Ejemplo de la configuración del cliente de FlexVPN y de Anyconnect IKEv2

Contenido

Introducción

Este documento describe cómo configurar al Cliente de movilidad Cisco AnyConnect Secure para utilizar el Remote Authentication Dial-In User Service (RADIUS) y los atributos de la autorización local para autenticar contra el Microsoft Active Directory.

> Nota: Actualmente, el uso de la base de datos de usuarios locales para la autenticación no funciona en los dispositivos del ® del Cisco IOS. Esto es porque el Cisco IOS no funciona como un authenticator EAP. Se ha clasifiado el pedido de mejora CSCui07025 de agregar el soporte.

Prerrequisitos

Requisitos

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.

- Versión deL Cisco IOS 15.2(T) o más adelante
- Versión 3.0 o posterior del Cliente de movilidad Cisco AnyConnect Secure
- Microsoft Active Directory

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

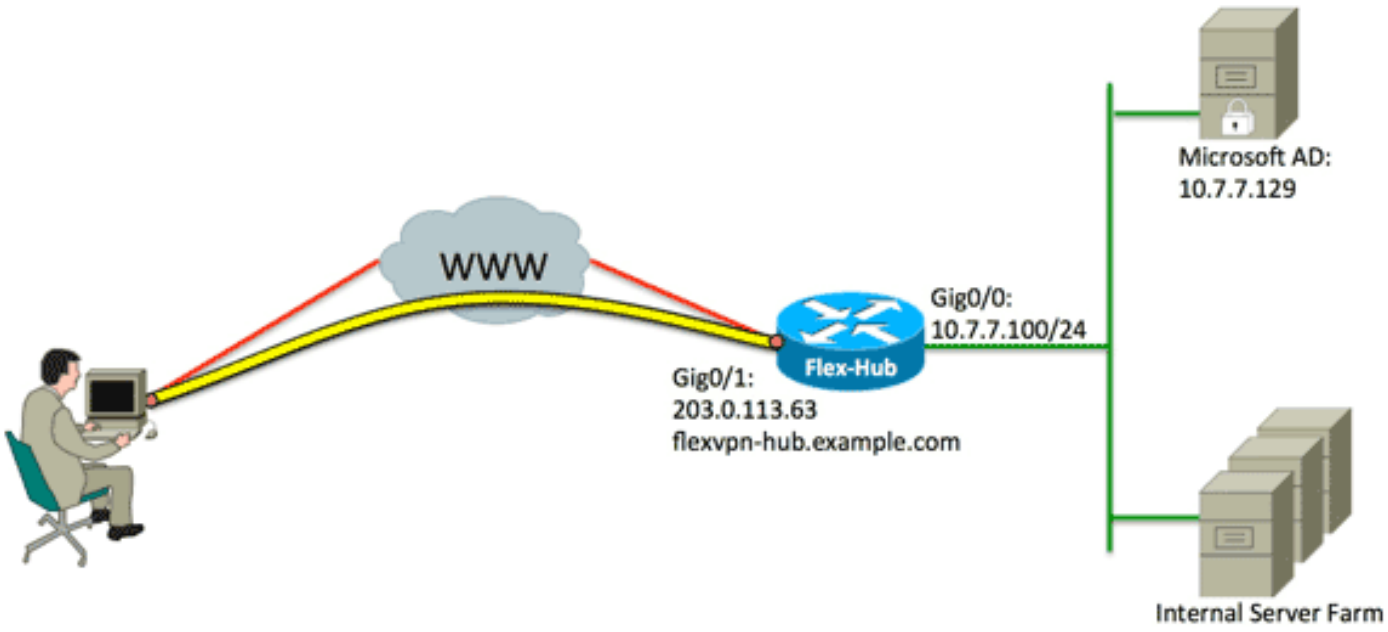
Configurar

En esta sección, le presentan con la información para configurar las características 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 del servidor del Microsoft Active Directory
- Configuración del Cliente

Configuración del hub

1. Configure RADIUS para la autenticación solamente 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 list de la conexión con el sistema de autenticación aaa refiere al grupo del Authentication, Authorization, and Accounting (AAA) (que define al servidor de RADIUS). Los estados de **comando list de la autorización de red AAA** que localmente definieron los usuarios/a los grupos deben ser utilizados. La configuración en el servidor de RADIUS se debe cambiar para permitir los pedidos de autenticación de este dispositivo.

2. Configure la directiva de la 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
```

   Utilizan al **comando ip local pool** de definir los IP Addresses que se asigna al cliente. Una directiva de la autorización se define con un nombre de usuario de *FlexVPN-Local-Policy-1*, y los atributos para el cliente (servidores DNS, netmask, lista partida, Domain Name, y así sucesivamente) se configuran aquí.

3. Asegúrese que el servidor utilice un certificado (RSA-SIG) para autenticarse.

   El Cliente de movilidad Cisco AnyConnect Secure requiere que el servidor se autentique usando un certificado (RSA-SIG). El router debe tener un certificado del *servidor Web* (es decir, un certificado con la “autenticación de servidor” dentro de la extensión dominante extendida del uso) de un Certificate Authority (CA) de confianza.

   Refiera a los pasos 1 a 4 en ASA 8.x instalan manualmente los Certificados del vendedor de las de otras compañías para el uso con el ejemplo de configuración del WebVPN, y cambian todos los casos del *Ca crypto al pki crypto*.

```
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 las configuraciones 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
```
Los ontains **crypto del profilec ikev2** la mayor parte de las configuraciones relevantes para esta conexión: **clave-identificación del telecontrol de la identidad de la coincidencia** - Refiere a la identidad IKE usada por el cliente. Este valor de la cadena se configura dentro del perfil de AnyConnect XML.**identidad dn local** - Define la identidad IKE usada por el concentrador de FlexVPN. Este valor utiliza el valor dentro del certificado usado.**telecontrol de la autenticación** - Estados que el EAP se debe utilizar para la autenticación de cliente.**los estados locales de la autenticación** que los Certificados se deben utilizar para el local autentican.**eap de la autenticación aaa** - Estados para utilizar la lista FlexVPN-AuthC-List-1 de la conexión con el sistema de autenticación aaa cuando el EAP se utiliza para la autenticación.**lista del eap del grupo de la autorización aaa** - Estados para utilizar la lista FlexVPN-AuthZ-List-1 de la autorización de red AAA con el nombre de usuario de *FlexVPN-Local-Policy-1* para los atributos de la autorización.**virtual-plantilla 10** - Define qué plantilla a utilizar cuando se reproduce una interfaz de acceso virtual.

