FlexVPN 및 AnyConnect IKEv2 클라이언트 컨피그레이션 예

목차

소개

이 문서에서는 Microsoft Active Directory에 대해 인증하기 위해 원격 인증 전화 접속 사용자 서비스(RADIUS) 및 로컬 권한 부여 특성을 사용하도록 Cisco AnyConnect Secure Mobility Client를 구성하는 방법에 대해 설명합니다.

> **참고:**현재 인증을 위해 로컬 사용자 데이터베이스를 사용하는 것은 Cisco IOS® 디바이스에서 작동하지 않습니다.이는 Cisco IOS가 EAP 인증자로 작동하지 않기 때문입니다.지원을 추가하기 위한 개선 요청 CSCui07025가 접수되었습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS 버전 15.2(T) 이상
- Cisco AnyConnect Secure Mobility Client 버전 3.0 이상
- Microsoft Active Directory

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

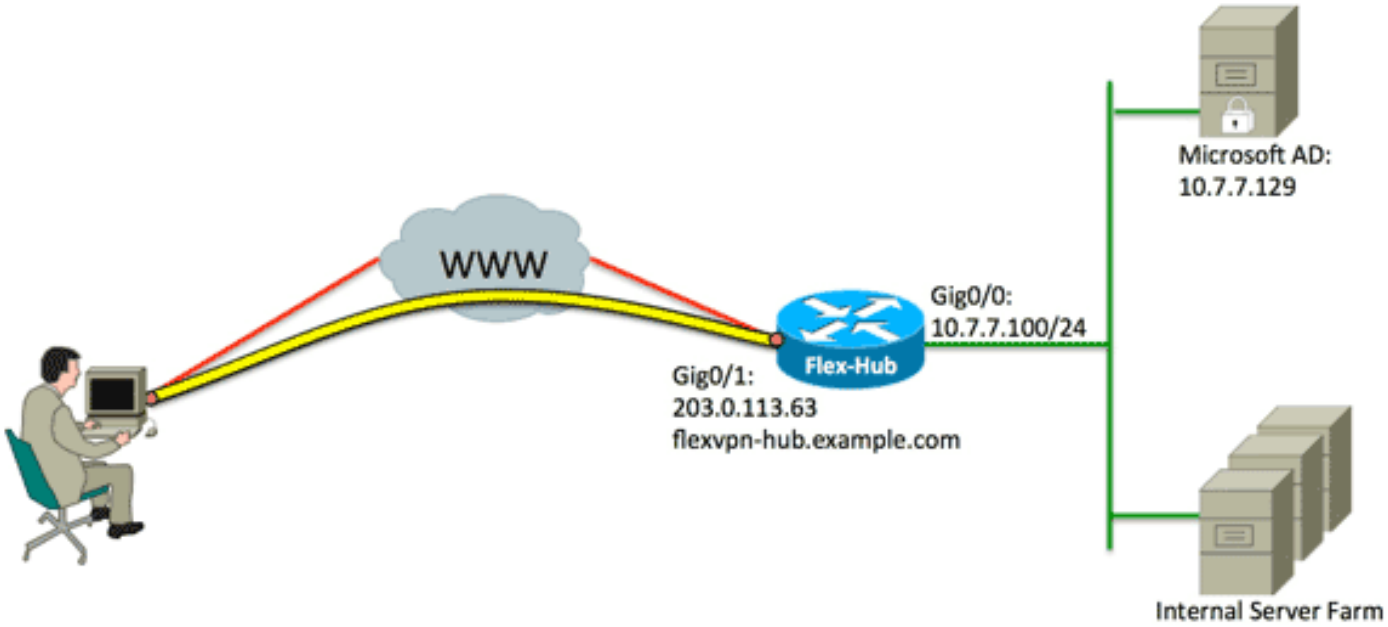
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하기 위한 정보가 제공됩니다.

이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- 허브 구성

- Microsoft Active Directory 서버 구성
- 클라이언트 구성

허브 구성

1. 인증에만 RADIUS를 구성하고 로컬 권한 부여를 정의합니다.

```
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** 명령은 RADIUS 서버를 정의하는 AAA(authentication, authorization, and accounting) 그룹을 참조합니다. aaa **authorization network list** 명령은 로컬에서 정의된 사용자/그룹을 사용할 것임을 나타냅니다.이 디바이스의 인증 요청을 허용하려면 RADIUS 서버의 컨피그레이션을 변경해야 합니다.

2. 로컬 권한 부여 정책을 구성합니다.

```
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** 명령은 클라이언트에 할당된 IP 주소를 정의하는 데 사용됩니다.권한 부여 정책은 사용자 이름 *FlexVPN-Local-Policy-1로 정의되며* 클라이언트(DNS 서버, 넷마스크, 분할 목록, 도메인 이름 등)에 대한 특성이 여기에 구성됩니다.

3. 서버에서 자체 인증을 위해 인증서(rsa-sig)를 사용하는지 확인합니다.

Cisco AnyConnect Secure Mobility Client에서는 서버가 인증서(rsa-sig)를 사용하여 자신을 인증해야 합니다. 라우터에는 신뢰할 수 있는 CA(인증 기관)의 *웹 서버* 인증서(즉, 확장된 키 사용 확장 내에 '서버 인증'이 있는 인증서)가 있어야 합니다.

WebVPN 컨피그레이션 예제에 사용할 수 있도록 ASA 8.x Manually Install third Party Vendor Certificates(ASA 8.x 수동 타사 벤더 인증서 설치)의 단계 1~4를 참조하고, *crypto ca*의 모든 인스턴스를 crypto pki로 *변경합니다*.

```
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. 이 연결에 대한 설정을 구성합니다.

```
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 ikev**2** 프로필에는 이 연결에 대한 대부분의 관련 설정이 포함되어 있습니다. **match identity remote key-id** - 클라이언트에서 사용하는 IKE ID를 참조합니다.이 문자열 값은 AnyConnect XML 프로파일 내에서 구성됩니다.**identity local dn** - FlexVPN 허브에서 사용되는 IKE ID를 정의합니다.이 값은 사용된 인증서 내의 값을 사용합니다.**authentication remote** - 클라이언트 인증에 EAP를 사용해야 함을 나타냅니다.**authentication local** - 로컬 인증에 인증서를 사용해야 함을 나타냅니다.**aaa authentication eap** - EAP가 인증에 사용될 때 aaa authentication login list FlexVPN-AuthC-List-1을 사용할 상태입니다.**aaa authorization group eap list** - aaa authorization network list FlexVPN-AuthZ-List-1을 권한 부여 특성에 대해 사용자 이름*의 FlexVPN-Local-Policy-1과* 함께 사용하도록 하는 상태입니다.**virtual-template 10** - 가상 액세스 인터페이스가 복제될 때 사용할 템플릿을 정의합니다.

5. 4단계에서 정의한 IKEv2 프로파일로 다시 연결되는 IPsec 프로파일을 구성합니다.

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

참고: Cisco IOS는 스마트 기본값을 사용합니다.따라서 변형 집합을 명시적으로 정의할 필요가 없습니다.

6. 가상 액세스 인터페이스가 복제되는 가상 템플릿을 구성합니다.
ip unnumbered - 인터페이스에서 IPv4 라우팅을 활성화할 수 있도록 *Inside* 인터페이스에서 인터페이스의 번호를 해제합니다.**tunnel mode ipsec ipv4 -** 인터페이스를 VTI 유형 터널로 정의합니다.

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

7. 협상을 SHA-1로 제한합니다(선택 사항).

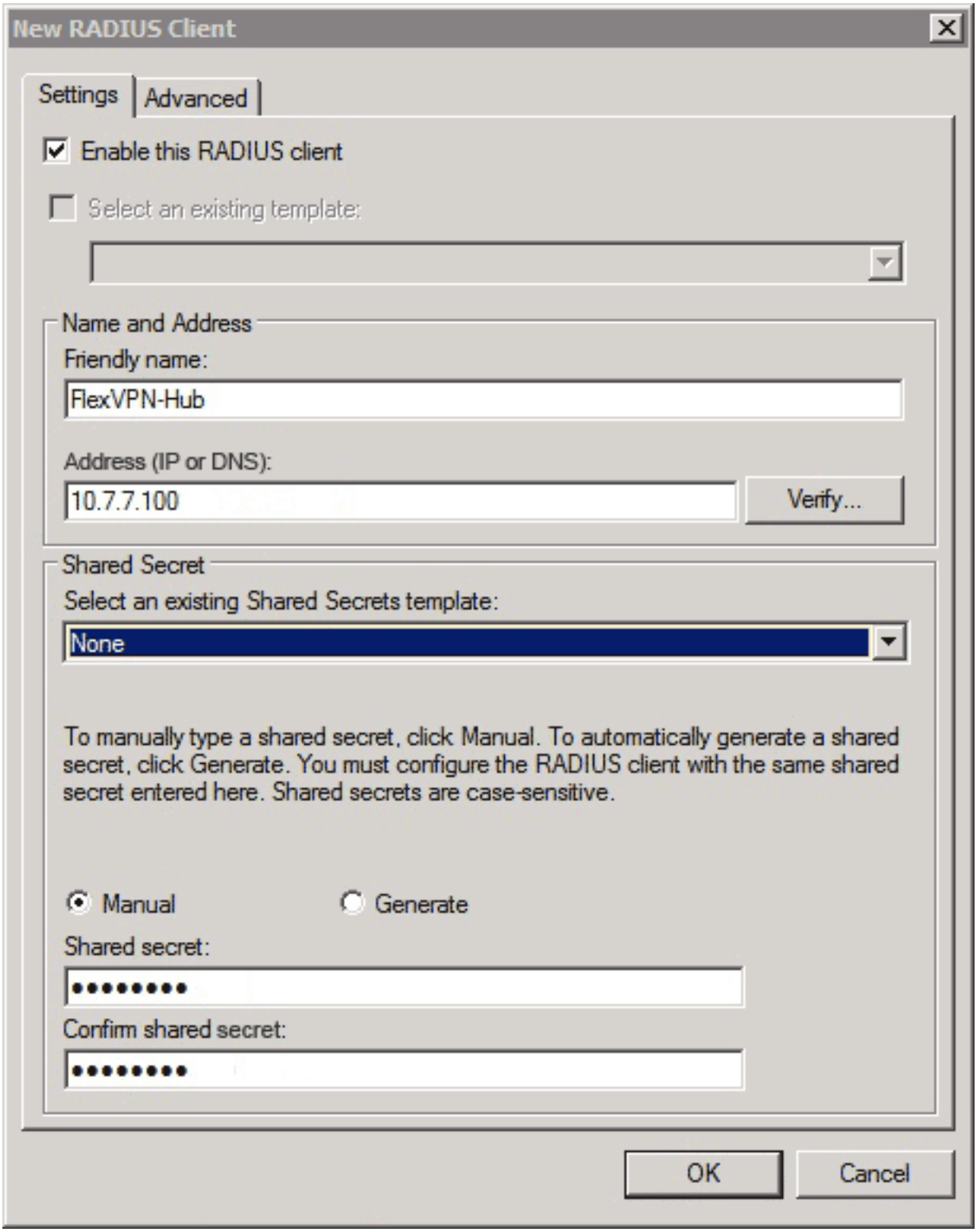
결함 CSCud96246(등록된 고객만 해당) 때문에 AnyConnect 클라이언트가 FlexVPN 허브 인증서의 유효성을 올바르게 검증하지 못할 수 있습니다.이 문제는 IKEv2가 PRF(Pseudo-Random Function)에 대해 SHA-2 기능을 협상하는 반면 FlexVPN-Hub 인증서는 SHA-1을 사용하여 서명되었기 때문입니다. 아래 컨피그레이션에서는 협상을 SHA-1로 제한합니다.

```
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 서버 구성

1. Windows Server Manager에서 Roles(역할) **> Network Policy and Access Server(네트워크 정책 및 액세스 서버) > NMPS(로컬) > RADIUS Clients and Servers(RADIUS 클라이언트 및 서버)를** 확장하고 **RADIUS Clients(RADIUS 클라이언트)**를 클릭합니다.

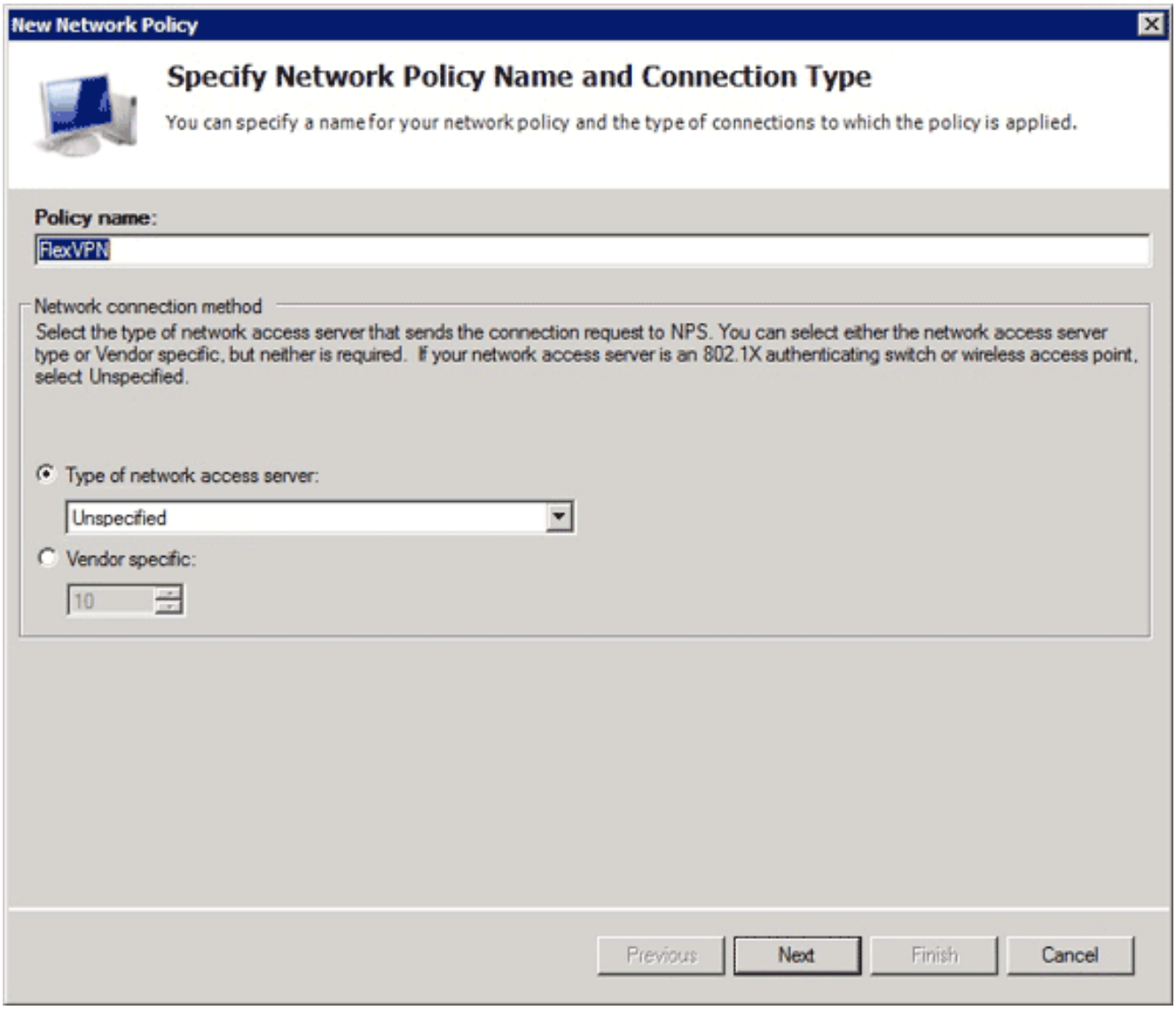
   New RADIUS Client 대화 상자가 나타납니다.



2. New RADIUS Client(새 RADIUS 클라이언트) 대화 상자에서 Cisco IOS 라우터를 RADIUS 클라이언트로 추가합니다.
   Enable this **RADIUS client(이 RADIUS 클라이언트 활성화)** 확인란을 클릭합니다.이름 필드에 이름을 입력합니다.이 예에서는 *FlexVPN-Hub를 사용합니다.*Address 필드에 라우터의 IP 주소를 입력합니다.Shared Secret(공유 암호) 영역에서 **Manual(수동)** 라디오 버튼을 클릭하고 Shared secret(공유 암호) 및 Confirm shared secret(공유 암호 확인) 필드에 공유 암호를 입력합니다.**참고:** 공유 암호는 라우터에 구성된 공유 암호와 일치해야 합니다.**확인을 클릭합니다**.

3. Server Manager(서버 관리자) 인터페이스에서 Policies(**정책**)를 확장하고 **Network Policies(네트워크 정책)를** 선택합니다.

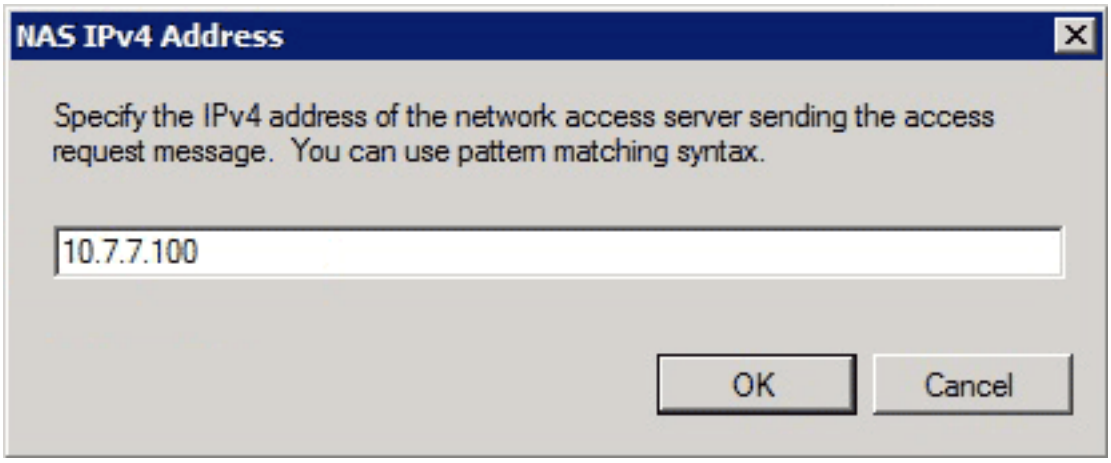
New Network Policy 대화 상자가 나타납니다.



4. New Network Policy(새 네트워크 정책) 대화 상자에서 새 네트워크 정책을 추가합니다.

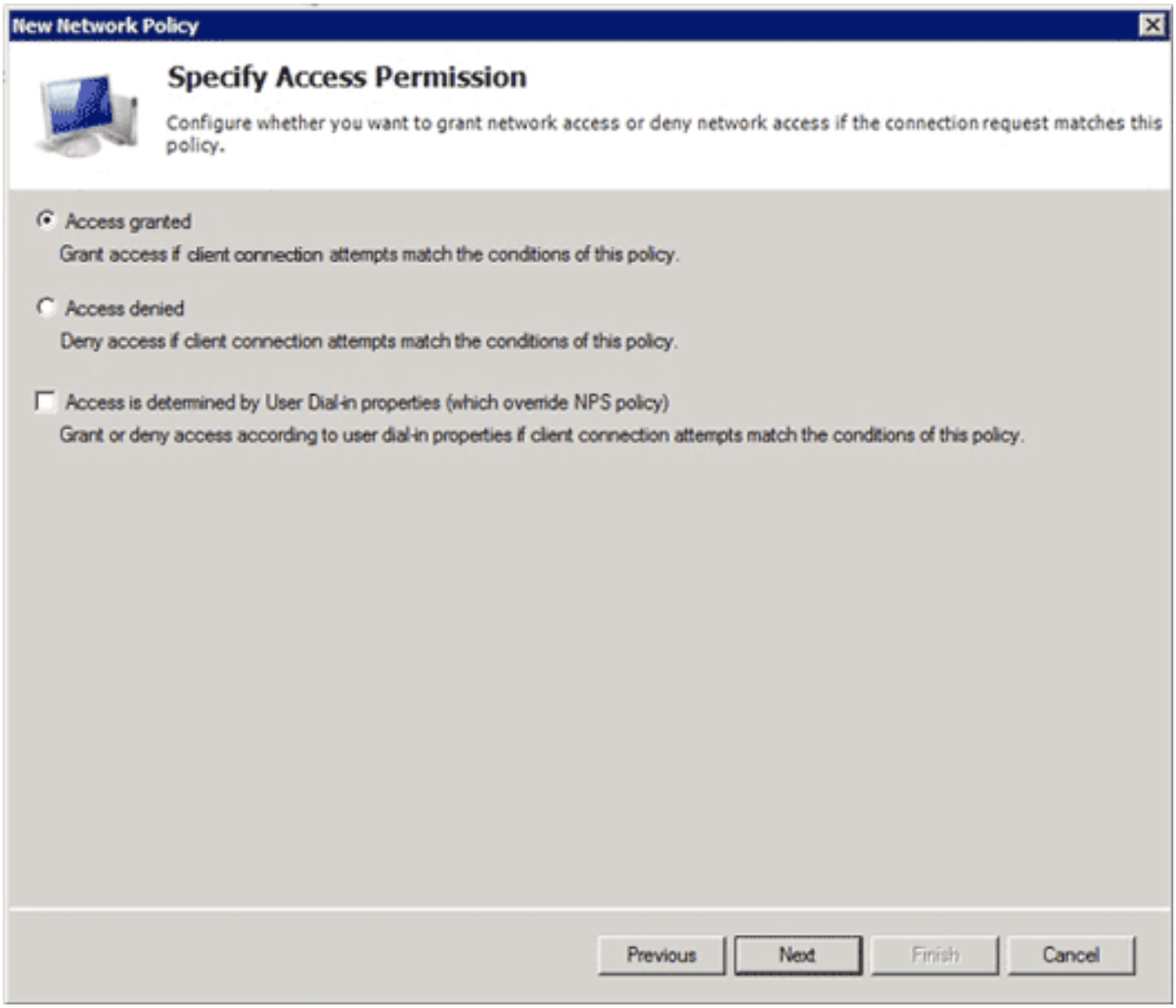
   Policy name 필드에 이름을 입력합니다.이 예에서는 FlexVPN을 *사용합니다*.**Type of network access server(네트워크 액세스 서버 유형)** 라디오 버튼을 클릭하고 드롭다운 목록에서 Unspecified(미지정)를 선택합니다.Next(**다음)를 클릭합니다**.New Network Policy(새 네트워크 정책) 대화 상자에서 Add(**추가**)를 클릭하여 새 조건을 추가합니다.Select condition(조건 선택) 대화 상자에서 **NAS IPv4 Address(NAS IPv4 주소**) 조건을 선택하고 Add(**추가)**를 클릭합니다.

   NAS IPv4 Address 대화 상자가 나타납니다.

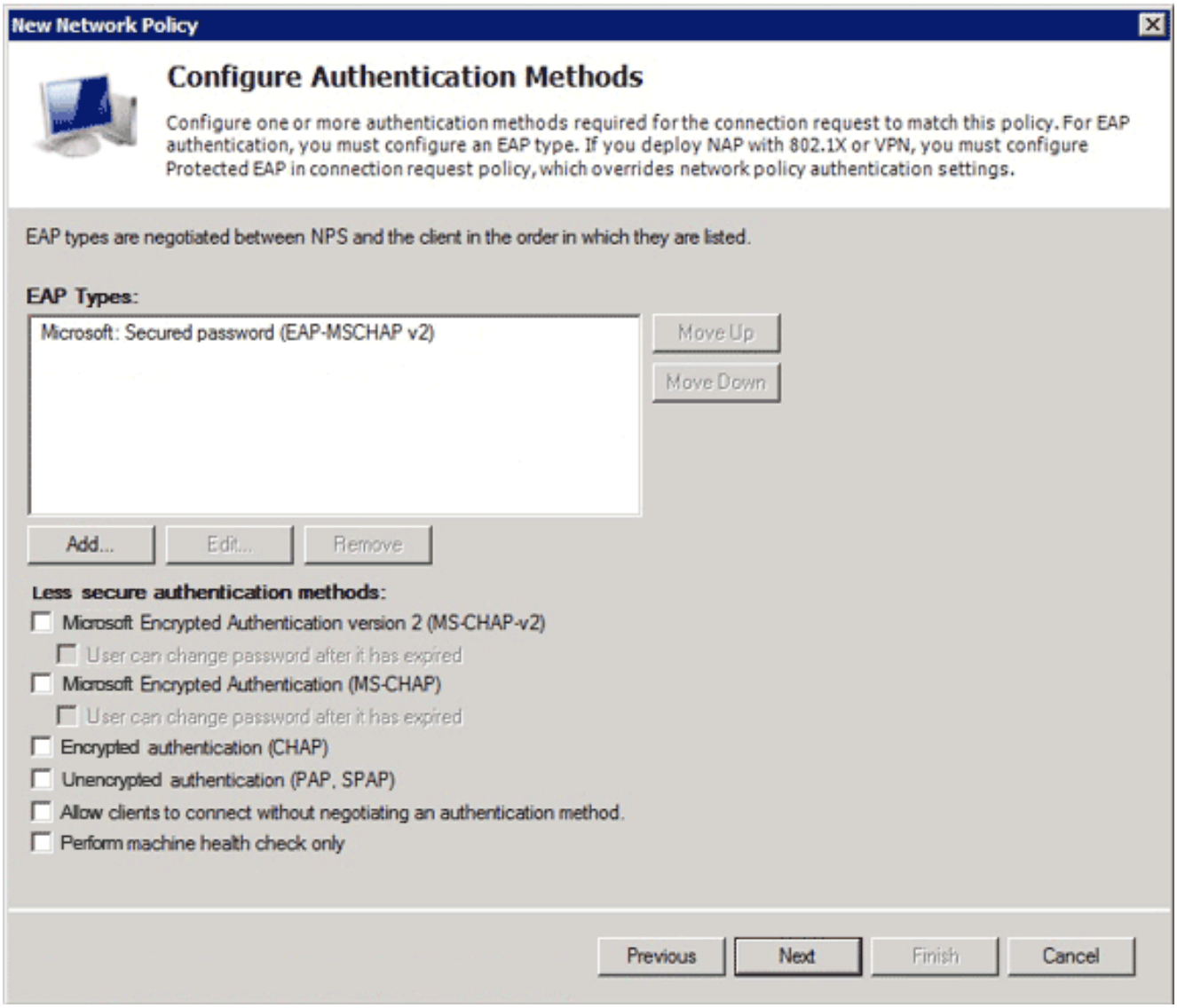


네트워크 정책을 이 Cisco IOS 라우터에서 시작된 요청만 제한하려면 네트워크 액세스 서버의 IPv4 주소를 NAS IPv4 주소 대화 상자에 입력합니다.

확인을 **클릭합니다**.



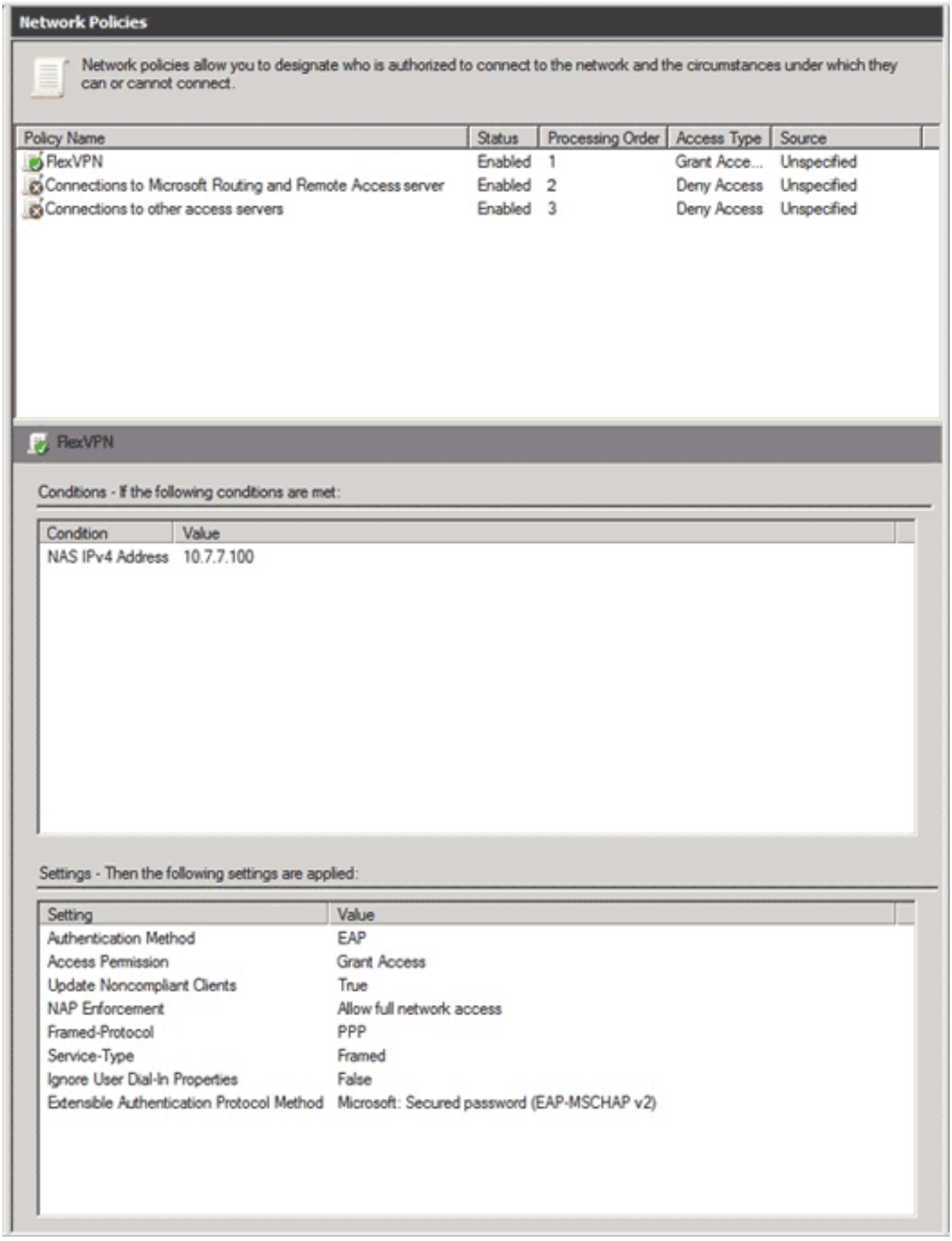
새 Network Policy(네트워크 정책) 대화 상자에서 클라이언트가 네트워크에 액세스할 수 있도록 허용하려면 **Access granted(액세스 부여됨)** 라디오 버튼을 클릭하고(사용자가 제공한 자격 증명이 유효한 경우) **Next(다음)**를 클릭합니다.



Microsoft만 확인:EAP-MSCHAPv2를 Cisco IOS 디바이스와 Active Directory 간의 통신 방법으로 사용하도록 허용하기 위해 보안 암호(EAP-MSCHAP v2)가 EAP Types(EAP 유형) 영역에 나타나고 **Next(다음)를** 클릭합니다.

참고:모든 'Less secure authentication methods' 옵션을 선택하지 않은 상태로 둡니다.

마법사를 계속 진행하고 조직 보안 정책에 정의된 추가 제약 조건 또는 설정을 적용합니다.또한 이 이미지에 표시된 대로 처리 순서에서 정책이 먼저 나열되는지 확인합니다.



클라이언트 구성

1. 텍스트 편집기 내에서 XML 프로파일을 생성하고 이름을 flexvpn.*xml로 지정합니다*.

이 예에서는 다음 XML 프로파일을 사용합니다.

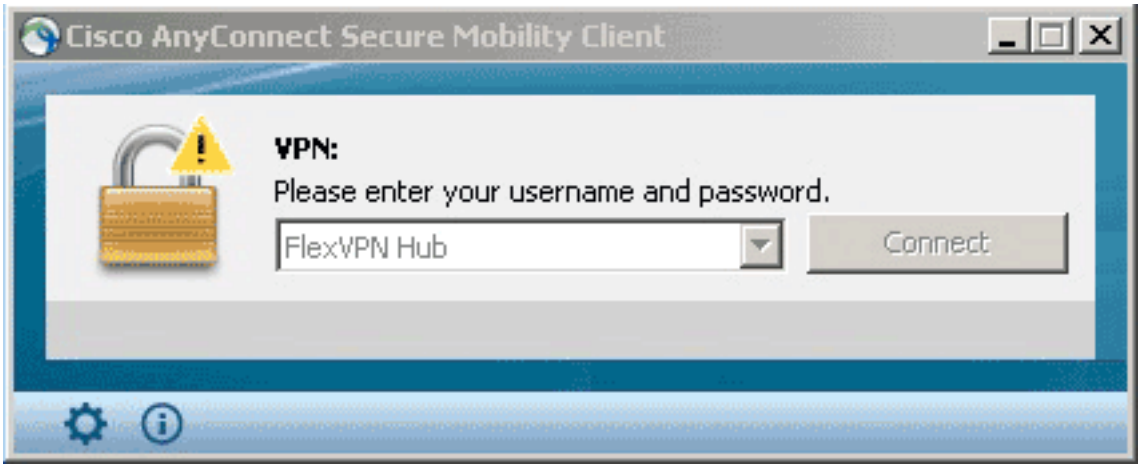
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false
</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>은 클라이언트에 나타나는 텍스트 문자열입니다.<HostAddress>는 FlexVPN 허브의 FQDN(정규화된 도메인 이름)입니다.<PrimaryProtocol>은 SSL 대신 IKEv2/IPsec을 사용하도록 연결을 구성합니다(AnyConnect의 기본값).<AuthMethodDuringIKENegotiation>은 EAP 내에서 MSCHAPv2를 사용하도록 연결을 구성합니다.이 값은 Microsoft Active Directory에 대한 인증에 필요합니다.<IKEIdentity>는 허브의 특정 IKEv2 프로파일과 클라이언트를 일치시키는 문자열 값을 정의합니다(위의 4단계 참조).
참고:클라이언트 프로파일은 클라이언트에서만 사용되는 것입니다.관리자는 클라이언트 프로파일을 생성하기 위해 Anyconnect 프로파일 편집기를 사용하는 것이 좋습니다.

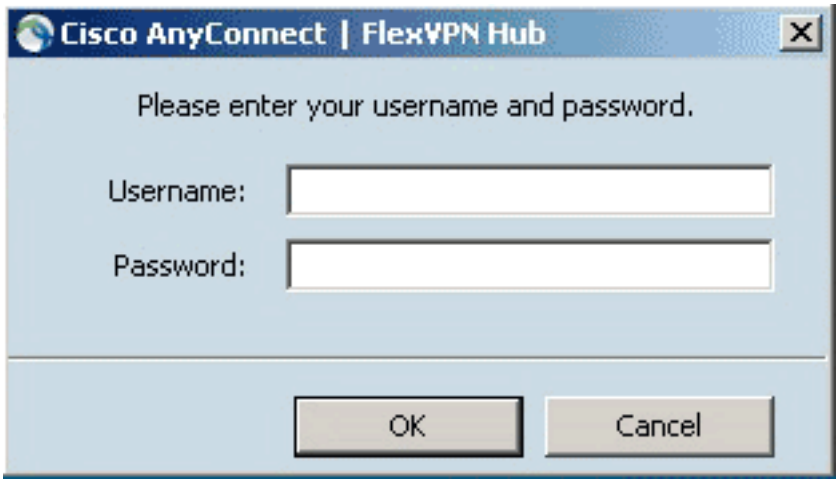
2. 다음 표에 나열된 대로 flexvpn.xml 파일을 적절한 디렉토리에 저장합니다.

3. AnyConnect 클라이언트를 닫고 다시 시작합니다.



4. Cisco AnyConnect Secure Mobility Client(Cisco AnyConnect Secure Mobility 클라이언트) 대화 상자에서 **FlexVPN Hub(FlexVPN 허브)**를 선택하고 **Connect(연결)**를 클릭합니다.

Cisco AnyConnect | FlexVPN Hub 대화 상자가 나타납니다.



5. 사용자 이름과 비밀번호를 입력하고 **OK**(확인)를 클릭합니다.

다음을 확인합니다.

연결을 확인하려면 show crypto session detail **remote client-ipaddress** 명령**을** 사용합니다.이 명령에 대한 자세한 내용은 show crypto session을 참조하십시오.

> **참고:**Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

문제 해결

연결 문제를 해결하려면 클라이언트에서 DART 로그를 수집 및 분석하고 라우터에서 다음 디버그 명령을 사용합니다. debug crypto ikev**2 packet** 및 debug crypto ikev**2 internal**.

> **참고:debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

관련 정보

- 기술 지원 및 문서 – Cisco Systems