

Cisco IOS/CCP - Configuración de DMVPN con Cisco CP

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de Spoke con Cisco CP](#)

[Configuración CLI para Spoke](#)

[Configuración del hub mediante Cisco CP](#)

[Configuración CLI para Hub](#)

[Editar la configuración de DMVPN mediante CCP](#)

[Más información](#)

[Verificación](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una configuración de ejemplo para el túnel Dynamic Multipoint VPN (DMVPN) entre routers hub y spoke mediante Cisco Configuration Professional (Cisco CP). Dynamic Multipoint VPN es una tecnología que integra diversos conceptos como GRE, encriptación de IPsec, NHRP y Ruteo para proporcionar una solución sofisticada que permita a los usuarios finales comunicarse con eficacia a través de los túneles IPsec spoke al spoke creados dinámicamente.

[Prerequisites](#)

[Requirements](#)

Para obtener la mejor funcionalidad de DMVPN, se recomienda ejecutar la línea principal 12.4 del software Cisco IOS®, 12.4T y posteriores.

[Componentes Utilizados](#)

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

hardware.

- Router Cisco IOS serie 3800 con versión de software 12.4 (22)
- Router Cisco IOS serie 1800 con versión de software 12.3 (8)
- Cisco Configuration Professional versión 2.5

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.

[Antecedentes](#)

Este documento proporciona información sobre cómo configurar un router como spoke y otro router como hub usando Cisco CP. Se muestra la configuración de spoke inicial, pero más adelante en el documento, la configuración relacionada con hub también se muestra en detalle para proporcionar una mejor comprensión. Otros radios también se pueden configurar utilizando el enfoque similar para conectarse al hub. El escenario actual utiliza estos parámetros:

- Red pública del router hub - 209.165.201.0
- Red de túnel: 192.168.10.0
- Protocolo de ruteo utilizado - OSPF

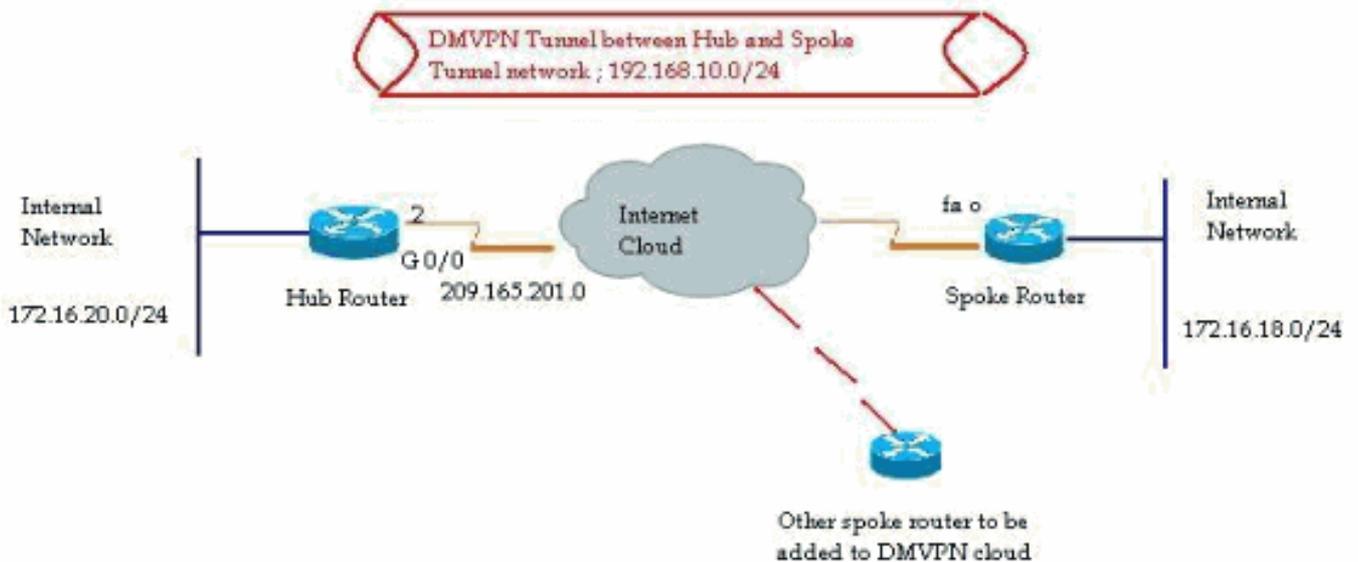
[Configurar](#)

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta [Command Lookup](#) (sólo para clientes [registrados](#)) para obtener más información sobre los comandos utilizados en esta sección.

[Diagrama de la red](#)

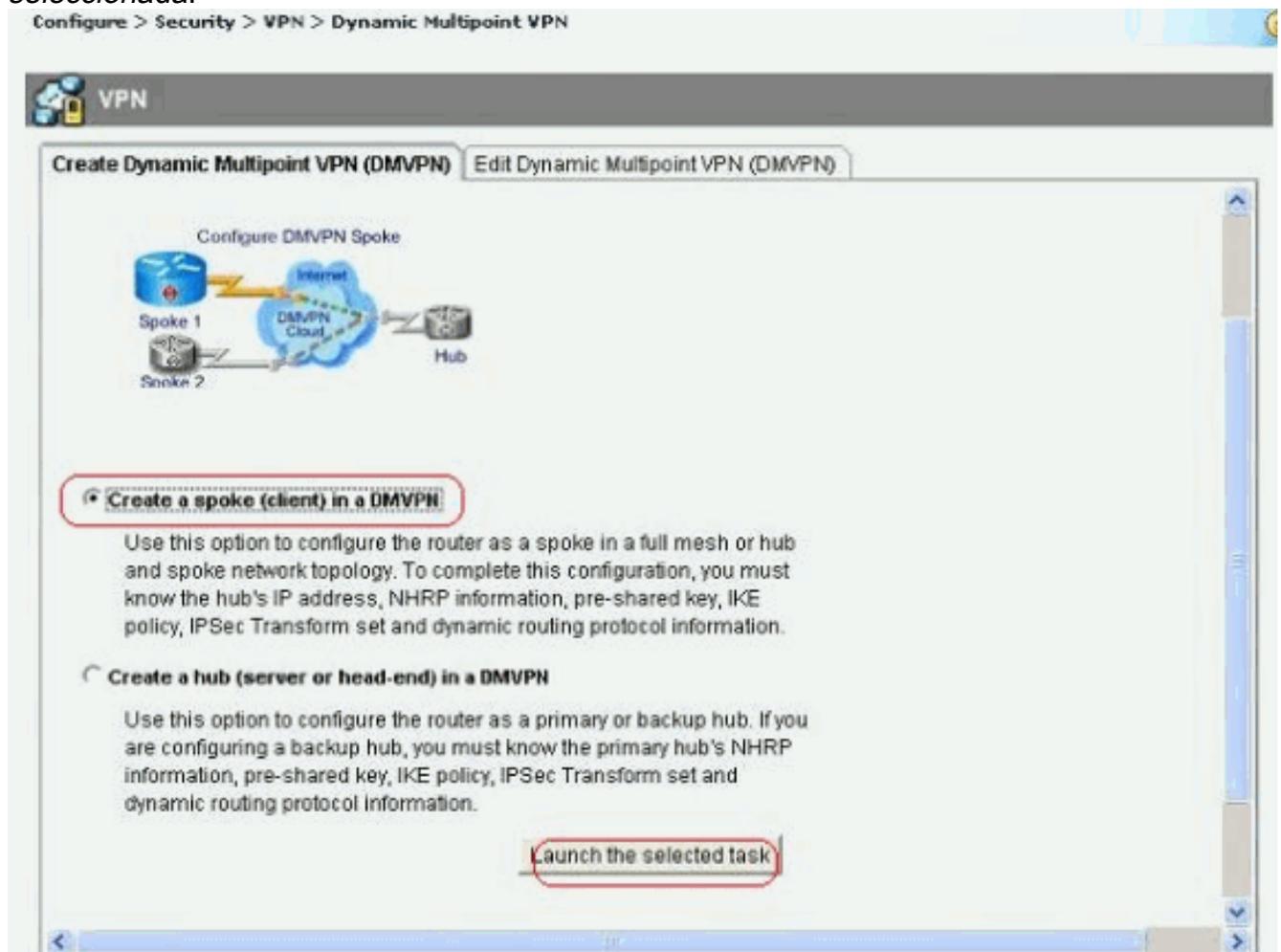
En este documento, se utiliza esta configuración de red:



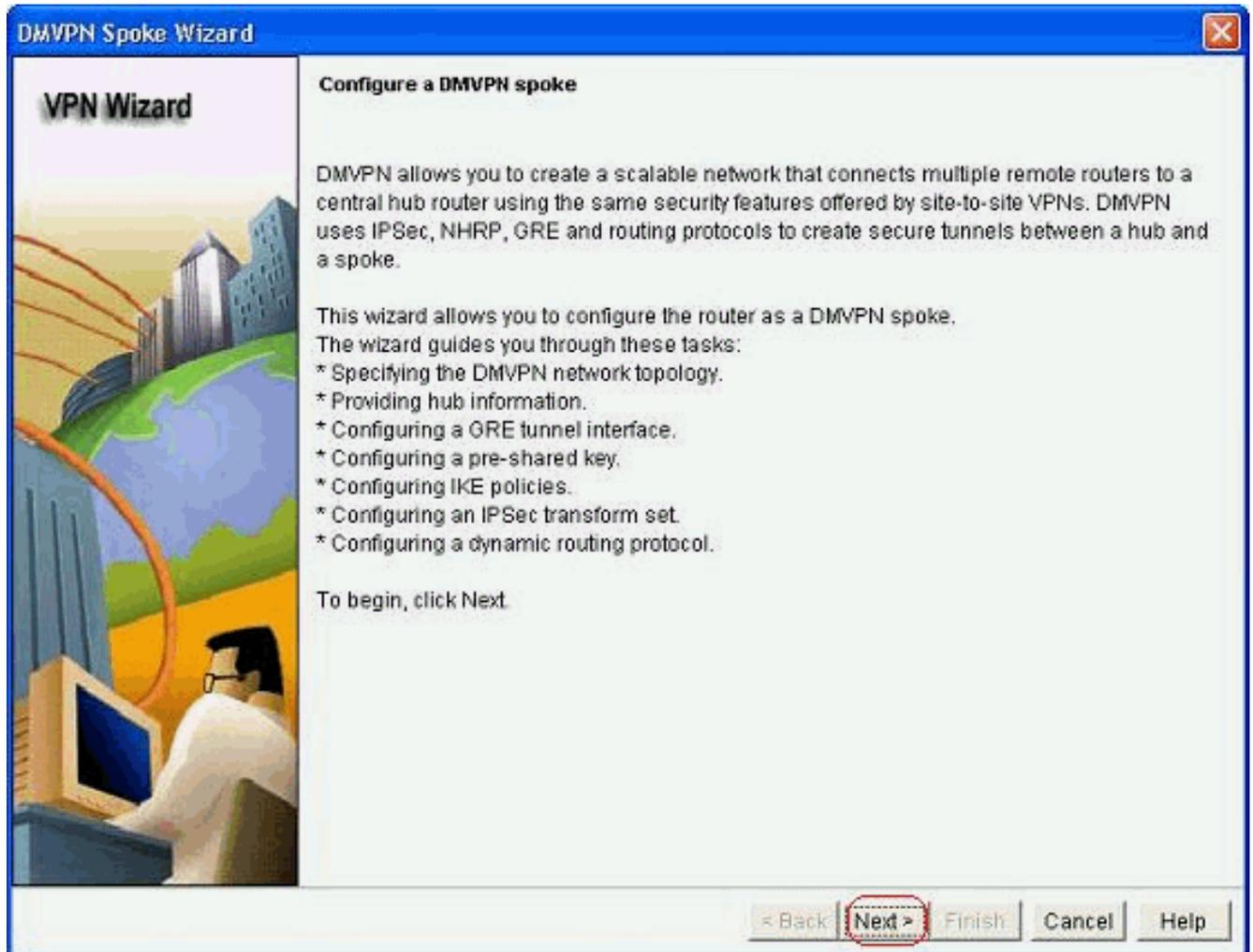
[Configuración de Spoke con Cisco CP](#)

Esta sección muestra cómo configurar un router como radio mediante el asistente de DMVPN paso a paso en Cisco Configuration Professional.

1. Para iniciar la aplicación Cisco CP e iniciar el asistente DMVPN, vaya a *Configurar > Seguridad > VPN > Dynamic Multipoint VPN*. A continuación, seleccione la opción *Crear un spoke en una DMVPN* y haga clic en *Iniciar la tarea seleccionada*.



2. Haga clic en *Siguiente* para comenzar.



3. Seleccione la opción *Hub and Spoke network* y haga clic en *Next*.

DMVPN Spoke Wizard - 10% Complete

VPN Wizard

DMVPN Network Topology

Select the DMVPN network topology.

Hub and Spoke network

In this topology, all DMVPN traffic is routed through the hub. A point-to-point GRE interface will be configured on the spoke, and the spoke will use it to create a tunnel to the hub which will remain up. Spokes do not create GRE tunnels to other spokes in this topology.

Fully meshed network

In this topology, the spoke dynamically establishes a direct tunnel to another spoke device, and sends DMVPN traffic directly to it. A multipoint GRE tunnel interface is configured on the spoke to support this functionality.

Note: Cisco supports fully meshed DMVPN networks only in the following Cisco IOS images: 12.3(8)T1 and 12.3(9) or later.

Hub and Spoke Network

< Back **Next >** Finish Cancel Help

4. Especifique la información relacionada con el concentrador, como la interfaz pública del router del concentrador y la interfaz de túnel del router del concentrador.

DMVPN Spoke Wizard (Hub and Spoke Topology) - 20% Complete

VPN Wizard

Specify Hub Information
Enter the IP address of the hub and the IP address of the hub's mGRE tunnel interface. Contact your network administrator to get this information.

Hub Information

IP address of hub's physical interface: 209.165.201.2

IP address of hub's mGRE tunnel interface: 192.168.10.2

Spoke
You are configuring this spoke router

Internet
DMVPN Cloud

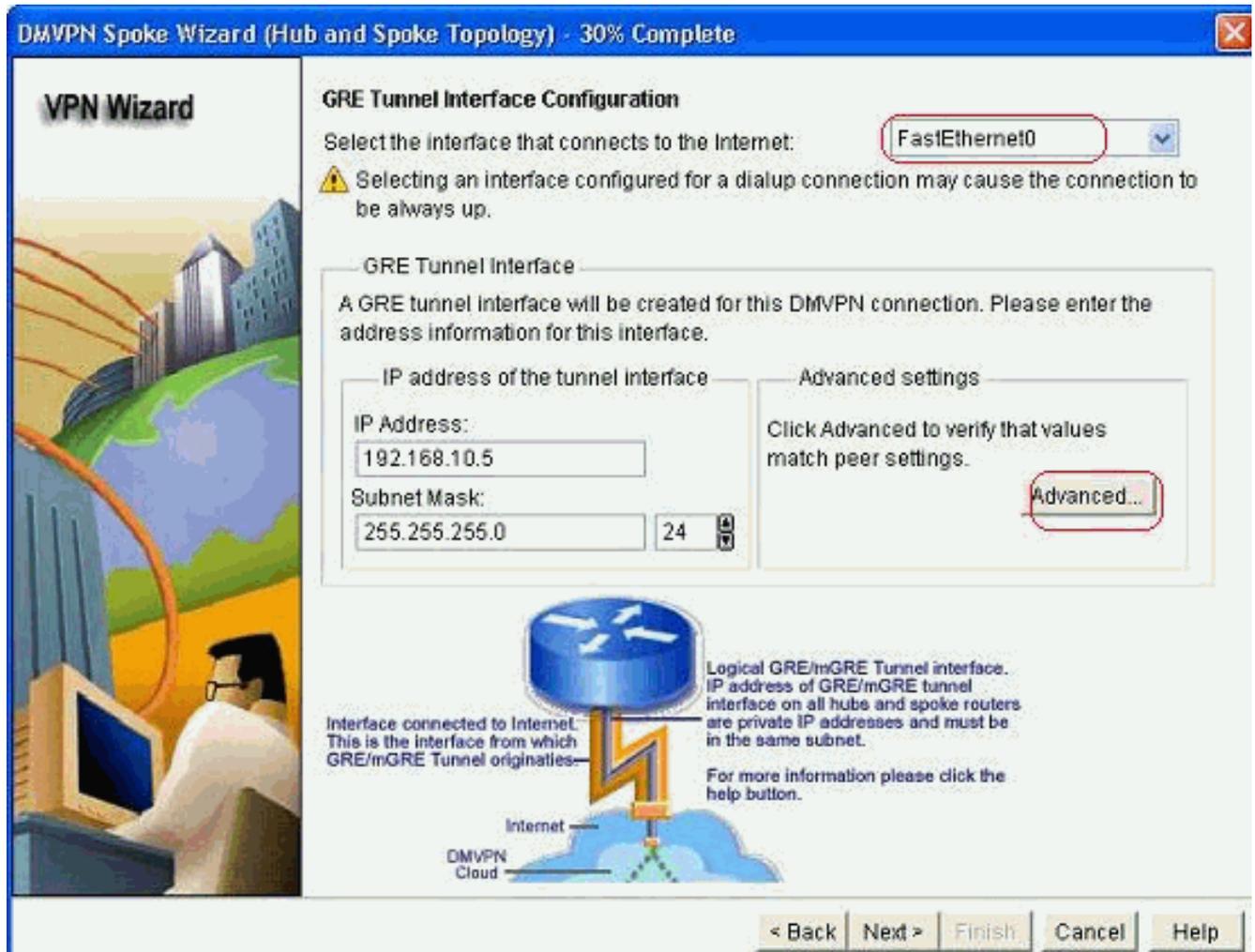
Hub

Public IP address to be entered above

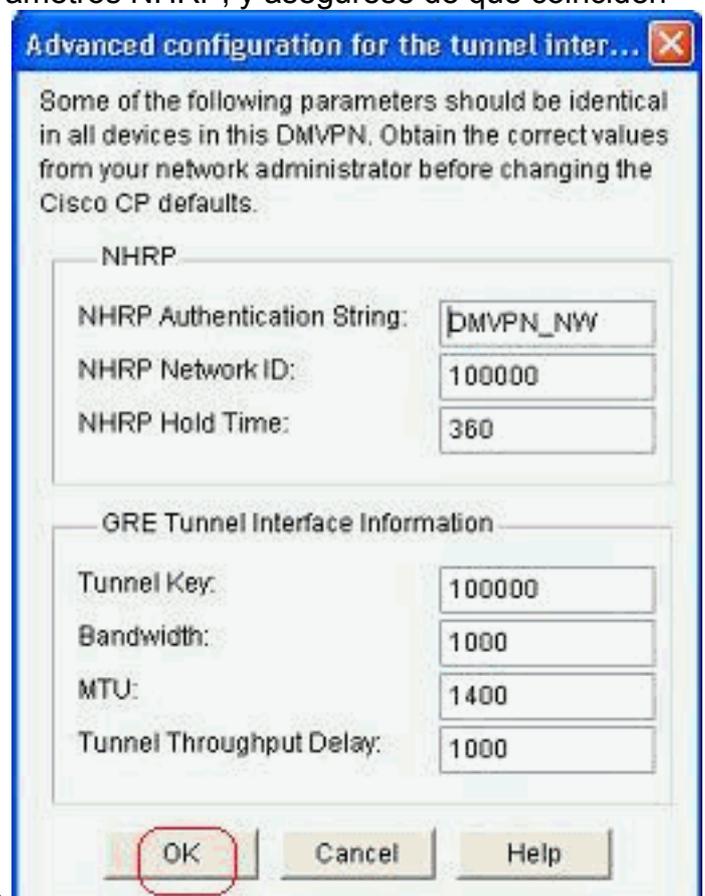
IP address of the mGRE tunnel to be entered above

< Back | **Next >** | Finish | Cancel | Help

5. Especifique los detalles de la interfaz de túnel del spoke y la interfaz pública del spoke. A continuación, haga clic en *Advanced*.



6. Verifique los parámetros del túnel y los parámetros NHRP, y asegúrese de que coinciden



perfectamente con los parámetros del Hub.

7. Especifique la clave previamente compartida y haga clic en

Siguiente.

VPN Wizard

Authentication

Select the method you want to use to authenticate this router to the peer device(s) in the DMVPN network. You can use digital certificate or a pre-shared key. If digital certificate is used, the router must have a valid certificate configured. If pre-shared key is used, the key configured on this router must match the keys configured on all other routers in the DMVPN network.

Digital Certificates

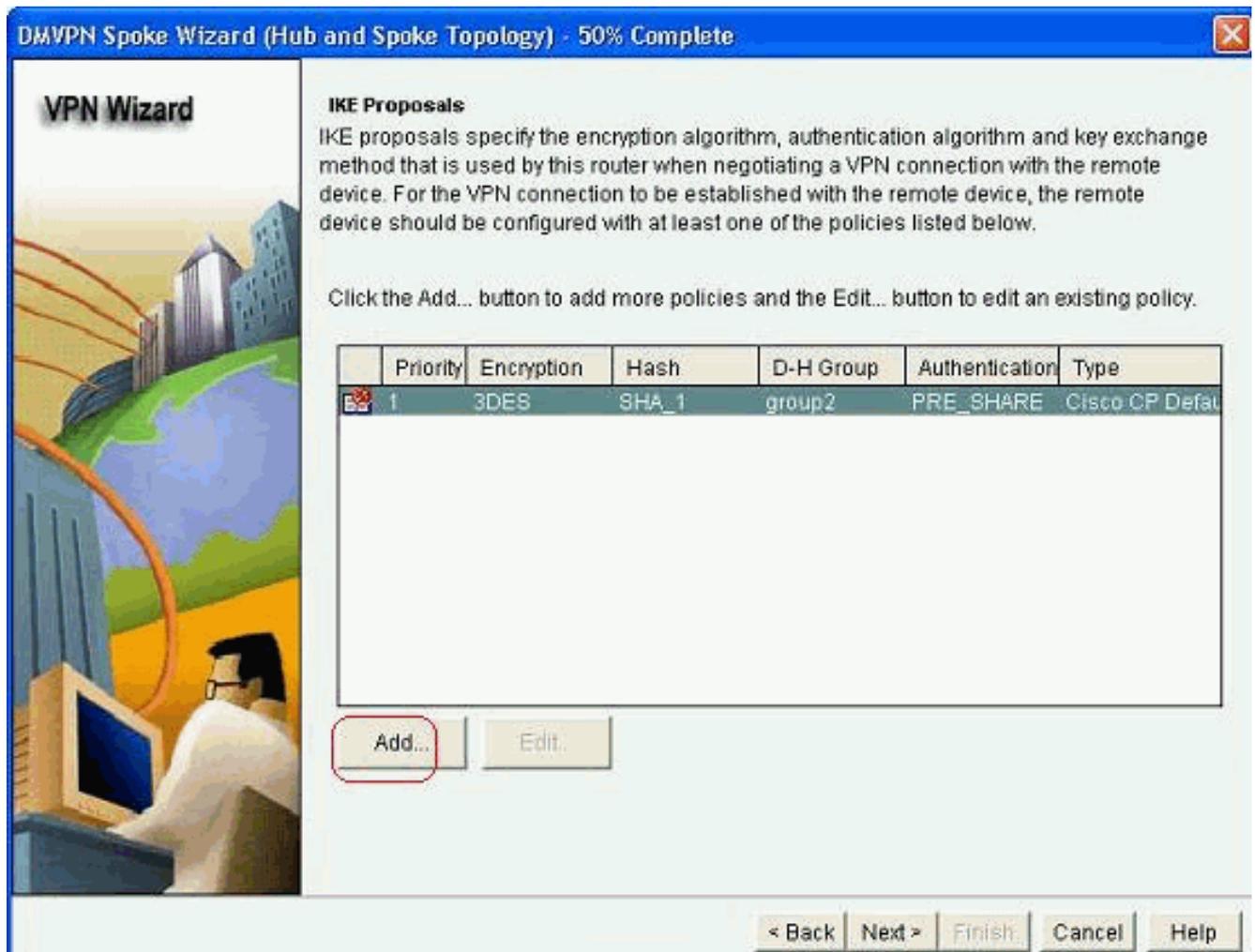
Pre-shared Keys

pre-shared key:

Reenter key:

< Back **Next >** Finish Cancel Help

8. Haga clic en *Agregar* para agregar una propuesta IKE independiente.

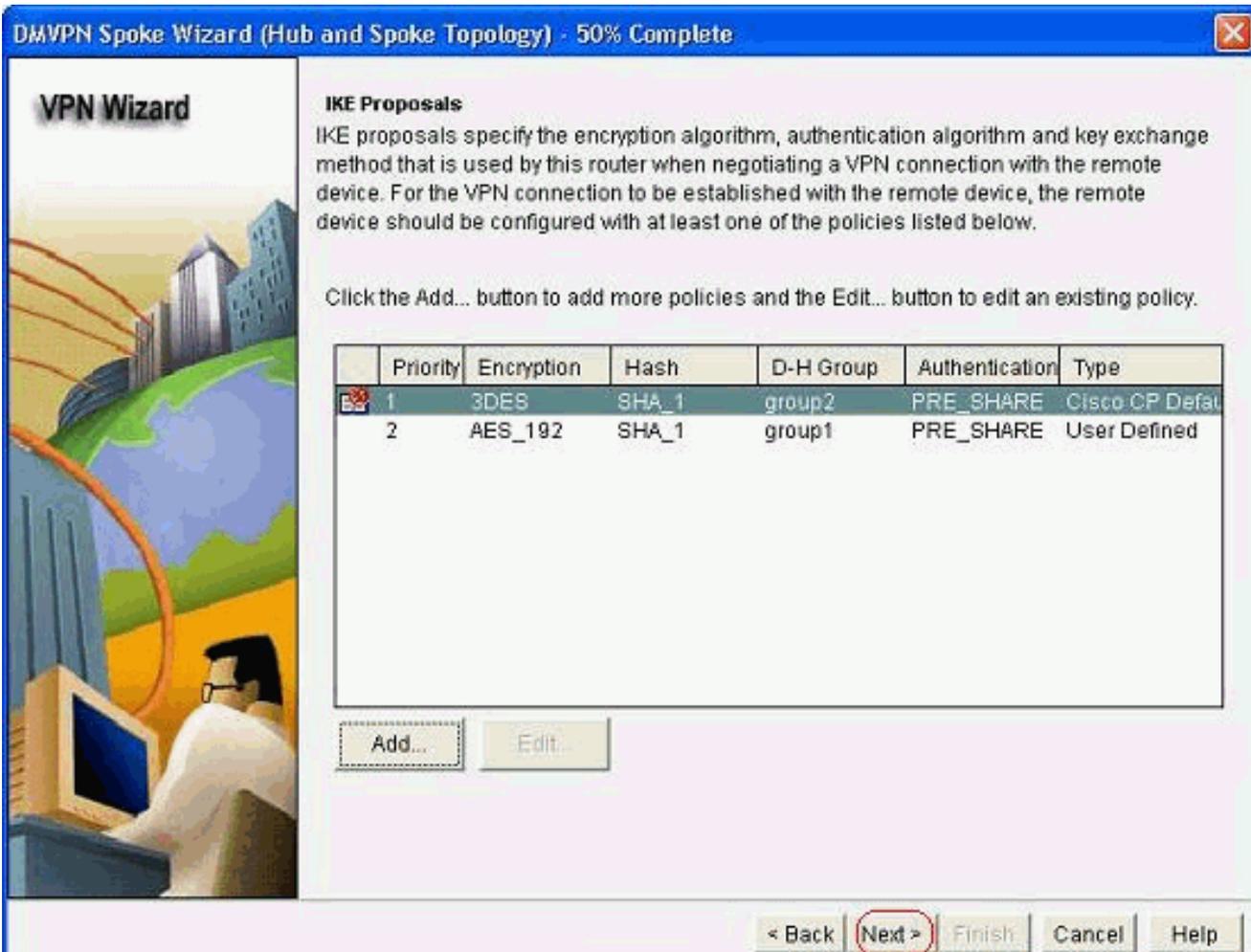


9. Especifique los parámetros de cifrado, autenticación y hash. A continuación, haga clic en

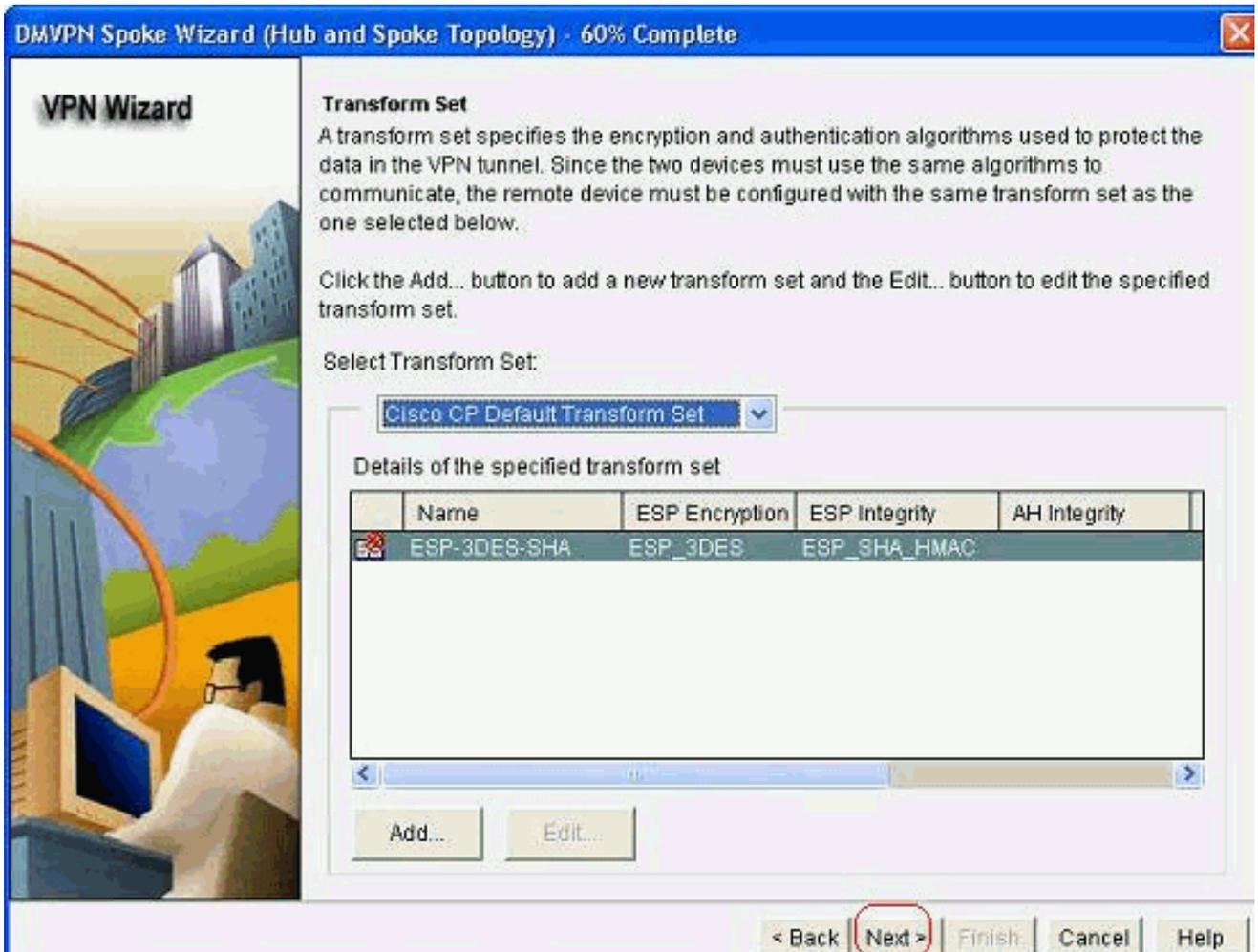


Aceptar.

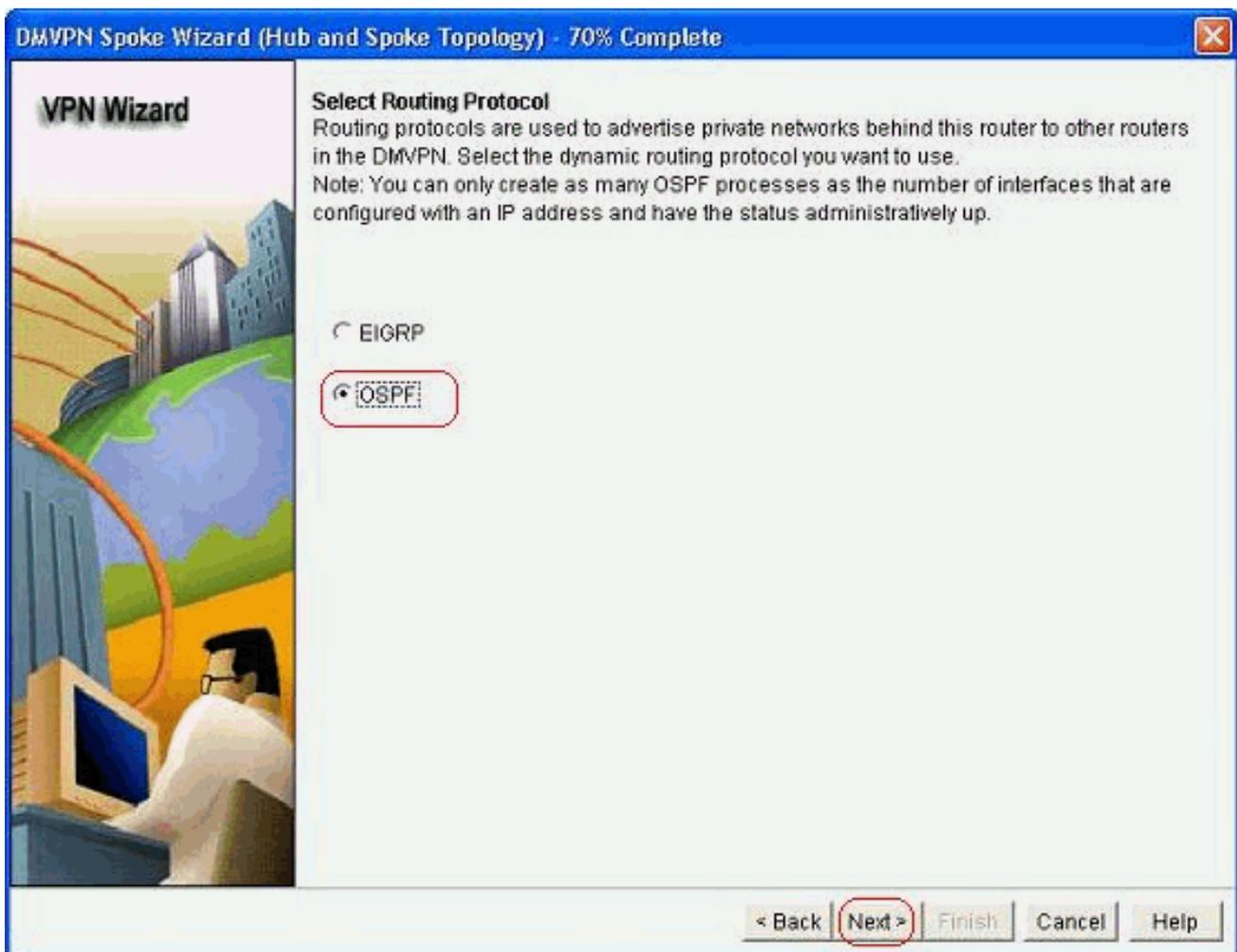
10. La nueva política IKE se puede ver aquí. Haga clic en Next (Siguiete).



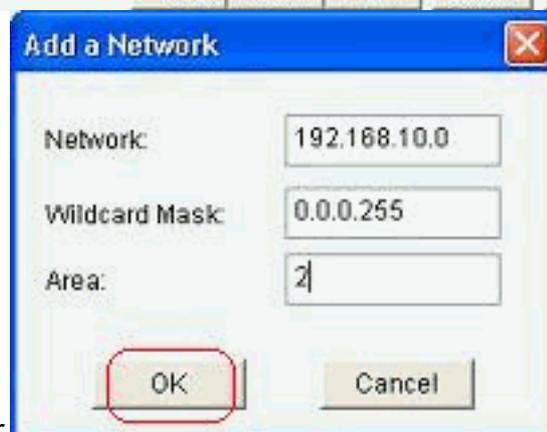
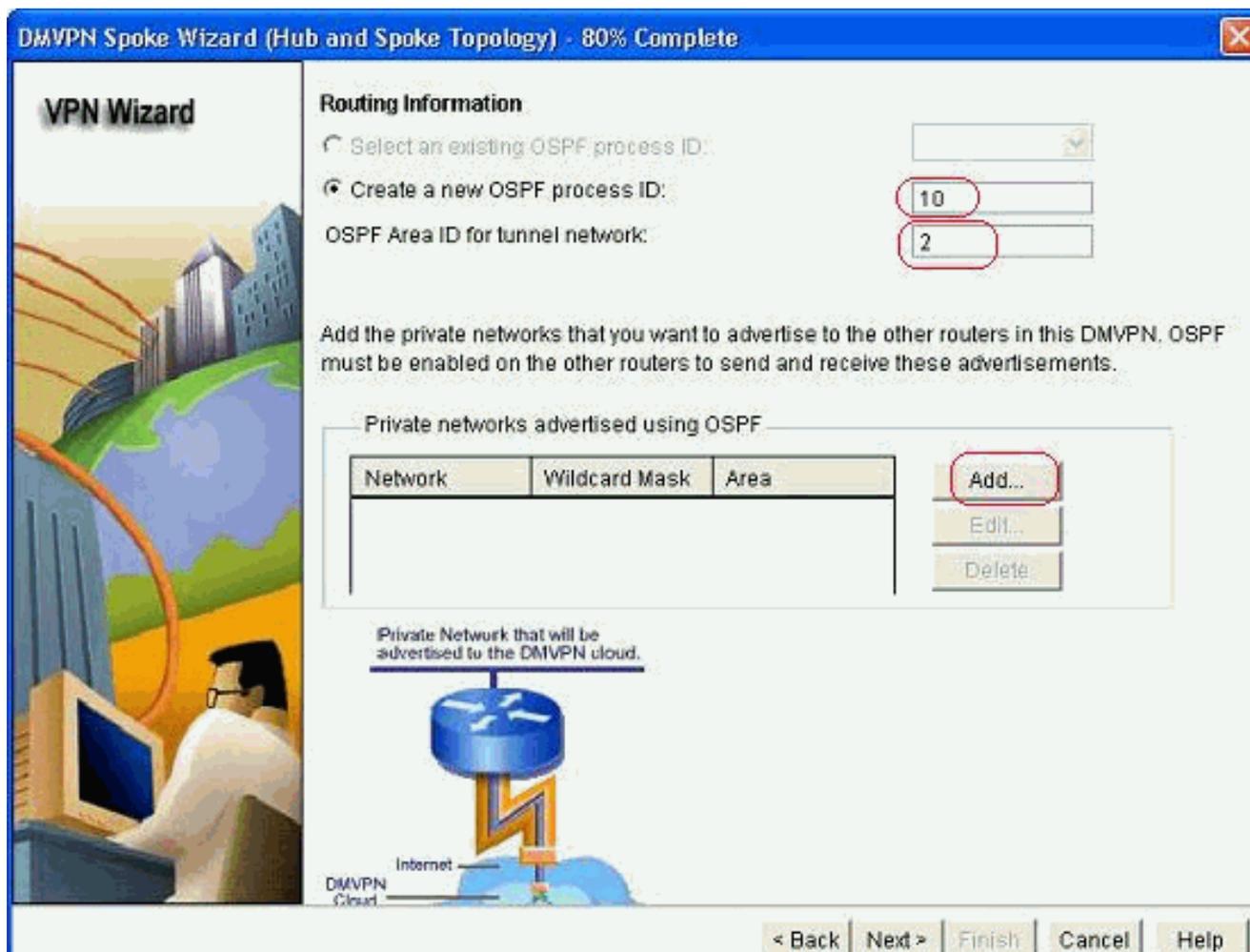
11. Haga clic en *Next* para continuar con el conjunto de transformación predeterminado.



12. Seleccione el protocolo de ruteo necesario. Aquí, se selecciona *OSPF*.

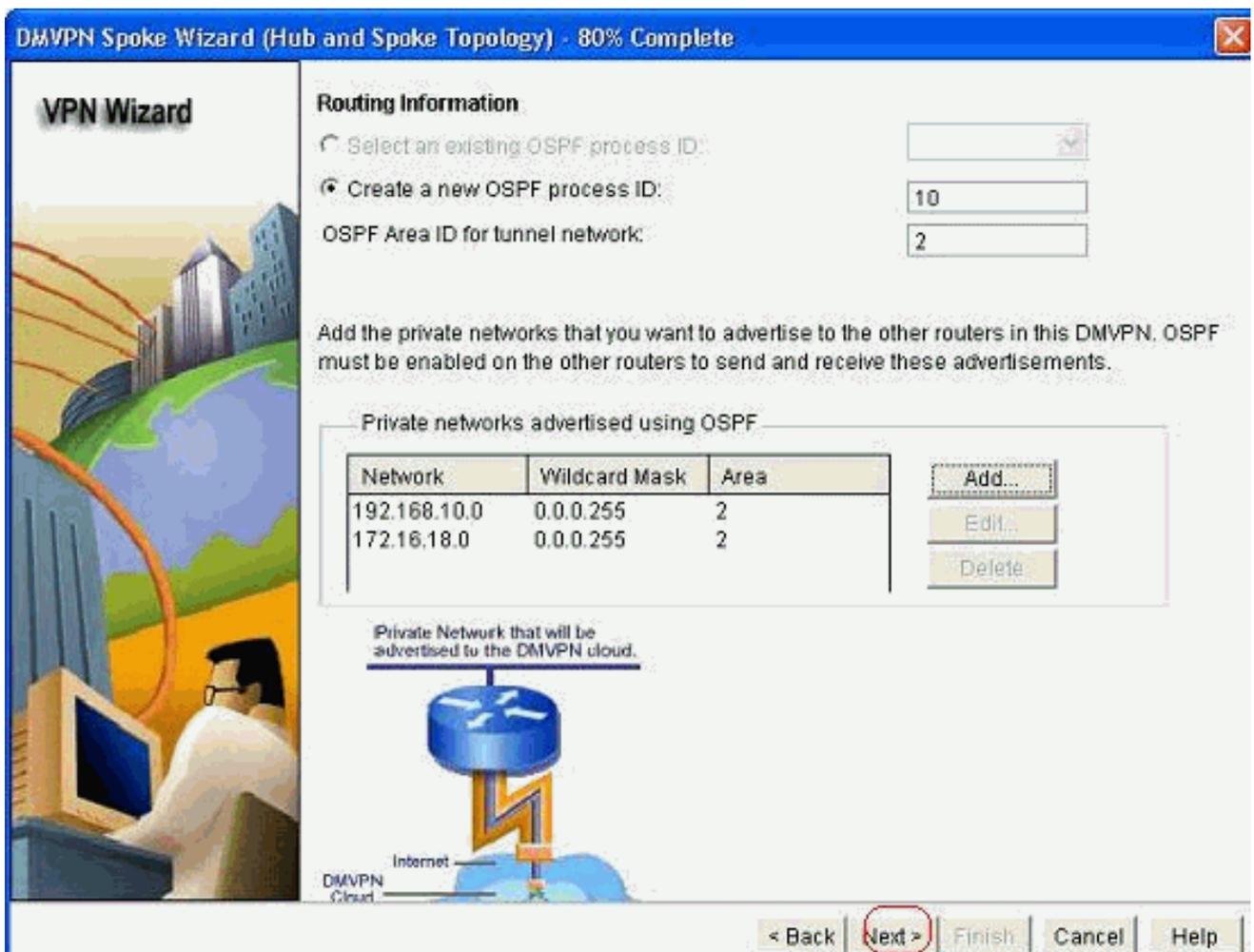


13. Especifique el ID de proceso OSPF y el ID de área. Haga clic en *Agregar* para agregar las redes que serán anunciadas por OSPF.

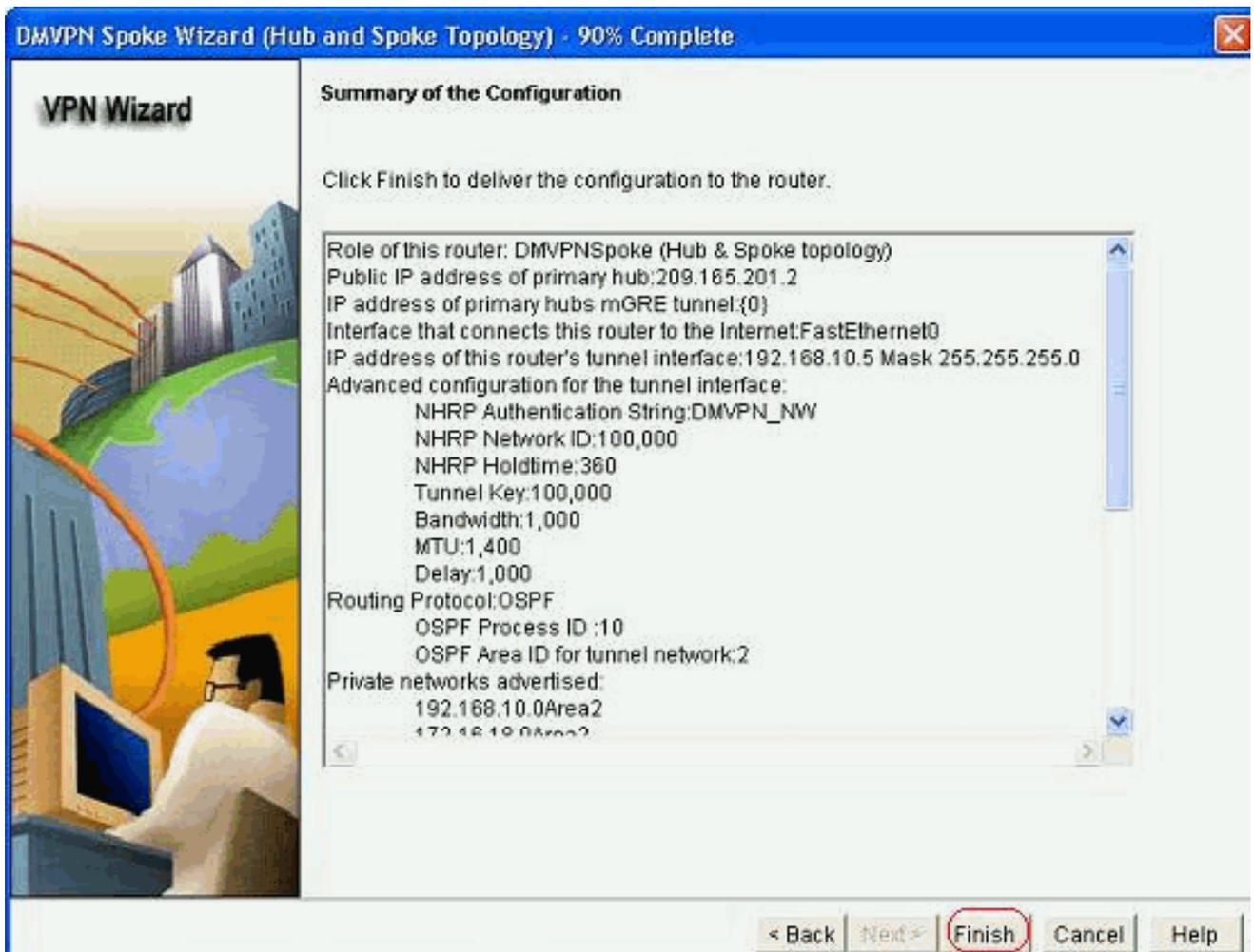


14. Agregue la red de túnel y haga clic en *Aceptar*.

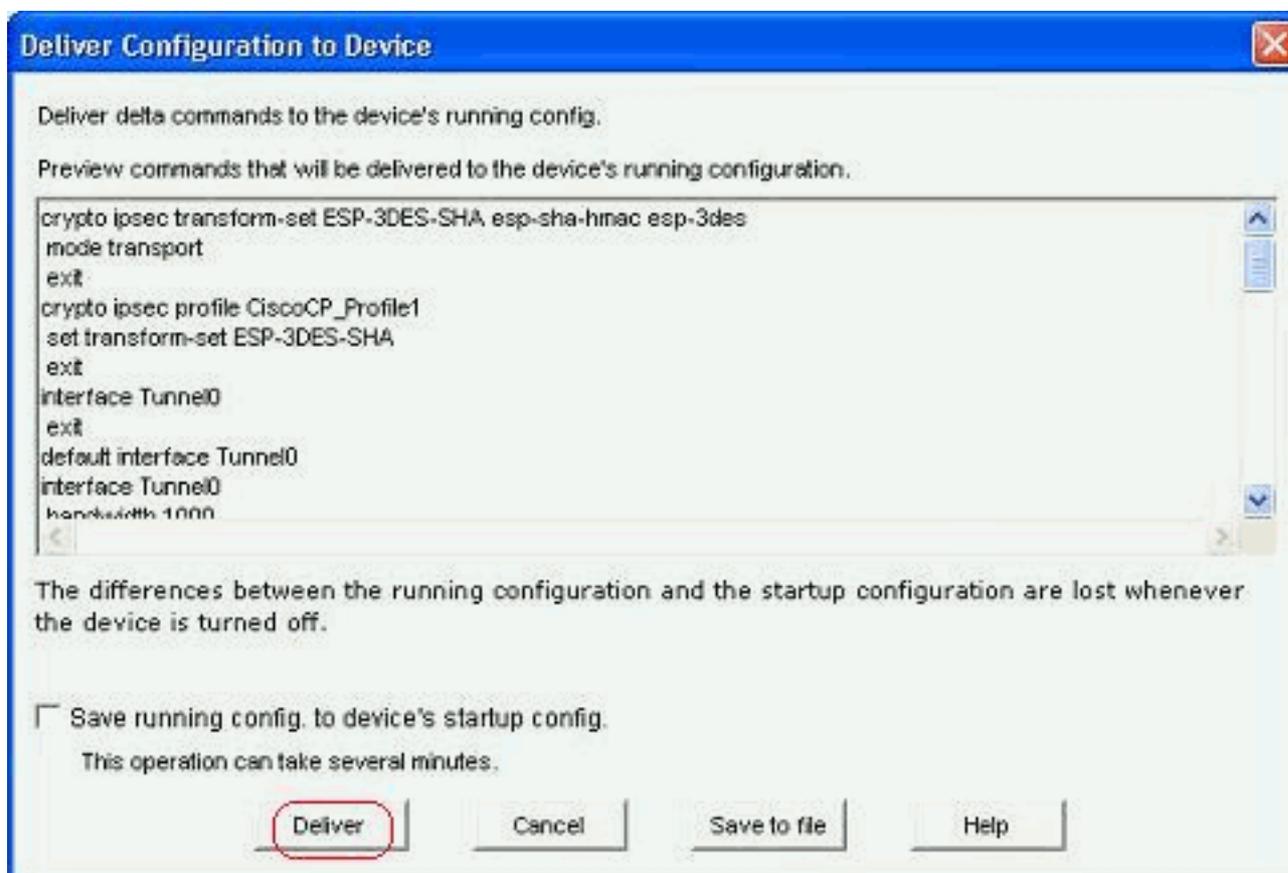
15. Agregue la red privada detrás del router spoke. A continuación, haga clic en *Siguiente*.



16. Haga clic en *Finalizar* para completar la configuración del asistente.



17. Haga clic en *Entregar* para ejecutar los comandos. Marque la casilla de verificación *Guardar configuración en ejecución en la configuración de inicio del dispositivo* si desea guardar la configuración.



Configuración CLI para Spoke

La configuración CLI relacionada se muestra aquí:

Router spoke
<pre>crypto ipsec transform-set ESP-3DES-SHA esp-sha-hmac esp-3des mode transport exit crypto ipsec profile CiscoCP_Profile1 set transform-set ESP-3DES-SHA exit interface Tunnel0 exit default interface Tunnel0 interface Tunnel0 bandwidth 1000 delay 1000 ip nhrp holdtime 360 ip nhrp network-id 100000 ip nhrp authentication DMVPN_NW ip ospf network point-to-multipoint ip mtu 1400 no shutdown ip address 192.168.10.5 255.255.255.0 ip tcp adjust-mss 1360 ip nhrp nhs 192.168.10.2 ip nhrp map 192.168.10.2 209.165.201.2 tunnel source FastEthernet0 tunnel destination 209.165.201.2 tunnel protection ipsec profile CiscoCP_Profile1 tunnel key 100000</pre>

```
exit
router ospf 10
 network 192.168.10.0 0.0.0.255 area 2
 network 172.16.18.0 0.0.0.255 area 2
exit
crypto isakmp key ***** address 209.165.201.2
crypto isakmp policy 2
 authentication pre-share
 encr aes 192
 hash sha
 group 1
 lifetime 86400
exit
crypto isakmp policy 1
 authentication pre-share
 encr 3des
 hash sha
 group 2
 lifetime 86400
exit
```

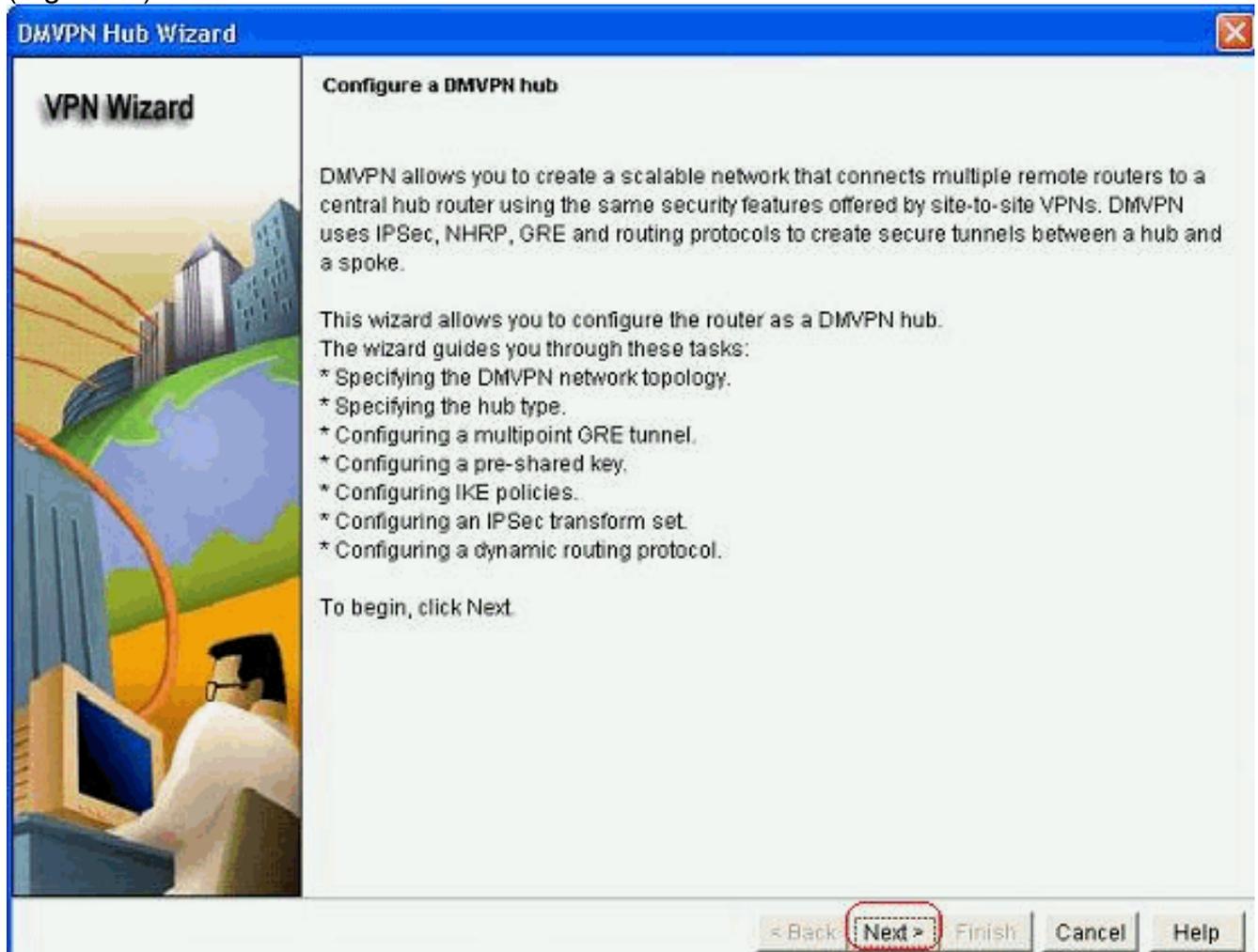
[Configuración del hub mediante Cisco CP](#)

En esta sección se muestra un enfoque paso a paso sobre cómo configurar el router hub para la DMVPN.

1. Vaya a *Configure > Security > VPN > Dynamic Multipoint VPN* y seleccione la opción *Create a hub in a DMVPN*. El, haga clic en *Iniciar la tarea seleccionada*.

The screenshot shows the Cisco Configuration Assistant (CCA) interface for configuring a Dynamic Multipoint VPN (DMVPN). The breadcrumb navigation is **Configure > Security > VPN > Dynamic Multipoint VPN**. The main heading is **VPN**. Below this, there are two tabs: **Create Dynamic Multipoint VPN (DMVPN)** (selected) and **Edit Dynamic Multipoint VPN (DMVPN)**. A diagram illustrates the DMVPN topology with two spokes (Spoke 1 and Spoke 2) connected to a central cloud labeled **DMVPN Cloud**, which is then connected to a **Hub** router. Below the diagram, there are two radio button options: **Create a spoke (client) in a DMVPN** (unselected) and **Create a hub (server or head-end) in a DMVPN** (selected). The selected option is highlighted with a red box. Below the selected option, there is a description: "Use this option to configure the router as a primary or backup hub. If you are configuring a backup hub, you must know the primary hub's NHRP information, pre-shared key, IKE policy, IPsec Transform set and dynamic routing protocol information." At the bottom right, there is a button labeled **Launch the selected task**, also highlighted with a red box.

2. Haga clic en Next (Siguiente).



3. Seleccione la opción *Hub and Spoke network* y haga clic en *Next*.

VPN Wizard

DMVPN Network Topology

Select the DMVPN network topology.

Hub and Spoke network

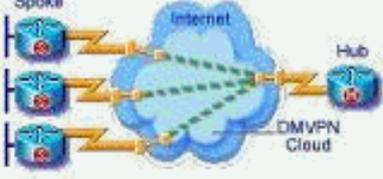
In this topology, all DMVPN traffic is routed through the hub. A point-to-point GRE interface will be configured on the spoke, and the spoke will use it to create a tunnel to the hub which will remain up. Spokes do not create GRE tunnels to other spokes in this topology.

Fully meshed network

In this topology, the spoke dynamically establishes a direct tunnel to another spoke device, and sends DMVPN traffic directly to it. A multipoint GRE tunnel interface is configured on the spoke to support this functionality.

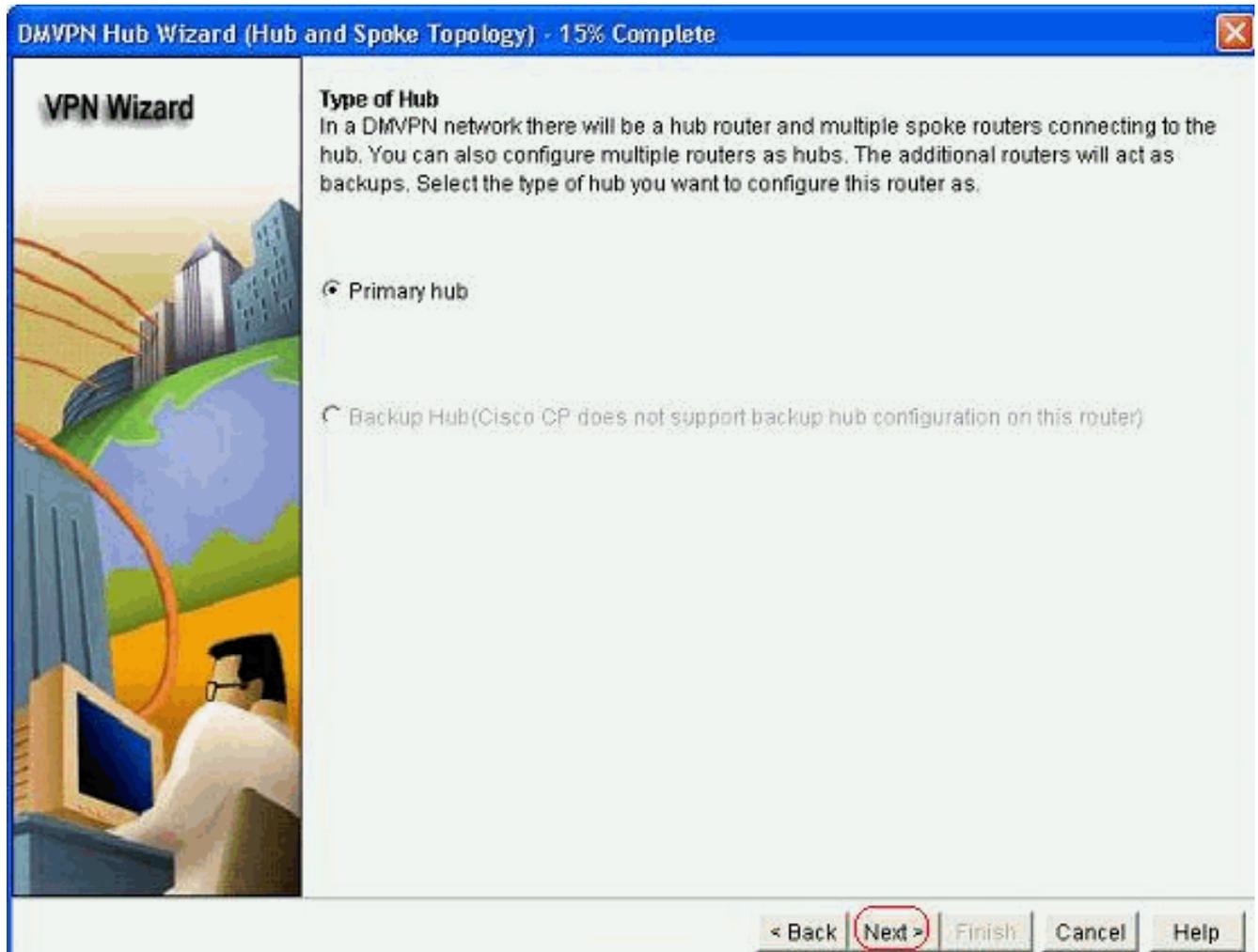
Note: Cisco supports fully meshed DMVPN networks only in the following Cisco IOS images: 12.3(8)T1 and 12.3(9) or later.

Hub and Spoke Network



< Back **Next >** Finish Cancel Help

4. Seleccione *Hub principal*. A continuación, haga clic en *Siguiente*.



5. Especifique los parámetros de la interfaz de túnel y haga clic en *Advanced*.

VPN Wizard



Multipoint GRE Tunnel Interface Configuration

Select the interface that connects to the Internet: GigabitEthernet0/0

⚠ Selecting an interface configured for a dialup connection may cause the connection to be always up.

Multi point GRE (mGRE) Tunnel Interface

A GRE tunnel interface will be created for this DMVPN connection. Please enter the address information for this interface.

IP address of the tunnel interface

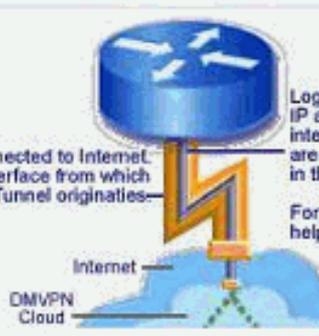
IP Address:

Subnet Mask:

Advanced settings

Click Advanced to verify that values match peer settings.

Advanced...



6. Especifique los parámetros de túnel y los parámetros NHRP. A continuación, haga clic en

Advanced configuration for the tunnel inter... ✖

Some of the following parameters should be identical in all devices in this DMVPN. Obtain the correct values from your network administrator before changing the Cisco CP defaults.

NHRP

NHRP Authentication String:

NHRP Network ID:

NHRP Hold Time:

GRE Tunnel Interface Information

Tunnel Key:

Bandwidth:

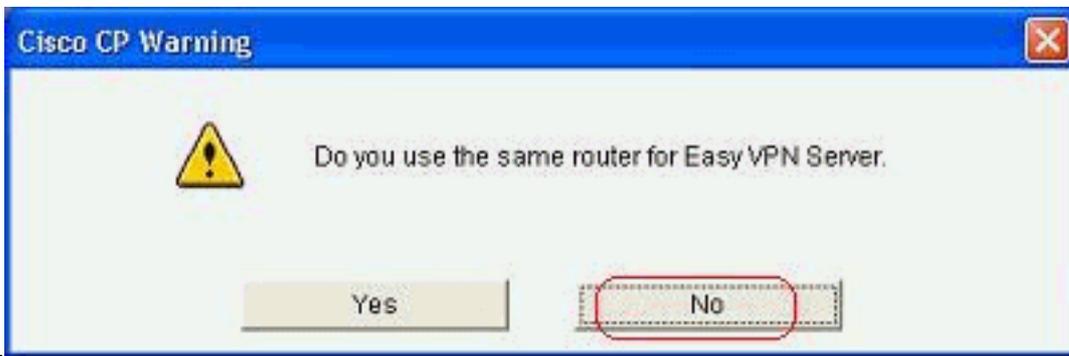
MTU:

Tunnel Throughput Delay:

OK
Cancel
Help

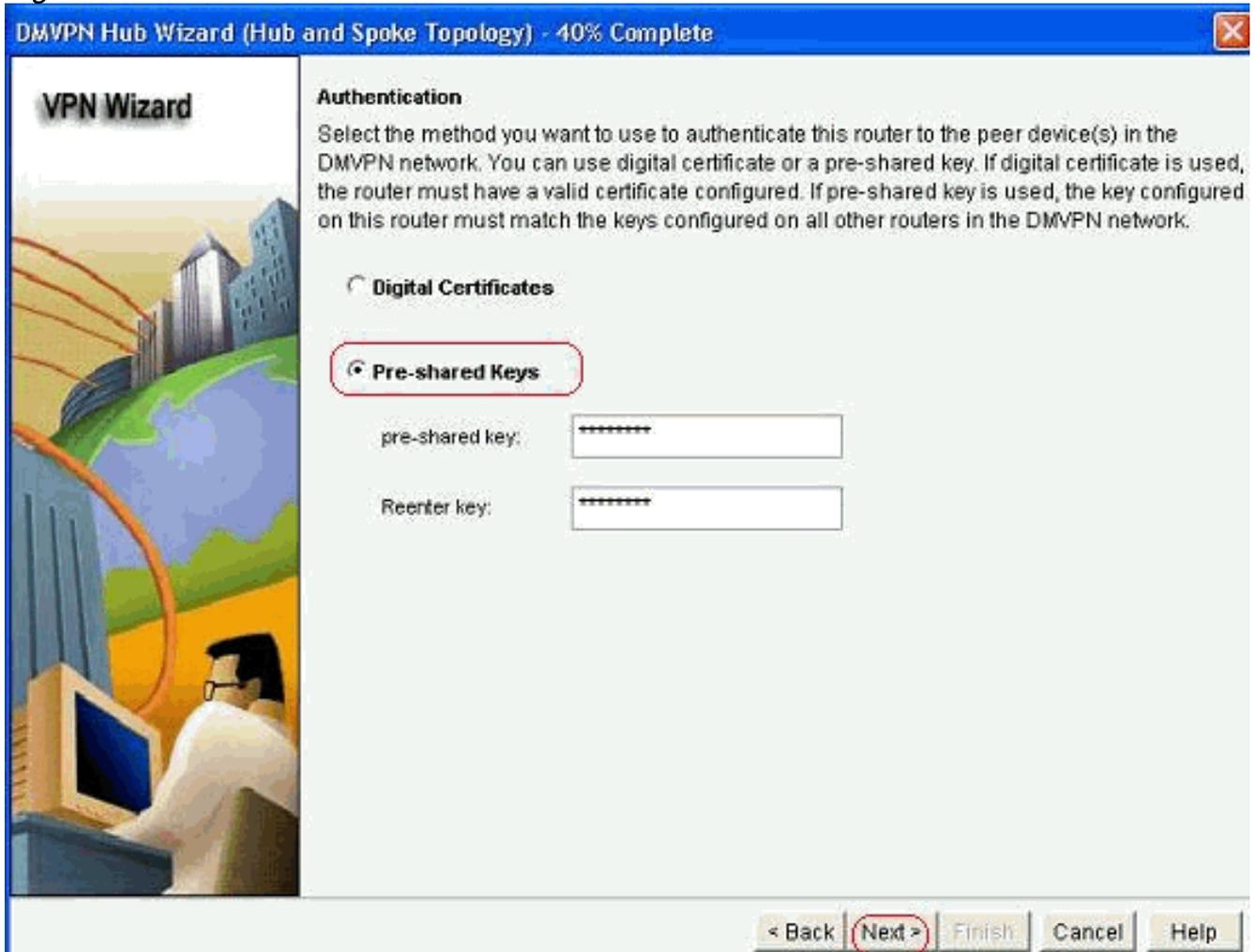
Aceptar.

7. Especifique la opción en función de la configuración de la

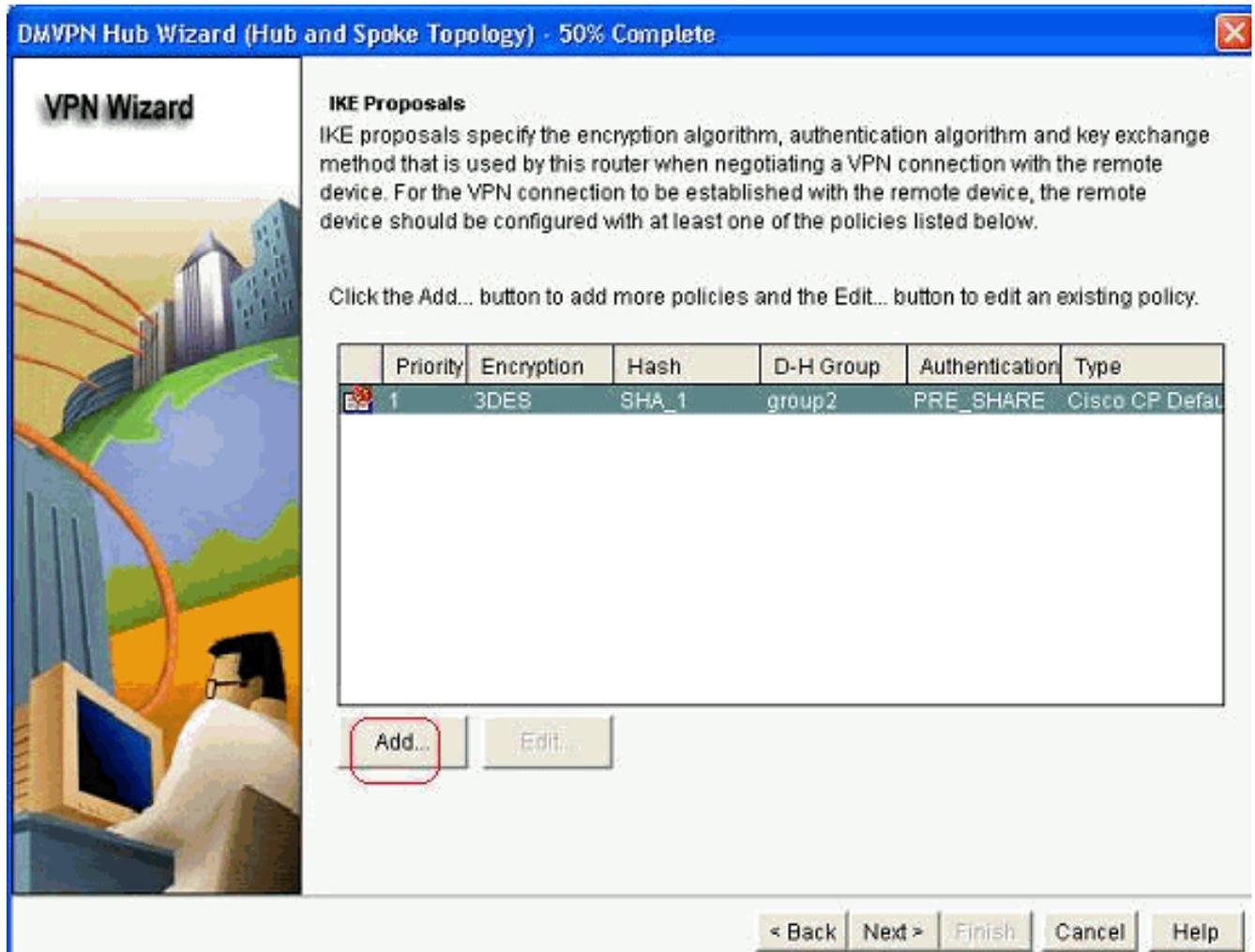


red.

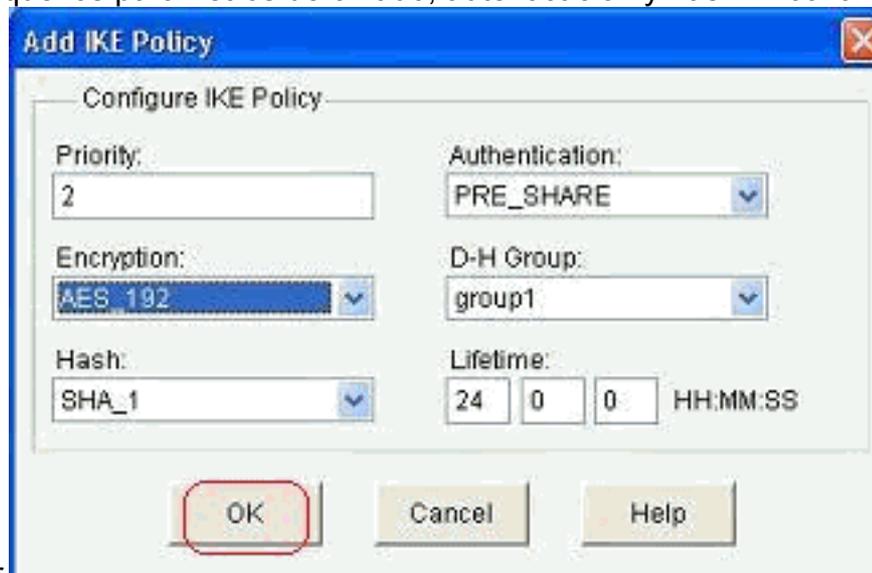
8. Seleccione *Pre-shared Keys* y especifique las claves previamente compartidas. A continuación, haga clic en *Siguiente*.



9. Haga clic en *Agregar* para agregar una propuesta IKE independiente.

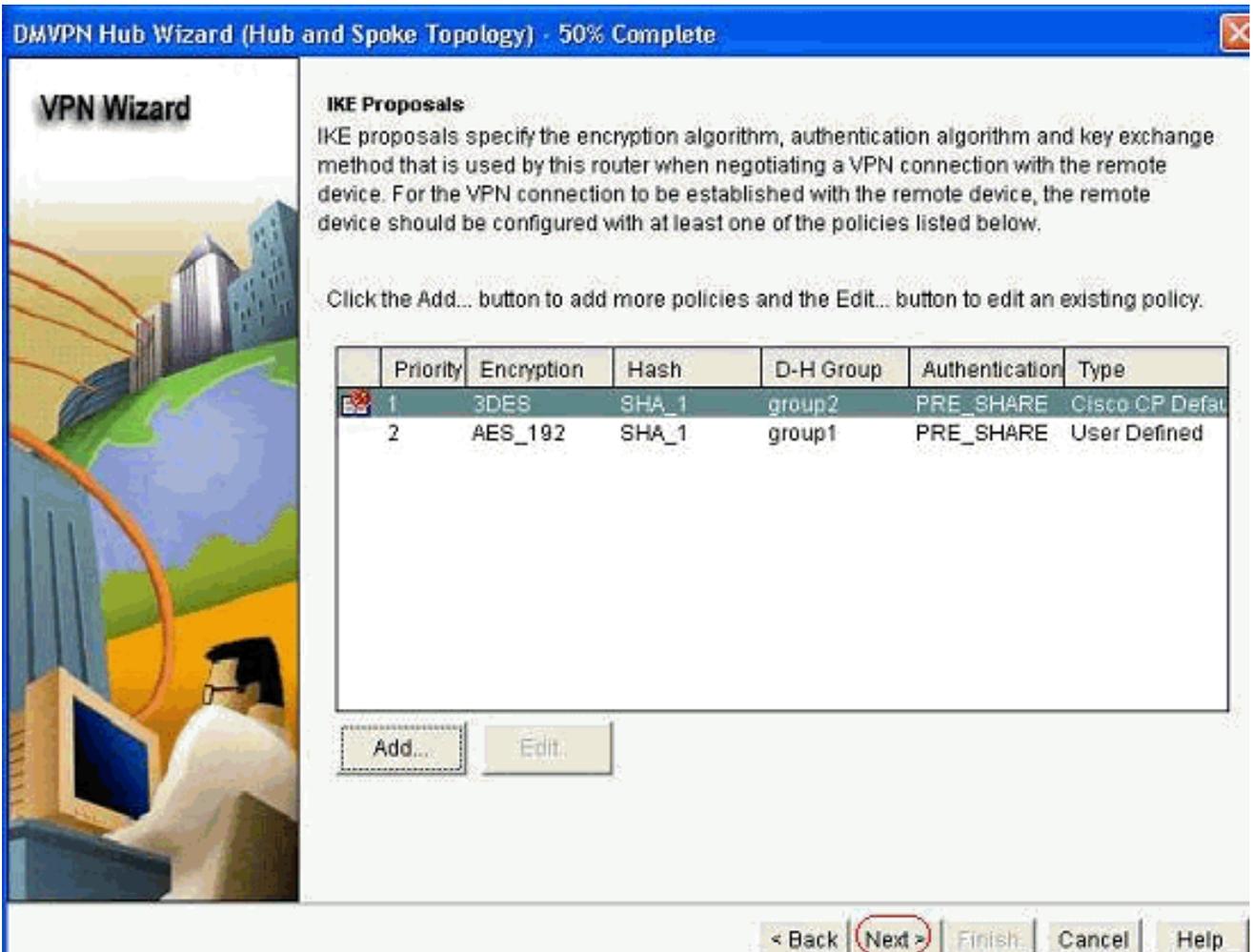


10. Especifique los parámetros de cifrado, autenticación y hash. A continuación, haga clic en

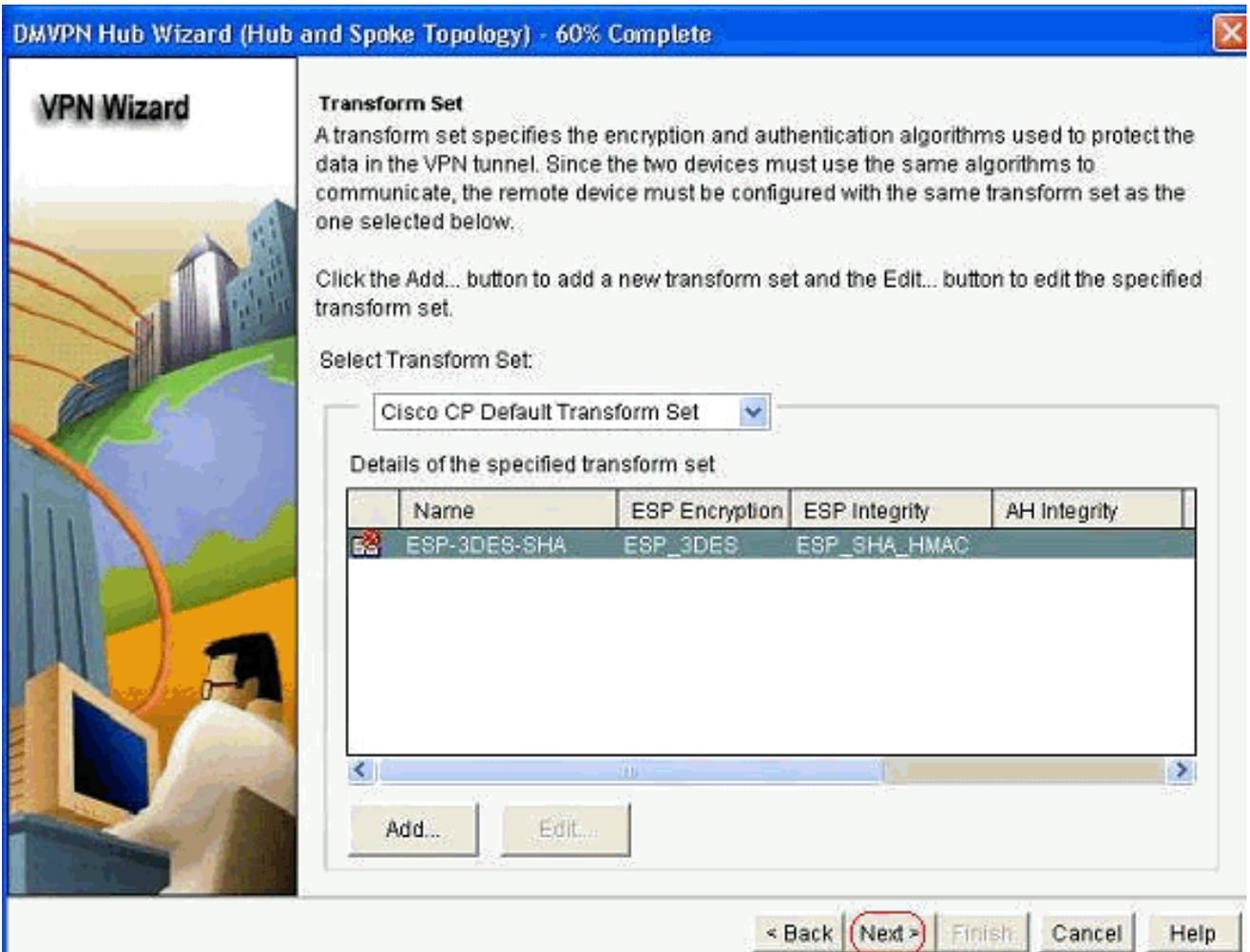


Aceptar.

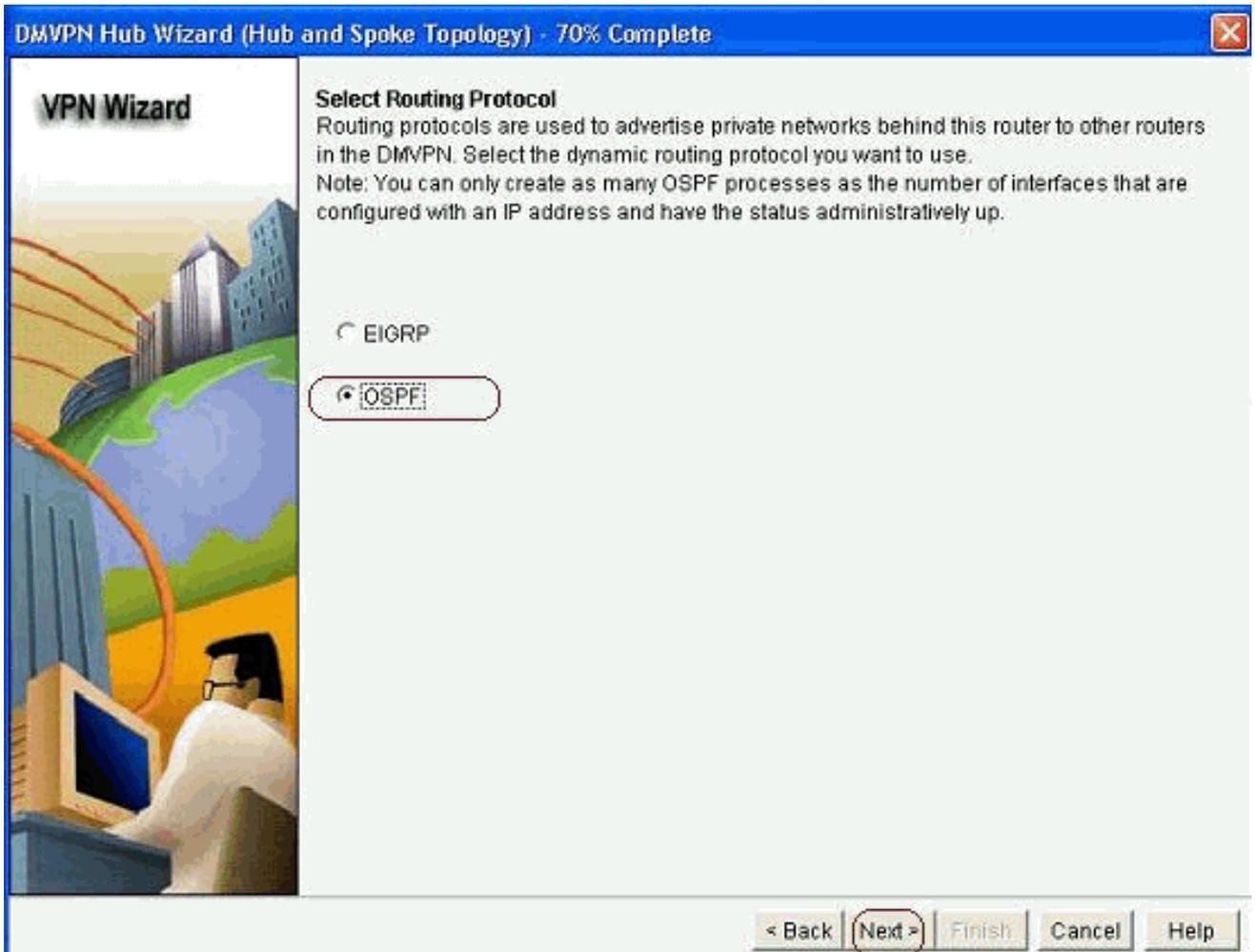
11. La nueva política IKE se puede ver aquí. Haga clic en Next (Siguiente).



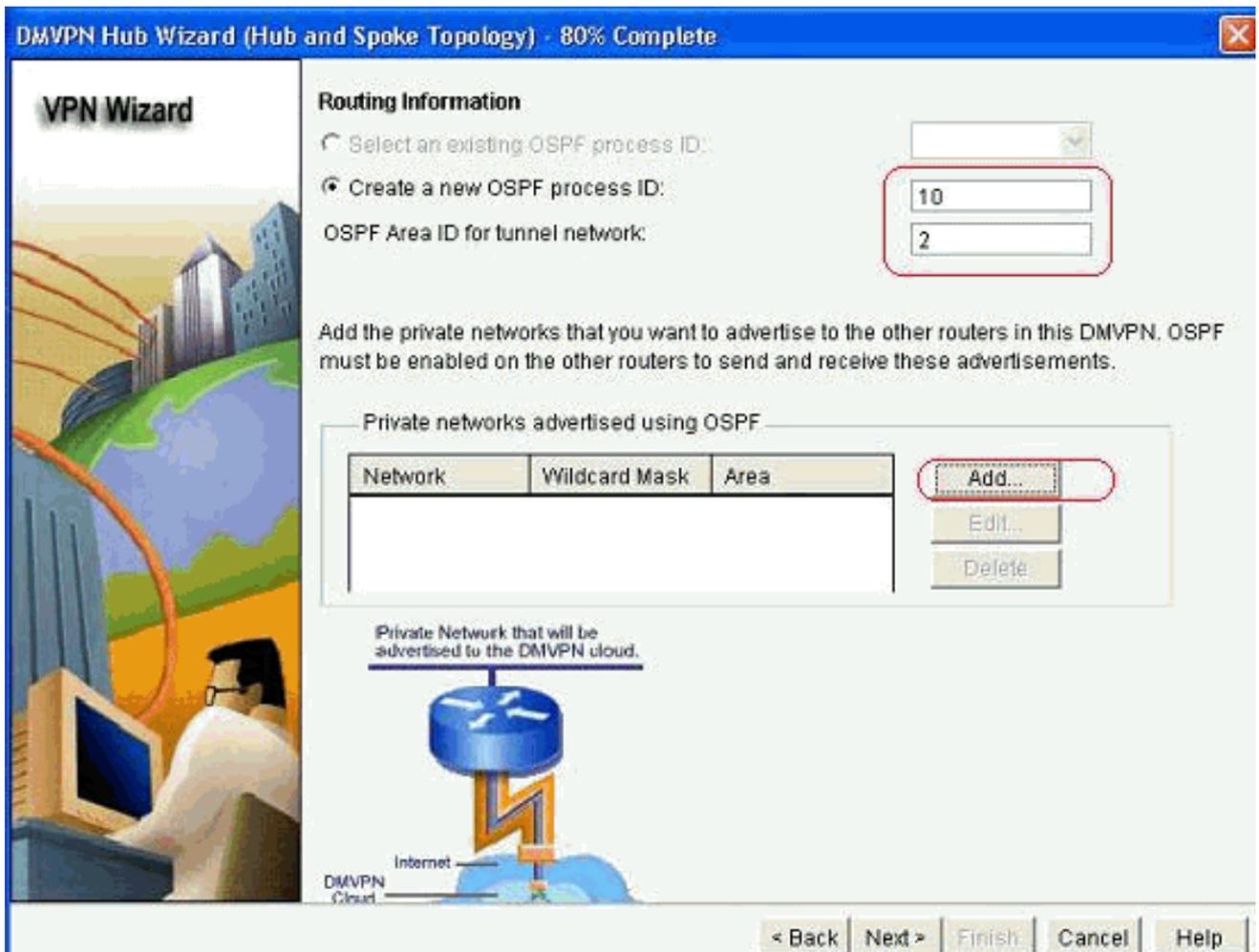
12. Haga clic en *Next* para continuar con el conjunto de transformación predeterminado.



13. Seleccione el protocolo de ruteo necesario. Aquí, se selecciona *OSPF*.

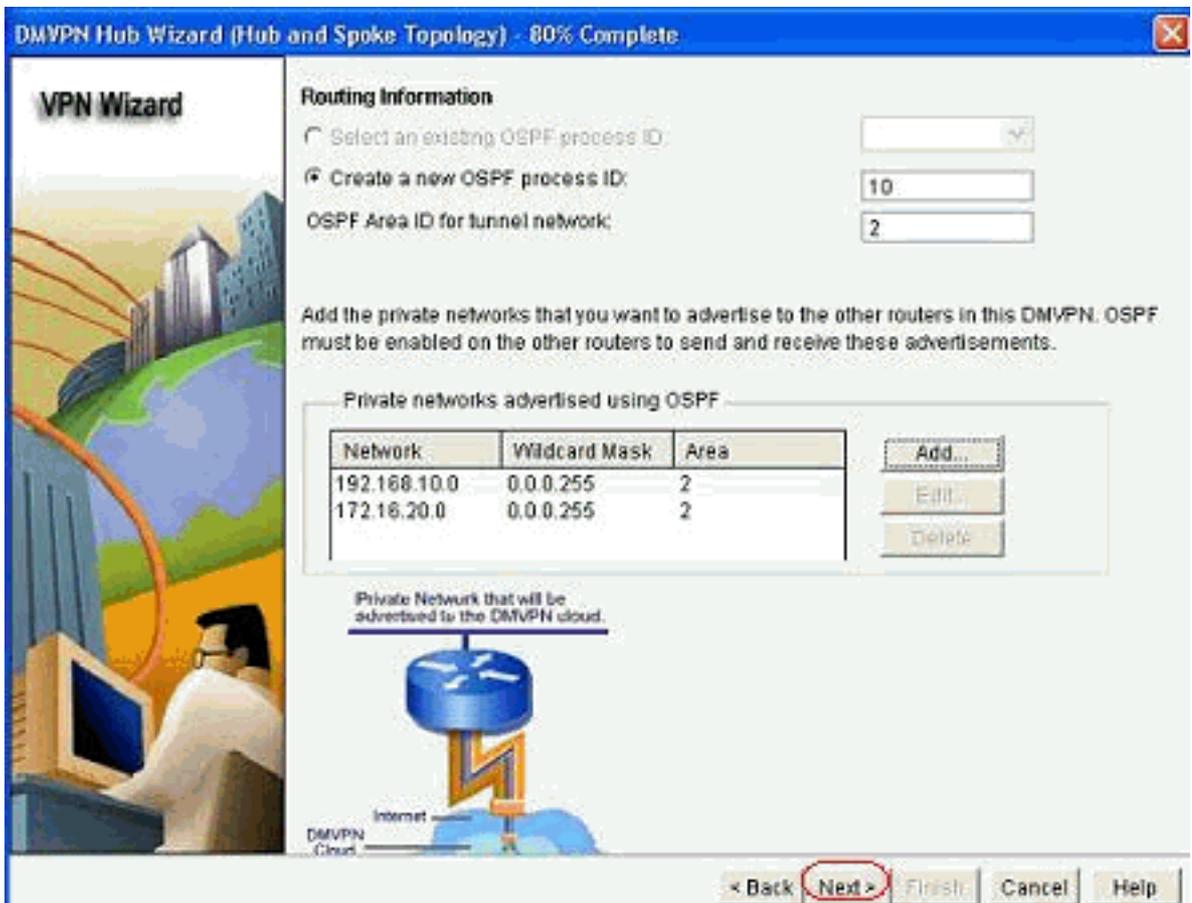


14. Especifique el ID de proceso OSPF y el ID de área. Haga clic en *Agregar* para agregar las redes que serán anunciadas por OSPF.



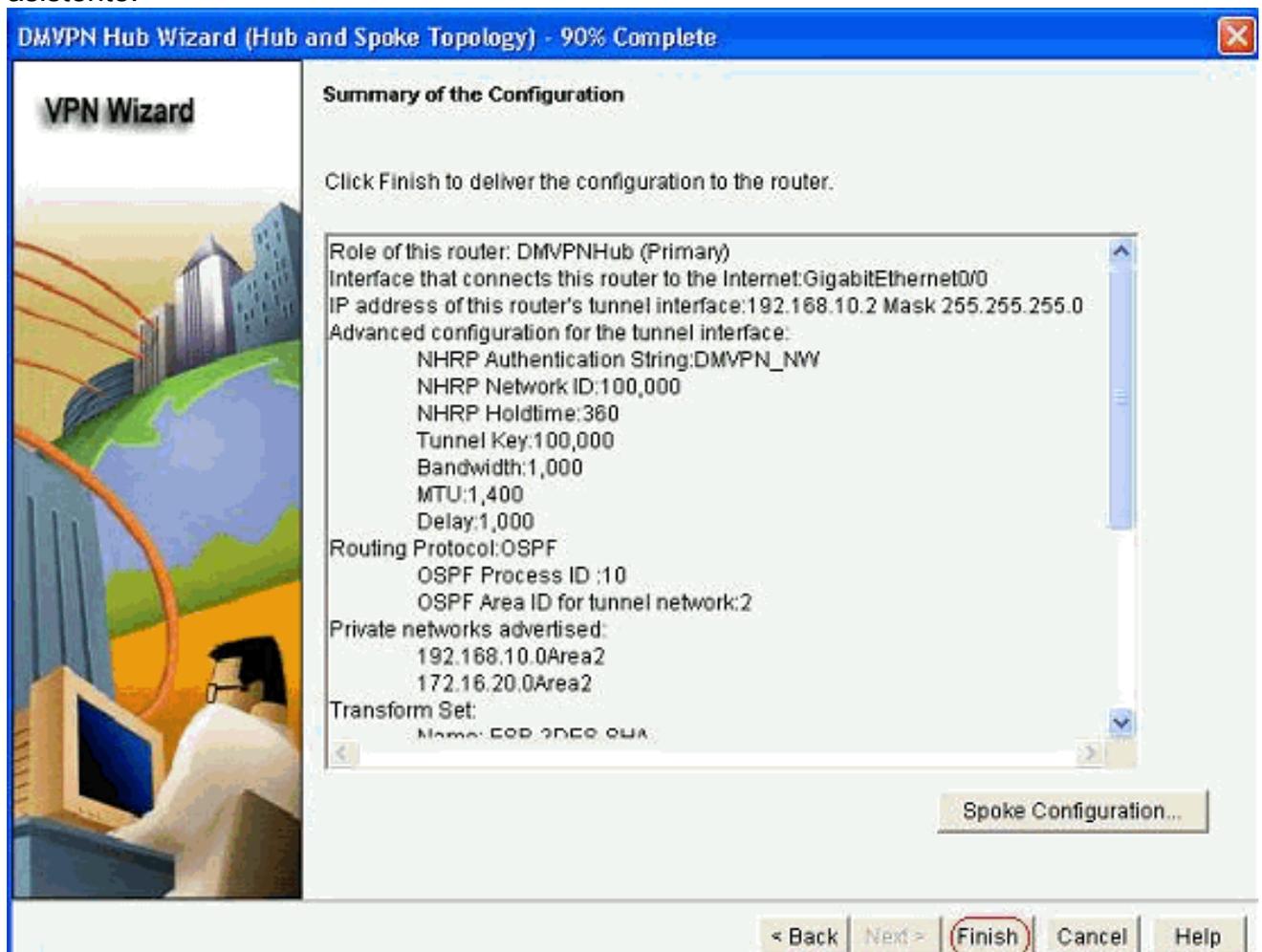
15. Agregue la red de túnel y haga clic en *Aceptar*.

16. Agregue la red privada detrás del router Hub y haga clic en



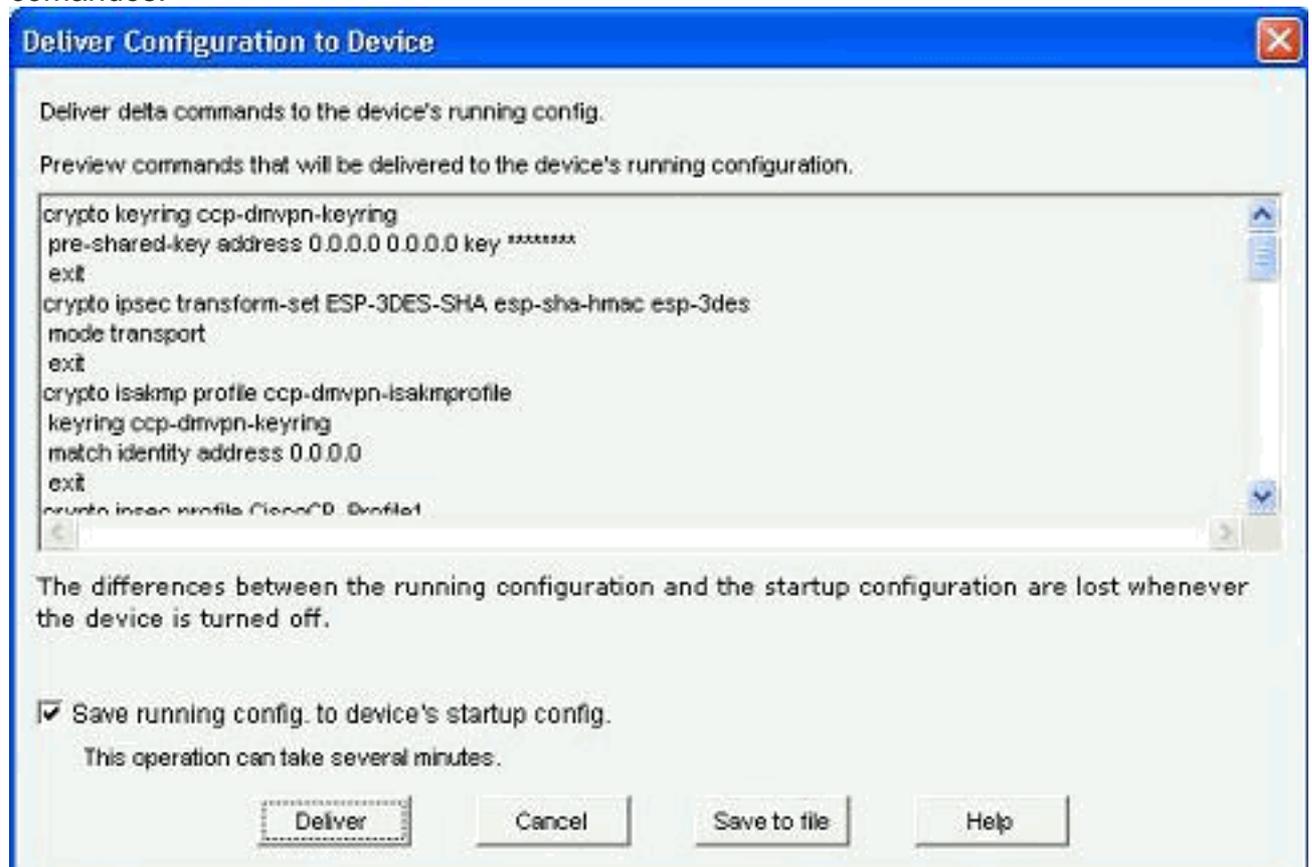
Next.

- Haga clic en *Finalizar* para completar la configuración del asistente.



- Haga clic en *Entregar* para ejecutar los

comandos.



[Configuración CLI para Hub](#)

Aquí se muestra la configuración de CLI relacionada:

```
Router del eje de conexión

!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
!
crypto isakmp policy 2
  encr aes 192
  authentication pre-share
crypto isakmp key abcd123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac
  mode transport
!
crypto ipsec profile CiscoCP_Profile1
  set transform-set ESP-3DES-SHA
!
interface Tunnel0
  bandwidth 1000
  ip address 192.168.10.2 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip nhrp authentication DMVPN_NW
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
```

```

ip nhrp holdtime 360
ip tcp adjust-mss 1360
ip ospf network point-to-multipoint
delay 1000
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile CiscoCP_Profile1
!
router ospf 10
 log-adjacency-changes
 network 172.16.20.0 0.0.0.255 area 2
 network 192.168.10.0 0.0.0.255 area 2
!

```

[Editar la configuración de DMVPN mediante CCP](#)

Puede editar manualmente los parámetros de túnel DMVPN existentes cuando seleccione la interfaz de túnel y haga clic en *Editar*.

Configure > Security > VPN > Dynamic Multipoint VPN

VPN

Create Dynamic Multipoint VPN (DMVPN) **Edit Dynamic Multipoint VPN (DMVPN)**

Add... **Edit...** Delete

Interface	IPSec Profile	IP Address	Description
Tunnel0	CiscoCP_Profile1	192.168.10.2	<None>

Details for interface Tunnel0:

Item Name	Item Value
Interface	Tunnel0
IPSec Profile	CiscoCP_Profile1
IP Address	192.168.10.2
Description	<None>
Tunnel Bandwidth	1000
MTU	1400
NHRP Authentication	DMVPN_NW
NHRP Network ID	100000
NHRP Hold Time	360
Delay{0}	1000

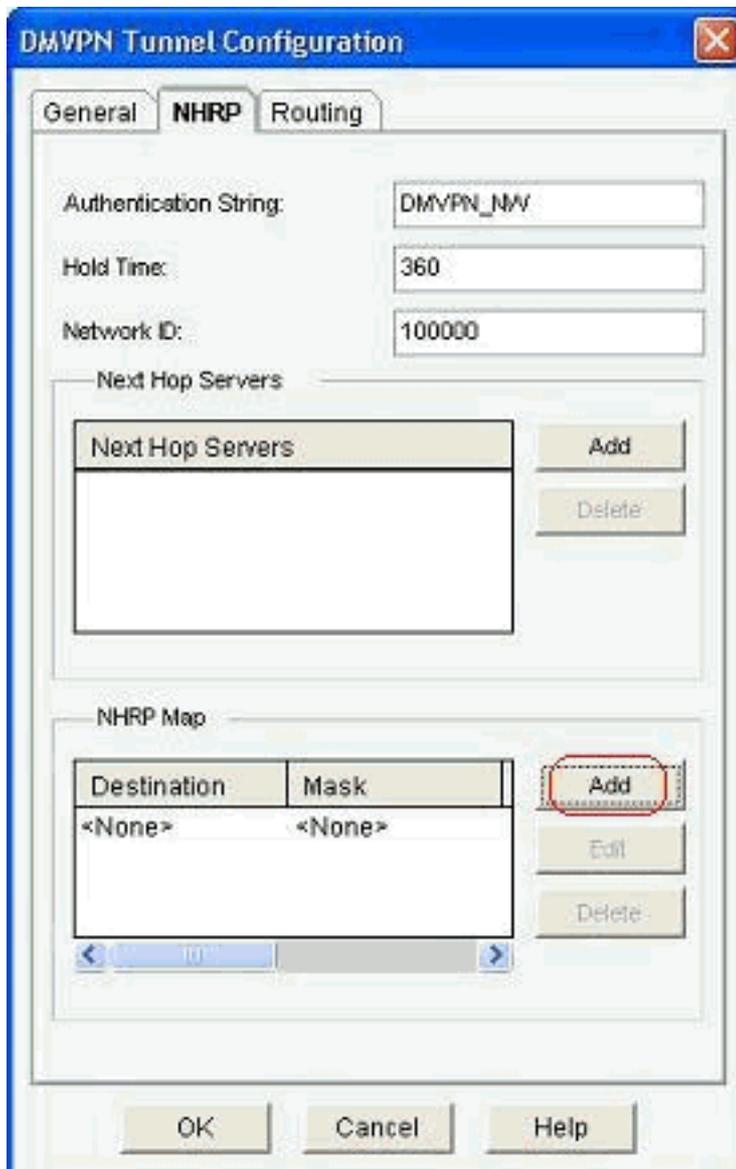
Los parámetros de la interfaz de túnel como MTU y la clave de túnel se modifican bajo la ficha *General*.

The image shows a 'DMVPN Tunnel Configuration' dialog box with three tabs: 'General', 'NHRP', and 'Routing'. The 'General' tab is active. It contains the following fields and options:

- IP address:** 192.168.10.2
- Mask:** 255.255.255.0, with a dropdown set to 24.
- Tunnel Source:**
 - Interface:** GigabitEthernet0/0
 - IP address:** (empty field)
- Tunnel Destination:**
 - This is an multipoint GRE Tunnel**
 - IP / Hostname:** (empty field)
- IPSec Profile:** CiscoCP_Profi (dropdown), with an 'Add...' button.
- MTU:** 1400
- Bandwidth:** 1000
- Delay:** 1000
- Tunnel Key:** 100000

At the bottom, there are three buttons: 'OK', 'Cancel', and 'Help'.

1. Los parámetros relacionados con NHRP se encuentran y modifican según el requisito de la pestaña *NHRP*. En el caso de un router radial, debe poder ver el NHS como la dirección IP del router hub. Haga clic en *Agregar* en la sección Mapa NHRP para agregar el mapping



NHRP.

2. Según la configuración de la red, los parámetros de asignación NHRP se pueden configurar

NHRP Map Configuration

Statically configure the IP-to-NMBA address mapping of IP destinations connected to a NBMA network.

Destination reachable through NBMA network

IP Address:

Mask (Optional):

NBMA address directly reachable

IP Address:

Configure NBMA addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network.

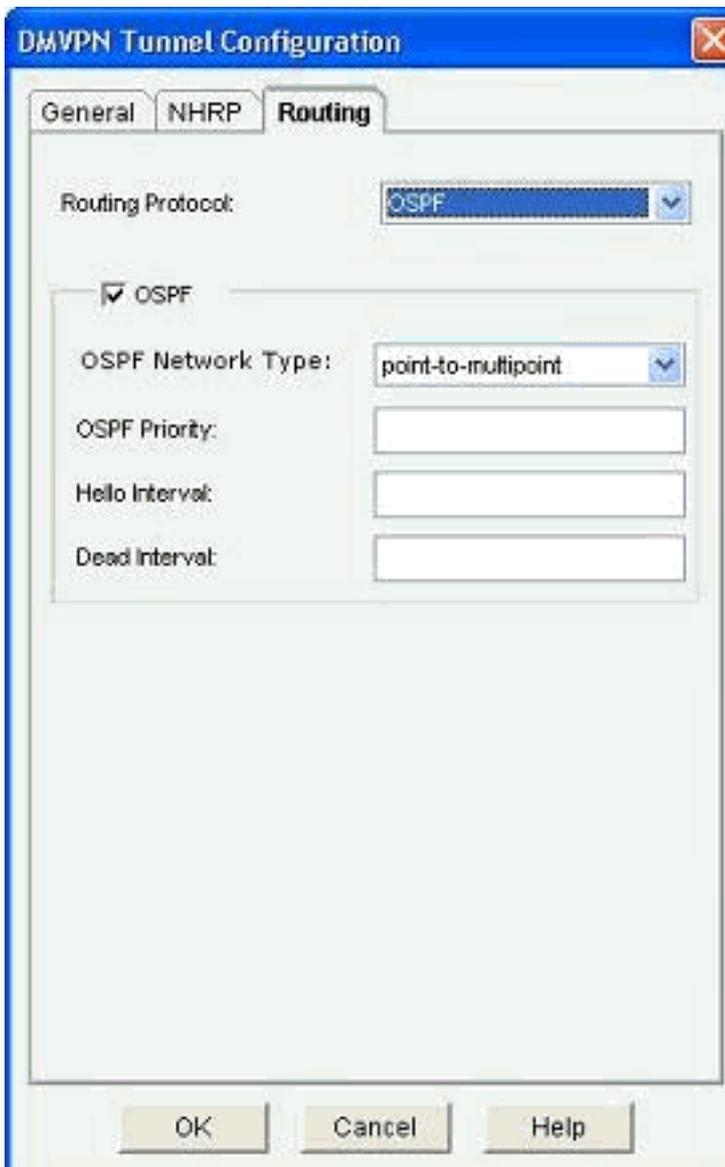
Dynamically add spokes' IP addresses to hub's multicast cache

IP address of NBMA address directly reachable

OK Cancel Help

como se muestra aquí:

Los parámetros relacionados con el ruteo se ven y modifican en la pestaña *Ruteo*.



Más información

Los túneles DMVPN se configuran de estas dos maneras:

- Comunicación de radio a radio a través del concentrador
- Comunicación de radio a radio sin el concentrador

En este documento, sólo se analiza el primer método. Para permitir el establecimiento de túneles IPsec dinámicos de radio a radio, este enfoque se utiliza para agregar el spoke a la nube DMVPN:

1. Inicie el asistente DMVPN y seleccione la opción *Configuración de Spoke*.
2. En la ventana *DMVPN Network Topology*, seleccione la opción *Red de malla completa* en lugar de la opción *Red de eje de conexión y radio*.

DMVPN Spoke Wizard - 10% Complete

VPN Wizard

DMVPN Network Topology

Select the DMVPN network topology.

Hub and Spoke network

In this topology, all DMVPN traffic is routed through the hub. A point-to-point GRE interface will be configured on the spoke, and the spoke will use it to create a tunnel to the hub which will remain up. Spokes do not create GRE tunnels to other spokes in this topology.

Fully meshed network

In this topology, the spoke dynamically establishes a direct tunnel to another spoke device, and sends DMVPN traffic directly to it. A multipoint GRE tunnel interface is configured on the spoke to support this functionality.

Note: Cisco supports fully meshed DMVPN networks only in the following Cisco IOS images: 12.3(8)T1 and 12.3(9) or later.

< Back Next > Finish Cancel Help

3. Complete el resto de la configuración con los mismos pasos que las otras configuraciones de este documento.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Información Relacionada

- [VPN multipunto dinámica de Cisco: Comunicaciones sencillas y seguras entre sucursales](#)
- [VPN multipunto dinámica \(DMVPN\) IOS 12.2](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)