Per-User Identification and Policy Enforcement Challenges in Secure Web Gateway (SWG) voor gedeelde computeromgevingen met SAML-verificatie en PAC-gebaseerde doorsturen van verkeer

Inhoud

uitgeven

In Cisco Secure Web Gateway (SWG)-implementaties met Secure Access met SAML-verificatie en PAC-gebaseerde of Branch to Internet-doorverwijzing, wordt alleen de eerste gebruiker die is aangemeld bij een gedeelde computer correct geïdentificeerd voor webverkeer en beleidshandhaving. Bij het wisselen van gebruiker wordt het volgende webverkeer nog steeds aan de eerste gebruiker toegewezen, zelfs wanneer de optie IP-surrogaat is uitgeschakeld en een PAC-bestand wordt gebruikt. DNS-query's geven de juiste actieve gebruiker weer via Umbrella Virtual Appliance, maar web- en firewalllogboeken wijzen voortdurend activiteiten toe aan de vorige gebruiker. Het verzoek is om te bepalen of SWG de identificatie per gebruiker en de handhaving van het beleid in gedeelde computeromgevingen ondersteunt en hoe de juiste toewijzing van gebruikers kan worden gewaarborgd.

milieu

- Virtueel apparaat voor DNS-resolutie.
- SAML-verificatie voor gebruikersidentiteit.
- Mix van traffic forwarding met PAC en zonder PAC-bestanden.
- IP-surrogaatoptie ingeschakeld, waarbij specifieke subnetten en hosts worden overgeslagen voor het surrogaatcookie.
- On-Prem-apparaten; geen externe eindpunten of gebruikers.

resolutie

Het probleem is opgelost door middel van gebruikerseducatie en configuratiebegeleiding met deze punten in gedachten:

- Gebruik Cookie Surrogate identificatie met PAC bestanden. Het verkeer kan in of uit een netwerktunnel lopen.
- Gebruik Cookie Surrogate-identificatie zonder PAC-bestanden, maar het verkeer moet door

een netwerktunnel lopen.
- Het toegangsbeleid dat u wilt afdwingen, moet SAML-verificatie hebben ingeschakeld in het beveiligingsprofiel.
- Het surrogaatverkeer van cookies is alleen voor browsergebaseerd verkeer. Er is een aparte regel nodig om niet-cookieverkeer van de machine (bijvoorbeeld Teams- of Webex-verkeer) te identificeren met de bronidentiteit als het netwerk.
- De SWG-module mag niet in gebruik zijn om het surrogaatcookie te laten werken.
- Wanneer ook IP-surrogaat is ingeschakeld, moet u de privé-IP-adressen/subnetten toevoegen die van plan zijn om het cookie-surrogaat te gebruiken in de bypasslijst (Gebruikers en groepen - Configuratiebeheer - Geavanceerde instellingen).
- De bypasslijst voor cookie surrogaat komt ook overeen met kortere voorvoegsels. Als u bijvoorbeeld 10.10.10.0/24 toevoegt aan de bypasslijst en u hebt ook een gedefinieerd netwerk als 10.10.10.5/32, moet u ook het kortste voorvoegsel selecteren.
- De surrogaatcookie ondersteunt de gebruiker die van een machine overschakelt zonder dat hij hoeft uit te loggen om meerdere identiteiten te behouden.

Veel van het oplossen van problemen is het testen van beleid en het zoeken naar activiteiten.

Oorzaak

De hoofdoorzaak van onjuiste gebruikersidentificatie in gedeelde computeromgevingen is voornamelijk te wijten aan gebruikerseducatie.

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.