Ejemplo de Configuración de Cliente FlexVPN y Anyconnect IKEv2

Contenido

Introducción

Este documento describe cómo configurar Cisco AnyConnect Secure Mobility Client para utilizar el servicio de usuario de acceso telefónico de autenticación remota (RADIUS) y los atributos de autorización local para autenticarse con Microsoft Active Directory.

> **Nota:** Actualmente, el uso de la base de datos de usuario local para la autenticación no funciona en los dispositivos Cisco IOS®. Esto se debe a que Cisco IOS no funciona como un autenticador EAP. La solicitud de mejora CSCui07025 se ha presentado para agregar soporte.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS versión 15.2(T) o posterior
- Cisco AnyConnect Secure Mobility Client versión 3.0 o posterior
- 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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

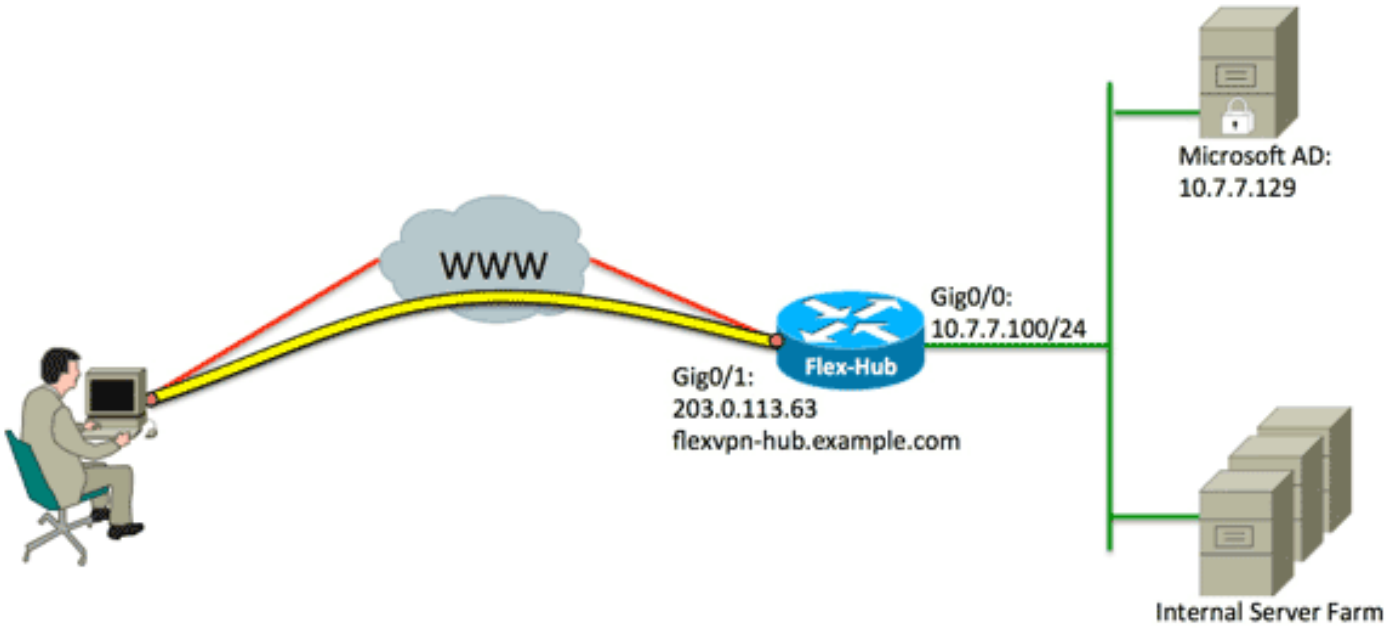
Configurar

En esta sección se ofrece información para configurar las funciones descritas en este documento.

Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración del hub
- Configuración de Microsoft Active Directory Server
- Configuración del Cliente

Configuración del hub

1. Configure RADIUS sólo para autenticación y defina la autorización local.

```
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
```

   El comando **aaa authentication login list** hace referencia al grupo de autenticación, autorización y contabilidad (AAA) (que define el servidor RADIUS). El comando **aaa authorization network list** establece que se deben utilizar los usuarios/grupos definidos localmente. La configuración en el servidor RADIUS se debe cambiar para permitir las solicitudes de autenticación de este dispositivo.

2. Configure la política de autorización local.

```
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
```

   El comando **ip local pool** se utiliza para definir las direcciones IP asignadas al cliente. Una política de autorización se define con un nombre de usuario de *FlexVPN-Local-Policy-1*, y los atributos para el cliente (servidores DNS, máscara de red, lista dividida, nombre de dominio, etc.) se configuran aquí.

3. Asegúrese de que el servidor utiliza un certificado (rsa-sig) para autenticarse.

   Cisco AnyConnect Secure Mobility Client requiere que el servidor se autentique utilizando un certificado (rsa-sig). El router debe tener un certificado de *servidor web* (es decir, un certificado con 'autenticación de servidor' dentro de la extensión de uso de clave extendida) de una autoridad de certificados de confianza (CA).

   Consulte los pasos 1 a 4 en ASA 8.x Instalación Manual de Certificados de Proveedor de Terceros para su Uso con el Ejemplo de Configuración de WebVPN, y cambie todas las instancias de *crypto ca* a *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. Configure los parámetros para esta conexión.

```
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
```

El perfil **crypto ikev2** contiene la mayoría de las configuraciones relevantes para esta conexión: **match identity remote key-id** - Hace referencia a la identidad IKE utilizada por el cliente. Este valor de cadena se configura dentro del perfil XML de AnyConnect.**identity local dn**: define la identidad IKE utilizada por el hub FlexVPN. Este valor utiliza el valor desde dentro del certificado utilizado.**authentication remote**: indica que EAP se debe utilizar para la autenticación de cliente.**authentication local**: indica que los certificados deben utilizarse para la autenticación local.**aaa authentication eap** - Estados para utilizar la lista de inicio de sesión de autenticación aaa FlexVPN-AuthC-List-1 cuando EAP se utiliza para la autenticación.**aaa authorization group eap list** - Estados para utilizar la lista de red de autorización aaa FlexVPN-AuthZ-List-1 con el nombre de usuario de *FlexVPN-Local-Policy-1* para los atributos de autorización.**virtual-template 10**: define qué plantilla se debe utilizar cuando se clona una interfaz de acceso virtual.

5. Configure un perfil IPsec que vuelva a enlazar con el perfil IKEv2 definido en el paso 4.

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

Nota: Cisco IOS utiliza valores predeterminados inteligentes. Como resultado, un conjunto de transformación no necesita ser definido explícitamente.

6. Configure la plantilla virtual desde la que se clonan las interfaces de acceso virtual:
ip unnumbered - Anule el número de la interfaz de una interfaz *interna* para que el ruteo IPv4 se pueda habilitar en la interfaz.**tunnel mode ipsec ipv4 -** Define la interfaz para que sea un túnel de tipo VTI.

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

7. Limite la negociación a SHA-1. (Opcional)

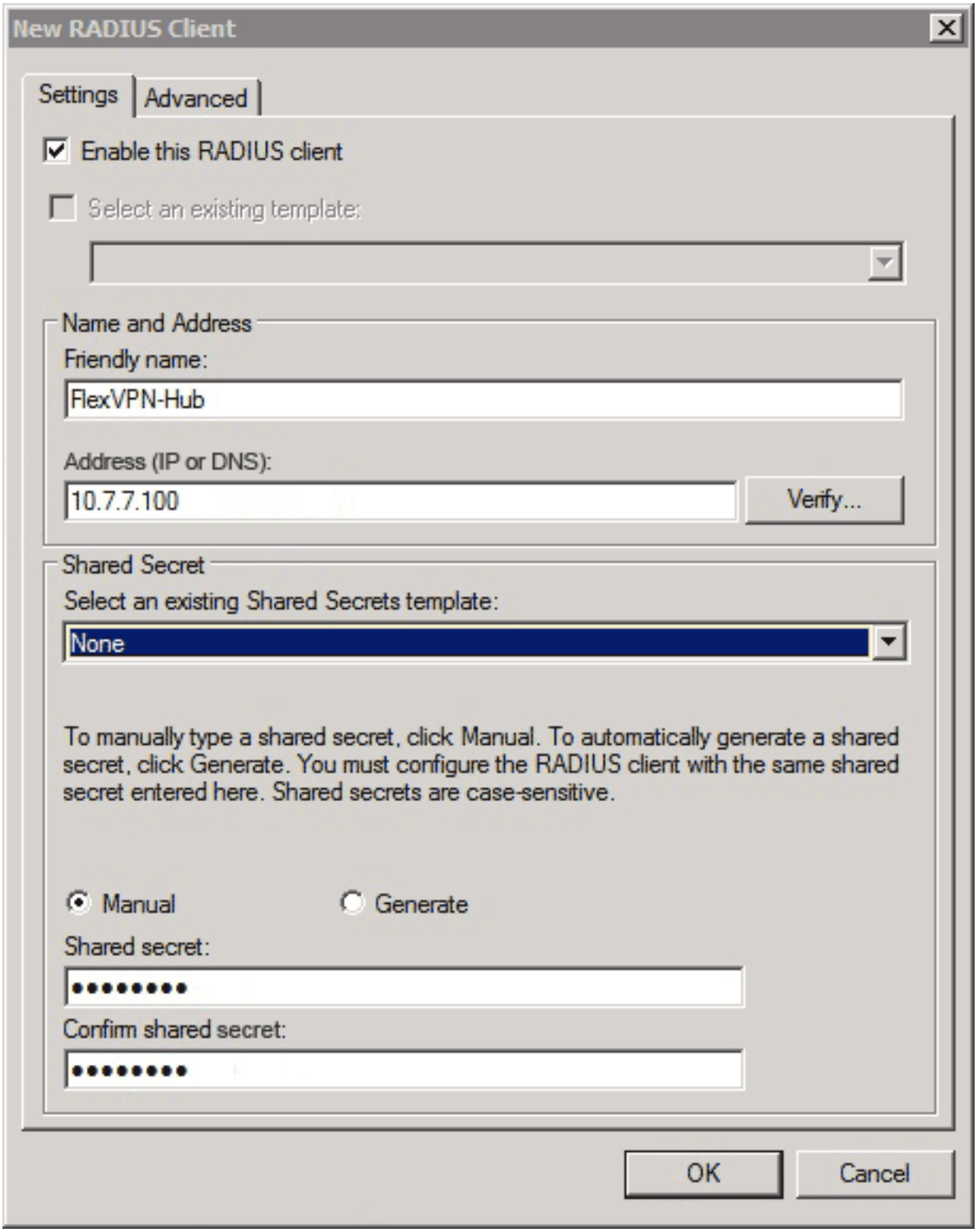
   Debido al defecto CSCud96246 (sólo clientes registrados) , el cliente AnyConnect podría no validar correctamente el certificado de FlexVPN Hub. Este problema se debe a que IKEv2 negoció una función SHA-2 para la función pseudo-aleatoria (PRF), mientras que el certificado de FlexVPN-Hub se firmó mediante SHA-1. La siguiente configuración limita la negociación a 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
```

Configuración de Microsoft Active Directory Server

1. En Windows Server Manager, expanda **Roles > Network Policy and Access Server > NMPS (Local) > RADIUS Clients and Servers**, y haga clic en **RADIUS Clients**.

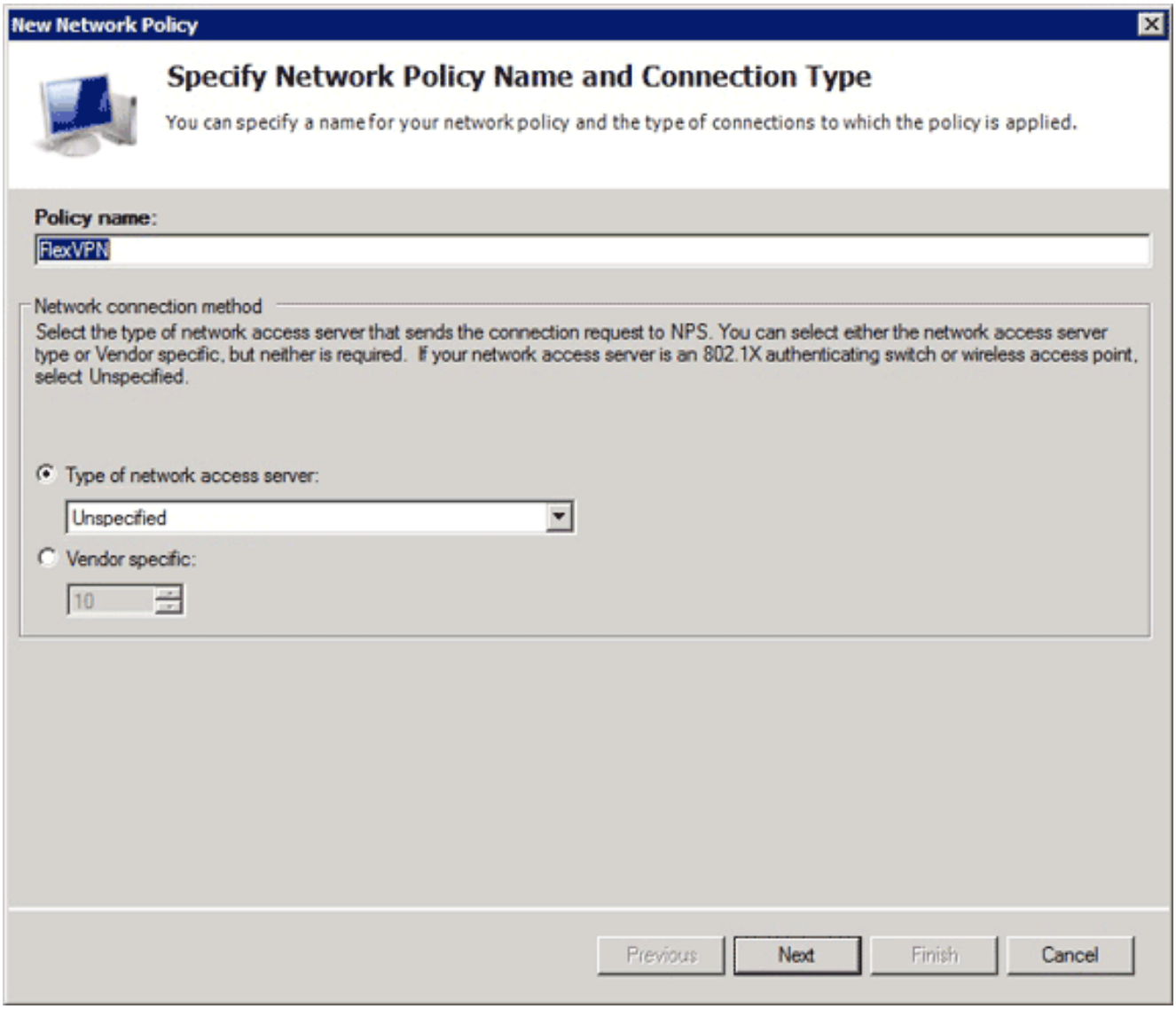
   Aparece el cuadro de diálogo Nuevo cliente RADIUS.



2. En el cuadro de diálogo Nuevo cliente RADIUS, agregue el router Cisco IOS como cliente RADIUS:
   Haga clic en la casilla de verificación **Enable this RADIUS client** .Introduzca un nombre en el campo Nombre descriptivo. Este ejemplo utiliza *FlexVPN-Hub*.Introduzca la dirección IP del router en el campo Dirección.En el área Secreto compartido, haga clic en el botón de opción **Manual** e introduzca el secreto compartido en los campos Secreto compartido y Confirmar secreto compartido.**Nota:** El secreto compartido debe coincidir con el secreto compartido configurado en el router.Click OK.

3. En la interfaz del Administrador de servidores, expanda **Políticas** y elija **Políticas de red**.

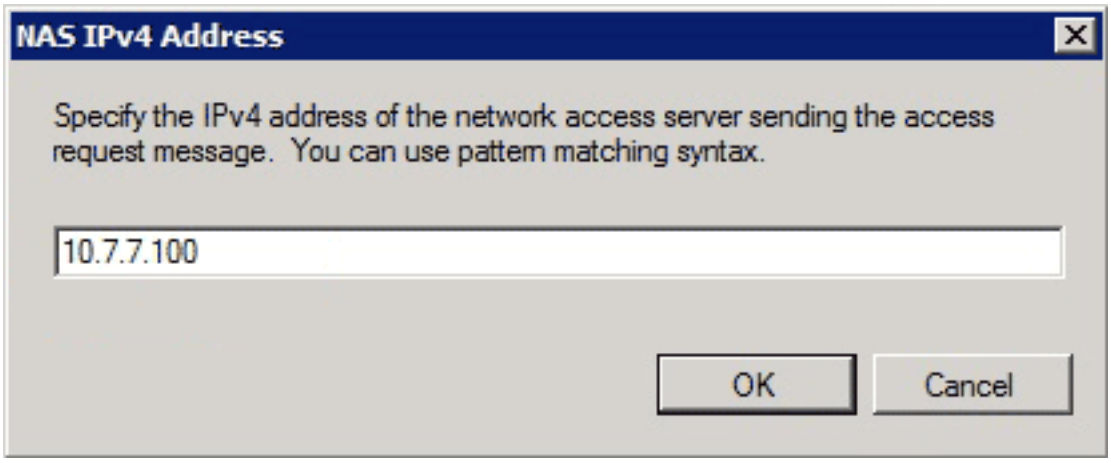
Aparece el cuadro de diálogo Nueva política de red.



4. En el cuadro de diálogo Nueva política de red, agregue una nueva política de red:

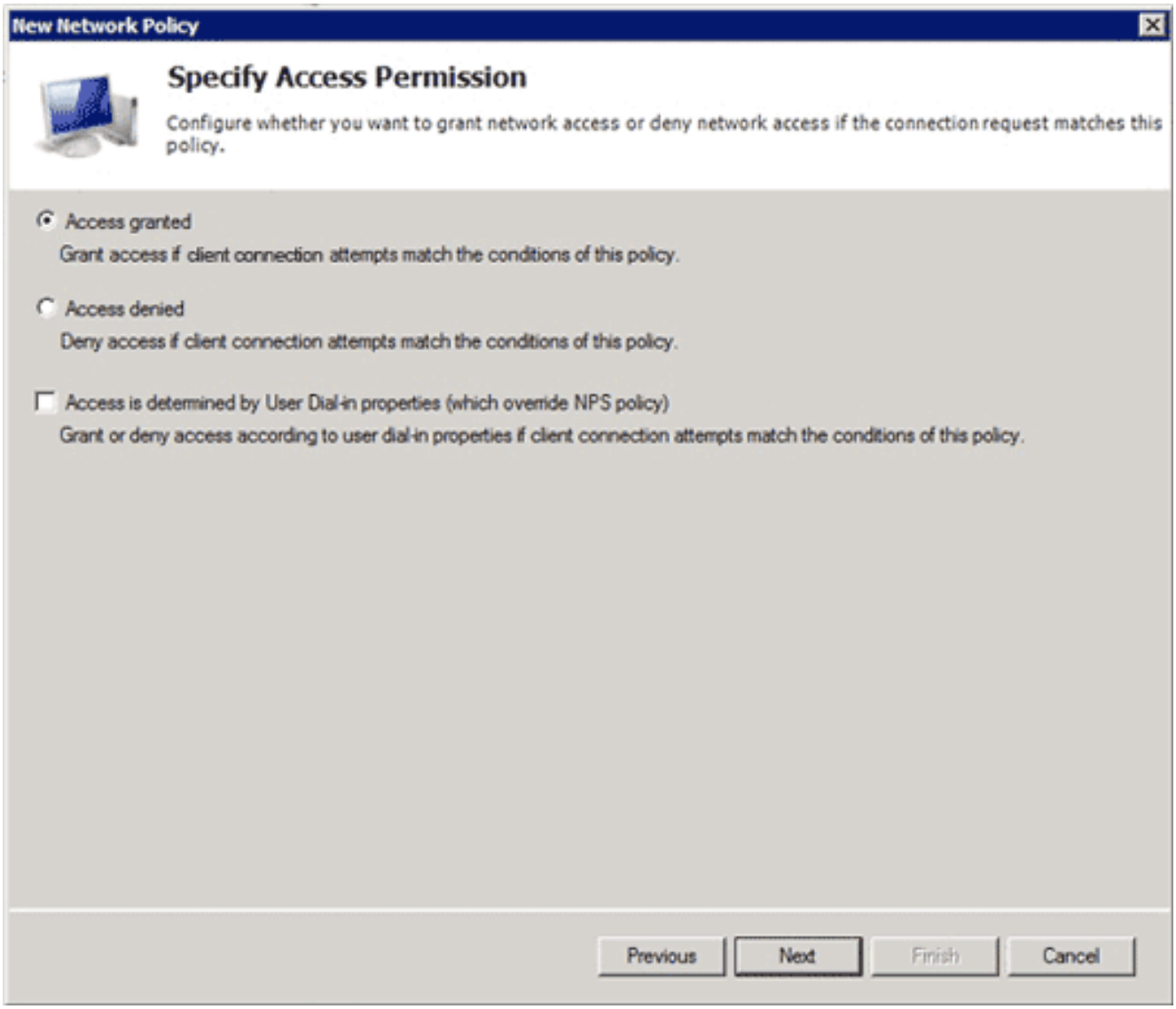
   Introduzca un nombre en el campo Policy name (Nombre de directiva). Este ejemplo utiliza *FlexVPN*.Haga clic en el botón de opción **Tipo de servidor de acceso a la red** y elija **No especificado** en la lista desplegable.Haga clic en Next (Siguiente).En el cuadro de diálogo Nueva política de red, haga clic en **Agregar** para agregar una nueva condición.En el cuadro de diálogo Seleccionar condición, seleccione la condición **NAS IPv4 Address** y haga clic en **Agregar**.

   Aparece el cuadro de diálogo Dirección IPv4 de NAS.



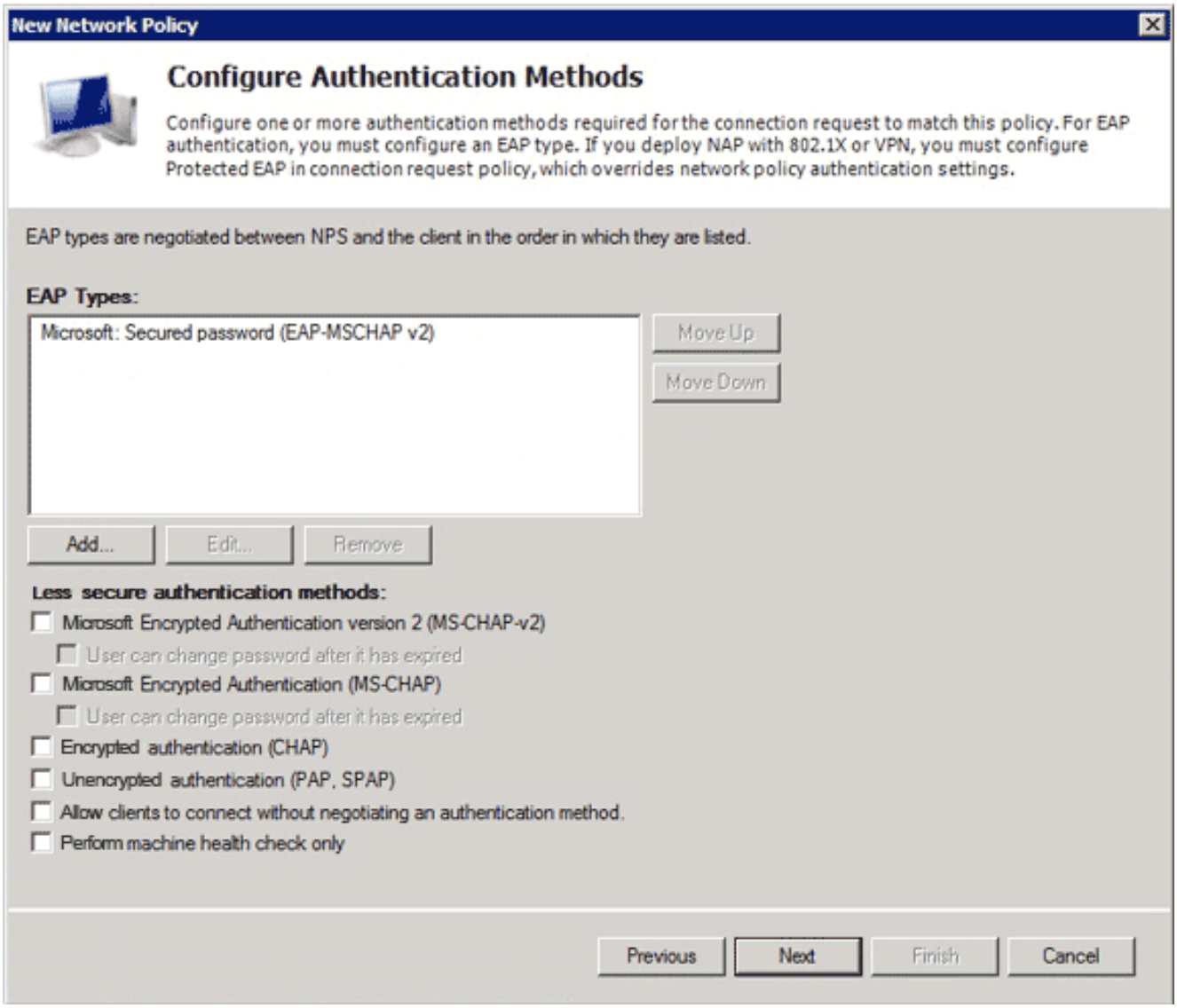
En el cuadro de diálogo NAS IPv4 Address (Dirección IPv4 de NAS), introduzca la dirección IPv4 del servidor de acceso a la red para limitar la política de red únicamente a las solicitudes que se originan en este router Cisco IOS.

Click OK.



En el nuevo cuadro de diálogo Política de red, haga clic en el botón de opción **Acceso concedido** para permitir el acceso del cliente a la red (si las credenciales proporcionadas por

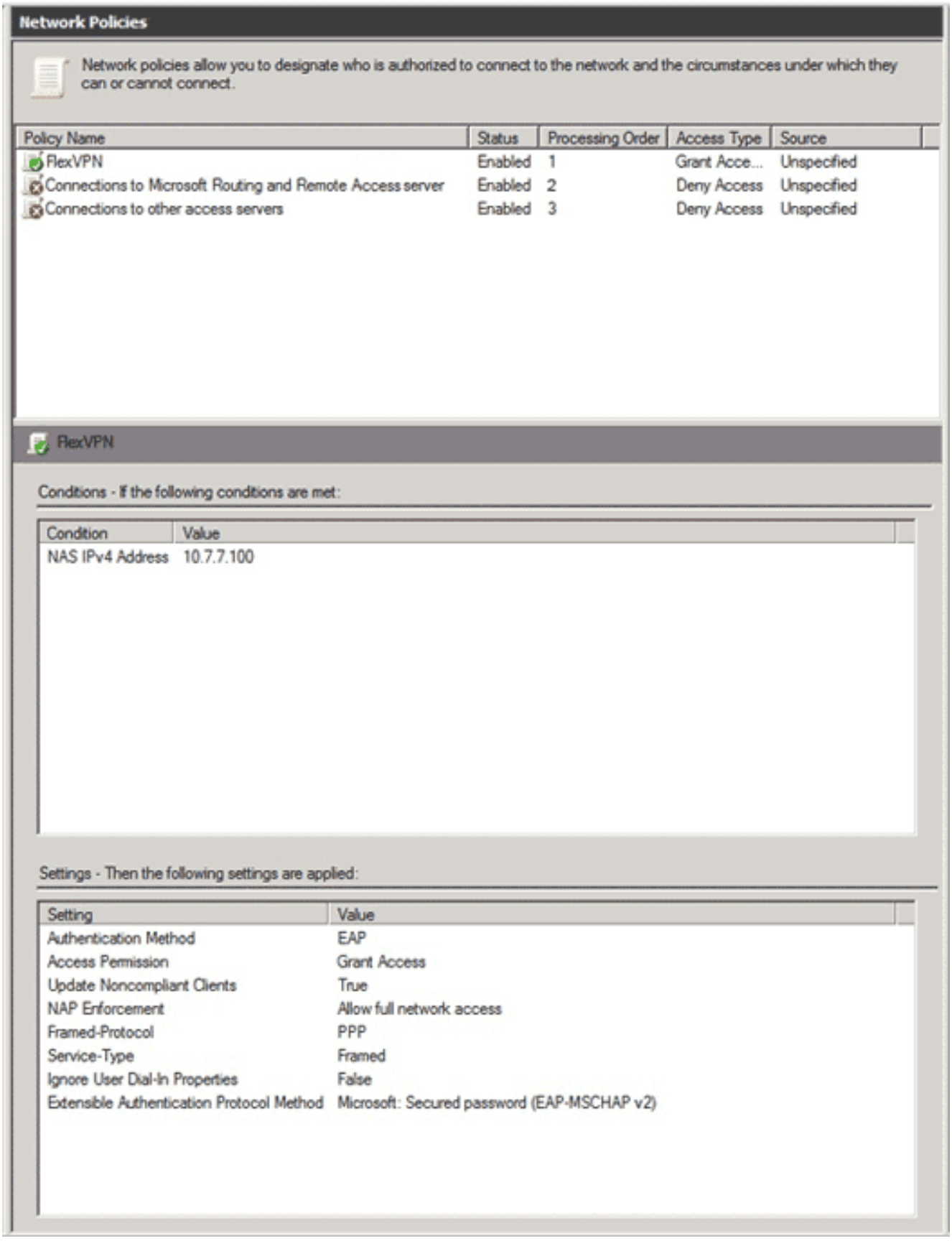
el usuario son válidas) y haga clic en **Siguiente**.



Asegúrese de que solo Microsoft: La contraseña segura (EAP-MSCHAP v2) aparece en el área Tipos de EAP para permitir que EAP-MSCHAPv2 se utilice como método de comunicación entre el dispositivo Cisco IOS y Active Directory, y haga clic en **Siguiente**.

Nota: Deje todas las opciones 'Método de autenticación menos seguro' sin marcar.

Continúe con el asistente y aplique cualquier restricción o configuración adicional definida por la directiva de seguridad de su organización. Además, asegúrese de que la política aparece primero en el orden de procesamiento, como se muestra en esta imagen:



Configuración del Cliente

1. Cree un perfil XML dentro de un editor de texto y asígnele el nombre *flexvpn.xml*.

Este ejemplo utiliza este perfil XML:

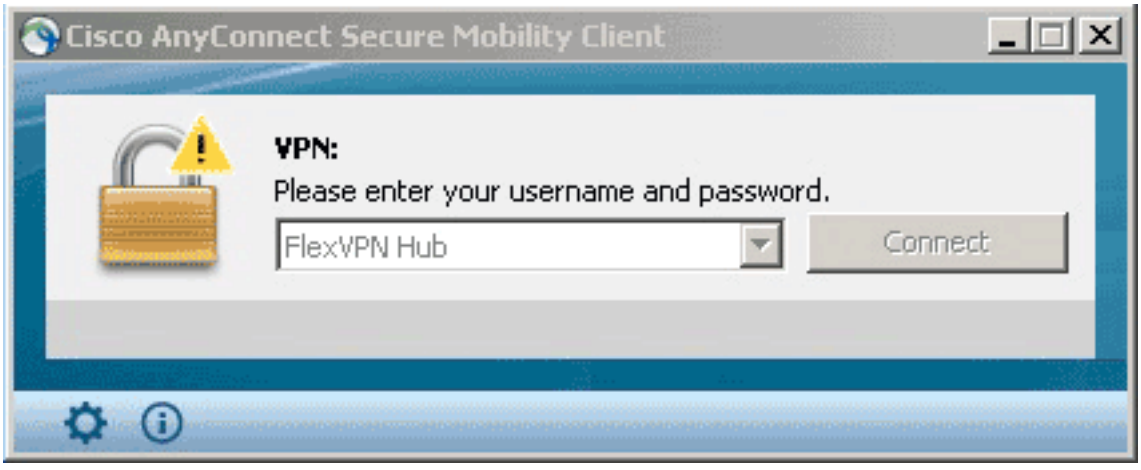
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false
</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> es una cadena de texto que aparece en el cliente.<HostAddress> es el nombre de dominio completo (FQDN) del hub FlexVPN.<PrimaryProtocol> configura la conexión para que use IKEv2/IPsec en lugar de SSL (el valor predeterminado en AnyConnect).<AuthMethodDuranteIKENegotiation> configura la conexión para utilizar MSCHAPv2 dentro de EAP. Este valor se requiere para la autenticación con Microsoft Active Directory.<IKEIdentity> define el valor de cadena que coincide con el cliente con un perfil IKEv2 específico en el hub (consulte el paso 4 anterior).
Nota: El perfil del cliente es algo que sólo utiliza el cliente. Se recomienda que un administrador utilice el editor de perfil de Anyconnect para crear el perfil del cliente.

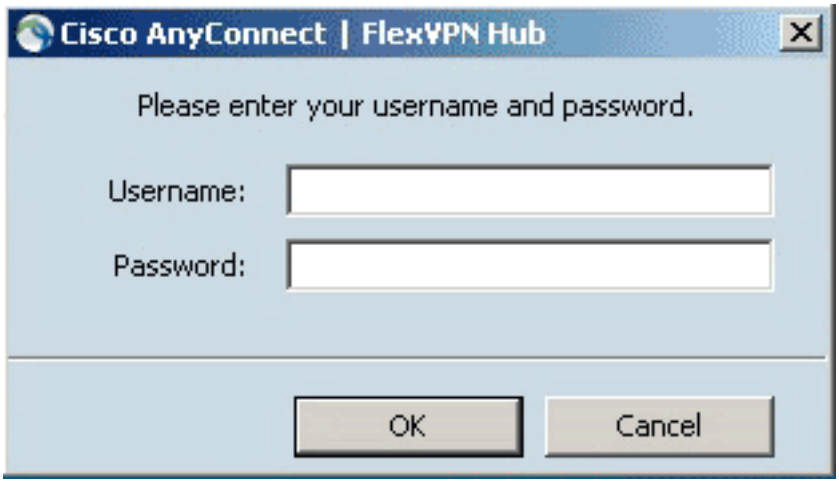
2. Guarde el archivo flexvpn.xml en el directorio adecuado como se muestra en esta tabla:

3. Cierre y reinicie el cliente AnyConnect.



4. En el cuadro de diálogo Cisco AnyConnect Secure Mobility Client, elija **FlexVPN Hub** y haga clic en **Connect**.

   Cisco AnyConnect | Aparecerá el cuadro de diálogo FlexVPN Hub.



5. Introduzca un nombre de usuario y una contraseña y haga clic en **Aceptar**.

Verificación

Para verificar la conexión, utilice el comando **show crypto session detail remote client-ipaddress**. Consulte show crypto session para obtener más información sobre este comando.

> **Nota:** La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshoot

Para resolver el problema de la conexión, recopile y analice los registros DART del cliente y use estos comandos debug en el router: **debug crypto ikev2 packet** y **debug crypto ikev2 internal**.

> **Nota:** Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug.**

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems