SAML ID가 보안 웹 게이트웨이 트래픽에 적용되지 않는 문제 해결

목차

소개

이 문서에서는 SAML ID가 Section Web Gateway 트래픽에 적용되지 않는 문제를 해결하는 방법에 대해 설명합니다.

SAML ID가 웹 트래픽에 적용되지 않음

SAML ID가 웹 트래픽에 적용되지 않은 경우 Umbrella 문서를 참조하여 설정이 올바르게 완료되었는지 확인하십시오. 이러한 구성 항목을 완료해야 합니다.

- 'Deployments(구축) > SAML Configuration(SAML 컨피그레이션)'에서 구성 및 테스트된 IdP 설정
- 'Deployments(구축) > Web Users and Groups(웹 사용자 및 그룹)'에서 프로비저닝된 사용자/그룹 목록
- SAML은 'Policies(정책) > Web Policies(웹 정책)'의 관련 policy*에서 활성화되어야 합니다.
- HTTPS 암호 해독은 관련 정책에서 'Policies(정책) > Web Policies(웹 정책)'에서 활성화해야 합니다.

웹 정책에서 SAML 활성화

SAML 및 HTTPS 암호 해독은 관련 네트워크 또는 터널 ID에 적용되는 정책에서 활성화해야 합니다. 이러한 기능은 사용자가 식별되기 전에 적용되므로 중요한 정책은 "연결 방법"에 적용됩니다.

SAML 정책은 다음과 같이 주문해야 합니다.

1. 높은 우선 순위 - 정책이 사용자/그룹에 적용됩니다. 이 정책은 인증된 사용자에 대한 콘텐츠/보안 설정을 결정합니다.
2. LOWER Priority(낮은 우선순위) - 정책이 네트워크/터널에 적용됩니다. 이 정책은 SAML을 활성화하고 초기 인증을 트리거합니다.

SAML ID가 특정 웹 트래픽에 적용되지 않음

IP 서로게이트(기본 동작)

사용자 식별의 일관성을 향상시키려면 새 IP 서로게이트 기능을 활성화하는 것이 좋습니다. 이 기능은 모든 신규 Umbrella SAML 고객에게 자동으로 활성화되지만 기존 Umbrella 고객에게는 수동으로 활성화해야 합니다.

IP 서로게이트에서는 Internal IP(내부 IP) > Username(사용자 이름) 정보 캐시를 사용합니다. 즉, SAML 식별을 모든 유형의 요청에 적용할 수 있습니다. 웹 브라우저 이외의 트래픽, 쿠키를 지원하지 않는 트래픽, SSL 암호 해독 대상이 아닌 트래픽도 포함됩니다.

IP 대리는 사용자 식별의 일관성을 크게 향상시키고 관리 부담을 줄일 수 있다.

IP 서로게이트에는 다음과 같은 요구 사항이 있습니다.

- 내부 IP 가시성은 Umbrella Network Tunnel 또는 Proxy-Chain 구축 및 X-Forwarded-For 헤더를 사용하여 제공해야 합니다. Umbrella의 호스트된 PAC 파일에서는 작동하지 않습니다.
- IP 서로게이트를 공유 IP 주소 시나리오에서 사용할 수 없습니다(터미널 서버, 빠른 사용자 전환).
- 브라우저에서 쿠키를 활성화해야 합니다. 초기 인증 단계에는 쿠키가 계속 필요합니다.

쿠키 서로게이트(IP 서로게이트 사용 안 함)

IP 서로게이트가 비활성화된 경우 사용자 ID는 지원되는 웹 브라우저의 요청에만 적용되며 웹 브라우저는 쿠키를 지원해야 합니다. SWG를 사용하려면 브라우저에서 쿠키의 사용자 세션을 추적하기 위해 모든 요청에 대해 쿠키를 지원해야 합니다. 그러나 이 모드에서는 모든 웹 요청이 사용자와 연결될 필요는 없습니다.

SAML은 이러한 상황에서 적용되지 않으며 네트워크/터널 ID에 할당된 기본 정책이 대신 사용됩니다.

