Detecção e remediação portais prisioneiras de AnyConnect

Índice

Introdução

Este documento descreve a característica portal prisioneira da detecção do cliente da mobilidade de Cisco AnyConnect e as exigências para que funcione corretamente. Muitos pontos quentes wireless em hotéis, em restaurantes, em aeroportos, e em outros lugares públicos usam os portais prisioneiros a fim obstruir o acesso de usuário ao Internet. Reorientam pedidos do HTTP a seus próprios Web site que exigem usuários incorporar suas credenciais ou reconhecer termos e condição do host do ponto quente.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do Cliente de mobilidade Cisco AnyConnect Secure.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Versão 3.1.04072 de AnyConnect
- Versão 9.1.2 adaptável da ferramenta de segurança de Cisco (ASA)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Muitas facilidades que oferecem o Wi-fi e o acesso prendido, tal como aeroportos, cafetarias, e hotéis, exigem usuários pagar antes que obtenham o acesso, concordam habitar por uma política de uso aceitável, ou por ambos. Estas facilidades usam uma técnica chamada o portal prisioneiro a fim impedir que os aplicativos conectem até que os usuários abrirem um navegador e aceitarem as condições para o acesso.

Exigências portais prisioneiras da remediação

O apoio para a detecção portal prisioneira e a remediação exige uma destas licenças:

- AnyConnect superior (edição do secure sockets layer (SSL) VPN)
- Mobilidade segura de Cisco AnyConnect

Você pode usar uma licença segura da mobilidade de Cisco AnyConnect a fim fornecer o apoio para a detecção e a remediação portais prisioneiras em combinação com fundamentos de um AnyConnect ou uma licença do prêmio de AnyConnect.

> **Note**: A detecção e a remediação portais prisioneiras são apoiadas nos sistemas operacionais de Microsoft Windows e do Macintosh OS X apoiados pela liberação de AnyConnect que está no uso.

Detecção portal prisioneira do ponto quente

AnyConnect indica o **incapaz de contactar a** mensagem do **servidor de VPN no** GUI se não pode conectar, apesar da causa. O servidor de VPN especifica o gateway seguro. Se Sempre-em é permitido e um portal prisioneiro não está atual, o cliente continua a tentar conectar ao VPN e atualiza o mensagem de status em conformidade.

Se Sempre-no VPN é permitido, a política da falha da conexão está fechada, a remediação portal prisioneira é desabilitada, e AnyConnect detecta a presença de um portal prisioneiro, a seguir o AnyConnect GUI indica esta mensagem uma vez pela conexão e uma vez por reconecte:

```
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.
```

