FlexVPN和Anyconnect IKEv2客户端配置示例

目录

简介

本文档介绍如何配置Cisco AnyConnect安全移动客户端以使用远程身份验证拨入用户服务(RADIUS)和本地授权属性，以便根据Microsoft Active Directory进行身份验证。

> **注意**：目前，在Cisco IOS®设备上使用本地用户数据库进行身份验证不起作用。这是因为Cisco IOS不用作EAP身份验证器。已提交增强请求CSCui07025以添加支持。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS 15.2(T)版或更高版本

- Cisco AnyConnect安全移动客户端3.0版或更高版本
- Microsoft Active Directory

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

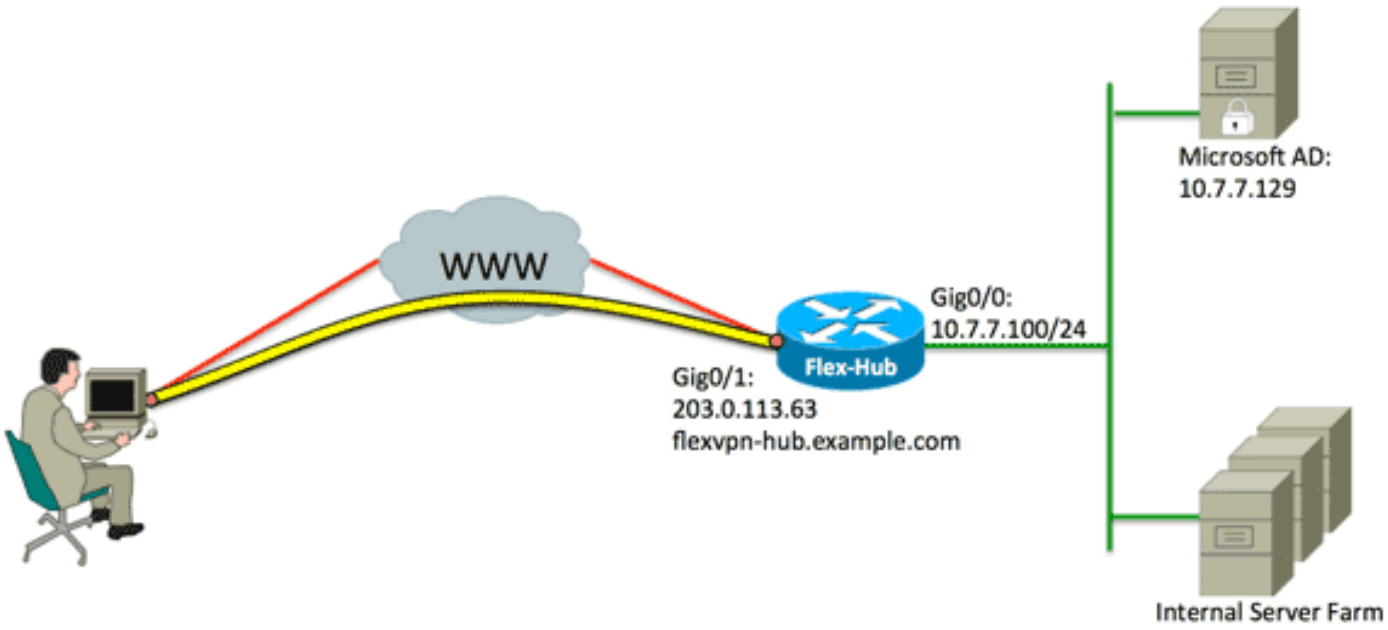
配置

本部分提供有关如何配置本文档中所述功能的信息。

使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- 中心配置
- Microsoft Active Directory服务器配置
- 客户端配置

中心配置

1. 配置RADIUS以仅进行身份验证并定义本地授权。

```
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
```

aaa authentication login list命令是指身份验证、授权和记帐(AAA)组（定义RADIUS服务器）。 aaa authorization network list **命令**表示要使用本地定义的用户/组。必须更改RADIUS服务器上的配置以允许来自此设备的身份验证请求。

2. 配置本地授权策略。

```
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
```

ip local pool命令用于定义分配给客户端的IP地址。授权策略是使用用户名*FlexVPN-Local-Policy-1*定义的，并在此处配置客户端的属性（DNS服务器、网络掩码、拆分列表、域名等）。

