iOS 14およびmacOS 11でのDNSリゾルバ選択の設定

内容

はじめに

このドキュメントでは、暗号化されたDNSのサポートを含む、iOS 14およびmacOS 11アップデートからのUmbrellaの変更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、次のソフトウェアとハードウェアのバージョンに基づいています。

- Ciscoセキュリティコネクタ(CSC)
- macOS Umbrellaローミングクライアント(RC)
- macOS AnyConnectクライアント(AC)

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

Appleは2020年9月16日にiOS 14のリリースを発表しました。特に、iOS 14とmacOS 11には、暗号化されたDNSのサポート、およびドメイン所有者が任意のDNSリゾルバを指定する機能が含まれています。この変更は、一部のドメイン名を解決するUmbrellaの機能に直接影響します。つまり、これらのドメインのポリシーとレポートに影響します。

iOS 14とmacOS 11の変更には、主に次の3つの影響があります。

1. ユーザは、DHCPまたはRAによって設定されたDNSリゾルバを上書きできる、システム全体のDoHリゾルバを指定できます。

2. ドメインの所有者は、ドメインに対して行われたクエリに対して、DHCPまたはRAによって設定されたDNSリゾルバを上書きできるDoHリゾルバを指定できます。

3. アプリケーションは、アプリケーションから作成されたクエリに対して、DHCPまたはRAによって設定されたDNSリゾルバを上書きできるDoHリゾルバを指定できます。Umbrellaには、どのアプリケーションが実行されているかが表示されません。

これらの更新に伴い、Appleはネットワークプロビジョンリゾルバと同じIP上で実行される暗号化リゾルバを検出するメカニズムを含んでいません。つまり、Umbrellaリゾルバにクエリを転送するネットワークは、doh.umbrella.comでUmbrellaのDoHサービスにアップグレードできません。

2020年10月1日の時点で、Umbrellaにより、ドメイン所有者によって指定されたDoHリゾルバの検出が阻止され、これらのドメインがUmbrella保護をバイパスできなくなります。Umbrellaクライアントがデバイスにインストールされていない限り、Umbrellaは#1および#3の影響を防ぐことはできません。これらの影響に対する保護を必要とするお客様は、この記事で説明されているように、既知のDoHプロバイダーのIPをブロックすることを検討できます。

iOS 14とmacOS 11の変更の詳細については、この記事を続けてください。

Umbrellaユーザへの影響

Ciscoセキュリティコネクタ(CSC)

CSCを使用するiOSデバイスは、iOSのリゾルバ検出メカニズムよりも優先されるAppleのDNSプロキシメカニズムを使用するため、この変更の影響を受けません。

macOS Umbrellaローミングクライアント(RC)

macOS RCは現在、localhost上でDNSプロキシを実行しており、macOSからは暗号化されていないリゾルバと見なされているため、RCを使用するmacOSデバイスがこの変更の影響を受ける可能性があります。RCはDNSCryptを使用してUmbrellaリゾルバと通信します。

Umbrellaは、Apple DNS Proxy Providerを使用してDNSを制御するAnyConnect Roaming Security Module（以下のACを参照）で、DoH検出に対する強制実行のサポートを提供しています。現時点では、このサポートはRCに含める予定はありません。Umbrellaパッケージは AC用にライセンスされています。こちらの記事をご覧ください。

macOS AnyConnectクライアント(AC)

acを使用するmacOSデバイスは、現在macOSのリゾルバ検出メカニズムよりも優先されるAppleのDNSプロキシメカニズムを使用しているため、この変更の影響を受けません。

仮想アプライアンス(VA)の背後にあるiOSまたはmacOSデバイス

CSC、RC、またはACがインストールされていないiOSまたはmacOSは、この変更の影響を受ける可能性があります。したがって、VAの背後にあるこのようなデバイスは、仮想アプライアンスをバイパスして、設定済みのDoHサーバにクエリを直接送信できます。

登録済みネットワークの背後にあるiOSまたはmacOSデバイス

CSC、RC、またはACがインストールされていないiOSまたはmacOSは、この変更の影響を受けません。そのため、登録されたネットワークの背後にあるこのようなデバイスは、ローカルリゾルバまたはUmbrellaをバイパスして、設定されたDoHサーバにクエリを直接送信できます。

