Fehlerbehebung bei nicht angewendeter SAML-Identität für sicheren Web-Gateway-Datenverkehr

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei SAML-Identitäten beschrieben, die nicht auf den Secure Web Gateway-Datenverkehr angewendet werden.

SAML-Identität für NICHT-Webdatenverkehr angewendet

Wenn die SAML-Identität für KEINEN Web-Datenverkehr übernommen wird, lesen Sie die Umbrella-Dokumentation, um sicherzustellen, dass die Einrichtung korrekt abgeschlossen wurde. Diese Konfigurationselemente müssen ausgefüllt werden.

- IDp-Einstellungen konfiguriert und getestet unter "Deployments > SAML Configuration"
- Liste der Benutzer/Gruppen, die in "Deployments > Web Users and Groups" (Bereitstellungen > Webbenutzer und Gruppen) bereitgestellt werden.
- SAML muss in der entsprechenden Richtlinie* unter 'Policies > Web Policies' (Richtlinien > Webrichtlinien) aktiviert werden.
- Die HTTPS-Entschlüsselung muss in der entsprechenden Richtlinie unter 'Richtlinien > Webrichtlinien' aktiviert werden

Aktivieren von SAML in Webrichtlinien

SAML- und HTTPS-Entschlüsselung müssen in der Richtlinie aktiviert werden, die für die jeweilige Netzwerk- oder Tunnelidentität gilt. Diese Funktionen gelten, bevor ein Benutzer identifiziert wurde. Die wichtigste Richtlinie ist daher die Richtlinie, die auf die "Verbindungsmethode" angewendet wird.

SAML-Richtlinien müssen wie folgt sortiert werden:

1. HÖHERE Priorität - Die Richtlinie gilt für Benutzer/Gruppen. Diese Richtlinie legt die Content-/Sicherheitseinstellungen für die authentifizierten Benutzer fest.
2. NIEDRIGERE Priorität - Richtlinie gilt für Netzwerk/Tunnel. Für diese Richtlinie ist SAML aktiviert, und die erste Authentifizierung wird ausgelöst.

SAML-Identität für spezifischen Web-Datenverkehr nicht angewendet

IP-Surrogate (Standardverhalten)

Zur Verbesserung der Konsistenz der Benutzeridentifizierung empfehlen wir die Aktivierung der neuen IP-Surrogate-Funktion. Diese Funktion wird automatisch für alle neuen Umbrella SAML-Kunden aktiviert, muss jedoch manuell für bestehende Umbrella-Kunden aktiviert werden.

IP-Surrogate verwendet einen Cache mit internen IP-Adressen > Benutzernamen, was bedeutet, dass die SAML-Identifizierung auf alle Arten von Anfragen angewendet werden kann: auch Nicht-Webbrowser-Datenverkehr, Datenverkehr, der keine Cookies unterstützt, und Datenverkehr, der nicht der SSL-Verschlüsselung unterliegt.

IP-Surrogate können die Konsistenz der Benutzeridentifizierung erheblich verbessern und den Verwaltungsaufwand verringern.

Beachten Sie, dass IP-Surrogate folgende Anforderungen erfüllen:

- Die interne IP-Transparenz muss über einen Umbrella Network Tunnel oder eine Proxy-Chain-Bereitstellung und X-Forwarded-For-Header gewährleistet werden. Dies funktioniert nicht mit der gehosteten PAC-Datei von Umbrella
- IP-Surrogate können nicht in Szenarien mit gemeinsam genutzten IP-Adressen verwendet werden (Terminalserver, Fast User Switching).
- Cookies müssen im Browser aktiviert sein. Für den ersten Authentifizierungsschritt sind weiterhin Cookies erforderlich.

Cookie-Surrogate (IP-Surrogate deaktiviert)

Wenn IP-Surrogate deaktiviert ist, wird die Benutzeridentität nur auf Anfragen von unterstützten Webbrowsern angewendet, und der Webbrowser MUSS Cookies unterstützen. SWG verlangt, dass der Browser Cookies für jede Anforderung unterstützt, um die Benutzersitzung in einem Cookie zu verfolgen. Leider bedeutet dies, dass nicht erwartet wird, dass jede Webanforderung einem Benutzer in diesem Modus zugeordnet wird.

