Problemen oplossen met SAML-identiteit die niet wordt toegepast voor veilig webgatewayverkeer

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen kunt oplossen met SAML-identiteiten die niet worden toegepast op Secure Web Gateway Traffic.

SAML-identiteit niet toegepast voor ENIG webverkeer

Als de SAML-identiteit niet wordt toegepast voor ENIG webverkeer, raadpleegt u de overkoepelende documentatie om ervoor te zorgen dat de installatie correct is voltooid. Deze configuratie-items moeten worden voltooid.

- IdP-instellingen geconfigureerd en getest in 'Implementaties > SAML-configuratie'
- Lijst van gebruikers/groepen die zijn voorzien in 'Implementaties > Webgebruikers en -groepen'
- SAML moet zijn ingeschakeld in het betreffende beleid* in 'Beleid > Webbeleid'.
- HTTPS-decodering moet zijn ingeschakeld in het relevante beleid in 'Beleid > Webbeleid'

SAML inschakelen in webbeleid

SAML- en HTTPS-decodering moeten zijn ingeschakeld in het beleid dat van toepassing is op de relevante netwerk- of tunnelidentiteit. Deze functies zijn van toepassing voordat een gebruiker is geïdentificeerd, dus het belangrijkste beleid is het beleid dat wordt toegepast op de "verbindingsmethode".

Het SAML-beleid moet als volgt worden besteld:

1. HOGERE PRIORITEIT - Het beleid is van toepassing op gebruikers/groepen. Dit beleid bepaalt de inhoud/beveiligingsinstellingen voor de geverifieerde gebruikers.
2. LAGERE PRIORITEIT - Het beleid is van toepassing op het netwerk/de tunnel. Met dit beleid

is SAML ingeschakeld en wordt de eerste verificatie geactiveerd.

SAML-identiteit niet toegepast voor specifiek webverkeer

IP-surrogaten (standaardgedrag)

Om de consistentie van gebruikersidentificatie te verbeteren, raden we aan de nieuwe IP-surrogaten-functie in te schakelen. Deze functie wordt automatisch ingeschakeld voor alle nieuwe Umbrella SAML-klanten, maar moet handmatig worden ingeschakeld voor bestaande Umbrella-klanten.

IP surrogates maakt gebruik van een cache van Interne IP > Gebruikersnaam informatie, wat betekent dat SAML identificatie kan worden toegepast op alle soorten verzoeken: zelfs niet-web browser verkeer, verkeer dat geen cookies ondersteunt, en verkeer dat niet onderworpen is aan SSL Decryptie.

IP-surrogaten kunnen de consistentie van gebruikersidentificatie aanzienlijk verbeteren en de administratieve lasten verminderen.

Houd er rekening mee dat IP-surrogaten deze vereisten heeft:

- Interne IP-zichtbaarheid moet worden geboden door gebruik te maken van een Umbrella Network Tunnel- of Proxy-Chain-implementatie en X-Forwarding-For-headers. Dit werkt niet met het gehoste PAC-bestand van Umbrella
- IP-surrogaten kunnen niet worden gebruikt in scenario's voor gedeelde IP-adressen (terminalservers, snelle gebruikerswisseling)
- Cookies moeten worden ingeschakeld in de browser. Cookies zijn nog steeds vereist voor de eerste authenticatiestap.

Cookie-surrogaten (IP-surrogaten uitgeschakeld)

Als IP-surrogaten zijn uitgeschakeld, wordt de gebruikersidentiteit alleen toegepast op verzoeken van ondersteunde webbrowsers en moet de webbrowser cookies ondersteunen. SWG vereist dat de browser cookies ondersteunt voor elk verzoek om de sessie van de gebruikers in een cookie te volgen. Helaas betekent dit dat het niet wordt verwacht dat elk webverzoek in deze modus aan een gebruiker wordt gekoppeld.