包括および暗号化されたDNS

Umbrellaは、暗号化DNSの使用と、暗号化DNSの使用を推進するイニシアチブを完全にサポートしています。Umbrellaリゾルバは、2011年以降、DNSトラフィックを暗号化する手段としてDNSCryptをサポートしており、すべてのUmbrellaクライアントソフトウェアはDNSCryptの使用をサポートし、デフォルト設定でそれを使用しています。また、2020年2月からHTTPS(DoH)経由のDNSをサポートしています。

さらに、Umbrellaは、キャッシュ内のすべてのレコードのデータ整合性を保証するために、アップストリーム機関に送信されたクエリに対してDNSSEC検証を実行します。

iOS 14とmacOS 11でのDNSの詳細な変更

iOS 14とmacOS 11では、DNSリゾルバを選択するための新しいメカニズムが導入されています。特定の詳細を必要とするお客様はAppleに確認できますが、このメカニズムに関するシスコの理解は、DNSリゾルバは次に説明する優先順位で選択できるということです。

1. ネットワーク提供DNSリゾルバを利用したキャプティブポータルテストゾーンの解決

2. VPNまたはDNSプロキシの設定（iOS用のCisco Security Connectorなど）およびエンタープライズポリシー（MDMまたはOTAなど）によって設定されたDNSリゾルバ。（DNSポリシーの設定の詳細については、MDMベンダーに問い合わせてください）

（三）システム全体を暗号化したリゾルバであって、デバイスの所有者が直接構成するもの

（四）ドメイン所有者の指定する暗号化リゾルバ

5. アプリが指定する暗号化リゾルバ

6. 暗号化されていないリゾルバ（DHCPまたはRAで指定されたリゾルバなど）

特に、3、4、5は、Umbrella管理者がUmbrellaリゾルバの使用をネットワークに完全に適用する機能に直接影響する可能性のある、リゾルバの選択に対する重要な変更と考えています。

システム全体の暗号化リゾルバ

ユーザはDNSプロバイダーから設定プロファイルアプリケーションをインストールできます。このアプリケーションを使用すると、システム全体で暗号化されたリゾルバを設定できます。このリゾルバは、DHCPまたはRA経由でネットワークによって指定されたDNSリゾルバに関係なく、すべてのクエリに使用できます。

現在、アンマネージドデバイスに対してこれらのリゾルバの使用を防止する唯一の既知の方法は、ファイアウォールで既知のDoHプロバイダーのIPをブロックすることです。この操作を行うと、iOSデバイスのユーザに対して警告が表示され、デバイスは暗号化されていないDNSにフォールバックできません。つまり、DNSホスト名を解決できなくなります。

ドメイン所有者によって指定された暗号化リゾルバ

DNSゾーンの所有者は、そのゾーンの解決に使用する特定のリゾルバを指定できます。iOS 14およびmacOS 11では、DoHリゾルバだけを指定できます。この指定は、専用のDNSレコードタイプ（タイプ65、「HTTPS」という名前）を使用して行われ、DNSSECまたは既知のURIのいずれかによって検証されます。

このような指定では、Umbrellaをバイパスするクエリが発生するため、Umbrellaリゾルバは HTTPS DNSレコードタイプのクエリに対してREFUSED応答を返します。これは、このような指定が検出されないことを意味します。

アプリケーションによって指定された暗号化されたリゾルバ

優先度の高いメカニズムで他の暗号化リゾルバが検出されない場合、アプリ作成者はフォールバック暗号化リゾルバを指定できます。このリゾルバは、代わりにDHCPまたはRAによって設定された暗号化されていないリゾルバを使用する場合にのみ使用できます。

現在、アンマネージドデバイスに対してこれらのリゾルバの使用を防止する唯一の既知の方法は、ファイアウォールで既知のDoHプロバイダーのIPをブロックすることです。このようなシナリオでiOSが暗号化されていないDNSにフォールバックできるかどうかは、まだ不明です。

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て、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。