Configuratievoorbeeld van FlexVPN- en AnyConnect IKEv2-client

Inhoud

Inleiding

Dit document beschrijft hoe u Cisco AnyConnect Secure Mobility Client kunt configureren om gebruik te maken van externe verificatie, inbelgebruikersservice (RADIUS) en lokale autorisatie-eigenschappen om te authentiseren tegen Microsoft Active Directory.

> Opmerking: Op dit moment werkt het gebruik van de lokale gebruikersdatabase voor verificatie niet op Cisco IOS® apparaten. Dit komt doordat Cisco IOS niet fungeert als MAP-authenticator. Er is een verzoek om verbetering ingediend om ondersteuning toe te voegen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-versie 15.2(T) of hoger
- Cisco AnyConnect Secure Mobility Client versie 3.0 of hoger
- Microsoft Active Directory

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

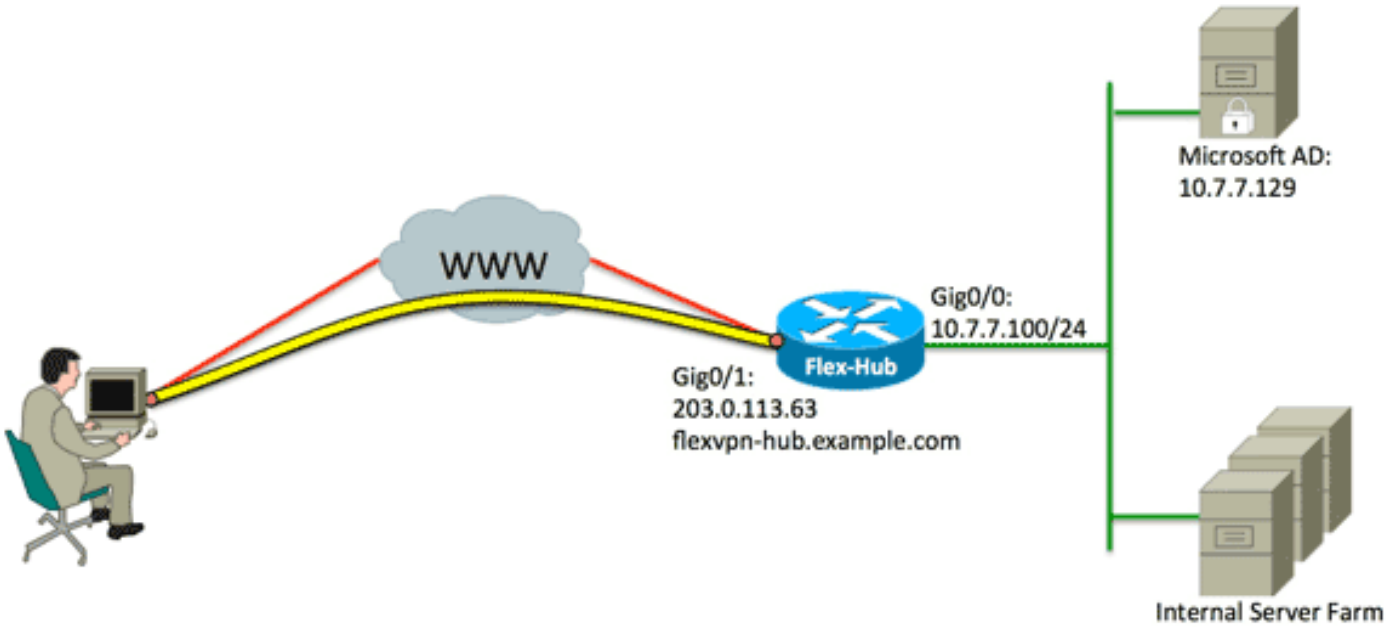
Configureren

In deze sectie wordt u voorzien van de informatie om de functies te configureren die in dit document worden beschreven.

Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

Hub-configuratie

1. RADIUS configureren voor alleen verificatie en lokale autorisatie definiëren.

```
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
```

   De opdracht in de **lijst met** verificatiegegevens verwijst naar de verificatie, autorisatie en accounting (AAA) groep (die de RADIUS-server definieert). De opdracht **van de** autorisatie-**netwerklijst** geeft aan dat lokaal gedefinieerde gebruikers/groepen moeten worden gebruikt. De configuratie op de RADIUS-server moet worden gewijzigd om authenticatieverzoeken van dit apparaat mogelijk te maken.

2. Configureer het lokale machtigingsbeleid.

```
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
```

   De **ip lokale pool** opdracht wordt gebruikt om de IP adressen te definiëren die aan de client worden toegewezen. Een vergunningsbeleid wordt gedefinieerd met een gebruikersnaam voor *FlexVPN-Local-Policy-1* en de eigenschappen voor de client (DNS-servers, netmask, gesplitste lijst, domeinnaam, enz.) worden hier geconfigureerd.

3. Zorg ervoor dat de server een certificaat (rsa-sig) gebruikt om zichzelf te authentificeren.

   Cisco AnyConnect Secure Mobility Client vereist dat de server zichzelf authentiek maakt met behulp van een certificaat (RSA-sig). De router moet beschikken over een *webservercertificaat* (dat wil zeggen een certificaat met 'serververificatie' binnen de uitgebreide toepassing) van een vertrouwde certificeringsinstantie (CA).

   Raadpleeg stap 1 tot en met 4 in ASA 8.x. Installeer de Verkrachters van de derde partij handmatig voor gebruik met het Configuratievoorbeeld van WebVPN en verander alle exemplaren van de *crypto-oplossing* naar *crypto-sleutel*.

```
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. Configureer de instellingen voor deze verbinding.

```
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
```

Het **crypto ikev2-**profiel bevat de meeste relevante instellingen voor deze verbinding: **Identificatie op afstand toetsen-id** - Hiermee wordt verwezen naar de IKE-identiteit die door de client wordt gebruikt. Deze string waarde wordt ingesteld in het AnyConnect XML-profiel.**Identity Local dn** - definieert de IKE-identiteit die wordt gebruikt door het FlexVPN-knooppunt. Deze waarde gebruikt de waarde van binnen het gebruikte certificaat.**verificatie op afstand** - staten dat MAP moet worden gebruikt voor de echtheidscontrole van cliënten.**lokale echtheidscontrole** - Staten dat certificaten voor lokale echtheid moeten worden gebruikt.**Een e-mail** over **verificatie** - Staten gebruiken voor de authenticatie van de loginloglijst FlexVPN-AuthC-List-1 wanneer EAP wordt gebruikt voor authenticatie.**Een lijst met vergunningverleningsgroepen** - Staten om de vergunningsnetwerklijst FlexVPN-AuthZ-List-1 te gebruiken met gebruikersnaam voor *FlexVPN-Local-Policy-1* voor vergunningskenmerken.**Virtual-sjabloon 10** - definieert welke sjabloon moet worden gebruikt wanneer een virtuele-toegangsinterface is gekloond.

5. Configuratie van een IPsec-profiel dat terugkoppelt naar het IKEv2-profiel dat in stap 4 is gedefinieerd.

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

Opmerking: Cisco IOS gebruikt slimme standaardwaarden. Als resultaat hiervan hoeft een transformatieset niet expliciet te worden gedefinieerd.

6. Configureer de virtuele sjabloon waaruit de virtuele toegangsinterfaces zijn gekloond: **ip ongenummerd -** Unnumber de interface van een *Inside*-interface zodat IPv4-routing op de interface kan worden ingeschakeld.**Tunnelmodus ipsec ipv4 -** definieert de interface om een VTI-type tunnel te zijn.

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

7. Beperk de onderhandeling tot SHA-1. (Optioneel)

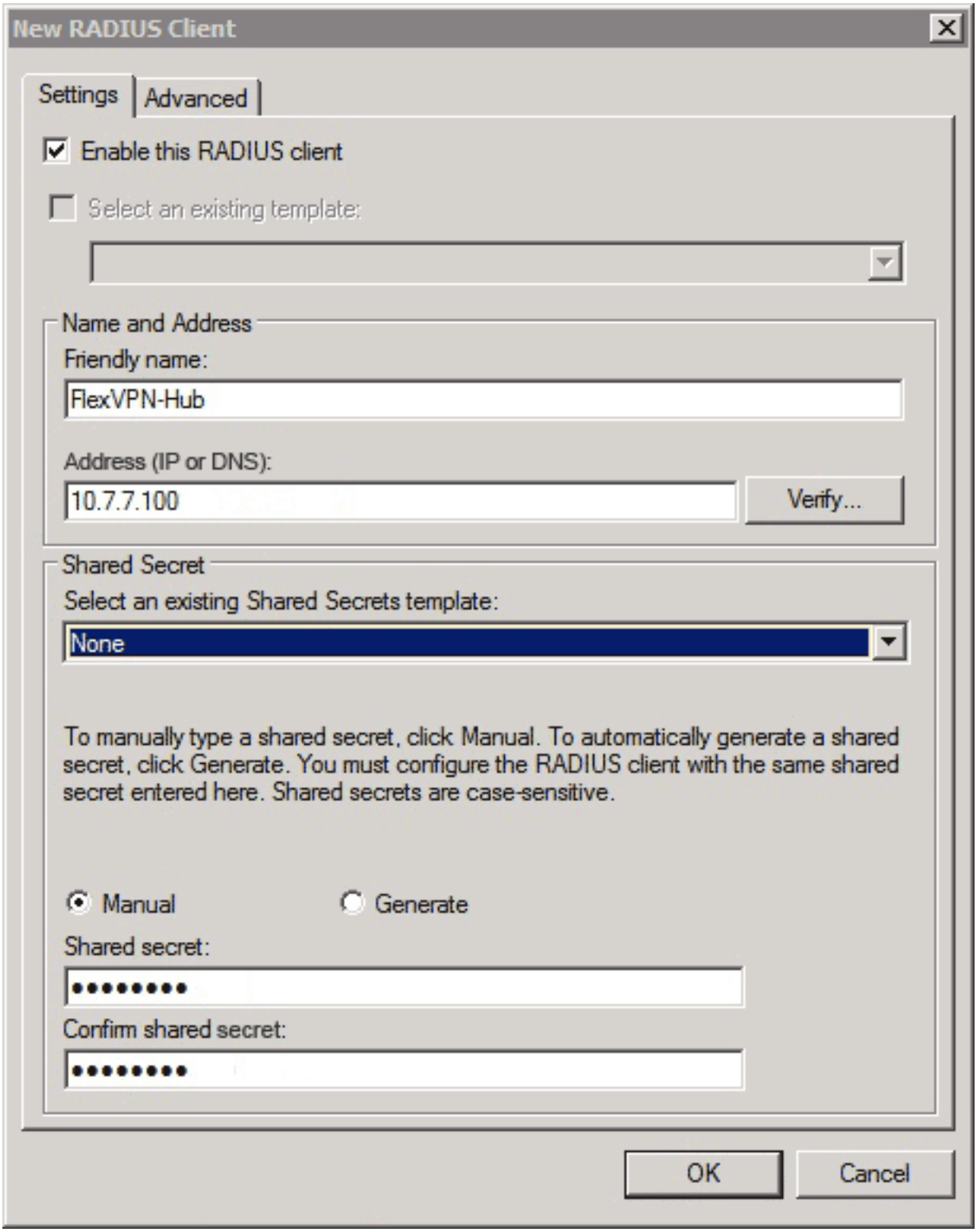
   Als gevolg van een defect CSCud96246 (alleen geregistreerde klanten) kan de AnyConnect-client er mogelijk niet in slagen het FlexVPN-hubcertificaat correct te valideren. Dit probleem is veroorzaakt doordat IKEv2 onderhandelt over een SHA-2-functie voor Pseudo-Random Functie (PRF) terwijl het FlexVPN-Hub certificaat is ondertekend met SHA-1. De configuratie hieronder beperkt de onderhandeling tot 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
```

Configuratie van Microsoft Active Directory Server

1. In Windows Server Manager **vouwt** u **rollen > Netwerkbeleid en toegangsserver > NMPS (lokaal) > RADIUS-clients en -servers uit** en klikt u op **RADIUS-clients**.

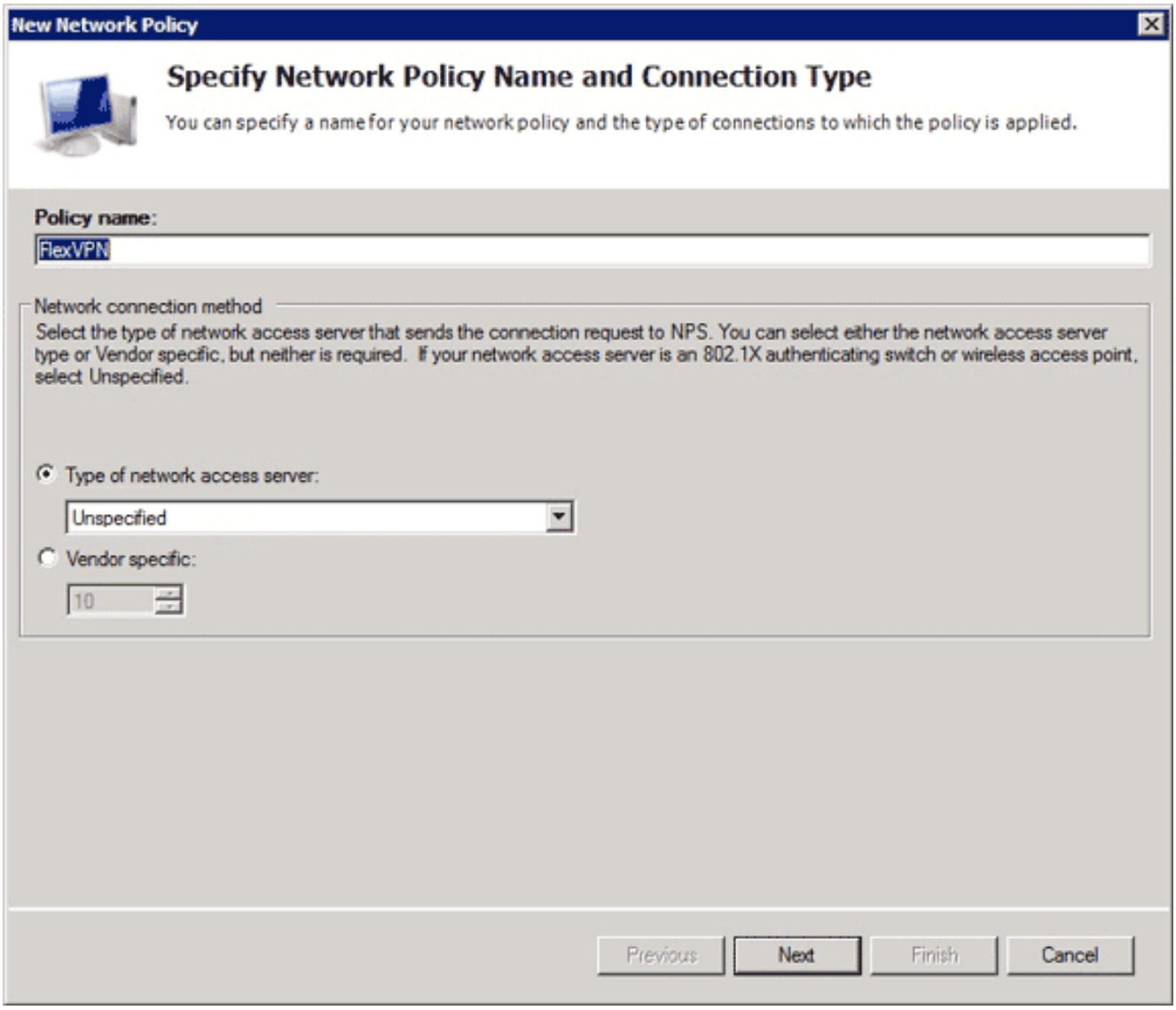
   Het dialoogvenster Nieuwe RADIUS-client wordt weergegeven.



2. In het dialoogvenster Nieuwe RADIUS-client voegt u de Cisco IOS-router toe als een RADIUS-client:
   Klik op het aanvinkvakje **RADIUS-client inschakelen**.Typ een naam in het veld Vriendelijke naam. Dit voorbeeld gebruikt *FlexVPN-Hub*.Voer het IP-adres van de router in het veld Adres in.In het Gedeelde Geheime gebied klik op de **Handmatige** radioknop, en voer het gedeelde geheim in het Gedeelde geheime gebied in en bevestig gedeelde geheime velden.**Opmerking:** het gedeelde geheim moet overeenkomen met het gedeelde geheim dat op de router is ingesteld.Klik op OK.

3. In de interface Server Manager **vouwt** u **beleid uit** en kiest u **Netwerkbeleid**.

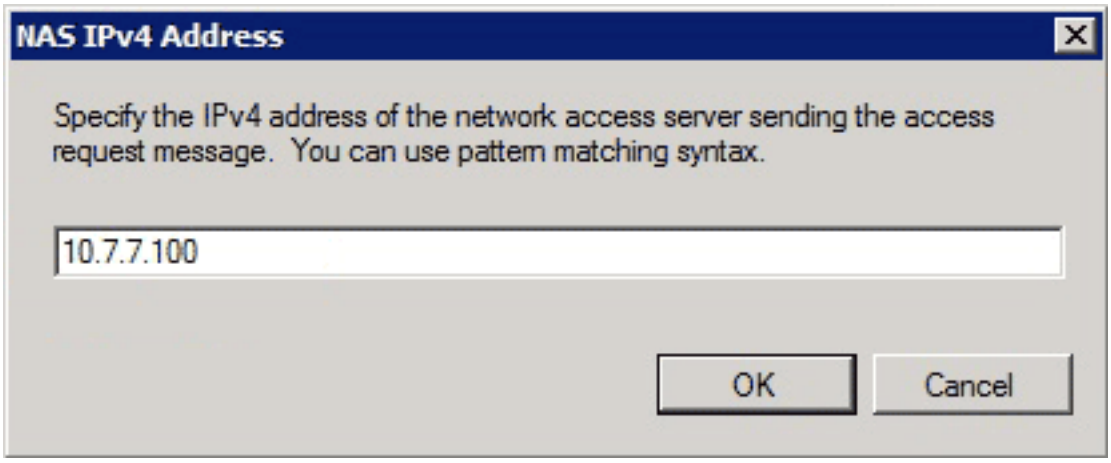
Het dialoogvenster Nieuw netwerkbeleid verschijnt.



4. In het dialoogvenster Nieuw netwerkbeleid kunt u een nieuw netwerkbeleid toevoegen:

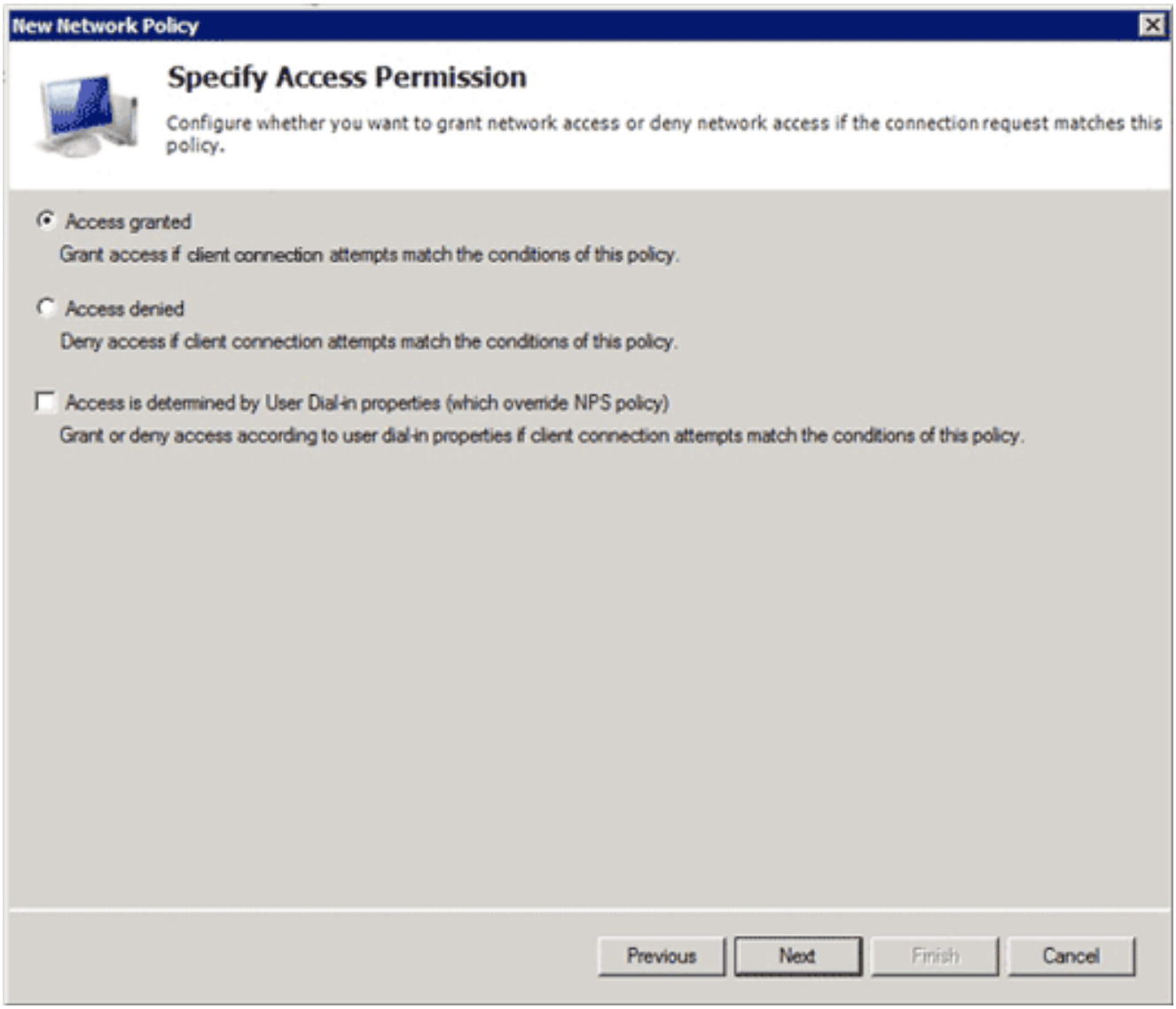
   Typ een naam in het veld Naam beleid. Dit voorbeeld gebruikt *FlexVPN*.Klik op de radioknop **Type of Network Access Server** en kies **Ongespecificeerd** in de vervolgkeuzelijst.Klik op **Volgende**.Klik in het dialoogvenster Nieuw netwerkbeleid op **Toevoegen** om een nieuwe voorwaarde toe te voegen.Selecteer in het dialoogvenster conditie selecteren de voorwaarde **NAS IPv4-adres** en klik op **Toevoegen**.

   Het dialoogvenster NAS IPv4-adres verschijnt.



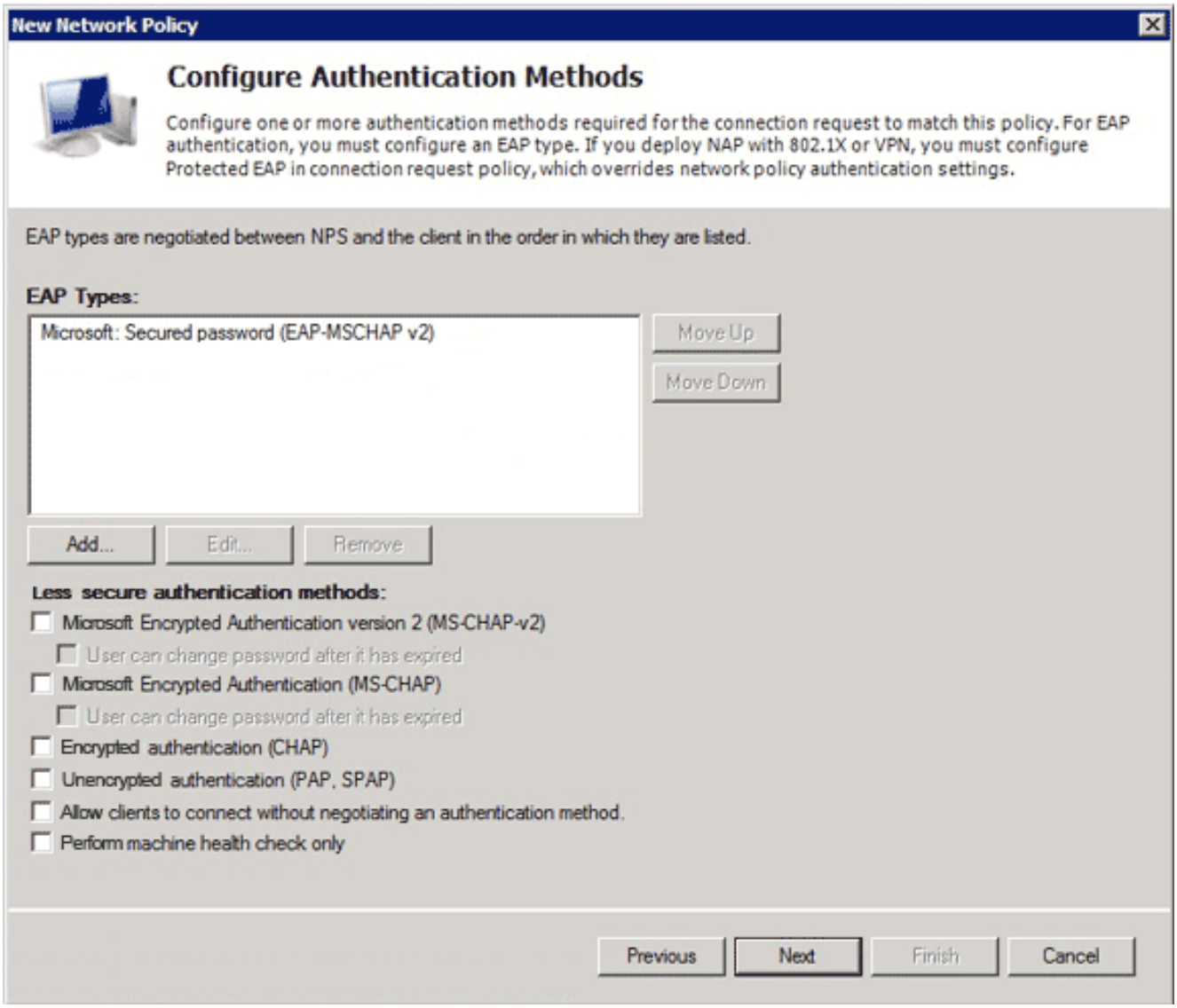
In het dialoogvenster NAS IPv4-adres specificeert u het IPv4-adres van de server voor netwerktoegang om het netwerkbeleid te beperken tot alleen verzoeken die afkomstig zijn van deze Cisco IOS-router.

Klik op OK.



In het nieuwe dialoogvenster Netwerkbeleid klikt u op de radioknop **Toegang verleend** om de klant toegang tot het netwerk te geven (als de door de gebruiker verstrekte

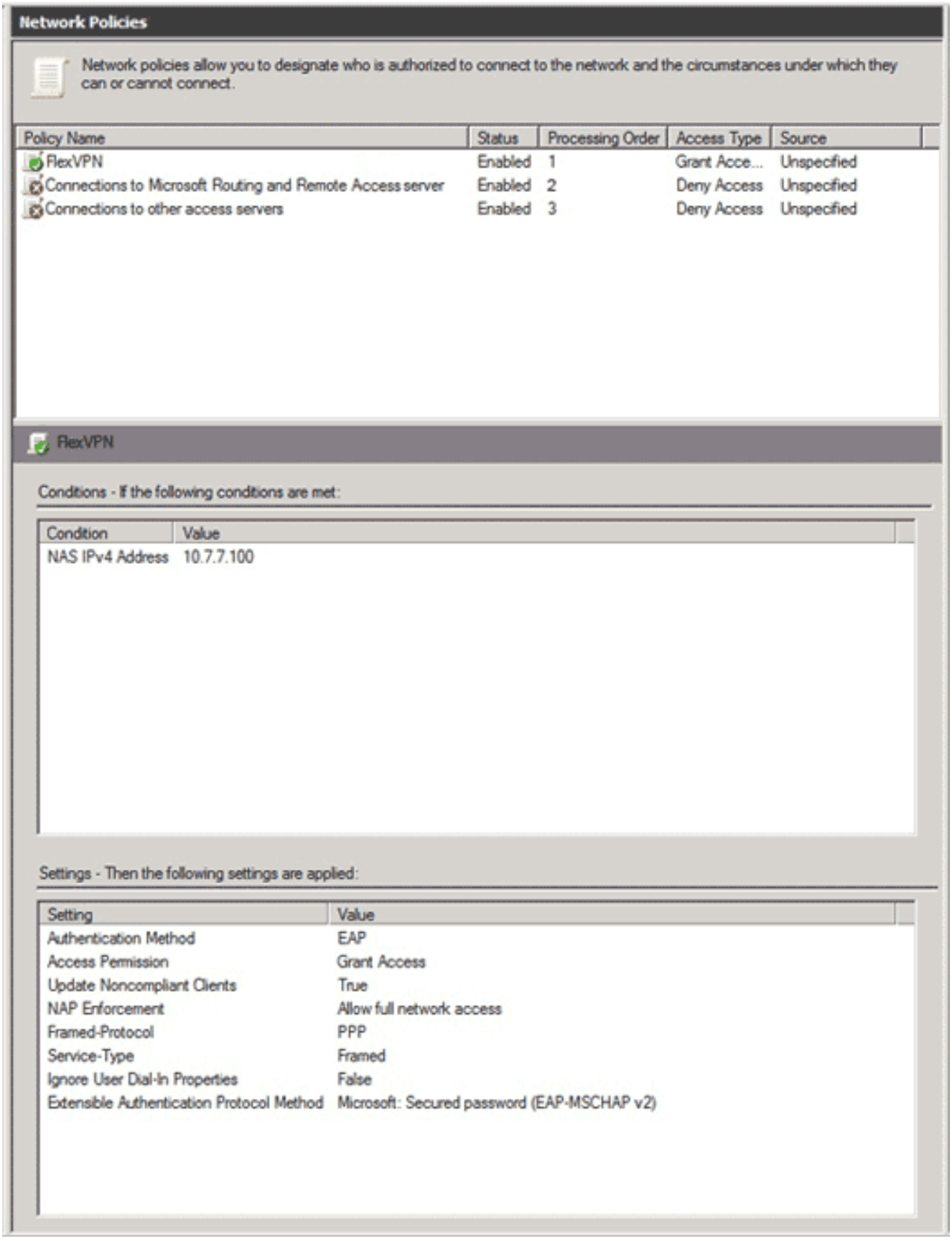
aanmeldingsgegevens geldig zijn) en vervolgens klikt u op **Volgende**.



Zorg ervoor dat alleen Microsoft: Het beveiligde wachtwoord (EAP-MSCHAP v2) verschijnt in het MAP Typen gebied om EAP-MSCHAPv2 als communicatiemethode tussen het Cisco IOS apparaat en de Actieve Map te gebruiken, en klik op **Volgende**.

Opmerking: Laat alle opties voor 'minder beveiligde authenticatiemethoden' ongecontroleerd.

Ga door de wizard en pas alle extra beperkingen of instellingen toe zoals gedefinieerd door het beveiligingsbeleid van uw organisatie. Zorg er bovendien voor dat het beleid als eerste in de verwerkingsvolgorde is opgenomen zoals in deze afbeelding:



Clientconfiguratie

1. Maak een XML-profiel binnen een teksteditor en noem het *flexvpn.xml*.

Dit voorbeeld gebruikt dit XML profiel:

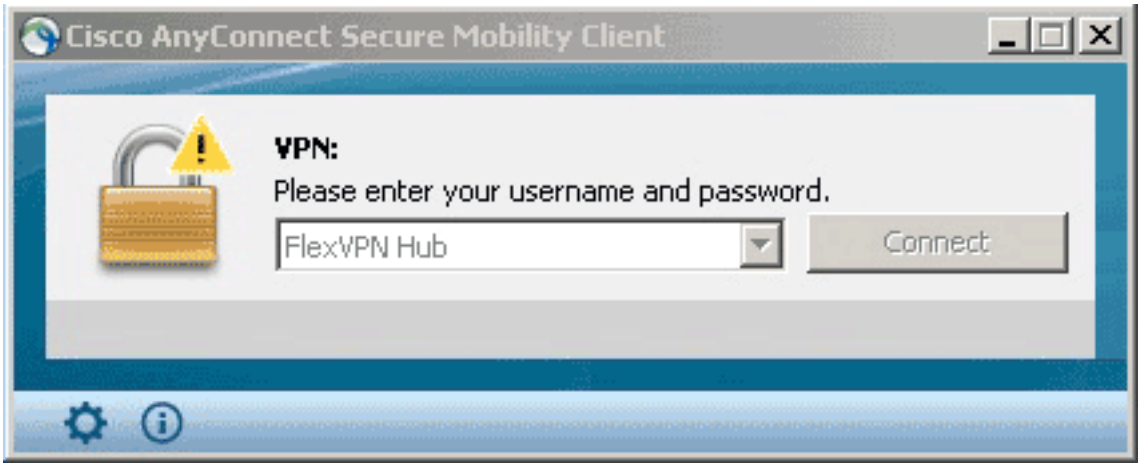
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false
</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> is een tekststring die in de client verschijnt.**<HostAddress>** is de volledig gekwalificeerde domeinnaam (FQDN) van het FlexVPN-knooppunt.**<PrimairProtocol>** vormt de verbinding om IKEv2/IPsec in plaats van SSL (de standaard in AnyConnect) te gebruiken.**<AuthMethodeDuringIKENonderhandeling>** vormt de verbinding om MSCHAPv2 binnen EAP te gebruiken. Deze waarde is vereist voor verificatie tegen Microsoft Active Directory.**<IKEIdentity>** definieert de string waarde die overeenkomt met de client voor een specifiek IKEv2-profiel op de hub (zie stap 4 hierboven).
Opmerking: Het clientprofiel is iets dat alleen door de cliënt wordt gebruikt. Aanbevolen wordt dat een beheerder de AnyConnect Profile editor gebruikt om het clientprofiel te maken.

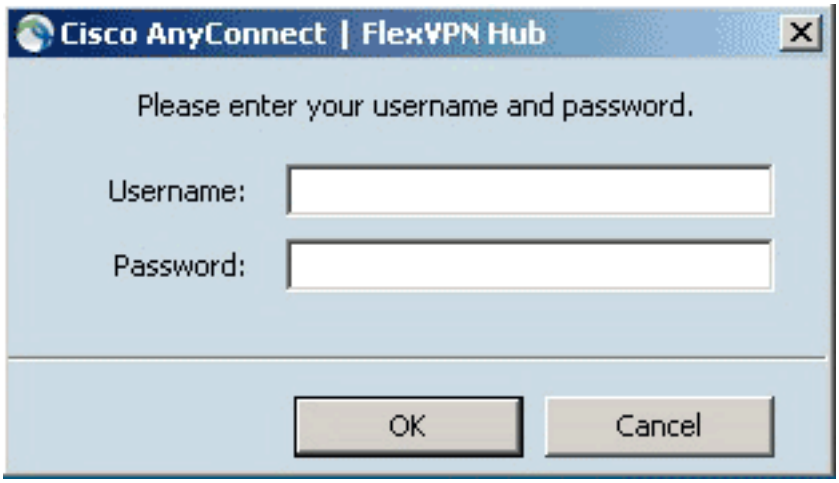
2. Sla het bestand flexvpn.xml in de juiste map op zoals in deze tabel wordt aangegeven:

3. Sluit de AnyConnect-client en start het programma opnieuw.



4. In het dialoogvenster Cisco AnyConnect Secure Mobility Client kiest u **FlexVPN-hub** en klikt u op **Connect**.

   Cisco AnyConnect | FlexVPN-hubdialoogvenster verschijnt.



5. Voer een gebruikersnaam en wachtwoord in en klik op **OK**.

Verifiëren

Om de verbinding te verifiëren, gebruik de opdracht van de **show crypto sessiedetails op afstand client-ipaddress**. Raadpleeg de cryptosessie voor meer informatie over deze opdracht.

> Opmerking: Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Problemen oplossen

Om de verbinding problemen op te lossen, verzamelt en analyseert u DART-logbestanden van de client en gebruikt u deze debug-opdrachten op de router: **debug crypto ikev2-pakje** en **debug crypto ikev2 interne**.

> Opmerking: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met debug opgeeft.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems