Comprendre comment le proxy SWG gère les demandes HTTPS non standard

Table des matières

Introduction

Aperçu

Questions courantes

- Le proxy SWG peut-il traiter des requêtes Web HTTPS non standard ?
- La désactivation de l'inspection HTTPS ou l'ajout du domaine en question à la liste de décodage sélective peuvent-ils vous aider ?

Solution

Introduction

Ce document décrit comment le proxy SWG traite les requêtes HTTPS non standard et souligne la conformité requise du client.

Aperçu

Umbrella s'appuie sur l'extension TLS SNI pour découvrir le domaine de destination et déterminer si une requête HTTPS nécessite un déchiffrement ou un contournement du déchiffrement à l'aide de listes de déchiffrement sélectif. Le client doit se conformer aux normes TLS telles que définies dans les documents RFC pertinents. La plupart des navigateurs bien connus sont conformes à ces normes et Umbrella les prend en charge.

Questions courantes

Le proxy SWG peut-il traiter des requêtes Web HTTPS non standard ?

Non. La requête HTTPS échoue si le client n'effectue pas une connexion TLS de base. Par exemple, si l'échange Client Hello ou Server Hello est manquant, la demande ne peut pas être exécutée.

La désactivation de l'inspection HTTPS ou l'ajout du domaine en question à la liste de décodage sélective peuvent-ils vous aider ?

Non, ces actions ne résolvent pas le problème.

Solution

Vous devez contourner complètement le proxy SWG pour le site HTTPS non standard en

question.

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.