Dépannage de la connexion aux points d'accès via un portail captif avec le module SWG AnyConnect activé

Table des matières

Introduction

Problème

Correctifs et recommandations pour un dépannage plus approfondi

Configuration des applications antivirus pour AnyConnect

Détails

Versions antérieures à 4.10.05095

Introduction

Ce document décrit le dépannage des connexions aux points d'accès via le portail captif avec le module AnyConnect SWG activé.

Problème

Les utilisateurs équipés du module AnyConnect Secure Web Gateway (SWG) peuvent rencontrer des difficultés pour se connecter à certains points d'accès publics.

Correctifs et recommandations pour un dépannage plus approfondi

Vérifiez que vous utilisez AnyConnect version 4.10.05095(4.10MR5). Les questions concernant le portail captif sont abordées dans cette version.

Toutefois, si le problème persiste même après la mise à niveau vers la version 4.10.05095, contactez l'assistance Umbrella.

Afin d'accélérer le processus d'assistance, nous demandons aux clients de suivre ces étapes et de collecter les journaux demandés avant de contacter l'assistance Umbrella.

1. Nous demandons aux clients de configurer tous les agents de sécurité installés sur leurs points d'extrémité pour exclure les binaires et les connexions AnyConnect afin d'éviter les conflits de stratégies. Par conséquent, TrendMicro et/ou tout autre agent de sécurité doivent être configurés en conséquence.
   Reportez-vous à l'extrait de code correspondant des notes de version d'AnyConnect et assurez-vous que les exceptions pour AnyConnect sont effectuées en conséquence.

2. Visitez les URL HTTP (par exemple, http://www.portquiz.net) et HTTPS (https://www.google.com) dans le navigateur et voyez si la redirection vers le portail captif se produit ou non.
3. Si le problème persiste, collectez un bundle DART (débogage max activé), un fichier PCAP (y compris le bouclage) et un enregistrement d'écran (facultatif) pour approfondir l'analyse.

Configuration des applications antivirus pour AnyConnect

Les applications telles que les antivirus, les logiciels anti-programme malveillant et les systèmes de prévention des intrusions (IPS) peuvent interpréter à tort le comportement des applications AnyConnect Secure Mobility Client comme malveillant. Vous pouvez configurer des exceptions pour éviter de telles erreurs d'interprétation. Après avoir installé les modules ou packages AnyConnect, configurez votre logiciel antivirus pour autoriser le dossier Installation d'AnyConnect ou faites des exceptions de sécurité pour les applications AnyConnect. Les répertoires communs à exclure sont répertoriés, bien que la liste puisse ne pas être complète :

- C:\Users<utilisateur>\AppData\Local\Cisco
- C:\ProgramData\Cisco
- C:\Program Fichiers (x86)\Cisco

Détails

Les problèmes de portail captif peuvent être causés par CSCwb39828 "La page du portail captif ne s'est pas ouverte lorsque SWG est activé pour fail open/fail close". Après la mise à niveau vers AnyConnect 4.10.05095 ultérieure, aucune configuration supplémentaire ou interaction utilisateur n'est nécessaire.

Certains hotspots sans fil et autres réseaux invités interrompent l'accès à Internet et redirigent le trafic Web vers un portail captif (parfois appelé jardin clos). Les versions d'AnyConnect SWG antérieures à la version 4.10.05095 peuvent tenter d'envoyer ce trafic Web vers le cloud Umbrella même si l'accès Internet n'est pas disponible, ce qui empêche le système d'interagir localement avec le portail captif. Cette interaction locale peut être nécessaire pour accorder l'accès via l'authentification, le paiement ou une page d'accord « click-through ».

Versions antérieures à 4.10.05095

La prise en charge des portails captifs utilisant des versions antérieures d'AnyConnect est limitée lorsque SWG est utilisé. Ces actions d'un portail captif le rendent probablement inaccessible à un client SWG :

- Redirection vers une destination située en dehors de l'espace d'adressage IP privé RFC-1918 ou chargement d'éléments à partir de cette destination.
- Acceptation d’une connexion TCP pour les serveurs proxy Umbrella sur le port 80 ou 443, puis fermeture de la connexion ou fourniture d’une réponse inattendue.

Pour contourner ce problème, ajoutez des exceptions dans la section Déploiements —> Gestion

du domaine —> Domaines et adresses IP externes du tableau de bord Umbrella, pour toute destination qui ne se charge pas. Le comportement du portail captif est spécifique à l'implémentation, de sorte que le ou les domaines de redirection ou les adresses IP requis varient en fonction de chaque point d'accès.

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.