- 비 웹 브라우저 트래픽
- 쿠키가 비활성화된 웹 브라우저 또는 IE 보안 강화 구성
- 쿠키를 지원하지 않는 OCSP/인증서 폐기 검사
- 쿠키를 지원하지 않는 개별 웹 요청입니다. 웹 사이트의 콘텐츠 보안 정책으로 인해 개별 요청에 대해 쿠키가 차단되는 경우도 있습니다. 이 제한은 널리 사용되는 많은 CDN에 적용됩니다.
- 대상 도메인/범주가 SAML에서 SAML Bypass List(SAML 우회 목록)를 사용하여 우회된 경우
- 대상 도메인/범주가 Umbrella Selective Decryption 목록을 사용하는 HTTPS 암호 해독에서 우회된 경우.

이러한 제한으로 인해 관련 네트워크/터널 정책에서 적절한 최소 액세스 수준을 구성하는 것이 중요합니다. 기본 정책은 비즈니스 크리티컬 애플리케이션/도메인/범주 및 CDN을 허용해야 합니다.

또는 IP 서로게이트 시스템을 사용하여 호환성을 개선하십시오.

SAML 바이패스

드문 경우이지만 예외가 필요합니다. 이는 SWG가 SAML 인증을 요청하지만 앱 또는 웹 사이트에서 이를 지원할 수 없는 경우 필요합니다. 다음과 같은 경우에 이러한 현상이 발생합니다.

- 브라우저가 아닌 앱은 웹 브라우저처럼 보이는 사용자 에이전트를 사용합니다
- 스크립트는 쿠키 테스트에서 수행하는 HTTP 리디렉션을 처리할 수 없습니다
- 브라우징 세션에서의 제1 요청은 POST 요청(예를 들어, SAML에 대해 제대로 리디렉션할 수 없는 SSO(Single Sign-On) URL

SAML Bypass List(SAML 우회 목록)는 보안을 유지하면서 도메인을 인증에서 제외하는 가장 좋은 방법입니다(File Inspection).

- SAML Bypass List(SAML 우회 목록) 예외는 연결에 사용되는 네트워크/터널에 영향을 주는 올바른 정책에 적용해야 합니다
- SAML Bypass List(SAML 우회 목록)에서는 트래픽을 자동으로 허용하지 않습니다. 도메인은 관련 정책의 카테고리 또는 대상 목록에 의해 계속 허용되어야 합니다.

SAML Bypass - 고려 사항

인기 사이트 및 "홈 페이지"에 대한 제외 항목을 추가할 때 SAML에 미치는 영향을 고려하는 것이 중요합니다. SAML은 브라우징 세션의 첫 번째 요청이 HTML 페이지에 대한 GET 요청일 때 가장 잘 작동합니다. 예: http://www.myhomepage.tld 이 요청은 SAML 인증을 위해 리디렉션되며 이후 요청에서는 IP 서로게이트 또는 쿠키를 사용하여 동일한 ID를 가정합니다.

SAML에서 홈 페이지를 우회하면 SAML 시스템에서 보이는 첫 번째 요청이 백그라운드 콘텐츠에 대한 것인 문제가 발생할 수 있습니다. 예: http://homepage-content.tld/script.js. 브라우저가 포함된 콘텐츠(예: JS 파일)를 로드하는 경우 SAML에서 SAML 로그인 페이지로 리디렉션할 수 없으므로 이 문제가 발생합니다. 이는 사용자가 로그온을 트리거하기 위해 다른 사이트로 이동할 때까지 페이지가 잘못 렌더링되거나 작동하는 것처럼 보인다는 것을 의미합니다.

인기 있는 사이트와 홈페이지를 고려할 때 다음 사항을 고려하십시오.

- 필요한 경우가 아니면 SAML 또는 HTTPS 암호 해독에서 홈 페이지와 인기 사이트를 제외하지 마십시오
- 홈페이지를 제외하면 해당 사이트에서 사용하는 모든 도메인(배경 콘텐츠 포함)을 제외해야 SAML 비호환성을 방지할 수 있습니다

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.