Cisco Secure Access - Verlängerung von SAML-Zertifikaten mit IDP (Microsoft Entra-ID)

Inhalt

Problem

Wenn die SSO-Authentifizierung mit Microsoft Entra ID SAML als Identity Provider (IdP) für Cisco Secure Access verwendet wird, laufen die SAML-Verifizierungszertifikate bald ab.

Unternehmen müssen den korrekten Zertifikatverlängerungsprozess kennen, um Authentifizierungsunterbrechungen zu vermeiden und zu bestimmen, ob bei der Verlängerung von Entra ID SAML-Zertifikaten in Secure Access eine neue Konfiguration für die einmalige Anmeldung erstellt werden muss.

Umwelt

- Cisco Secure Access mit konfigurierter SSO-Authentifizierung
- Microsoft Entra ID SAML als Identitätsanbieter
- SAML-Verifizierungszertifikate mit bevorstehenden Ablaufdaten
- Bestehende SSO-Konfiguration für SWG (Secure Web Gateway) und ZTNA (Zero Trust Network Access)

Auflösung

Schritt 1 - Erkennen der Zertifikatverlängerung

- Identity Provider (IdP) erneuert oder dreht sein SAML-Signaturzertifikat.
- Dies geschieht in der Regel, wenn das Zertifikat bald abläuft.

Schritt 2 - Abrufen aktualisierter IDp-Metadaten

- Exportieren Sie die neue IdP-Metadaten-XML oder das neue Signaturzertifikat aus der IdP.

Schritt 3: Überprüfen der Zertifikatänderung

Bestätigen Sie, dass das Zertifikat tatsächlich geändert wurde.

Überprüfen:

- Daumenabdruck
- Ablaufdatum
- Emittent

So wird sichergestellt, dass der SP mit dem richtigen Zertifikat aktualisiert wird

Konfiguration des Dienstanbieters aktualisieren

Melden Sie sich beim Cisco Secure Access Dashboard an, und aktualisieren Sie die Konfiguration.

Navigieren Sie zu Verbinden - Benutzer und Gruppen.

Klicken Sie auf Konfigurationsmanagement

Laden Sie unter SSO Authentication - Edit the SSO Authentication Profile (SSO-Authentifizierungsprofil bearbeiten) die Metadatendatei mit dem neuen Zertifikat hoch, oder laden Sie das Zertifikat bei manueller Konfiguration hoch.

Schritt 5 - Speichern und Anwenden der Konfiguration

- Die aktualisierte Konfiguration speichern

Schritt 6 - Validierung der SSO-Authentifizierung

Führen Sie einen SSO-Anmeldetest durch.

Ursache

Das Identitätsanbieter-Signaturzertifikat (IdP) wird vom Dienstanbieter verwendet, um die Signatur der SAML-Assertion zu überprüfen. Wenn das Zertifikat erneuert wird, muss der SP sein vertrauenswürdiges Zertifikat aktualisieren, damit die Authentifizierungsanforderungen weiterhin validiert werden.

Verwandte Inhalte

- Cisco Secure Access - SAML Single Sign-On - Überblick und Konfiguration
- Konfigurieren von SAML SSO für Cisco Secure Access (Beispiel für Microsoft Entra ID)
- 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.