ID 제공자가 NTLM을 사용하는 SaaS가 플로우와 NTLM을 시작할 때 인증을 요청하는 사용자

목차

질문

ID 제공자가 포함된 SaaS가 흐름과 NTLM을 시작할 때 사용자에게 인증을 요청하는 이유는 무엇입니까?

환경

- AsyncOS 버전 7.0 이상을 실행하는 Cisco WSA(Web Security Appliance)
- 투명 인증에 사용되는 NTLM
- ID 제공자가 시작한 플로우를 사용하여 구성된 SaaS 액세스 제어
- SaaS SSO 구성

외부 애플리케이션으로 SaaS Access Control을 구성했으며, ID 제공자가 시작한 흐름과 SAML을 사용하여 단일 로그인을 지원합니다.또한 NTLM을 사용하여 사용자를 투명하게 인증합니다.그러나 이 프롬프트가 표시되지 않도록 하려면 어떻게 해야 합니까?

증상

- 사용자가 SaaS SSO URL에 대한 북마크를 클릭하면 인증 프롬프트가 표시되는 경우가 있습니다.
- 사용자가 다른 외부 웹 사이트에 액세스한 다음 SaaS SSO URL 북마크를 클릭하면 액세스가 제대로 작동합니다.

이 문제는 WSA에서 클라이언트에서 처음 확인하는 요청이 WSA에서 직접 제공하는 특수 SSO URL에 도달하는 경우/이기 때문에 발생합니다.

EUN 페이지 또는 PAC 파일과 같이 WSA에서 직접 제공되는 콘텐츠는 일반적으로 인증에서 제외됩니다.SaaS 기능은 프록시에서 유지 관리하는 인증 서로게이트에 액세스할 수 있지만, 양식 기반 인증(NTLM 또는 LDAP) 이외의 방법을 사용하여 자체에서 인증을 요청할 수는 없습니다. 따라서 관찰된 동작은 설계에 따라 수행되지만 최적의 솔루션은 아닙니다.

결함 CSCzv55859는 이 문제를 추적하고 이 문제를 해결하는 더 나은 메커니즘을 제공하기 위해 제출되었습니다.

두 가지 해결 방법이 있습니다.

해결 방법 1

1. 첫 번째는 SaaS 컨피그레이션에서 서비스 제공자가 시작한 플로우를 사용하는 것입니다 .SP에서 시작된 흐름에서 사용자는 대상 SaaS 애플리케이션을 탐색하는 것으로 시작하여 SSO URL을 통해 리디렉션을 실행합니다.
   이 초기 트래픽은 프록시를 통과하므로 사용자는 NTLM을 사용하여 올바르게 인증됩니다.이 해결 방법은 대상 애플리케이션이 SP 시작 플로우를 지원하는 경우에만 작동합니다.
2. WSA 정책에서 새 SSO URL을 생성하여 강제로 인증한 다음 클라이언트를 "실제" SSO URL로 리디렉션합니다.

해결 방법 2

1. 새 SSO URL을 결정합니다.이 URL은 프록시에서 실제로 액세스하지 않습니다.로그인 프로세스를 시작할 수 있습니다.

   예를 들어, 현재 SSO URL이 "**wsa.mycompany.com/SSOURL/WebEx**"이면 "wsa.example.com/SSOURL/WebEx"을 사용할 수 있습니다.중요한 고려 사항은 사용 중인 호스트 이름 부분이 WSA를 통해 프록시되는지 확인하는 것입니다.

   WSA가 명시적 프록시로 구축되면 호스트 이름은 무엇이든 될 수 있습니다.WSA가 투명 프록시로 구축된 경우 호스트 이름은 외부 IP 주소로 확인되는 실제 호스트 이름이어야 합니다.

2. 새 URL과 일치하는 맞춤형 URL 카테고리(**GUI > Web Security Manager > Custom URL categories**)를 생성합니다.해결 방법을 적용해야 하는 각 SaaS 애플리케이션에 대해 하나의 맞춤형 URL 카테고리를 생성해야 합니다.
   정규식 일치를 사용하여 전체 URL에 일치시킵니다.

3. 액세스 정책(**GUI > Web Security Manager > Access Policies**)으로 이동하고 사용자의 요청이 일치할 액세스 정책에 대한 URL 필터링 열 아래로 이동합니다. 이는 전역 정책 또는 테이블의 다른 정책일 수 있습니다.
   이 액세스 정책에 새 사용자 지정 URL 카테고리를 포함하고 해당 작업을 리디렉션하도록 **설정합니다**.리디렉션의 대상은 "실제" SSO URL이어야 합니다.

4. 변경 사항을 제출하고 커밋하여 새 컨피그레이션을 적용합니다.

이제 사용자는 새 SSO URL을 사용하여 애플리케이션에 액세스해야 합니다.이 URL에 대한 액세스는 프록시에서 처리되므로 NTLM 인증이 호출되고 사용자는 항상 투명하게 로그인되어 인증 프롬프트를 방지합니다.