Configurar Autenticação Baseada em Certificado do Anyconnect para Acesso Móvel

Contents

Introdução

Este documento descreve um exemplo da implementação da autenticação baseada em certificado em dispositivos móveis.

Pré-requisitos

As ferramentas e dispositivos usados no guia são:

- Defesa contra ameaças (FTD) do Cisco Firepower
- Firepower Management Center (FMC)
- Dispositivo Apple iOS (iPhone, iPad)
- autoridade de certificado (CA)
- Software Cisco Anyconnect Client

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- VPN básica
- SSL/TLS
- Infraestrutura de Chave Pública
- Experiência com o FMC
- OpenSSL
- Cisco Anyconnect

Componentes Utilizados

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

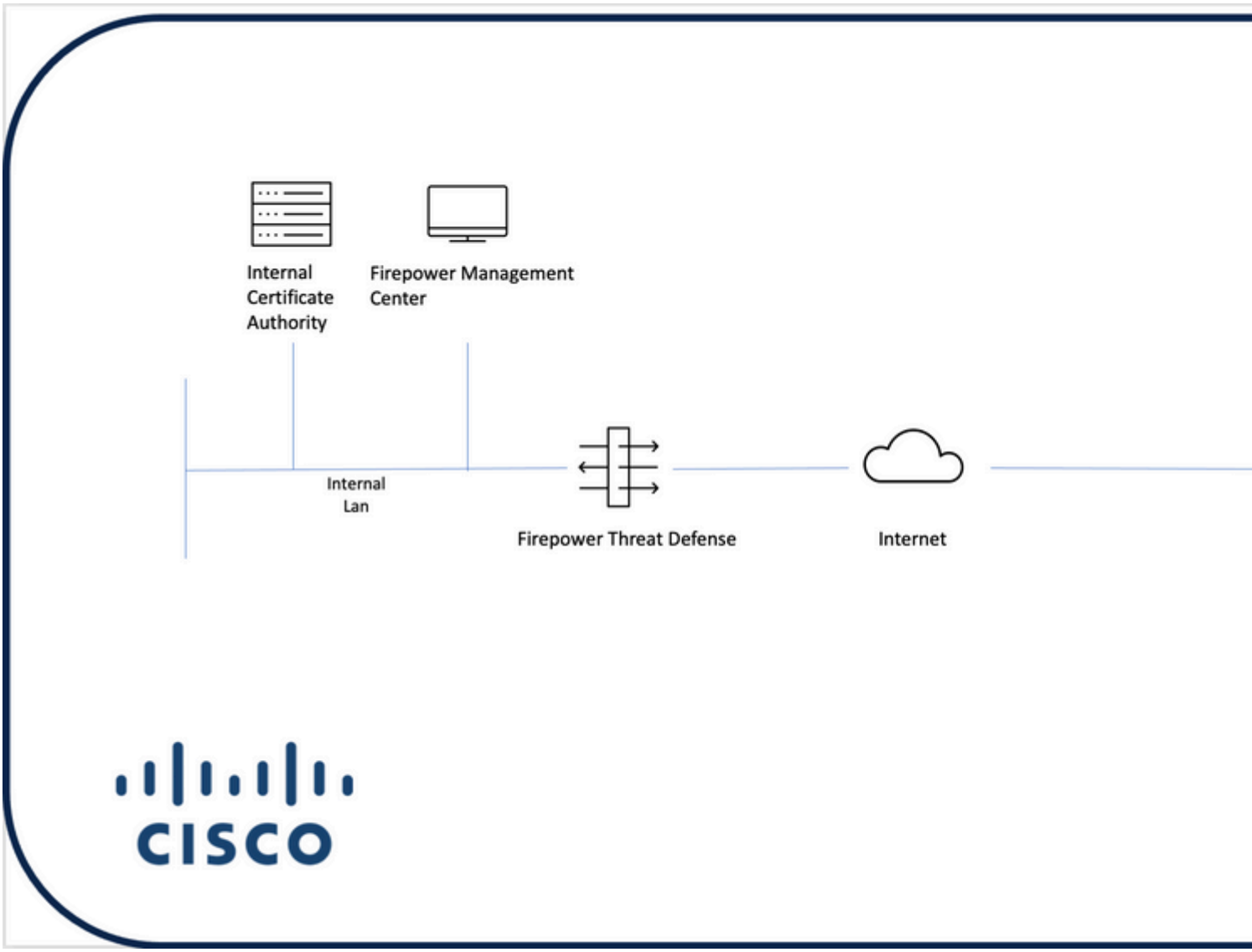
- FTD da Cisco
- FMC da Cisco
- Servidor de CA da Microsoft
- XCA
- Cisco Anyconnect
- Ipad de Apple

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

Configurar o Cisco Anyconnect no FTD

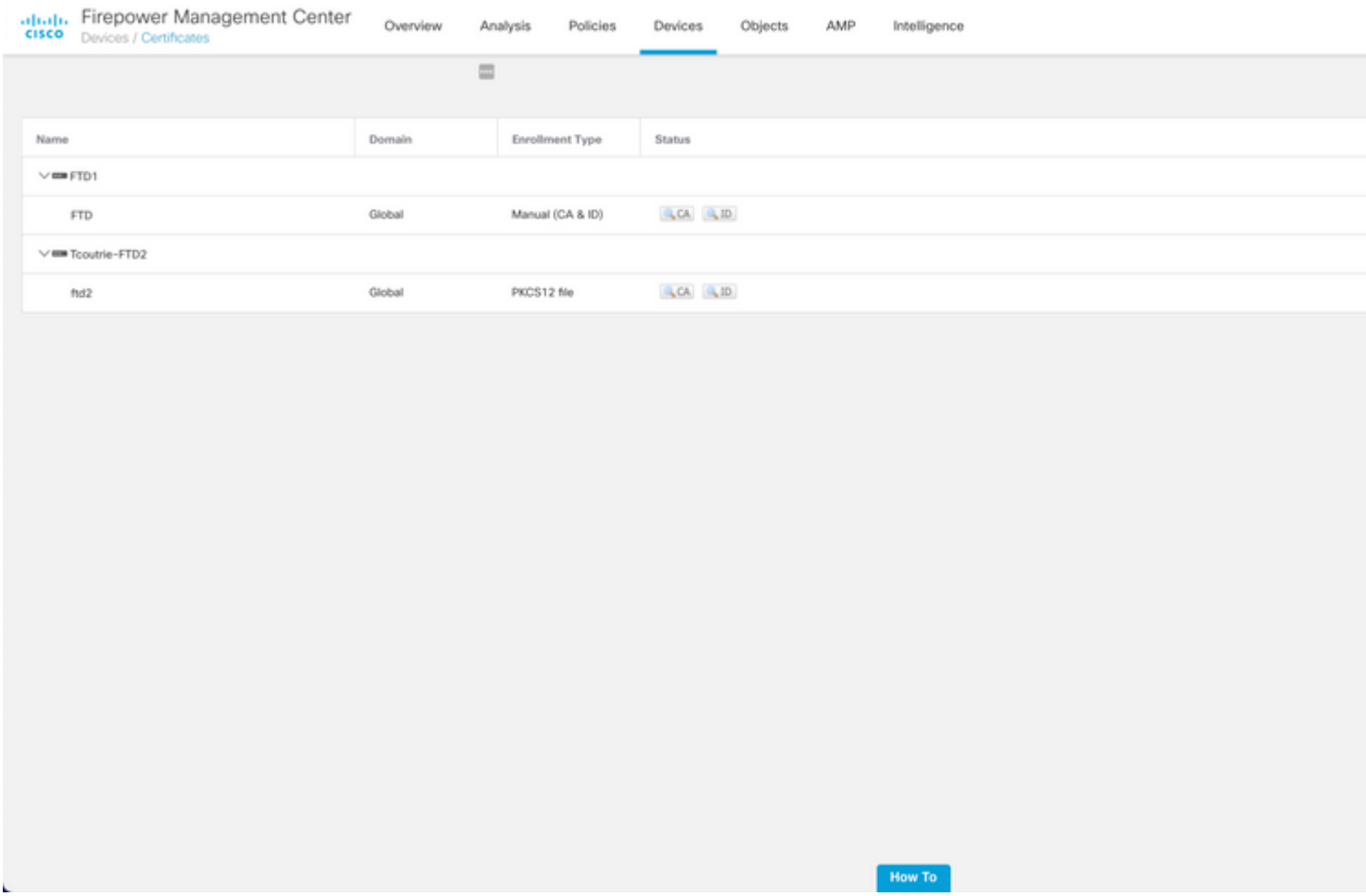
Esta seção descreve as etapas para configurar o Anyconnect via FMC. Antes de começar, assegure-se de implantar todas as configurações.

