排除Umbrella中的非浏览器应用程序故障

目录

简介

本文档介绍如何对Cisco Umbrella中的非浏览器应用程序进行故障排除。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Umbrella。

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。

概述

本文解释配置非浏览器应用程序以与Umbrella安全Web网关配合使用的最佳实践和故障排除步骤。在大多数情况下，不需要更改配置。但是，某些应用程序在安全/检查功能（如SSL解密）上无法正常工作，必须添加例外情况才能使应用程序通过Web代理运行。这适用于Umbrella SWG及其他Web代理解决方案。

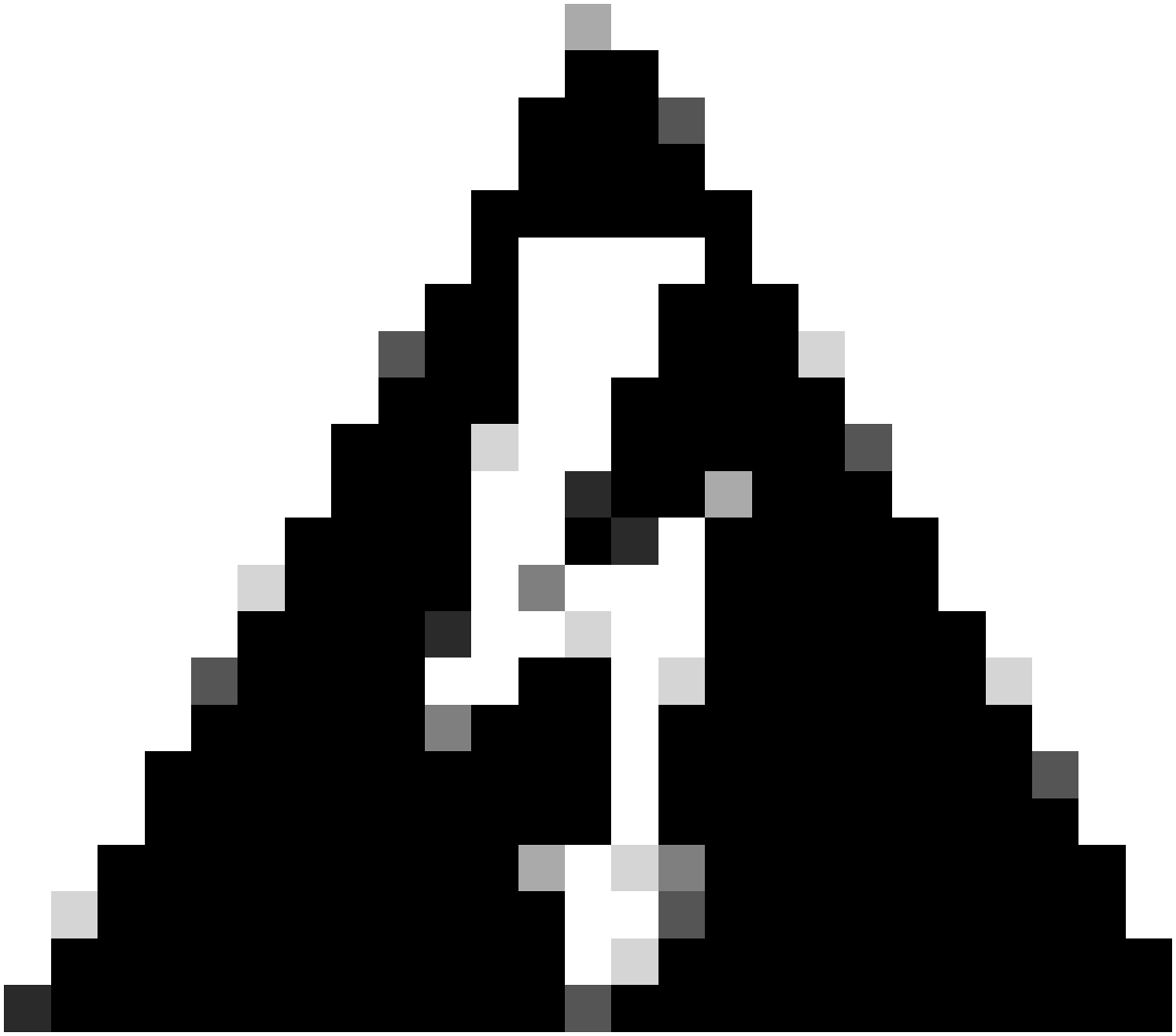
这在应用程序的网站/浏览器版本工作但应用程序的桌面/移动版本不起作用的情况下很有用。

兼容性问题

应用可能由于以下原因不兼容：

Umbrella根CA安装	Cisco Umbrella根CA必须始终受信任，才能进行无错TLS连接。 • 解决方案：对于非Web应用，请确保Cisco Umbrella Root CA在系统/本地计算机证书存储中受信任。
证书固定	证书固定(PKP)是应用程序期望接收精确的枝叶（或CA证书）以验证TLS握手。 应用程序无法接受Web代理生成的证书，并且与SSL解密功能不兼容。 • 解决方案：使用选择性解密列表绕过SSL解密中的应用程序或域(请参阅表后的警告) 有关已知受证书固定影响的应用的详细信息，请点击此处： 公钥绑定/证书绑定
TLS版本支持	应用可以使用旧的TLS版本/密码，出于安全原因，SWG不支持该版本/密码。 • 解决方案：使用External Domains功能(PAC/AnyConnect)或VPN例外项（隧道）绕过发送到Umbrella的流量(请参阅表后的警告)。
非Web协议	某些应用程序使用非http(s)协议，但仍通过由SWG拦截的常见Web端口发送此数据。SWG无法理解此流量。 • 解决方案：请咨询应用供应商，确定软件使用的目标地址/IP范围。 需要使用外部域(PAC/AnyConnect)或VPN排除（隧道）将此软件从SWG中排除(请参阅表后的警告)。
SAML身份验证	大多数非浏览器应用程序无法执行SAML身份验证。 Umbrella不会对SAML的非浏览器应用提出质询，因此基于用户/组的过滤策略无法匹配。 • 解决方案： 启用IP Surrogates功能，以便可以缓存用户信息以用于非浏览器应用程序。 • 备选: 根据网络或隧道身份（非用户/组）在Web规则中允许应用/域。
HTTP范围请求	有些应用程序在下载数据时使用HTTP“Byte-Range”请求；意味着一次只能下载一小部分文件。由于安全原因，在SWG中禁用这些请求，因为此方法也可用于绕过防病毒检测。 • 解决方案(HTTPS):使用选择性解密列表绕过Umbrella中SSL Decryption*的应用或域。 • 解决方案(HTTP): 使用带有Override Security选项的Web规则，绕过来自防病毒

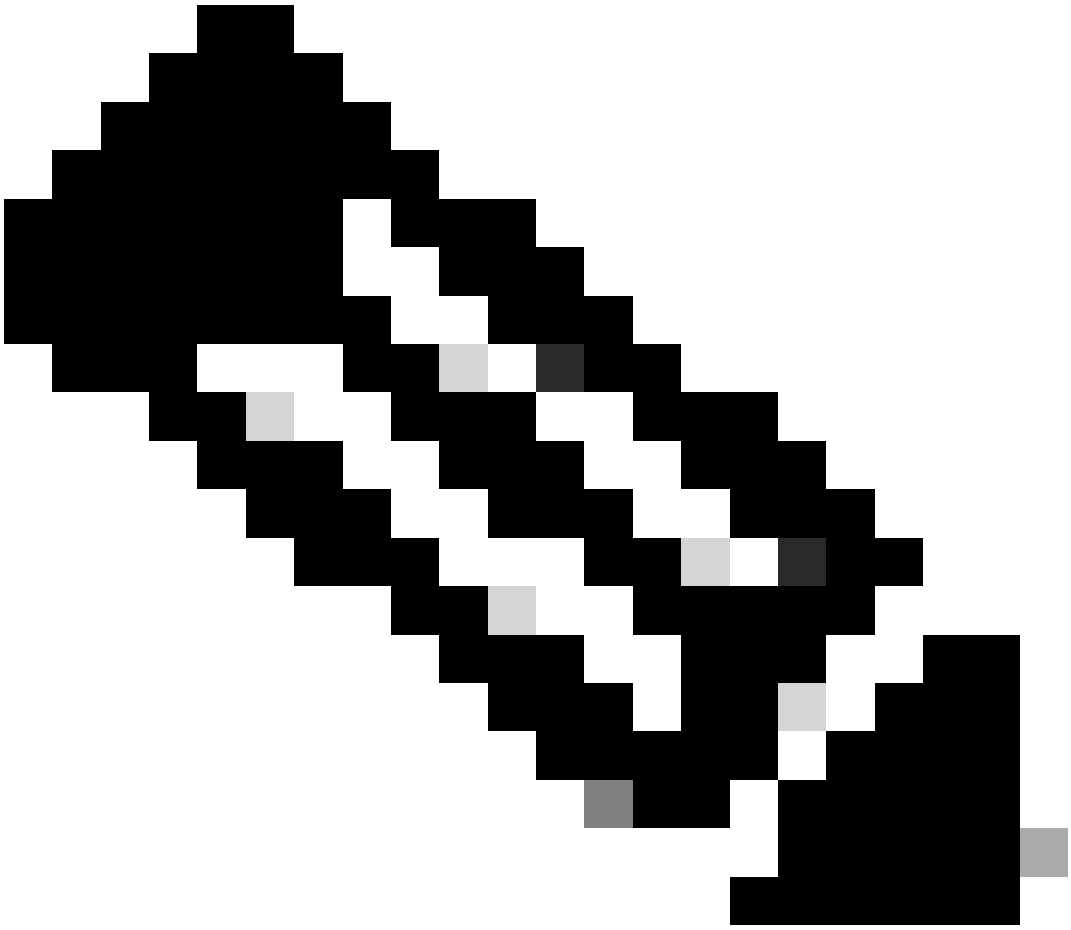
	扫描*的应用或域。 • 备选: 如果您希望为您的组织默认启用*范围请求，请与Umbrella支持联系。
显式代理兼容性	某些应用程序不考虑系统代理设置(例如PAC文件)，通常与显式Web代理不兼容。在PAC文件部署中，这些应用不会通过Umbrella SWG路由。 • 解决方案：必须通过本地网络防火墙允许该应用。 有关允许的目标/端口的详细信息，请咨询应用供应商。



警告：创建这些例外可禁用安全检测功能，包括防病毒扫描、DLP扫描、租户控制、文件类型控制和URL检测。 只有当您乐意信任这些文件的来源时才执行此操作。必须权衡应用的业务需求与禁用这些功能的安全影响。

Microsoft 365应用

Microsoft 365兼容性功能自动将许多Microsoft域从SSL解密和策略实施功能中排除。可以启用此功能以解决桌面版本的Microsoft应用的问题。 有关详细信息，请参阅管理全局设置。

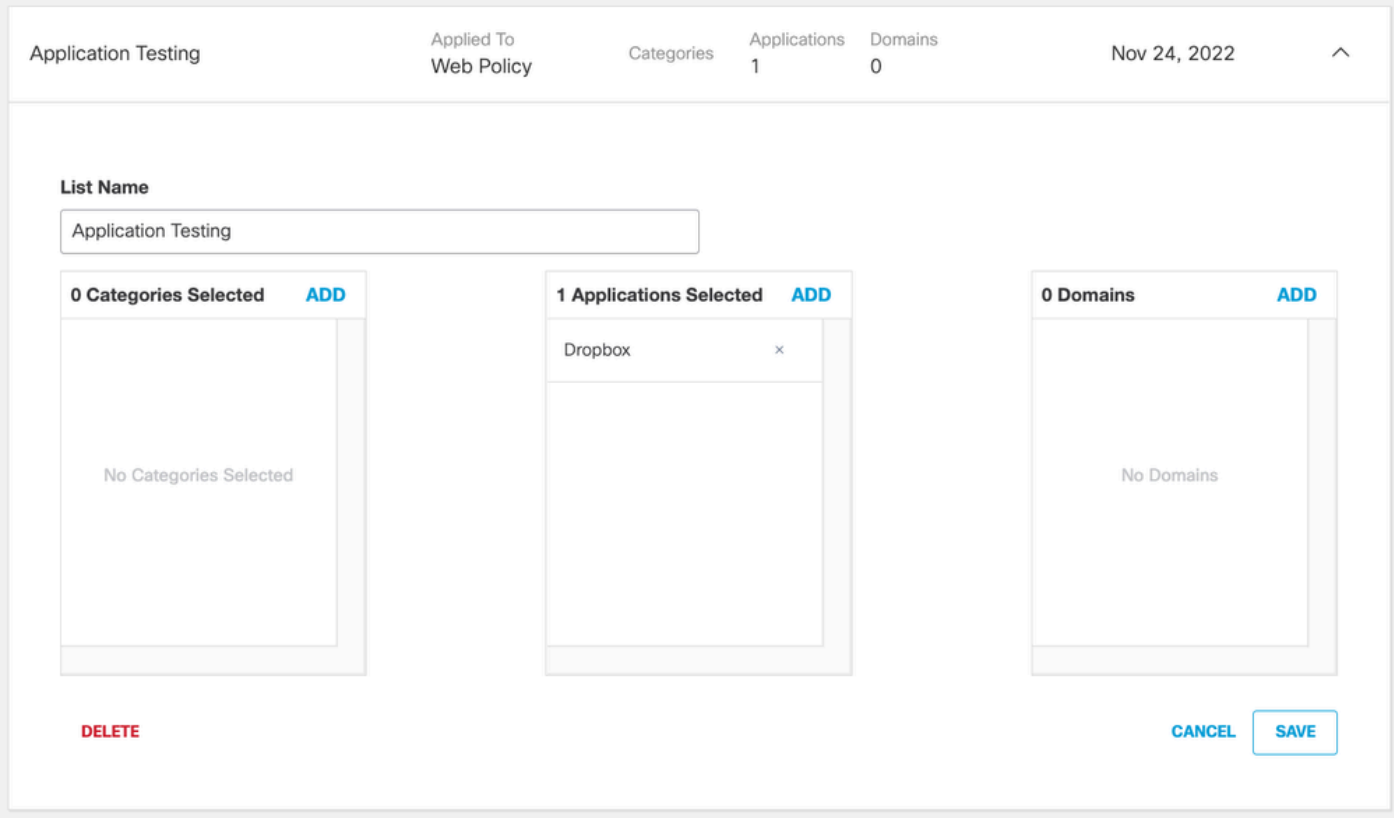


注意：Microsoft 365兼容性功能不排除所有Microsoft域。 Umbrella使用Microsoft对必须从过滤中排除的域列表的建议。有关详细信息，请参阅新的Office365终端类别。

证书固定绕行

证书锁定(PKP)是应用兼容性问题的常见原因。 思科提供可配置为绕过SSL解密解决方法的已命名应用的综合列表。可以在Policies > Selective Decryption Lists中配置选择性解密。

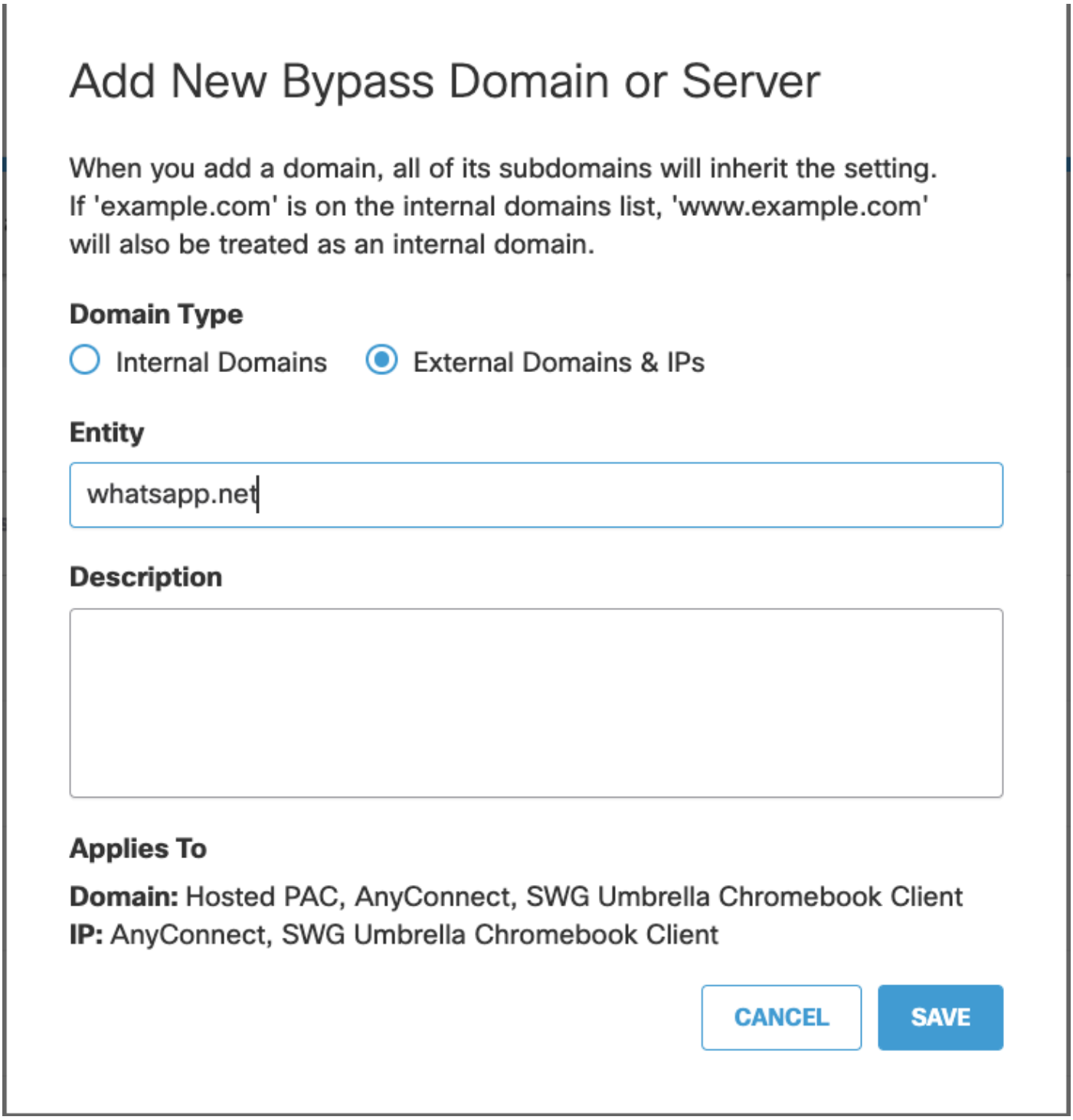
在大多数情况下，管理员只需通过按应用名称排除应用即可解决证书固定问题。这意味着无需学习或维护域列表即可解决这些问题。



或者，可以根据目标域/IP地址绕过应用。联系应用供应商，确定适用的域/IP列表，或参阅识别证书绑定的例外项。

TLS兼容性绕行

传统或自定义TLS版本是应用兼容性问题的常见原因。这些问题可以通过在部署>域管理>外部域和IP中排除来自Umbrella的流量来解决。在隧道部署中，只能通过在VPN配置中添加例外来排除该流量。



与应用程序供应商联系，确定要排除的域/IP的适用列表，或查看“识别不兼容TLS版本的排除项”（本文稍后部分）。

故障排除（高级）

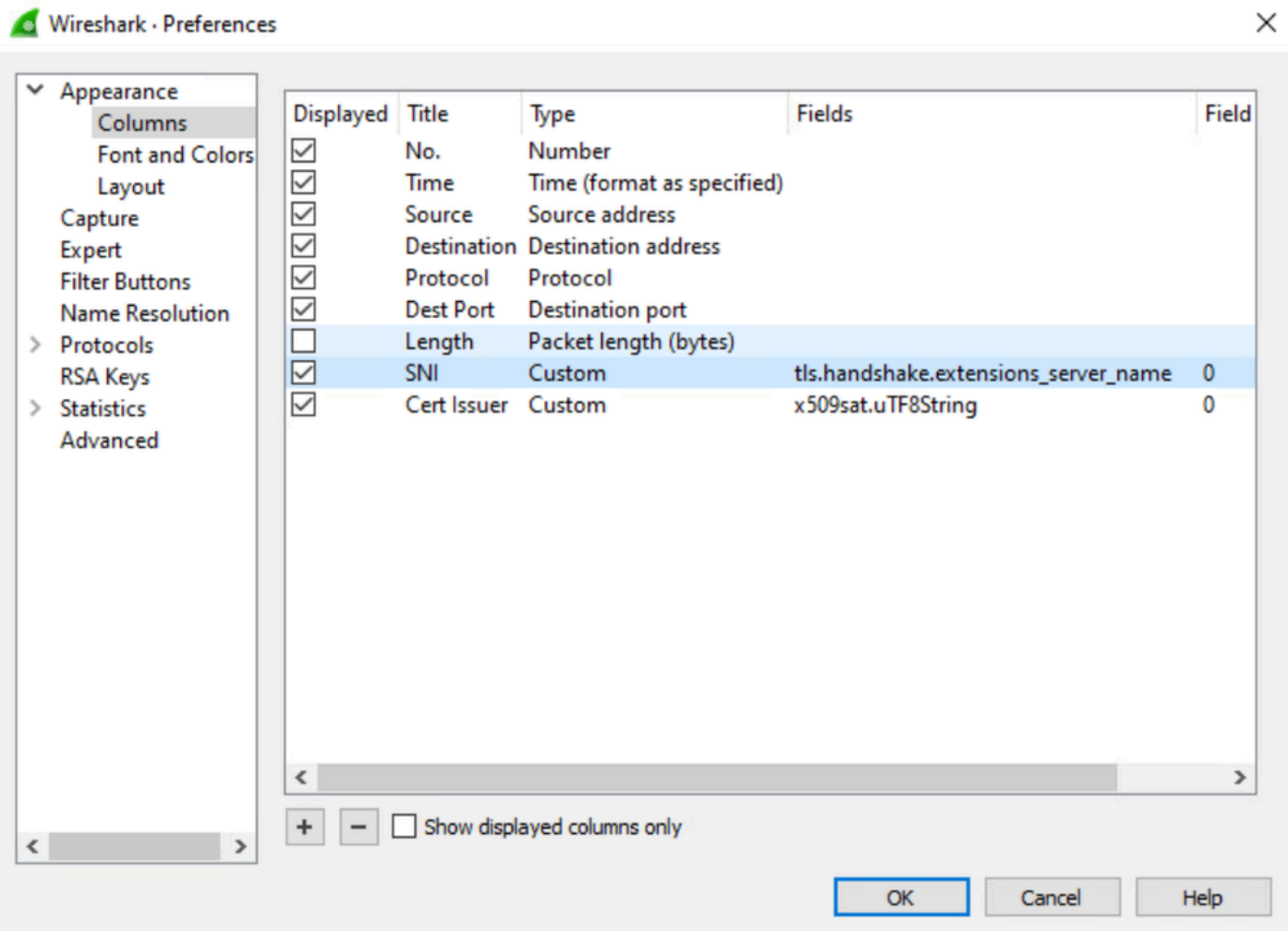
本文中的其余说明使用Wireshark(www.wireshark.org)数据包捕获进行故障排除。Wireshark可帮助确定应用程序使用哪些域来帮助实施自定义排除。开始之前，请在Wireshark中添加以下自定义列：

1.从www.wireshark.org下载Wireshark。

2.转至编辑>首选项>列。

3.使用以下字段创建Custom类型的列：

```
http.host
tls.handshake.extensions_server_name
x509sat.uTF8String
```



要执行数据包捕获，请完成以下说明或参阅使用Wireshark捕获网络流量。

1.以管理员身份运行Wireshark。

2.在Capture > Options中选择相关的网络接口。

- 对于PAC/隧道部署，在正常的LAN网络接口上捕获。
- 对于AnyConnect部署，捕获您的LAN网络接口和环回接口。

3.关闭除问题应用程序之外的所有其他应用程序。

4.刷新DNS缓存：`ipconfig /flushdns`

5.开始Wireshark捕获。

6.快速复制问题并停止Wireshark捕获。

识别证书绑定的例外项

在客户端上实施证书固定，这意味着每个应用的确切行为和解决步骤各不相同。在capture（捕获）输出中，查找TLS连接发生故障的迹象：

- TLS连接正在快速关闭或重置（RST或FIN）。
- 正在重复重试TLS连接。
- TLS连接的证书由Cisco Umbrella颁发，因此正在被解密。

以下示例Wireshark过滤器可帮助查看TLS连接的重要详细信息。

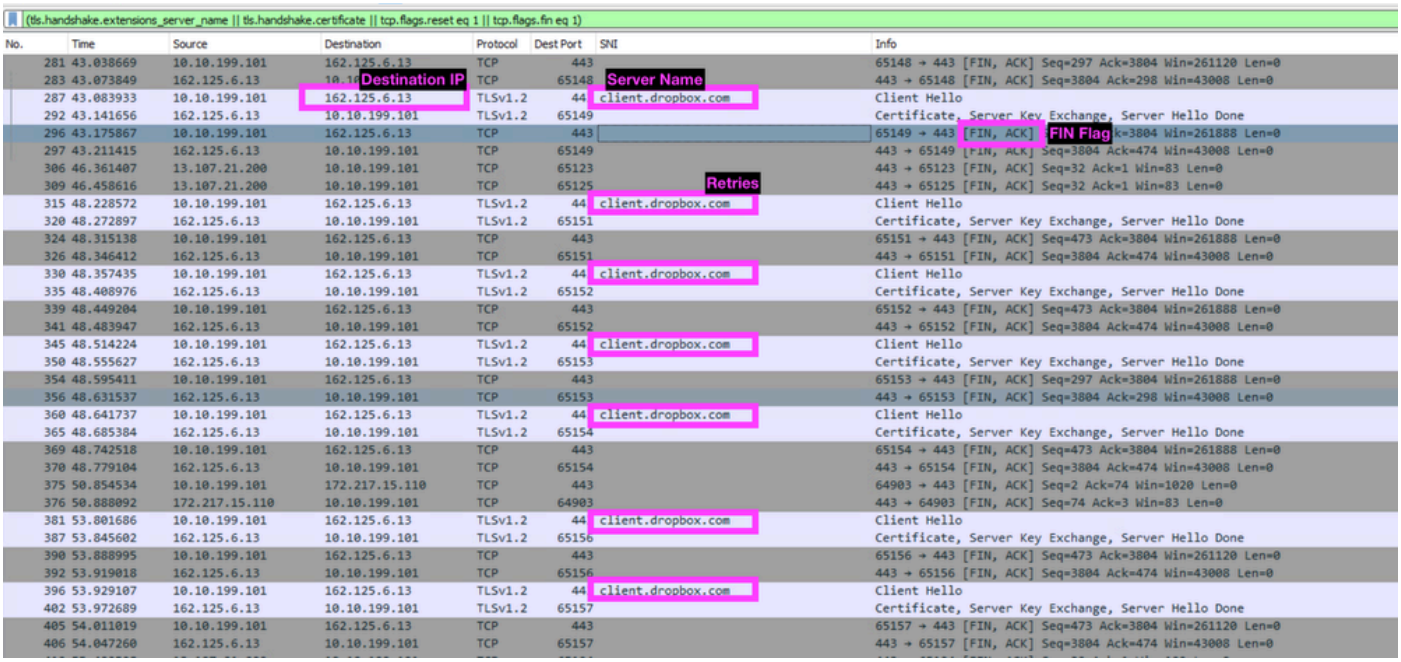
隧道/AnyConnect

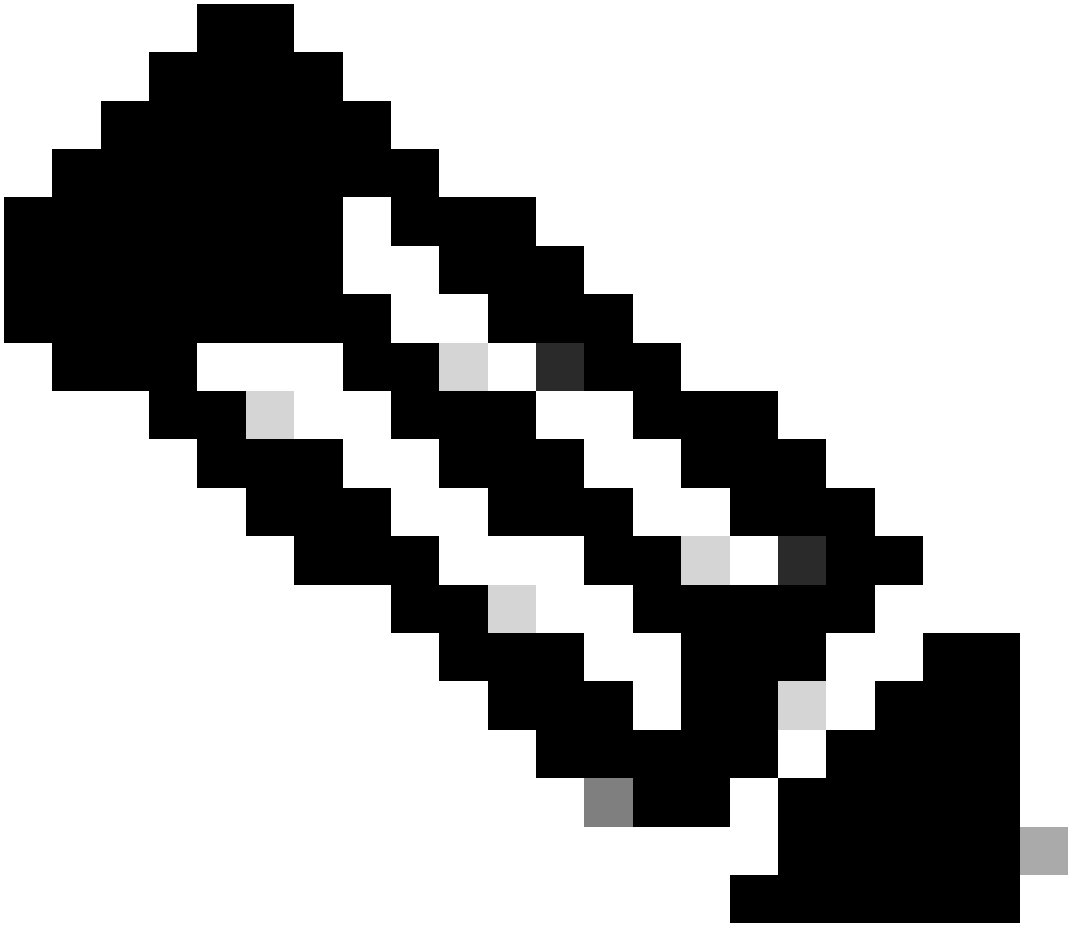
```
tcp.port eq 443 && (tls.handshake.extensions_server_name || tls.handshake.certificate || tcp.flags.rese
```

PAC/代理链

```
tcp.port eq 443 && (http.request.method eq CONNECT || tcp.flags.reset eq 1)
```

在本示例中，DropBox桌面应用程序在尝试连接到client.dropbox.com时受证书固定影响。





注意：添加必要的排除项后，您可以多次重复这些步骤，以确定应用程序使用的所有目标。

识别不兼容的TLS版本的例外项

查找不使用Umbrella SWG支持的强制TLS1.2+协议的SSL/TLS连接。这可以包括传统协议（TLS1.0或更早版本）或应用实施的定制协议。

此示例过滤器显示初始TLS握手数据包以及DNS查询。

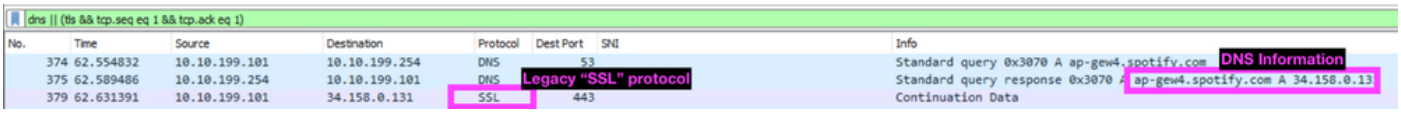
隧道/AnyConnect

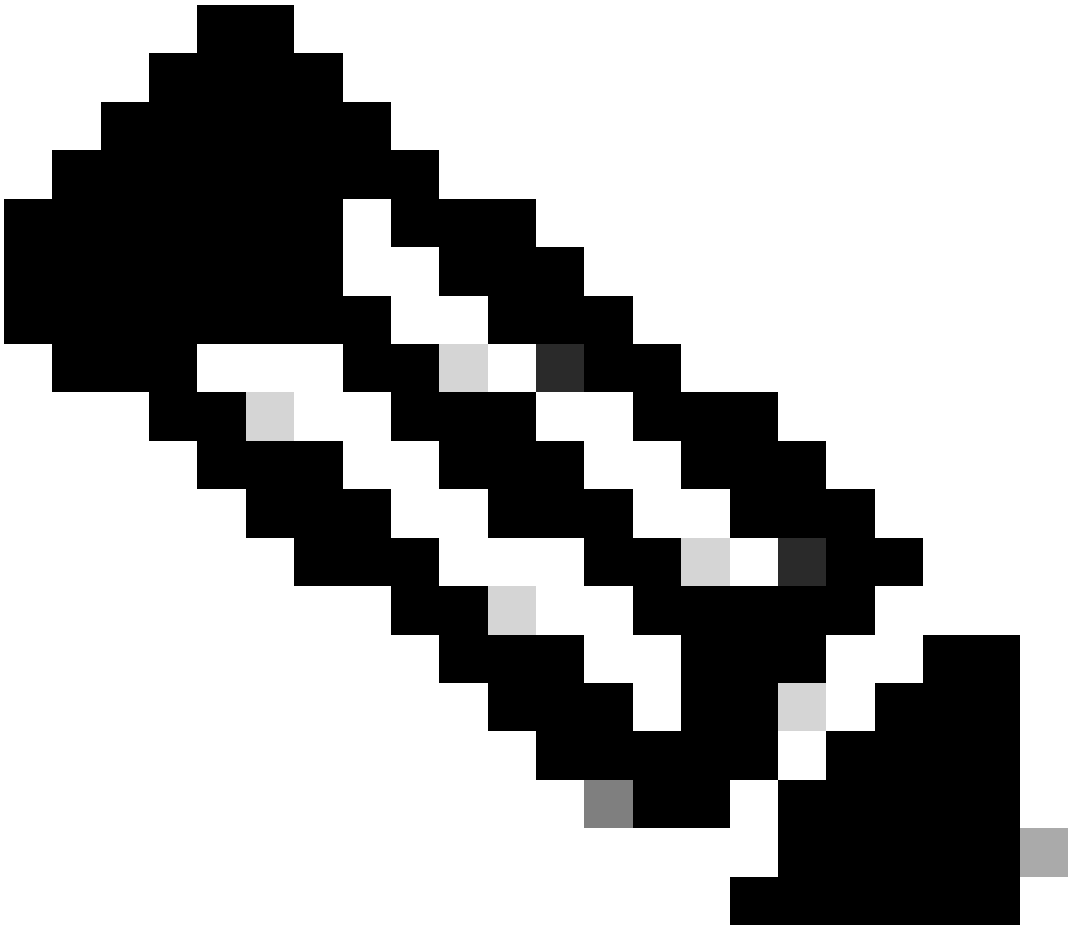
```
dns || (tls && tcp.seq eq 1 && tcp.ack eq 1)
```

PAC/代理链

```
dns || http.request.method eq CONNECT
```

在本示例中，Spotify桌面应用程序正在尝试使用非标准或传统“SSL”协议（无法通过SWG发送）连接到ap-gew4.spotify.com。





注意：添加必要的排除项后，您可以多次重复这些步骤，以确定应用程序使用的所有目标。

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）。