Konfigurieren der Auswahl der DNS-Resolver in iOS 14 und macOS 11

Inhalt

Einleitung

In diesem Dokument werden die Änderungen bei Umbrella von iOS 14- und macOS 11-Updates beschrieben, die Unterstützung für verschlüsseltes DNS beinhalten.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Security Connector (CSC)
- macOS Umbrella Roaming-Client (RC)
- macOS AnyConnect-Client (AC)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Apple gab die Veröffentlichung von iOS 14 am 16. September 2020 bekannt. Unter anderem unterstützen iOS 14 und macOS 11 verschlüsseltes DNS und die Möglichkeit für Domäneninhaber, einen DNS-Resolver ihrer Wahl festzulegen. Diese Änderung hat direkte Auswirkungen auf die Fähigkeit von Umbrella, einige Domänennamen aufzulösen, was bedeutet, dass Richtlinien und Reporting für diese Domänen betroffen wären.

Die Änderungen in iOS 14 und macOS 11 haben drei wesentliche Auswirkungen:

1. Benutzer können einen systemweiten DoH-Resolver angeben, der den durch DHCP oder RA festgelegten DNS-Resolver überschreiben kann.

2. Domäneninhaber können DoH-Resolver festlegen, die den DNS-Resolver überschreiben können, der von DHCP oder RA für Abfragen ihrer Domäne festgelegt wurde.

3. Apps können einen DoH-Resolver angeben, der den DNS-Resolver überschreiben kann, der von DHCP oder RA für Abfragen von ihrer App festgelegt wurde. Umbrella hat keine Einsicht, welche Apps dies tun.

Mit diesen Updates hat Apple keinen Mechanismus zur Erkennung eines verschlüsselten Resolvers bereitgestellt, der auf derselben IP wie der vom Netzwerk bereitgestellte Resolver ausgeführt wird. Das bedeutet, dass Netzwerke, die Abfragen an die Umbrella Resolver weiterleiten, kein Upgrade auf den DoH-Dienst von Umbrella unter doh.umbrella.com durchführen können.

Seit dem 1. Oktober 2020 verhindert Umbrella die Erkennung von DoH-Resolvern, die von Domänenbesitzern festgelegt wurden. Diese Domänen werden so daran gehindert, den Umbrella-Schutz zu umgehen. Umbrella kann die Effekte #1 und #3 nur verhindern, wenn ein Umbrella-Client auf dem Gerät installiert ist. Kunden, die Schutz vor diesen Effekten benötigen, können die Blockierung der IPs bekannter DoH-Anbieter in Betracht ziehen, wie in diesem Artikel beschrieben.

Vollständige Details zu den Änderungen in iOS 14 und macOS 11 finden Sie in diesem Artikel.

Auswirkungen auf Umbrella-Benutzer

Cisco Security Connector (CSC)

iOS-Geräte, die den CSC verwenden, können von dieser Änderung nicht betroffen sein, da sie den DNS-Proxy-Mechanismus von Apple verwenden, der Vorrang vor dem Erkennungsmechanismus für iOS-Resolver hat.

macOS Umbrella Roaming-Client (RC)

macOS-Geräte, die den RC verwenden, können von dieser Änderung betroffen sein, da der macOS RC derzeit einen DNS-Proxy auf localhost ausführt, der von macOS als unverschlüsselter Resolver angesehen wird. Der RC verwendet DNSCrypt für die Kommunikation mit den Umbrella-Resolvern.

Umbrella bietet Unterstützung für die DoH-Erkennung in unserem AnyConnect Roaming Security-Modul (siehe AC unten), das den Apple DNS Proxy Provider zur Kontrolle von DNS nutzt. Diese Unterstützung ist derzeit nicht für den RC vorgesehen. Umbrella-Pakete sind für AC lizenziert. Siehe unseren Artikel.

macOS AnyConnect-Client (AC)

macOS-Geräte, die den AC verwenden, können von dieser Änderung nicht betroffen sein, da sie derzeit den DNS-Proxy-Mechanismus von Apple verwenden, der Vorrang vor dem Erkennungsmechanismus des macOS-Resolvers hat.

iOS- oder MacOS-Geräte hinter einer virtuellen Appliance (VA)

iOS oder macOS, auf denen CSC, RC oder AC nicht installiert ist, kann von dieser Änderung betroffen sein. Solche Geräte hinter einem VA können daher Anfragen direkt an konfigurierte DoH-Server senden und die virtuelle Appliance umgehen.

iOS- oder macOS-Geräte hinter einem registrierten Netzwerk

iOS oder macOS ohne installierten CSC, RC oder AC sind von dieser Änderung nicht betroffen. Solche Geräte hinter einem registrierten Netzwerk können daher Anfragen direkt an konfigurierte DoH-Server senden und dabei den lokalen Resolver oder Umbrella umgehen.

Umbrella und verschlüsseltes DNS

Umbrella unterstützt die Verwendung von verschlüsseltem DNS und Initiativen zur Förderung der Verwendung von verschlüsseltem DNS. Die Umbrella-Resolver unterstützen DNSCrypt seit 2011 als Mittel zur Verschlüsselung des DNS-Verkehrs, und alle Umbrella-Client-Software unterstützt die Verwendung von DNSCrypt und verwendet es in ihren Standardkonfigurationen. Darüber hinaus unterstützen wir seit Februar 2020 DNS over HTTPS (DoH).

Umbrella führt zusätzlich eine DNSSEC-Validierung für Abfragen durch, die an Upstream-Behörden gesendet werden, um die Datenintegrität für alle Datensätze in unserem Cache sicherzustellen.

Detaillierte DNS-Änderungen in iOS 14 und macOS 11

iOS 14 und macOS 11 führen einen neuen Mechanismus zur Auswahl eines DNS-Resolvers ein. Kunden, die spezifische Details benötigen, können dies bei Apple bestätigen. Cisco ist sich jedoch

bewusst, dass ein DNS-Resolver mit der hier beschriebenen Priorität ausgewählt werden kann:

1. Auflösung der Testzonen des Captive Portals mithilfe des vom Netzwerk bereitgestellten DNS-Resolvers

2. VPN- oder DNS-Proxy-Konfigurationen (wie der Cisco Security Connector für iOS) und DNS-Resolver, die durch Unternehmensrichtlinien (wie MDM oder OTA) festgelegt werden. (Weitere Informationen zum Festlegen von DNS-Richtlinien erhalten Sie von Ihrem MDM-Anbieter.)

3. Systemweite verschlüsselte Resolver, die direkt von den Gerätebesitzern konfiguriert wurden

4. Verschlüsselte Resolver, die von Domäneninhabern festgelegt wurden

5. Von Apps designierter verschlüsselter Resolver

6. Nicht verschlüsselte Resolver (wie über DHCP oder RA angegebene Resolver)

Insbesondere sehen wir die Zahlen 3, 4 und 5 als wesentliche Änderungen bei der Resolverauswahl an, die sich direkt auf die Fähigkeit von Umbrella-Administratoren auswirken können, die Verwendung der Umbrella-Resolver in ihren Netzwerken vollständig durchzusetzen.

Systemweite verschlüsselte Resolver

Benutzer können eine Konfigurationsprofil-App von einem DNS-Anbieter installieren, mit der sie einen systemweiten verschlüsselten Resolver konfigurieren können. Dieser Resolver kann für alle Abfragen verwendet werden, unabhängig vom DNS-Resolver, der vom Netzwerk über DHCP oder RA angegeben wird.

Derzeit ist die einzige bekannte Methode, um die Verwendung dieser Resolver für nicht verwaltete Geräte zu verhindern, die Blockierung der IPs bekannter DoH-Anbieter an der Firewall. Dies kann zu einer Warnung für den Benutzer des iOS-Geräts führen, und das Gerät kann nicht auf unverschlüsselten DNS zurückgreifen, d. h. es kann keine DNS-Hostnamen auflösen.

Von Domäneninhabern designierte verschlüsselte Resolver

Der Besitzer einer DNS-Zone kann einen bestimmten Resolver festlegen, der zum Auflösen der Zone verwendet wird. In iOS 14 und macOS 11 können nur DoH-Resolver festgelegt werden. Diese Bezeichnung wird mithilfe eines dedizierten DNS-Eintragstyps (Typ 65 mit dem Namen "HTTPS") vorgenommen und entweder durch DNSSEC oder bekannte URIs validiert.

Da solche Bezeichnungen dazu führen würden, dass Abfragen Umbrella umgehen, geben die Umbrella-Resolver eine REFUSED-Antwort für Abfragen des HTTPS-DNS-Datensatztyps zurück, was bedeutet, dass solche Bezeichnungen nicht erkannt werden.

Von Apps designierter verschlüsselter Resolver

Ein App-Ersteller kann einen Fallback-verschlüsselten Resolver angeben, wenn in keinem der Mechanismen mit höherer Priorität ein anderer verschlüsselter Resolver erkannt wird. Dieser

Resolver kann nur verwendet werden, wenn als Alternative der durch DHCP oder RA festgelegte unverschlüsselte Resolver verwendet werden kann.

Derzeit ist die einzige bekannte Methode, um die Verwendung dieser Resolver für nicht verwaltete Geräte zu verhindern, die Blockierung der IPs bekannter DoH-Anbieter an der Firewall. Es ist noch nicht bekannt, ob iOS in einem solchen Szenario auf unverschlüsseltes DNS zurückgreifen kann.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.