Configurar o túnel de divisão dinâmica do AnyConnect no FTD gerenciado pelo FMC

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Limitações](#)
[Configurar](#)
[Etapa 1. Edite a Política de Grupo para usar o Túnel Dividido Dinâmico](#)
[Etapa 2. Configurar o atributo personalizado do AnyConnect](#)
[Etapa 3. Verificar a configuração, Salvar e Implantar](#)
[Verificar](#)
[Troubleshoot](#)
[Problema](#)
[Solução](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar o AnyConnect Dynamic Split Tunnel no Firepower Threat Defense (FTD) gerenciado pelo Firepower Management Center (FMC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco AnyConnect
- Conhecimentos básicos de CVP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- FMC versão 7.0
- FTD versão 7.0

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A configuração do túnel dividido dinâmico AnyConnect no FTD gerenciado pelo FMC está totalmente disponível no FMC versão 7.0 e mais recente. Se você executar uma versão mais antiga, precisará configurá-la via FlexConfig, conforme instruído em Advanced AnyConnect VPN Deployments for Firepower Threat Defense with FMC.

Com a configuração de túnel dividido dinâmico, você pode ajustar a configuração de túnel dividido com base nos nomes de domínio DNS. Como os endereços IP associados a nomes de domínio totalmente qualificados (FQDN) podem mudar, a configuração de túnel dividido com base em nomes DNS fornece uma definição mais dinâmica de qual tráfego está ou não incluído no túnel VPN de acesso remoto. Se algum endereço retornado para nomes de domínio excluídos estiver dentro do pool de endereços incluído na VPN, esses endereços serão excluídos. Os domínios excluídos não são bloqueados. Em vez disso, o tráfego para esses domínios é mantido fora do túnel VPN.

Observe que você também pode configurar o túnel de divisão dinâmica para definir domínios a serem incluídos no túnel que seriam excluídos de outra forma com base no endereço IP.

Limitações

No momento, esses recursos ainda não são suportados:

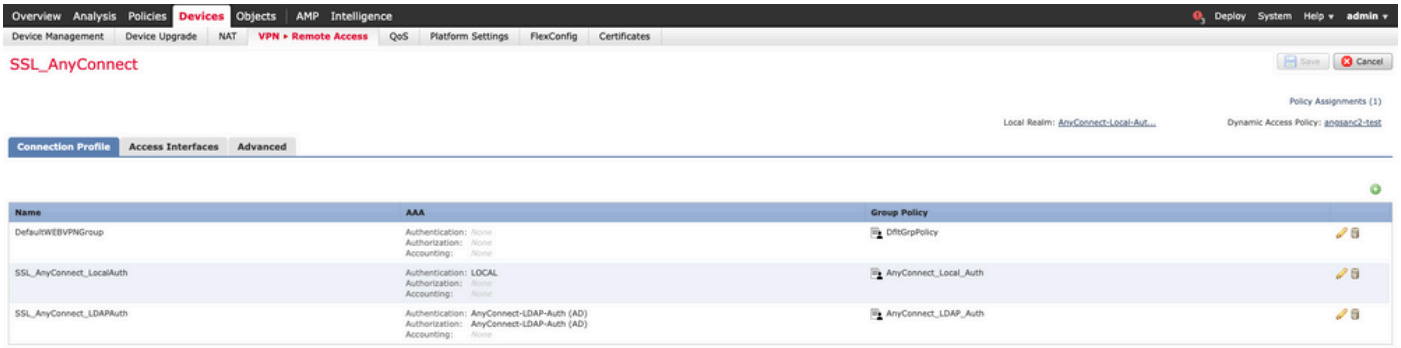
- O Dynamic Split Tunnel não é suportado em dispositivos iOS (Apple). Consulte o bug da Cisco ID CSCvr54798
- O Dynamic Split Tunnel não é suportado em clientes Anyconnect Linux. Consulte o bug da Cisco IDCSCvt64988

