使用GPO在Firefox和Chrome中维护DoH

目录

简介

本文档介绍如何使用Cisco Umbrella中的组策略对象(GPO)在Firefox和Chrome中维护和禁用通过HTTPS的DNS(DoH)。

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Cisco Umbrella。

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

HTTPS上的DNS(DoH)是添加到多个Web浏览器的功能，允许DNS绕过通过HTTPS的系统DNS堆栈。在许多情况下，您可以禁用此功能以确保Web浏览器不会覆盖任何Umbrella设置。

Firefox和Chrome都提供DoH功能，并且能够阻止在网络或受管计算机上使用DoH。但是，不同浏览器的DoH实施差异很大。

Firefox

Firefox使用默认打开DoH设置运行，其中DNS默认发送到CloudFlare的时间为1.1.1.1。此设置不考虑系统DNS设置。

为了解决此问题，Umbrella默认将覆盖设置为禁用DoH（有关详细信息，请参阅本文的文章）。 但是，仅当没有显式设置DoH设置时，此覆盖才能生效。要确保从未启用DoH以将Firefox DNS从系统设置中转移，需要GPO设置。

要禁用，请将“network.trr.mode”的值设置为0。有关详细信息，请参阅Firefox TRR设置。

有关在Firefox中管理企业策略的详细信息，请参阅Mozilla文档。

铬

Chrome支持包括Umbrella在内的多个提供商的DoH。与Firefox不同，Chrome DoH只能在系统DNS被视为参与的DNS提供商时启用。因此，如果系统DNS是本地DNS服务器或漫游客户端，则它无法启用，但如果本地DNS是208.67.220.220和208.67.222.222，则它可以启用。因此，Chrome不会将您的DNS从系统DNS转发出去，而是通过DoH对其进行增强。

在Chrome DoH实验的初始阶段，如果设备受管、AD加入或应用了企业策略，Chrome可以禁用DoH。

有关详细信息，请参阅Chrome网站。

有关在Chrome中管理企业策略的详细信息，请参阅Chrome文档。

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）。