Configurer DNS sur HTTPS (DoH) avec Umbrella

Table des matières

Introduction

Ce document décrit comment Umbrella prend en charge DNS sur HTTPS (DoH), chiffrant les requêtes DNS pour la confidentialité.

Aperçu

Cisco Umbrella prend en charge le protocole DNS sur HTTPS (DoH), ce qui permet de chiffrer les requêtes DNS et de les protéger contre toute interception ou modification. Utiliser ce point de terminaison DoH :

Nom de l'hôte	Description
doh.umbrella.com	FrontLine pour le service DNS standard d'Umbrella (208.67.222.222/220.220)

Les étapes d'utilisation du DoH avec Umbrella dépendent de votre navigateur et de votre système d'exploitation.

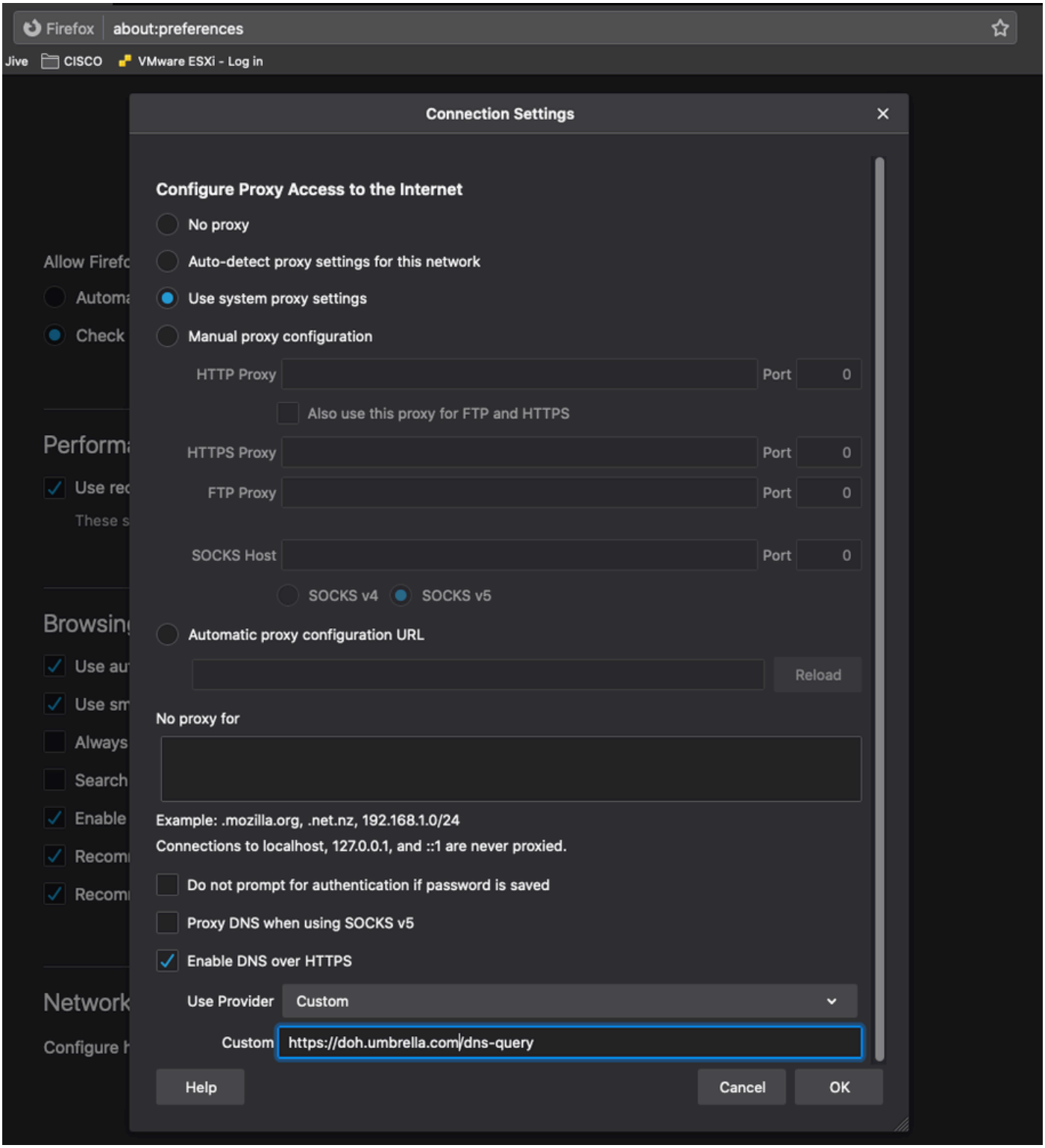
Mozilla Firefox

Les détails et les instructions sont disponibles auprès de Mozilla. Firefox peut être configuré pour utiliser Umbrella comme un DNS personnalisé sur le fournisseur HTTPS.

1. Accédez à Options > General > Network Settings et sélectionnez Enable DNS over HTTPS.
2. Sous Use Provider, choisissez Custom et entrez le modèle URI :
3.

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

4. Sélectionnez OK et vos requêtes sont chiffrées.



Préférences.png

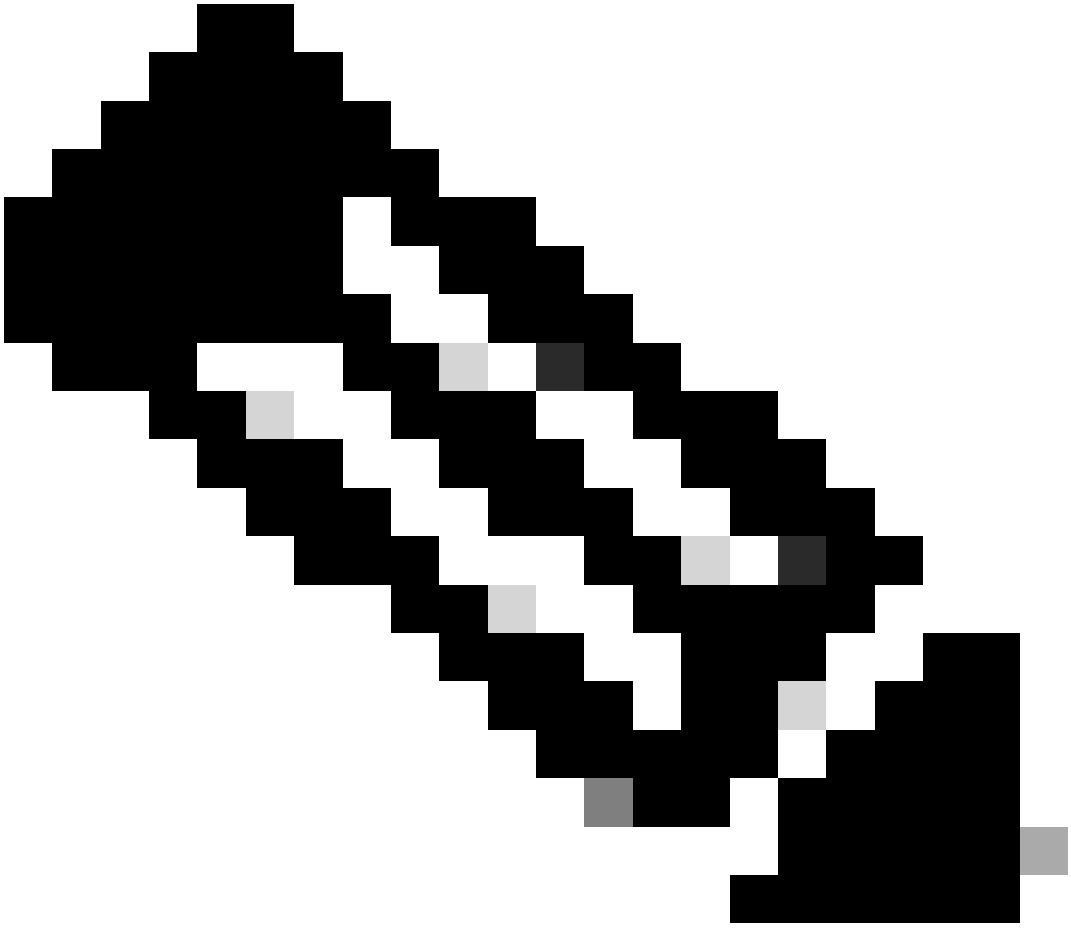
Google Chrome

Des détails et des instructions sur la configuration sont disponibles sur le blog Chromium. Chrome active automatiquement l'utilisation du DoH si le DNS sécurisé est activé et il voit les adresses IP anycast Umbrella utilisées par le système d'exploitation pour DNS.

Configurez votre système d'exploitation pour utiliser ces adresses IP comme serveurs DNS :

Service	Adresses IPv4	Adresses IPv6
DNS parapluie	208.67.222.222 208.67.220.220	2620:119:35::35 2620:119:53::53

1. Dans les paramètres de Chrome, naviguez à Confidentialité et sécurité >Sécurité (Ou entrez chrome://settings/security dans la barre d'adresse).
2. Activez Utiliser DNS sécurisé.
3. Vos requêtes DNS sont maintenant chiffrées. Vous pouvez visiter la page de test Umbrella DoH pour vérifier votre configuration.



> Remarque : Chrome recherche les adresses IP Umbrella spécifiquement lors de la décision de mettre à niveau vers DoH. Cela signifie que si vous êtes configuré pour utiliser l'adresse IP d'un serveur DNS local ou d'un redirecteur, Chrome ne peut pas mettre à niveau à l'aide de DoH, même si ce serveur transmet à Umbrella.

Si votre ordinateur est considéré comme géré par Chrome, ce qui est probable si votre ordinateur vous est fourni par votre travail ou votre école, il ne peut pas mettre à niveau automatiquement à l'aide de DoH, et ce paramètre ne peut pas être visible ou configurable.

Au lieu de procéder à une mise à niveau automatique basée sur IP, vous pouvez configurer directement Umbrella en définissant un fournisseur personnalisé. Sous Use secure DNS, sélectionnez With et choisissez Custom dans la liste déroulante. Lorsqu'il vous demande d'entrer un fournisseur personnalisé, ajoutez le modèle URI Umbrella au format suivant :

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

Mises en garde

Certaines situations peuvent entraîner un conflit entre le DoH et Umbrella SWG (notamment le module AnyConnect) :

1. La fonctionnalité Domaines externes d'AnyConnect permet aux domaines et aux adresses IP de contourner Umbrella SWG en accédant directement à Internet. Il ne peut pas être configuré par nom de domaine ou par nom de domaine fréquemment qualifié (FQDN) lors de l'utilisation du DoH. En effet, AnyConnect s’appuie sur le cache DNS du système d’exploitation pour lier les noms de domaine aux adresses IP lorsqu’il détecte les requêtes qui sont envoyées à SWG et celles qui les contournent. Lorsque DOH est utilisé (en particulier par un navigateur), le résolveur de stub DNS pour le système d'exploitation est contourné et par conséquent aucune entrée de cache DNS n'est créée. AnyConnect ne peut donc pas établir de corrélation entre un nom de domaine ou un nom de domaine complet à contourner et le paquet qu’il voit.

Solution De Contournement

Désactivez DOH sur les stations de travail à l'aide d'AnyConnect pour Umbrella SWG et/ou configurez les domaines externes (exceptions SWG) par adresse IP au lieu du domaine ou du nom de domaine complet.

2. Si le DoH est utilisé pour la résolution de ressources internes (par exemple.local ou exemple.corp) par un serveur DNS interne, AnyConnect Umbrella SWG doit être configuré pour ne pas intercepter ces requêtes DOH. En effet, le DoH ressemble à n'importe quelle autre requête HTTPS, et le module SWG l'intercepte et la redirige vers Umbrella. Si le serveur DoH n'est pas accessible à partir du cloud Umbrella, la requête n'atteint jamais le serveur DNS interne destiné.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.