Implantação do AnyConnect Web Security por meio do ASA

Contents

Introduction

Este documento descreve a implantação do módulo de segurança da Web do AnyConnect para VPN baseada em cliente terminando em Cisco Adaptive Security Appliances (ASA).

Prerequisites

Requirements

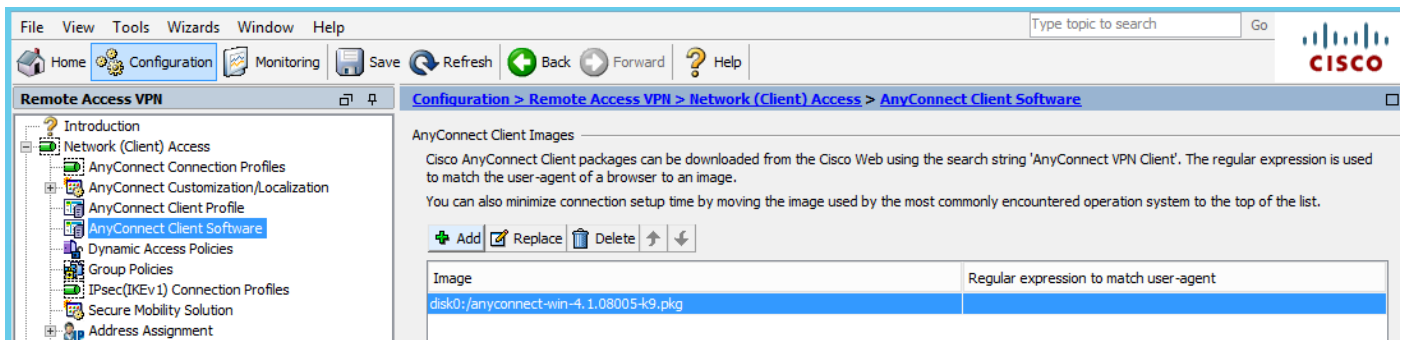Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.
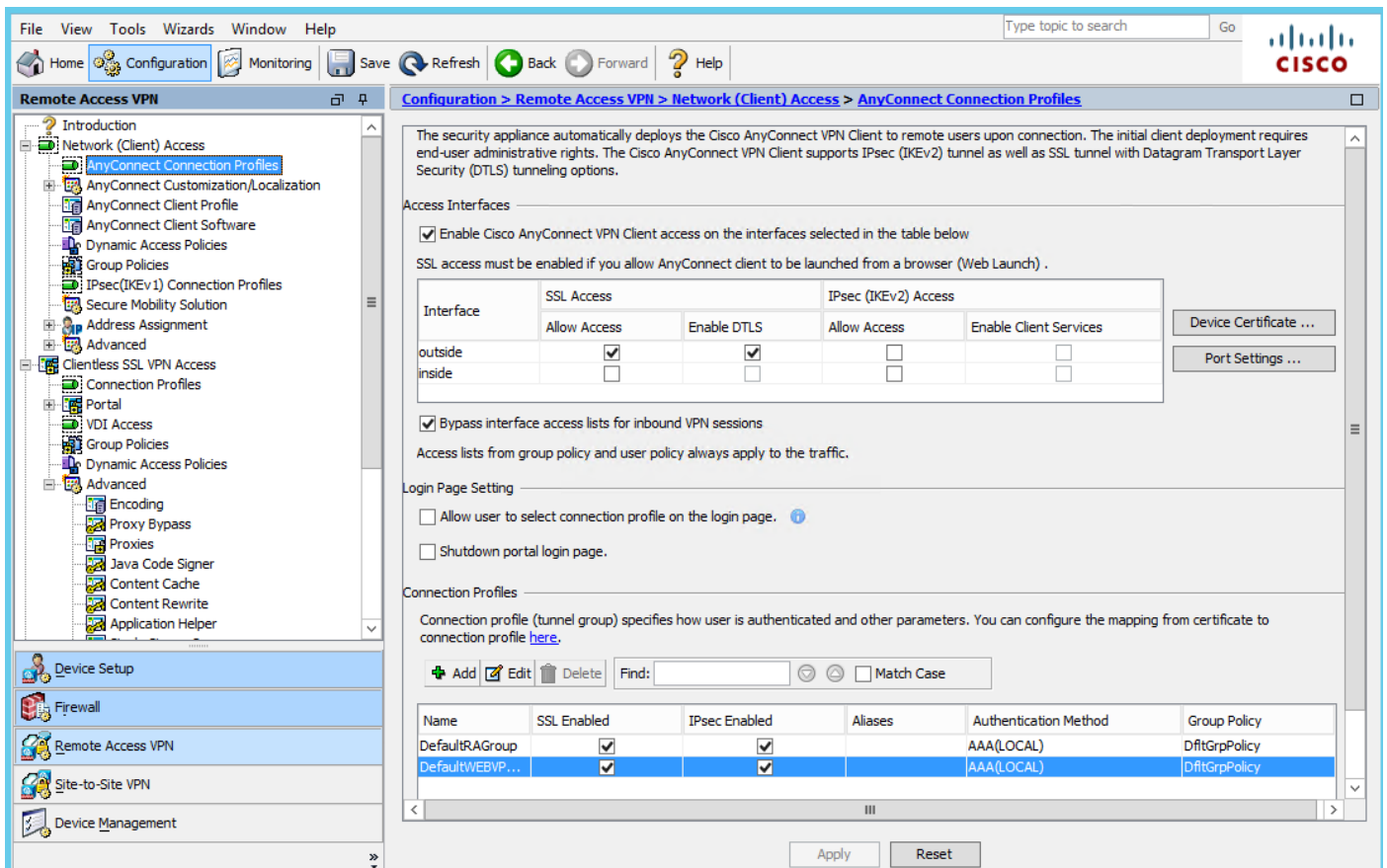
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

- Carregue a imagem do Anyconnect (recomendável v4.1+) no ASA

- Ative o perfil de VPN no ASA, como mostrado na imagem

Configurar

Implantação do Anyconnect WebSecurity por meio do ASA

As etapas envolvidas na configuração são:

- Configurar perfil do cliente do Anyconnect Websecurity
- Editar política de grupo do Anyconnect VPN
- Definir exclusão de divisão para Web Security e selecionar o módulo de cliente Web Security de download
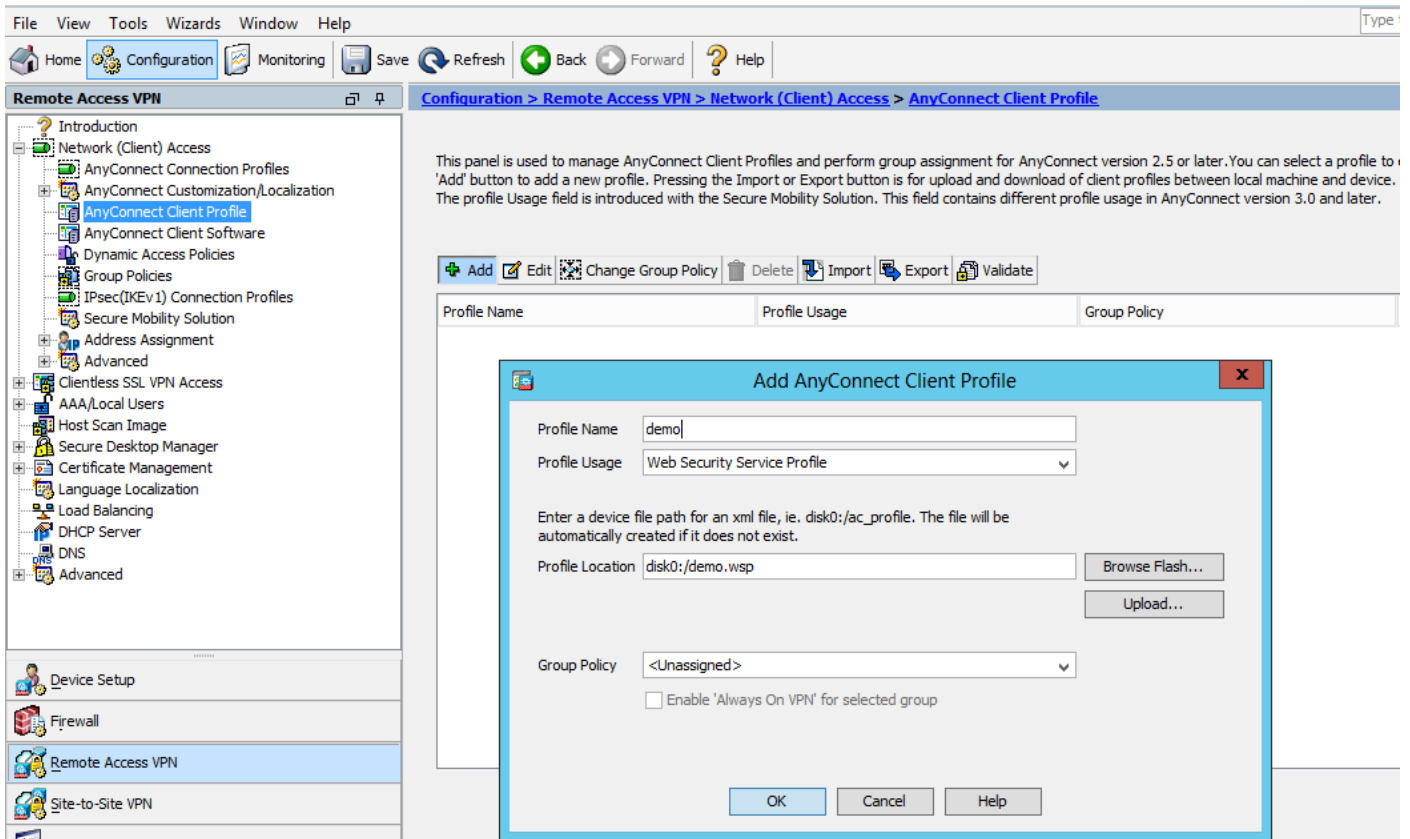- Edite a política de grupo do Anyconnect VPN e selecione o perfil do cliente Web Security

Etapa 1. Configurando o perfil do Cliente do Anyconnect Websecurity

Navegue até **Configuração >Remover VPN de Acesso >Acesso de Rede (Cliente) >Perfil do Cliente Anyconnect,** clique em

Adicione e selecione o perfil do AnyConnect Web Security Client.

> **Note**: O nome do perfil é codificado no lado do cliente, portanto, independentemente do nome configurado, o ASA sempre envia **Websecurity_serviceprofile.wso** para o cliente.

> **Note**: Este é um perfil padrão sem chave de licença de autenticação.

Etapa 2. Edite o perfil recém-criado para adicionar a chave de licença de autenticação e personalize a configuração.

Screen 1: Scanning Proxy

AnyConnect Client Profile Editor - demo

Profile: demo   About

- Introduction
- Network (Client) Access
  - AnyConnect Connection P
  - AnyConnect Customization
  - AnyConnect Client Profile
  - AnyConnect Client Softwa
  - Dynamic Access Policies
  - Group Policies
  - IPsec(IKEv1) Connection P
  - Secure Mobility Solution
  - Address Assignment
  - Advanced
- Clientless SSL VPN Access
- AAA/Local Users
- Host Scan Image
- Secure Desktop Manager
- Certificate Management
- Language Localization
- Load Balancing
- DHCP Server
- DNS
- Advanced

Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management

Device configuration loaded successful

Tree (right panel):
- Web Security
  - Scanning Proxy
  - Exceptions
  - Preferences
  - Authentication
  - Advanced

Scanning Proxy

Scanning Proxy list is currently up-to-date.

Scanning Proxy	Host Name	Plain Port	SSL Port	Display/Hide
UK	108.171.128.156	8080	443	Display
Germany	108.171.129.156	8080	443	Display
France	80.254.150.66	8080	443	Display
Denmark	80.254.154.66	8080	443	Display
Switzerland	80.254.155.66	8080	443	Display
South Africa	196.26.220.66	8080	443	Display

Display   Hide   Display All

Default Scanning Proxy

India

Traffic Listen Port

Add   Delete

80
8080
3128
443

OK   Cancel   Help

Screen 2: Authentication

AnyConnect Client Profile Editor - demo

Profile: demo   About

- Introduction
- Network (Client) Access
  - AnyConnect Connection P
  - AnyConnect Customization
  - AnyConnect Client Profile
  - AnyConnect Client Softwa
  - Dynamic Access Policies
  - Group Policies
  - IPsec(IKEv1) Connection P
  - Secure Mobility Solution
  - Address Assignment
  - Advanced
- Clientless SSL VPN Access
- AAA/Local Users
- Host Scan Image
- Secure Desktop Manager
- Certificate Management
- Language Localization
- Load Balancing
- DHCP Server
- DNS
- Advanced

Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management

Device configuration loaded successful

Tree (right panel):
- Web Security
  - Scanning Proxy
  - Exceptions
  - Preferences
  - Authentication
  - Advanced

Authentication

Proxy Authentication License Key   F90A686F696FF779CB758B69F84A5688   **

Service Password   websecurity

◉ Enable Enterprise Domains

All Domains   Use   Group Include List

Add   Add
Delete   Delete

○ Custom matching and reporting for machines not joined to domains
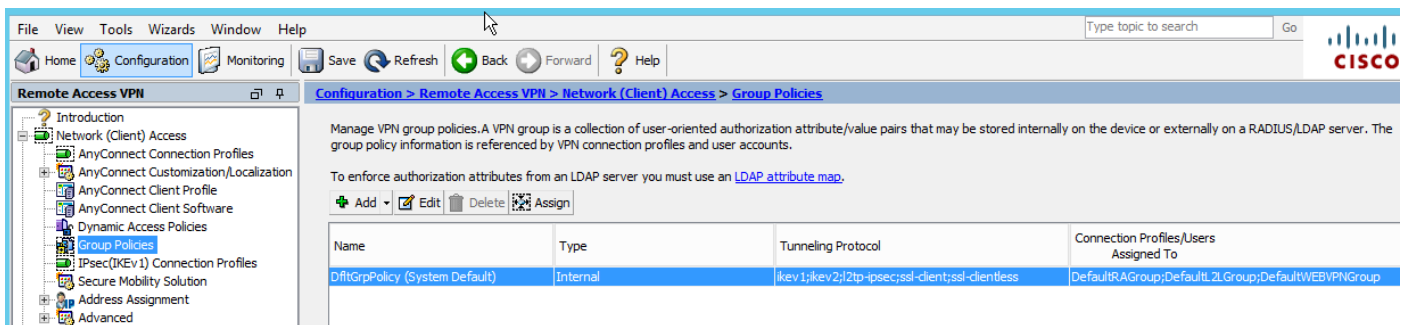
Computer Name

Custom Groups (optional)

