Umbrella DNS与MacOS上的Broadcom WSS的安全共存问题

目录

问题

当与Broadcom WSS（网络安全服务）共存时，Umbrella模块不会拦截macOS上的DNS流量。 当WSS代理配置为截取特定Web端口（如80和443）时，Umbrella DNS安全功能无法捕获所有DNS查询。但是，当WSS被禁用时，Umbrella会按预期继续拦截DNS流量。启用WSS时，Umbrella只处理某些DNS查询，而不是拦截所有DNS流量。

环境

- 操作系统：macOS
- Cisco Umbrella DNS安全模块
- Broadcom WSS（网络安全服务）代理
- WSS代理配置为拦截Web端口80和443

分辨率

此问题已分析并被确定为macOS的架构限制，其中DNS安全无法在当前macOS架构中与WSS共存。此限制适用于Infoblox和Cisco Umbrella DNS安全解决方案。

技术分析

根本原因与macOS DNS代理限制有关：

- 由于macOS限制，系统中一次只能有一个DNS代理处于活动状态

- 如果DNS解析器绑定到utunX接口或代理注入的解析器，则macOS解析隧道内的DNS，而不是通过Umbrella
- 当另一个NEDnsProxyProvider在macOS上的系统上处于活动状态时，Umbrella不会拦截DNS流量

诊断命令

要验证哪个DNS解析程序在macOS上获得优先级，请使用以下命令：

```
scutil --dns
```

此命令将显示哪个解析程序标记为：范围、补充或接口：utunX，帮助识别DNS代理冲突。

解决方法选项

对于macOS环境，WSS将继续在不使用任何单独的DNS代理的情况下拦截DNS。要继续实施DNS安全覆盖，一个选项是实施以支持被动旁路架构。使用此方法，提供商将完全绕过流量，允许处理流量，就像提供商未处于活动状态一样。

原因

此问题是由于macOS架构限制导致的，在该架构限制中，系统一次只能激活一个NEDnsProxyProvider。当同时安装Umbrella DNS Security和Broadcom WSS时，它们会争夺DNS代理控制，导致WSS优先处理，并阻止Umbrella拦截DNS流量。这是macOS网络堆栈的基本限制，影响所有DNS安全解决方案，而不仅仅是Cisco Umbrella。

相关内容

- 思科技术支持和下载

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）。