Exemplo da configuração de cliente de FlexVPN e de Anyconnect IKEv2

Índice

Introdução

Este documento descreve como configurar o Cliente de mobilidade Cisco AnyConnect Secure para usar o Remote Authentication Dial-In User Service (RADIUS) e os atributos da autorização local a fim autenticar contra o microsoft ative directory.

> Nota: Atualmente, o uso da base de dados de usuário local para a autenticação não funciona em dispositivos do ® do Cisco IOS. Isto é porque o Cisco IOS não funciona como um autenticador EAP. A requisição de aprimoramento CSCui07025 foi arquivada adicionar o apoio.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Versão do Cisco IOS 15.2(T) ou mais atrasado
- Versão 3.0 ou mais recente do Cliente de mobilidade Cisco AnyConnect Secure
- Microsoft ative directory

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

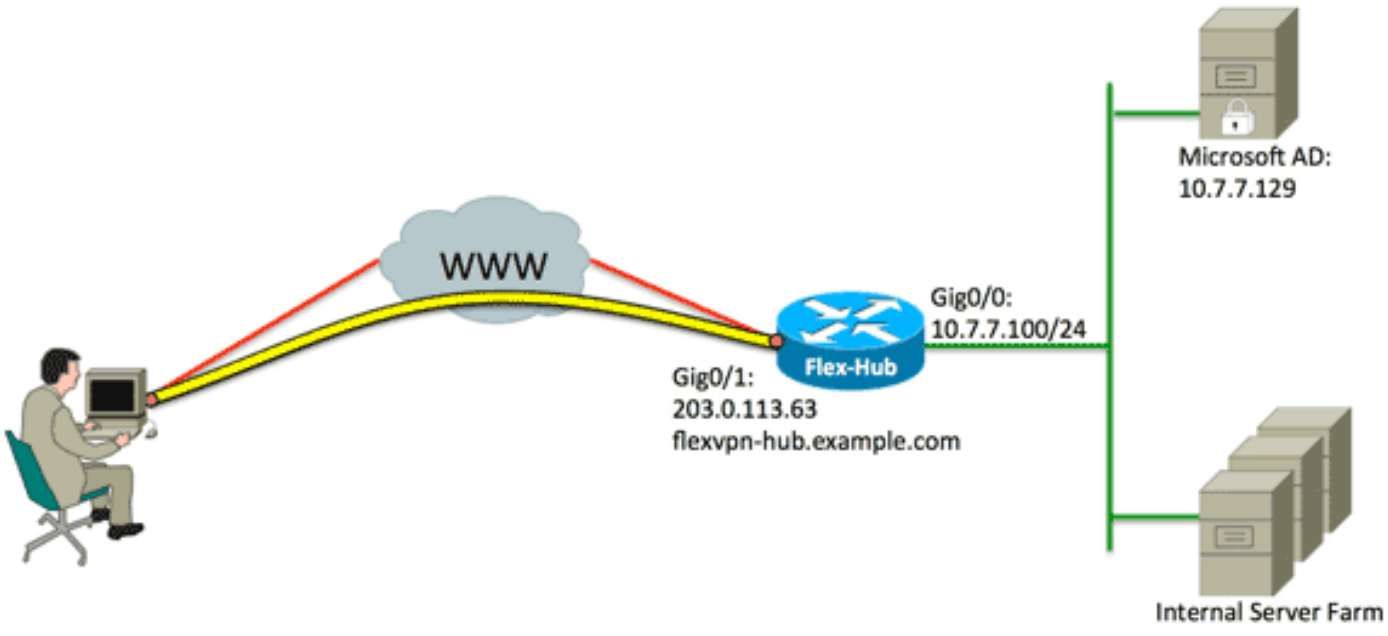
Configurar

Nesta seção, você é presentado com a informação a fim configurar as características descritas 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 servidor do microsoft ative directory
- Configuração do Cliente

Configuração do hub

1. Configurar o RADIUS de autenticação somente 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 list da autentificação de login aaa refere o grupo do Authentication, Authorization, and Accounting (AAA) (que define o servidor Radius). Os estados de **comando list da rede de autorização AAA** que definiram localmente usuários/grupos devem ser usada. A configuração no servidor Radius deve ser mudada para permitir pedidos de autenticação deste dispositivo.

2. Configurar a política da 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 definir os endereços IP de Um ou Mais Servidores Cisco ICM NT que são atribuídos ao cliente. Uma política da autorização é definida com um username de *FlexVPN-Local-Policy-1*, e os atributos para o cliente (servidores DNS, netmask, lista rachada, Domain Name, e assim por diante) são configurados aqui.

3. Assegure-se de que o server use um certificado (RSA-SIG) a fim se autenticar.

   O Cliente de mobilidade Cisco AnyConnect Secure exige que o server se autentica que usa um certificado (RSA-SIG). O roteador deve ter um certificado do *servidor de Web* (isto é, um certificado com “autenticação de servidor” dentro da extensão chave prolongada do uso) de um Certificate Authority (CA) confiado.

   Refira etapas 1 a 4 em ASA 8.x instalam manualmente Certificados do vendedor da 3ª parte para o uso com exemplo de configuração WebVPN, e mudam todos os exemplos do *Ca cripto ao pki cripto*.

```
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. Configurar ajustes 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
```
Os ontains **criptos do profilec ikev2** mais dos ajustes relevantes para esta conexão: **chave-identificação remota da identidade do fósforo** - Refere a identidade IKE usada pelo cliente. Este valor de série é configurado dentro do perfil de AnyConnect XML.**identidade dn local** - Define a identidade IKE usada pelo hub de FlexVPN. Este valor usa o valor de dentro do certificado usado.**telecontrole da autenticação** - Estados que o EAP deve ser usado para a authenticação do cliente.**os estados locais da autenticação** que os Certificados devem ser usados para o local autenticam.**eap da autenticação aaa** - Estados para usar a lista FlexVPN-AuthC-List-1 da autentificação de login aaa quando o EAP for usado para a autenticação.**lista do eap do grupo da autorização aaa** - Estados para usar a lista FlexVPN-AuthZ-List-1 da rede de autorização AAA com o username de *FlexVPN-Local-Policy-1* para atributos da autorização.**virtual-molde 10** - Define que molde a se usar quando uma interface de acesso virtual for clonada.

5. Configurar um perfil IPSec que ligue de volta ao perfil IKEv2 definido em etapa 4.
```
crypto ipsec profile FlexVPN-IPsec-Profile-1
set ikev2-profile FlexVPN-IKEv2-Profile-1
```
Nota: O Cisco IOS utiliza padrões espertos. Em consequência, um grupo da transformação não precisa de ser definido explicitamente.

6. Configurar o molde virtual de que as interfaces de acesso virtual são clonadas:
IP unnumbered - Unnumber a relação de uma distribuição da *interface interna* assim que do IPv4 pode ser permitido na relação.**IPv4 do IPsec do modo de túnel -** Define a relação para ser um tipo túnel 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 ao SHA-1. (Opcional)

   Devido defect CSCud96246 (clientes registrados somente), o cliente de AnyConnect pôde não valida corretamente o certificado do hub de FlexVPN. Esta edição é devido a IKEv2 que negocia uma função SHA-2 para a função Pseudo--aleatória (PRF) visto que o certificado do FlexVPN-hub foi assinado usando o SHA-1. Os limites abaixo da configuração a negociação ao SHA-1:

