

Cisco IOS/CCP: Cisco CPによるDMVPNの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[Cisco CPを使用したスポークの設定](#)

[スポークのCLI設定](#)

[Cisco CPを使用したハブの設定](#)

[ハブのCLI設定](#)

[CCPを使用したDMVPN設定の編集](#)

[その他の情報](#)

[確認](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Configuration Professional(Cisco CP)を使用したハブルータとスポークルータ間のダイナミックマルチポイントVPN(DMVPN)トンネルの設定例を紹介します。Dynamic Multipoint VPNは、エンドユーザがダイナミックに作成されたスポーク間のIPSecトンネルを介して効率的に通信できる高度なソリューションを提供するように、GRE、IPSec暗号化、NHRPおよびルーティングなどの異なる概念を統合するテクノロジーです。

前提条件

要件

最適なDMVPN機能を得るには、Cisco IOS®ソフトウェアリリース12.4メインライン、12.4T以降を実行することを推奨します。

使用するコンポーネント

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

- Cisco IOSルータ3800シリーズ(ソフトウェアリリース12.4(22))
- Cisco IOSルータ1800シリーズ(ソフトウェアリリース12.3(8))

- Cisco Configuration Professionalバージョン2.5

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

表記法

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

背景説明

このドキュメントでは、Cisco CPを使用してルータをスポークとして、別のルータをハブとして設定する方法について説明します。最初のスポークの設定は示されていますが、このドキュメントの後半では、ハブ関連の設定も詳細に示され、より理解を深めることができます。他のスポークも、同様の方法でハブに接続するように設定できます。現在のシナリオでは、次のパラメータを使用します。

- ハブルータパブリックネットワーク – 209.165.201.0
- トンネルネットワーク : 192.168.10.0
- 使用されるルーティングプロトコル – OSPF

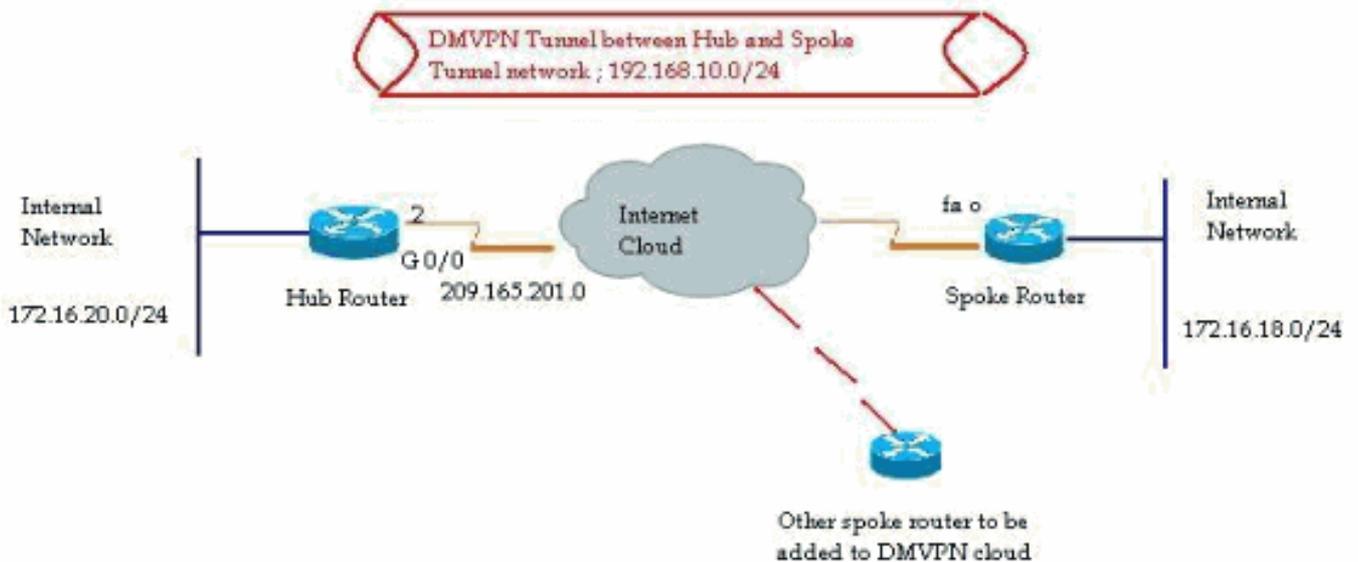
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool (登録ユーザ専用) を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

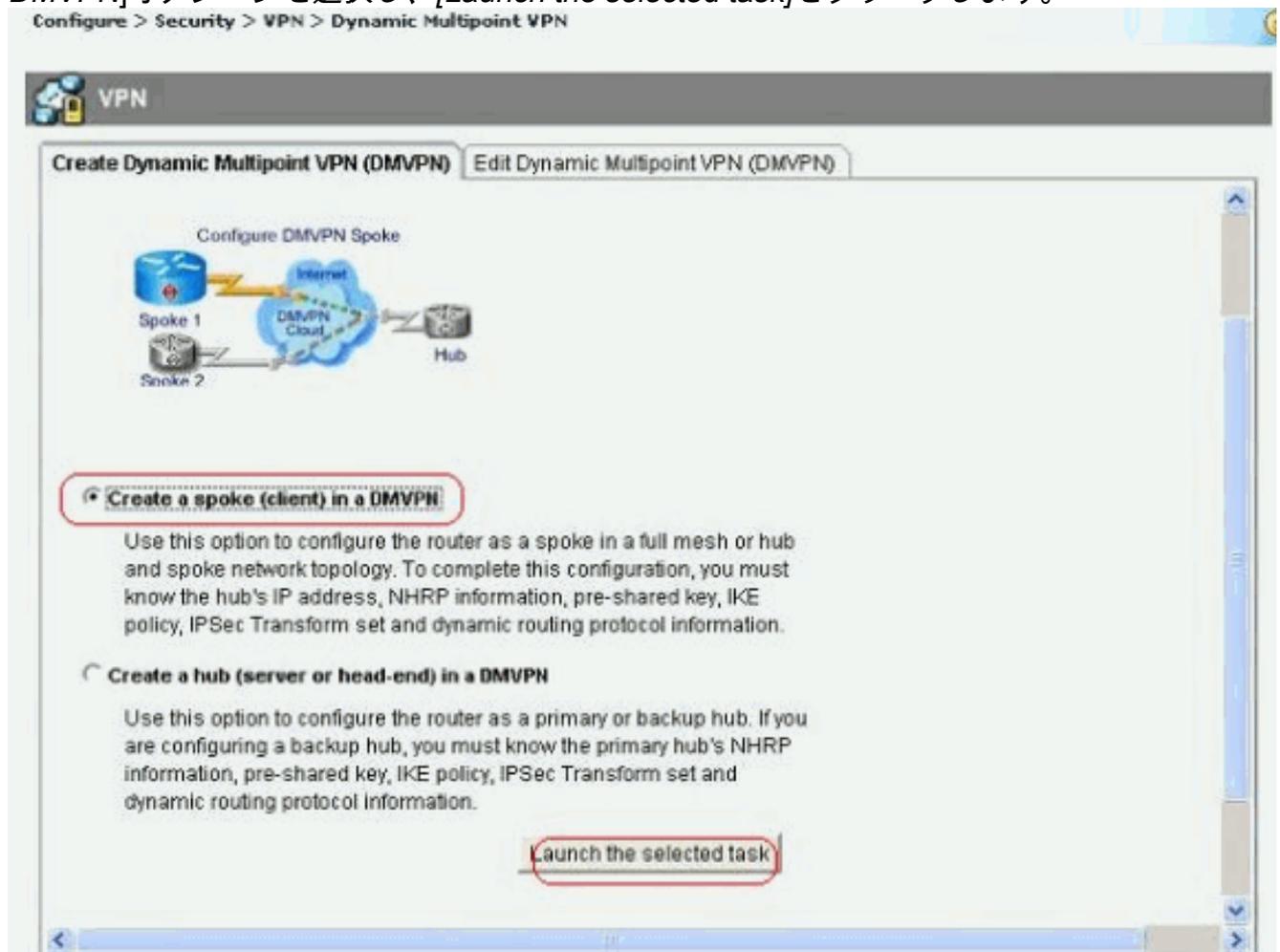
このドキュメントでは、次のネットワーク セットアップを使用します。



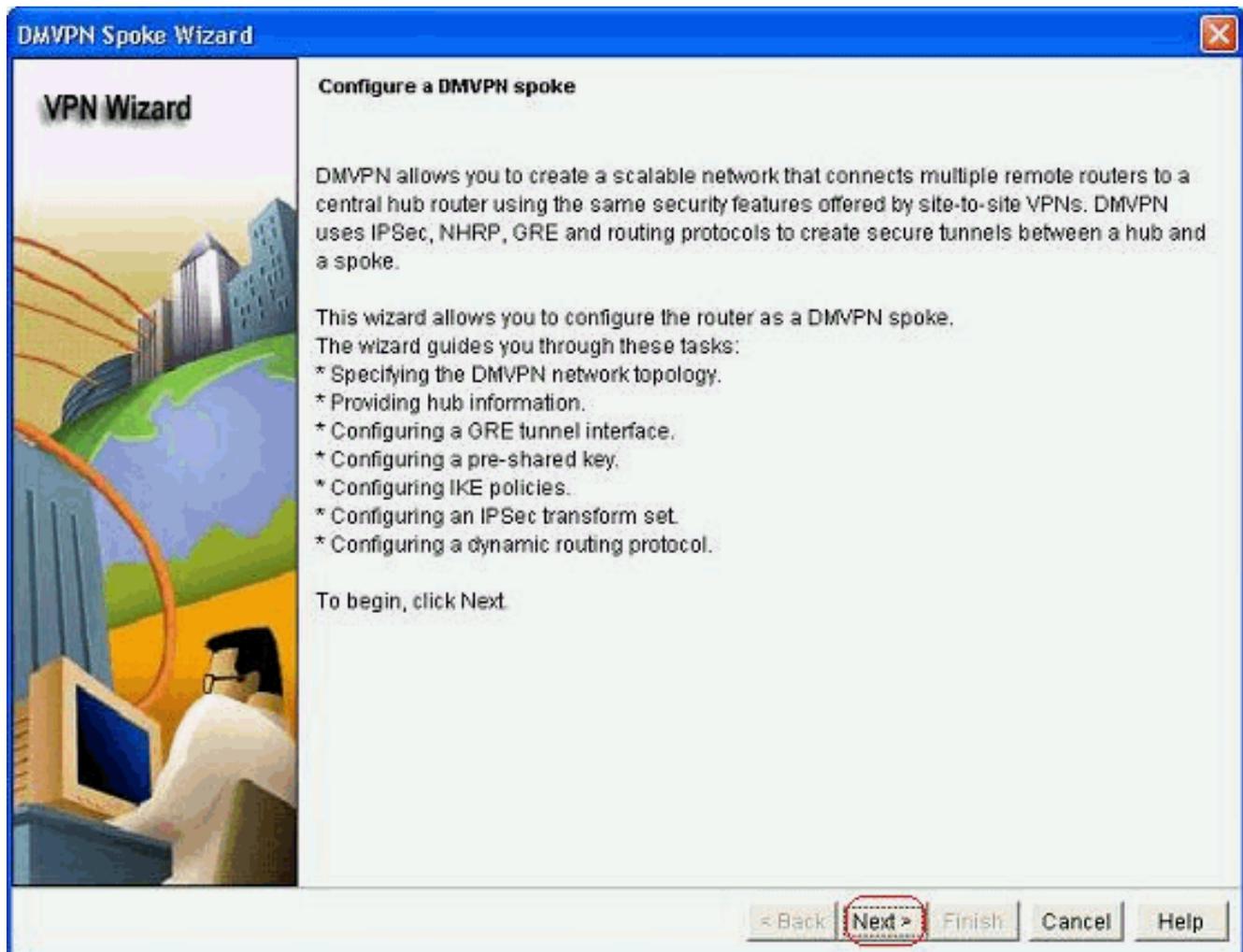
Cisco CPを使用したスポークの設定

このセクションでは、Cisco Configuration ProfessionalのDMVPNウィザードを使用して、スポークとしてルータを設定する方法を示します。

1. Cisco CPアプリケーションを起動してDMVPNウィザードを起動するには、[Configure] > [Security] > [VPN] > [Dynamic Multipoint VPN]に移動します。次に、[Create a spoke in a DMVPN]オプションを選択し、[Launch the selected task]をクリックします。



2. [次へ]をクリックして開始してください。



3. [ハブとスポーク]ネットワークオプションを選択し、[次へ]をクリックします。

VPN Wizard

DMVPN Network Topology

Select the DMVPN network topology.

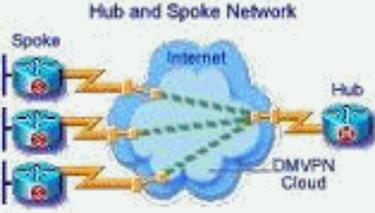
Hub and Spoke network

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.



The diagram, titled "Hub and Spoke Network", shows three "Spoke" routers on the left and one "Hub" router on the right. All routers are connected to a central "DMVPN Cloud" (represented by a blue cloud). The spokes are connected to the cloud via orange arrows, and the hub is also connected to the cloud via an orange arrow. The cloud is labeled "Internet" and "DMVPN Cloud".

< Back **Next >** Finish Cancel Help

4. ハブルータのパブリックインターフェイスやハブルータのトンネルインターフェイスなど、ハブ関連情報を指定します。

VPN Wizard

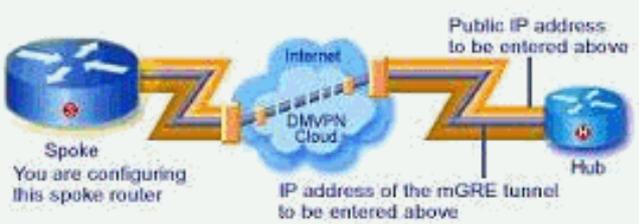
Specify Hub Information

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

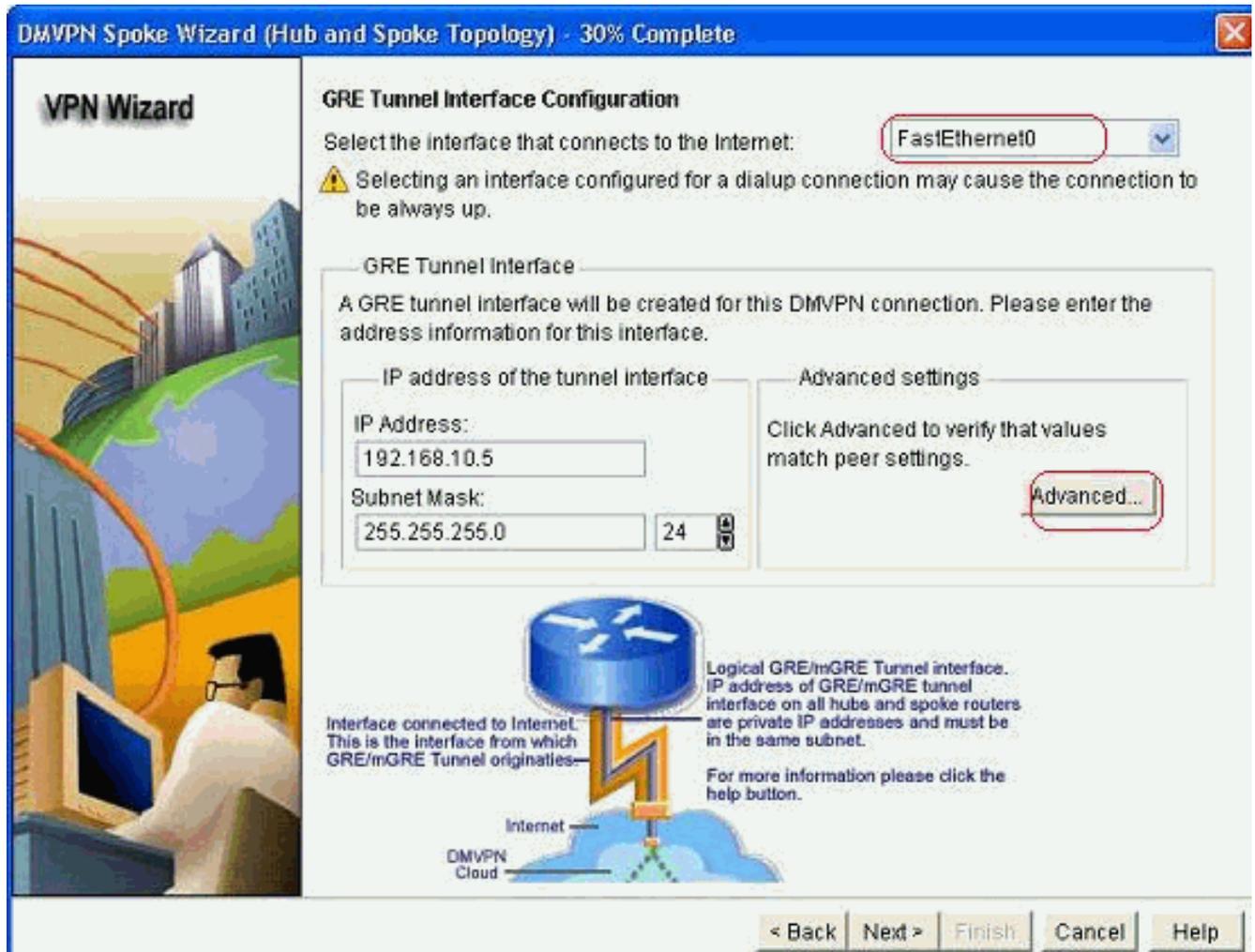
IP address of hub's physical interface: 209.165.201.2

IP address of hub's mGRE tunnel interface: 192.168.10.2

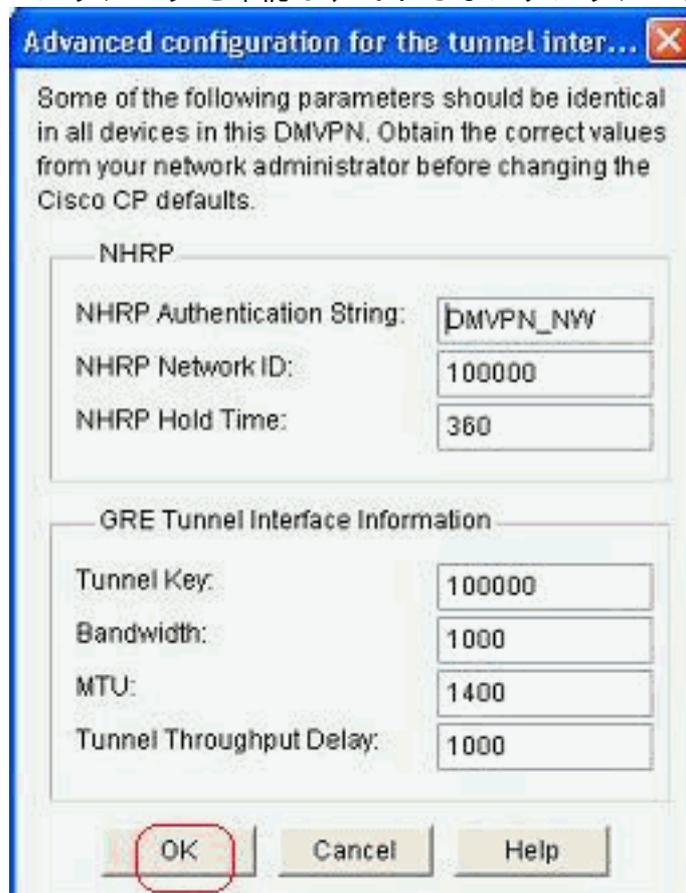


< Back | **Next >** | Finish | Cancel | Help

5. スポークのトンネルインターフェイスの詳細と、スポークのパブリックインターフェイスを指定します。次に、[詳細]をクリックします。



6. トンネルパラメータとNHRPパラメータを確認し、それらがハブパラメータに完全に一致し



ていることを確認します。

7. 事前共有キーを指定し、[次へ]をクリックします。



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

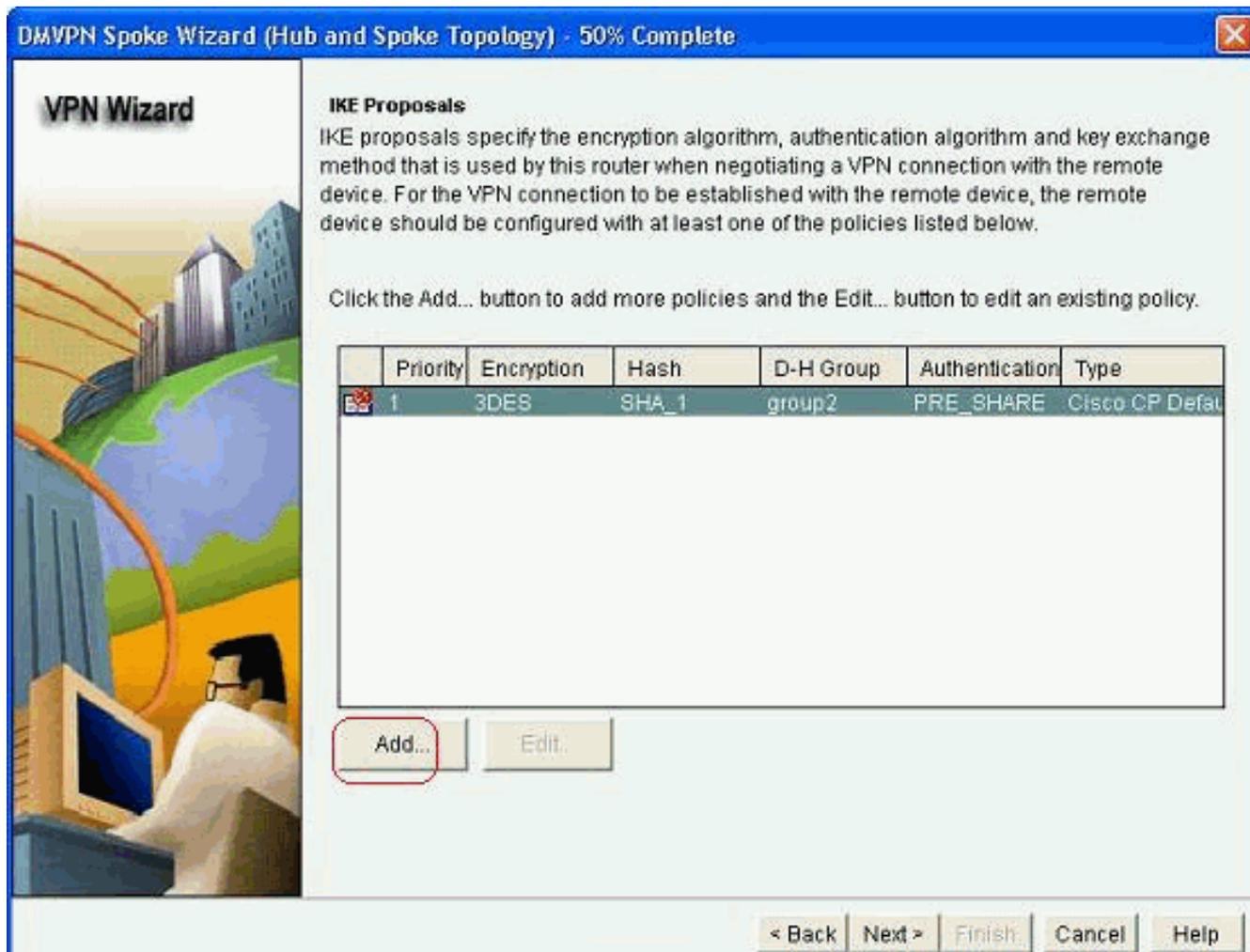
Pre-shared Keys

pre-shared key:

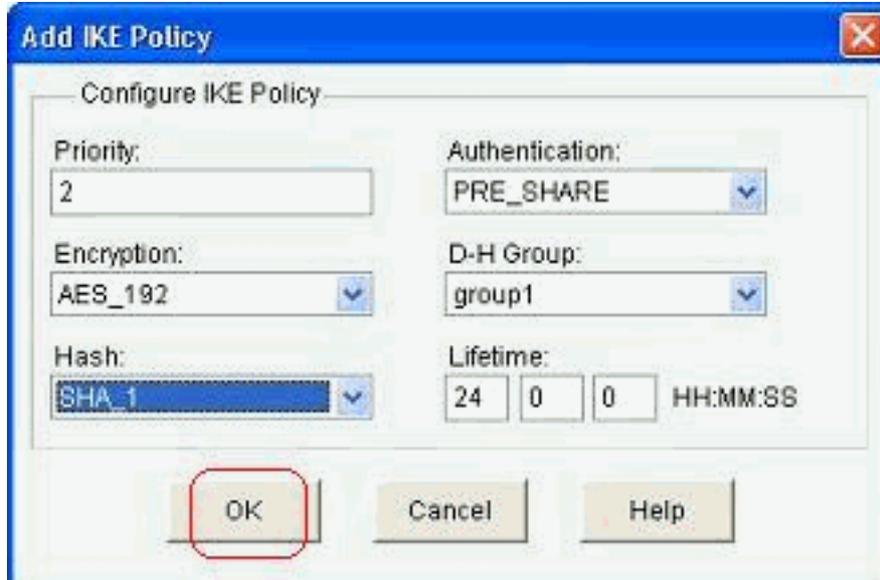
Reenter key:

< Back **Next >** Finish Cancel Help

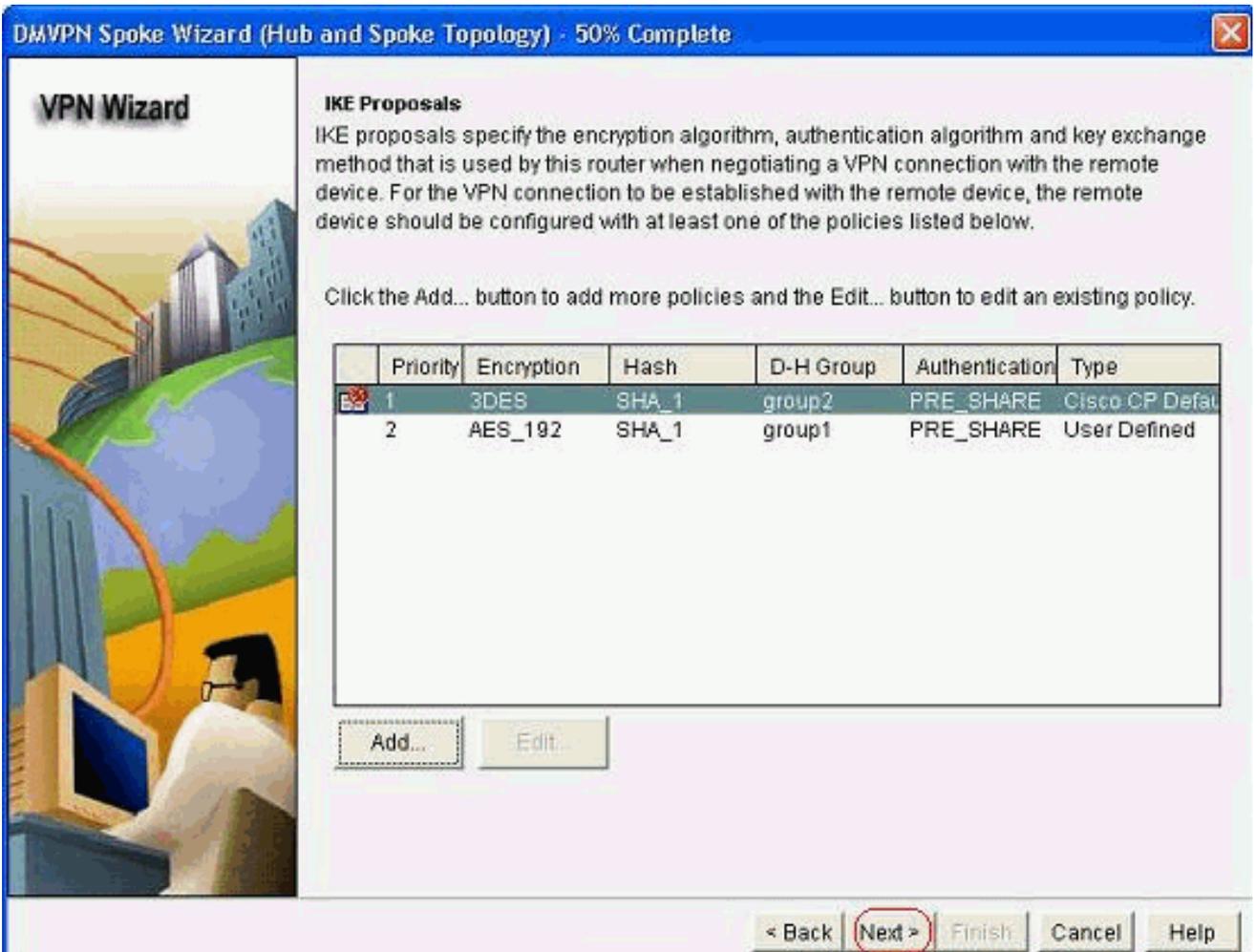
8. 別のIKEプロポーザルを追加するには、[Add]をクリックします。



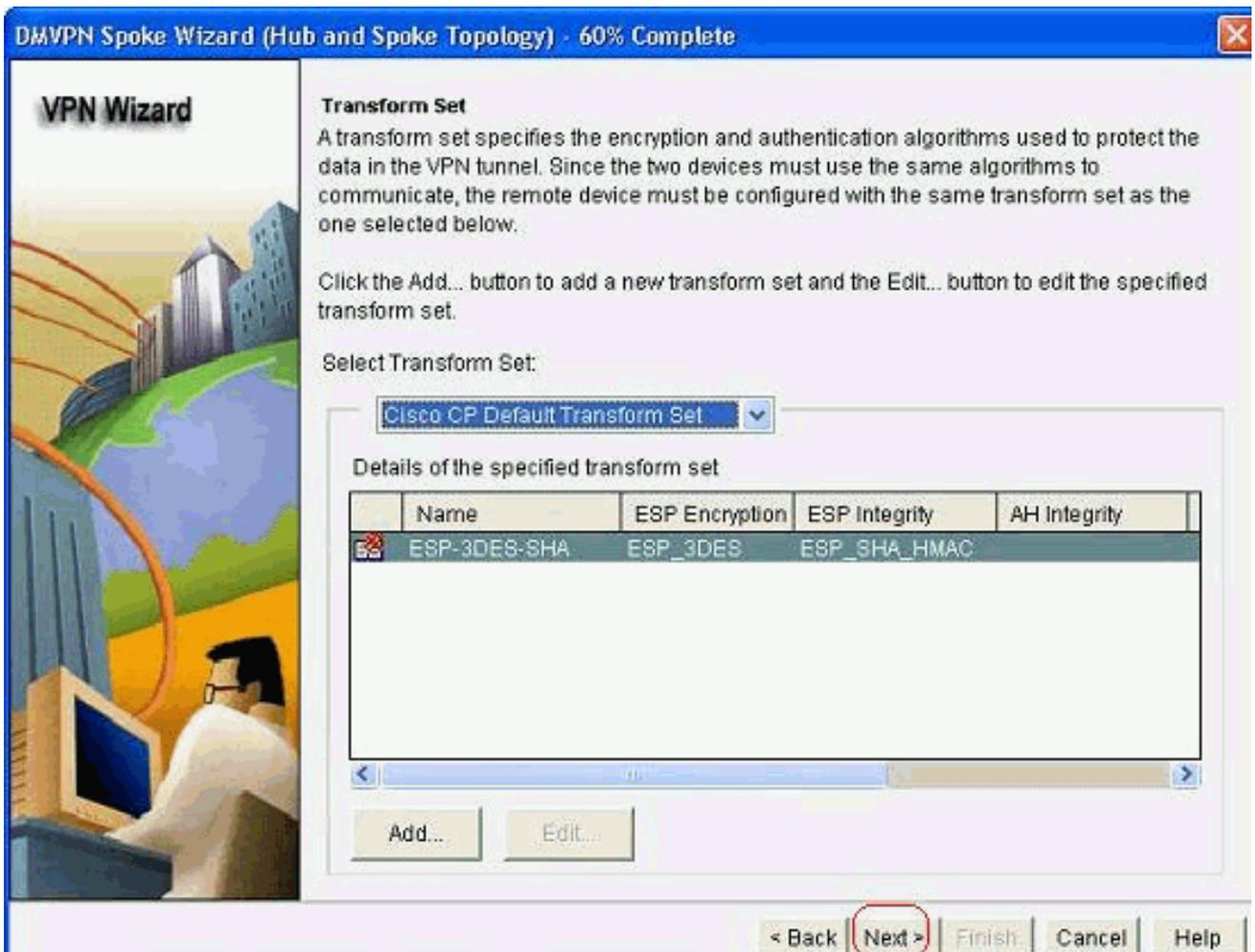
9. 暗号化、認証、およびハッシュパラメータを指定します。次に、[OK] をクリックします。



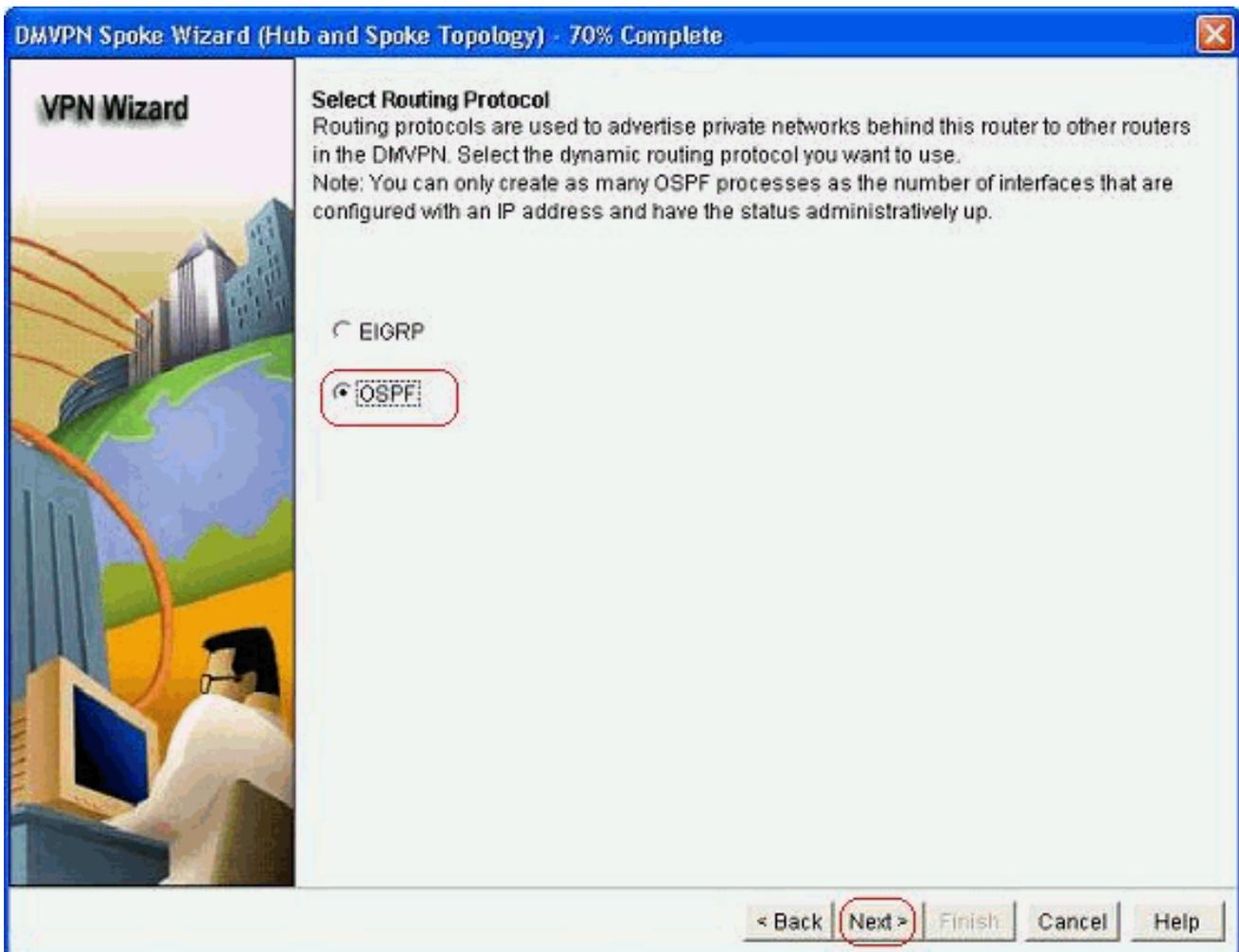
10. 新しく作成されたIKEポリシーは、ここで確認できます。[next] をクリックします。



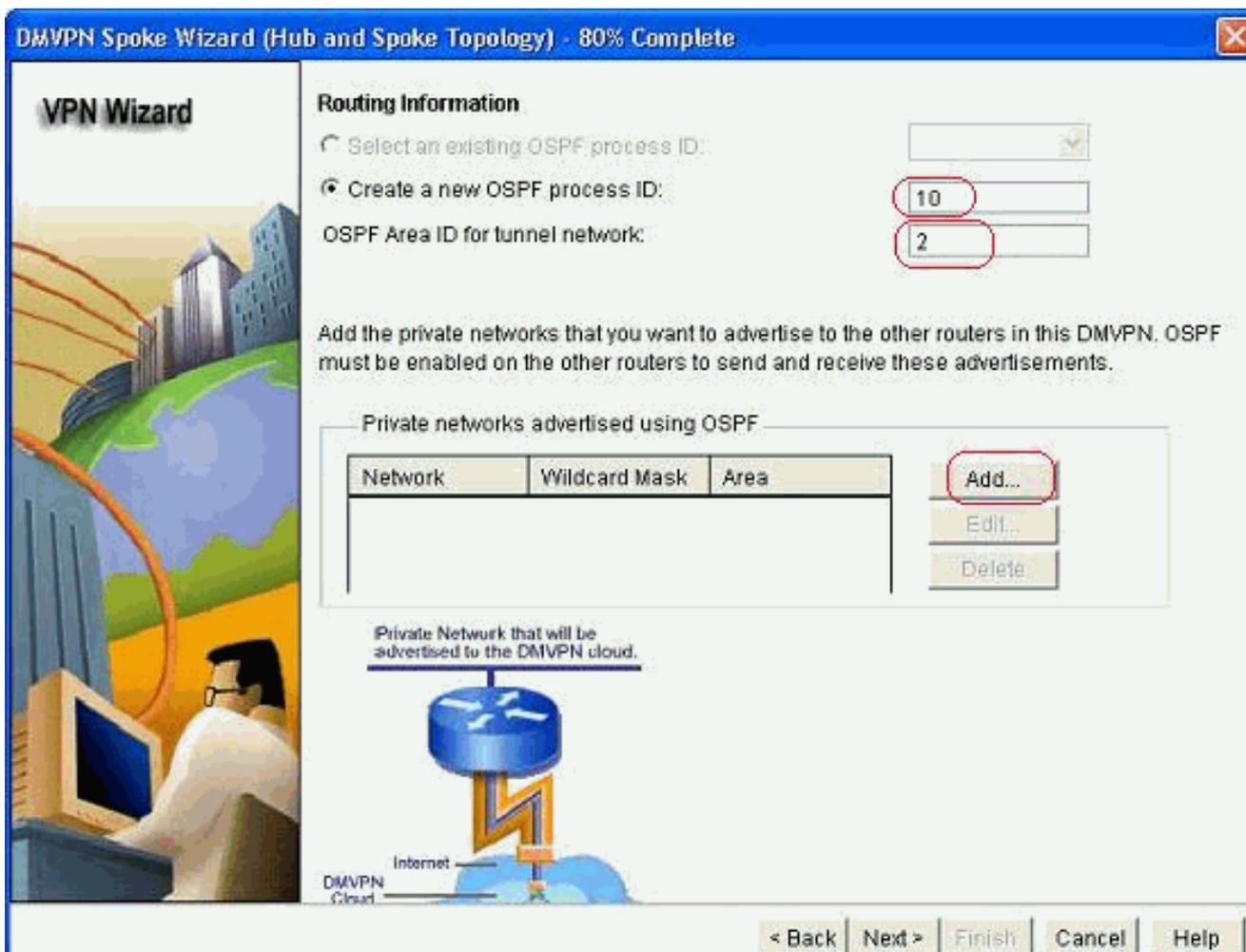
11. [次へ]をクリックし、デフォルトトランスフォームセットを続行します。



12. 必要なルーティングプロトコルを選択します。ここでは、OSPFが選択されています。



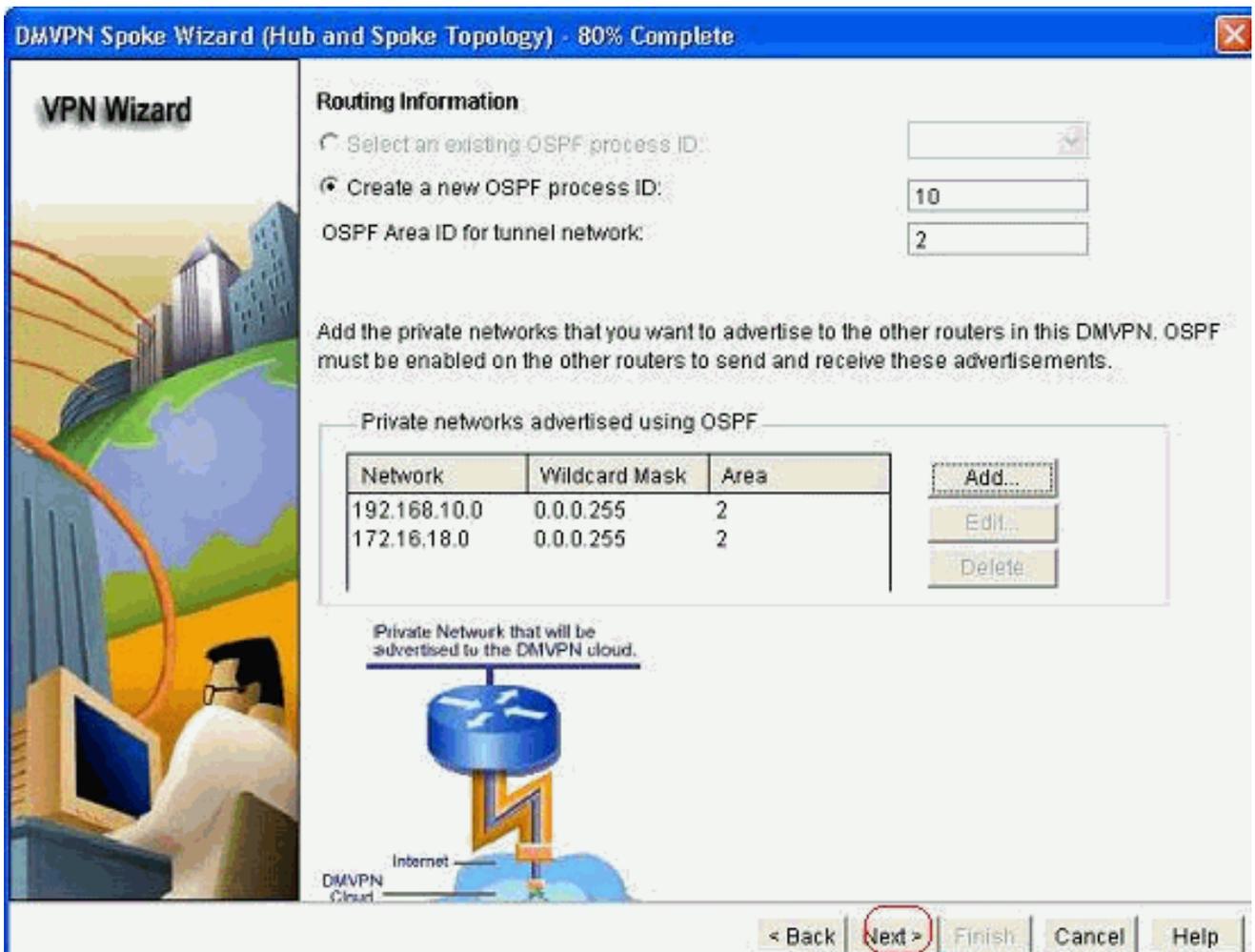
13. OSPFプロセスIDとエリアIDを指定します。[Add] をクリックして、OSPFによってアドバタイズされるネットワークを追加します。



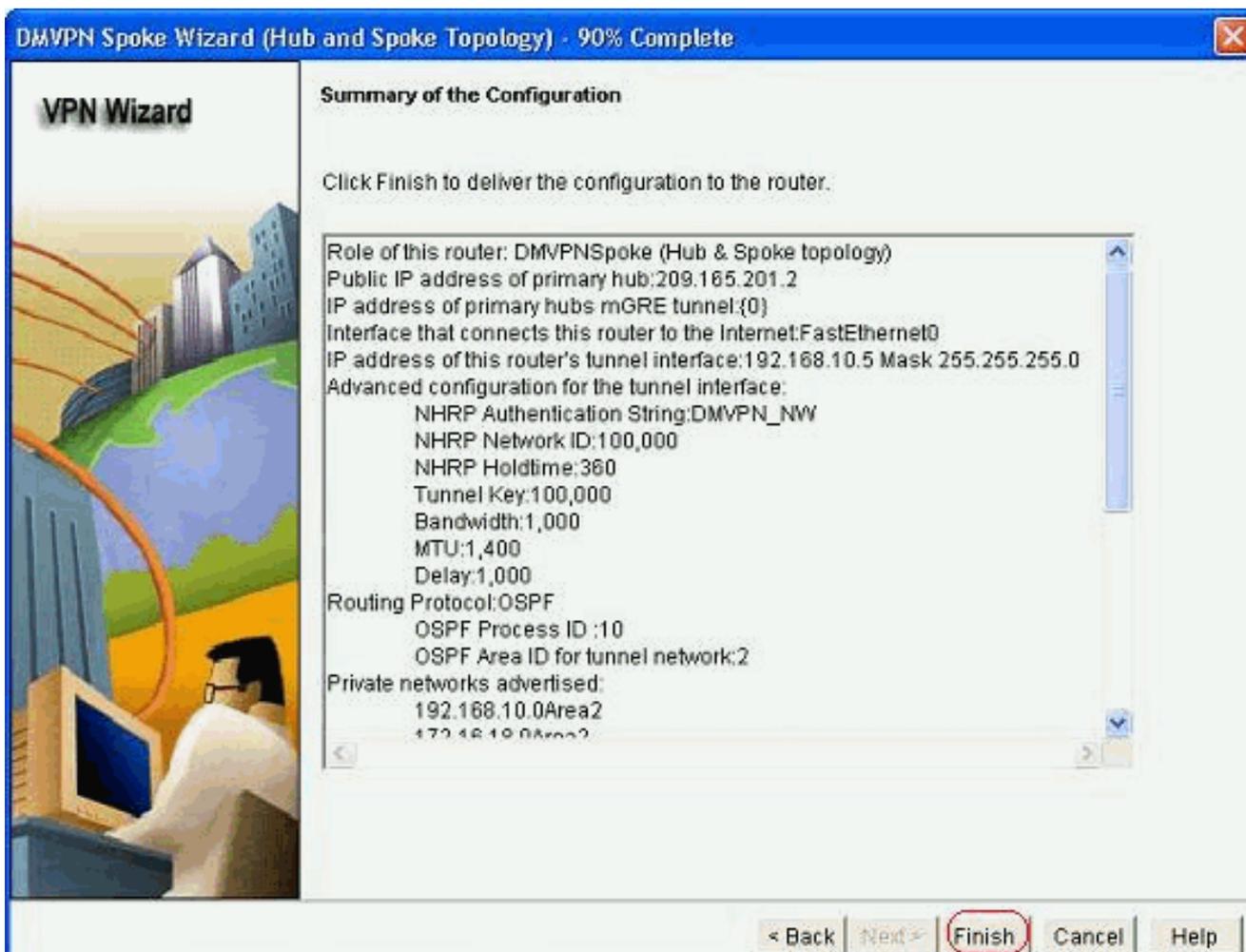
14. トンネルネットワークを追加し、[OK]をクリックします。



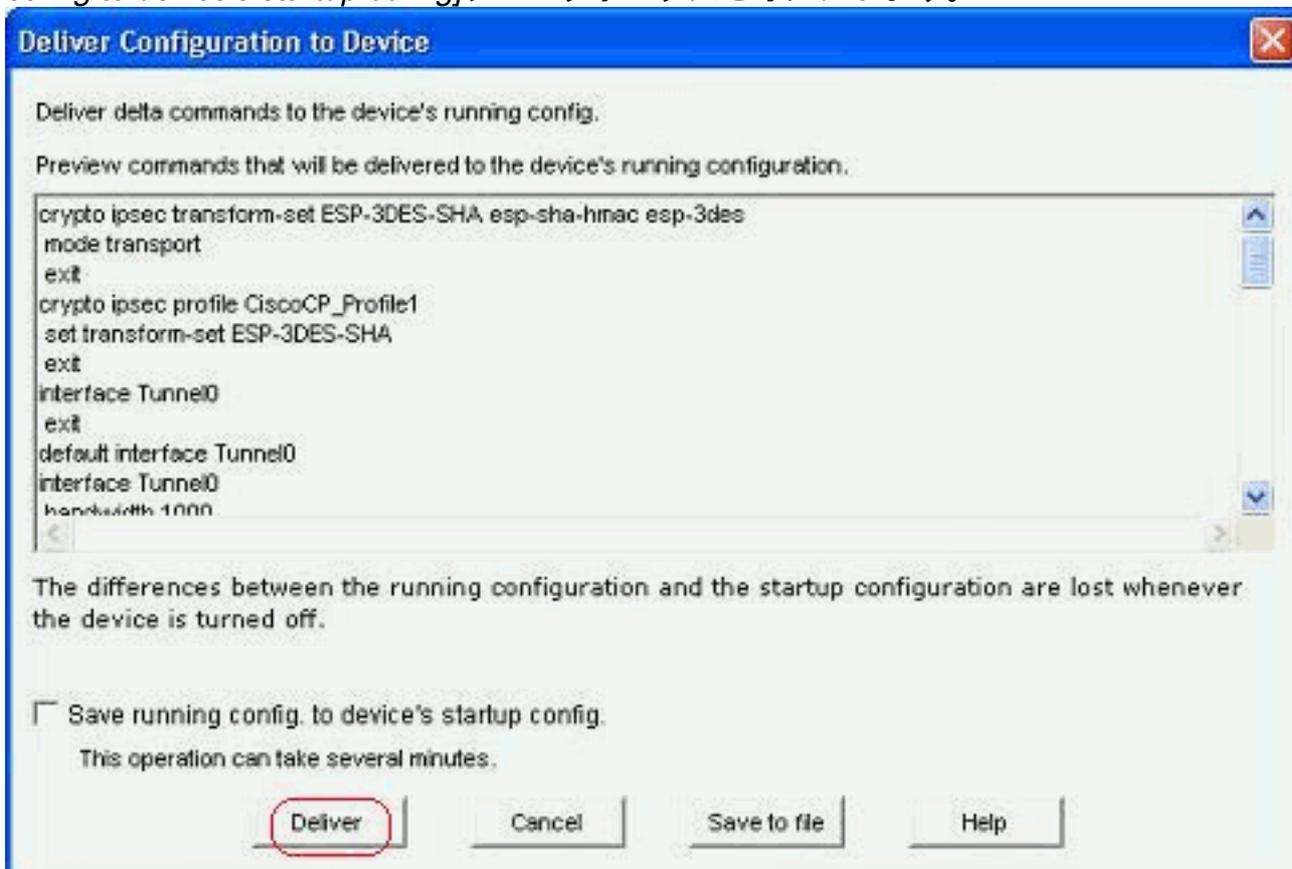
15. スポークルータの背後にプライベートネットワークを追加します。次に、[Next] をクリックします。



16. [完了]をクリックして、ウィザードの構成を完了します。



17. 「配信」をクリックして、コマンドを実行します。設定を保存する場合は、[Save running config to device's startup config]チェックボックスをオンにします。



関連するCLI設定を次に示します。

スポーク ルータ

```
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
```

Cisco CPを使用したハブの設定

このセクションでは、DMVPN用にハブルータを設定する方法を段階的に説明します。

1. [Configure] > [Security] > [VPN] > [Dynamic Multipoint VPN]に移動し、[Create a hub in a DMVPN]オプションを選択します。で、[選択したタスクの起動]をクリックします。



Create Dynamic Multipoint VPN (DMVPN)

Edit Dynamic Multipoint VPN (DMVPN)

 Create a spoke (client) in a DMVPN

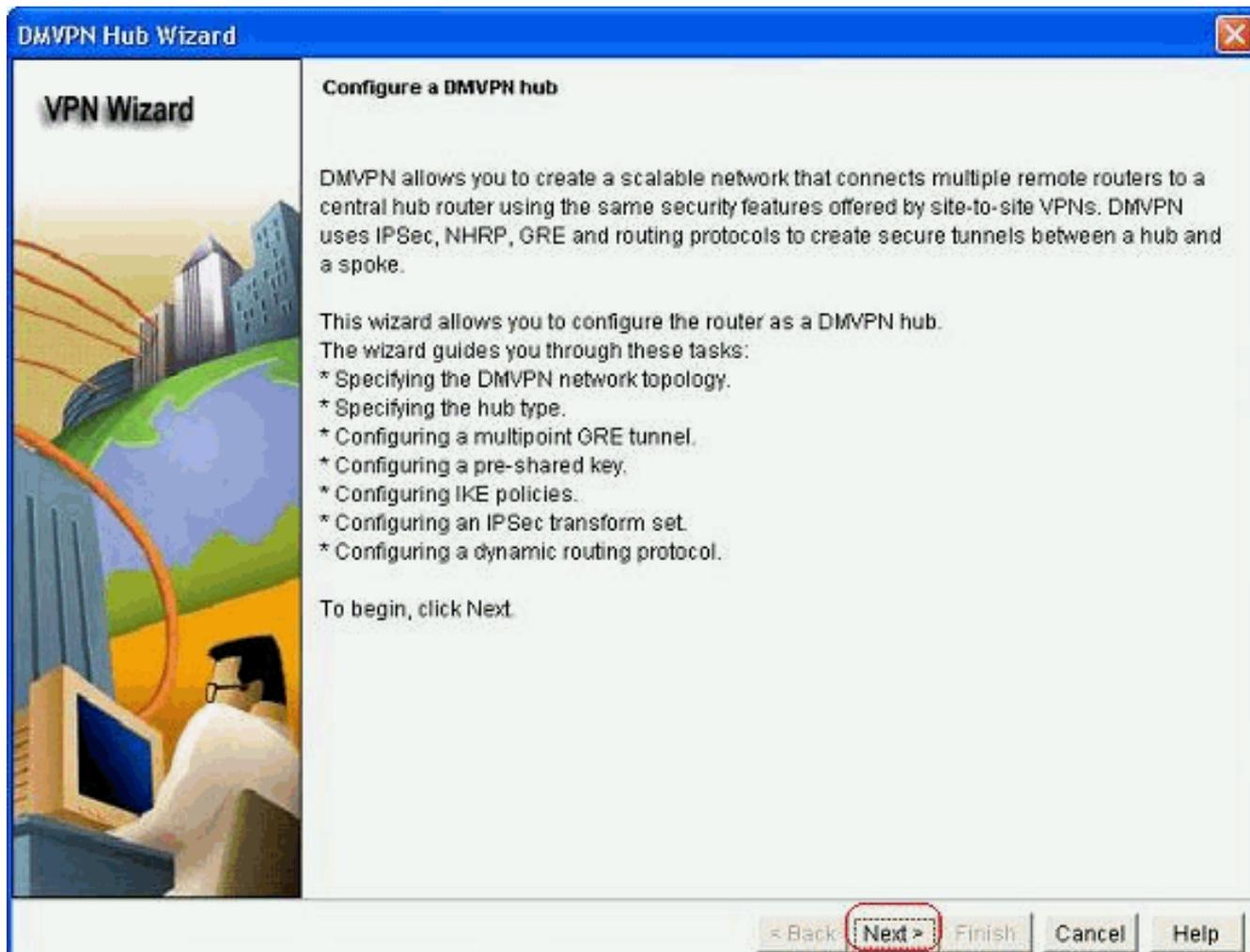
Use this option to configure the router as a spoke in a full mesh or hub and spoke network topology. To complete this configuration, you must know the hub's IP address, NHRP information, pre-shared key, IKE policy, IPsec Transform set and dynamic routing protocol information.

 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.

Launch the selected task

2. [next] をクリックします。



3. [ハブとスポーク]ネットワークオプションを選択し、[次へ]をクリックします。

VPN Wizard



DMVPN Network Topology

Select the DMVPN network topology.

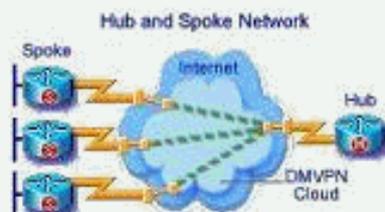
Hub and Spoke network

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

4. [プライマリハブ]を選択します。次に、[Next] をクリックします。

VPN Wizard



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)

< Back **Next >** Finish Cancel Help

5. トンネルインターフェイスのパラメータを指定し、[Advanced]をクリックします。

VPN Wizard

Multipoint GRE Tunnel Interface Configuration

Select the interface that connects to the Internet:

⚠ 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.

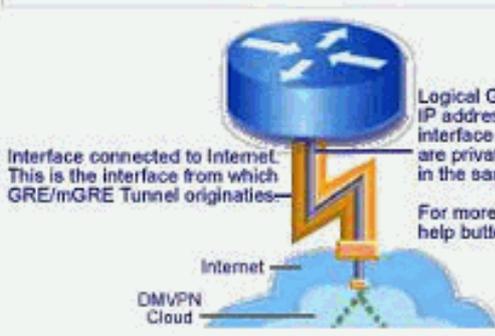
IP address of the tunnel interface

IP Address:

Subnet Mask:

Advanced settings

Click Advanced to verify that values match peer settings.



6. トンネルパラメータとNHRPパラメータを指定します。次に、[OK] をクリックします。

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

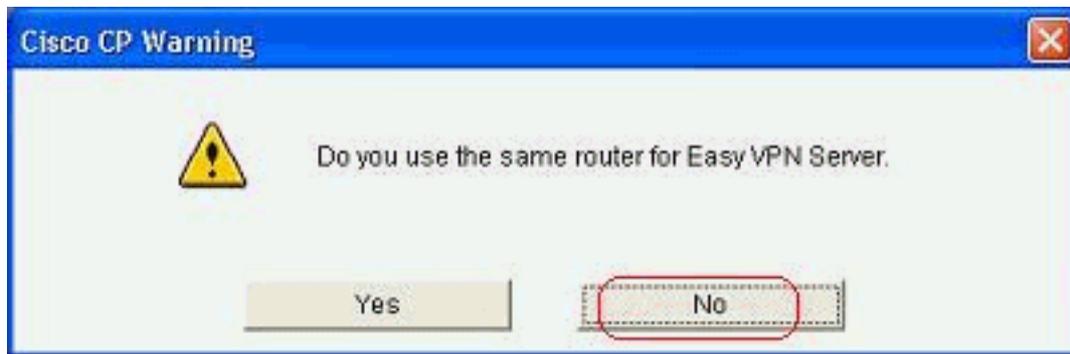
Tunnel Key:

Bandwidth:

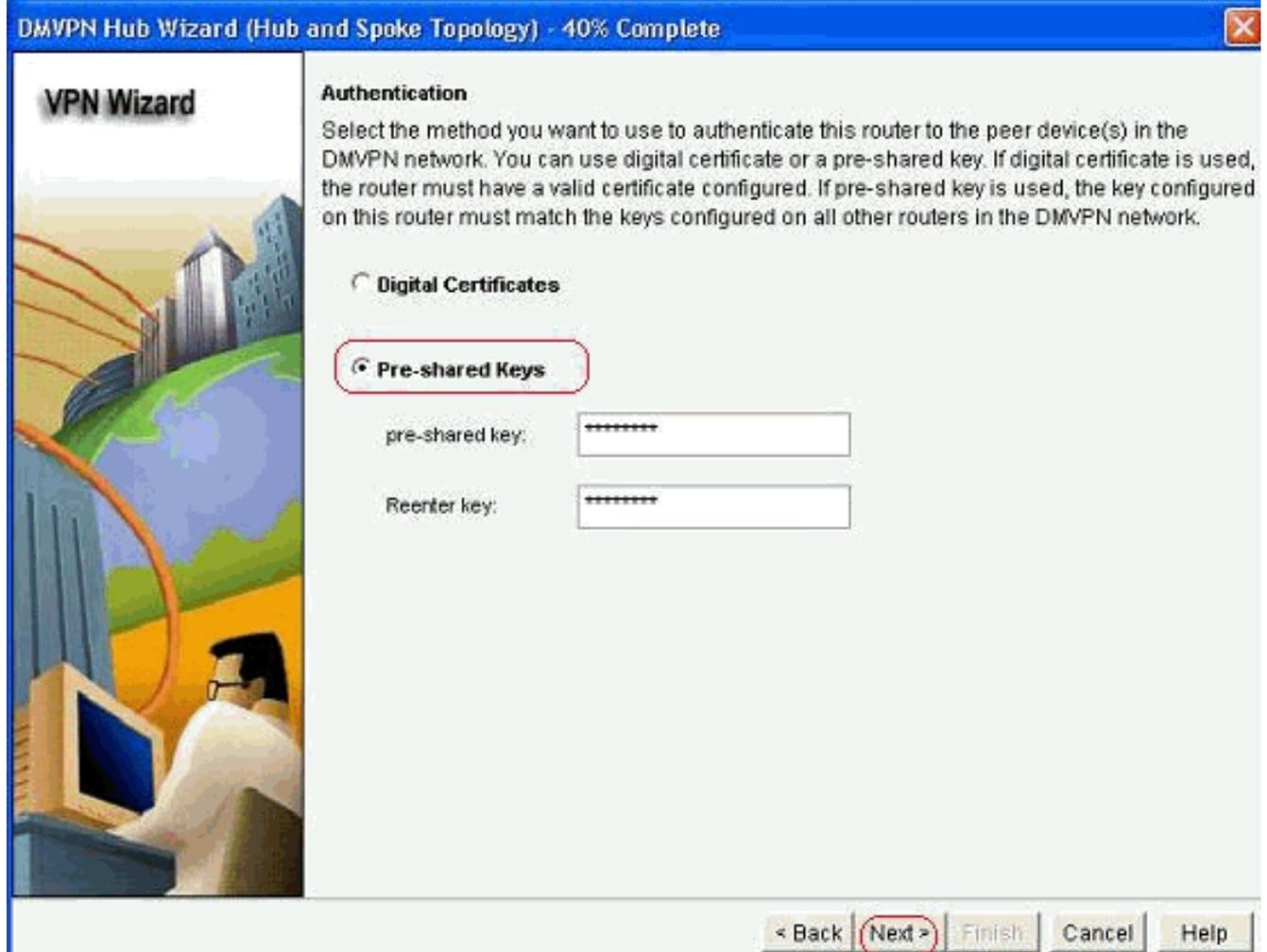
MTU:

Tunnel Throughput Delay:

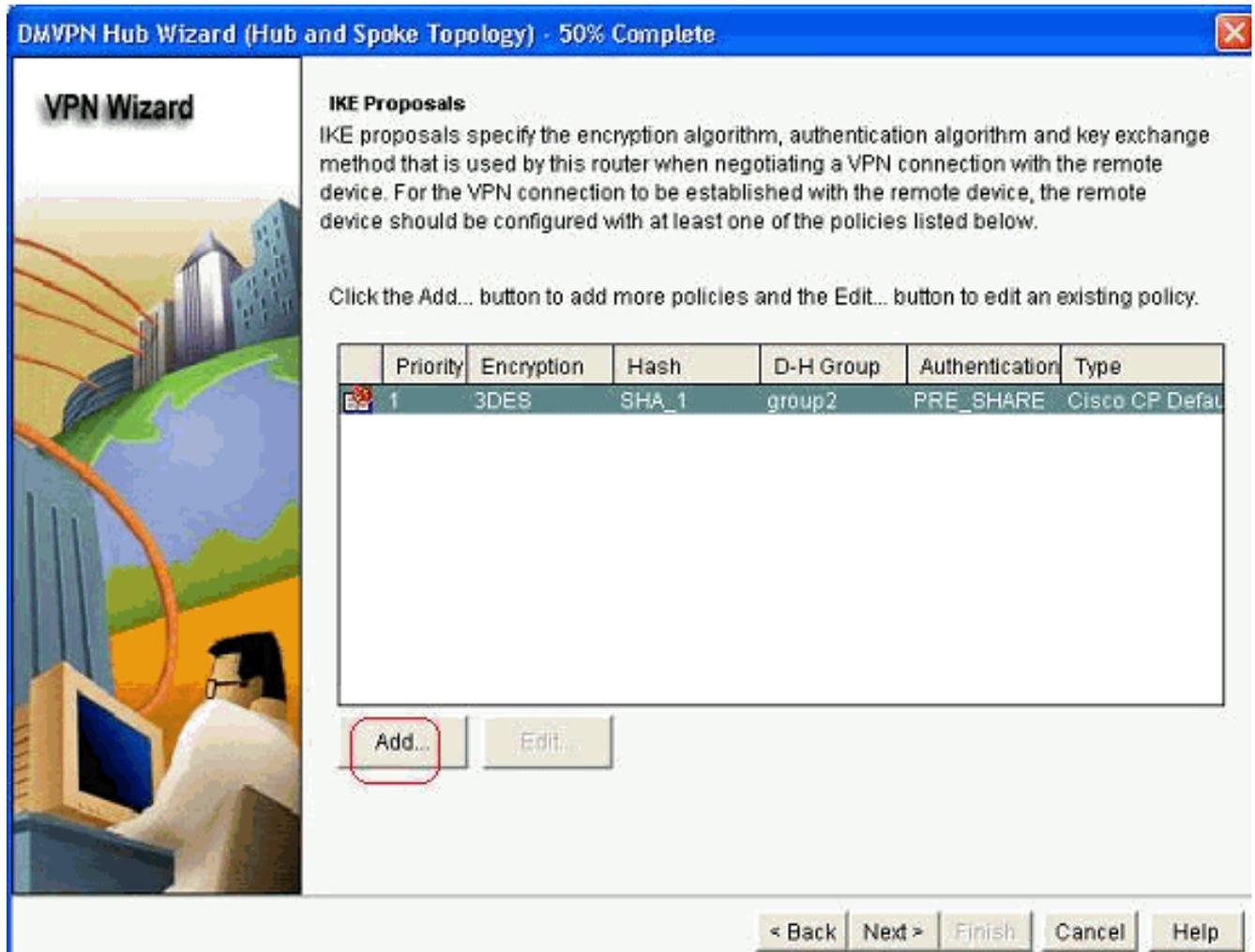
7. ネットワーク設定に基づいてオプションを指定します。



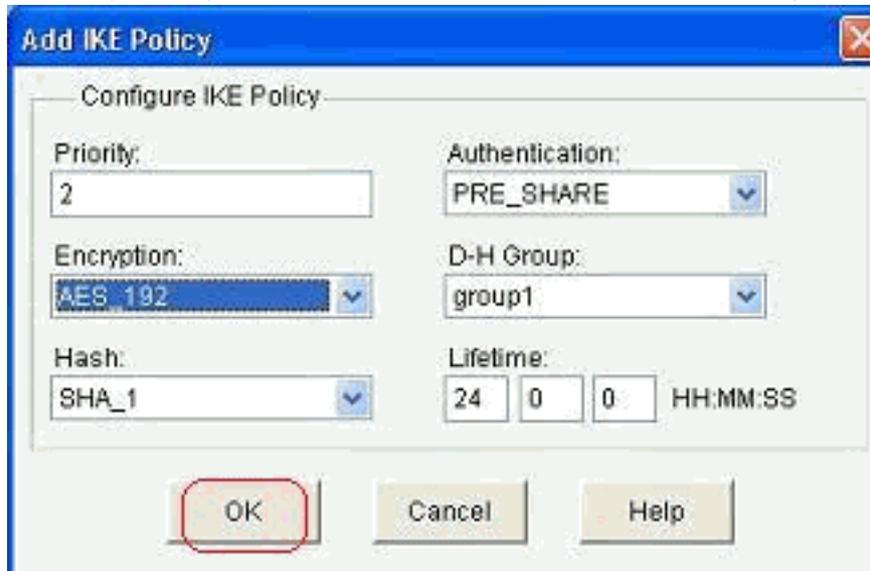
8. [事前共有キー]を選択し、事前共有キーを指定します。次に、[Next] をクリックします。



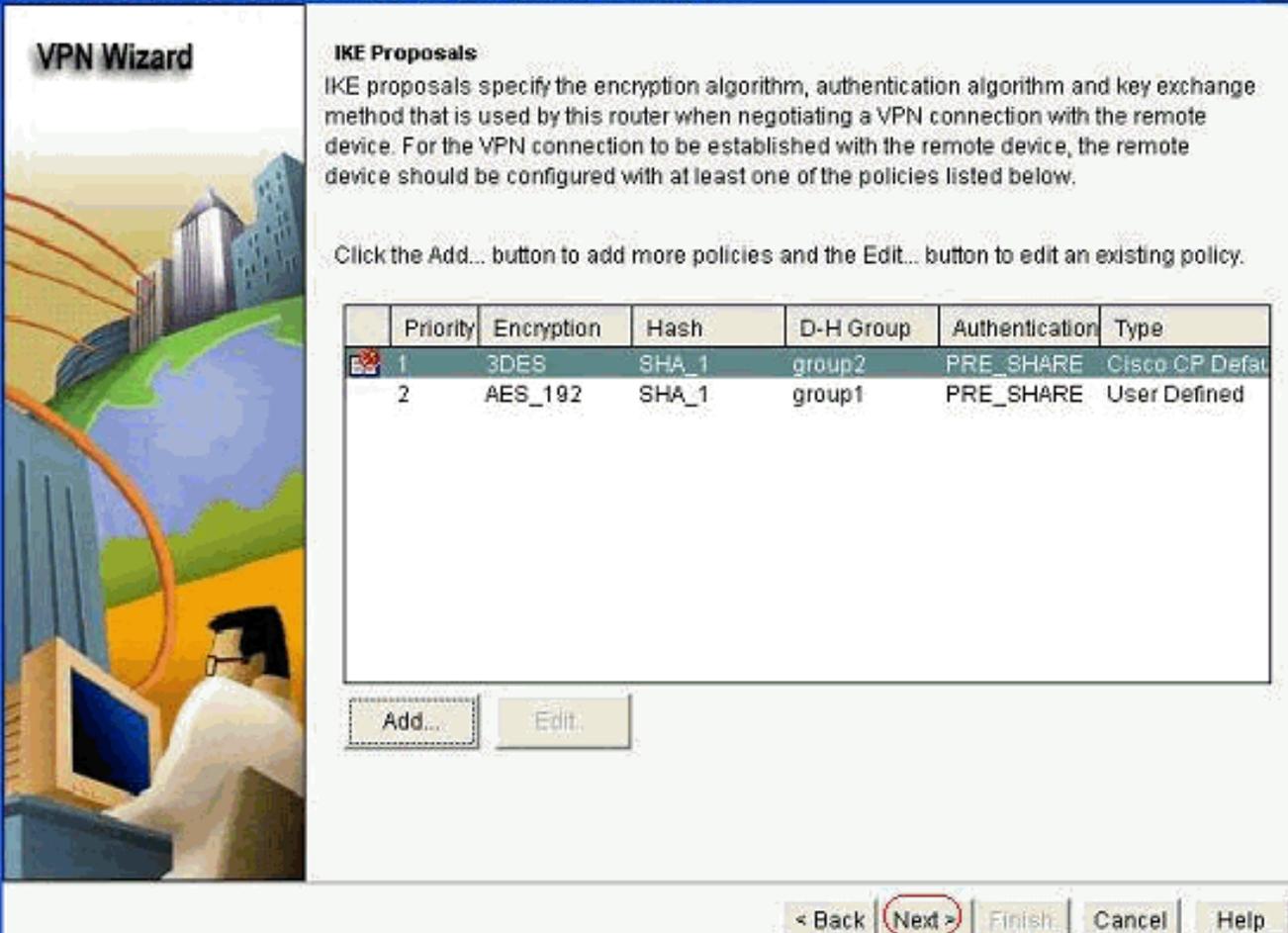
9. 別のIKEプロポーザルを追加するには、[Add]をクリックします。



10. 暗号化、認証、およびハッシュパラメータを指定します。次に、[OK] をクリックします。



11. 新しく作成されたIKEポリシーは、ここで確認できます。[next] をクリックします。



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.

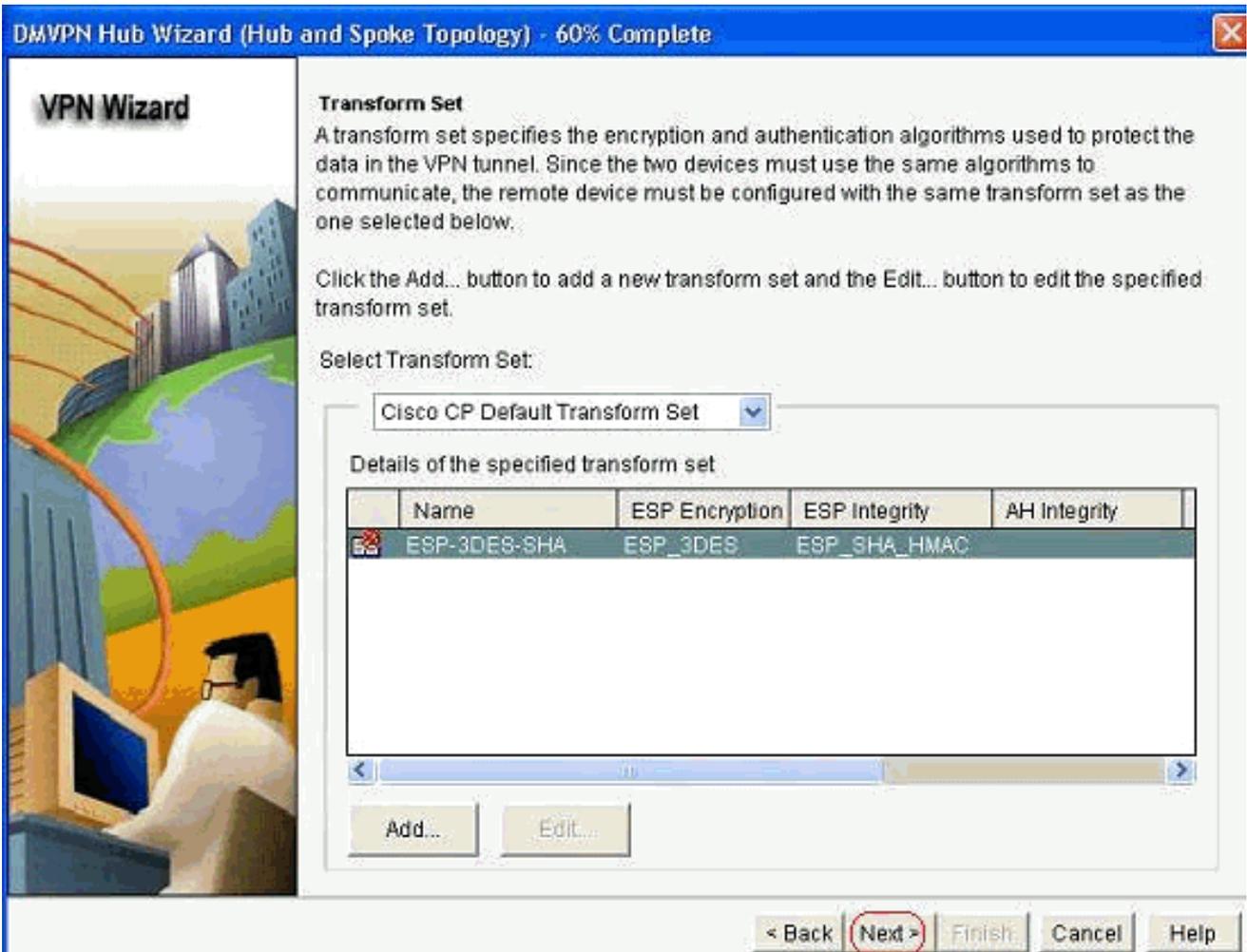
Click the Add... button to add more policies and the Edit... button to edit an existing policy.

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

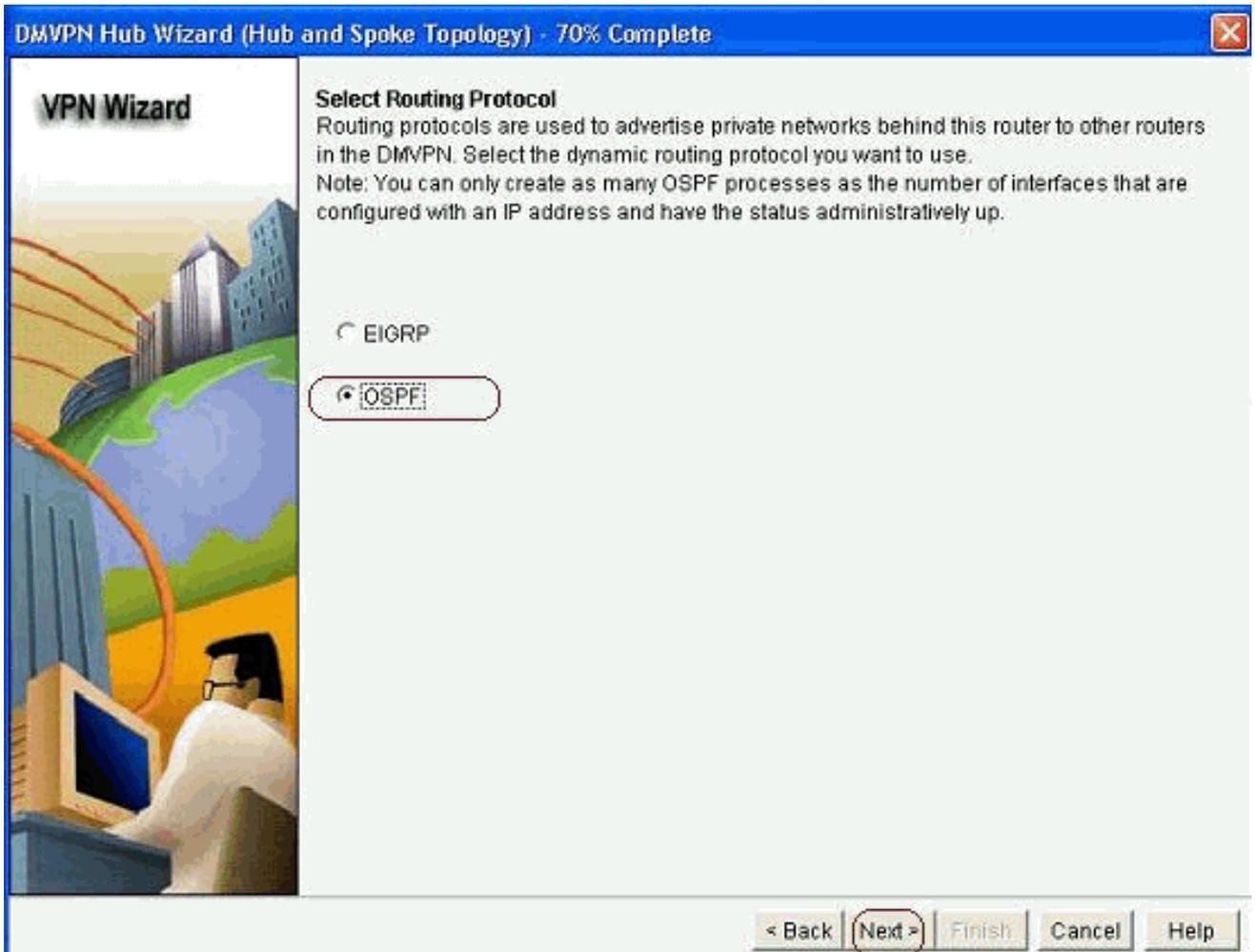
Add... Edit...

< Back **Next >** Finish Cancel Help

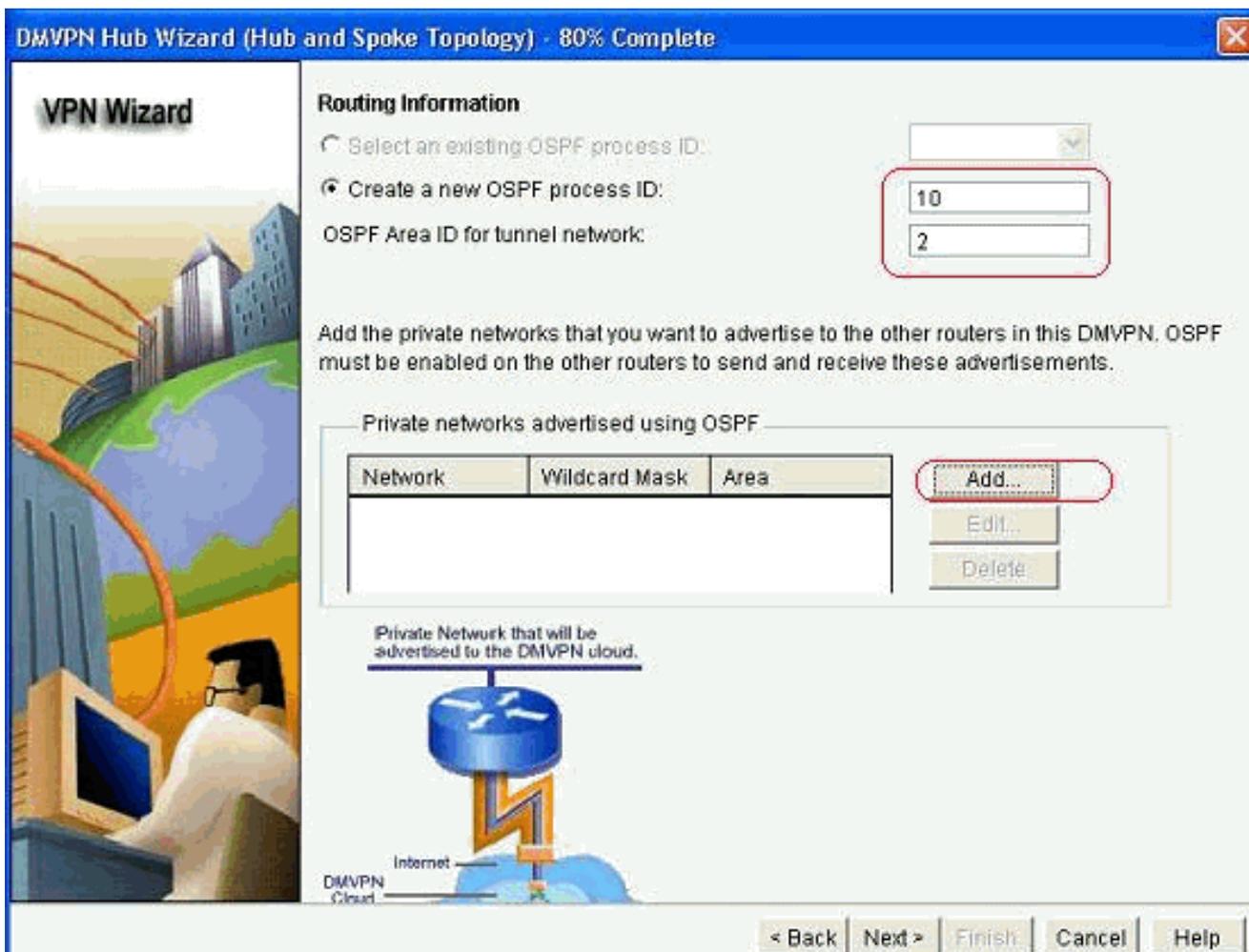
12. [次へ]をクリックし、デフォルトトランスフォームセットを続行します。



13. 必要なルーティングプロトコルを選択します。ここでは、OSPFが選択されています。



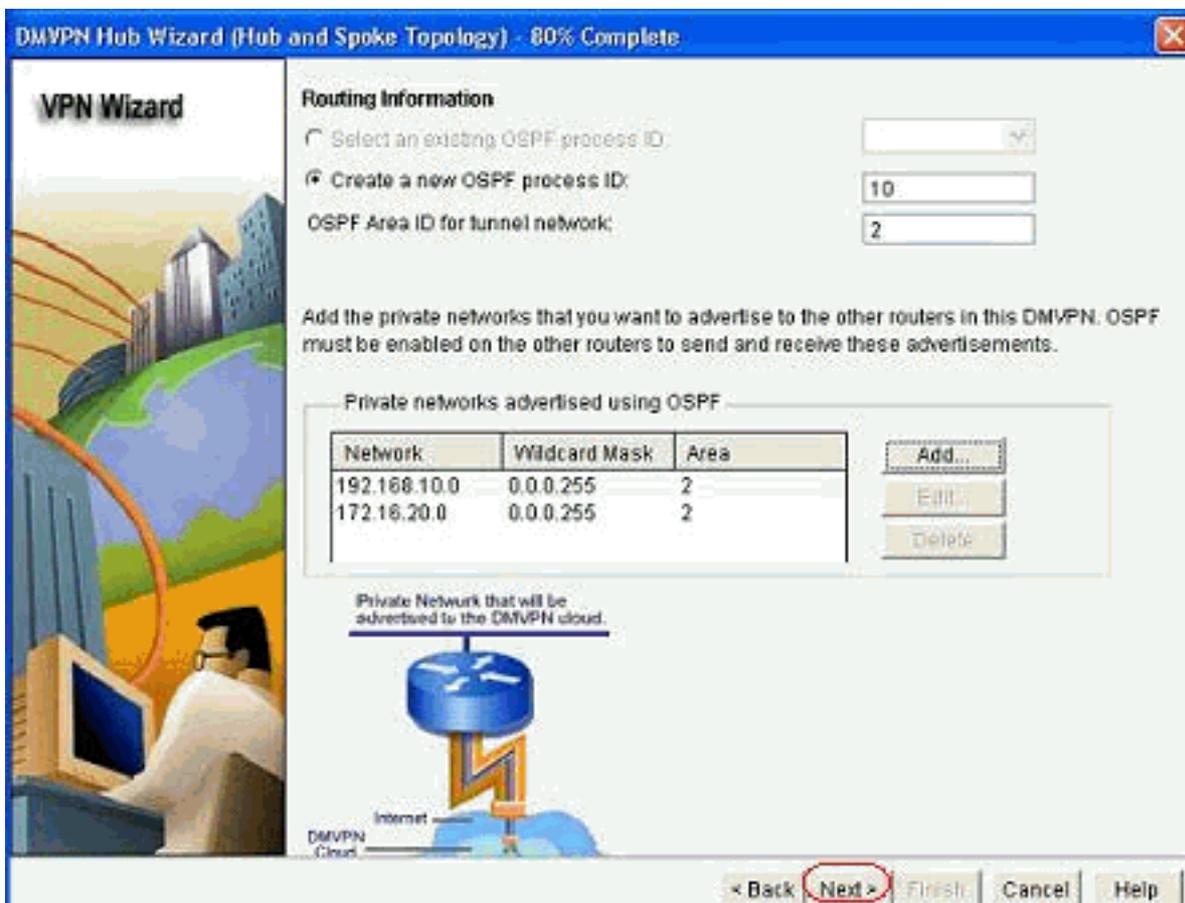
14. OSPFプロセスIDとエリアIDを指定します。[Add] をクリックして、OSPFによってアドバタイズされるネットワークを追加します。



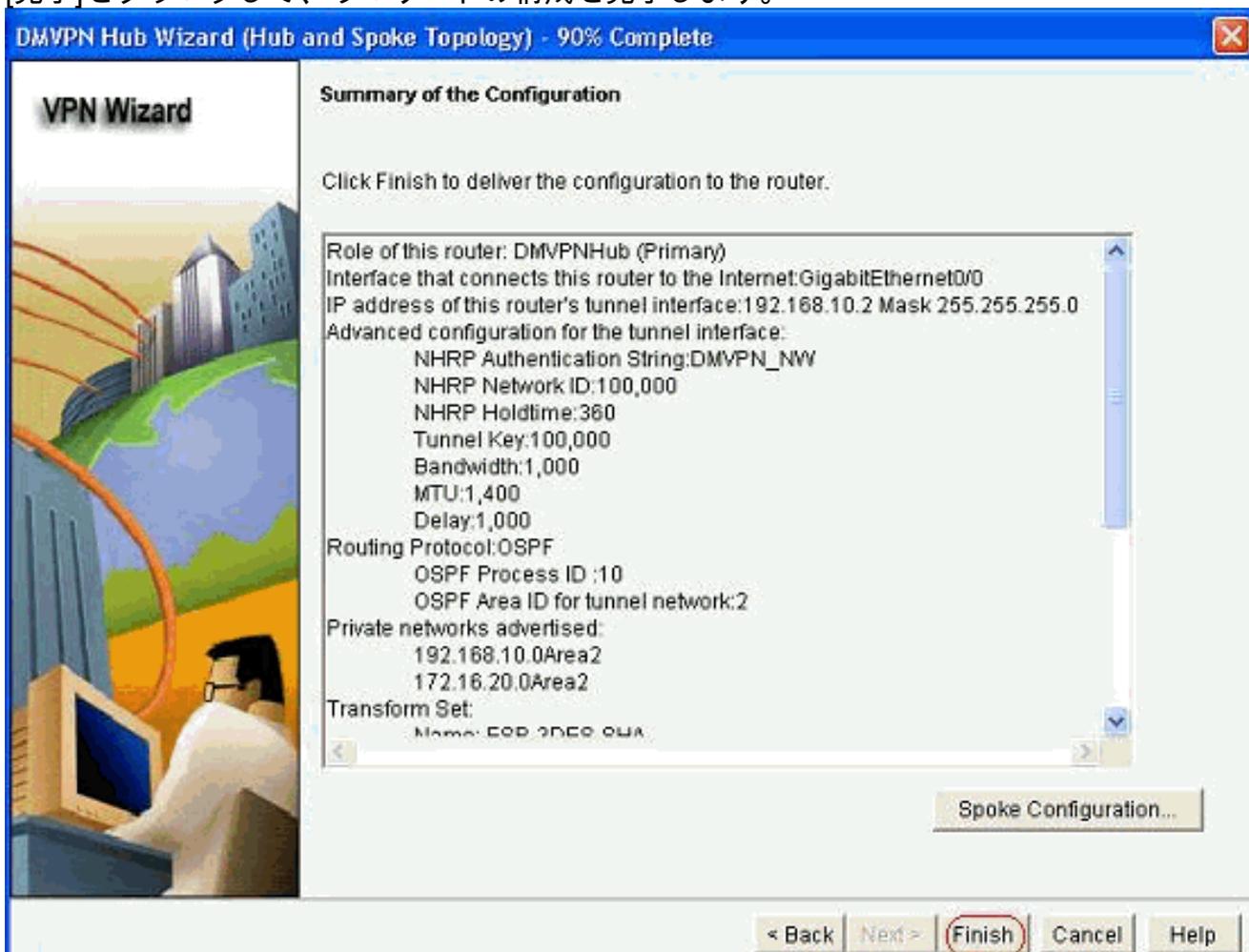
15. トンネルネットワークを追加し、[OK]をクリックします。



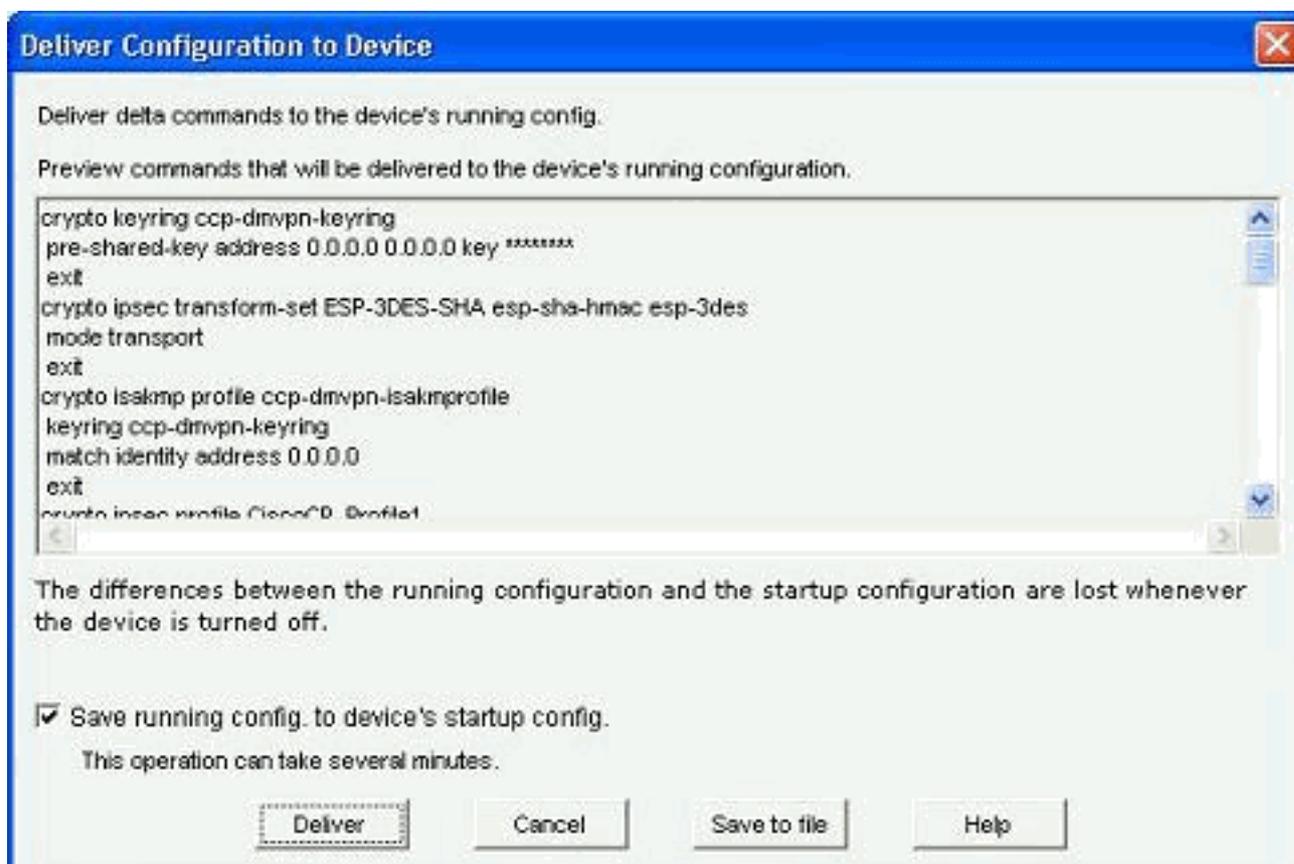
16. ハブルーターの背後にプライベートネットワークを追加し、[Next]をクリックします。



17. [完了]をクリックして、ウィザードの構成を完了します。



18. 「配信」をクリックして、コマンドを実行します。



ハブのCLI設定

関連するCLI設定を次に示します。

Hub ルータ
<pre>! 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</pre>

```

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
!

```

CCPを使用したDMVPN設定の編集

トンネルインターフェイスを選択して[Edit]をクリックすると、既存のDMVPNトンネルパラメータを手動で編集できます。

Configure > Security > VPN > Dynamic Multipoint VPN

VPN

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

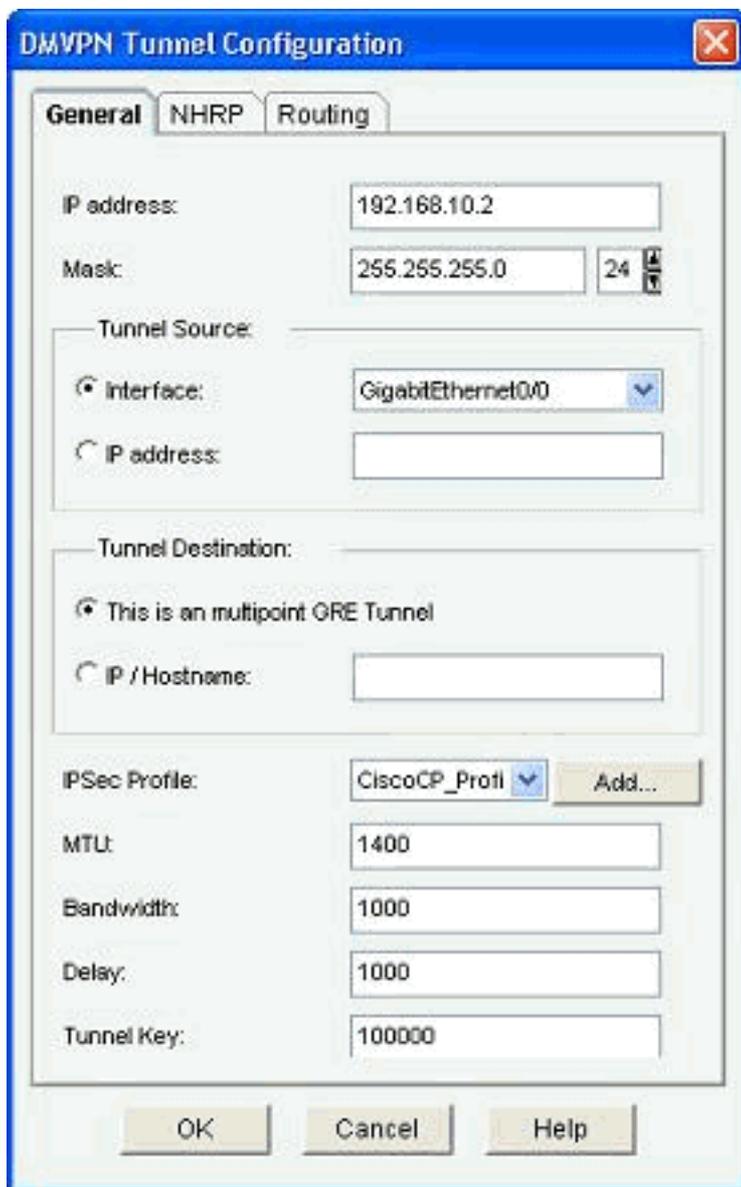
Add... **Edit...** Delete

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

MTUやトンネルキーなどのトンネルインターフェイスパラメータは、[General]タブで変更されます。



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 menu 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 menu) 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. NHRP関連のパラメータは、[NHRP]タブの要件に従って検索および変更されます。スポークルータでは、ハブルータのIPアドレスとしてNHSを表示できます。NHRPマッピングを追加するには、[NHRP Map]セクションで[Add]をクリックします。

DMVPN Tunnel Configuration

General **NHRP** Routing

Authentication String: DMVPN_NW

Hold Time: 360

Network ID: 100000

Next Hop Servers

Next Hop Servers

Add
Delete

NHRP Map

Destination	Mask
<None>	<None>

Add
Edit
Delete

< | >

OK Cancel Help

2. ネットワーク設定に応じて、次に示すようにNHRPマッピングパラメータを設定できます。

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): 1
2

NBMA address directly reachable

IP Address:

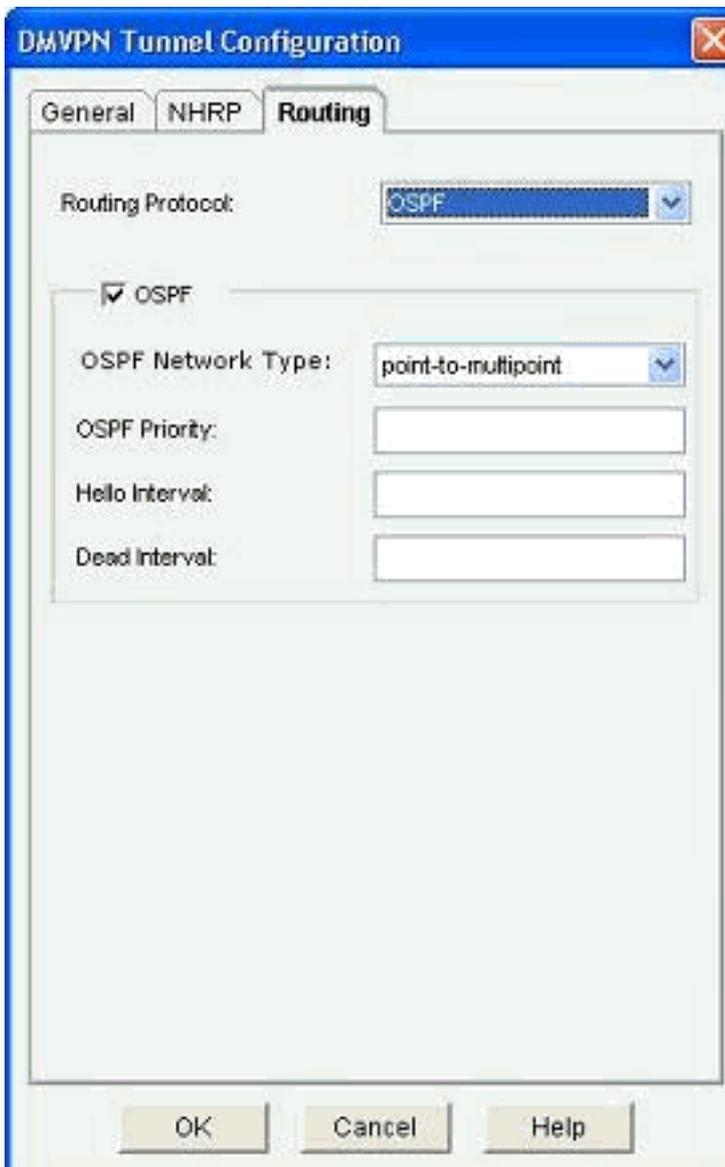
Configure NBMA addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network.

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

IP address of NBMA address directly reachable

OK Cancel Help

ルーティング関連のパラメータは、「ルーティング」(Routing)タブで表示および変更されます。



その他の情報

DMVPNトンネルは、次の2つの方法で設定します。

- ハブを介したスポーク間の通信
- ハブを使用しないスポーク間の通信

このドキュメントでは、最初の方法についてのみ説明します。スポーク間のダイナミックIPSecトンネルの確立を可能にするには、次のアプローチを使用してスポークをDMVPNクラウドに追加します。

1. DMVPNウィザードを起動し、[スポークの構成]オプションを選択します。
2. [DMVPN Network Topology]ウィンドウから、[Hub and Spoke network]オプションの代わりに[Full mesh network]オプションを選択してください。

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. このドキュメントの他の設定と同じ手順を使用して、残りの設定を完了します。

確認

現在、この設定に使用できる確認手順はありません。

関連情報

- [Cisco Dynamic Multipoint VPN:シンプルでセキュアなブランチ間通信](#)
- [IOS 12.2 Dynamic Multipoint VPN\(DMVPN\)](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)