Configuration Professional 컨피그레이션을 사용하여 Easy VPN 서버로서의 IOS 라우터 예

목차

소개

이 문서에서는 Cisco CP(Cisco Configuration Professional) 및 CLI를 사용하여 Cisco IOS® 라우터를 Easy VPN(EzVPN) 서버로 구성하는 방법에 대해 설명합니다.Easy VPN Server 기능을 사용하면 원격 최종 사용자가 Cisco IOS VPN(Virtual Private Network) 게이트웨이와 IPsec(IP Security)을 사용하여 통신할 수 있습니다.중앙에서 관리되는 IPsec 정책은 서버에서 클라이언트 디바이스에 "푸시됨"되므로 최종 사용자의 컨피그레이션이 최소화됩니다.

Easy VPN Server에 대한 자세한 내용은 Cisco IOS Release 12.4T Secure Connectivity Configuration Guide Library의 Easy VPN Server 섹션을 참조하십시오.

사전 요구 사항

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 1841 Router with Cisco IOS Software 릴리스 12.4(15T)
- Cisco CP 버전 2.1

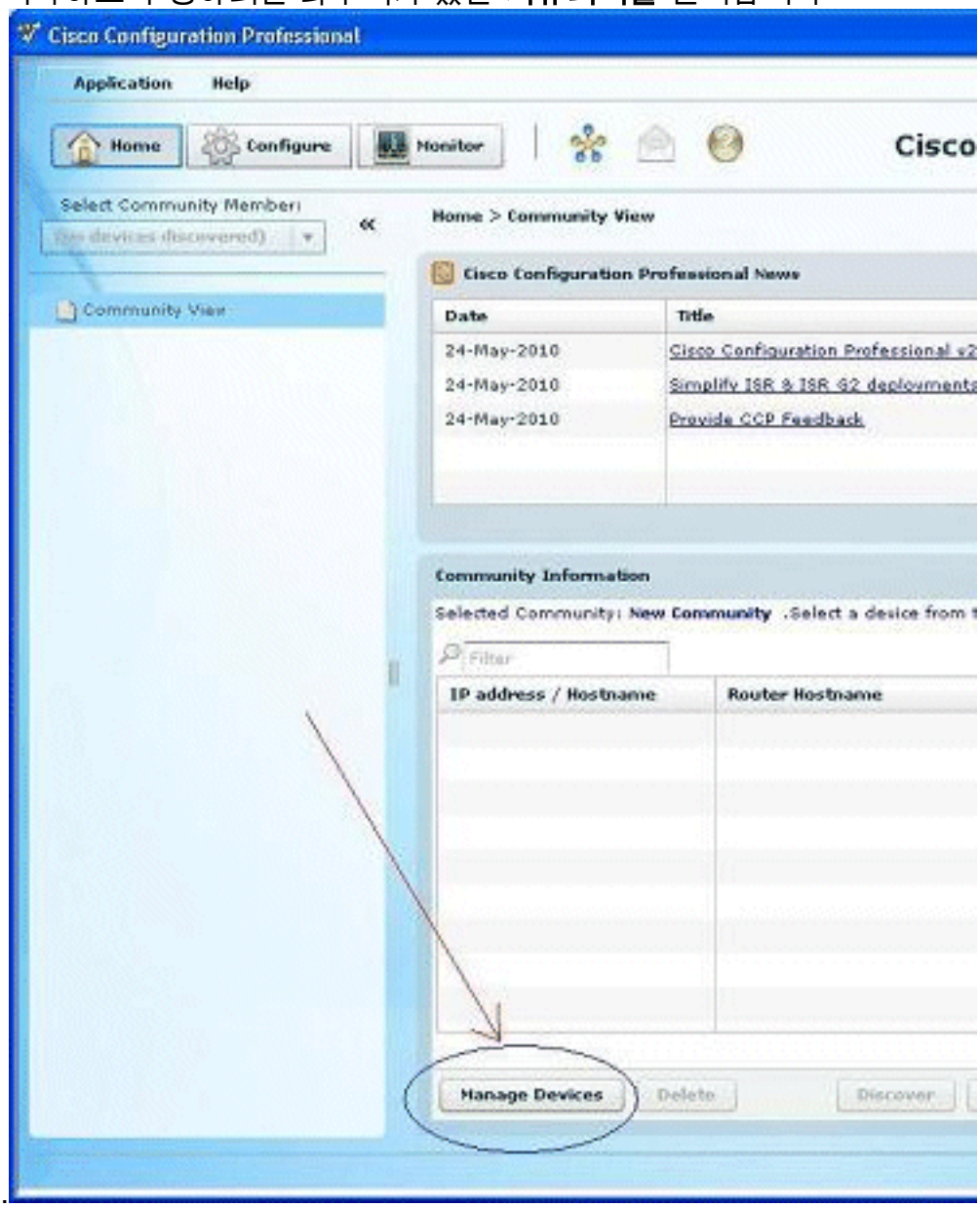
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든

