Maintain DoH in Firefox and Chrome Using GPO

Contents

Introduction

This document describes how to maintain and disable DNS over HTTPS (DoH) in Firefox and Chrome using Group Policy Objects (GPO) in Cisco Umbrella.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

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. If your network is live, ensure that you understand the potential impact of any command.

Overview

DNS over HTTPS (DoH) is a feature added to several web browsers that allows DNS to bypass the system DNS stack over HTTPS. In many cases, you can disable this functionality to ensure that web browsers do not override any Umbrella settings.

Firefox and Chrome both provide DoH functionality and the ability to prevent DoH use on your network and managed computers. However, DoH implementations differ greatly between browsers.

Firefox

Firefox operates with a default-on DoH setting where DNS is sent to CloudFlare by default at 1.1.1.1. This setting does not take the system DNS setting into account.

To combat this, Umbrella by default sets the override to disable DoH (see our article here for more information). However, this override can only take effect if there are no explicitly set DoH settings. To

ensure that DoH is never enabled to divert Firefox DNS away from the system settings, GPO settings are required.

To disable, set the value for "network.trr.mode" to 0. For more information, see the Firefox TRR settings in detail.

For more information on managing enterprise policies in Firefox, see the Mozilla documentation.

Chrome

Chrome has support for DoH for several providers including Umbrella. Unlike Firefox, Chrome DoH can only enable when system DNS is observed to be a participating DNS provider. Therefore, it cannot enable if system DNS is a local DNS server or the roaming client, but can enable if local DNS is 208.67.220.220 and 208.67.222.222. Therefore, Chrome does not direct your DNS away from system DNS, but enhances it with DoH.

During the initial stages of the Chrome DoH experiment, Chrome can disable DoH if the device is managed, AD joined, or has an Enterprise policy applied.

See the Chrome website for more details.

For more information on managing enterprise policies in Chrome, see the Chrome documentation.