Détection et correction portailes captives d'AnyConnect

Contenu

Introduction

Ce document décrit la caractéristique portaile captive de détection de client de mobilité de Cisco AnyConnect et les conditions requises pour qu'il fonctionne correctement. Beaucoup de points d'accès sans fil aux hôtels, aux restaurants, aux aéroports, et à d'autres lieux publics emploient les portails captifs afin de bloquer l'accès client à l'Internet. Ils réorientent des demandes de HTTP à leurs propres sites Web qui exigent des utilisateurs d'entrer dans leurs qualifications ou de reconnaître des termes et conditions générales de l'hôte de point névralgique.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du Client à mobilité sécurisé Cisco AnyConnect.

Composants utilisés

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

- Version 3.1.04072 d'AnyConnect
- Version 9.1.2 de l'appliance de sécurité adaptable Cisco (ASA)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Beaucoup d'équipements qui offrent le WiFi et l'accès de câble, tel que des aéroports, des cafés, et des hôtels, exigent des utilisateurs de payer avant qu'ils obtiennent l'accès, acceptent de se conformer à une politique d'utilisation acceptable, ou à chacun des deux. Ces équipements emploient une technique appelée le portail captif afin d'empêcher des applications de se connecter jusqu'à ce que les utilisateurs ouvrent un navigateur et reçoivent les conditions pour l'accès.

Conditions requises portailes captives de correction

Le soutien de la détection portaile captive et de la correction exige un de ces permis :

- AnyConnect de la meilleure qualité VPN Edition (de Secure Sockets Layer (SSL))
- Mobilité sécurisée de Cisco AnyConnect

Vous pouvez employer un permis sécurisé de mobilité de Cisco AnyConnect afin de fournir le support pour la détection et la correction portailes captives en combination avec AnyConnect Essentials ou une licence premium d'AnyConnect.

> **Note**: La détection et la correction portailes captives est prise en charge des systèmes d'exploitation sur de Microsoft Windows et de Macintosh OS X pris en charge par la release d'AnyConnect qui est en service.

Détection portaile captive de point névralgique

AnyConnect affiche l'**incapable d'entrer en contact avec le** message de **serveur VPN** sur le GUI s'il ne peut pas se connecter, indépendamment de la cause. Le serveur VPN spécifie la passerelle sécurisée. Si illimité est activé et un portail captif n'est pas présent, le client continue à tenter de se connecter au VPN et met à jour le message d'état en conséquence.

Si le VPN illimité est activé, la stratégie de panne de connecter est fermée, la correction portaile captive est désactivée, et AnyConnect détecte la présence d'un portail captif, alors le GUI d'AnyConnect affiche ce message une fois par connexion et une fois par rebranchez :

```
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 la configuration d'AnyConnect diffère de cela précédemment décrite, le GUI d'AnyConnect affiche ce message une fois par connexion et une fois par rebranchez :

```
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 portaile captive est activée par défaut et est nonconfigurable. AnyConnect ne modifie aucun paramètre de configuration de navigateur pendant la détection portaile captive.

Correction portaile captive de point névralgique

La correction portaile captive est le processus où vous répondez aux exigences d'un point névralgique portail captif afin d'obtenir l'accès au réseau.

AnyConnect ne fait pas remediate le portail de captif ; il se fonde sur l'utilisateur final pour exécuter la correction.

Afin d'exécuter la correction portaile captive, l'utilisateur final répond aux exigences du fournisseur de point névralgique. Ces conditions requises pourraient inclure le paiement des frais pour accéder au réseau, une signature sur une politique d'utilisation acceptable, ou une autre condition qui soit défini par le fournisseur.

On doit explicitement permettre la correction portaile captive dans un profil d'AnyConnect VPN Client si AnyConnect illimité est activé et la stratégie de panne de connecter est placée à fermé. Si illimité est activé et la stratégie de panne de connecter est placée pour s'ouvrir, vous n'a pas besoin de permettre explicitement la correction portaile captive dans un profil d'AnyConnect VPN Client parce que l'utilisateur n'est pas limité de l'accès au réseau.

