Configurar o túnel VPN de gerenciamento do AnyConnect no ASA

Contents

Introduction

Este documento descreve como configurar um ASA quando o gateway VPN aceita conexões do Cisco AnyConnect Secure Mobility Client através do túnel VPN de gerenciamento.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de VPN através do Adaptive Security Device Manager (ASDM)
- Configuração CLI do ASA (Basic Adaptive Security Appliance)
- Certificados X509

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco ASA versão 9.12(3)9
- Software Cisco ASDM versão 7.12.2
- Windows 10 com Cisco AnyConnect Secure Mobility Client versão 4.8.03036

Observação: faça download do pacote de implantação Web do AnyConnect VPN (anyconnect-

win*.pkg or anyconnect-macos*.pkg) no Download de Software da Cisco (somente clientes registrados). Copie o AnyConnect VPN Client para a memória flash do ASA que deve ser baixada para os computadores de usuários remotos para estabelecer a conexão VPN SSL com o ASA. Consulte a seção Instalação do AnyConnect Client do guia de configuração do ASA para obter mais informações.

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

Um túnel VPN de gerenciamento garante a conectividade com a rede corporativa sempre que o sistema cliente é ligado, não apenas quando uma conexão VPN é estabelecida pelo usuário final. Você pode executar o gerenciamento de patches em endpoints fora do escritório, especialmente em dispositivos que raramente são conectados pelo usuário, via VPN, à rede do escritório. Os scripts de login de SO de endpoint que exigem conectividade de rede corporativa também se beneficiam desse recurso.

O túnel de gerenciamento do AnyConnect permite que os administradores conectem o AnyConnect sem intervenção do usuário antes de quando o usuário faz login. O túnel de gerenciamento do AnyConnect pode funcionar em conjunto com a Detecção de rede confiável e, portanto, é acionado somente quando o endpoint está fora do local e desconectado de uma VPN iniciada pelo usuário. O túnel de gerenciamento do AnyConnect é transparente para o usuário final e se desconecta automaticamente quando o usuário inicia a VPN.

SO/aplicativo	Requisitos mínimos de versão
ASA	9.0.1
ASDM	7.10.1
Versão do Windows AnyConnect	4.7.00136
Versão do AnyConnect para MacOS	4.7.01076
Linux	Sem suporte

Funcionamento do túnel de gerenciamento

O serviço AnyConnect VPN Agent é iniciado automaticamente na inicialização do sistema. Ele detecta que o recurso de túnel de gerenciamento está habilitado (através do perfil VPN de gerenciamento), portanto, inicia a aplicação cliente de gerenciamento para iniciar uma conexão de túnel de gerenciamento. O aplicativo cliente de gerenciamento usa a entrada de host do perfil de VPN de gerenciamento para iniciar a conexão. Em seguida, o túnel VPN é estabelecido como de costume, com uma exceção: nenhuma atualização de software é executada durante uma conexão de túnel de gerenciamento, já que o túnel de gerenciamento deve ser transparente para o usuário.

O usuário inicia um túnel VPN por meio da interface do usuário do AnyConnect, que aciona a terminação do túnel de gerenciamento. No término do túnel de gerenciamento, o estabelecimento do túnel do usuário continua como de costume.

O usuário desconecta o túnel VPN, o que aciona o restabelecimento automático do túnel de gerenciamento.

Limitações

- Não há suporte para interação do usuário
- Somente há suporte para autenticação baseada em certificado por meio do Repositório de Certificados de Computador (Windows)
- A verificação estrita do certificado do servidor é imposta
- Não há suporte para um proxy privado
- Não há suporte para um proxy público (o valor ProxyNative tem suporte em plataformas nas quais as configurações de Proxy Nativo não são recuperadas do navegador)
- Scripts de personalização do AnyConnect não são suportados

Observação: para obter mais informações, consulte Sobre o Túnel VPN de Gerenciamento.

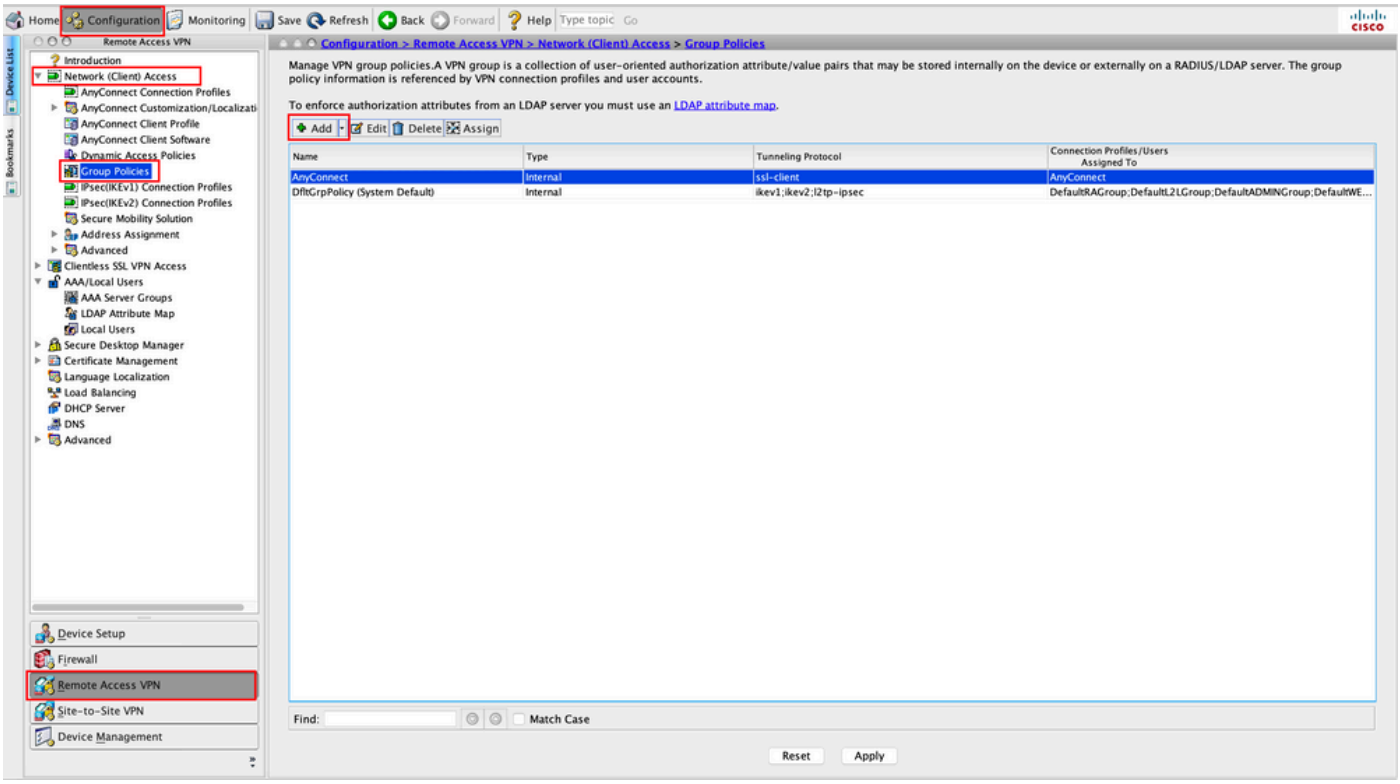
Configurar

Esta seção descreve como configurar o Cisco ASA como o gateway VPN para aceitar conexões de clientes AnyConnect através do túnel VPN de gerenciamento.

Configuração no ASA através do ASDM/CLI

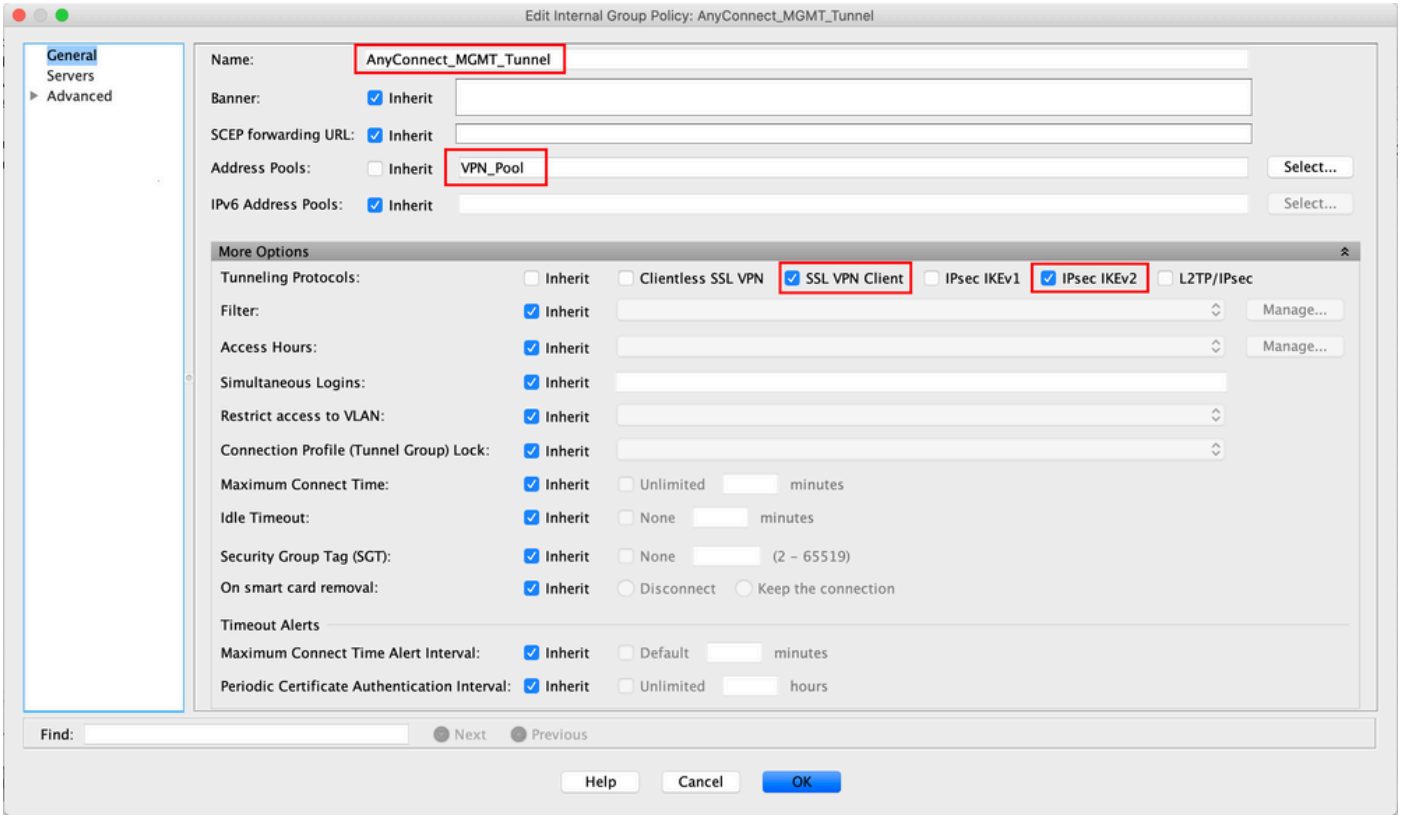
Etapa 1. Crie a política de grupo do AnyConnect. Navegue até Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Clique em Add.

Observação: é aconselhável criar uma nova Política de grupo do AnyConnect que é usada apenas para o túnel de gerenciamento do AnyConnect.

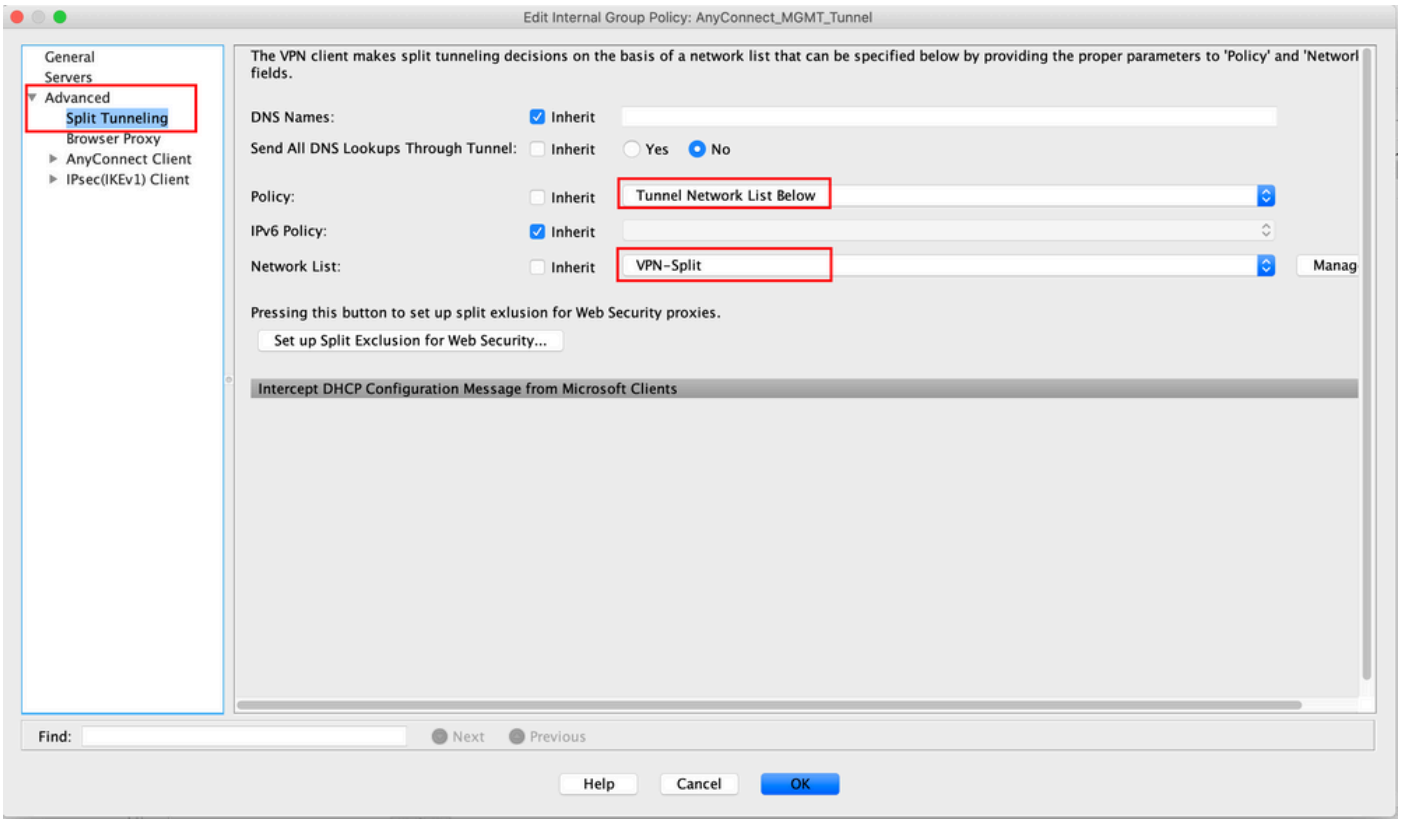


Etapa 2. Fornecer uma Name para a Política de Grupo. Atribuir/Criar um Address Pool.

Escolher Tunneling Protocols como SSL VPN Client e/ou IPsec IKEv2,conforme mostrado na imagem.



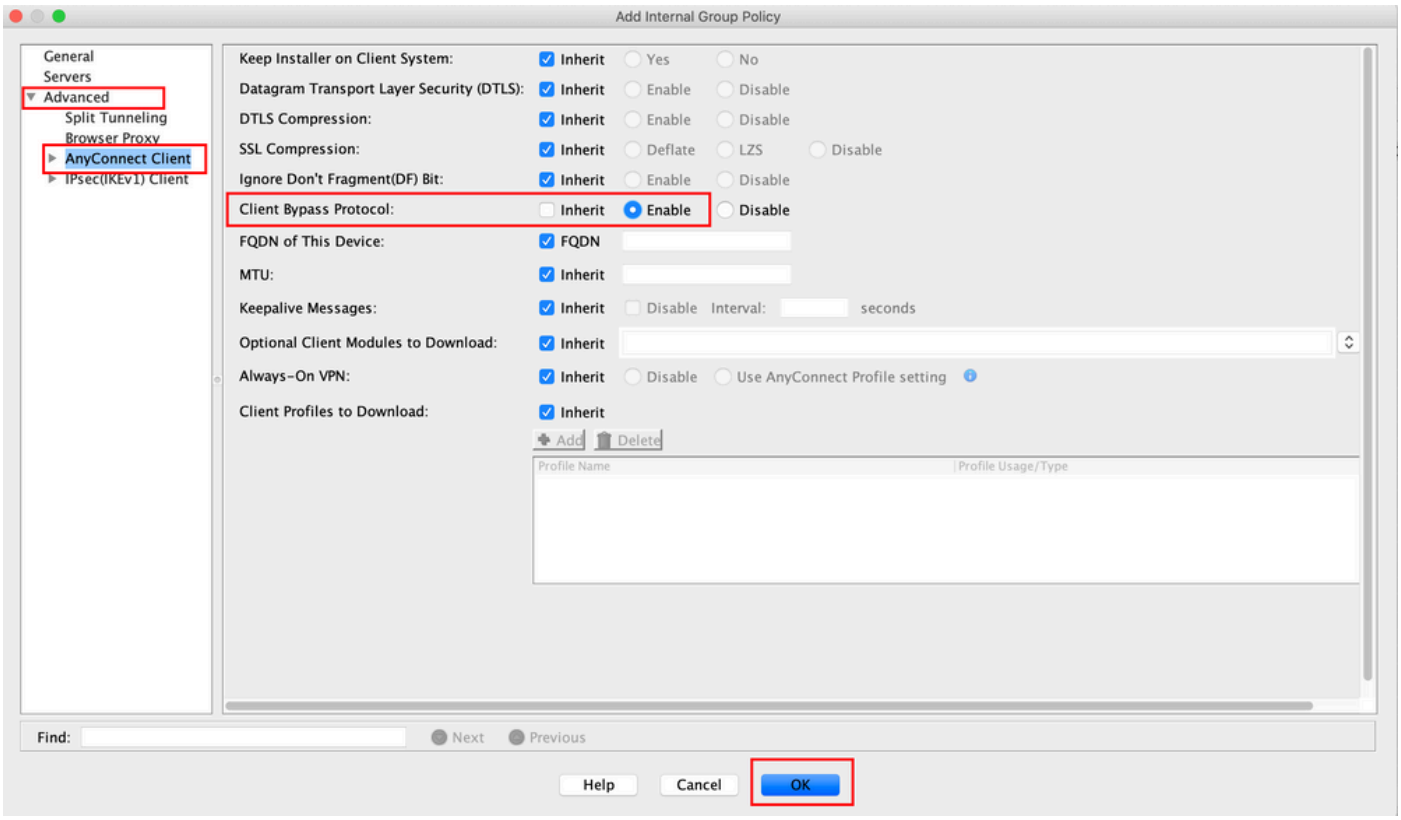
Etapa 3. Navegue até Advanced > Split Tunneling. Configurar o Policy como Tunnel Network List Below e escolha a opção Network List,conforme mostrado na imagem.



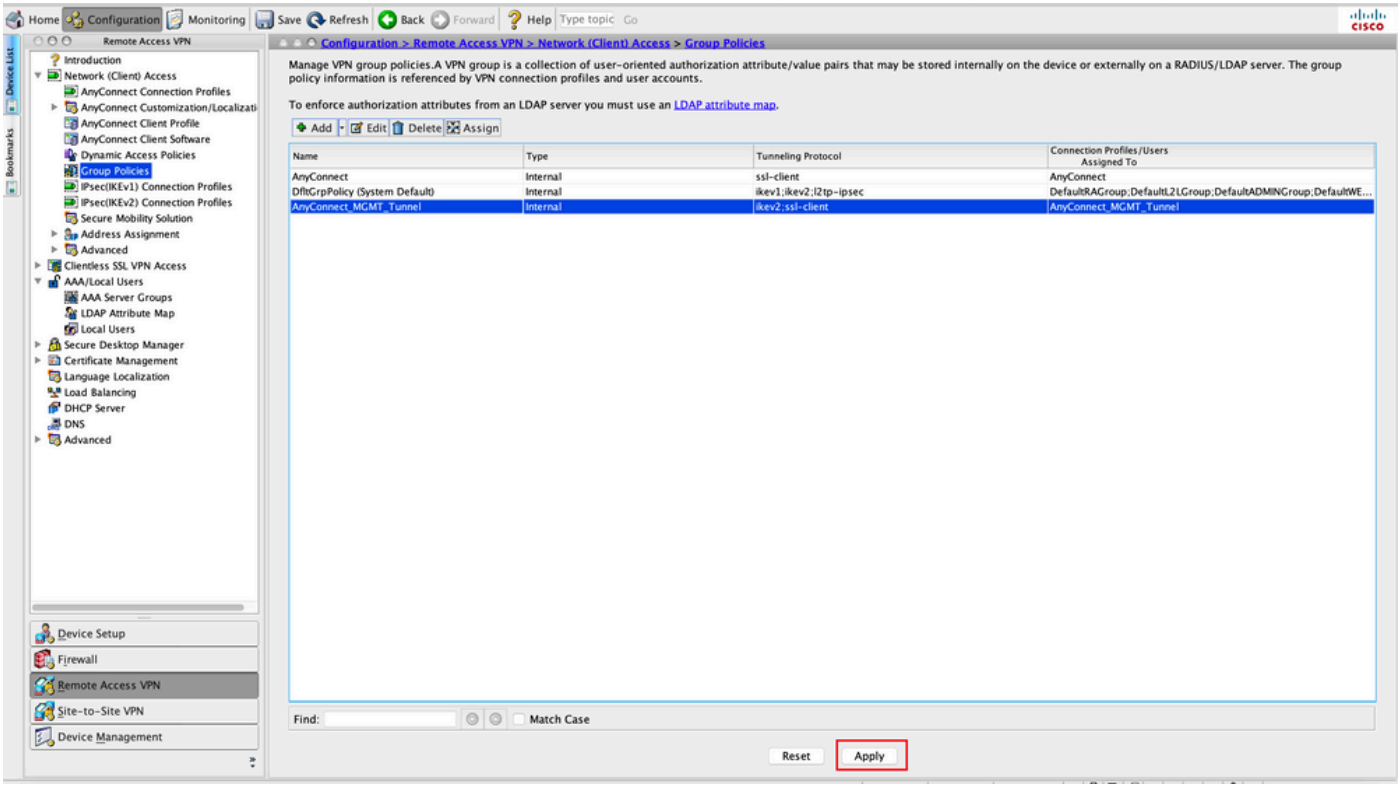
Observação: se um endereço de cliente não for enviado para ambos os protocolos IP (IPv4 e IPv6), o **Client Bypass Protocol** configuração deve ser enabled para que o tráfego correspondente não seja interrompido pelo túnel de gerenciamento. Para configurar o,

consulte a Etapa 4.

Etapa 4. Navegue até Advanced > AnyConnect Client. Configurado Client Bypass Protocol para Enable. Clique em OK para Salvar, como mostrado na imagem.



Etapa 5. Como mostrado nesta imagem, clique em Apply para enviar a configuração para o ASA.

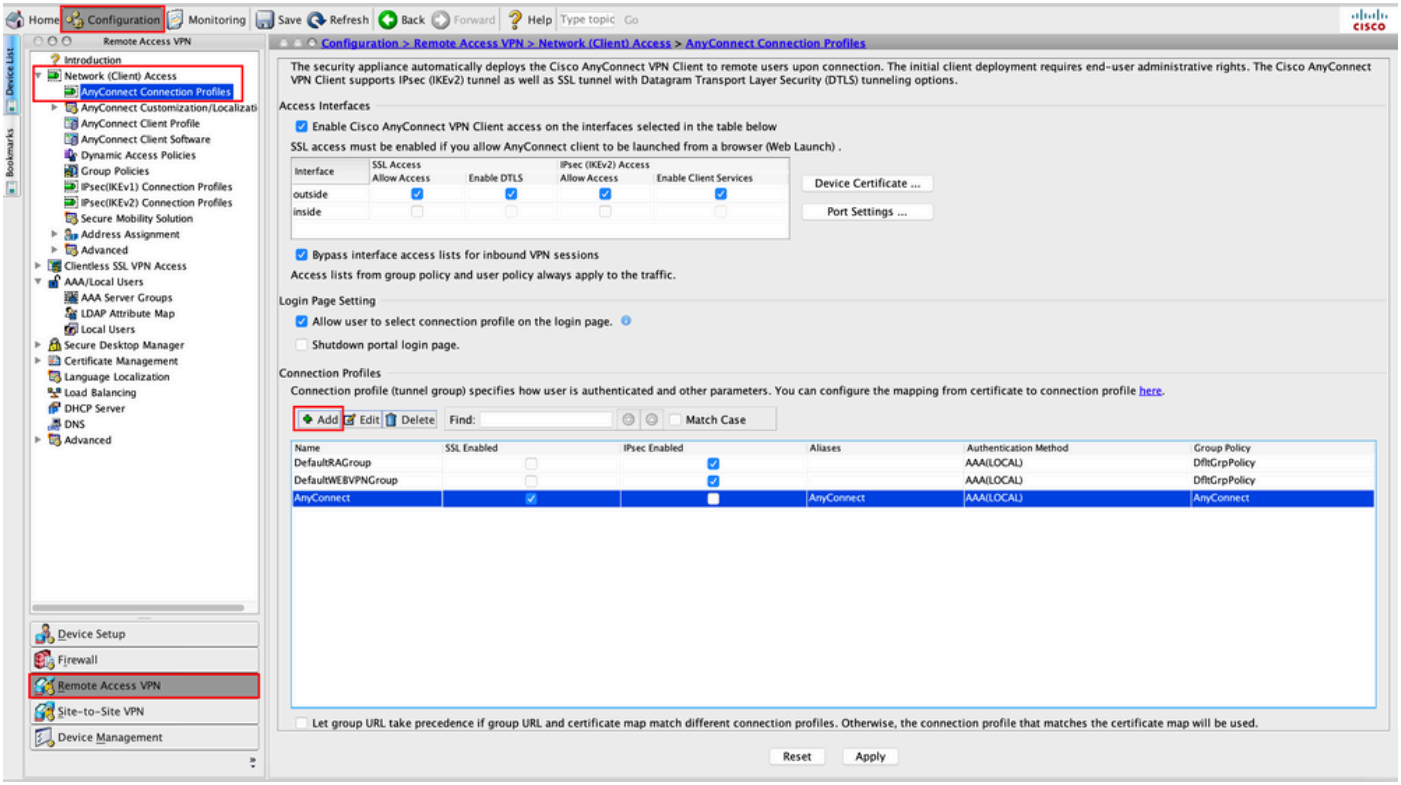


Configuração CLI para Diretiva de Grupo:

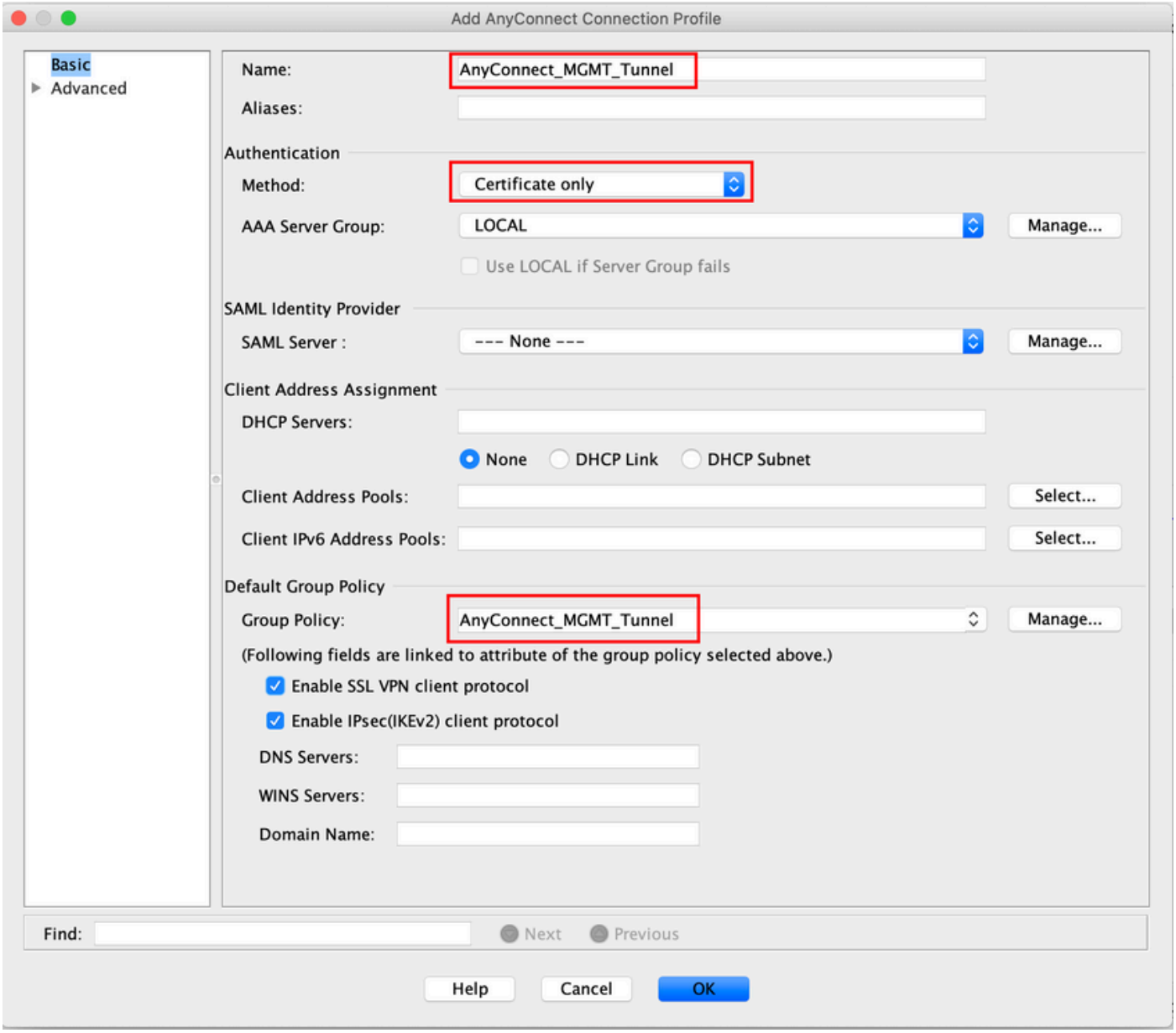
```
ip local pool VPN_Pool 192.168.10.1-192.168.10.100 mask 255.255.255.0
! access-list VPN-Split standard permit 172.16.0.0 255.255.0.0
! group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool
```

Etapa 6. Crie o perfil de conexão do AnyConnect. Navegue até Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. Clique em Add.

> **Nota:** É aconselhável criar um novo Perfil de conexão do AnyConnect que é usado somente para o túnel de gerenciamento do AnyConnect.



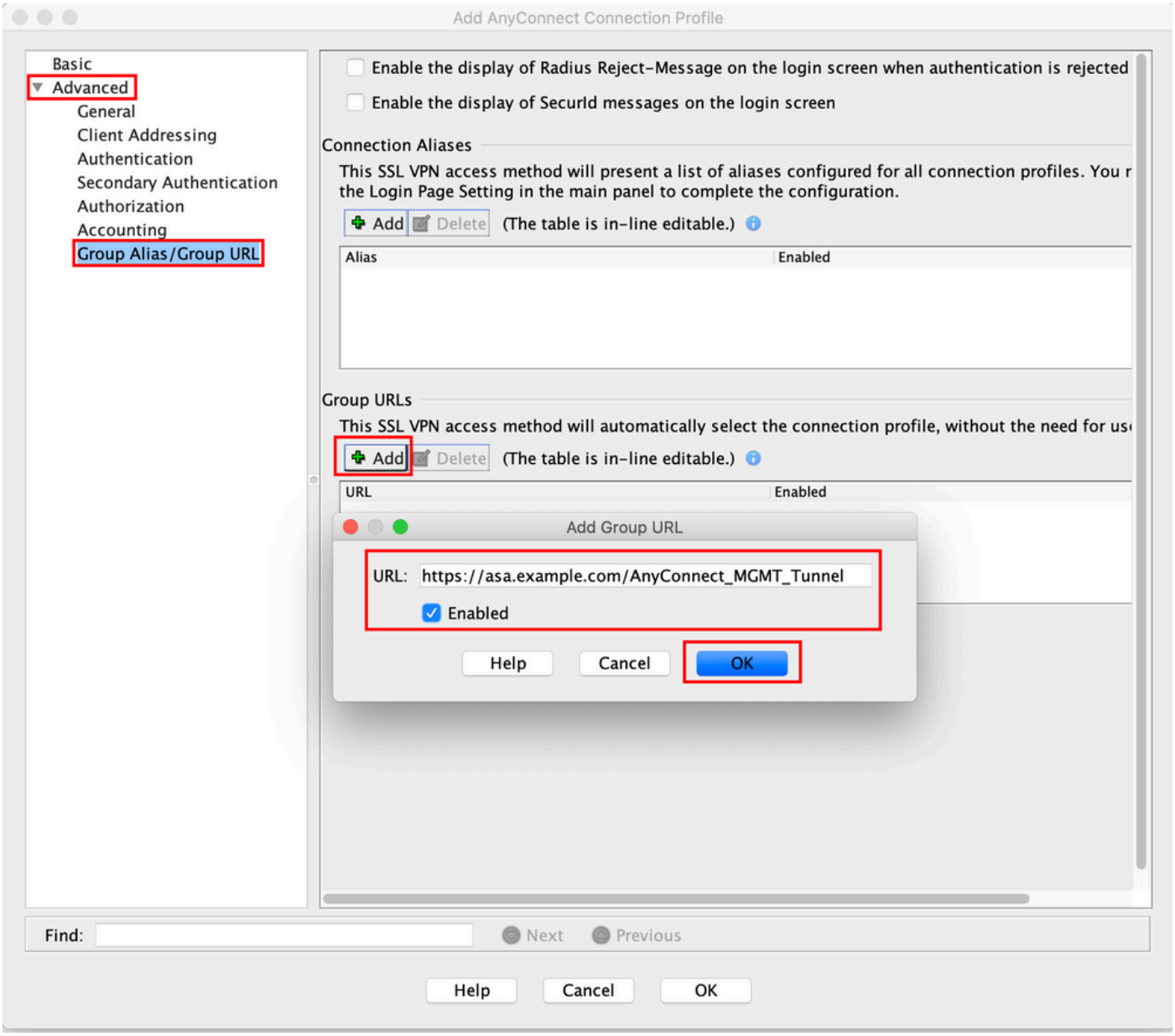
Passo 7. Fornecer uma Name para o Perfil de Conexão e defina Authentication Method como Certificate only. Escolha o Group Policy como o criado na Etapa 1.



Observação: verifique se o certificado raiz da CA local está presente no ASA. Navegue até Configuration > Remote Access VPN > Certificate Management > CA Certificates para adicionar/exibir o certificado.

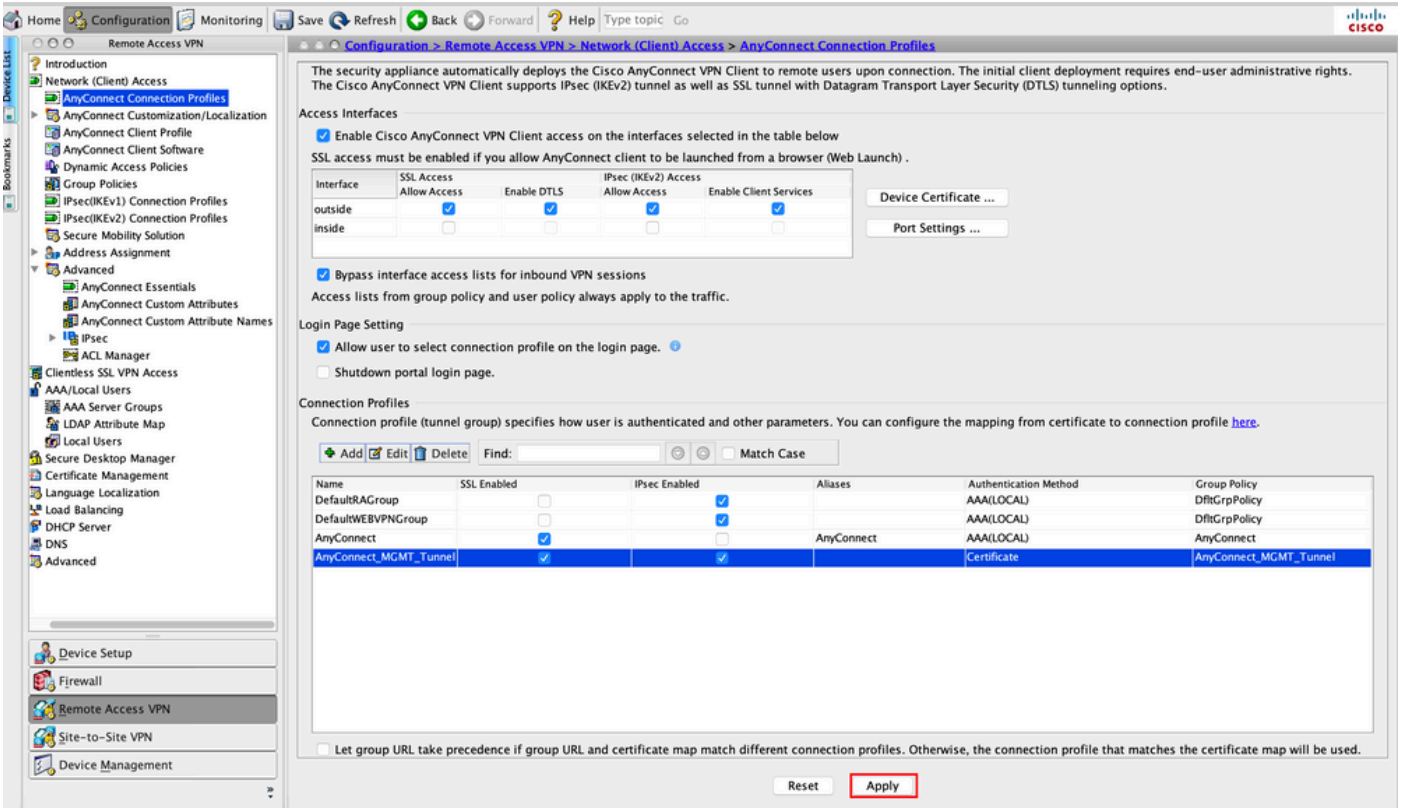
Observação: verifique se um certificado de Identidade emitido pela mesma CA Local existe no Repositório de Certificados do Computador (para Windows) e/ou no Conjunto de Chaves do Sistema (para macOS).

Etapa 8. Navegue até Advanced > Group Alias/Group URL. Clique em Add sob Group URLs e adicionar um URL. Garantir Enabled está marcado. Clique em OK para Salvar, como mostrado na imagem.



Se IKEv2 for usado, verifique IPsec (IKEv2) Access está ativado na interface usada para o AnyConnect.

Etapa 9. Clique em Apply para enviar a configuração para o ASA.

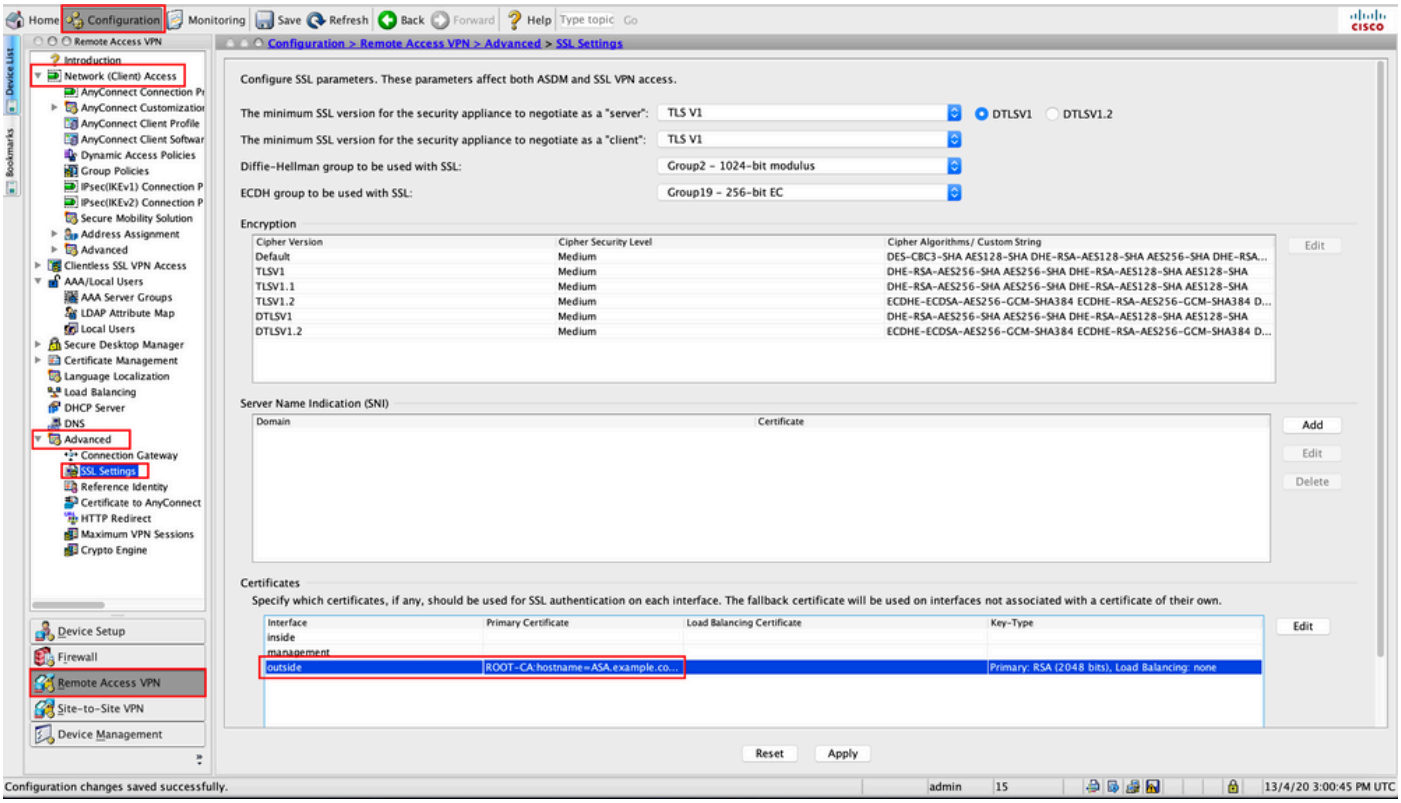


Configuração CLI para perfil de conexão (grupo de túneis):

```
tunnel-group AnyConnect_MGMT_Tunnel type remote-access
tunnel-group AnyConnect_MGMT_Tunnel general-attributes
 default-group-policy AnyConnect_MGMT_Tunnel
tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes
 authentication certificate
 group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable
```

Etapa 10. Verifique se um certificado confiável está instalado no ASA e associado à interface usada para conexões do AnyConnect. Navegue até Configuration > Remote Access VPN > Advanced > SSL Settings para adicionar/exibir essa configuração.

Observação: consulte Instalação do Certificado de Identidade no ASA.

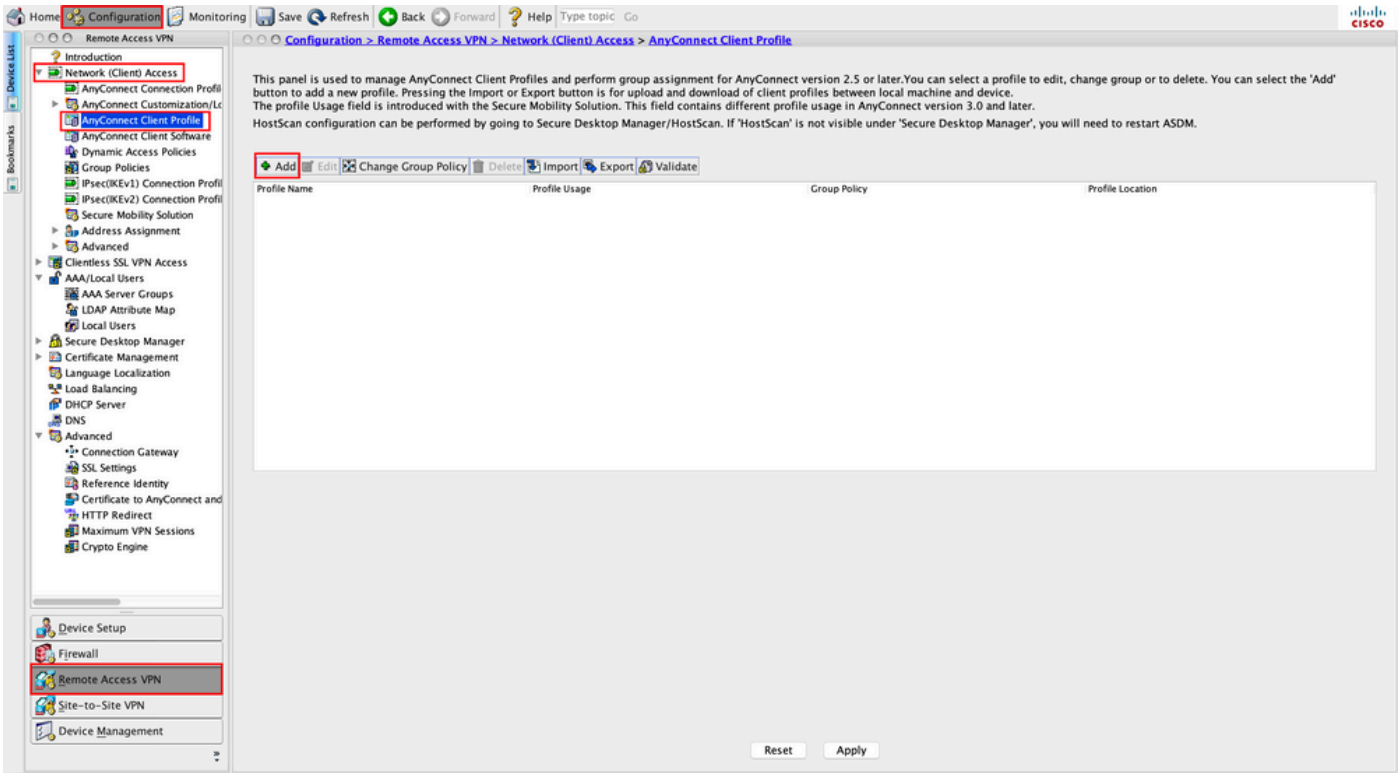


Configuração CLI para Ponto de Confiança SSL:

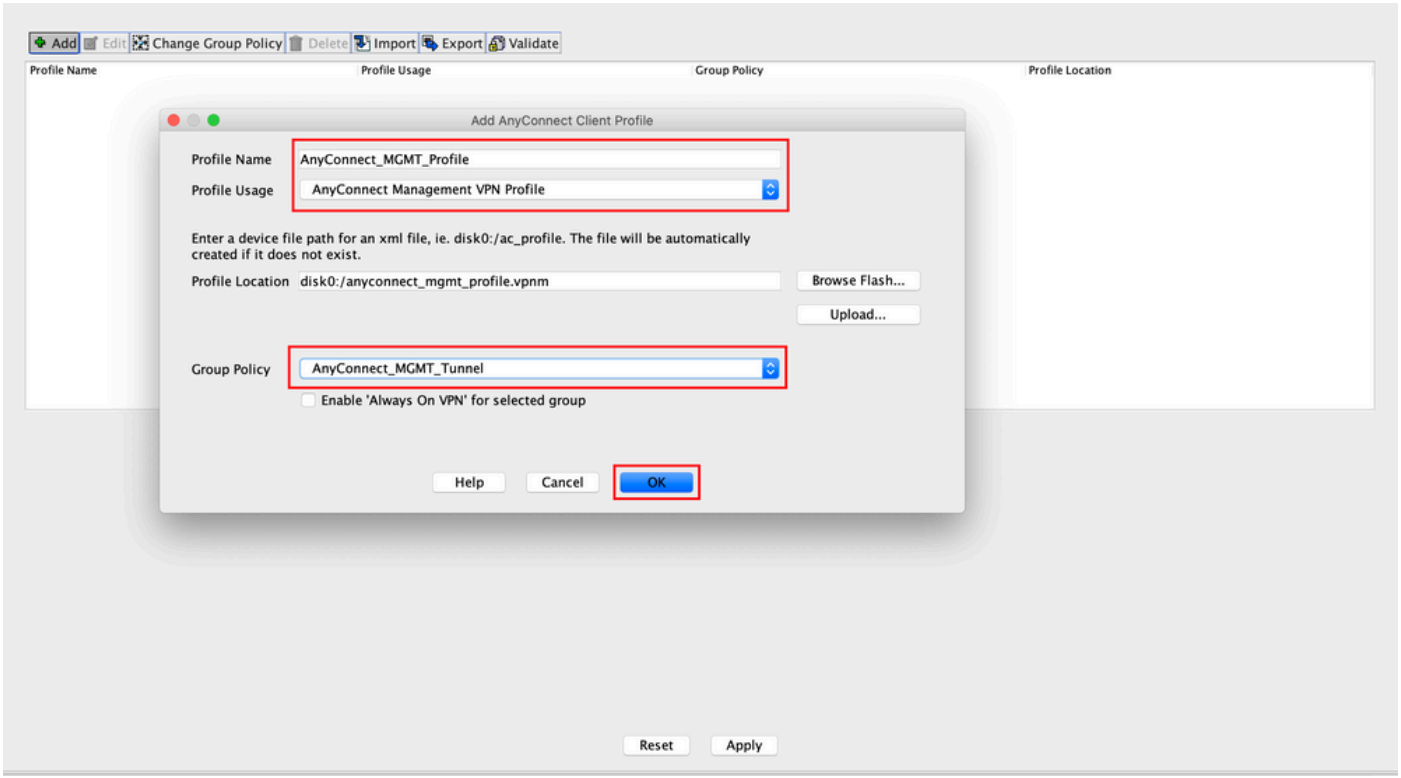
```
ssl trust-point ROOT-CA outside
```

Criação do perfil de VPN de gerenciamento do AnyConnect

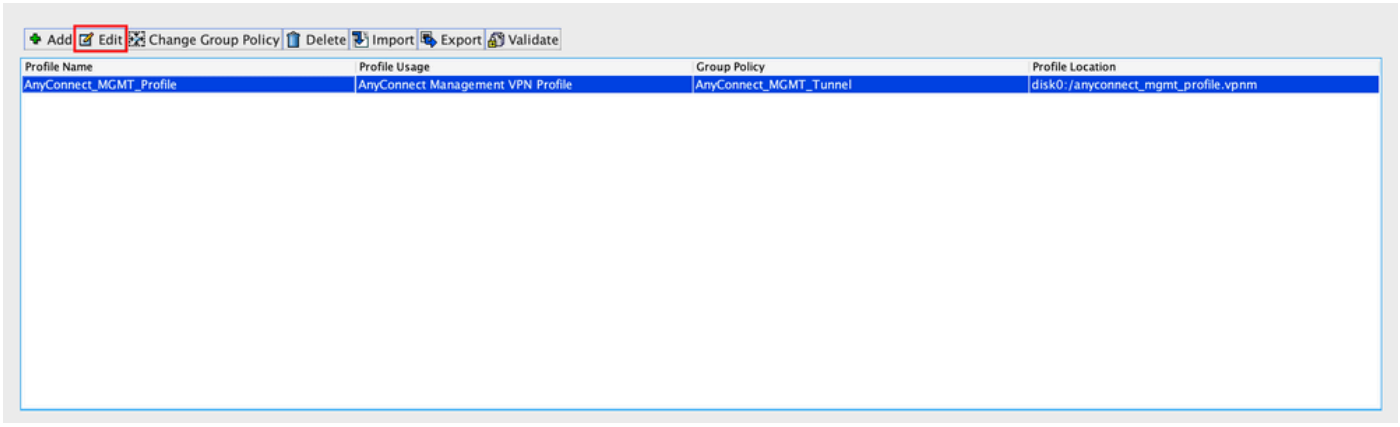
Etapa 1. Crie o perfil do AnyConnect Client. Navegue até Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. Clique em Add,conforme mostrado na imagem.



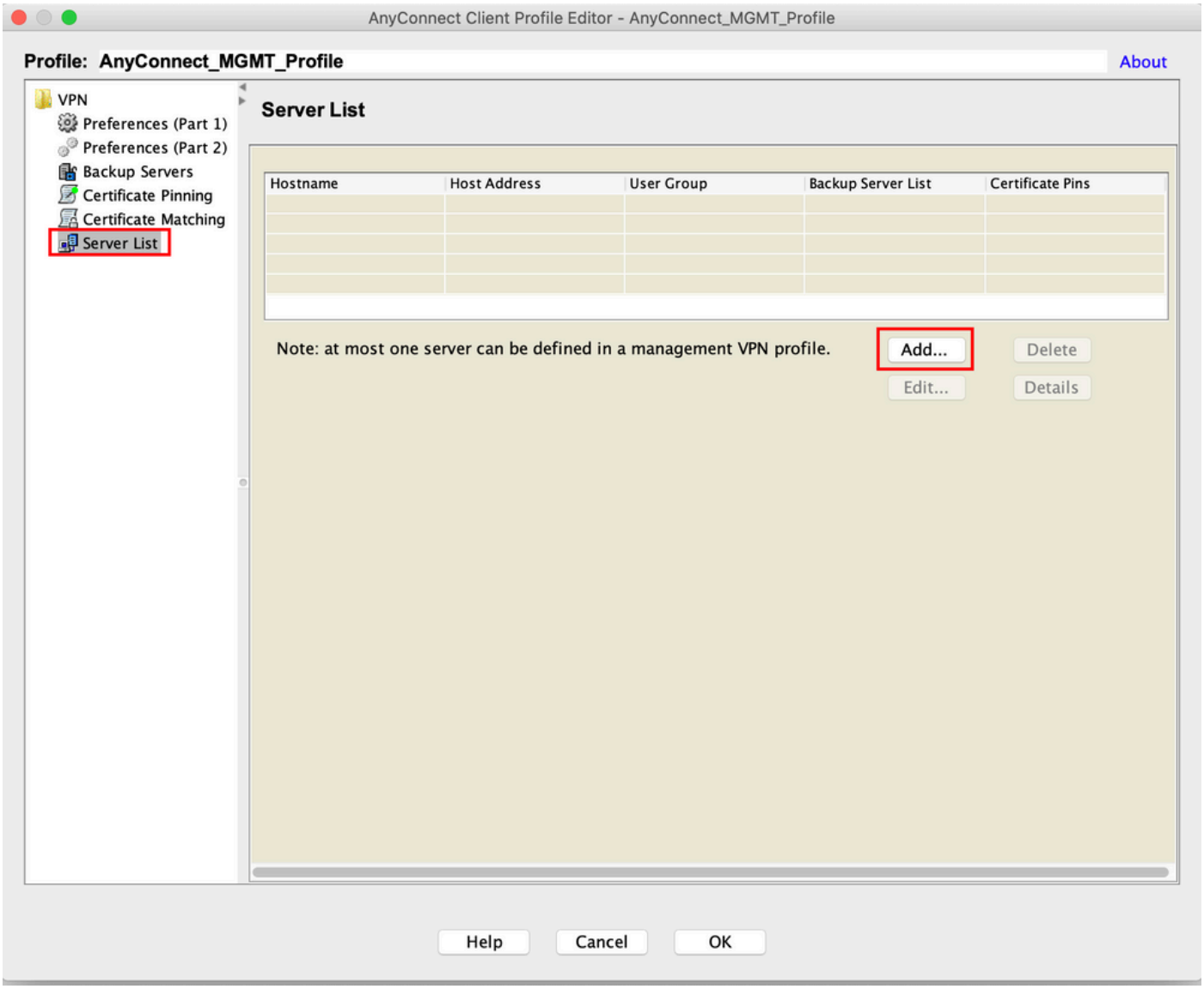
Etapa 2. Fornecer uma Profile Name. Escolha o Profile Usage como AnyConnect Management VPN profile. Escolha o Group Policy criado na Etapa 1. Clique em OK ,conforme mostrado na imagem.



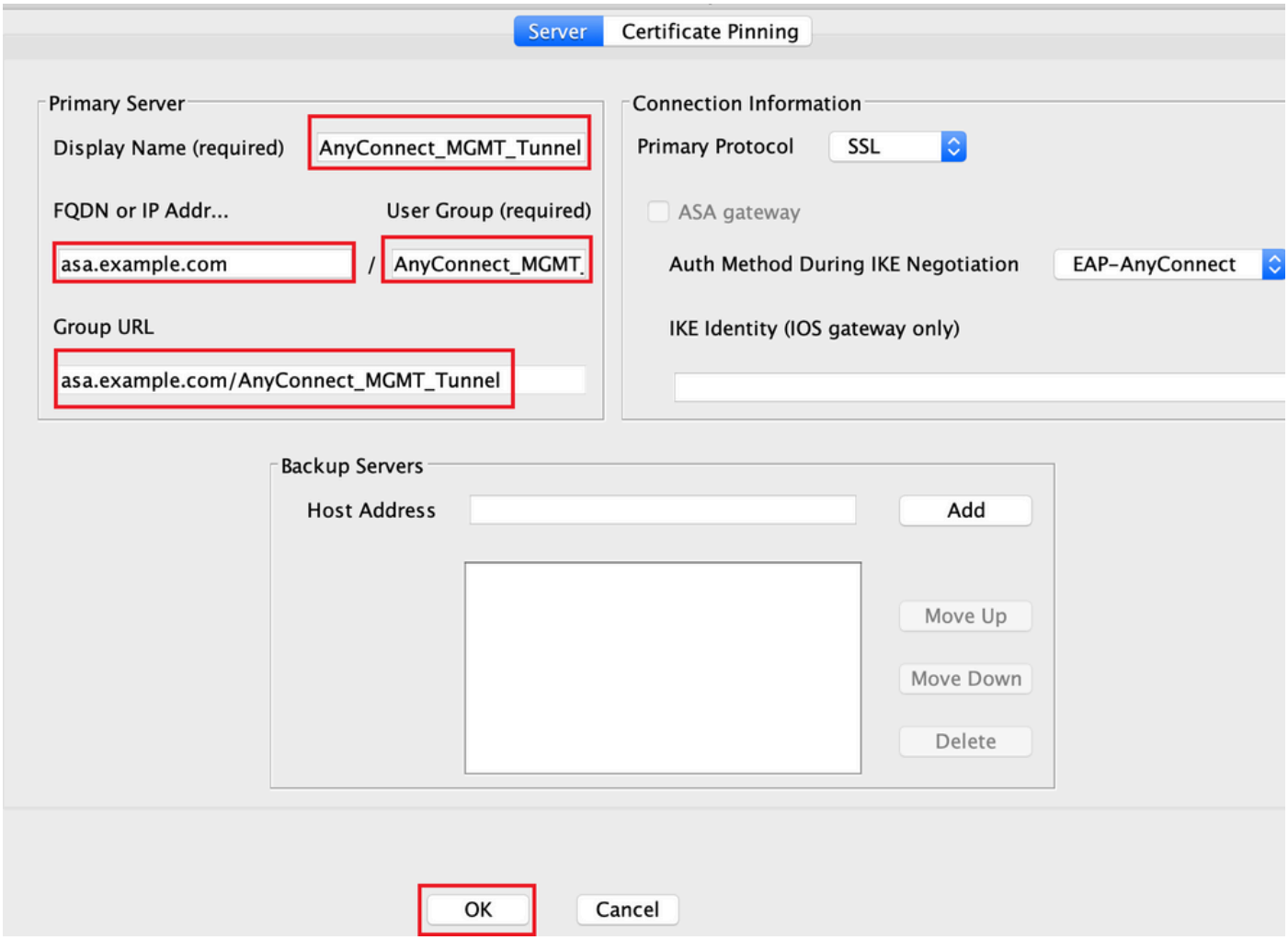
Etapa 3. Escolha o perfil criado e clique em Edit,conforme mostrado na imagem.



Etapa 4. Navegue até Server List. Clique em Add para adicionar uma nova Entrada da Lista de Servidores, como mostrado na imagem.



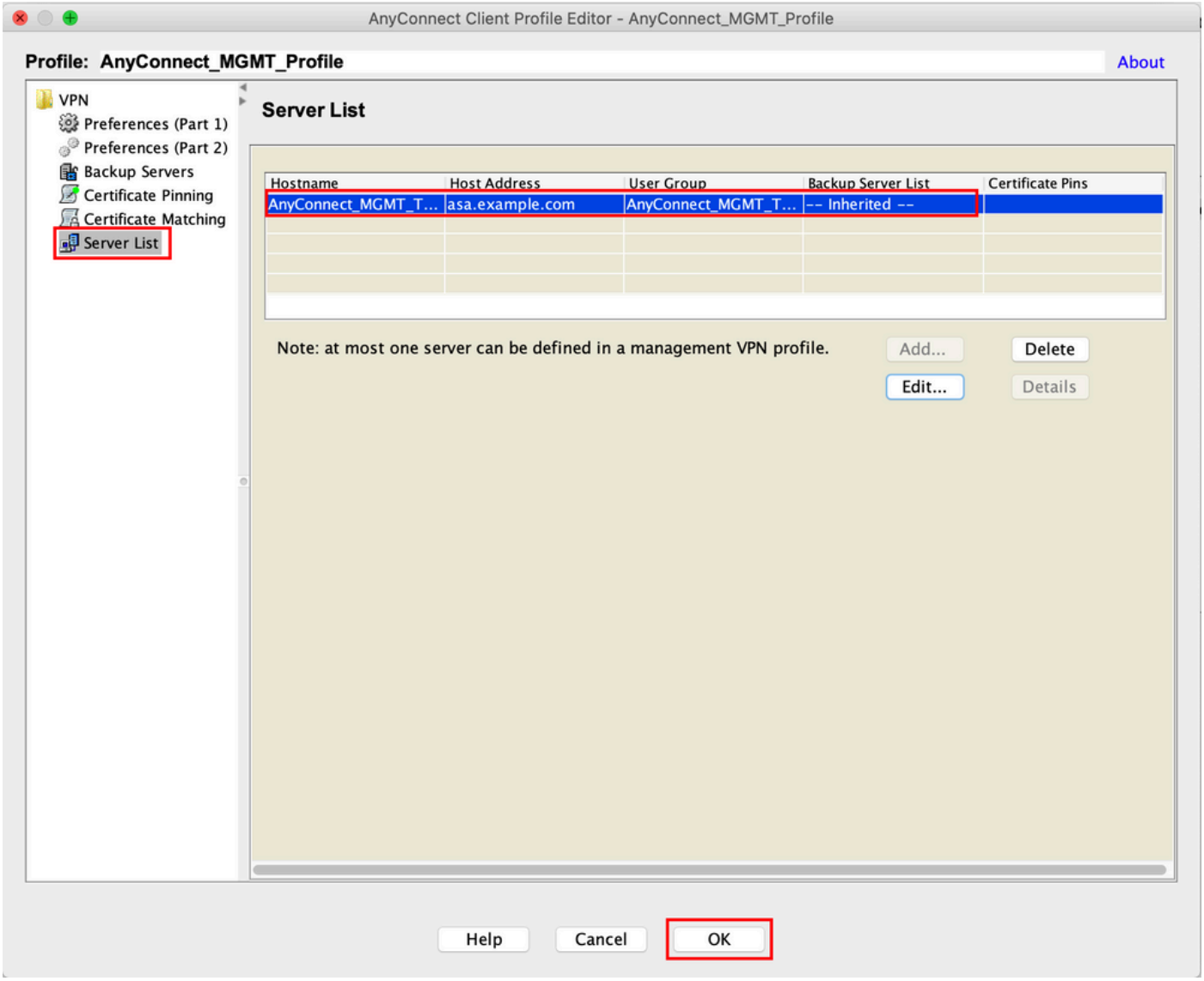
Etapa 5. Fornecer uma Display Name. Adicione o comando FQDN/IP address do ASA. Forneça o User Group como o nome do grupo do túnel. Group URL é preenchido automaticamente com o FQDN e User Group. Clique em OK.



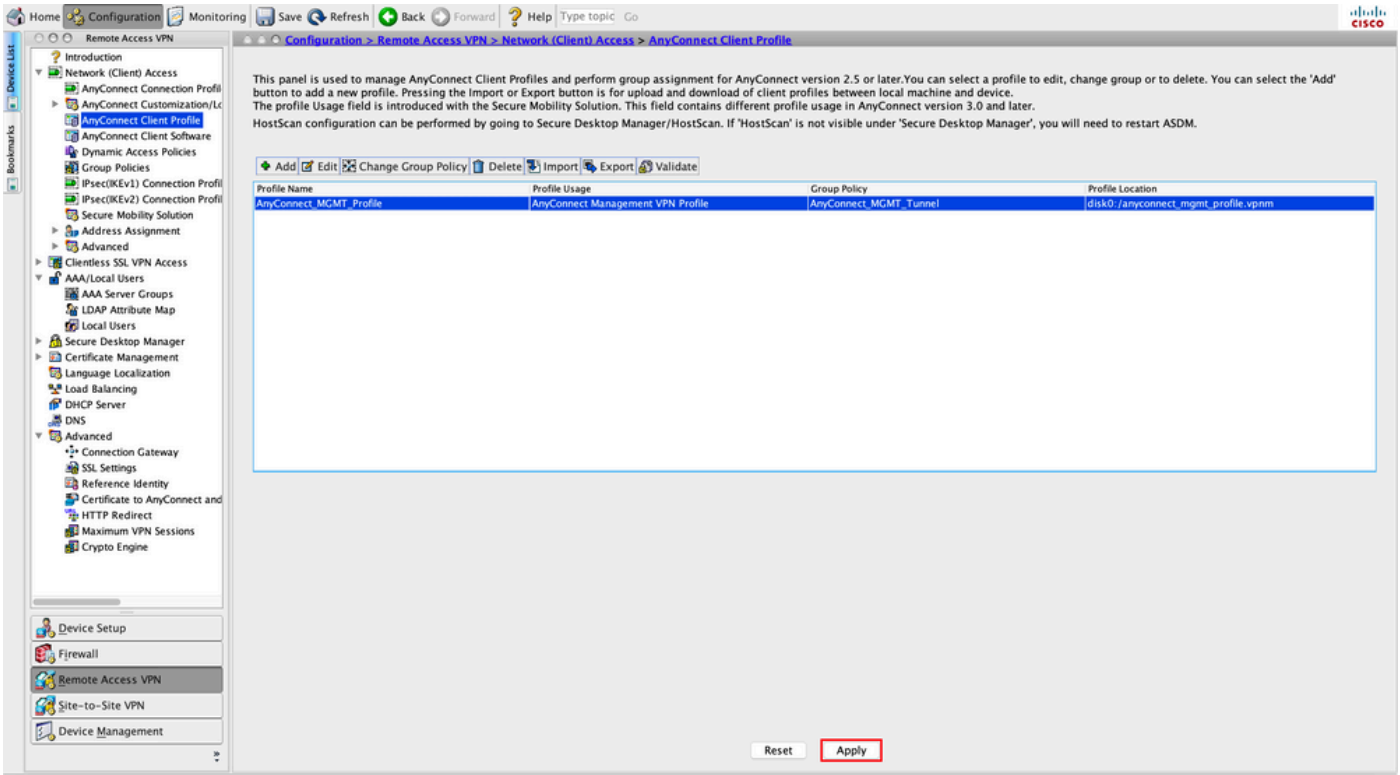
Observação: o FQDN/endereço IP + grupo de usuários deve ser o mesmo que o URL do grupo mencionado durante a configuração do Perfil de conexão do AnyConnect na Etapa 8.

Observação: o AnyConnect com IKEv2 como protocolo também pode ser usado para estabelecer a VPN de gerenciamento para o ASA. Garantir Primary Protocol está definido como IPsec na Etapa 5.

Etapa 6. Como mostrado na imagem, clique em OK para Salvar.



Passo 7. Clique em Apply tPara enviar a configuração para o ASA, como mostrado na imagem.



Configuração da CLI após a adição do Perfil de VPN de gerenciamento do AnyConnect.

```
webvpn
 enable outside
 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool
 webvpn
  anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

Perfil de VPN de gerenciamento do AnyConnect no computador cliente do AnyConnect:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>




        <ShowPreConnectMessage>false</ShowPreConnectMessage>




        <ProxySettings>IgnoreProxy</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>

--- Output Omitted ---
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>
```

```
</AnyConnectProfile>
```

Observação: se a TND (Trusted Network Detection, detecção de rede confiável) for usada no perfil de VPN do AnyConnect do usuário, é aconselhável corresponder as mesmas configurações no perfil de VPN de gerenciamento para uma experiência de usuário consistente. O túnel VPN de gerenciamento é acionado com base nas configurações TND aplicadas ao perfil de túnel VPN do usuário. Além disso, a ação TND Connect no perfil de VPN de gerenciamento (aplicada somente quando o túnel VPN de gerenciamento está ativo), sempre se aplica ao túnel VPN do usuário, para garantir que o túnel VPN de gerenciamento seja transparente para o usuário final.

Observação: em qualquer PC de usuário final, se o perfil de VPN de gerenciamento tiver as configurações de TND habilitadas e se o perfil de VPN do usuário estiver ausente, ele considerará as configurações de preferências padrão para o TND (ele está desabilitado nas preferências padrão na aplicação de cliente AC) em vez do perfil de VPN do usuário ausente. Essa incompatibilidade pode levar a um comportamento inesperado/indefinido.
Por padrão, as configurações de TND são desabilitadas nas preferências padrão.
Para superar as configurações codificadas de preferências padrão no aplicativo AnyConnect Client, o PC do usuário final deve ter dois perfis de VPN, um perfil de VPN do usuário e um perfil de VPN de gerenciamento de CA, e ambos devem ter as mesmas configurações de TND.
A lógica por trás da conexão e desconexão do túnel VPN de gerenciamento é que para estabelecer um túnel VPN de gerenciamento, o agente AC usa as configurações TND do perfil VPN do usuário e para desconexão do túnel VPN de gerenciamento, ele verifica as configurações TND do perfil VPN de gerenciamento.

Métodos de implantação para o perfil de VPN de gerenciamento do AnyConnect

- Uma conexão VPN de usuário bem-sucedida é concluída com o Perfil de conexão ASA para fazer o download do Perfil de VPN de gerenciamento do AnyConnect do Gateway VPN.

  Nota: se o protocolo usado para o túnel VPN de gerenciamento for IKEv2, a primeira conexão será necessária através de SSL (para baixar o perfil de VPN de gerenciamento do AnyConnect do ASA).

- O Perfil de VPN de gerenciamento do AnyConnect pode ser carregado manualmente para as máquinas cliente por meio de um envio de GPO ou por instalação manual (Verifique se o nome do perfil é `VpnMgmtTunProfile.xml`).

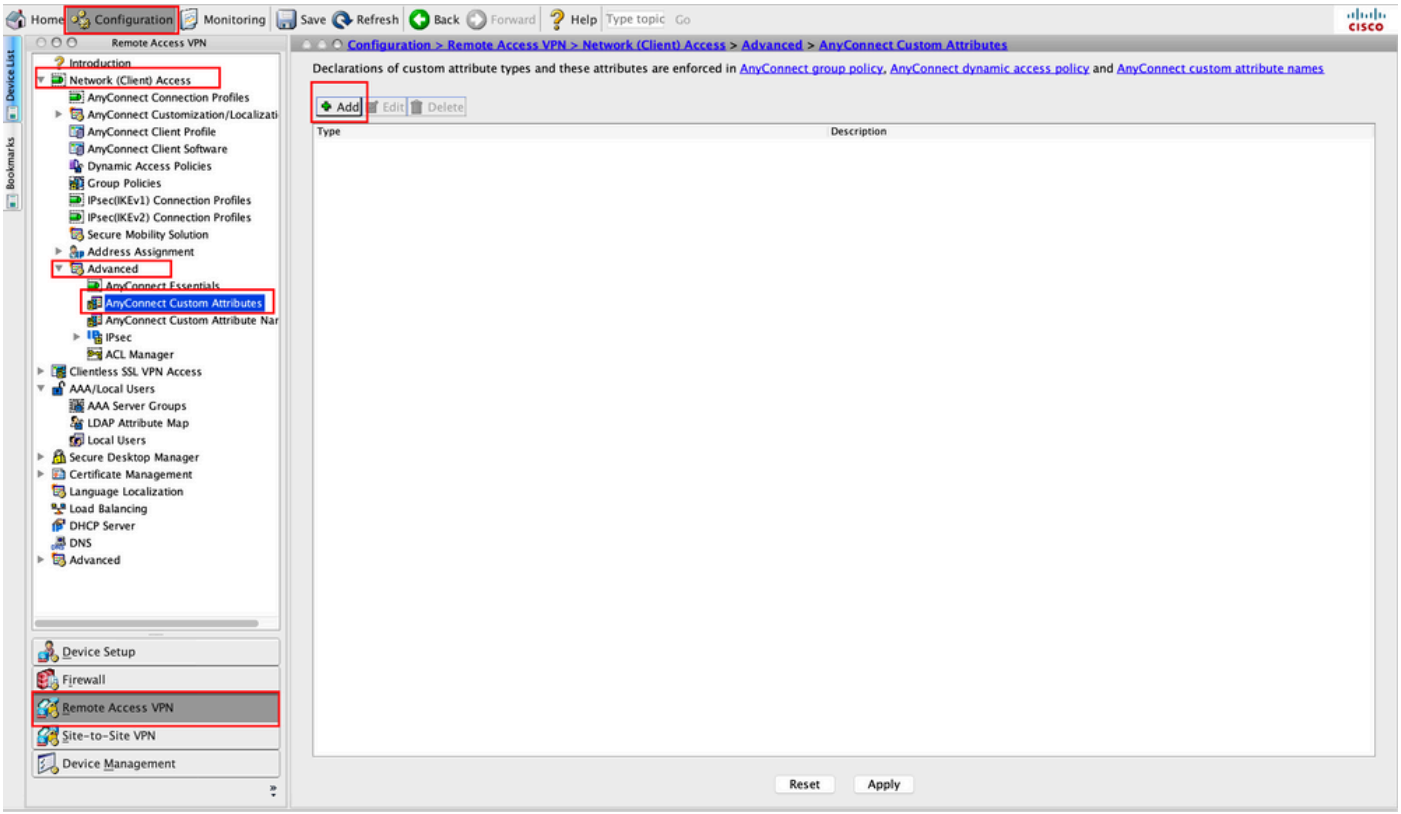
  Local da pasta onde o perfil precisa ser adicionado:
  Windows: **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**
  MacOS: /opt/cisco/anyconnect/profile/mgmttun/

(Opcional) Configure um Atributo Personalizado para Suportar a Configuração Tunnel-All

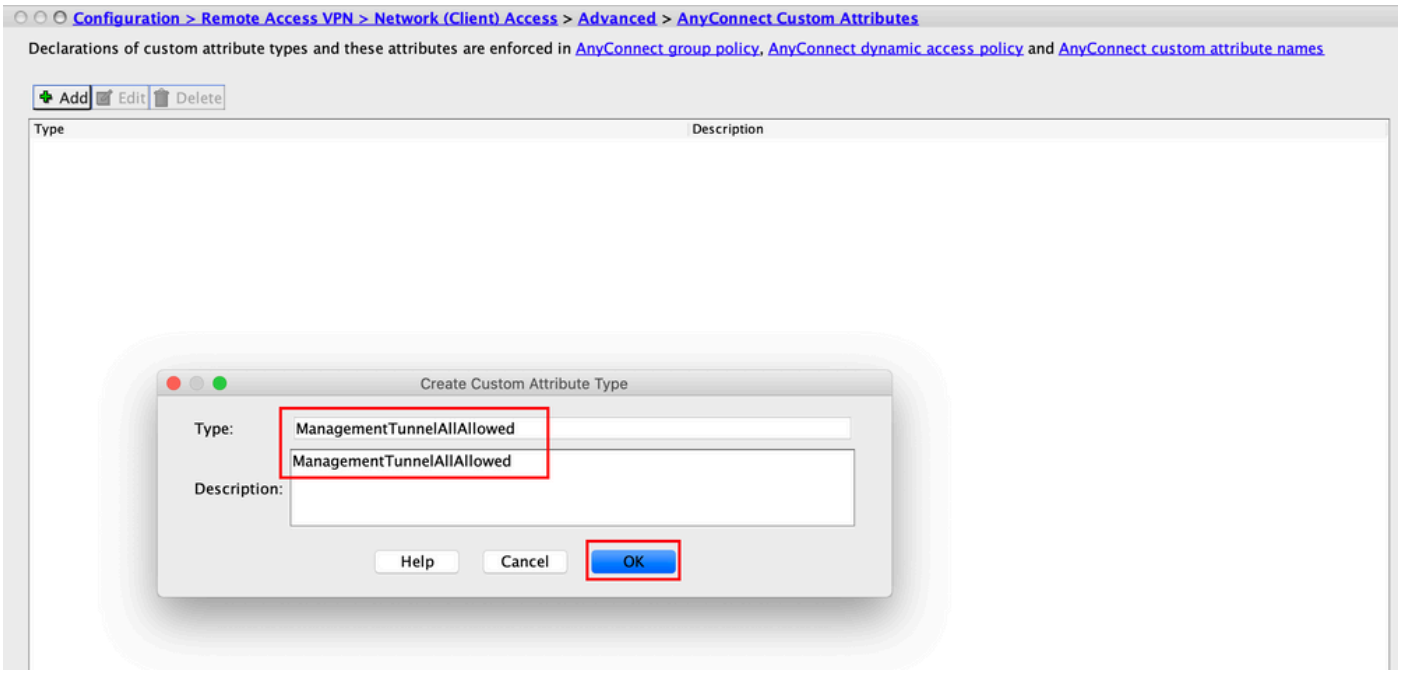
O túnel VPN de gerenciamento requer uma divisão que inclui configuração de tunelamento, por padrão, para evitar um impacto na comunicação de rede iniciada pelo usuário. Isso pode ser substituído quando você configura o atributo personalizado na política de grupo usada pela

conexão de túnel de gerenciamento.

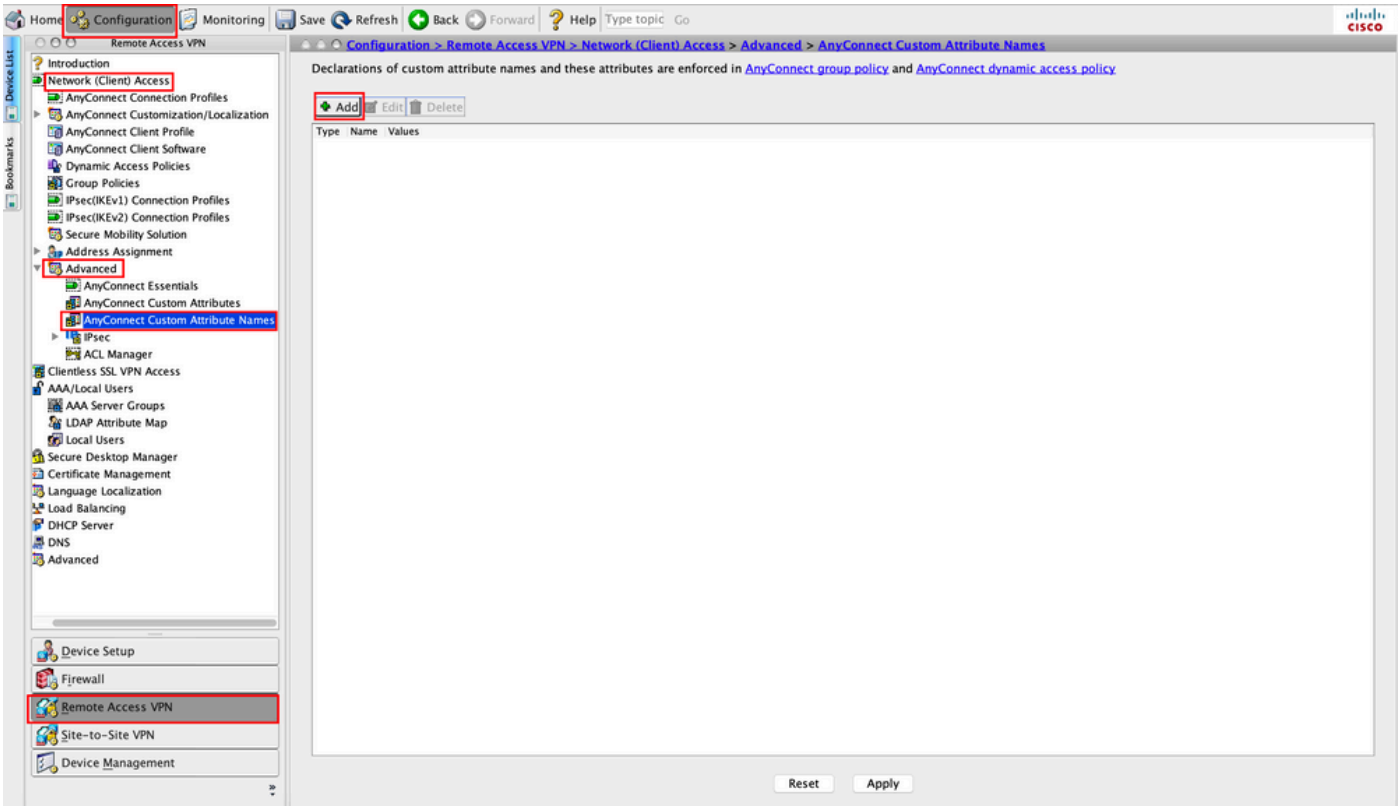
Etapa 1. Navegue atéConfiguration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Clique em Add,conforme mostrado na imagem.



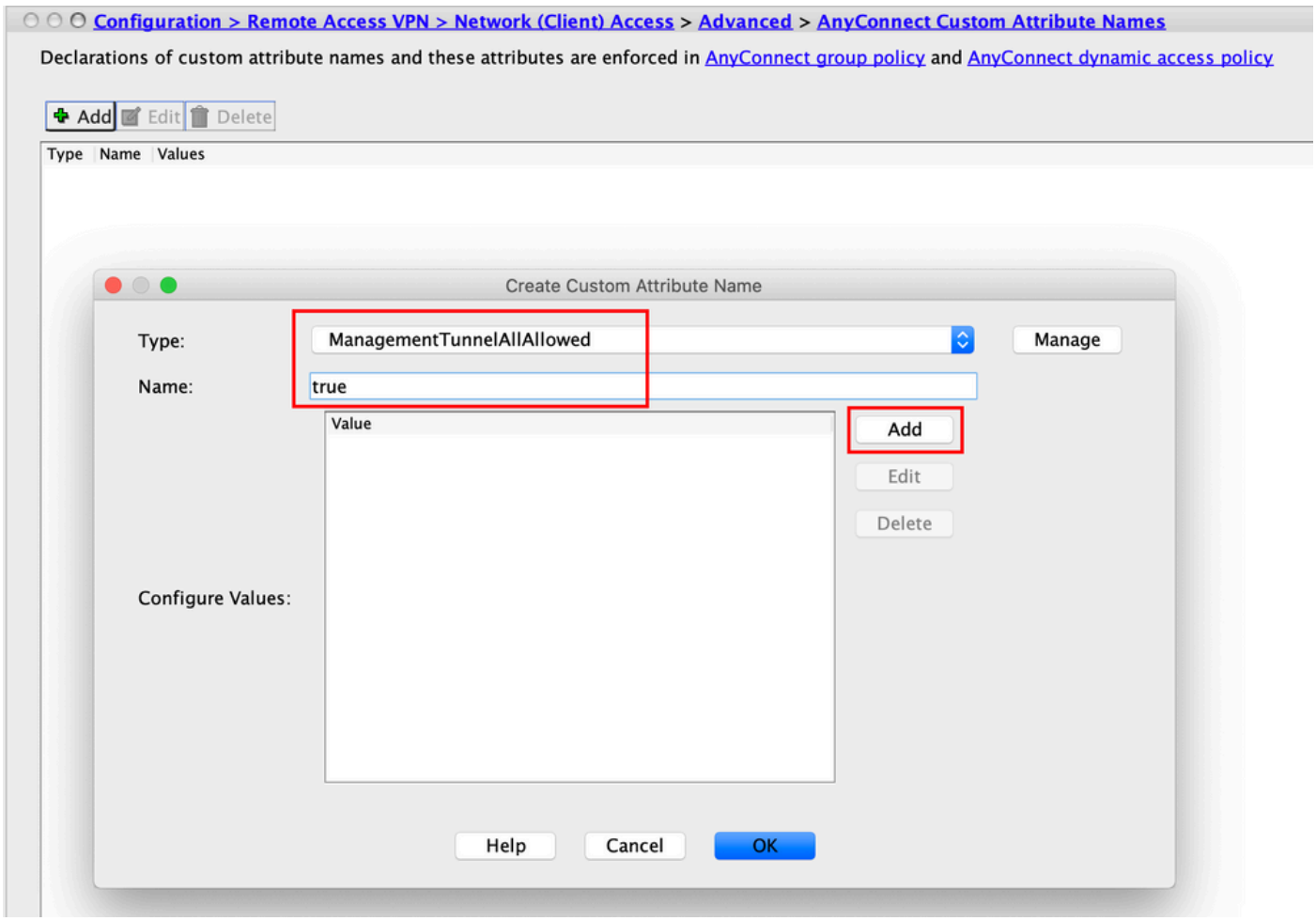
Etapa 2. Defina o Tipo de atributo personalizado como ManagementTunnelAllAllowed e fornecer uma Description. Clique em OK,conforme mostrado na imagem.



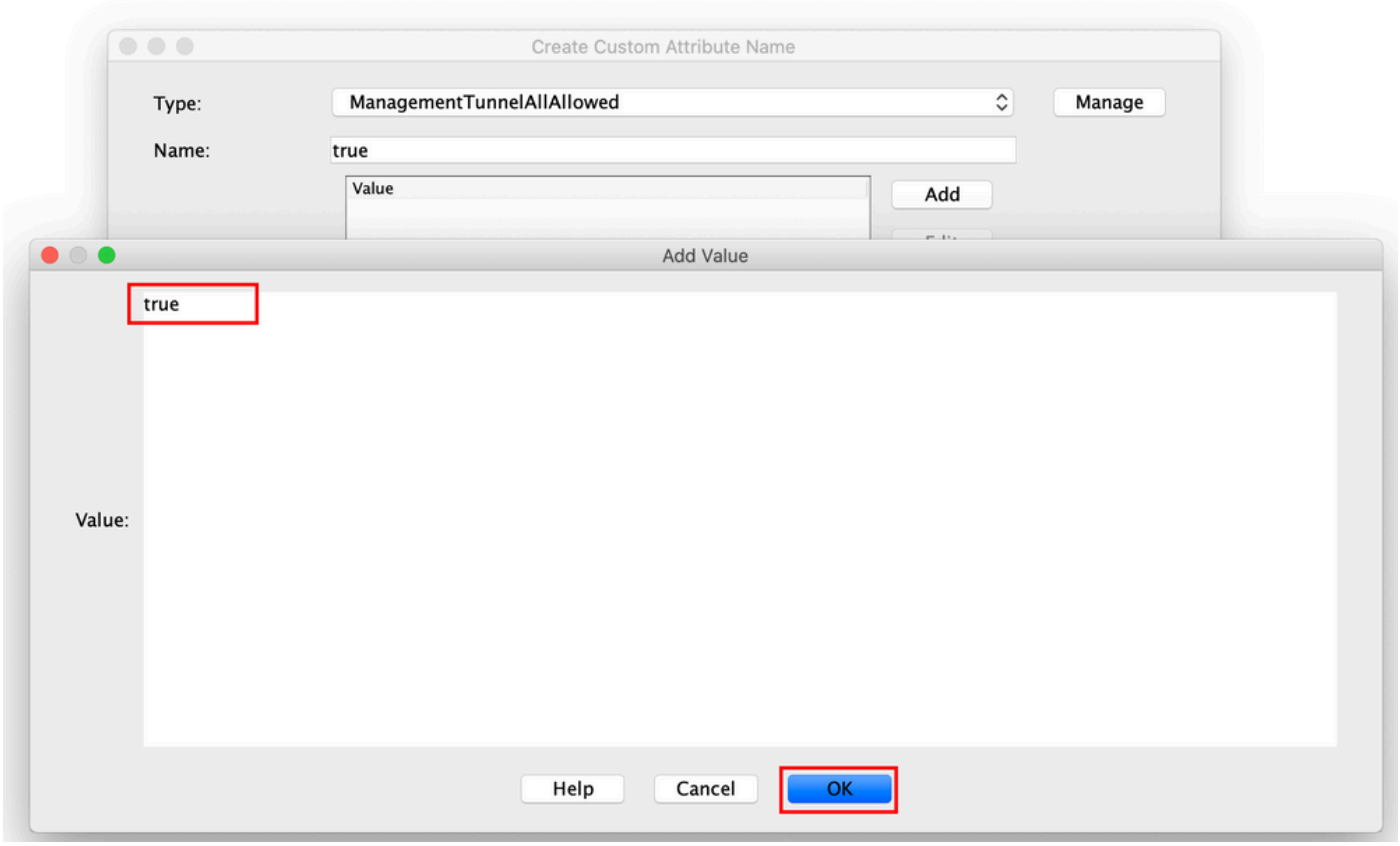
Etapa 3. Navegue até **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names.** Clique em Add,conforme mostrado na imagem.



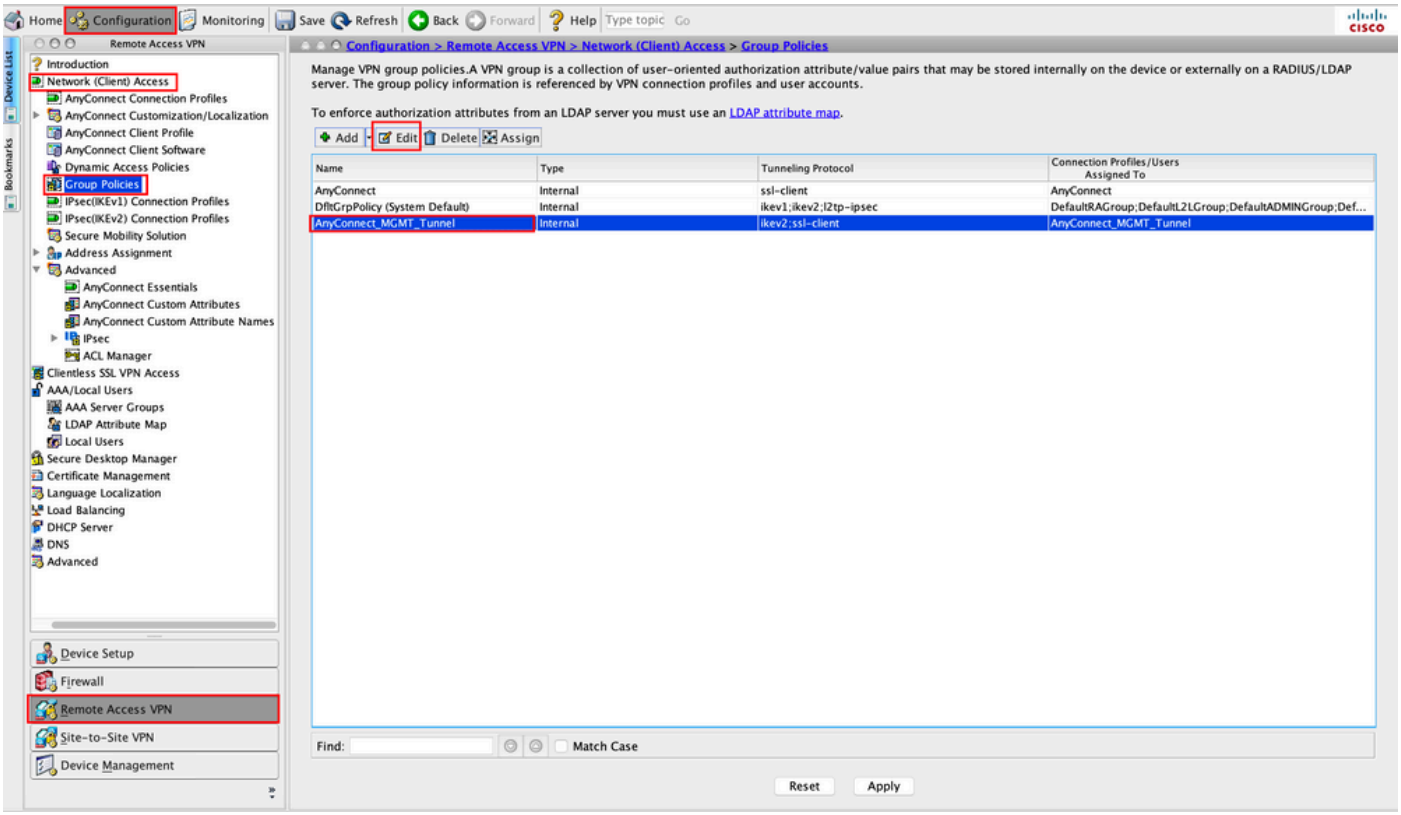
Etapa 4. Escolha o Tipo como **ManagementTunnelAllAllowed** . Defina o nome como true. Clique em Addpara fornecer um valor de atributo personalizado, como mostrado na imagem.



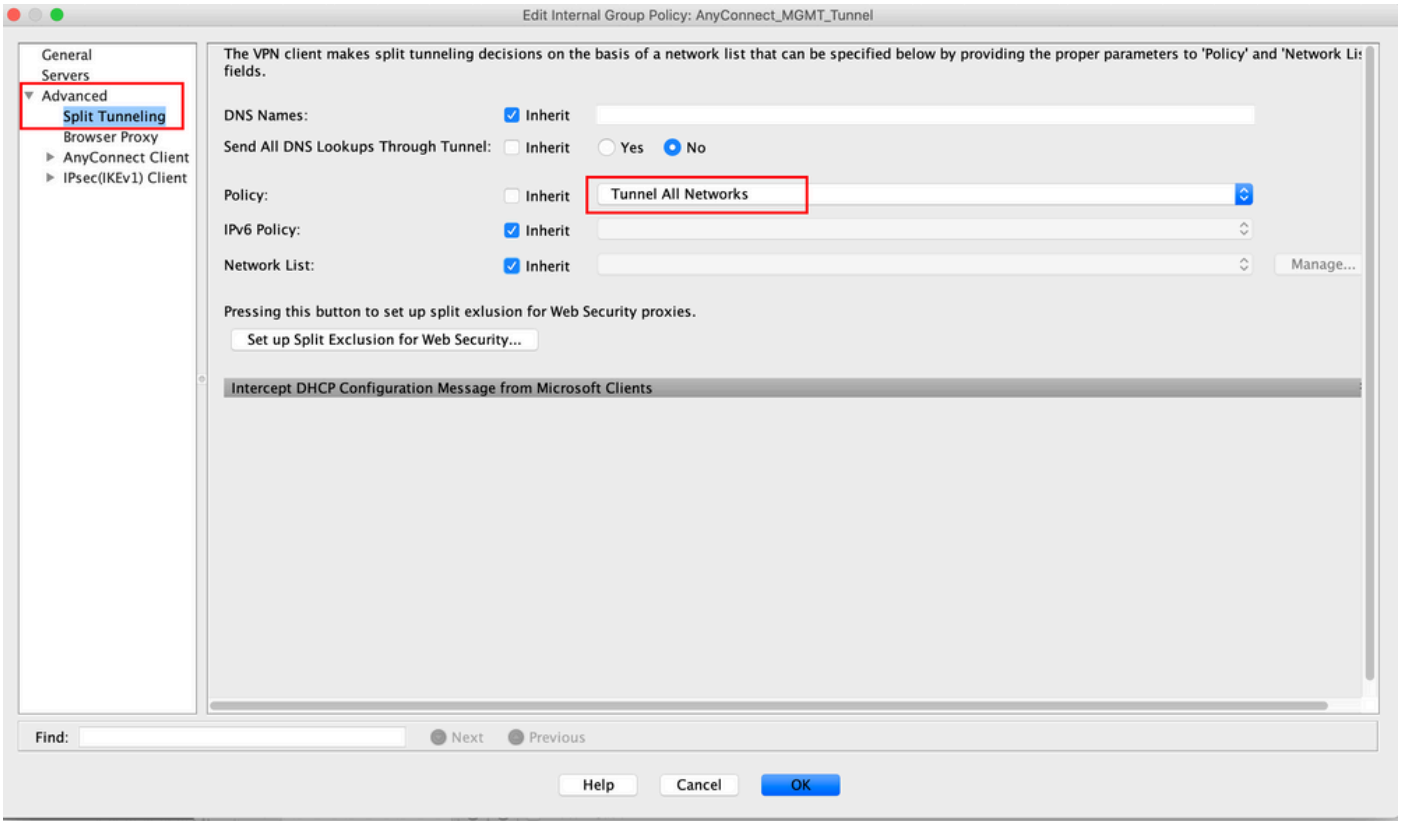
Etapa 5. Definir o valor como true. Clique em OK,conforme mostrado na imagem.



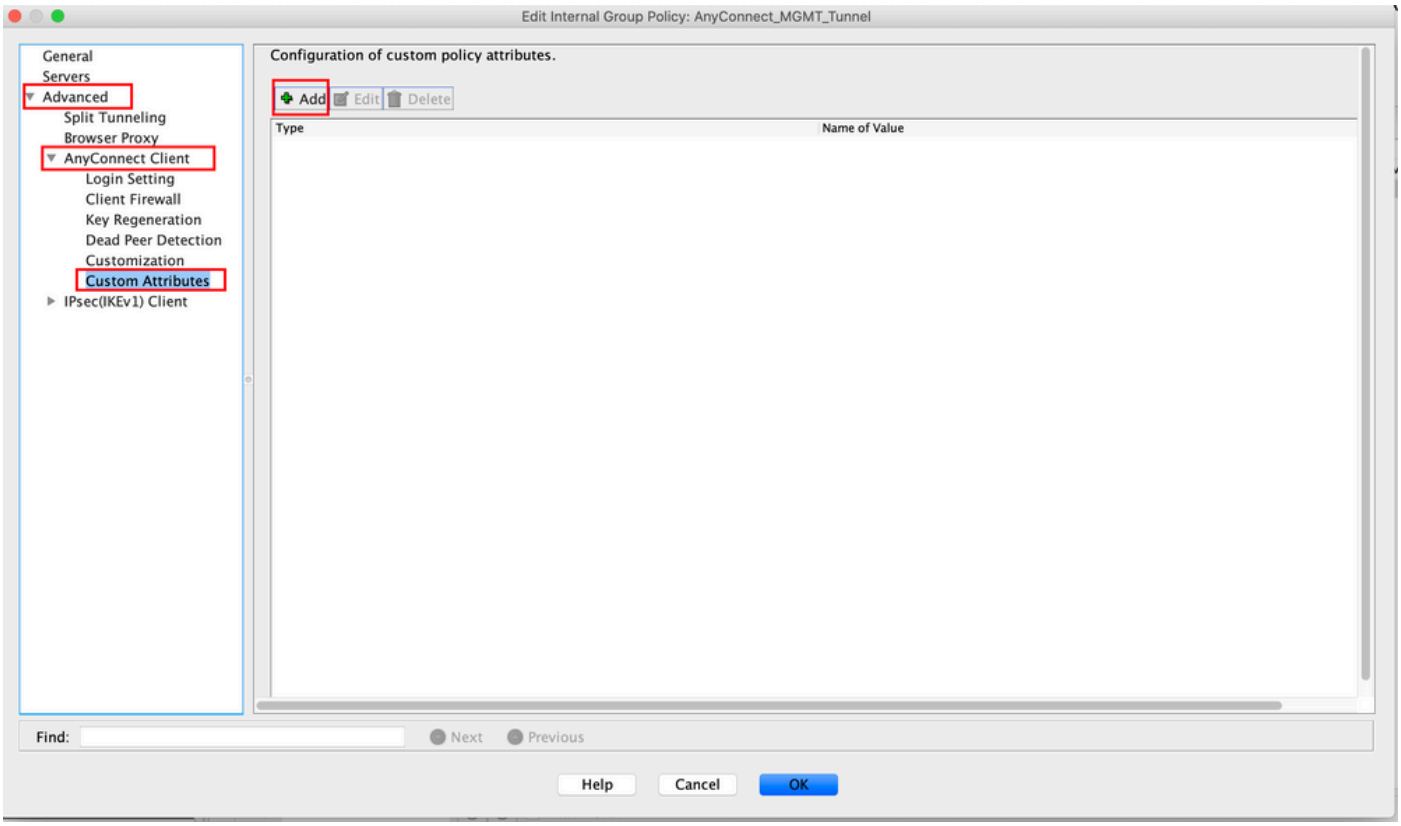
Etapa 6. Navegue até Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Escolha a Diretiva de Grupo. Clique em Edit ,conforme mostrado na imagem.



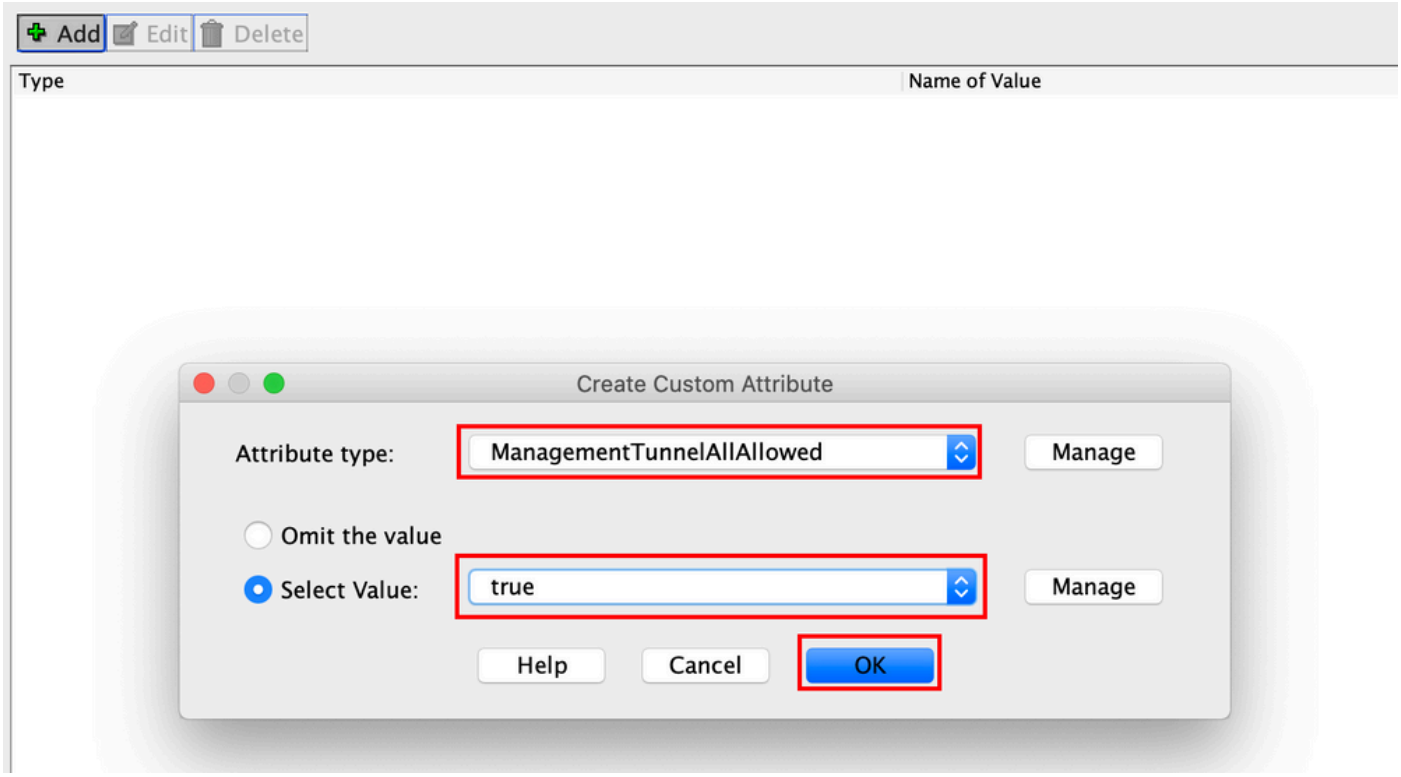
Passo 7. Como mostrado nesta imagem, navegue até Advanced > Split Tunneling. Configure a política como Tunnel All Networks.



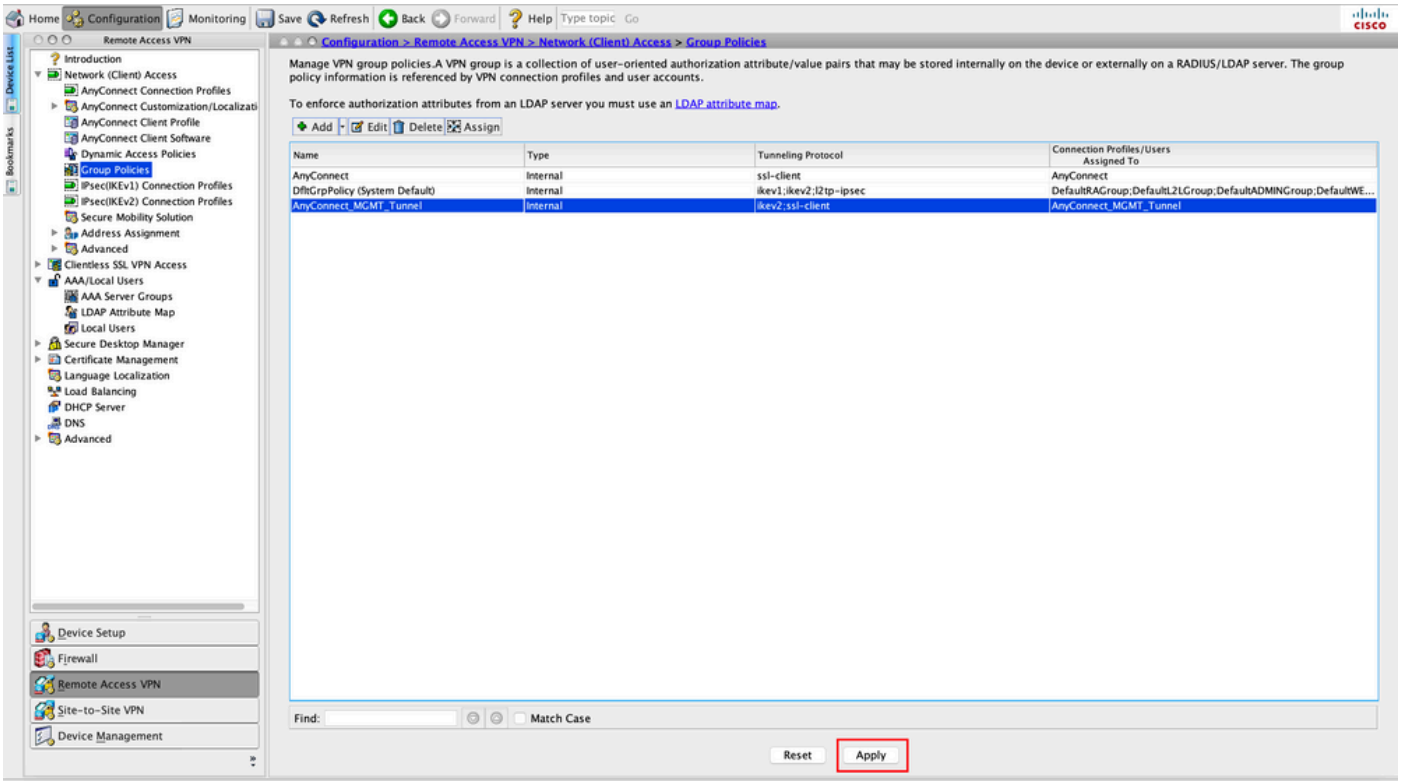
Etapa 8. Navegue até Advanced > Anyconnect Client > Custom Attributes. Clique em Add,conforme mostrado na imagem.



Etapa 9. Escolha o tipo de Atributo como ManagementTunnelAllAllowed e escolha o Valor como true. Clique em OK,conforme mostrado na imagem.



Etapa 10. Clique em Apply para enviar a configuração para o ASA, como mostrado na imagem.



Configuração da CLI após o comando ManagementTunnelAllAllowed Atributo Personalizado é adicionado:

```
webvpn
 enable outside
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
 hsts
  enable
```

```
  max-age 31536000
  include-sub-domains
  no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
anyconnect-custom-data ManagementTunnelAllAllowed true true
!
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelall
 client-bypass-protocol enable
 address-pools value VPN_Pool
 anyconnect-custom ManagementTunnelAllAllowed value true
 webvpn
  anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

Verificar

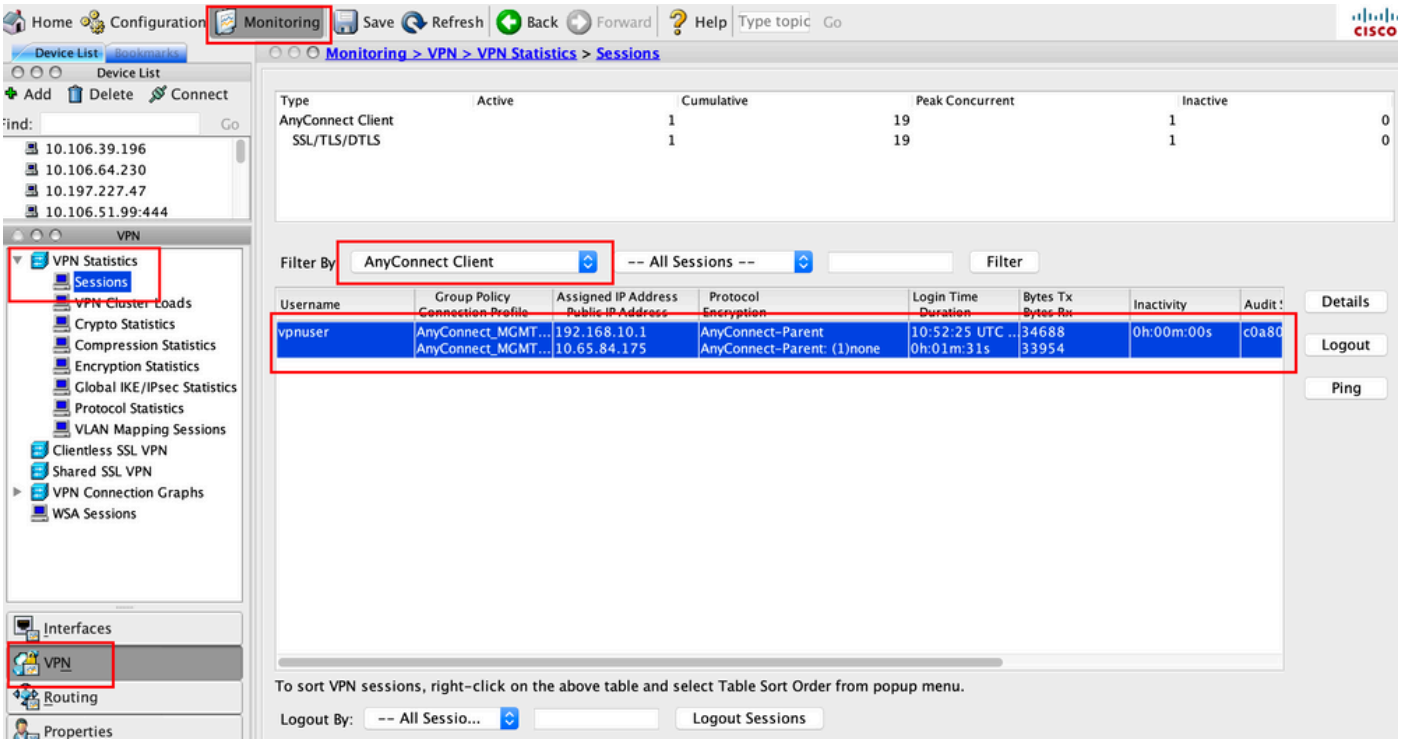
Verifique a conexão do túnel VPN de gerenciamento no ASA CLI com o comando `show vpn-sessiondb detail anyconnect` comando.

```
ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : vpnuser                Index        : 10
Assigned IP  : 192.168.10.1           Public IP    : 10.65.84.175
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-
256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 17238                  Bytes Rx     : 1988
Pkts Tx      : 12                     Pkts Rx      : 13
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel
Login Time   : 01:23:55 UTC Tue Apr 14 2020
Duration     : 0h:11m:36s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

--- Output Omitted ---
DTLS-Tunnel:
  Tunnel ID    : 10.3
  Assigned IP  : 192.168.10.1           Public IP    : 10.65.84.175
  Encryption   : AES-GCM-256            Hashing      : SHA384
```

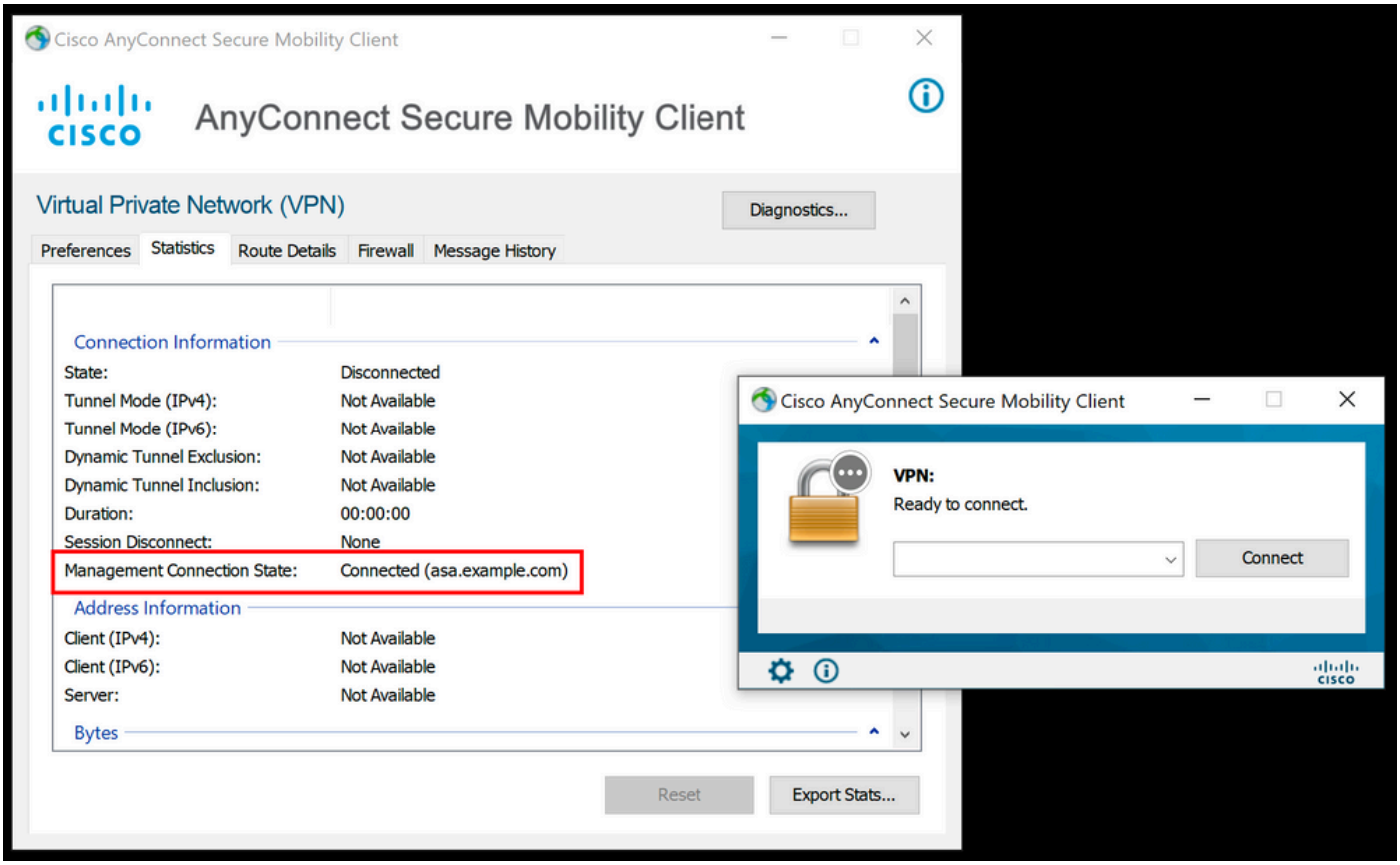
```
Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2               UDP Src Port : 57053
UDP Dst Port : 443                    Auth Mode    : Certificate
Idle Time Out: 30 Minutes             Idle TO Left : 18 Minutes
Client OS    : Windows
Client Type  : DTLS VPN Client
Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03036
Bytes Tx     : 17238                  Bytes Rx     : 1988
Pkts Tx      : 12                     Pkts Rx      : 13
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
```

Verifique a conexão do túnel VPN de gerenciamento no ASDM.

Navegue para **Monitoring > VPN > VPN Statistics > Sessions** . Filtre por **AnyConnect Client** para ver a sessão do cliente.



Verificação da conexão do túnel VPN de gerenciamento na máquina cliente:



Troubleshoot

A nova linha de estatísticas da interface do usuário (Estado da conexão de gerenciamento) pode ser usada para solucionar problemas de conectividade do túnel de gerenciamento. Estes são os estados de erro comumente vistos:

Desconectado (desabilitado):

- O recurso está desabilitado.
- Certifique-se de que o perfil de VPN de gerenciamento foi implantado no cliente, através da conexão de túnel do usuário (requer que você adicione o perfil de VPN de gerenciamento à política de grupo de túnel do usuário) ou fora da banda através do upload manual do perfil.
- Verifique se o perfil de VPN de gerenciamento está configurado com uma única entrada de host que inclua um grupo de túneis.

Desconectado (rede confiável):

- O TND detectou uma rede confiável, portanto, o túnel de gerenciamento não foi estabelecido.

Desconectado (túnel do usuário ativo):

- Um túnel VPN de usuário está ativo no momento.

Desconectado (falha na inicialização do processo):

- Uma falha de inicialização de processo foi encontrada quando houve uma tentativa de conexão do túnel de gerenciamento.

Desconectado (falha na conexão):

- Uma falha de conexão foi encontrada quando o túnel de gerenciamento foi estabelecido.
- Verifique se a autenticação de certificado está configurada no grupo de túneis, se não há nenhum banner presente na política de grupo e se o certificado do servidor deve ser confiável.

Desconectado (configuração de VPN inválida):

- Uma configuração inválida de separação de túneis foi recebida do servidor VPN.
- Verifique a configuração do tunelamento dividido na política de grupo de túneis de gerenciamento.

Desconectado (atualização de software pendente):

- Uma atualização de software do AnyConnect está pendente.

Desconectado:

- O túnel de gerenciamento está prestes a ser estabelecido ou não pode ser estabelecido por alguma outra razão.

Colete o DART para solucionar problemas.

Informações Relacionadas

- Configuração do túnel VPN de gerenciamento
- Troubleshooting de Túnel VPN de Gerenciamento
- Suporte Técnico e Documentação - Cisco Systems

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.