在安全Web设备中配置上游代理

目录

简介

本文档介绍在安全网络设备(SWA)中配置上游代理的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- SWA管理。
- 基本网络和代理协议。

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

- 对SWA命令行界面(CLI)的管理访问

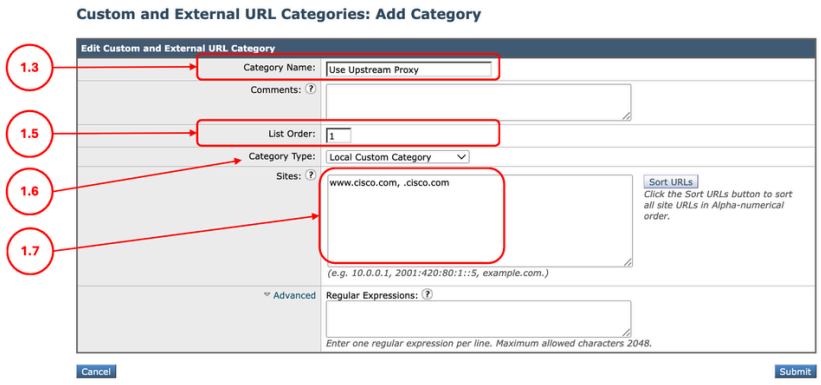
使用的组件

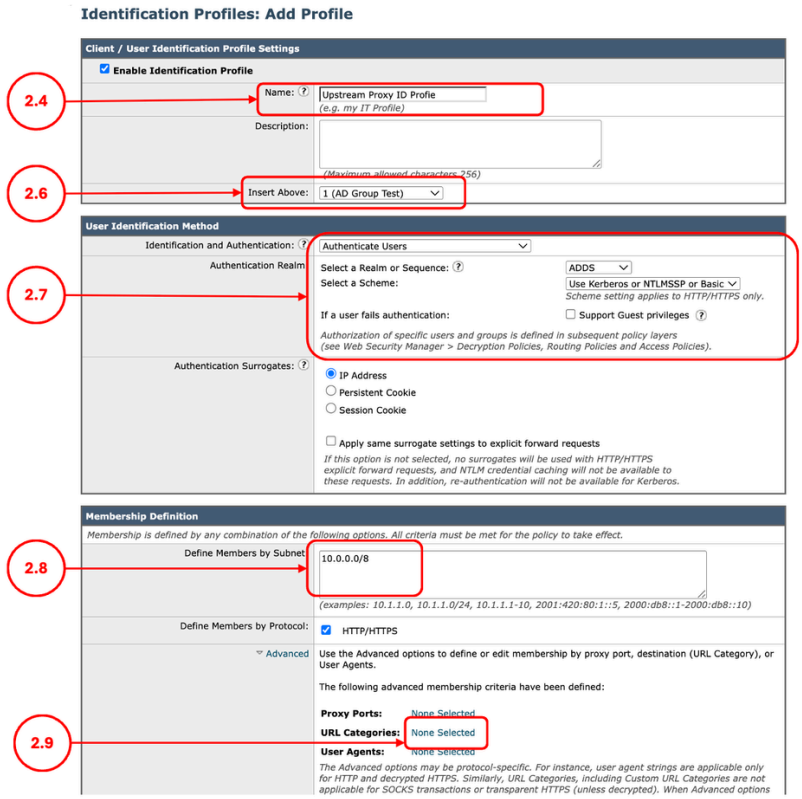
本文档不限于特定的软件和硬件版本。

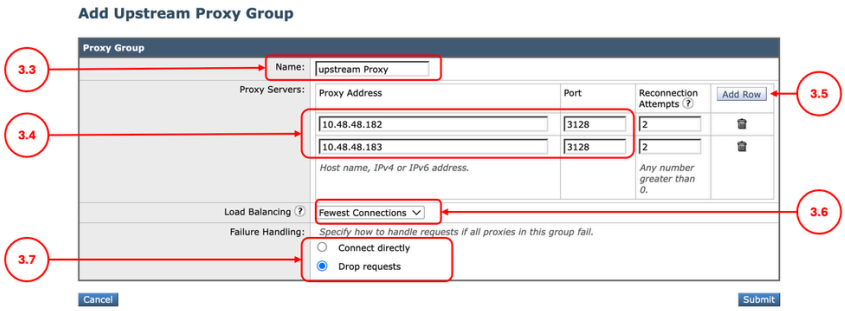
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

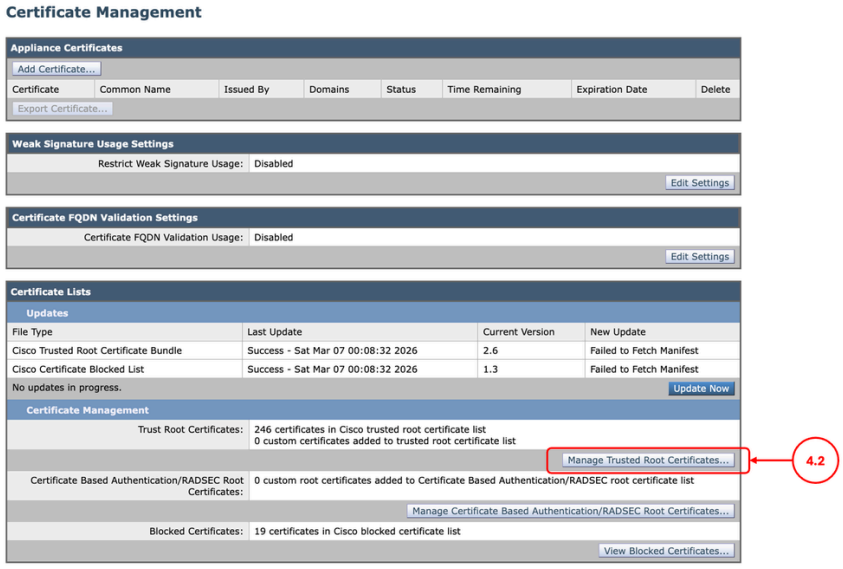
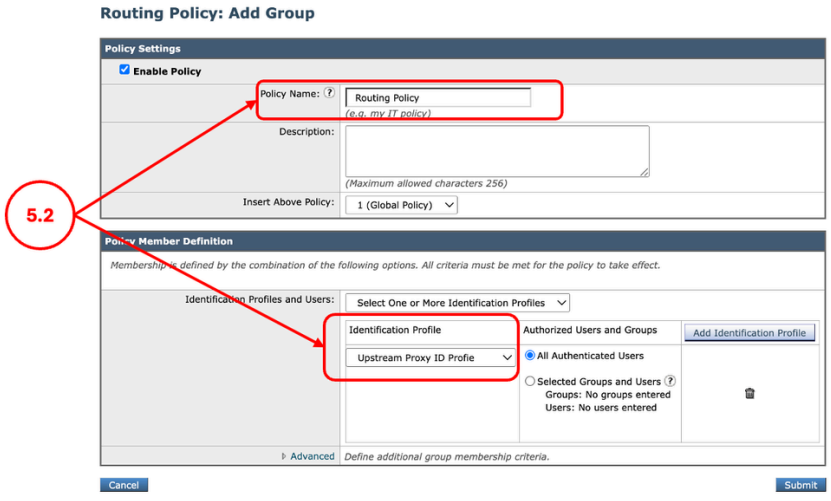
配置上游代理

使用以下步骤在SWA中配置上游代理。

步骤	步骤
步骤1.（可选）为URL创建自定义URL类别 注意：如果要为所有流量定义上游代理，可以跳过此步骤。	第1.1步：从GUI，选择Web Security Manager，然后单击Custom and External URL Categories。 第1.2步：点击添加类别以添加自定义URL类别。 第1.3步：分配唯一的CategoryName。 第1.4步(可选)添加说明。 第1.5步：从列表顺序中选择要放在首位的第一个类别。 第1.6步：从Category Type下拉列表中，选择Local Custom Category。 第1.7步：在站点部分添加所需的URL。 步骤1.8.提交。  图像 — 创建自定义URL类别

步骤2.（可选）创建标识配置文件以使用上游代理 注意：如果要为所有流量定义上游代理，可以跳过此步骤。	第2.1步：从GUI，选择Web Security Manager，然后单击Identification Profiles。 第2.2步：点击添加配置文件添加配置文件。 第2.3步：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。 第2.4步：分配唯一的profileName。 第2.5步(可选)添加说明。 第2.6步：从Insert Above下拉列表中，选择此配置文件在表中的显示位置。 第2.7步。如果您不想对执行此策略的用户进行身份验证，请在User Identification Methodsection中选择Exempt from authentication/identication，否则配置身份验证参数。 第2.8步：在按子网定义成员中，将此字段留空以包含所有客户端IP地址，除非您想要通过特定IP地址的流量。 第2.9.(可选:如果您需要对访问某些网站的特定用户使用上游代理，请完成此步骤。) 在Advanced部分中，选择Custom URL Categories,Add在第1步中创建的Custom URL Category 步骤2.10.提交。  图像 — 创建标识配置文件
步骤3.创建上游代理	第3.1步：从GUI，选择Network，然后单击Upstream Proxy。

	步骤3.2.单击Add Group。 第3.3步：分配uniqueName。 第3.4步：定义代理地址和端口号。 第3.5步(可选)如果有多个上游代理，请点击添加行以定义下一个代理。 第3.6步(可选)如果从Load Balancing部分输入了多个Upstream Proxy，请定义所需的Load Balancing方法， • 无(故障转移):Web代理将事务定向到组中的一个外部代理。它会尝试按照代理的列出顺序连接到这些代理。如果无法访问一个代理，Web代理会尝试连接到列表中的下一个代理。 • 连接最少:Web代理跟踪有多少活动请求与组中的不同代理一起，并将事务定向到当前为最少数量连接提供服务的代理。 • 基于哈希：最近最少使用。如果所有代理当前都处于活动状态，则Web代理会将事务定向到最近最少收到事务的代理。此设置类似于轮询，除了Web代理还考虑代理作为不同代理组中的成员而收到的事务。也就是说，如果一个代理在多个代理组中列出，则“最近最少使用”选项不太可能给该代理带来过重的负担。 • 轮询:Web代理按所列顺序在组中的所有代理之间平均循环事务。 步骤3.7.选择故障处理选项取决于您的内部策略。 • 直接连接:将请求直接发送到其目标服务器。 • 丢弃请求:放弃请求而不转发它们。 步骤3.8.提交。  图像 — 添加上游代理组
步骤4.（可选）上传解密证书	第4.1步：从GUI，选择Network，然后单击Certificate Management。

注意：如果上游代理未解密流量或其CA服务器已在SWA中受信任，您可以跳过此步骤	第4.2步：从证书管理(Certificate Management)部分，点击管理受信任根证书(Manage Trusted Root Certificates)。  映像 — 管理受信任的根证书 步骤4.3.提交并提交更改。 注意:如果需要根和中间CA证书，请先上传根CA证书，然后点击Submit and Commit。提交完成后，导入中间CA证书，然后再次提交并确认更改。
步骤5.配置路由策略	第5.1步：从GUI中，选择Web Security Manager，然后单击Routing Policy。 第5.2步(可选)如果要为特定用户或网站使用上游代理，请点击Add Policy，并选择您在第2步中创建的Identification Profile。 

	图像 — 将ID配置文件添加到路由策略 第5.3步：对于要使用上游代理的所需条件，请点击Routing Destination链接并选择您在第3步中创建的上游代理组。  图像 — 配置路由目标 注意：如果您希望使用上游代理的所有流量，请从全局路由策略中选择所需的上游代理。 步骤5.4.提交并提交更改。
步骤6.（可选）配置上游代理无响应超时设置 提示:建议不要修改这些值，除非您完全了解其行为和潜在影响。	步骤6.1.登录到CLI并运行advancedproxyconfig 步骤6.2.选择其他项 步骤6.3.按Enter键，直到您看到Enter minimum idle timeout for checking unresponsive upstream proxy(in seconds)。 您可以配置最短时间，SWA等待重试之前声明为Sick的上游代理。默认值为 10 秒。 步骤6.4.按Enter继续下一个设置。当定义用于检查无响应上游代理的最大空闲超时时，请注意，如果在已用完配置的重新连接尝试次数之前达到此超时值(步骤3)，则SWA会考虑上游代理脱机。 步骤6.7.继续按Enter键，直到退出向导为止，运行commit以保存更改。

日志记录

访问日志

在访问日志中，路由到上游代理的流量显示为DEFAULT_PARENT，后跟上游代理的名称。以下是示例：

```
1775659642.780 462 10.20.3.15 TCP_MISS_SSL/200 129 CONNECT tunnel://www.cisco.com:443/ "AMOJARRA\amojar
```

代理日志

从代理日志中，您可以验证上游代理的运行状况。

提示：您可以过滤对等以查看与上游代理相关的日志。

下面是一些示例，因为我们将第3步中的重新连接尝试配置为两次，在两次连接到上游代理失败后，上游代理被声明为dad，并且SWA从列表中删除此上游代理，直到代理进程重新启动。

```
Thu Apr  2 13:52:35 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer-upstream 10.48.48.182:3128 was hea
Thu Apr  2 13:52:36 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer 10.48.48.182:3128 was sick, now he
...
Thu Apr  2 13:59:37 2026 Info: PROX_CONNTRACK : 60 : [71197:0] Peer 10.48.48.183:3128 remains sick afte
Thu Apr  2 13:59:39 2026 Warning: PROX_CONNTRACK : 70 : [71197:0] Peer-upstream 10.48.48.183:3128 decla
```

注意：如果上游代理不响应TCP SYN请求、无法返回HTTP响应代码或返回HTTP 504（网关超时）响应，SWA会认为上游代理不可用，并将其状态从Healthy更改为Sick。

提示：如果SWA返回VIA报头，则认为上游代理运行正常。

相关信息

- 思科安全Web设备AsyncOS 15.0用户指南
- 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
- 使用安全Web设备最佳实践 — 思科
- 阻止安全网络设备中的流量
- 阻止安全Web设备中的上传流量
- 阻止SWA中的可执行文件下载
- 绕过安全Web设备中的Microsoft更新流量
- 绕过安全Web设备中的身份验证 — 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）。