Configurer la sélection du résolveur DNS dans iOS 14 et macOS 11

Table des matières

Introduction

Ce document décrit les changements dans Umbrella à partir des mises à jour d'iOS 14 et macOS 11 qui incluent la prise en charge du DNS chiffré.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Connecteur de sécurité Cisco (CSC)
- Client d'itinérance macOS Umbrella (RC)
- Client macOS AnyConnect (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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Apple a annoncé la sortie d'iOS 14 le 16 septembre 2020. Entre autres changements, iOS 14 et macOS 11 incluent la prise en charge du DNS chiffré et la possibilité pour les propriétaires de domaines de désigner un résolveur DNS de leur choix. Cette modification a un effet direct sur la capacité d'Umbrella à résoudre certains noms de domaine, ce qui signifie que la politique et les rapports pour ces domaines seraient affectés.

Les modifications apportées à iOS 14 et macOS 11 ont trois effets principaux :

1. Les utilisateurs peuvent spécifier un résolveur DoH à l’échelle du système qui peut remplacer le résolveur DNS défini par DHCP ou RA.

2. Les propriétaires de domaine peuvent désigner des résolveurs DoH qui peuvent remplacer le résolveur DNS défini par DHCP ou RA pour les requêtes effectuées pour leur domaine.

3. Les applications peuvent spécifier un résolveur DoH qui peut remplacer le résolveur DNS défini par DHCP ou RA pour les requêtes effectuées à partir de leur application. Umbrella n'a pas de visibilité sur les applications qui le font.

Avec ces mises à jour, Apple n'a pas inclus de mécanisme permettant de détecter un résolveur crypté s'exécutant sur la même adresse IP que le résolveur provisionné sur le réseau, ce qui signifie que les réseaux qui transfèrent des requêtes aux résolveurs Umbrella ne peuvent pas effectuer la mise à niveau vers le service DoH d'Umbrella à l'adresse doh.umbrella.com.

Depuis le 1er octobre 2020, Umbrella empêche la découverte de résolveurs DoH désignés par les propriétaires de domaines, ce qui empêche ces domaines de contourner la protection Umbrella. Umbrella ne peut pas empêcher les effets #1 et #3 à moins qu'un client Umbrella ne soit installé sur le périphérique. Les clients qui ont besoin d'une protection contre ces effets peuvent envisager de bloquer les adresses IP des fournisseurs DoH connus, comme décrit dans cet article.

Pour plus de détails sur les changements dans iOS 14 et macOS 11, continuer la lecture de cet article.

Impact sur les utilisateurs parapluie

Connecteur de sécurité Cisco (CSC)

Le périphérique iOS utilisant le CSC ne peut pas être affecté par ce changement, car il utilise le mécanisme proxy DNS d'Apple qui a la priorité sur le mécanisme de détection de résolveur d'iOS.

Client d'itinérance macOS Umbrella (RC)

Les périphériques macOS utilisant le RC peuvent être affectés par ce changement, car le RC macOS exécute actuellement un proxy DNS sur localhost, qui est vu par macOS comme un résolveur non chiffré. Le RC utilise DNSCrypt pour communiquer avec les résolveurs Umbrella.

Umbrella a fourni une assistance contre la découverte DoH dans notre module de sécurité d'itinérance AnyConnect (voir AC ci-dessous) qui utilise le fournisseur de proxy DNS d'Apple pour contrôler DNS. Il n'est pas prévu que cette assistance soit incluse dans le CR pour le moment. Les packages Umbrella sont concédés sous licence pour AC. Voir notre article.

Client macOS AnyConnect (AC)

Les périphériques macOS utilisant le contrôle d'accès ne peuvent pas être affectés par cette modification, car ils utilisent actuellement le mécanisme proxy DNS d'Apple, qui a la priorité sur le mécanisme de détection du résolveur de macOS.

Périphériques iOS ou macOS derrière une appliance virtuelle (VA)

Les systèmes iOS ou macOS sur lesquels CSC, RC ou AC ne sont pas installés peuvent être affectés par cette modification. Ces périphériques derrière un VA peuvent donc envoyer des requêtes directement aux serveurs DoH configurés, en contournant l'appliance virtuelle.

Périphériques iOS ou macOS derrière un réseau enregistré

Les systèmes iOS ou macOS sur lesquels CSC, RC ou AC ne sont pas installés ne sont pas concernés par cette modification. Ces périphériques derrière un réseau enregistré peuvent donc envoyer des requêtes directement aux serveurs DoH configurés, en contournant soit le résolveur local, soit Umbrella.

Parapluie et DNS chiffré

Umbrella prend entièrement en charge l'utilisation du DNS chiffré et les initiatives visant à faire progresser l'utilisation du DNS chiffré. Les résolveurs Umbrella prennent en charge DNSCrypt comme moyen de crypter le trafic DNS depuis 2011, et tous les logiciels clients Umbrella prennent en charge l'utilisation de DNSCrypt et l'utilisent dans leurs configurations par défaut. En outre, nous prenons en charge le DNS sur HTTPS (DoH) depuis février 2020.

Umbrella effectue également une validation DNSSEC sur les requêtes envoyées aux autorités en amont afin de garantir l'intégrité des données pour tous les enregistrements de notre cache.

Modifications DNS détaillées dans iOS 14 et macOS 11

iOS 14 et macOS 11 introduisent un nouveau mécanisme de sélection d'un résolveur DNS. Alors que les clients ayant besoin de détails spécifiques peuvent le confirmer auprès d'Apple, Cisco comprend le mécanisme selon lequel un résolveur DNS peut être sélectionné avec la priorité décrite ici :

1. Résolution des zones de test du portail captif à l’aide du résolveur DNS fourni par le réseau

2. Configurations de proxy VPN ou DNS (comme le connecteur de sécurité Cisco pour iOS) et résolveurs DNS définis par les stratégies d'entreprise (comme MDM ou OTA). (Veuillez consulter votre fournisseur MDM pour plus de détails sur la définition des stratégies DNS)

3. Résolveurs chiffrés à l’échelle du système configurés directement par les propriétaires de périphériques

4. Résolveurs chiffrés désignés par les propriétaires de domaine

5. Résolveur chiffré désigné par les applications

6. Résolveurs non chiffrés (comme les résolveurs spécifiés via DHCP ou RA)

En particulier, nous considérons les numéros 3, 4 et 5 comme des modifications importantes de la sélection du résolveur qui peuvent avoir un impact direct sur la capacité des administrateurs Umbrella d'appliquer pleinement l'utilisation des résolveurs Umbrella sur leurs réseaux.

Résolveurs chiffrés au niveau du système

Les utilisateurs peuvent installer une application de profil de configuration à partir d'un fournisseur DNS qui leur permet de configurer un résolveur chiffré à l'échelle du système. Ce résolveur peut être utilisé pour toutes les requêtes, quel que soit le résolveur DNS spécifié par le réseau via DHCP ou RA.

Actuellement, la seule méthode connue pour empêcher l'utilisation de ces résolveurs pour les périphériques non gérés est de bloquer les adresses IP des fournisseurs DoH connus au niveau du pare-feu. Cela peut entraîner un avertissement pour l'utilisateur du périphérique iOS, et le périphérique ne peut pas revenir à un DNS non chiffré, ce qui signifie qu'il ne peut pas résoudre les noms d'hôte DNS.

Résolveurs chiffrés désignés par les propriétaires de domaine

Le propriétaire d’une zone DNS peut désigner un résolveur spécifique à utiliser pour la résolution de sa zone. Dans iOS 14 et macOS 11, seuls les résolveurs DoH peuvent être désignés. Cette désignation est effectuée à l'aide d'un type d'enregistrement DNS dédié (type 65, nommé « HTTPS »), et validée soit par DNSSEC, soit par des URI bien connus.

Comme de telles désignations résulteraient en des requêtes contournant Umbrella, les résolveurs Umbrella renvoient une réponse REFUSED pour les requêtes pour le type d'enregistrement DNS HTTPS, ce qui signifie que de telles désignations ne seraient pas découvertes.

Résolveur chiffré désigné par les applications

Un créateur d'application peut spécifier un résolveur chiffré de secours si aucun autre résolveur chiffré n'est découvert dans l'un des mécanismes de priorité supérieure. Ce résolveur ne peut être utilisé que si l'autre solution consiste à utiliser le résolveur non chiffré défini par DHCP ou RA.

Actuellement, la seule méthode connue pour empêcher l'utilisation de ces résolveurs pour les périphériques non gérés est de bloquer les adresses IP des fournisseurs DoH connus au niveau du pare-feu. On ne sait pas encore si iOS peut revenir à un DNS non chiffré dans un tel scénario.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.