Comprendre les modifications importantes apportées au pare-feu pour Umbrella Roaming Client

Table des matières

[Introduction](#)

[Informations générales](#)

[Modifications du pare-feu](#)

Introduction

Ce document décrit les modifications importantes du pare-feu qui s'appliquent au client d'itinérance Umbrella.

Informations générales

Mise à jour: Tous les clients d'itinérance Umbrella ont été transférés vers la nouvelle destination de synchronisation `sync.hydra.opendns.com` via une redirection HTTP à partir du point d'extrémité `api.opendns.com`. Au cours de la nouvelle année, les clients passent directement à la synchronisation avec `sync.hydra.opendns.com` ; toutefois, comme tous les clients sont déjà synchronisés avec cet hôte, aucun impact n'est attendu.

Dans le cadre d'une mise à niveau des fonctionnalités de synchronisation sous-jacentes pour les clients en itinérance, un nouveau domaine pour le client en itinérance Umbrella synchronisant avec Umbrella a été créé. Cette modification permet d'accélérer les réponses de synchronisation et d'actualiser les états des clients itinérants dans le tableau de bord. Une action est requise pour garantir que ce domaine est autorisé dans votre pare-feu.

Modifications du pare-feu

Le changement est le suivant : autoriser TCP 443 à `sync.hydra.opendns.com` (bidirectionnellement)

`sync.hydra.opendns.com` peut résoudre plusieurs adresses IP, toutes comprises dans la plage IP `146.112.63.0/24`. Nous vous recommandons d'ajouter cette plage complète car les adresses IP de `sync.hydra.opendns.com` sont Anycast et peuvent être modifiées. Actuellement, les 4 adresses IP auxquelles ce domaine répond sont les suivantes : `146.112.63.3` à `146.112.63.9` et `146.112.63.11` à `146.112.63.13`

Si cette modification n'est pas effectuée, le client itinérant ne peut pas se synchroniser et risque de perdre la liste des domaines internes qu'il obtient du tableau de bord.

Si vous utilisez un proxy HTTP qui est configuré au niveau de l'utilisateur (normalement à l'aide de l'objet de stratégie de groupe), vous devez vous assurer que l'utilisateur « SYSTEM » est également configuré pour utiliser le proxy. Toutes ces règles sont requises dans votre pare-feu pour que le client d'itinérance puisse se synchroniser avec l'API :

Port	Protocol	Destination
80	TCP	ocsp.digicert.com et crl4.digicert.com
443	TCP	67.215.92.201, 67.215.92.210, sync.hydra.opendns.com, ocsp.digicert.com et crl4.digicert.com

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.