Erkennung und Beseitigung von Captive Portal mit AnyConnect

Inhalt

Einführung

In diesem Dokument werden die Funktion zur Erkennung von Captive Portals des Cisco AnyConnect Mobility Client und die Voraussetzungen für eine ordnungsgemäße Funktion beschrieben. Viele Wireless-Hotspots in Hotels, Restaurants, Flughäfen und anderen öffentlichen Orten nutzen firmeneigene Portale, um den Benutzerzugriff auf das Internet zu blockieren. HTTP-Anfragen werden an ihre eigenen Websites weitergeleitet, auf denen Benutzer ihre Anmeldeinformationen eingeben oder die Geschäftsbedingungen des Hotspot-Hosts bestätigen müssen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse des Cisco AnyConnect Secure Mobility Client verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- AnyConnect Version 3.1.04072
- Cisco Adaptive Security Appliance (ASA) Version 9.1.2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Viele Einrichtungen wie Flughäfen, Cafés und Hotels, die Wi-Fi-Zugang und kabelgebundenen Zugang bieten, verlangen von den Benutzern, dass sie bezahlen, bevor sie Zugang erhalten, dass sie sich an eine Richtlinie zur akzeptablen Nutzung halten oder beides. Diese Einrichtungen nutzen eine Technik, die als Captive Portal bezeichnet wird, um zu verhindern, dass Anwendungen eine Verbindung herstellen, bis die Benutzer einen Browser öffnen und die Bedingungen für den Zugriff akzeptieren.

Voraussetzungen für die Sanierung des Captive Portals

Für die Erkennung und Beseitigung von Captive Portals ist eine der folgenden Lizenzen erforderlich:

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

Sie können eine Cisco AnyConnect Secure Mobility-Lizenz verwenden, um die Erkennung und Beseitigung von Captive Portals in Kombination mit einer AnyConnect Essentials- oder einer AnyConnect Premium-Lizenz zu unterstützen.

> **Hinweis**: Die Captive Portal-Erkennung und -Problembehebung wird von den verwendeten AnyConnect-Betriebssystemen Microsoft Windows und Macintosh OS X unterstützt.

Erkennung von Captive Portal Hotspots

AnyConnect zeigt die Meldung **VPN-Server kann nicht** über die Benutzeroberfläche **kontaktiert** werden, wenn keine Verbindung hergestellt werden kann, unabhängig von der Ursache. Der VPN-Server legt das sichere Gateway fest. Wenn Always-on aktiviert ist und kein Captive Portal vorhanden ist, versucht der Client weiterhin, eine Verbindung zum VPN herzustellen, und aktualisiert die Statusmeldung entsprechend.

Wenn das Always-On-VPN aktiviert ist, die Verbindungsausfallrichtlinie geschlossen ist, die Korrektur des Captive Portal deaktiviert ist und AnyConnect das Vorhandensein eines Captive-Portals erkennt, zeigt die AnyConnect-GUI diese Nachricht einmal pro Verbindung und einmal pro Verbindung an:

```
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.
```

Wenn AnyConnect ein Captive-Portal erkennt und sich die AnyConnect-Konfiguration von der zuvor beschriebenen unterscheidet, zeigt die AnyConnect-GUI diese Meldung einmal pro Verbindung und einmal pro Verbindung an:

```
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.
```

> **Vorsicht**: Die Captive Portal-Erkennung ist standardmäßig aktiviert und kann nicht konfiguriert werden. AnyConnect ändert während der Erkennung des Captive Portals keine

Browserkonfigurationseinstellungen.

Captive Portal Hotspot-Problembehebung

Die Wiederherstellung des Captive Portals ist ein Prozess, bei dem Sie die Anforderungen eines Captive Portal Hotspots erfüllen, um Zugriff auf das Netzwerk zu erhalten.

AnyConnect behebt das Captive Portal nicht. Die Problembehebung erfolgt durch den Endbenutzer.

Um die Sanierung des Captive Portals durchzuführen, erfüllt der Endbenutzer die Anforderungen des Hotspot-Providers. Diese Anforderungen können die Zahlung einer Gebühr für den Netzwerkzugriff, eine Signatur für eine Richtlinie zur akzeptablen Nutzung (beides) oder eine andere vom Anbieter definierte Anforderung umfassen.

Die Korrektur des Captive Portals muss in einem AnyConnect VPN Client-Profil explizit zugelassen werden, wenn AnyConnect Always-on aktiviert und die Connect-Fehlerrichtlinie auf Closed (geschlossen) festgelegt ist. Wenn Always-on aktiviert ist und die Connect Failure-Richtlinie auf "Open" (Öffnen) gesetzt ist, müssen Sie in einem AnyConnect VPN Client-Profil keine explizite Korrektur des Captive Portals zulassen, da der Benutzer nicht vom Netzwerkzugriff beschränkt ist.

Erkennung von Captive Portal

In diesen Situationen kann AnyConnect fälschlicherweise davon ausgehen, dass es sich in einem Captive Portal befindet.

- Wenn AnyConnect versucht, eine ASA mit einem Zertifikat zu kontaktieren, das einen falschen Servernamen (CN) enthält, wird der AnyConnect-Client annehmen, dass er sich in einer Captive Portal-Umgebung befindet.

  Um dieses Problem zu vermeiden, stellen Sie sicher, dass das ASA-Zertifikat korrekt konfiguriert ist. Der CN-Wert im Zertifikat muss mit dem Namen des ASA-Servers im VPN-Clientprofil übereinstimmen.

- Wenn ein anderes Gerät im Netzwerk vor der ASA vorhanden ist, das auf den Versuch des Clients reagiert, eine ASA zu kontaktieren, indem der HTTPS-Zugriff auf die ASA blockiert wird, wird der AnyConnect-Client annehmen, dass er sich in einer Captive Portal-Umgebung befindet. Diese Situation kann auftreten, wenn sich ein Benutzer in einem internen Netzwerk befindet und eine Verbindung über eine Firewall herstellt, um eine Verbindung mit der ASA herzustellen.

  Wenn Sie den Zugriff auf die ASA innerhalb des Unternehmens beschränken müssen, konfigurieren Sie Ihre Firewall so, dass der HTTP- und HTTPS-Datenverkehr an die ASA-Adresse keinen HTTP-Status zurückgibt. Der HTTP-/HTTPS-Zugriff auf die ASA sollte entweder zugelassen oder vollständig blockiert werden (auch als Blackholed bekannt), um sicherzustellen, dass an die ASA gesendete HTTP-/HTTPS-Anfragen keine unerwartete Antwort zurückgeben.

AnyConnect-Verhalten

In diesem Abschnitt wird das Verhalten von AnyConnect beschrieben.

1. AnyConnect versucht eine HTTPS-Abfrage an den FQDN (Fully Qualified Domain Name) zu senden, der im XML-Profil definiert ist.

2. Wenn ein Zertifikatfehler vorliegt (nicht vertrauenswürdiger/falscher FQDN), versucht AnyConnect eine HTTP-Anfrage an den im XML-Profil definierten FQDN. Wenn eine andere Antwort als ein HTTP 302 vorliegt, gilt dies als hinter einem Captive Portal.

Mit IKEV2 falsch erkanntes Captive Portal

Wenn Sie eine Internet Key Exchange Version 2 (IKEv2)-Verbindung mit einer ASA mit deaktivierter SSL-Authentifizierung versuchen, die das ASDM-Portal (Adaptive Security Device Manager) an Port 443 ausführt, führt die für die Erkennung des Captive Portals durchgeführte HTTPS-Anfrage zu einer Umleitung zum ASDM-Portal (**/admin/public/index.html**). Da dies vom Client nicht erwartet wird, sieht es aus wie eine Captive Portal-Umleitung, und der Verbindungsversuch wird verhindert, da anscheinend eine Sanierung des Captive Portals erforderlich ist.

Workarounds

Wenn dieses Problem auftritt, finden Sie hier einige Problemumgehungen:

- Entfernen Sie HTTP-Befehle auf dieser Schnittstelle, sodass die ASA keine HTTP-Verbindungen auf der Schnittstelle abhört.

- Entfernen Sie den SSL-Vertrauenspunkt auf der Schnittstelle.

- Aktivieren Sie IKEV2-Client-Services.

- Aktivieren Sie WebVPN auf der Schnittstelle.

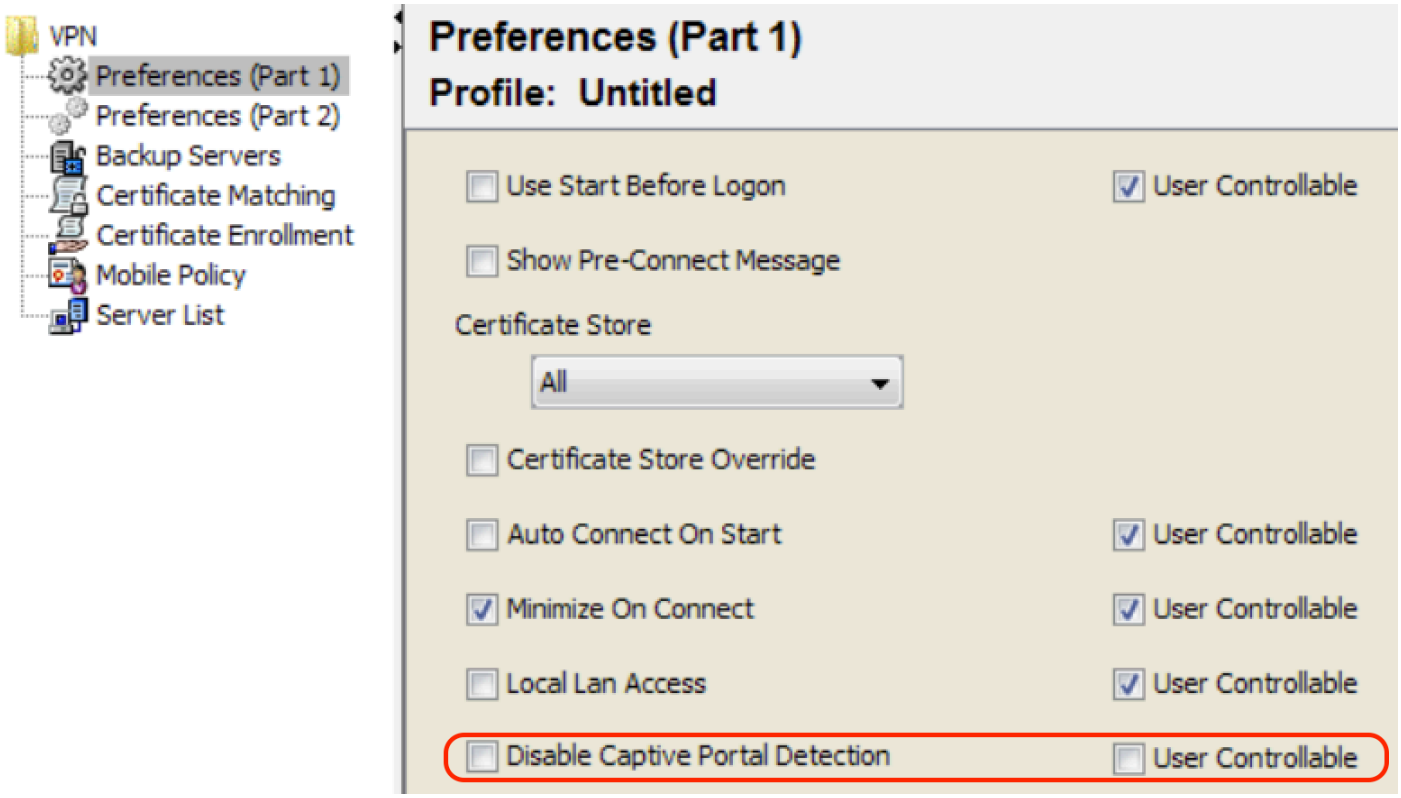
Dieses Problem wird durch die Cisco Bug-ID CSCud17825 in Version 3.1(3103) behoben.

> **Vorsicht**: Das gleiche Problem besteht auch bei Cisco IOS® Routern. Wenn **ip http server** auf Cisco IOS aktiviert ist, was erforderlich ist, wenn dieselbe Box wie der PKI-Server verwendet wird, erkennt AnyConnect das Captive Portal fälschlicherweise. Die Lösung besteht darin, **ip http access-class** zu verwenden, um Antworten auf AnyConnect HTTP-Anforderungen zu stoppen, anstatt eine Authentifizierung anzufordern.

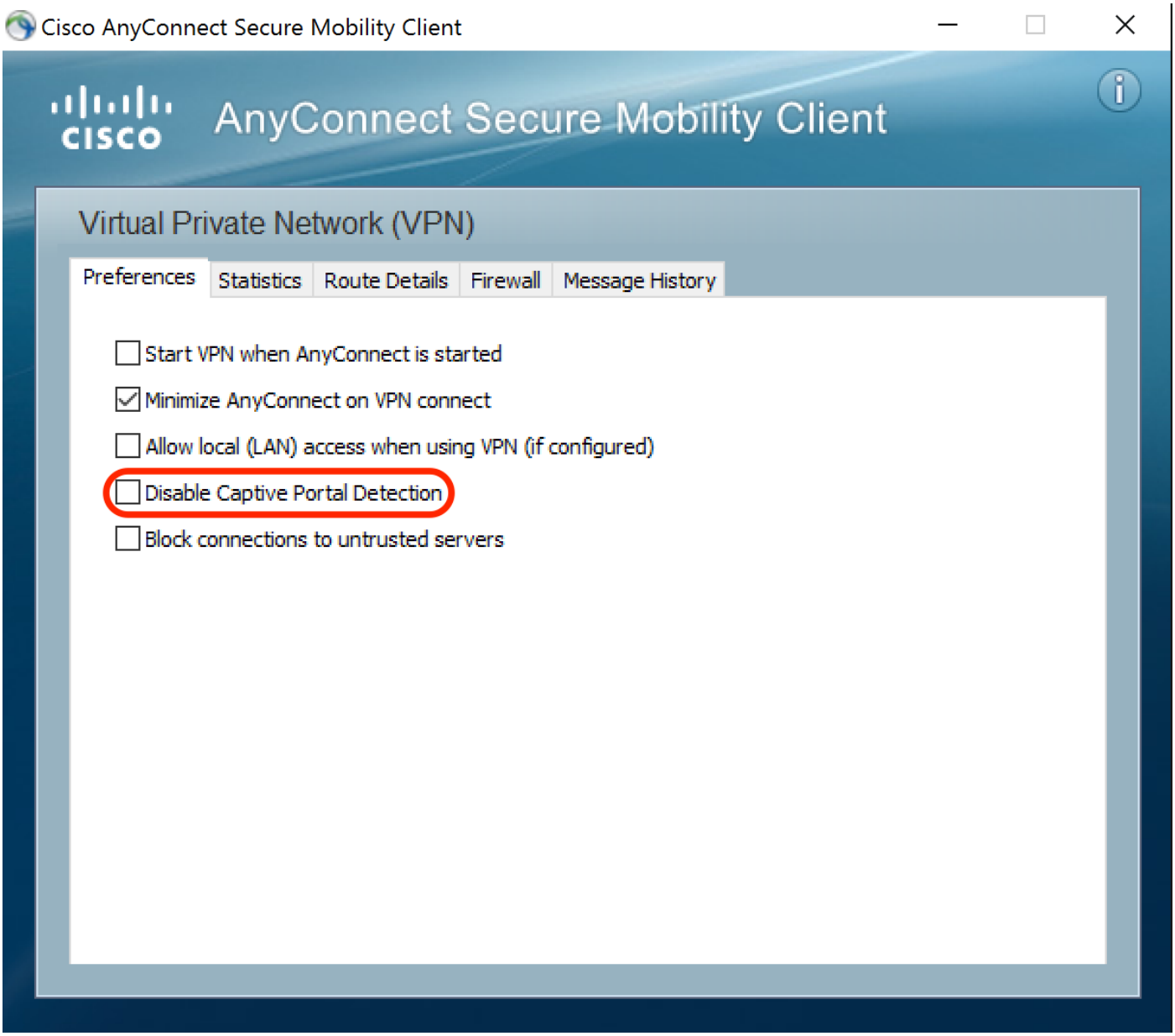
Captive Portal-Funktion deaktivieren

Die Captive Portal-Funktion in AnyConnect Client Version 4.2.0096 und höher kann deaktiviert werden (siehe Cisco Bug ID CSCud97386). Der Administrator kann festlegen, ob die Option vom Benutzer konfigurierbar oder deaktiviert sein soll. Diese Option ist im Profil-Editor im Abschnitt "Voreinstellungen (Teil 1)" verfügbar. Der Administrator kann **Disable Captive Portal Detection**

oder **User Controllable** wählen, wie in diesem Profil-Editor-Snapshot gezeigt:



Wenn die Option Benutzersteuerbarkeit aktiviert ist, wird das Kontrollkästchen auf der Registerkarte Preferences (Voreinstellungen) der AnyConnect Secure Mobility Client-Benutzeroberfläche angezeigt, wie hier gezeigt:


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