3. 确保服务器使用证书(rsa-sig)进行自身身份验证。

Cisco AnyConnect安全移动客户端要求服务器使用证书(rsa-sig)对自身进行身份验证。 路由器必须具有来自受信*任证书颁发机*构(CA)的Web服务器证书（即，在扩展密钥使用扩展内具有“服务器身份验证”的证书）。

请参阅ASA 8.x手动安装第三方供应商证书以与WebVPN配置示例中的步骤1到4，并将加密ca的所有实例更*改为*加密*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. 配置此连接的设置。

```
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
```

crypto ikev2配置文件包含此连接的大部分相关设置： **match identity remote key-id** — 指客户端使用的IKE身份。此字符串值在AnyConnect XML配置文件中配置。**identity local dn** — 定义FlexVPN中心使用的IKE身份。此值使用所用证书内的值。**authentication remote** — 表示EAP应用于客户端身份验证。**authentication local** — 表示证书应用于本地身份验证。**aaa authentication eap** — 当EAP用于身份验证时使用aaa authentication login list FlexVPN-AuthC-List-1的状态。**aaa authorization group eap list** — 使用用户名为FlexVPN-Local-Policy-1的aaa授权网络列表FlexVPN-AuthZ-List-1进*行授权属*性的状态。**virtual-template 10** — 定义克隆虚拟访问接口时使用的模板。