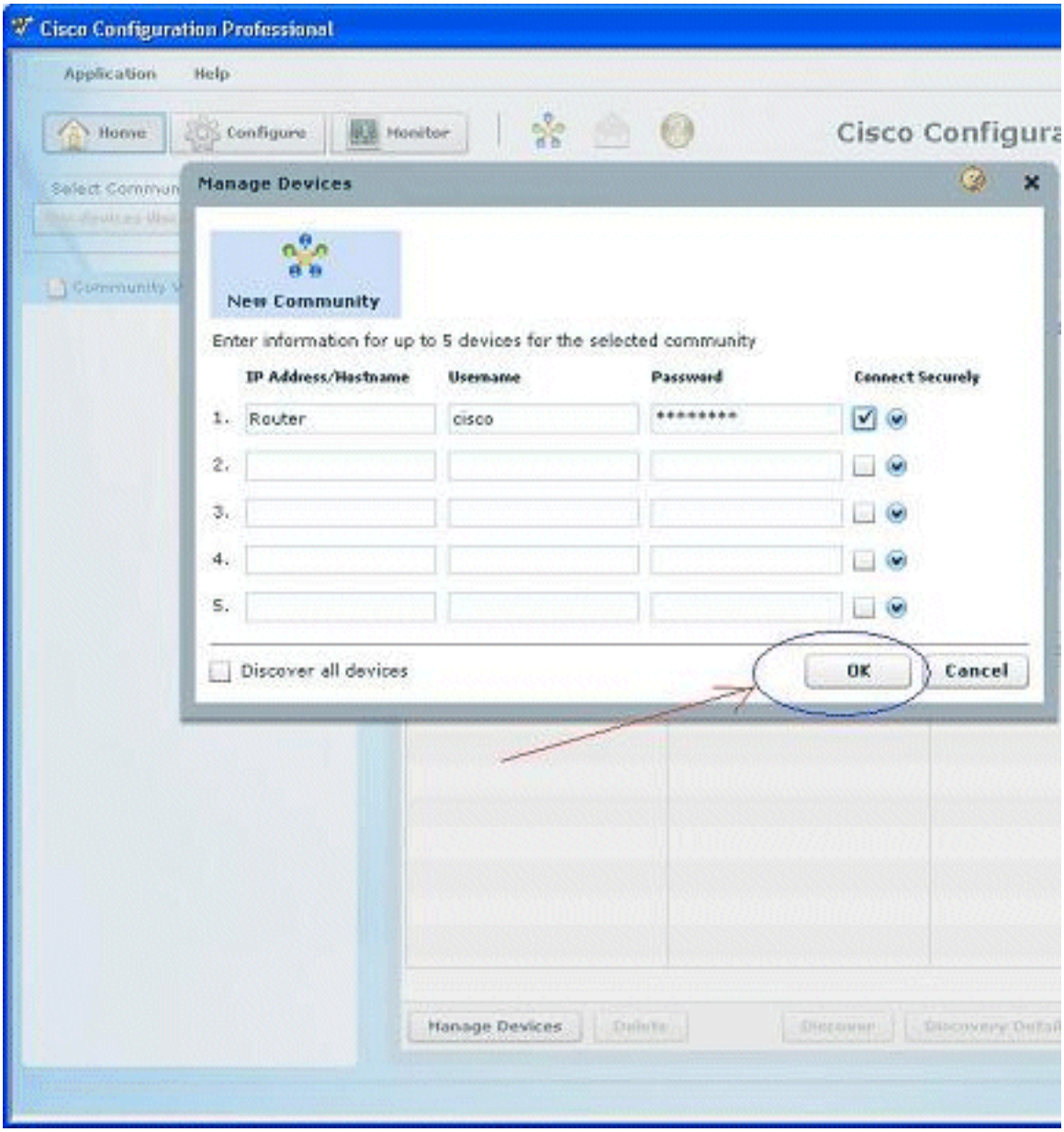
명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Cisco CP 설치

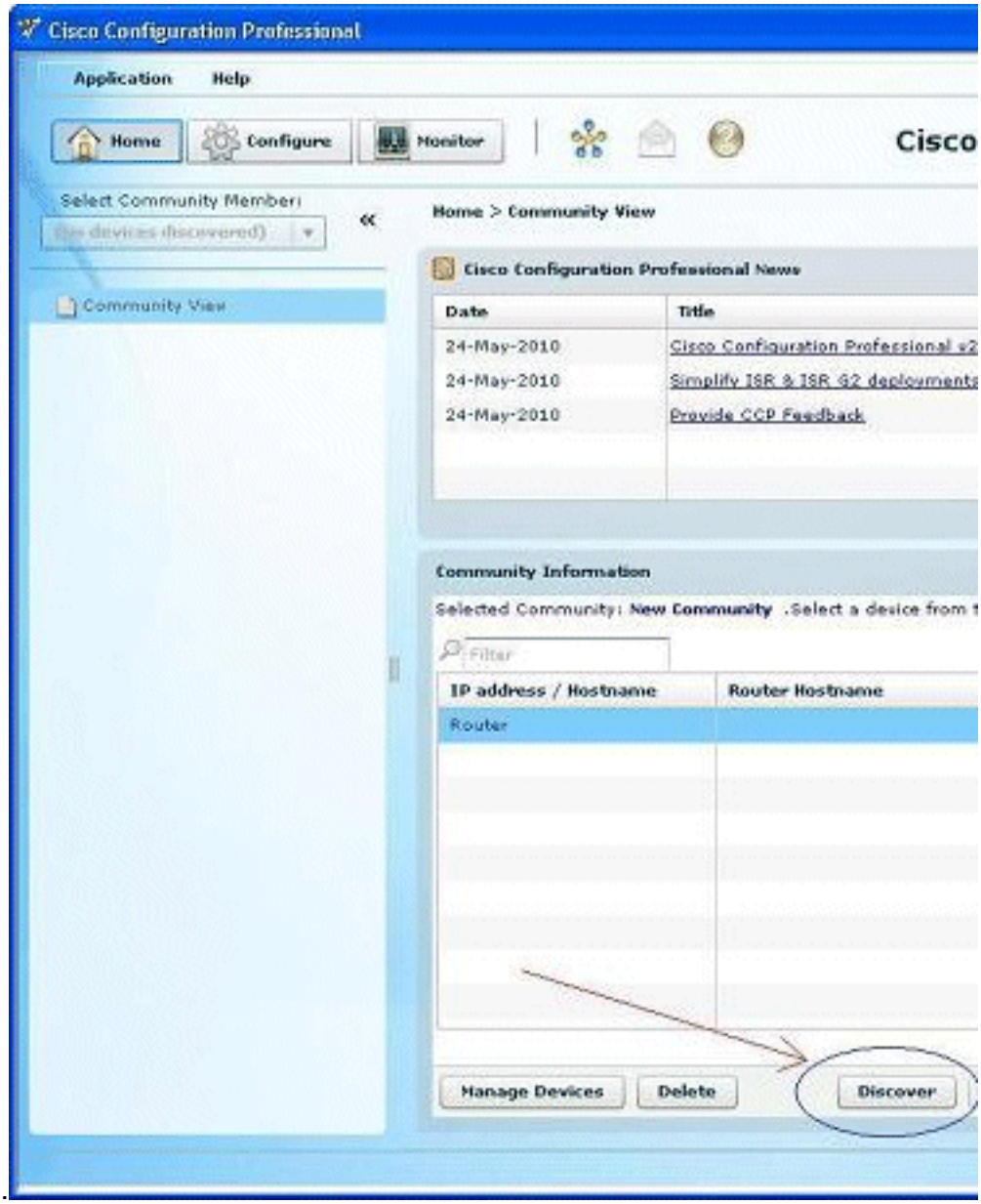
Cisco CP를 설치하려면 다음 단계를 수행하십시오.

1. Cisco Software Center에서 Cisco CP V2.1(등록된 고객만 해당)을 다운로드하여 로컬 PC에 설치합니다.최신 버전의 Cisco CP는 Cisco CP 웹 사이트에서 확인할 수 있습니다.
2. 로컬 PC에서 **시작 > 프로그램 > Cisco Configuration Professional(CCP)**을 통해 Cisco CP를 시작하고 구성하려는 라우터가 있는 **커뮤니티를** 선택합니다





3. 구성할 디바이스를 검색하려면 라우터를 강조 표시하고 Discover를 **클릭합니다**



참고: Cisco CP v2.1과 호환되는 Cisco 라우터 모델 및 IOS 릴리스에 대한 자세한 내용은 Compatible Cisco IOS 릴리스 섹션을 참조하십시오.

참고: Cisco CP v2.1을 실행하는 PC 요구 사항에 대한 자세한 내용은 시스템 요구 사항 섹션을 참조하십시오.

Cisco CP를 실행할 라우터 컨피그레이션

Cisco 라우터에서 Cisco CP를 실행하려면 다음 컨피그레이션 단계를 수행하십시오.

1. 텔넷, SSH 또는 콘솔을 통해 라우터에 연결합니다.다음 명령을 사용하여 전역 컨피그레이션 모드를 시작합니다.
```
Router(config)#enable
Router(config)#
```
2. HTTP 및 HTTPS가 활성화되어 비표준 포트 번호를 사용하도록 구성된 경우 이 단계를 건너뛰고 이미 구성된 포트 번호를 사용할 수 있습니다.다음 Cisco IOS Software 명령을 사용하여 라우터 HTTP 또는 HTTPS 서버를 활성화합니다.
```
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
```

3. 권한 수준이 15인 사용자를 만듭니다.
```
Router(config)# username privilege 15 password 0
```

참고: <username> 및 <password>를 구성하려는 사용자 이름과 암호로 **바꾸십시오.**

4. 로컬 로그인 및 권한 수준 15에 대해 SSH 및 텔넷을 구성합니다.
```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

5. (선택 사항) 로컬 로깅을 활성화하여 로그 모니터링 기능을 지원합니다.
```
Router(config)# logging buffered 51200 warning
```

요구 사항

이 문서에서는 Cisco 라우터가 완전히 작동 중이고 Cisco CP가 컨피그레이션을 변경할 수 있도록 구성되어 있다고 가정합니다.

Cisco CP를 사용하는 방법에 대한 자세한 내용은 Cisco Configuration Professional 시작 을 참조하십시오.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

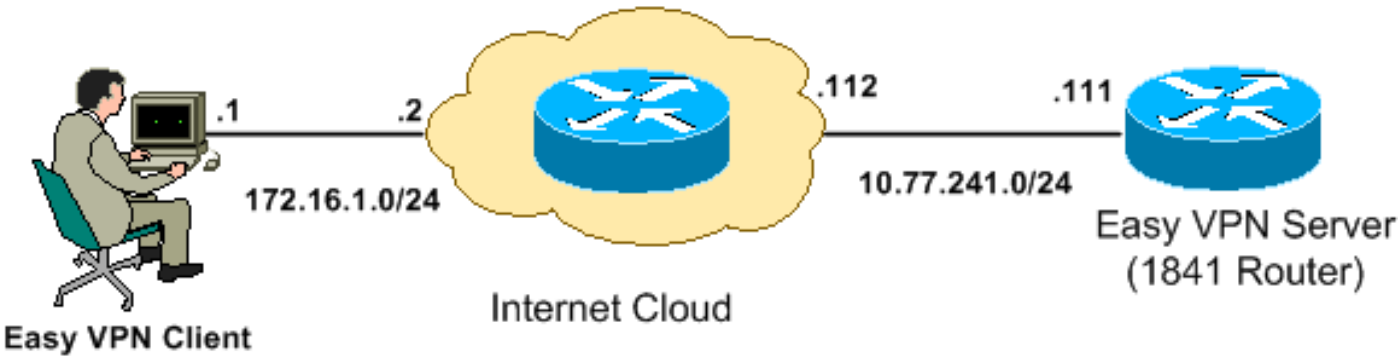
구성

이 섹션에서는 네트워크의 라우터에 대한 기본 설정을 구성하는 정보를 제공합니다.

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.

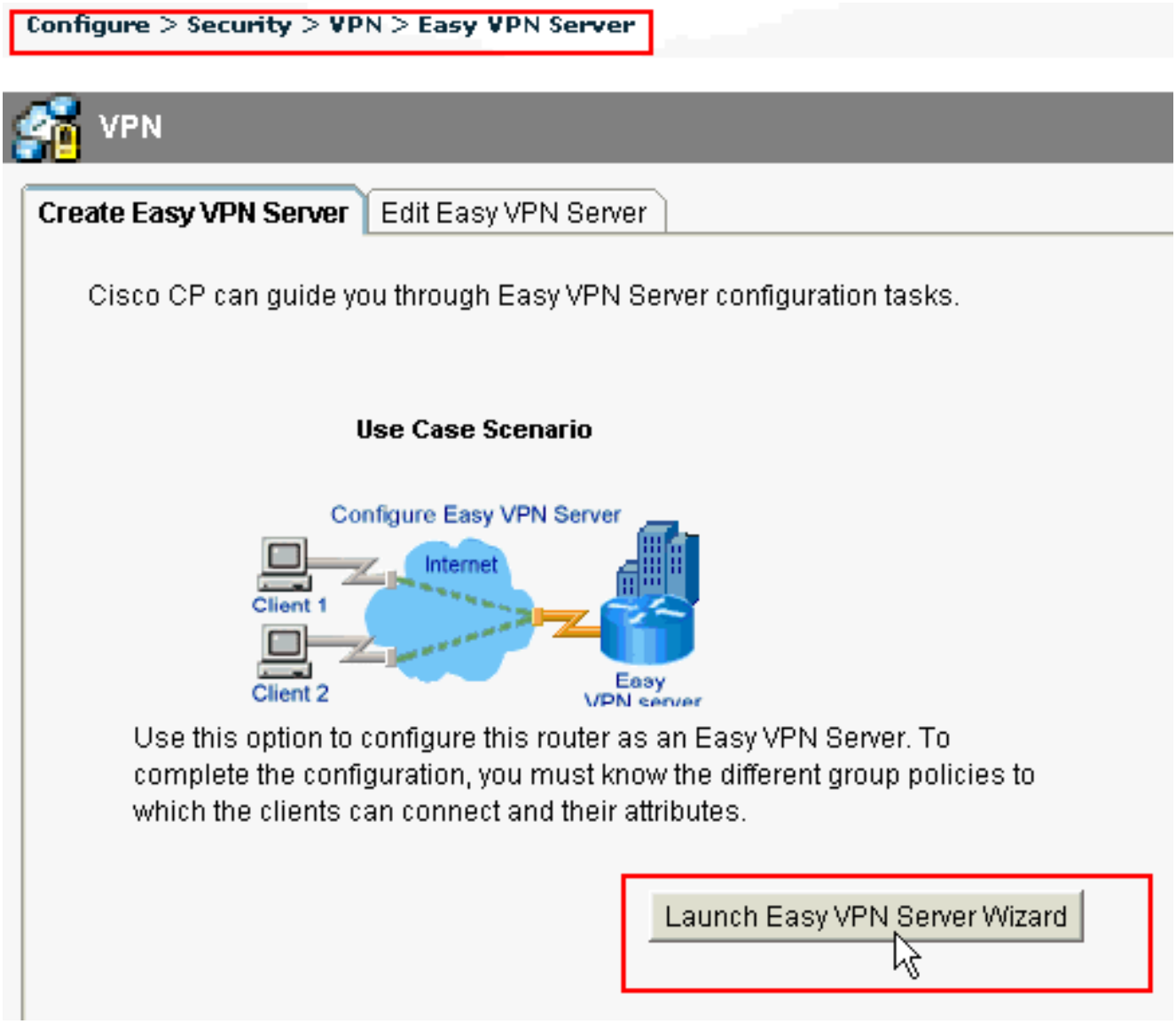


참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

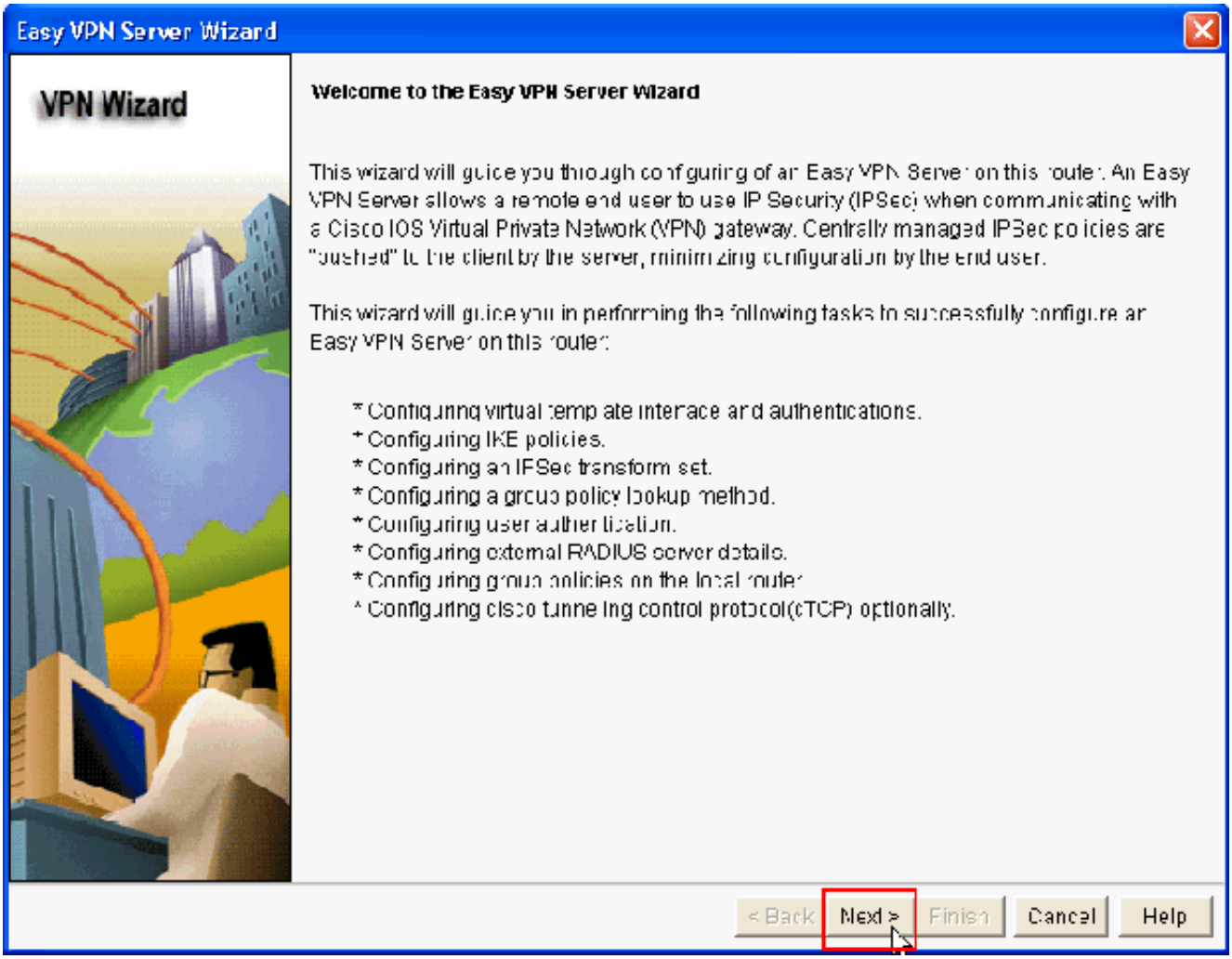
Cisco CP - Easy VPN 서버 컨피그레이션

Cisco IOS 라우터를 Easy VPN 서버로 구성하려면 다음 단계를 수행합니다.

