

보안 액세스 SWG를 통해 애플리케이션에 액세스 할 때 HTTP 429 속도 제한 및 연결 오류

목차

문제

사용자는 Cisco Secure Access SWG(Secure Web Gateway)를 통해 <https://xxxx.com>과 같은 애플리케이션에 액세스를 시도할 때 HTTP 429 속도 제한 [오류](#)가 발생합니다. 이 문제는 기업 관리 랩톱에 영향을 미치며, 케이스를 열기 약 2주 전에 시작되었습니다. 사용자는 로그인 시도 중에 또는 성공적인 인증 후 특정 애플리케이션 기능에 액세스 할 때 이러한 오류를 경험 합니다.

또한 도메인을 Secure Access Bypass 목록에 추가하면 OTP(One-Time Password) 입력 중에 HTTP 500 서버 오류가 발생하거나 트래픽이 더 이상 SWG IP 범위(151.186.x.x)를 통과하지 않을 때 일반 연결 오류가 발생합니다.

애플리케이션 소유자가 최근 서버 측에서 속도 제한이 변경되지 않았음을 확인했으며, 이 문제는 Cisco Secure Access SWG 이그레스 IP 주소에서 시작된 트래픽과 관련된 것으로 보입니다.

환경

- SWG를 지원하는 Cisco Secure Access(이전의 Cisco Umbrella)
- Cisco SSE(Security Service Edge) 클라이언트를 사용하는 기업 관리형 노트북 컴퓨터
- SWG 이그레스 IP 범위: 151.186.x.x
- 데이터 센터: AWS 싱가포르(아시아 태평양 1) 및 AWS 미국 서부(오레곤)
- 애플리케이션: <https://sbstransit.aereacommercial.com>

해결

해결에는 바이패스 컨피그레이션을 구현하고 애플리케이션 소유자와 조정하여 특정 IP 주소를 허용하는 작업이 포함됩니다.

다음 단계를 수행합니다.

1단계: 현재 SWG 동작 확인

영향을 받는 디바이스에서 이 URL에 액세스하여 현재 정책 및 이그레스 IP 정보를 확인합니다.

<https://policy.test.sse.cisco.com/?host=https://sbstransit.aereacommercial.com>

이는 현재 사용되고 있는 SWG 이그레스 IP(일반적으로 151.186.x.x 범위)를 보여주며, Secure Access SWG를 통해 트래픽이 처리되고 있는지 확인합니다.

2단계: Secure Access Bypass 목록에 도메인 추가

Cisco Secure Access 대시보드에서 Internet Settings(인터넷 설정) > Bypass Secure Access(보안 액세스 우회)로 이동하고 문제가 있는 도메인을 추가하여 DNS 및 SWG 검사를 모두 우회합니다.

sbstransit.aereacommercial.com

3단계: 회사 네트워크가 아닌 네트워크에서 액세스 테스트

Secure Access SWG(151.186.x.x 범위)를 통해 트래픽이 이그레스(egress)하지 않는 네트워크에서 애플리케이션 액세스를 테스트합니다. 이 작업은 개인 디바이스에서 수행하거나 SSE 클라이언트를 일시적으로 비활성화하여 수행할 수 있습니다.

다음은 방문하여 공용 ISP IP 주소를 식별합니다.

<https://whatismyip.com>

4단계: 애플리케이션 소유자와 IP 허용 목록 조정

식별된 공용 ISP IP 주소를 애플리케이션 소유자에게 제공하고 이 IP를 애플리케이션 측에서 허용 되도록 요청합니다. 이를 통해 애플리케이션이 보안 액세스 SWG 이그레스 IP에 영향을 주는 IP 기반 제한을 구현하고 있는지 확인할 수 있습니다.

5단계: 해결 확인

애플리케이션 소유자가 IP 허용 목록을 구현한 후 액세스 동작을 테스트하여 사용자가 HTTP 429 또는 연결 오류가 발생하지 않고 애플리케이션에 성공적으로 액세스할 수 있는지 확인합니다.

원인

애플리케이션이 소스 IP 주소를 기반으로 속도 제한 또는 액세스 제한을 구현하는 것으로 보입니다. 여러 사용자가 Cisco Secure Access SWG를 통해 애플리케이션에 액세스하는 경우 모든 트래픽은 공유 SWG 이그레스 IP 범위(151.186.x.x)에서 시작되는 것으로 보입니다. 그러면 단일 IP 주소 또는 IP 범위에서 과도한 요청이 오는 것을 감지하므로 애플리케이션의 속도 제한 메커니즘이 트리거됩니다.

이 문제는 기업 관리 디바이스가 개인 네트워크에 연결된 경우에도 SSE 클라이언트를 통해 트래픽을 계속 라우팅하여 애플리케이션의 제한을 트리거하는 것과 동일한 이그레스 IP 동작을 유지한다는 점에서 더욱 심각해집니다.

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.