Exemplo de configuração de cliente FlexVPN e Anyconnect IKEv2

Contents

Introduction

Este documento descreve como configurar o Cisco AnyConnect Secure Mobility Client para usar o Remote Authentication Dial-In User Service (RADIUS) e atributos de autorização local para autenticar no Microsoft Ative Diretory.

> **Note**: Atualmente, o uso do banco de dados de usuário local para autenticação não funciona em dispositivos Cisco IOS®. Isso porque o Cisco IOS não funciona como um autenticador EAP. Solicitação de aprimoramento CSCui07025 foi arquivada para adicionar suporte.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco IOS versão 15.2(T) ou posterior
- Cisco AnyConnect Secure Mobility Client versão 3.0 ou posterior
- Microsoft Ative Diretory

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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

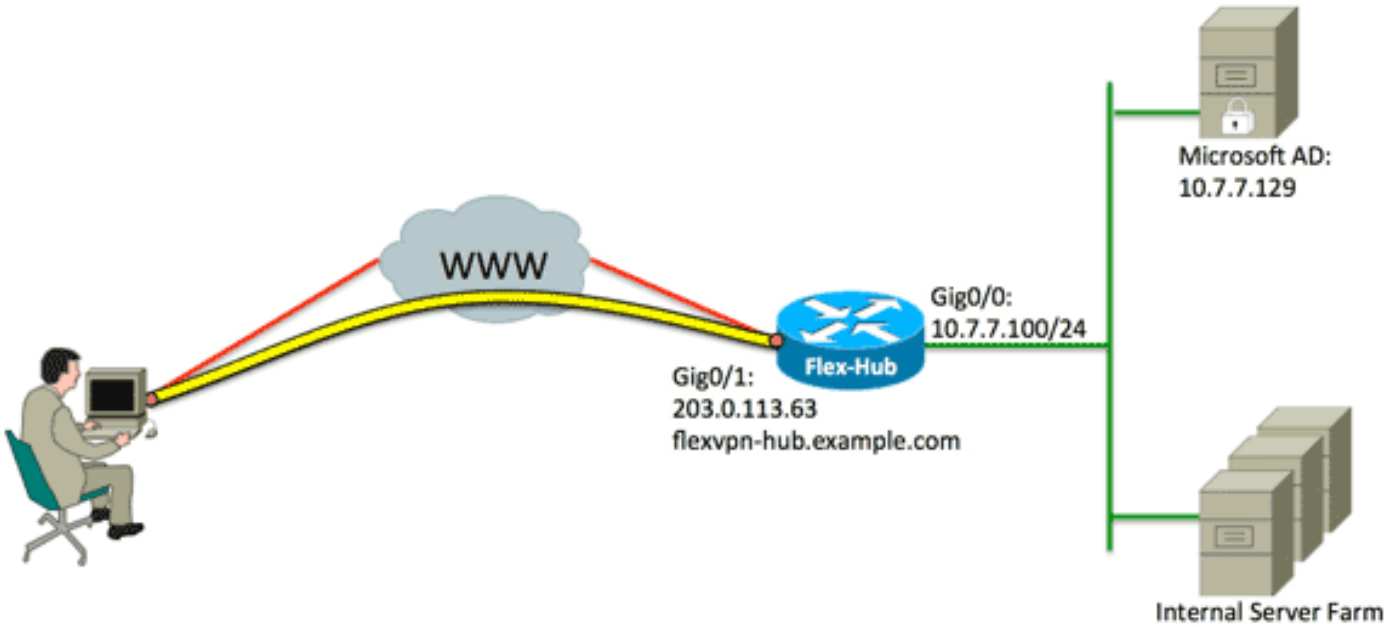
Configurar

Nesta seção, você verá informações sobre a configuração dos recursos descritos neste documento.

Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- Configuração do hub
- Configuração do Microsoft Ative Diretory Server
- Configuração do Cliente

Configuração do hub

1. Configure o RADIUS somente para autenticação e defina a autorização local.

```
aaa new-model
aaa group server radius FlexVPN-AuthC-Server-Group-1
server-private 10.7.7.129 key Cisco123
aaa authentication login FlexVPN-AuthC-List-1 group
FlexVPN-AuthC-Server-Group-1
aaa authorization network FlexVPN-AuthZ-List-1 local
```

   O comando **aaa authentication login list** se refere ao grupo de autenticação, autorização e contabilização (AAA) (que define o servidor RADIUS). O comando **aaa authorization network list** afirma que os usuários/grupos definidos localmente devem ser usados. A configuração no servidor RADIUS deve ser alterada para permitir solicitações de autenticação deste dispositivo.

