

Configurar a VPN de Acesso Remoto no FTD Gerenciado pelo FDM

Contents

- [Introdução](#)
- [Pré-requisitos](#)
- [Requisitos](#)
- [Licenciamento](#)
- [Componentes Utilizados](#)
- [Informações de Apoio](#)
- [Configurar](#)
- [Diagrama de Rede](#)
- [Verificar Licenciamento no FTD](#)
- [Definir redes protegidas](#)
- [Criar usuários locais](#)
- [Adicionar certificado](#)
- [Configurar a VPN de acesso remoto](#)
- [Verificar](#)
- [Troubleshooting](#)
- [Problemas do AnyConnect Client](#)
- [Problemas iniciais de conectividade](#)
- [Problemas específicos de tráfego](#)

Introdução

Este documento descreve como configurar a implantação de uma VPN RA no FTD gerenciado pelo FDM do gerenciador em pacote que executa a versão 6.5.0 e posterior.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento da configuração da Rede virtual privada (RA VPN) de acesso remoto no Firepower Device Manager (FDM).

Licenciamento

- O Firepower Threat Defense (FTD) foi registrado no portal de licenciamento inteligente com Export Controlled Features habilitados (para permitir que a guia de configuração do RA VPN seja habilitada)
- Qualquer uma das licenças do AnyConnect habilitadas (APEX, Plus ou somente VPN)

Componentes Utilizados

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

- FTD da Cisco que executa a versão 6.5.0-115
- Cisco AnyConnect Secure Mobility Client versão 4.7.01076

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.

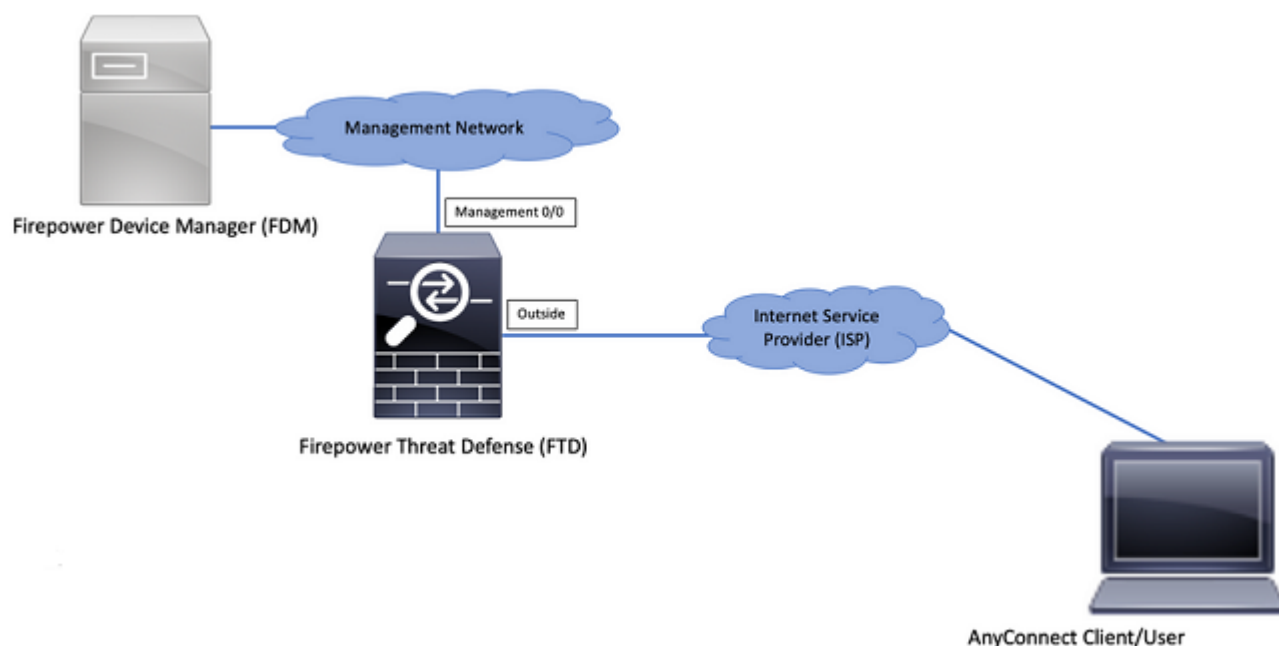
Informações de Apoio

A configuração do FTD por meio do FDM apresenta dificuldades quando você tenta estabelecer conexões para clientes do AnyConnect por meio da interface externa, enquanto o gerenciamento é acessado por meio da mesma interface. Esta é uma limitação conhecida do FDM. A solicitação de aprimoramento [CSCvm76499](#) foi preenchida para este problema.

Configurar

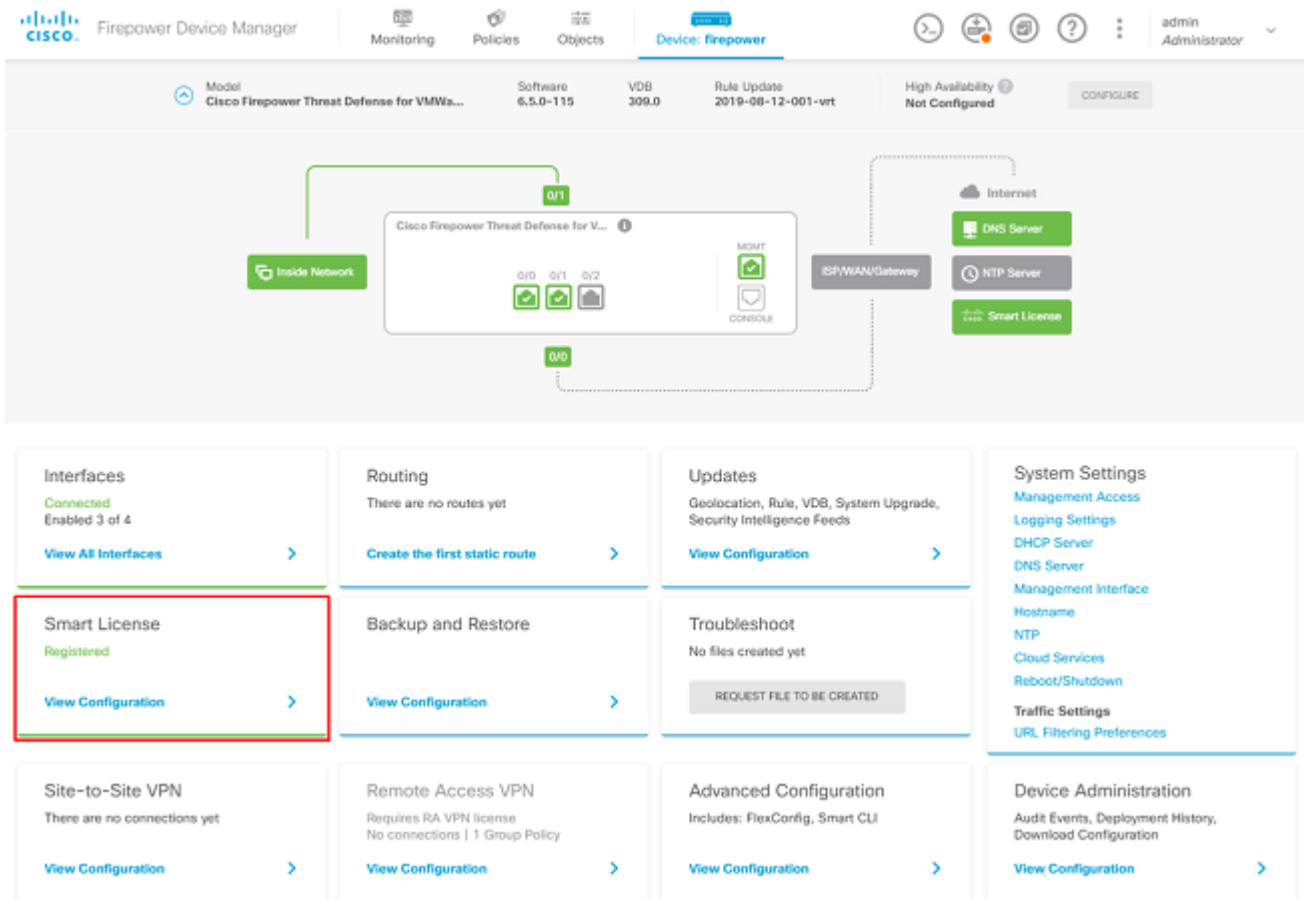
Diagrama de Rede

Autenticação do AnyConnect Client com o uso de Local.

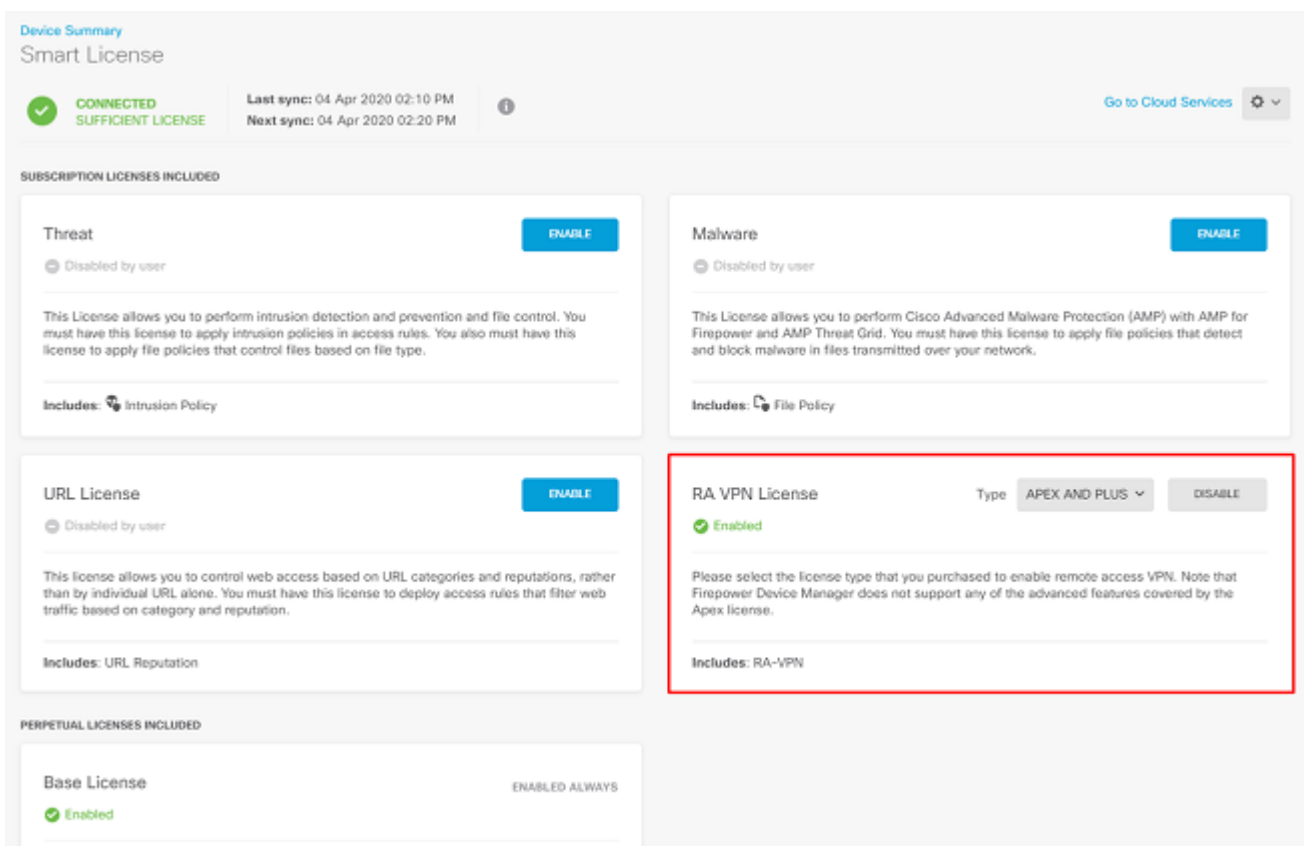


Verificar Licenciamento no FTD

Etapa 1. Verifique se o dispositivo está registrado no Smart Licensing conforme mostrado na imagem:

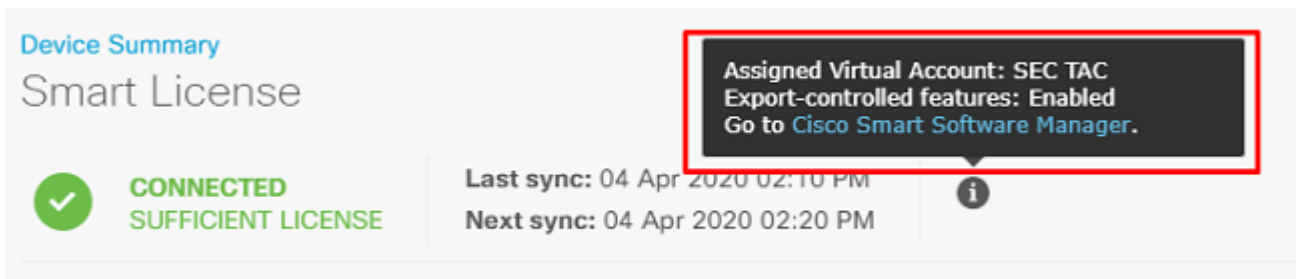


Etapa 2. Verifique se as licenças do AnyConnect estão ativadas no dispositivo conforme mostrado na imagem.



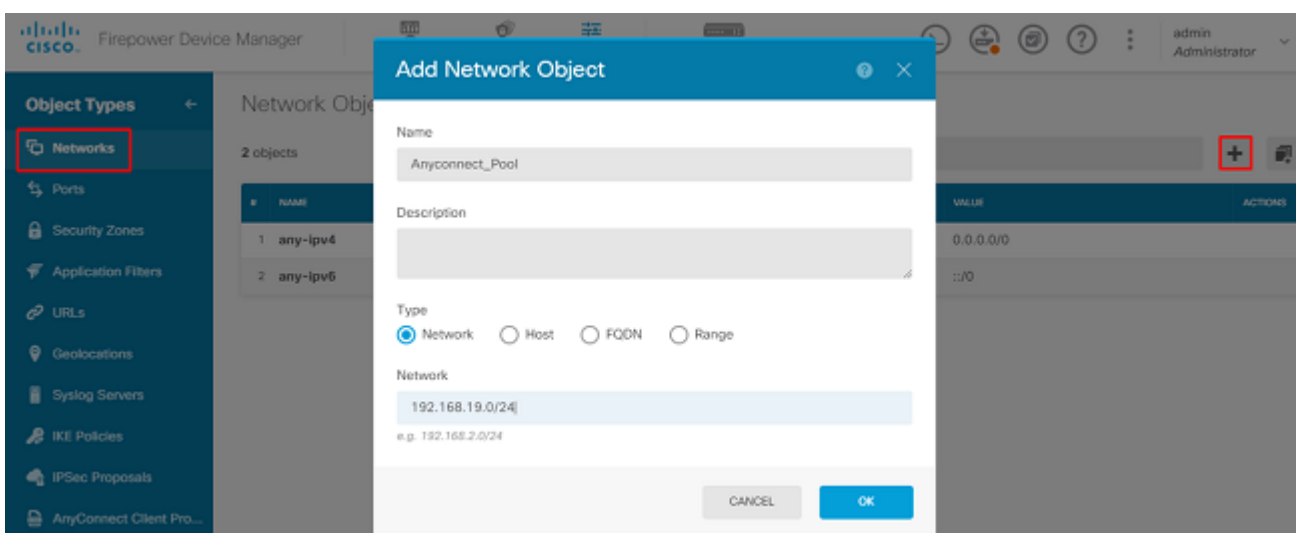
Etapa 3. Verifique se os recursos controlados por exportação estão ativados no token como mostrado na

imagem:

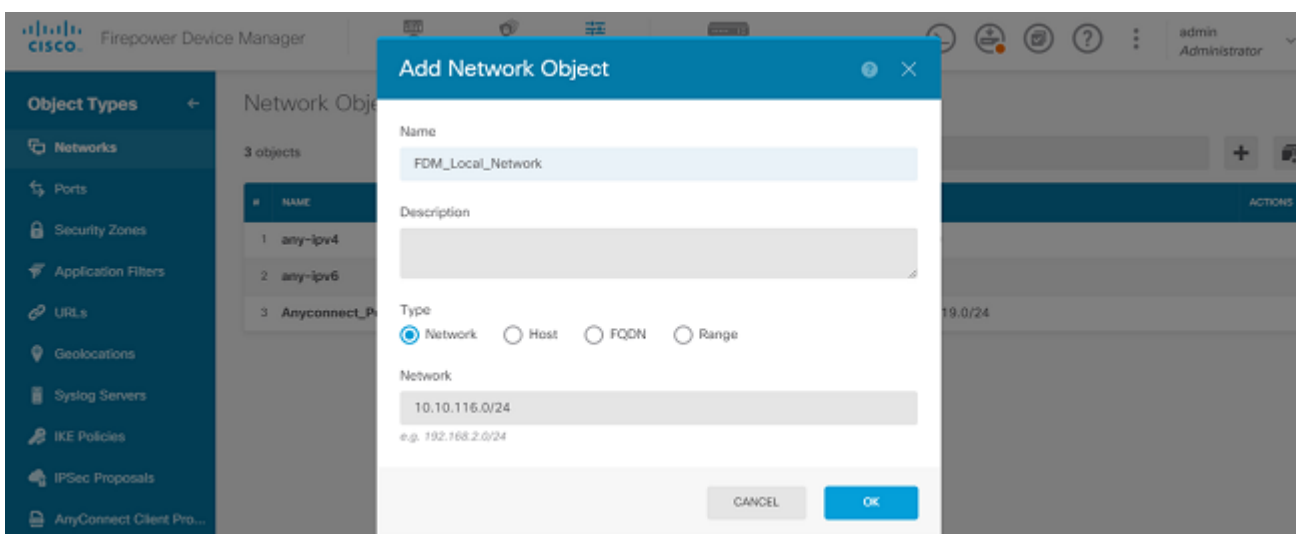


Definir redes protegidas

Navegue até Objects > Networks > Add new Network. Configure o Pool de VPN e as Redes LAN na GUI do FDM. Crie um pool de VPN para ser usado para atribuição de endereço local para usuários do AnyConnect, como mostrado na imagem:

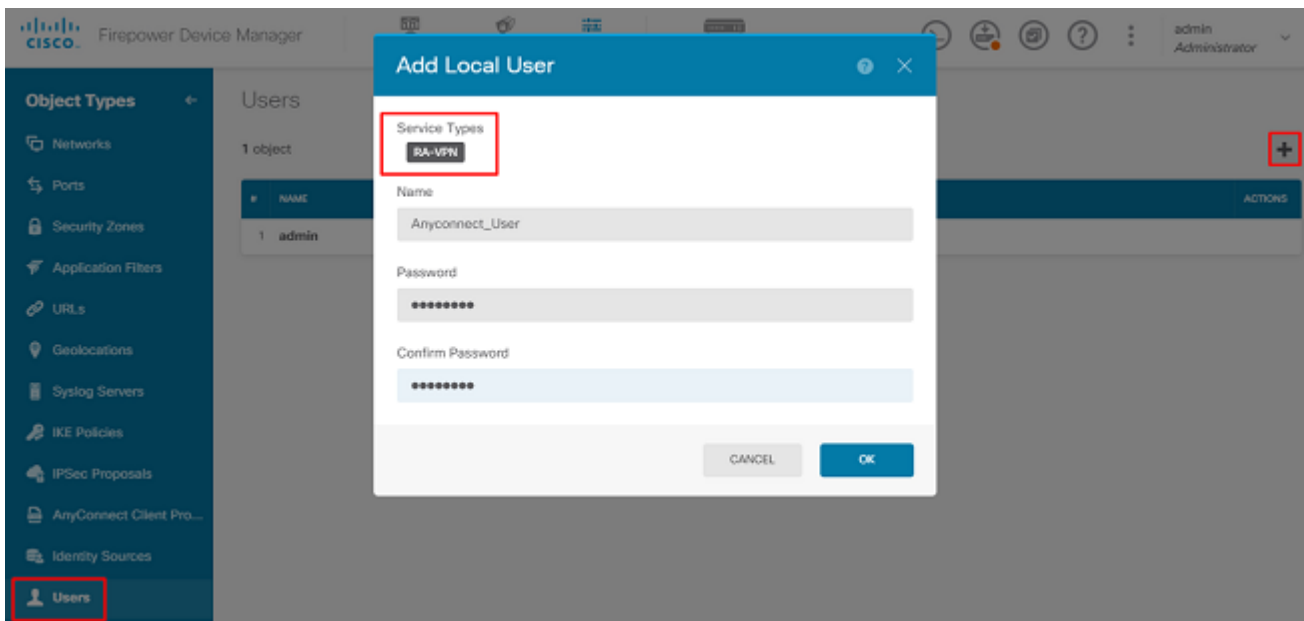


Crie um objeto para a rede local através do dispositivo FDM, conforme mostrado na imagem:



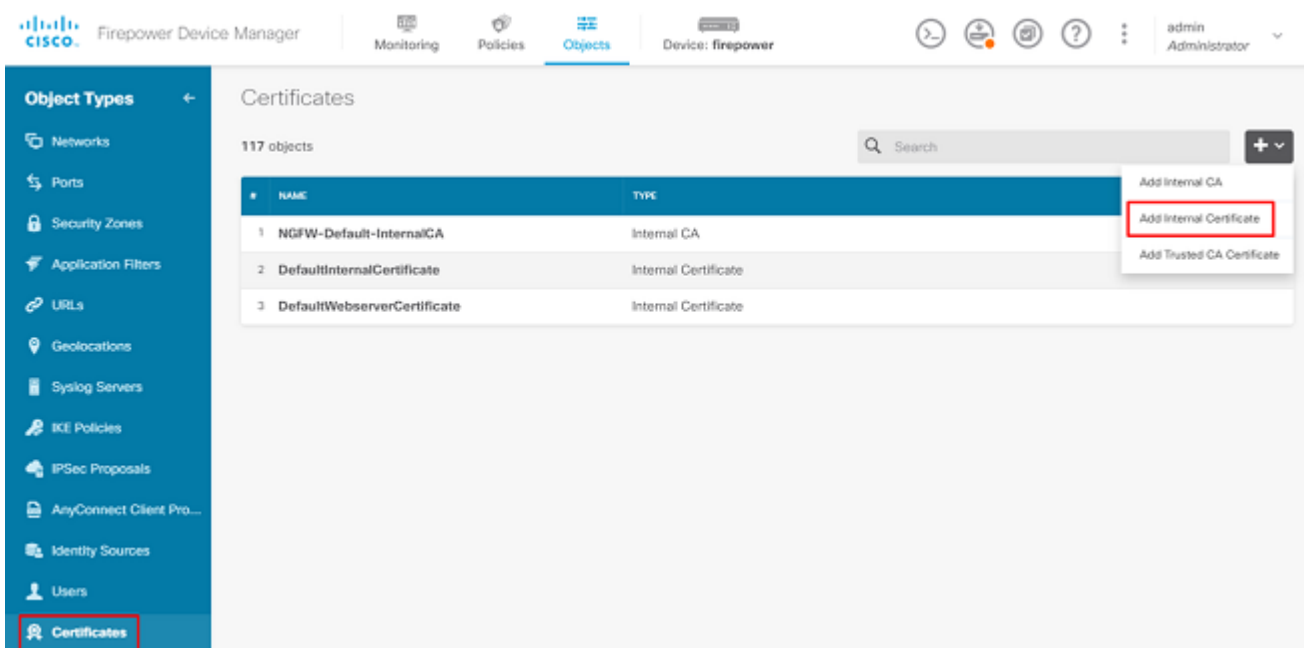
Criar usuários locais

Navegue até Objects > Users > Add User. Adicione usuários do VPN Local que se conectam ao FTD via Anyconnect. Crie usuários locais conforme mostrado na imagem:



Adicionar certificado

Navegue até Objects > Certificates > Add Internal Certificate. Configure um certificado conforme mostrado na imagem:



Carregue o certificado e a chave privada como mostrado na imagem:

Choose the type of internal certificate you want to create



Upload Certificate and Key

Create a certificate from existing files.
PEM and DER files are supported.



Self-Signed Certificate

Create a new certificate that is signed
by the device.

O certificado e a chave podem ser carregados por meio de cópia e colagem ou do botão de carregamento para cada arquivo, como mostrado na imagem:

Add Internal Certificate



Name

Anyconnect_Certificate

SERVER CERTIFICATE (USER AGENT)

Paste certificate, or choose file:

UPLOAD CERTIFICATE

The supported formats are: PEM, DER.

```
wkM7QqtRuyzBzGhnoSebJkP/Hiky/Q+r6UrYSnv++UJSrq777/9NgonwTpLI/8/J  
idGSN0b/ic6iPh2aGpB1Lra3MGCL1pJaRxa3+1vBDsfVFCaKt9wWcnUveQd6LZp  
k+iaN+V24yQj3vCJILlhtxwdllqeSs8F8XdaL4LQObcTfZ/3YNBWqvevV2TL  
-----END CERTIFICATE-----
```

CERTIFICATE KEY

Paste key, or choose file:

UPLOAD KEY

The supported formats are: PEM, DER.

```
QzYPpjkCgYEAgJ9nlk8sfPfmotyQwprlBEdwMMDeKLX3KDY58jiv1/8a/wsX+uz  
3A7VQn6gA6iSWHqxHdmgYnD38P6kCuK/hQMUcadiKUITXkh0ZpglQbfW2lJ0VD4M  
gKugRI5t0Zva5j+bO5q0f8D/mtYYTBf8JGggEfSju0Zsy2ifWtsbJrE=  
-----END RSA PRIVATE KEY-----
```

CANCEL

OK

Configurar a VPN de acesso remoto

Navegue até Remote Access VPN > Create Connection Profile. Navegue pelo Assistente de VPN do RA no FDM como mostrado na imagem:

The image shows two screenshots from the Cisco Firepower Device Manager (FDM) interface. The top screenshot displays the main configuration page for a Cisco Firepower Threat Defense (FTD) device. The 'Remote Access VPN' section is highlighted with a red box, indicating it is configured. The bottom screenshot shows the 'RA VPN' page, which displays a table for Remote Access VPN Connection Profiles. The table is currently empty, and a 'CREATE CONNECTION PROFILE' button is highlighted with a red box, indicating the next step in the configuration process.

Remote Access VPN Configuration Summary:

NAME	AAA	GROUP POLICY	ACTIONS
There are no Remote Access Connections yet. Start by creating the first Connection.			

Crie um perfil de conexão e inicie a configuração conforme mostrado na imagem:

Connection and Client Configuration

Specify how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

Connection Profile Name

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Anyconnect

Group Alias

Anyconnect

[Add Group Alias](#)

Group URL

[Add Group URL](#)

Escolha os métodos de autenticação conforme mostrado na imagem. Este guia usa Autenticação local.

Primary Identity Source

Authentication Type

AAA Only

Client Certificate Only

AAA and Client Certificate

Primary Identity Source for User Authentication

LocalIdentitySource

Fallback Local Identity Source

Please Select Local Identity Source

Strip Identity Source server from username

Strip Group from Username

Secondary Identity Source

Secondary Identity Source for User Authentication

Please Select Identity Source

Advanced

Authorization Server

Please select

Accounting Server

Please select

Escolha o Anyconnect_Pool como mostrado na imagem:

Client Address Pool Assignment

IPv4 Address Pool

Endpoints are provided an address from this pool



Anyconnect_Pool

IPv6 Address Pool

Endpoints are provided an address from this pool



DHCP Servers



CANCEL

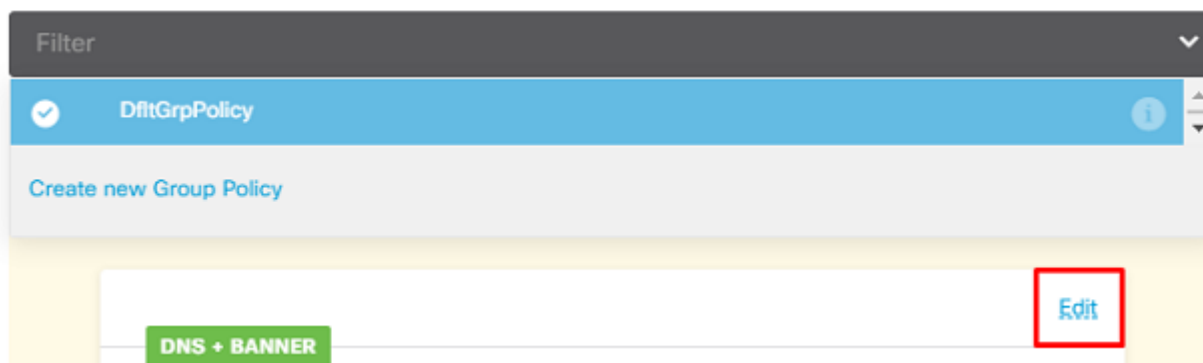
NEXT

Um resumo da Política de Grupo padrão é exibido na próxima página. Uma nova política de grupo pode ser criada quando você pressiona a lista suspensa e escolhe a opção para *Create a new Group Policy*. Para este guia, é usada a Diretiva de Grupo padrão. Escolha a opção de edição na parte superior da política, conforme mostrado na imagem:

Remote User Experience

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

View Group Policy



Na política de grupo, adicione o tunelamento dividido para que os usuários conectados ao Anyconnect enviem apenas o tráfego destinado à rede FTD interna pelo cliente Anyconnect, enquanto todo o tráfego restante sai da conexão do usuário com o ISP, como mostrado na imagem:

Corporate Resources (Split Tunneling)

IPv4 Split Tunneling

Allow specified traffic over tunnel



IPv6 Split Tunneling

Allow all traffic over tunnel



IPv4 Split Tunneling Networks



FDM_Local_Network

Na próxima página, escolha o botão `Anyconnect_Certificate` adicionado na seção de certificado. Em seguida, escolha a interface na qual o FTD escuta as conexões do AnyConnect. Escolha a política Ignorar Controle de Acesso para tráfego descriptografado (`sysopt permit-vpn`). Esse é um comando opcional se o comando `sysopt permit-vpn` não é escolhido. Uma política de controle de acesso deve ser criada para permitir que o tráfego dos clientes do Anyconnect acesse a rede interna como mostrado na imagem:

Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity

Anyconnect_Certificate



Outside Interface

outside (GigabitEthernet0/0)



Fully-qualified Domain Name for the Outside Interface

e.g. `ravpn.example.com`

Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

Bypass Access Control policy for decrypted traffic (`sysopt permit-vpn`)

A isenção de NAT pode ser configurada manualmente em `Policies > NAT` ou pode ser configurado automaticamente pelo assistente. Escolha a interface interna e as redes que os clientes do Anyconnect precisam para acessar, como mostrado na imagem.

NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside (GigabitEthernet0/1)

Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



FDM_Local_Network

Escolha o Pacote do Anyconnect para cada sistema operacional (Windows/Mac/Linux) com o qual os usuários possam se conectar, como mostrado na imagem.

AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from software.cisco.com. You must have the necessary AnyConnect software license.

Packages

UPLOAD PACKAGE

Windows: anyconnect-win-4.7.04056-webdeploy-k9.pkg

BACK

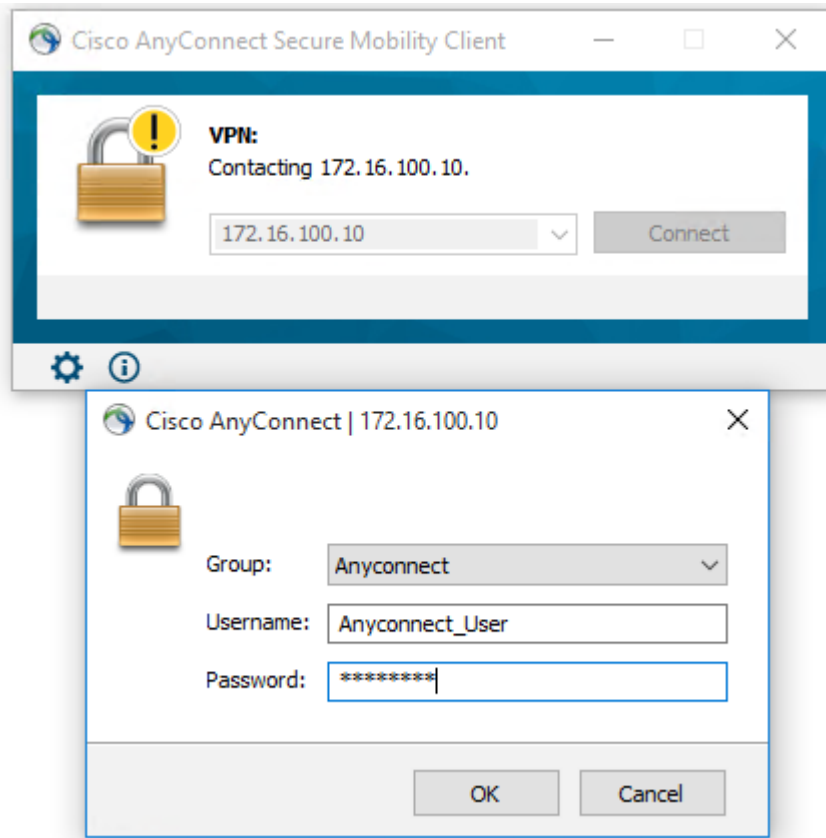
NEXT

A última página fornece um resumo de toda a configuração. Confirme se os parâmetros corretos foram definidos, pressione o botão Finish (Concluir) e implante a nova configuração.

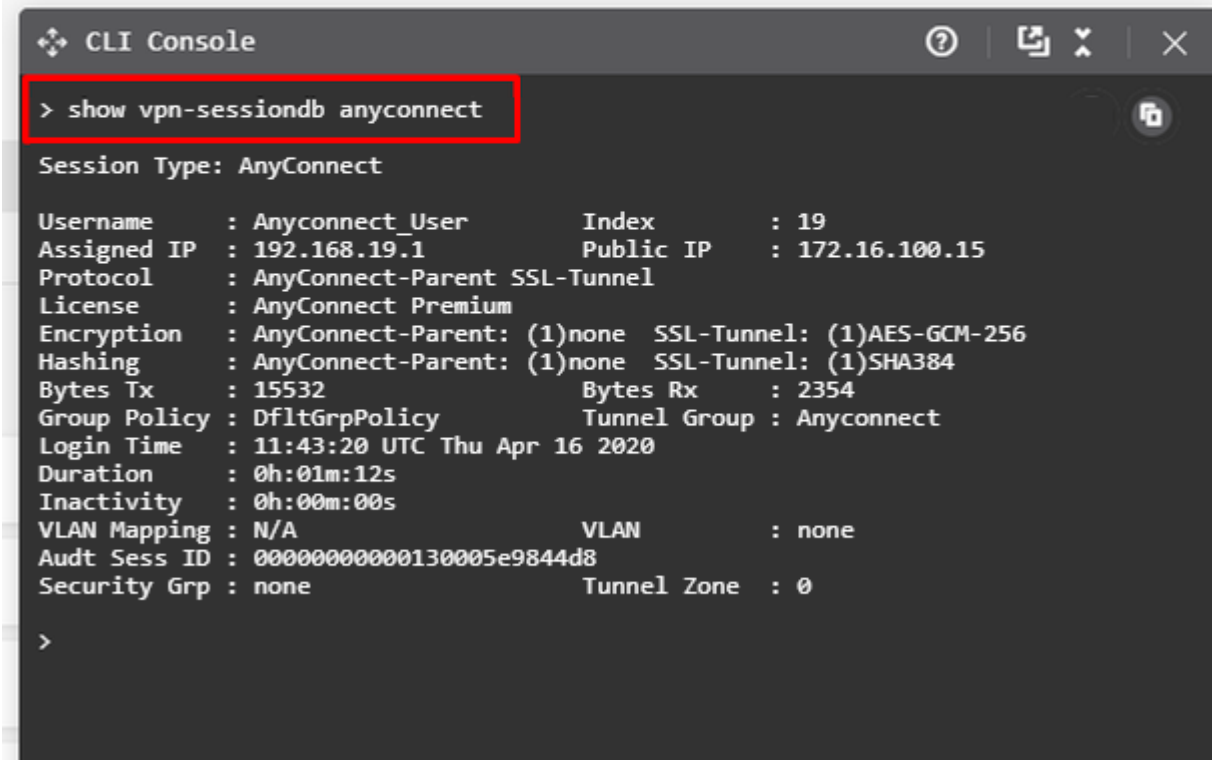
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Após a implantação da configuração, tente se conectar. Se você tiver um FQDN resolvido para o IP externo do FTD, insira-o na caixa de conexão do Anyconnect. Neste exemplo, o endereço IP externo do FTD é usado. Use o nome de usuário/senha criados na seção de objetos do FDM, conforme mostrado na imagem.



A partir do FDM 6.5.0, não há como monitorar os usuários do Anyconnect por meio da GUI do FDM. A única opção é monitorar os usuários do Anyconnect via CLI. O console CLI da GUI do FDM também pode ser usado para verificar se os usuários estão conectados. Use esse comando, `Show vpn-sessiondb anyconnect`.



O mesmo comando pode ser executado diretamente do CLI.

```
> show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

```
Username      : Anyconnect_User      Index      : 15
Assigned IP   : 192.168.19.1         Public IP  : 172.16.100.15
Protocol      : AnyConnect-Parent SSL-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx      : 38830                Bytes Rx   : 172
Group Policy  : DfltGrpPolicy        Tunnel Group : Anyconnect
Login Time    : 01:08:10 UTC Thu Apr 9 2020
Duration      : 0h:00m:53s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                  VLAN       : none
Audt Sess ID  : 000000000000f0005e8e757a
Security Grp  : none                  Tunnel Zone : 0
```

Troubleshooting

Esta seção fornece as informações que você pode usar para solucionar problemas da sua configuração.

Se um usuário não conseguir se conectar ao FTD com SSL, execute estas etapas para isolar os problemas de negociação de SSL:

1. Verifique se o endereço IP fora do FTD pode receber ping através do computador do usuário.
2. Use um farejador externo para verificar se o handshake triplo do TCP é bem-sucedido.

Problemas do AnyConnect Client

Esta seção fornece diretrizes para solucionar os dois problemas mais comuns do AnyConnect VPN Client. Um guia de solução de problemas para o AnyConnect Client pode ser encontrado aqui: [AnyConnect VPN Client Troubleshooting Guide](#).

Problemas iniciais de conectividade

Se um usuário tiver problemas de conectividade inicial, habilite o comando debug `webvpn AnyConnect` no FTD e analisar as mensagens de depuração. As depurações devem ser executadas no CLI do FTD. Use o comando `debug webvpn anyconnect 255`.

Colete um pacote DART da máquina cliente para obter os logs do AnyConnect. As instruções sobre como coletar um pacote DART podem ser encontradas aqui: [Collecting DART bundles](#).

Problemas específicos de tráfego

Se uma conexão tiver êxito, mas o tráfego falhar no túnel VPN SSL, examine as estatísticas de tráfego no cliente para verificar se o tráfego está sendo recebido e transmitido pelo cliente. Estatísticas detalhadas de clientes estão disponíveis em todas as versões do AnyConnect. Se o cliente mostrar que o tráfego está sendo enviado e recebido, verifique o FTD para o tráfego recebido e transmitido. Se o FTD aplicar um filtro, o nome do filtro será mostrado e você poderá examinar as entradas da ACL para verificar se o tráfego está sendo descartado. Os problemas comuns de tráfego enfrentados pelos usuários são:

- Problemas de roteamento por trás do FTD - a rede interna não consegue rotear pacotes de volta para os endereços IP e clientes VPN atribuídos
- Listas de controle de acesso bloqueando o tráfego
- A conversão de endereço de rede não está sendo ignorada para o tráfego VPN

Para obter mais informações sobre VPNs de acesso remoto no FTD gerenciado pelo FDM, consulte o guia de configuração completo aqui: [FTD de Acesso Remoto gerenciado pelo FDM](#).

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.