如何为Webex应用配置网络安全设备其他直通设置

简介

本文档介绍如何配置安全网络设备(SWA/WSA)旁路策略，以确保在特殊部署条件下具有正确的Cisco Webex应用功能。

先决条件

要求

Cisco 建议您了解以下主题：

- Async OS for Secure Web Appliance 14.x或更高版本。
- 管理用户对安全Web设备图形用户界面(GUI)的访问。
- 管理用户对Secure Web Appliance命令行界面(CLI)的访问。

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。

问题

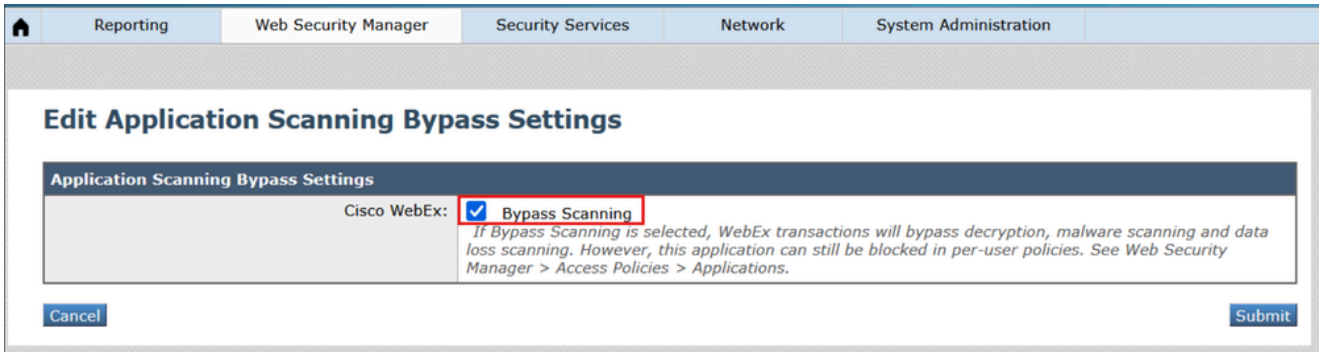
根据Webex服务的网络要求的Webex公共文档，必须将代理服务器配置为允许Webex信令流量访问文档中列出的域/URL。通过在旁路设置中启用Webex Application Bypass复选框，安全Web设备可以满足大多数环境的需求，但是，为了避免Webex应用中的服务中断，安全Web设备上可能需要一些其他配置。对于此类情况，建议执行后续步骤：

Webex应用扫描旁路

Cisco Webex：旁路扫描功能是使Webex应用流量能够通过安全网络设备而不受过滤的第一步。它应该在所有Webex桌面或移动应用用户通过安全Web设备代理网络流量的环境和部署方案中启用。

启用Webex Application Scanning Bypass的步骤：

1. 在WSA GUI中，浏览到Web Security Manager > Bypass Settings > Edit Application Bypass Settings。
2. 选中“Cisco WebEx”复选框。



1_wsa_bypass_scanning_settings

3. 提交并提交更改

启用此设置时，它不会像FQDN添加到安全网络设备的旁路列表后预期的那样绕过透明流量。相反，Webex应用流量仍然通过安全网络设备进行代理，但会通过带有决策标签“PASSTHRU_AVC”的解密过程传递该流量。 以下是访问日志中如何显示此内容的示例：

```
1761695285.658 55398 192.168.100.100 TCP_MISS/200 4046848 TCP_CONNECT 3.161.225.70:443 - DIRECT/binarie
```

独特环境的注意事项

当流量通过安全网络设备代理时，Webex应用需要额外配置才能正常工作。

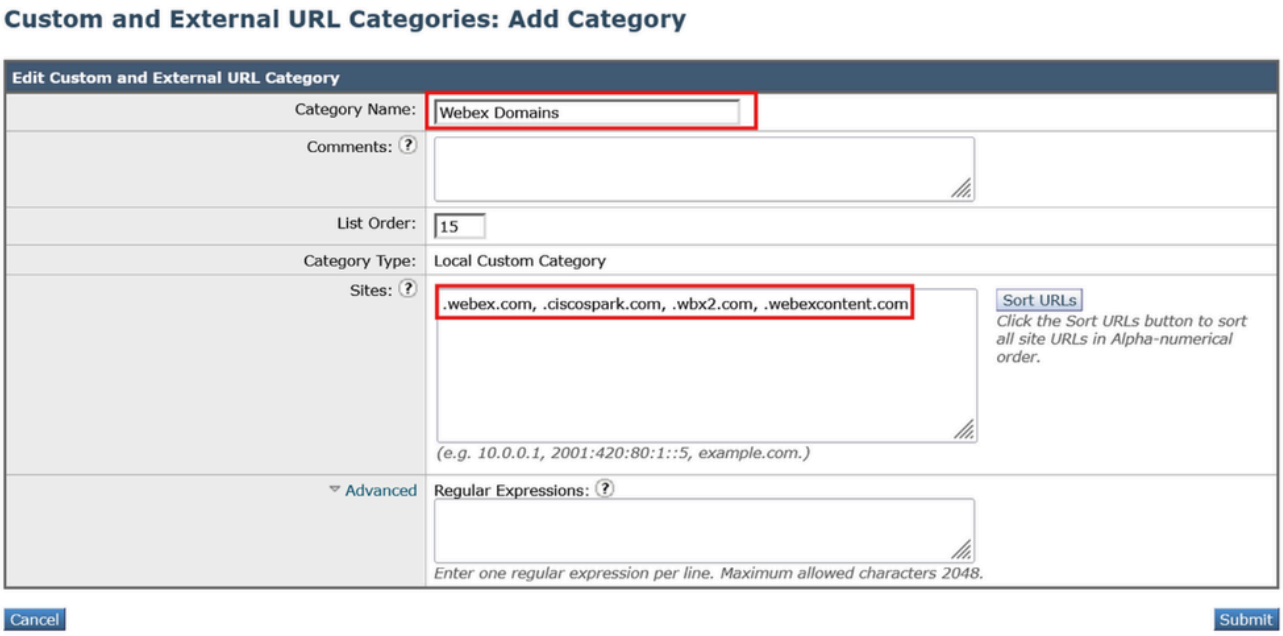
情形 1：Webex域需要免除身份验证

这在识别配置文件中未启用IP代理，并且使用透明重定向的环境中尤为明显。根据现有文档，Webex应用能够在显式定义代理的加入域的工作站上进行NTLMSSP身份验证。否则，最佳实践是为Webex域配置自定义类别并免除对其进行身份验证。

免除Webex域身份验证的步骤：

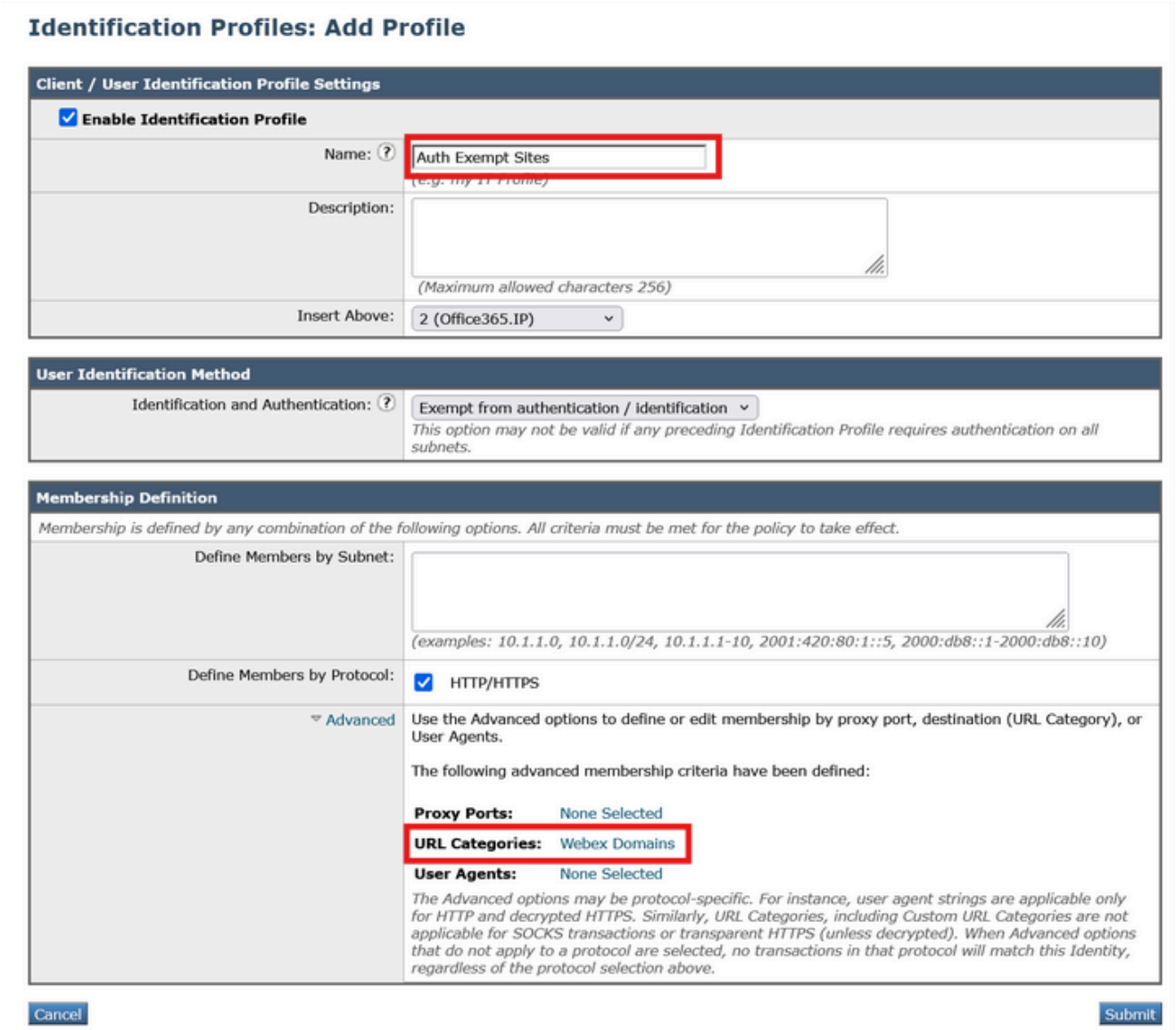
1. 在WSA GUI中，导航到Web Security Manager > Custom and External URL Categories > Add Category。
2. 为新类别命名，并将以下域放入站点部分：

```
.webex.com, .ciscospark.com, .wbx2.com, .webexcontent.com
```



2_wsa_custom_url_category

3. 单击 submit。然后导航到网络安全管理器 > 识别配置文件 > 添加识别配置文件
4. 为新配置文件命名，并在URL类别的高级部分，选择在步骤10中创建的新类#2



3_wsa_id_profile

5. 确保新配置文件中的Identification and Authentication设置为Exempt from authentication / identication
6. 提交并提交更改。

方案 2：Webex内容域不能完全用于解密绕行。

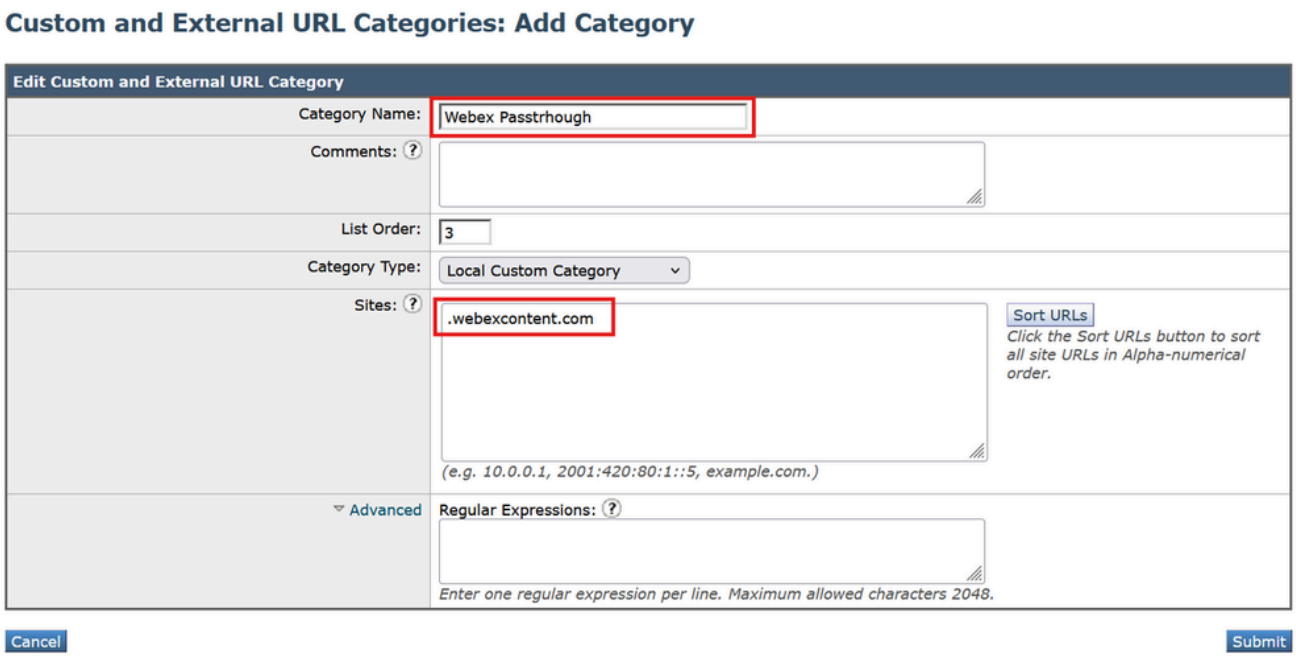
启用了Webex应用程序扫描绕行时，与webexcontent.com相关的几个子域不会在解密时自动通过。只要安全Web设备的解密证书已添加到设备的受信任根证书存储中，或者由运行Webex应用的设备已信任的内部证书颁发机构签名，Webex应用就会在解密时信任这些域提供的内容。但是，如果设备不受管理，并且安全网络设备的解密证书不受信任，则这些域应配置为在解密时通过。

当透明重定向部署已到位且重定向组正用于客户端IP欺骗的多个SWA时，可以配置流量以基于目标IP重定向到安全Web设备，同样，来自Web服务器的返回流量配置为基于源地址通过安全Web设备重新定向。当安全Web设备配置为使用它使用DNS查找解析的IP连接到Web服务器时，返回流量可能会被无意重定向到其他安全Web设备，随后被丢弃。由于在Web服务器上使用轮换IP地址，此问题不仅影响到Webex，还会影响其他视频流应用。

为所有Webex域配置解密直通的步骤：

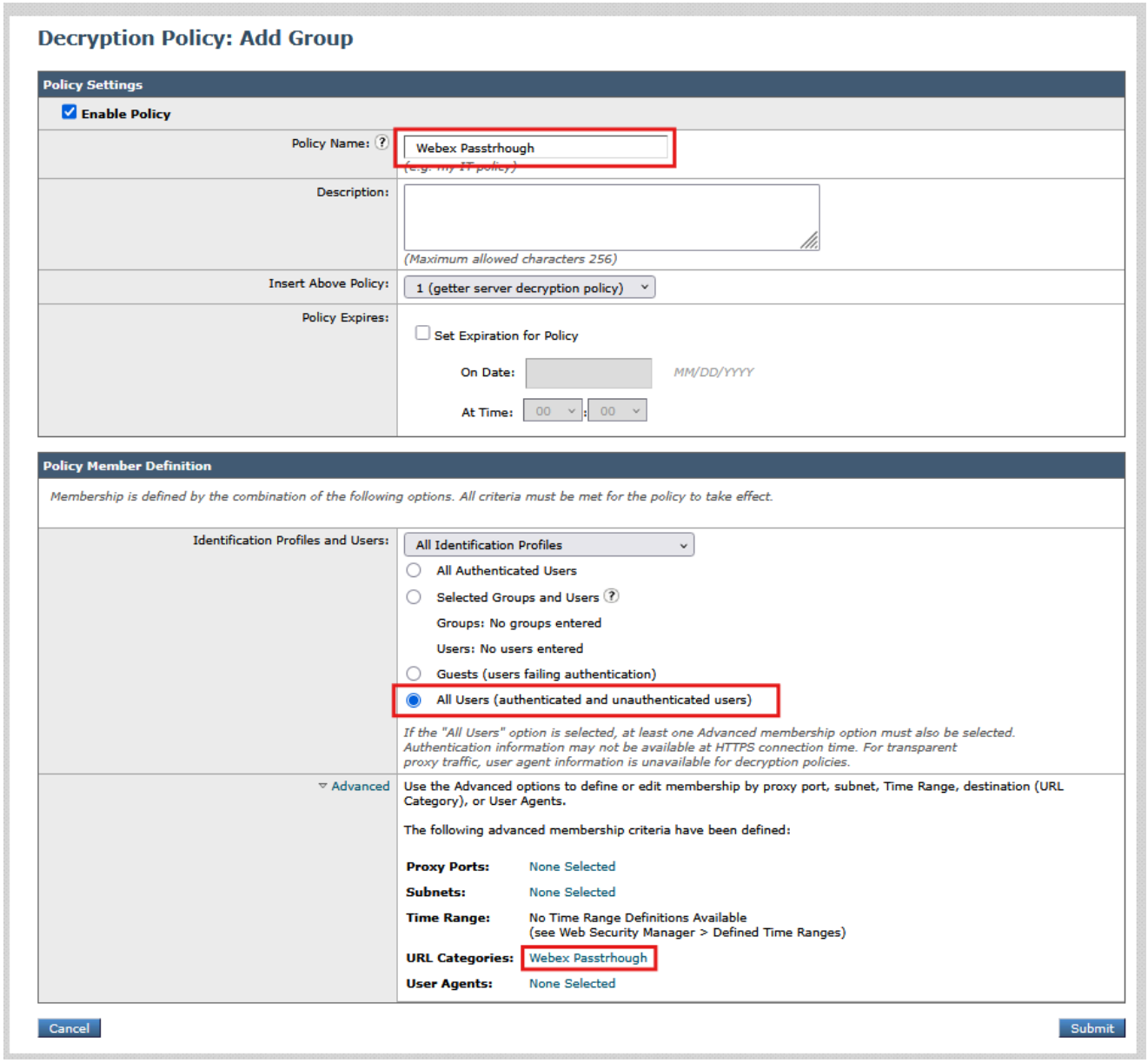
1. 确保按照上述说明启用Webex Application Scanning Bypass。
2. 在WSA GUI中，导航到Web Security Manager > Custom and External URL Categories > Add Category。
3. 为新类别命名，并将下一个域放在站点部分：

```
.webexcontent.com
```



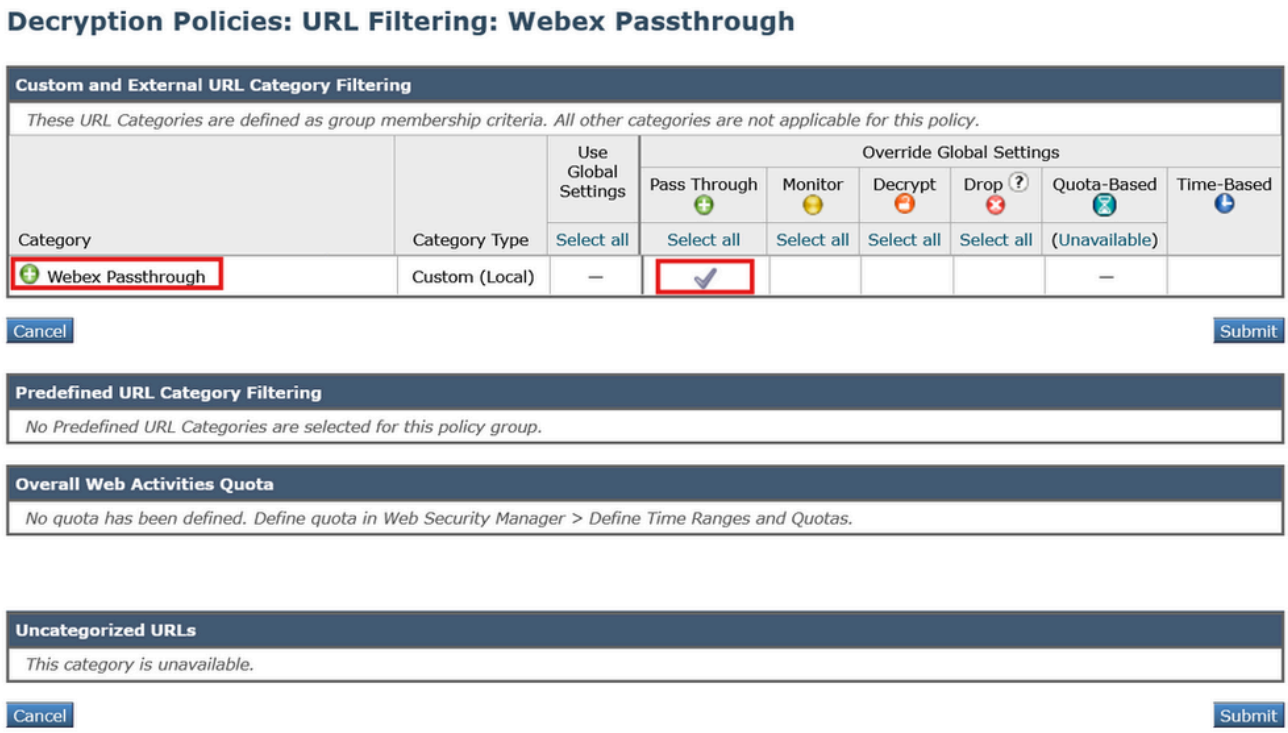
4_wsa_url_category

4. 单击 submit。现在，导航到Web Security Manager > Decryption Policies > Add Policy
5. 将新策略命名为，将Identification Profiles and Users设置为All Users，并在URL Categories的Advanced部分中选择在步骤100中创建的新类#3



5_wsa_decryption_policy

6. 单击 submit。然后，点击URL Filtering部分，将在步骤#3创建的自定义类别设置为“Pass Through”。



6_wsa_url_filtering

7. 提交并提交更改。

如果部署了多个安全网络设备以实现透明重定向，并且启用了客户端IP欺骗，则有两种解决方案：

1. 将传出和返回WCCP服务设置为根据客户端地址而不是服务器地址进行负载均衡。
2. 在WSA CLI中，将advancedproxyconfig > DNS > "Find web server by"设置为在与Web服务器的连接上始终使用客户端提供的IP地址（选项2和3）。 有关此设置的详细信息，请参阅使用安全Web设备最佳实践指南的DNS部分。

确认

直通设置完成后，Webex流量将在访问日志中根据策略处理为通过：

```
1763752739.797 457 192.168.100.100 TCP_MISS/200 6939 TCP_CONNECT 135.84.171.165:443 - DIRECT/da3-wxt08-
1763752853.942 109739 192.168.100.100 TCP_MISS/200 7709 TCP_CONNECT 170.72.245.220:443 - DIRECT/avatar-
1763752862.299 109943 192.168.100.100 TCP_MISS/200 8757 TCP_CONNECT 18.225.2.59:443 - DIRECT/highlights
1763752870.293 109949 192.168.100.100 TCP_MISS/200 8392 TCP_CONNECT 170.72.245.190:443 - DIRECT/retenti
```

查看和监控webex应用，如果报告任何缓慢或服务中断，请再次查看访问日志并验证所有webex端流量是否正确处理。

相关信息

- Webex服务的网络要求

- 使用安全Web设备最佳实践

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）。