이제 Umbrella SWG에 대한 SAML Bypass를 사용할 수 있습니다.

목차

소개

이 문서에서는 Umbrella SWG(Secure Web Gateway)에 대한 SAML Bypass의 사용 가능성에 대해 설명합니다.

개요

이제 도메인 또는 IP 주소별로 SAML 사용자 ID 챌린지를 우회할 수 있습니다.

SAML을 사용하여 사용자 ID를 가져오면 특정 유형의 웹 요청과 호환되지 않는 경우가 있습니다. 예를 들어, 비 브라우저 애플리케이션 또는 IoT(Internet of Things) 디바이스 트래픽이 SAML ID 문제에 올바르게 응답하지 못할 수 있습니다. 사용자 ID를 가져올 수 없는 경우 요청이 차단됩니다. SAML 챌린지에 올바르게 응답하지 못한 이유가 비호환성 문제인 것으로 알려진 경우 SAML 바이패스를 추가하여 향후 SAML 챌린지를 방지할 수 있습니다.

대상에 대해 SAML을 우회하면 사용자 ID를 사용자 기반 정책과 일치시킬 수 없습니다. 네트워크 또는 터널과 같은 다른 ID 유형은 정책 결과에 따라 허용되거나 차단된 웹 정책 및 요청을 매칭하는 데 사용됩니다.

이제 'SAML Bypass'라는 새 대상 목록 유형을 사용할 수 있습니다. SAML 설정을 편집하여 대상 목록을 규칙 세트에 추가할 수 있습니다.

SAML 바이패스 구성에 대한 자세한 내용은 Umbrella 설명서를 참조하십시오.

1. SAML Bypass Destination List 추가 - https://docs.umbrella.com/umbrella-user-guide/docs/add-a-saml-bypass-destination-list
2. 웹 정책에 규칙 세트 추가-https://docs.umbrella.com/umbrella-user-guide/docs/add-a-rules-based-policy

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.