Comprendre le décodage du trafic SWG avec le décodage HTTPS activé

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Problème

Solution

Motif

Introduction

Ce document décrit comment Cisco Secure Web Gateway (SWG) gère le déchiffrement du trafic lorsque le déchiffrement HTTPS est activé.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Secure Web Gateway.

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

Dans un ensemble de règles de stratégie Web avec déchiffrement HTTPS activé, le trafic est déchiffré uniquement si un indicateur de nom de serveur (SNI) est présent dans la connexion TLS.

Solution

Les stratégies de sécurité et d'utilisation acceptable peuvent toujours être appliquées en fonction des serveurs de destination vers lesquels la demande est envoyée. Des listes de destinations peuvent être créées pour ces serveurs de destination et des règles peuvent être appliquées en

conséquence.

Tous les blocs pour les stratégies DNS pour les tunnels et AnyConnect peuvent toujours s'appliquer.

Motif

Ce comportement est intentionnel.

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.