Exemple de configuration du client FlexVPN et Anyconnect IKEv2

Contenu

Introduction

Ce document décrit comment configurer le client Cisco AnyConnect Secure Mobility pour utiliser le service RADIUS (Remote Authentication Dial-In User Service) et les attributs d'autorisation locale afin de s'authentifier auprès de Microsoft Active Directory.

> **Note**: Actuellement, l'utilisation de la base de données des utilisateurs locaux pour l'authentification ne fonctionne pas sur les périphériques Cisco IOS®. En effet, Cisco IOS ne fonctionne pas en tant qu'authentificateur EAP. La demande d'amélioration CSCui07025 a été déposée pour ajouter le support.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco IOS version 15.2(T) ou ultérieure
- Cisco AnyConnect Secure Mobility Client version 3.0 ou ultérieure
- Microsoft Active Directory

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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

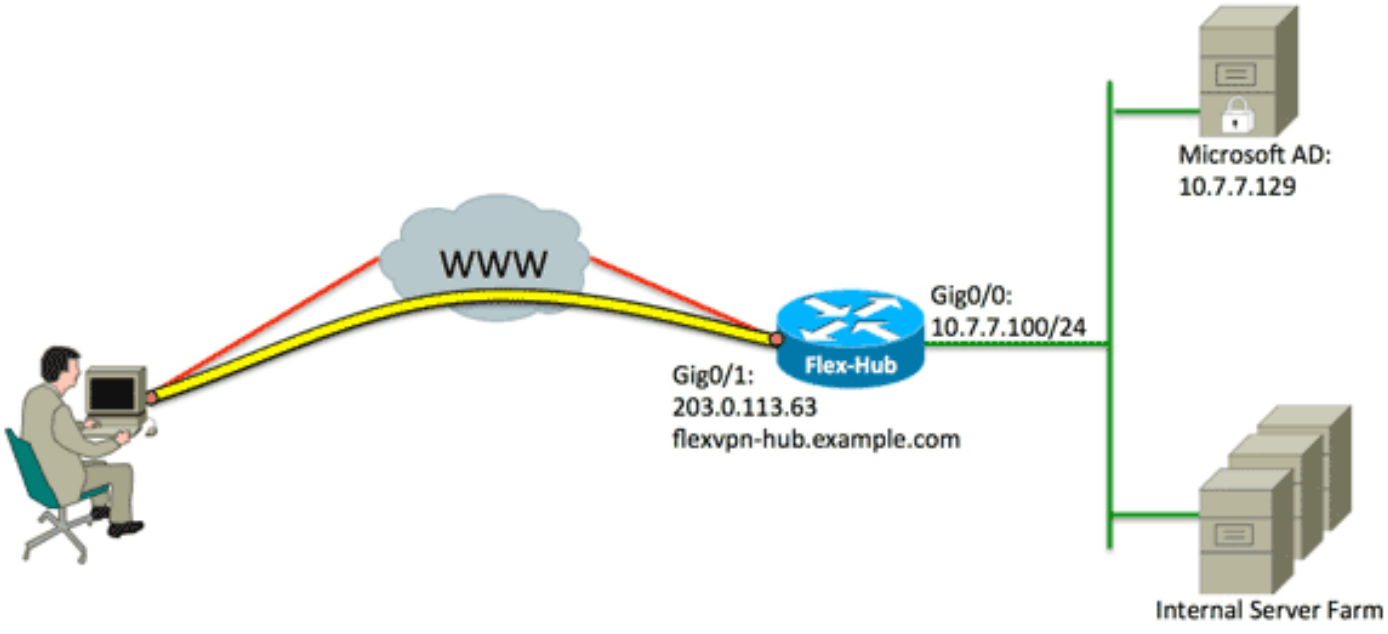
Configuration

Cette section vous fournit des informations utilisées pour configurer les fonctionnalités décrites dans ce document.

Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- Configuration du concentrateur
- Configuration du serveur Microsoft Active Directory
- Configuration du client

Configuration du concentrateur

1. Configurez RADIUS uniquement pour l'authentification et définissez l'autorisation locale.

```
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
```

   La commande **aaa authentication login list** fait référence au groupe AAA (Authentication, Authorization, and Accounting) (qui définit le serveur RADIUS). La commande **aaa Authorization network list** indique que des utilisateurs/groupes définis localement doivent être utilisés. La configuration sur le serveur RADIUS doit être modifiée pour autoriser les demandes d'authentification à partir de ce périphérique.

2. Configurez la stratégie d'autorisation locale.

```
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
```

   La commande **ip local pool** permet de définir les adresses IP attribuées au client. Une stratégie d'autorisation est définie avec un nom d'utilisateur *FlexVPN-Local-Policy-1*, et les attributs du client (serveurs DNS, masque de réseau, liste partagée, nom de domaine, etc.) sont configurés ici.

