将DNS解析与CNAME记录域策略和报告进行匹配

目录

简介

本文档介绍如何将DNS解决方案与CNAME记录域策略和报告相匹配。

问题

在使用域名系统(DNS)缓存服务器(例如BIND（已启用缓存）或Infoblox时，您的DNS解析与您的CNAME记录域的预期策略和报告不匹配。允许的A-record请求将通过CNAME对另一个已阻止域中的其他A-record的引用进行应答。

例如，允许domain.com且blocked.com被阻止，而domain.com是指向blocked.com（具有A记录）的CNAME记录。此问题将自己显示为被阻塞的允许域，控制面板上未记录此类事件。

解决方案

有多种方法可以解决此问题：

- 禁用转发到Umbrella的DNS的DNS缓存。这可防止出现此问题。
- 允许目标CNAME在Umbrella控制面板中出现。
- 避免缓存CNAME记录类型或选择性地不主动缓存受影响的域。

原因

此问题的根本原因是指向不同域的CNAME记录的DNS缓存，在该域中目标域被阻止。由于域被允许，Umbrella解析程序将整个查询标记为允许，并沿着CNAME链向下传送。这将生成一个允许的查询。

由于不同域的TTL不同，并且恶意类别的Umbrella阻止记录的TTL为零，因此缓存会受到干扰。

以下场景是允许domain.com且blocked.com被阻止，并且domain.com是指向blocked.com且具有A记录的CNAME记录。

初始查询：

domain.com的A记录：Allow list， CNAME for blocked.com -> A-record query for blocked.com,

from a CNAME， allow bit passed inside Umbrella - A-record for blocked.com returned。
分析:对Umbrella的查询：domain.com -> blocked.com。结果：允许。Umbrella按照允许登录domain.com，按照允许登录blocked.com。

后续查询：

domain.com的A记录：CACHED — 它是blocked.com的CNAME -> blocked.com的A记录查询：CACHED — 返回blocked.com的A记录。
分析:对Umbrella的查询：无.没有Umbrella日志。

将来的查询（触发问题）：

domain.com的A记录：CACHED — 它是blocked.com的CNAME -> blocked.com的A记录查询（独立查询 — CNAME已缓存） — 已阻止。
分析:对Umbrella的查询：blocked.com。结果：已阻止。Umbrella将blocked.com记录为已阻止。

Additional Information

- Umbrella文档：DNS解析

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）。