In deze omstandigheden wordt SAML niet toegepast en wordt in plaats daarvan het standaardbeleid gebruikt dat aan de identiteit van het netwerk/de tunnel is toegewezen:

- Niet-webbrowserverkeer
- Webbrowsers met uitgeschakelde cookies of verbeterde beveiligingsconfiguratie van IE
- OCSP/Certificaat Intrekking controles die geen cookies ondersteunen
- Individuele webverzoeken die geen cookies ondersteunen. In sommige gevallen worden cookies geblokkeerd voor individuele verzoeken vanwege het Content Security Policy van de website. Deze beperking geldt voor veel populaire Content Delivery Networks.
- Wanneer het doeldomein/de doelcategorie is overgeslagen van SAML met behulp van een

SAML-bypasslijst
- Wanneer het doeldomein/de doelcategorie is overgeslagen van HTTPS-decryptie met behulp van een lijst met selectieve decryptie.

Vanwege deze beperkingen is het belangrijk om een passend minimumtoegangsniveau te configureren in het relevante netwerk-/tunnelbeleid. Het standaardbeleid moet bedrijfskritieke toepassingen/domeinen/categorieën en netwerken voor de levering van inhoud toestaan.

U kunt ook het IP Surrogates-systeem gebruiken om de compatibiliteit te verbeteren.

SAML-bypass

In zeldzame gevallen zijn uitzonderingen nodig. Dit is nodig wanneer SWG een verzoek voor SAML-verificatie indient, maar de app of website deze niet kan ondersteunen. Dit gebeurt wanneer:

- Een niet-browser-app gebruikt een user agent die eruit ziet als een webbrowser
- Een script kan geen HTTP-omleidingen verwerken die door onze cookietests worden uitgevoerd
- Het eerste verzoek in een browsesessie is een POST-verzoek (bijv. URL voor eenmalige aanmelding) dat niet correct kan worden omgeleid voor SAML

De SAML Bypass List is de beste manier om een domein uit te sluiten van authenticatie terwijl de beveiliging behouden blijft (File Inspection).

- De uitzondering SAML Bypass List moet worden toegepast op het juiste beleid dat van invloed is op het netwerk/de tunnel die wordt gebruikt om verbinding te maken
- De SAML-bypasslijst staat het verkeer niet automatisch toe. De domein(en) moeten nog steeds zijn toegestaan op categorie- of bestemmingslijsten in het relevante beleid.

SAML Bypass - Overwegingen

Bij het toevoegen van uitsluitingen voor populaire sites en "homepages" is het belangrijk om rekening te houden met de impact op SAML. SAML werkt het beste wanneer het eerste verzoek in een browsesessie een GET-verzoek naar een HTML-pagina is. Bijvoorbeeld: http://www.myhomepage.tld. Dit verzoek wordt omgeleid voor SAML-verificatie en latere verzoeken nemen dezelfde identiteit aan met behulp van IP-surrogaten of cookies.

Het omzeilen van homepages van SAML kan een probleem veroorzaken waarbij het eerste verzoek dat door het SAML-systeem wordt gezien, betrekking heeft op achtergrondinhoud. Bijvoorbeeld http://homepage-content.tld/script.js. Dit is een probleem omdat SAML-omleiding naar een SAML-aanmeldingspagina niet mogelijk is wanneer de browser ingesloten inhoud laadt (zoals JS-bestanden). Dit betekent dat de pagina lijkt te renderen of onjuist werkt totdat de gebruiker naar een andere site gaat om de aanmelding te activeren.

Overweeg bij het overwegen van populaire sites en homepages deze keuzes:

- Sluit homepages en populaire sites niet uit van SAML- of HTTPS-decodering, tenzij nodig

- Als een startpagina wordt uitgesloten, moeten alle domeinen die door die site worden gebruikt (inclusief achtergrondinhoud) worden uitgesloten om SAML-incompatibiliteiten te voorkomen

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.