Add
Delete

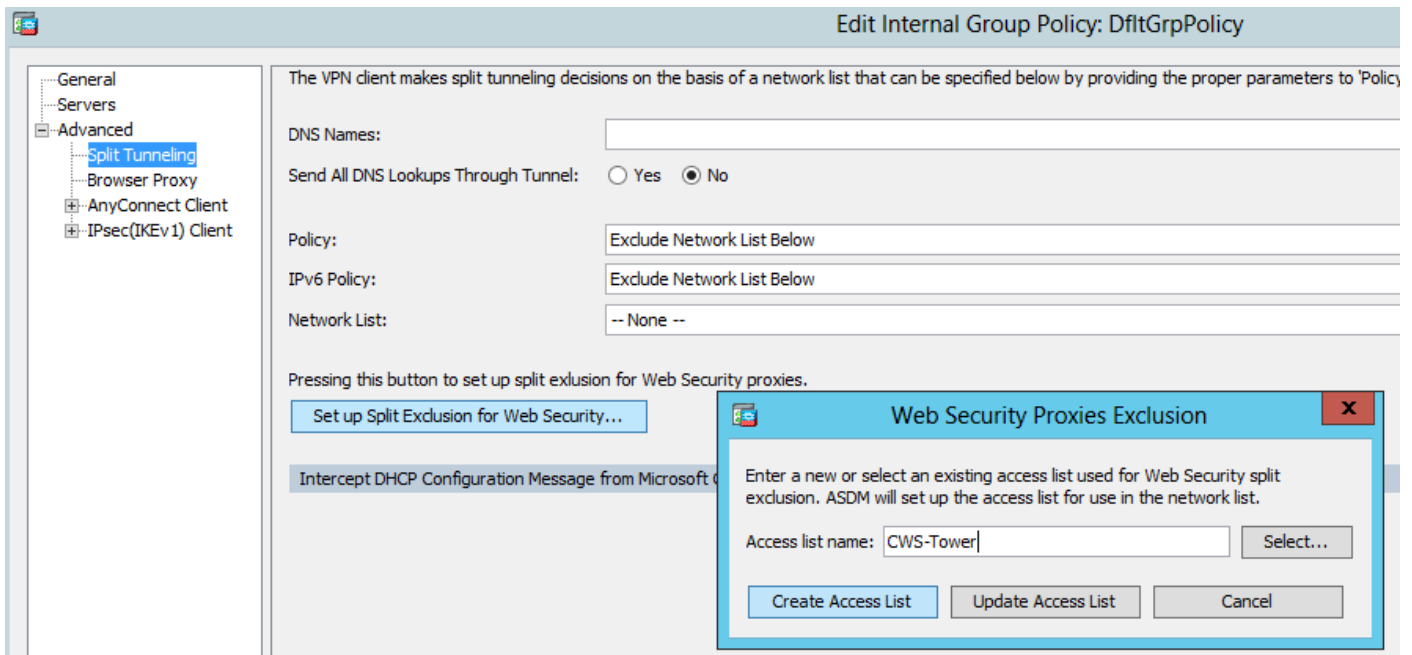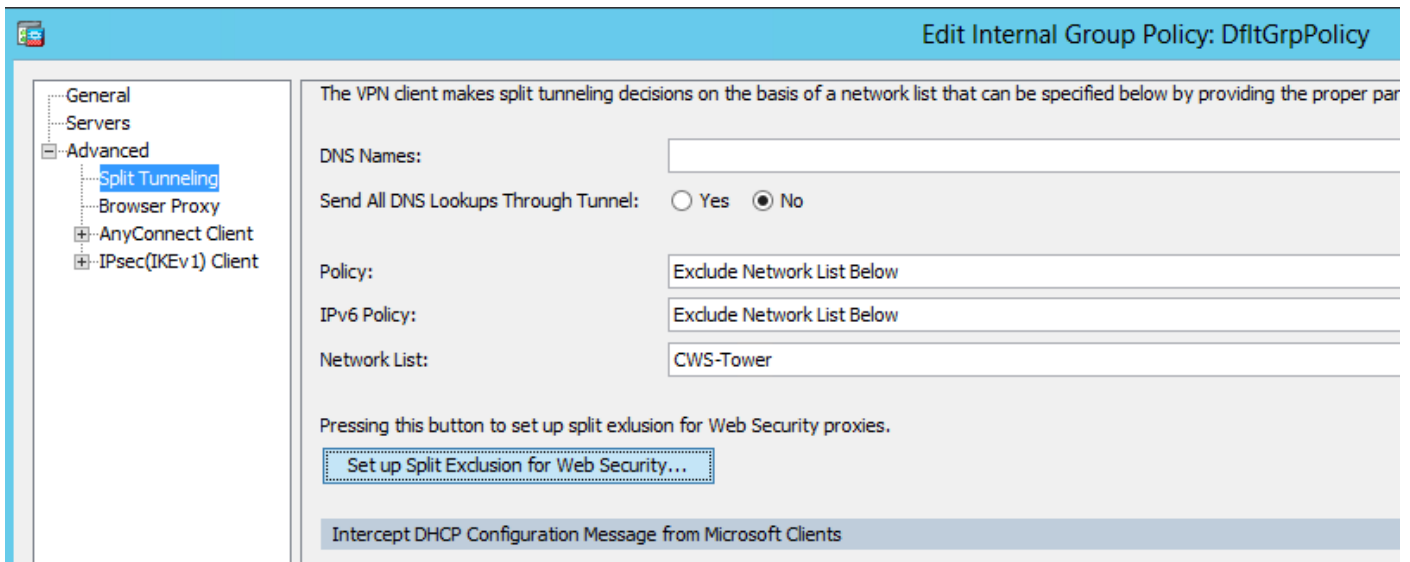** change requires WebSecurity service restart

OK   Cancel   Help

Etapa 3. Definir exclusão de divisão para Web Security e selecionar o módulo de cliente de segurança da Web de download

Edite a política de grupo do Anyconnect VPN, como mostrado na imagem.

Como mostrado na imagem, configure a exclusão de divisão para o Web Security.
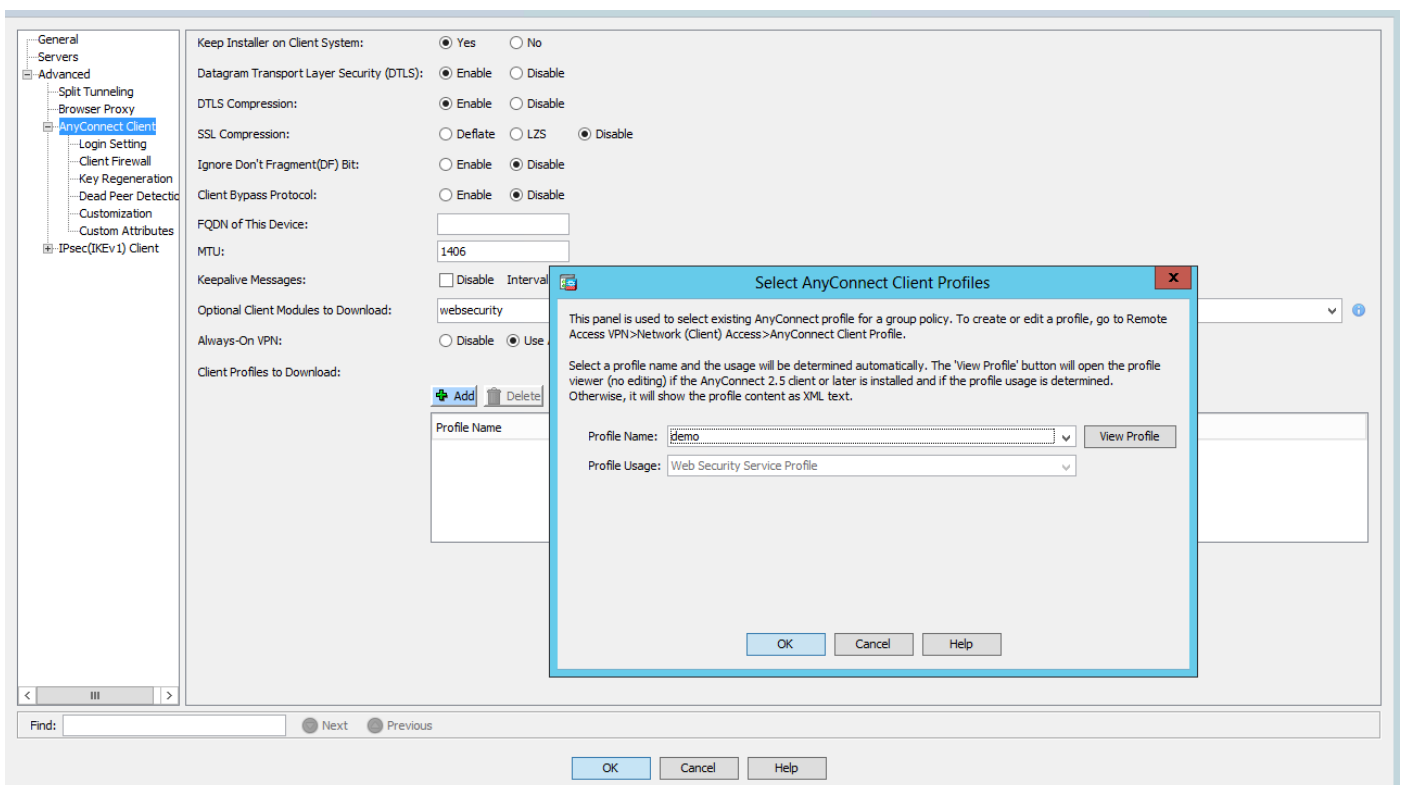
Selecione o módulo cliente do Web Security de download, conforme mostrado na imagem.

Etapa 4. Baixar perfil do cliente de segurança da Web

Editar **política de grupo do Anyconnect VPN > Perfis do cliente para Download > Adicionar,** agora escolha o perfil criado (como na Etapa 1)

Clique em OK e aplique as alterações.

Verificar

Quando você se conecta ao AnyConnect VPN, o ASA empurra o módulo de segurança da Web do Anyconnect através da VPN, como mostrado na imagem.

Cisco AnyConnect | 10.106.36.30

Username: user1
Password: *********

OK   Cancel

Cisco AnyConnect Secure Mobility Client

VPN:
Contacting 10.106.36.30.
10.106.36.30   Connect

Cisco AnyConnect Secure Mobility Client

AnyConnect Secure Mobility Client

Status Overview

VPN   >

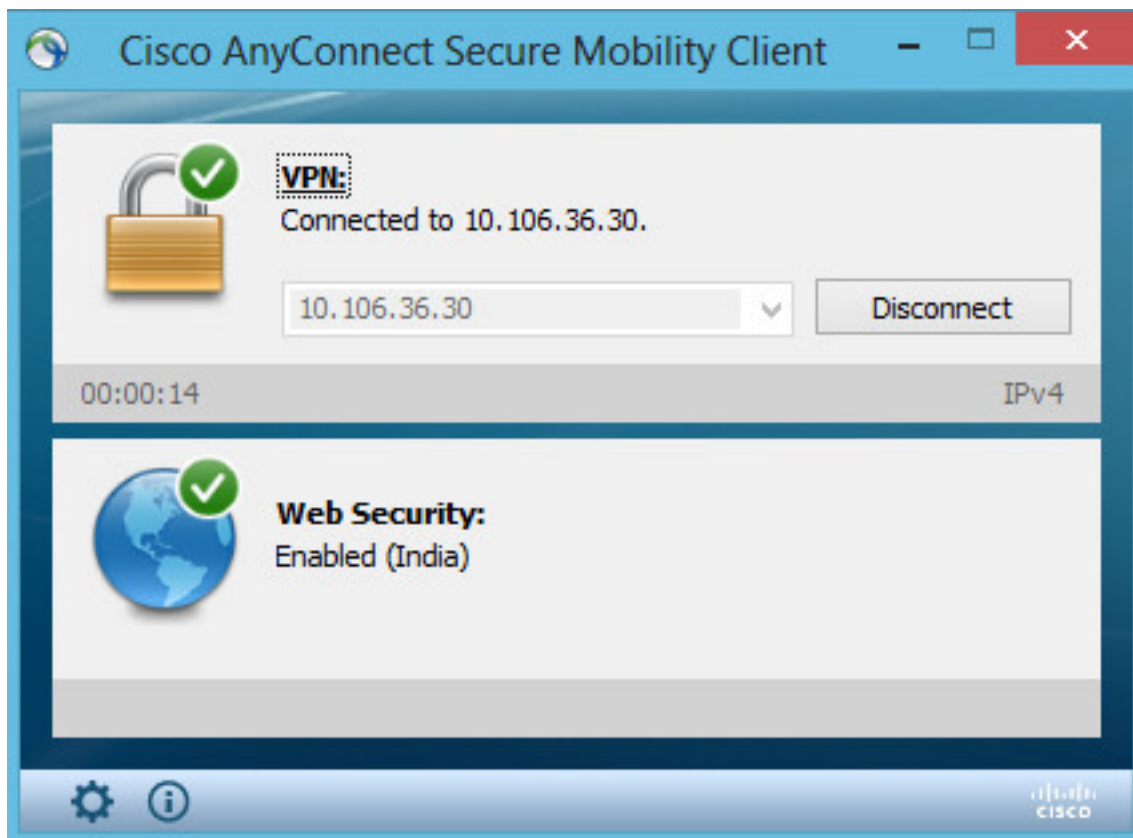Web Security

Collect diagnostic information for all
installed components.

Diagnostics...

Virtual Private Network (VPN)   Diagnostics...

Preferences | Statistics | Route Details | Firewall | Message History

5:21:58 AM   Disconnect in progress, please wait...
5:21:59 AM   Ready to connect.
5:29:49 AM   Contacting 10.106.36.30.
5:29:53 AM   User credentials entered.
5:29:53 AM   Establishing VPN session...
5:29:53 AM   The AnyConnect Downloader is performing update checks...
5:29:53 AM   Checking for profile updates...
5:29:54 AM   Downloading Web Security Service Profile - 100%
5:29:54 AM   Checking for product updates...
5:29:54 AM   Downloading AnyConnect Web Security 4.1.08005 - 100%
5:29:54 AM   Checking for customization updates...
5:29:54 AM   Performing any required updates...
5:29:58 AM   The AnyConnect Downloader updates have been completed.
5:30:02 AM   Establishing VPN session...
5:30:02 AM   Establishing VPN - Initiating connection...
5:30:02 AM   Establishing VPN - Examining system...
5:30:02 AM   Establishing VPN - Activating VPN adapter...
5:30:03 AM   Establishing VPN - Configuring system...
5:30:03 AM   Establishing VPN...
5:30:03 AM   Connected to 10.106.36.30.

Clear

Se você já estiver conectado, é recomendável fazer logoff e, em seguida, fazer logon novamente para que a funcionalidade seja habilitada.

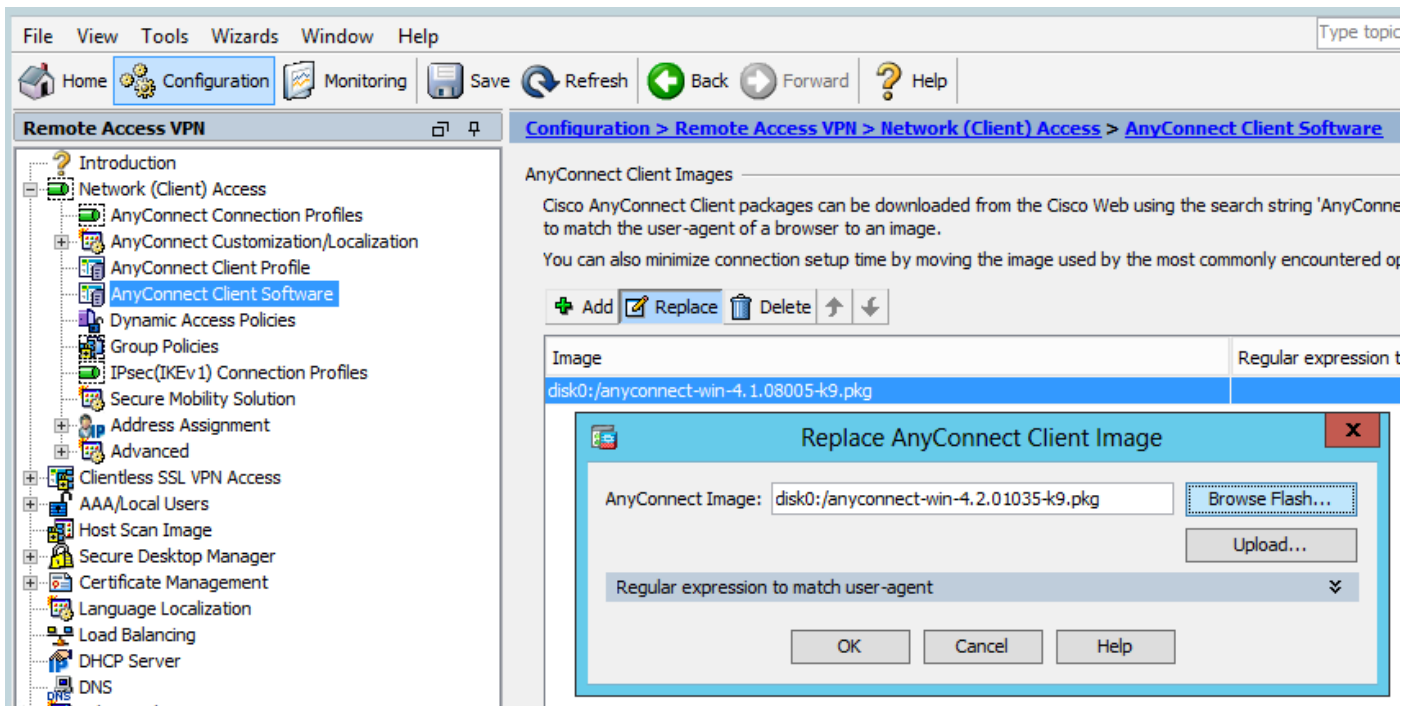## Atualizar/rebaixar versão do Anyconnect

A funcionalidade de implantação permanecerá inalterada se a versão for atualizada. No entanto, não é possível fazer downgrade. Assim, com o exemplo atual de 4.1.x, ele pode ser atualizado para a versão 4.2
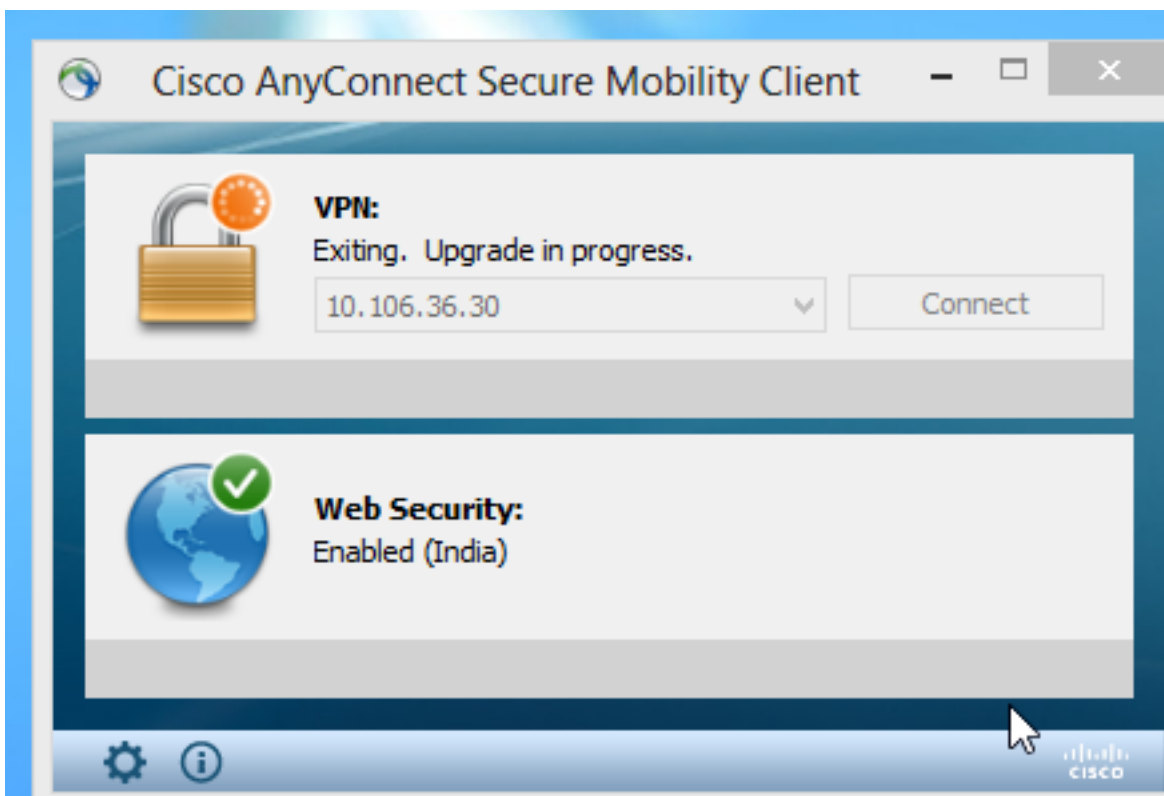
As etapas envolvidas são as seguintes:

Etapa 1. Carregue o pacote 4.2 do Anyconnect mais recente para flash e substitua 4.1 pelo arquivo mais recente.
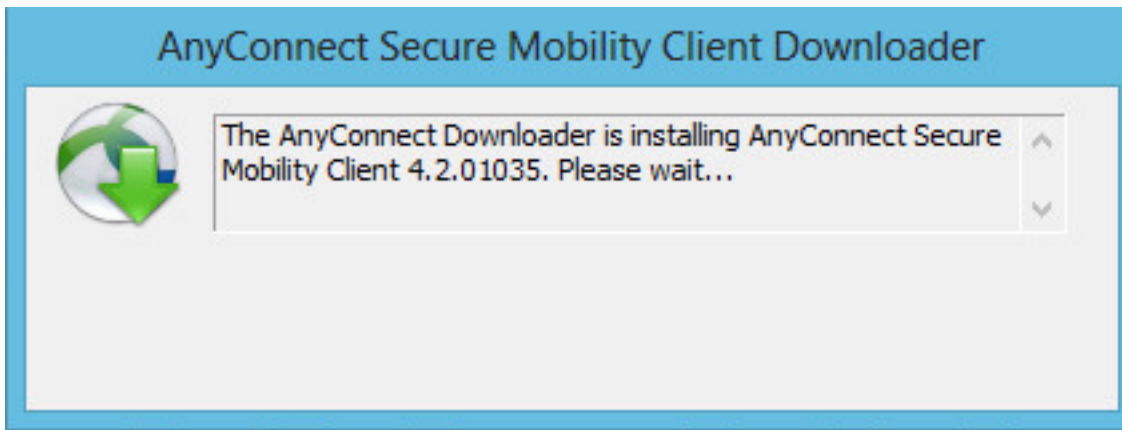
Em **Anyconnect Client Software > Replace** e escolha o arquivo de imagem recente.

Etapa 2. Quando você se reconecta ao AnyConnect VPN, o ASA empurra o módulo Anyconnect mais recente através da VPN sem alterações no perfil de segurança da Web.

AnyConnect Secure Mobility Client Downloader

The AnyConnect Downloader is installing AnyConnect Secure Mobility Client 4.2.01035. Please wait...

Note: Não há suporte para downgrade.

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Usando o DART para coletar informações de solução de problemas:

DART é a ferramenta de diagnóstico e relatório do AnyConnect que você pode usar para coletar dados úteis para solucionar problemas de instalação e conexão do AnyConnect. O DART suporta Windows 7, Windows Vista, Windows XP, Mac versão 10.5 e 10.6 e Linux Redhat. O assistente DART é executado no computador que executa o AnyConnect. Ele reúne os registros, o status e as informações de diagnóstico para a análise do Cisco Technical Assistance Center (TAC) e não exige privilégios de administrador.

Embora o DART não confie em nenhum componente do software AnyConnect para ser executado, ainda que você possa iniciá-lo a partir do AnyConnect, ele coletará o arquivo de log do AnyConnect, se disponível. Atualmente, o DART está disponível como uma instalação independente ou o administrador pode enviar esse aplicativo para o PC cliente como parte da infraestrutura de download dinâmico do AnyConnect. Depois de instalado, o usuário final pode iniciar o assistente na pasta Cisco disponível por meio do botão **Iniciar**.