Problemen oplossen met op een browser gebaseerde SAML-verificatie met een leeg wit scherm met EntraID

Inhoud

uitgifte

Wanneer u Cisco Secure Access configureert om browsergebaseerde SAML-verificatie te forceren op apparaten zonder dat Cisco Secure Client is geïnstalleerd, wordt het verificatieproces omgeleid naar een leeg wit scherm in plaats van de EntraID-verificatiepagina weer te geven. Dit probleem doet zich specifiek voor in de normale (niet-InPrivate) modus van Microsoft Edge en in Google Chrome-browsers. De verificatie werkt correct wanneer u de modus Edge InPrivate gebruikt. Het SAML-verificatieprofiel heeft zowel Decryptie als SSO-verificatie ingeschakeld.

De geconfigureerde beleidsstructuur omvat:

- Sta beleid toe voor gebruikers na verificatie. (bron: elke gebruiker, bestemming: elke)
- SAML-verificatiebeleid toestaan met SAML-verificatieprofiel. (bron: eindpunt IP, bestemming: 0.0.0.0 TCP 80,443)
- SAML-verificatiehulpbeleid toestaan met SAML-verificatieprofiel. (bron: IP-eindpunt, bestemming: alle)
- Blokkeer het beleid. (bron: IP-eindpunt, bestemming: alle)

milieu

- Cisco Secure Access (module voor internettoegang)
- EntraID als Identity Provider (IdP)
- Browsergebaseerde SAML-verificatie voor apparaten zonder Cisco Secure Client

- SAML-verificatieprofiel met decodering en SSO-verificatie ingeschakeld
- Microsoft Edge en Google Chrome browsers

resolutie

Het probleem wordt opgelost door specifieke EntraID-gerelateerde domeinen toe te voegen aan de uitsluitingslijst voor decodering in de SAML-verificatieprofielconfiguratie. Dit voorkomt dat het SSL/TLS-decoderingsproces de EntraID-verificatiestroom verstoort.

Stap 1: EntraID-domeinen toevoegen aan de lijst met uitsluitingen voor decodering

Configureer deze vier EntraID-domeinen in de lijst met uitsluitingen voor decodering voor het SAML-verificatieprofiel:

```
login.live.com
login.microsoftonline.com
msauth.net
msftauth.net
```

Stap 2: Configuratie toepassen op SAML-beleid

Zorg ervoor dat de decoderingsuitsluitingsinstellingen op beide worden toegepast:

- Het verificatiebeleid voor SAML toestaan. (bron: eindpunt IP, bestemming: 0.0.0.0 TCP 80,443)
- Het Help-beleid voor SAML-verificatie toestaan. (bron: IP-eindpunt, bestemming: alle)

Stap 3: Resolutie controleren

Test de verificatiestroom nadat u de decoderingsuitsluitingsconfiguratie hebt toegepast:

- Microsoft Edge (normale modus): kan met succes worden omgeleid naar de EntraID-verificatiepagina.
- Google Chrome: kan met succes omleiden naar de EntraID-verificatiepagina.
- Beide browsers kunnen het invoerscherm voor EntraID-verificatie consistent weergeven.

Oorzaak

Het blanco witte scherm treedt op omdat het SSL/TLS-decoderingsproces in Cisco Secure Access de EntraID-verificatiestroom verstoort wanneer decodering is ingeschakeld voor het SAML-verificatieprofiel. Het decoderingsproces breekt de beveiligde communicatie tussen de browser en EntraID-verificatieservers, waardoor de verificatiepagina niet correct kan worden geladen. InPrivate-modus werkt omdat het SSL / TLS-sessies anders behandelt, waarbij de decoderingsinterferentie wordt omzeild. Door de EntraID-domeinen toe te voegen aan de lijst met uitsluitingen voor decodering kan het verificatieverkeer zonder decodering worden doorgegeven, waardoor de integriteit van de beveiligde verificatiestroom behouden blijft.

Gerelateerde inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.