VPNaaS SAML 인증 실패(" 릴레이 상태 암호 해독 실패") Duo IdP 사용 오류

목차

문제

SAML 인증 및 Duo를 IdP(Identity Provider)로 사용하는 보안 클라이언트 원격 액세스를 사용하여 VPNaaS 연결을 설정하려고 하면 다음 오류가 발생합니다.

- SSO 인증 요청을 처리하지 못했습니다. 시스템 관리자에게 문의하십시오
- relaystate의 암호 해독에 실패했습니다.

ZTNA(Zero Trust Network Access)에서는 동일한 IdP 및 Duo 구성을 사용한 인증이 성공하지만 VPN 연결에서는 실패합니다. ZTNA 및 VPN용 Duo에 동일한 IdP를 사용하는 두 개의 개별 응용 프로그램이 구성되어 있습니다.

환경

- 기술: 솔루션 지원(SSPT - 계약 필요)
- 하위 기술: 보안 액세스 - 보안 클라이언트 원격 액세스(VPN, 보안 상태, 개인 리소스)
- 인증 방법: 듀오 IdP가 포함된 SAML
- 2개의 Duo 애플리케이션 구성: ZTNA용 1개, VPN용 1개
- ZTNA에 대한 인증 작동, VPN에 대한 실패
- 소프트웨어 버전: 모두
- 최근 하드웨어/소프트웨어 버전 변경 사항이 지정되지 않았습니다.

해결

VPN용 Duo 응용 프로그램에서 엔터티 ID 및 ACS(Assertion Consumer Service) URL의 구성을 수정하여 문제가 해결되었습니다. 올바른 메타데이터는 Secure Access에서 다운로드되고 VPN Duo 앱에 업로드되었으며, SAML 릴레이 상태 암호 해독 오류가 해결되었습니다.

1. CSA 대시보드에 로그인합니다. 접속 > Enduser 접속 -> Virtual Private Networks로 이동합니다. 접속하는 프로파일을 확인합니다.
2. 해당 프로필 및 편집을 클릭합니다. 인증 탭으로 이동합니다.
3. 보안 액세스를 위한 SAML 메타데이터를 다운로드합니다.
4. Check entityID="https://X.vpn.sse.cisco.com/saml/sp/metadata/saml" and <AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://X.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=Profilename"></AssertionCo
니다.

5. entityID 및 AssertionConsumerService가 VPN SSO 인증을 위해 구성된 Duo 애플리케이션과 일치하는지 확인합니다.

원인

Duo VPN 애플리케이션에서 엔터티 ID 및 ACS URL을 잘못 구성하면 SAML relaystate 암호 해독이 실패했습니다. ZTNA 인증이 동일한 IdP로 작동하지만 VPN용 Duo에 올바른 컨피그레이션이 없습니다. Secure Access에서 정확한 메타데이터를 사용하여 Duo VPN 애플리케이션을 업데이트하면 문제가 해결되었습니다.

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.