

Cisco IOS/CCP - Cisco CP로 DMVPN 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[Cisco CP를 사용한 스포크 구성](#)

[스포크에 대한 CLI 컨피그레이션](#)

[Cisco CP를 사용한 허브 컨피그레이션](#)

[허브에 대한 CLI 컨피그레이션](#)

[CCP를 사용하여 DMVPN 컨피그레이션 수정](#)

[추가 정보](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 Cisco CP(Configuration Professional)를 사용하여 허브와 스포크 라우터 간 DMVPN(Dynamic Multipoint VPN) 터널의 샘플 컨피그레이션을 제공합니다. Dynamic Multipoint VPN은 GRE, IPSec 암호화, NHRP 및 라우팅과 같은 다양한 개념을 통합하여 최종 사용자가 동적으로 생성된 스포크 투 스포크 IPSec 터널을 통해 효과적으로 통신할 수 있는 정교한 솔루션을 제공하는 기술입니다.

사전 요구 사항

요구 사항

최상의 DMVPN 기능을 위해서는 Cisco IOS® Software Release 12.4 메인라인 12.4T 이상을 실행하는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Router 3800 Series with Software 릴리스 12.4(22)
- Cisco IOS Router 1800 Series with Software 릴리스 12.3(8)

- Cisco Configuration Professional 버전 2.5

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

배경 정보

이 문서에서는 Cisco CP를 사용하여 라우터를 스포크로 구성하고 다른 라우터를 허브로 구성하는 방법에 대해 설명합니다. 초기 스포크 컨피그레이션이 표시되지만, 이 문서의 뒷부분에는 허브 관련 컨피그레이션이 자세히 표시되어 더 잘 이해할 수 있습니다. 허브에 연결하기 위해 유사한 접근 방식을 사용하여 다른 스포크를 구성할 수도 있습니다. 현재 시나리오는 다음 매개변수를 사용합니다.

- 허브 라우터 공용 네트워크 - 209.165.201.0
- 터널 네트워크 - 192.168.10.0
- 사용된 라우팅 프로토콜 - OSPF

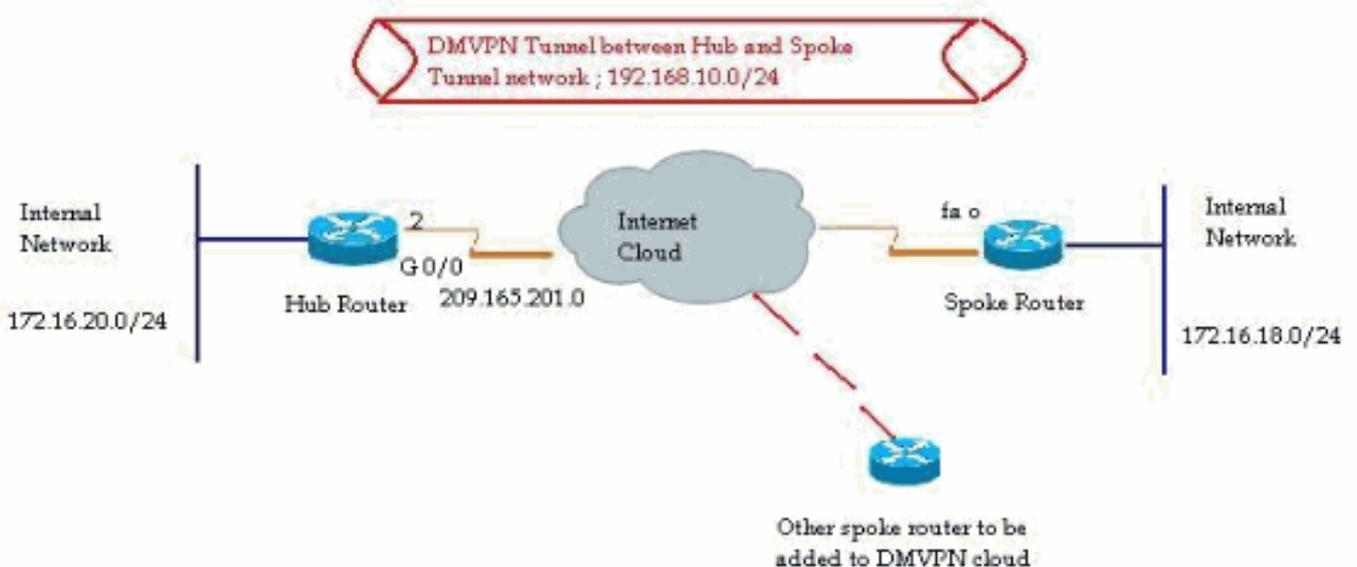
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: [명령 조회 도구](#) ([등록된](#) 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

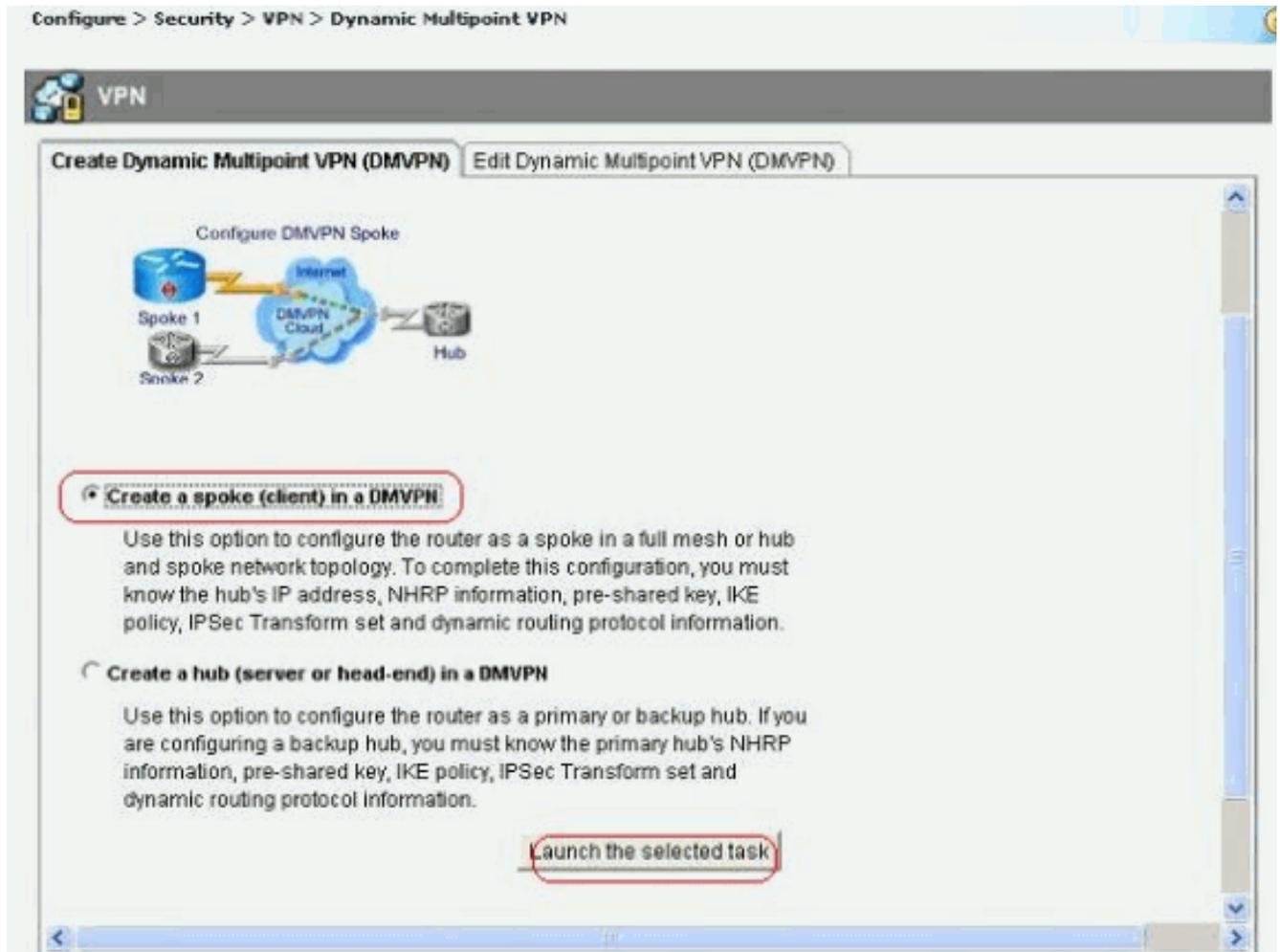
이 문서에서는 다음 네트워크 설정을 사용합니다.



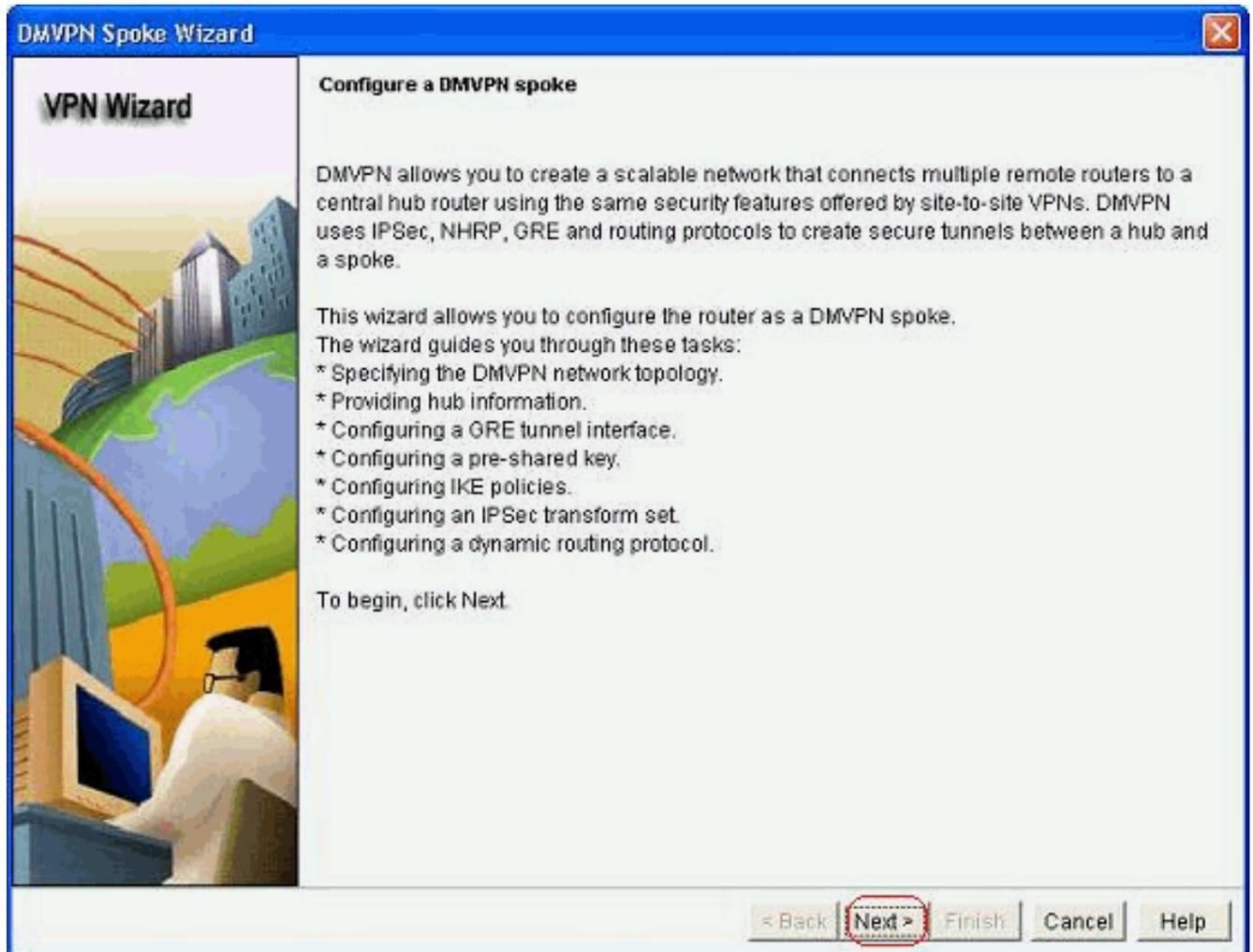
Cisco CP를 사용한 스포크 구성

이 섹션에서는 Cisco Configuration Professional에서 단계별 DMVPN 마법사를 사용하여 라우터를 스포크로 구성하는 방법을 보여줍니다.

1. Cisco CP 애플리케이션을 시작하고 DMVPN 마법사를 시작하려면 Configure(구성) > Security(보안) > VPN > Dynamic Multipoint VPN(동적 멀티포인트 VPN)으로 이동합니다. 그런 다음 DMVPN에서 스포크 생성 옵션을 선택하고 선택한 작업을 클릭합니다



2. Next(다음)를 클릭하여 시작합니다



3. Hub and Spoke 네트워크 옵션을 선택하고 Next를 클릭합니다

VPN Wizard



DMVPN Network Topology

Select the DMVPN network topology.

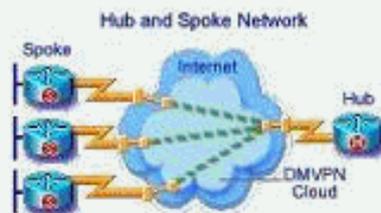
Hub and Spoke network

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. 허브 라우터의 공용 인터페이스 및 허브 라우터의 터널 인터페이스와 같은 허브 관련 정보를 지정합니다

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

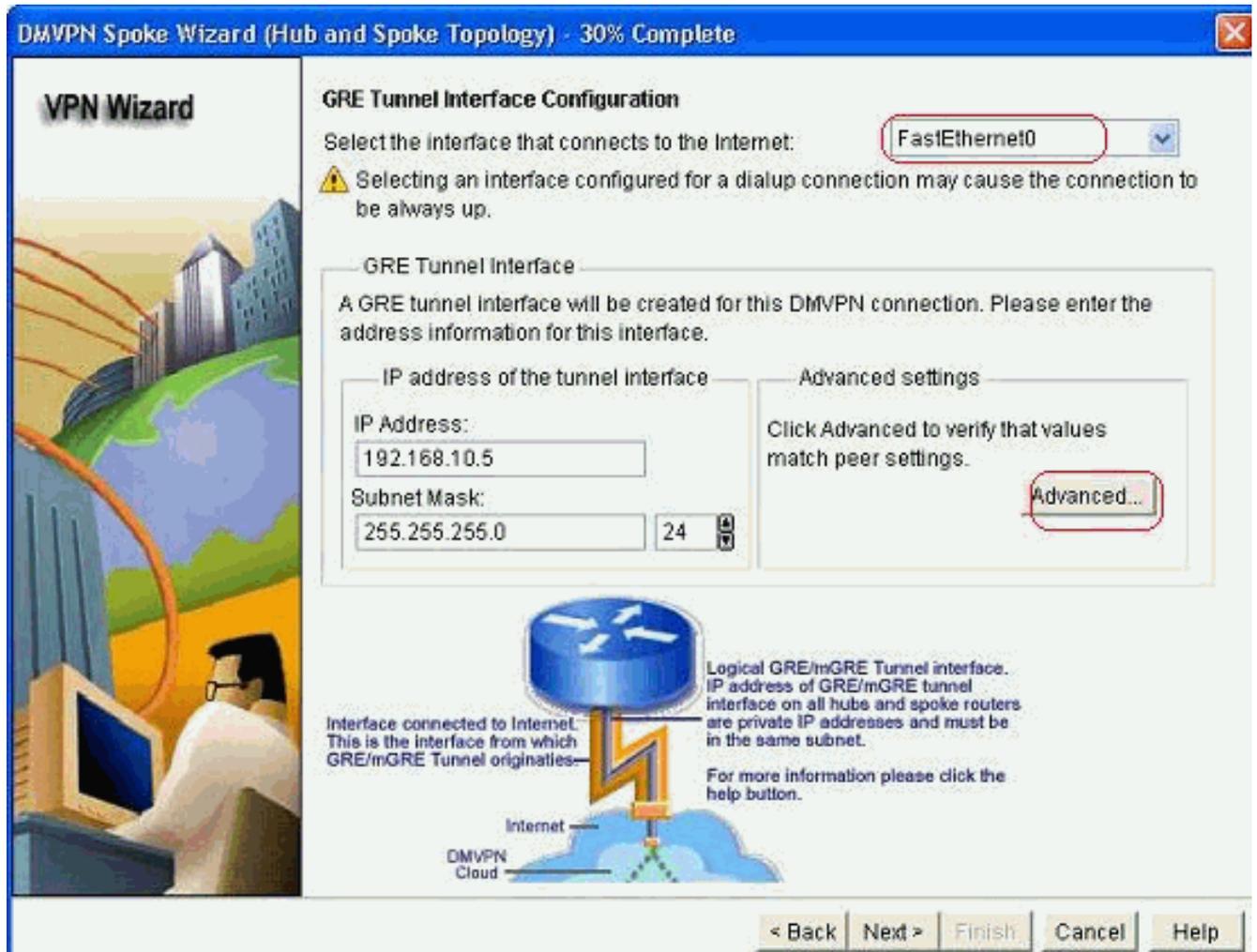
Hub

Public IP address to be entered above

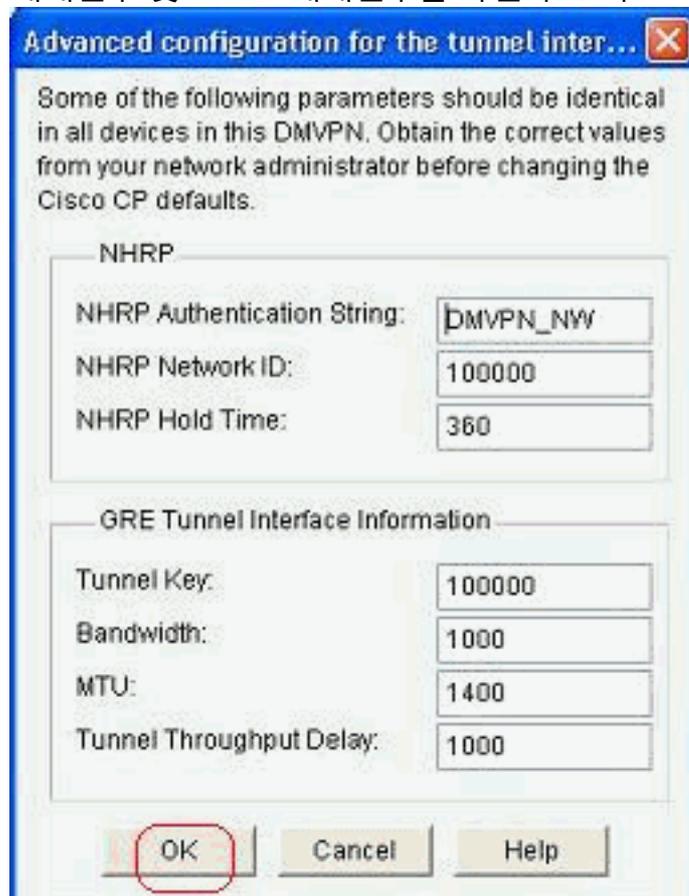
IP address of the mGRE tunnel to be entered above

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

5. 스포크의 터널 인터페이스 세부 정보 및 스포크의 공용 인터페이스를 지정합니다. 그런 다음 *Advanced*(고급)를 클릭합니다

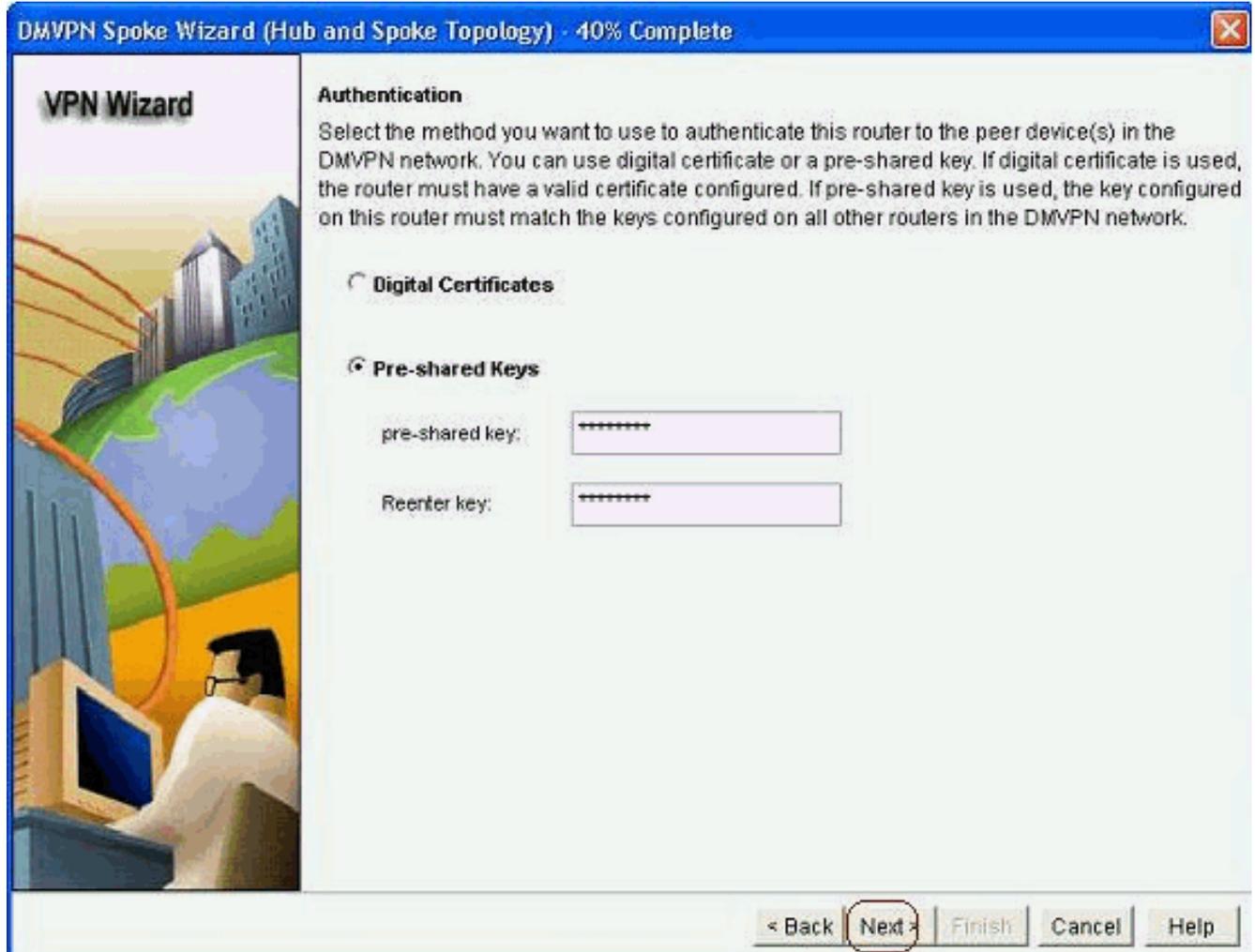


6. 터널 매개변수 및 NHRP 매개변수를 확인하고 허브 매개변수와 완벽하게 일치하는지 확인합

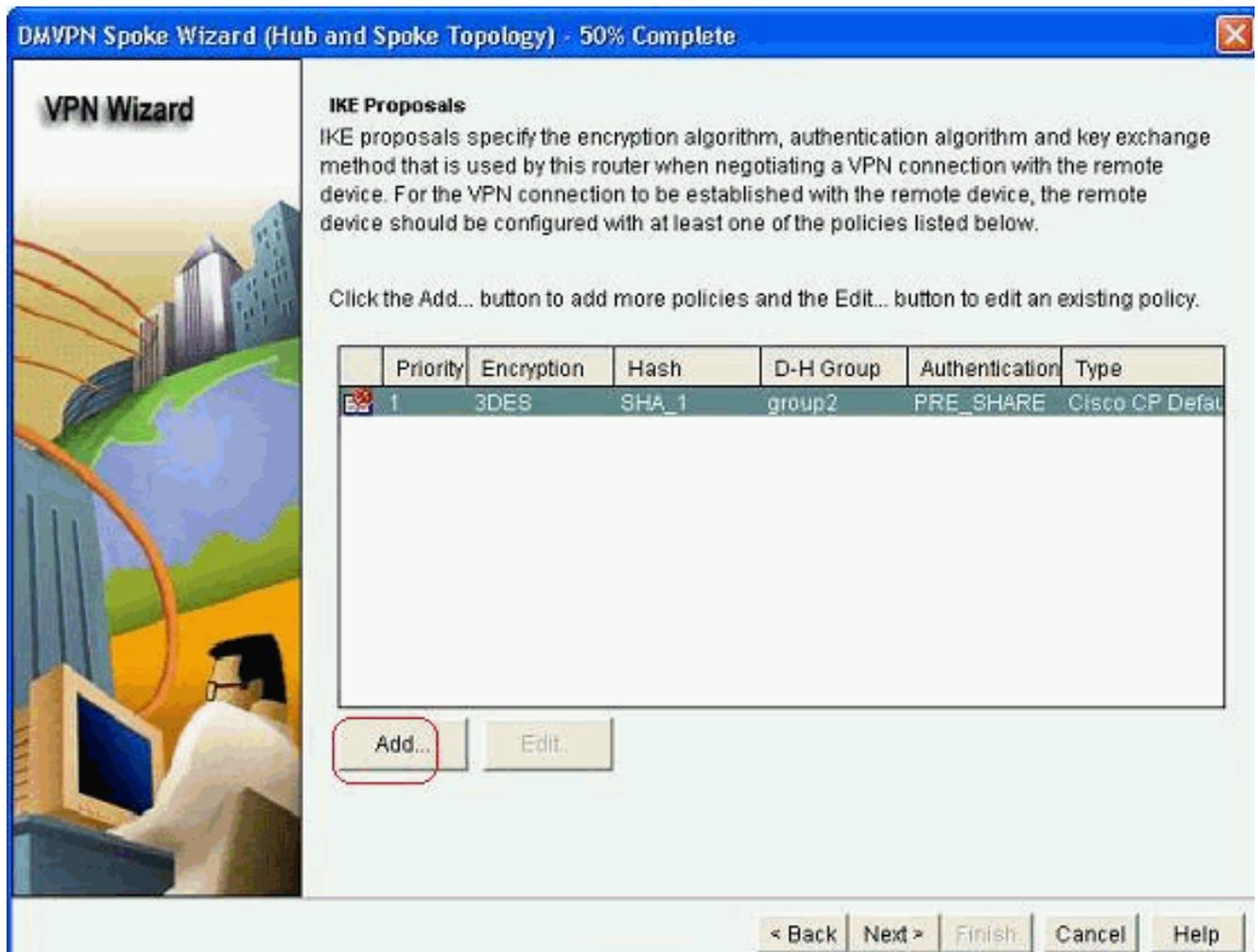


니다.

7. 사전 공유 키를 지정하고 Next(다음)를 클릭합니다



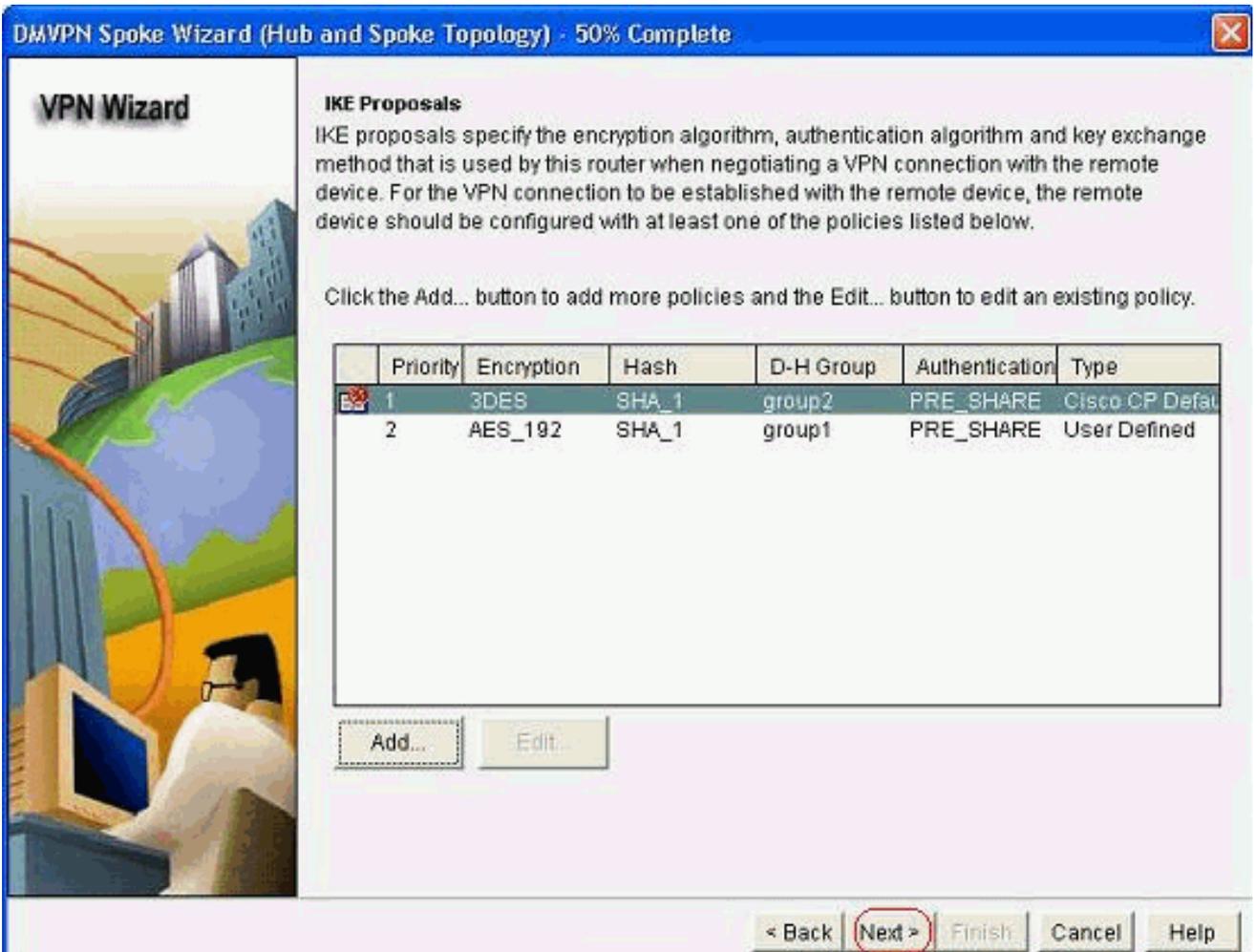
8. 별도의 IKE 제안을 추가하려면 *Add*를 클릭합니다



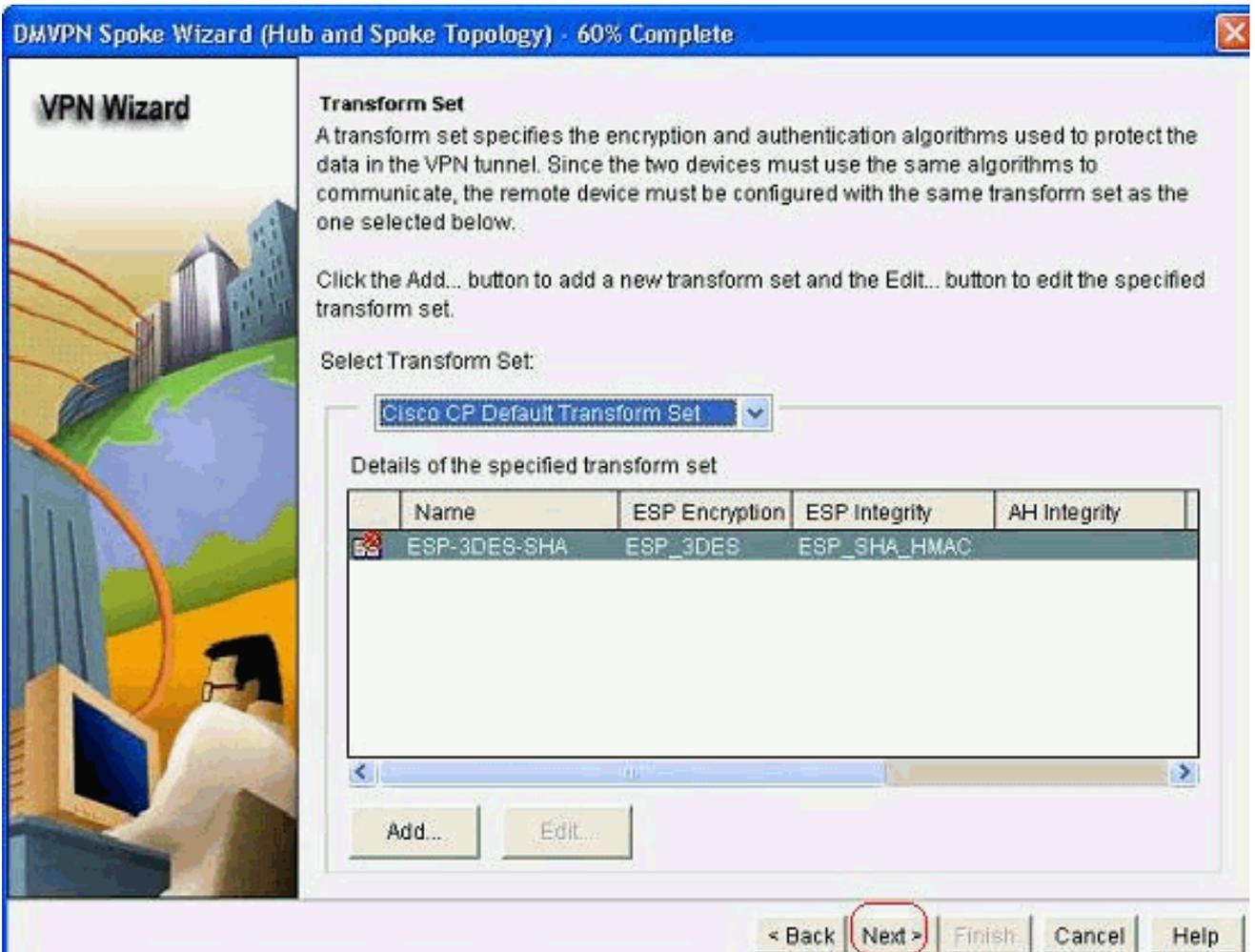
9. 암호화, 인증 및 해시 매개변수를 지정합니다. 그런 다음 **확인**을 클릭합니다



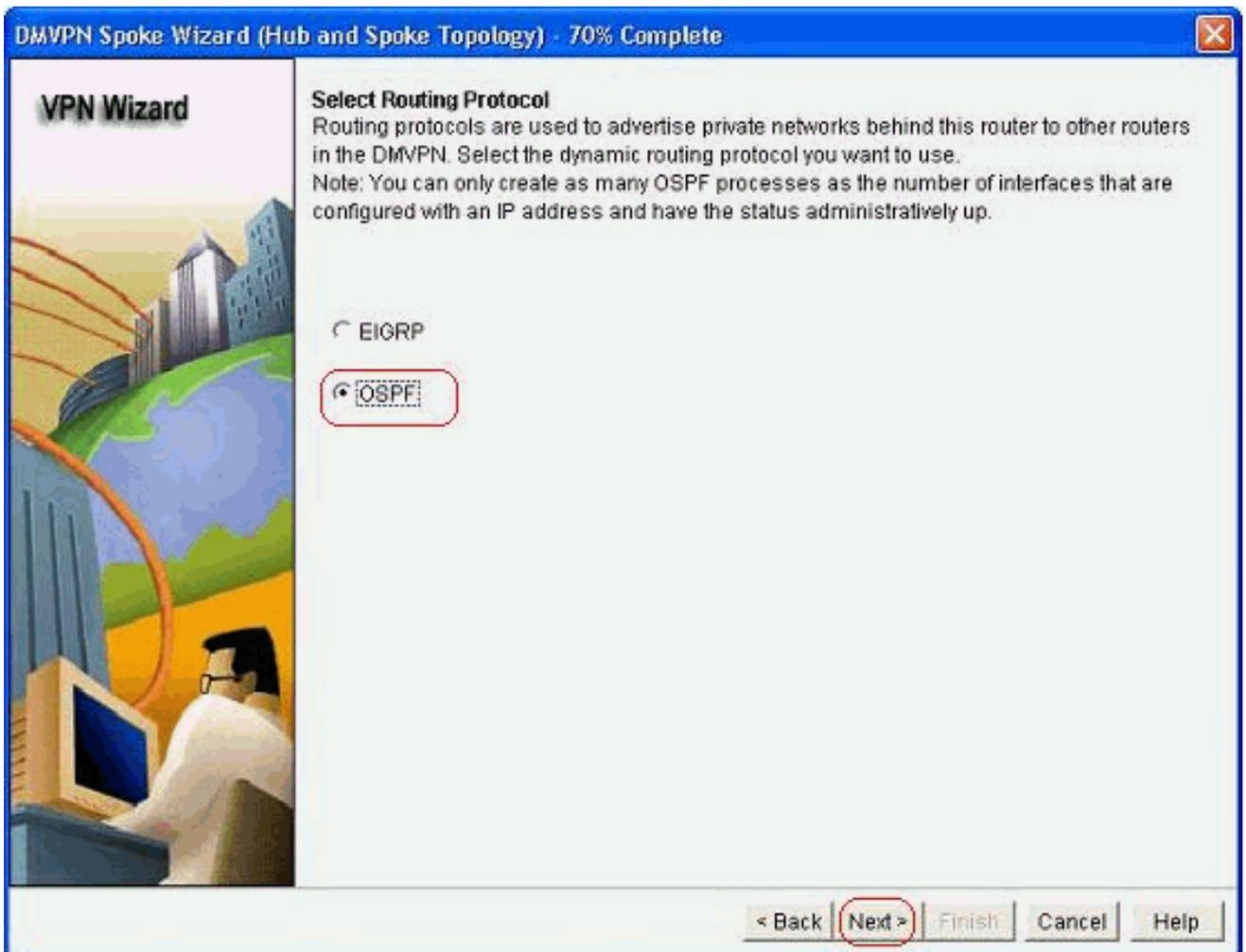
10. 새로 생성된 IKE 정책은 여기에서 확인할 수 있습니다. **Next(다음)**를 클릭합니다



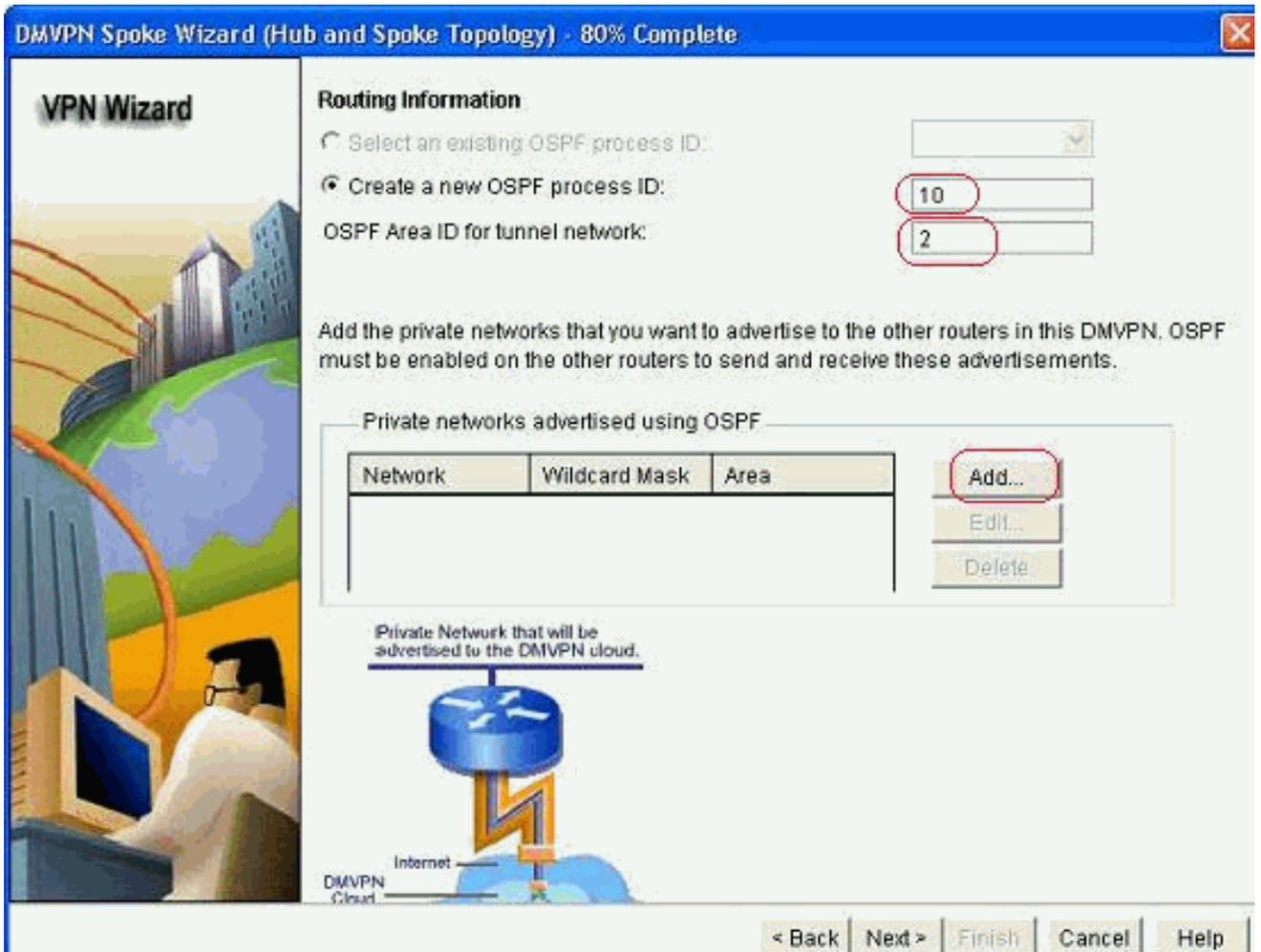
11. Next(다음)를 클릭하여 기본 변형 집합을 계속 진행합니다



12. 필요한 라우팅 프로토콜을 선택합니다. 여기서 OSPF가 선택됩니다

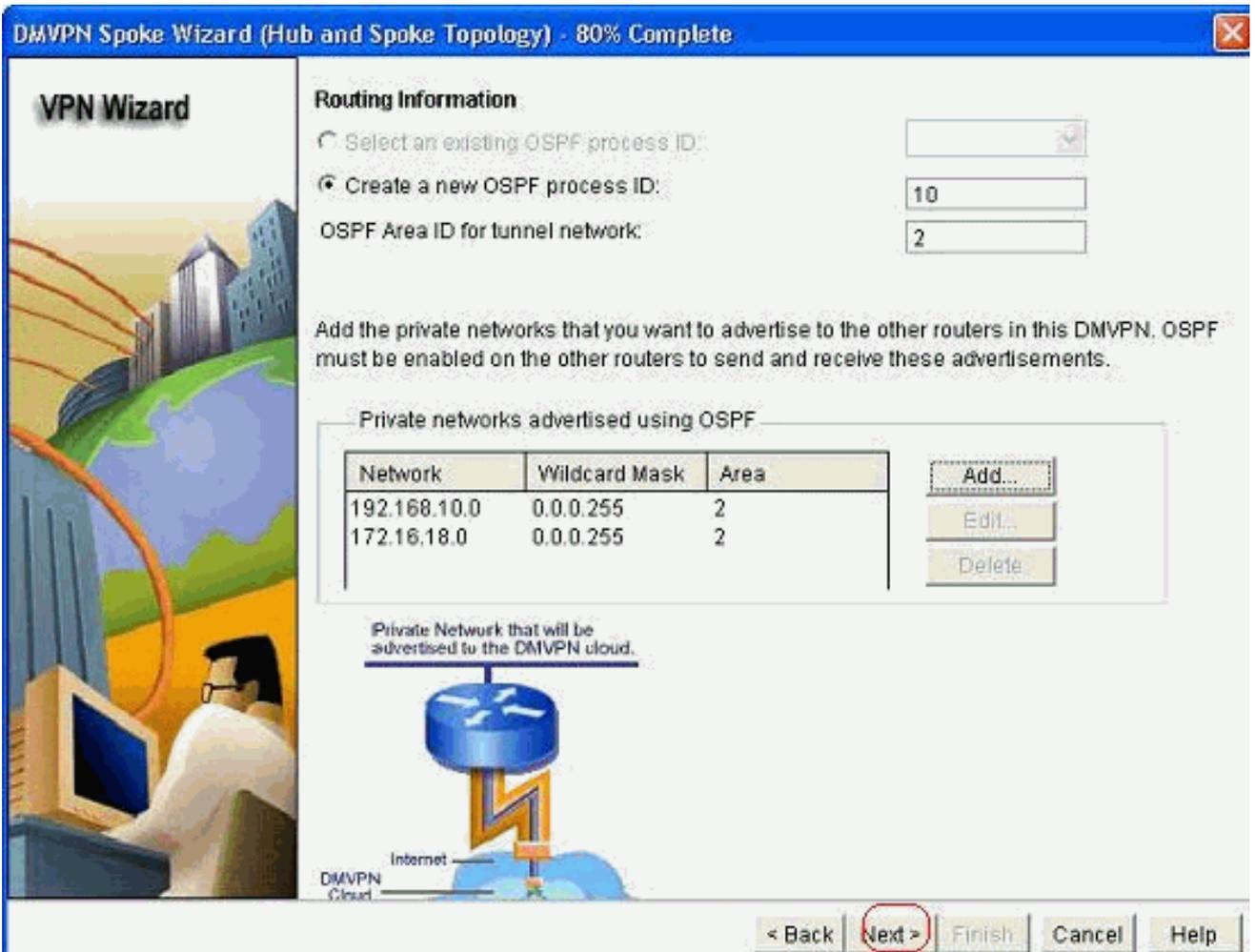


13. OSPF 프로세스 ID 및 영역 ID를 지정합니다. OSPF에서 알릴 네트워크를 추가하려면 Add를 클릭합니다

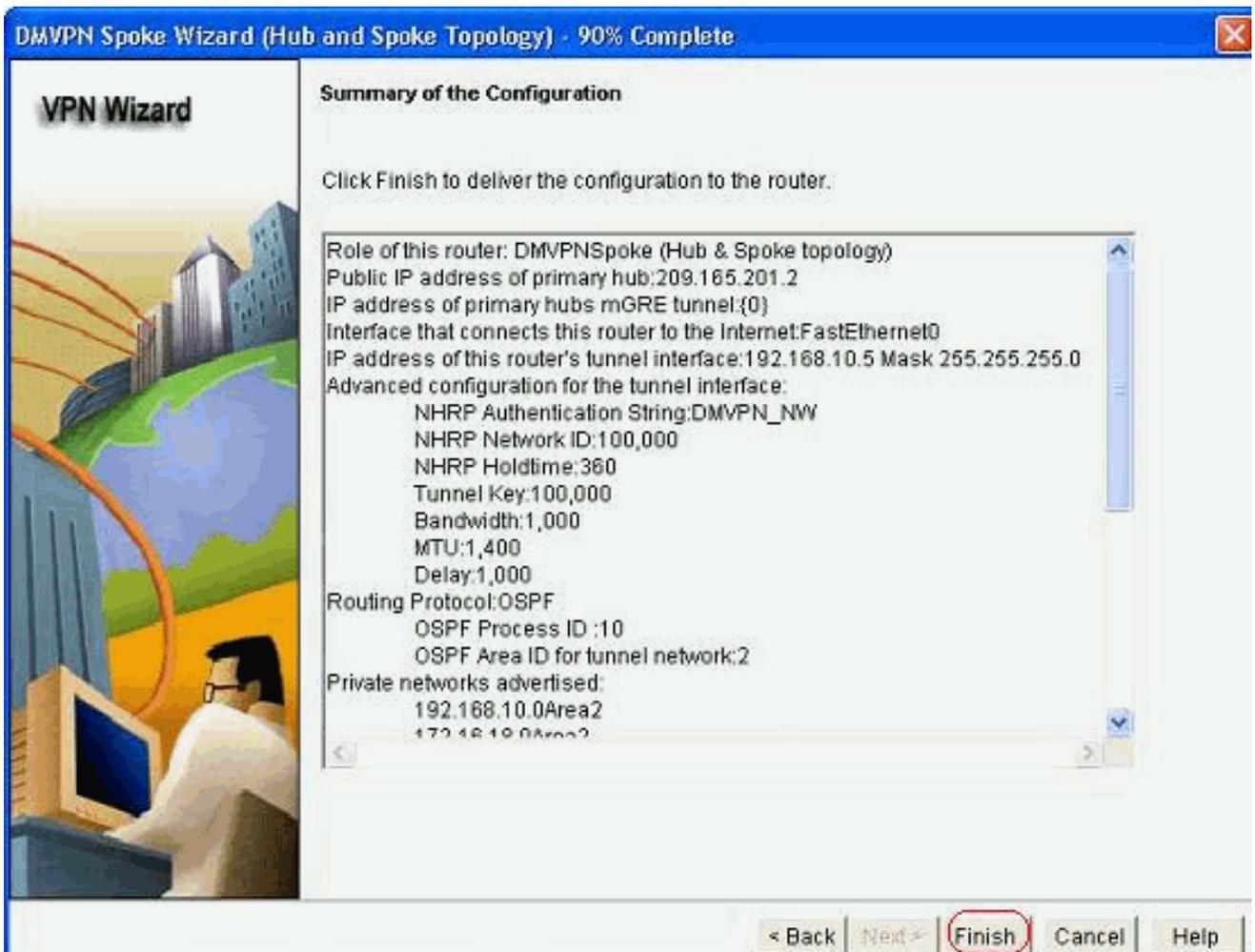


14. 터널 네트워크를 추가하고 OK(확인)를 클릭합니다.

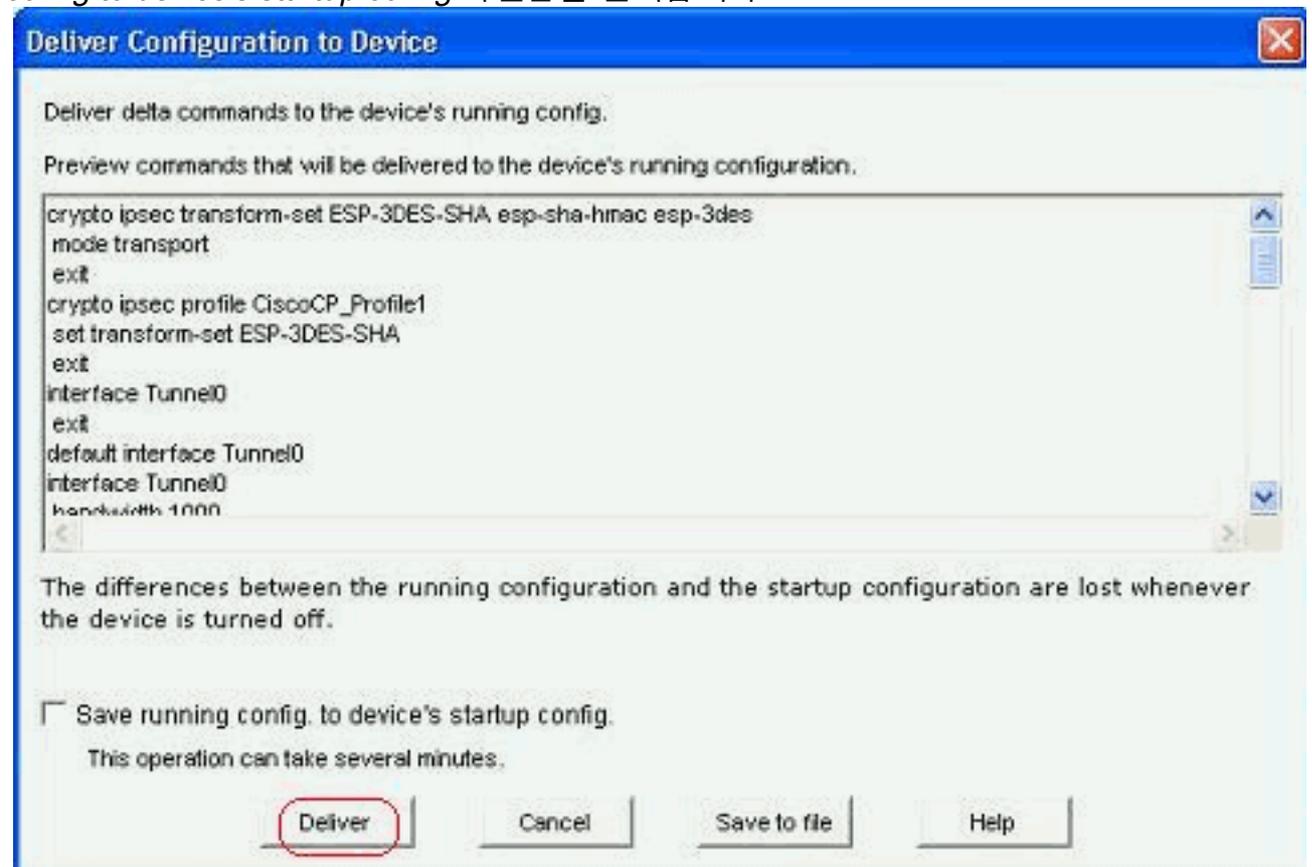
15. 스포크 라우터 뒤에 사설 네트워크를 추가합니다. 그런 다음 다음을 클릭합니다



16. 마침을 클릭하여 마법사 구성을 완료합니다



17. Deliver(전달)를 클릭하여 명령을 실행합니다. 컨피그레이션을 저장하려면 *Save running config to device's startup config* 확인란을 선택합니다



스포크에 대한 CLI 컨피그레이션

관련 CLI 컨피그레이션은 다음과 같습니다.

스포크 라우터

```
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 CP를 사용한 허브 컨피그레이션

이 섹션에서는 DMVPN에 대한 허브 라우터를 구성하는 방법에 대한 단계별 접근 방식을 보여줍니다.

1. Configure(구성) > Security(보안) > VPN > Dynamic Multipoint VPN으로 이동하고 Create a hub in a DMVPN 옵션을 선택합니다. 에서 선택한 작업 시작을 클릭합니다

Configure > Security > VPN > Dynamic Multipoint VPN

VPN

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



Create a spoke (client) in a DMVPN

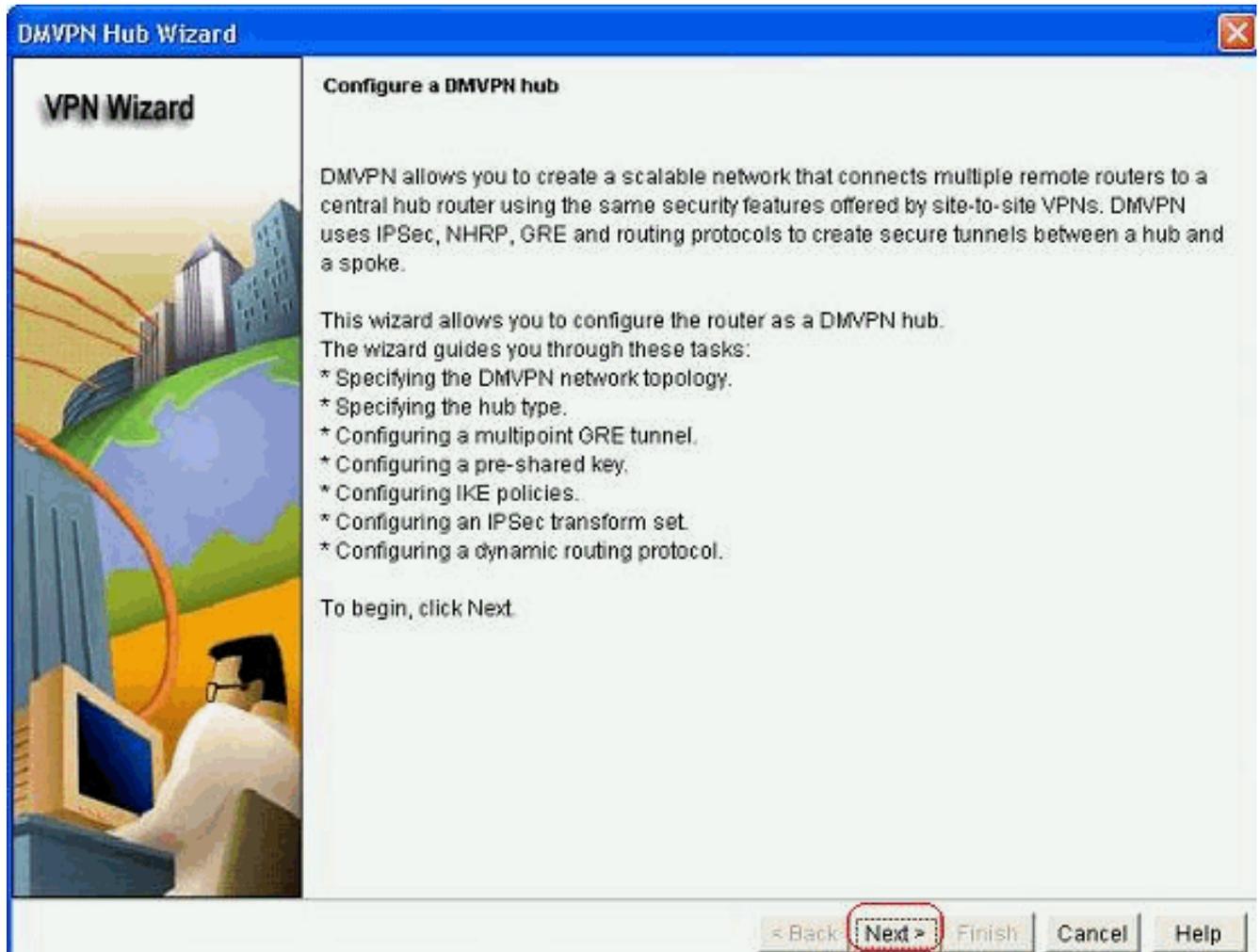
Use this option to configure the router as a spoke in a full mesh or hub and spoke network topology. To complete this configuration, you must know the hub's IP address, NHRP information, pre-shared key, IKE policy, IPsec Transform set and dynamic routing protocol information.

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.

Launch the selected task

2. Next(다음)를 클릭합니다



3. Hub and Spoke 네트워크 옵션을 선택하고 Next를 클릭합니다

VPN Wizard



DMVPN Network Topology

Select the DMVPN network topology.

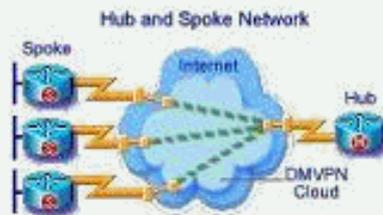
Hub and Spoke network

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

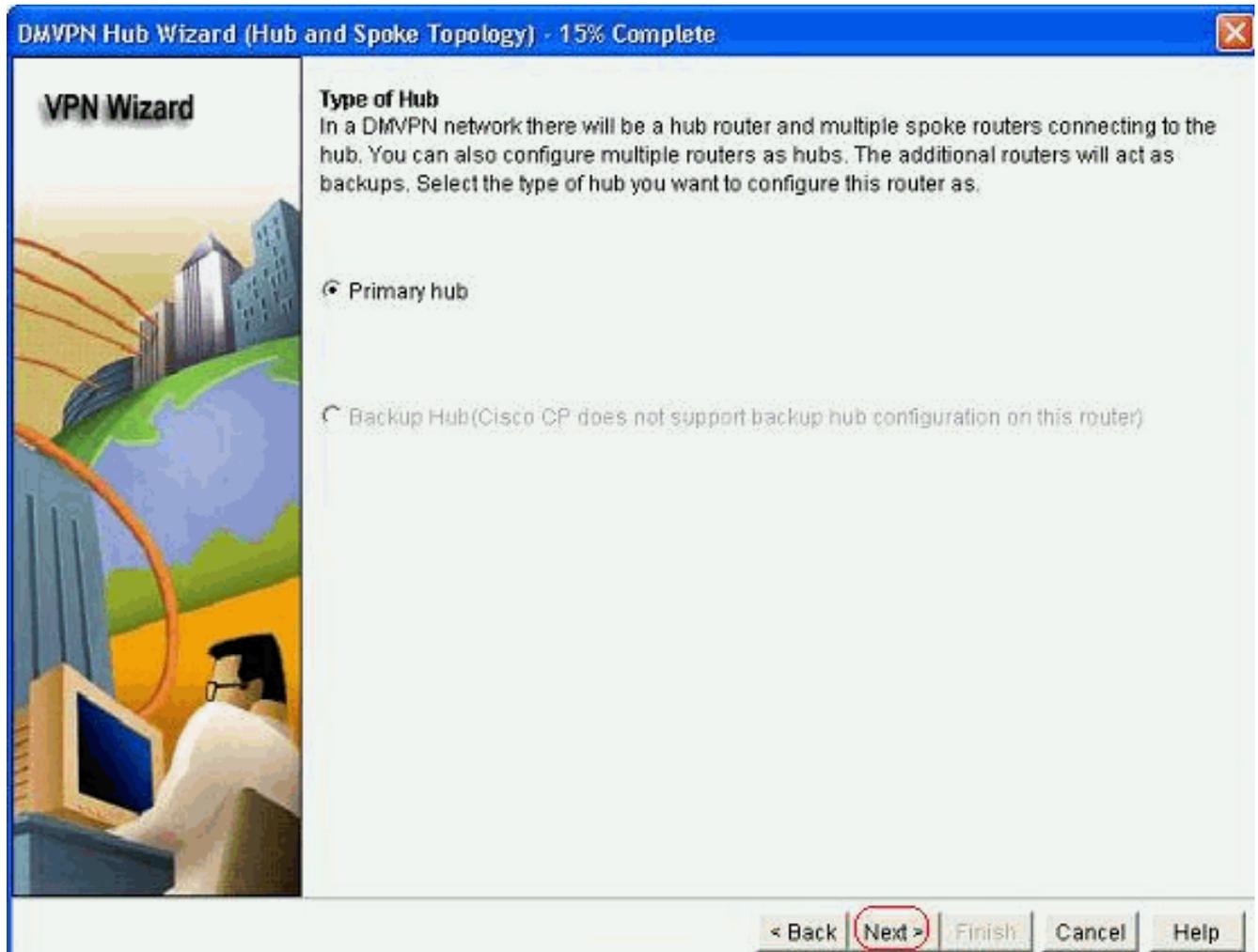
Next >

Finish

Cancel

Help

4. 기본 허브를 선택합니다. 그런 다음 다음을 클릭합니다



5. Tunnel 인터페이스 매개변수를 지정하고 Advanced(고급)를 클릭합니다

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

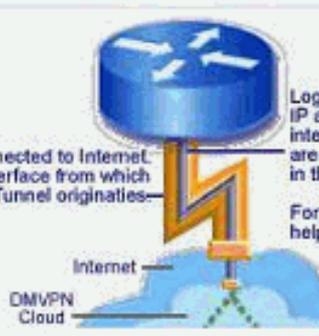
IP Address:

Subnet Mask:

Advanced settings

Click Advanced to verify that values match peer settings.

Advanced...



Interface connected to Internet. This is the interface from which GRE/mGRE Tunnel originates.

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.

6. Tunnel(터널) 매개변수 및 NHRP 매개변수를 지정합니다. 그런 다음 확인을 클릭합니다

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:

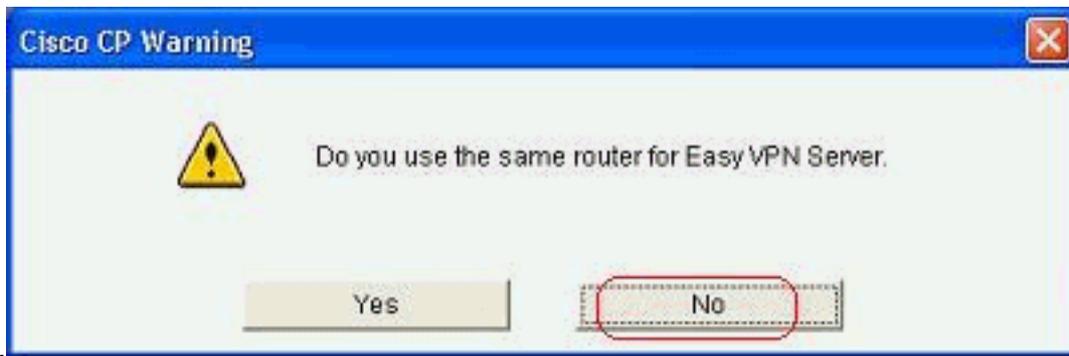
Bandwidth:

MTU:

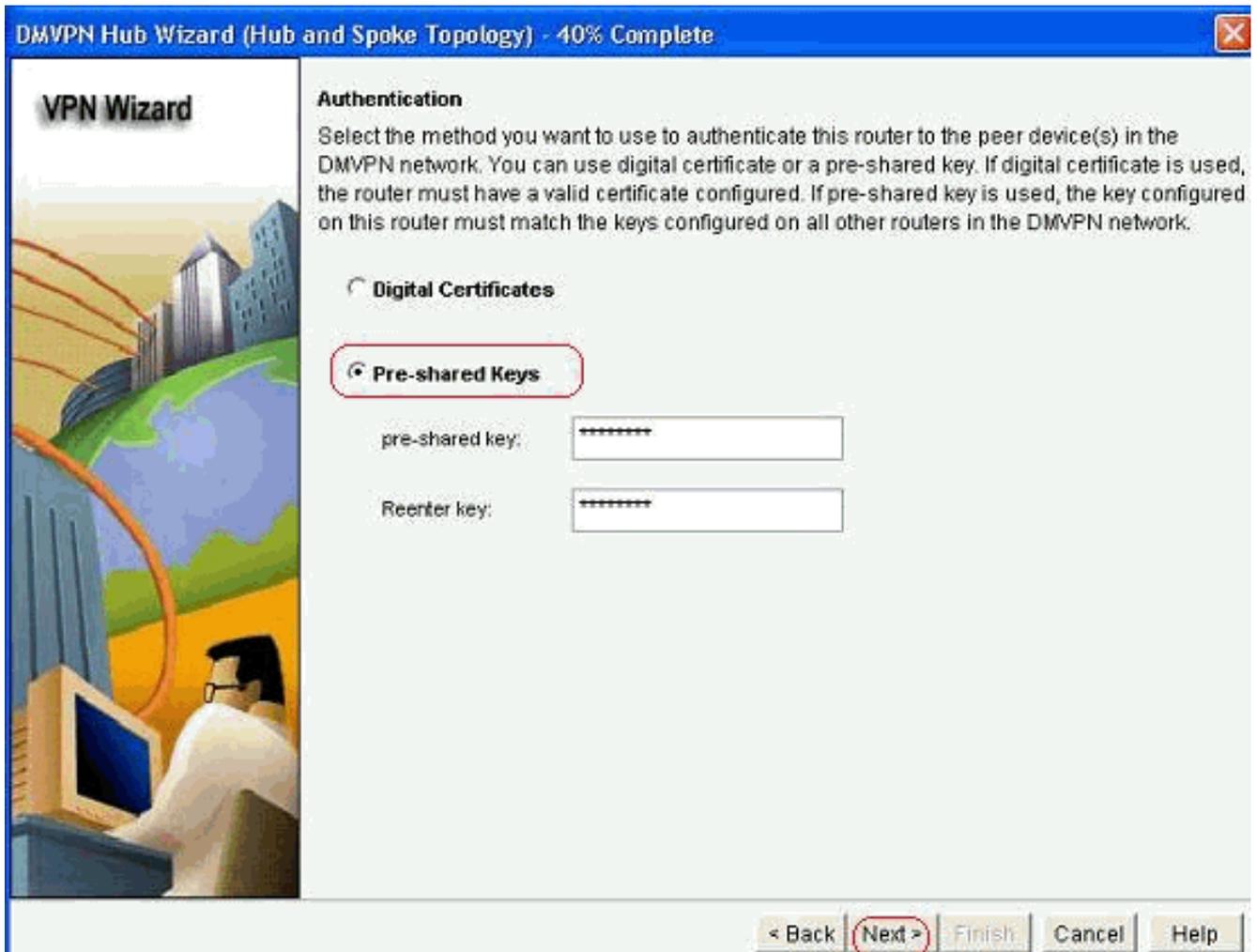
Tunnel Throughput Delay:

OK
Cancel
Help

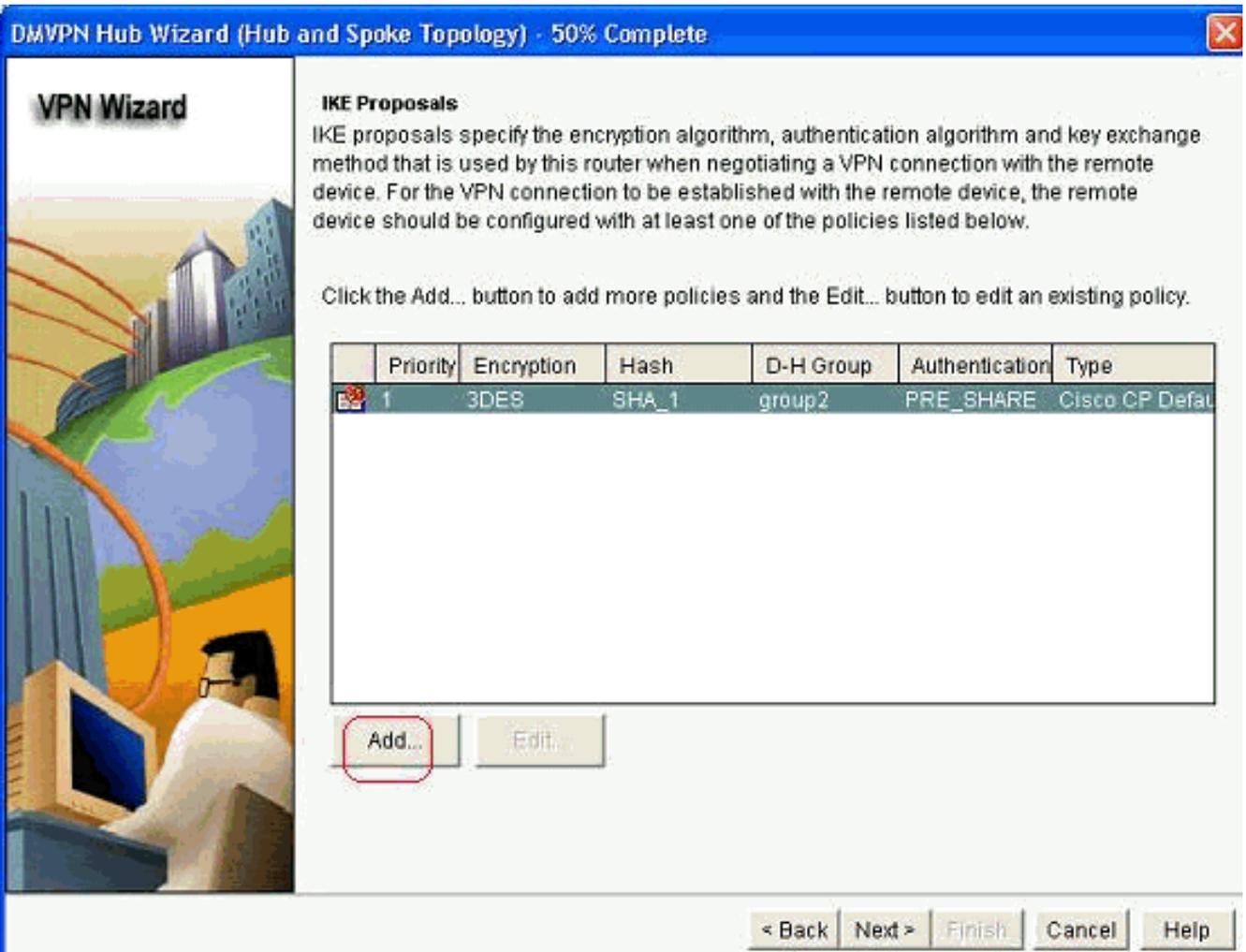
7. 네트워크 설정에 따라 옵션을 지정합니다



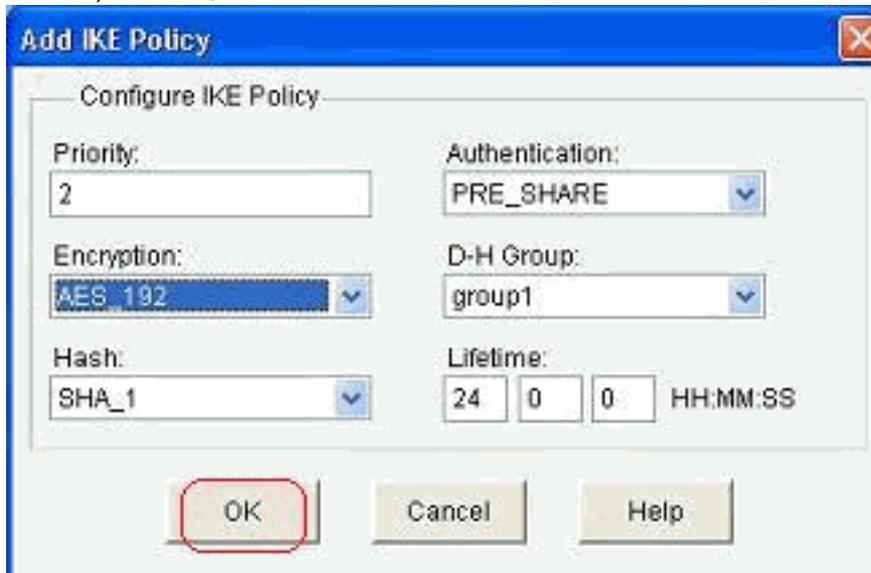
8. 사전 공유 키를 선택하고 사전 공유 키를 지정합니다. 그런 다음 다음을 클릭합니다



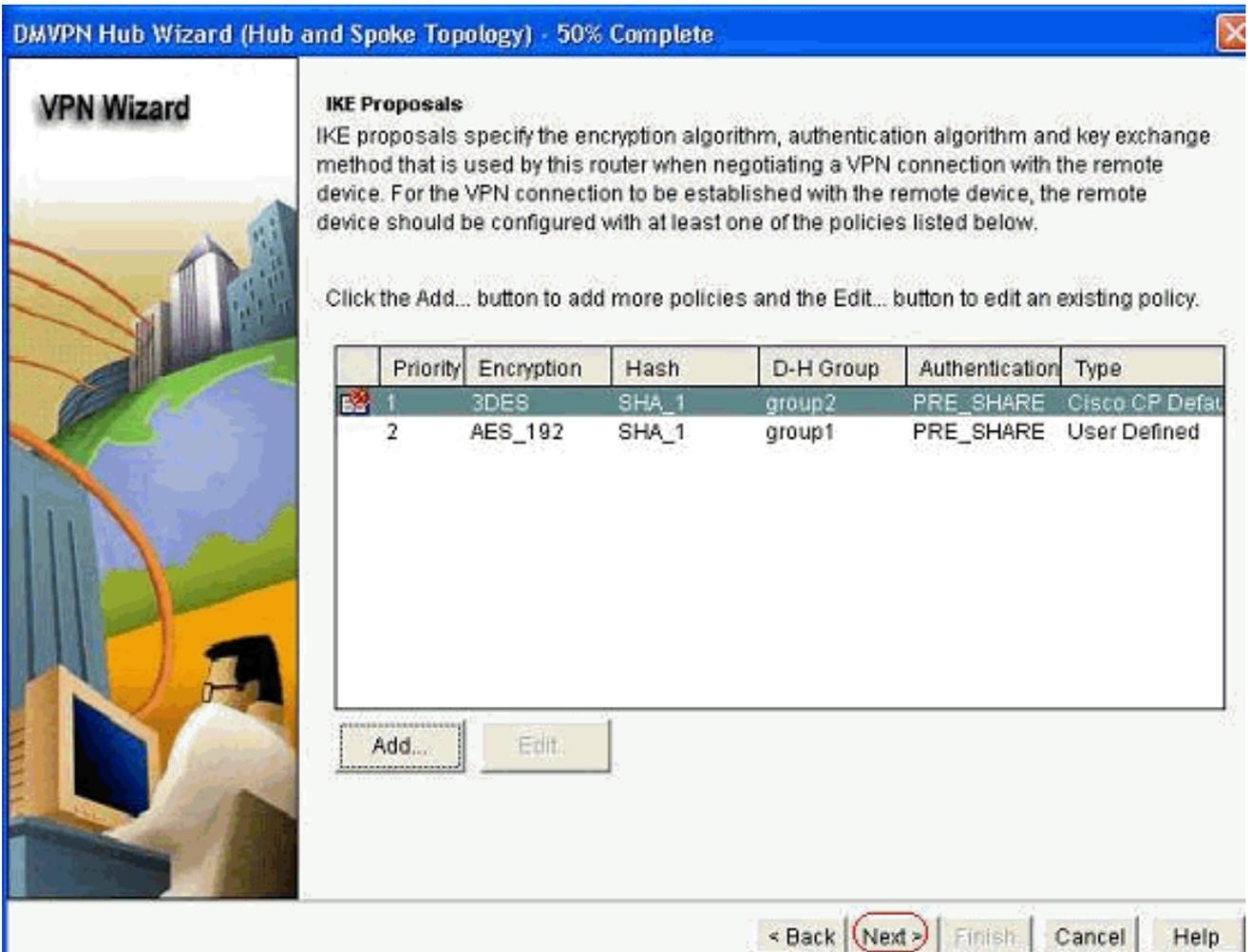
9. 별도의 IKE 제안을 추가하려면 Add를 클릭합니다



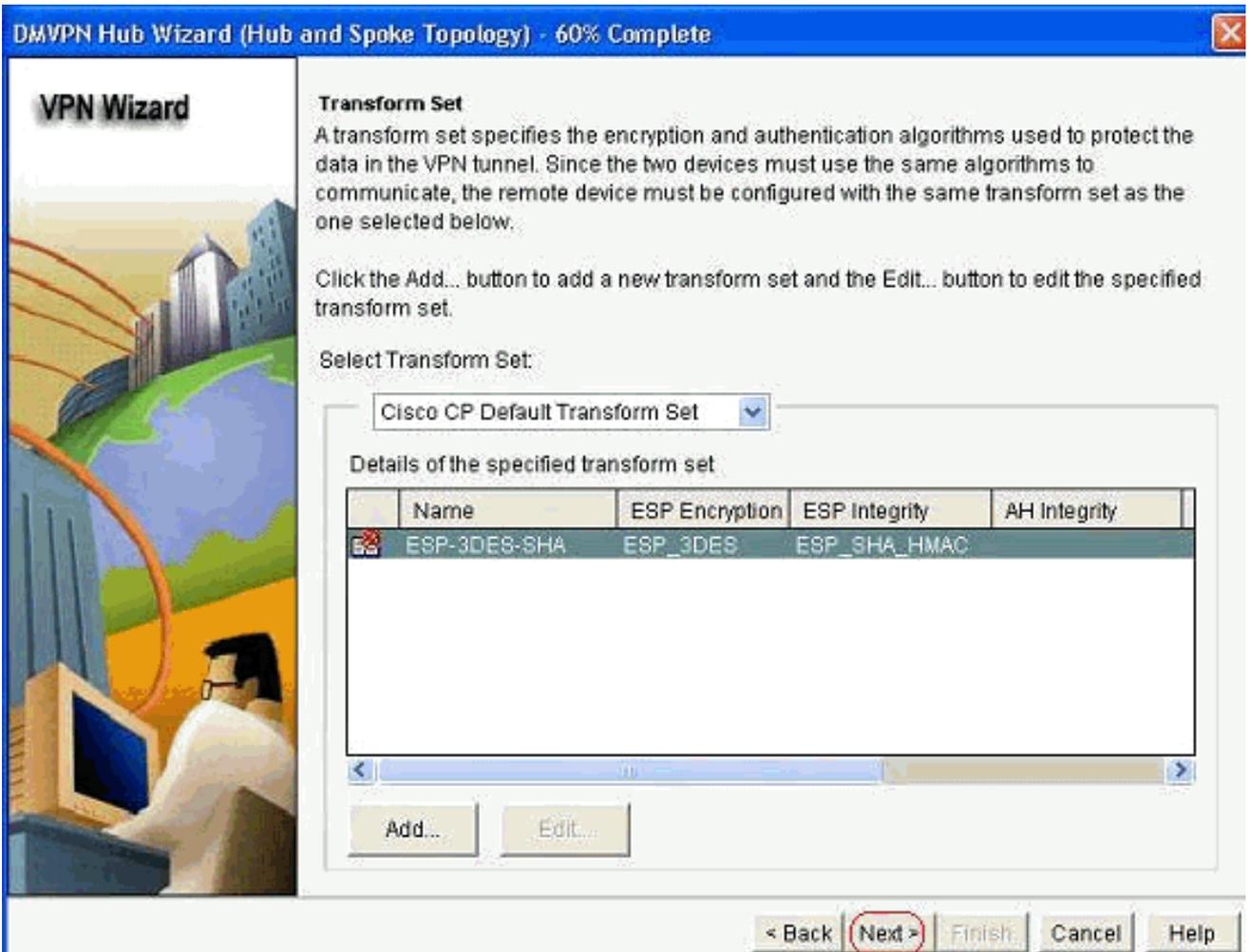
10. 암호화, 인증 및 해시 매개변수를 지정합니다. 그런 다음 **확인**을 클릭합니다



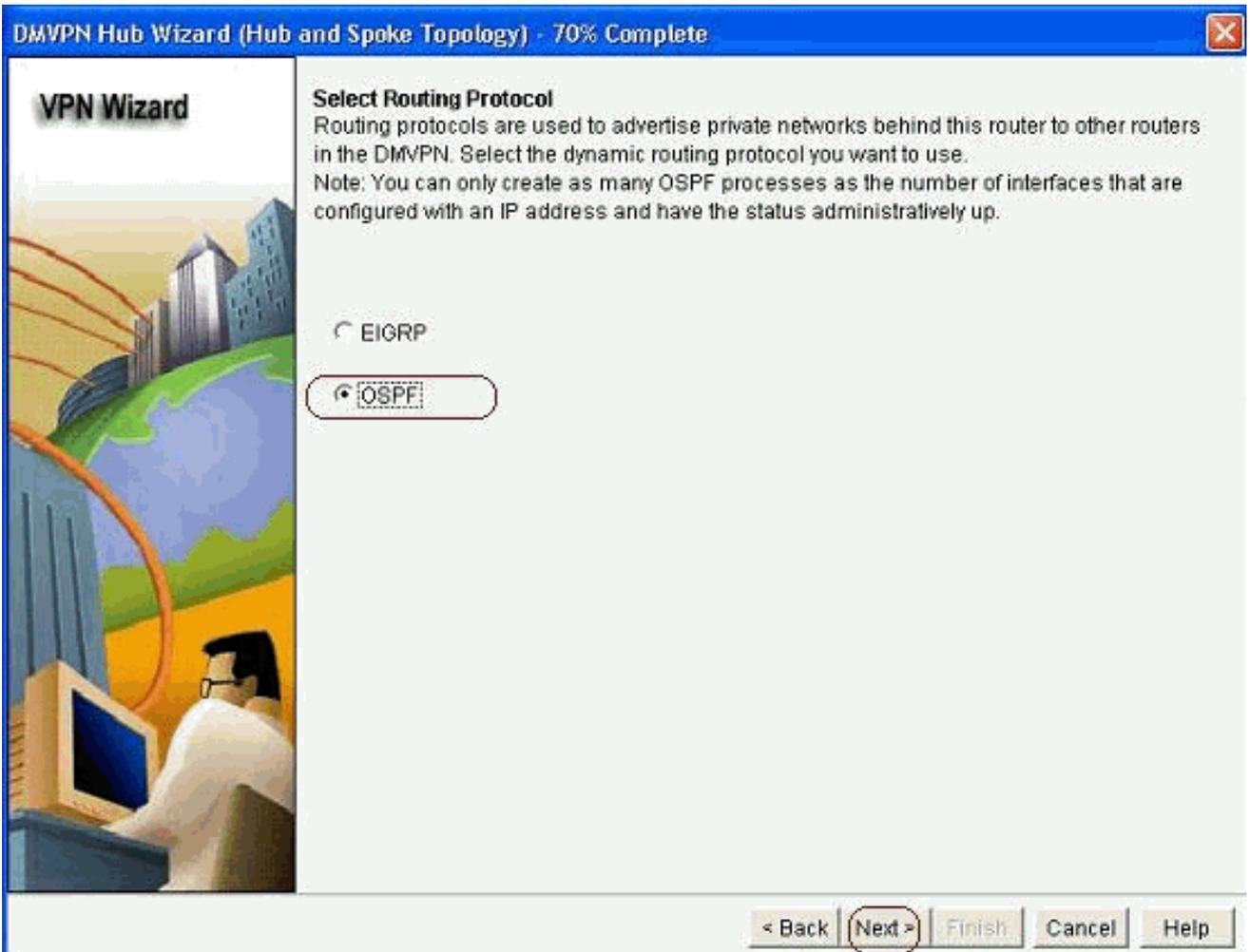
11. 새로 생성된 IKE 정책은 여기에서 확인할 수 있습니다. **Next(다음)**를 클릭합니다



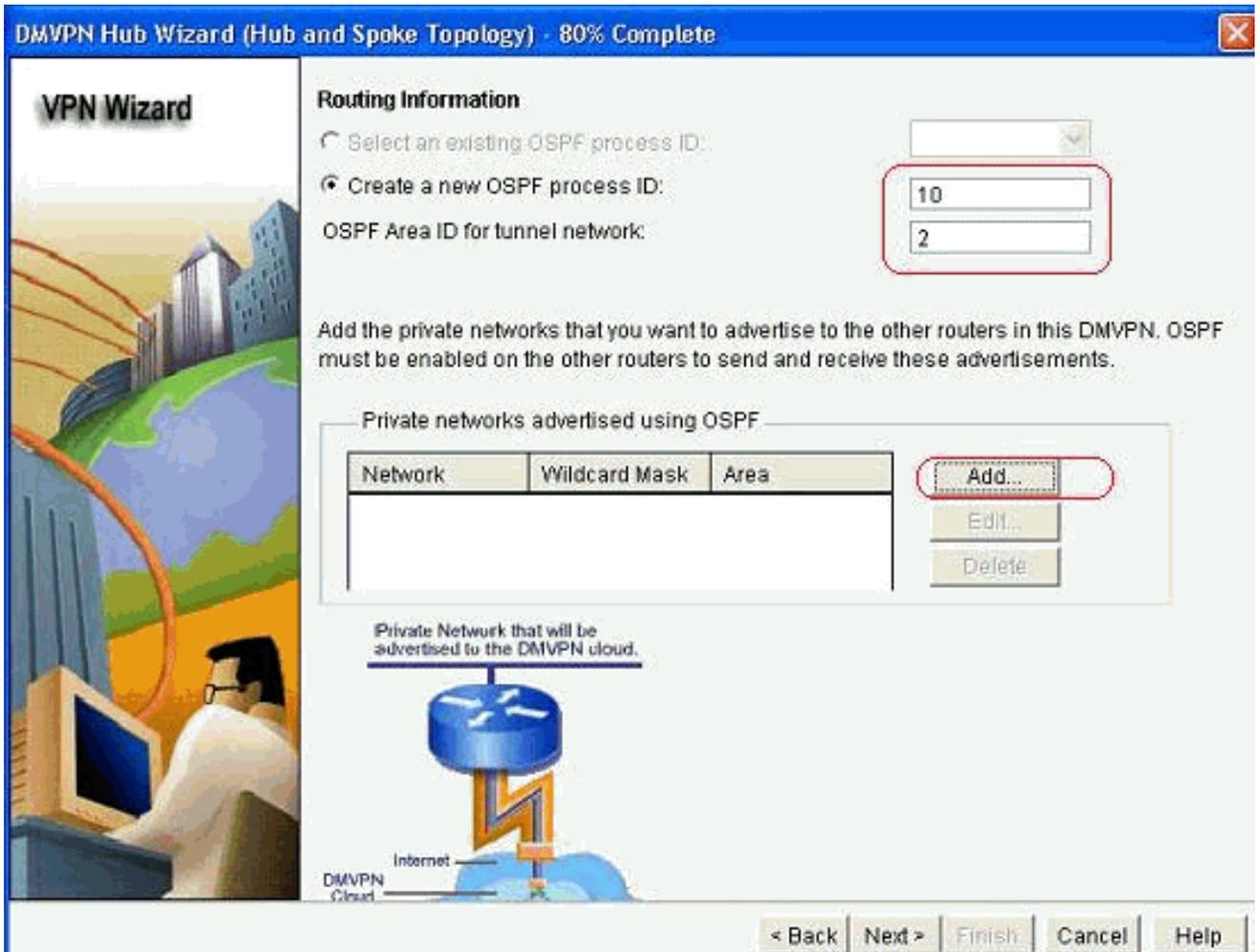
12. Next(다음)를 클릭하여 기본 변형 집합을 계속 진행합니다



13. 필요한 라우팅 프로토콜을 선택합니다. 여기서 OSPF가 선택됩니다

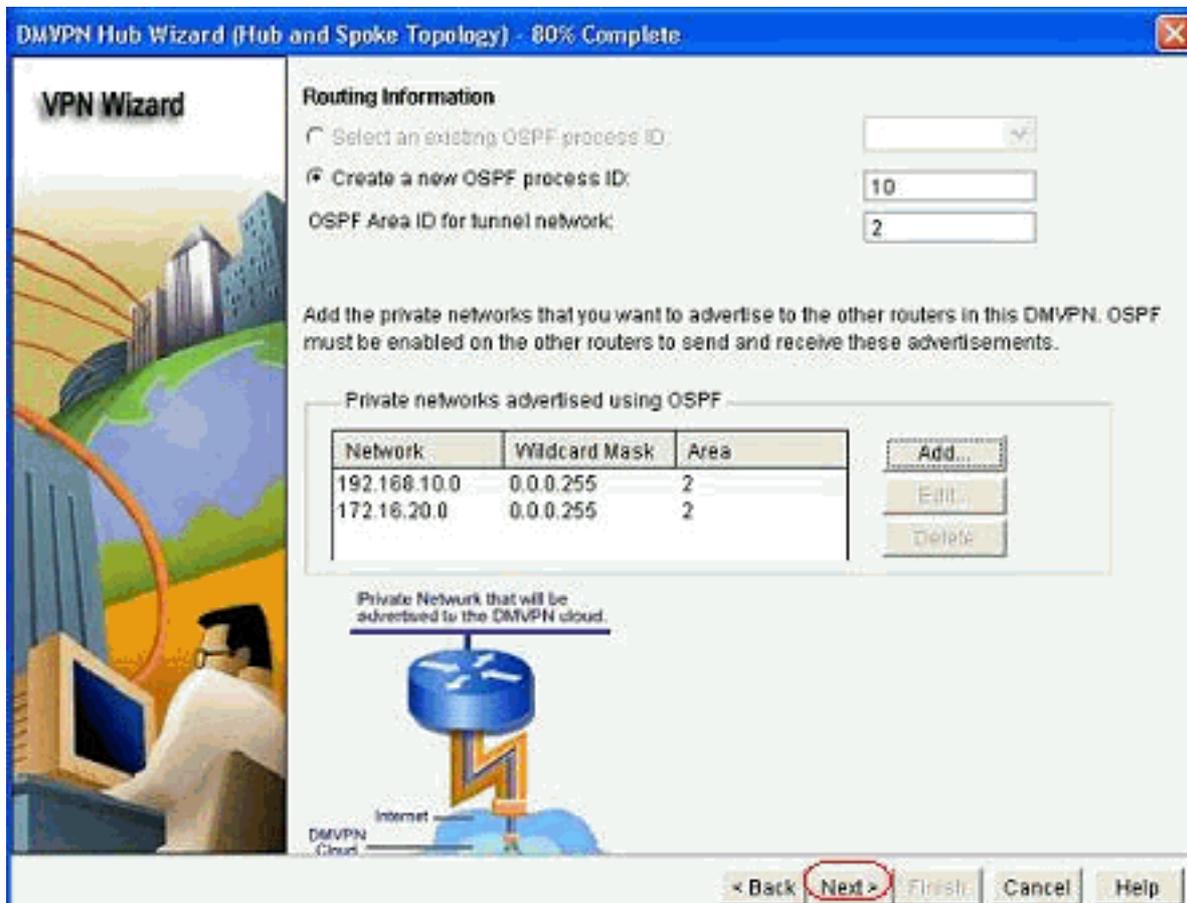


14. OSPF 프로세스 ID 및 영역 ID를 지정합니다. OSPF에서 알릴 네트워크를 추가하려면 Add를 클릭합니다



15. 터널 네트워크를 추가하고 OK(확인)를 클릭합니다.

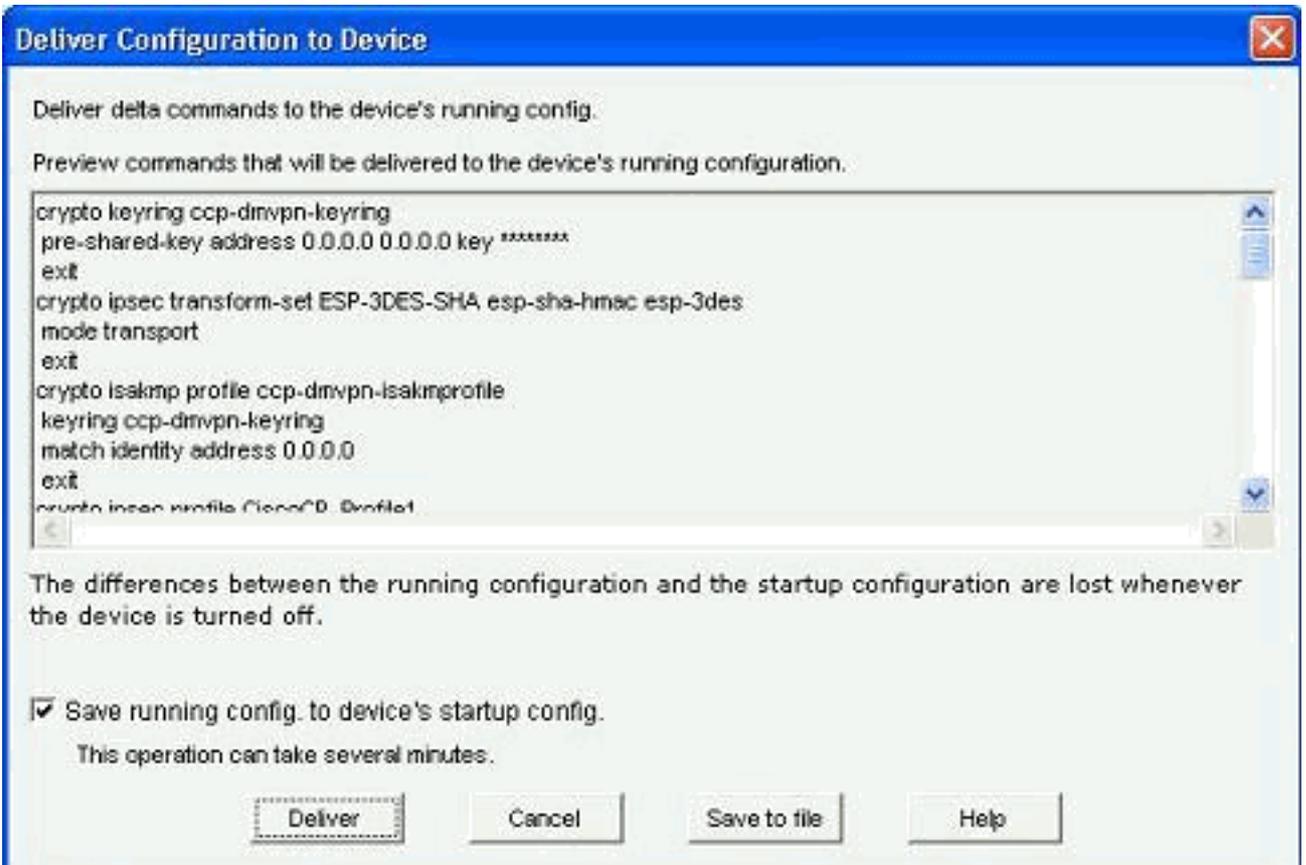
16. 허브 라우터 뒤에 프라이빗 네트워크를 추가하고 Next(다음)를 클릭합니다



17. 마침을 클릭하여 마법사 구성을 완료합니다



18. Deliver(전달)를 클릭하여 명령을 실행합니다



[허브에 대한 CLI 컨피그레이션](#)

관련 CLI 컨피그레이션은 다음과 같습니다.

허브 라우터
<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
!

```

CCP를 사용하여 DMVPN 컨피그레이션 수정

터널 인터페이스를 선택하고 Edit(수정)를 클릭할 때 기존 DMVPN 터널 매개변수를 수동으로 편집할 수 있습니다.

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 및 터널 키와 같은 터널 인터페이스 매개변수는 *General* 탭에서 수정됩니다.

DMVPN Tunnel Configuration

General | NHRP | Routing

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 Add...

MTU: 1400

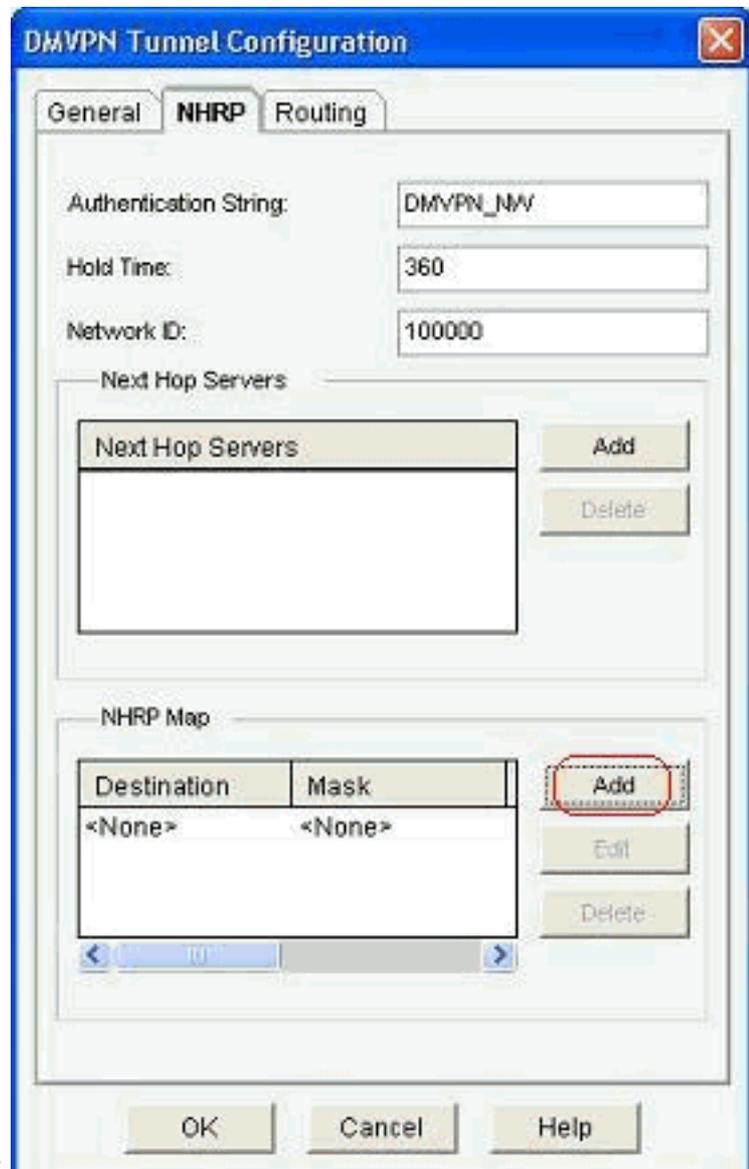
Bandwidth: 1000

Delay: 1000

Tunnel Key: 100000

OK Cancel Help

1. NHRP 관련 매개변수는 NHRP 탭의 요구 사항에 따라 찾아 수정됩니다. 스포크 라우터의 경우 NHS를 허브 라우터의 IP 주소로 볼 수 있어야 합니다. NHRP 매핑을 추가하려면 NHRP



Map 섹션에서 Add를 클릭합니다.

2. 네트워크 설정에 따라 NHRP 매핑 매개변수를 다음과 같이 구성할 수 있습니다

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): 16
 32

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

라우팅 관련 매개변수는 라우팅(Routing) 탭 아래에서 보고 수정됩니다.



추가 정보

DMVPN 터널은 다음 두 가지 방법으로 구성됩니다.

- 허브를 통한 스포크 간 통신
- 허브가 없는 스포크 간 통신

이 문서에서는 첫 번째 방법만 설명합니다. 스포크 투 스포크(spoke-to-spoke) 동적 IPsec 터널을 설정하기 위해 이 접근 방식을 사용하여 DMVPN 클라우드에 스포크를 추가합니다.

1. DMVPN 마법사를 시작하고 Spoke 구성 옵션을 선택합니다.
2. DMVPN Network Topology(DMVPN 네트워크 토폴로지) 창에서 Hub and Spoke 네트워크 옵션 대신 Full meshed network 옵션을 선택합니다

DMVPN Spoke Wizard - 10% Complete

VPN Wizard

DMVPN Network Topology

Select the DMVPN network topology.

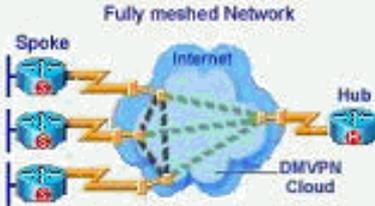
Hub and Spoke network

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. 이 문서의 다른 구성과 동일한 단계를 사용하여 나머지 구성을 완료합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

관련 정보

- [Cisco Dynamic Multipoint VPN: 간단하고 안전한 지사 간 커뮤니케이션](#)
- [IOS 12.2 DMVPN\(Dynamic Multipoint VPN\)](#)
- [기술 지원 및 문서 - Cisco Systems](#)