

將DNS解析與CNAME記錄域策略和報告匹配

目錄

[簡介](#)

[問題](#)

[解決方案](#)

[原因](#)

[其他資訊](#)

簡介

本文檔介紹如何將DNS解決方案與CNAME記錄域策略和報告相匹配。

問題

在使用域名系統(DNS)快取伺服器(例如BIND (已啟用快取) 或Infoblox)時，您的DNS解析與您的CNAME記錄域的預期策略和報告不匹配。允許的A-record請求將通過CNAME引用到另一個已阻止域上的其他A-record來應答。

例如，允許domain.com且blocked.com被阻止，而domain.com是指向blocked.com的CNAME記錄，後者具有A記錄。此問題將自己顯示為被阻塞的允許域，儀表板中不會記錄此類事件。

解決方案

有幾種方法可以解決此問題：

- 禁用轉發到Umbrella的DNS的DNS快取。這可防止發生此問題。
- 允許目標CNAME在出現Umbrella Dashboard時。
- 避免快取CNAME記錄型別或有選擇地不以反應方式快取受影響的域。

原因

此問題的根本原因是指向其他域（目標域被阻止）的CNAME記錄的DNS快取。由於允許該域，Umbrella解析程式會將整個查詢標籤為允許，並沿著CNAME鏈向下移動。這將生成允許的查詢。

由於不同域的TTL不同，並且惡意類別的Umbrella塊記錄的TTL為零，因此快取會干擾。

在此案例中，允許domain.com且blocked.com被阻止，而domain.com是指向blocked.com且具有A記錄的CNAME記錄。

初始查詢：

domain.com的A-record: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：對Umbrella的查詢：domain.com -> blocked.com。Result:已允許.Umbrella按照允許登入domain.com，按照允許登入blocked.com。

後續查詢：

domain.com的A-record:CACHED — 它是blocked.com的CNAME -> blocked.com的A記錄查詢：
：CACHED — 返回blocked.com的A記錄。

分析：對Umbrella的查詢：無.沒有雨傘日誌。

將來查詢（觸發問題）：

domain.com的A-record:CACHED — 它是blocked.com的CNAME -> blocked.com的A記錄查詢（獨立查詢 — CNAME已快取） — 已阻止。

分析：對Umbrella的查詢：blocked.com。Result:已阻止。Umbrella將blocked.com記錄為已阻止。

其他資訊

- [Umbrella文檔：DNS解析](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。