管理Umbrella漫游客户端和VPN兼容性

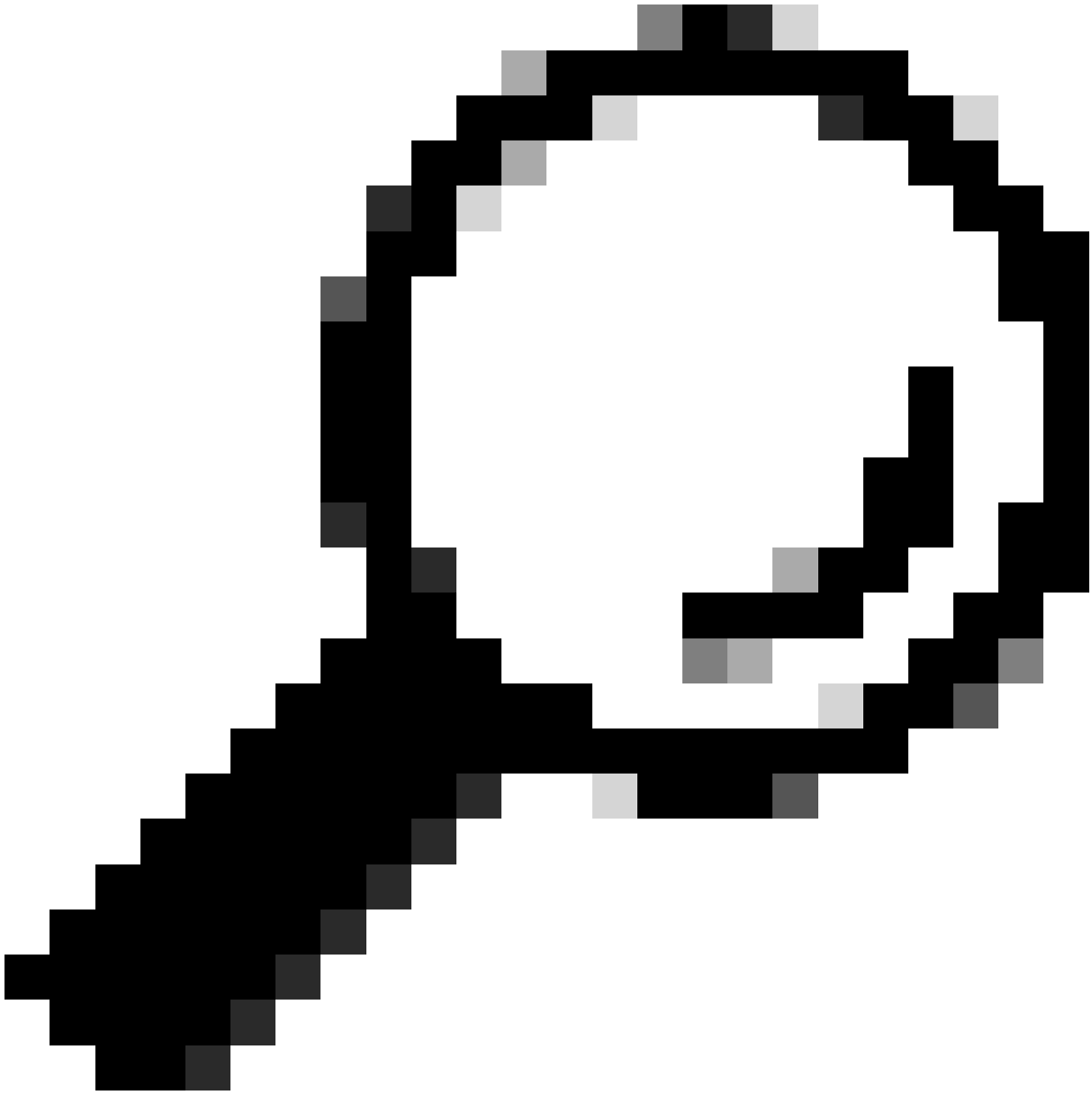
目录

简介

本文档介绍Cisco Umbrella漫游客户端与各种VPN软件的交互和兼容性。

概述

Cisco Umbrella Roaming Client可与大多数VPN软件配合使用，但可能需要执行其他步骤才能进行预期操作。Cisco Umbrella建议部署Cisco安全客户端和漫游安全模块，以实现最大兼容性。此模块可以不使用VPN组件进行部署。



提示：本文档可用作一般指导，并不作为受支持软件的正式列表。Cisco Umbrella不测试、验证或验证任何第三方软件或VPN客户端的功能。

本文档为可能需要进一步配置的特定VPN客户端提供了技术信息和其他情景。有关已知不兼容的VPN软件的列表，请参阅Umbrella漫游客户端不兼容部分。DNS与漫游客户端的不兼容也会导致带SWG的Cisco安全客户端+漫游安全模块出现故障，因为SWG客户端还依赖于成功建立DNS连接。

Umbrella漫游客户端如何与VPN客户端配合运行

Umbrella漫游客户端绑定到所有网络适配器，并将计算机上的DNS设置更改为127.0.0.1(localhost)。 这允许Umbrella漫游客户端将所有DNS查询直接转发到Umbrella，同时允许通过内部域功能解析本地域。在建立与VPN服务器的连接时，Umbrella漫游客户端在系统中检测到新的网络连接，并将连接DNS设置更改为指向Umbrella漫游客户端。Umbrella漫游客户端依靠对

Umbrella AnyCast DNS IP地址(208.67.222.222/208.67.220.220)执行DNS查找。

如果用户连接到VPN，则与VPN关联的防火墙必须允许访问Umbrella。

Umbrella漫游客户端不兼容

Umbrella漫游客户端当前提供DNS层实施。DNS层是漫游客户端的主要功能，可在任何网络上应用基于DNS的安全策略。漫游客户端的此功能可能会遇到已知的软件不兼容。根据支持团队的测试，Umbrella漫游客户端的DNS层与下面列出的客户端不兼容。Cisco Umbrella Engineering不验证或测试这些客户端，所有条目都要进行检查。本文参考独立式Umbrella漫游客户端。有关适用于Cisco安全客户端（和旧版）的Umbrella漫游安全模块的配套文章，请参阅相关文档。

VPN 客户	问题/不兼容	分辨率
Pulse Secure	在断开连接时，由于VPN连接期间的Pulse修改，保存的本地DNS可以保留VPN值而不是WiFi/以太网值。	通过Umbrella模块解决 — 包含在大多数许可证中。
Avaya VPN	不兼容。	通过Umbrella模块解决 — 包含在大多数许可证中。
Windows VPN（尤其是始终在VPN上）	可能导致本地DNS无法解析为内部答案，尽管DNS主机名在内部域列表中。	通过Umbrella模块解决 — 包含在大多数许可证中。
基于Windows通用平台构建的VPN“应用”	这些应用必须使用Microsoft连接API，该API要求将DNS发送到本地网卡，而不是127.0.0.1。因此，应用显示错误，指示其无法连接。	通过Umbrella模块解决 — 包含在大多数许可证中。
OpenVPN	不兼容。	没有可用的修补程序。
Palo Alto GlobalProtect VPN	3.0.110之后的任何独立漫游客户端版本都无法使用。	使用Umbrella模块修复 — 包含在大多数许可证中。
F5 VPN	不兼容。	由Umbrella模块修复 — 包含在大多数许可证中。
检查点VPN	仅限MacOS，仅限拆分隧道模式。	在macOS上禁用拆分隧道。
SonicWall	不兼容。	由Umbrella模块修复 — 包含在大多数

VPN 客户	问题/不兼容	分辨率
NetExtender		许可证中。
Zscaler VPN	不兼容。	由Umbrella模块修复 — 包含在大多数许可证中。
Akamai终端保护(ETPclient)	不兼容。	由Umbrella模块修复 — 包含在大多数许可证中。
NordVPN	使用解决方法。	有两个选项可用于添加兼容性： 1. 使用OpenVPN连接方法，如如何使用OpenVPN在Windows上设置手动连接 2. 在Advanced设置下允许自定义DNS。将DNS设置为208.67.220.220和208.67.222.222。
Azure VPN	不兼容。	由Umbrella模块修复 — 包含在大多数许可证中。
AWS VPN	使用解决方法。	编辑配置文件（手动从AWS下载），使其具有第二行pull-filter ignore "block-outside-dns"。
基本VPN	不兼容。	由Umbrella模块修复 — 包含在大多数许可证中。

VPN客户端不兼容的原因

某些VPN客户端的DNS行为类似于Umbrella漫游客户端。如果VPN连接DNS服务器更改为意外值，则VPN软件会将系统DNS设置更改回最初连接时设置的VPN值。Umbrella漫游客户端也执行相同的操作，将任何DNS服务器改回127.0.0.1。这种反复的行为在VPN和Umbrella漫游客户端之间造成冲突。此冲突会导致VPN连接重置的DNS服务器循环无尽。漫游客户端检测到此情况并禁用自身以维护VPN连接（如果可能）。

虚拟设备和受保护的网络

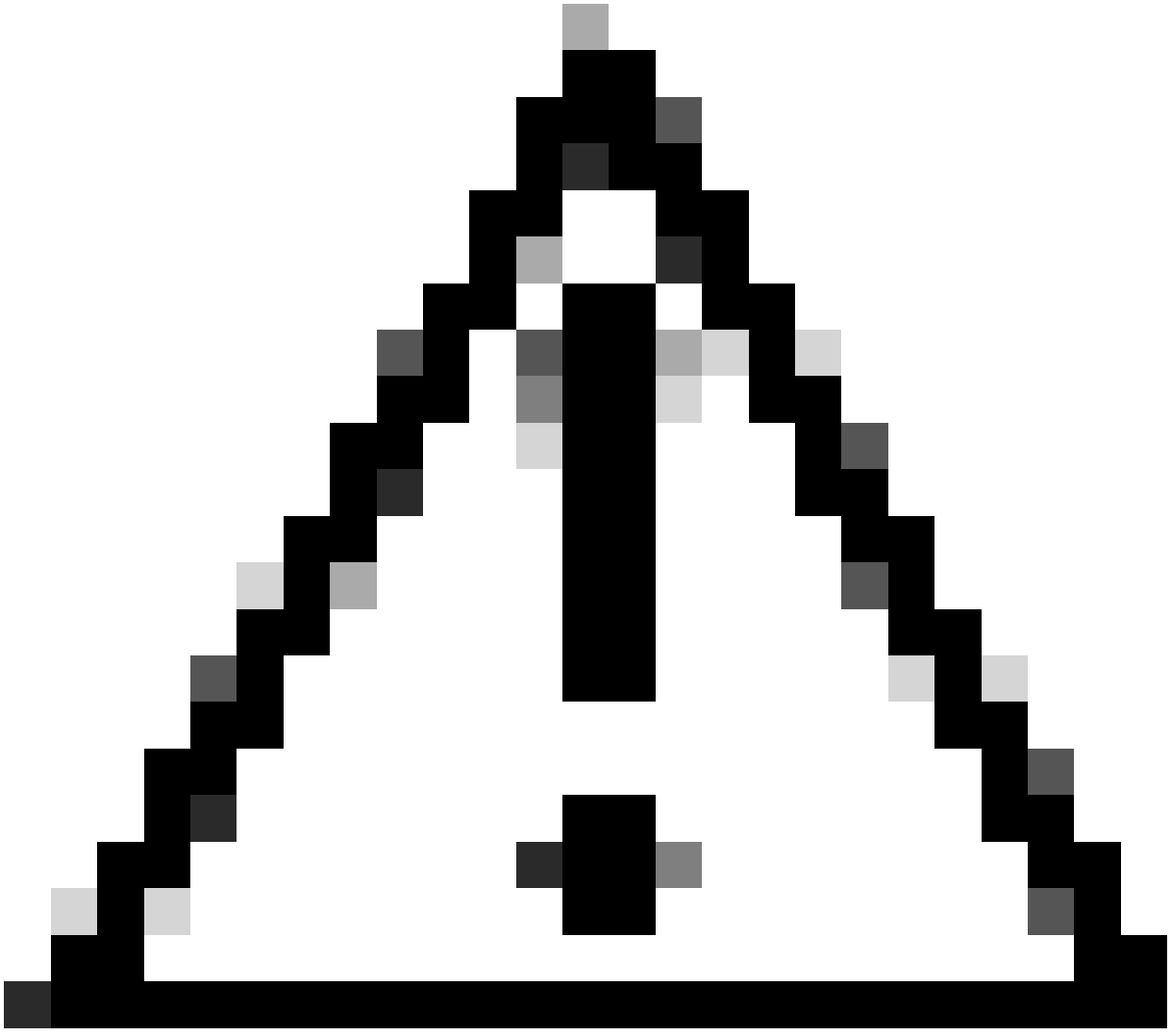
当连接到使用Umbrella虚拟设备(VA)或受保护网络功能的网络时，Umbrella漫游客户端的行为会有

所不同。这适用于用户是本地连接到网络还是通过VPN连接到网络。有关详细信息，请参阅漫游客户端和虚拟设备或受保护的网络文档。

独立和Cisco安全客户端+漫游安全模块的特殊注意事项

此处提供的信息特定于独立的Umbrella漫游客户端，不会扩展到思科安全客户端(CSC)+漫游安全模块。寻求轻松安装插件的用户可以使用集成到CSC的Umbrella Roaming。如果VPN出现功能问题，Cisco安全客户端VPN用户必须迁移到CSC +漫游安全模块。Cisco Umbrella需要在CSC +漫游安全模块上进行验证，并建议完全迁移。

Cisco安全客户端VPN软件提供了在VPN连接建立时系统如何处理DNS的选项。有关其他详细信息，请参阅有关不同OS中DNS查询和域名解析的行为差异一文。此信息基于使用思科安全客户端和Umbrella漫游客户端的经验。建议测试启用了Cisco Secure Client VPN的Umbrella漫游客户端，以确保内部和外部DNS解析功能达到预期效果。



警告：如果您还使用思科安全客户端实现DNS服务兼容性，思科要求使用CSC +漫游安全

模块。提供的步骤仅适用于非集成漫游客户端（如果需要）。CSC +漫游安全模块不需要这些步骤。

在全隧道模式和拆分隧道模式下，需要特殊说明以允许漫游客户端在连接Cisco安全客户端时工作。为了允许DNS流到漫游客户端，而不是被内核驱动程序覆盖，这是必需的。对于全通道，症状是客户端被强制禁用。对于分割隧道，症状是在连接到VPN时丢失内部DNS。

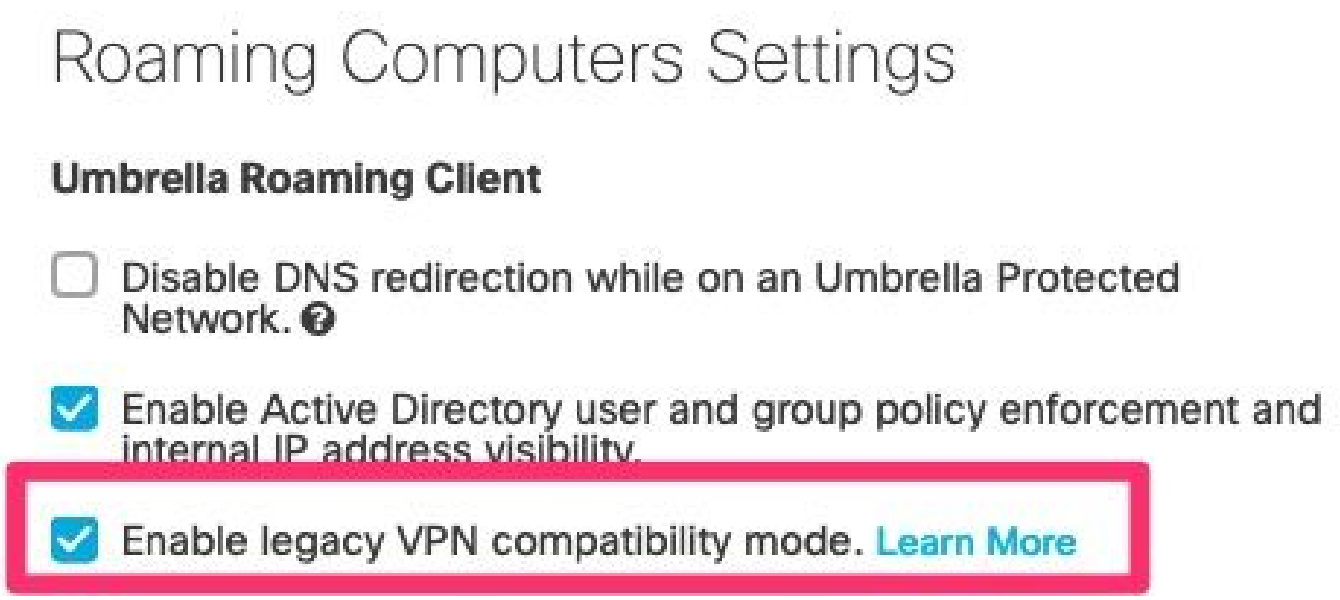
Windows 10和11的DNS绑定顺序VPN兼容模式

有限的Windows 10用户遇到一个特定问题，即本地LAN优先于使用DNS的VPN NIC。在这种情况下，当公共DNS正常运行时，漫游客户端的内部域列表中的本地DNS无法解析。这会影响版本2.0.338和2.0.341（默认）及所有更高版本。版本2.0.255未出现问题。

以前受影响的VPN客户端包括：

- AnyConnect 3.x
- AnyConnect 4.x（AnyConnect Umbrella或CSC +漫游模块不受影响）
- Sophos VPN
- 一些Palo Alto GlobalProtect配置在较旧版本上
- WatchGuard移动VPN
- Shrew软件VPN
- Barracuda VPN

分辨率
将Roaming Client设置Enable legacy VPN compatibility mode切换为enabled。



360027547111

要确认问题是否存在，请运行诊断测试并点击的结果resolv.confs。如果首先列出VPN适配器，则问题不会影响用户。如果VPN适配器列在第二位，则问题可能会影响用户。

resolv.confs输出示例

```
Results for: resolv.confs
C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf
# resolvers for Local Area Connection
nameserver 192.168.2.1
```

```
C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf
# resolvers for Cisco AnyConnect Secure Mobility
nameserver 10.1.1.27
nameserver 10.1.1.28
```

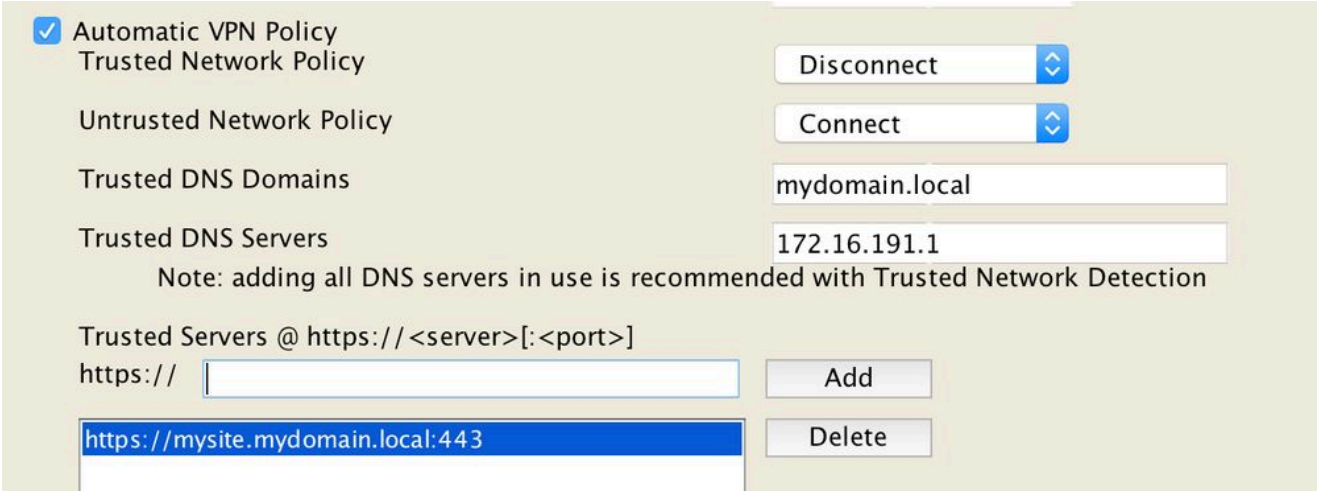
第三方VPN的特殊注意事项

永远在线VPN

定义受信任DNS服务器时，独立漫游客户端与Cisco Secure Client Always On VPN设置不兼容。激活时，独立漫游客户端始终将DNS设置为127.0.0.1，从而从NIC设置中取消所有受信任DNS服务器。可以在网络上禁用漫游客户端以恢复DHCP设置；但是，所有与漫游客户端相关的保护在配置后都会停止。请联系Umbrella支持了解有关在受信任网络中禁用客户端的详细信息。

解决方案

- CSC +漫游安全模块（Cisco安全客户端的漫游客户端）不受影响，并可通过自动VPN策略有效运行。
- 将127.0.0.1添加到受信任DNS服务器列表。
- 确保定义了其他受信任检测方法（DNS名称和服务器），以防止所有网络被声明为受信任。



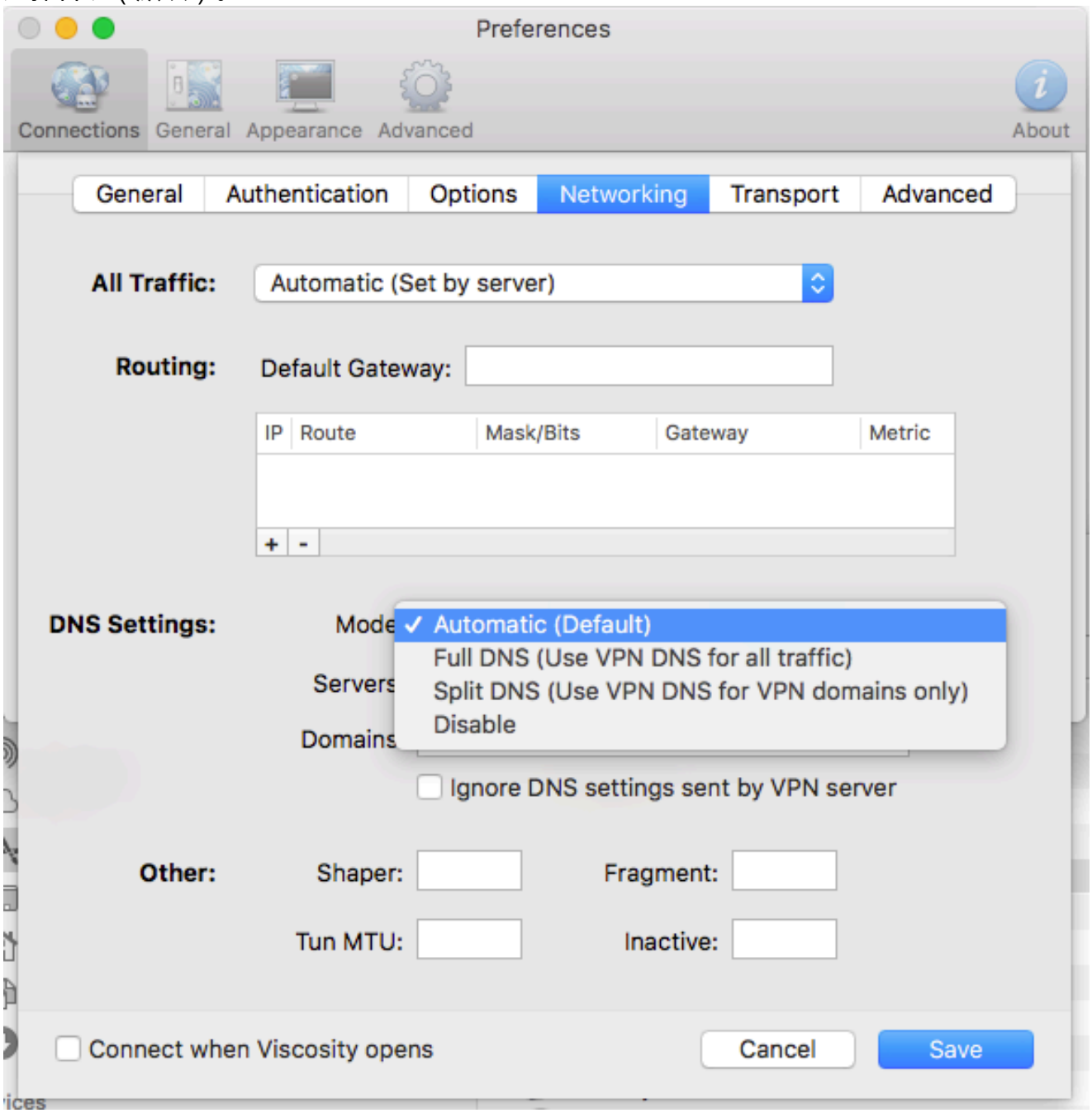
360031250911

粘性VPN

粘性VPN需要更改设置才能与Umbrella漫游客户端配合使用。如果未进行此更改，则Viscosity默认行为会模仿其他不兼容的VPN的行为。此更改指示Viscosity对搜索域中的所有域使用通过Umbrella服务器推送的DNS设置，127.0.0.1继续用于任何其他请求。

配置粘度

1. 在Viscosity中，导航到Preferences > Connections > <your connection>(site specific)> Networking > DNS Settings。
2. 选择自动（默认）。



115013433283

使用OpenVPN服务器时，请确保persist-tun在服务器端未启用，以确保在断开连接或重新连接时触发网络更改。

Tunelblick

Tunnelblick需要进行两项更改：

- 允许更改适配器的DNS服务器。
- 建立隧道后应用DNS设置。

通过确保Advanced菜单中提供的设置，Tunnelblick可与Umbrella漫游客户端配合使用：

在Connecting and Disconnecting选项卡中，启用以下两种设置：

- 在连接或断开连接后刷新DNS缓存（默认）
- 在设置路由后而不是设置路由前设置DNS

在While Connected选项卡中，将此设置更改为忽略：

- DNS:Servers > When更改为pre-VPN值，When更改为任何其他值。

使用OpenVPN服务器时，请确保persist-tun在服务器端未启用，以确保在断开连接或重新连接时触发网络更改。

Tunnelblick VPN断开问题

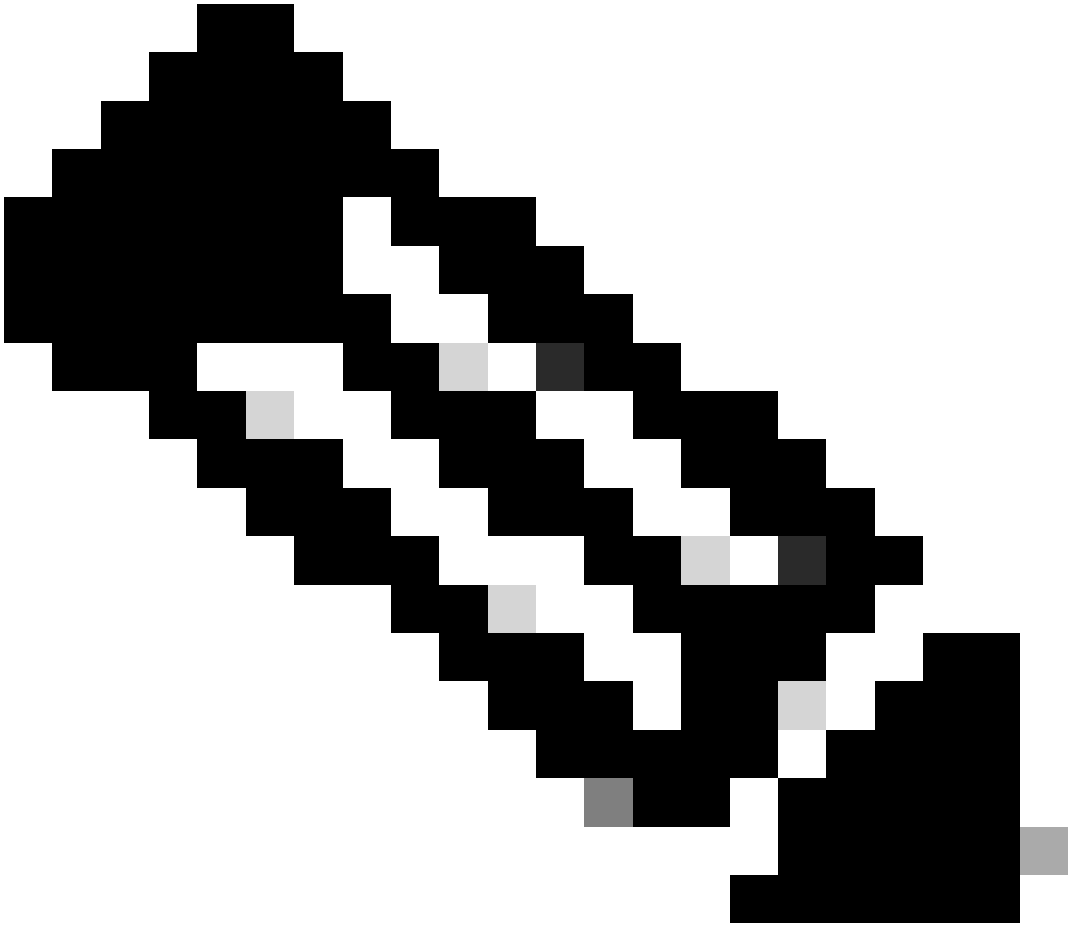
对于某些Tunnelblick版本，在VPN断开连接后，漫游客户端无法正确识别正确的内部DNS服务器。如果在VPN断开连接后出现Internal Domains问题，Umbrella建议执行以下步骤：

此更改会导致Tunnelblick在VPN断开连接后关闭和打开主网络接口。这在Tunnelblick配置面板的设置选项卡上进行管理：

- 在Tunnelblick的早期版本（3.7.5beta03之前）中，使用断开连接后重置主接口复选框。
- 在Tunnelblick的较新版本（3.7.5beta03及更高版本）上，将On expected disconnect和On unexpected disconnect设置都设置为Reset Primary Interface。

光速火箭

Lightspeed Rocket有与漫游客户端不兼容的某些功能。具体而言，对No SSL Search和SafeSearch CNAME redirection of www.google.com分别进行和更改的DNS修改会导致所有www.google.com DNS解析失败，只要启用Lightspeed Rocket DNS重定向nosslsearch.google.com forcesafesearch.com。



注意：本文参考独立式Umbrella漫游客户端。有关适用于Cisco安全客户端和传统软件的Umbrella漫游安全模块的配套文章，请参阅相关文档。

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）。