配置安全Web设备和Umbrella SWG之间的代理链

目录

[简介](#)

[概述](#)

[安全Web设备策略配置](#)

[用于透明代理部署](#)

[Umbrella控制面板中的SWG Web策略配置](#)

简介

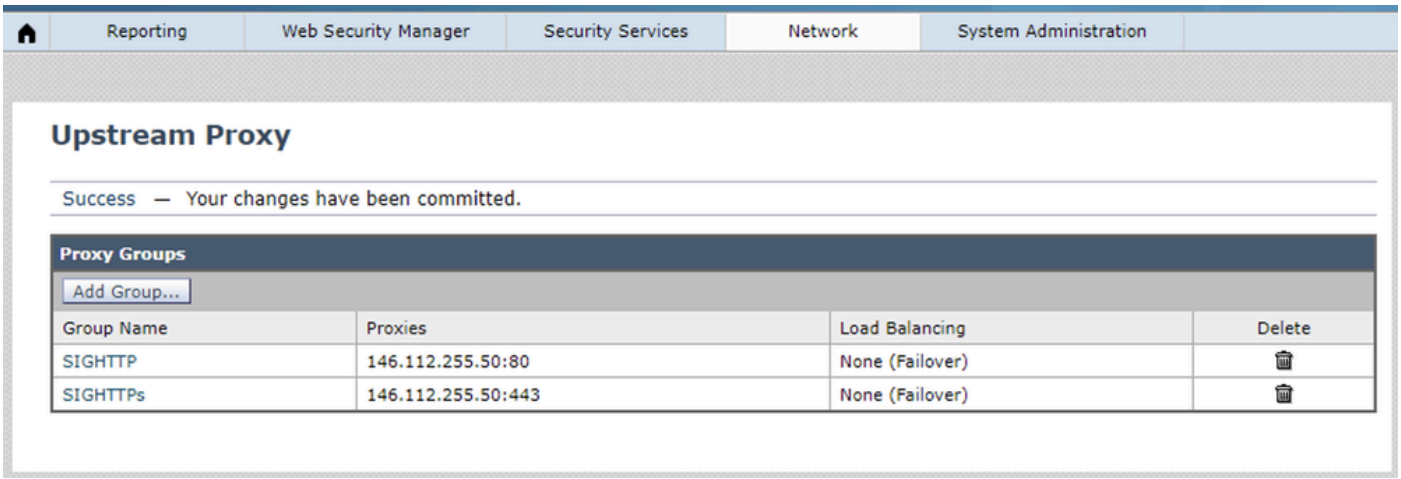
本文档介绍如何配置安全Web设备和Umbrella安全Web网关(SWG)之间的代理链。

概述

Umbrella SIG支持代理链，并可处理来自下游代理服务器的所有HTTP/HTTPs请求。这是在Cisco Secure Web Appliance（以前称为Cisco WSA）和Umbrella Secure Web Gateway(SWG)之间实施代理链的综合指南，包括安全Web设备和SWG的配置。

安全Web设备策略配置

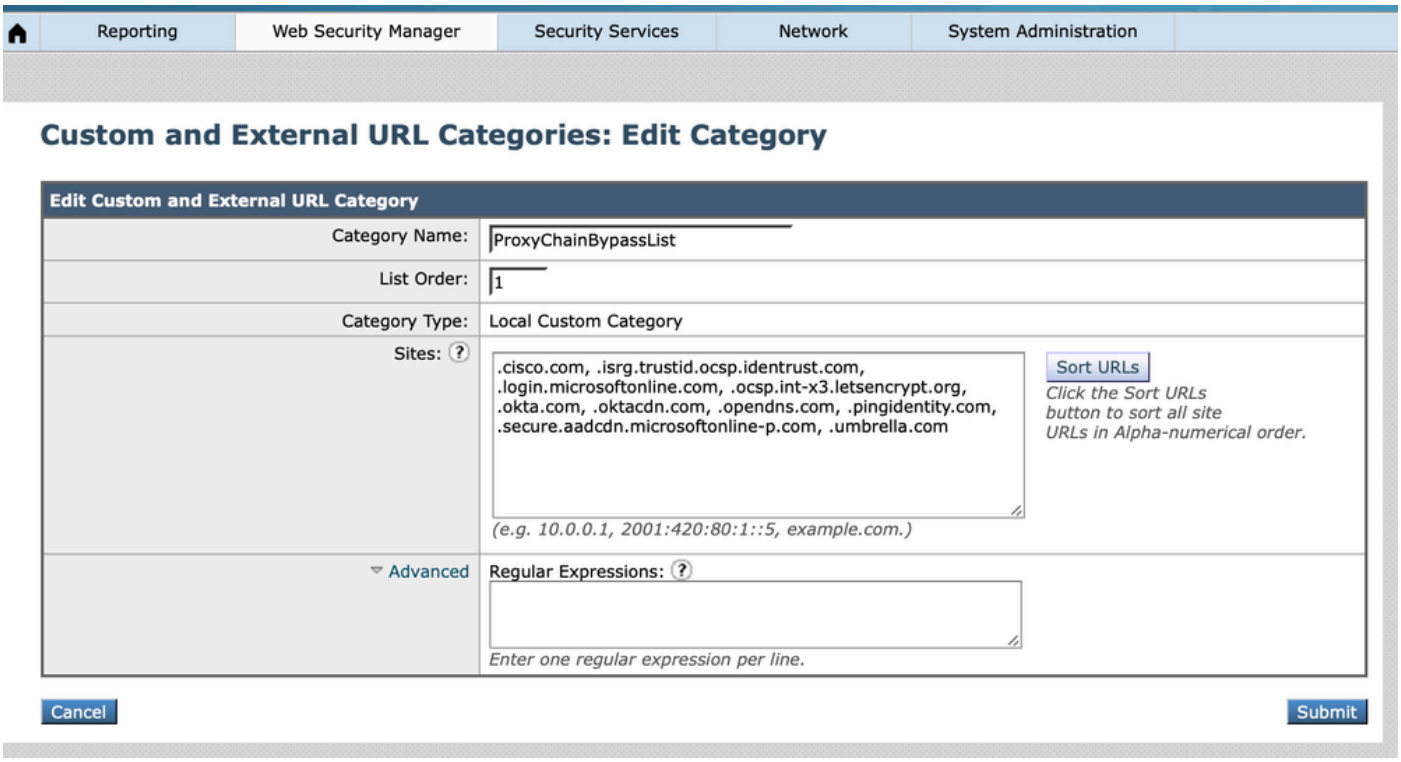
1.通过Network>Upstream Proxy将SWG HTTP和HTTPs链路配置为Upstream Proxy。



360079596451

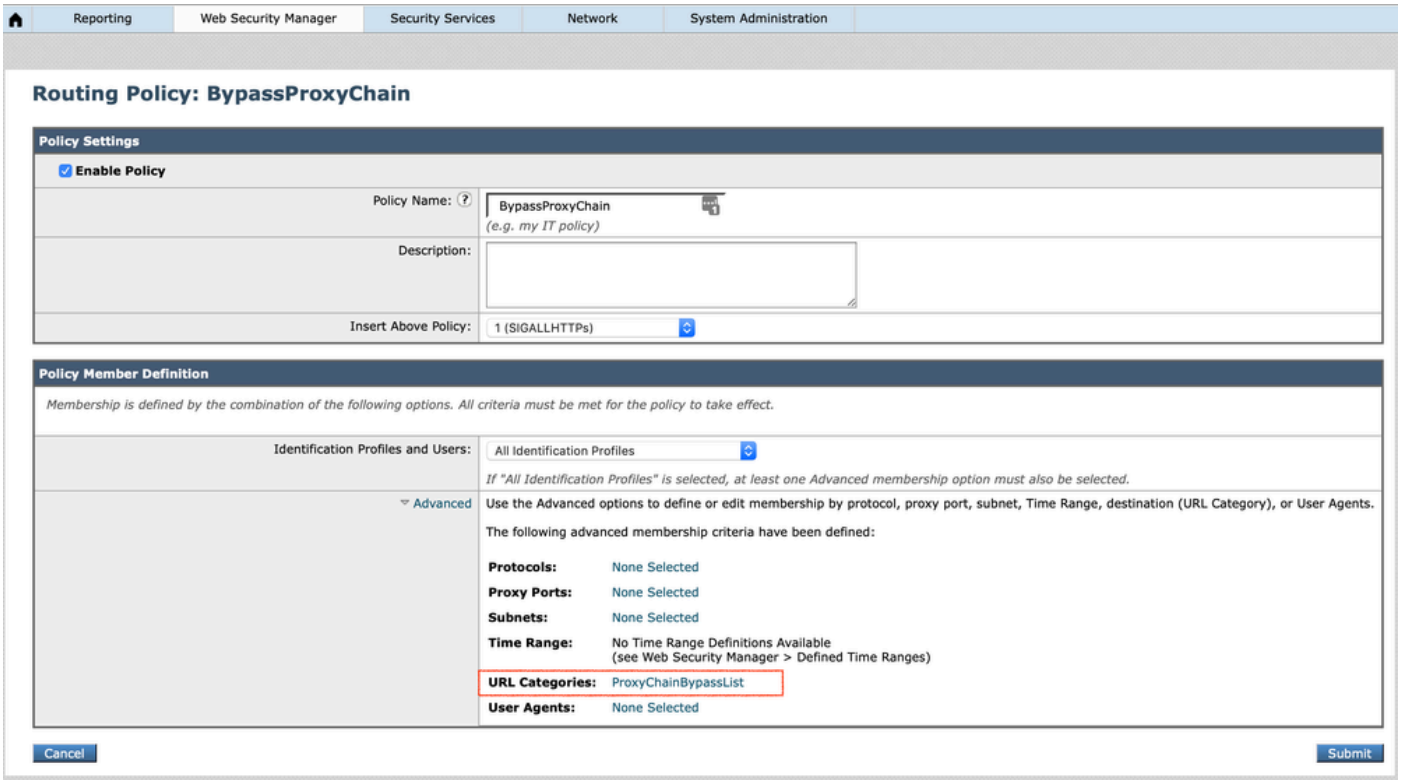
2.通过Web Security Manager>Routing Policy创建绕过策略，将所有建议的URL直接路由到Internet。所有绕过的URL可在我们的文档中找到：Cisco Umbrella SIG用户指南：管理代理链接

- 首先创建一个新的“自定义类别”，导航到Web Security Manager>自定义和外部URL类别，如此处所示。绕过策略基于“自定义类别”。



360050592552

- 接下来，通过导航到网络安全管理器>路由策略创建新的绕行路由策略。请确保此策略是第一个策略，因为安全网络设备根据策略顺序匹配策略。

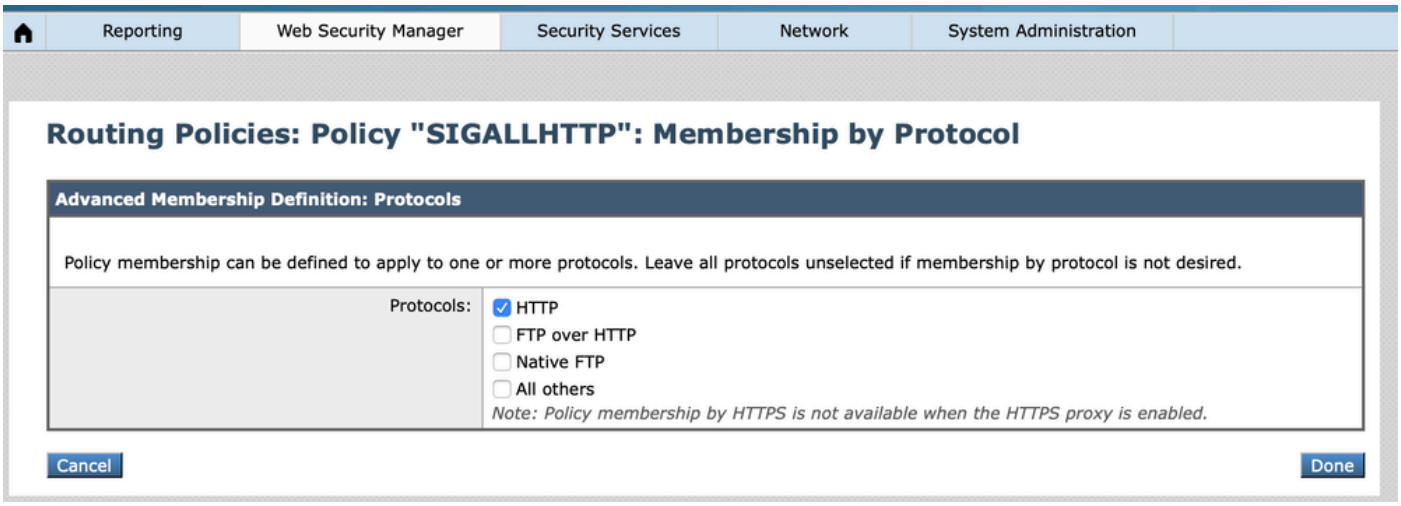


360050703131

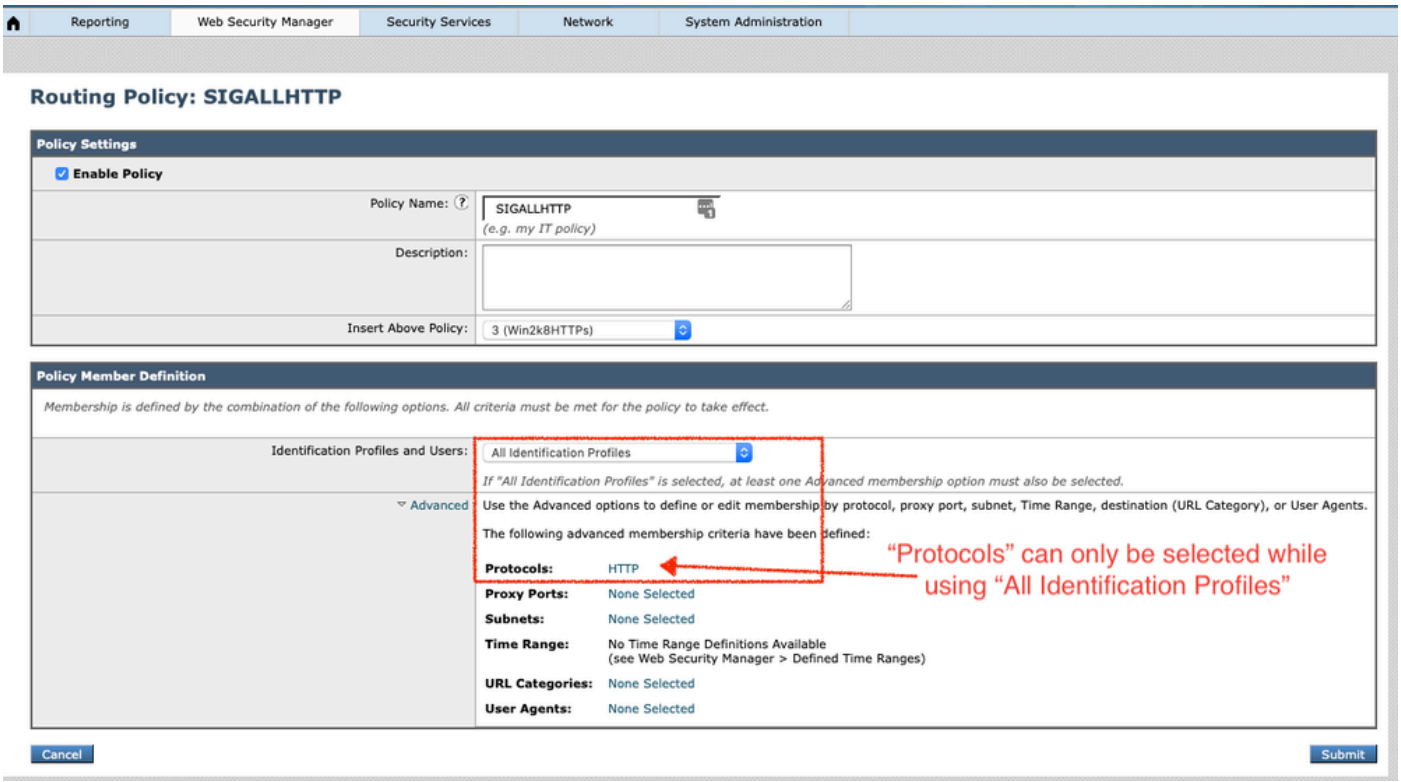
3.为所有HTTP请求创建新的路由策略。

- 在安全Web设备路由策略成员定义中，协议选项为HTTP、FTP over HTTP、本地FTP和“所有

其他”，同时选择“所有标识配置文件”。由于HTTP没有选项，因此为所有HTTP请求实施此路由策略后，分别创建HTTP请求的路由策略。

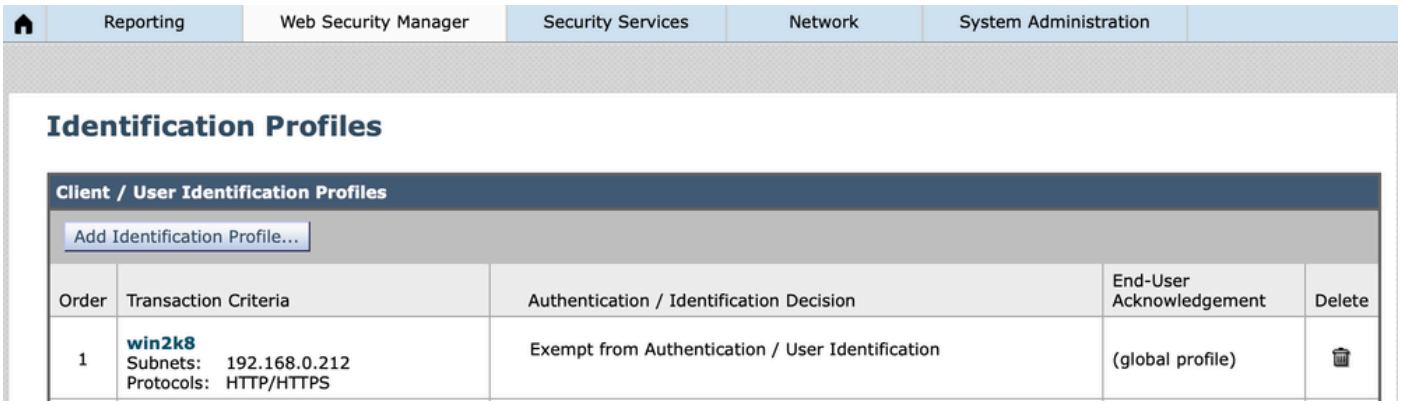


360050592772

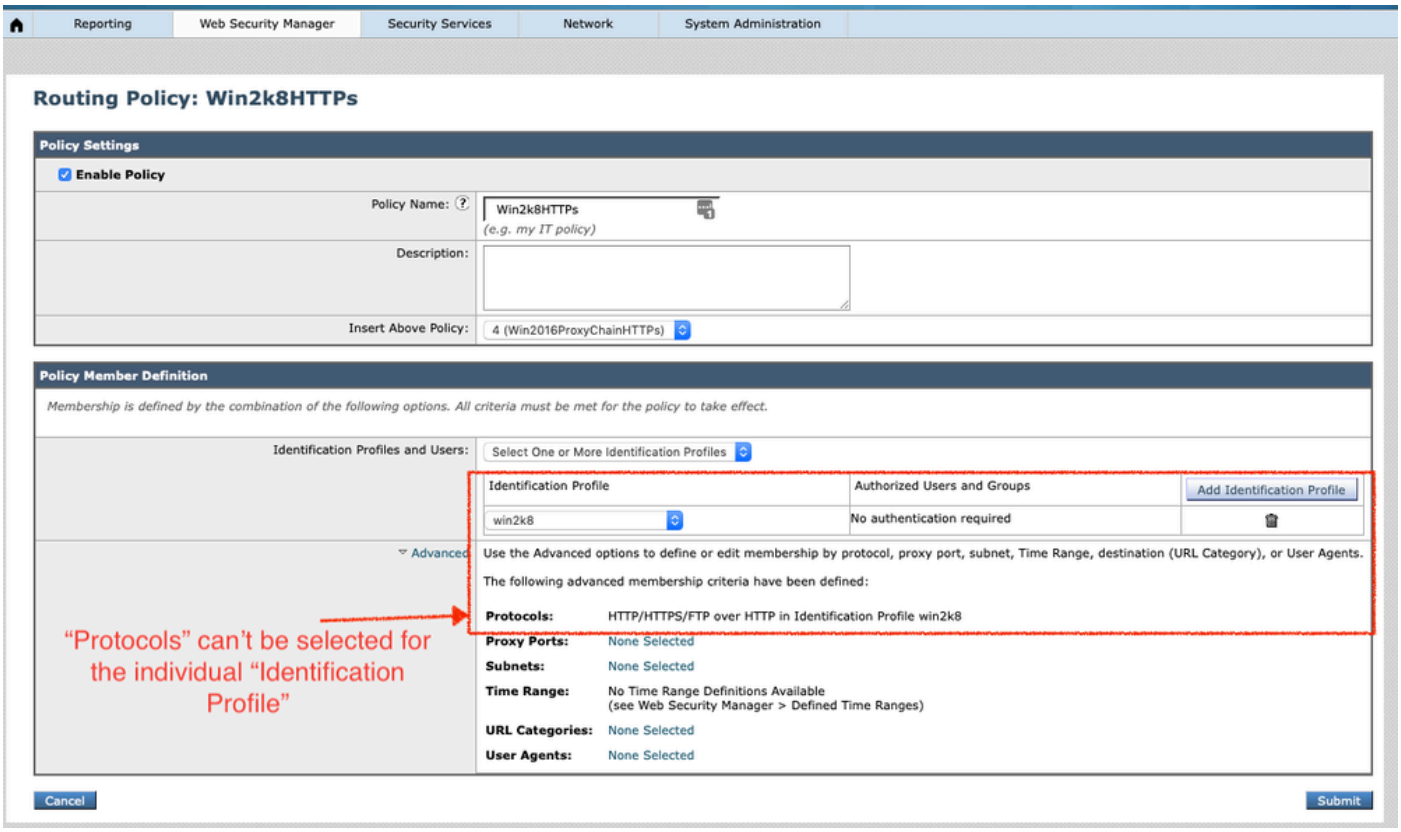


360050589572

4.根据“标识配置文件”为HTTPs请求创建路由策略。 请注意定义的“标识配置文件”的顺序，因为安全网络设备会匹配第一个匹配项的“标识”。在本示例中，标识配置文件“win2k8”是基于IP的内部标识。



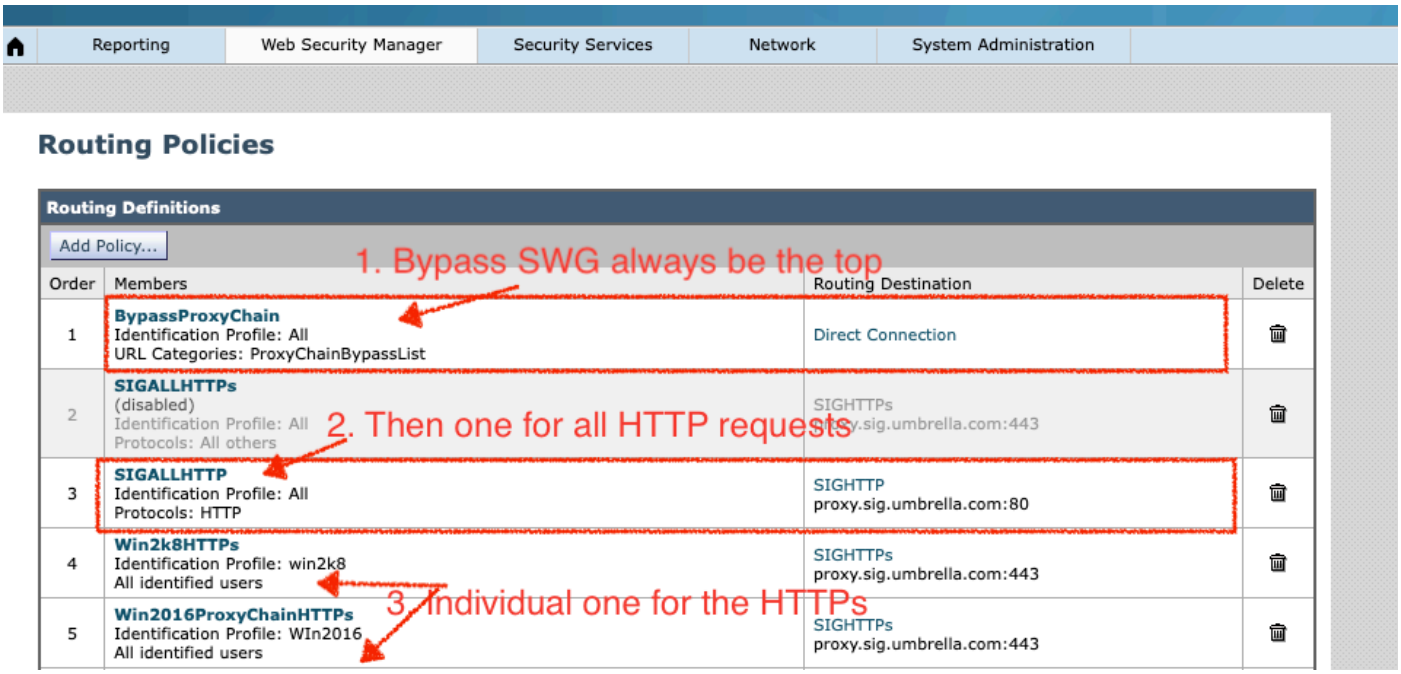
360050703971



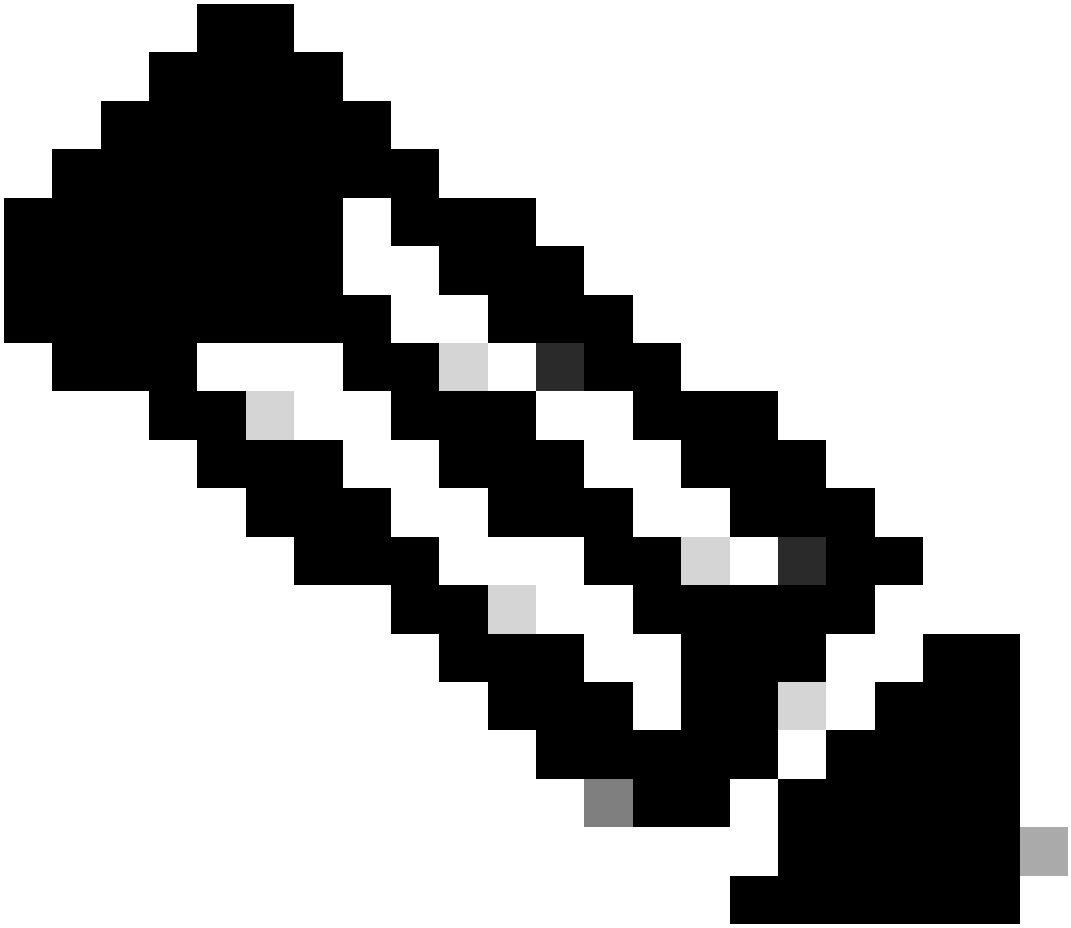
360050700091

5.安全Web设备路由策略的最终配置：

- 请注意，安全Web设备使用"自上而下"规则处理方法评估身份和访问策略。这意味着在处理过程中任意点进行的第一次匹配都会导致安全Web设备执行的操作。
- 此外，首先评估身份。一旦客户端的访问与特定身份匹配，安全网络设备将检查所有配置为使用与客户端访问匹配的身份的访问策略。



360050700131



注意：上述策略配置仅适用于显式代理部署。

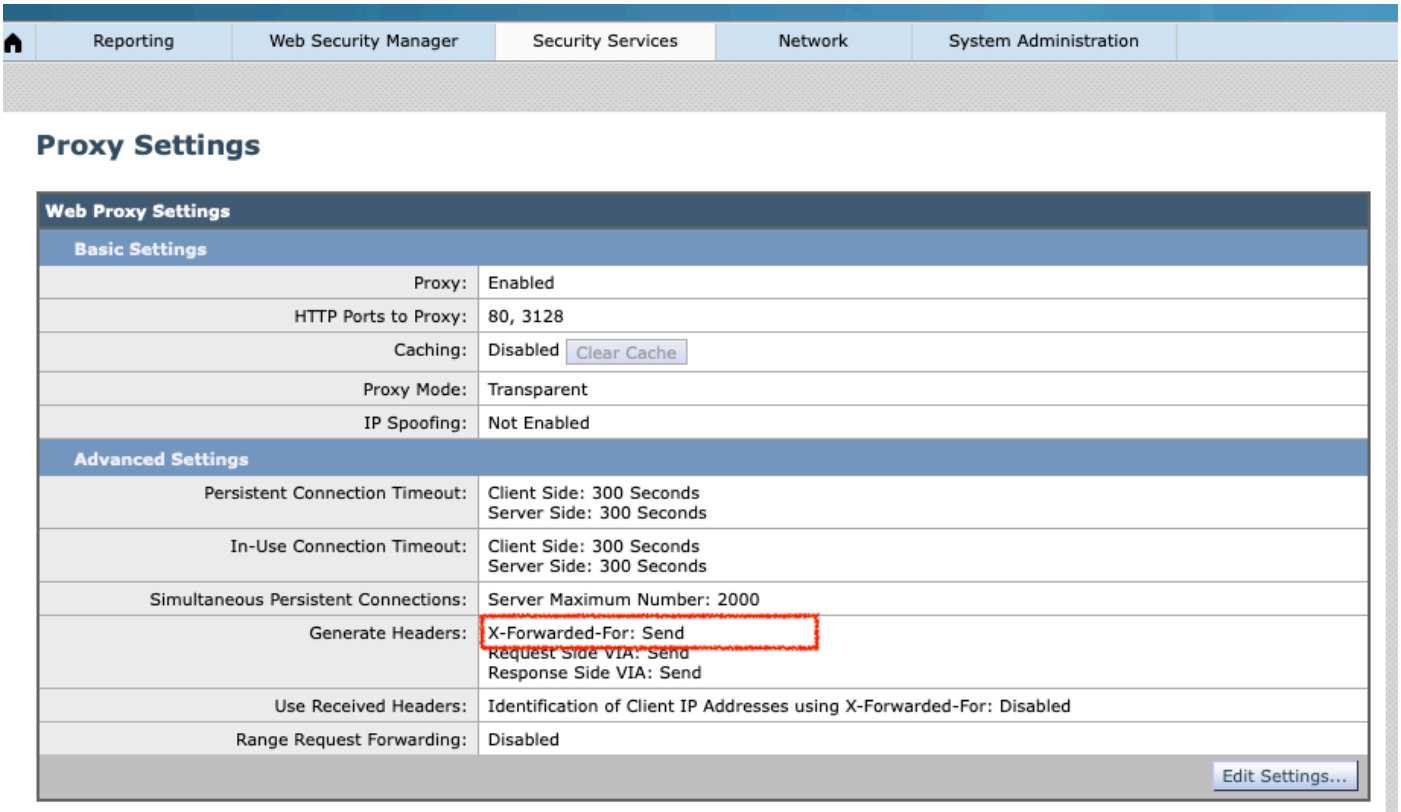
用于透明代理部署

对于透明HTTPS，AsyncOS无权访问客户端报头中的信息。因此，如果任何路由策略或标识配置文件依赖于客户端报头中的信息，AsyncOS将无法实施路由策略。

1. 透明重定向的HTTPS事务仅在以下情况下与路由策略匹配：
   - 路由策略组未定义策略成员资格条件，如URL类别、用户代理等。
   - 标识配置文件没有定义策略成员资格条件，如URL类别、用户代理等。
2. 如果任何标识配置文件或路由策略定义了自定义URL类别，则所有透明HTTPS事务都与默认路由策略组匹配。
3. 请尽可能避免使用所有标识配置文件配置路由策略，因为这样可能会导致透明HTTPS事务与默认路由策略组匹配。

1. X-Forwarded-For Header

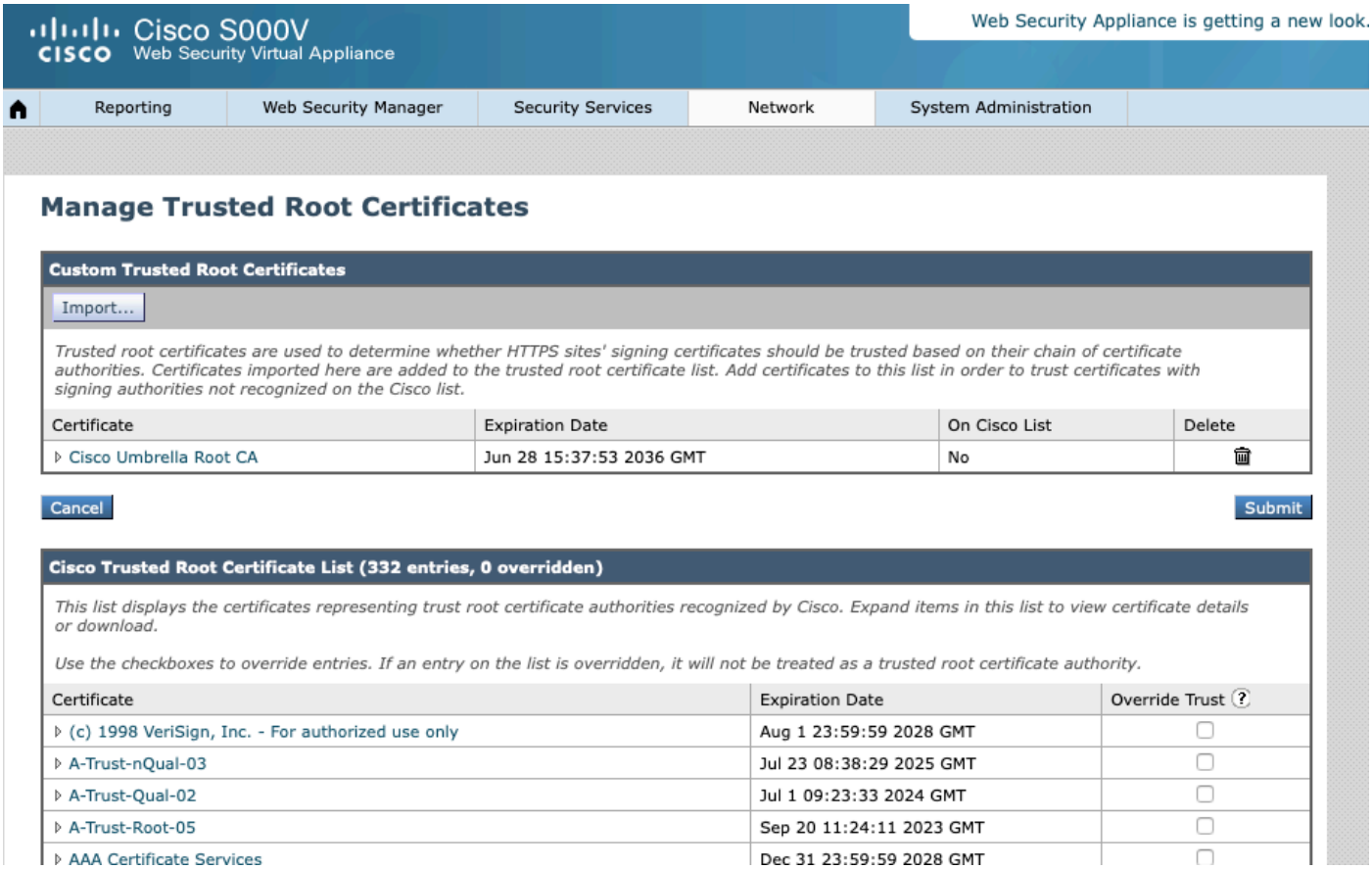
- 在SWG中实施基于IP的内部Web策略。确保通过Security Services > Proxy Settings，在安全Web设备中启用“X-Forwarded-For”信头。



360050700111

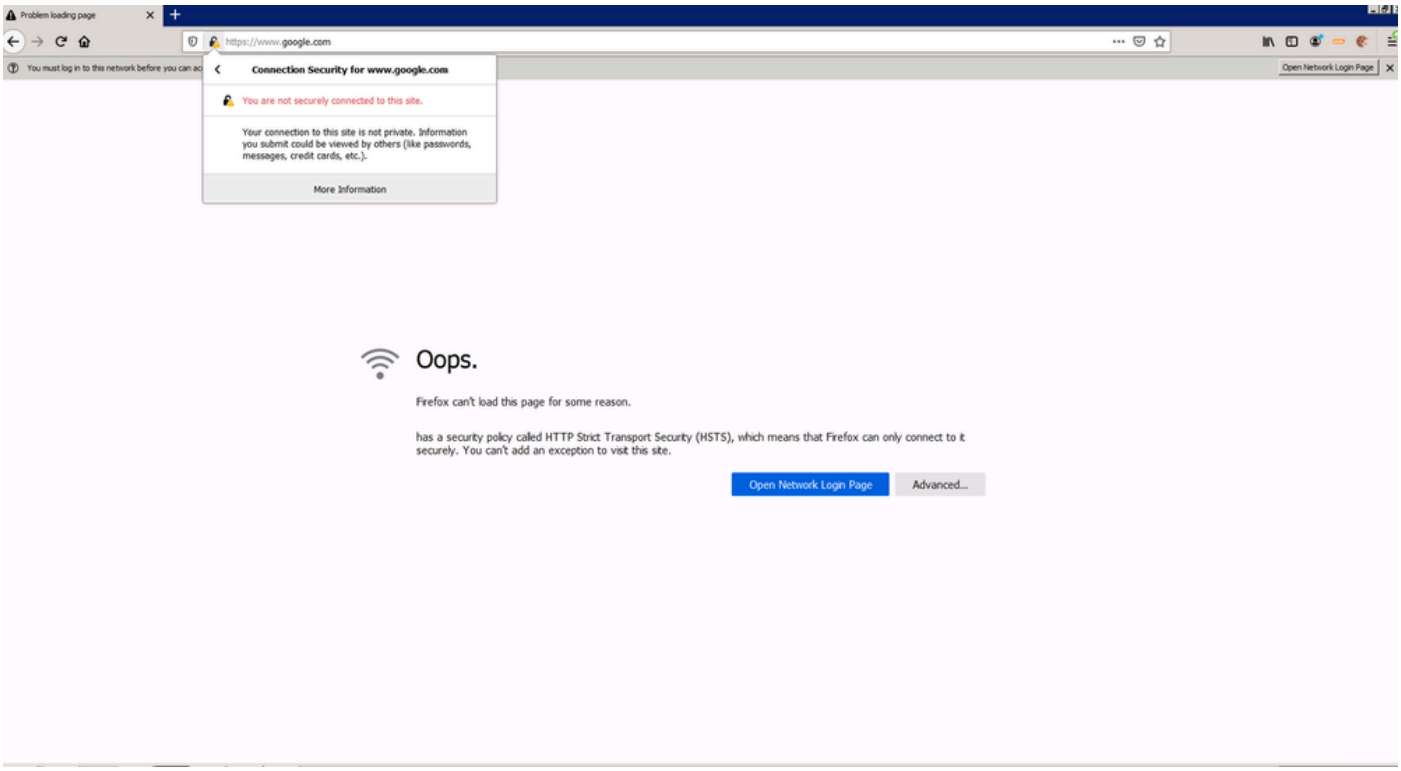
2.用于HTTP解密的受信任根证书。

- 如果在Umbrella控制面板中的Web Policy上启用HTTP解密，请从Umbrella控制面板>部署>配置下载“思科根证书”，并将其导入到安全Web设备受信任的根证书中。



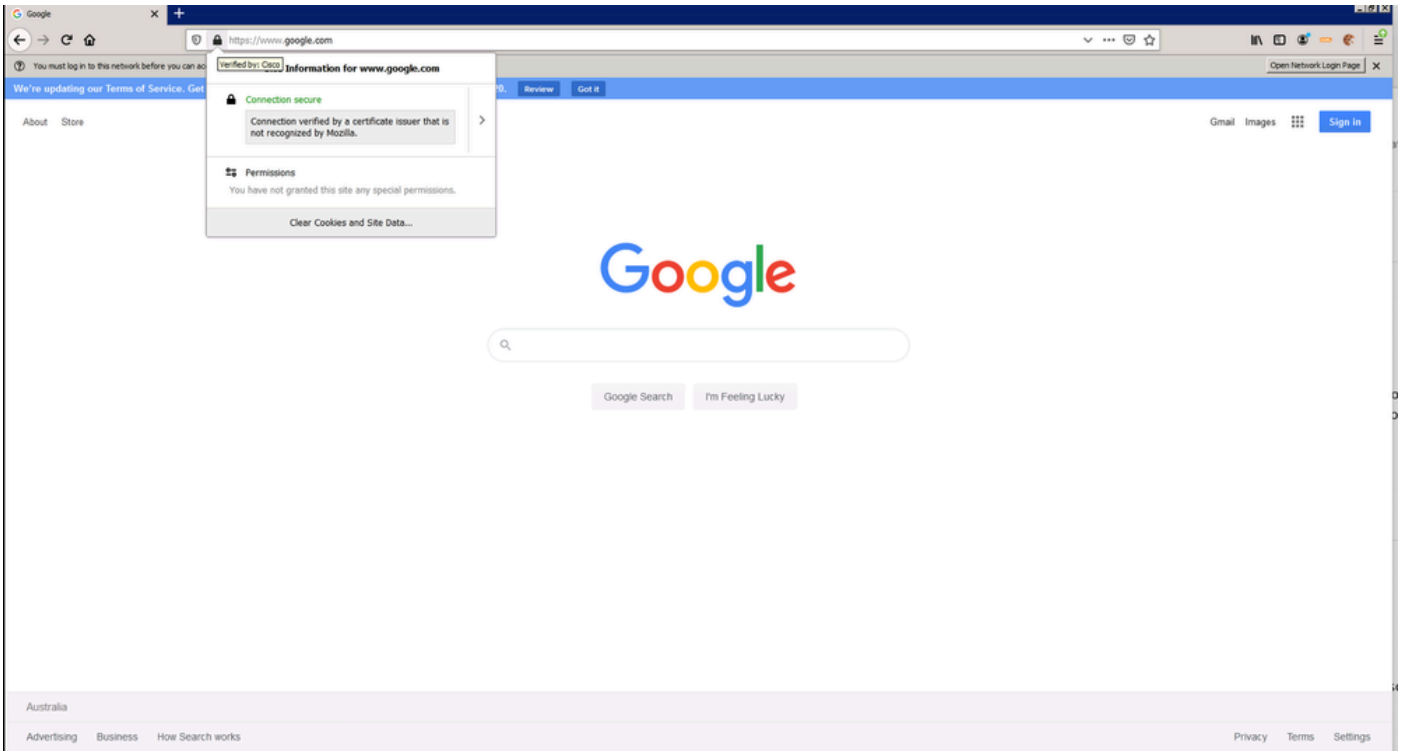
360050589612

- 如果在SWG Web策略中启用HTTP解密时尚未将“Cisco Root Certificate”导入到安全Web设备，则最终用户会收到类似于以下示例的错误：
  - “哎呀。（浏览器）由于某种原因无法加载此页面。具有称为HTTP严格传输安全(HSTS)的安全策略，这意味着（浏览器）只能安全连接到该策略。您不能添加例外来访问此站点。"
  - “您没有安全连接到此站点。”



360050700171

- 这是Umbrella SWG解密的HTTP的一个示例。证书由名为“Cisco”的“Cisco Root Certificate”验证。



360050700191

Umbrella控制面板中的SWG Web策略配置

基于内部IP的SWG Web策略：

- 确保启用安全网络设备中的“X-Forwarded-For”报头，因为SWG依靠其识别内部IP。
- 在Deployment > Networks中注册安全网络设备的出口IP。
- 在Deployment > Configuration > Internal Networks中创建客户端计算机的内部IP。请在勾选/选择“Show Networks”后选择注册安全Web设备出口IP（第1步）。
- 根据步骤2中创建的内部IP创建新的Web策略。
- 确保在Web策略中禁用了“启用SAML”选项。

基于AD用户/组的SWG网络策略：

- 确保所有AD用户和组都调配到Umbrella控制面板。
- 根据安全网络设备的已注册出口IP创建新的Web策略，并启用“启用SAML”选项。
- 根据AD用户/组创建另一个新的Web策略，禁用“启用SAML”选项。还需要将此Web策略置于第2步中创建的Web策略之前。

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）。