Detección y corrección porta prisioneras de AnyConnect

Contenido

Introducción

Este documento describe la característica porta prisionera de la detección del cliente de la movilidad de Cisco AnyConnect y los requisitos para que funcione correctamente. Muchos hotspots inalámbricos en los hoteles, los restaurantes, los aeropuertos, y otros lugares públicos utilizan los portales prisioneros para bloquear el acceso del usuario a Internet. Reorientan los pedidos de HTTP a sus propios Web site que requieran a los usuarios ingresar sus credenciales o reconocer los términos y condición del host del hotspot.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento del Cliente de movilidad Cisco AnyConnect Secure.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Versión 3.1.04072 de AnyConnect
- Versión 9.1.2 adaptante del dispositivo de seguridad de Cisco (ASA)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Muchos recursos que ofrecen el Wi-Fi y el acceso atado con alambre, tal como aeropuertos, las cafeterías, y los hoteles, requieren a los usuarios pagar antes de que obtengan el acceso, acuerdan seguir un Acceptable Use Policy, o ambos. Estos recursos utilizan una técnica llamada el portal prisionero para evitar que las aplicaciones conecten hasta que los usuarios abran a un navegador y validen las condiciones para el acceso.

Requisitos porta prisioneros de la corrección

El soporte para la detección porta prisionera y la corrección requiere una de estas licencias:

- Premio de AnyConnect (edición de Secure Sockets Layer (SSL) VPN)
- Movilidad segura de Cisco AnyConnect

Usted puede utilizar una licencia segura de la movilidad de Cisco AnyConnect para proporcionar el soporte para la detección y la corrección porta prisioneras conjuntamente con el esencial de un AnyConnect o una licencia del premio de AnyConnect.

> **Note**: La detección y la corrección porta prisioneras se soporta en los sistemas operativos de Microsoft Windows y del Macintosh OS X soportados por la versión de AnyConnect que sea funcionando.

Detección porta prisionera del hotspot

AnyConnect visualiza el **incapaz de entrar en contacto el** mensaje del **servidor VPN** en el GUI si no puede conectar, sin importar la causa. El servidor VPN especifica el gateway seguro. Si Siempre-en se habilita y un portal prisionero no está presente, el cliente continúa intentando conectar con el VPN y pone al día el mensaje de estado por consiguiente.

Si Siempre-en el VPN se habilita, la directiva del error de la conexión es cerrada, se inhabilita la corrección porta prisionera, y AnyConnect detecta la presencia de un portal prisionero, después el AnyConnect GUI visualiza este mensaje una vez por la conexión y una vez por vuelva a conectar:

```
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 detecta la presencia de un porta prisionero y la configuración de AnyConnect diferencia de ésa descrita previamente, el AnyConnect GUI visualiza este mensaje una vez por la conexión y una vez por vuelva a conectar:

```
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.
```

> **Caution**: La detección porta prisionera se habilita por abandono y es nonconfigurable. AnyConnect no modifica ninguna ajustes de la configuración del navegador durante la detección porta prisionera.

Corrección porta prisionera del hotspot

La corrección porta prisionera es el proceso donde usted satisface los requisitos de un hotspot porta prisionero para obtener el acceso a la red.

AnyConnect no hace remediate el portal del cautivo; confía en el usuario final para realizar la corrección.

Para realizar la corrección porta prisionera, el usuario final cumple los requisitos del proveedor del hotspot. Estos requisitos pudieron incluir el pago de una tarifa para acceder la red, una firma en un Acceptable Use Policy, o un cierto otro requisito que es definido por el proveedor.

La corrección porta prisionera se debe permitir explícitamente en un perfil del cliente VPN de AnyConnect si AnyConnect Siempre-en se habilita y la directiva del error de la conexión se fija a cerrado. Si Siempre-en se habilita y la directiva del error de la conexión se fija para abrirse, usted no necesita permitir explícitamente la corrección porta prisionera en un perfil del cliente VPN de AnyConnect porque el usuario no es restricto del acceso a la red.

Detección porta prisionera falsa

AnyConnect puede asumir falso que está en un portal del cautivo en estas situaciones.

- Si AnyConnect intenta entrar en contacto un ASA con un certificado que contenga un incorrecto Nombre del servidor (CN), después el cliente de AnyConnect pensará que está en un entorno porta prisionero.

  Para prevenir este problema, aseegurese que el certificado ASA esté configurado correctamente. El valor CN en el certificado debe hacer juego el nombre del servidor ASA en el perfil del cliente VPN.

- Si hay otro dispositivo en la red antes de que el ASA que responde a la tentativa del cliente de entrar en contacto un ASA bloqueando el acceso HTTPS al ASA, después el cliente de AnyConnect pensará que está en un entorno porta prisionero. Esta situación puede ocurrir cuando un usuario está en una red interna y conecta con un Firewall para conectar con el ASA.

  Si usted debe restringir el acceso al ASA por dentro de la sociedad, configure su Firewall tales que el tráfico HTTP y HTTPS al direccionamiento ASA no vuelve un estatus HTTP. El acceso HTTP/HTTPS al ASA se debe permitir o bloquear totalmente (también conocido como negro-agujereado) para asegurarse de que las peticiones HTTP/HTTPS enviadas al ASA no vuelvan una respuesta inesperada.

Comportamiento de AnyConnect

Esta sección describe cómo el AnyConnect se comporta.

1. AnyConnect intenta una sonda HTTPS al nombre de dominio completo (FQDN) definido en el perfil XML.

2. Si hay un FQDN () no confiado en/incorrecto del error del certificado, después AnyConnect intenta un sondeo HTTP al FQDN definido en el perfil XML. Si hay cualquier otra respuesta que un HTTP 302, después se considera estar detrás de un portal del cautivo.

Portal prisionero detectado incorrectamente con IKEV2

Cuando usted intenta una conexión del intercambio de claves de Internet versión 2 (IKEv2) a un ASA con la autenticación SSL inhabilitada que ejecuta el portal adaptante del Administrador de dispositivos de seguridad (ASDM) en el puerto 443, la sonda HTTPS se realizó para los resultados porta prisioneros de la detección en una reorientación al portal del ASDM (**/admin/public/index.html**). Puesto que esto no es esperada por el cliente, parece un portal prisionero reorienta, y se previene el intento de conexión puesto que parece que la corrección porta prisionera está requerida.

Soluciones alternativas

Si usted encuentra este problema, aquí están algunas soluciones alternativas:

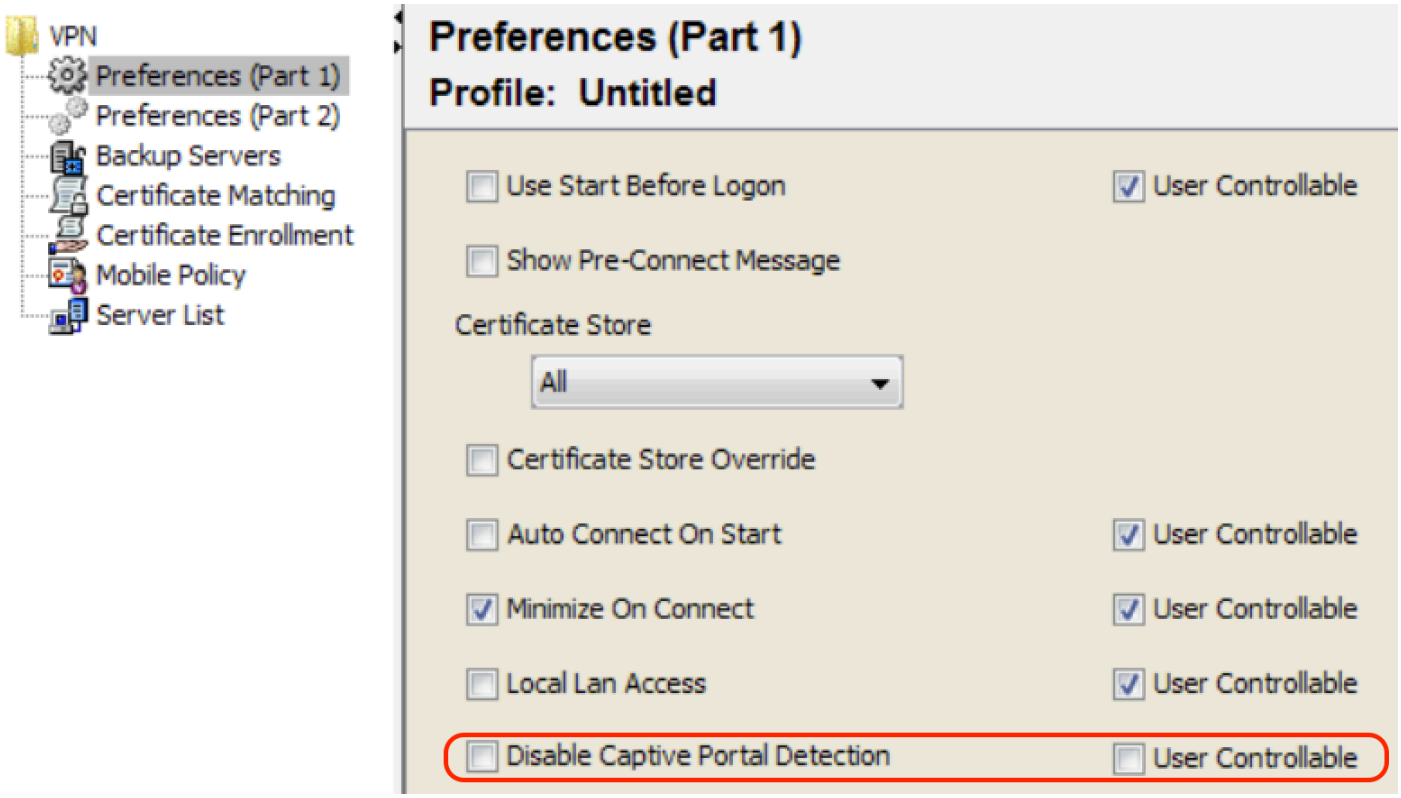
- Quite los comandos HTTP en esa interfaz de modo que el ASA no escuche las conexiones HTTP en la interfaz.
- Quite el trustpoint SSL en la interfaz.
- Habilite los Servicios al cliente IKEV2.
- Habilite el WebVPN en la interfaz.

Este problema es resuelto por el Id. de bug Cisco CSCud17825 en la versión 3.1(3103).

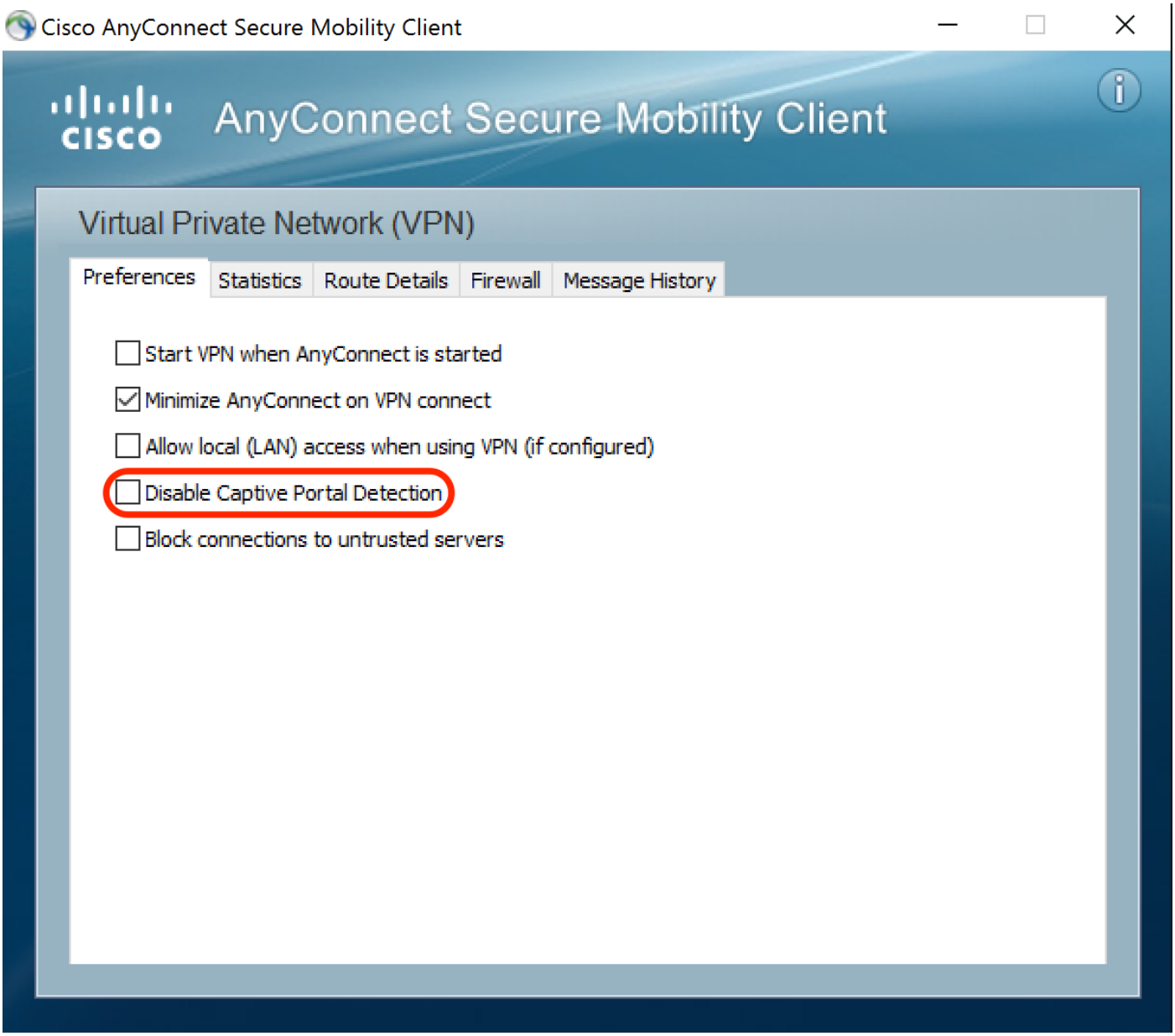
> **Caution**: El mismo problema existe para el Routers del ® del Cisco IOS. Si **ip http el servidor** se habilita en el Cisco IOS, se requiere que si el mismo cuadro se utiliza como el servidor pki, AnyConnect detecta falso el portal prisionero. La solución alternativa es utilizar **ip http la acceso-clase** para parar las respuestas a los pedidos de HTTP de AnyConnect, en vez de pedir la autenticación.

Inhabilite la característica porta prisionera

Es posible inhabilitar la característica porta prisionera en la versión de cliente 4.2.00096 de AnyConnect y posterior (véase el Id. de bug Cisco CSCud97386). El administrador puede determinar si la opción es usuario configurable o discapacitado. Esta opción está disponible bajo preferencias (sección de la parte 1) en el editor del perfil. El administrador puede elegir la **detección porta prisionera** o al **usuario de la neutralización controlable** tal y como se muestra en de esta foto del editor del perfil:



Si marcan al usuario controlable, el checkbox aparece en la lengueta de las preferencias del cliente seguro UI de la movilidad de AnyConnect como se muestra aquí:


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