Configurar

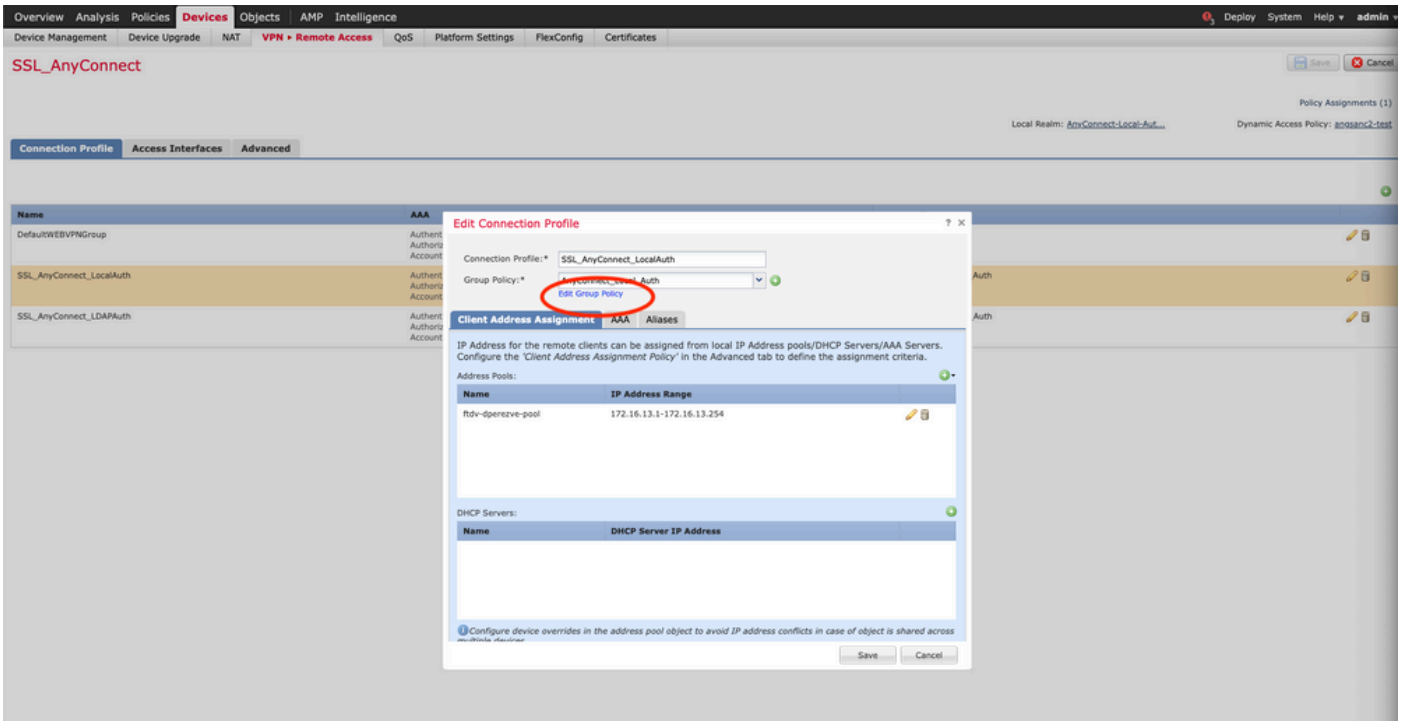
Esta seção descreve como configurar o túnel de divisão dinâmica do AnyConnect no FTD gerenciado pelo FMC.

Etapa 1. Edite a Política de Grupo para usar o Túnel Dividido Dinâmico

1. No FMC, navegue até **Devices > VPN > Remote Access** e selecione o **Perfil de Conexão** ao qual deseja aplicar a configuração.

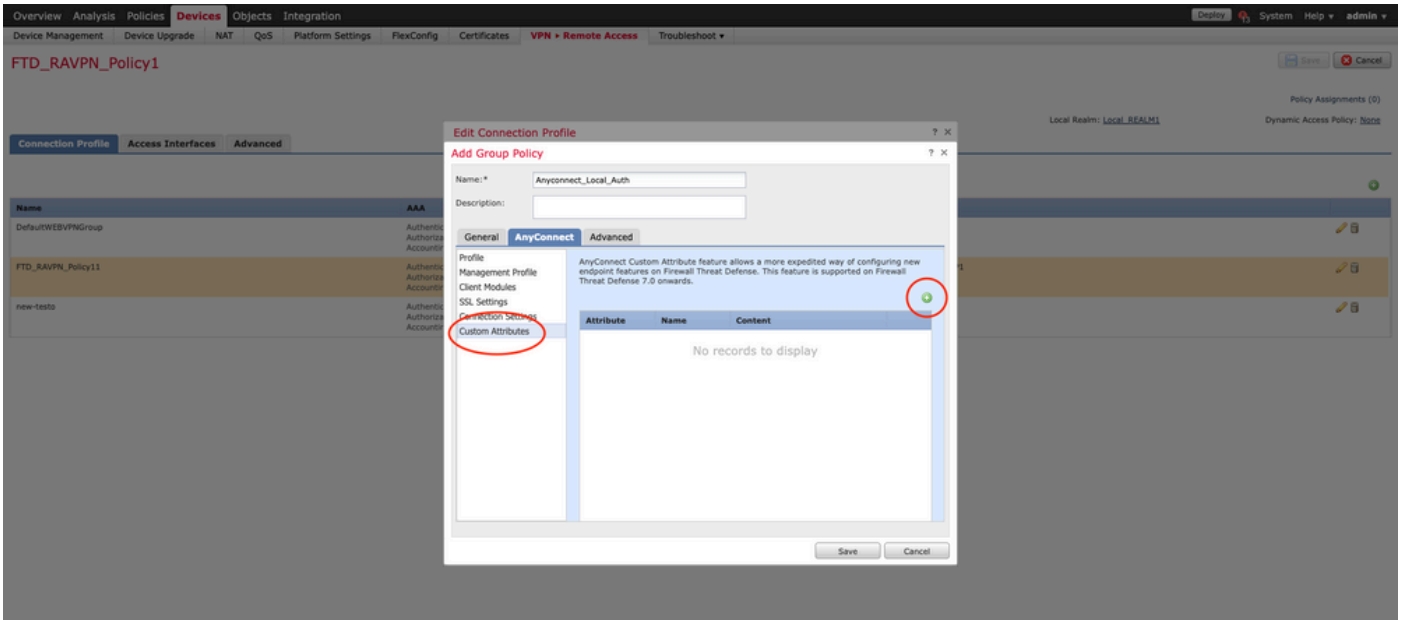


2. Selecione **Editar Política de Grupo** para modificar uma das políticas de grupo já criadas.

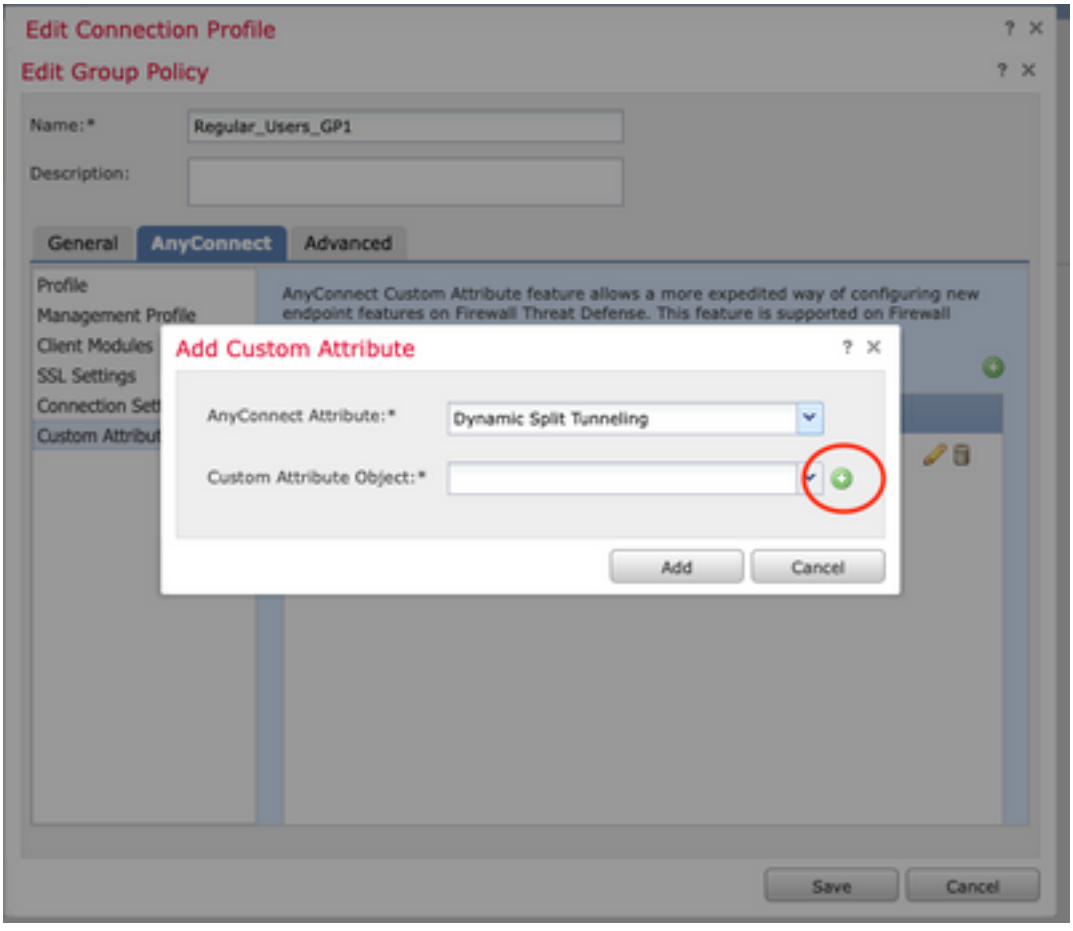


Etapa 2. Configurar o atributo personalizado do AnyConnect

1. Na configuração de Diretiva de Grupo, navegue até **Anyconnect** > Custom Attributes, clique no botão **Add (+)**:

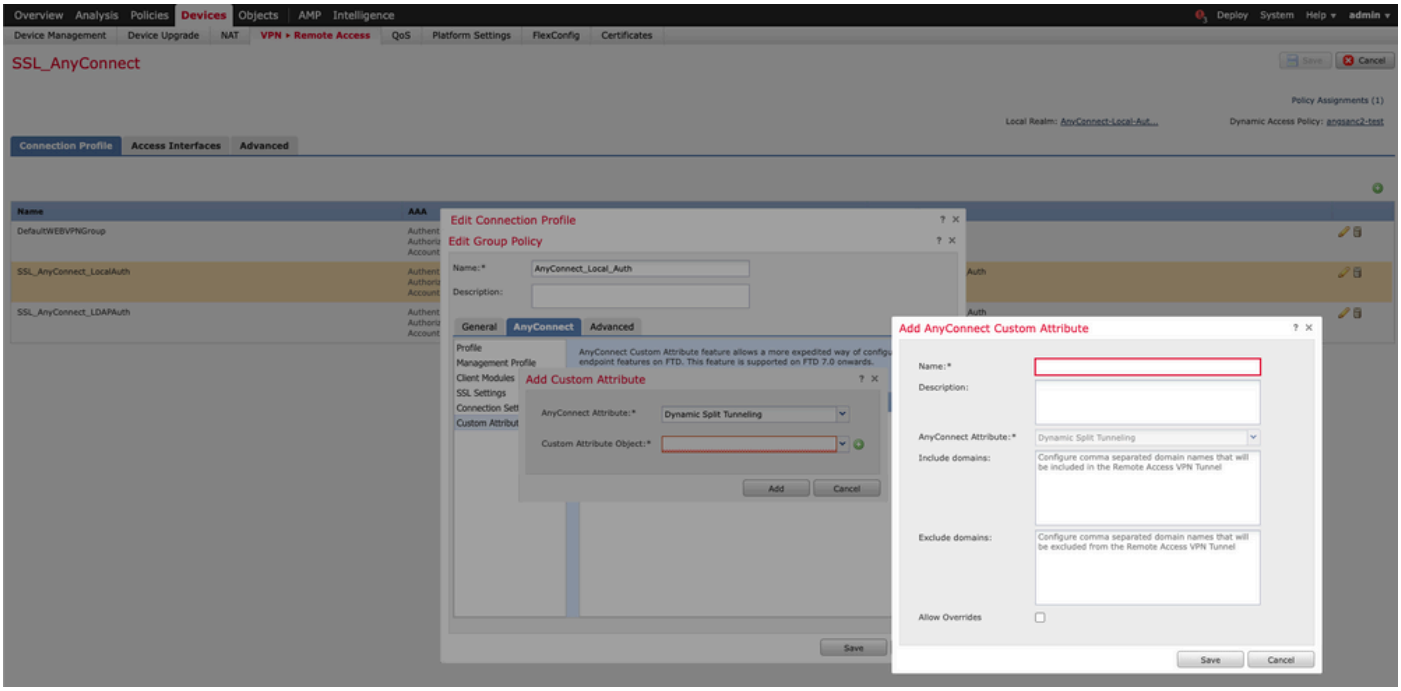


2. Selecione o atributo **Dynamic Split Tunneling** AnyConnect e clique no botão **Add (+)** para criar um novo objeto de atributo personalizado:

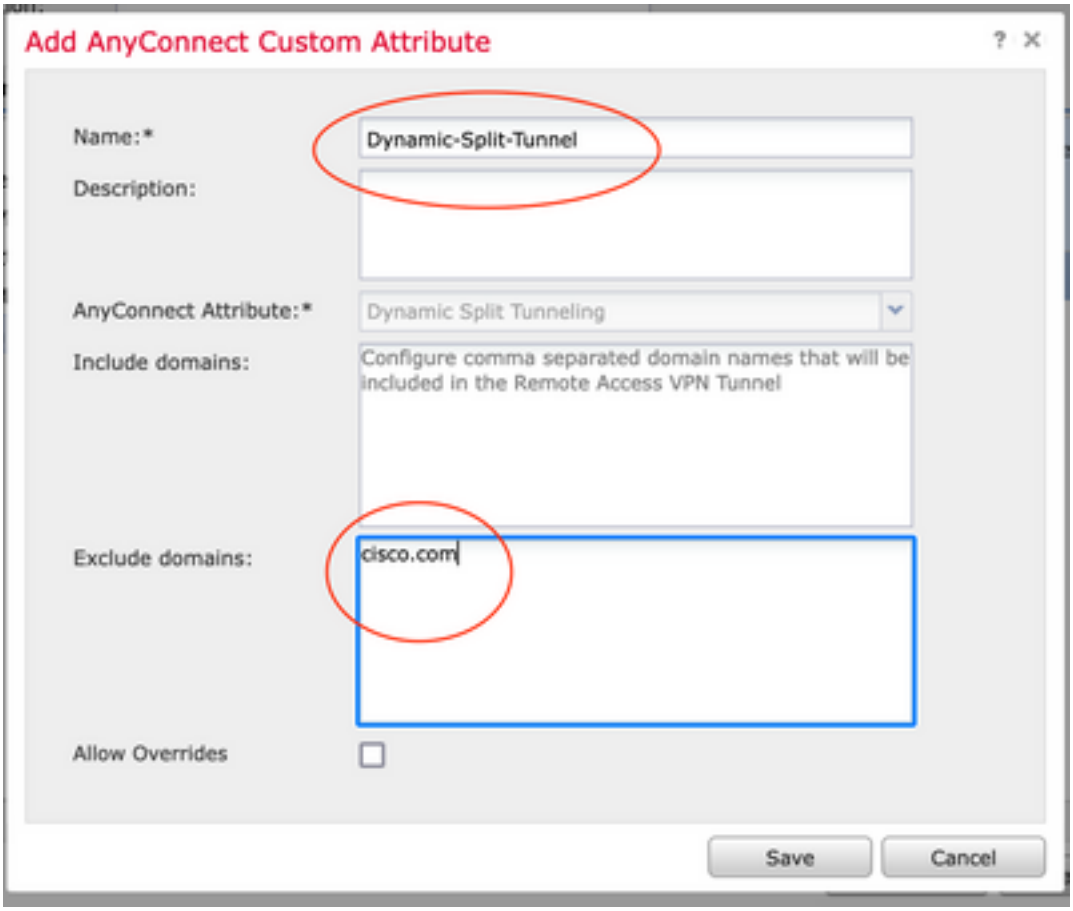


3. Insira o **Nome** do **Atributo personalizado do AnyConnect** e configure os domínios para serem dinamicamente incluídos ou excluídos.

> **Observação**: você só pode configurar **Incluir domínios** ou **Excluir domínios**.

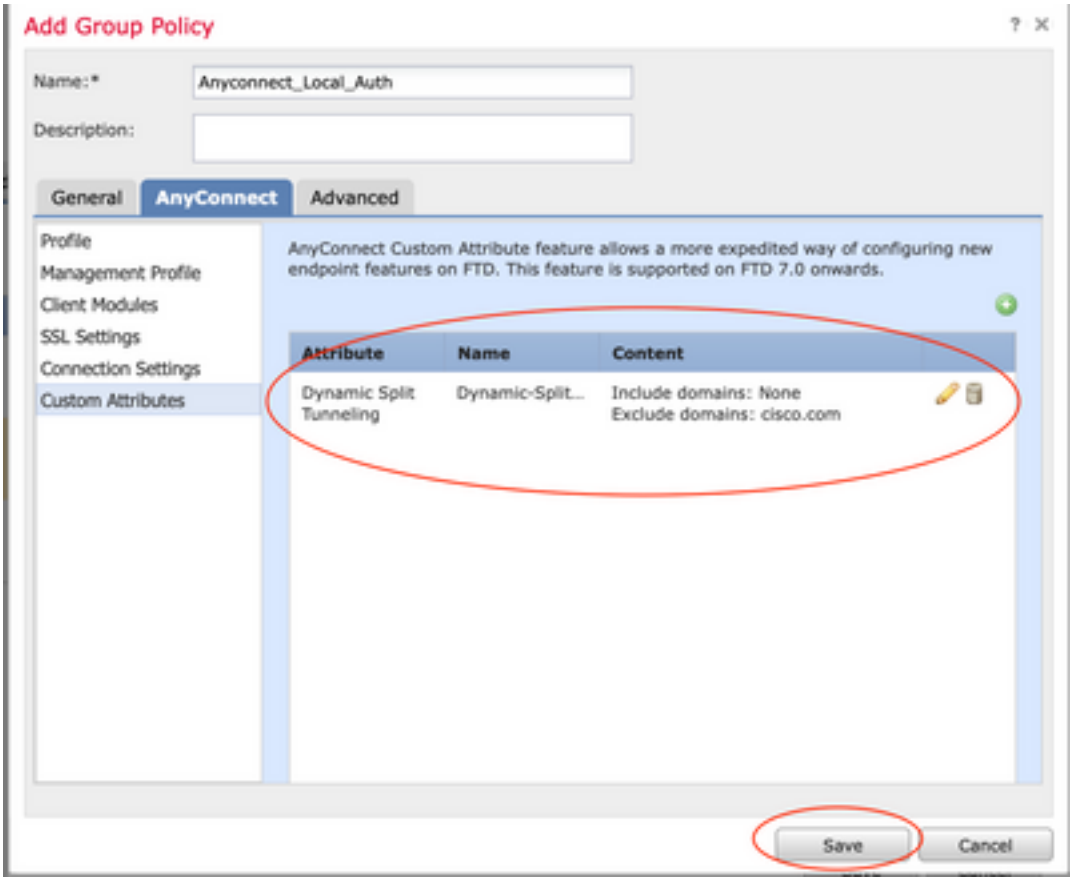


Neste exemplo, configuramos **cisco.com** como o domínio a ser excluído e nomeamos o atributo personalizado **Dynamic-Split-Tunnel**, como mostrado na imagem:



Etapa 3. Verificar a configuração, Salvar e Implantar

Verifique se o atributo personalizado configurado está correto, salve a configuração e implante as alterações no FTD em questão.



Verificar

Você pode executar estes comandos no FTD através da interface de linha de comando (CLI) para confirmar a configuração do túnel dividido dinâmico:

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy **<Nome da diretiva de grupo>**

Neste exemplo, a configuração é a seguinte:

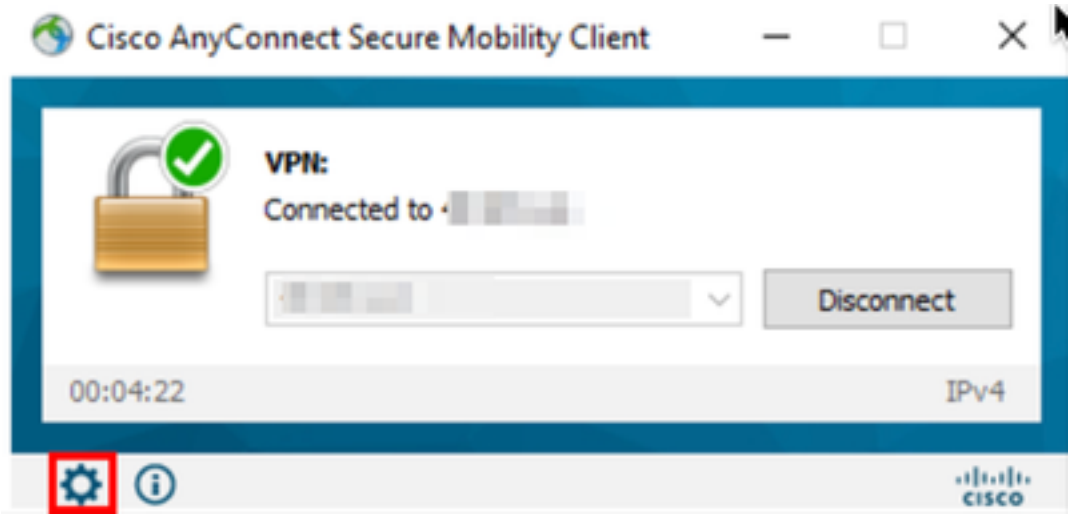
```
ftd# show run group-policy Anyconnect_Local_Auth
group-policy Anyconnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list value AC_networks
Default-domain none
split-dns none
address-pools value AC_pool
anyconnect-custom dynamic-split-exclude-domains value cisco.com
anyconnect-custom dynamic-split-include-domains none

ftd# show run webvpn
webvpn
enable outside
anyconnect-custom-attr dynamic-split-exclude-domains
```

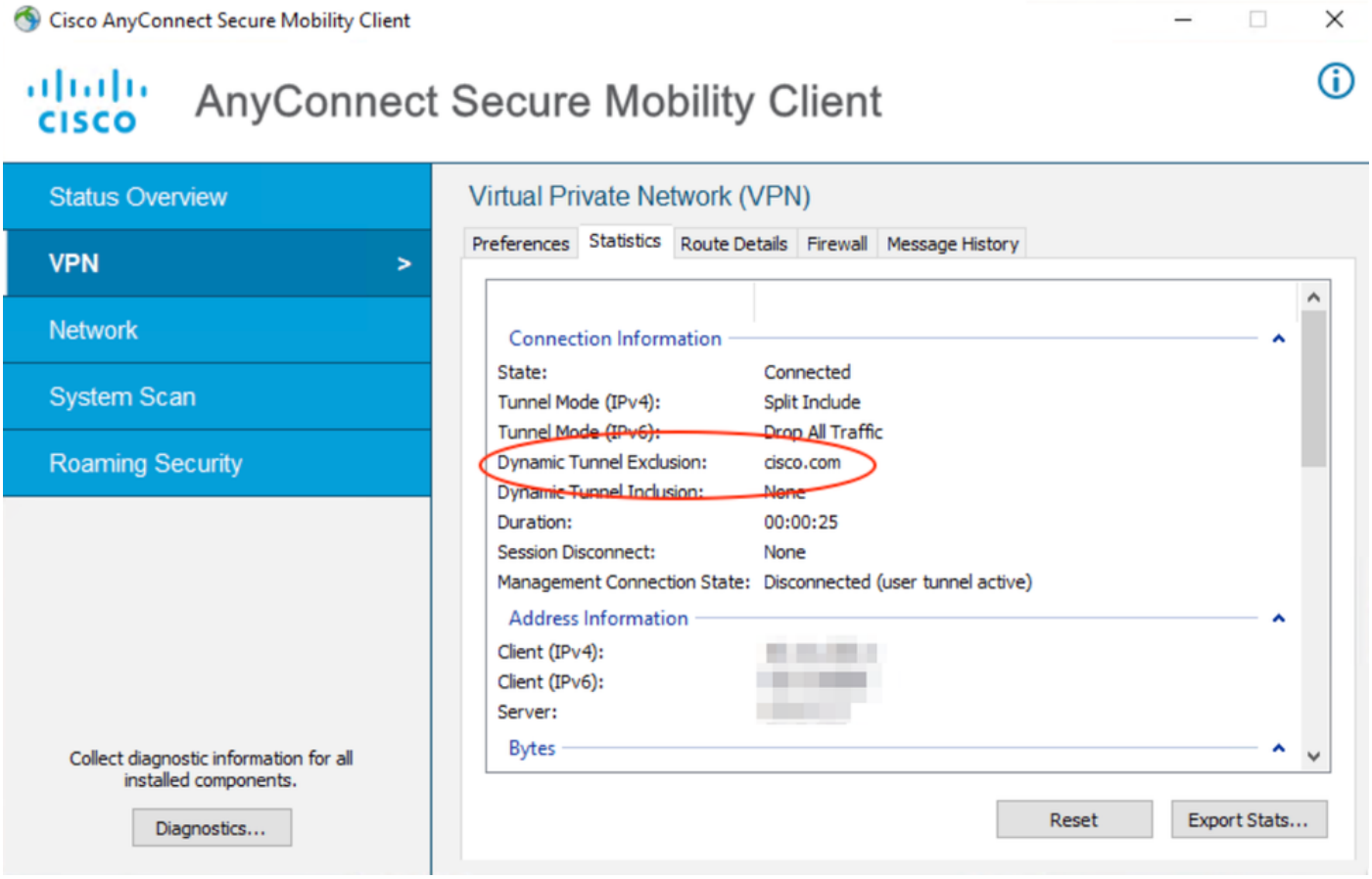
```
anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert_map_test 10 cert_auth
error-recovery disable
```

Para verificar as exclusões de túnel dinâmico configuradas no cliente:

1. Inicie o software AnyConnect e clique no ícone da engrenagem, como mostrado na imagem:



2. Navegue até **VPN > Statistics** e confirme os domínios exibidos em **Dynamic Split Exclusion/Inclusion**:



Troubleshoot

Você pode usar o AnyConnect Diagnostics and Reporting Tool (DART) para coletar os dados que são úteis para solucionar problemas de instalação e conexão do AnyConnect.

O DART reúne os registros, o status e as informações de diagnóstico para a análise do Cisco Technical Assistance Center (TAC) e não exige os privilégios de administrador para ser executado no computador cliente.

Problema

Se um curinga for configurado nos atributos personalizados do AnyConnect, por exemplo, ***.cisco.com**, a sessão do AnyConnect será desconectada.

Solução

Você pode usar o valor de domínio **cisco.com** para permitir o substituto do curinga. Essa alteração permite incluir ou excluir domínios como **www.cisco.com** e **tools.cisco.com**.

Informações Relacionadas

- Para obter assistência adicional, entre em contato com o Centro de Assistência Técnica (TAC). É necessário um contrato de suporte válido: Contatos de suporte da Cisco no mundo inteiro.
- Você também pode visitar a Comunidade Cisco VPN aqui.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.