Troubleshoot SAML Identity Not Being Applied for Secure Web Gateway Traffic

Contents

Introduction

This document describes how to troubleshoot SAML identities not being applied to Secture Web Gateway Traffic.

SAML Identity not applied for ANY web traffic

If the SAML identity is not applied for ANY web traffic, please consult the Umbrella documentation to ensure the setup has been completed correctly. These configuration items must be completed.

- IdP settings configured and tested in '**Deployments > SAML Configuration**'
- List of users/groups provisioned in '**Deployments > Web Users and Groups**'
- SAML must be enabled in the relevant policy* in '**Policies > Web Policies**'.
- HTTPS Decryption must be enabled in the relevant policy in '**Policies > Web Policies**'

Enabling SAML in Web Policies

SAML and HTTPS Decryption must be enabled in the policy that applies to the relevant Network or Tunnel identity. These features apply before a user has been identified, so the important policy is the one applied to the "connection method".

SAML policies must be ordered as follows:

1. HIGHER Priority - Policy applies to Users/Groups. This policy decides the content/security settings for the authenticated users.
2. LOWER Priority - Policy applies to Network/Tunnel. This policy has SAML enabled and triggers the initial authentication.

SAML Identity not applied for specific web traffic

IP Surrogates (Default Behaviour)

To improve consistency of user identification we recommend to enable the new IP Surrogates feature.

This feature is enabled automatically for all new Umbrella SAML customers but needs to be manually enabled for existing Umbrella customers.

IP surrogates uses a cache of *Internal IP > Username* information which means SAML identification can be applied to all types of requests: even non-web browser traffic, traffic which does not support cookies, and traffic not subject to SSL Decryption.

IP surrogates can greatly improve the consistency of user identification and reduce administrative burden.

Please note that IP surrogates has these requirements:

- **Internal IP visibility** must be provided by using an Umbrella Network Tunnel or Proxy-Chain deployment and X-Forwarded-For headers. This does not work with Umbrella's hosted PAC file
- IP surrogates **cannot be used in shared IP address scenarios** (Terminal Servers, Fast User Switching)
- **Cookies must be enabled in the browser.** Cookies are still required for the initial authentication step.

Cookie surrogates (IP Surrogates Disabled)

With IP Surrogates disabled, user identity is only applied to requests from supported web browsers and the web browser MUST support cookies. SWG requires that the browser supports cookies for every request in order to track the users' session in a cookie. Unfortunately this means it is not expected for every web request to be associated with a user in this mode.

SAML is not applied in these circumstances and the default policy assigned to the Network/Tunnel identity is used instead:

- **Non-Web browser** traffic
- Web Browsers with **cookies disabled** or **IE Enhanced Security Configuration**
- **OCSP/Certificate Revocation checks** which do not support cookies
- Individual web requests which do not support cookies. In some cases cookies are blocked for individual requests due to the **Content Security Policy** of the website. This restriction applies to many popular **Content Delivery Networks**.
- When the target domain/category has been bypassed from SAML using a **SAML Bypass List**
- When the target domain/category has been bypassed from HTTPS Decryption using an **Umbrella Selective Decryption** list.

Due to these restrictions, it is important to **configure an appropriate minimum level of access** in the relevant Network/Tunnel policy. The default policy must allow business critical applications/domains/categories and Content Delivery Networks.

Alternatively, use the **IP Surrogates** system to improve compatibility.

SAML Bypass

In rare cases exceptions are required. This is necessary when SWG subjects a request for SAML authentication but the app or website cannot support it. This happen whens:

- A **non-browser app** uses a user agent that looks like a web browser
- A **script** cannot handle HTTP redirects performed by our cookie tests
- The first request in a browsing session is a **POST request** (eg. single sign-on URL) which cannot be properly redirected for SAML

The SAML Bypass List is the best way to exclude a domain from authentication whilst still maintaing

security (File Inspection).

- The SAML Bypass List exception must be applied to the correct policy affecting the Network / Tunnel used to connect
- The SAML Bypass List does not automatically allow the traffic. The domain(s) must still be allowed by category or destination lists in the relevant policy.

SAML Bypass - Considerations

When adding exclusions for popular sites and "homepages" it is important to consider the impact on SAML. SAML works best when the first request in a browsing session is a GET request to a HTML page. Eg: http://www.myhomepage.tld. This request is redirected for SAML authentication and subsequent requests assume the same identity using IP surrogates or cookies.

Bypassing homepages from SAML can trigger a problem where the first request seen by the SAML system is for background content. For example, http://homepage-content.tld/script.js. This is a problem because SAML redirecting to a SAML login page is not possible when the browser is loading embedded content (like JS files). This means the page appears to render or operate incorrectly until the user goes to a different site to trigger the logon.

When considering popular sites and homepages consider these choices:

- **Do not** exclude homepages and popular sites from SAML or HTTPS decryption unless necessary
- **If** excluding a homepage, then all domains used by that site (including background content) must be excluded to avoid SAML incompatibilities