2. Configure a política de autorização local.

```
ip local pool FlexVPN-Pool-1 10.8.8.100 10.8.8.200
crypto ikev2 authorization policy FlexVPN-Local-Policy-1
pool FlexVPN-Pool-1
dns 10.7.7.129
netmask 255.255.255.0
def-domain example.com
```

   O comando **ip local pool** é usado para definir os endereços IP atribuídos ao cliente. Uma política de autorização é definida com um nome de usuário de *FlexVPN-Local-Policy-1*, e os atributos para o cliente (servidores DNS, máscara de rede, lista dividida, nome de domínio e assim por diante) são configurados aqui.

3. Verifique se o servidor usa um certificado (rsa-sig) para se autenticar.

   O Cisco AnyConnect Secure Mobility Client exige que o servidor se autentique usando um certificado (rsa-sig). O roteador deve ter um certificado *do servidor web* (ou seja, um certificado com 'autenticação do servidor' dentro da extensão de uso da chave estendida) de uma autoridade de certificação (AC) confiável.

   Consulte as etapas de 1 a 4 no ASA 8.x Instalar manualmente certificados de terceiros para uso com o exemplo de configuração de WebVPN e altere todas as instâncias de *crypto ca* para *crypto pki*.

```
crypto pki trustpoint FlexVPN-TP-1
enrollment url
```

```
serial-number none
fqdn flex-hub.example.com
ip-address none
subject-name cn=flex-hub.example.com
revocation-check crl
rsakeypair FlexVPN-TP-1-Key 2048
```

4. Defina as configurações para esta conexão.

```
crypto ikev2 profile FlexVPN-IKEv2-Profile-1
match identity remote key-id example.com
identity local dn
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint FlexVPN-TP-1
dpd 60 2 on-demand
aaa authentication eap FlexVPN-AuthC-List-1
aaa authorization group eap list FlexVPN-AuthZ-List-1
FlexVPN-Local-Policy-1
virtual-template 10
```

O perfil **crypto ikev2** contém a maioria das configurações relevantes para esta conexão: **match identity remote key-id** - Refere-se à identidade IKE usada pelo cliente. Esse valor de string é configurado no perfil XML do AnyConnect.**identity local dn** - Define a identidade IKE usada pelo hub FlexVPN. Esse valor usa o valor de dentro do certificado usado.**authentication remote** - Indica que o EAP deve ser usado para autenticação de cliente.**authentication local** - Indica que os certificados devem ser usados para autenticação local.**aaa authentication eap** - Estados para usar a lista de login de autenticação AAA FlexVPN-AuthC-List-1 quando EAP é usado para autenticação.**aaa group eap list** - estados para usar a lista de rede de autorização FlexVPN-AuthZ-List-1 com o nome de usuário de *FlexVPN-Local-Policy-1* para atributos de autorização.**virtual-template 10** - Define qual modelo usar quando uma interface de acesso virtual é clonada.

5. Configure um perfil de IPsec que se conecte de volta ao perfil de IKEv2 definido na etapa 4.

```
crypto ipsec profile FlexVPN-IPsec-Profile-1
set ikev2-profile FlexVPN-IKEv2-Profile-1
```

Note: O Cisco IOS utiliza Smart Defaults. Como resultado, um conjunto de transformações não precisa ser explicitamente definido.