Détection portaile captive fausse

AnyConnect peut faussement supposer qu'il est dans un portail de captif dans ces situations.

- Si les tentatives d'AnyConnect d'entrer en contact avec une ASA avec un certificat qui contient un nom du serveur incorrect (NC), alors le client d'AnyConnect penseront qu'il est dans un environnement portail captif.

  Afin d'empêcher cette question, assurez-vous que le certificat ASA est correctement configuré. La valeur NC dans le certificat doit apparier le nom du serveur ASA dans le profil de client vpn.

- S'il y a un autre périphérique sur le réseau avant que l'ASA qui répond à la tentative du client d'entrer en contact avec une ASA en bloquant l'accès HTTPS à l'ASA, alors le client d'AnyConnect pensera qu'elle est dans un environnement portail captif. Cette situation peut se produire quand un utilisateur est sur un réseau interne et se connecte par un Pare-feu afin de se connecter à l'ASA.

  Si vous devez limiter l'accès à l'ASA de l'intérieur de la société, configurez votre Pare-feu tels que le trafic de HTTP et HTTPS à l'adresse de l'ASA ne renvoie pas un état de HTTP. L'accès HTTP/HTTPS à l'ASA devrait être permis ou complètement bloqué (également connu en tant que noir-troué) afin de s'assurer que les demandes HTTP/HTTPS envoyées à l'ASA ne renverront pas une réponse inattendue.

Comportement d'AnyConnect

Cette section décrit comment l'AnyConnect se comporte.

1. AnyConnect essaye une sonde HTTPS au nom de domaine complet (FQDN) défini dans le

profil XML.

2. S'il y a FQDN de confiance/faux d'erreur de certificat (), alors AnyConnect essaye une sonde de HTTP au FQDN défini dans le profil XML. S'il y a n'importe quelle autre réponse qu'un HTTP 302, alors il se considère être derrière un portail de captif.

Portail captif inexactement détecté avec IKEV2

Quand vous tentez une connexion de la version 2 d'échange de clés Internet (IKE) (IKEv2) à une ASA avec l'authentification SSL désactivée qui exécute le portail d'Adaptive Security Device Manager (ASDM) sur le port 443, la sonde HTTPS a exécuté pour les résultats portaiux captifs de détection dans un redirect to le portail ASDM (**/admin/public/index.html**). Puisque ceci n'est pas prévu par le client, il ressemble à un portail captif réorientent, et la tentative de connexion est empêchée puisqu'il semble que la correction portaile captive est exigée.

Contournements

Si vous rencontrez cette question, voici quelques contournements :

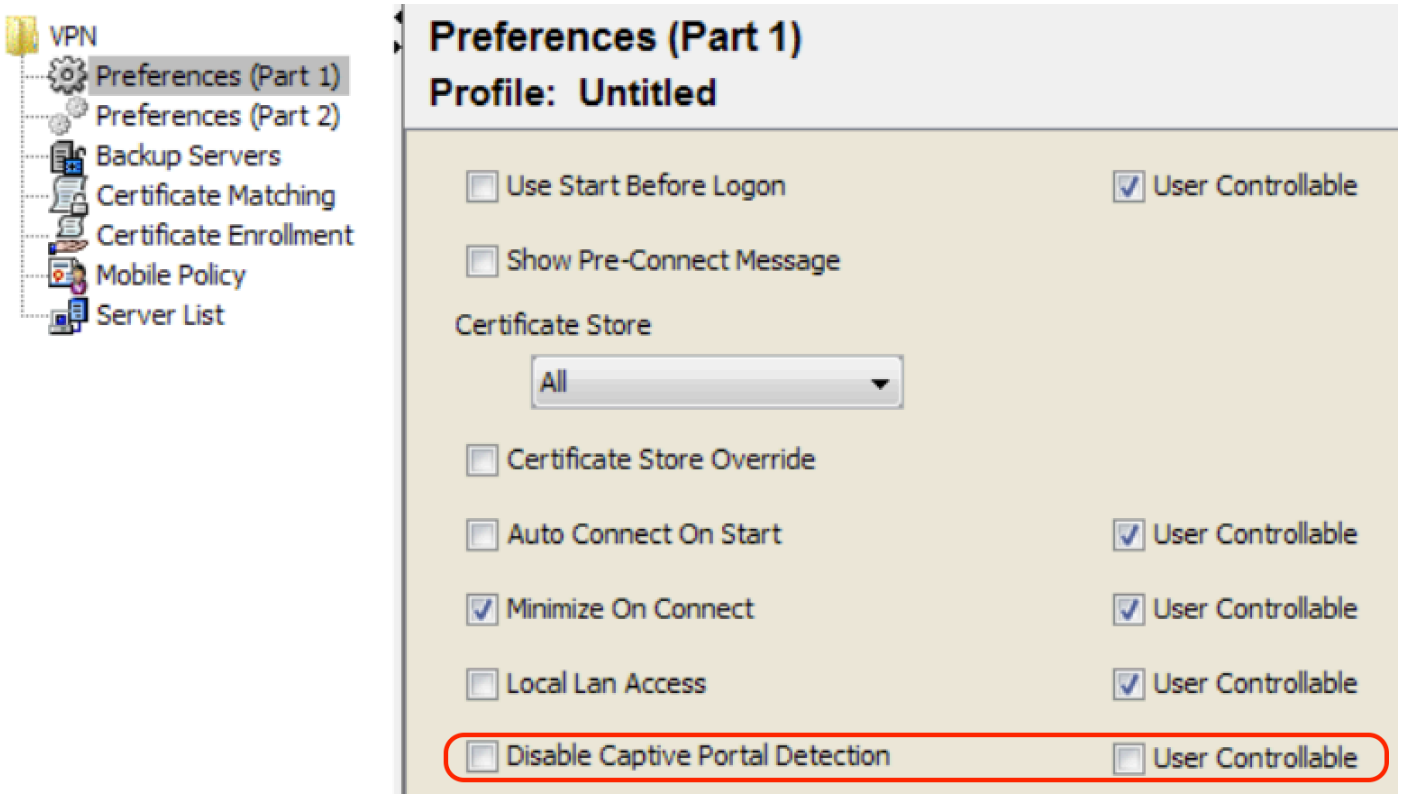
- Retirez les commandes de HTTP sur cette interface de sorte que l'ASA n'écoute pas des connexions HTTP sur l'interface.
- Retirez le point de confiance SSL sur l'interface.
- Services clientèle de l'enable IKEV2.
- Webvpn d'enable sur l'interface.

Cette question est résolue de l'ID de bogue Cisco CSCud17825 dans la version 3.1(3103).

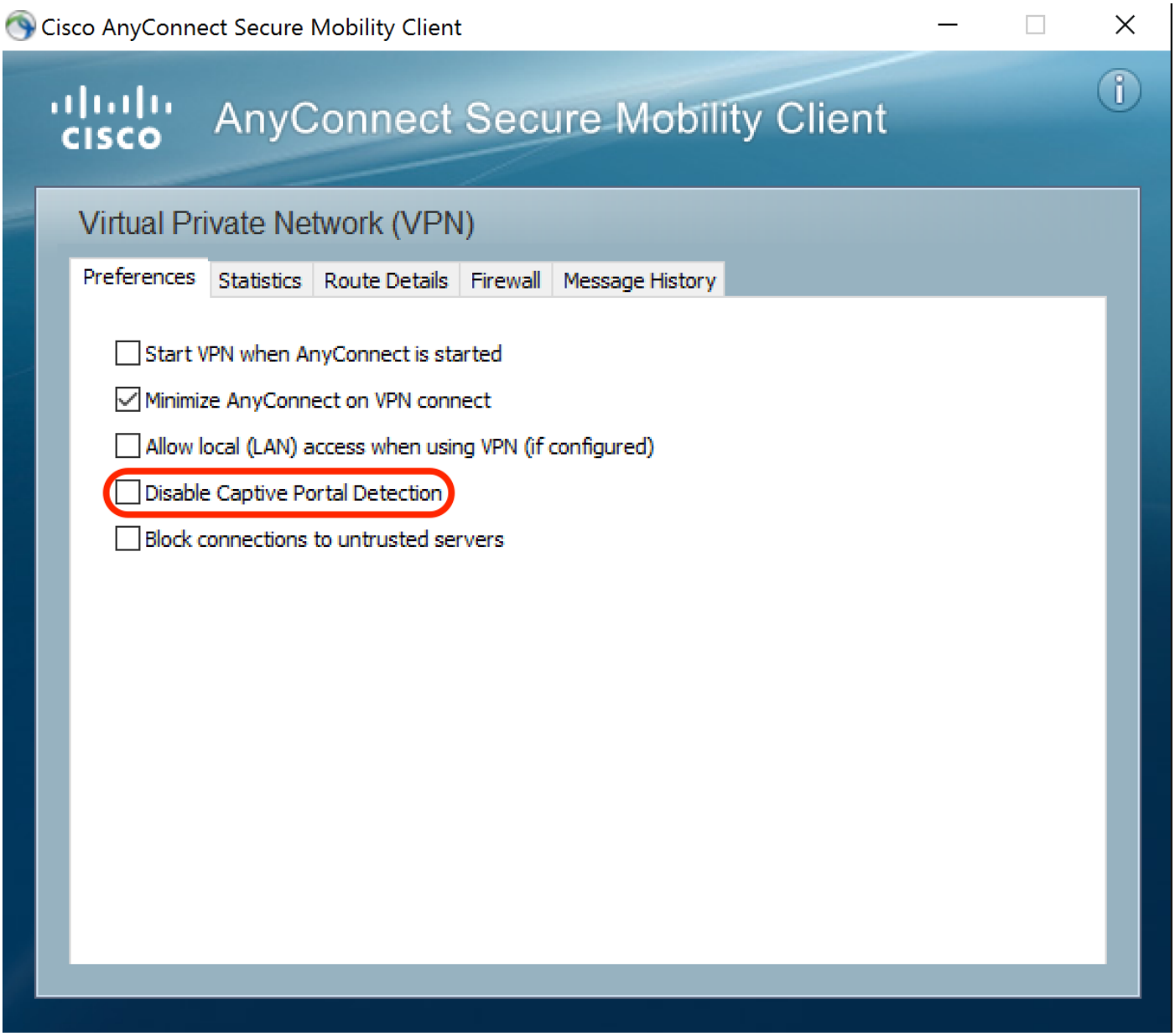
> **Attention** : Le même problème existe pour des Routeurs de Cisco IOS®. Si l'**ip http server** est activé sur le Cisco IOS, qui est exigé si la même case est utilisée en tant que serveur de PKI, AnyConnect détecte faussement le portail captif. Le contournement est d'employer l'**ip http access-class** afin d'arrêter des réponses aux demandes de HTTP d'AnyConnect, au lieu de demander l'authentification.

Désactivez la configuration portaile captive

Il est possible de désactiver la configuration portaile captive dans la version du client 4.2.00096 d'AnyConnect et plus tard (voir l'ID de bogue Cisco CSCud97386). L'administrateur peut déterminer si l'option est utilisateur configurable ou handicapé. Cette option est disponible sous les préférences (section de partie 1) dans l'éditeur de profil. L'administrateur peut choisir la **détection portaile captive** ou l'**utilisateur de débronchement contrôlable** suivant les indications de cet instantané d'éditeur de profil :



Si l'utilisateur contrôlable est vérifié, la case à cocher apparaît sur l'onglet de préférences du client sécurisé UI de mobilité d'AnyConnect comme affiché ici :


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