Configure DNS Resolver Selection in iOS 14 and macOS 11

Contents

Introduction

This document describes changes in Umbrella from iOS 14 and macOS 11 updates that include support for encrypted DNS.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

Apple announced the release of iOS 14 on Sept 16, 2020. Among other changes, iOS 14 and macOS 11 include support for encrypted DNS, and the ability for domain owners to designate a DNS resolver of their choosing. This change has a direct effect on the ability of Umbrella to resolve some domain names, meaning that policy and reporting for those domains would be affected.

The changes in iOS 14 and macOS 11 have 3 primary effects:

1. Users can able to specify a system wide DoH resolver that can override the DNS resolver set by DHCP or RA.

2. Domain owners can designate DoH resolvers that can override the DNS resolver set by DHCP or RA for queries made for their domain.

3. Apps can specify a DoH resolver that can override the DNS resolver set by DHCP or RA for queries made from their app. Umbrella does not have visibility into which apps are doing so.

With these updates, Apple has not included a mechanism to discover an encrypted resolver running on the same IP as the network provisioned resolver, meaning that networks forwarding queries to the Umbrella resolvers can not upgrade to Umbrella's DoH service at doh.umbrella.com.

As of Oct 1, 2020, Umbrella prevents the discovery of DoH resolver that have been designated by domain owners, which prevents those domains from bypassing Umbrella protection. Umbrella cannot prevent effects #1 and #3 unless an Umbrella client is installed on the device. Customers that need protection against those effects can consider blocking the IPs of known DoH providers as described in this article.

For full details on the changes in iOS 14 and macOS 11, continue reading this article.

Impact to Umbrella Users

Cisco Security Connector (CSC)

iOS device using the CSC cannot be affected by this change, as it uses Apple's DNS proxy mechanism which has priority over iOS' resolver discovery mechanism.

macOS Umbrella Roaming Client (RC)

macOS devices using the RC can be affected by this change, as the macOS RC currently runs a DNS proxy on localhost, which is viewed by macOS as an unencrypted resolver. The RC uses DNSCrypt to communicate with the Umbrella resolvers.

Umbrella has delivered support enforcing against DoH discovery in our AnyConnect Roaming Security Module (See AC below) which makes use of the Apple DNS Proxy Provider to control DNS. This support is not scheduled to be included in the RC at this time. Umbrella packages are licensed for AC. See our article.

macOS AnyConnect Client (AC)

macOS devices using the AC cannot be affected by this change, as they currently use Apple's DNS Proxy mechanism which has priority over macOS' resolver discovery mechanism.

iOS or macOS devices behind a Virtual Appliance (VA)

iOS or macOS that do not have the CSC, RC, or AC installed can be affected by this change. Such devices behind a VA can therefore send queries directly to configured DoH servers, bypassing the Virtual Appliance.

iOS or macOS devices behind a registered network

iOS or macOS that do not have the CSC, RC, or AC installed are not affected by this change. Such devices behind a registered network can therefore send queries directly to configured DoH servers, bypassing either the local resolver or Umbrella.

Umbrella and Encrypted DNS

Umbrella fully supports the use of encrypted DNS and initiatives to advance the use of encrypted DNS. The Umbrella resolvers have supported DNSCrypt as a means to encrypt DNS traffic since 2011, and all Umbrella client software supports the use of DNSCrypt and uses it in their default configurations. Additionally, we have supported DNS over HTTPS (DoH) since February 2020.

Umbrella additionally performs DNSSEC validation on queries sent to upstream authorities in order to ensure data integrity for all records in our cache.

Detailed DNS changes in iOS 14 and macOS 11

iOS 14 and macOS 11 introduce a new mechanism for selecting a DNS resolver. While customers requiring specific details can confirm with Apple, Cisco's understanding of the mechanism is that a DNS resolver can be selected with the priority described here:

1. Resolution of captive portal test zones using the network provided DNS resolver

2. VPN or DNS proxy configurations (like the Cisco Security Connector for iOS) and DNS resolvers set by enterprise policies (like MDM or OTA). (Please consult your MDM vendor for details on setting DNS policies)

3. System wide encrypted resolvers configured directly by device owners

4. Encrypted resolvers designated by domain owners

5. Encrypted resolver designated by apps

6. Unencrypted resolvers (like resolvers specified via DHCP or RA)

In particular, we view numbers 3, 4, and 5 as significant changes to resolver selection that can have a direct impact on the ability for Umbrella administrators to fully enforce the use of the Umbrella resolvers on their networks.

System wide encrypted resolvers

Users can install a configuration profile app from a DNS provider which allows them to configure a system wide encrypted resolver. This resolver can be used for all queries, regardless of the DNS resolver specified by the network via DHCP or RA.

Currently, the only known method to prevent the use of these resolvers for unmanaged devices is to block the IPs of known DoH providers at the firewall. Doing so can result in a warning for the user of the iOS device, and the device cannot fall back to unencrypted DNS, meaning it cannot be able to resolve DNS

hostnames.

Encrypted resolvers designated by domain owners

The owner of a DNS zone can designate a specific resolver to be used for resolving its zone. In iOS 14 and macOS 11, only DoH resolvers can be designated. This designation is made using a dedicated DNS record type (type 65, named “HTTPS”), and validated either by DNSSEC or well known URIs.

As such designations would result in queries bypassing Umbrella, the Umbrella resolvers return a REFUSED response for queries for the HTTPS DNS record type, meaning that such designations would not be discovered.

Encrypted resolver designated by apps

An app creator can specify a fallback encrypted resolver if no other encrypted resolver is discovered in any of the higher priority mechanisms. This resolver can only be used if the alternative would be to use the unencrypted resolver set by DHCP or RA.

Currently, the only known method to prevent the use of these resolvers for unmanaged devices is to block the IPs of known DoH providers at the firewall. It is not yet known if iOS can fall back to unencrypted DNS in such a scenario.