排除SAML身份未应用于安全网络网关流量的故障

目录

简介

本文档介绍如何对未应用于安全网络网关流量的SAML标识进行故障排除。

SAML身份未应用于任何Web流量

如果未对任何网络流量应用SAML身份，请查阅Umbrella文档以确保设置已正确完成。必须完成这些配置项目。

- IdP设置在“Deployments > SAML Configuration”中配置和测试
- 在“Deployments”>“Web Users and Groups”(部署>“Web用户和组”)中调配的用户/组列表
- 必须在相关策略*的“Policies > Web Policies”中启用SAML。
- 必须在相关策略的“Policies > Web Policies”中启用HTTPS解密

在Web策略中启用SAML

必须在适用于相关网络或隧道标识的策略中启用SAML和HTTPS解密。这些功能在用户被识别之前应用，因此重要策略是应用于“连接方法”的策略。

SAML策略必须按如下方式排序：

1. 更高优先级 — 策略适用于用户/组。此策略决定已验证用户的内容/安全设置。
2. LOWER Priority — 策略应用于网络/隧道。此策略启用了SAML并触发初始身份验证。

SAML身份不适用于特定网络流量

IP代理（默认行为）

为了提高用户标识的一致性，我们建议启用新的IP代理功能。此功能对所有新Umbrella SAML客户自动启用，但需要为现有Umbrella客户手动启用。

IP代理使用Internal IP > Username信息的缓存，这意味着SAML标识可应用于所有类型的请求：即使是非Web浏览器流量、不支持cookie的流量和不受SSL解密约束的流量。

IP代理可大大提高用户识别的一致性，减轻管理负担。

请注意，IP代理具有以下要求:

- 必须使用Umbrella网络隧道或代理链部署和X-Forwarded-For报头来提供内部IP可视性。 这不适用于Umbrella的托管PAC文件
- IP代理不能在共享IP地址场景中使用（终端服务器、快速用户交换）
- 必须在浏览器中启用Cookie。 初始身份验证步骤仍然需要Cookie。

Cookie替代（禁用IP替代）

禁用IP代理后，用户身份仅应用于来自受支持的Web浏览器的请求，Web浏览器必须支持cookie。 SWG要求浏览器支持每个请求的Cookie，以便在Cookie中跟踪用户会话。遗憾的是，这意味着并不是期望每个Web请求都与此模式中的用户关联。

SAML未在这些情况下应用，而是使用分配给网络/隧道标识的默认策略：

- 非Web浏览器流量
- 禁用cookie或IE增强型安全配置的Web浏览器
- 不支持cookie的OCSP/证书吊销检查
- 不支持Cookie的个人Web请求。在某些情况下，由于网站的内容安全策略，个人请求的cookie被阻止。 此限制适用于许多常见的内容交付网络。
- 使用SAML旁路列表从SAML绕过目标域/类别时
- 当使用Umbrella Selective Decryption列表从HTTPS解密绕过目标域/类别时。

由于这些限制，必须在相关网络/隧道策略中配置适当的最低访问级别。默认策略必须允许关键业务应用/域/类别和内容交付网络。

或者，使用IP代理系统提高兼容性。

SAML旁路

在极少数情况下需要例外。 当SWG对SAML身份验证请求进行审核但应用或网站无法支持该请求时，必须执行此操作。 在以下情况下会发生这种情况：

- 非浏览器应用使用类似于Web浏览器的用户代理
- script无法处理由cookie测试执行的HTTP重定向
- 浏览会话中的第一个请求是POST请求(例如，单一登录URL)，无法为SAML正确重定向

SAML Bypass List是在仍保持安全性（文件检查）的情况下将域从身份验证中排除的最佳方法。

- SAML Bypass List例外必须应用于影响用于连接的网络/隧道的正确策略
- SAML旁路列表不会自动允许流量。 在相关策略中仍必须按类别或目标列表允许域。

SAML旁路 — 注意事项

添加热门网站和“主页”的例外项时，必须考虑对SAML的影响。当浏览会话中的第一个请求是对HTML页面的GET请求时，SAML效果最佳。 例如： http://www.myhomepage.tld。 此请求被重定向以进行SAML身份验证，后续请求使用IP代理或cookie采用相同的身份。

绕过来自SAML的主页可能会触发一个问题，其中SAML系统看到的第一个请求是针对背景内容。例如，http://homepage-content.tld/script.js。这是一个问题，因为在浏览器加载嵌入内容（如JS文件）时，无法将SAML重定向到SAML登录页。 这意味着在用户转到其他站点触发登录之前，页面似乎呈现或操作不正确。

在考虑热门网站和主页时，请考虑以下选择：

- 除非必要，否则请勿将主页和常用站点从SAML或HTTPS解密中排除
- 如果排除主页，则必须排除该站点使用的所有域（包括背景内容）以避免SAML不兼容

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。