解决MacOS中的DNS惩罚和内部域的访问问题

目录

简介

本文档介绍如何解决新版MacOS Big Sur影响DNS解析的问题。

背景信息

范围

- 网络上的AnyConnect漫游安全模块或Umbrella（例如VA或转发）
  - Umbrella独立漫游客户端不受影响。存在单DNS环境，其中所有DNS都被127.0.0.1覆盖。
- 发生在具有多个网络接口的环境中，但只有一个接口可以解析内部地址。例如：
  - VPN和非VPN
  - 多个NIC — 一个公司网卡和一个非公司网卡

症状

- 无法（或间歇性）访问本地域，同时保留访问公共域的能力
  - nslookup未具体受到影响并继续运行
    - ping、traceroute等解析错误或找不到内部域

问题

此问题是由MacOS中的代码引起的，该代码处理多个DNS服务器存在时管理DNS解析的方式。这些解析器可以是单个网络适配器上的多个解析器，也可以是跨不同网络适配器的多个解析器。以REFUSED做出响应的DNS服务器将被“处罚”60秒。发生这种情况时，将在未受处罚的备用DNS服务器上尝试在此时间段内发生的任何其他DNS查询。

例如，如果DHCP为网络A和B通告两个DNS服务器，A以REFUSED响应，那么B优先于A60秒，只要B不受惩罚。

如果所有DNS服务器都受到处罚，则MacOS偏向于最近受到处罚程度最低的服务器。例如，如果B受到处罚，而A已经受到处罚，则MacOS偏向A，而不是B。

MacOS 11和更高版本尝试主张DoH（通过HTTPS的DNS）的方式更加剧了这一点。 MacOS被编程为尽可能首选用户设置DoH提供程序。这将规避Umbrella DNS安全，这意味着当MacOS发起DoH请求时，我们将返回REFUSED响应（根据RFC）。由于DNS惩罚，可能导致内部域无法正确解析。有关此问题的详细信息，请参阅以下文章：iOS 14和macOS 11中的DNS解析器选择。

解决方案

我们尚不清楚苹果是否计划改变这种行为，或者Umbrella能否改变他们的行为来解决这个问题。就目前而言，有两个选项可以用作工作方法：

第 1 项

在组策略中启用拆分DNS，并特别将内部域添加到拆分DNS配置中，以便它们只能通过隧道进行解析。这可确保这些域只能通过本地操作系统解析程序通过隧道进行解析，而任何其他域只能通过隧道外部进行解析。

第 2 项

在组策略中启用tunnel-all-DNS，以阻止任何DNS流量进入隧道外部。

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）。