Configuración de DNS sobre HTTPS (DoH) con Umbrella

Contenido

Introducción

Este documento describe cómo Umbrella soporta DNS sobre HTTPS (DoH), cifrando las consultas DNS para la privacidad.

Overview

Cisco Umbrella admite DNS a través de HTTPS (DoH), lo que permite cifrar y proteger las consultas DNS frente a interceptaciones o modificaciones. Utilice este punto final de DoH:

Hostname	Descripción
doh.umbrella.com	Frontend para el servicio DNS estándar de Umbrella (208.67.222.222/220.220)

Los pasos para usar DoH con Umbrella dependen de tu navegador y sistema operativo.

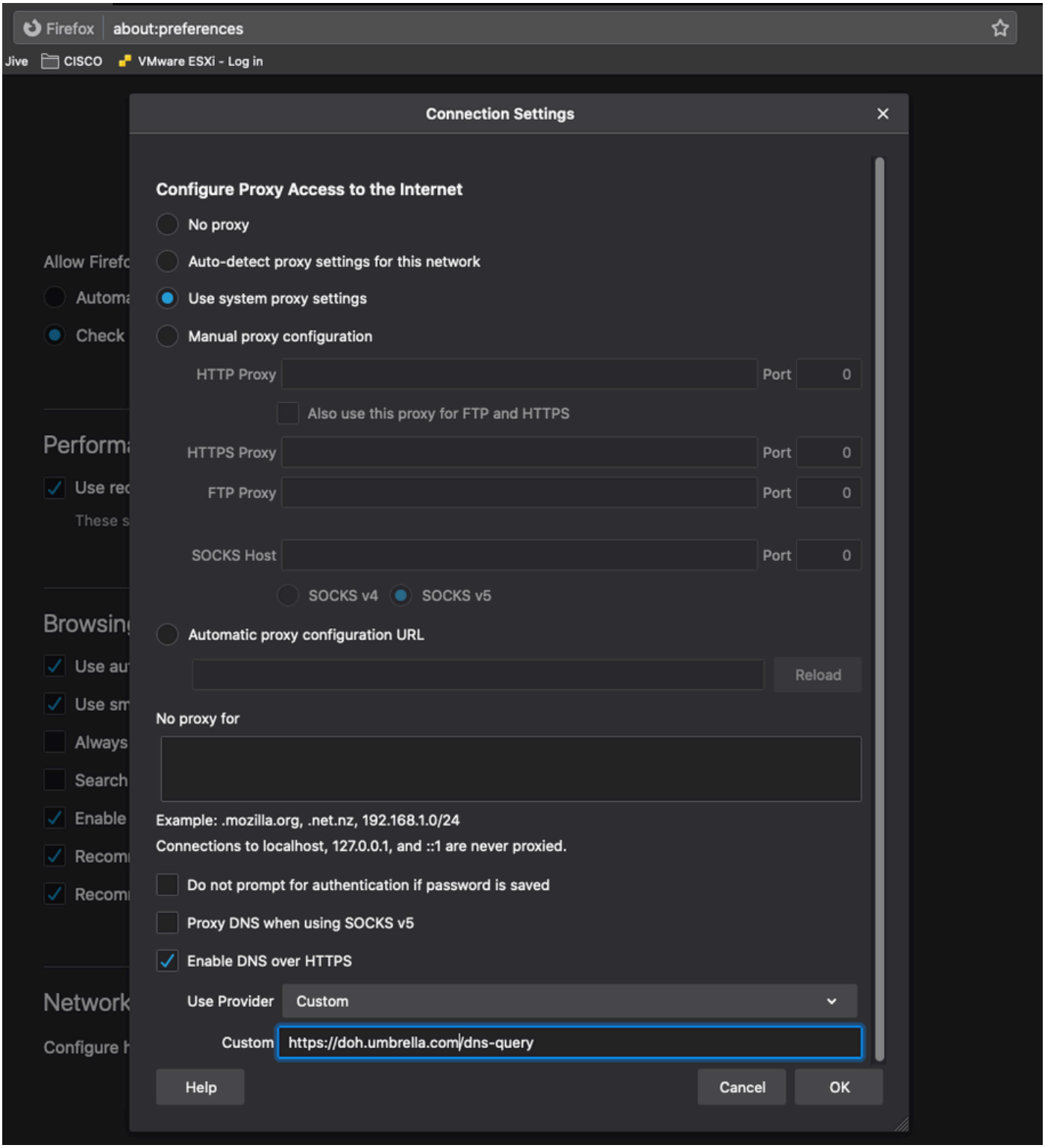
Mozilla Firefox

Los detalles e instrucciones están disponibles en Mozilla. Firefox se puede configurar para usar Umbrella como proveedor personalizado de DNS sobre HTTPS.

1. Navegue hasta Opciones > General > Configuración de red y seleccione Habilitar DNS sobre HTTPS.
2. En Usar proveedor, elija Personalizado e ingrese la plantilla URI:
3.

```
https://umbrella.cisco.com/doh-help
```

4. Seleccione Aceptar y sus consultas se cifrarán.



Preferences.png

Google Chrome

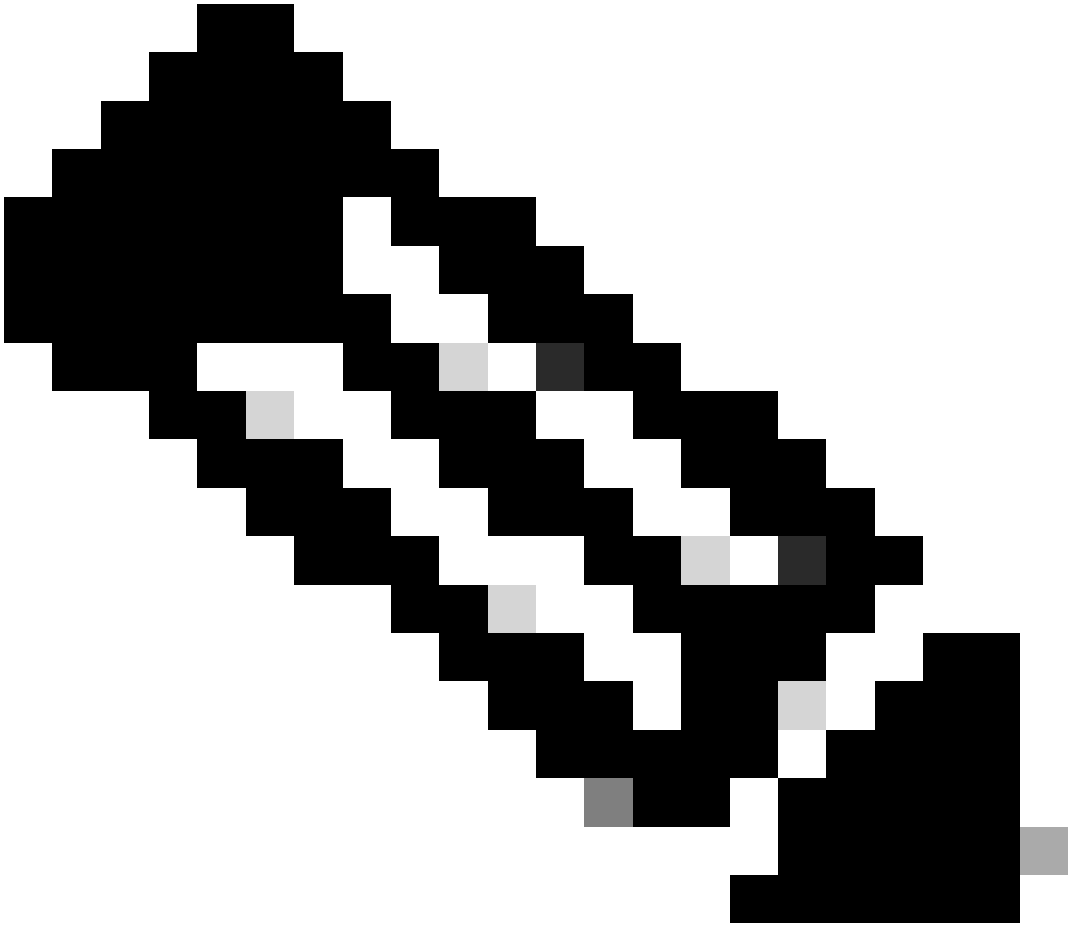
Los detalles y las instrucciones sobre la configuración están disponibles en el [blog Chromium](#).

Chrome habilita automáticamente el uso de DoH si DNS seguro está habilitado y ve las direcciones IP de difusión por proximidad de Umbrella utilizadas por el sistema operativo para DNS.

Configure el sistema operativo para que utilice estas direcciones IP como servidores DNS:

Servicio	Direcciones IPv4	Direcciones IPv6
DNS general	208.67.222.222 208.67.220.220	2620:119:35::35 2620:119:53::53

1. En la configuración de Chrome, navegue hasta Privacidad y seguridad >Seguridad (o ingrese chrome://settings/security en la barra de direcciones).
2. Habilite Usar DNS seguro.
3. Las consultas de DNS ahora están cifradas. Puede visitar la página de prueba de DoH de Umbrella para comprobar su configuración.



> Nota: Chrome busca las direcciones IP de Umbrella específicamente al decidir si actualizar a DoH. Esto significa que si está configurado para utilizar la dirección IP de un servidor DNS local o un reenviador, Chrome no puede actualizar a usar DoH, incluso si ese servidor se reenvía a Umbrella.

Si el equipo se considera administrado por Chrome, lo que es probable si el trabajo o la escuela le proporcionan el equipo, no se puede actualizar automáticamente al uso de DoH, y esta configuración no puede ser visible ni configurable.

En lugar de la actualización automática basada en IP, puede configurar Umbrella directamente estableciendo un proveedor personalizado. En Use secure DNS, seleccione With y elija Custom en el menú desplegable. Cuando solicite introducir un proveedor personalizado, agregue la plantilla URI de Umbrella con este formato:

```
https://doh.umbrella.com/dns-query
```

Advertencias

Hay algunas situaciones que puede encontrar que causan un conflicto entre DoH y Umbrella SWG (especialmente el módulo AnyConnect):

1. La función External Domains (Dominios externos) de AnyConnect permite que los dominios y las direcciones IP omitan Umbrella SWG y, en su lugar, accedan directamente a Internet. No se puede configurar por nombre de dominio o nombre de dominio calificado con frecuencia (FQDN) cuando se usa DoH. Esto se debe a que AnyConnect se basa en la caché DNS del sistema operativo para vincular los nombres de dominio a las direcciones IP al detectar qué solicitudes se dirigen a SWG y cuáles lo omiten. Cuando se utiliza DOH (especialmente en un explorador), se omite la resolución de rutas internas de DNS para el sistema operativo y, por consiguiente, no se crea ninguna entrada de caché de DNS. Esto hace que AnyConnect no pueda correlacionar un nombre de dominio o FQDN para omitir, con el paquete que está viendo.

Soluciones alternativas

Inhabilite DOH en estaciones de trabajo que utilicen AnyConnect para Umbrella SWG y/o configure dominios externos (excepciones SWG) por dirección IP en lugar de dominio o FQDN.

2. Si un servidor DNS interno utiliza DoH para la resolución de recursos internos (como example.local o example.corp), se debe configurar AnyConnect Umbrella SWG para no interceptar esas solicitudes DOH. Esto se debe a que DoH se parece a cualquier otra solicitud HTTPS y el módulo SWG la intercepta y la redirige a Umbrella. Si no se puede acceder al servidor DoH desde la nube de Umbrella, la consulta nunca llega al servidor DNS interno de destino.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).