Cisco IOS/CCP - Configurer DMVPN avec Cisco CP

Contenu

Introduction

Ce document fournit un exemple de configuration pour le tunnel DMVPN (Dynamic Multipoint VPN) entre les routeurs concentrateurs et en étoile à l'aide de Cisco Configuration Professional (Cisco CP). Dynamic Multipoint VPN est une technologie qui intègre différents concepts tels que GRE, le cryptage IPSec, NHRP et le routage pour fournir une solution sophistiquée qui permet aux utilisateurs finaux de communiquer efficacement via les tunnels IPSec en étoile créés dynamiquement.

Conditions préalables

Conditions requises

Pour une fonctionnalité DMVPN optimale, il est recommandé d'exécuter le logiciel Cisco IOS® version 12.4 mainline,12.4T et ultérieure.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur Cisco IOS série 3800 avec logiciel version 12.4 (22)
- Routeur Cisco IOS de la gamme 1800 avec logiciel version 12.3 (8)
- Cisco Configuration Professional version 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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Ce document fournit des informations sur la configuration d'un routeur en étoile et d'un autre routeur en concentrateur à l'aide de Cisco CP. La configuration en étoile initiale est affichée, mais plus loin dans le document, la configuration liée au concentrateur est également présentée en détail afin de fournir une meilleure compréhension. D'autres rayons peuvent également être configurés à l'aide d'une approche similaire pour se connecter au concentrateur. Le scénario actuel utilise les paramètres suivants :

- Réseau public du routeur concentrateur - 209.165.201.0
- Réseau de tunnel - 192.168.10.0
- Protocole de routage utilisé - OSPF

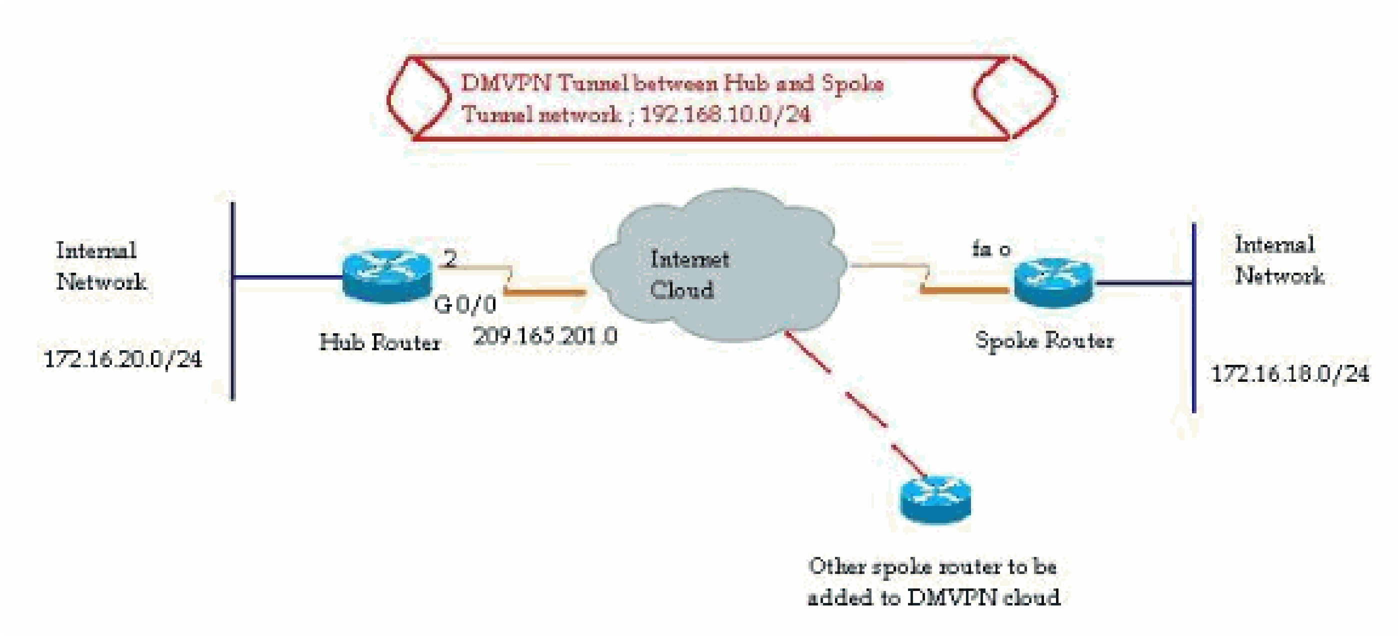
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

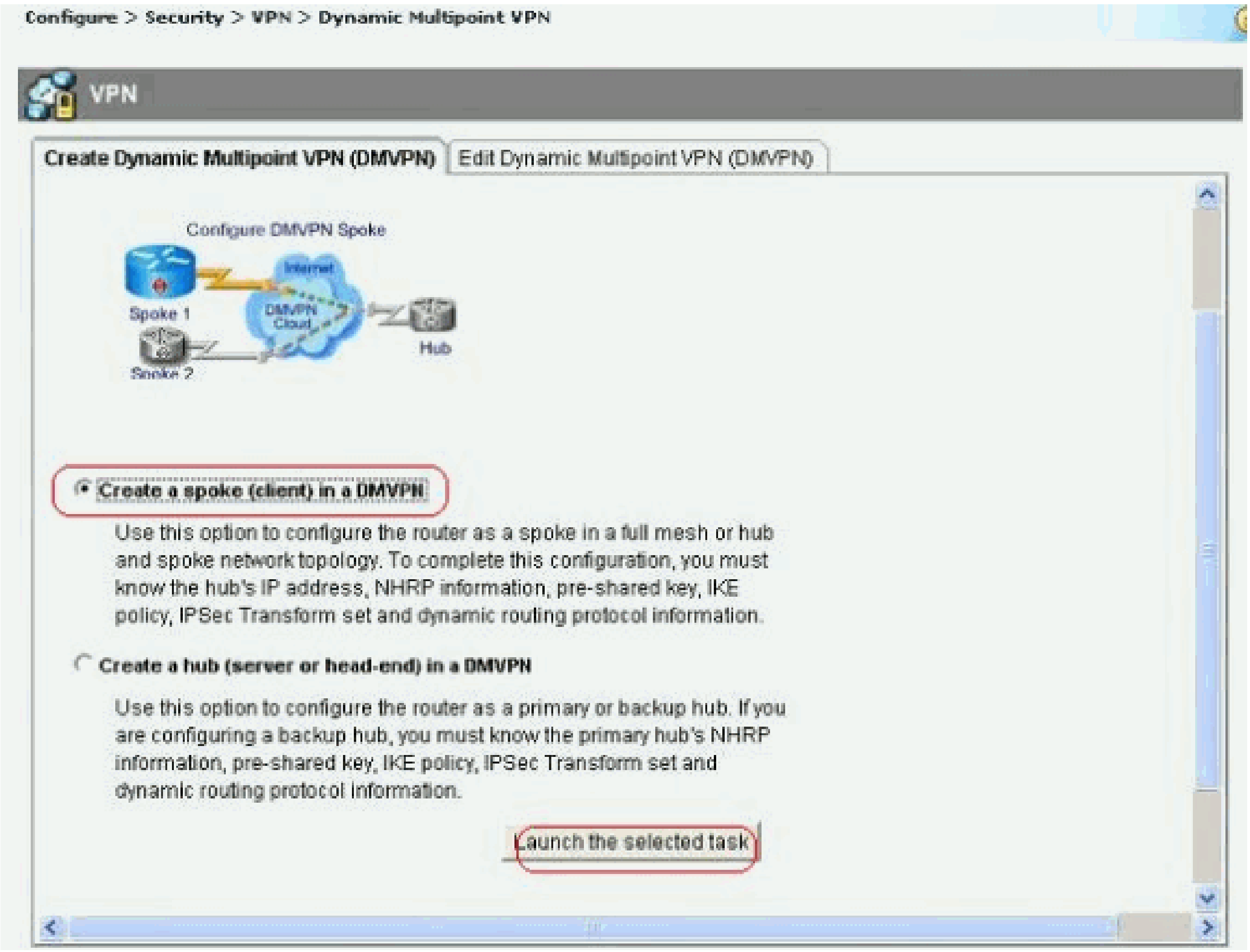
Ce document utilise la configuration réseau suivante :



Configuration satellite à l'aide de Cisco CP

Cette section explique comment configurer un routeur en étoile à l'aide de l'assistant DMVPN étape par étape dans Cisco Configuration Professional.

1. Afin de démarrer l'application Cisco CP et de lancer l'assistant DMVPN, accédez à *Configure > Security > VPN > Dynamic Multipoint VPN*. Ensuite, sélectionnez l'option *Créer un rayon dans un DMVPN* et cliquez sur *Lancer la tâche sélectionnée*.


Configure > Security > VPN > Dynamic Multipoint VPN
VPN
Create Dynamic Multipoint VPN (DMVPN)
Edit Dynamic Multipoint VPN (DMVPN)
Configure DMVPN Spoke
Spoke 1
Internet
DMVPN Cloud
Hub
Spoke 2
Launch the selected task

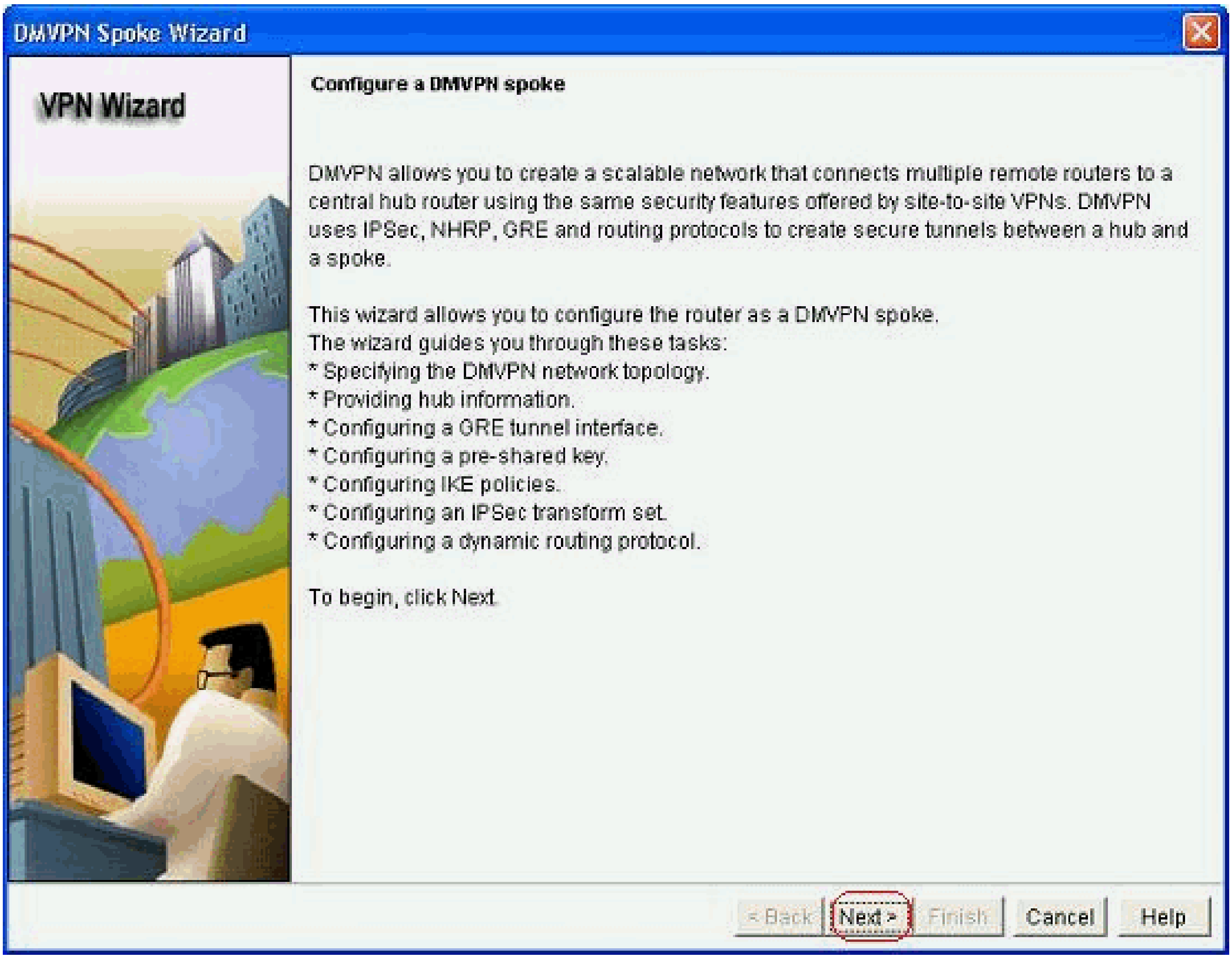
● Create a spoke (client) in a DMVPN

Use this option to configure the router as a spoke in a full mesh or hub and spoke network topology. To complete this configuration, you must know the hub's IP address, NHRP information, pre-shared key, IKE policy, IPSec Transform set and dynamic routing protocol information.

○ Create a hub (server or head-end) in a DMVPN

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.

2. Cliquez sur *Suivant* pour commencer.



DMVPN Spoke Wizard

VPN Wizard

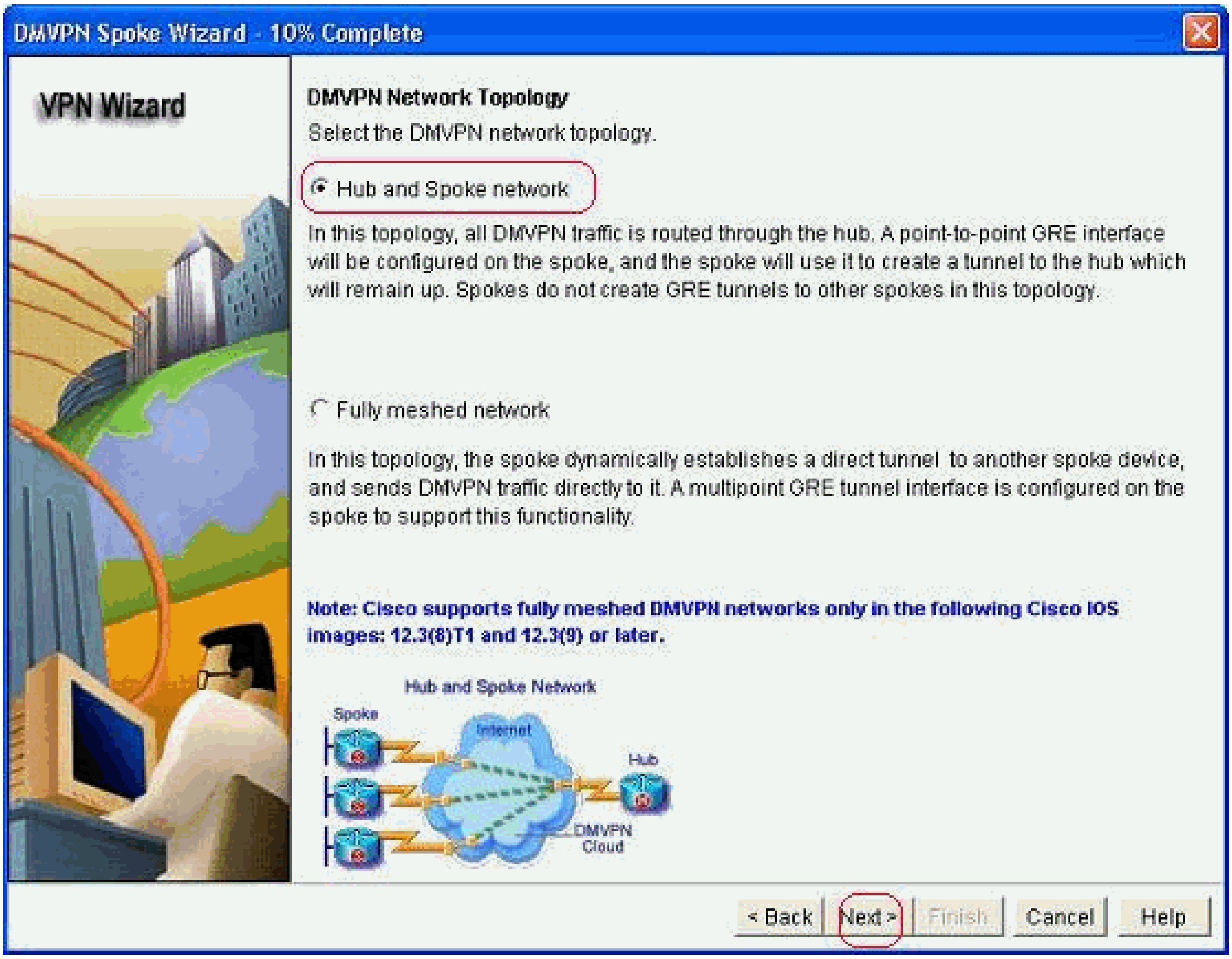
Configure a DMVPN spoke

DMVPN allows you to create a scalable network that connects multiple remote routers to a central hub router using the same security features offered by site-to-site VPNs. DMVPN uses IPSec, NHRP, GRE and routing protocols to create secure tunnels between a hub and a spoke.

This wizard allows you to configure the router as a DMVPN spoke.
The wizard guides you through these tasks:
* Specifying the DMVPN network topology.
* Providing hub information.
* Configuring a GRE tunnel interface.
* Configuring a pre-shared key.
* Configuring IKE policies.
* Configuring an IPSec transform set.
* Configuring a dynamic routing protocol.

To begin, click Next.

3. Sélectionnez l'option *Réseau Hub and Spoke* et cliquez sur *Suivant*.



DMVPN Network Topology

Select the DMVPN network topology.

● Hub and Spoke network

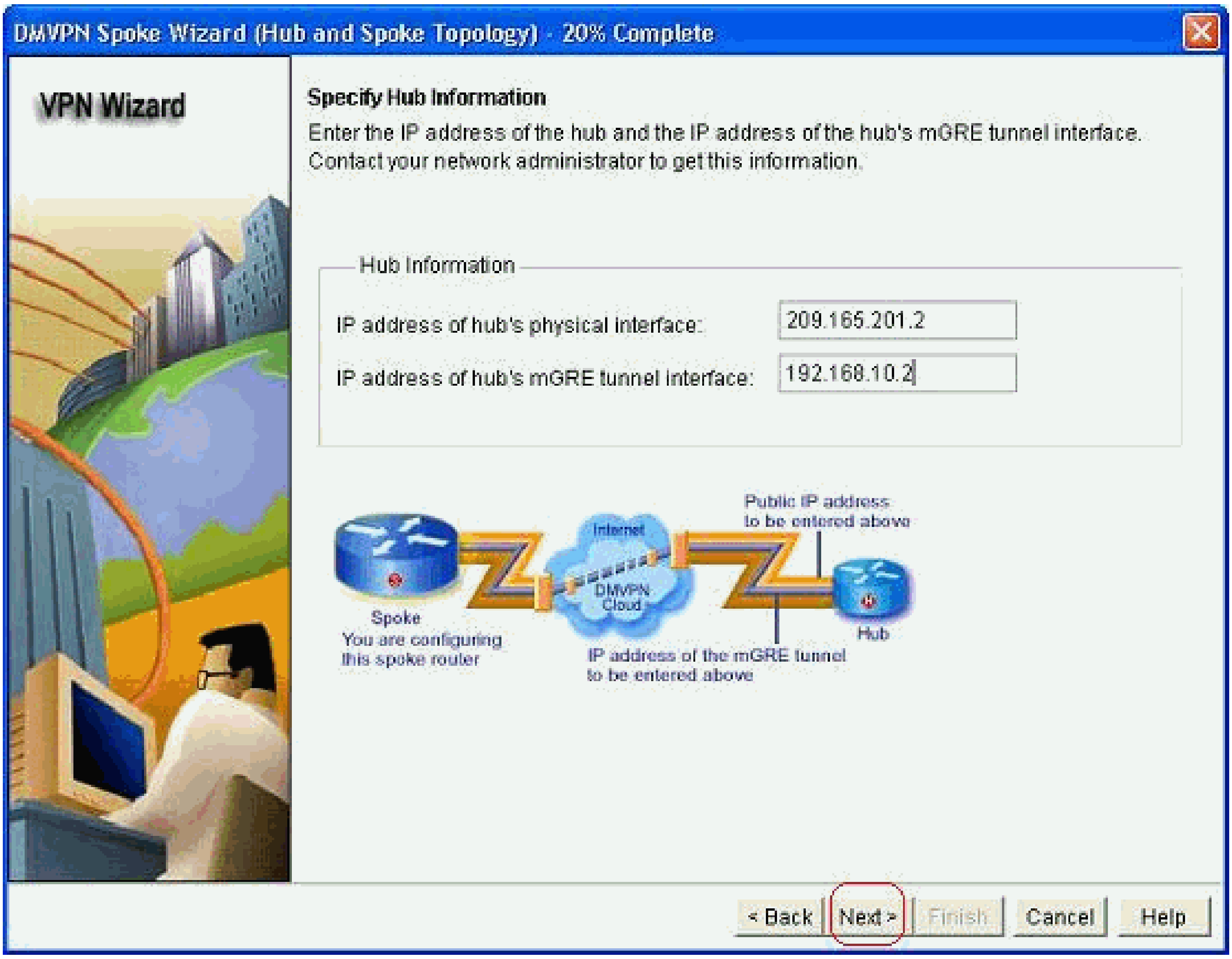
In this topology, all DMVPN traffic is routed through the hub. A point-to-point GRE interface will be configured on the spoke, and the spoke will use it to create a tunnel to the hub which will remain up. Spokes do not create GRE tunnels to other spokes in this topology.

○ 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.

4. Spécifiez les informations associées au concentrateur, telles que l'interface publique du routeur concentrateur et l'interface de tunnel du routeur concentrateur.


DMVPN Spoke Wizard (Hub and Spoke Topology) - 20% Complete
VPN Wizard
Internet
DMVPN Cloud
Public IP address to be entered above
Spoke
You are configuring this spoke router
Hub
IP address of the mGRE tunnel to be entered above
< Back
Next >
Finish
Cancel
Help

Specify Hub Information

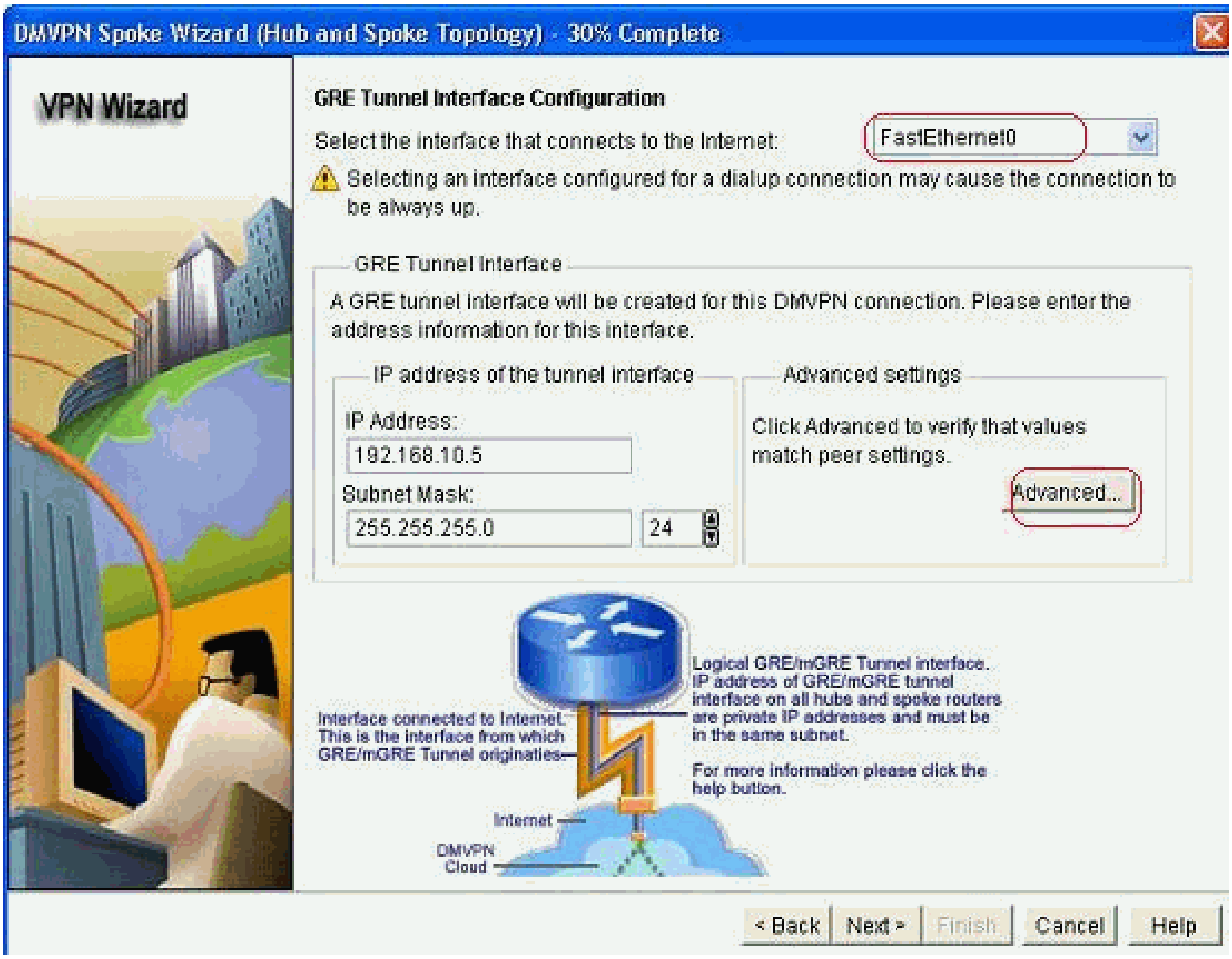
Enter the IP address of the hub and the IP address of the hub's mGRE tunnel interface. Contact your network administrator to get this information.

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

5. Spécifiez les détails de l'interface de tunnel du rayon et de l'interface publique du rayon. Ensuite, cliquez sur *Avancé*.



DMVPN Spoke Wizard (Hub and Spoke Topology) - 30% Complete

GRE Tunnel Interface Configuration

Select the interface that connects to the Internet: FastEthernet0

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

GRE 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: 192.168.10.5

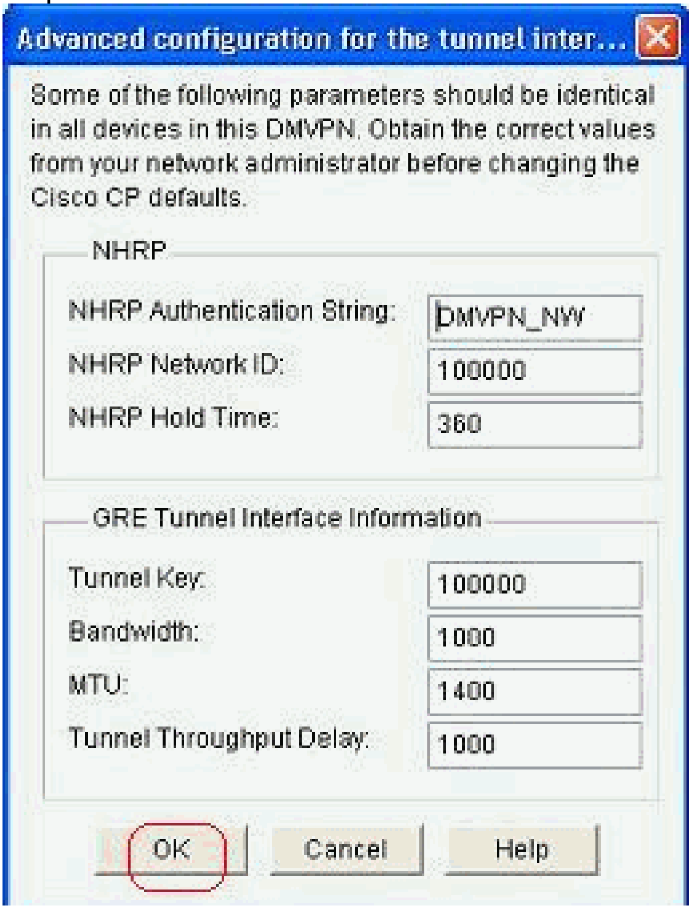
Subnet Mask: 255.255.255.0 24

Advanced settings

Click Advanced to verify that values match peer settings.

Advanced...
Interface connected to Internet. This is the interface from which GRE/mGRE Tunnel originaties
Logical GRE/mGRE Tunnel interface. IP address of GRE/mGRE tunnel interface on all hubs and spoke routers are private IP addresses and must be in the same subnet.
For more information please click the help button.
Internet
DMVPN Cloud
< Back
Next >
Finish
Cancel
Help

6. Vérifiez les paramètres de tunnel et de NHRP, et assurez-vous qu'ils correspondent parfaitement aux paramètres du concentrateur.



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: DMVPN_NW

NHRP Network ID: 100000

NHRP Hold Time: 360

GRE Tunnel Interface Information

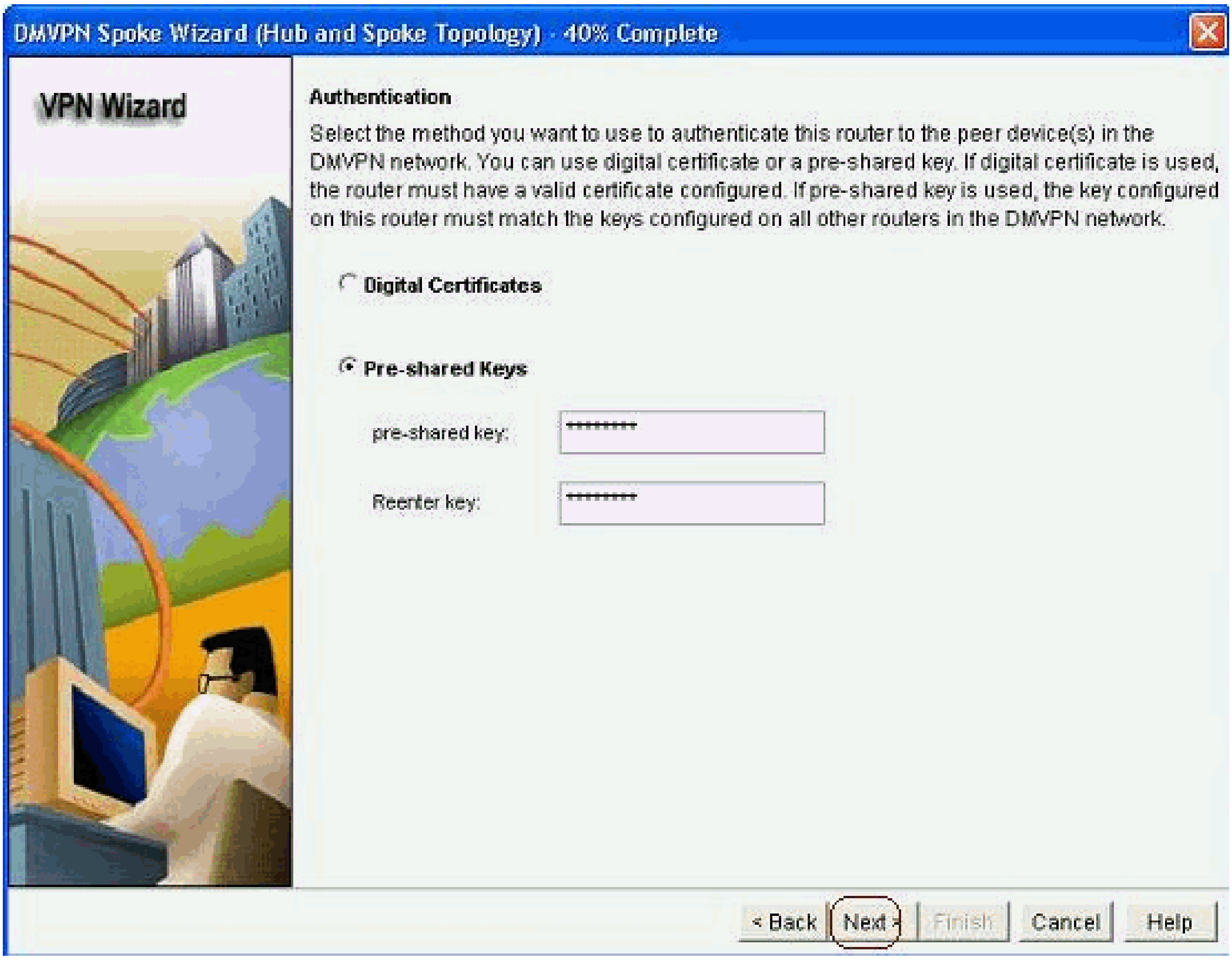
Tunnel Key: 100000

Bandwidth: 1000

MTU: 1400

Tunnel Throughput Delay: 1000

7. Spécifiez la clé pré-partagée et cliquez sur *Suivant*.



DMVPN Spoke Wizard (Hub and Spoke Topology) - 40% Complete

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.

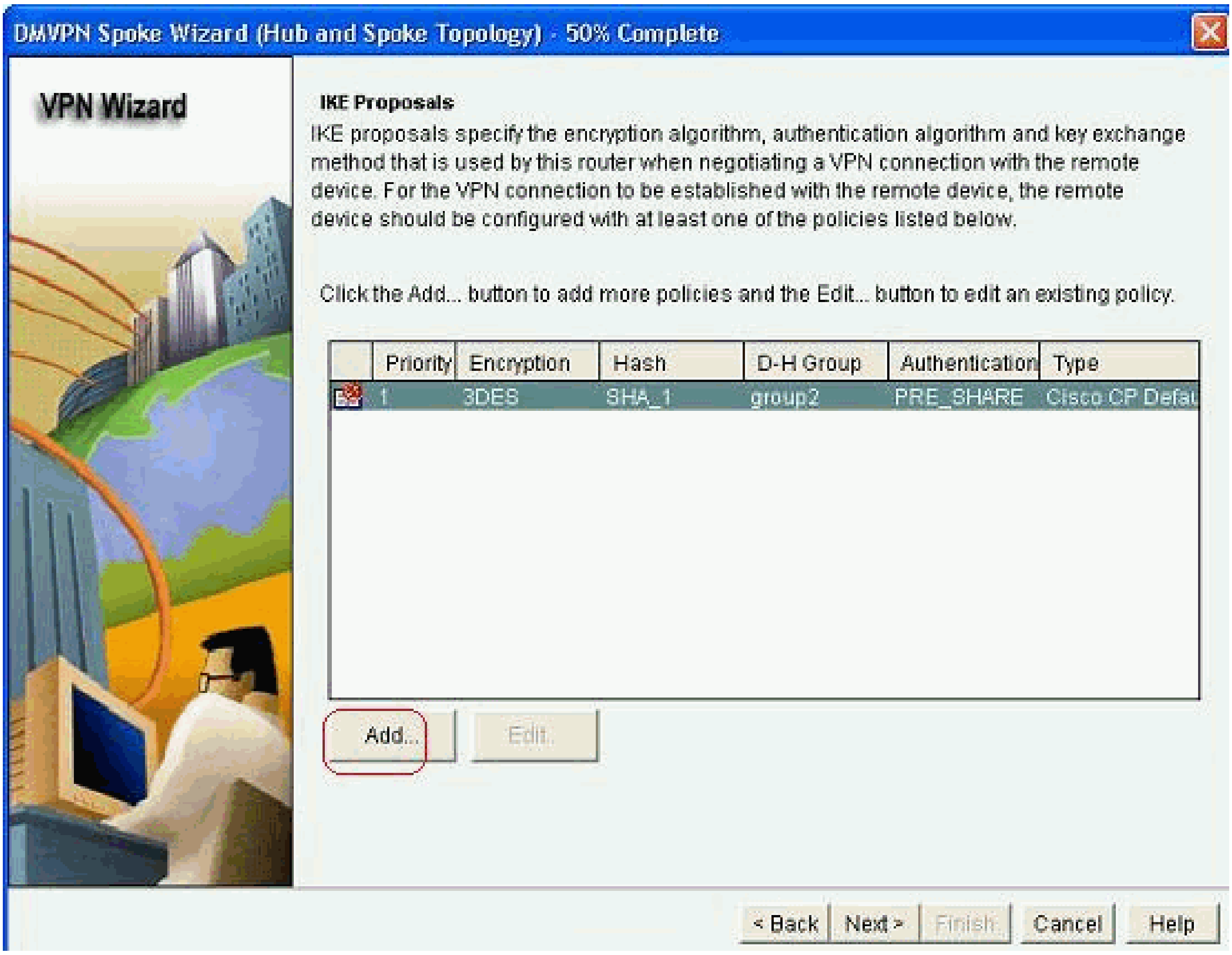
○ Digital Certificates

● Pre-shared Keys

pre-shared key: *********

Reenter key: *********

8. Cliquez sur *Add* afin d'ajouter une proposition IKE distincte.



DMVPN Spoke Wizard (Hub and Spoke Topology) - 50% Complete

VPN Wizard

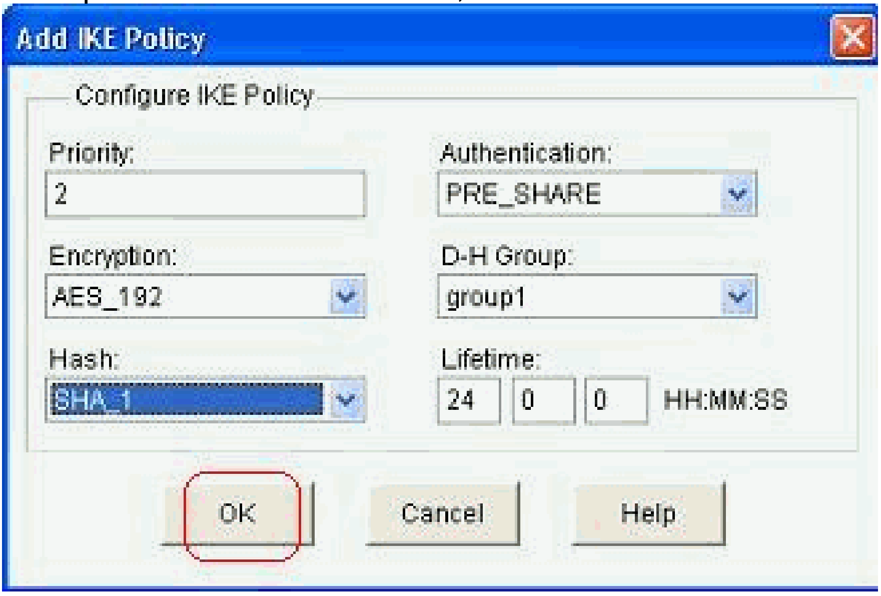
IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

	Priority	Encryption	Hash	D-H Group	Authentication	Type
	1	3DES	SHA_1	group2	PRE_SHARE	Cisco CP Defau

9. Spécifiez les paramètres de chiffrement, d'authentification et de hachage. Cliquez ensuite sur *OK*.



Add IKE Policy

Configure IKE Policy

Priority: 2

Authentication: PRE_SHARE

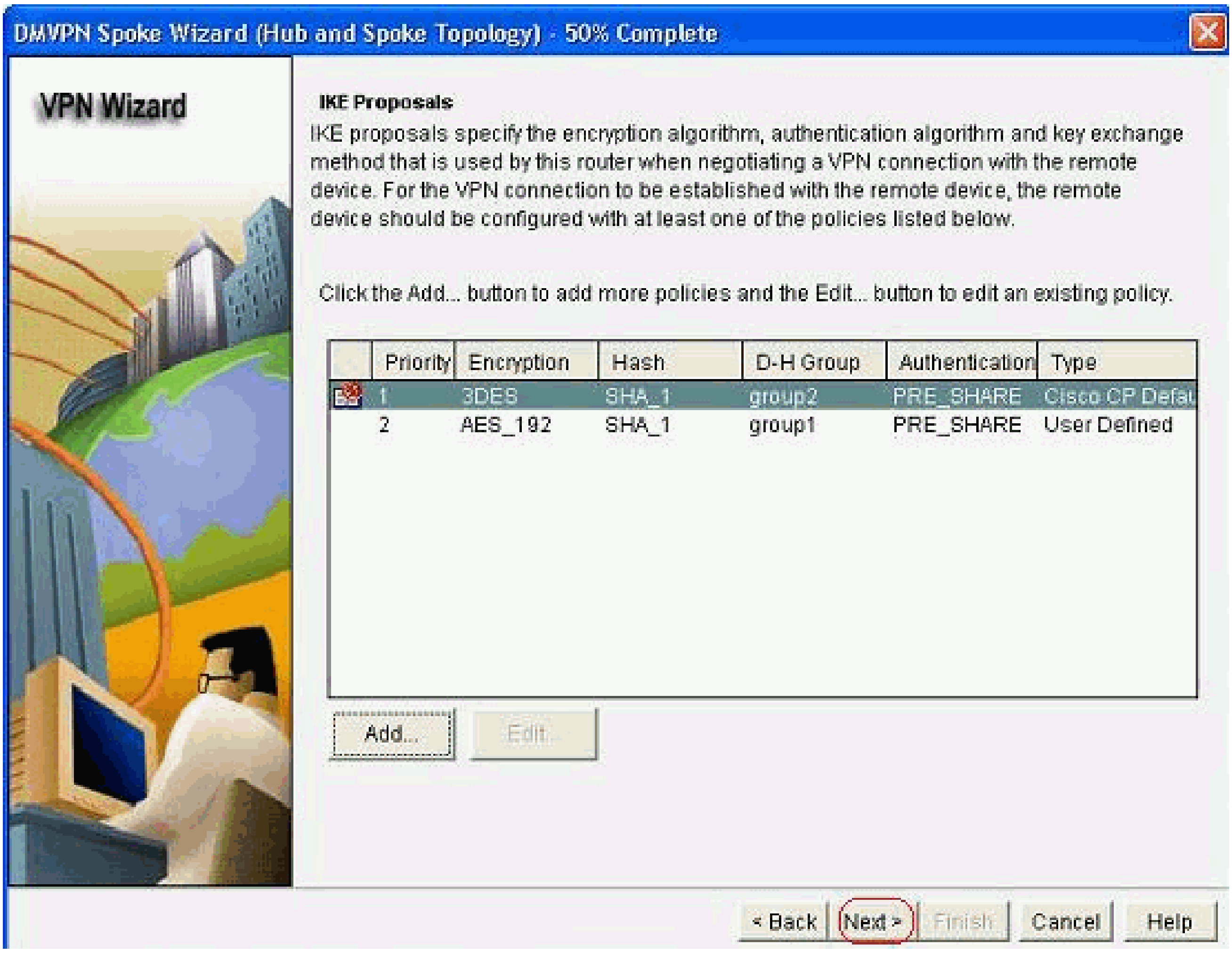
Encryption: AES_192

D-H Group: group1

Hash: SHA_1

Lifetime: 24 0 0 HH:MM:SS

10. La nouvelle stratégie IKE est visible ici. Cliquez sur *Next* (Suivant).



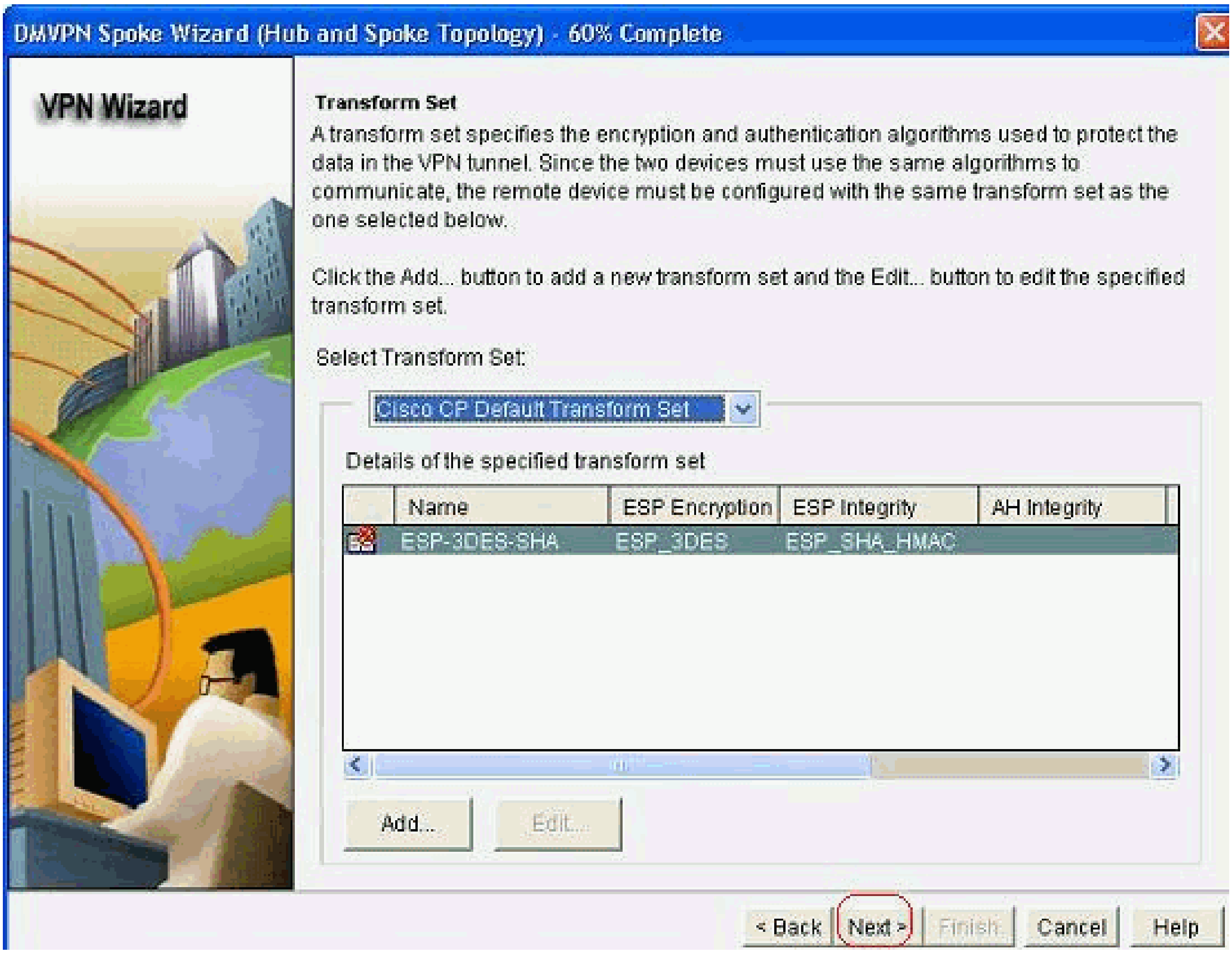
IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

	Priority	Encryption	Hash	D-H Group	Authentication	Type
	1	3DES	SHA_1	group2	PRE_SHARE	Cisco CP Defau
	2	AES_192	SHA_1	group1	PRE_SHARE	User Defined

11. Cliquez sur *Suivant* pour continuer avec le jeu de transformation par défaut.



Transform Set

A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must use the same algorithms to communicate, the remote device must be configured with the same transform set as the one selected below.

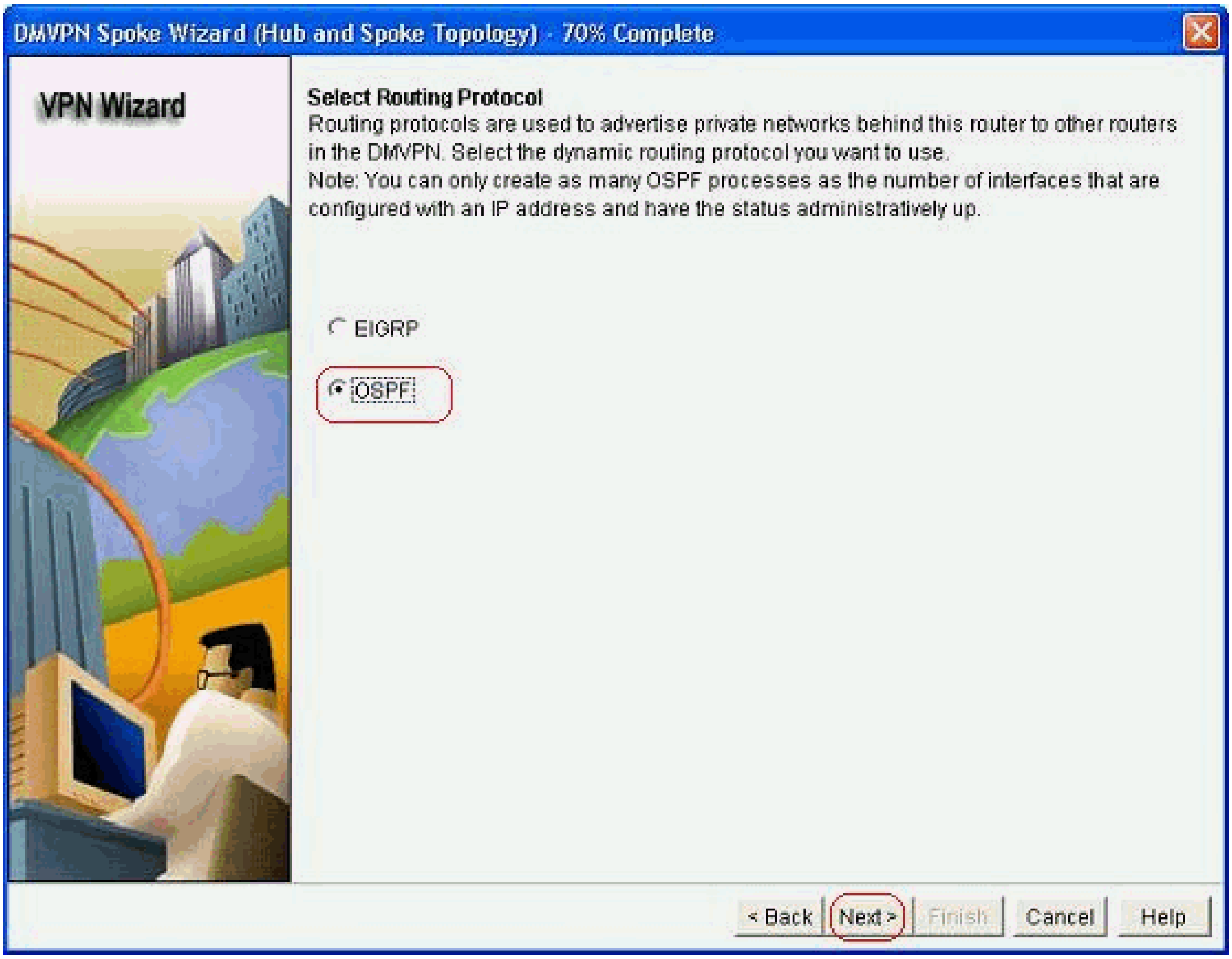
Click the Add... button to add a new transform set and the Edit... button to edit the specified transform set.

Select Transform Set: Cisco CP Default Transform Set

Details of the specified transform set

Name	ESP Encryption	ESP Integrity	AH Integrity
ESP-3DES-SHA	ESP_3DES	ESP_SHA_HMAC	

12. Sélectionnez le protocole de routage requis. Ici, *OSPF* est sélectionné.



DMVPN Spoke Wizard (Hub and Spoke Topology) - 70% Complete

VPN Wizard

Select Routing Protocol

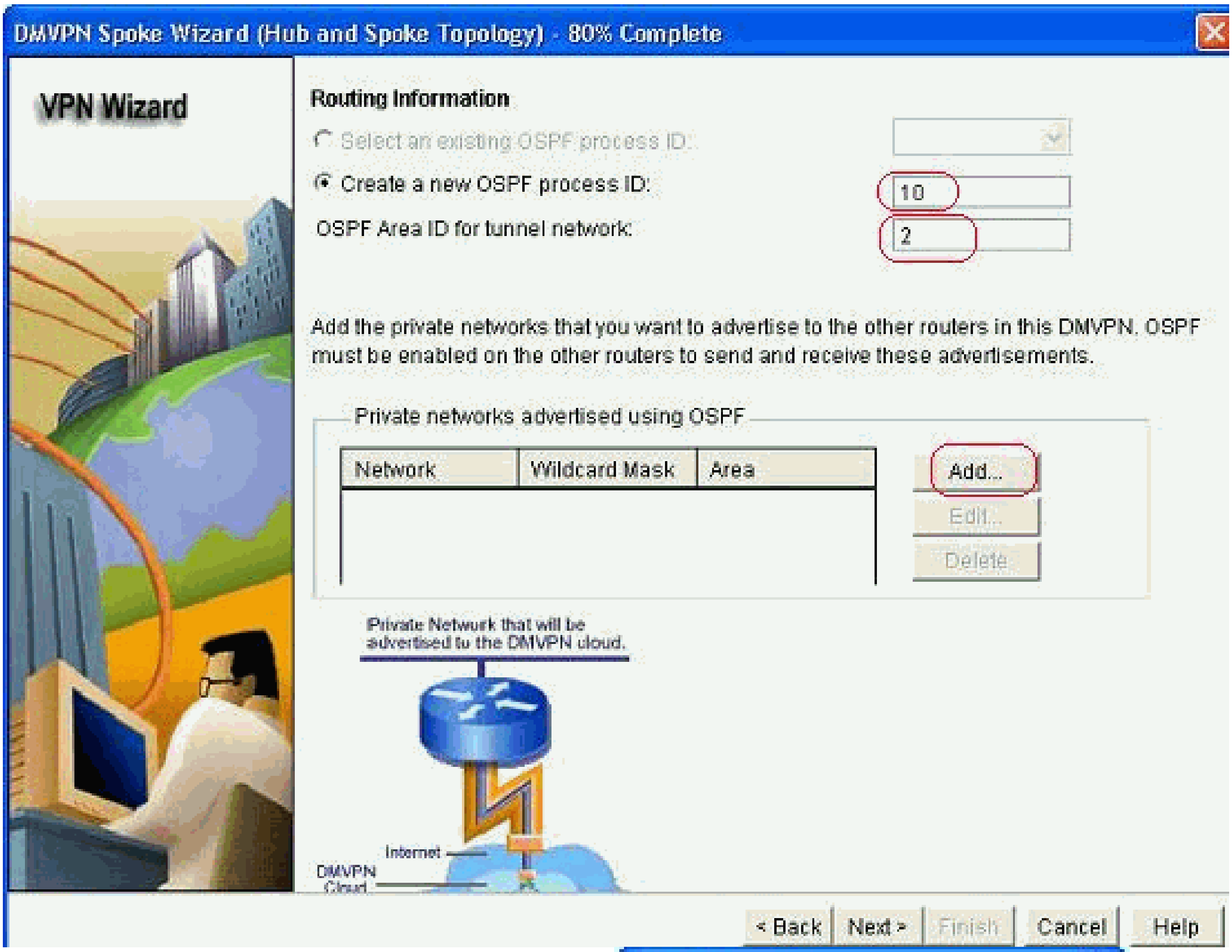
Routing protocols are used to advertise private networks behind this router to other routers in the DMVPN. Select the dynamic routing protocol you want to use.

Note: You can only create as many OSPF processes as the number of interfaces that are configured with an IP address and have the status administratively up.

○ EIGRP

● OSPF

13. Spécifiez l'ID de processus OSPF et l'ID de zone. Cliquez sur *Add* afin d'ajouter les réseaux à annoncer par
    OSPF.



DMVPN Spoke Wizard (Hub and Spoke Topology) - 80% Complete

Routing Information

○ Select an existing OSPF process ID:

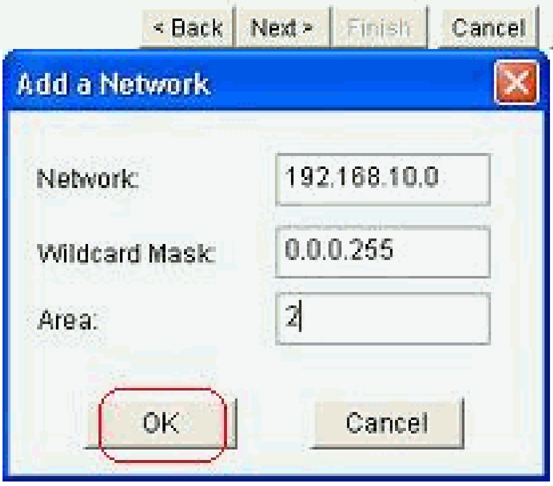
● Create a new OSPF process ID: 10

OSPF Area ID for tunnel network: 2

Add the private networks that you want to advertise to the other routers in this DMVPN. OSPF must be enabled on the other routers to send and receive these advertisements.

Private networks advertised using OSPF

Network	Wildcard Mask	Area



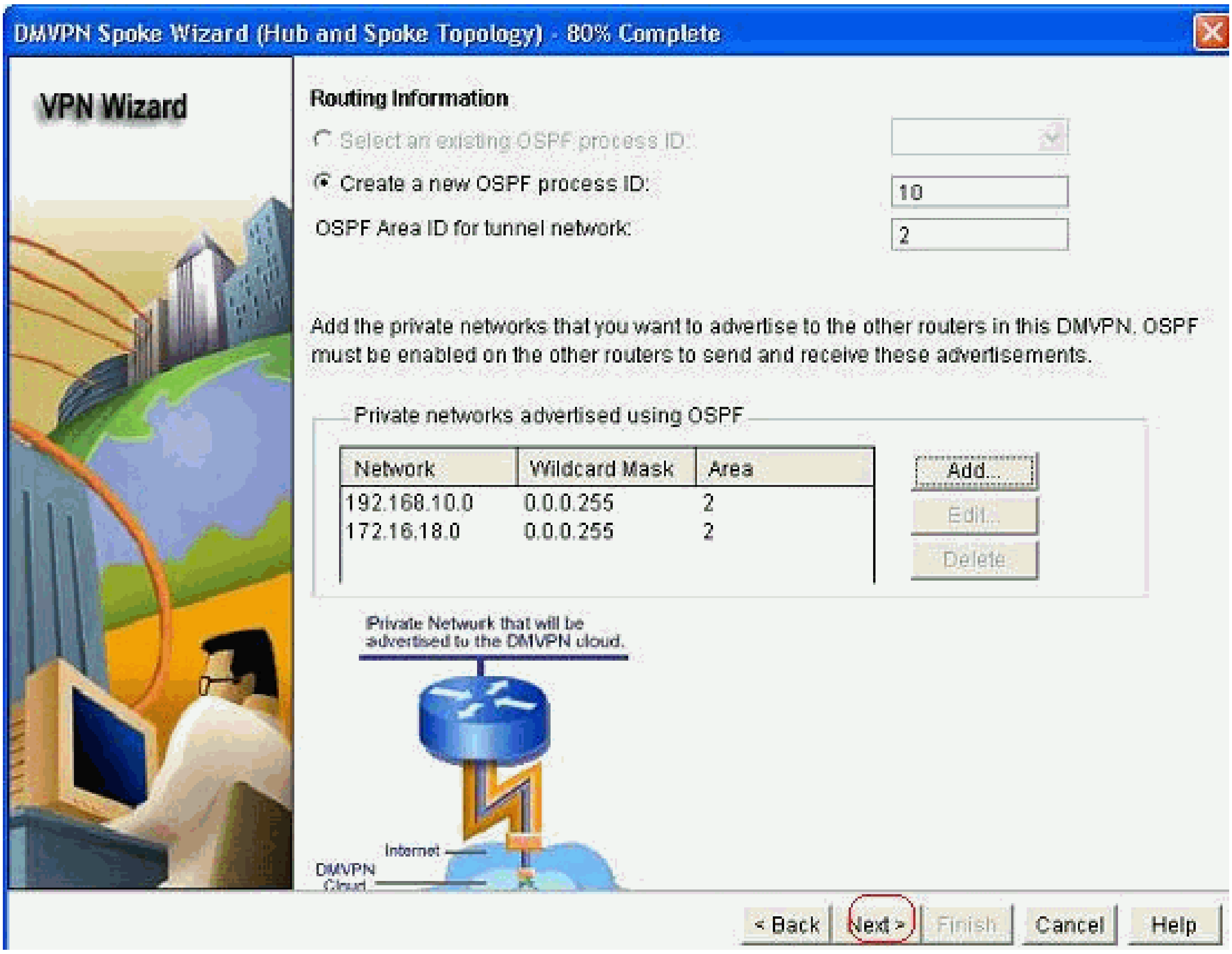
Add a Network

Network: 192.168.10.0

Wildcard Mask: 0.0.0.255

Area: 2

14. Ajoutez le réseau du tunnel et cliquez sur *OK*.
15. Ajoutez le réseau privé derrière le routeur en étoile. Cliquez ensuite sur *Next*.



DMVPN Spoke Wizard (Hub and Spoke Topology) - 80% Complete

VPN Wizard

Routing Information

○ Select an existing OSPF process ID:

● Create a new OSPF process ID: 10

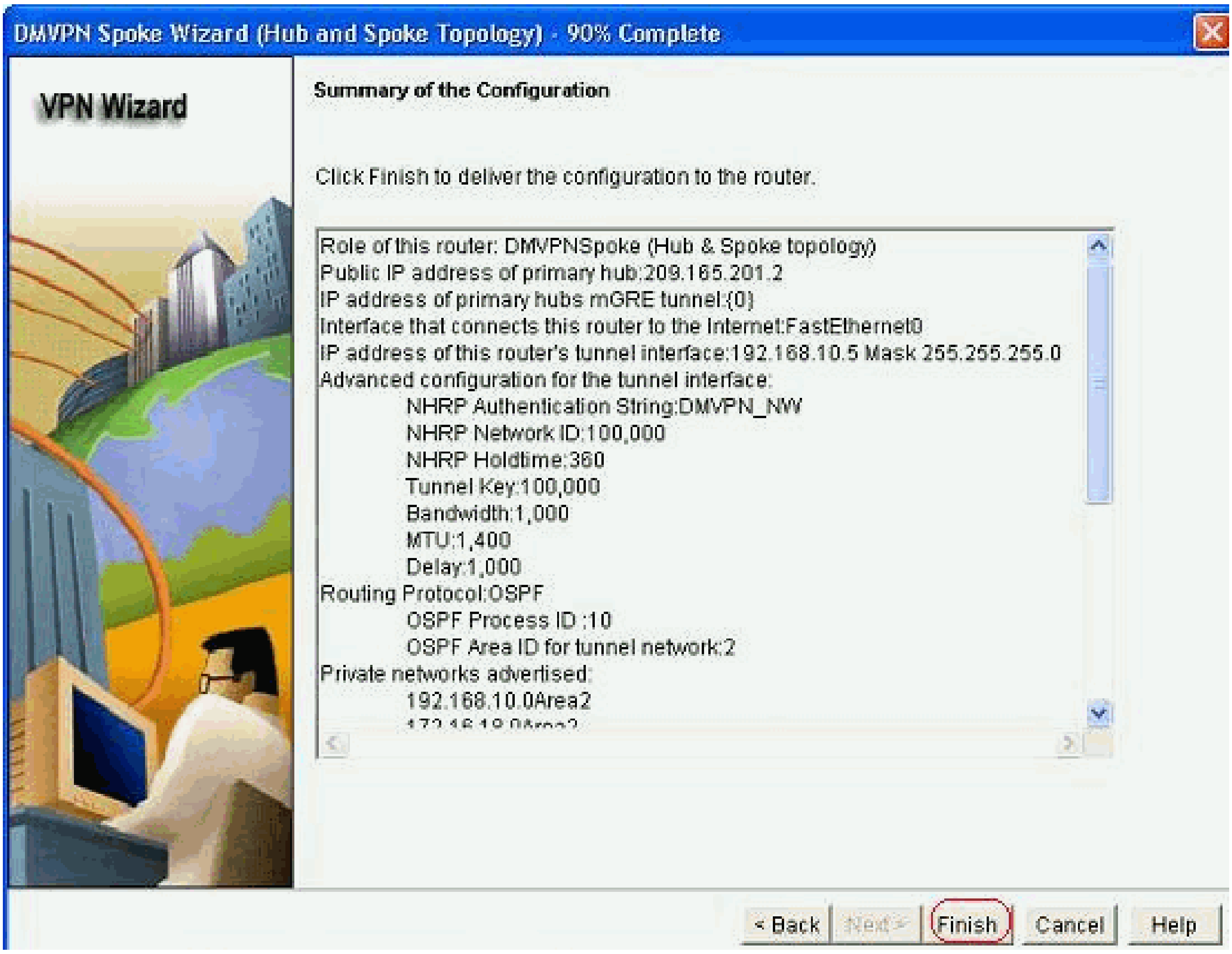
OSPF Area ID for tunnel network: 2

Add the private networks that you want to advertise to the other routers in this DMVPN. OSPF must be enabled on the other routers to send and receive these advertisements.

Private networks advertised using OSPF

Network	Wildcard Mask	Area
192.168.10.0	0.0.0.255	2
172.16.18.0	0.0.0.255	2

16. Cliquez sur *Terminer* pour terminer la configuration de l'assistant.

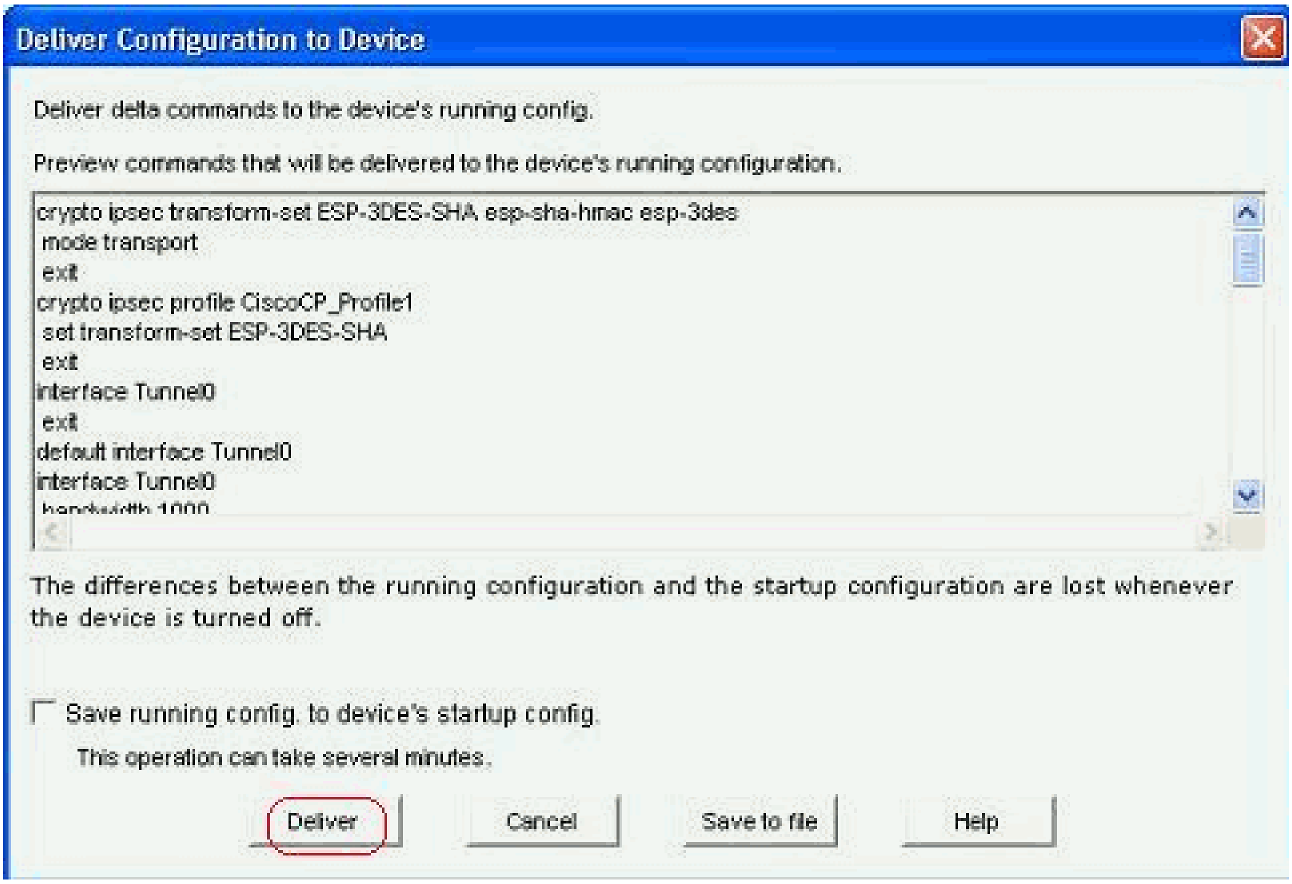


Summary of the Configuration

Click Finish to deliver the configuration to the router.

```
Role of this router: DMVPNSpoke (Hub & Spoke topology)
Public IP address of primary hub:209.165.201.2
IP address of primary hubs mGRE tunnel:{0}
Interface that connects this router to the Internet:FastEthernet0
IP address of this router's tunnel interface:192.168.10.5 Mask 255.255.255.0
Advanced configuration for the tunnel interface:
          NHRP Authentication String:DMVPN_NW
          NHRP Network ID:100,000
          NHRP Holdtime:360
          Tunnel Key:100,000
          Bandwidth:1,000
          MTU:1,400
          Delay:1,000
Routing Protocol:OSPF
          OSPF Process ID :10
          OSPF Area ID for tunnel network:2
Private networks advertised:
          192.168.10.0Area2
          172.16.18.0Area2
```

17. Cliquez sur *Deliver* pour exécuter les commandes. Cochez la case *Enregistrer la configuration en cours dans la configuration de démarrage du périphérique* si vous voulez enregistrer la configuration.



Deliver delta commands to the device's running config.

Preview commands that will be delivered to the device's running configuration.

```
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
```

The differences between the running configuration and the startup configuration are lost whenever the device is turned off.

□ Save running config. to device's startup config.

This operation can take several minutes.

Configuration CLI pour Spoke

La configuration CLI associée est présentée ici :

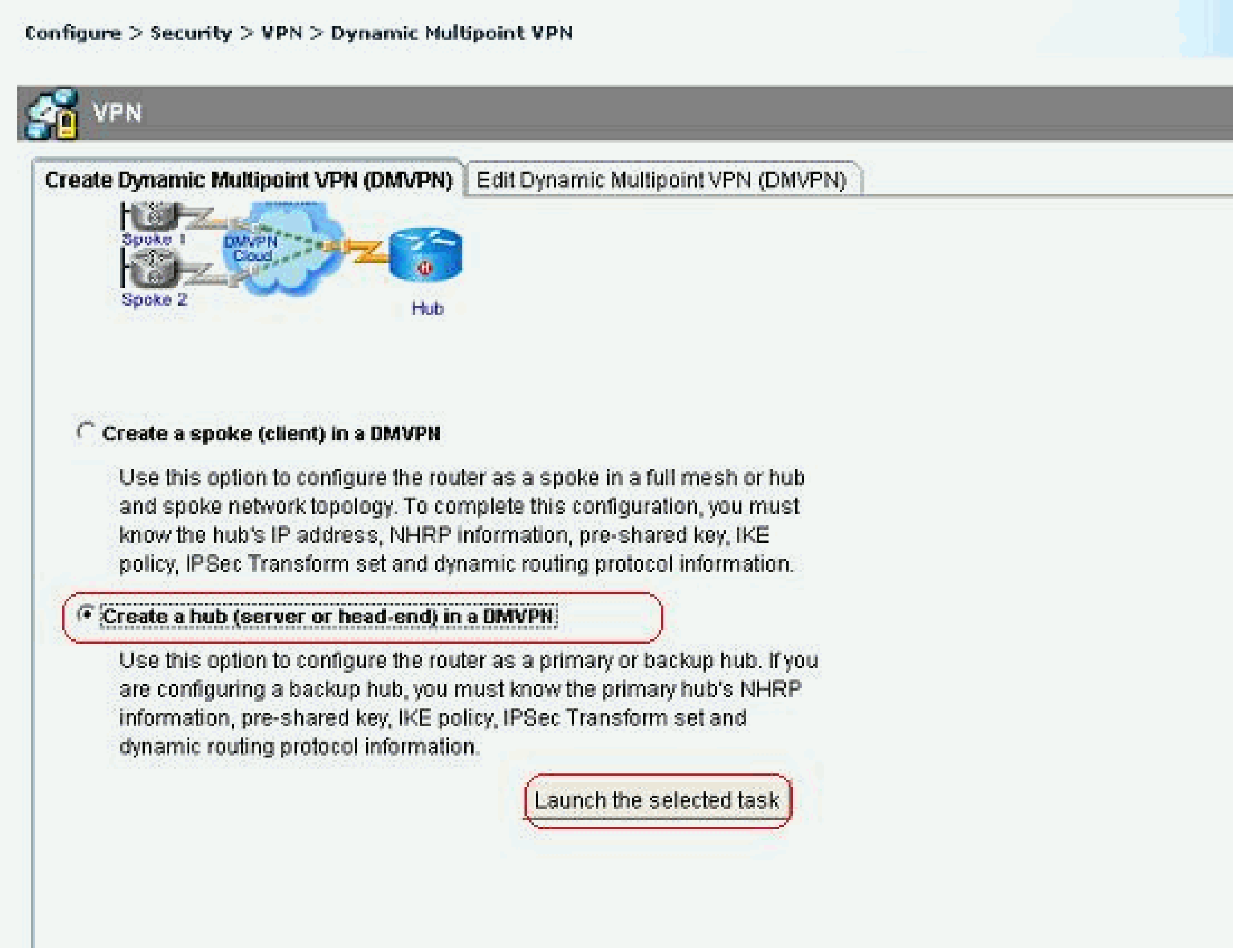
Routeur satellite

```
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
 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
```

Configuration du concentrateur à l'aide de Cisco CP

Cette section présente une approche pas à pas de la configuration du routeur concentrateur pour le DMVPN.

1. Accédez à *Configure > Security > VPN > Dynamic Multipoint VPN* et sélectionnez l'option *Create a hub in a DMVPN*. Cliquez sur *Lancer la tâche sélectionnée*.



Configure > Security > VPN > Dynamic Multipoint VPN

VPN

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

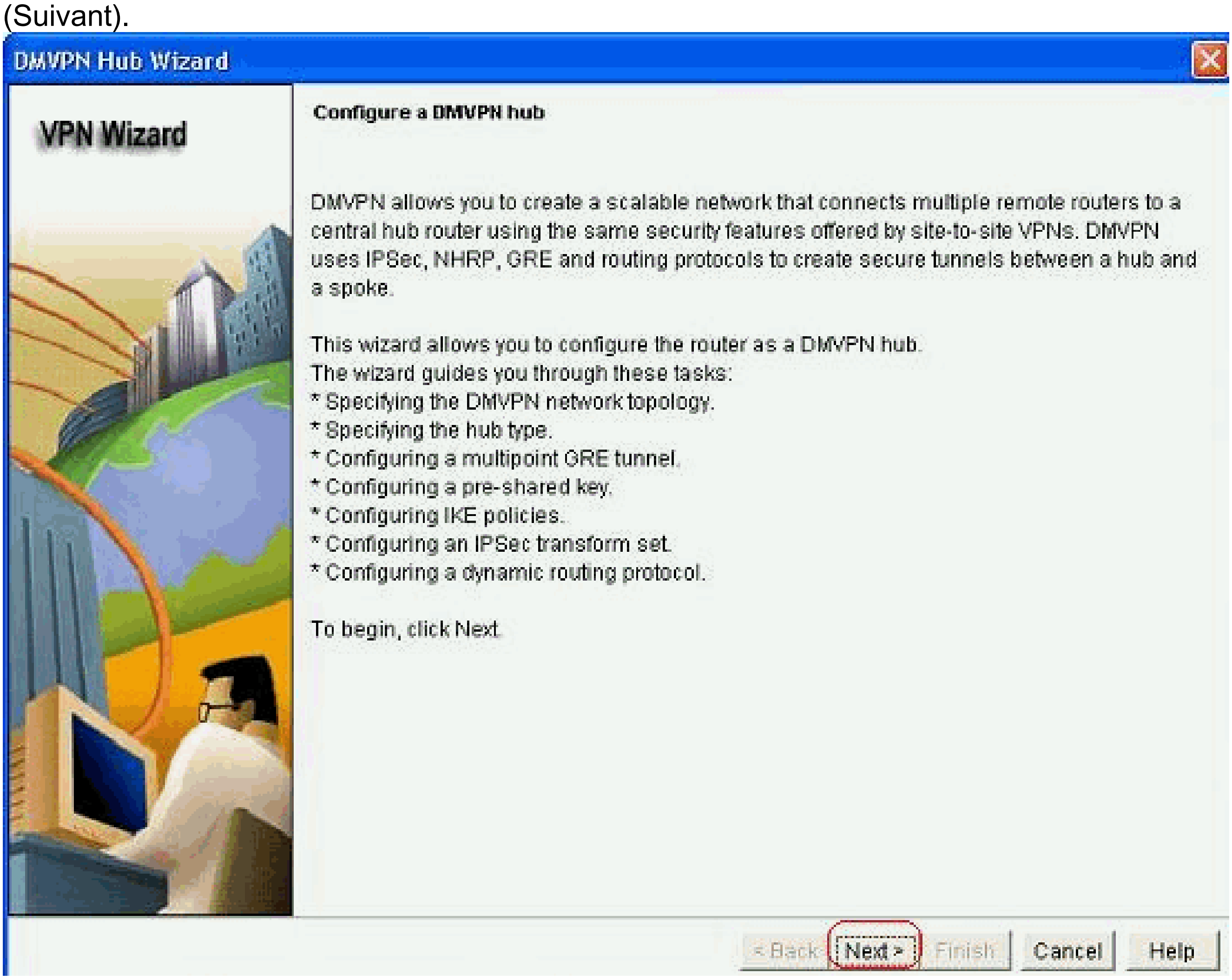
○ Create a spoke (client) in a DMVPN

Use this option to configure the router as a spoke in a full mesh or hub and spoke network topology. To complete this configuration, you must know the hub's IP address, NHRP information, pre-shared key, IKE policy, IPSec Transform set and dynamic routing protocol information.

● Create a hub (server or head-end) in a DMVPN

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.

2. Cliquez sur *Next* (Suivant).



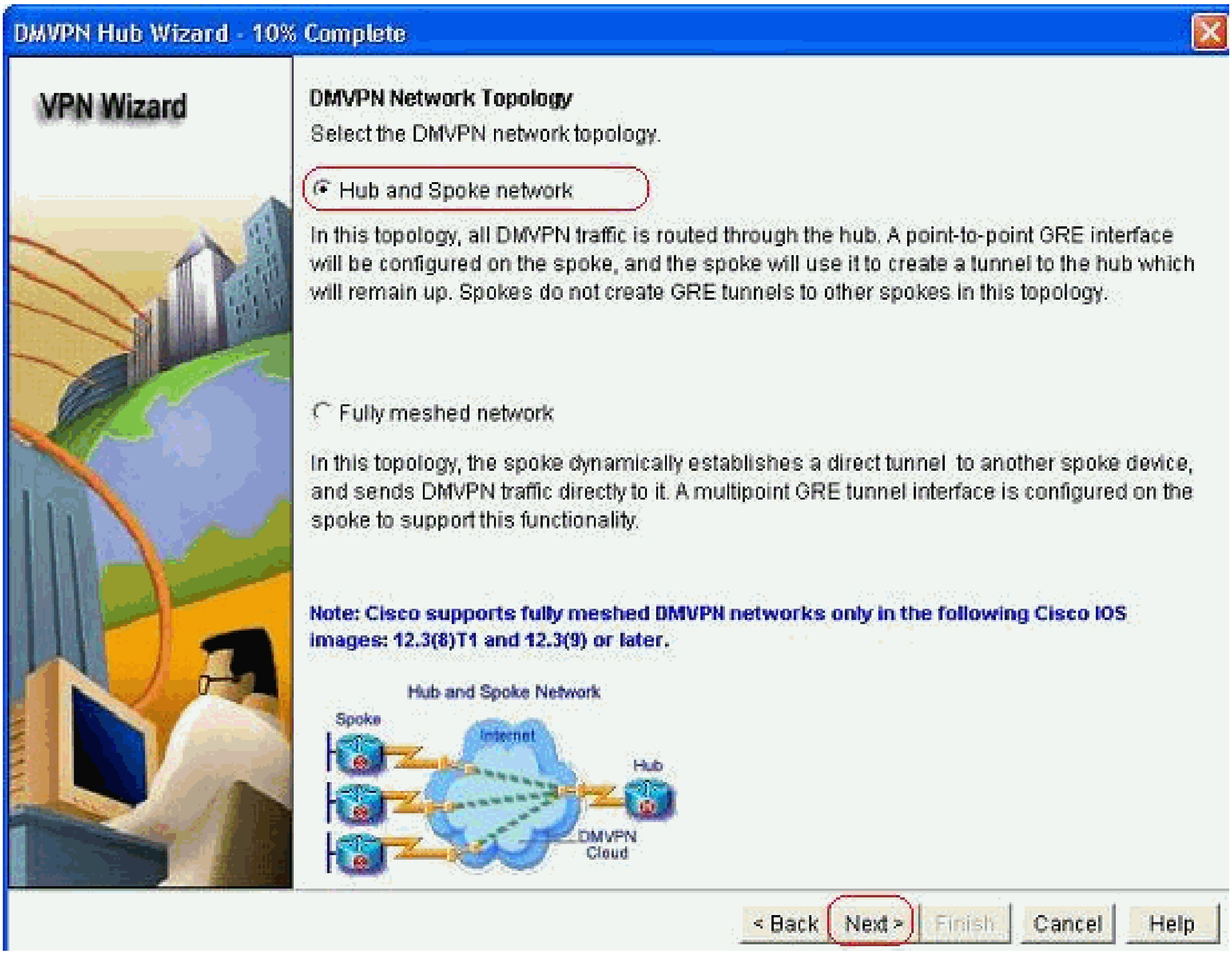
Configure a DMVPN hub

DMVPN allows you to create a scalable network that connects multiple remote routers to a central hub router using the same security features offered by site-to-site VPNs. DMVPN uses IPSec, NHRP, GRE and routing protocols to create secure tunnels between a hub and a spoke.

This wizard allows you to configure the router as a DMVPN hub.
The wizard guides you through these tasks:
* Specifying the DMVPN network topology.
* Specifying the hub type.
* Configuring a multipoint GRE tunnel.
* Configuring a pre-shared key.
* Configuring IKE policies.
* Configuring an IPSec transform set.
* Configuring a dynamic routing protocol.

To begin, click Next.

3. Sélectionnez l'option *Réseau Hub and Spoke* et cliquez sur *Suivant*.



DMVPN Hub Wizard - 10% Complete

VPN Wizard

DMVPN Network Topology

Select the DMVPN network topology.

● Hub and Spoke network

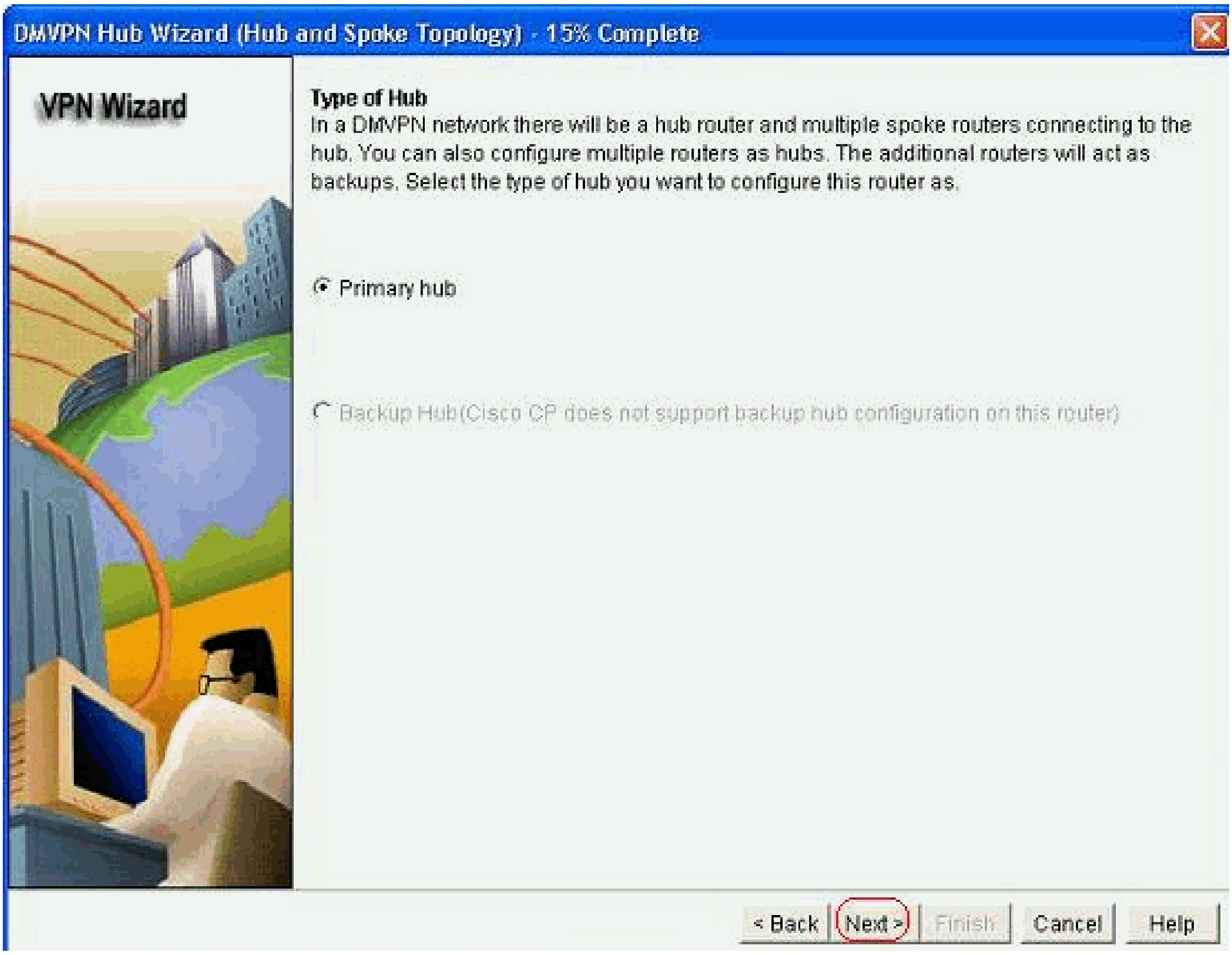
In this topology, all DMVPN traffic is routed through the hub. A point-to-point GRE interface will be configured on the spoke, and the spoke will use it to create a tunnel to the hub which will remain up. Spokes do not create GRE tunnels to other spokes in this topology.

○ 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.

4. Sélectionnez *Concentrateur principal*. Cliquez ensuite sur *Next*.



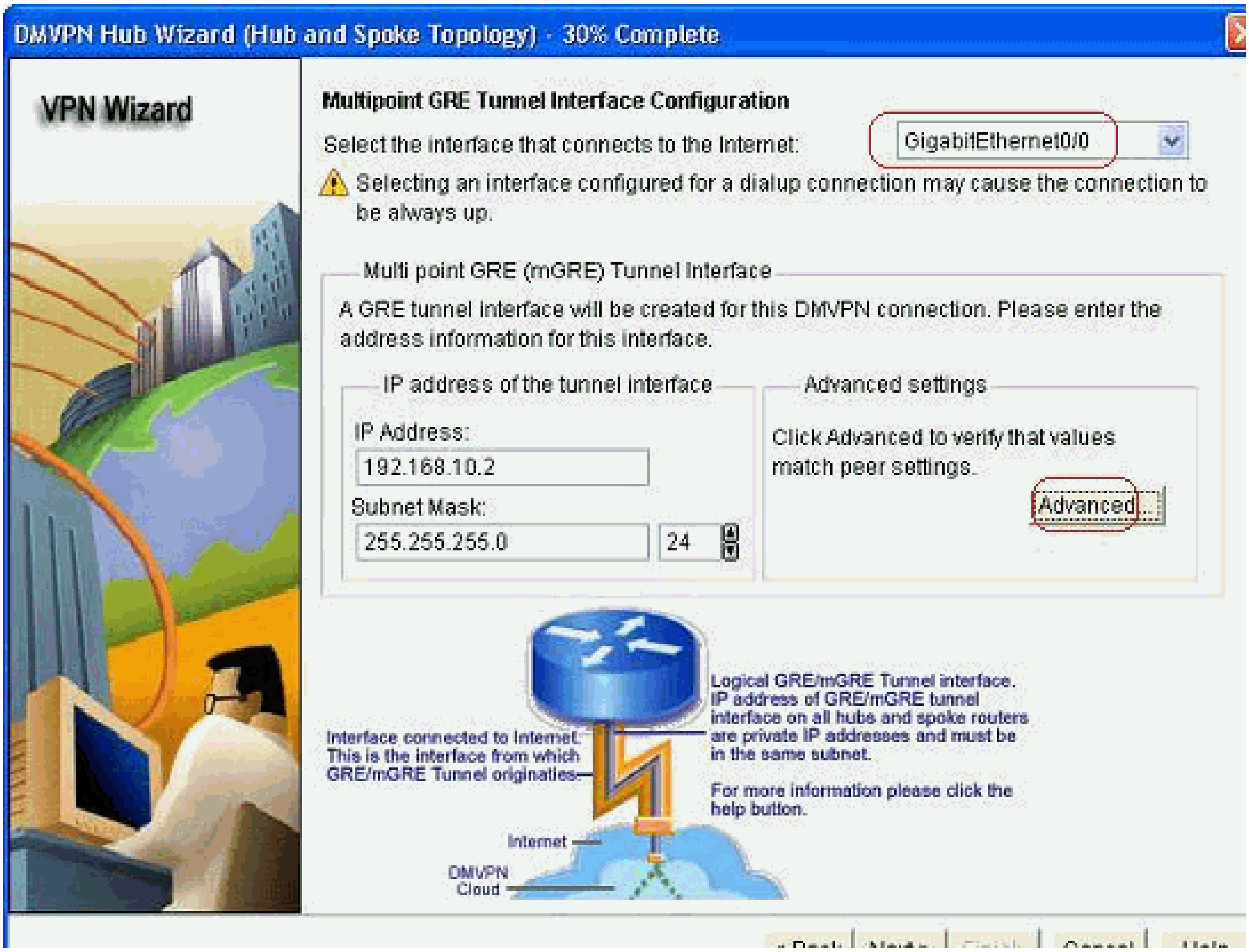
Type of Hub

In a DMVPN network there will be a hub router and multiple spoke routers connecting to the hub. You can also configure multiple routers as hubs. The additional routers will act as backups. Select the type of hub you want to configure this router as.

● Primary hub

○ Backup Hub(Cisco CP does not support backup hub configuration on this router)

5. Spécifiez les paramètres d'interface du tunnel et cliquez sur *Avancé*.



DMVPN Hub Wizard (Hub and Spoke Topology) - 30% Complete

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: 192.168.10.2

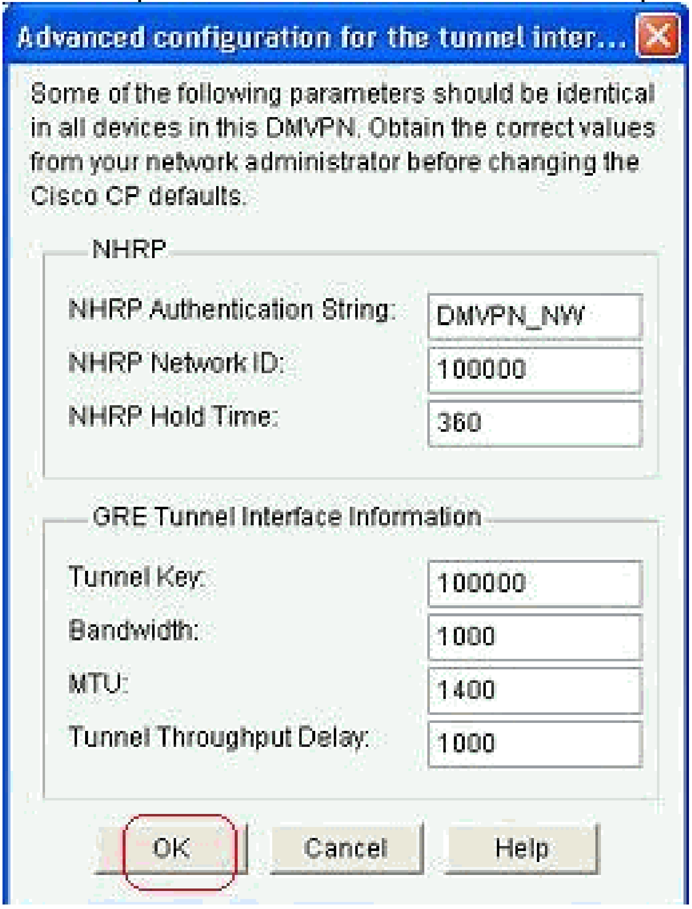
Subnet Mask: 255.255.255.0 24

Advanced settings

Click Advanced to verify that values match peer settings.

Advanced...
Logical GRE/mGRE Tunnel interface. IP address of GRE/mGRE tunnel interface on all hubs and spoke routers are private IP addresses and must be in the same subnet.
For more information please click the help button.
Interface connected to Internet. This is the interface from which GRE/mGRE Tunnel originates
Internet
DMVPN Cloud

6. Spécifiez les paramètres de tunnel et NHRP. Cliquez ensuite sur



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: DMVPN_NW

NHRP Network ID: 100000

NHRP Hold Time: 360

GRE Tunnel Interface Information

Tunnel Key: 100000

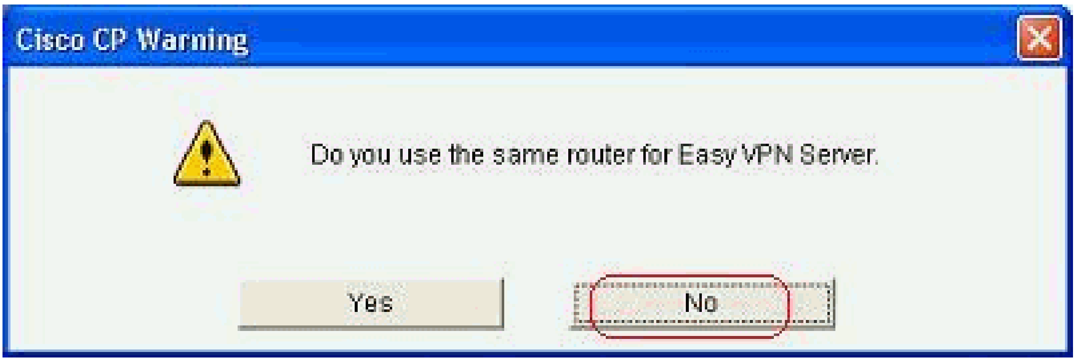
Bandwidth: 1000

MTU: 1400

Tunnel Throughput Delay: 1000

OK.

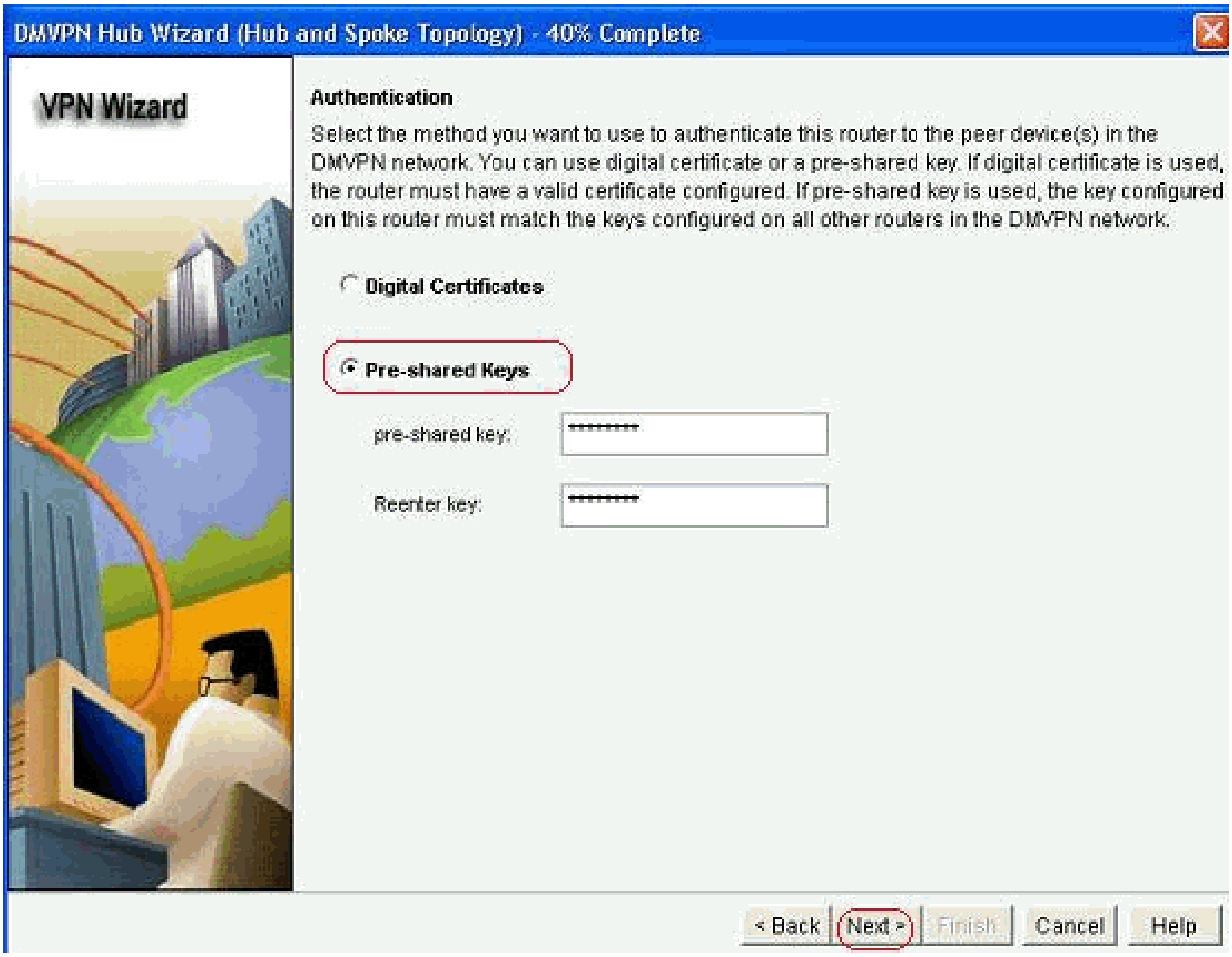
7. Spécifiez l'option en fonction de la configuration de votre

réseau.

Cisco CP Warning

Do you use the same router for Easy VPN Server.

8. Sélectionnez *Clés prépartagées* et spécifiez les clés prépartagées. Cliquez ensuite sur *Next*.



DMVPN Hub Wizard (Hub and Spoke Topology) - 40% Complete

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.

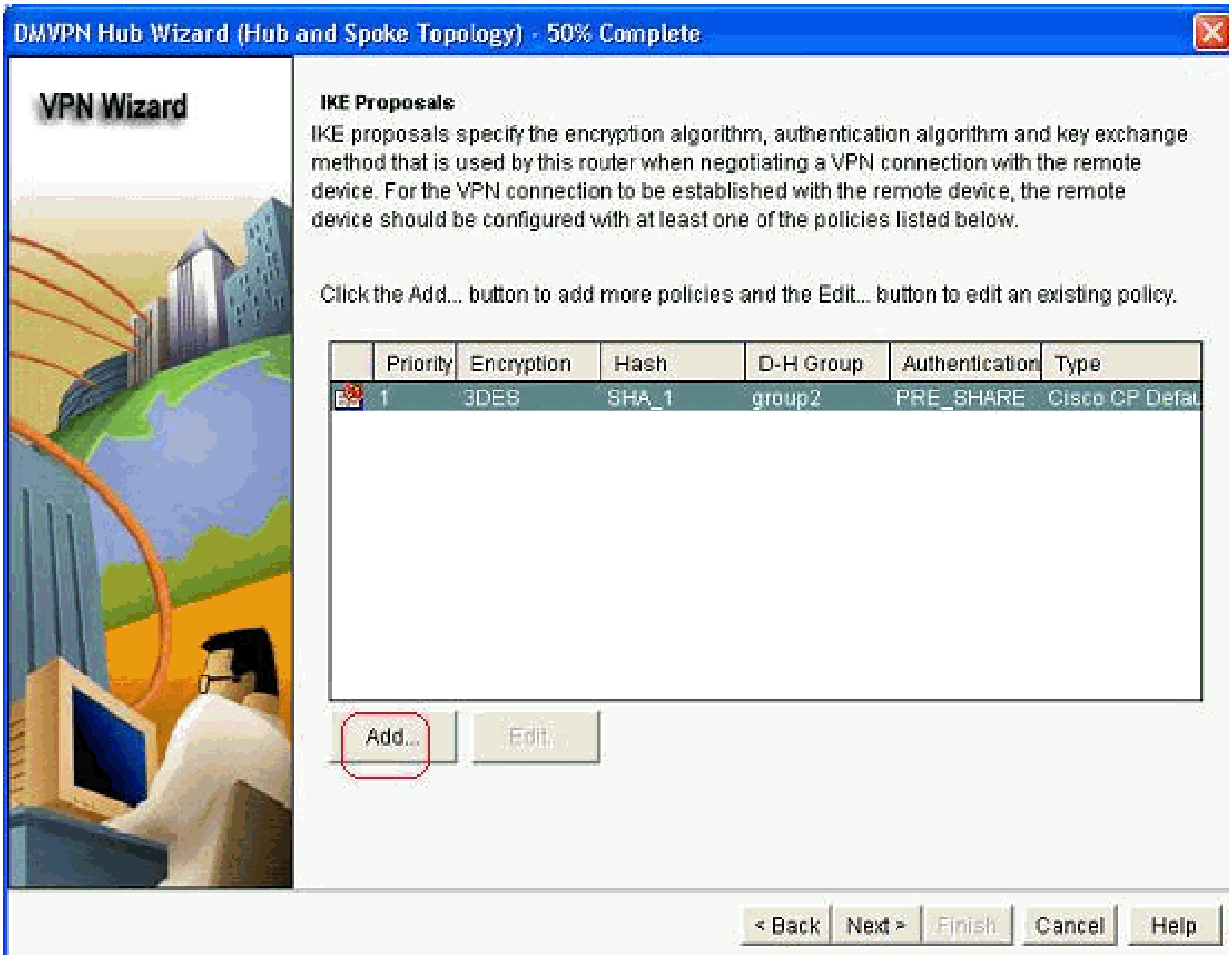
○ Digital Certificates

● Pre-shared Keys

pre-shared key: *********

Reenter key: *********

9. Cliquez sur *Add* afin d'ajouter une proposition IKE distincte.



DMVPN Hub Wizard (Hub and Spoke Topology) - 50% Complete

VPN Wizard

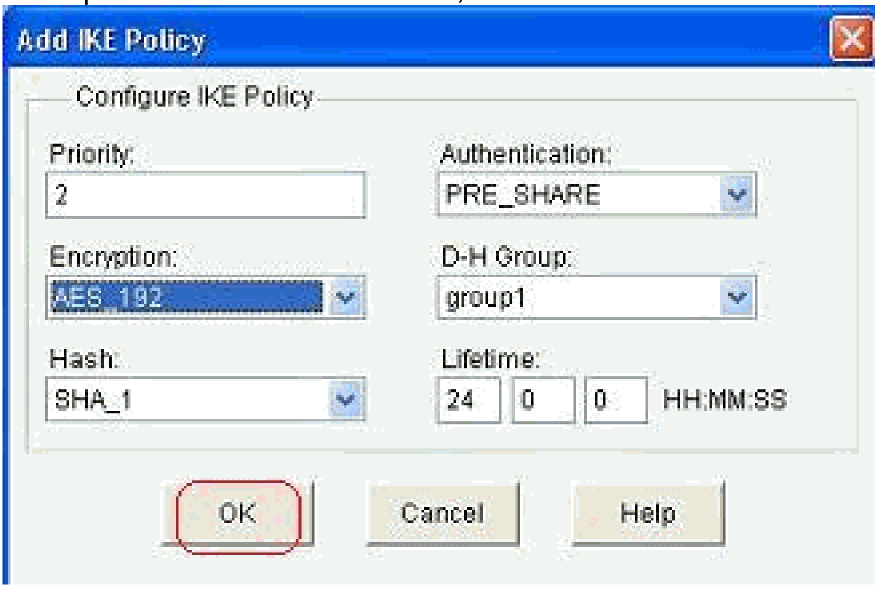
IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

	Priority	Encryption	Hash	D-H Group	Authentication	Type
	1	3DES	SHA_1	group2	PRE_SHARE	Cisco CP Defau

10. Spécifiez les paramètres de chiffrement, d'authentification et de hachage. Cliquez ensuite sur *OK*.



Add IKE Policy

Configure IKE Policy

Priority: 2

Authentication: PRE_SHARE

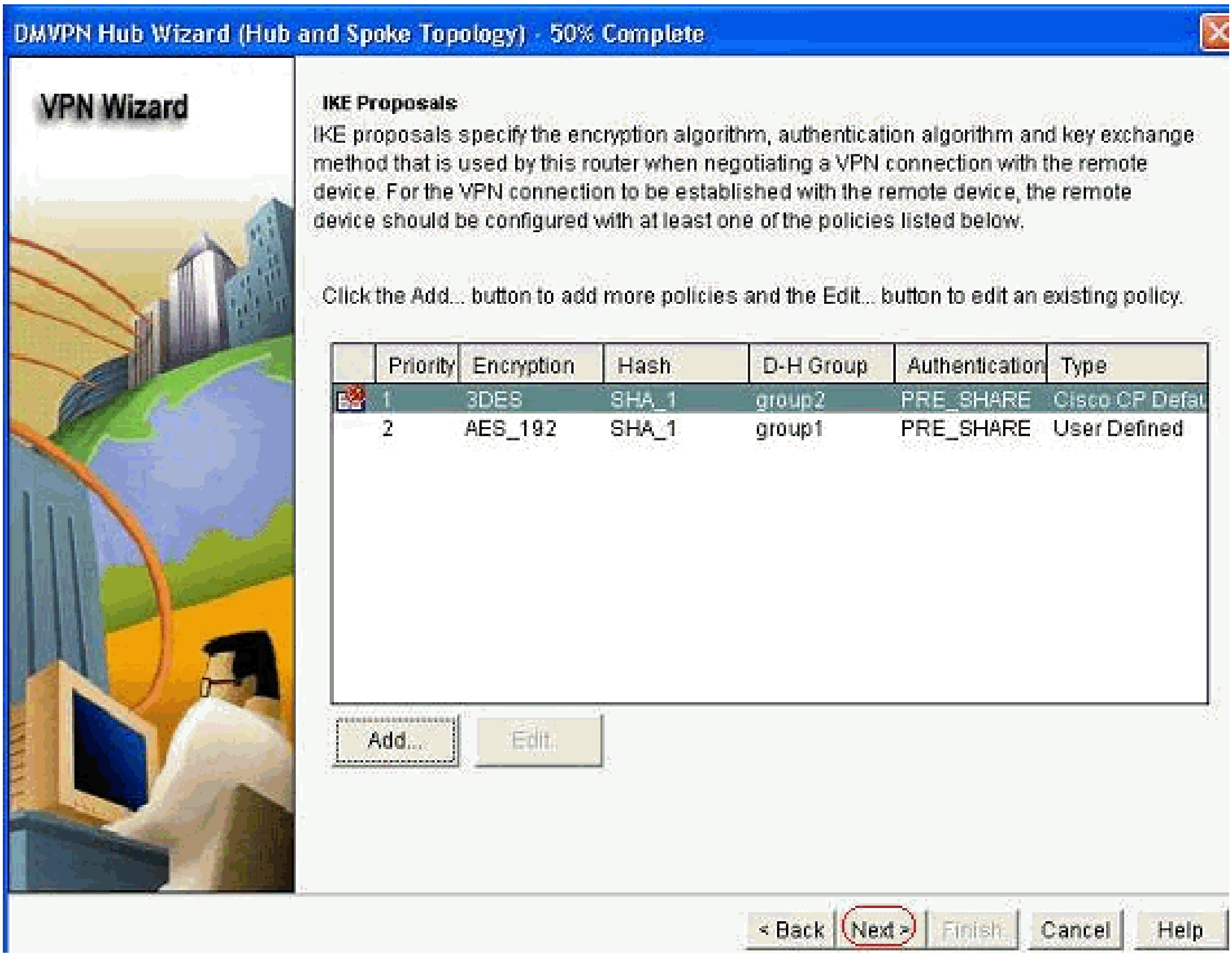
Encryption: AES_192

D-H Group: group1

Hash: SHA_1

Lifetime: 24 0 0 HH:MM:SS

11. La nouvelle stratégie IKE est visible ici. Cliquez sur *Next* (Suivant).



DMVPN Hub Wizard (Hub and Spoke Topology) - 50% Complete

VPN Wizard

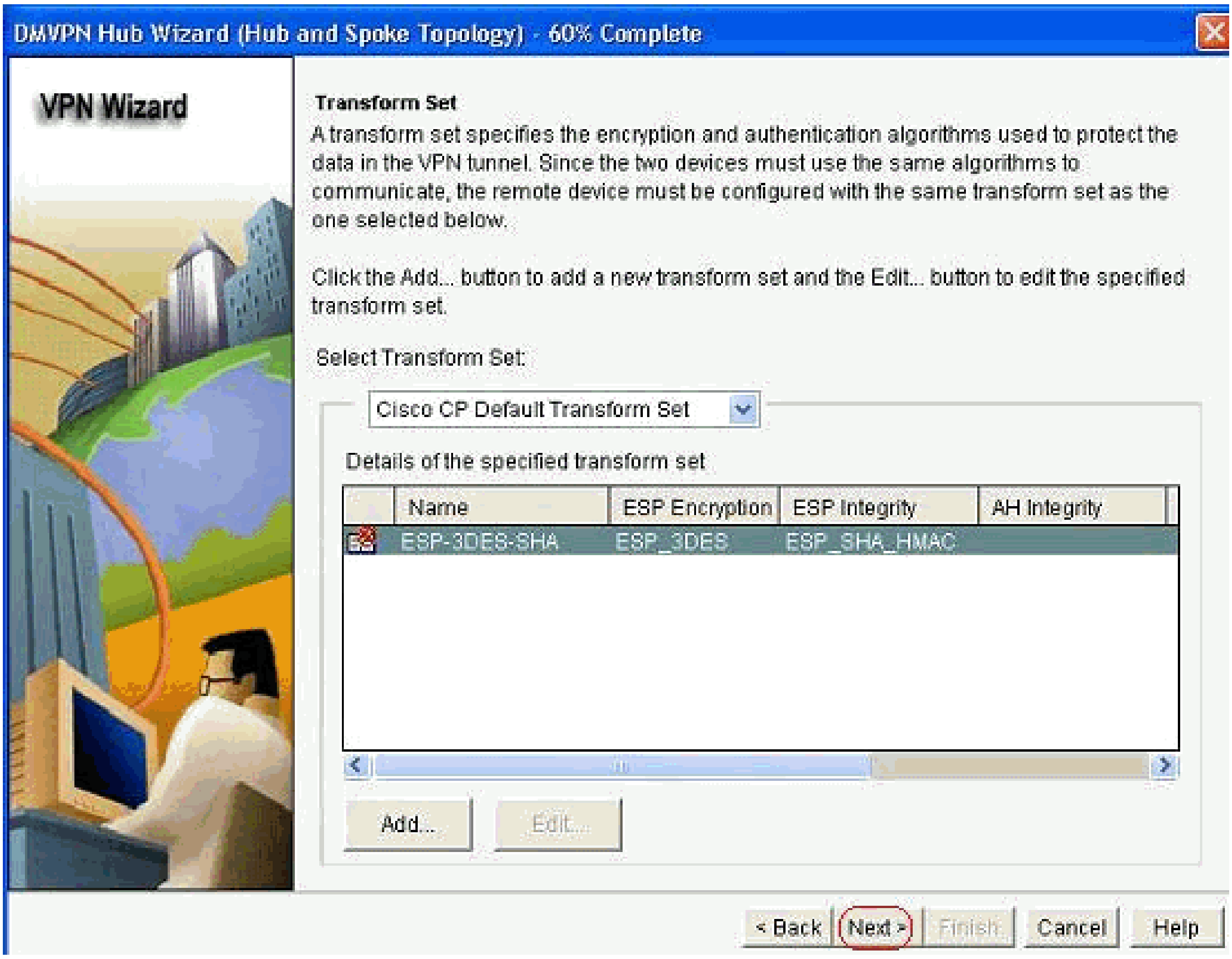
IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

Priority	Encryption	Hash	D-H Group	Authentication	Type
1	3DES	SHA_1	group2	PRE_SHARE	Cisco CP Defau
2	AES_192	SHA_1	group1	PRE_SHARE	User Defined

12. Cliquez sur *Suivant* pour continuer avec le jeu de transformation par défaut.



DMVPN Hub Wizard (Hub and Spoke Topology) - 60% Complete

Transform Set

A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must use the same algorithms to communicate, the remote device must be configured with the same transform set as the one selected below.

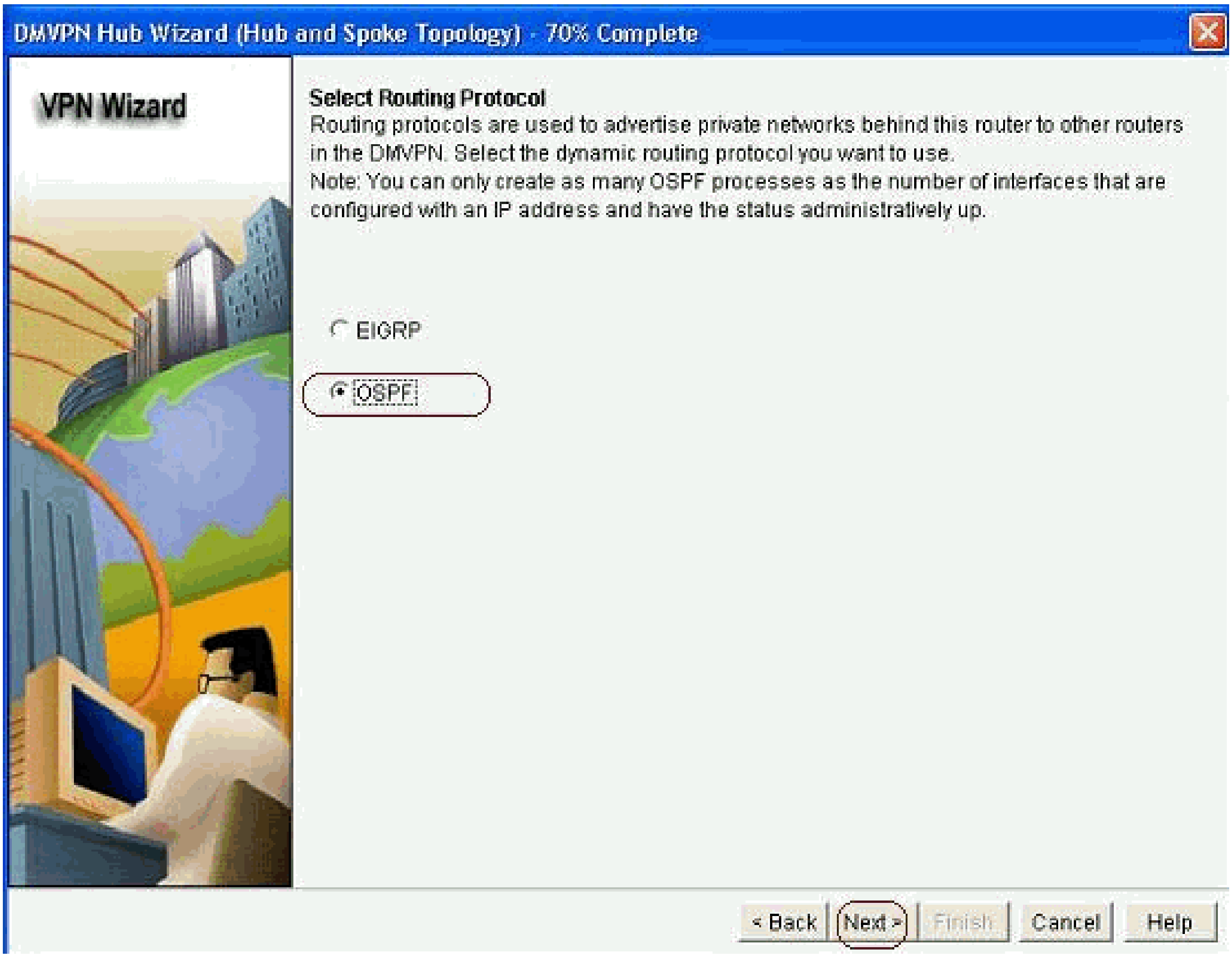
Click the Add... button to add a new transform set and the Edit... button to edit the specified transform set.

Select Transform Set: Cisco CP Default Transform Set

Details of the specified transform set

Name	ESP Encryption	ESP Integrity	AH Integrity
ESP-3DES-SHA	ESP_3DES	ESP_SHA_HMAC	

13. Sélectionnez le protocole de routage requis. Ici, *OSPF* est sélectionné.



DMVPN Hub Wizard (Hub and Spoke Topology) - 70% Complete

Select Routing Protocol

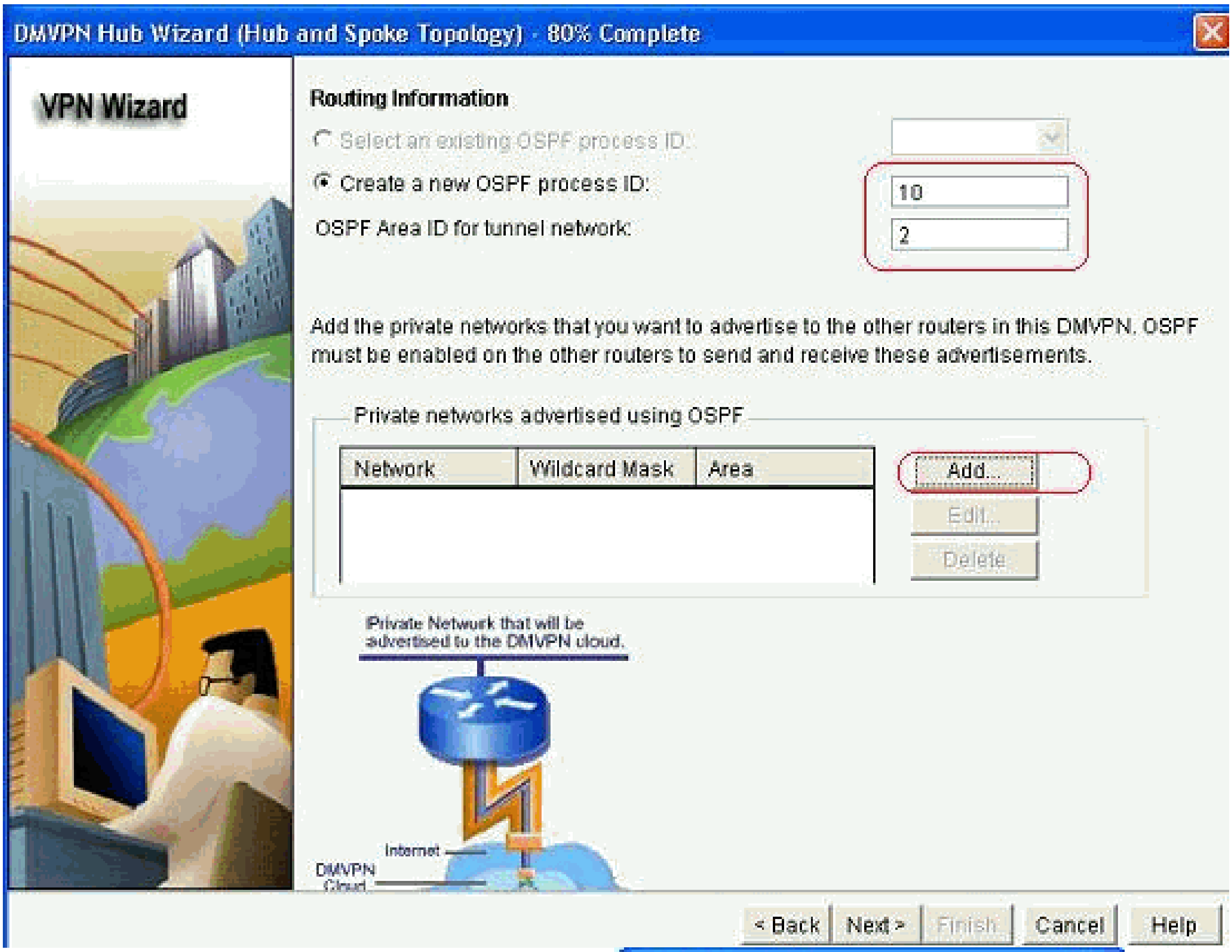
Routing protocols are used to advertise private networks behind this router to other routers in the DMVPN. Select the dynamic routing protocol you want to use.

Note: You can only create as many OSPF processes as the number of interfaces that are configured with an IP address and have the status administratively up.

○ EIGRP

● OSPF

14. Spécifiez l'ID de processus OSPF et l'ID de zone. Cliquez sur *Add* afin d'ajouter les réseaux à annoncer par
OSPF.



DMVPN Hub Wizard (Hub and Spoke Topology) - 80% Complete

VPN Wizard

Routing Information

○ Select an existing OSPF process ID:

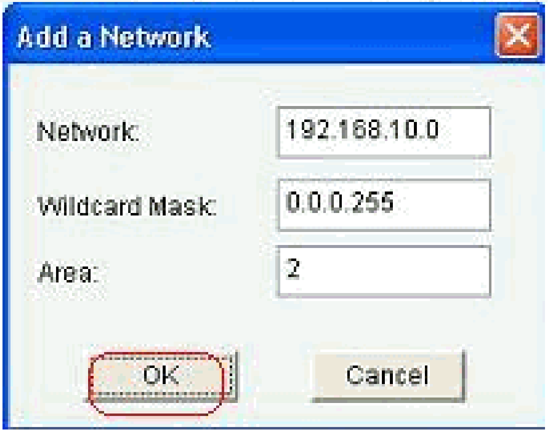
● Create a new OSPF process ID: 10

OSPF Area ID for tunnel network: 2

Add the private networks that you want to advertise to the other routers in this DMVPN. OSPF must be enabled on the other routers to send and receive these advertisements.

Private networks advertised using OSPF

Network	Wildcard Mask	Area



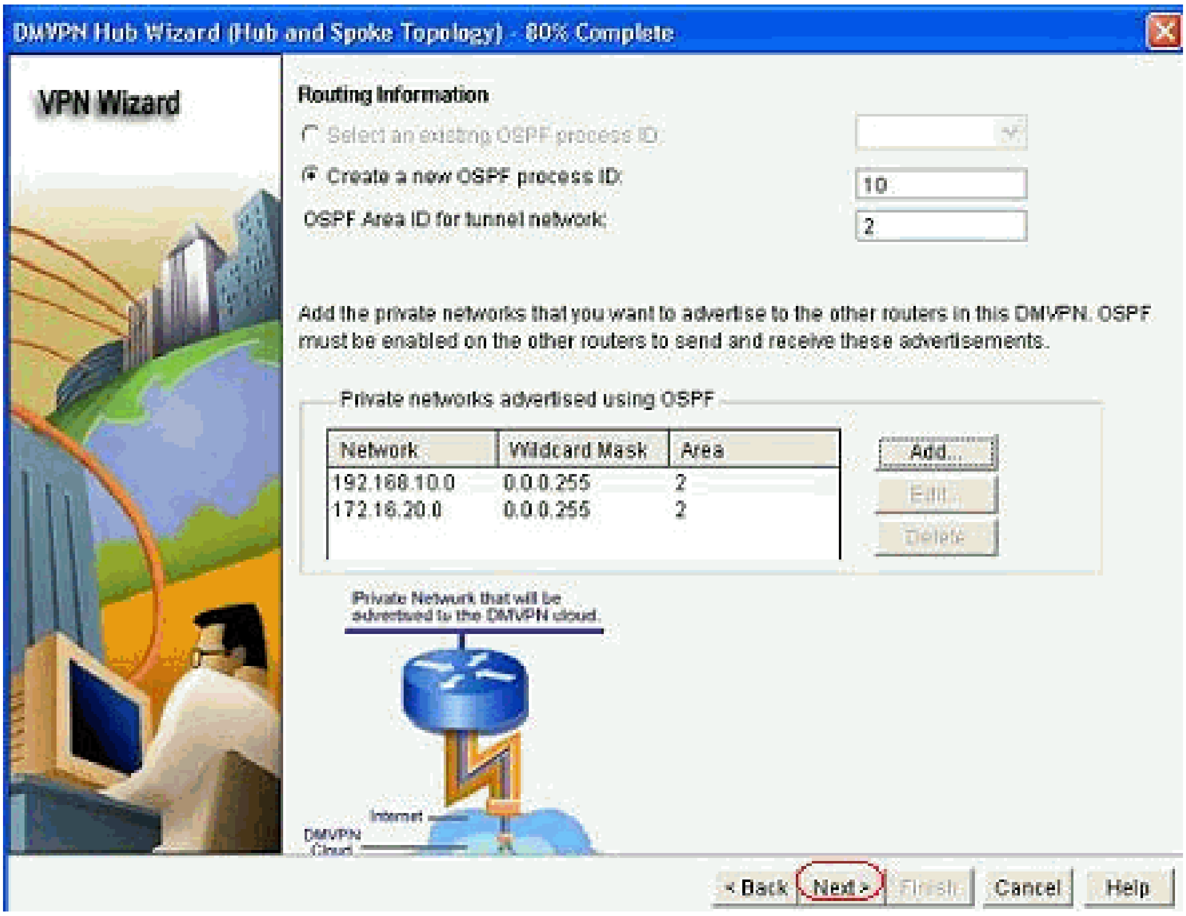
Add a Network

Network: 192.168.10.0

Wildcard Mask: 0.0.0.255

Area: 2

15. Ajoutez le réseau du tunnel et cliquez sur *OK*.
16. Ajoutez le réseau privé derrière le routeur Hub et cliquez sur *Next (Suivant)*.



DMVPN Hub Wizard (Hub and Spoke Topology) - 80% Complete

VPN Wizard

Routing Information

○ Select an existing OSPF process ID:

● Create a new OSPF process ID: 10

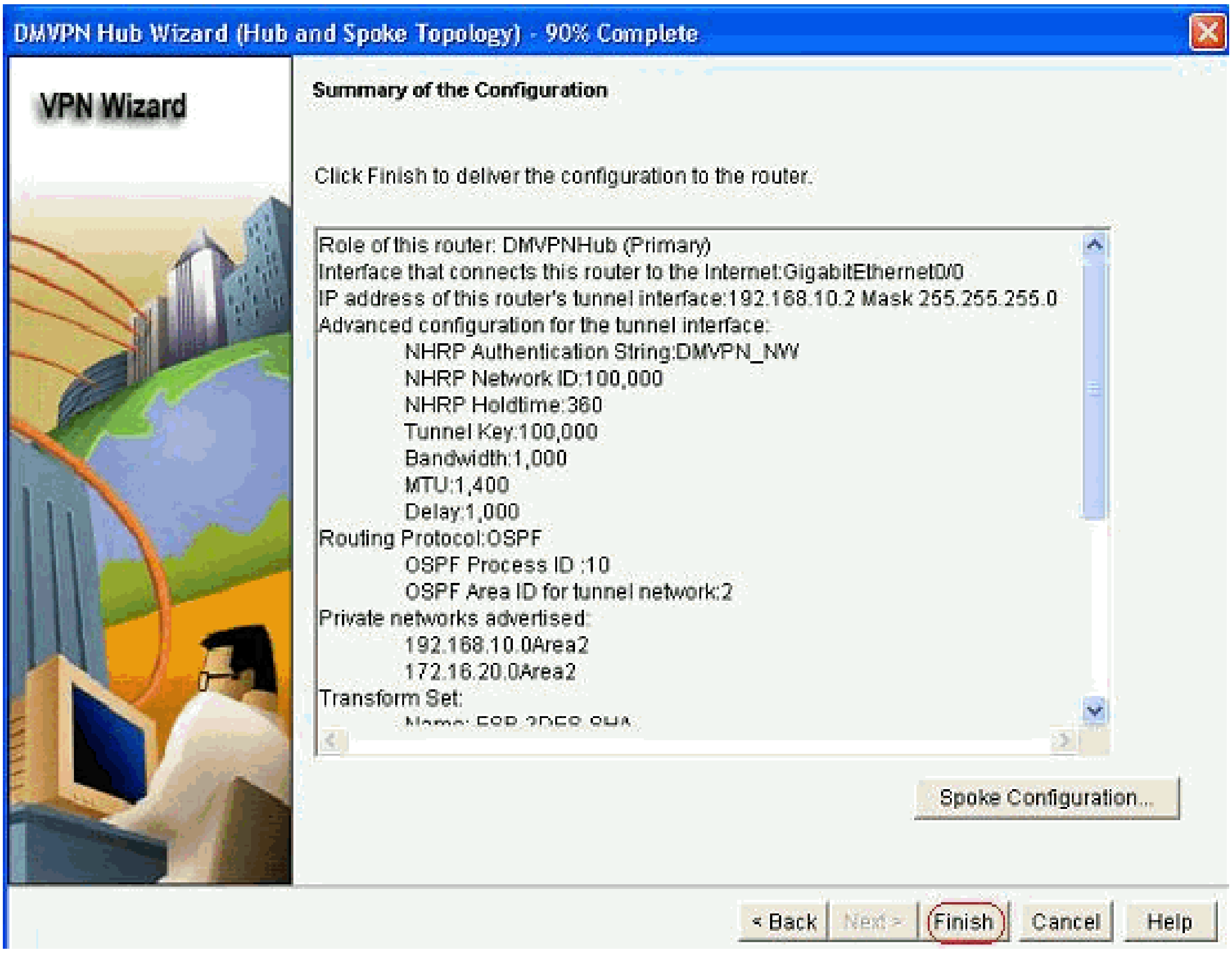
OSPF Area ID for tunnel network: 2

Add the private networks that you want to advertise to the other routers in this DMVPN. OSPF must be enabled on the other routers to send and receive these advertisements.

Private networks advertised using OSPF

Network	Wildcard Mask	Area
192.168.10.0	0.0.0.255	2
172.16.20.0	0.0.0.255	2

17. Cliquez sur *Terminer* pour terminer la configuration de l'assistant.



DMVPN Hub Wizard (Hub and Spoke Topology) - 90% Complete

VPN Wizard

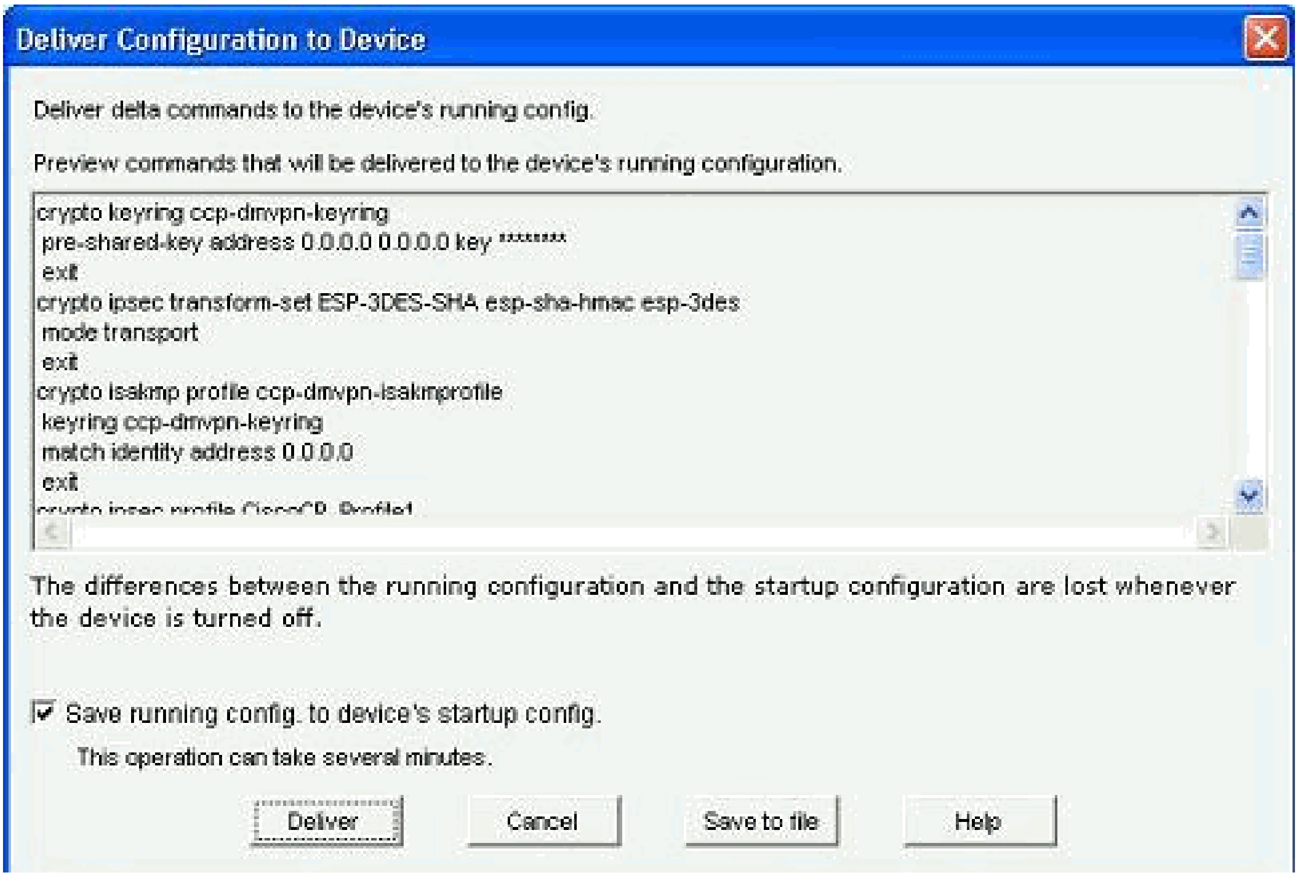
Summary of the Configuration

Click Finish to deliver the configuration to the router.

```
Role of this router: DMVPNHub (Primary)
Interface that connects this router to the Internet:GigabitEthernet0/0
IP address of this router's tunnel interface:192.168.10.2 Mask 255.255.255.0
Advanced configuration for the tunnel interface:
          NHRP Authentication String:DMVPN_NW
          NHRP Network ID:100,000
          NHRP Holdtime:360
          Tunnel Key:100,000
          Bandwidth:1,000
          MTU:1,400
          Delay:1,000
Routing Protocol:OSPF
          OSPF Process ID :10
          OSPF Area ID for tunnel network:2
Private networks advertised:
          192.168.10.0Area2
          172.16.20.0Area2
Transform Set:
          Name: ESP-3DES-SHA
```

18. Cliquez sur *Deliver* pour exécuter les

commandes.



Deliver delta commands to the device's running config.

Preview commands that will be delivered to the device's running configuration.

```
crypto keyring ccp-dmvpn-keyring
 pre-shared-key address 0.0.0.0 0.0.0.0 key ********
 exit
crypto ipsec transform-set ESP-3DES-SHA esp-sha-hmac esp-3des
 mode transport
 exit
crypto isakmp profile ccp-dmvpn-isakmprofile
 keyring ccp-dmvpn-keyring
 match identity address 0.0.0.0
 exit
crypto ipsec profile CiscoCP_Profile1
```

The differences between the running configuration and the startup configuration are lost whenever the device is turned off.

☑ Save running config. to device's startup config.

This operation can take several minutes.

Configuration CLI pour concentrateur

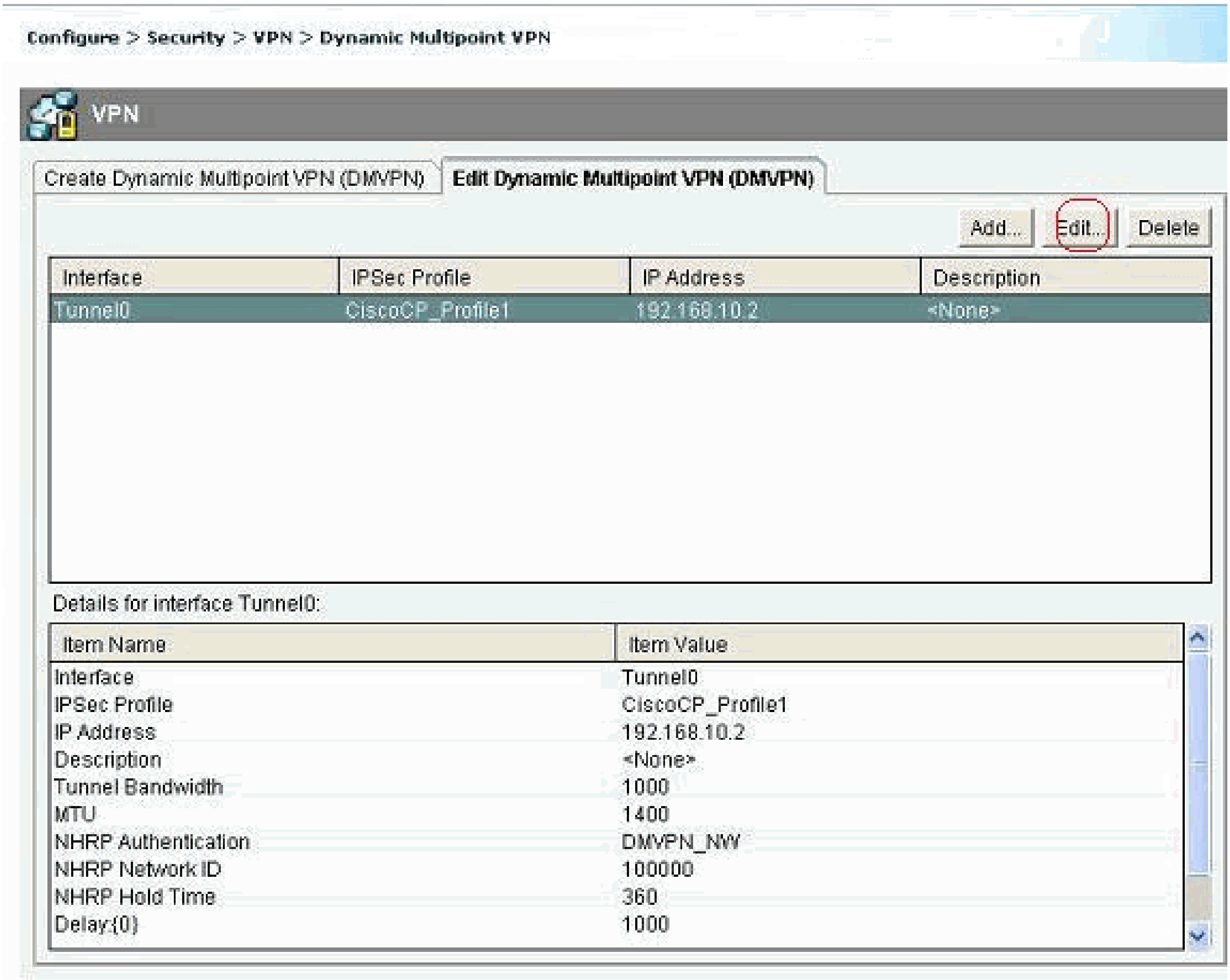
La configuration CLI associée est présentée ici :

Routeur concentrateur

```
!
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
!
```

Modifier la configuration DMVPN à l'aide de CCP

Vous pouvez modifier manuellement les paramètres de tunnel DMVPN existants lorsque vous sélectionnez l'interface du tunnel et cliquez sur *Modifier*.

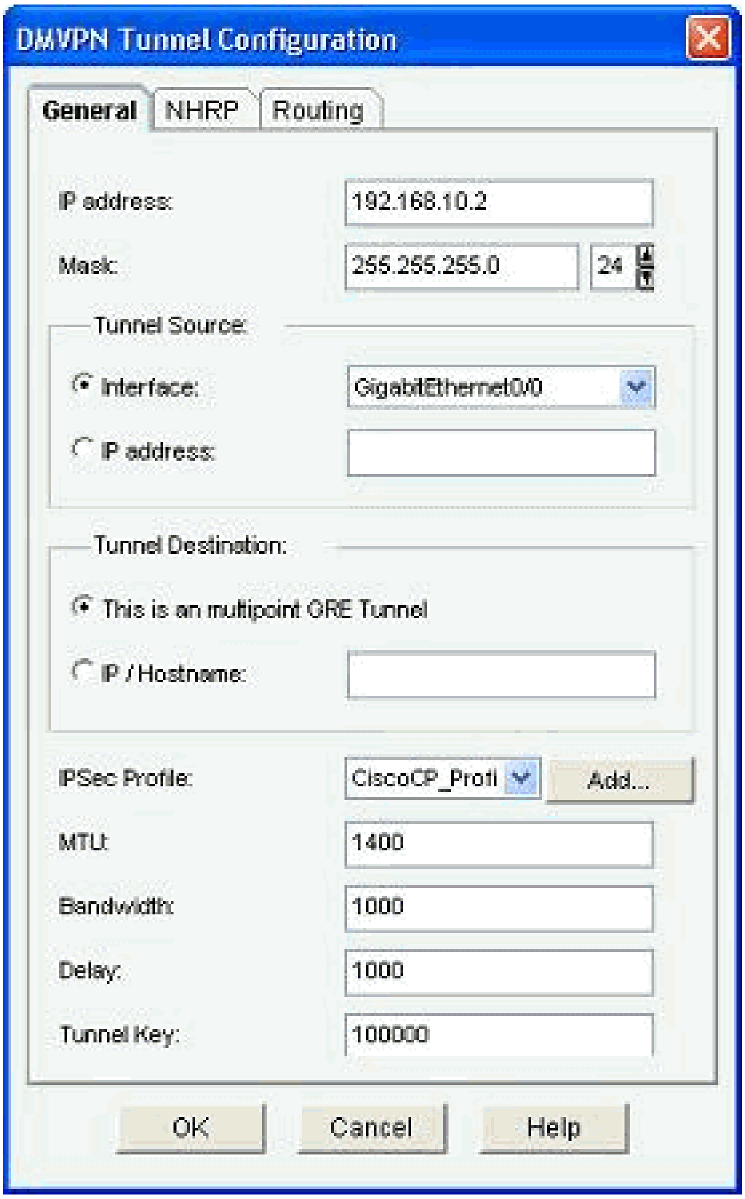

Configure > Security > VPN > Dynamic Multipoint VPN
VPN
Create Dynamic Multipoint VPN (DMVPN)
Edit Dynamic Multipoint VPN (DMVPN)
Add...
Edit...
Delete

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

Les paramètres d'interface de tunnel tels que MTU et la clé de tunnel sont modifiés sous l'onglet *Général*.



IP address: 192.168.10.2

Mask: 255.255.255.0 24

Tunnel Source:

● Interface: GigabitEthernet0/0

○ IP address:

Tunnel Destination:

● This is an multipoint GRE Tunnel

○ IP / Hostname:

IPSec Profile: CiscoCP_Profi

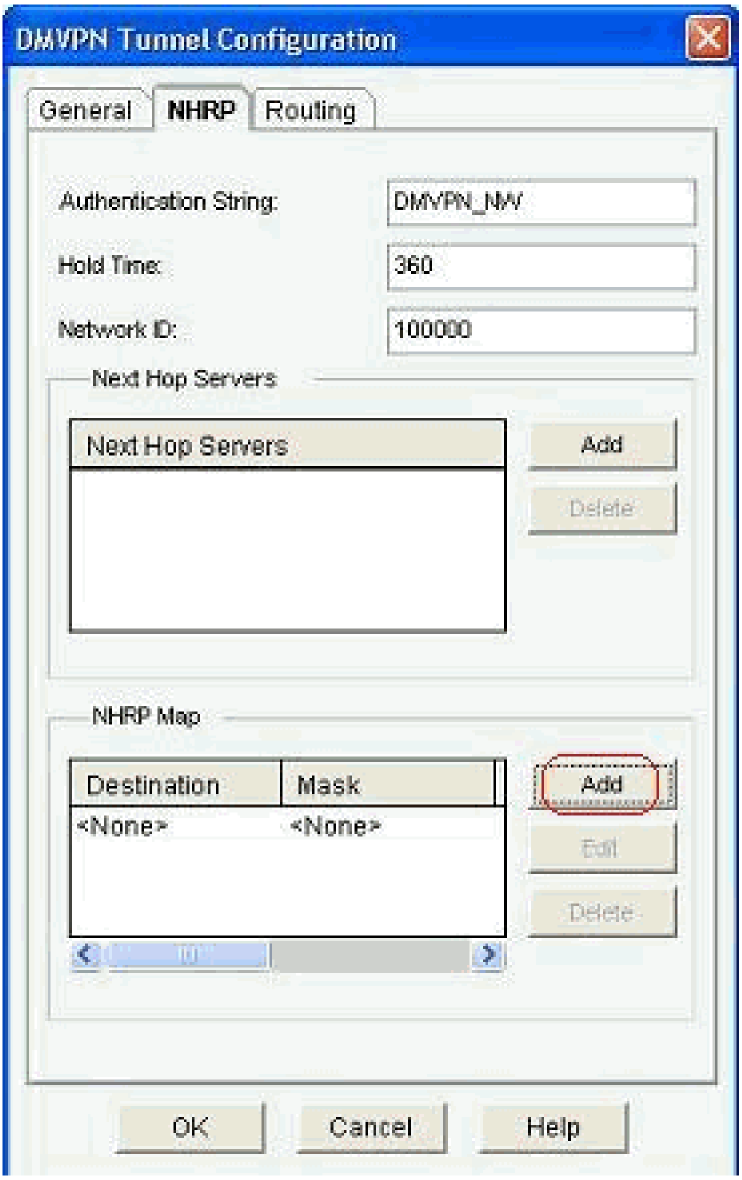
MTU: 1400

Bandwidth: 1000

Delay: 1000

Tunnel Key: 100000

1. Les paramètres liés au PNRDS sont trouvés et modifiés conformément aux exigences de l'onglet *PNRDS*. Pour un routeur en étoile, vous devez être en mesure d'afficher le NHS comme adresse IP du routeur concentrateur. Cliquez sur *Add* dans la section NHRP Map


DMVPN Tunnel Configuration

General | NHRP | Routing

Authentication String: DMVPN_NW

Hold Time: 360

Network ID: 100000

Next Hop Servers

Next Hop Servers

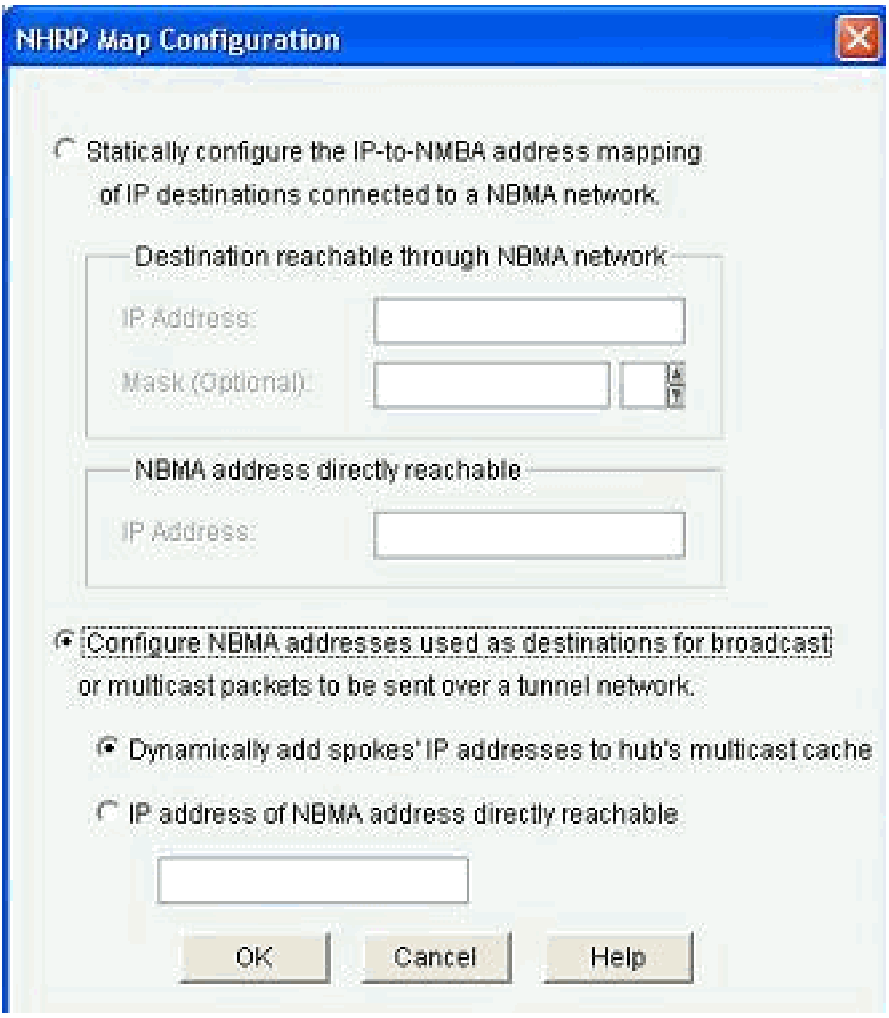
NHRP Map

Destination	Mask
<None>	<None>

afin d'ajouter le mappage NHRP.

2. Selon la configuration du réseau, les paramètres de mappage NHRP peuvent être configurés

comme indiqué ici :



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

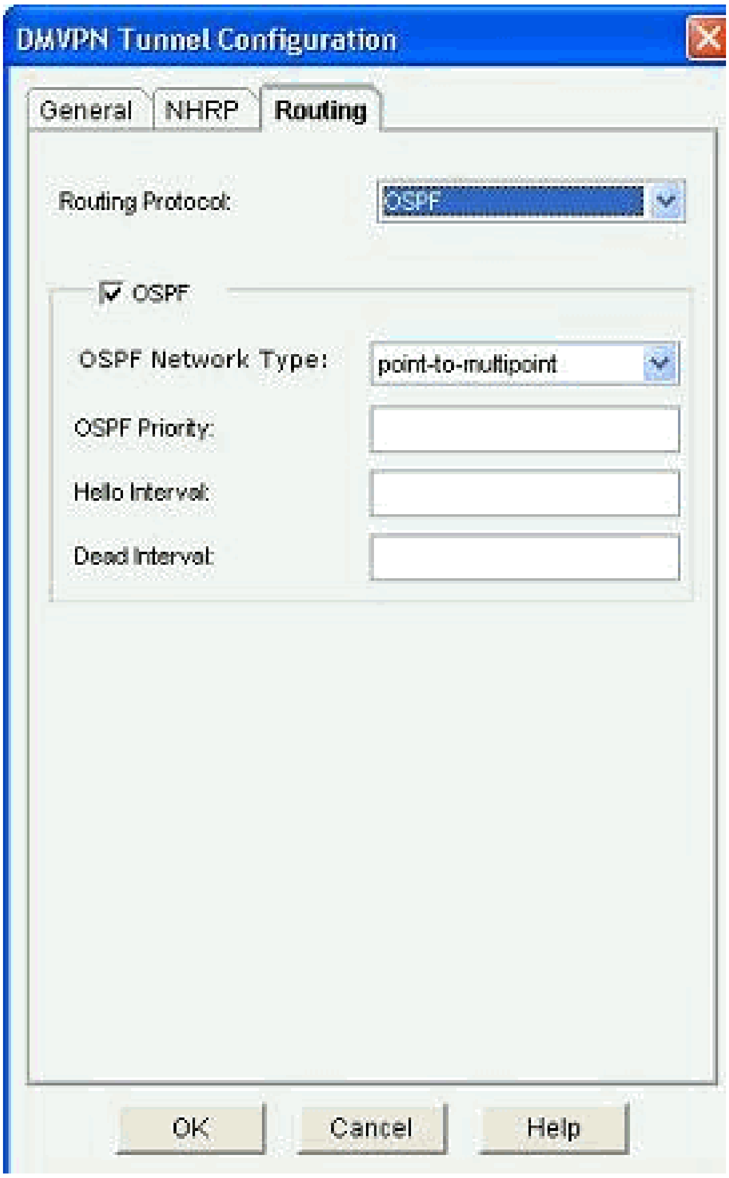
IP Address:

● 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

Les paramètres liés au routage sont affichés et modifiés sous l'onglet *Routage*.


DMVPN Tunnel Configuration

Routing Protocol: OSPF

☑ OSPF

OSPF Network Type: point-to-multipoint

OSPF Priority:

Hello Interval:

Dead Interval:

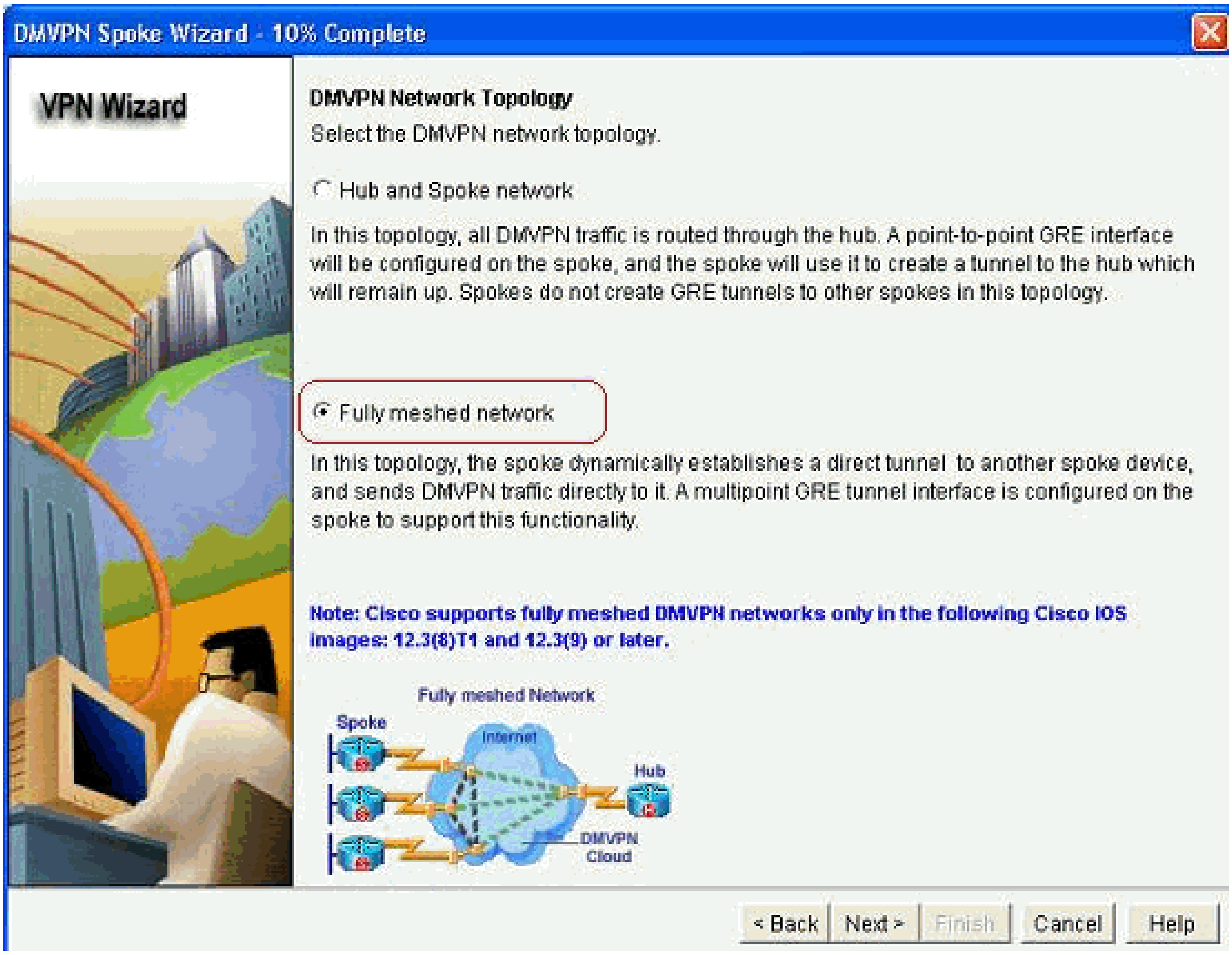
Plus d'informations

Les tunnels DMVPN sont configurés de deux manières :

- Communication satellite à satellite via le concentrateur
- Communication satellite à satellite sans concentrateur

Dans ce document, seule la première méthode est abordée. Afin de permettre l'établissement de tunnels IPSec dynamiques de rayon à rayon, cette approche est utilisée pour ajouter le rayon au cloud DMVPN :

1. Lancez l'assistant DMVPN et sélectionnez l'option *de configuration Spoke*.
2. Dans la fenêtre *Topologie du réseau DMVPN*, sélectionnez l'option *Réseau maillé complet* au lieu de l'option *Réseau concentrateur et satellite*.



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.

3. Complétez le reste de la configuration en suivant les mêmes étapes que les autres configurations de ce document.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Informations connexes

- VPN multipoint dynamique Cisco : Communications de filiale à filiale simples et sécurisées
- VPN multipoint dynamique (DMVPN) IOS 12.2
- Support et documentation techniques - Cisco Systems