3. Assurez-vous que le serveur utilise un certificat (rsa-sig) pour s'authentifier.

   Le client Cisco AnyConnect Secure Mobility nécessite que le serveur s'authentifie à l'aide d'un certificat (rsa-sig). Le routeur doit avoir un certificat de *serveur Web* (c'est-à-dire un certificat avec 'authentification serveur' dans l'extension d'utilisation de clé étendue) d'une autorité de certification (CA) de confiance.

   Référez-vous aux étapes 1 à 4 dans ASA 8.x Installation manuelle de certificats de fournisseurs tiers pour utilisation avec l'exemple de configuration WebVPN, et modifiez toutes les instances de *crypto ca* en *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. Configurez les paramètres de cette connexion.

```
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
```

Le profil **crypto ikev2** contient la plupart des paramètres pertinents pour cette connexion : **match identity remote key-id** : fait référence à l'identité IKE utilisée par le client. Cette valeur de chaîne est configurée dans le profil XML AnyConnect.**identity local dn** : définit l'identité IKE utilisée par le concentrateur FlexVPN. Cette valeur utilise la valeur du certificat utilisé.**authentication remote** - États selon lesquels le protocole EAP doit être utilisé pour l'authentification du client.**authentication local** : indique que les certificats doivent être utilisés pour l'authentification locale.**aaa authentication eap** - États pour utiliser la liste de connexion d'authentification aaa FlexVPN-AuthC-List-1 lorsque le protocole EAP est utilisé pour l'authentification.**liste eap du groupe d'autorisations aaa** - États pour utiliser la liste de réseau d'autorisations aaa FlexVPN-AuthZ-List-1 avec le nom d'utilisateur *FlexVPN-Local-Policy-1* pour les attributs d'autorisation.**virtual-template 10** - Définit le modèle à utiliser lorsqu'une interface d'accès virtuel est clonée.

5. Configurez un profil IPsec qui renvoie au profil IKEv2 défini à l'étape 4.

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

Note: Cisco IOS utilise Smart Defaults. Par conséquent, un jeu de transformation n'a pas besoin d'être explicitement défini.

6. Configurez le modèle virtuel à partir duquel les interfaces d'accès virtuel sont clonées : **ip unnumbered -** Annule le numéro de l'interface d'une interface *interne* afin que le routage IPv4 puisse être activé sur l'interface.**tunnel mode ipsec ipv4 -** Définit l'interface comme un tunnel de type VTI.

