AnyConnect強制網路門戶檢測和補救

目錄

簡介

本文檔介紹Cisco AnyConnect移動客戶端強制網路門戶檢測功能及其正常運行的要求。酒店、餐館、機場和其他公共場所的許多無線熱點使用強制網路門戶來阻止使用者訪問Internet。它們將HTTP請求重定向到自己的網站，這些網站要求使用者輸入其憑據或確認熱點主機的條款和條件。

必要條件

需求

思科建議您瞭解Cisco AnyConnect安全移動客戶端。

採用元件

本檔案中的資訊是根據以下軟體版本：

- AnyConnect版本3.1.04072
- 思科調適型安全裝置(ASA)版本9.1.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

許多提供Wi-Fi和有線接入的設施（如機場、咖啡廳和酒店）都要求使用者在獲得接入之前先付費，同意遵守可接受的使用策略，或者同時遵守兩者。這些設施使用一種稱為強制網路門戶的技術，在使用者開啟瀏覽器並接受訪問條件之前，阻止應用程式連線。

強制網路門戶補救要求

支援強制網路門戶檢測和補救需要以下許可證之一：

- AnyConnect高級版(安全套接字層(SSL)VPN版)
- Cisco AnyConnect Security Mobility

您可以使用Cisco AnyConnect Security Mobility License結合使用AnyConnect Essentials或AnyConnect Premium許可證，為強制網路門戶檢測和補救提供支援。

> **注意**：使用中的AnyConnect版本支援的Microsoft Windows和Macintosh OS X作業系統支援強制網路門戶檢測和補救。

強制網路門戶熱點檢測

AnyConnect在GUI上顯示**Unable to contact VPN server**消息（如果無法連線，無論原因如何）。VPN伺服器指定安全網關。如果啟用了Always-on且不存在強制網路門戶，則客戶端會繼續嘗試連線到VPN並相應地更新狀態消息。

如果啟用永遠線上VPN，則連線失敗策略關閉，強制網路門戶補救被禁用，並且AnyConnect檢測到強制網路門戶的存在，則AnyConnect GUI會在每次連線時顯示此消息一次，並在每次重新連線時顯示此消息：

```
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.
```

如果AnyConnect檢測到存在強制網路門戶，並且AnyConnect配置與前面描述的不同，則AnyConnect GUI會在每次連線時和每次重新連線時顯示一次此消息：

```
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**：強制網路門戶檢測預設處於啟用狀態，並且不可配置。在強制網路門戶檢測期間，AnyConnect不會修改任何瀏覽器配置設定。

強制網路門戶熱點補救

強制網路門戶補救是滿足強制網路門戶熱點要求以獲取網路訪問許可權的過程。

AnyConnect不會修復強制網路門戶；它依靠終端使用者執行補救。

為了執行強制網路門戶補救，終端使用者滿足熱點提供商的要求。這些要求可能包括支付訪問網路的費用、可接受使用策略的簽名（兩者）或由提供商定義的一些其他要求。

如果已啟用AnyConnect Always-on且連線失敗策略設定為「已關閉」，則必須在AnyConnect VPN客戶端配置檔案中明確允許強制網路門戶補救。如果啟用Always-on且Connect Failure策略設定為Open，則無需在AnyConnect VPN客戶端配置檔案中明確允許強制網路門戶修復，因為使用者不受網路訪問限制。

錯誤強制網路門戶檢測

在這些情況下，AnyConnect可以錯誤地假設它位於強制網路門戶中。

- 如果AnyConnect嘗試使用包含不正確伺服器名稱(CN)的證書聯絡ASA，則AnyConnect客戶端會認為它位於強制網路門戶環境中。

  為了防止此問題，請確保正確配置了ASA證書。證書中的CN值必須與VPN客戶端配置檔案中的ASA伺服器名稱相匹配。

- 如果ASA之前的另一個裝置通過阻止對ASA的HTTPS訪問來響應客戶端聯絡ASA的嘗試，則AnyConnect客戶端會認為它處於強制網路門戶環境中。當使用者位於內部網路並通過防火牆連線至ASA時，可能發生這種情況。

  如果必須限制企業內部對ASA的訪問，請配置防火牆，使指向ASA地址的HTTP和HTTPS流量不會返回HTTP狀態。應允許或完全阻止對ASA的HTTP/HTTPS訪問（也稱為黑洞），以確保傳送到ASA的HTTP/HTTPS請求不會返回意外響應。

AnyConnect行為

本節介紹AnyConnect的行為。

1. AnyConnect嘗試對XML配置檔案中定義的完全限定域名(FQDN)進行HTTPS探測。

2. 如果存在證書錯誤（不受信任/錯誤的FQDN），則AnyConnect會嘗試對XML配置檔案中定義的FQDN執行HTTP探測。如果除了HTTP 302還有任何其他響應，則它認為自己位於強制網路門戶之後。

IKEV2未正確檢測到強制網路門戶

當您嘗試通過Internet金鑰交換版本2(IKEv2)連線到在埠443上運行自適應安全裝置管理器(ASDM)門戶並禁用SSL身份驗證的ASA時，針對強制網路門戶檢測執行的HTTPS探測會導致重定向到ASDM門戶(**/admin/public/index.html**)。 由於客戶端不預期發生這種情況，它看起來像強制網路門戶重定向，並且連線嘗試被阻止，因為強制網路門戶補救似乎是必需的。

因應措施

如果您遇到此問題，以下為一些解決方法：

- 刪除介面上的HTTP命令，以便ASA不會偵聽介面上的HTTP連線。

- 刪除介面上的SSL信任點。

- 啟用IKEV2客戶端服務。

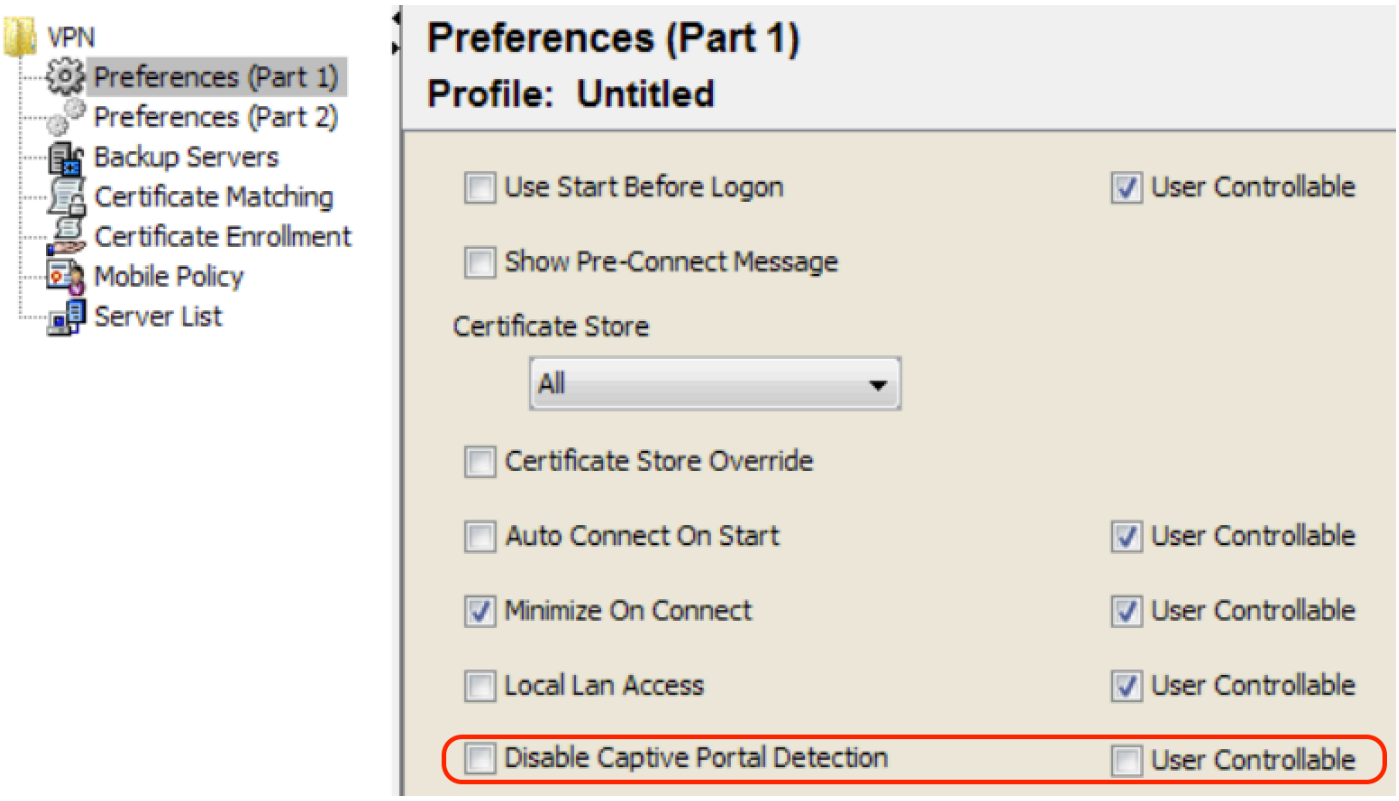
- 在介面上啟用WebVPN。

此問題由3.1(3103)版中的思科錯誤ID CSCud17825解決。

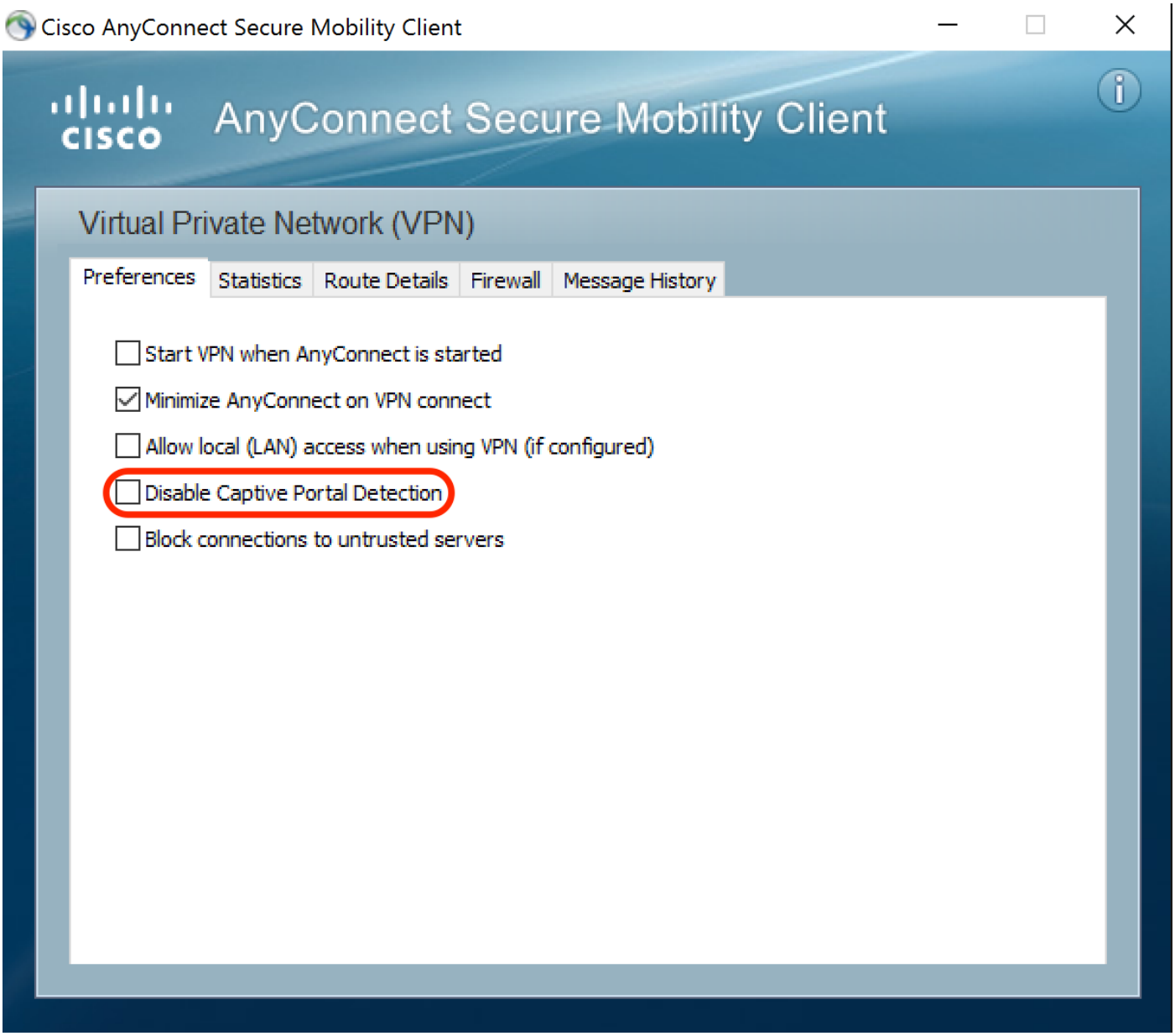
注意：Cisco IOS®路由器也存在同樣的問題。如果在Cisco IOS上啟用了**ip http server**（如果使用與PKI伺服器相同的盒，則此為必需設定），則AnyConnect會錯誤檢測強制網路門戶。因應措施是使用**ip http access-class**停止對AnyConnect HTTP請求的響應，而不是請求身份驗證。

禁用強制網路門戶功能

您可以在AnyConnect客戶端4.2.00096版和更新版本中禁用強制網路門戶功能(請參閱思科錯誤ID CSCud97386)。 管理員可以確定該選項是使用者可配置還是禁用。此選項在配置檔案編輯器的「首選項（第1部分）」(Preferences(Part 1))部分下可用。管理員可以選擇**Disable Captive Portal Detection**或**User Controlled**，如以下配置檔案編輯器快照所示：



如果選中「使用者可控制」，則覈取方塊將顯示在AnyConnect安全移動客戶端UI的「首選項」頁籤上，如下所示：


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