5. 配置IPsec配置文件，该配置文件链接回步骤4中定义的IKEv2配置文件。

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

注意：Cisco IOS使用智能默认值。因此，转换集不需要显式定义。

6. 配置从中克隆虚拟访问接口的虚拟模板：
ip unnumbered -从内部接口取消*接口*编号，以便在接口上启用IPv4路由。**tunnel mode ipsec ipv4 -**将接口定义为VTI类型隧道。
```
interface Virtual-Template10 type tunnel
ip unnumbered GigabitEthernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

7. 将协商限制为SHA-1。（可选）

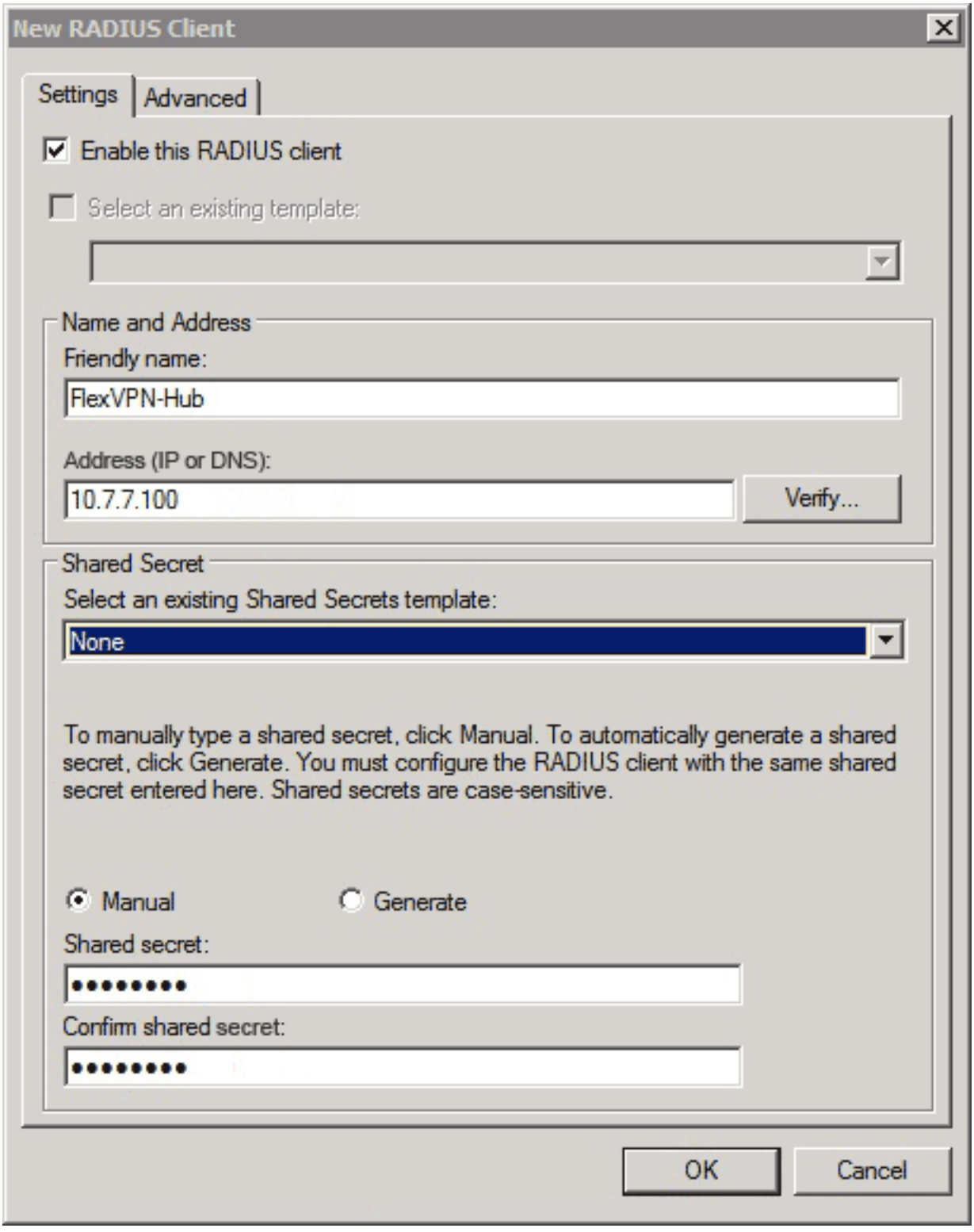
由于缺陷CSCud96246(仅注册客户),AnyConnect客户端可能无法正确验证FlexVPN集线器证书。此问题是由于IKEv2为伪随机函数(PRF)协商SHA-2函数，而FlexVPN-Hub证书已使用SHA-1签名。以下配置将协商限制为SHA-1:

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

Microsoft Active Directory服务器配置

1. 在Windows Server Manager中，展开**Roles > Network Policy and Access Server > NMPS(Local)> RADIUS Clients and Servers，然**后单击**RADIUS Clients**。

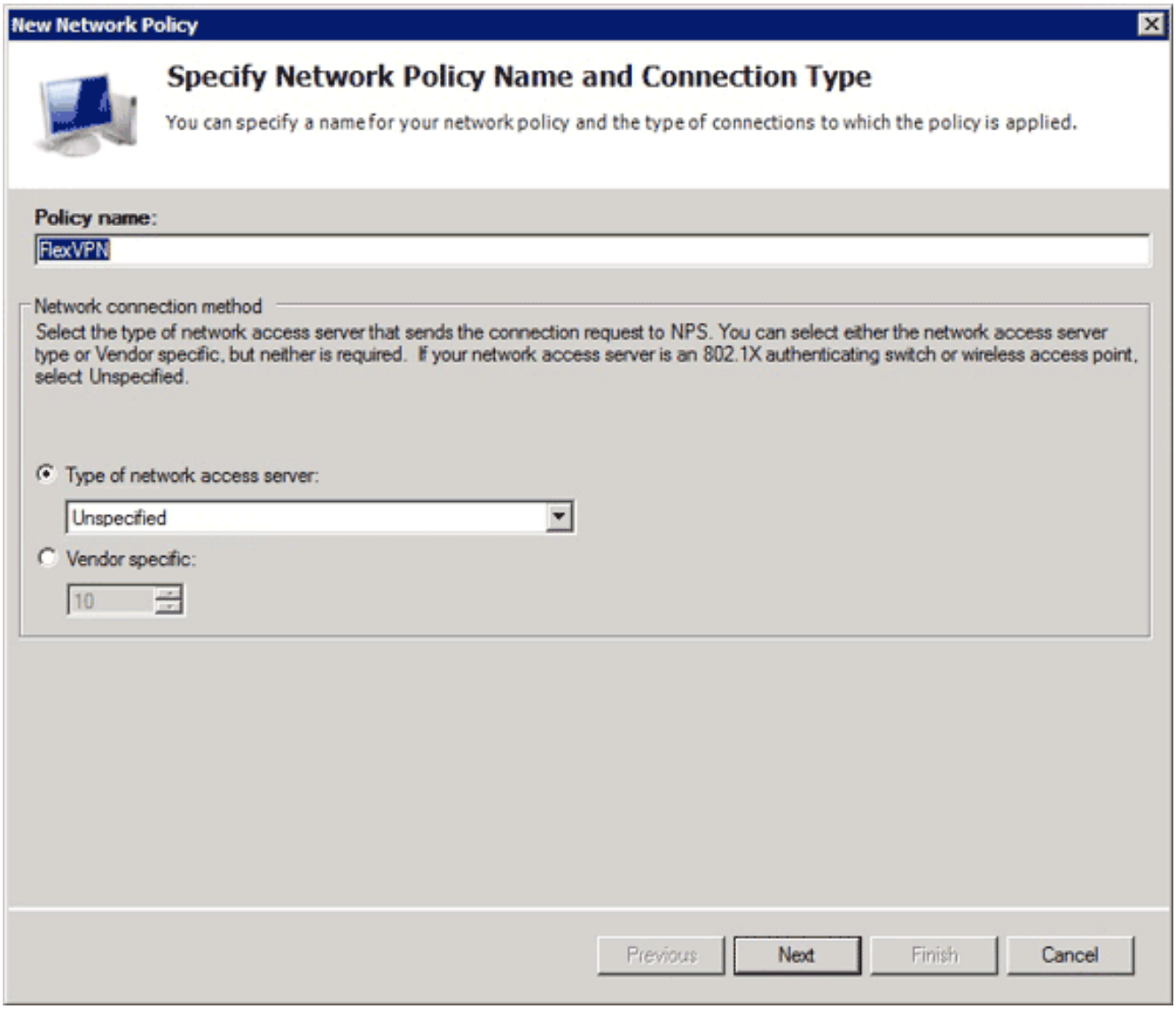
系统将显示New RADIUS Client对话框。



2. 在New RADIUS Client（新建RADIUS客户端）对话框中，将Cisco IOS路由器添加为RADIUS客户端：
   单击**Enable this RADIUS client**复选框。在友好名称字段中输入名称。本示例使用*FlexVPN-Hub*。在Address字段中输入路由器的IP地址。