Cisco Secure Access SSO-verificatie met Duo IdP voor roaming-client SWG-verkeer

Inhoud

uitgeven

Wanneer wordt geprobeerd om SSO-verificatie te gebruiken met een Duo IdP voor Secure Access SWG-verkeer (Secure Web Gateway) dat afkomstig is van een roamende client, wordt gebruikers niet gevraagd om Duo SSO-verificatie en wordt de gebruikersidentiteit niet ingevuld in het dashboard voor Secure Access. Hoewel het webverkeer overeenkomt met de beoogde SWG-regel met verificatie ingeschakeld en het verkeer wordt gedecodeerd, wordt de verificatiestroom niet gestart voor roamingclientverkeer, waardoor identificatie van webactiviteiten op gebruikersniveau wordt voorkomen.

In het bijzonder werd het volgende gedrag waargenomen:

- SWG-logboekregistratie en -activiteit toonden aan dat het verkeer overeenkwam met de beoogde SWG-regel en dat het bestemmingsverkeer werd gedecodeerd
- Logboeken en de weergave van de activiteit Secure Access toonden alleen de identiteit van de pc en de netwerkidentiteit; er werd geen Duo/SAML-verificatie-uitdaging, SSO-redirect of interactieve prompt waargenomen
- Beleidsvermeldingen toonden alleen roaming- en herkomstinformatie; er was geen gebruikersidentiteit aanwezig voordat de advertentie werd toegevoegd
- Toen de test-VM tijdens het oplossen van problemen werd gekoppeld aan Active Directory, werd de gebruikersidentiteit zichtbaar in Secure Access Activity Search, maar de interactieve vraag Duo/SAML kwam nog steeds niet voor

milieu

- Cisco Secure Access met SWG-functionaliteit
- Secure Client versie 5.1.13.177
- Duo IdP geconfigureerd voor SSO-verificatie
- Organisatie-abonnement: Secure Access Essentials

- Webproxy-interval opnieuw verifiëren, ingesteld op Dagelijks
- Geen PAC-bestand of VPN in gebruik tijdens tests
- Testomgeving met roamingcomputerconfiguratie

resolutie

Na uitgebreide analyse en testen werd vastgesteld dat SSO-verificatie met behulp van SAML niet wordt ondersteund voor Secure Access-roamingclientverkeer vanwege beperkingen in het productontwerp. De volgende stappen voor probleemoplossing werden uitgevoerd om deze beperking te bevestigen:

Stap 1: Live probleemoplossing en gedragsreproductie

De test bevestigde dat SWG-beleidsmatching en SSL-decodering correct zijn uitgevoerd, maar dat de verificatiestroom (interactieve SAML/Duo SSO-redirect en uitdaging) niet is gestart voor roamingclientverkeer.

Stap 2: Regel- en bronwijzigingen

De bron van de SWG-regel is tijdens repro-pogingen gewijzigd van de naam van de roamende computer in een specifieke gebruikersidentiteit. Beveiligde clientservices werden opnieuw gestart en beleidspropagatie werd waargenomen. Deze wijzigingen hebben het probleem met de verificatiestroom niet opgelost.

Stap 3: Active Directory Join Testing

De test-VM is gekoppeld aan Active Directory om het effect op de zichtbaarheid van de gebruikersidentiteit te bepalen. Hoewel de gebruikersidentiteit hierdoor zichtbaar werd in Secure Access Activity Search, kwam de interactieve vraag Duo/SAML nog steeds niet voor, wat bevestigt dat het probleem niet alleen te maken had met de zichtbaarheid van de gebruikersidentiteit.

Stap 4: DART-bundelanalyse

Een DART bundel werd verzameld en geanalyseerd. De analyse bevestigde de SWG-beleidstoepassing, maar toonde geen initiatie van de verificatiestroom voor roamingclientverkeer aan, wat de conclusie ondersteunt dat dit gedrag door het ontwerp wordt bepaald.

Stap 5: validatie van de Duo IDp-configuratie

De Duo IdP-metagegevens en -configuratie zijn onafhankelijk getest en met succes voltooid, waarbij werd bevestigd dat de Duo-configuratie zelf niet de bron van het probleem was.

Stap 6: Interne validatie

SSO-verificatie met behulp van SAML wordt niet ondersteund voor Secure Access-clientverkeer voor roaming als beperking van het productontwerp.

Conclusie: er is geen verkeerde configuratie gevonden in de setup. Het gebrek aan interactieve SSO-prompting werd toegeschreven aan een expliciete beperking van de productondersteuning in plaats van een probleem met de te verhelpen configuratie.

Oorzaak

Het probleem wordt veroorzaakt door een beperking in het productontwerp waarbij SSO-verificatie met SAML (inclusief Duo IdP-integratie) niet wordt ondersteund voor Secure Access-roamingclientverkeer. Dit is een inherente beperking van de huidige architectuur van het Secure Access-platform en is niet gerelateerd aan configuratieproblemen of softwarebugs.

Verwante 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.