6. Configure o modelo virtual a partir do qual as interfaces de acesso virtual são clonadas: **ip unnumbered -** Desnumere a interface de uma interface *interna* para que o roteamento IPv4 possa ser ativado na interface.**tunnel mode ipsec ipv4 -** Define a interface como sendo um túnel do tipo VTI.

```
interface Virtual-Template10 type tunnel
ip unnumbered GigabitEthernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

7. Limite a negociação a SHA-1. (Opcional)

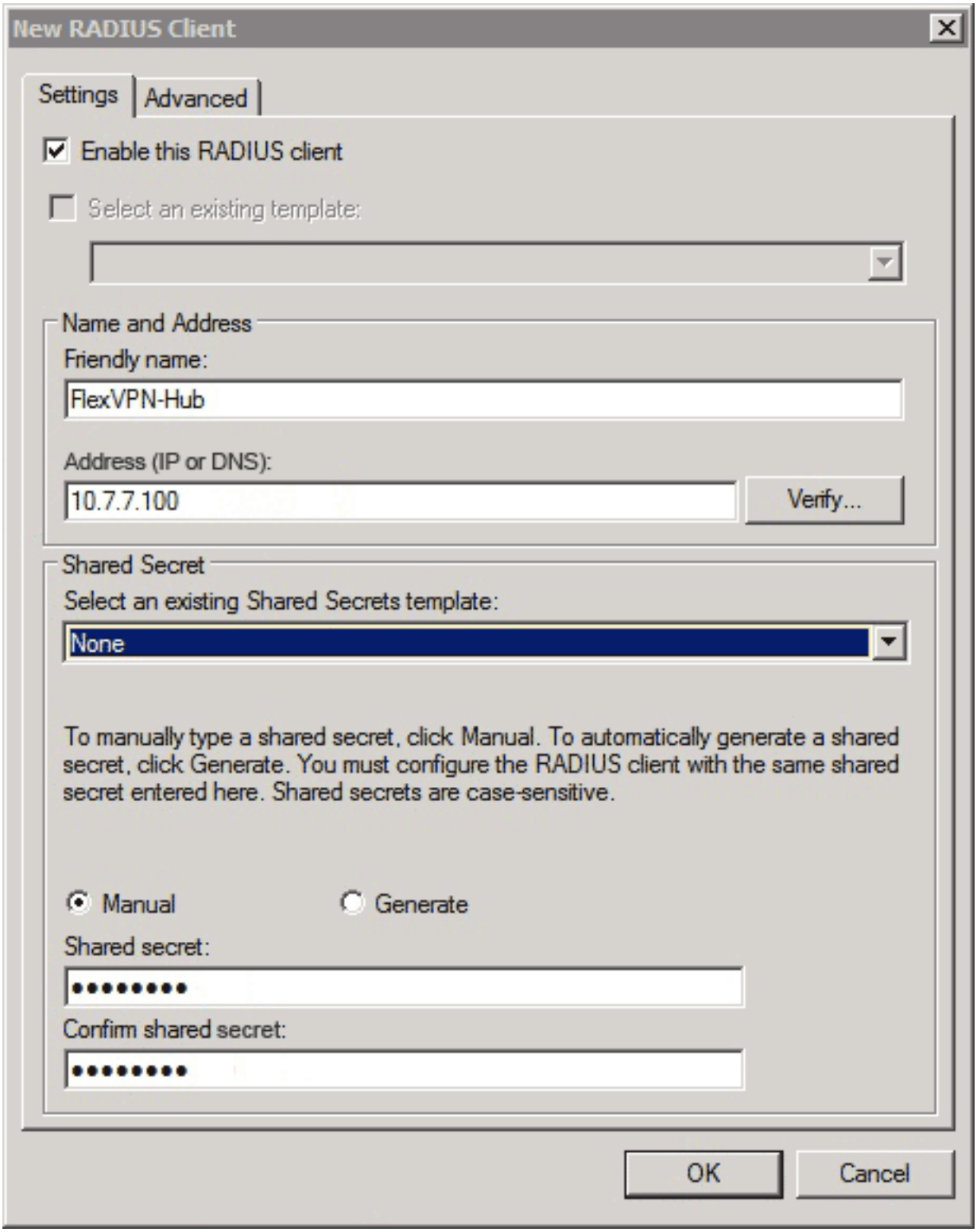
Devido ao defeito CSCud96246 (somente clientes registrados) , o cliente AnyConnect pode falhar ao validar corretamente o certificado do FlexVPN Hub. Esse problema é devido ao IKEv2 negociando uma função SHA-2 para a função pseudo-aleatória (PRF), enquanto o certificado FlexVPN-Hub foi assinado usando SHA-1. A configuração abaixo limita a negociação para SHA-1:

```
crypto ikev2 proposal SHA1-only
encryption aes-cbc-256
integrity sha1
group 5
crypto ikev2 policy SHA1-only
match fvrf any
proposal SHA1-only
```

Configuração do Microsoft Ative Diretory Server

1. No Windows Server Manager, expanda **Funções > Política de Rede e Servidor de Acesso > NMPS (Local) > Clientes e Servidores RADIUS** e clique em **Clientes RADIUS**.

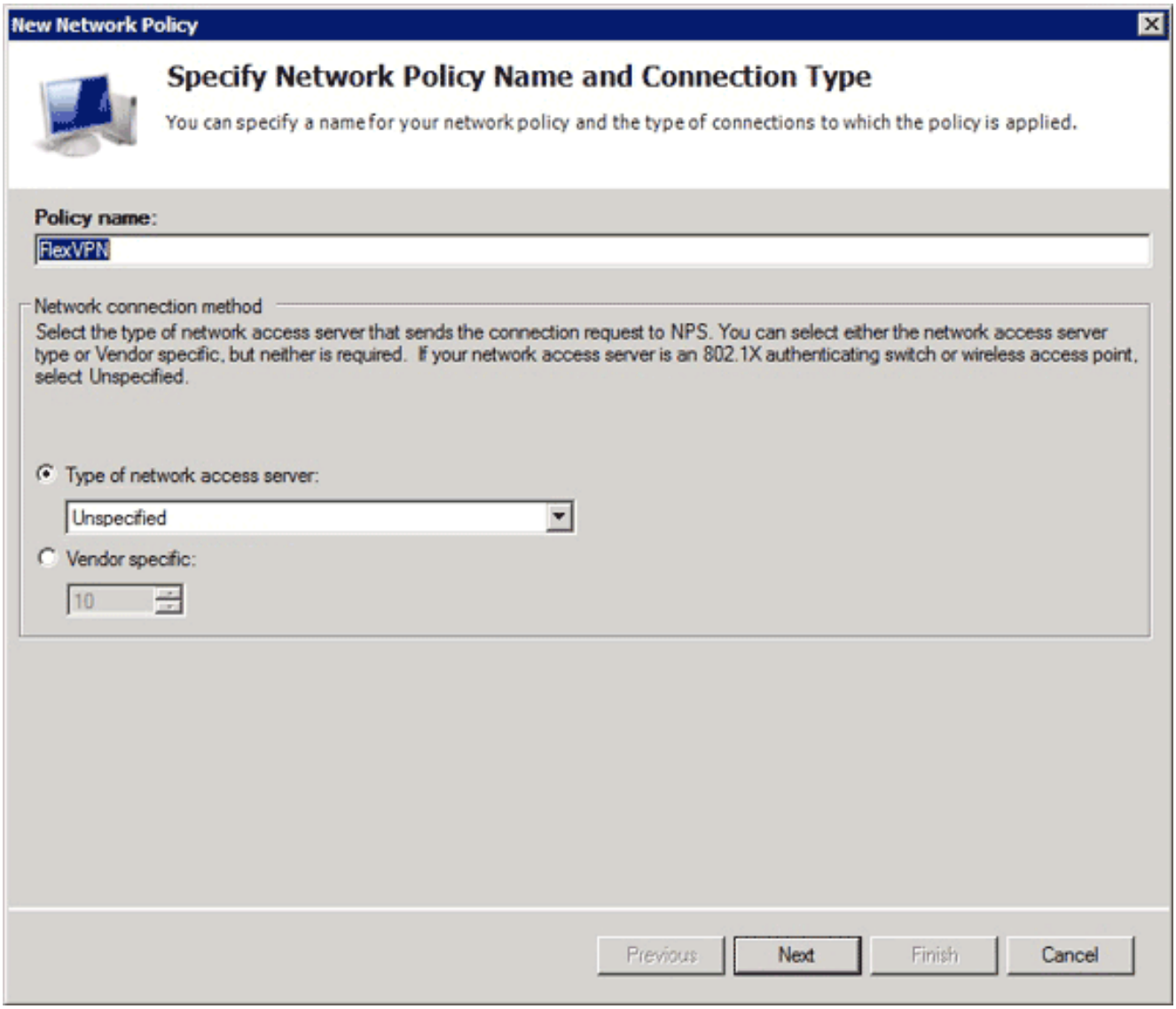
   A caixa de diálogo Novo cliente RADIUS é exibida.



2. Na caixa de diálogo Novo cliente RADIUS, adicione o roteador Cisco IOS como um cliente RADIUS:
   Clique na caixa de seleção **Enable this RADIUS client**.Digite um nome no campo Nome amigável. Este exemplo usa *FlexVPN-Hub*.Insira o endereço IP do roteador no campo Address (Endereço).Na área Shared Secret, clique no botão de opção **Manual** e insira o segredo compartilhado nos campos Shared secret e Confirm shared secret.**Observação:** o segredo compartilhado deve corresponder ao segredo compartilhado configurado no roteador.Click OK.

3. Na interface do Server Manager, expanda **Policies** e escolha **Network Policies**.

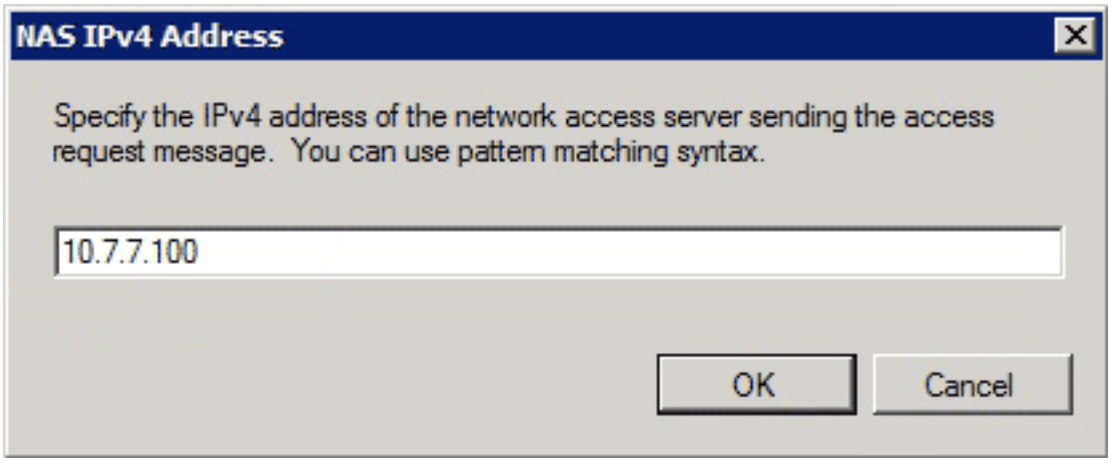
A caixa de diálogo Nova política de rede é exibida.



4. Na caixa de diálogo Nova política de rede, adicione uma nova política de rede:

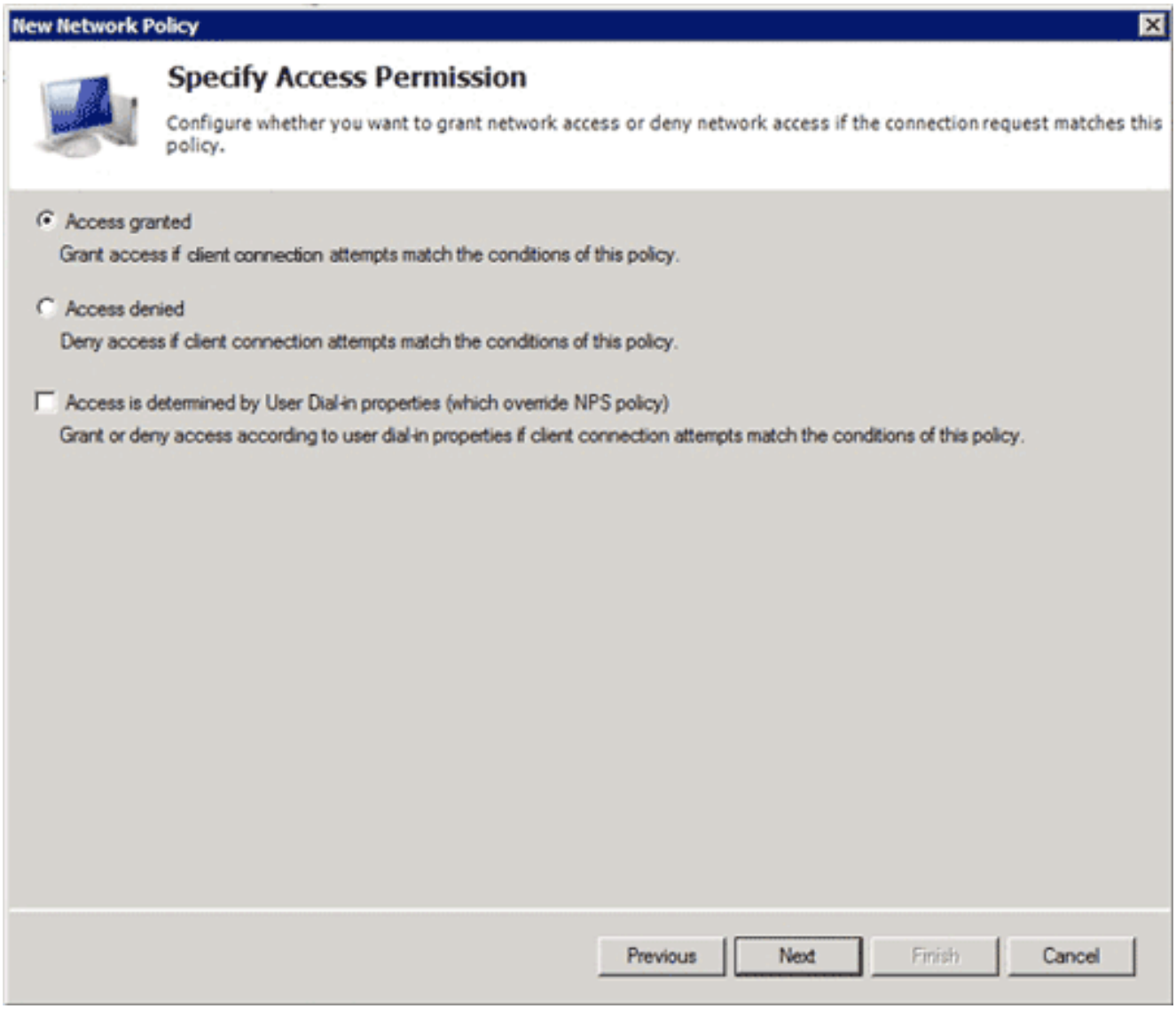
   Insira um nome no campo Nome da política. Este exemplo usa *FlexVPN*.Clique no botão de opção **Tipo de servidor de acesso à rede** e escolha **Não especificado** na lista suspensa.Clique em Next.Na caixa de diálogo Nova diretiva de rede, clique em **Adicionar** para adicionar uma nova condição.Na caixa de diálogo Selecionar condição, selecione a condição **de endereço IPv4 do NAS** e clique em **Adicionar**.

   A caixa de diálogo Endereço IPv4 do NAS é exibida.



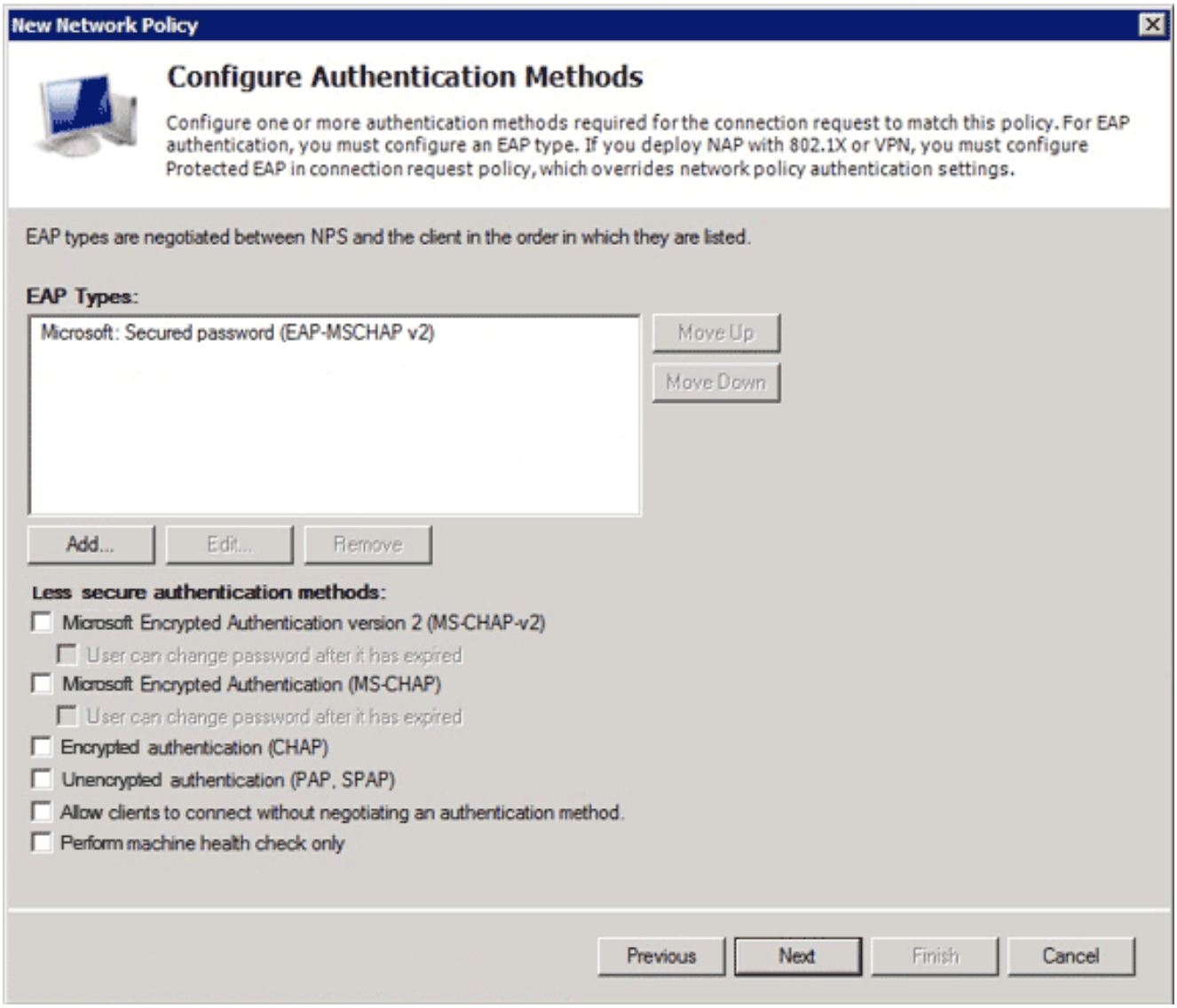
Na caixa de diálogo Endereço IPv4 do NAS, insira o endereço IPv4 do servidor de acesso à rede para limitar a política de rede somente às solicitações originadas desse roteador Cisco IOS.

Click OK.



Na caixa de diálogo Nova política de rede, clique no botão de opção **Acesso concedido** para permitir que o cliente acesse a rede (se as credenciais fornecidas pelo usuário forem

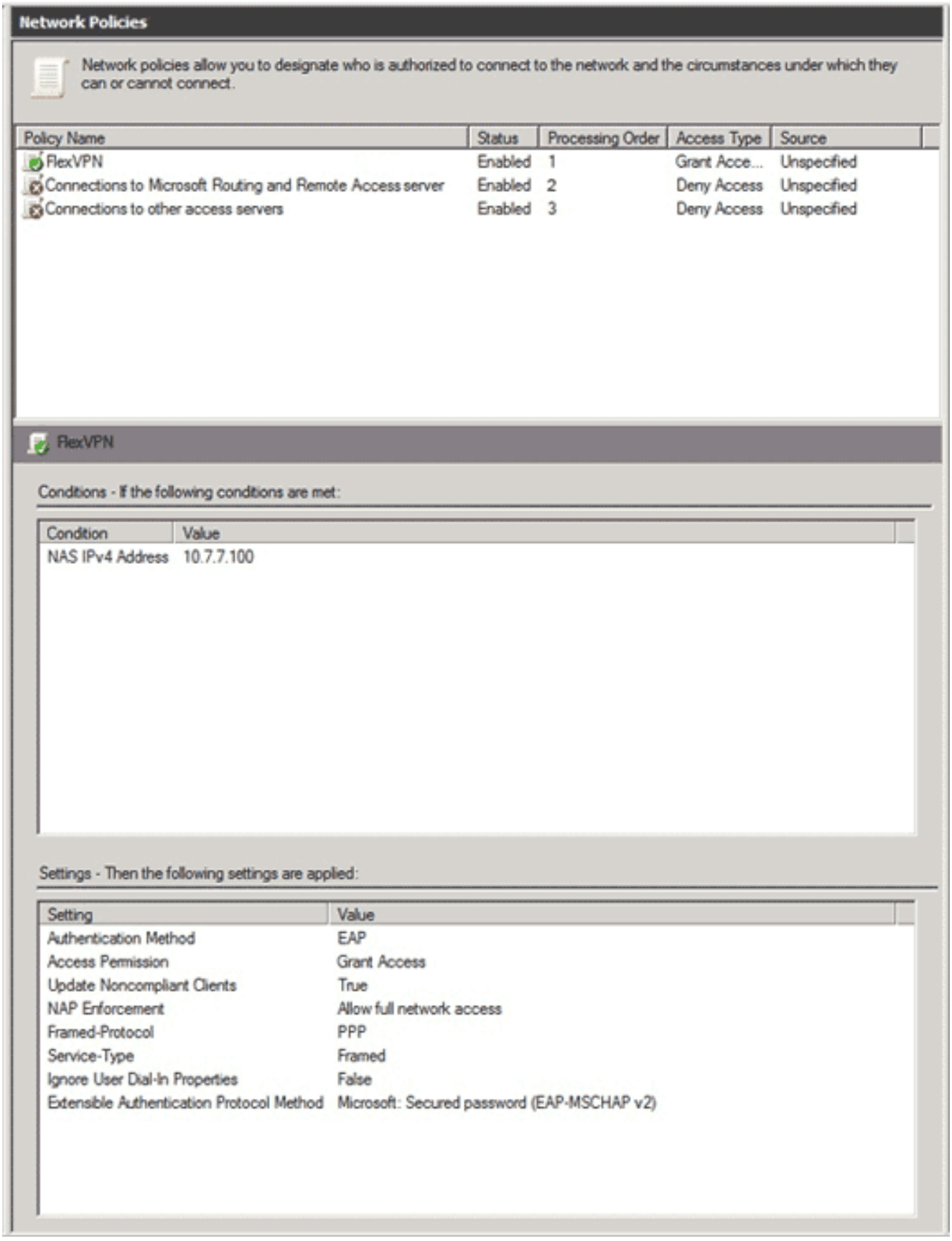
válidas) e clique em **Avançar**.



Certifique-se apenas da Microsoft: A senha segura (EAP-MSCHAP v2) é exibida na área EAP Types para permitir que EAP-MSCHAPv2 seja usado como o método de comunicação entre o dispositivo IOS Cisco e o Ative Diretory e clique em **Next**.

Note: Deixe todas as opções de 'Métodos de autenticação menos seguros' desmarcadas.

Continue no assistente e aplique quaisquer restrições ou configurações adicionais conforme definido pela política de segurança da sua empresa. Além disso, certifique-se de que a política esteja listada primeiro na ordem de processamento, conforme mostrado nesta imagem:



Configuração do Cliente

1. Crie um perfil XML em um editor de texto e nomeie-o *flexvpn.xml*.

Este exemplo usa este perfil XML:

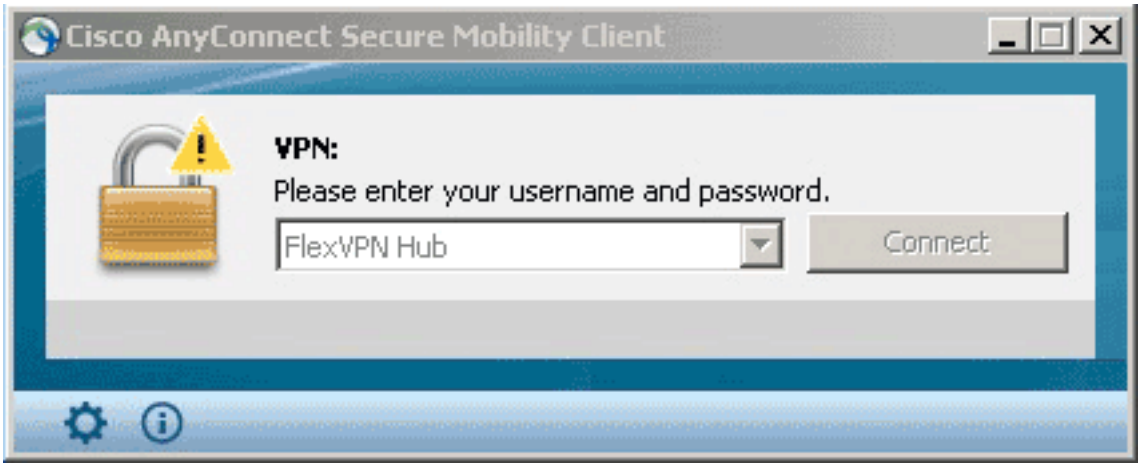
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false
</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true
</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true
</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false
</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true
</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false
</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">false
</ClearSmartcardPin>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="true">false</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
Automatic
</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon
</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly
</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false">
</PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="true">true
<TerminateScriptOnNextEvent>true
</TerminateScriptOnNextEvent>
<EnablePostSBLOnConnectScript>true
</EnablePostSBLOnConnectScript>
</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20
</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4
</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
<ServerList>
<HostEntry>
```

```
<HostName>FlexVPN Hub</HostName>
<HostAddress>flexvpn-hub.example.com</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>EAP-MSCHAPv2</AuthMethodDuringIKENegotiation>
<IKEIdentity>example.com</IKEIdentity>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

<HostName> é uma cadeia de caracteres de texto que aparece no cliente.<HostAddress> é o nome de domínio totalmente qualificado (FQDN) do hub FlexVPN.<PrimaryProtocol> configura a conexão para usar IKEv2/IPsec em vez de SSL (o padrão no AnyConnect).<AuthMethodDuranteIKENegotiation> configura a conexão para usar MSCHAPv2 dentro do EAP. Este valor é necessário para autenticação no Microsoft Ative Diretory.<IKEIdentity> define o valor da cadeia de caracteres que corresponde o cliente a um perfil IKEv2 específico no hub (consulte a etapa 4 acima).
Note: O perfil do cliente é algo usado somente pelo cliente. Recomenda-se que um administrador use o editor do Anyconnect Profile para criar o perfil do cliente.

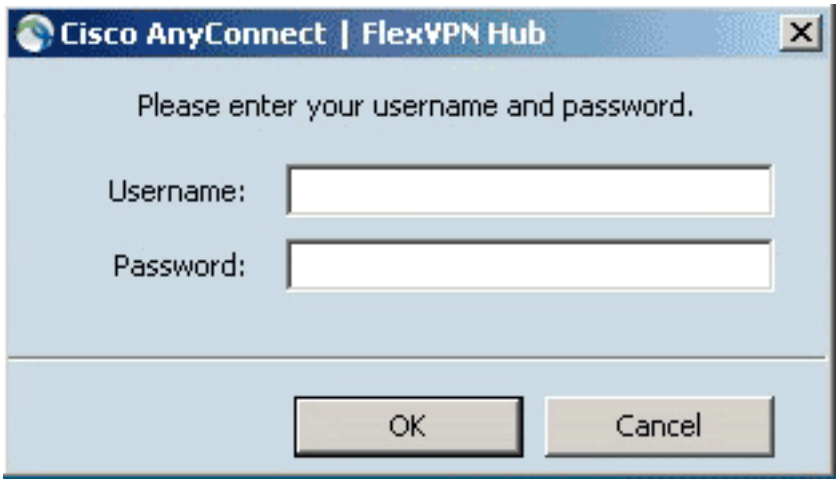
2. Salve o arquivo flexvpn.xml no diretório apropriado conforme listado nesta tabela:

3. Feche e reinicie o cliente AnyConnect.



4. Na caixa de diálogo Cisco AnyConnect Secure Mobility Client, escolha **FlexVPN Hub** e clique em **Connect**.

   O Cisco AnyConnect | A caixa de diálogo FlexVPN Hub é exibida.



5. Digite um nome de usuário e uma senha e clique em **OK**.

Verificar

Para verificar a conexão, use o comando **show crypto session detail remote client-ipaddress**. Consulte show crypto session para obter mais informações sobre esse comando.

> **Note**: A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Troubleshoot

Para solucionar problemas de conexão, colete e analise registros DART do cliente e use esses comandos debug no roteador: **debug crypto ikev2 packet** e **debug crypto ikev2 internal**.

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems