Utiliser la détection et la correction du portail captif AnyConnect

Table des matières

Introduction

Ce document décrit la fonctionnalité de détection du portail captif du client Cisco AnyConnect Mobility et les conditions requises pour son bon fonctionnement.

Conditions préalables

Exigences

Cisco vous recommande de connaître le client Cisco AnyConnect Secure Mobility.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- AnyConnect version 4.7
- Appareil de sécurité adaptatif Cisco (ASA) version 9.10

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.

Informations générales

De nombreux points d'accès sans fil des hôtels, restaurants, aéroports et autres lieux publics utilisent des portails captifs afin de bloquer l'accès des utilisateurs à Internet. Ils redirigent les requêtes HTTP vers leurs propres sites Web qui exigent que les utilisateurs saisissent leurs informations d'identification ou acceptent les conditions générales de l'hôte du point d'accès.

Aperçu

De nombreuses installations qui offrent un accès Wi-Fi et filaire, telles que les aéroports, les cafés et les hôtels, exigent que les utilisateurs paient avant d'obtenir l'accès, acceptent de se conformer à une politique d'utilisation acceptable, ou les deux. Ces installations utilisent une technique appelée portail captif afin d'empêcher les applications d'accéder jusqu'à ce que les utilisateurs ouvrent un navigateur et acceptent les conditions d'accès.

Besoins de correction du portail captif

La prise en charge de la détection et de la correction du portail captif nécessite l'une des licences suivantes :

- AnyConnect Premium (SSL (Secure Sockets Layer) VPN Edition)
- Cisco AnyConnect Secure Mobility

Vous pouvez utiliser une licence Cisco AnyConnect Secure Mobility afin de prendre en charge la détection et la correction du portail captif en combinaison avec une licence AnyConnect Essentials ou AnyConnect Premium.

Remarque : la détection et la correction du portail captif sont prises en charge sur les systèmes d'exploitation Microsoft Windows et Macintosh OS X pris en charge par la version d'AnyConnect utilisée.

Remarque : le VPN Always-ON ne prend pas en charge la connexion via un proxy

---

Détection des points chauds du portail captif

AnyConnect affiche le message Unable to contact VPN server sur l'interface graphique utilisateur s'il ne peut pas se connecter, quelle qu'en soit la cause. Le serveur VPN spécifie la passerelle sécurisée. Si l'option Always-on est activée et qu'aucun portail captif n'est présent, le client continue à tenter de se connecter au VPN et met à jour le message d'état en conséquence.

Si le VPN Always-on est activé, que la stratégie d'échec de connexion est fermée, que la correction du portail captif est désactivée et qu'AnyConnect détecte la présence d'un portail captif, l'interface utilisateur graphique d'AnyConnect affiche ce message une fois par connexion et une fois par reconnexion :

```
The service provider in your current location is restricting access to the internet.
The AnyConnect protection settings must be lowered for you to log on with the service
provider. Your current enterprise security policy does not allow this.
```

Si AnyConnect détecte la présence d’un portail captif et que la configuration AnyConnect diffère de celle décrite précédemment, l’interface utilisateur graphique d’AnyConnect affiche ce message une fois par connexion et une fois par reconnexion :

```
The service provider in your current location is restricting access to the internet.
You need to log on with the service provider before you can establish a VPN session.
You can try this by visiting any website with your browser.
```

⚠ Attention : la détection du portail captif est activée par défaut et n'est pas configurable. AnyConnect ne modifie aucun paramètre de configuration du navigateur pendant la détection du portail captif.

Correction des hotspots du portail captif

La conversion d'un portail captif est le processus par lequel vous répondez aux exigences d'un point d'accès à un portail captif afin d'obtenir un accès réseau.

AnyConnect ne corrige pas le portail captif ; il s’appuie sur l’utilisateur final pour effectuer la correction.

Afin d'effectuer la correction du portail captif, l'utilisateur final répond aux exigences du fournisseur de hotspots. Ces exigences peuvent inclure le paiement d'une redevance pour accéder au réseau, une signature sur une politique d'utilisation acceptable, les deux, ou toute autre exigence définie par le fournisseur.

La correction du portail captif doit être explicitement autorisée dans un profil client VPN AnyConnect si AnyConnect Always-on est activé et si la stratégie d'échec de connexion est définie sur Fermé. Si l'option Always-on est activée et que la stratégie Échec de la connexion est définie sur Open, vous n'avez pas besoin d'autoriser explicitement la conversion du portail captif dans un profil de client VPN AnyConnect, car l'accès au réseau de l'utilisateur n'est pas restreint.

Détection de faux portail captif

AnyConnect peut supposer à tort qu’il se trouve dans un portail captif dans les situations suivantes :

- Si AnyConnect tente de contacter un ASA avec un certificat qui contient un nom de serveur (CN) incorrect, le client AnyConnect le traite comme un environnement de portail captif.

  Afin d'éviter ce problème, assurez-vous que le certificat ASA est correctement configuré. La

valeur CN dans le certificat doit correspondre au nom du serveur ASA dans le profil client VPN.

- S'il existe un autre périphérique sur le réseau avant l'ASA qui répond lorsque l'utilisateur tente de contacter un ASA en bloquant l'accès HTTPS à l'ASA, alors le client AnyConnect le traite comme un environnement de portail captif. Cette situation peut se produire lorsqu'un utilisateur se trouve sur un réseau interne et se connecte via un pare-feu afin de se connecter à l'ASA.

  Si vous devez restreindre l'accès à l'ASA depuis l'intérieur de l'entreprise, configurez votre pare-feu de sorte que le trafic HTTP et HTTPS vers l'adresse ASA ne retourne pas un état HTTP. L'accès HTTP/HTTPS à l'ASA est autorisé ou complètement bloqué (également appelé trou noir) afin de s'assurer que les requêtes HTTP/HTTPS envoyées à l'ASA ne renvoient pas de réponse inattendue.

Comportement AnyConnect

Cette section décrit le comportement d’AnyConnect.

1. AnyConnect tente une sonde HTTPS vers le nom de domaine complet (FQDN) défini dans le profil XML.

2. En cas d’erreur de certificat (FQDN non approuvé/incorrect), AnyConnect tente une sonde HTTP vers le FQDN défini dans le profil XML. S'il y a une réponse autre qu'un HTTP 302, alors il fonctionne comme s'il était derrière un portail captif.

Portail captif mal détecté avec IKEv2

Lorsque vous tentez une connexion IKEv2 (Internet Key Exchange Version 2) à un ASA avec authentification SSL désactivée, qui exécute le portail ASDM (Adaptive Security Device Manager) sur le port 443, la sonde HTTPS effectuée pour la détection du portail captif entraîne une redirection vers le portail ASDM (/admin/public/index.html). Comme ce n'est pas attendu par le client, il apparaît comme une redirection de portail captif et la tentative de connexion est empêchée car il semble que la correction du portail captif est requise.

Solution De Contournement

Si vous rencontrez ce problème, voici quelques solutions possibles :

- Supprimez les commandes HTTP sur cette interface afin que l'ASA n'écoute pas les connexions HTTP sur l'interface.

- Supprimez le point de confiance SSL sur l'interface.

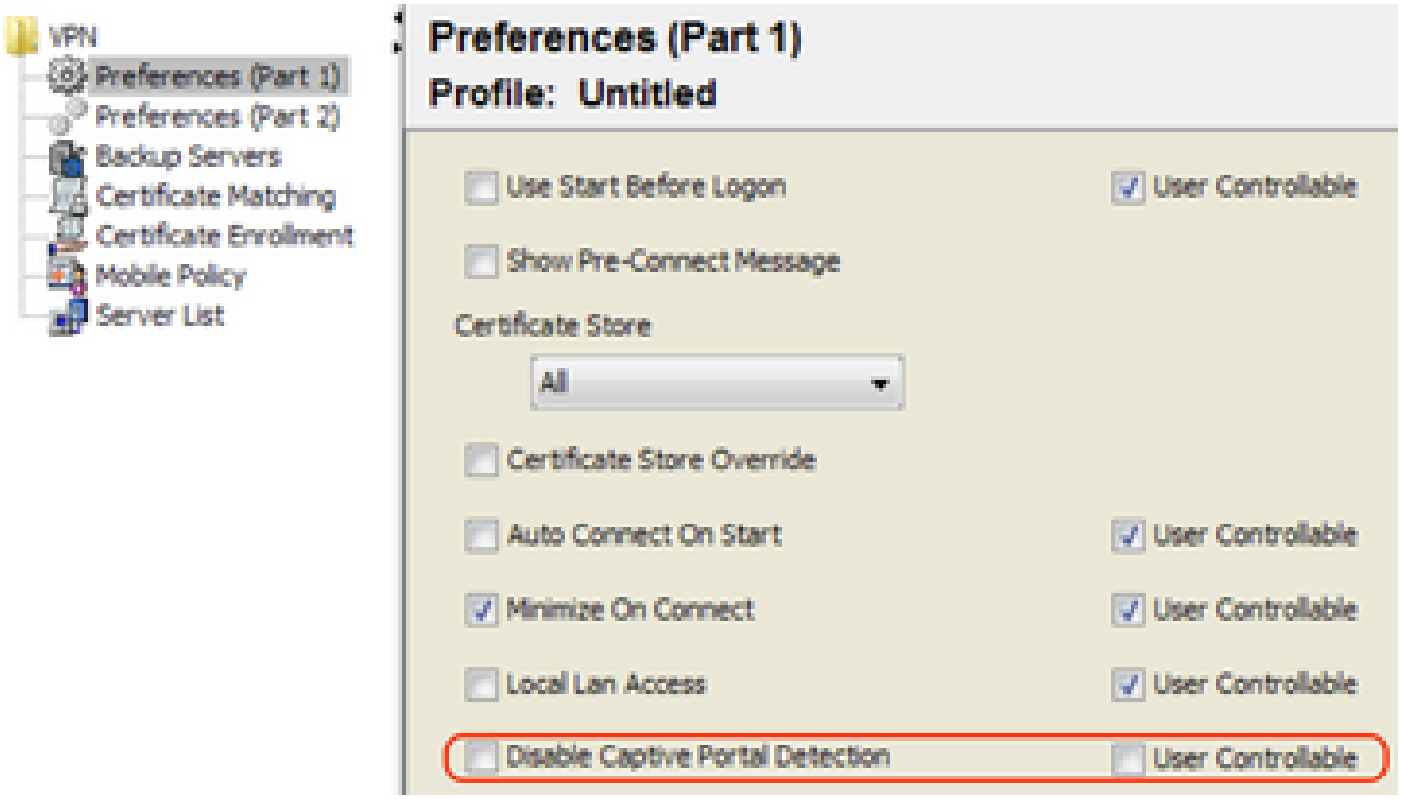
- Activez les services client IKEV2.

- Activez WebVPN sur l'interface.

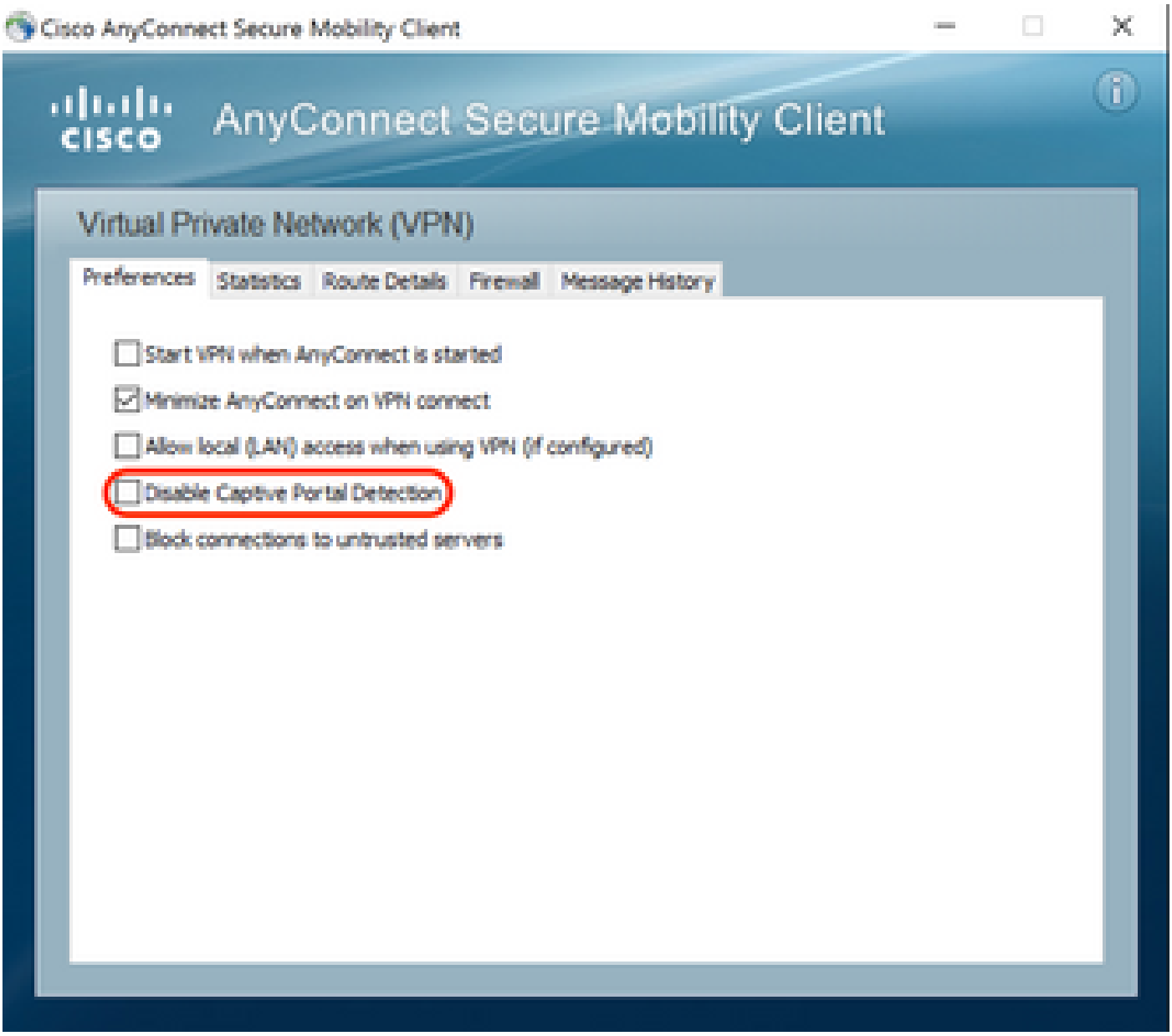
⚠ Attention : le même problème existe pour les routeurs Cisco IOS®. Si ip http server est activé sur Cisco IOS, ce qui est obligatoire si le même boîtier est utilisé comme serveur PKI, AnyConnect détecte faussement le portail captif. La solution de contournement consiste à utiliser ip http access-class afin d'arrêter les réponses aux requêtes HTTP AnyConnect, au lieu d'une demande d'authentification.

Désactiver la fonctionnalité Captive Portal

Il est possible de désactiver la fonctionnalité de portail captif dans le client AnyConnect version 4.2.00096 et ultérieures. L'administrateur peut déterminer si l'option peut être configurée ou désactivée par l'utilisateur. Cette option est disponible dans la section Préférences (Partie 1) de l'éditeur de profil. L'administrateur peut sélectionner Disable Captive Portal Detection ou User Controllable comme indiqué dans cette capture d'écran de l'éditeur de profil :



Si la case Contrôlable par l'utilisateur est cochée, la case apparaît dans l'onglet Préférences de l'interface utilisateur du client AnyConnect Secure Mobility, comme indiqué ci-dessous :


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Preferences
Statistics
Route Details
Firewall
Message History
Start VPN when AnyConnect is started
Minimize AnyConnect on VPN connect
Allow local (LAN) access when using VPN (if configured)
Disable Captive Portal Detection
Block connections to untrusted servers

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.