AnyConnect のキャプティブ ポータルの検出と修復

目次

概要

このドキュメントでは、Cisco AnyConnect モビリティ クライアントのキャプティブ ポータル検出機能について説明し、この機能が正しく動作するための要件を説明します。 ホテル、レストラン、空港および他の公共の場の多くのワイヤレス ホットスポットはインターネットにユーザアクセスをブロックするために捕虜ポータルを使用します。 ホットスポットは HTTP 要求を各自の Web サイトへリダイレクトします。この Web サイトでは、ユーザが各自のクレデンシャルを入力するか、またはホットスポット ホストの利用規約に同意する必要があります。

前提条件

要件

Cisco AnyConnect セキュア モビリティ クライアントの知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- AnyConnect バージョン 3.1.04072
- Cisco 適応型セキュリティ アプライアンス（ASA）バージョン 9.1.2

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

空港、喫茶店、ホテルなど、Wi-Fi や有線アクセスを提供している施設では、アクセスする前に料金を支払ったり、アクセプタブル ユース ポリシーを順守することに同意したりする必要があります。 こうした施設では、キャプティブ ポータルと呼ばれる技術を使用することにより、ユーザがブラウザを開いてアクセス条件に同意するまではアプリケーションの接続が行えないようにしています。

キャプティブ ポータルの修復に関する要件

キャプティブ ポータルの検出と修復をどちらもサポートするためには、次のライセンスのうちいずれか 1 つが必要です。

- AnyConnect Premium（Secure Sockets Layer (SSL) VPN Edition）
- Cisco AnyConnect セキュア モビリティ

Cisco AnyConnect セキュア モビリティ ライセンスを、AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのどちらかと組み合わせて使用することにより、キャプティブ ポータルの検出および修復をサポートできます。

> **注:** キャプティブ ポータルの検出と修復は、使用されている AnyConnect のリリースでサポートされている Microsoft Windows および Macintosh OS X オペレーティング システムでサポートされています。

キャプティブ ポータル ホットスポットの検出

AnyConnect では、接続できない場合、その原因を問わず GUI に「Unable to contact VPN server」というメッセージが表示されます。 VPN サーバはセキュア ゲートウェイを指定します。 常時接続が有効であり、かつキャプティブ ポータルが存在しない場合、クライアントでは VPN への接続が継続的に試行され、それによってステータス メッセージが更新されます。

常時接続 VPN が有効であり、接続障害ポリシーがクローズしており、かつキャプティブ ポータルの修復が無効の場合に、AnyConnect でキャプティブ ポータルの存在が検出されると、AnyConnect の GUI には接続および再接続のたびに次のようなメッセージが表示されます。

```
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.
```

AnyConnect によりキャプティブ ポータルの存在が検出され、かつ AnyConnect の設定が前述した内容と異なる場合、AnyConnect の GUI には接続および再接続のたびに次のようなメッセージが表示されます。

```
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.
```

> **注意**： キャプティブ ポータルの検出はデフォルトで有効になっており、設定を行うことはできません。 キャプティブ ポータル検出中は、AnyConnect によりブラウザの設定が変更されることはありません。

キャプティブ ポータル ホットスポットの修復

キャプティブ ポータルの修復は、ネットワーク アクセス権を取得できるように、キャプティブ ポータルのホット スポット要件を満たすためのプロセスです。

AnyConnect はキャプティブ ポータルを修復しません。 修復は、エンド ユーザが実行します。

キャプティブ ポータルの修復を実行するには、エンドユーザがホットスポット プロバイダの要件を満たしている必要があります。 これらの要件には、ネットワークにアクセスするための料金の支払い、アクセプタブル ユース ポリシーへの署名、その両方、またはプロバイダーが定義するその他の要件などがあります。

AnyConnect の常時接続が有効になっており、接続障害ポリシーが [Closed] に設定されている場合は、AnyConnect VPN Client プロファイルで、キャプティブ ポータル修復を明示的に許可する必要があります。 常時接続が有効になっており、接続障害ポリシーが [Open] に設定されている場合は、ユーザはネットワークへのアクセスを制限されることはないため、AnyConnect VPN Client プロファイルでキャプティブ ポータル修復を明示的に許可する必要はありません。

キャプティブ ポータルの検出の失敗

次のような状況では、AnyConnect が誤ってキャプティブ ポータルと見なす場合があります。

- AnyConnect が、サーバ名が正しくない証明書（CN）を持った ASA に接続しようとしている場合、AnyConnect クライアントは、その環境を「キャプティブ ポータル」環境と見なします。

  この問題を回避するには、ASA 証明書が正しく設定されていることを確認します。 証明書の CN 値は、VPN クライアント プロファイルの ASA サーバの名前と一致する必要があります。

- ASA の前に別のデバイスがネットワーク上に存在し、そのデバイスが ASA への HTTPS アクセスをブロックして、クライアントによる ASA への接続に応答すると、AnyConnect クライアントは、その環境を「キャプティブ ポータル」環境と見なします。 これは、ユーザが内部ネットワークに存在し、ファイアウォールを介して ASA に接続している場合に発生する可能性があります。

  企業内から ASA へのアクセスを制限する必要がある場合、ASA のアドレスへの HTTP および HTTPS トラフィックが HTTP ステータスを返さないようにファイアウォールを設定します。 ASA への HTTP/HTTPS アクセスは許可するか、完全にブロック（ブラック ホール化とも呼ばれます）し、ASA に送信された HTTP/HTTPS 要求が予期しない応答を返さないようにします。

AnyConnect の動作

ここでは、AnyConnect の動作について説明します。

1. AnyConnect は、XML プロファイルで定義されている完全修飾ドメイン名（FQDN）に対し HTTPS プローブを試行します。

2. 証明書エラー（信頼されていない FQDN/誤った FQDN）が発生すると、AnyConnect は XML プロファイルで定義されている FQDN に対して HTTP プローブを試行します。 HTTP 302 より他の応答がある場合、それ自身が捕虜ポータルの後ろにあると考慮します。

IKEV2 を使用して誤って検出されたキャプティブ ポータル

SSL 認証が無効であり、ポート 443 で Adaptive Security Device Manager（ASDM）ポータルを実行している ASA との間でインターネット キー エクスチェンジ バージョン 2（IKEv2）接続を試行すると、キャプティブ ポータル検出結果に対して HTTPS プローブを実行した結果として、ASDM ポータルへのリダイレクトが発生します（**/admin/public/index.html**）。 クライアントがこの状況を予期していないため、キャプティブ ポータル リダイレクトのように見え、またキャプティブ ポータルの修復が必要であるように見えることから、接続の試行が防止されます。

回避策

この問題が発生した場合には、次に示すいくつかの回避策があります。

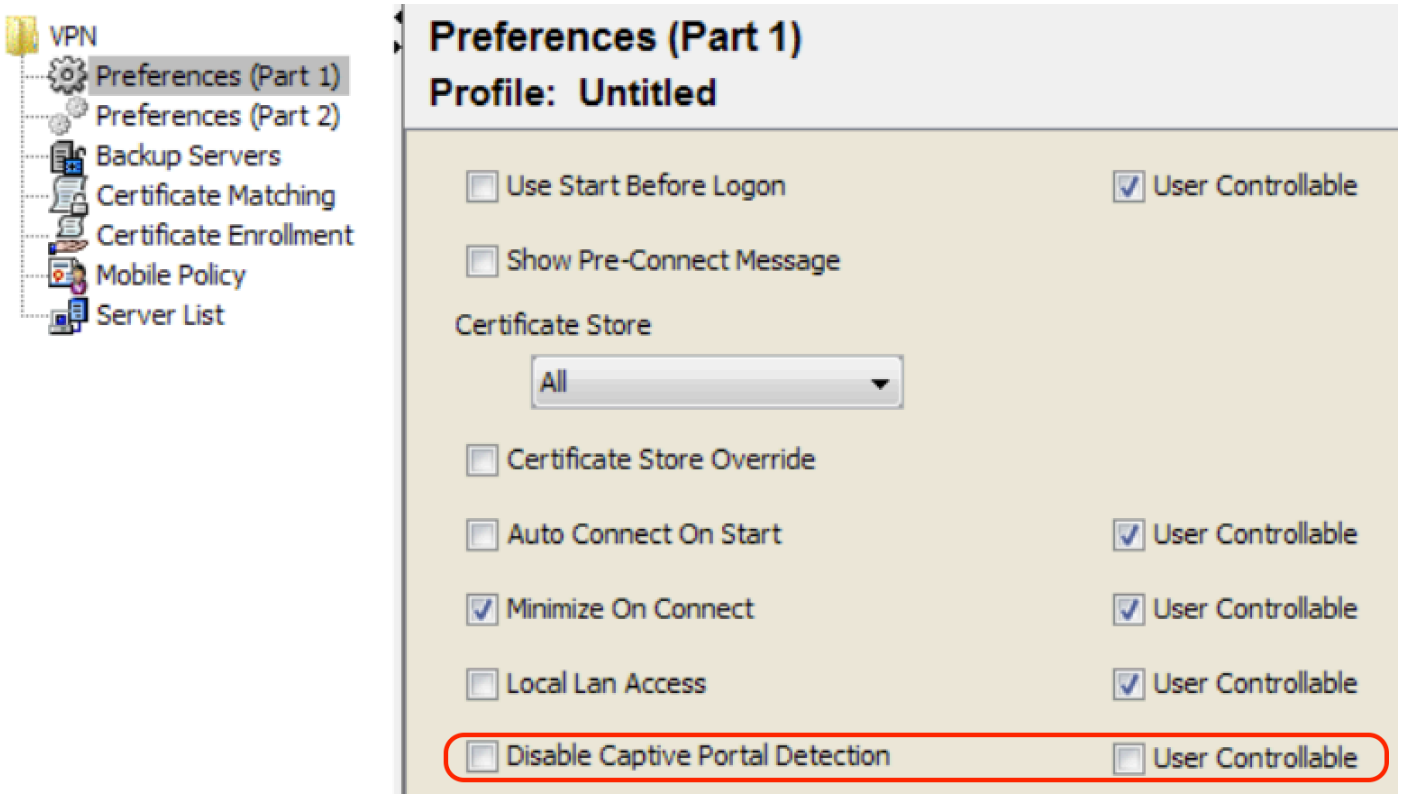
- そのインターフェイスで HTTP コマンドを削除し、ASA がインターフェイスで HTTP 接続をリッスンしないようにする。
- インターフェイスで SSL トラストポイントを削除する。
- IKEV2 クライアント サービスを有効にする。
- インターフェイスで WebVPN を有効にする。

この問題は、バージョン 3.1(3103) で Cisco Bug ID CSCud17825 で解決されました。

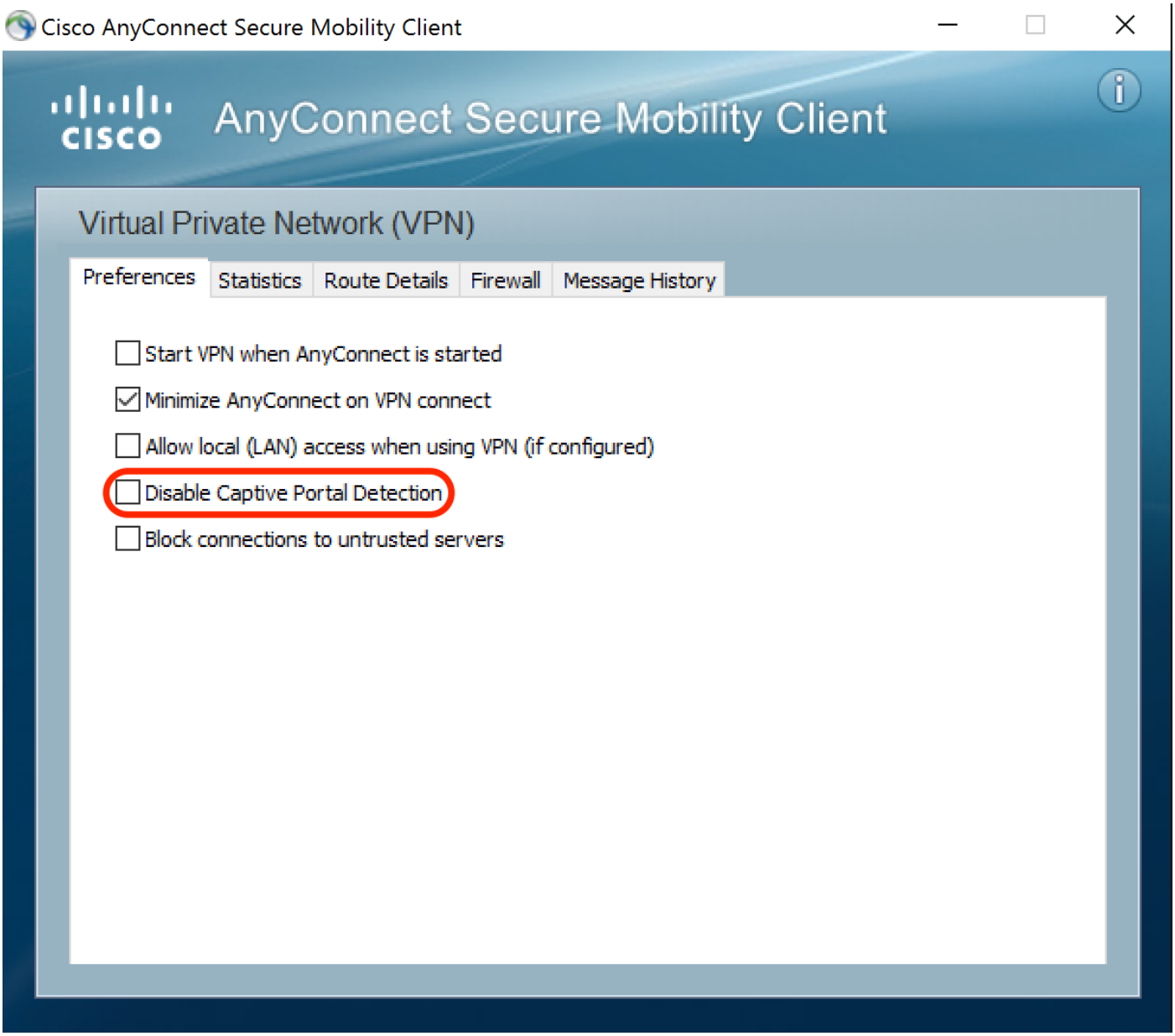
> **注意**： Cisco IOS® ルータでも同じ問題が発生します。 Cisco IOS で **ip http server** が有効な場合（PKI サーバとして同じボックスを使用する場合に必要）、AnyConnect がキャプティブ ポータルを誤検出します。 この回避策は、認証を要求する代わりに、**ip http access-class** を使用して AnyConnect HTTP 要求への応答を停止することです。

キャプティブ ポータル機能を無効にする

AnyConnect クライアントバージョン 4.2.00096 およびそれ以降の捕虜門脈機能をディセーブルにすることは可能性のあるです（Cisco バグ ID CSCud97386 を参照して下さい）。 管理者はオプションがべきである設定可能なか無効ユーザだったかどうか確認できます。 このオプションはユーザー設定（プロファイル エディタの下で利用できますの 1）一部セクション。 管理者はプロファイル エディタ スナップショットこれに示すように**制御可能な捕虜門脈検出**か**ユーザを**『Disable』 を選択 することができます:



制御可能なユーザがチェックされる場合、チェックボックスはここに示されているように AnyConnect セキュア モビリティ クライアント UI の Preferences タブで現われます:


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