

ChromeOS SWG Web Protection werkt niet en er worden achtereenvolgens geen weblogs weergegeven in het zoeken naar activiteiten

Inhoud

uitgifte

Weblogs werden niet gegenereerd voor ChromeOS-gebruikers ondanks Secure Web Gateway (SWG)-bescherming die voor de organisatie leek te zijn ingeschakeld. De getroffen ChromeOS-eindpunten toonden alleen DNS-beveiliging zonder SWG/weblogactiviteit die zichtbaar was in de Activity Search-interface. Gebruikers hadden een volledig gebrek aan webverkeerslogs terwijl de SWG-beveiligingsstatus aangaf dat deze was ingeschakeld.

Tijdens het onderzoek, diagnostische logs bleek herhaalde sync mislukkingen aan het eindpunt <http://407.checkumbrella.com> met HTTP 407 (proxy authenticatie vereist) foutreacties. De ChromeOS-client/extensie kon niet correct worden geverifieerd met de proxyservice, waardoor de juiste SWG-beveiligingsactivering en de daaropvolgende generatie van weblogs werd voorkomen.

milieu

- Cisco Secure Access
- ChromeOS-eindpunten met Cisco Secure Access-client/extensie
- Google Admin console voor ChromeOS-beheer

resolutie

Het probleem is opgelost door het basisverificatieschema voor de Google Admin Organizational Unit (OU) met de getroffen ChromeOS-gebruikers in te schakelen en een beleidsherlaad uit te

voeren om SWG-beveiliging te activeren.

Stap 1: Logverzameling en analyse

Verzamelde HAR-vastlegging (bekijk netwerk- en consolelogs) om de hoofdoorzaak van de synchronisatiefout te identificeren. De logs vertoonden herhaalde verificatiefouten bij pogingen om te synchroniseren met de Cisco Secure Access-service.

Stap 2: Basisautorisatie inschakelen voor Google Admin OU

Navigeer in de Google Admin-console naar de organisatorische eenheid met de getroffen ChromeOS-gebruikers en schakel het basisverificatieschema voor autorisatie in. Hierdoor kan de ChromeOS-client/extensie correct worden geverifieerd met de Cisco Secure Access-proxyservice.

Stap 3: Beleid herladen en verificatie

Nadat u Basic Auth hebt ingeschakeld, voert u een beleidsherlaad uit op de getroffen ChromeOS-apparaten. Controleer of SWG-beveiliging actief wordt door de beveiligingsstatus te controleren. De SWG-beveiliging moet nu als actief worden weergegeven in plaats van alleen als DNS-beveiliging.

Stap 4: Validatie

Test webbrowse-activiteit van de getroffen ChromeOS-gebruikers en bevestig dat weblogs nu worden gegenereerd en zichtbaar zijn in de Activity Search-interface. De logs moeten een goede webverkeersinspectie en logboekregistratie via de SWG-service tonen.

Oorzaak

Bij de ChromeOS-client/extensie is het verificatieschema Basic Auth uitgeschakeld voor de

Google Admin Organizational Unit met de betrokken gebruikers. Zonder Basic Auth ingeschakeld, konden de ChromeOS-apparaten niet goed verifiëren met de Cisco Secure Access-proxy-service, wat resulteerde in HTTP 407 (proxy-verificatie vereist) fouten tijdens synchronisatiepogingen. Hierdoor kon de SWG-beveiliging niet goed worden geactiveerd, waardoor de apparaten terugvielen naar DNS-only-beveiliging en het genereren van weblogs werd voorkomen.

Gerelateerde inhoud

- [Problemen oplossen en basisinformatie verzamelen voor Cisco Secure Access](#)
- [Cisco Secure Access Chromebook-client](#)
- [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.