1. Configure(**구성**) > **Security** > **VPN** > **Easy VPN Server(Easy VPN 서버)** > Create Easy VPN Server(**Easy VPN 서버 생성)를 선택하고 Launch Easy VPN Server Wizard(Easy VPN 서버 마법사 실행)를 클릭하여 Cisco IOS 라우터를 Easy VPN 서버로 구성합니다**
   .

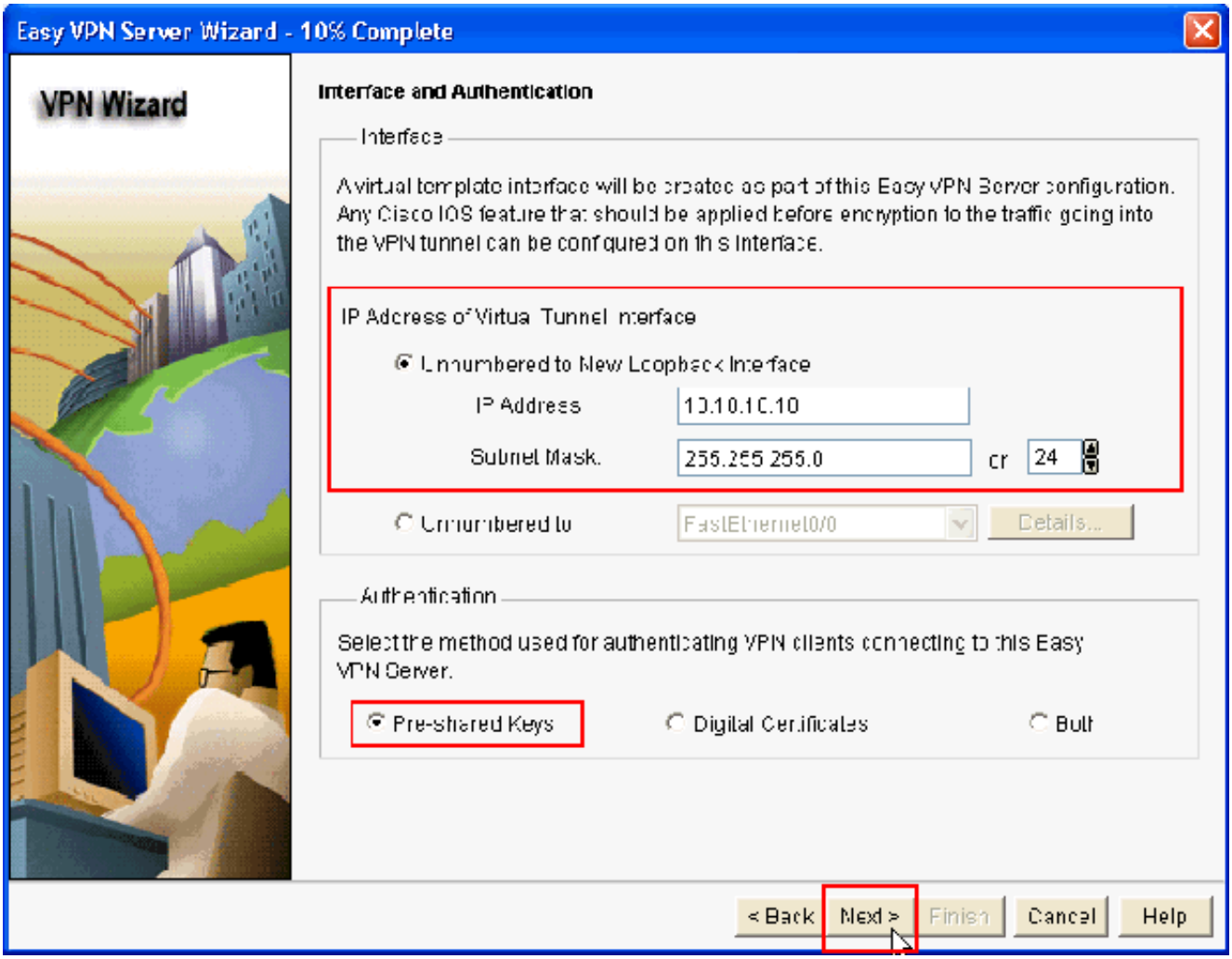


2. Easy **VPN Server** 컨피그레이션을 진행하려면 Next(다음)를 클릭합니다
   .



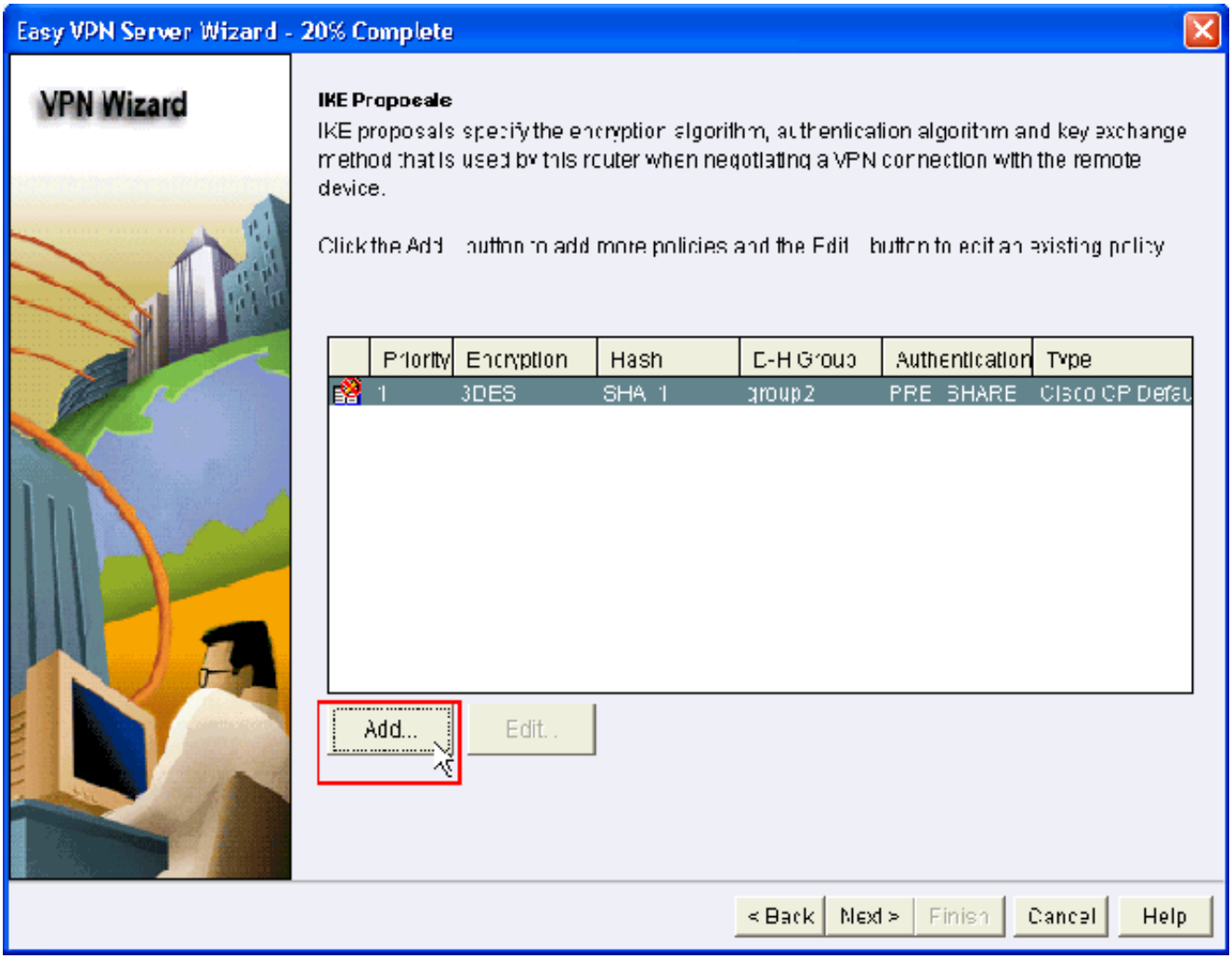
3. 결과 창에서 **가상 인터페이스**가 Easy VPN 서버 컨피그레이션의 일부로 구성됩니다.가상 **터널 인터페이스의 IP 주소를** 제공하고 VPN 클라이언트 인증에 사용되는 **인증 방법**을 선택합니다.여기서 **사전 공유 키**는 사용되는 인증 방법입니다.다음을 **클릭합니다**

.

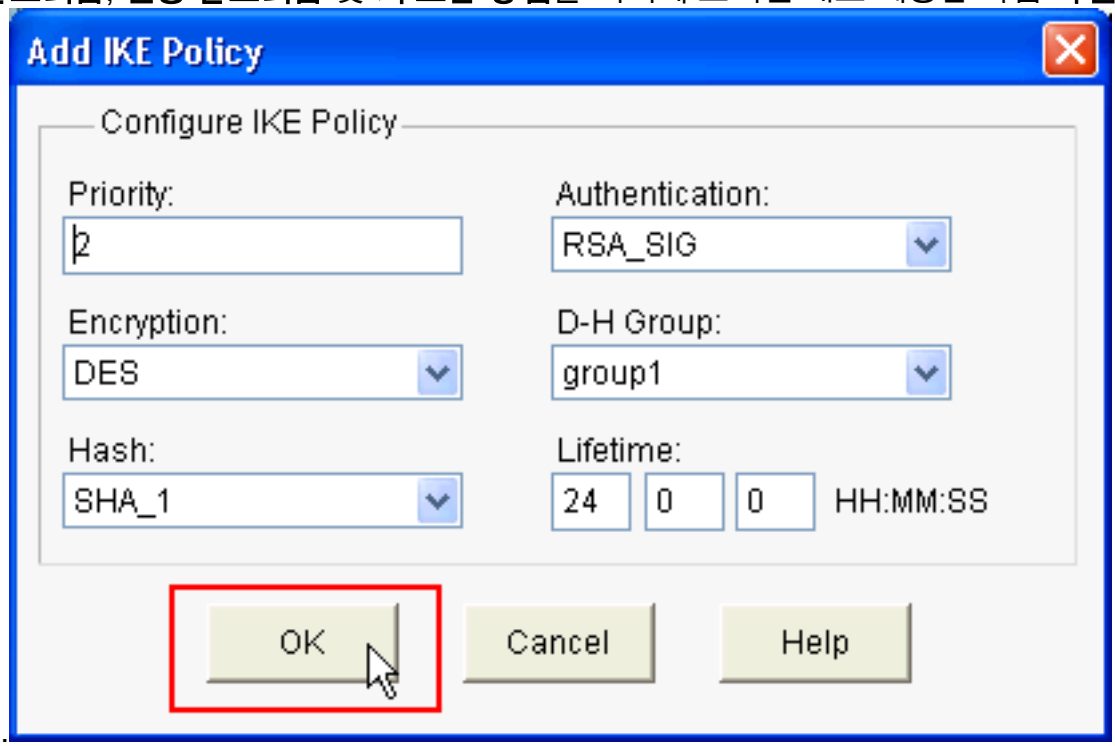


4. 원격 디바이스와 협상할 때 이 라우터에서 사용할 **암호화 알고리즘, 인증 알고리즘 및 키 교환 방법**을 지정합니다.필요한 경우 사용할 수 있는 기본 IKE 정책이 라우터에 있습니다.새 IKE 정책을 추가하려면 Add를 클릭합니다

.

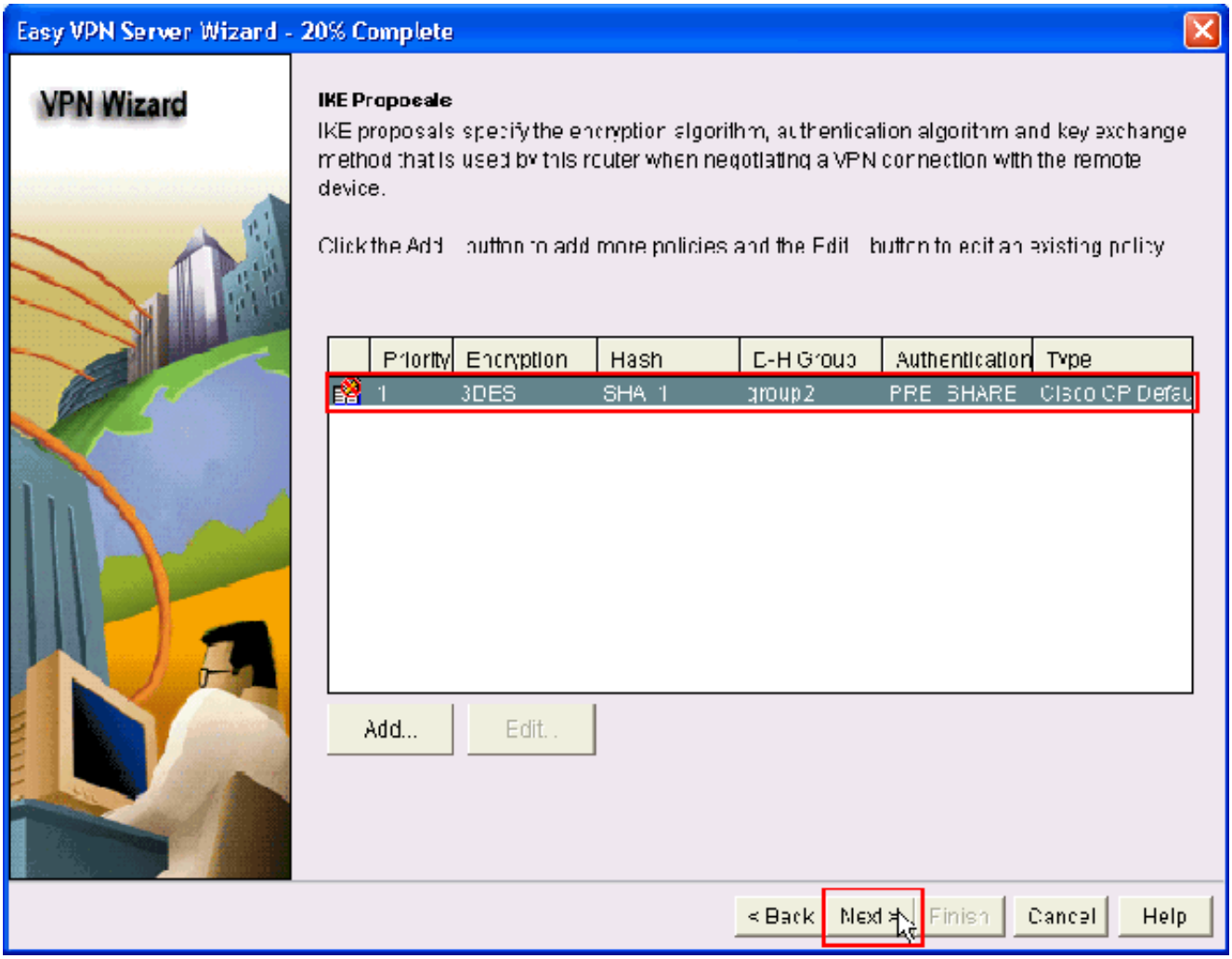


5. **암호화 알고리즘**, **인증 알고리즘** 및 **키 교환 방법**을 여기에 표시된 대로 제공한 다음 **확인**을 클릭합니다.



