PAC 파일에 대한 보안 액세스 SWG 프록시 연결 문제 해결

목차

문제

사용자는 SWG(Secure Web Gateway) 프록시 URL swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com을 사용하여 Cisco Secure Access를 통해 웹 사이트에 액세스하려고 시도할 때 연결 실패를 경험했습니다.

구체적인 증상은 다음과 같습니다.

- 브라우저에서 연결 오류가 발생하여 웹 요청(예: https://www.google.com)이 실패했습니다.
- 활동 검색 로그에 트래픽이 표시되지 않음
- 클라이언트 소스 IP/클라이언트 이그레스 IP에서 대상 엔드포인트로 향하는 서버 재설정이 관찰되었습니다.
    - k8s-sigpro-sigpro-c10eb6eb-38fbeb0455191ac5.elb.eu-central-1.amazonaws.com
    - k8s-sigpro-sigpro-f8f3d861-14341dd91e659675.elb.eu-central-1.amazonaws.com
- 문제가 CEST 기준 오전 09:30에 시작됨
- SWG 호스트 이름에 대한 DNS 확인이 올바르게 작동함
- 포트 443에서 swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com에 대한 텔넷 연결에 성공했습니다.
- 외부 방화벽이 대상 IP에 대한 연결을 차단하지 않았습니다.

패킷 캡처 분석을 통해 프록시에서 오는 TCP RST 패킷이 확인되었으며, 이는 프록시 레벨에서 연결 종료를 나타냅니다.

환경

- 기술: Cisco SSE(Secure Access)
- 구성 요소: SWG(Secure Web Gateway)
- SWG 프록시 URL: swg-url-proxy-https-8385532.sseproxy.qq.opendns.com을 참조하십시오.
- 영향을 받는 포트: 443 및 80
- 원래 NAT IP: 20.x.x.x
- 업데이트된 NAT IP: 21.x.x.x
- AWS ELB 엔드포인트 예: EU 중부 또는 미국 동부 지역
- 브라우저를 SWG 프록시로 안내하는 WPAD 컨피그레이션

해결

올바른 NAT IP 주소를 포함하도록 허용 목록 컨피그레이션을 업데이트하여 문제를 해결했습니다.

다음 섹션에서 설명하는 단계를 수행하여 문제를 식별하고 해결했습니다.

1단계: 진단 데이터 수집

트래픽 흐름 및 프록시 컨피그레이션을 분석하기 위해 수집된 패킷 캡처 및 WPAD 스크립트 컨피그레이션.

그 외에도 https://policy.test.sse.cisco.com에서 "401 unauthorized" 오류를 보여주고 있다는 주요 단서가 있었습니다. 즉, http 연결 요청이 프록시에 도달하지만 프록시가 정책을 적용하고 트래픽을 허용하기 위해 OrgID 및 기타 메타 데이터 세부 정보에 따라 사용자 트래픽을 인증할 수 없습니다.

2단계: 트래픽 분석

패킷 캡처 분석 결과:

- 프록시에서 TCP RST 패킷을 전송하고 있습니다.

- 활동 검색 로그에 실패한 트래픽이 표시되지 않음
- 트래픽 흐름의 소스 IP가 변경되었습니다.

3단계: NAT IP 주소 식별

조사 결과 NAT 공용 IP 주소가 20.x.x.x에서 21.x.x.x로 변경된 것으로 나타났습니다. 변경된 IP가 사용자 CSA UI에 등록된 네트워크로 추가되고, CSA 포털에 올바른 IP를 등록한 후 SWG 트래픽이 PAC 파일 구축에 대해 작동하기 시작했습니다.

4단계: 허용 목록 구성 업데이트

새 NAT IP 주소 21.x.x.x로부터의 트래픽을 허용하도록 allow-list/firewall 규칙을 업데이트했습니다.

5단계: 확인

새 NAT IP 주소로 허용 목록을 업데이트한 후 일반 보안 액세스 트래픽 흐름이 복원되고 SWG 프록시를 통해 웹 요청이 올바르게 작동하기 시작했습니다.

원인

근본 원인은 사용자 NAT 공용 IP 주소가 20.x.x.x에서 21.x.x.x로 변경된 것입니다. Secure Access SWG 프록시가 원래 IP 주소의 트래픽만 허용하도록 구성되어 새 IP 주소에서 트래픽이 도착하면 연결이 재설정됩니다. 그 외에도, 주요 단서는 https://policy.test.sse.cisco.com에서 "401 unauthorized" 오류를 표시하고 있었는데, 이는 http connect 요청이 프록시에 도달하고 있음을 의미합니다. 이는 PCAP에서도 확인되지만 프록시가 정책을 적용하고 트래픽을 허용하기 위해 OrgID 및 기타 메타 데이터 세부 정보를 기반으로 사용자 트래픽을 인증할 수 없습니다. 이로 인해 프록시에서 TCP RST 패킷과의 연결을 종료하여 웹 요청이 정상적으로 처리되지 않게 되었습니다.

SWG PAC 파일에 대한 웹 트래픽 흐름 문제를 해결하기 위해 사용자 CSA UI의 등록된 네트워크 아래에 새 NATed IP를 추가했습니다.

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.