非浏览器Web流量的安全访问SSO身份验证行为

目录

问题

实施具有IPsec连接的思科安全访问(CSA)时，需要明确安全配置文件中的SSO身份验证行为。具体而言，当站点通过IPsec隧道连接时，会出现关于哪些类型的出站Internet流量触发SSO身份验证的问题。

主要关注点是了解SSO身份验证是否只适用于通过TCP端口80和443进行的基于浏览器的Web访问，或者是否也适用于非浏览器应用程序和设备（例如打印机或生成网络流量的非Windows终端）。需要说明在身份验证提示和重定向到身份提供者(IdP)时，来自所连接站点的不同类型的Web流量会发生什么行为。

环境

- 思科安全访问(CSA)部署
- 站点和CSA之间的IPsec隧道连接
- 使用SSO身份验证配置的安全配置文件
- 包含各种设备（包括打印机和非Windows终端）的混合环境
- 已启用HTTPS检查
- 已配置SAML集成

分辨率

思科安全访问中的SSO身份验证行为专门设计为仅针对基于浏览器的网络流量。系统执行复杂的检测过程以确定Web请求是否必须接受SSO身份验证。

SSO身份验证过程

将Web请求重定向到身份提供程序(IdP)之前，思科安全访问使用HTTPS检查来确定请求是否来自支持cookie的浏览器。此检测过程是区分基于浏览器的Web流量和非浏览器Web流量的关键机制。

通信分类

基于浏览器的流量（接受SSO身份验证）

- 来自支持cookie的浏览器的Web请求
- 来自浏览器应用的TCP端口80和443上的HTTP/HTTPS流量
- 通过HTTPS检查Cookie/浏览器检测的流量

非浏览器流量（不接受SSO身份验证）

- 来自打印机和其他网络设备的网络流量
- 不支持Cookie或未识别为浏览器的应用程序
- 生成浏览器检测失败的网络流量的非Windows终端
- 未通过HTTPS检查浏览器验证的所有Web流量

SSO身份验证的必备条件

要使SSO身份验证在环境中正常工作，必须满足几个先决条件：

- 工作SAML配置必须到位。
- 使用XFF和/或没有NAT的隧道的代理网络（IP代理需要内部专用IP的可见性）。

- 必须启用HTTPS检查。
- 浏览器会话必须维护Cookie（建议不要在会话结束时删除Cookie或不识别浏览）。
- 跨位置的非重叠IP地址，如果存在重叠，则进行适当的站点分离。

原因

该行为是思科安全访问中的设计行为。SSO身份验证机制经过专门设计，旨在通过Web浏览器将交互式用户会话作为目标，同时允许自动化系统和非交互式设备访问Web资源而不中断身份验证。此设计可防止对无法处理身份验证重定向或基于Cookie的会话的自动化流程、设备管理接口和应用程序造成中断。

相关内容

- 配置SAML集成 — 为SAML启用IP代理
- 思科技术支持和下载

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）。