绕过安全网络设备中的身份验证

目录

简介

先决条件

- 要求
- 使用的组件

免除身份验证

在Cisco SWA中免除身份验证的方法

绕过身份验证的步骤

相关内容

简介

本文档介绍如何绕过安全网络设备(SWA)中的身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- SWA管理。

思科建议您安装以下工具：

- 物理或虚拟SWA
- 对SWA图形用户界面(GUI)的管理访问

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

免除身份验证

在Cisco SWA中对某些用户或系统免除身份验证对于保持运营效率和满足特定要求至关重要。首先，一些用户或系统需要不间断地访问可能受身份验证过程阻碍的关键资源或服务。例如，执行定期更新或备份的自动化系统或服务帐户需要无缝访问而不会出现身份验证机制导致的延迟或潜在故障。

此外，有些情况下，Web服务提供商建议不要使用代理来访问其服务。在这种情况下，免除身份验证可确保符合提供商准则并保持服务可靠性。此外，为了有效地阻止某些用户的流量，通常必须首先免除这些用户的身份验证，然后应用适当的阻止策略。此方法允许对访问权限进行精确控制。

在某些情况下，所访问的Web服务是受信任的，并且普遍可以接受的，例如Microsoft更新。免除此类服务的身份验证可简化所有用户的访问。此外，在某些情况下，用户操作系统或应用不支持SWA中配置的身份验证机制，需要旁路以确保连接。

最后，具有固定IP地址的服务器（这些服务器没有用户登录且受信任的Internet访问有限）不需要身份验证，因为它们的访问模式是可预测和安全的。

通过在战略上免除对这些案例的身份验证，组织可以在安全需求与运营效率之间取得平衡。

在Cisco SWA中免除身份验证的方法

SWA中的免认证可通过各种方法实现，每种方法都根据特定场景和要求进行定制。以下是配置身份验证豁免的一些常用方法：

- IP地址或子网掩码：最直接的方法之一是免除对特定IP地址或整个子网进行身份验证。这对于具有固定IP地址或受信任网段的服务器特别有用，这些服务器需要不间断地访问Internet或内部资源。通过在SWA配置中指定这些IP地址或子网掩码，您可以确保这些系统绕过身份验证过程。

- 代理端口：您可以将SWA配置为根据特定代理端口免除流量。当某些应用程序或服务使用指定端口进行通信时，此功能非常有用。通过标识这些端口，可以设置SWA以绕过对这些端口上的流量的身份验证，从而确保相关应用或服务的无缝访问。

- URL类别：另一种方法是根据URL类别免除身份验证。这可以包括预定义的思科类别和根据您的组织特定需求定义的自定义URL类别。例如，如果某些Web服务（例如Microsoft更新）被视为受信任且普遍可接受，您可以将SWA配置为绕过这些特定URL类别的身份验证。这可确保所有用户无需身份验证即可访问这些服务。

- 用户代理：在处理不支持所配置的身份验证机制的特定应用或设备时，基于用户代理的免除身份验证非常有用。通过标识这些应用或设备的用户代理字符串，您可以配置SWA以绕过来自这些应用或设备的流量的身份验证，从而确保无缝连接。

绕过身份验证的步骤

以下是创建身份配置文件以免除身份验证的步骤：

步骤1.在GUI中，选择网络安全管理器，然后单击标识配置文件。
步骤2.单击Add Profile添加配置文件。
步骤3.使用Enable Identification Profile复选框启用此配置文件，或快速禁用此配置文件而不将其删除。
步骤4.分配唯一的配置文件名称。
步骤5.（可选）添加说明。
步骤6.从Insert Above下拉列表中，选择此配置文件在表中的显示位置。



注意：将不需要身份验证的标识配置文件置于列表顶部。此方法可减少SWA上的负载，最大限度地减少身份验证队列，并加快其他用户的身份验证。

步骤7.在User Identification Method部分，选择Exempt from authentication/identication。

步骤8.在按子网定义成员中，输入此标识配置文件应用的IP地址或子网。您可以使用IP地址、无类域间路由(CIDR)块和子网。

步骤9.（可选）单击Advanced以定义其他成员资格条件，例如Proxy Ports、URL Categories或User Agents。

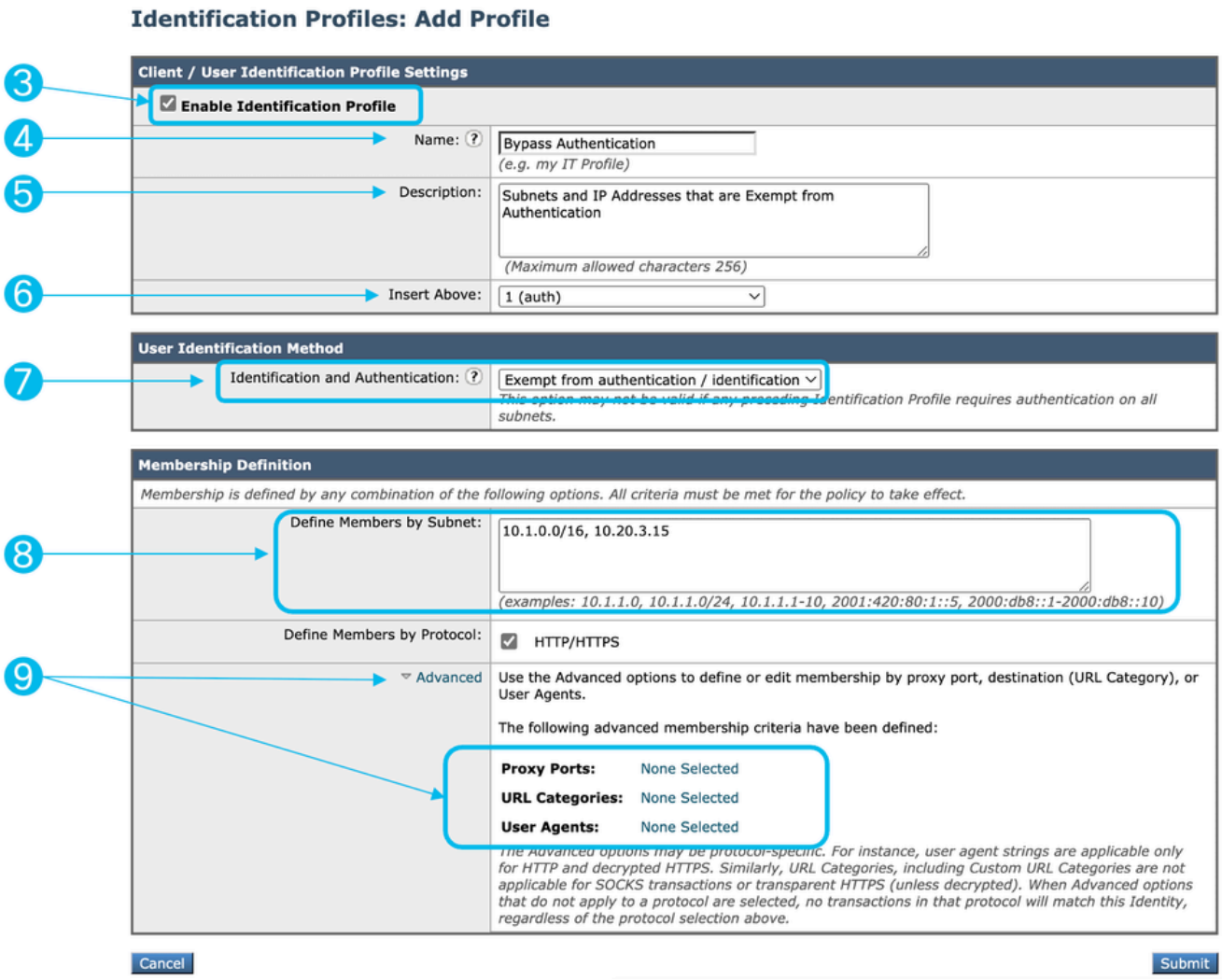


警告：在透明代理部署中，SWA无法读取HTTPS流量的用户代理或完整URL，除非流量已解密。因此，如果使用用户代理配置标识配置文件或使用正则表达式配置自定义URL类别，此流量将无法与标识配置文件匹配。

有关如何配置自定义URL类别的详细信息，请访问：[配置安全Web设备中的自定义URL类别 — 思

科

提示：策略使用AND逻辑，这意味着必须满足所有条件才能匹配ID配置文件。设置Advanced选项后，必须满足每一项要求才能应用策略。



映像 — 创建ID配置文件以绕过身份验证的步骤

步骤10.提交并提交更改。

相关内容

- 思科安全Web设备AsyncOS 15.0用户指南 — GD（通用部署） — 对最终用户进行策略应用分类[思科安全Web设备] — 思科
- 在安全Web设备中配置自定义URL类别 — 思科
- 如何免除Office 365流量在思科网络安全设备(WSA)上的身份验证和解密 — 思科

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）。