

QNAMEの最小化を伴うUmbrella DNSについて

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[概要](#)

[クエリの最小化について](#)

[潜在的な副作用](#)

はじめに

このドキュメントでは、QNAME最小化でCisco Umbrellaドメインネームシステム(DNS)を使用する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づいています

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

2019年6月、Cisco Umbrellaはクエリ名の最小化([RFC7816](#))のサポートを追加しました。QNAMEの最小化は、ドメインの完全な宛先のルートネームサーバへの送信を制限することを目的としたDNSのプライバシー指向機能です。その結果、DNSクエリーの応答を決定するためのDNSクエリーのフローが変更されます。

QNAMEの最小化は世界的な話題です。Internet Systems Consortium(ISC)には、[QNAMEの最小化](#)に関する紹介記事があります。Mozilla Firefoxでは、リゾルバがDNS over HTTPS実装にQNAME Minimizationを使用する必要があります。また、[このトピックに関する記事](#)があります。

クエリの最小化について

クエリの最小化は、DNS権威クエリに対するデータプライバシー中心の新しいアプローチです。クエリの最小化とは何かを調べるには、まず、現在のDNS要求の仕組みについて説明します。

人間とインターネットとのやり取りのほとんどはDNSクエリから始まるため、ユーザがアクセスする場所に関するビッグデータは貴重な情報であり、プライベートデータと見なすことができます。

この例では、umbrella.cisco.comにアクセスします。このサーバの場所を特定するにはDNSクエリが必要です。Umbrellaはこのクエリを再帰DNSサーバに送信し、次の手順を使用して認証局からの応答を検索します。

1. 再帰DNSリゾルバに対するユーザークエリ： umbrella.cisco.com
2. 再帰的なDNSサーバは、ルートネームサーバからの応答を照会します。umbrella.cisco.com to root > answer for .comはどこにありますか。
3. .comネームサーバのクエリー： umbrella.cisco.com to .com >cisco.comネームサーバの場所を取得
4. cisco.comネームサーバに問い合わせる： umbrella.cisco.comからcisco.com >回答を入力

多くの場合、Aレコードが見つかるまで、異なるネームサーバに対してさらに何度か繰り返し実行することで、この処理を続行できます。ステップ1～2では、Umbrellaは.comネームサーバの場所をアクティブに探しているだけです。ただし、完全なumbrella.cisco.comドメインがルートおよび.comネームサーバに送信されます。クエリ全体を受信するcisco.comネームサーバについても同じことが言えます。

クエリの最小化を使用すると、アルゴリズムはアップストリームクエリで必要な詳細レベルだけを要求するように移行します。

1. 再帰DNSリゾルバに対するユーザークエリ： umbrella.cisco.com
2. 再帰的なDNSサーバがルートネームサーバに問い合わせる： .comの場所> .comの回答
3. .comネームサーバ(cisco.comから.com >cisco.comの場所)でクエリーを実行します。
4. cisco.comのネームサーバでumbrella.cisco.comを照会し、「Answer」と入力します。

ほとんどの場合、この方法は適切に機能し、ルートまたはTLDネームサーバに対して行われている一意のクエリーを明らかにせずに、応答を特定できます。

このプライバシーは、EDNSクライアントサブネットを使用するドメインにとってさらに重要です。このサブネットでは、クエリの際にDNS機関がユーザーのソースCブロック(/24)を通知されます。QNAMEを最小限に抑えないと、ルートと.com（この例では）ネームサーバは、ユーザの一般的な場所とユーザの正確な目的地を認識します。QNAME Minimizationを使用すると、ルートは誰かが.comを探していることを認識するだけで、要求者のプライバシーは維持されます。QMINのプライバシー保護なしに提供される今日の詳細レベルを必要としません。

潜在的な副作用

QNAMEの最小化は、ほとんどの場合、問題なく機能します。ただし、直接クエリと比較すると、障害の原因が増える可能性があります。完全な宛先は、プロセスの最後のステップで権威ネームサーバに到達するまで明らかにされないため、DNSチェーンが切断されるとドメインの解決が中断する可能性があります。たとえば、長い架空の名前のumbrellas.in.the.rain.umbrella.cisco.comです。これにより、次のクエリが発生する可能性があります。

1. ルートサーバへの.comのネームサーバは何ですか。
2. cisco.comの.comサーバへのネームサーバは何ですか。
3. umbrella.cisco.comからcisco.comへのネームサーバは何ですか。
4. rain.umbrella.cisco.comからumbrella.cisco.comへのネームサーバは何ですか。
5. the.rain.umbrella.cisco.comからrain.umbrella.cisco.comへのネームサーバは何ですか。
6. in.the.rain.umbrella.cisco.comからrain.umbrella.cisco.comへのネームサーバ：SERVFAILとは何ですか。
7. umbrellas.in.the.rain.umbrella.cisco.comからrain.umbrella.cisco.comへのネームサーバとは何ですか（以前にSERVFAILが原因で照会されませんでした）。
8. 以前に見つかった（以前にSERVFAILが原因で照会されなかった）umbrellas.in.the.rain.umbrella.cisco.comネームサーバに対するumbrellas.in.the.rain.umbrella.cisco.comの応答は何ですか。

ルートには完全なクエリーが与えられていないため、ドメインのレベルの1つからNXDOMAIN、SERVFAIL、RFC-1918内部ネームサーバのIP、またはその他の貧弱な応答が返された場合、クエリーはアップストリームの正常な権威のある応答を受信できない可能性があります。たとえば、前述の6番目のステップ（太字、下線付き）が失敗した場合、umbrellas.in.the.rain.umbrella.cisco.comに対するクエリは解決しない可能性があります。これらの問題を解決するには、ドメイン所有者は各レベルに有効なパブリック応答があることを確認する必要があります。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせ、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。