Configuración de la selección de resolución de DNS en iOS 14 y macOS 11

Contenido

Introducción

Este documento describe los cambios en Umbrella de las actualizaciones de iOS 14 y macOS 11 que incluyen soporte para DNS cifrado.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Apple anunció el lanzamiento de iOS 14 el 16 de septiembre de 2020. Entre otros cambios, iOS 14 y macOS 11 incluyen compatibilidad con DNS cifrado y la capacidad de los propietarios de dominios para designar una resolución de DNS de su elección. Este cambio tiene un efecto directo en la capacidad de Umbrella para resolver algunos nombres de dominio, lo que significa que la política y los informes para esos dominios se verían afectados.

Los cambios en iOS 14 y macOS 11 tienen 3 efectos principales:

1. Los usuarios pueden especificar una resolución DoH para todo el sistema que puede invalidar la resolución DNS establecida por DHCP o RA.

2. Los propietarios de dominios pueden designar resolvers DoH que pueden invalidar la resolución DNS establecida por DHCP o RA para las consultas realizadas para su dominio.

3. Las aplicaciones pueden especificar una resolución de DoH que pueda invalidar la resolución de DNS establecida por DHCP o RA para las consultas realizadas desde su aplicación. Umbrella no tiene visibilidad de qué aplicaciones lo están haciendo.

Con estas actualizaciones, Apple no ha incluido un mecanismo para detectar una resolución cifrada que se ejecute en la misma IP que la resolución aprovisionada por la red, lo que significa que las redes que reenvían consultas a las resoluciones de Umbrella no pueden actualizar al servicio DoH de Umbrella en doh.umbrella.com.

A partir del 1 de octubre de 2020, Umbrella impide la detección de solucionadores de DoH designados por los propietarios de dominios, lo que impide que estos pasen por alto la protección de Umbrella. Umbrella no puede evitar los efectos #1 y #3 a menos que esté instalado un cliente Umbrella en el dispositivo. Los clientes que necesiten protección frente a estos efectos pueden considerar el bloqueo de las IP de los proveedores de DoH conocidos, tal y como se describe en este artículo.

Para obtener más información sobre los cambios en iOS 14 y macOS 11, sigue leyendo este artículo.

Impacto para los usuarios generales

Cisco Security Connector (CSC)

Este cambio no puede afectar a los dispositivos iOS que utilizan CSC, ya que utilizan el mecanismo de proxy DNS de Apple, que tiene prioridad sobre el mecanismo de detección de resolución de iOS.

macOS Umbrella Roaming Client (RC)

Los dispositivos macOS que usan el RC pueden verse afectados por este cambio, ya que el MAC OS RC actualmente ejecuta un proxy DNS en el host local, que macOS ve como una resolución sin cifrar. El RC utiliza DNSCrypt para comunicarse con los resolvers de Umbrella.

Umbrella ha proporcionado compatibilidad con la aplicación frente a la detección de DoH en nuestro módulo de seguridad de roaming de AnyConnect (consulte AC a continuación), que hace uso del proveedor de proxy DNS de Apple para controlar DNS. Este soporte no está programado para ser incluido en el RC en este momento. Los paquetes Umbrella tienen licencia para AC. Vea nuestro artículo.

cliente AnyConnect (AC) para macOS

Los dispositivos macOS que utilizan el AC no pueden verse afectados por este cambio, ya que actualmente utilizan el mecanismo de proxy DNS de Apple que tiene prioridad sobre el mecanismo de detección de resolución de macOS.

Dispositivos iOS o macOS detrás de un dispositivo virtual (VA)

Este cambio puede afectar a iOS o macOS que no tengan instalado CSC, RC o AC. Por lo tanto, estos dispositivos detrás de un VA pueden enviar consultas directamente a los servidores DoH configurados, omitiendo el dispositivo virtual.

Dispositivos iOS o macOS detrás de una red registrada

Este cambio no afecta a iOS o macOS que no tengan instalado CSC, RC o AC. Estos dispositivos detrás de una red registrada pueden, por lo tanto, enviar consultas directamente a los servidores DoH configurados, omitiendo la resolución local o Umbrella.

Paraguas y DNS cifrado

Umbrella es totalmente compatible con el uso de DNS cifrado y las iniciativas para avanzar en el uso de DNS cifrado. Los resolvers de Umbrella han soportado DNSCrypt como medio para cifrar el tráfico DNS desde 2011, y todo el software cliente de Umbrella soporta el uso de DNSCrypt y lo utiliza en sus configuraciones predeterminadas. Además, admitimos DNS sobre HTTPS (DoH) desde febrero de 2020.

Umbrella también realiza la validación de DNSSEC en las consultas enviadas a las autoridades ascendentes para garantizar la integridad de los datos de todos los registros de nuestra caché.

Cambios detallados de DNS en iOS 14 y macOS 11

iOS 14 y macOS 11 introducen un nuevo mecanismo para seleccionar una resolución de DNS. Mientras que los clientes que necesitan detalles específicos pueden confirmar con Apple, Cisco entiende que el mecanismo es que se puede seleccionar una resolución de DNS con la prioridad

que se describe a continuación:

1. Resolución de las zonas de prueba del portal cautivo mediante la resolución DNS proporcionada por la red

2. Configuraciones de VPN o proxy DNS (como Cisco Security Connector para iOS) y resoluciones DNS establecidas por políticas empresariales (como MDM u OTA). (Consulte a su proveedor de MDM para obtener más información sobre la configuración de políticas DNS)

3. Resoluciones cifradas en todo el sistema configuradas directamente por los propietarios de los dispositivos

4. Resoluciones cifradas designadas por los propietarios de dominio

5. Resolución cifrada designada por las aplicaciones

6. Resoluciones no cifradas (como las resoluciones especificadas mediante DHCP o RA)

En particular, consideramos que los números 3, 4 y 5 son cambios significativos en la selección de resolución que pueden tener un impacto directo en la capacidad de los administradores de Umbrella para aplicar plenamente el uso de los resolvers de Umbrella en sus redes.

Resoluciones cifradas en todo el sistema

Los usuarios pueden instalar una aplicación de perfil de configuración desde un proveedor DNS que les permite configurar una resolución cifrada en todo el sistema. Esta resolución se puede utilizar para todas las consultas, independientemente de la resolución de DNS especificada por la red mediante DHCP o RA.

Actualmente, el único método conocido para evitar el uso de estos resolvers para dispositivos no administrados es bloquear las IP de los proveedores de DoH conocidos en el firewall. Esto puede dar lugar a una advertencia para el usuario del dispositivo iOS y el dispositivo no puede recurrir a DNS no cifrado, lo que significa que no puede resolver los nombres de host DNS.

Resoluciones cifradas designadas por los propietarios de dominio

El propietario de una zona DNS puede designar una resolución específica que se utilizará para resolver su zona. En iOS 14 y macOS 11, solo se pueden designar resolvers DoH. Esta designación se realiza mediante un tipo de registro DNS dedicado (tipo 65, denominado "HTTPS") y validado por DNSSEC o por URI conocidos.

Como tales designaciones resultarían en consultas que omitan a Umbrella, los resolvers de Umbrella devuelven una respuesta REFUSED para consultas para el tipo de registro HTTPS DNS, lo que significa que tales designaciones no serían descubiertas.

Resolución cifrada designada por las aplicaciones

El creador de una aplicación puede especificar una resolución cifrada de reserva si no se

descubre ninguna otra resolución cifrada en ninguno de los mecanismos de mayor prioridad. Esta resolución sólo se puede utilizar si la alternativa es utilizar la resolución sin cifrar establecida por DHCP o RA.

Actualmente, el único método conocido para evitar el uso de estos resolvers para dispositivos no administrados es bloquear las IP de los proveedores de DoH conocidos en el firewall. Todavía no se sabe si iOS puede recurrir a DNS no cifrado en tal escenario.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).