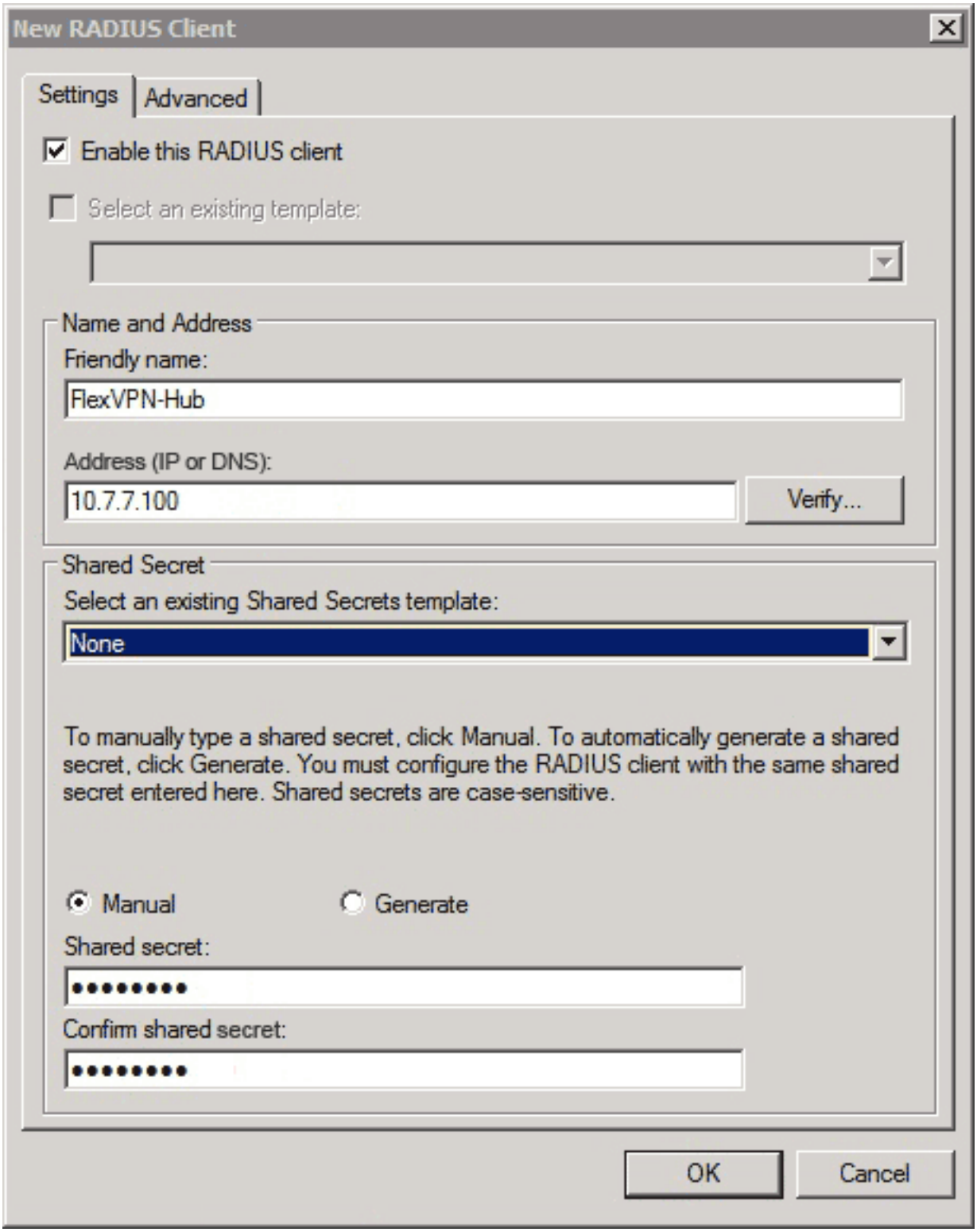
```
crypto ikev2 proposal SHA1-only
encryption aes-cbc-256
```

```
integrity sha1
group 5
crypto ikev2 policy SHA1-only
match fvrf any
proposal SHA1-only
```

Configuração do servidor do microsoft ative directory

1. No gerente de Windows Server, expanda **papéis > política de rede e servidor de acesso > NMP (locais) > clientes RADIUS e server**, e clique **clientes RADIUS**.

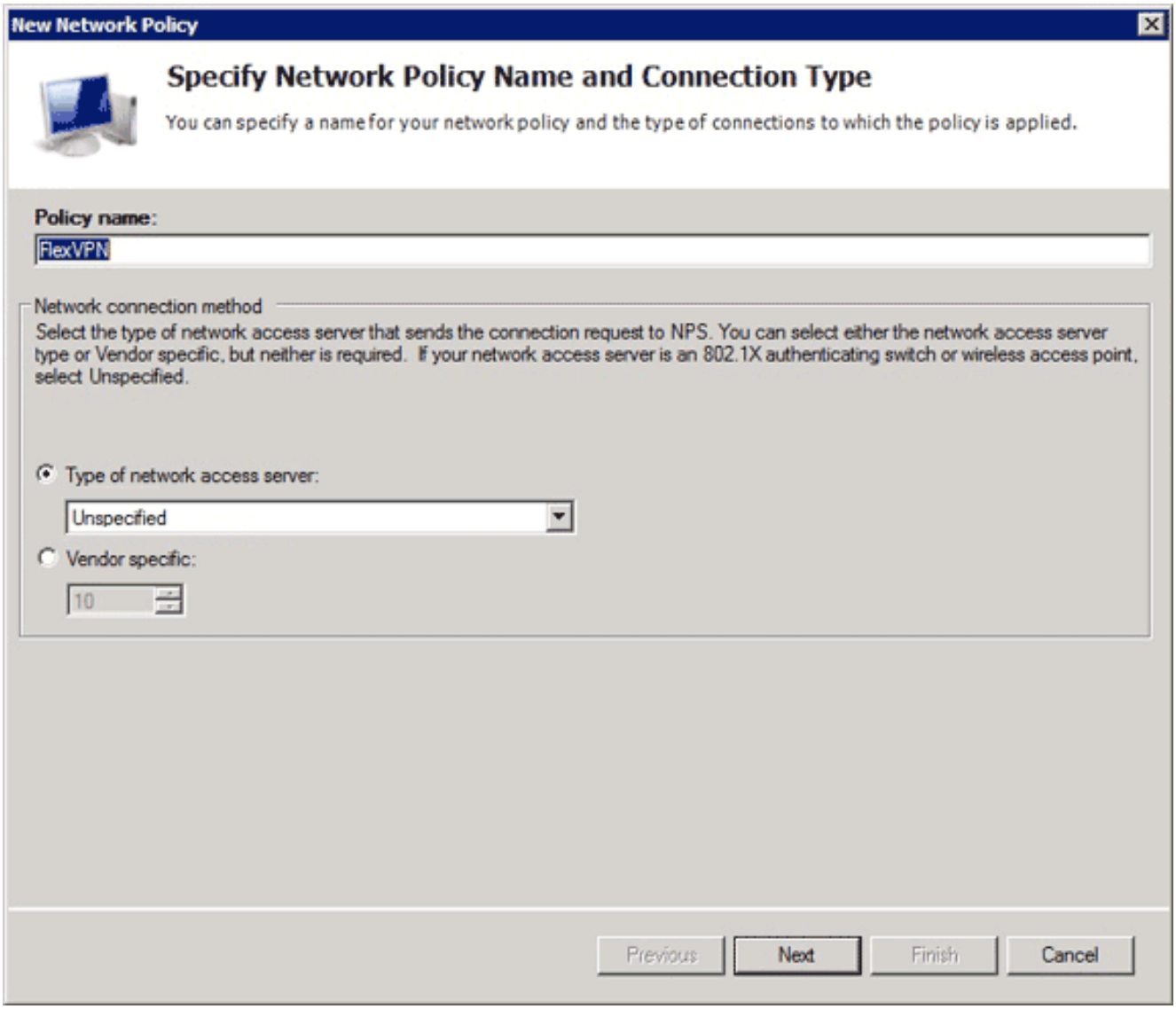
   A caixa de diálogo nova do cliente RADIUS aparece.



2. Na caixa de diálogo nova do cliente RADIUS, adicionar o roteador do Cisco IOS como um cliente RADIUS:
   Clique a **possibilidade esta** caixa de verificação do **cliente RADIUS**.Dê entrada com um nome no campo de nome amigável. Este exemplo usa o FlexVPN-*hub*.Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do roteador ao campo de endereço.Na área secreta compartilhada, clique o botão de rádio **manual**, e incorpore o segredo compartilhado ao segredo compartilhado e aos campos secretos compartilhados Confirm.**Nota:** O segredo compartilhado deve combinar o segredo compartilhado configurado no roteador.Clique em **OK**.

3. Na relação do gerenciador do servidor, expanda **políticas**, e escolha **políticas de rede**.

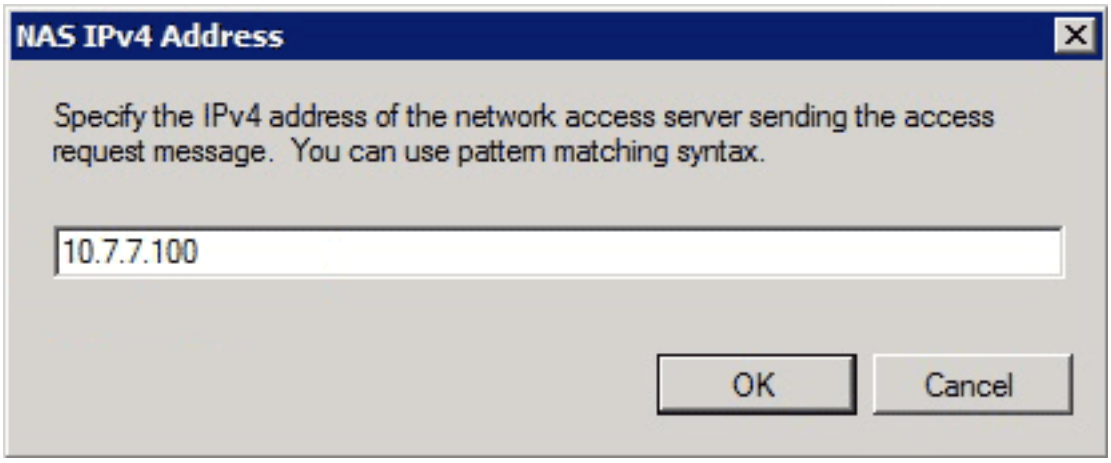
A caixa de diálogo nova da política de rede aparece.



4. Na caixa de diálogo nova da política de rede, adicionar uma política de rede nova:

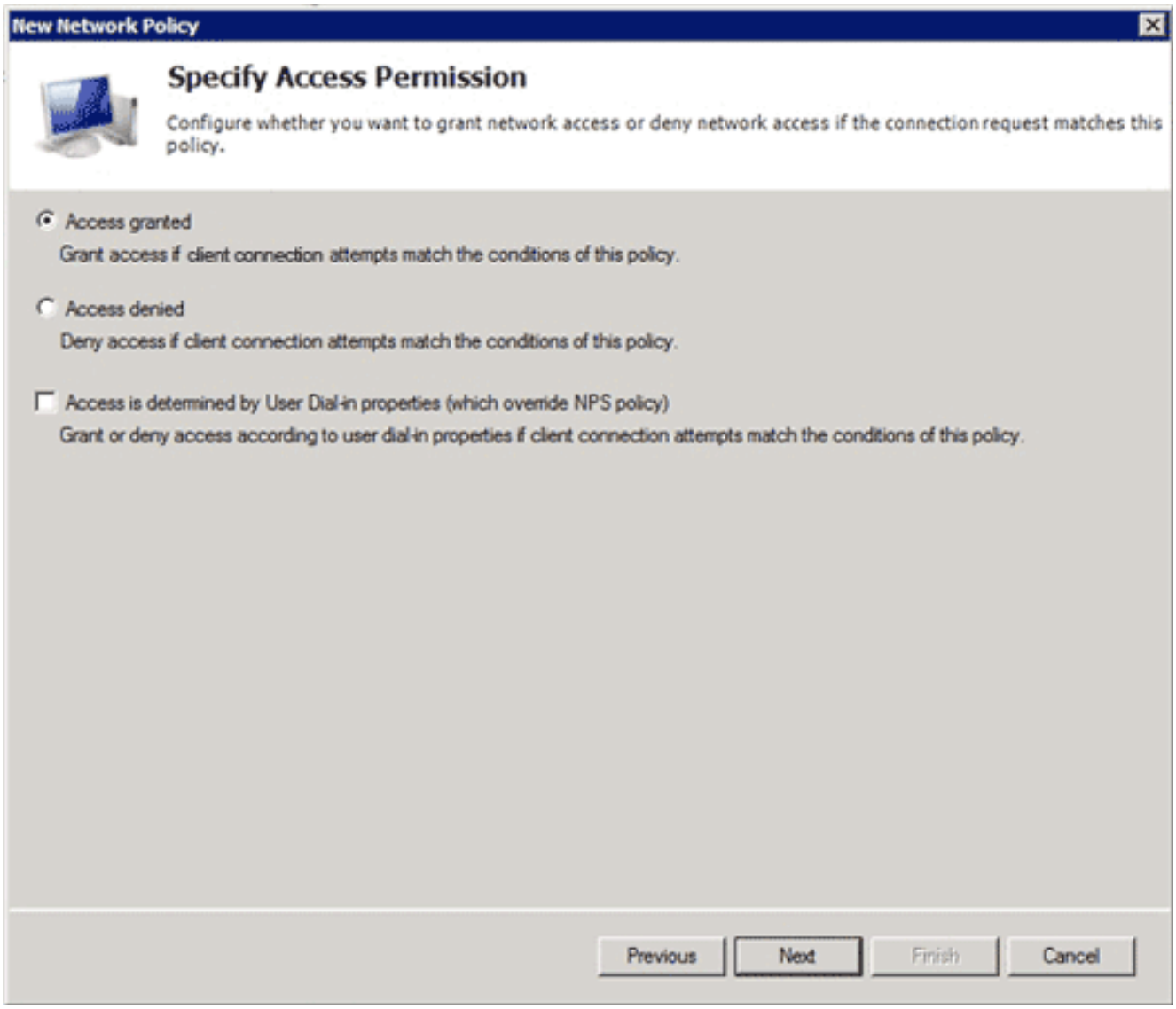
   Dê entrada com um nome no campo de nome da política. Este exemplo usa *FlexVPN*.Clique o botão de rádio do **servidor de acesso do tipo de rede**, e escolha **não especificado da** lista de drop-down.Clique em Next.Na caixa de diálogo nova da política de rede, o clique **adiciona** para adicionar uma condição nova.Na caixa de diálogo seleta da circunstância, selecione a condição do **endereço do IPv4 NAS**, e o clique **adiciona**.

   A caixa de diálogo do endereço do IPv4 NAS aparece.



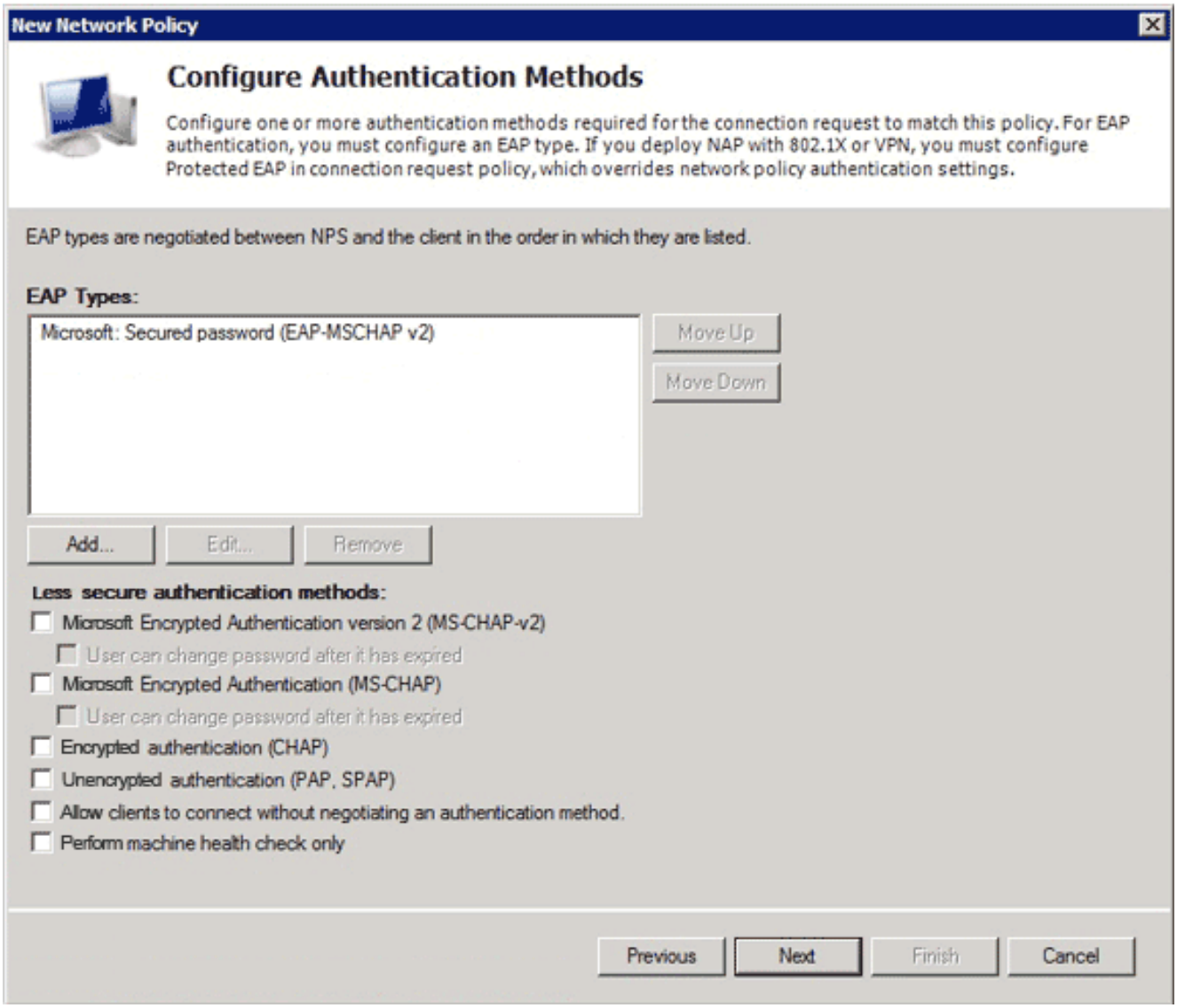
Na caixa de diálogo do endereço do IPv4 NAS, incorpore o endereço do IPv4 do servidor do acesso de rede a fim limitar a política de rede somente aos pedidos que originam deste roteador do Cisco IOS.

Clique em **OK**.



Na caixa de diálogo nova da política de rede, clique o **acesso concedeu o** botão de rádio a fim permitir o acesso do cliente à rede (se as credenciais fornecidas pelo usuário são

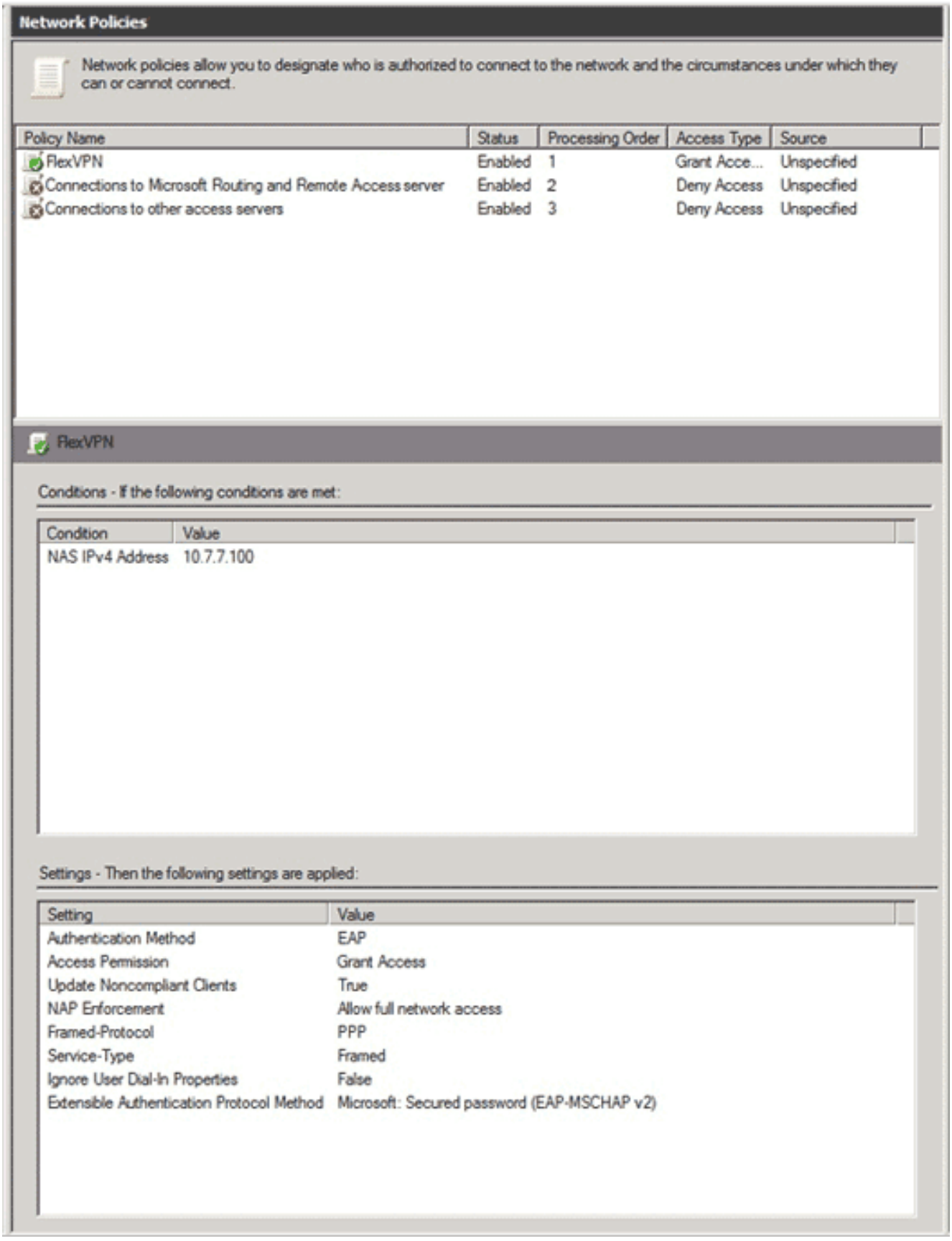
válidas), e clicam-no **em seguida**.



Assegure somente Microsoft: A senha segura (EAP-MSCHAP v2) aparece nos tipos área EAP a fim permitir que o EAP-MSCHAPv2 seja usado como o método de comunicação entre o dispositivo IOS Cisco e o diretório ativo, e clica **em seguida**.

Nota: Deixe as opções de todos os “métodos de autenticação menos seguros desmarcadas.

Continue através do assistente e aplique quaisquer limitações ou ajustes adicionais como definidos por sua política de segurança das organizações. Além, assegure-se de que a política esteja alistada primeiramente no ordem de processamento segundo as indicações desta imagem:



Configuração do Cliente

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

Este exemplo usa este perfil XML:

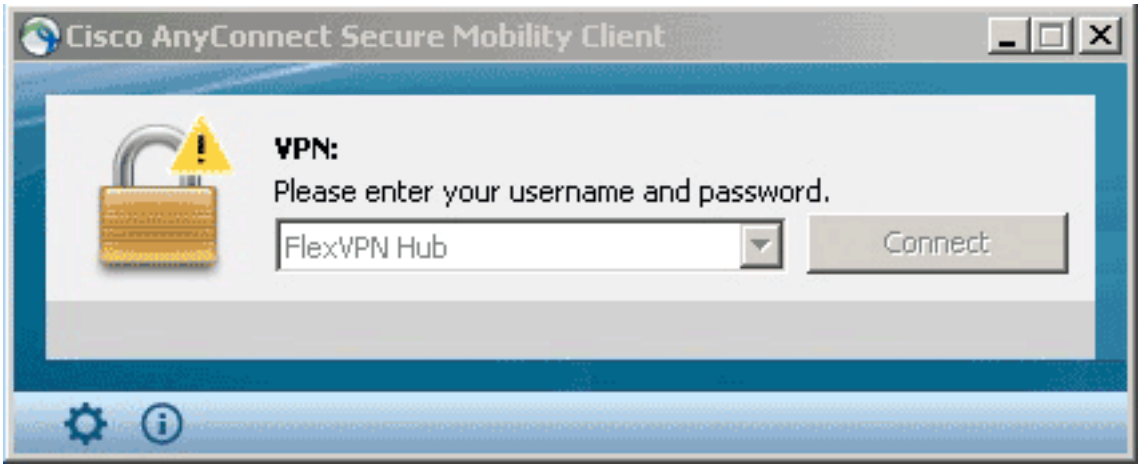
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false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

o <hostname> é uma sequência de caracteres de texto que apareça no cliente.o <HostAddress> é o nome de domínio totalmente qualificado (FQDN) do hub de FlexVPN.o <PrimaryProtocol> configura a conexão para usar IKEv2/IPsec um pouco do que SSL (o padrão em AnyConnect).o <AuthMethodDuringIKENegotiation> configura a conexão para usar o MSCHAPv2 dentro do EAP. Este valor é exigido para a autenticação contra o microsoft ative directory.o <IKEIdentity> define o valor de série que combina o cliente a um perfil IKEv2 específico no hub (veja etapa 4 acima).
Nota: O perfil do cliente é algo que é usado somente pelo cliente. Recomenda-se que um administrador usa o editor do perfil de Anyconnect a fim criar o perfil do cliente.

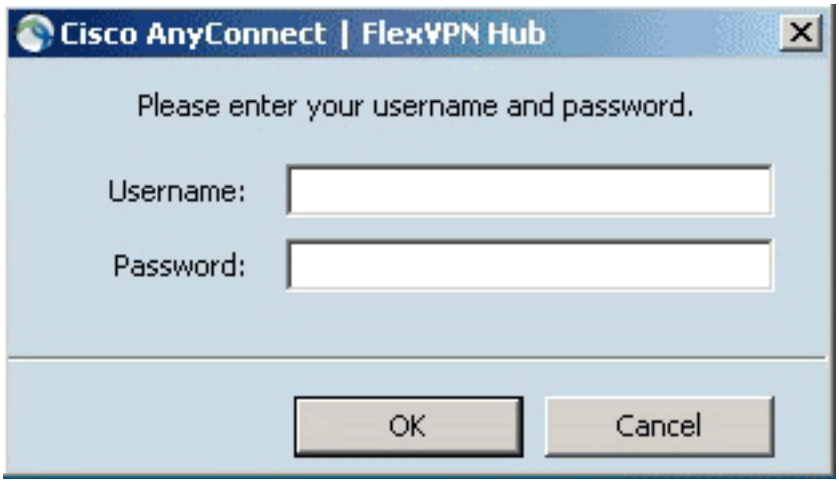
2. Salvar o arquivo flexvpn.xml ao diretório apropriado como catalogado nesta tabela:

3. O fim e reinicia o cliente de AnyConnect.



4. Na caixa de diálogo do Cliente de mobilidade Cisco AnyConnect Secure, escolha o **hub de FlexVPN**, e o clique **conecta**.

Cisco AnyConnect | A caixa de diálogo do hub de FlexVPN aparece.



5. Incorpore um nome de usuário e senha, e clique a **APROVAÇÃO**.

Verificar

A fim verificar a conexão, use o comando **remoto do cliente-IP address do detalhe da sessão de criptografia da mostra**. Refira a sessão de criptografia da mostra para obter mais informações sobre deste comando.

> Nota: A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Troubleshooting

A fim pesquisar defeitos a conexão, recolher e analisar logs do DARDO do cliente e usar estes comandos debug no roteador: **pacote do debug crypto ikev2** e **debug crypto ikev2 internos**.

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

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems