Dépannage de l'interaction Captive Portal avec Umbrella Roaming Client

Table des matières

Introduction

Ce document décrit les interactions du portail captif avec le client d'itinérance Umbrella.

Aperçu

Les portails captifs sont le nom courant des connexions Internet publiques ou « en tant que service » qui nécessitent un paiement, une authentification ou une acceptation des conditions de service/de la politique d'utilisation acceptable (TOS/AUP) avant d'autoriser la connectivité à un périphérique.

Les portails captifs sont généralement vus dans les aéroports, les hôtels, les cafés ou vraiment n'importe où où le wifi gratuit ou payant est offert. Vous pouvez également les voir dans les réseaux Wi-Fi invités dans les environnements d'entreprise ou d'école.

Un portail captif se présente généralement comme une « porte » ou une fenêtre contextuelle dans le navigateur, dans laquelle l'utilisateur final doit agir pour fournir des informations d'identification, payer ou accepter les conditions de service afin d'accéder à Internet. Tant que le portail captif n'est pas effacé, l'utilisateur ne peut pas parcourir d'autres ressources que celles du sous-réseau dans lequel se trouve le portail.

Comportements et scénarios prévus

La plupart des portails captifs redirigent toutes les requêtes du navigateur (HTTP/HTTPS) vers leur portail Web local. Le portail Web local est généralement basé sur IP et non sur DNS. Cela signifie qu'aucun problème de comportement n'est provoqué lors de l'utilisation du client d'itinérance Umbrella sur un ordinateur qui se connecte à un portail captif.

Dans les rares cas où un portail captif utilise le DNS d'une manière ou d'une autre pour faciliter son service, ce comportement se produit avant de remplir les conditions du portail captif

(paiement, acceptation TOS/AUP, etc.).]

Les portails captifs basés sur DNS peuvent uniquement rediriger des requêtes HTTP sans échec. Les navigateurs modernes gèrent automatiquement les requêtes connues comme google.com pour être https://www.google.com/, ce qui peut casser certains portails captifs. Essayez d'utiliser le site de vérification du portail captif d'Apple pour accéder à la page de connexion du portail captif qui est uniquement http. Pour ce faire, visitez le site http://captive.apple.com.

Connecteur de sécurité Cisco (CSC)

Tout comme le client itinérant, le CSC reste protégé et chiffré si le protocole UDP 443 est autorisé derrière un portail captif. Il en résulte que le DNS local vers le portail captif ne parvient pas à résoudre le résultat local. Par conséquent, pour accéder au portail captif, un domaine de la liste des domaines internes doit être visité pour ces portails semi-captifs.

Pour permettre à la détection automatique du portail captif iOS de fonctionner :

- Ajoutez-les à la liste des domaines internes
  - captive.apple.com
  - www.airport.us
  - www.thinkdifferent.us

DNS tiers bloqué

Si le portail captif bloque les requêtes DNS destinées à Umbrella, la connectivité DNS est bloquée pendant environ six secondes par le client d'itinérance Umbrella. Au bout de six secondes, le client d'itinérance Umbrella passe à l'état Unprotected/Unencryption jusqu'à ce qu'il puisse à nouveau communiquer avec Umbrella.

DNS tiers redirigé

Si le portail captif redirige les requêtes DNS destinées à Umbrella, la connectivité DNS est bloquée pendant environ deux à six secondes par le client d'itinérance Umbrella. Après ce temps, le client d'itinérance Umbrella passe à l'état Unprotected/Unencrypted jusqu'à ce qu'il puisse à nouveau communiquer avec Umbrella.

DNS tiers autorisé

Si le portail captif ne manipule pas ou ne bloque pas les requêtes DNS destinées à Umbrella, le client d'itinérance Umbrella fonctionne comme prévu et peut entraîner le contournement complet de la partie connexion du portail captif.

Solution : Visitez un domaine de votre liste de domaines internes. Cela permet la redirection du portail captif même lorsque le DNS tiers est autorisé. Procédez de la sorte lorsque le client itinérant reste protégé derrière un portail captif.

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.