在“共享密钥”区域，单击**手动**单选按钮，然后在“共享密钥”和“确认共享密钥”字段中输入共享密钥。**注意：**共享密钥必须与路由器上配置的共享密钥匹配。Click OK.

3. 在服务器管理器界面中，展开**策略**，然后选择**网络策略**。

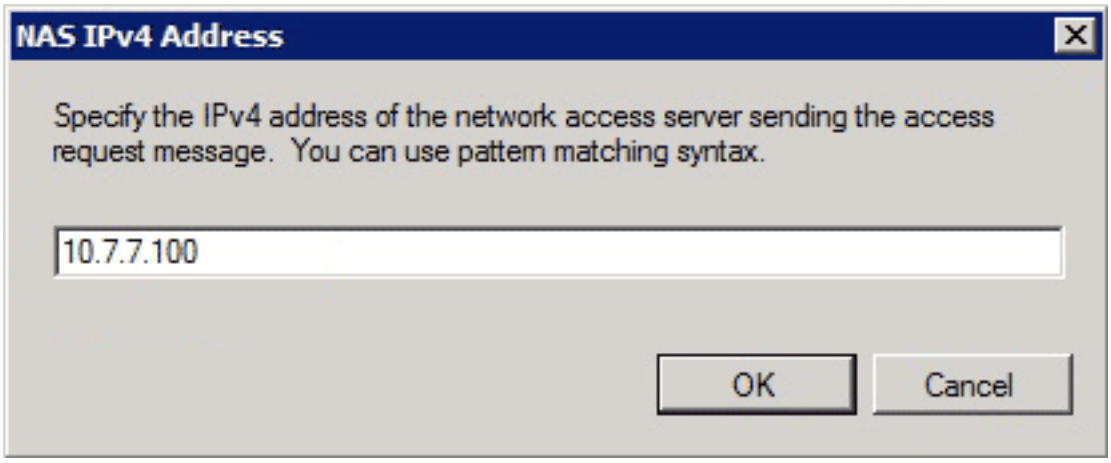
系统将显示New Network Policy对话框。



4. 在New Network Policy对话框中，添加新网络策略：

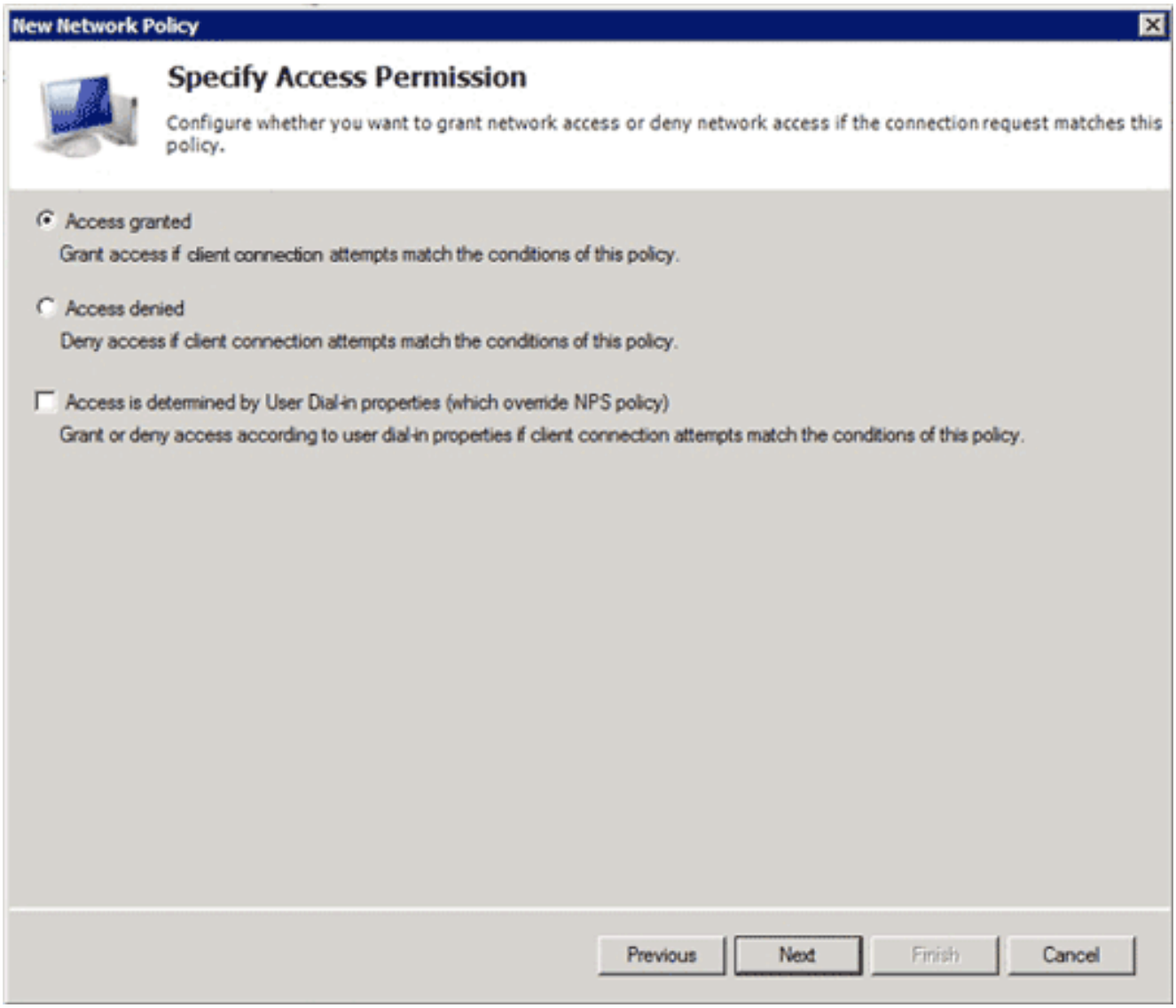
   在策略名称字段中输入名称。本示例使*用FlexVPN*。单击“**Type of network access server”单选**按钮，然后从下拉列**表中**选择“Unspecified”。单击 Next。在New Network Policy（新建网络策略）对话框中，单**击Add**（添加）添加新条件。在选择条件对话框中，选择NAS **IPv4地址条**件，然后单**击添加**。

   系统将显示NAS IPv4地址对话框。

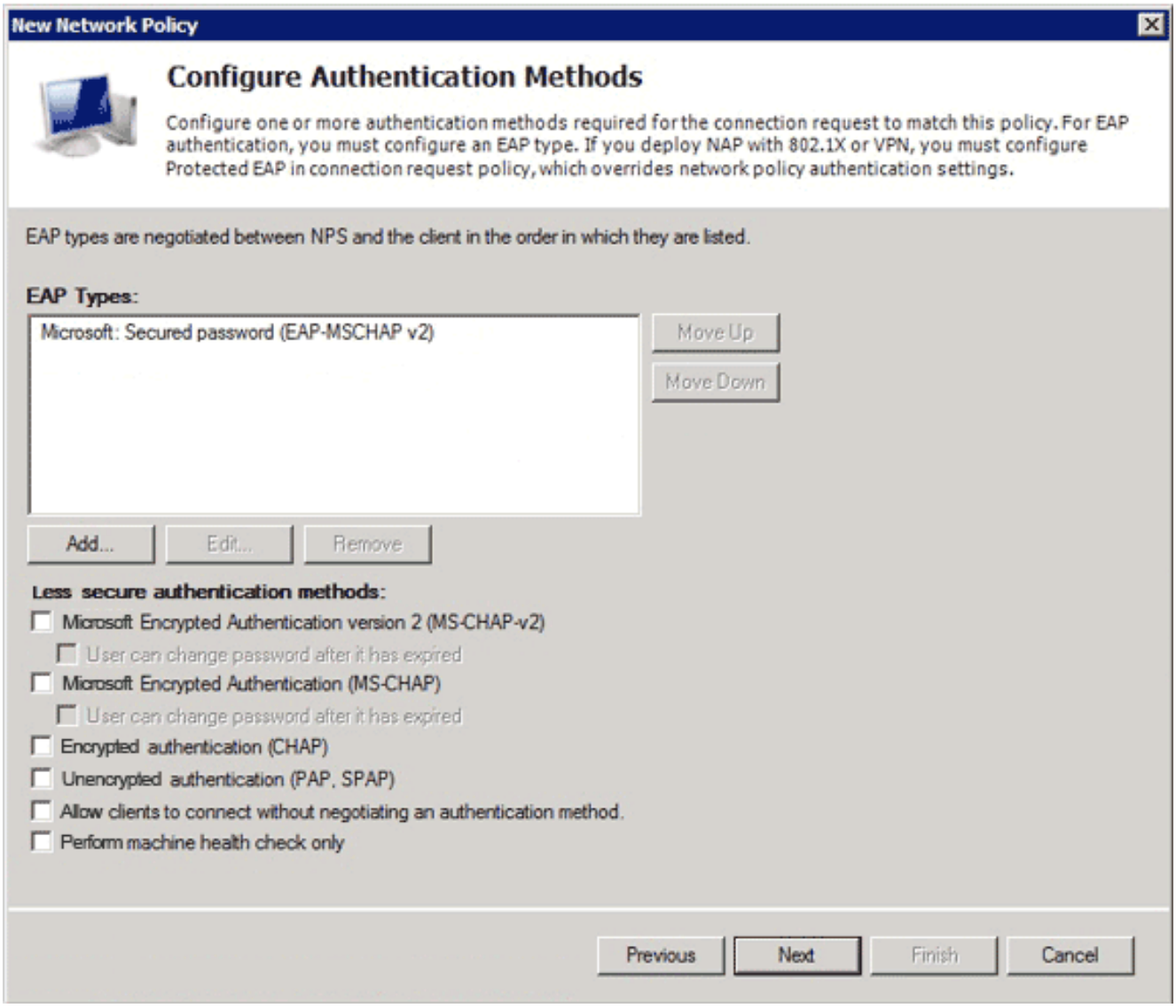


在NAS IPv4地址对话框中，输入网络接入服务器的IPv4地址，以便将网络策略限制为仅允许来自此Cisco IOS路由器的请求。

Click OK.



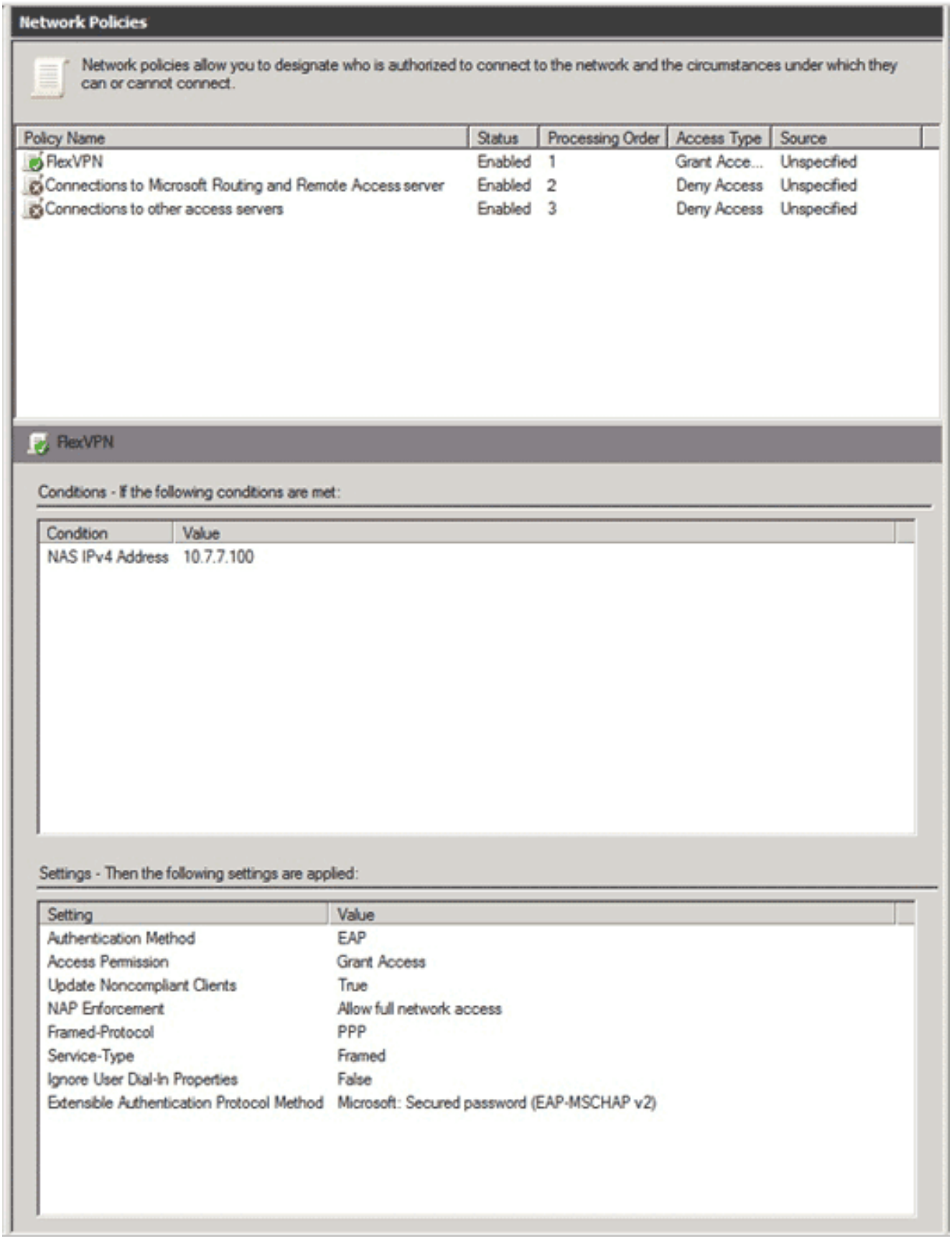
在新的Network Policy对话框中，单击**Access granded** 单选按钮以允许客户端访问网络（如果用户提供的凭据有效），然后单击**Next**。



仅确保Microsoft:安全密码(EAP-MSCHAP v2)显示在EAP Types区域中，以允许EAP-MSCHAPv2用作Cisco IOS设备与Active Directory之间的通信方法，然后单击**Next**。

注意：不选中所有“安全性较低的身份验证方法”选项。

继续通过向导，并应用组织安全策略定义的任何其他限制或设置。此外，请确保策略在处理顺序中列在第一位，如下图所示：



客户端配置

1. 在文本编辑器中创建XML配置文件，并将其命*名为flexvpn.xml*。

本示例使用以下XML配置文件：

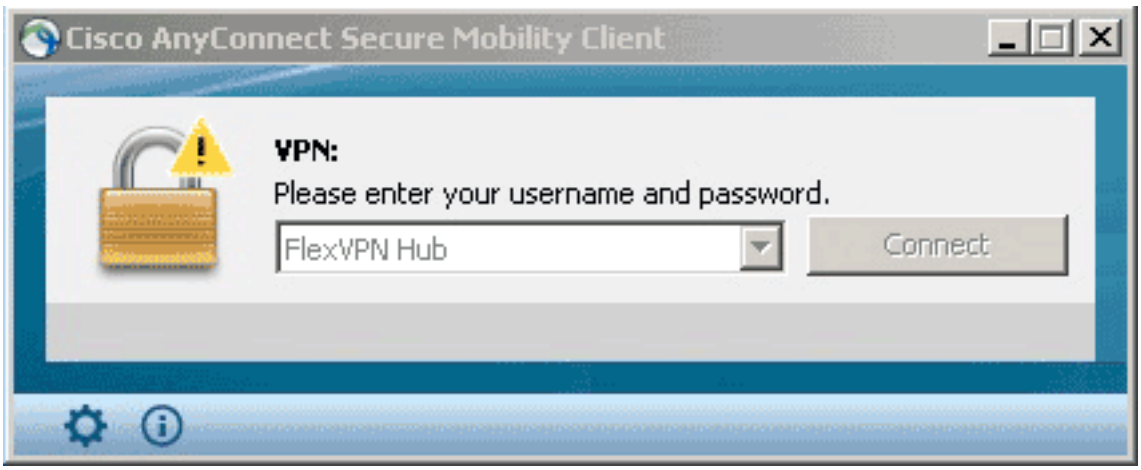
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false
</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>是显示在客户端中的文本字符串。<HostAddress>是FlexVPN中心的完全限定域名(FQDN)。<PrimaryProtocol>将连接配置为使用IKEv2/IPsec而非SSL（AnyConnect中的默认设置）。<AuthMethodDuringIKENegotiation>将连接配置为在EAP中使用MSCHAPv2。对Microsoft Active Directory进行身份验证时需要此值。<IKEIdentity>定义将客户端与集线器上的特定IKEv2配置文件匹配的字符串值（请参阅上面的步骤4）。
注意：客户端配置文件是仅供客户端使用的内容。建议管理员使用Anyconnect配置文件编辑器创建客户端配置文件。

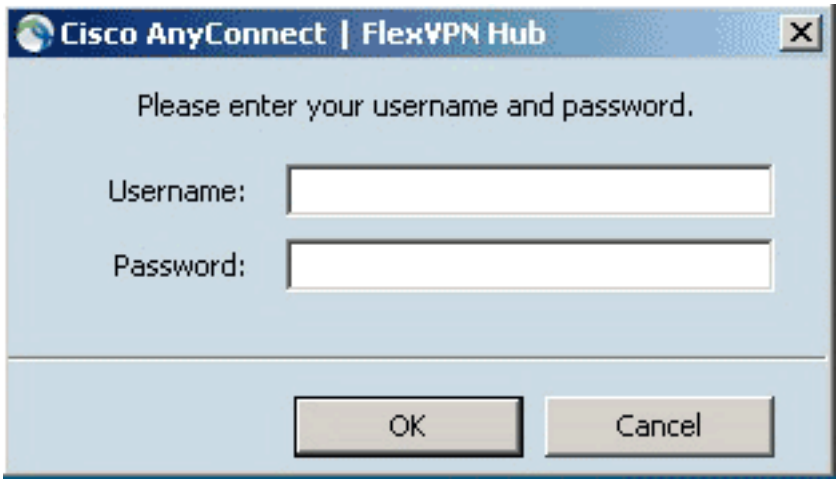
2. 将flexvpn.xml文件保存到下表中列出的相应目录：

3. 关闭并重新启动AnyConnect客户端。



4. 在Cisco AnyConnect安全移动客户端对话框中，选择**FlexVPN中心**，然后单**击连接**。

Cisco AnyConnect | FlexVPN中心对话框。



5. 输入用户名和密码，然后单击**OK**。

验证

要验证连接，请使用**show crypto session detail remote client-ipaddress命**令。有关此命令的详细信息，请参阅show crypto session。

> **注意**：命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

要排除连接故障，请从客户端收集并分析DART日志，并在路由器上使用以下debug命令：**debug crypto ikev2 packet**和**debug crypto ikev2 internal**。

> **注意**：使用 debug 命令之前，请参阅有关 Debug 命令的重要信息。

相关信息

- 技术支持和文档 - Cisco Systems