# 将端口地址转换与Umbrella组件一起使用时，排除端口耗尽故障

## 目录



## 简介

本文档介绍使用漫游客户端和/或虚拟设备的Umbrella客户，以及在使用端口地址转换的防火墙中遇到端口耗尽的问题。在拥有大量漫游客户端和/或通过VA的大量流量的环境中，这种情况最有可能发生。症状可能包括DNS查询返回缓慢或超时。

## 原因

漫游客户端和虚拟设备都不会对DNS查询做出响应。此外，漫游客户端会发送频繁的“探测”DNS请求，以分析网络环境并检查运行状况。

## 建议

- 确保在Umbrella控制面板上的“域管理”(Domain Management)中正确配置内部域。它们必须包含您的Active Directory区域（和/或其他内部区域），以便减少高频查询的量。
- 检查防火墙上的某些PAT设置：
  - 较长的UDP会话超时可能是个问题。我们通常建议大约15秒的UDP会话超时。但是，请注意，如果UDP被网络上的其他应用程序大量使用，则它们可能会有更长的超时，您必须考虑这些超时。
  - 根据您的防火墙，可以增加其PAT池的大小以增加同时连接的数量。
- 如果您有专门用于VA的IP地址，请在防火墙上使用1:1 NAT而不是PAT。注意：“1:1 NAT”有时也称为“直接NAT”，但这是用词不当；正确的技术术语是“1:1 NAT”。
- 检查您的每IP连接限制。通常，并不适用于相关设备的策略实际上是在应用限制。有关如何确认，请参阅下一节。

## 检查ASA上的每IP连接限制

使用以下步骤：

- 为ASA配置捕获以查看防火墙丢弃数据包的原因：

```
capture asp type asp-drop all match ip any host 208.67.222.222
```

- 查找有关IP的数据包被丢弃。连接限制原因显示为“Drop-reason:（连接限制）”
- 使用命令检查主机连接限制：

```
show local-host detail | begin <IP Address of VA or roaming client>
```

  - 此数字是否在某个限制（即999）下保持静态，并且从不增加？如果是，则表示连接限制。
- 检查应用此服务的服务策略；如果找到，请检查其策略映射：

```
show run service-policy, show policy-map NAME
```

  - 如果找到策略映射“NAME”，将每主机连接限制设置为1000（例如），这将导致从设备丢弃所有新DNS数据包，直到有更多连接可用。UDP是无状态且不会重试。
- 要解决此问题，请删除该service-policy（内部没有service-policy NAME）。 连接必须开始超出1K的限制（如本例所示）。 与漫游客户端相比，VA的出现速度更快。

# 进一步建议

如果这些建议没有帮助，则可能的解决方法是：

1. 使用“Umbrella dashboard —> Reporting —> Top Destinations”报告可以识别在过去24小时内具有大量请求的一个或多个域。
2. 在Umbrella控制面板 — > Configuration —> Domain Management中，将一个或多个大容量域添加到列表中，将“Apply to”设置为“All Appliances and Devices”。
3. 之后，这些域的查询由VA转发到本地DNS。理想情况下，本地DNS必须配置为转发到位于208.67.220.220/208.67.222.222的Umbrella DNS，但可以配置为转发到任何外部DNS。
4. 本地DNS处理其授权的任何域的查询。
5. 假设本地DNS接受非本地域的查询，则其他域的查询会转发到外部DNS。

这是因为本地DNS可以缓存DNS结果，而漫游客户端和虚拟设备不缓存。请注意，使用此解决方法会导致内部DNS上的流量增加和负载增加，因此请仔细监控这些流量，以确保它们不会过载。

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）。