强制网络门户与Umbrella漫游客户端的交互故障排除

目录

简介

本文档介绍强制网络门户与Umbrella漫游客户端的交互。

概述

强制网络门户是公共或“即服务”Internet连接的常用名称，此类连接需要付款、身份验证或服务条款/可接受使用策略(TOS/AUP)接受，然后才允许连接到设备。

强制性的门户通常出现在机场、酒店、咖啡店或真正提供免费或付费的wifi的任何地方。您也可以在公司或学校环境中的访客wifi网络中看到它们。

强制网络门户在浏览器中通常显示为“入口”或弹出窗口，最终用户需要执行操作来提供凭证、付款或接受服务条款，才能访问互联网。在清除强制网络门户之前，用户无法浏览除门户所在的子网内的资源之外的任何资源。

预期行为和场景

大多数强制网络门户将所有浏览器请求(HTTP/HTTPS)重定向到其本地Web门户。本地Web门户通常基于IP而不是基于DNS。这意味着在连接到强制网络门户的计算机上使用Umbrella漫游客户端时，不会出现行为问题。

在强制网络门户以某种方式使用DNS促进其服务的极少数情况下，此行为发生在完成强制网络门户的要求（付款、TOS/AUP接受等）之前。]

基于DNS的强制网络门户可能只能重定向无故障的HTTP查询。现代浏览器会自动处理已知请求，例如google.com到https://www.google.com/，这些请求可能会中断一些强制网络门户。尝试使用Apple的强制网络门户检查站点访问仅http的强制网络门户登录页面。为此，请访问http://captive.apple.com。

思科安全连接器(CSC)

与漫游客户端一样，如果强制网络门户后面允许UDP 443，则CSC将保持受保护状态并加密。这会导致强制网络门户的本地DNS无法解析为本地结果。因此，要访问强制网络门户，必须访问这些半强制网络门户的内部域列表中的域。

要允许iOS自动强制网络门户检测正常工作，请执行以下操作：

- 将这些域添加到内部域列表
  - captive.apple.com
  - www.airport.us
  - www.thinkdifferent.us

阻止第三方DNS

如果强制网络门户阻止发往Umbrella的DNS请求，则Umbrella漫游客户端会阻止DNS连接约6秒。6秒后，Umbrella漫游客户端将转换到Unprotected/Unencrypted状态，直到可以再次与Umbrella通信。

重定向的第三方DNS

如果强制网络门户重定向发往Umbrella的DNS请求，则Umbrella漫游客户端会阻止DNS连接大约2到6秒。此后，Umbrella漫游客户端将转换到未保护/未加密状态，直到可以再次与Umbrella通信。

允许第三方DNS

如果强制网络门户没有控制或阻止发往Umbrella的DNS请求，则Umbrella漫游客户端会按预期工作，并可能导致完全绕过强制网络门户的登录部分。

解决方案：访问内部域列表中的域。这允许强制网络门户重定向，即使允许第三方DNS也是如此。当漫游客户端在强制网络门户后保持受保护状态时，执行此操作。

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）。