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

7. Limitez la négociation à SHA-1. (Facultatif)

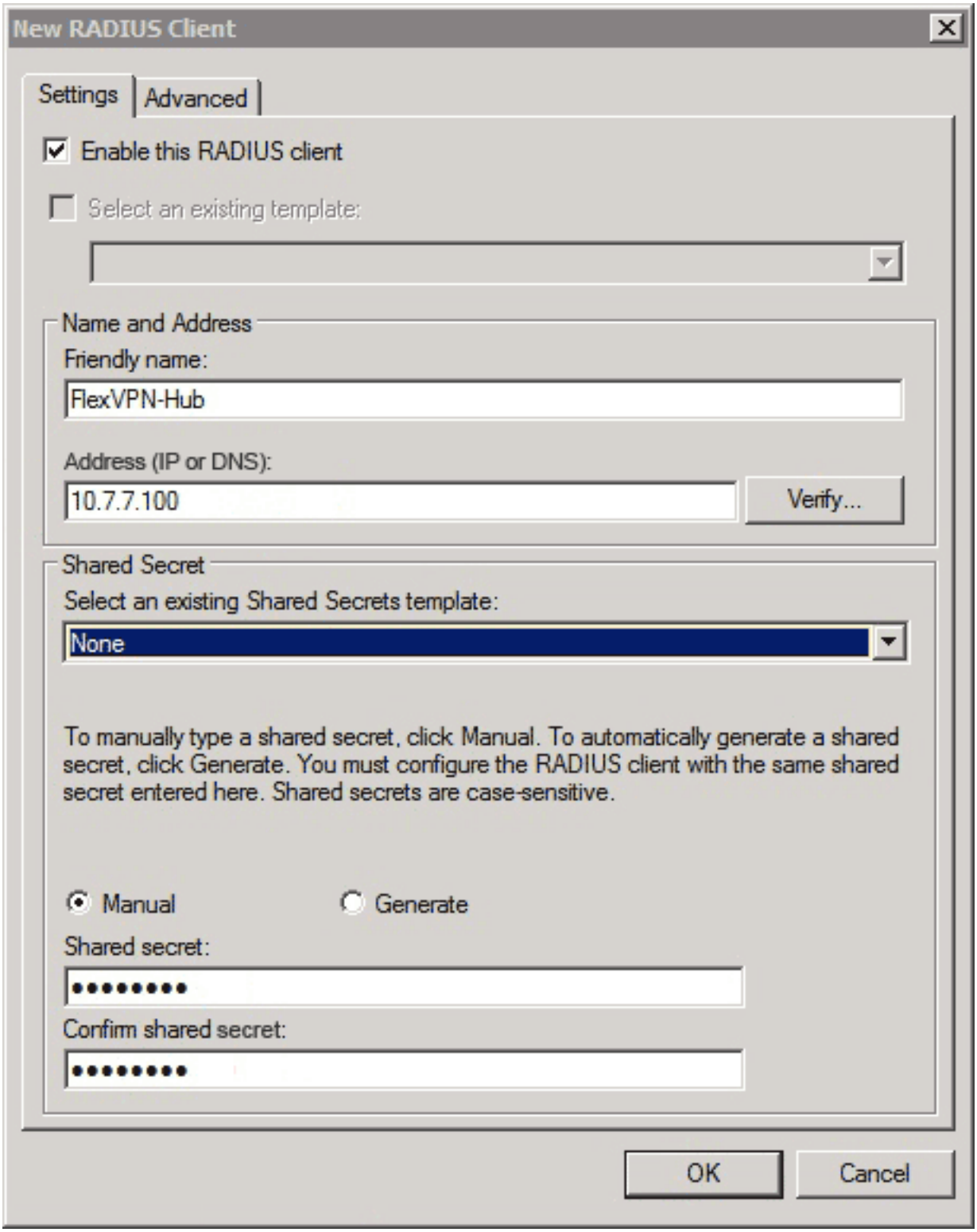
   En raison d'un défaut CSCud96246 (clients enregistrés uniquement) , le client AnyConnect peut ne pas valider correctement le certificat FlexVPN Hub. Ce problème est dû à la négociation par IKEv2 d'une fonction SHA-2 pour la fonction pseudo-aléatoire (PRF) alors que le certificat FlexVPN-Hub a été signé à l'aide de SHA-1. La configuration ci-dessous limite la négociation à 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
```

Configuration du serveur Microsoft Active Directory

1. Dans le Gestionnaire de serveur Windows, développez **Rôles > Stratégie réseau et serveur d'accès > NMPS (Local) > Clients et serveurs RADIUS**, puis cliquez sur **Clients RADIUS**.

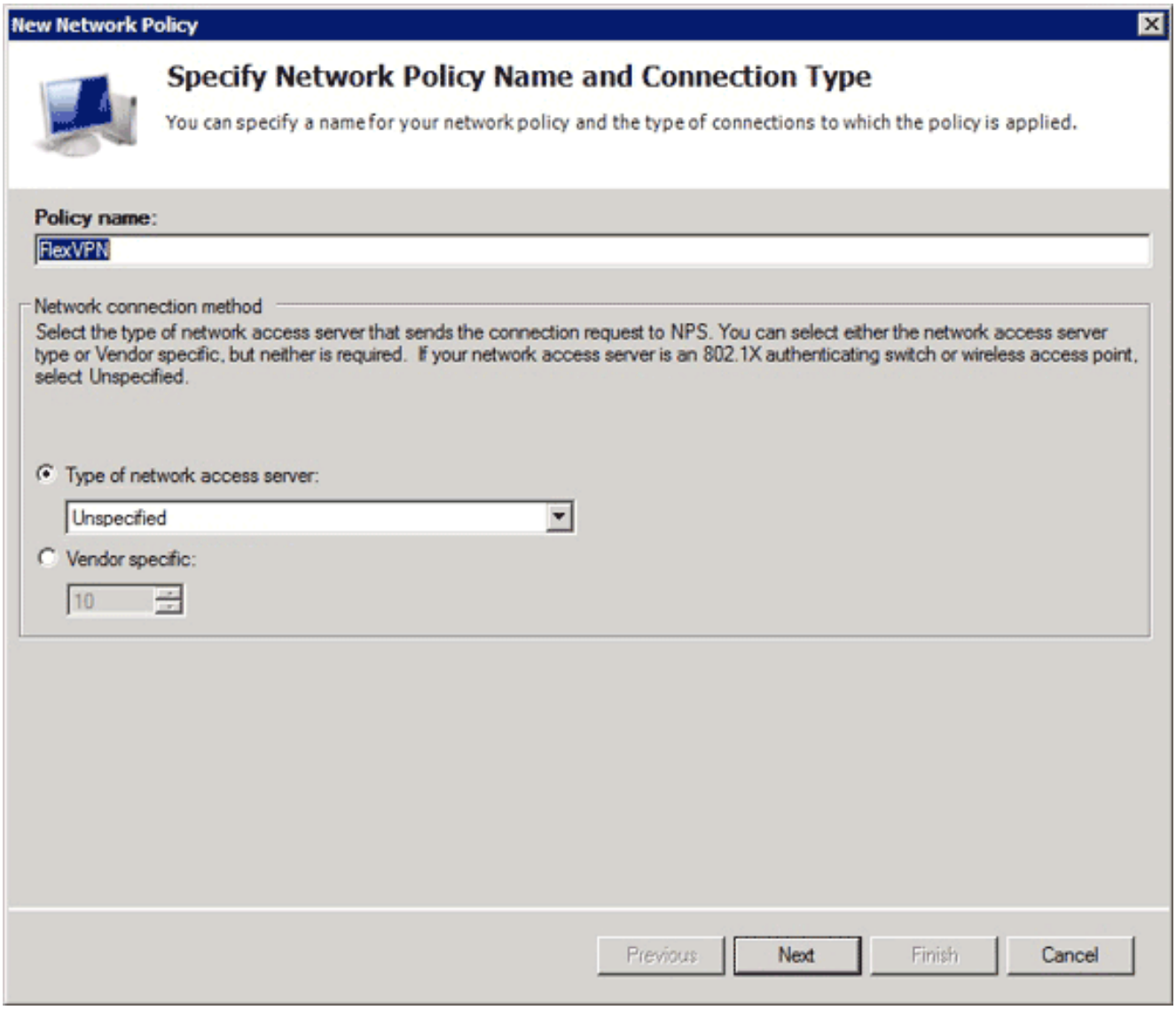
   La boîte de dialogue Nouveau client RADIUS apparaît.



2. Dans la boîte de dialogue Nouveau client RADIUS, ajoutez le routeur Cisco IOS en tant que client RADIUS :
   Cochez la case **Activer ce client RADIUS**.Saisissez un nom dans le champ Nom convivial. Cet exemple utilise *FlexVPN-Hub*.Saisissez l'adresse IP du routeur dans le champ Address (Adresse).Dans la zone Secret partagé, cliquez sur la case d'option **Manuel**, puis saisissez le secret partagé dans les champs secret partagé et Confirmer le secret partagé.**Remarque :** le secret partagé doit correspondre au secret partagé configuré sur le routeur.Click OK.

3. Dans l'interface du Gestionnaire de serveur, développez **Stratégies**, puis sélectionnez **Stratégies réseau**.

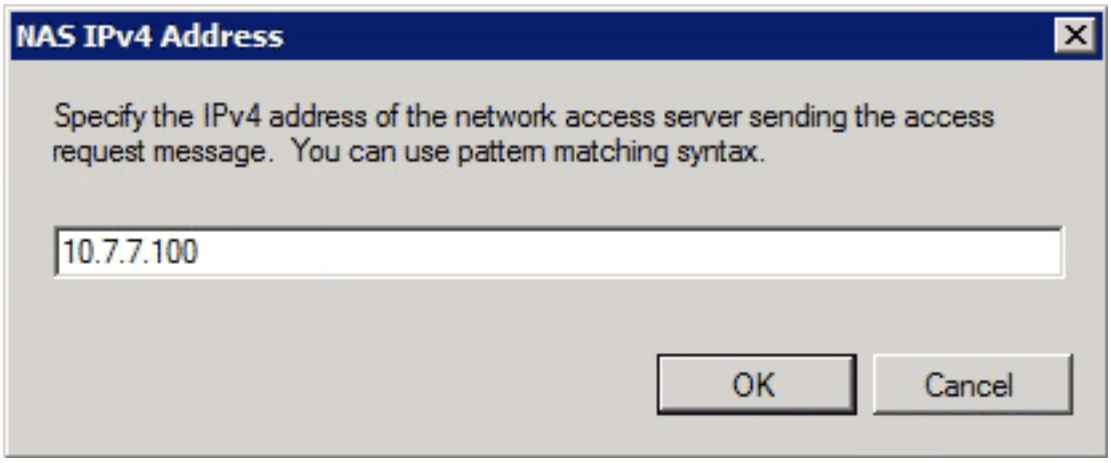
La boîte de dialogue Nouvelle stratégie réseau apparaît.



4. Dans la boîte de dialogue Nouvelle stratégie réseau, ajoutez une nouvelle stratégie réseau :

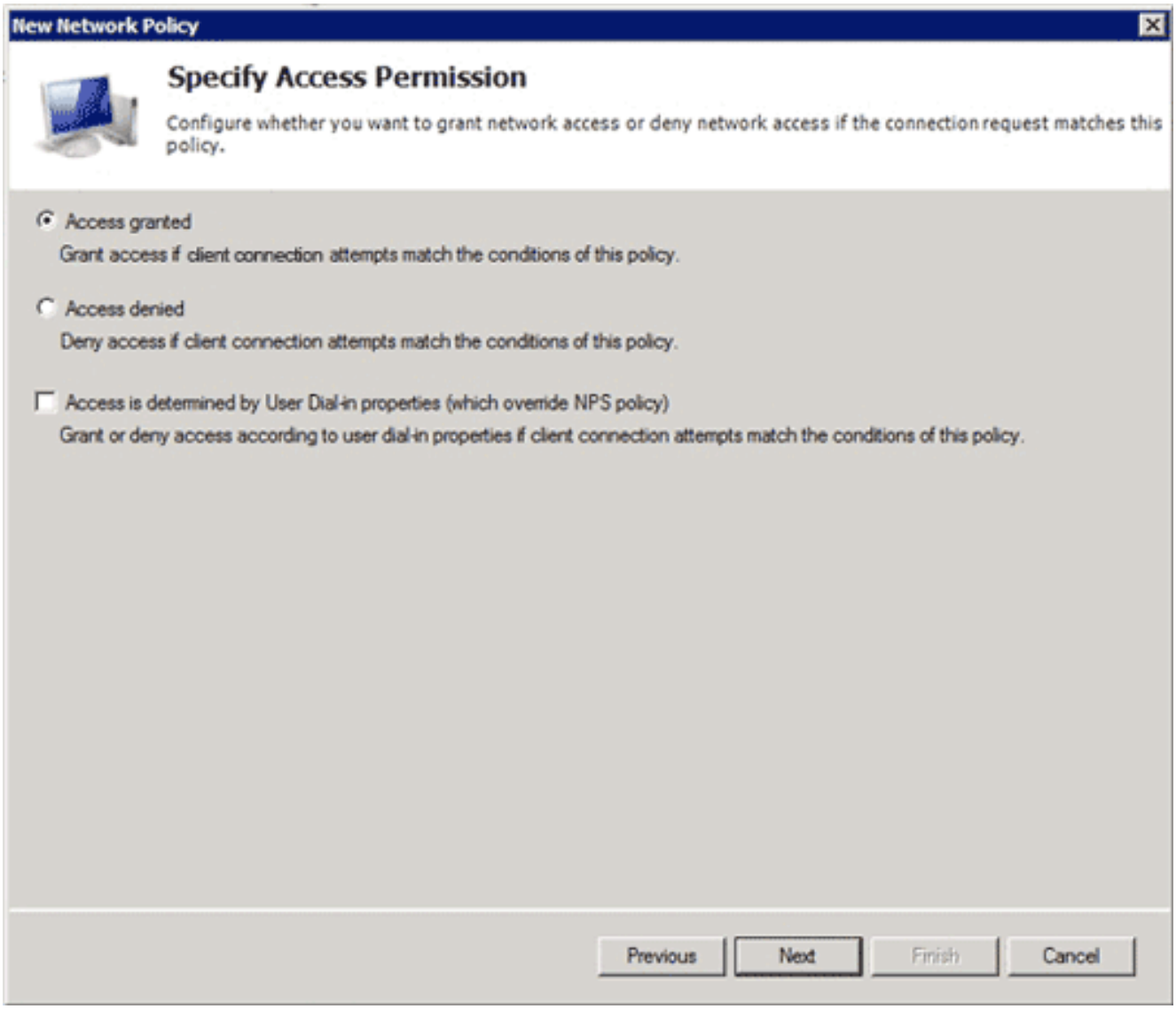
   Entrez un nom dans le champ Nom de la stratégie. Cet exemple utilise *FlexVPN*.Cliquez sur la case d'option **Type de serveur d'accès réseau**, puis sélectionnez **Non spécifié** dans la liste déroulante.Cliquez sur Next (Suivant).Dans la boîte de dialogue Nouvelle stratégie réseau, cliquez sur **Ajouter** pour ajouter une nouvelle condition.Dans la boîte de dialogue Sélectionner la condition, sélectionnez la condition **Adresse IPv4 NAS**, puis cliquez sur **Ajouter**.

   La boîte de dialogue Adresse IPv4 NAS s'affiche.



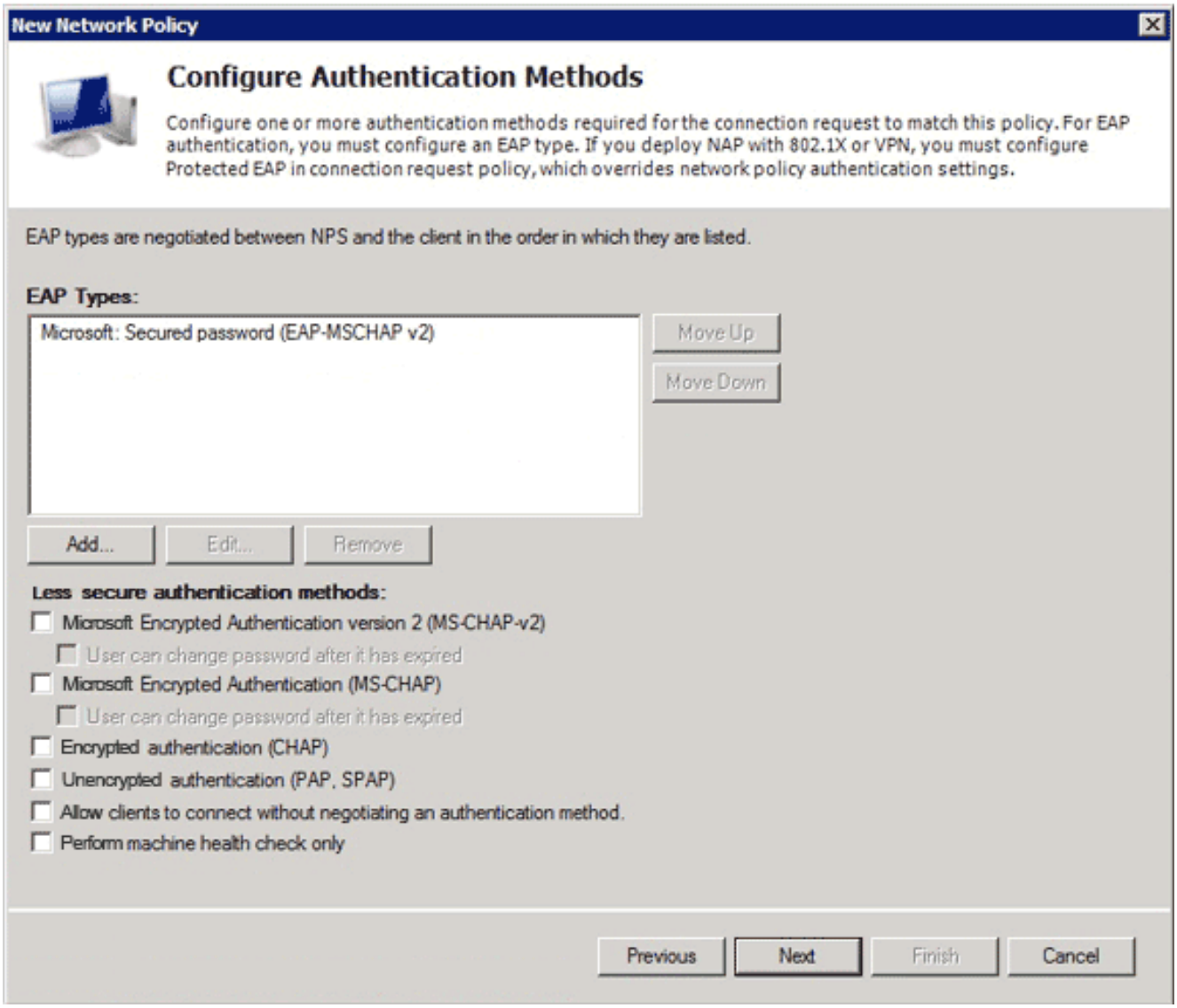
Dans la boîte de dialogue Adresse IPv4 NAS, saisissez l'adresse IPv4 du serveur d'accès au réseau afin de limiter la stratégie réseau aux seules requêtes provenant de ce routeur Cisco IOS.

Click OK.



Dans la nouvelle boîte de dialogue Stratégie réseau, cliquez sur la case d'option **Accès accordé** afin d'autoriser le client à accéder au réseau (si les informations d'identification

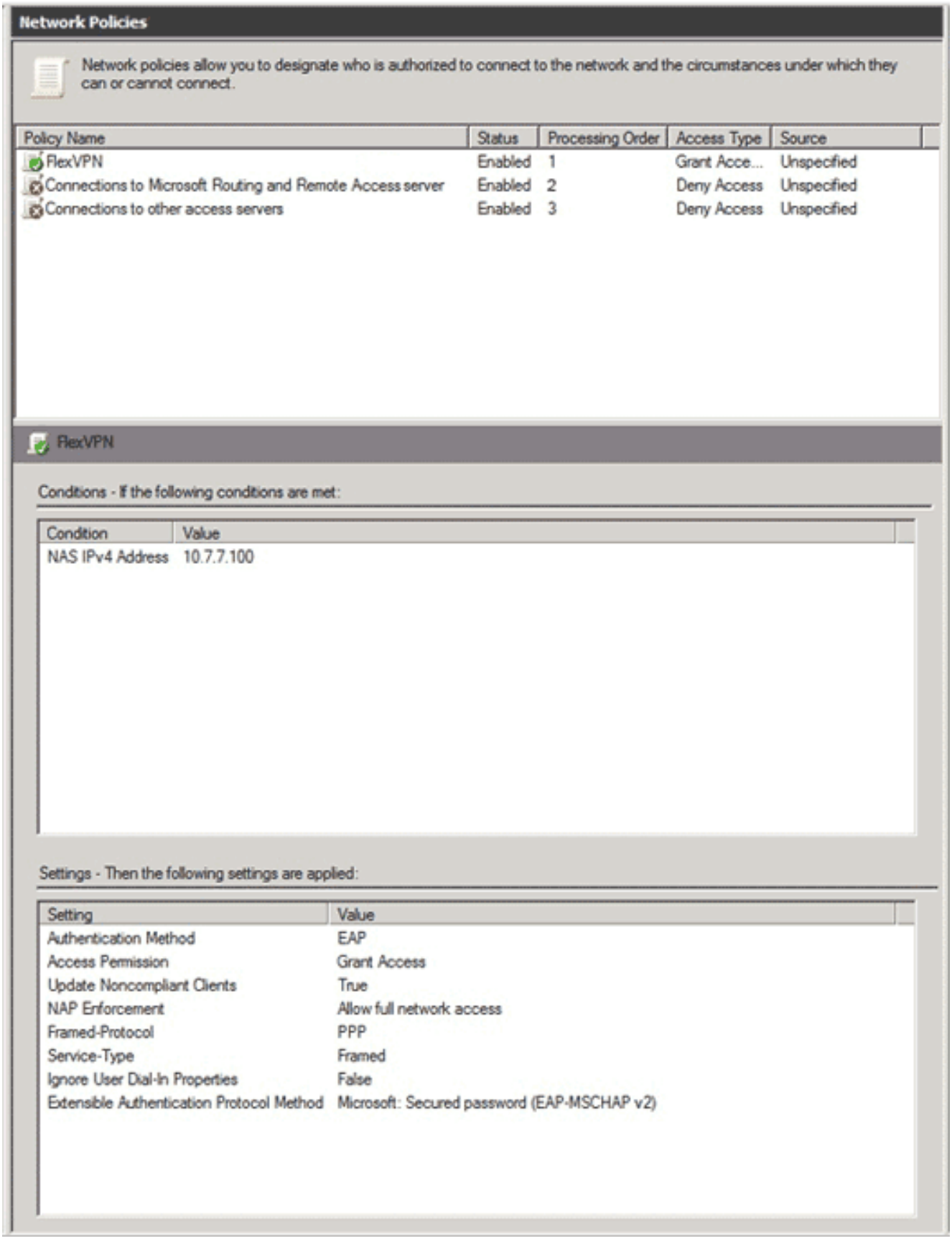
fournies par l'utilisateur sont valides), puis cliquez sur **Suivant**.



Assurez-vous que Microsoft : Le mot de passe sécurisé (EAP-MSCHAP v2) apparaît dans la zone Types EAP afin de permettre à EAP-MSCHAPv2 d'être utilisé comme méthode de communication entre le périphérique Cisco IOS et Active Directory, puis cliquez sur **Suivant**.

Note: Ne cochez pas toutes les options des méthodes d'authentification moins sécurisées.

Poursuivez l'exécution de l'Assistant et appliquez les contraintes ou paramètres supplémentaires définis par la stratégie de sécurité de votre entreprise. En outre, assurez-vous que la stratégie est répertoriée en premier dans l'ordre de traitement, comme illustré dans cette image :



Configuration du client

1. Créez un profil XML dans un éditeur de texte et nommez-le *flexvpn.xml*.

Cet exemple utilise ce profil XML :

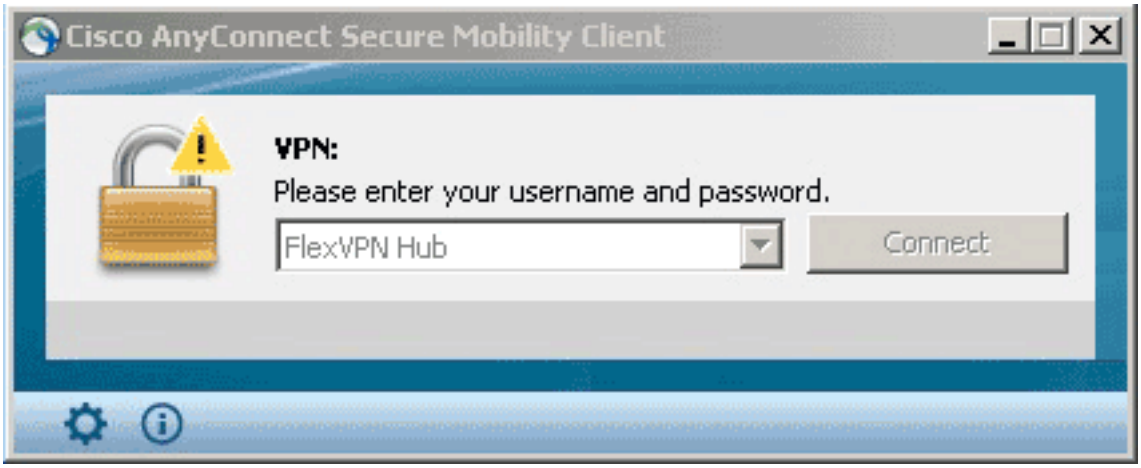
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false
</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> est une chaîne de texte qui apparaît dans le client.<HostAddress> est le nom de domaine complet (FQDN) du concentrateur FlexVPN.<PrimaryProtocol> configure la connexion pour utiliser IKEv2/IPsec plutôt que SSL (la valeur par défaut dans AnyConnect).<AuthMethodUnderIKENegotiation> configure la connexion pour utiliser MSCHAPv2 dans EAP. Cette valeur est requise pour l'authentification par rapport à Microsoft Active Directory.<IKEIdentity> définit la valeur de chaîne qui fait correspondre le client à un profil IKEv2 spécifique sur le concentrateur (voir étape 4 ci-dessus).
Note: Le profil client est utilisé uniquement par le client. Il est recommandé qu'un administrateur utilise l'éditeur Anyconnect Profile afin de créer le profil client.

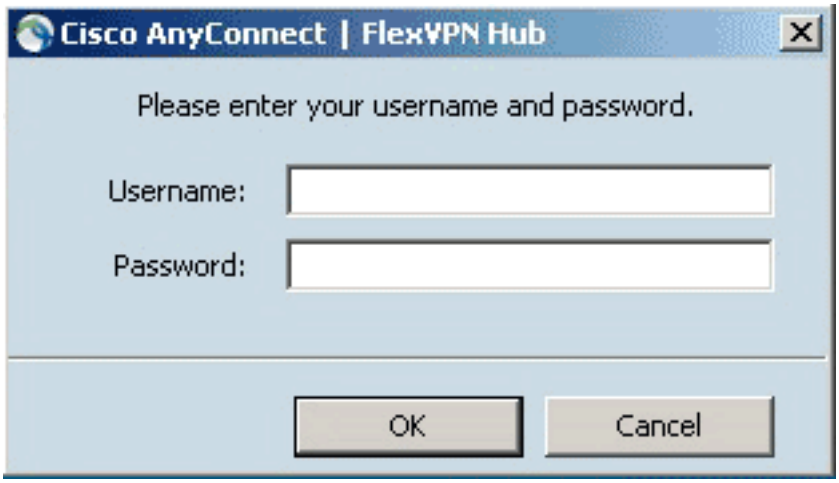
2. Enregistrez le fichier flexvpn.xml dans le répertoire approprié, comme indiqué dans ce tableau :

3. Fermez et redémarrez le client AnyConnect.



4. Dans la boîte de dialogue Cisco AnyConnect Secure Mobility Client, sélectionnez **FlexVPN Hub**, puis cliquez sur **Connect**.

Cisco AnyConnect | La boîte de dialogue FlexVPN Hub s'affiche.



5. Entrez un nom d'utilisateur et un mot de passe, puis cliquez sur **OK**.

Vérification

Afin de vérifier la connexion, utilisez la commande **show crypto session detail remote client-ipaddress**. Référez-vous à show crypto session pour plus d'informations sur cette commande.

> **Note**: L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande show .

Dépannage

Afin de dépanner la connexion, collectez et analysez les journaux DART du client et utilisez ces commandes de débogage sur le routeur : **debug crypto ikev2 packet** et **debug crypto ikev2 internal**.

> **Note**: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage.**

Informations connexes

- Support et documentation techniques - Cisco Systems