解析未受保护或未加密的漫游客户端模式

目录

简介

本文档介绍Umbrella漫游客户端中“未保护”和“未加密”状态的含义以及如何对其进行故障排除。

未保护和未加密状态

当Umbrella漫游客户端处于未保护或未加密模式时，托盘图标(Windows)或菜单栏(OS X)显示黄色状态。状态显示为Unprotected和Unencrypted。

通信要求

要提供安全和内容过滤，Umbrella漫游客户端必须使用UDP和TCP在提供的端口和目标上与Umbrella进行通信，此外，漫游客户端前提条件文章中列出的HTTP目标也如此：

端口	协议	IPv4	IPv6
53	UDP	208.67.222.222，208.67.220.220	2620:119:53::53，2620:119:35::35
53	TCP	208.67.222.222，208.67.220.220	2620:119:53::53，2620:119:35::35
443	UDP	208.67.222.222，208.67.220.220	2620:119:53::53，2620:119:35::35
443	TCP	208.67.222.222，208.67.220.220	2620:119:53::53，2620:119:35::35

如果存在以下两种情况，则Umbrella漫游客户端无法保护计算机：

- 计算机位于不允许第三方DNS请求的连接之后。
- 计算机位于具有默认deny outbound firewall策略的连接之后。

当满足这些条件时，Umbrella漫游客户端将DHCP委派DNS服务器恢复到网络连接属性，并继续测试，直到可以联系Umbrella DNS服务器并恢复提供安全和内容过滤为止。在无法与Umbrella DNS服务器进行通信期间，策略实施和报告不可用。

测试网络连接

要验证网络是否允许与Umbrella DNS服务器通信，请手动执行DNS查询。如果网络阻止查询，则输出为：

```
$ nslookup opendns.com 208.67.222.222
;; connection timed out; no servers could be reached
```

如果测试成功，但Umbrella漫游客户端仍然报告“未保护/未加密”，请打开支持票证并提供诊断测试的结果。成功的查询显示为：

```
$ nslookup opendns.com 208.67.222.222
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
Name: opendns.com
```

仅未加密状态

如果Umbrella漫游客户端显示Unencrypted，则无法通过端口443/UDP进行通信。出于安全考虑，建议允许此端口通过防火墙，但客户端无需加密DNS查询即可继续运行。有关详细信息，请参阅漫游客户端前提条件文章。

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）。