5. Configure un perfil de ipsec que conecte de nuevo al perfil IKEv2 definido en el paso 4.
```
crypto ipsec profile FlexVPN-IPsec-Profile-1
set ikev2-profile FlexVPN-IKEv2-Profile-1
```
Nota: El Cisco IOS utiliza los valores por defecto elegantes. Como consecuencia, un conjunto de la transformación no necesita ser definido explícitamente.

6. Configure la plantilla virtual de la cual se reproducen las interfaces de acceso virtual:
IP innumerable - Unnumber la interfaz de rutear de la *interfaz interior* así que del IPv4 se puede habilitar en la interfaz.**IPSec ipv4 del modo túnel -** Define la interfaz para ser un túnel del 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 al SHA-1. (Opcional)

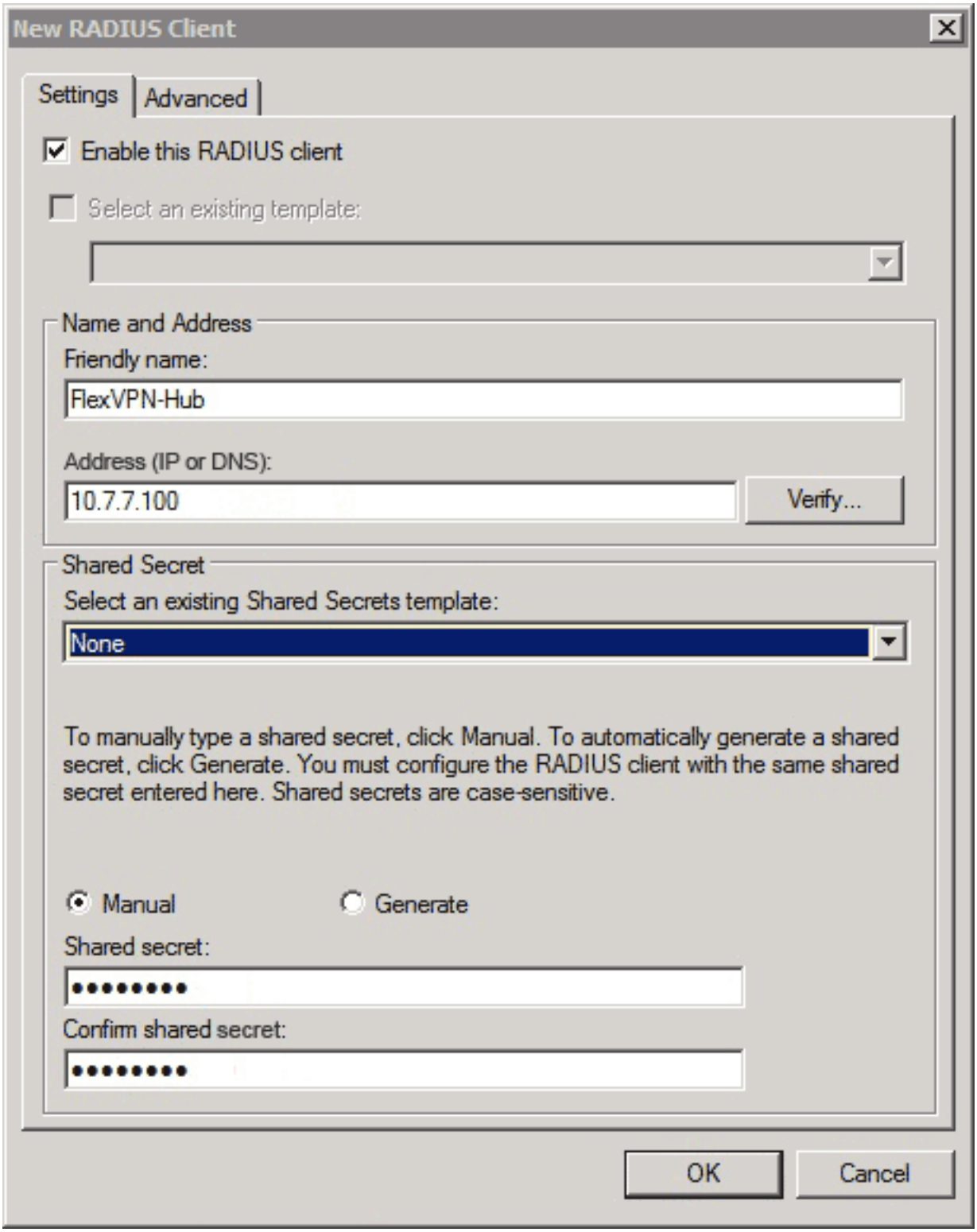
   Debido desertar CSCud96246 (clientes registrados solamente), el cliente de AnyConnect pudo no poder validar correctamente el certificado del concentrador de FlexVPN. Este problema es debido a IKEv2 que negocia una función SHA-2 para la función pseudoaleatoria (PRF) mientras que el certificado del FlexVPN-concentrador se ha firmado usando el SHA-1. Los límites abajo de la configuración la negociación al 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 del servidor del Microsoft Active Directory

1. En el administrador de Servidor Windows, amplíe los **papeles > la política de red y el servidor de acceso > los NMP (locales) > los clientes RADIUS y los servidores**, y haga clic a los **clientes RADIUS**.

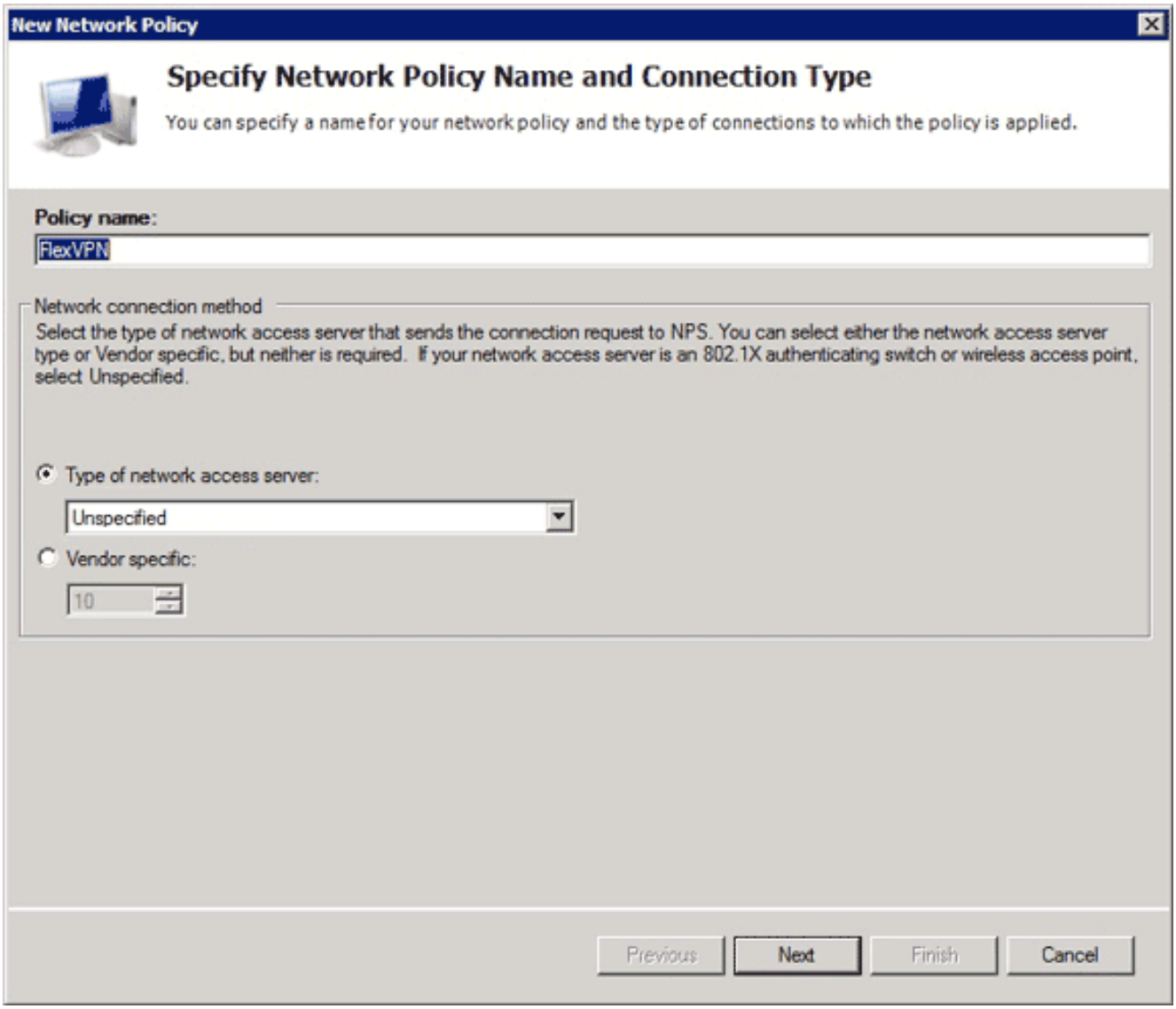
   El nuevo cuadro de diálogo del cliente RADIUS aparece.



2. En el nuevo cuadro de diálogo del cliente RADIUS, agregue al router del Cisco IOS como cliente RADIUS:
   Haga clic el **permiso esta** casilla de verificación del **cliente RADIUS**.Ingrese un nombre en el campo de nombre cómodo. Este ejemplo utiliza el FlexVPN-*concentrador*.Ingrese el IP Address del router en el campo de dirección.En el área secreta compartida, haga clic el botón de radio **manual**, y ingrese el secreto compartido en el secreto compartido y los campos secretos compartidos Confirm.**Nota:** El secreto compartido debe hacer juego el secreto compartido configurado en el router.Haga clic en OK.

3. En la interfaz del administrador de servidor, amplíe las **directivas**, y elija las **políticas de red**.

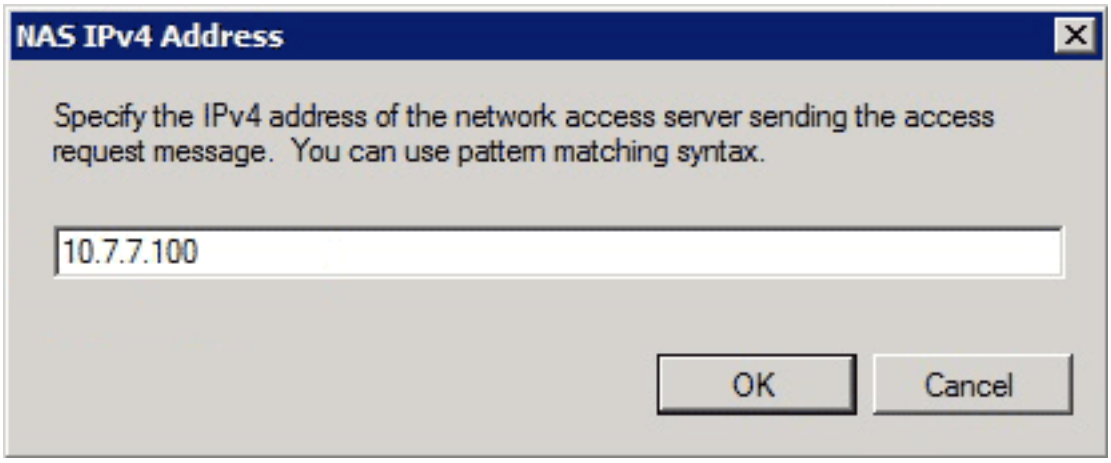
El nuevo cuadro de diálogo de la política de red aparece.



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

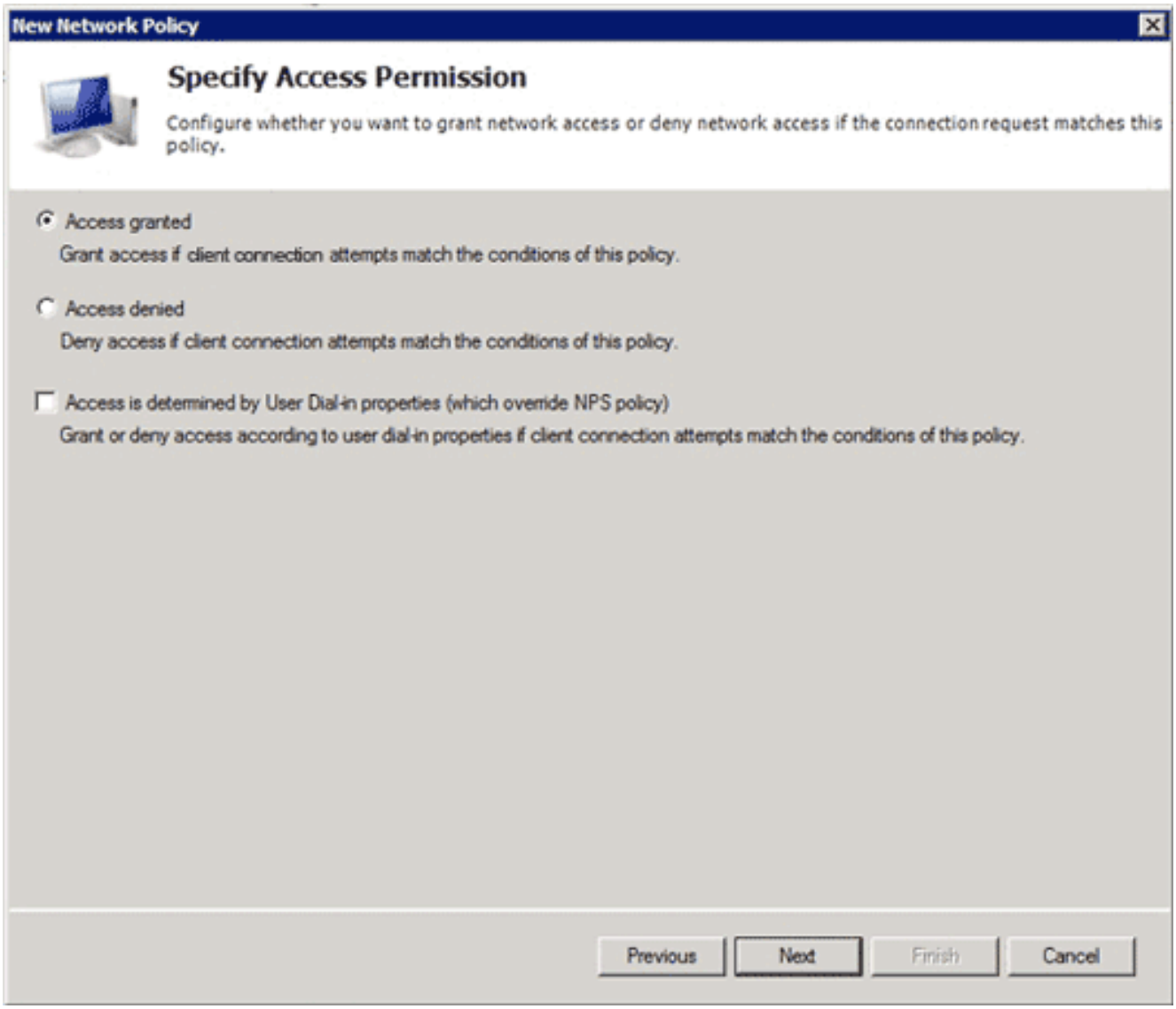
   Ingrese un nombre en el campo de nombre de la directiva. Este ejemplo utiliza *FlexVPN*.Haga clic el botón de radio del **servidor de acceso del tipo de red**, y elija **sin especificar de la** lista desplegable.Haga clic en Next (Siguiente).En el nuevo cuadro de diálogo de la política de red, el tecleo **agrega** para agregar una nueva condición.En el cuadro de diálogo selecto de la condición, seleccione la condición del **direccionamiento del IPv4 NAS**, y el haga click en Add

   El cuadro de diálogo del direccionamiento del IPv4 NAS aparece.



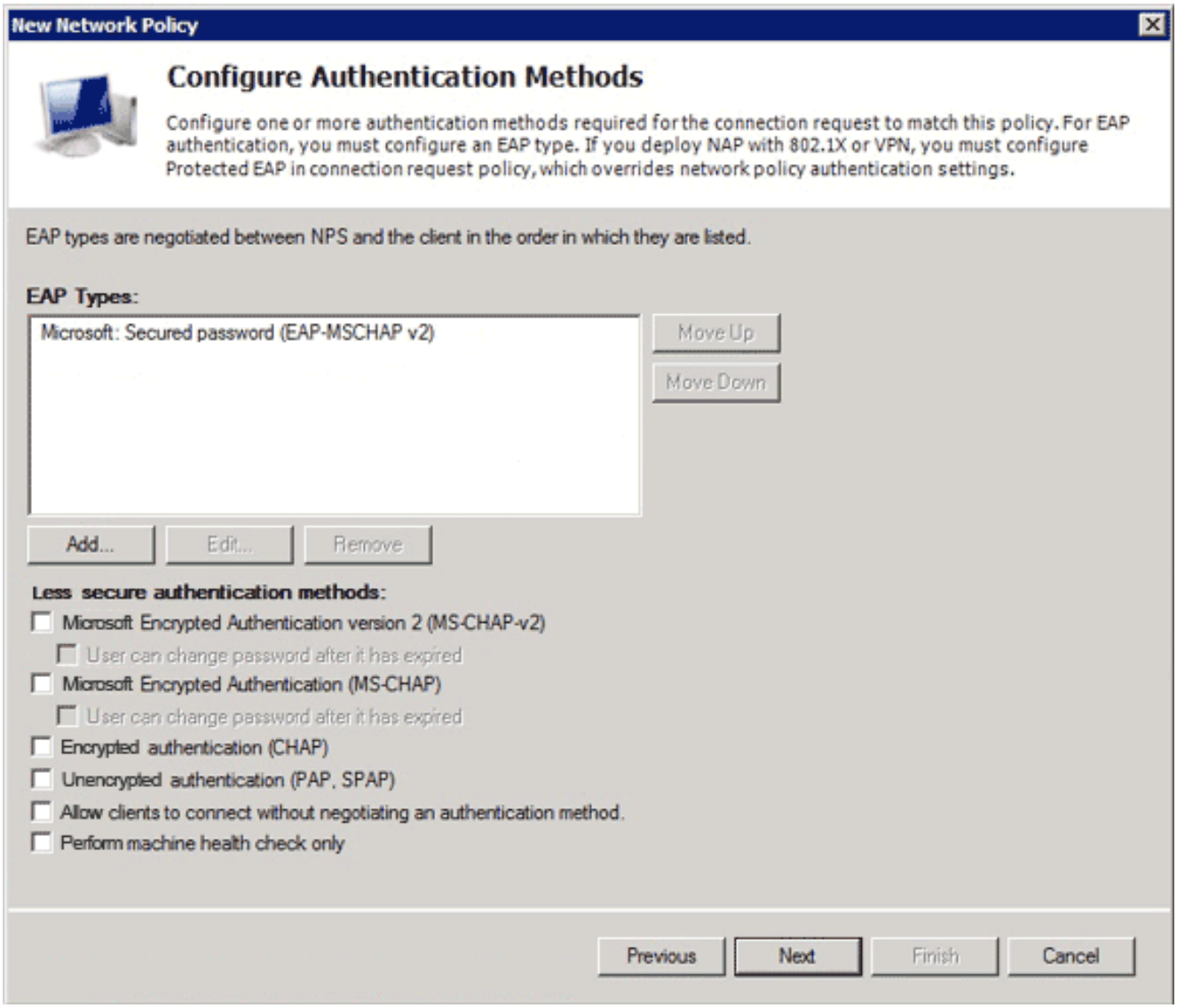
En el cuadro de diálogo del direccionamiento del IPv4 NAS, ingrese el direccionamiento del IPv4 del servidor de acceso a la red para limitar la política de red solamente a las peticiones que originan de este router del Cisco IOS.

Haga clic en OK.



En el nuevo cuadro de diálogo de la política de red, haga clic el **acceso concedió el** botón de radio para permitir el acceso al cliente a la red (si las credenciales proporcionadas por el

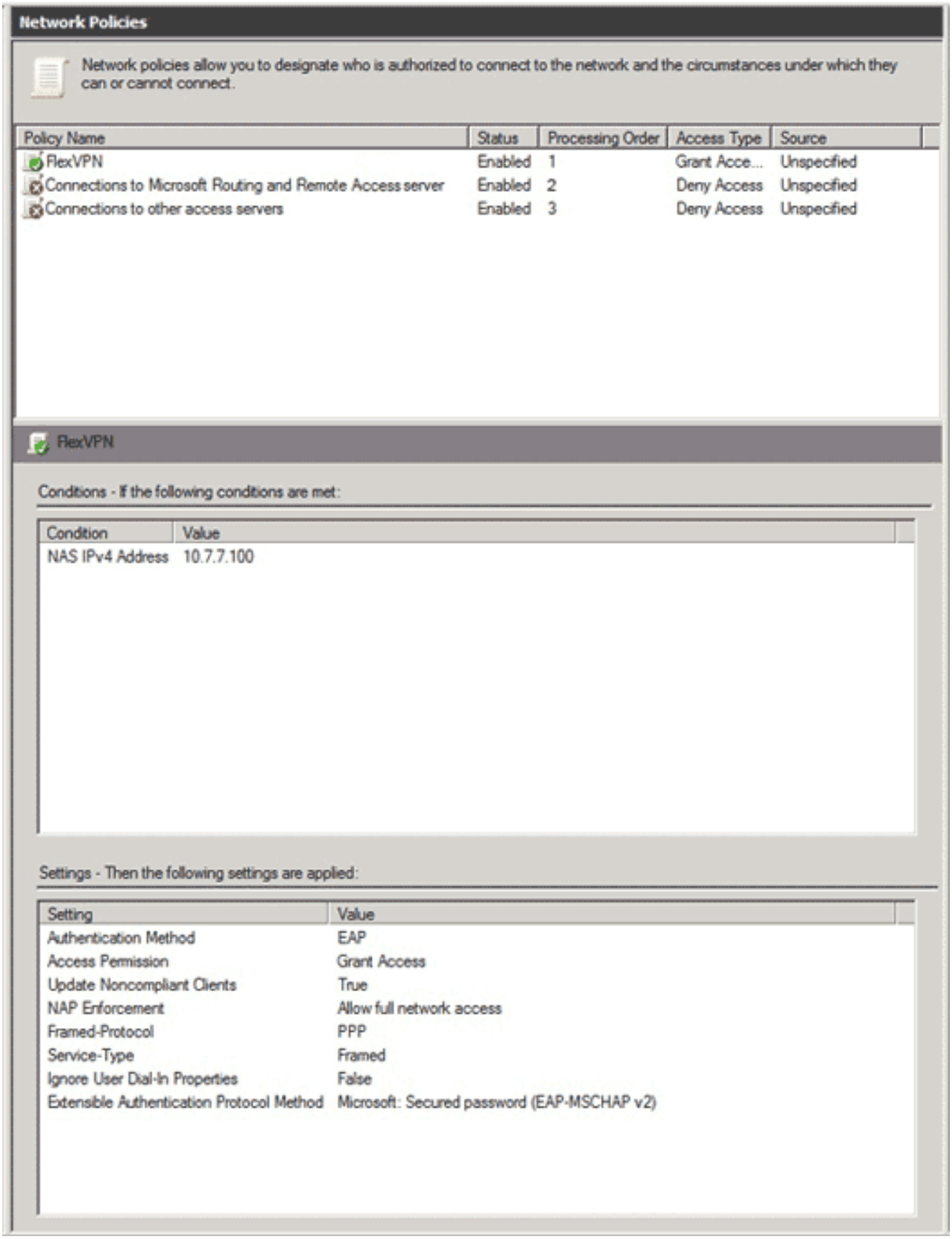
usuario son válidas), y hacen clic **después**.



Asegure solamente Microsoft: La contraseña segura (v2 EAP-MSCHAP) aparece en el área de tipos EAP para permitir que el EAP MSCHAPv2 sea utilizado como el método de comunicación entre el dispositivo Cisco IOS y el Active Directory, y hace clic **después**.

Nota: Deje las opciones de todos los “métodos de autentificación menos seguros desmarcadas.

Continúe a través del Asisitente y aplique cualesquiera apremios o configuraciones adicionales según lo definido por su política de seguridad de las organizaciones. Además, asegúrese de que la directiva esté enumerada primero en el orden de procesamiento tal y como se muestra en de esta imagen:



Configuración del Cliente

1. Cree un perfil XML dentro de un editor de textos, y nómbrelo *flexvpn.xml.*

Este ejemplo utiliza este perfil XML:

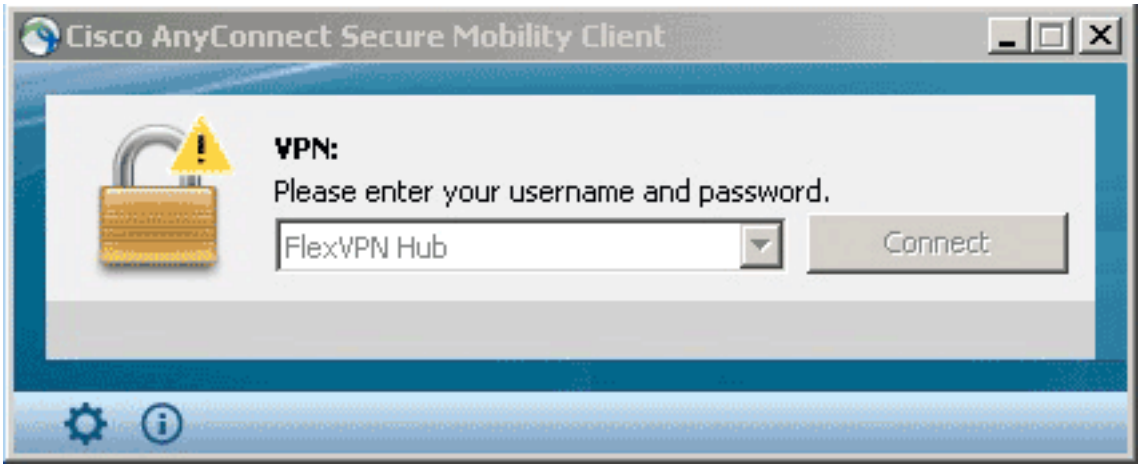
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false
</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>
```

el **<hostname>** es una cadena de texto que aparece en el cliente.el **<HostAddress>** es el nombre de dominio completo (FQDN) del concentrador de FlexVPN.el **<PrimaryProtocol>** configura la conexión para utilizar IKEv2/IPsec bastante que SSL (el valor por defecto en AnyConnect).el **<AuthMethodDuringIKENegotiation>** configura la conexión para utilizar el MSCHAPv2 dentro del EAP. Este valor se requiere para la autenticación contra el Microsoft Active Directory.el **<IKEIdentity>** define el valor de la cadena que hace juego al cliente a un perfil específico IKEv2 en el concentrador (véase el paso 4 antedicho). Nota: El perfil del cliente es algo que es utilizado solamente por el cliente. Se recomienda que un administrador utiliza el editor del perfil de Anyconnect para crear el perfil del cliente.

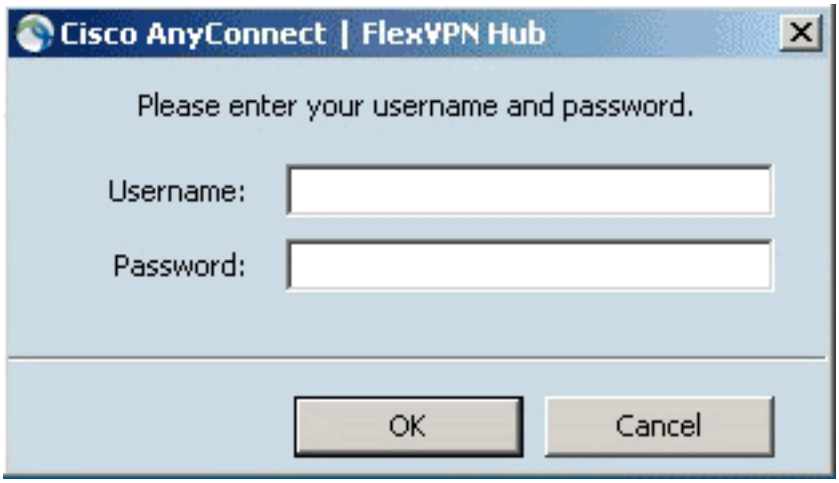
2. Salve el archivo flexvpn.xml al directorio apropiado como se lista en esta tabla:

3. El cierre y recomienza al cliente de AnyConnect.



4. En el cuadro de diálogo del Cliente de movilidad Cisco AnyConnect Secure, elija el **concentrador de FlexVPN**, y el tecleo **conecta**.

Cisco AnyConnect | El cuadro de diálogo del concentrador de FlexVPN aparece.



5. Ingrese un nombre de usuario y contraseña, y haga clic la **AUTORIZACIÓN**.

Verificación

Para verificar la conexión, utilice el comando **remoto del cliente-IP address del detalle de la sesión de criptografía de la demostración**. Refiera a la sesión de criptografía de la demostración para 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.

Troubleshooting

Para resolver problemas la conexión, recoger y analizar los registros del DARDO del cliente y utilizar estos comandos debug en el router: **paquete** y **debug crypto ikev2 del debug crypto ikev2 internos**.

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

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems