FlexVPN および AnyConnect IKEv2 クライアントの設定例

内容

概要

このドキュメントでは、Microsoft Active Directory に対する認証のために、Remote Authentication Dial-In User Service（RADIUS）とローカルの認証属性を使用するように、Cisco AnyConnect セキュア モビリティ クライアントを設定する方法について説明します。

> **注**：現在、認証用のローカル ユーザ データベースの使用は、Cisco IOS® デバイスでは機能しません。これは、Cisco IOS が EAP オーセンティケータとして機能しないためです。機能拡張要求 CSCui07025 が、サポートを追加するために提出されました。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS バージョン 15.2(T) 以降
- Cisco AnyConnect セキュア モビリティ クライアント バージョン 3.0 以降
- Microsoft Active Directory

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

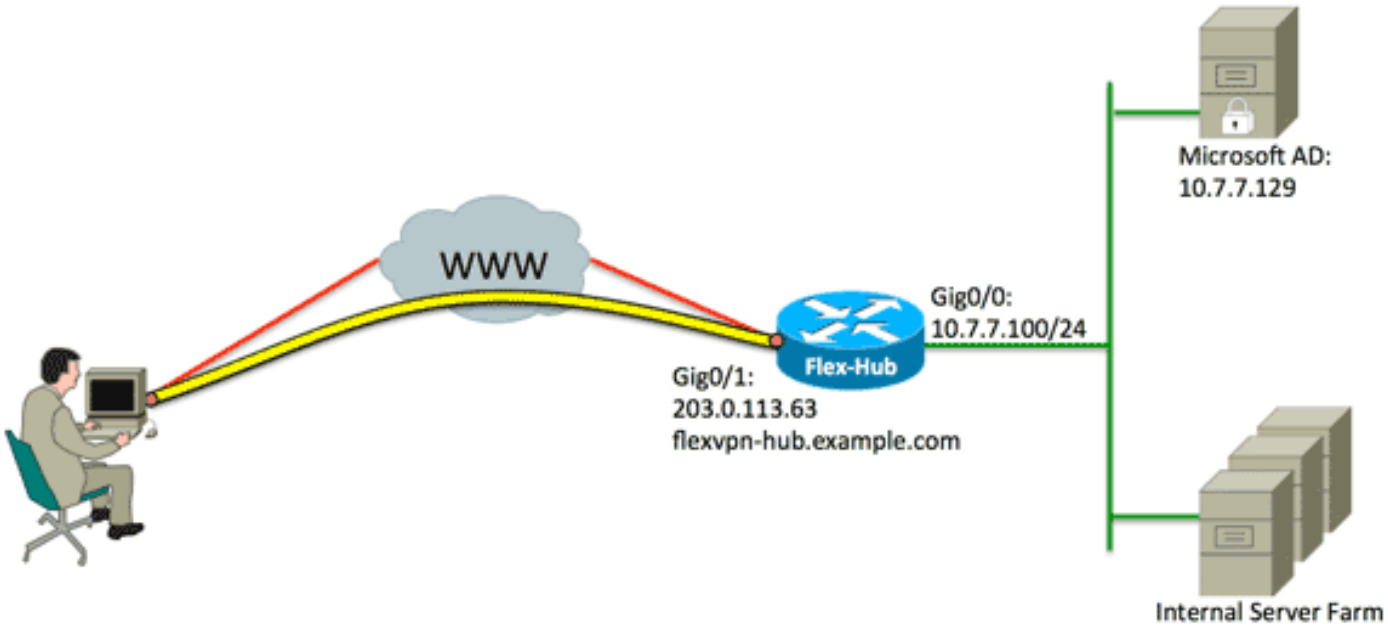
設定

ここでは、このドキュメントで説明する機能を設定するための情報を示します。

このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

ハブ設定

1. RADIUS を認証用にのみ設定し、ローカル認証を定義します。

```
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 コマンドは、認証、許可、およびアカウンティング（AAA）グループ（RADIUS サーバを定義する）を参照します。 aaa authorization network list コマンドは、ローカルに定義されたユーザ/グループを使用する必要があることを明示します。 RADIUS サーバの設定は、このデバイスから認証要求を行えるように変更する必要があります。

2. ローカル認証ポリシーを設定します。

```
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 コマンドは、クライアントに割り当てる IP アドレスを定義するために使用されます。認証ポリシーは、*FlexVPN-Local-Policy-1* のユーザ名で定義され、クライアント（DNS サーバ、ネットマスク、分割されたリスト、ドメイン名など）の属性がここで設定されます。

3. サーバがサーバ自体を認証するために証明書（rsa-sig）を使用していることを確認してください。

Cisco AnyConnect セキュア モビリティ クライアントには、証明書（rsa-sig）を使用してサーバ自体を認証しているサーバが必要です。 ルータは、信頼できる認証局（CA）から *Web サーバの証明書（つまり、拡張キー使用法の拡張内の「サーバ認証」による証明書）を取得する必要があります。*

「ASA 8.x WebVPN で使用するサードパーティ ベンダーの証明書を手動でインストールする設定例」のステップ 1 ～ 4 を参照して、*crypto ca* のすべてのインスタンスを *crypto pki* に変更します。

```
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. この接続の設定を構成します。

```
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 profile には、以下に記載するとおり、この接続に関連するほとんどの設定が含まれています。 match identity remote key-id：クライアントが使用する IKE ID を参照します。この文字列値は、AnyConnect XML プロファイル内に設定されます。**identity local dn：FlexVPN ハブで使用する IKE ID を定義します。**この値は、使用する証明書内の値を使用します。**authentication remote：クライアント認証に EAP を使用する必要があることを明示します。authentication local：ローカル認証に証明書を使用する必要があることを明示します。aaa authentication eap：EAP を認証に使用する場合、aaa authentication login list FlexVPN-AuthC-List-1 を使用することを明示します。aaa authorization group eap list：認可属性に** *FlexVPN-Local-Policy-1 のユーザ名を含む aaa authorization network list FlexVPN-AuthZ-List-1 を使用することを明示します。***virtual-template 10：仮想アクセス インターフェイスがクローンされるときに使用するテンプレートを定義します。**

5. ステップ 4.で定義した IKEv2 プロファイルに戻るようにリンク付けされる IPsec プロファイルを設定します。

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

注：Cisco IOS は、スマート デフォルトを利用します。その結果、トランスフォーム設定を明示的に定義する必要はありません。

6. 仮想アクセス インターフェイスがクローンされる仮想テンプレートを設定します。
ip unnumbered：インターフェイス上で IPv4 ルーティングを有効化できるように、*内部インターフェイスからのインターフェイスをアンナンバーにします。***tunnel mode ipsec ipv4**：インターフェイスを VTI タイプのトンネルとして定義します。

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

7. ネゴシエーションをSHA-1に制限します（オプション）。

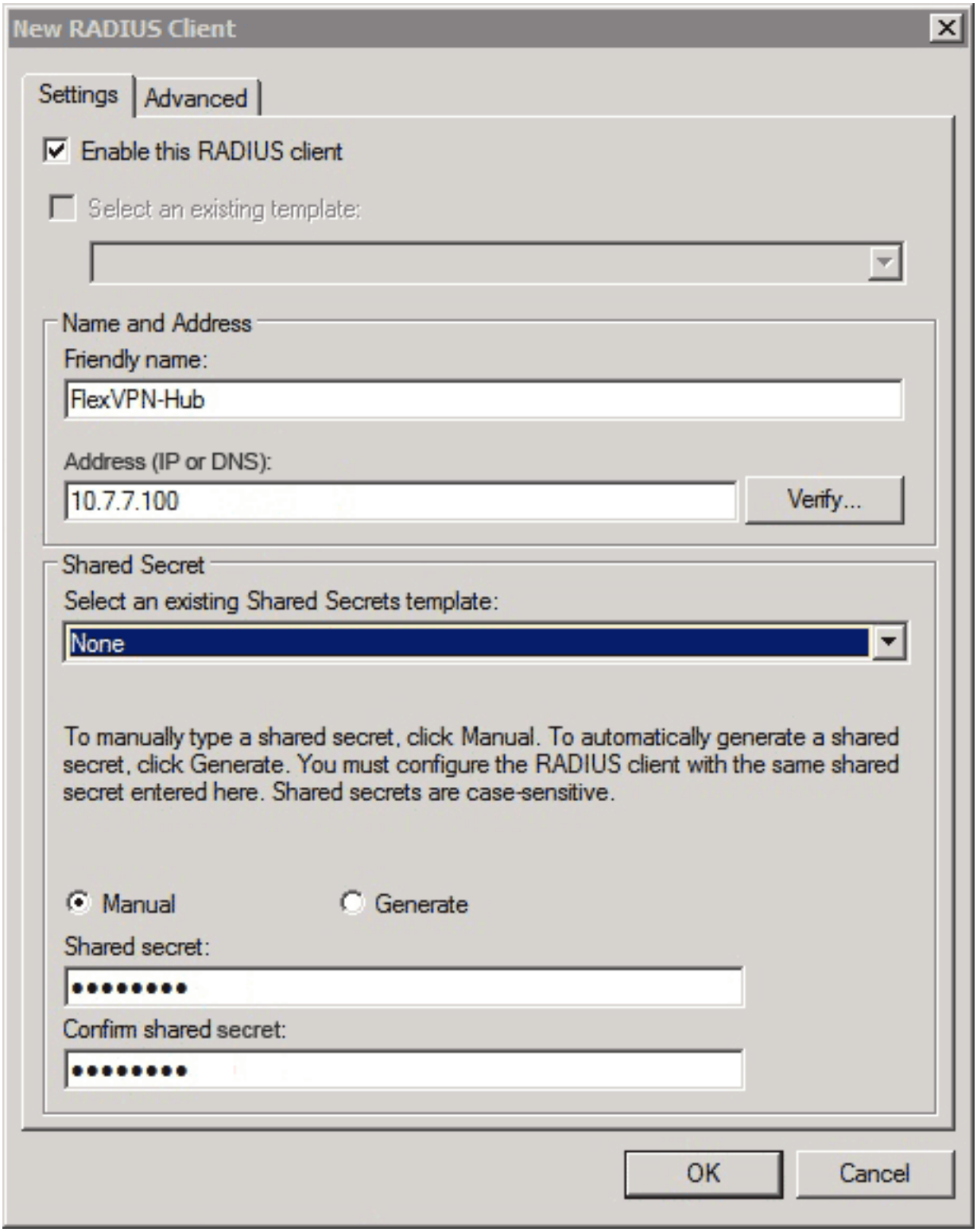
CSCud96246（登録ユーザ専用）に記述された不具合のため、AnyConnect クライアントは FlexVPN ハブ証明書を正し検証できない場合があります。この問題は、IKEv2が疑似ランダム機能(PRF)のSHA-2機能をネゴシエートするのに対し、FlexVPN-Hub証明書はSHA-1を使用して署名されているためです。次の設定では、ネゴシエーションをSHA-1に制限します。

```
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 のサーバの設定

1. Windows Server Manager で、[Roles] > [Network Policy and Access Server] > [NMPS (Local)] > [RADIUS Clients and Servers] の順に展開し、[RADIUS Clients] をクリックします。

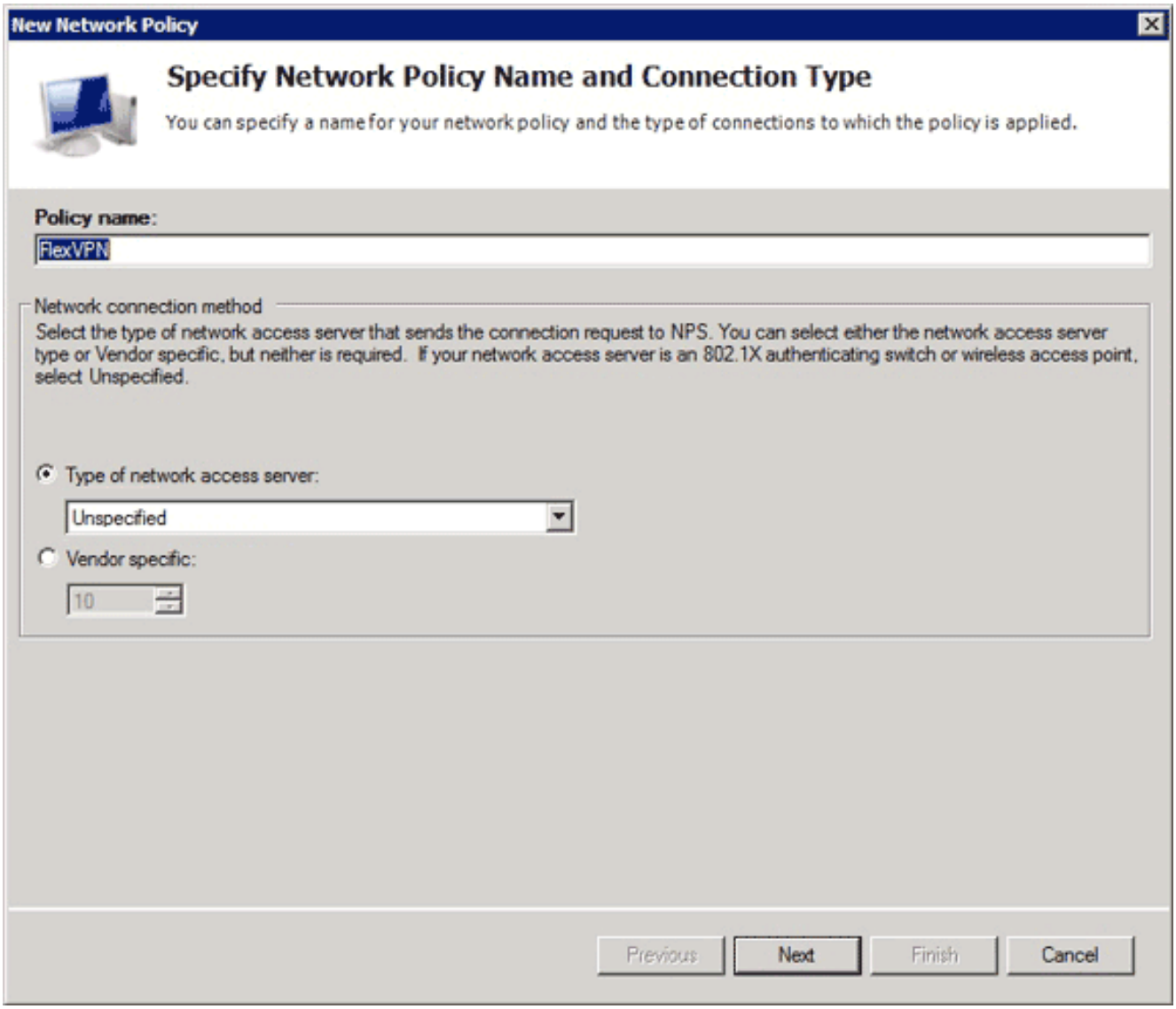
   [New RADIUS Client] ダイアログボックスが表示されます。



2. [New RADIUS Client] ダイアログボックスで、次の手順に従い Cisco IOS ルータを RADIUS クライアントとして追加します。
   [Enable this RADIUS client] **チェックボックスをクリックします。**[Friendly name] フィールドに名前を入力します。この例では *FlexVPN-Hub* を使用しています。[Address] フィールドにルータの IP アドレスを入力します。共有秘密エリアで、[Manual] **オプション ボタンをクリックし、[Shared secret] および [Confirm shared secret] フィールドに共有秘密を入力します。注：共有秘密**は、ルータに設定されている共有秘密と一致している必要があります。
   [OK] をクリックします。

3. サーバ マネージャ インターフェイスで、[Policies] を展開し、[Network Policies] を選択します。

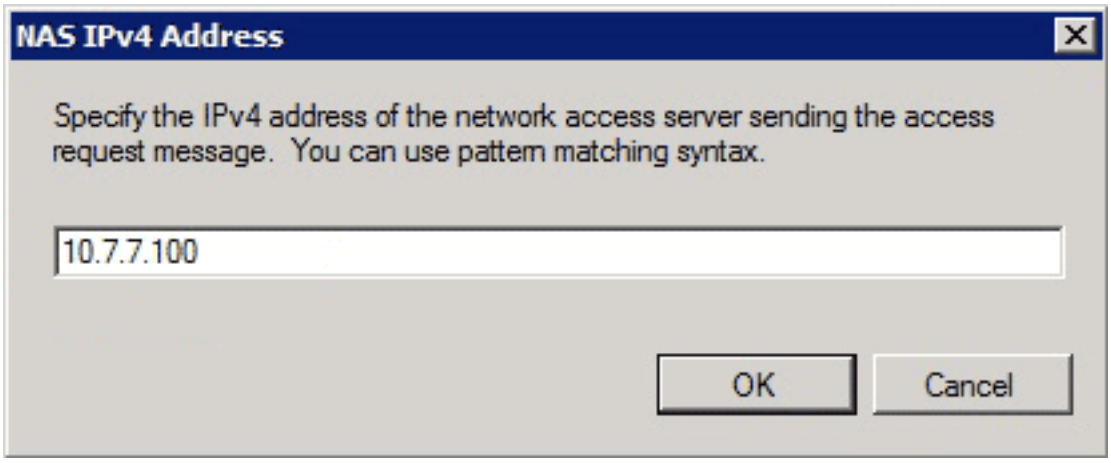
[New Network Policy] ダイアログボックスが表示されます。



4. [New Network Policy] ダイアログボックスで、次の手順に従い、新しいネットワーク ポリシーを追加します。

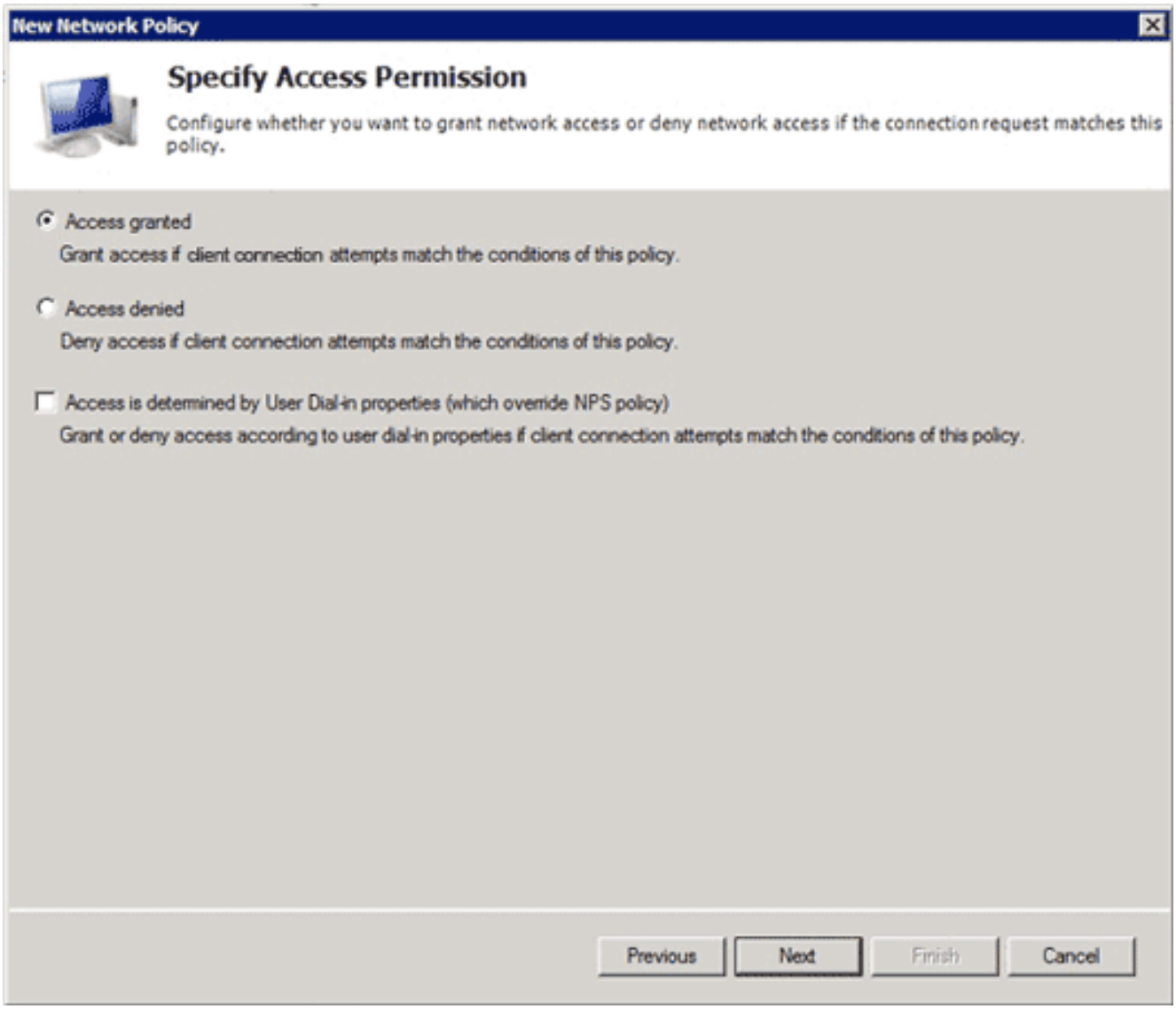
   [Policy name] フィールドに名前を入力します。この例では *FlexVPN* を使用しています。[Type of network access server] **オプション ボタンをクリックし、ドロップダウン リストから [Unspecified] を選択します。**[next] をクリックします。[New Network Policy] ダイアログボックスで、[Add] をクリックして、新しい条件を追加します。[Select condition] ダイアログボックスで、[NAS IPv4 Address] **条件を選択し、[Add] をクリックします。**

   [NAS IPv4 Address] ダイアログボックスが表示されます。



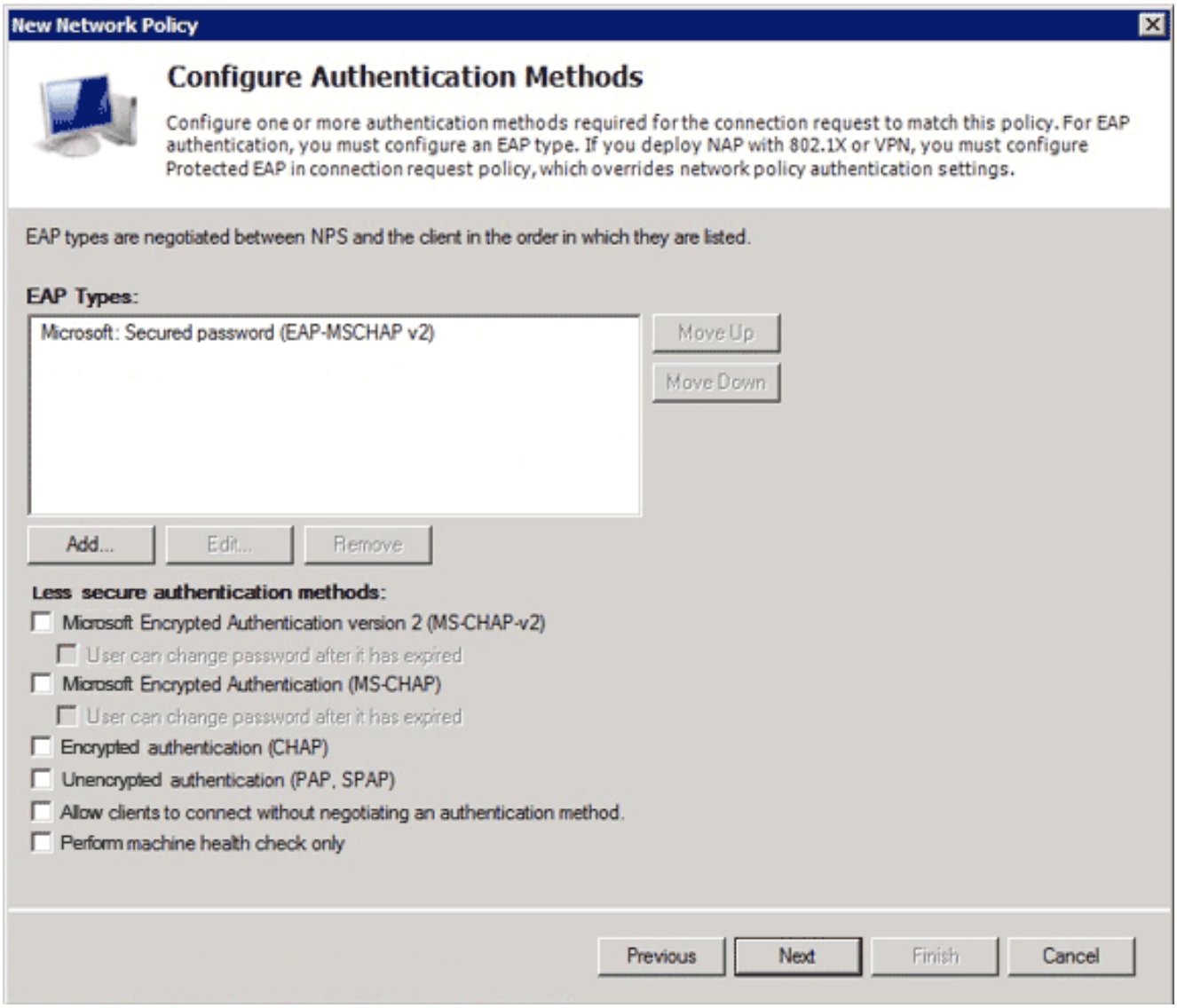
[NAS IPv4 Address] ダイアログボックスで、ネットワーク アクセス サーバの IPv4 アドレスを入力し、ネットワークポリシーを、この Cisco IOS ルータから送信される要求のみに制限します。

[OK] をクリックします。



[New Network Policy] ダイアログボックスで、[Access granted] **オプション ボタンをクリックし、ネットワークへのクライアント アクセスを許可して (ユーザが入力するクレデンシ**

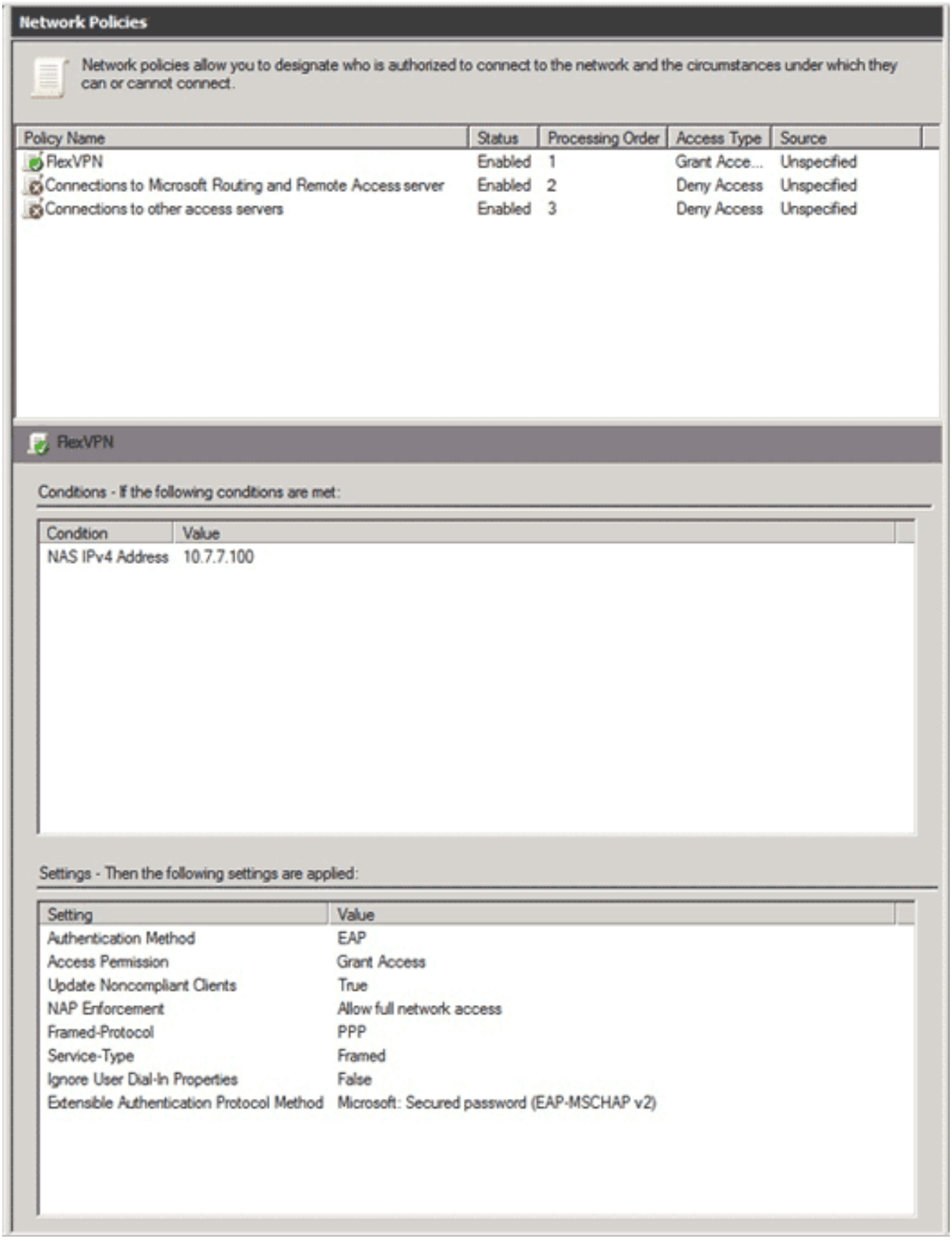
ャルが有効の場合）、[Next] をクリックします。



Microsoft の場合のみ、セキュリティで保護されたパスワード（EAP-MSCHAP v2）が EAP タイプ エリアに表示され、Cisco IOS デバイスと Active Directory 間の通信方式として EAP MSCHAPv2 の使用が許可されていることを確認し、[Next] をクリックします。

注：「低セキュリティの認証方式」のオプションをすべてオフのままにします。

ウィザードで手順を続行し、組織のセキュリティ ポリシーで定義されている追加の制限や設定を適用します。さらに、このポリシーが次の図に示す処理順序の最初にリストされていることを確認します。



クライアントの設定

1. テキスト エディタで XML プロファイルを作成し、*flexvpn.xml* という名前を付けます。

次に、XML プロファイルを使用する例を示します。

```
<?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>
```

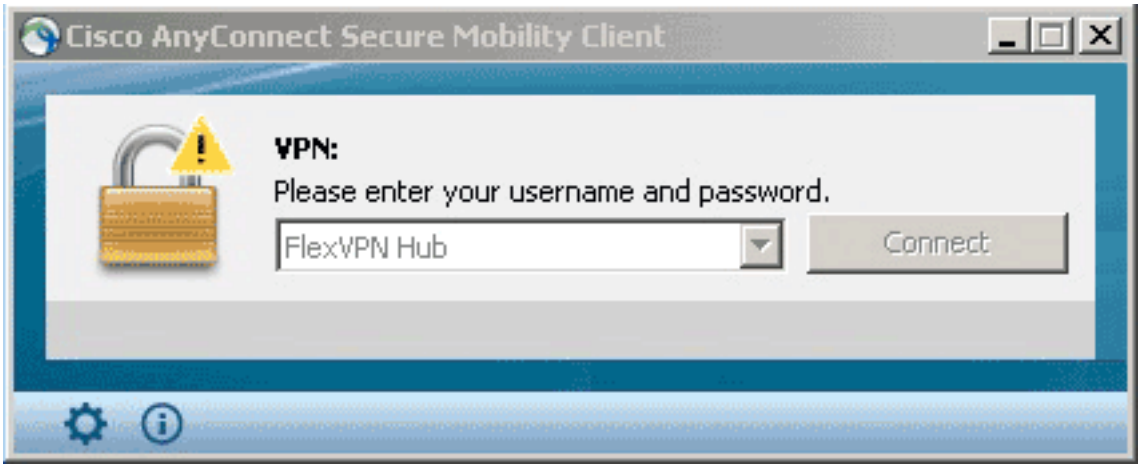
```
<HostName>FlexVPN Hub</HostName>
<HostAddress>flexvpn-hub.example.com</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>EAP-MSCHAPv2</AuthMethodDuringIKENegotiation>
<IKEIdentity>example.com</IKEIdentity>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

<HostName> は、クライアントに表示されるテキスト文字列です。<HostAddress> は、FlexVPN ハブの完全修飾ドメイン名（FQDN）です。<PrimaryProtocol> は、SSL（AnyConnect のデフォルト）ではなく、IKEv2/IPSec を使用する接続を設定します。<AuthMethodDuringIKENegotiation> は、EAP 内で MSCHAPv2 を使用する接続を設定します。この値は、Microsoft Active Directory に対する認証に必要です。<IKEIdentity> は、ハブ上の特定の IKEv2 プロファイルにクライアントを一致させる文字列値を定義します（上記ステップ 4 を参照）。

注：クライアント プロファイルは、クライアントのみが使用する設定です。管理者は、Anyconnect プロファイル エディタを使用して、クライアント プロファイルを作成することが推奨されます。

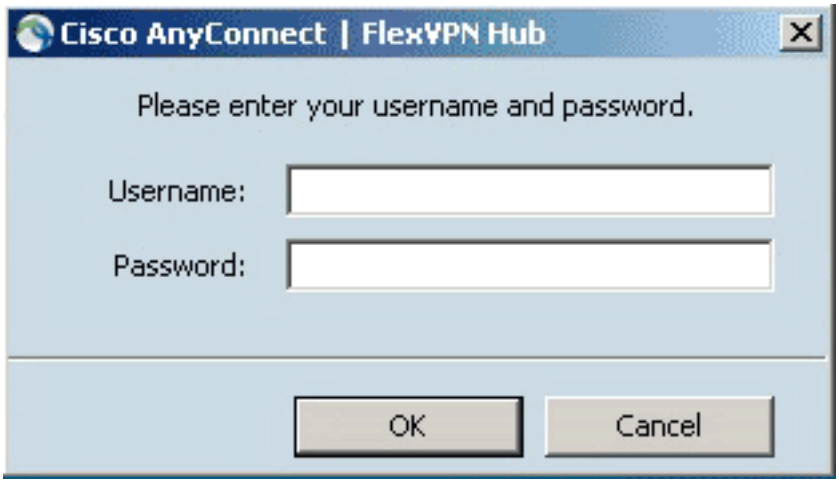
2. 次の表に記載されているとおり、flexvpn.xml ファイルを適切なディレクトリに保存してください。

3. AnyConnect クライアントを終了し、再起動します。



4. [Cisco AnyConnect Secure Mobility Client] ダイアログボックスで、[FlexVPN Hub] を選択し、[Connect] をクリックします。

   [Cisco AnyConnect | FlexVPN Hubダイアログボックスが表示されます。



5. ユーザ名とパスワードを入力し、[OK] をクリックします。

確認

接続を確認するには、[show crypto session detail remote client-ipaddress] コマンドを使用します。このコマンドの詳細については、「暗号化セッションを表示する」を参照してください。

> **注**：アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

トラブルシュート

接続をトラブルシューティングするには、クライアントからDARTログを収集して分析し、ルータで次のデバッグコマンドを使用します。**debug crypto ikev2 packet**および**debug crypto ikev2 internal**。

> **注**：debug コマンドを使用する前に、「デバッグ コマンドの重要な情報」を参照してください。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems