Configurar a seleção do DNS Resolver no iOS 14 e no macOS 11

Contents

Introdução

Este documento descreve as alterações no Umbrella a partir das atualizações do iOS 14 e macOS 11 que incluem suporte para DNS criptografado.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Security Connector (CSC)
- Cliente de Roaming Umbrella (RC) para MacOS
- Cliente AnyConnect (AC) do macOS

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

A Apple anunciou o lançamento do iOS 14 em 16 de setembro de 2020. Entre outras mudanças, o iOS 14 e o macOS 11 incluem suporte para DNS criptografado e a capacidade dos proprietários de domínio de designar um resolvedor de DNS de sua escolha. Essa alteração tem um efeito direto na capacidade do Umbrella de resolver alguns nomes de domínio, o que significa que a política e os relatórios para esses domínios seriam afetados.

As alterações no iOS 14 e no macOS 11 têm 3 efeitos principais:

1. Os usuários podem especificar um resolvedor DoH para todo o sistema que possa substituir o resolvedor DNS definido por DHCP ou RA.

2. Os proprietários de domínio podem designar resolvedores do DoH que podem substituir o resolvedor DNS definido por DHCP ou RA para consultas feitas para seu domínio.

3. Os aplicativos podem especificar um resolvedor do DoH que pode substituir o resolvedor DNS definido por DHCP ou RA para consultas feitas de seu aplicativo. A Umbrella não tem visibilidade sobre quais aplicativos estão fazendo isso.

Com essas atualizações, a Apple não incluiu um mecanismo para descobrir um resolvedor criptografado em execução no mesmo IP que o resolvedor provisionado pela rede, o que significa que as redes que encaminham consultas para os resolvedores Umbrella não podem atualizar para o serviço DoH da Umbrella em doh.umbrella.com.

A partir de 1º de outubro de 2020, o Umbrella impede a descoberta de resolvedor DoH que foram designados por proprietários de domínio, o que impede que esses domínios contornem a proteção Umbrella. O Umbrella não pode evitar efeitos #1 e #3, a menos que um cliente Umbrella esteja instalado no dispositivo. Os clientes que precisam de proteção contra esses efeitos podem considerar bloquear os IPs de provedores conhecidos de DoH, conforme descrito neste artigo.

Para obter detalhes completos sobre as alterações no iOS 14 e no macOS 11, continue lendo este artigo.

Impacto para usuários do Umbrella

Cisco Security Connector (CSC)

O dispositivo iOS que usa o CSC não pode ser afetado por essa alteração, pois ele usa o mecanismo de proxy DNS da Apple, que tem prioridade sobre o mecanismo de descoberta do resolvedor do iOS.

Cliente de Roaming Umbrella (RC) para MacOS

os dispositivos macOS que usam o RC podem ser afetados por essa alteração, pois o macOS RC atualmente executa um proxy DNS no localhost, que é visto pelo macOS como um resolvedor não criptografado. O RC usa DNSCrypt para se comunicar com os resolvedores Umbrella.

A Umbrella forneceu suporte para aplicação contra descoberta do DoH em nosso AnyConnect Roaming Security Module (Consulte AC abaixo), que usa o Apple DNS Proxy Provider para controlar o DNS. Este suporte não está programado para ser incluído no RC no momento. Os pacotes Umbrella são licenciados para AC. Veja nosso artigo.

Cliente AnyConnect (AC) do macOS

Os dispositivos macOS que usam o AC não podem ser afetados por essa alteração, pois atualmente usam o mecanismo DNS Proxy da Apple, que tem prioridade sobre o mecanismo de descoberta de resolvedor do macOS.

Dispositivos iOS ou macOS atrás de um dispositivo virtual (VA)

O iOS ou o macOS que não têm o CSC, o RC ou o AC instalado pode ser afetado por essa alteração. Esses dispositivos atrás de um VA podem, portanto, enviar consultas diretamente para servidores DoH configurados, ignorando o Virtual Appliance.

Dispositivos iOS ou macOS por trás de uma rede registrada

iOS ou macOS que não têm o CSC, o RC ou o AC instalado não são afetados por essa alteração. Tais dispositivos por trás de uma rede registrada podem, portanto, enviar consultas diretamente para servidores DoH configurados, ignorando o resolvedor local ou o Umbrella.

DNS Umbrella e criptografado

O Umbrella suporta totalmente o uso de DNS criptografado e iniciativas para avançar o uso de DNS criptografado. Os resolvedores do Umbrella têm suportado o DNSCrypt como um meio de criptografar o tráfego DNS desde 2011, e todo o software cliente Umbrella suporta o uso do DNSCrypt e o usa em suas configurações padrão. Além disso, oferecemos suporte a DNS sobre HTTPS (DoH) desde fevereiro de 2020.

Além disso, a Umbrella executa a validação DNSSEC em consultas enviadas a autoridades upstream, a fim de garantir a integridade dos dados para todos os registros em nosso cache.

Alterações detalhadas de DNS no iOS 14 e no macOS 11

iOS 14 e macOS 11 introduzem um novo mecanismo para selecionar um resolvedor de DNS. Embora os clientes que precisam de detalhes específicos possam confirmar com a Apple, o entendimento da Cisco sobre o mecanismo é que um resolvedor de DNS pode ser selecionado com a prioridade descrita aqui:

1. Resolução de zonas de teste do portal cativo usando o resolvedor DNS fornecido pela rede

2. Configurações de proxy VPN ou DNS (como o Cisco Security Connector para iOS) e resolvedores DNS definidos pelas políticas corporativas (como MDM ou OTA). (Consulte o fornecedor de MDM para obter detalhes sobre a definição de políticas DNS)

3. Resolvedores criptografados em todo o sistema configurados diretamente pelos proprietários do dispositivo

4. Resolvedores criptografados designados pelos proprietários do domínio

5. Resolvedor criptografado designado por aplicativos

6. Resolvedores não criptografados (como resolvedores especificados via DHCP ou RA)

Em particular, vemos os números 3, 4 e 5 como alterações significativas na seleção do resolvedor que podem ter um impacto direto na capacidade dos administradores do Umbrella de aplicar totalmente o uso dos resolvedores do Umbrella em suas redes.

Resolvedores criptografados em todo o sistema

Os usuários podem instalar um aplicativo de perfil de configuração a partir de um provedor DNS que lhes permite configurar um resolvedor criptografado em todo o sistema. Este resolvedor pode ser usado para todas as consultas, independentemente do resolvedor DNS especificado pela rede via DHCP ou RA.

Atualmente, o único método conhecido para impedir o uso desses resolvedores para dispositivos não gerenciados é bloquear os IPs de provedores DoH conhecidos no firewall. Isso pode resultar em um aviso para o usuário do dispositivo iOS, e o dispositivo não pode retornar para DNS não criptografado, o que significa que ele não pode resolver nomes de host DNS.

Resolvedores criptografados designados pelos proprietários do domínio

O proprietário de uma zona DNS pode designar um resolvedor específico a ser usado para resolver sua zona. No iOS 14 e no macOS 11, somente os resolvedores do DoH podem ser designados. Essa designação é feita usando um tipo de registro DNS dedicado (tipo 65, chamado "HTTPS") e validado pelo DNSSEC ou por URIs bem conhecidos.

Como tais designações resultariam em consultas ignorando o Umbrella, os resolvedores do Umbrella retornam uma resposta REFUSED para consultas para o tipo de registro HTTPS DNS, significando que tais designações não seriam descobertas.

Resolvedor criptografado designado por aplicativos

Um criador de aplicativo pode especificar um resolvedor criptografado de fallback se nenhum outro resolvedor criptografado for descoberto em nenhum dos mecanismos de prioridade mais alta. Este resolvedor só poderá ser usado se a alternativa for usar o resolvedor não criptografado definido por DHCP ou RA.

Atualmente, o único método conhecido para impedir o uso desses resolvedores para dispositivos

não gerenciados é bloquear os IPs de provedores DoH conhecidos no firewall. Ainda não se sabe se o iOS pode retornar ao DNS não criptografado em tal cenário.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.