

了解Umbrella DNS和QNAME最小化

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[概述](#)

[了解查询最小化](#)

[潜在的副作用](#)

简介

本文档介绍如何使用Cisco Umbrella域名系统(DNS)和QNAME最小化。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Umbrella

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

2019年6月，Cisco Umbrella添加了对查询名称最小化([RFC7816](#))的支持。QNAME最小化是DNS中面向隐私的功能，旨在限制向根名称服务器发送完整域目标。因此，用于确定DNS查询响应的DNS查询流将被修改。

QNAME最小化是一个全球性的主题。Internet Systems Consortium有一篇关于QNAME最小化的[介绍性文章](#)。Mozilla Firefox要求解析程序对HTTPS上的DNS使用QNAME最小化，并发表了[有关此主题的文章](#)。

了解查询最小化

查询最小化是一种以数据隐私为中心的新的DNS权威查询方法。要了解什么是查询最小化，首先要解释当前DNS请求的工作方式。

由于大多数人类与Internet的交互都以DNS查询开头，因此关于用户去向的大数据是无价的信息，可以视为私有数据。

在本例中，您希望访问umbrella.cisco.com。您需要使用DNS查询来确定此服务器所在的位置，因此Umbrella将该查询发送到递归DNS服务器，以使用以下步骤从机构查找答案：

- 1.用户查询递归DNS解析程序：umbrella.cisco.com
- 2.递归DNS服务器从根名称服务器查询答案：在哪里可以找到umbrella.cisco.com到root > answer for .com
- 3.在.com名称服务器上查询：umbrella.cisco.com to .com >获取cisco.com名称服务器的位置
- 4.查询cisco.com域名服务器：umbrella.cisco.com到cisco.com >提供答案

在许多情况下，这可以继续多次迭代到不同的名称服务器，直到找到A记录。在第1-2步中，Umbrella只主动寻找.com名称服务器的位置。但是，完整的umbrella.cisco.com域将发送到根和.com名称服务器。接收完整查询的cisco.com名称服务器也一样。

使用查询最小化，算法将转向仅请求上游查询中所需的详细程度：

- 1.用户查询递归DNS解析程序：umbrella.cisco.com
- 2.递归DNS服务器查询根名称服务器：在哪里可以找到.com > answer for .com
- 3.在.com名称服务器上查询：cisco.com to .com > location of cisco.com
- 4.在cisco.com名称服务器中查询umbrella.cisco.com >答案

这在大多数情况下都非常有效，并且可以在不向根或TLD名称服务器显示唯一查询的情况下找到答案。

对于使用EDNS客户端子网的域而言，这种隐私更加重要，因为查询时，DNS机构会获知用户的源C地址块(/24)。如果没有QNAME最小化，根目录和.com（在本例中）名称服务器会知道您的常规位置以及您确切的去向。通过QNAME最小化，根节点仅知道有人正在查找.com，且请求者的隐私得以维护。如果没有QMIN隐私保护，他们无需提供当前所需的详细程度。

潜在的副作用

在大多数情况下，QNAME最小化工作没有问题。但是，与直接查询相比，它可能会受到其他故障源的影响。由于直到进程的最后一步才向授权域名服务器显示完整的目的地，因此DNS链中的中断可能会中断域的解析。例如，这是一个长长的虚构名称——umbrellas.in.the.rain.umbrella.cisco.com。这可能会导致以下查询：

1. .com到根服务器的名称服务器是什么。
2. cisco.com到.com服务器的名称服务器是什么
3. umbrella.cisco.com的名称服务器与cisco.com名称服务器之间的名称服务器是什么

4. rain.umbrella.cisco.com的名称服务器与umbrella.cisco.com名称服务器之间的名称服务器是什么。

5. the.rain.umbrella.cisco.com的名称服务器与rain.umbrella.cisco.com名称服务器之间的名称服务器是什么

6. in.the.rain.umbrella.cisco.com的名称服务器与rain.umbrella.cisco.com名称服务器之间的名称服务器是什么：SERVFAIL

7. umbrellas.in.the.rain.umbrella.cisco.com的名称服务器与rain.umbrella.cisco.com名称服务器之间的名称服务器是什么（由于之前的SERVFAIL未查询）

8.对于之前找到的umbrellas.in.the.rain.umbrella.cisco.com名称服务器（由于之前的SERVFAIL未查询），umbrellas.in.the.rain.umbrella.cisco.com的答案是什么？

由于根没有给出完整的查询，如果域的一个级别返回NXDOMAIN、SERVFAIL、RFC-1918内部名称服务器的IP或其他较差的响应，查询可能无法收到成功的上游授权响应。例如，如果前面的第六步（粗体、带下划线）失败，则对umbrellas.in.the.rain.umbrella.cisco.com的查询可能无法解决。要解决这些问题，域所有者必须确保每个级别都有有效的公共响应。

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）。