

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[捕虜門脈治療必要条件](#)

[捕虜門脈ホットスポット検出](#)

[捕虜門脈ホットスポット治療](#)

[偽捕虜門脈検出](#)

[AnyConnect 動作](#)

[不正確に IKEV2 と検出する捕虜ポータル](#)

[回避策](#)

[捕虜門脈機能の無効化](#)

概要

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。それらはユーザが資格情報を入力するか、またはホットスポット ホストの契約 条件を確認するように要求する自身の Webサイトに HTTP 要求をリダイレクトします。この資料は正しく機能するそのための Cisco AnyConnect モビリティ クライアント捕虜門脈検出 機能および必要条件を記述したものです。

前提条件

要件

Cisco は Cisco AnyConnect セキュア モビリティ クライアントのナレッジがあることを推奨します。

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 適応性があるセキュリティ アプライアンス モデル (ASA) バージョン 9.1.2

このドキュメントの情報は、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、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

Wi-Fi および配線されたアクセスを、空港のような、喫茶店およびホテル提供する多くのファシリティは、アクセスを得る前にユーザが支払うように要求したり、インターネット接続規定、または両方従うことに同意します。これらのファシリティはユーザがブラウザを開き、アクセスのための条件を受け入れるまでアプリケーションが接続することを防ぐために捕虜ポータルと呼ばれる手法を使用します。

捕虜門脈治療必要条件

捕虜門脈検出および治療両方のためのサポートはこれらのライセンスの 1 つを必要とします:

- AnyConnect 事項 (Secure Sockets Layer (SSL) VPN 版)
- Cisco AnyConnect セキュアな機動性

AnyConnect 概要が AnyConnect 優れたライセンスと組み合わせて捕虜門脈検出および治療にサポートを提供するために Cisco AnyConnect セキュアな機動性 ライセンスを使用できます。

注捕虜門脈検出および治療は使用中である AnyConnect のリリースによってサポートされる 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ます。

捕虜門脈ホットスポット検出

AnyConnect は接続できなければ原因に関係なく GUI の VPN サーバ メッセージに連絡することが不可能の表示する。VPN サーバはセキュア ゲートウェイを規定します。常時接続なら有効にされ、捕虜ポータルはありません、クライアントは VPN に接続するように試み続け、ステータスメッセージをそれに応じてアップデートします。

常時接続 VPN が有効になる場合、接続失敗ポリシーは閉じます、捕虜門脈治療は無効であり、AnyConnect は捕虜ポータルの存在を検出する、AnyConnect GUI は接続ごとのこのメッセージを一度表示する、一度毎に再接続して下さい:

AnyConnect が捕虜門脈の存在を検出する、AnyConnect 設定が以前に記述されているそれと異なれば AnyConnect GUI は接続ごとのこのメッセージを一度表示する、一度毎に再接続して下さい:

注意: 捕虜門脈検出はデフォルトで有効になり、設定不可能です。AnyConnect は捕虜門脈検出の間にブラウザ コンフィギュレーションの設定を修正しません。

捕虜門脈ホットスポット治療

捕虜門脈治療はネットワーク アクセスを得るために捕虜門脈ホットスポットの必要条件を満たすプロセスです。

AnyConnect は remediate 捕虜ポータル; それはエンドユーザに治療を行うために頼ります。

捕虜門脈治療を行うために、エンドユーザはホットスポット プロバイダの必要条件を満たします。これらの必要条件は、ネットワークに、プロバイダによって定義される他のある要件またはインターネット接続規定のシグニチャ アクセスするために、料金の支払いを含むかもしれません。

捕虜門脈治療は AnyConnect VPN クライアント プロファイルで常時接続 AnyConnect が有効になり、接続応答失敗ポリシーが閉じるに設定 されれば場合はっきりと認める必要があります。常時接続なら有効にされ、ユーザがネットワーク アクセスから制限 されないので接続応答失敗ポリシーは開くためにはっきりと AnyConnect VPN クライアント プロファイルの捕虜門脈治療を認める必要はありません設定 されます。

偽捕虜門脈検出

AnyConnect は不当に仮定できます捕虜ポータルにこの場合あることを。

- AnyConnect が間違ったサーバ名 (CN) が含まれている認証が付いている ASA に接触するように試みれば、AnyConnect クライアントは考えます捕虜門脈環境にあることを。

ASA 認証が正しく設定されることをこの問題を防ぐために、確かめて下さい。認証の CN 値は VPN クライアント プロファイルの ASA サーバの名前を一致する必要があります。

- ネットワークにもう一つのデバイスが前に ASA に HTTPS アクセスのブロックによって ASA に連絡するクライアントの試みに応答する ASA あれば AnyConnect クライアントは考えます捕虜門脈環境にあることを。この状況はユーザが内部ネットワークにあり、ファイアウォールによって ASA に接続するために接続するとき発生する場合があります。

株式会社の中から ASA に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ことファイアウォールをそのような物設定して下さい。ASA への HTTP/HTTPS アクセスは (別名ブラックホール化されず) ASA に送信された HTTP/HTTPS 要求が予想外応答を返さないことを確認するために許可されるか、または完全にブロックする必要があります。

AnyConnect 動作

このセクションは AnyConnect がどのように動作するか記述します。

1. AnyConnect は XML プロファイルで定義される完全修飾ドメイン名 (FQDN) に HTTPS プローブを試みます。
2. Certificate エラーが (信頼されない/間違っ FQDN) あれば、Anyconnect は XML プロファイルで定義される FQDN に HTTP プローブを試みます。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。

不正確に IKEV2 と検出する捕虜ポータル

ポート 443 の適応性がある Security Device Manager (ASDM) ポータルを実行する SSL 認証がディセーブルの状態 ASA へのインターネット鍵交換 バージョン 2 (IKEv2) 接続を試みると、HTTPS プローブは ASDM ポータル (/admin/public/index.html) にリダイレクトという結果

に捕虜門脈検出のために終わります実行しました。これはクライアントによって期待されないので、捕虜門脈リダイレクトのように見え、捕虜門脈治療が必要となることにそれがようであるので接続の試みは防がれます。

回避策

この問題に出会う場合、いくつかの回避策はここにあります:

- ASA がインターフェイスの HTTP 接続を受信しないようにそのインターフェイスの HTTP コマンドを削除して下さい。
- インターフェイスの SSL トラストポイントを取除いて下さい。
- IKEV2 クライアント サービスを有効に して下さい。
- インターフェイスの WebVPN を有効に して下さい。

この問題はバージョン 3.1(3103)の Cisco バグ ID [CSCud17825](#) によって解決されます。

注意: Cisco IOS[®] ルータのために存在 する同じ問題。 `ip http server` が Cisco IOS で有効になる場合、同じボックスが PKI サーバとして使用される場合必要となる、AnyConnect は不当に捕虜ポータルを検出する。 対応策は認証を要求するかわりに AnyConnect HTTP 要求への応答を、停止するために `ip http access-class` を使用することです。

捕虜門脈機能の無効化

現在捕虜門脈機能をディセーブルにすることはできません。ただし、AnyConnect が不当に多くのカスタマーネットワークの捕虜ポータルを検出するかもしれませんのでこれを達成できる機能拡張 (Cisco バグ ID [CSCud97386](#)) があります。