Problemen oplossen met SWG SAML-verificatiecookie-surrogaatprobleem voor beveiligde toegang

Inhoud

uitgifte

Gebruikers die webtoepassingen benaderen via Cisco Secure Access, ervaren verificatiefouten wanneer toepassingen omleidingen over meerdere domeinen uitvoeren of bronnen ophalen uit meerdere gerelateerde domeinen. De kwestie manifesteert zich als:

- Webtoepassingen die niet correct worden geïnitialiseerd na SAML-verificatie.
- Verzoeken om cross-domain resources (CORS-fout) te blokkeren worden standaard geblokkeerd.
- Activiteitenlogboeken met aanvragen die zijn toegewezen aan netwerk- of tunnelidentiteit in plaats van geverifieerde gebruikersidentiteit.
- CORS-beleidsfouten die worden weergegeven in de browserconsole voor omgeleide verzoeken.
- Toepassingen die correct werken op fysieke machines bij gebruik van IP-surrogaat, maar die falen op virtuele desktopomgevingen van Citrix met behulp van Cookie-surrogaat.

Het probleem treedt specifiek op wanneer cookie surrogaat authenticatie wordt gebruikt in gevirtualiseerde omgevingen, waar omgeleide verzoeken verliezen de gebruiker-naar-cookie mapping tijdens cross-domein resource ophalen.

milieu

- Cisco Secure Access met SAML-verificatie geconfigureerd
- Cookie Surrogate-verificatie ingeschakeld voor virtuele desktopomgevingen van Citrix

- IP-surrogaatverificatie voor fysieke machines
- Webtoepassingen die omleidingen voor meerdere domeinen uitvoeren (CORS-fout in logboeken van hulpprogramma's voor webontwikkelaars)
- Gemengde omgeving met zowel fysieke als virtuele desktopinfrastructuur

resolutie

Het probleem wordt opgelost door IP Surrogate-bypass voor de getroffen netwerkbereiken te implementeren, waardoor een juiste gebruikersidentiteitstoewijzing mogelijk is, zelfs tijdens omleidingen over meerdere domeinen.

Stap 1: Navigeer naar IP-surrogaatconfiguratie

Ga naar het Cisco Secure Access-dashboard en navigeer naar Verbinden > Gebruikers en groepen > Configuratiebeheer > Geavanceerde instellingen > IP-surrogaat.

Stap 2: Interne netwerkbypass inschakelen

Voeg de betreffende netwerkbereiken toe aan de bypass-configuratie van het interne netwerk. Hierdoor kan het systeem de gebruikersidentiteitsattributie behouden voor verzoeken die afkomstig zijn van deze netwerken.

Stap 3: Toepassingstoegang testen

Test na het implementeren van het IP-surrogaat de betreffende toepassingen om te controleren of:

- Verzoeken om bronnen over meerdere domeinen worden correct toegeschreven aan de gebruikersidentiteit
- Toepassingen zonder CORS-fouten succesvol initialiseren

- Activiteitenlogboeken tonen gebruikersidentiteit in plaats van netwerk- of tunnelgebaseerde identiteit voor alle verzoeken

Stap 5: Activiteitenrapporten bewaken

Gebruik Monitor > Zoeken naar activiteiten om te controleren of aanvragen nu correct worden toegewezen aan geverifieerde gebruikers in plaats van te worden weergegeven als netwerk- of tunnelgebaseerde identiteit.

Oorzaak

Dit gedrag wordt verwacht vanwege de aard van SAML-verificatie in combinatie met Cookie Surrogate in gevirtualiseerde omgevingen. Wanneer webapplicaties cross-domain redirects uitvoeren of bronnen ophalen uit meerdere gerelateerde domeinen, dragen de omgeleide verzoeken mogelijk niet de surrogaat-cookie op een manier die Cisco Secure Access kan koppelen aan de geverifieerde gebruikerssessie.

De oorzaak is omdat:

- Cookie Surrogate vertrouwt op browser cookie propagatie over redirects.
- Cross-domain security policies (CORS) kunnen cookies verwijderen tijdens 307/redirect scenario's.
- Browserbeveiligingsmaatregelen voorkomen het delen van cookies in verschillende domeinen.
- Virtuele desktopomgevingen gaan anders om met het propageren van cookies dan met fysieke machines.

Zodra de gebruiker-naar-cookie-toewijzing verloren is gegaan, kan Secure Access het verzoek niet aan de geverifieerde gebruiker oplossen, waardoor het verzoek alleen wordt toegeschreven aan het geregistreerde netwerk / andere identiteit als bron en vervolgens wordt geblokkeerd door standaard weigeringsregels.

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.