在iOS 14和macOS 11中配置DNS解析器选择

目录

简介

本文档介绍iOS 14和macOS 11更新中的Umbrella更改，包括支持加密DNS。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全连接器(CSC)
- macOS Umbrella漫游客户端(RC)
- macOS AnyConnect客户端(AC)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

Apple于2020年9月16日宣布发布iOS 14。除了其他更改，iOS 14和macOS 11还包括对加密DNS的支持，以及域所有者指定自己选择的DNS解析器的能力。此更改会直接影响Umbrella解析某些域名的能力，这意味着这些域的策略和报表会受到影响。

iOS 14和macOS 11中的更改有3个主要影响：

1.用户可以指定系统范围的DoH解析程序，该解析程序可以覆盖DHCP或RA设置的DNS解析程序。

2.域所有者可以指定DoH解析器，这些解析器可以覆盖DHCP或RA为其域进行的查询设置的DNS解析器。

3.应用可以指定一个DoH解析程序，该解析程序可以覆盖由DHCP或RA为从其应用发出的查询设置的DNS解析程序。Umbrella无法了解哪些应用正在这样做。

有了这些更新，Apple没有包含发现与网络调配的解析程序运行在同一IP上的加密解析程序的机制，这意味着将查询转发到Umbrella解析程序的网络无法升级到Umbrella的DoH服务(doh.umbrella.com)。

截至2020年10月1日，Umbrella阻止发现由域所有者指定的DoH解析器，从而防止这些域绕过Umbrella保护。Umbrella无法防止影#1和影#3，除非在设备上安装Umbrella客户端。需要防止这些影响的客户可以考虑按本文所述阻止已知DoH提供商的IP。

有关iOS 14和macOS 11更改的完整详细信息，请继续阅读本文内容。

对Umbrella用户的影响

思科安全连接器(CSC)

使用CSC的iOS设备不会受到此更改的影响，因为它使用的是苹果的DNS代理机制，其优先级高于iOS的解析程序发现机制。

macOS Umbrella漫游客户端(RC)

使用RC的macOS设备可能会受到此更改的影响，因为macOS RC当前在localhost上运行DNS代理，而macOS将其视为未加密的解析程序。RC使用DNSCrypt与Umbrella解析器通信。

Umbrella提供了在AnyConnect漫游安全模块（请参阅下面的AC）中实施针对DoH发现的支持，该模块利用Apple DNS代理提供程序控制DNS。此支持暂未安排在RC中。Umbrella软件包授权用于AC。请参阅我们的文章。

macOS AnyConnect客户端(AC)

使用AC的MacOS设备不会受到此更改的影响，因为它们当前使用的是优先于MacOS的解析程序发现机制的Apple DNS代理机制。

虚拟设备(VA)后面的iOS或macOS设备

未安装CSC、RC或AC的iOS或macOS可能会受到此更改的影响。因此，VA后面的此类设备可以绕

过虚拟设备，直接将查询发送到已配置的DoH服务器。

注册网络后面的iOS或macOS设备

未安装CSC、RC或AC的iOS或macOS不受此更改的影响。因此，注册网络后的此类设备可以直接将查询发送到已配置的DoH服务器，绕过本地解析器或Umbrella。

Umbrella和加密DNS

Umbrella完全支持使用加密DNS和推动使用加密DNS的计划。自2011年以来，Umbrella解析器支持DNSCrypt作为加密DNS流量的方法，所有Umbrella客户端软件都支持使用DNSCrypt并将其用于其默认配置。此外，自2020年2月以来，我们一直支持HTTPS上的DNS(DoH)。

Umbrella还对发送给上游主管机构的查询执行DNSSEC验证，以确保缓存中所有记录的数据完整性。

iOS 14和macOS 11中的详细DNS更改

iOS 14和macOS 11引入了用于选择DNS解析器的新机制。虽然需要特定详细信息的客户可以与Apple确认，但思科对该机制的理解是，可以选择DNS解析器，其优先级如下所述：

1.使用网络提供的DNS解析器解析强制网络门户测试区域

2. VPN或DNS代理配置(如iOS的思科安全连接器)以及企业策略设置的DNS解析器（如MDM或OTA）。（有关设置DNS策略的详细信息，请咨询您的MDM供应商）

3.设备所有者直接配置的系统范围加密解析器

4.域所有者指定的加密解析程序

5.应用指定的加密解析程序

6.未加密解析器（例如通过DHCP或RA指定的解析器）

特别是，我们将数字3、4和5视为对解析程序选择的重大更改，这些更改会对Umbrella管理员在其网络上完全强制使用Umbrella解析程序的能力产生直接影响。

系统范围的加密解析程序

用户可以从DNS提供商安装配置配置文件应用，从而配置系统范围的加密解析程序。无论网络通过DHCP或RA指定的DNS解析器如何，此解析器都可用于所有查询。

目前，防止非受管设备使用这些解析程序的唯一已知方法是在防火墙上阻止已知DoH提供程序的IP。这样做会导致iOS设备的用户发出警告，并且设备无法回退到未加密的DNS，这意味着它无法解析DNS主机名。

由域所有者指定的加密解析程序

DNS区域的所有者可以指定特定解析程序用于解析其区域。在iOS 14和macOS 11中，只能指定DoH解析器。此指定使用专用DNS记录类型（类型65，名为“HTTPS”）进行，并由DNSSEC或已知的URI进行验证。

由于此类指定会导致查询绕过Umbrella，Umbrella解析程序会针对HTTPS DNS记录类型的查询返回REFUSED响应，这意味着不会发现此类指定。

应用指定的加密解析程序

如果在任何较高优先级的机制中找不到其他加密解析程序，应用创建者可以指定回退加密解析程序。仅当备用方案是使用DHCP或RA设置的未加密解析程序时，才能使用此解析程序。

目前，防止非受管设备使用这些解析程序的唯一已知方法是在防火墙上阻止已知DoH提供程序的IP。目前还不知道iOS在这种情况下是否可以回退到未加密的DNS。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。