SAML wird unter diesen Umständen nicht angewendet, stattdessen wird die Standardrichtlinie verwendet, die der Netzwerk-/Tunnelidentität zugewiesen ist:

- Nicht-Webbrowser-Datenverkehr
- Webbrowser mit deaktivierten Cookies oder IE-Sicherheitskonfiguration
- OCSP-/Zertifikatsperrungsprüfungen, die keine Cookies unterstützen
- Einzelne Webanfragen, die keine Cookies unterstützen, in einigen Fällen werden Cookies

aufgrund der Inhaltssicherheitsrichtlinie der Website für einzelne Anfragen gesperrt. Diese Einschränkung gilt für viele gängige Content Delivery Networks.
- Wenn die Zieldomäne/-kategorie mithilfe einer SAML-Umgehungsliste von SAML umgangen wurde
- Wenn die Zieldomäne bzw. -kategorie von der HTTPS-Entschlüsselung mithilfe einer Umbrella Selective Entschlüsselungsliste umgangen wurde.

Aufgrund dieser Einschränkungen ist es wichtig, eine angemessene Mindestzugriffsstufe in der entsprechenden Netzwerk-/Tunnelrichtlinie zu konfigurieren. Die Standardrichtlinie muss geschäftskritische Anwendungen/Domänen/Kategorien und Content Delivery Networks zulassen.

Alternativ können Sie das IP Surrogates-System zur Verbesserung der Kompatibilität verwenden.

SAML-Umgehung

In seltenen Fällen sind Ausnahmen erforderlich. Dies ist erforderlich, wenn die SWG eine Anforderung zur SAML-Authentifizierung stellt, diese aber von der App oder der Website nicht unterstützt wird. Dies geschieht, wenn:

- Eine Nicht-Browser-App verwendet einen Benutzer-Agenten, der wie ein Webbrowser aussieht.
- Ein Skript kann keine HTTP-Umleitungen verarbeiten, die von unseren Cookie-Tests durchgeführt wurden
- Die erste Anforderung in einer Browsersitzung ist eine POST-Anforderung (z. B. Single Sign-On (URL), die für SAML nicht richtig umgeleitet werden können

Die SAML-Umgehungsliste ist die beste Möglichkeit, eine Domäne von der Authentifizierung auszuschließen und gleichzeitig die Sicherheit aufrechtzuerhalten (Dateiinspektion).

- Die SAML-Umgehungslistenausnahme muss auf die richtige Richtlinie angewendet werden, die sich auf das Netzwerk/den Tunnel auswirkt, das/der für die Verbindung verwendet wird.
- Die SAML Bypass List lässt den Datenverkehr nicht automatisch zu. Die Domäne(n) muss/müssen nach Kategorie oder Zielliste in der entsprechenden Richtlinie weiterhin zugelassen sein.

SAML-Umgehung - Überlegungen

Beim Hinzufügen von Ausschlüssen für beliebte Websites und "Homepages" ist es wichtig, die Auswirkungen auf SAML zu berücksichtigen. SAML funktioniert am besten, wenn die erste Anforderung in einer Browsersitzung eine GET-Anforderung an eine HTML-Seite ist. Beispiel: http://www.myhomepage.tld Diese Anfrage wird zur SAML-Authentifizierung umgeleitet, und nachfolgende Anfragen übernehmen dieselbe Identität mithilfe von IP-Surrogaten oder Cookies.

Das Umgehen von Homepages aus SAML kann ein Problem auslösen, bei dem die erste vom SAML-System erkannte Anforderung auf Hintergrundinhalte ausgerichtet ist. Beispiel: http://homepage-content.tld/script.js. Dies ist problematisch, da die SAML-Umleitung auf eine SAML-Anmeldeseite nicht möglich ist, wenn der Browser eingebettete Inhalte lädt (wie JS-Dateien). Dies bedeutet, dass die Seite anscheinend falsch gerendert wird oder nicht korrekt

funktioniert, bis der Benutzer an eine andere Site geht, um die Anmeldung auszulösen.

Wenn Sie beliebte Websites und Homepages in Betracht ziehen, berücksichtigen Sie folgende Optionen:

- Schließen Sie Homepages und beliebte Websites nicht von der SAML- oder HTTPS-Entschlüsselung aus, es sei denn, dies ist erforderlich.
- Wenn eine Homepage ausgeschlossen wird, müssen alle von dieser Website verwendeten Domänen (einschließlich Hintergrundinhalte) ausgeschlossen werden, um SAML-Inkompatibilitäten zu vermeiden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.