VPNaaS SAML-Authentifizierung schlägt fehl"Entschlüsselung des Relay-Zustands fehlgeschlagen" Fehler bei Verwendung von Duo IDp

Inhalt

Problem

Bei dem Versuch, eine VPNaaS-Verbindung mithilfe von Secure Client Remote Access mit SAML-Authentifizierung und Duo als Identity Provider (IdP) herzustellen, wird dieser Fehler beobachtet:

- Fehler beim Verarbeiten der SSO-Authentifizierungsanforderung. Wenden Sie sich an Ihren Systemadministrator.
- Entschlüsselung von RelayState fehlgeschlagen

Die Authentifizierung mit derselben IdP- und Duo-Konfiguration funktioniert für ZTNA (Zero Trust Network Access) erfolgreich, schlägt jedoch bei VPN-Verbindungen fehl. Duo für ZTNA und VPN verfügt über zwei separate Anwendungen, die beide dieselbe IdP verwenden.

Umwelt

- Technologie: Solution Support (SSPT - Vertrag erforderlich)
- Subtechnologie: Sicherer Zugriff - Sicherer Client-Remote-Zugriff (VPN, Status, private Ressource)
- Authentifizierungsmethode: SAML mit Duo IdP
- Konfiguration von zwei Duo Anwendungen: einer für ZTNA, einer für VPN
- Authentifizierung funktioniert für ZTNA, VPN ist fehlgeschlagen
- Software-Version: ALLE
- Keine Änderungen der letzten Hardware-/Softwareversion angegeben

Auflösung

Das Problem wurde durch Korrigieren der Konfiguration der Objektkennung und der ACS-URL (Assertion Consumer Service) in der Duo-Anwendung für VPN behoben. Die richtigen Metadaten wurden von Secure Access heruntergeladen und in die VPN Duo-Anwendung hochgeladen, wodurch der SAML-Entschlüsselungsfehler behoben wurde.

1. Melden Sie sich beim CSA Dashboard an. Gehen Sie zu Verbinden > Endbenutzerverbindungen -> Virtuelle private Netzwerke. Finden Sie heraus, mit welchem

Profil Sie verbunden sind.
2. Klicken Sie auf dieses Profil und Bearbeiten. Wechseln Sie zur Registerkarte Authentifizierung.
3. SAML-Metadaten für sicheren Zugriff herunterladen
4. Überprüfen Sie entityID="https://X.vpn.sse.cisco.com/saml/sp/metadata/saml" und <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
5. Stellen Sie sicher, dass entityID und AssertionConsumerService mit der für die VPN SSO-Authentifizierung konfigurierten Duo-Anwendung übereinstimmen.

Ursache

Eine Fehlkonfiguration der Objektkennung und der ACS-URL in der Duo VPN-Anwendung führte zum SAML-Entschlüsselungsfehler. Die richtige Konfiguration war in Duo für VPN nicht vorhanden, obwohl die ZTNA-Authentifizierung mit derselben IDp funktionierte. Das Problem konnte durch die Aktualisierung der Duo VPN-Anwendung mit genauen Metadaten von Secure Access behoben werden.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.