Se AnyConnect detecta a presença de um portal prisioneiro e a configuração de AnyConnect difere daquela descrita previamente, o AnyConnect GUI indica esta mensagem uma vez pela conexão e uma vez por reconecte:

```
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**: A detecção portal prisioneira é permitida à revelia e é não-configurável. AnyConnect não altera nenhuns ajustes de configuração do navegador durante a detecção portal prisioneira.

Remediação portal prisioneira do ponto quente

A remediação portal prisioneira é o processo onde você satisfaz as exigências de um ponto quente portal prisioneiro a fim obter o acesso de rede.

AnyConnect não faz remediate o portal prisioneiro; confia no utilizador final para executar a remediação.

A fim executar a remediação portal prisioneira, o utilizador final cumpre as exigências do fornecedor do ponto quente. Estas exigências puderam incluir o pagamento de uma taxa para alcançar a rede, uma assinatura em uma política de uso aceitável, ou em alguma outra exigência que é definida pelo fornecedor.

A remediação portal prisioneira deve explicitamente ser permitida em um perfil do cliente VPN de AnyConnect se AnyConnect Sempre-em é permitido e a política da falha da conexão está ajustada a fechado. Se Sempre-em é permitido e a política da falha da conexão está ajustada para abrir, você não precisa de permitir explicitamente a remediação portal prisioneira em um perfil do cliente VPN de AnyConnect porque o usuário não é restrito do acesso de rede.

Detecção portal prisioneira falsa

AnyConnect pode falsamente supor que está em um portal prisioneiro nestas situações.

- Se AnyConnect tenta contactar um ASA com um certificado que contenha um nome do servidor incorreto (CN), a seguir o cliente de AnyConnect pensará que está em um ambiente portal prisioneiro.

  A fim impedir esta edição, certifique-se de que o certificado ASA está configurado corretamente. O valor do CN no certificado deve combinar o nome do server ASA no perfil do cliente VPN.

- Se esteja um outro dispositivo na rede antes que o ASA que responde à tentativa do cliente de contactar um ASA obstruindo o acesso HTTPS ao ASA, a seguir o cliente de AnyConnect pensará que está em um ambiente portal prisioneiro. Esta situação pode ocorrer quando um usuário está em uma rede interna e conecta com um Firewall a fim conectar ao ASA.

  Se você deve restringir o acesso ao ASA do interior do corporaçõ, configurar seu Firewall tais que o tráfego HTTP e HTTPS ao endereço do ASA não retorna um estado HTTP. O acesso HTTP/HTTPS ao ASA deve ser permitido ou completamente obstruído (igualmente sabido como preto-furado) a fim assegurar-se de que os pedidos HTTP/HTTPS enviados ao ASA não retornem uma resposta inesperada.

Comportamento de AnyConnect

Esta seção descreve como o AnyConnect se comporta.

1. AnyConnect tenta uma ponta de prova HTTPS ao nome de domínio totalmente qualificado (FQDN) definido no perfil XML.

2. Se há FQDN não confiado/errado do erro do certificado (), a seguir AnyConnect tenta uma prova HTTP ao FQDN definida no perfil XML. Se há qualquer outra resposta do que um HTTP 302, a seguir considera-se ser atrás de um portal prisioneiro.

Portal prisioneiro detectado incorretamente com IKEV2

Quando você tenta uma conexão da versão 2 do intercâmbio de chave de Internet (IKEv2) a um ASA com a autenticação SSL desabilitada que executa o portal adaptável do Security Device Manager (ASDM) na porta 443, a ponta de prova HTTPS executou para os resultados portais prisioneiros da detecção em uma reorientação ao portal ASDM (**/admin/public/index.html**). Desde que isto não é esperado pelo cliente, olha como um portal prisioneiro reorienta, e a tentativa de conexão é impedida desde que parece que a remediação portal prisioneira está exigida.

Soluções

Se você encontra esta edição, estão aqui algumas ações alternativas:

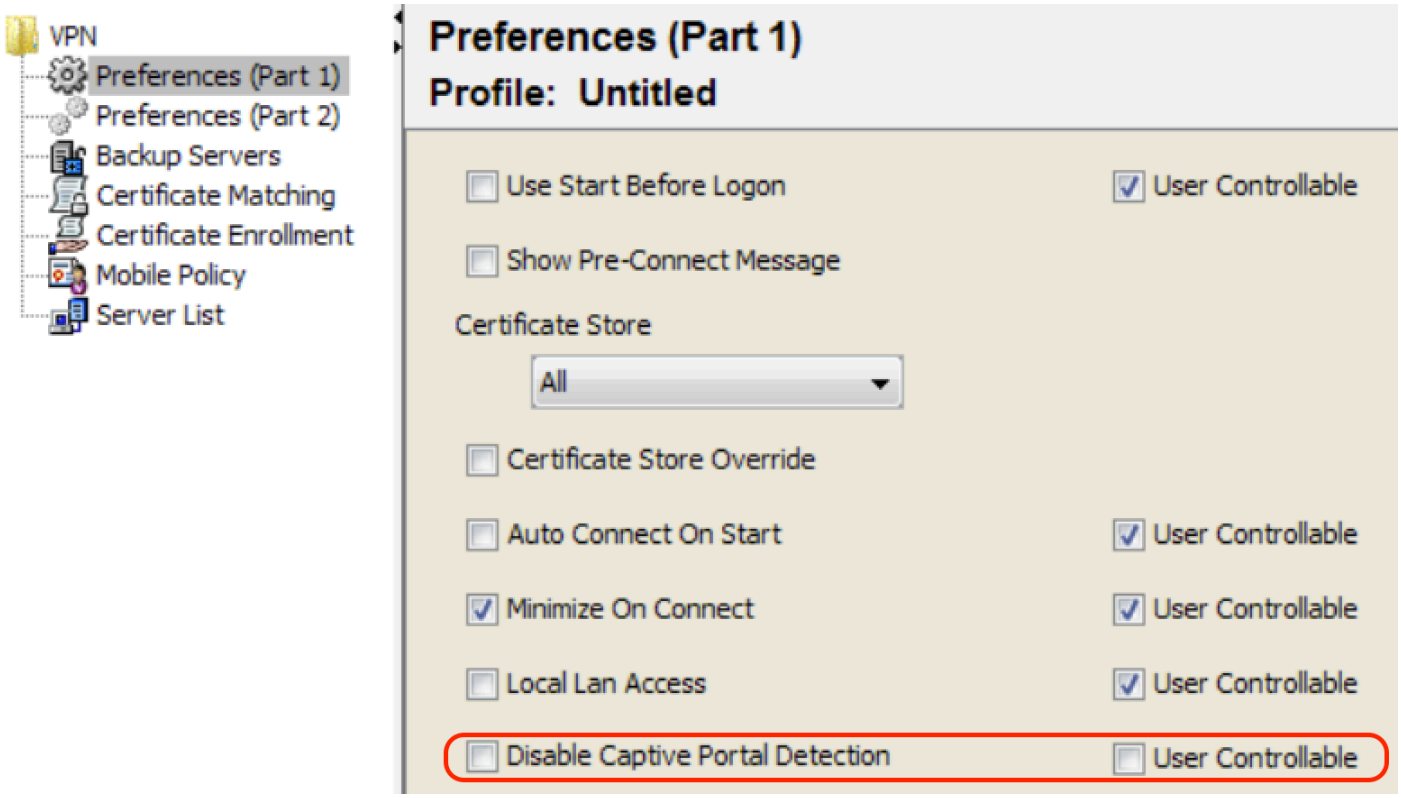
- Remova os comandos HTTP nessa relação de modo que o ASA não escute conexões de HTTP na relação.
- Remova o ponto confiável SSL na relação.
- Permita os serviços de cliente IKEV2.
- Permita o WebVPN na relação.

Esta edição é resolvida pela identificação de bug Cisco CSCud17825 na versão 3.1(3103).

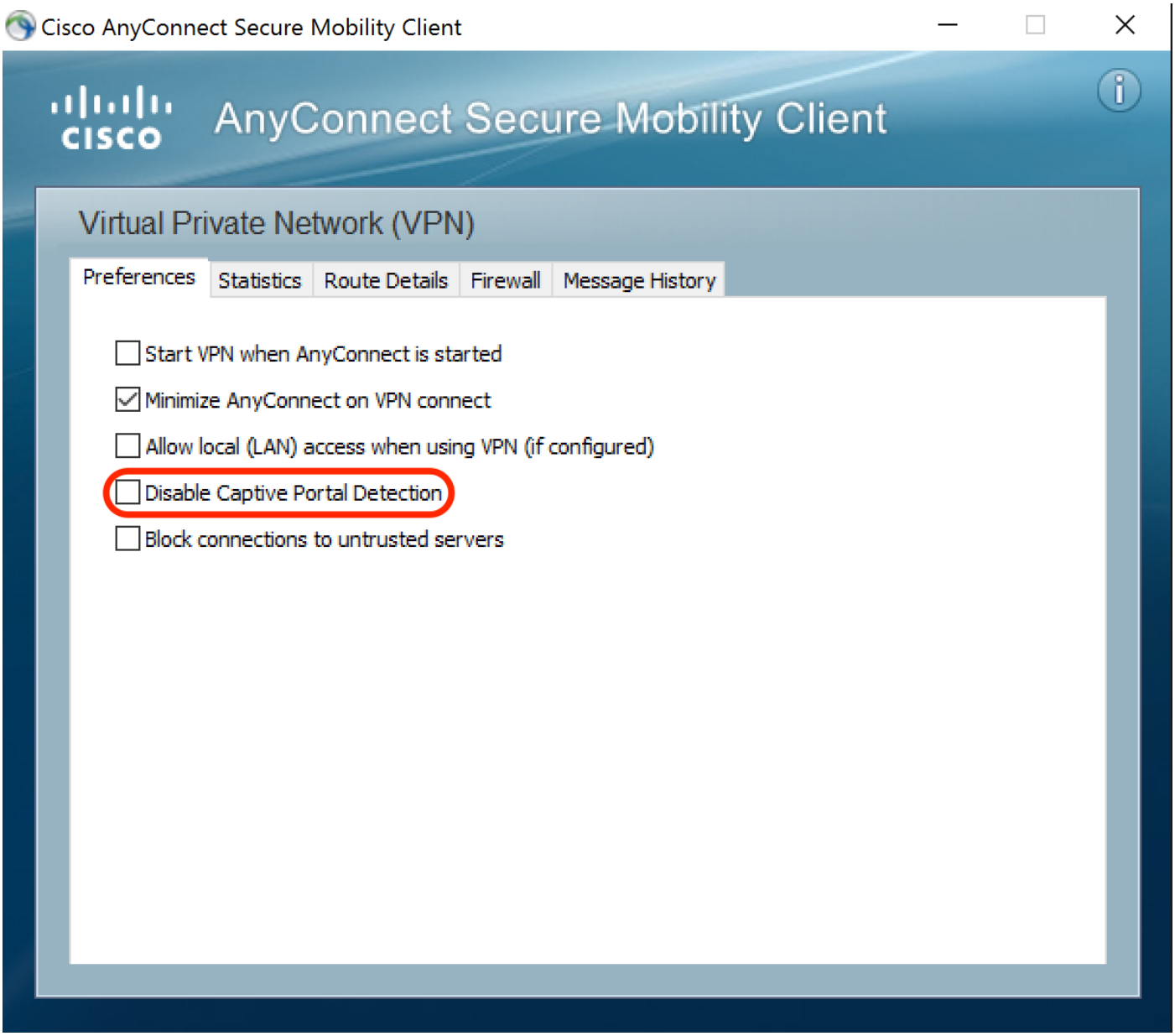
> **Caution**: O mesmo problema existe para o Roteadores do ® do Cisco IOS. Se o **server do HTTP de IP** é permitido no Cisco IOS, que está exigido se a mesma caixa é usada como o servidor PKI, AnyConnect detecta falsamente o portal prisioneiro. A ação alternativa é usar a acesso-**classe do HTTP de IP** a fim parar respostas aos pedidos do HTTP de AnyConnect, em vez de pedir a autenticação.

Desabilite a característica portal prisioneira

Épossível desabilitar a característica portal prisioneira na versão de cliente 4.2.00096 de AnyConnect e mais atrasado (veja a identificação de bug Cisco CSCud97386). O administrador pode determinar se a opção for usuário configurável ou deficiente. Esta opção está disponível sob a seção das preferências (parte 1) no editor do perfil. O administrador pode escolher a **detecção portal prisioneira** ou o **usuário do desabilitação verificável** segundo as indicações deste instantâneo do editor do perfil:



Se o usuário verificável é verificado, a caixa de seleção aparece na aba das preferências do cliente seguro UI da mobilidade de AnyConnect como mostrado aqui:


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