Diagrama de Rede

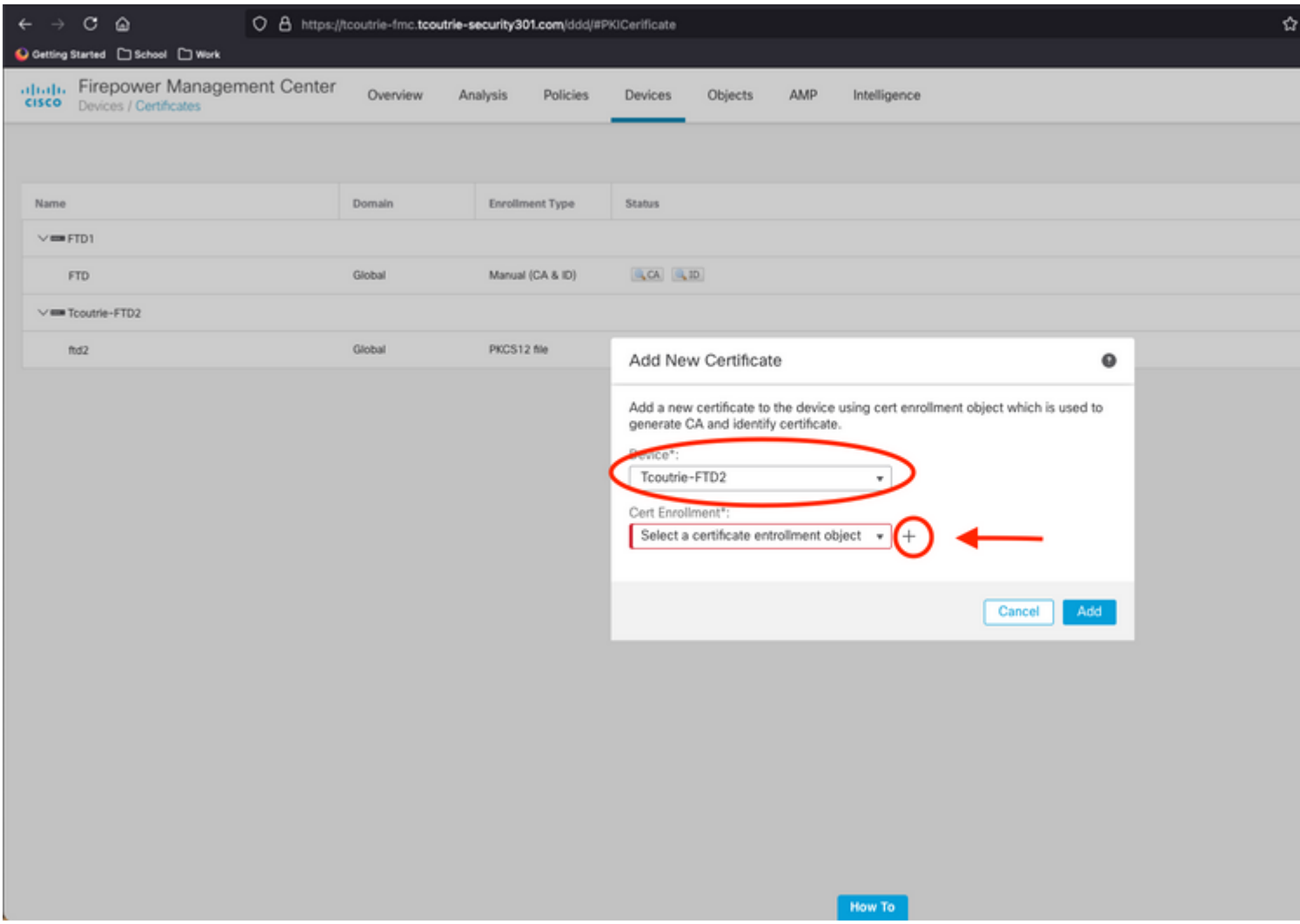


Adicionar certificado ao FTD

Etapa 1. Criar um certificado para o FTD no dispositivo FMC. Navegue até **Devices > Certificate** e escolha **Add**, como mostrado nesta imagem:



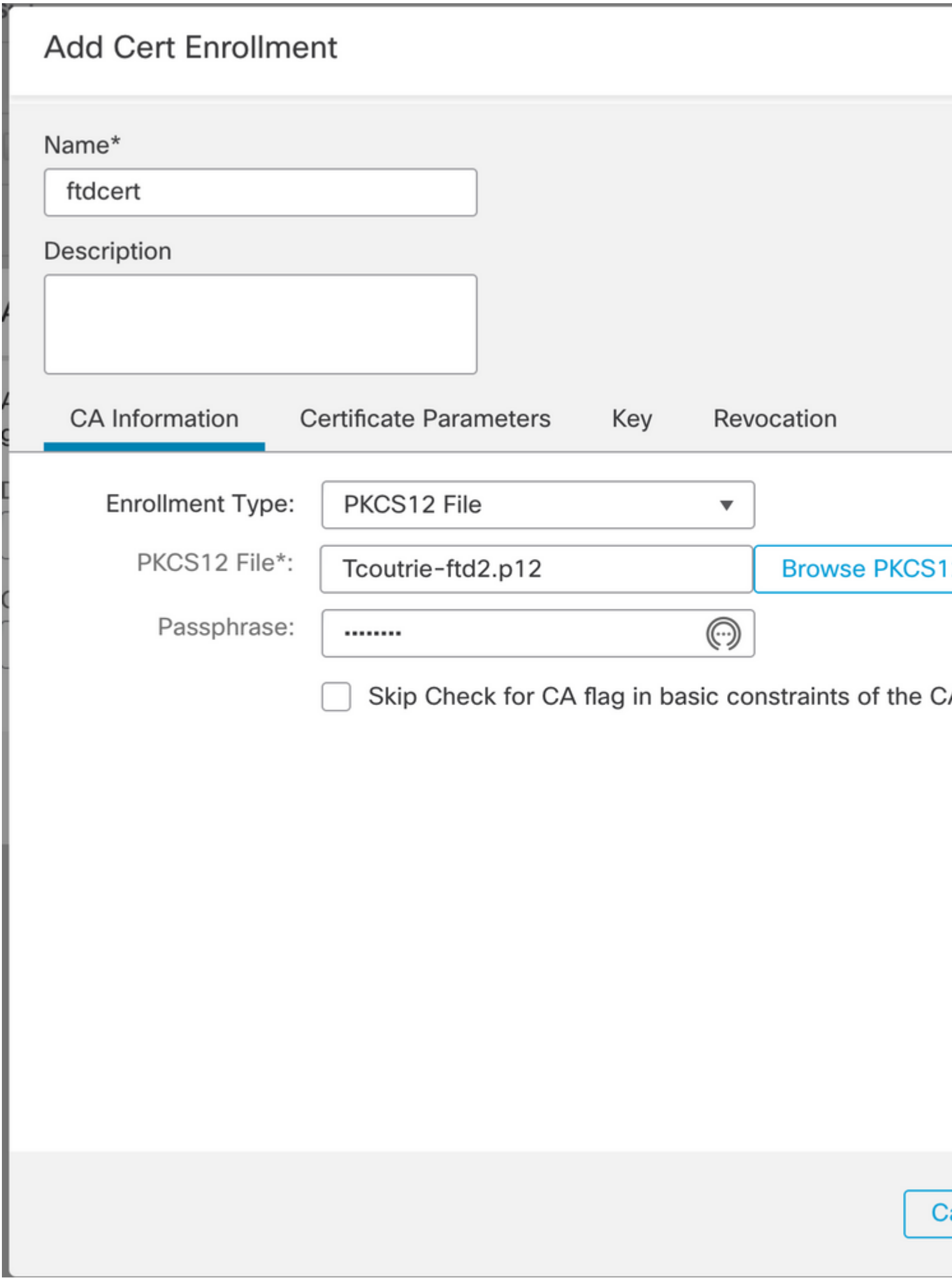
Etapa 2. Escolha o FTD desejado para a conexão VPN. Escolha o **dispositivo FTD** no menu suspenso de dispositivos. Clique no ícone + para adicionar um novo método de registro de certificado, como mostrado nesta imagem:



Etapa 3. Adicione os certificados ao dispositivo. Escolha a opção que é o método preferencial para obter certificados no ambiente.

> **Dica**: as opções disponíveis são: Certificado Autoassinado - Gerar um novo certificado localmente, SCEP - Usar o Simple Certificate Enrollment Protocol para obter um certificado de uma CA, Manual - Instalar manualmente o certificado de Raiz e Identidade, PKCS12 - Carregar o pacote de certificados criptografados com raiz, identidade e chave privada.

Etapa 4. Carregue o certificado no dispositivo FTD. Insira a senha (somente PKCS12) e clique em **Save**, como mostrado nesta imagem:


Add Cert Enrollment
Name*
ftdcert
Description
CA Information
Certificate Parameters
Key
Revocation
Enrollment Type:
PKCS12 File
PKCS12 File*:
Tcoutrie-ftd2.p12
Browse PKCS1
Passphrase:
.....
Skip Check for CA flag in basic constraints of the CA

Observação

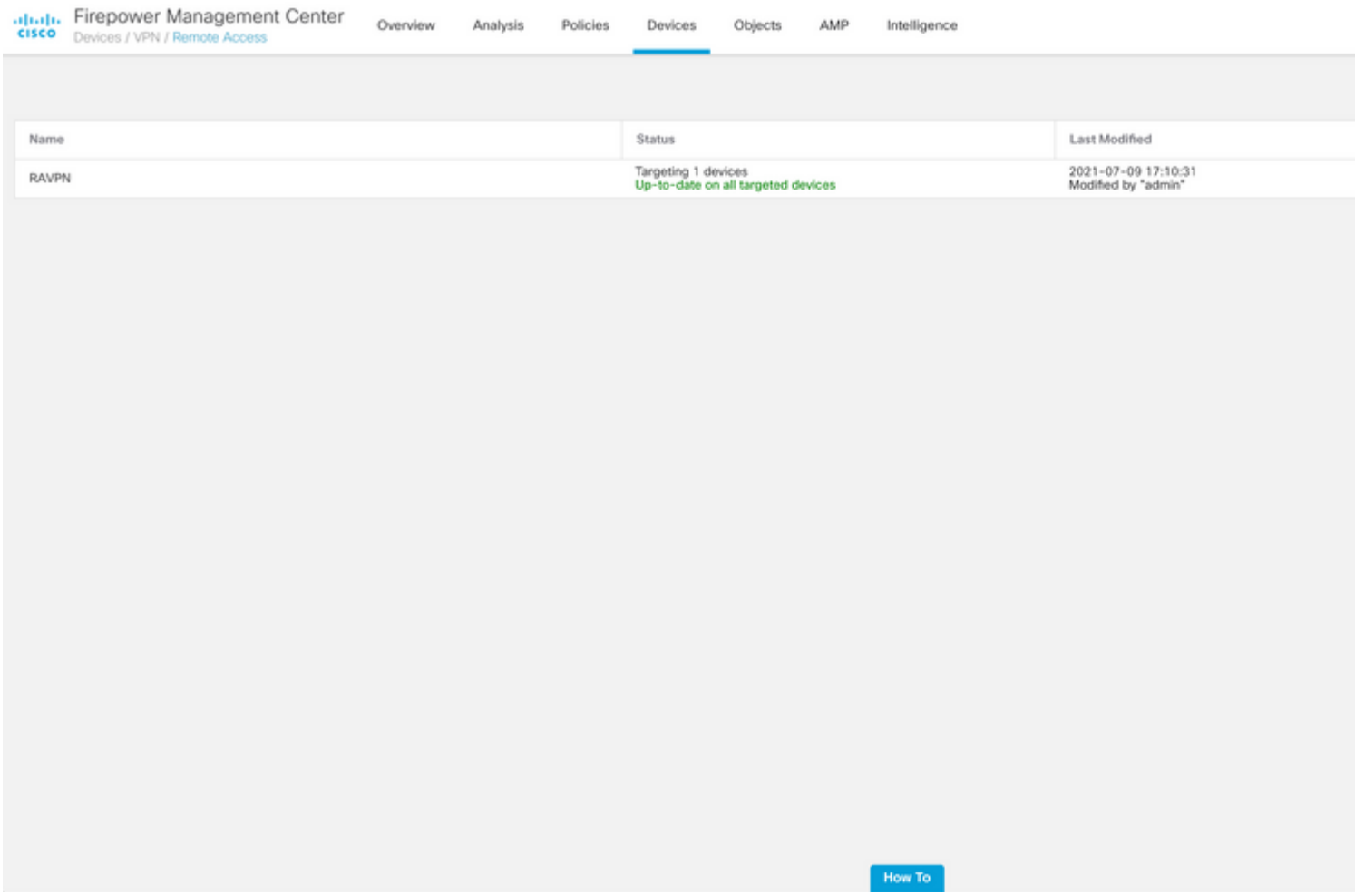
: depois de salvar o arquivo, a implantação dos certificados ocorre imediatamente. Para ver detalhes do certificado, escolha a ID.

Configurar o Cisco Anyconnect

Configure o Anyconnect via FMC com o assistente de acesso remoto.

Etapa 1. Inicie o assistente de política de VPN de acesso remoto para configurar o Anyconnect.

Navegue até **Devices > Remote Access** e escolha **Add**.

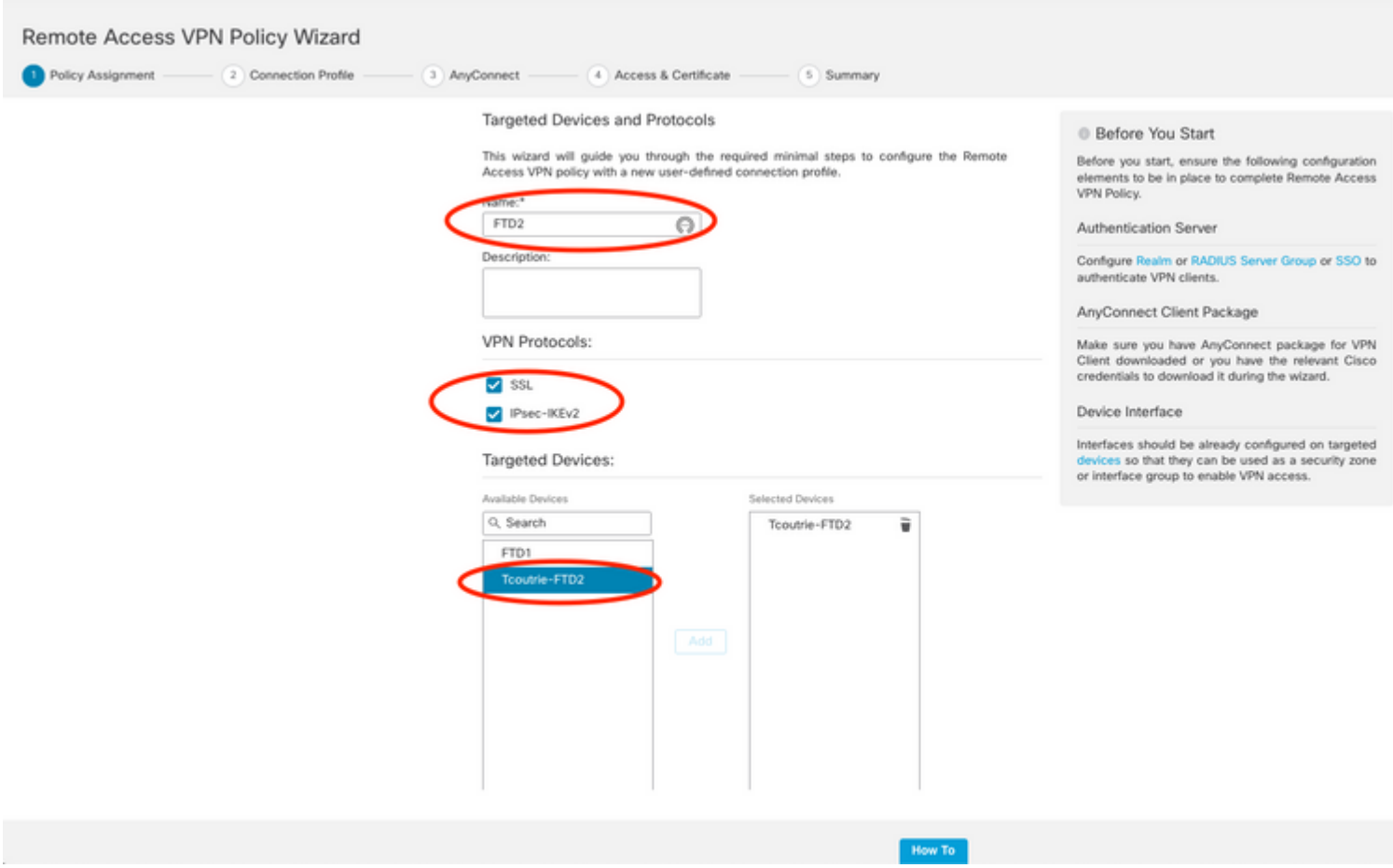


Etapa 2. Atribuição de política.

Conclua a atribuição de política:
a. Nomeie a política.

b. Escolha os protocolos VPN desejados.

c. Escolha o dispositivo de destino para aplicar a configuração.

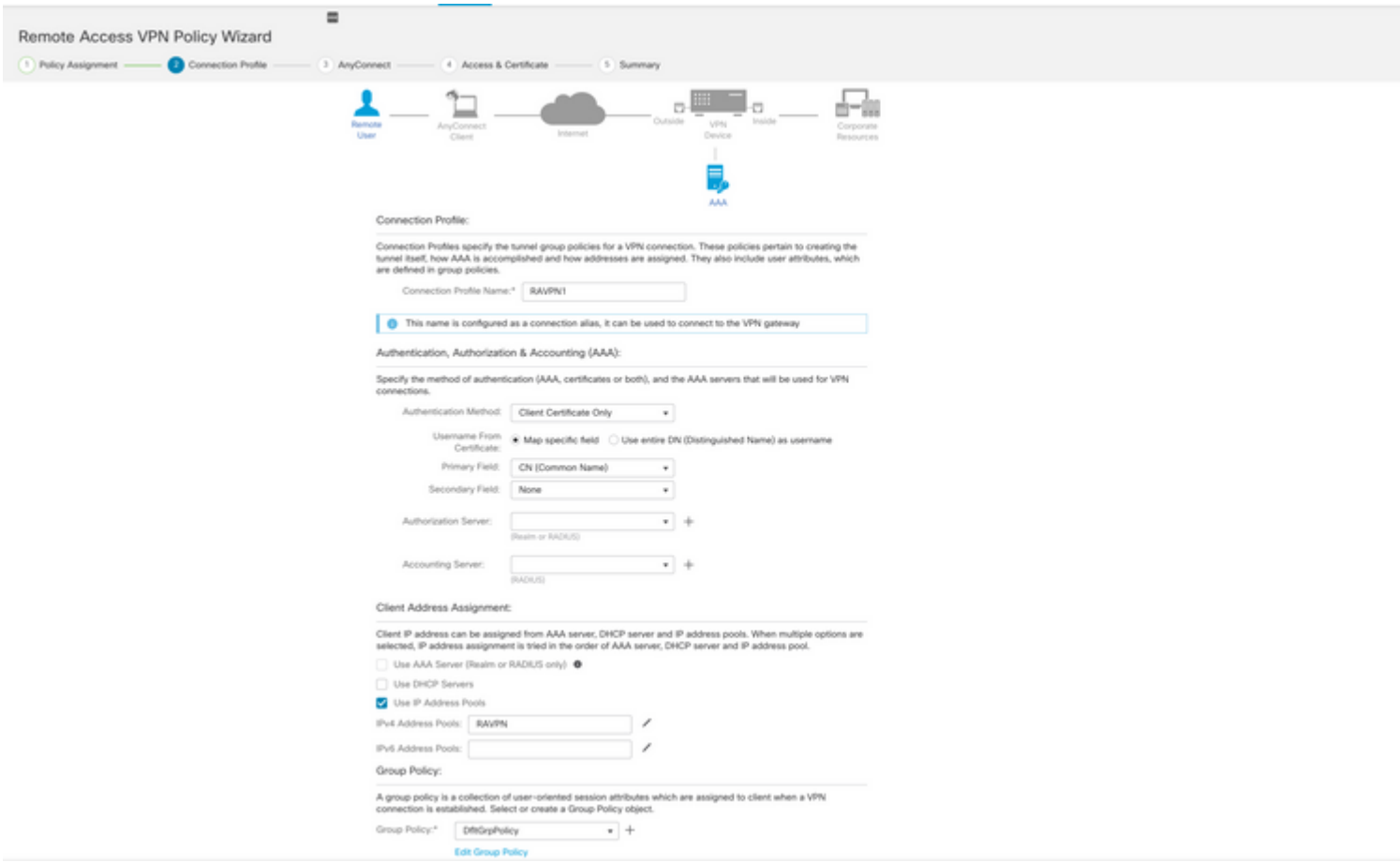


Etapa 3. Connection Profile (Perfil de conexão).

a. Nomeie o Perfil de Conexão.
b. Defina o método de autenticação como Somente certificado do cliente.

c. Atribua um pool de endereços IP e, se necessário, crie uma nova Diretiva de Grupo.

d. Clique em Next.



Observação: escolha o campo Primário a ser usado para inserir o nome de usuário para sessões de autenticação. O CN do certificado é usado neste guia.

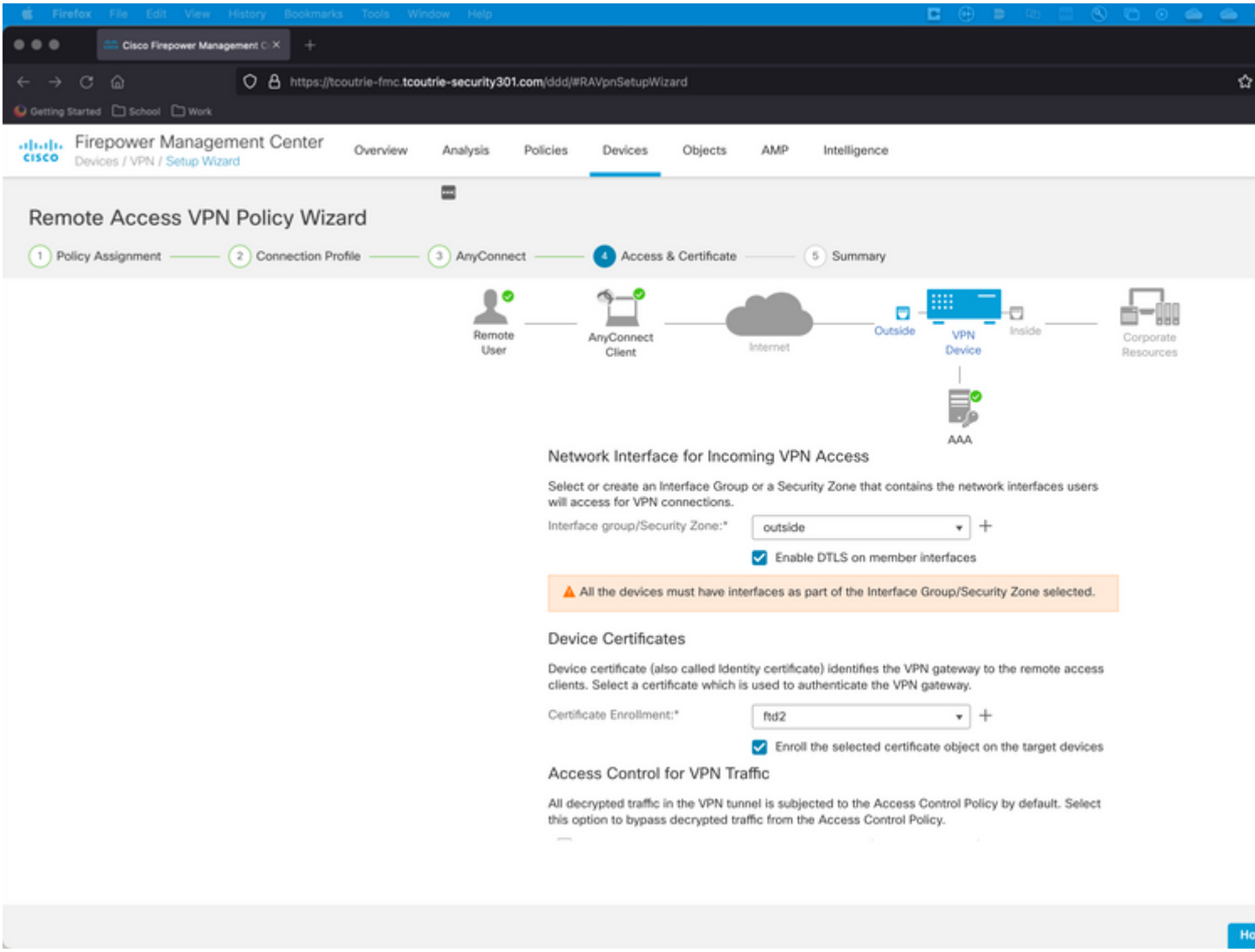
Etapa 4. AnyConnect.

Adicione uma imagem do Anyconnect ao equipamento. Carregue a versão preferencial do Anyconnect e clique em **Avançar**.

Observação: os pacotes do Cisco Anyconnect podem ser baixados em **Software.Cisco.com**.

Etapa 5. Acesso e certificado.

Aplique o certificado a uma interface e habilite o Anyconnect no nível da interface, como mostrado nesta imagem, e clique em **Avançar**.



Etapa 6. Summary.

Revise as configurações. Se todos fizerem check-out, clique em **concluir** e em **implantar**.

Criar Certificado para Usuários Móveis

Crie um certificado a ser adicionado ao dispositivo móvel usado na conexão.

Etapa 1. XCA.

a. Abrir XCA

b. Iniciar um novo Banco de Dados

Etapa 2. Criar CSR.

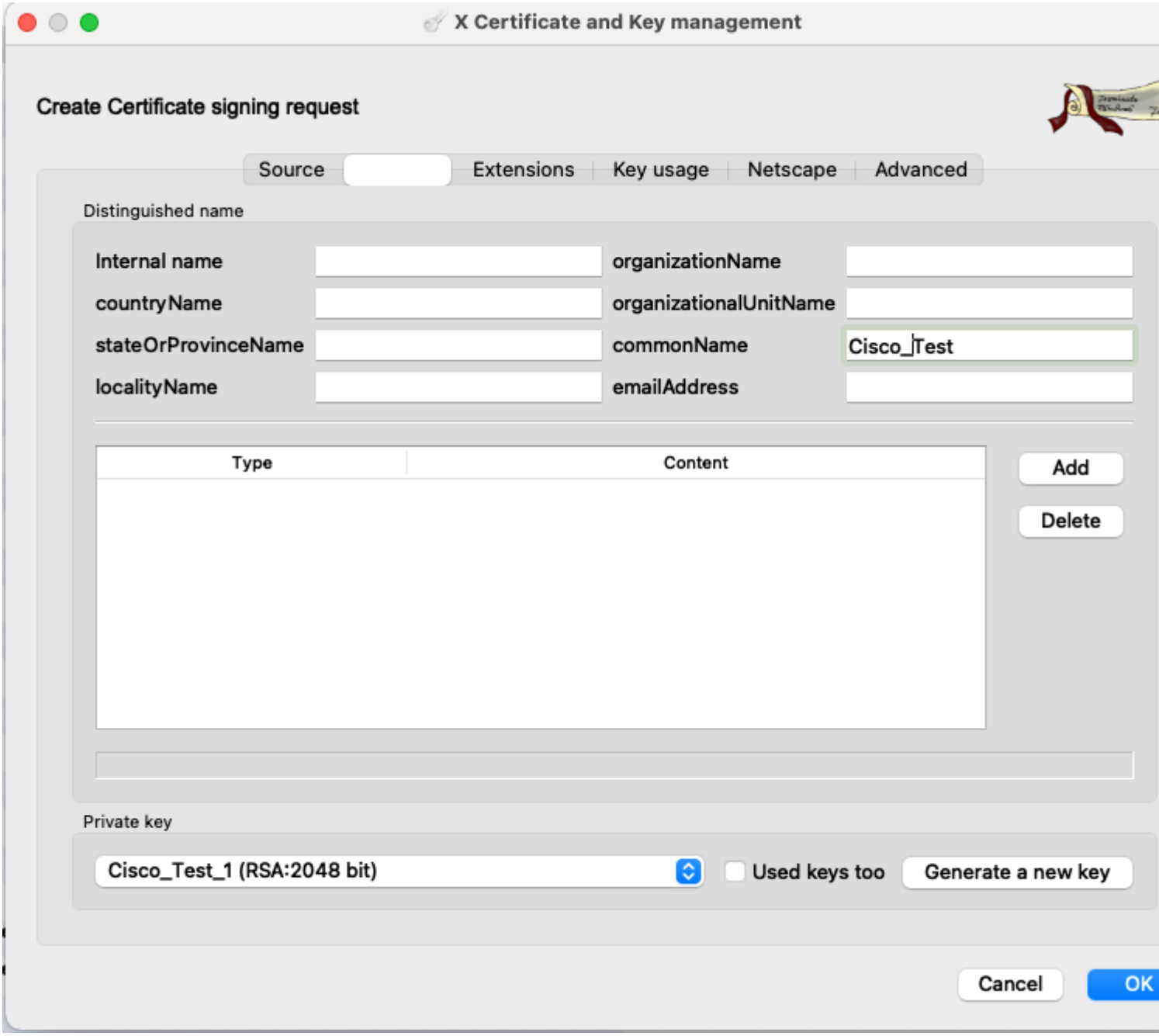
a. Escolha **Solicitação de Assinatura de Certificado** (CSR)

b. Escolher **Nova Solicitação**

c. Insira o valor com todas as informações necessárias para o certificado

d. Gerar uma nova chave

e. Ao terminar, clique em **OK**

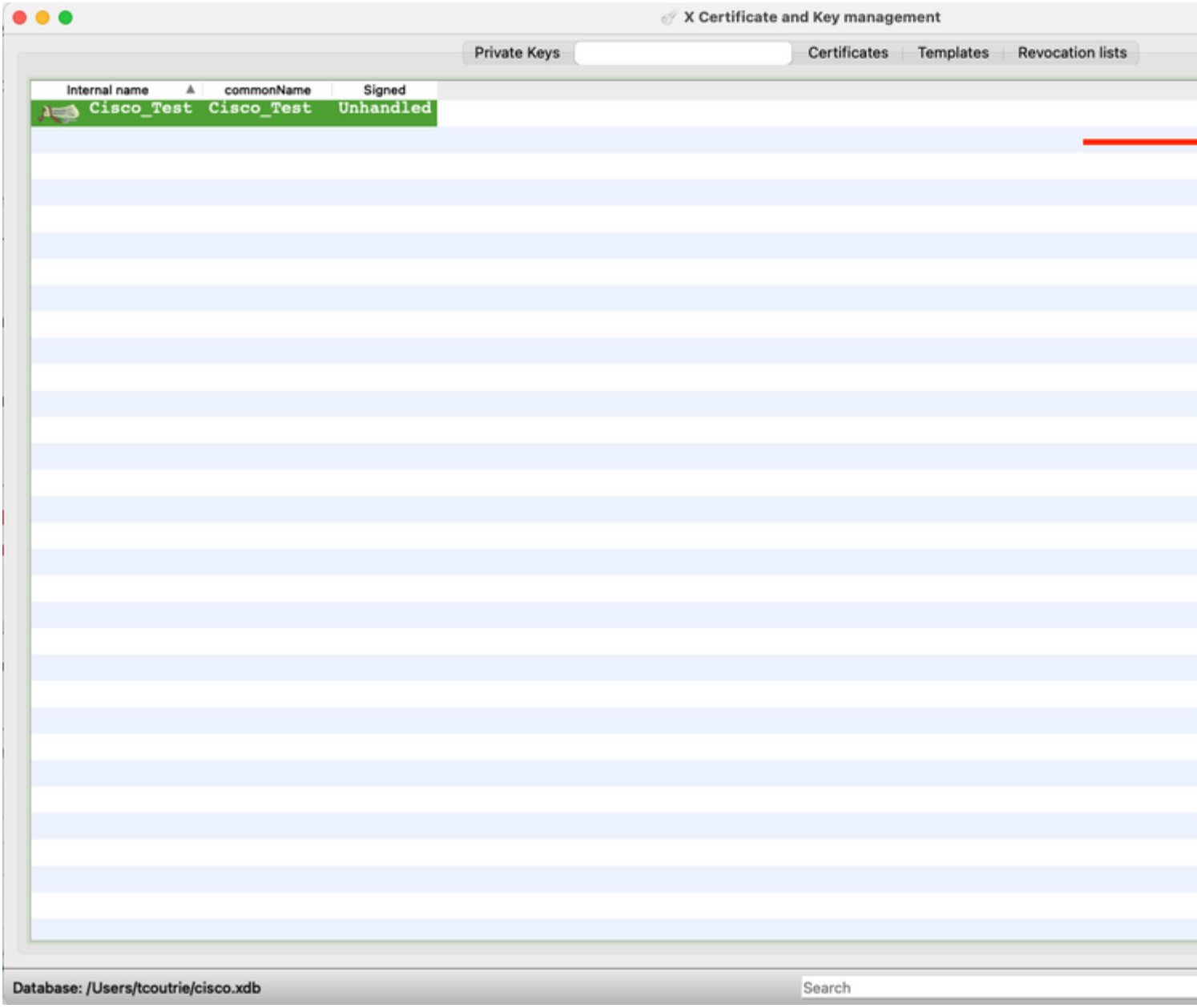


Observação: este documento usa o CN do certificado.

Etapa 3. Enviar CSR.

a. Exportar o CSR

b. Enviar CSR para CA para obter um novo certificado

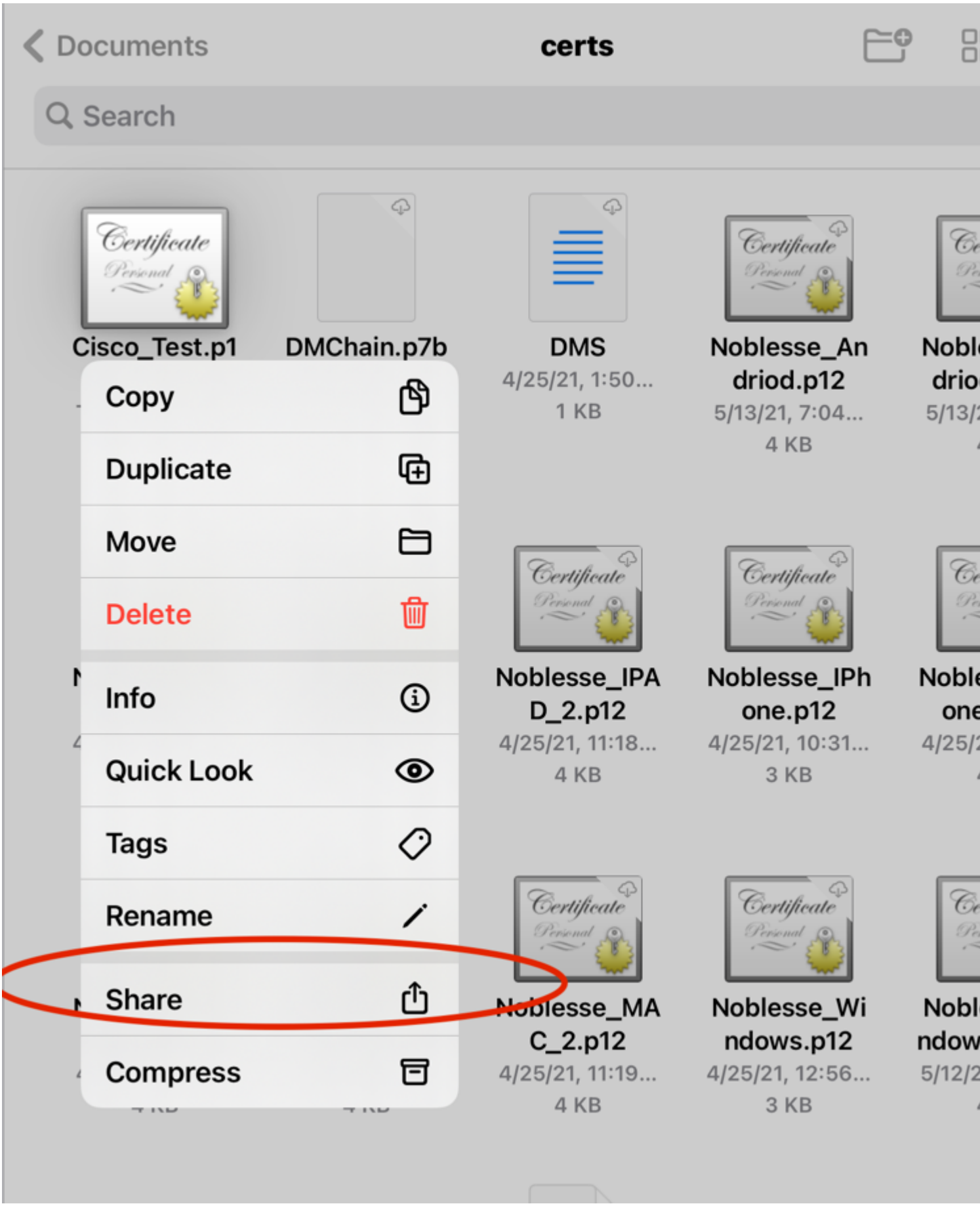


Observação: use o formato PEM do CSR.

Instalar no Dispositivo Móvel

Etapa 1. Adicione o certificado do dispositivo ao dispositivo móvel.
Etapa 2. Compartilhe o certificado com o aplicativo Anyconnect para adicionar o novo aplicativo de certificado.

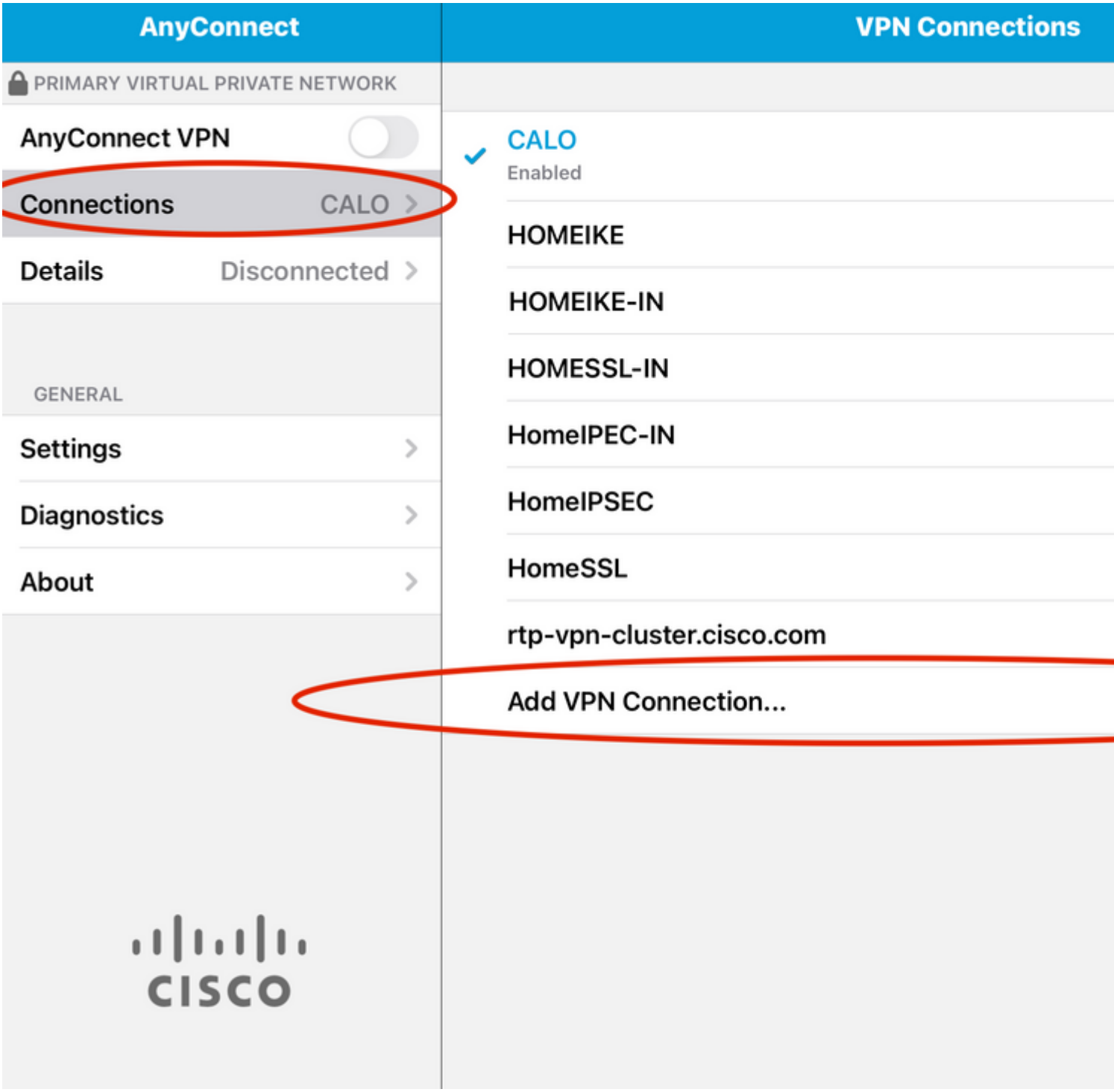
Cuidado: a instalação manual exige que o usuário compartilhe o certificado com o aplicativo. Isso não se aplica a certificados enviados via MDMs.



Etapa 3. Insira a senha do certificado para o arquivo **PKCS12**.

Etapa 4. Crie uma nova conexão no Anyconnect.

Etapa 5. Navegue para novas conexões; **Conexões > Adicionar conexão VPN**.



Etapa 6. Digite as informações para a nova conexão.â€*f*

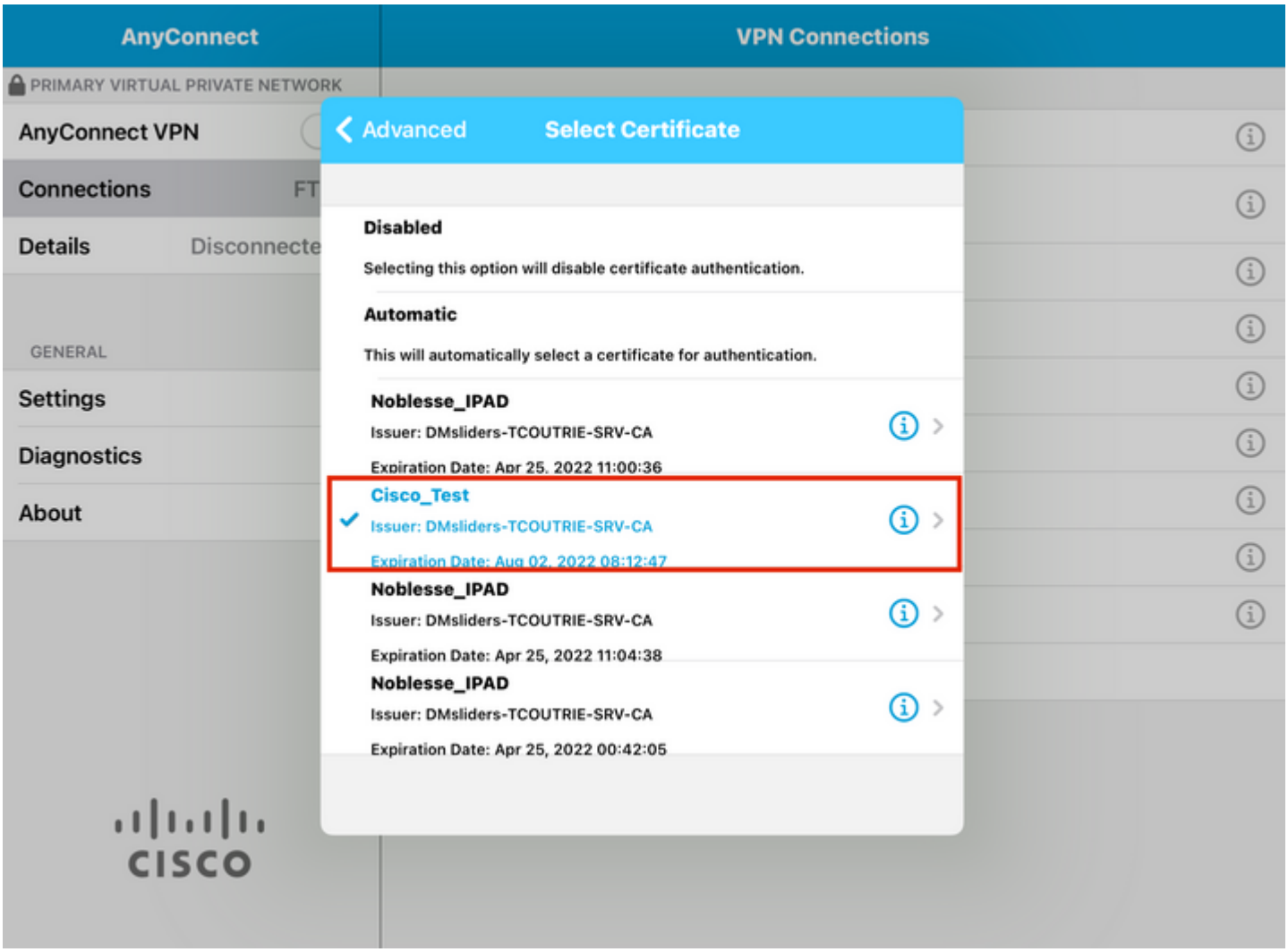
Descrição: Nomeie a conexão

Endereço do servidor: endereço IP ou FQDN do FTD

Avançado: configurações adicionais

Passo 7. Escolha **Advanced**.

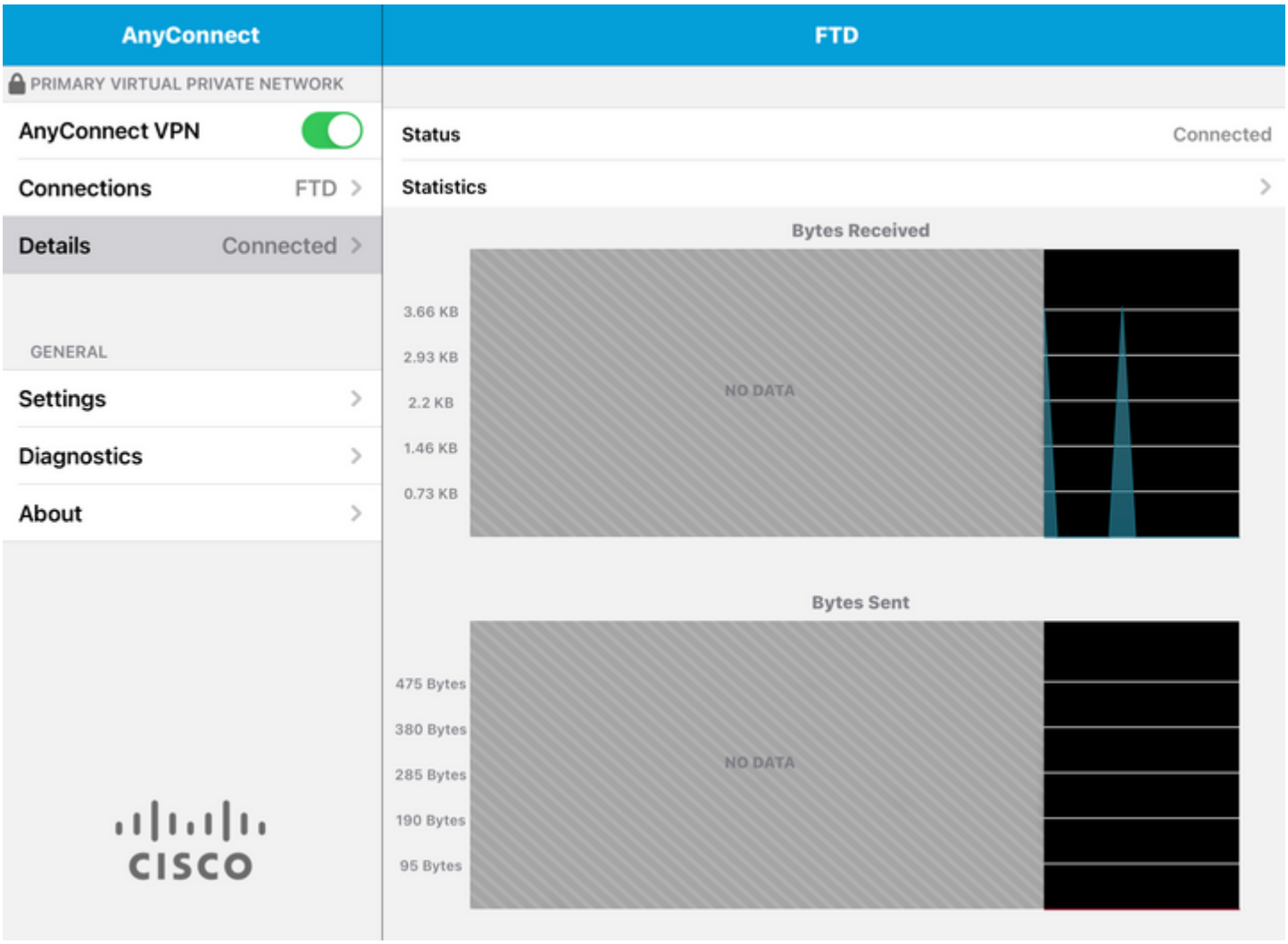
Etapa 8. Escolha **Certificate** e escolha o certificado recém-adicionado.



â€ƒ

Etapa 9. Navegue de volta para **Conexões** e teste.

Uma vez bem-sucedida, a alternância permanece ativa e os detalhes mostram conectado no status.



Verificar

O comando **show vpn-sessiondb detail Anyconnect** mostra todas as informações sobre o host conectado.

> **Dica**: a opção para filtrar ainda mais este comando são as palavras-chave 'filter' ou 'sort' adicionadas ao comando.

Por exemplo:

```
Tcoutrie-FTD3# show vpn-sessiondb detail Anyconnect


Username : Cisco_Test Index : 23
Assigned IP : 10.71.1.2 Public IP : 10.118.18.168
Protocol : Anyconnect-Parent SSL-Tunnel DTLS-Tunnel
License : Anyconnect Premium, Anyconnect for Mobile
Encryption : Anyconnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hash : Anyconnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 8627 Bytes Rx : 220
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : SSL Tunnel Group : SSL
Login Time : 13:03:28 UTC Mon Aug 2 2021
```

```
Duration : 0h:01m:49s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a7aa95d000170006107ed20
Security Grp : none Tunnel Zone : 0

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

Anyconnect-Parent:
Tunnel ID : 23.1
Public IP : 10.118.18.168
Encryption : none Hashing : none
TCP Src Port : 64983 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : apple-ios
Client OS Ver: 14.6
Client Type : Anyconnect
Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099
Bytes Tx : 6299 Bytes Rx : 220
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 23.2
Assigned IP : 10.71.1.2 Public IP : 10.118.18.168
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 64985
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Apple iOS
Client Type : SSL VPN Client
Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099
Bytes Tx : 2328 Bytes Rx : 0
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 23.3
Assigned IP : 10.71.1.2 Public IP : 10.118.18.168
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 51003
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Apple iOS
Client Type : DTLS VPN Client
Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Troubleshooting

Debugs

As depurações que devem ser exigidas para solucionar esse problema são:

```
Debug crypto ca 14

Debug webvpn 255

Debug webvpn Anyconnect 255
```

Se a conexão for IPSEC e não SSL:

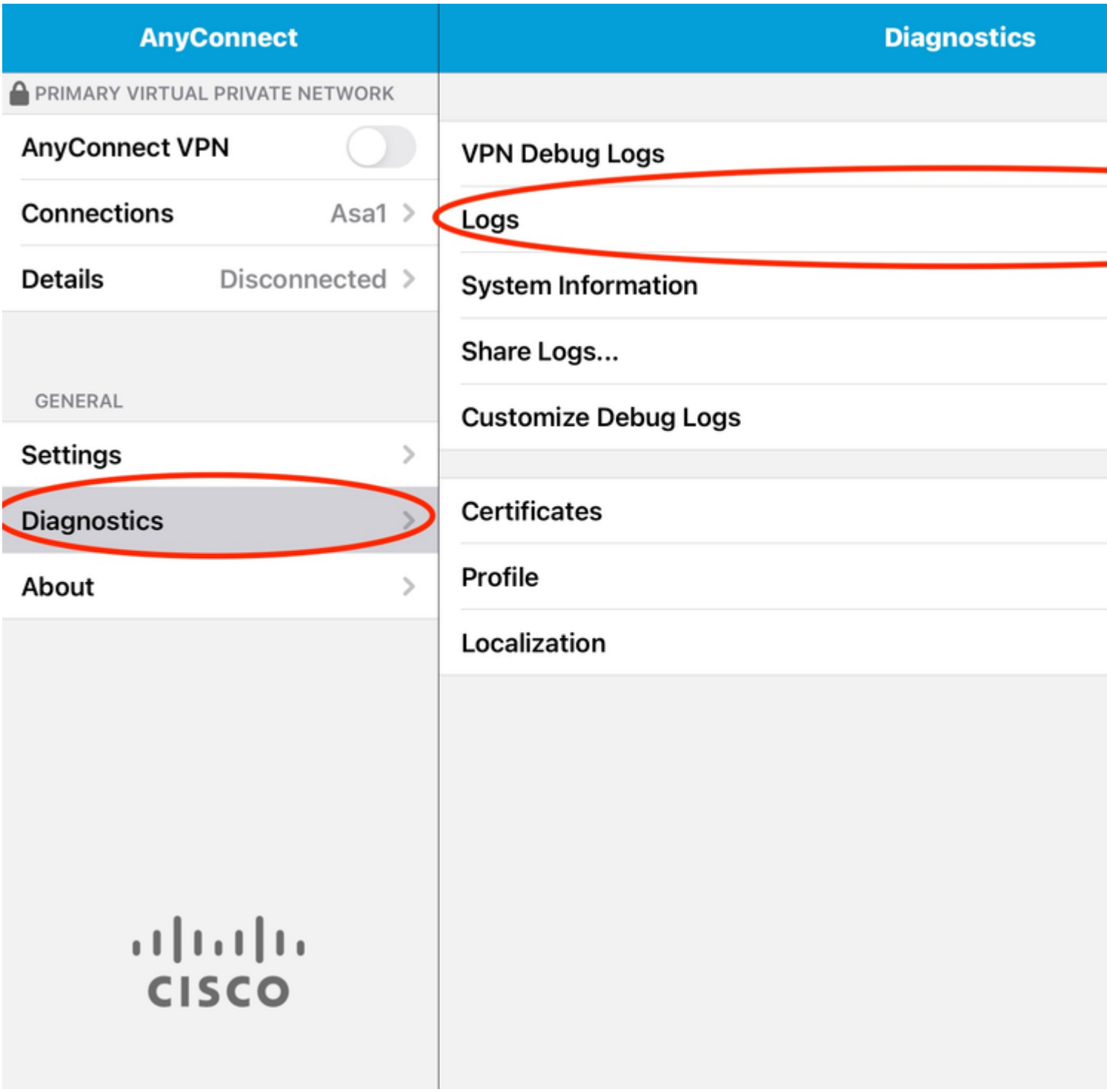
```
Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

debug crypto CA 14
```

Logs do aplicativo móvel Anyconnect:

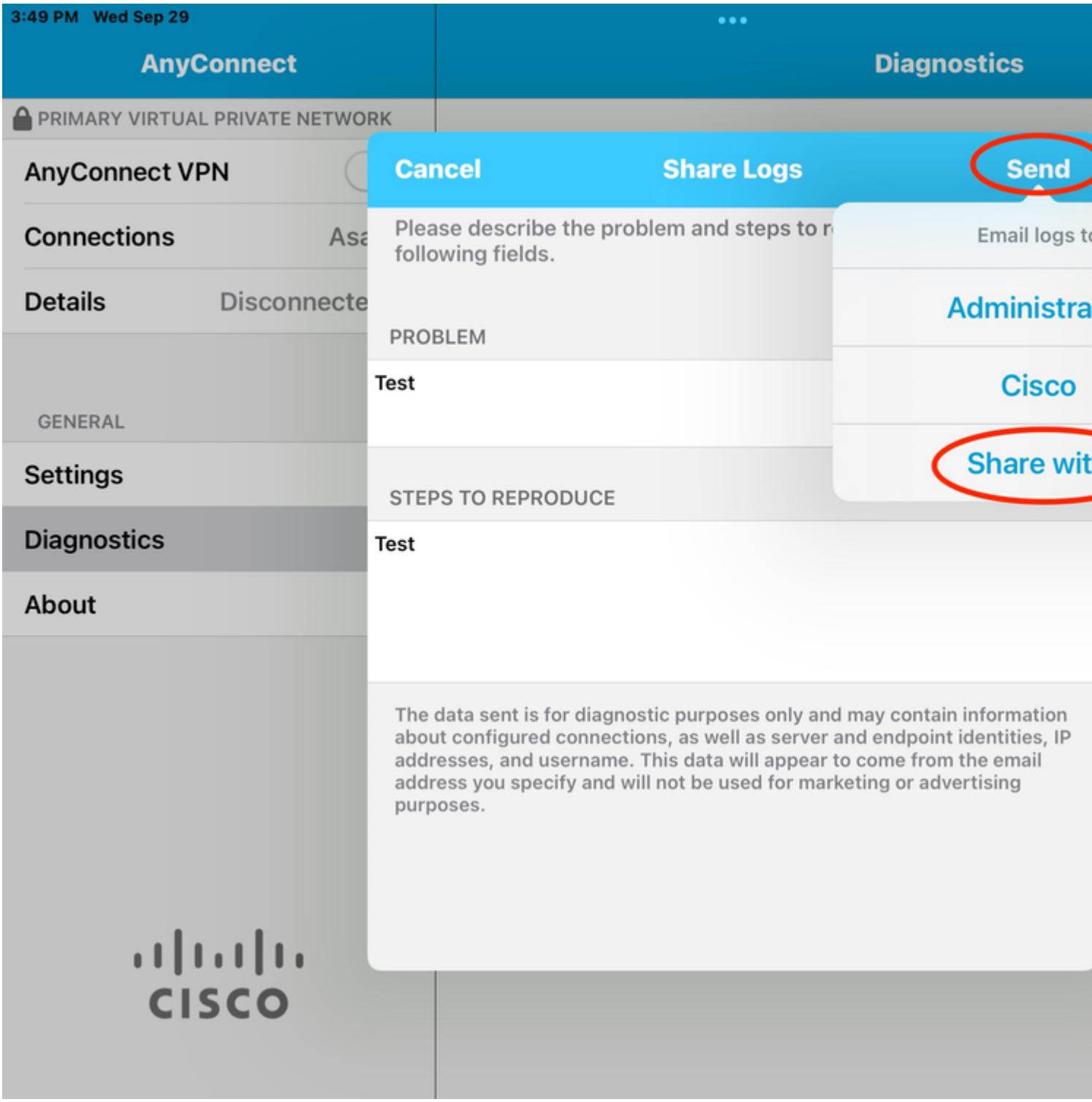
Navegue até **Diagnostic > VPN Debug Logs > Share logs**.



Digite as informações:

- Problema
- Etapas para reprodução

Em seguida, navegue até **Enviar > Compartilhar com**.



Isso apresenta a opção de usar um cliente de e-mail para enviar os logs.

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.