

# Entender o DNS do Umbrella com minimização de QNAME

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Entender a Minimização de Consultas](#)

[Efeitos secundários potenciais](#)

---

## Introdução

Este documento descreve como usar o Cisco Umbrella Domain Name System (DNS) com minimização de QNAME.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Overview

Em junho de 2019, o Cisco Umbrella adicionou suporte para a minimização de nome de consulta ([RFC7816](#)). A minimização de QNAME é um recurso orientado à privacidade no DNS que visa limitar o envio do destino de domínio completo para os servidores de nome raiz. Como resultado, o fluxo de consultas DNS para determinar a resposta de consulta DNS é modificado.

A minimização do QNAME é um tópico mundial. O Internet Systems Consortium tem um [artigo introdutório sobre a minimização do QNAME](#). O Mozilla Firefox requer que os resolvedores usem

a Minimização de QNAME para implementações de DNS sobre HTTPS e tem um [artigo sobre este tópico](#).

## Entender a Minimização de Consultas

A minimização de consultas é uma nova abordagem centrada na privacidade de dados para consultas autoritativas de DNS. Para explorar o que é a minimização de consulta, comece com uma explicação de como uma solicitação DNS funciona atualmente.

Como a maior parte da interação humana com a Internet começa com uma consulta DNS, o big data sobre para onde os usuários estão indo são informações inestimáveis, que podem ser consideradas dados privados.

Neste exemplo, você está procurando acessar `umbrella.cisco.com`. Você precisa de uma consulta DNS para determinar onde esse servidor está localizado, portanto o Umbrella envia essa consulta a um servidor DNS recursivo para encontrar a resposta da autoridade usando estas etapas:

1. Consulta de usuário ao resolvedor DNS recursivo: `umbrella.cisco.com`
2. O servidor DNS recursivo consulta a resposta dos servidores de nome raiz: onde posso encontrar `umbrella.cisco.com` para `root` > responda para `.com`
3. Consulte os servidores de nomes `.com`: `umbrella.cisco.com` para `.com` > obtém a localização de servidores de nomes `cisco.com`
4. Consulte os servidores de nomes `cisco.com`: `umbrella.cisco.com` para `cisco.com` > Resposta fornecida

Em muitos casos, isso pode continuar com várias iterações para servidores de nome diferentes até que um registro A seja localizado. Nas etapas de 1 a 2, a Umbrella está apenas buscando ativamente a localização dos servidores de nome `.com`. No entanto, o domínio `umbrella.cisco.com` completo é enviado à raiz e ao servidor de nome `.com`. O mesmo vale para o servidor de nome `cisco.com` que recebe a consulta completa.

Com a minimização de consulta, o algoritmo passa a solicitar somente o nível de detalhe necessário nas consultas upstream:

1. Consulta de usuário ao resolvedor DNS recursivo: `umbrella.cisco.com`
2. O servidor DNS recursivo consulta os servidores de nomes raiz: onde posso encontrar `.com` > responda `.com`
3. Consulte os servidores de nomes `.com`: `cisco.com` para `.com` > local de `cisco.com`
4. Consulte os servidores de nomes `cisco.com` para `umbrella.cisco.com` > Responder

Isso funciona muito bem na maioria dos casos e permite que a resposta seja localizada sem revelar a consulta exclusiva que está sendo feita aos servidores de nome raiz ou TLD.

Essa privacidade é ainda mais importante para domínios que fazem uso da Sub-rede do Cliente EDNS, onde a autoridade DNS é informada do Bloco C de origem do usuário (/24) ao consultar. Sem a minimização do QNAME, a raiz e os servidores de nome .com (neste exemplo) conhecem sua localização geral e para onde você está indo exatamente. Com o QNAME Minimization, as raízes só sabem que alguém está procurando por .com e a privacidade do solicitante é mantida. Eles não exigem o nível de detalhes fornecido a eles hoje sem as proteções de privacidade QMIN.

## Efeitos secundários potenciais

A minimização de QNAME funciona sem problemas na maioria dos casos. No entanto, ele está sujeito a fontes adicionais de falha em comparação a uma consulta direta. Como o destino completo não é revelado até a última etapa do processo para o servidor de nome autoritativo, as quebras na cadeia DNS podem quebrar a resolução do domínio. Por exemplo, aqui está um nome fictício longo - `umbrellas.in.the.rain.umbrella.cisco.com`. Isso pode resultar nestas consultas:

1. Qual é o nameservers para .com para os servidores raiz .
2. Qual é o nameservers de cisco.com para os servidores .com?
3. Qual é o nameservers de umbrella.cisco.com para o cisco.com nameservers
4. Qual é o nameservers de rain.umbrella.cisco.com para os nameservers umbrella.cisco.com.
5. Qual é o nameservers de the.rain.umbrella.cisco.com para o rain.umbrella.cisco.com nameservers
6. Quais são os nameservers de in.the.rain.umbrella.cisco.com para os nameservers rain.umbrella.cisco.com: SERVFAIL
7. Quais são os nameservers de umbrellas.in.the.rain.umbrella.cisco.com para os nameservers rain.umbrella.cisco.com (não consultados devido a SERVFAIL anteriormente)
8. Qual é a resposta para umbrellas.in.the.rain.umbrella.cisco.com para os servidores de nomes umbrellas.in.the.rain.umbrella.cisco.com que foram encontrados anteriormente (não consultados devido a SERVFAIL anteriormente)

Como as raízes não recebem a consulta completa, se um dos níveis do domínio retornar um NXDOMAIN, SERVFAIL, o IP de um servidor de nome interno RFC-1918 ou outra resposta ruim, a consulta pode falhar ao receber uma resposta autoritativa upstream com êxito. Por exemplo, se a sexta etapa anterior (negrito, sublinhado) falhar, a consulta para `umbrellas.in.the.rain.umbrella.cisco.com` poderá falhar. Para resolver esses problemas, o proprietário do domínio deve garantir que cada nível tenha uma resposta pública válida.

### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.