Configurer SWG pour éviter les conflits avec le trafic VPN SSL

Table des matières

Introduction

Ce document décrit comment résoudre les problèmes d'incompatibilité entre la passerelle Web sécurisée (SWG) et les VPN SSL à l'aide de ports interceptés.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Umbrella SWG pour AnyConnect peut rencontrer des problèmes d'incompatibilité avec certains VPN SSL qui utilisent des ports interceptés par l'agent SWG, tels que TCP 443. AnyConnect SWG peut échouer à activer et appliquer la couverture de manière fiable. La fiabilité du réseau peut se dégrader ou devenir indisponible lorsque SWG est actif et que le trafic VPN passe par SWG. Le trafic non Web est abandonné dans ce scénario. Ce problème affecte tous les VPN SSL utilisant les ports 80 et 443.

Solution

Pour empêcher SWG d'intercepter le trafic VPN, configurez un contournement pour vos domaines VPN et adresses IP :

1. Dans le tableau de bord Umbrella, accédez à Déploiements > Gestion des domaines > Domaines externes.

2. Ajoutez le domaine et l'adresse IP de vos serveurs de tête de réseau VPN à la liste Domaines externes. L'entrée IP garantit que le trafic VPN n'est jamais intercepté par l'agent SWG en raison du grand nombre de connexions.

3. Attendez une heure pour que le nouveau paramètre se propage.

Pour utiliser le VPN SSL avec SWG :

1. Ajoutez le domaine VPN à la liste Domaines externes.

2. Si le domaine de tête de réseau VPN est un suffixe de recherche DNS, le client ajoute automatiquement ce domaine pendant la durée de la connexion.

3. Ajoutez les adresses IP de tête de réseau VPN ou la plage d'adresses IP à la liste Domaines externes.

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.