

목차

문제

사용자가 FCBanking에 성공적으로 인증한 후 502 잘못된 게이트웨이 HTTP 오류 코드를 받았다고 보고했습니다. 인증 프로세스가 성공적으로 완료되어 사용자가 로그인 자격 증명을 입력할 수 있지만, 인증 직후 브라우저에 502 잘못된 게이트웨이 오류가 표시되었습니다.

FCBanking용 도메인 및 관련 카테고리는 SSL 및 IPS 해독에서 제외되었으며 이 컨피그레이션 변경으로 502 HTTP 오류가 해결되지 않았습니다. 문제가 간헐적으로 발생했으며 FCBanking 도메인에 대해 보안 액세스를 완전히 우회한 후에만 해결되었습니다. HAR 파일 분석에서 'my.fcbanking.com'의 대상에서 502개의 오류가 발견되었으며, 활동 검색 로그에는 HAR 파일에서 캡처된 502개의 오류가 표시되지 않았으며, 이는 이러한 오류가 중간 디바이스 레벨에서 발생했음을 나타냅니다.

환경

- Cisco Secure Access - 인터넷 액세스(로밍 모듈, VA, DNS, SWG, PAC, IPS, 인증서)
- 네트워크 토폴로지: User PC(사용자 PC) > Switch(스위치) > Catalyst SD-WAN Router(Catalyst SD-WAN 라우터) > Local internet or CSA tunnel(로컬 인터넷 또는 CSA 터널)
- NTG(Network Tunnel Group)를 우회하여 DIA(Direct Internet Access)를 통해 포트 80 및 443의 모든 트래픽을 전송하도록 애플리케이션 정책 규칙으로 구성된 Catalyst SD-WAN 에지
- Cisco Secure Client Secure Access에 대한 트래픽 라우팅을 확인하기 위해 바이패스 목록에 의존
- 은행 업무 영역: fcbanking.com 및 관련 하위 도메인(my.fcbanking.com, treasury.fcbanking.com)

해결

기본 해결 방법에는 보안 액세스를 완전히 우회하기 위해 뱅킹 도메인을 추가하는 작업이 포함되며, 이를 통해 DNS 레이어 보안을 유지하면서 트래픽을 인터넷에 직접 전달할 수 있습니다.

1단계: Bypass 목록에 주 도메인 추가

- Secure Access 컨피그레이션의 bypass proxy only 목록에 fcbanking.com을 추가합니다. 이렇게 하면 웹 트래픽이 보안 액세스 프록시를 우회하는 동안 DNS 레이어 보안이 적용되고 작업 검색에 기록됩니다.

2단계: 도메인 별칭 식별 및 추가

- 뱅킹 사이트에서는 우회 목록에 추가해야 하는 여러 별칭을 사용하는 경우가 많습니다. 캐시 검사를 사용하여 뱅킹 도메인에 대한 모든 별칭을 식별합니다.
- fcbanking.com의 경우 이러한 별칭이 식별되어 우회 목록에 추가되었습니다.
    - treasury.fcbanking.com(별칭: treasuryvanity.jackhenry.com)
    - my.fcbanking.com(별칭: banno-online.jackhenry.bank)
    - treasuryvanity.jackhenry.com
    - banno-online.jackhenry.bank

3단계: IP 주소를 사용한 대체 해결

- 도메인 기반 우회에 대한 대안으로, 은행 사이트의 확인된 IP 주소를 우회 목록에 추가할 수 있습니다. Cisco Secure Client는 우회 목록에 있는 FQDN을 IP 주소로 변환하고 웹 트래픽을 인터넷으로 직접 라우팅합니다.

4단계: 문제 해결을 위해 디버그 로깅 활성화

- 추가 분석을 위해 자세한 로그를 캡처하려면 최대 디버그 로깅을 활성화합니다.
- 다음 내용으로 'SWGConfigOverride.json'이라는 파일을 만드십시오.

```
{"logLevel": "1"}
```

SWGConfigOverride.json 파일을 SWG 폴더에 배치합니다.

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
```

SWG 또는 Umbrella 서비스를 다시 시작하거나 시스템을 다시 시작하여 디버그 로깅 컨피그레이션을 적용합니다.

참고: 디버그 로깅은 시스템 성능에 영향을 미치지 않지만 로그 파일 크기를 늘릴 수 있습니다. DART 번들을 가져온 후 SWGConfigOverride.json 파일을 제거하여 정상 로깅 수준으로 돌아갑니다.

5단계: 확인

- 우회 구성을 구현한 후 사용자가 은행 사이트에 액세스할 때 더 이상 502개의 오류를 보고하지 않았습니다. DNS 트래픽은 액티비티 검색에 계속 로깅되는 반면 웹 트래픽은 인터넷으로 직접 이동합니다.

원인

은행 사이트는 일반적으로 프록시 서버 또는 공유 IP 주소 범위에서 발생하는 트래픽을 탐지하고 차단하는 보안 조치를 구현합니다. Cisco Secure Access는 프록시 트래픽에 공유 IP 범위(151.186.144.0/20 및 151.186.176.0/20)를 사용합니다. 이 프록시 트래픽은 은행 사이트에서 HTTP 502 오류를 감지하고 자동으로 삭제 또는 응답할 수 있습니다.

도메인이 do not decrypt 목록에 있으면 소스 IP가 Secure Access 공유 IP 범위에서 시작되는 것으로 나타나 은행 사이트의 보안 메커니즘이 트리거됩니다. 또한 뱅킹 트래픽 및 도메인 별칭에 대한 IPS 검사가 제대로 면제되지 않을 경우 연결 실패에 기여할 수 있습니다. 이 문제의 간헐적 특성과 HAR 파일에 나타나지만 활동 검색 로그에는 나타나지 않는 502개의 오류는 대상 은행 서버가 아닌 중간 프록시 처리에 의해 오류가 발생했음을 나타냅니다.

관련 콘텐츠

- SWG 웹 사이트 액세스 문제 해결

- QUIC 프로토콜을 비활성화하여 적절한 웹 트래픽 검사 보장
- Cisco Secure Access IP 범위 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.