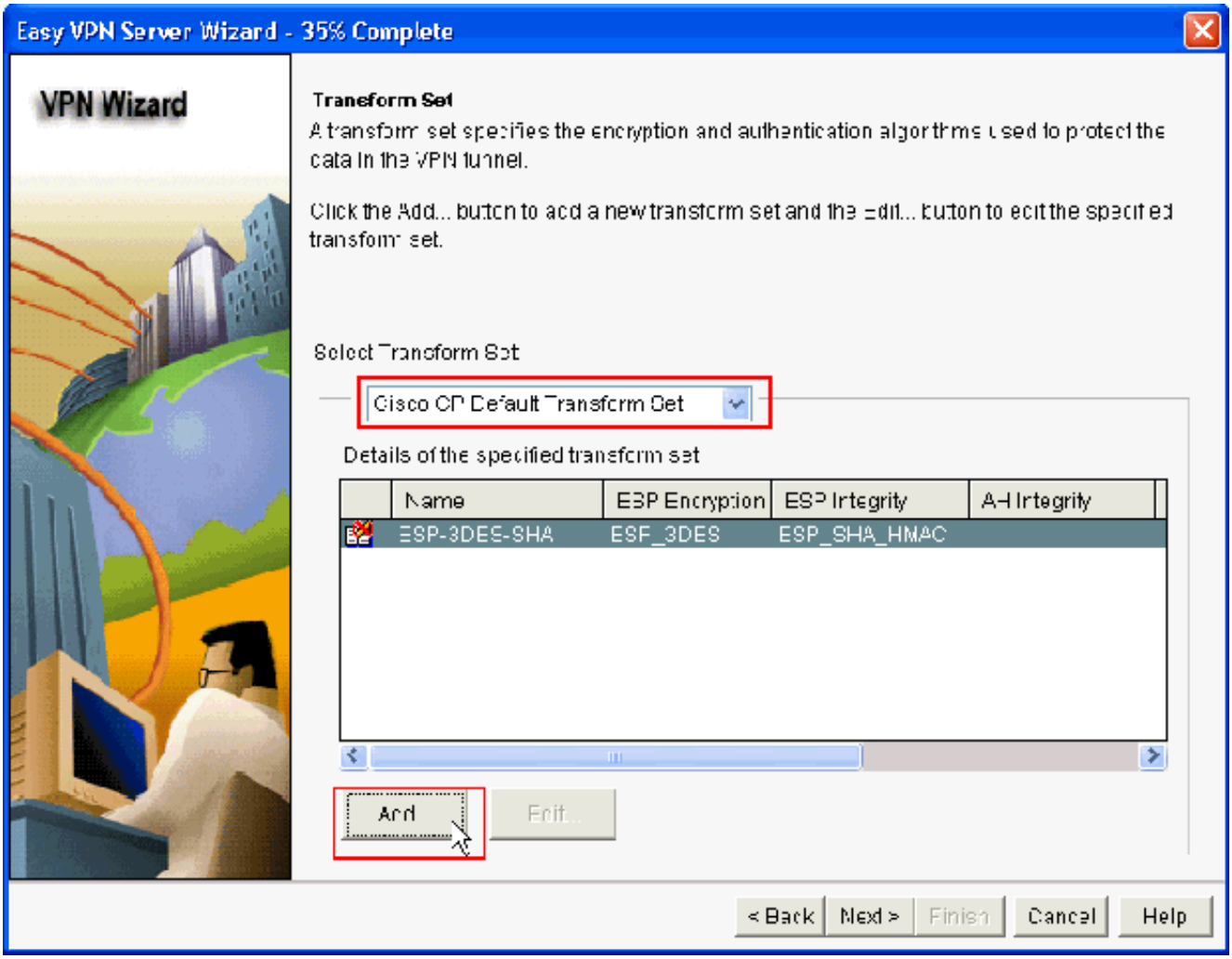
6. 이 **예에서는 기본 IKE 정책**이 사용됩니다.따라서 기본 IKE 정책을 선택하고 **Next(다음)**를 클릭합니다

.

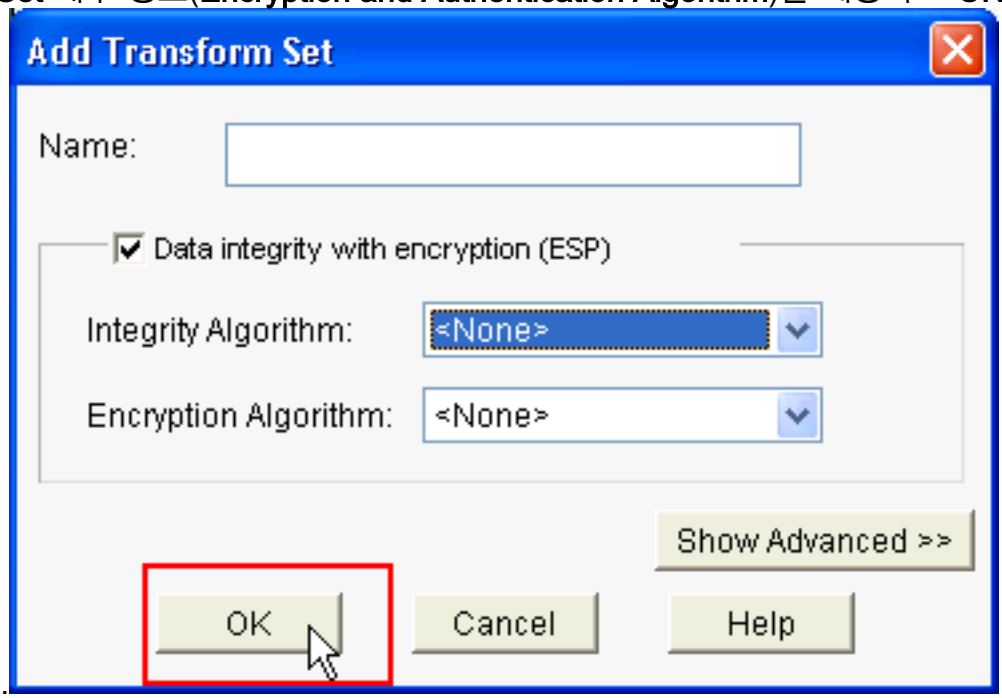


7. 새 창에서 **변형 집합** 세부사항을 제공해야 합니다.Transform Set는 **VPN 터널**에서 **데이터를 보호하는 데 사용되는 암호화** 및 **인증 알고리즘을 지정합니다**.Add(**추가**)를 클릭하여 이러한 세부 정보를 제공합니다.**추가**를 클릭하고 세부 정보를 제공할 때 필요에 따라 원하는 만큼의 변형 집합을 추가할 수 있습니다.**참고: Cisco CP**를 사용하여 구성할 경우 라우터에 **CP 기본 변형 집합**이 기본적으로 **표시됩니다**

.

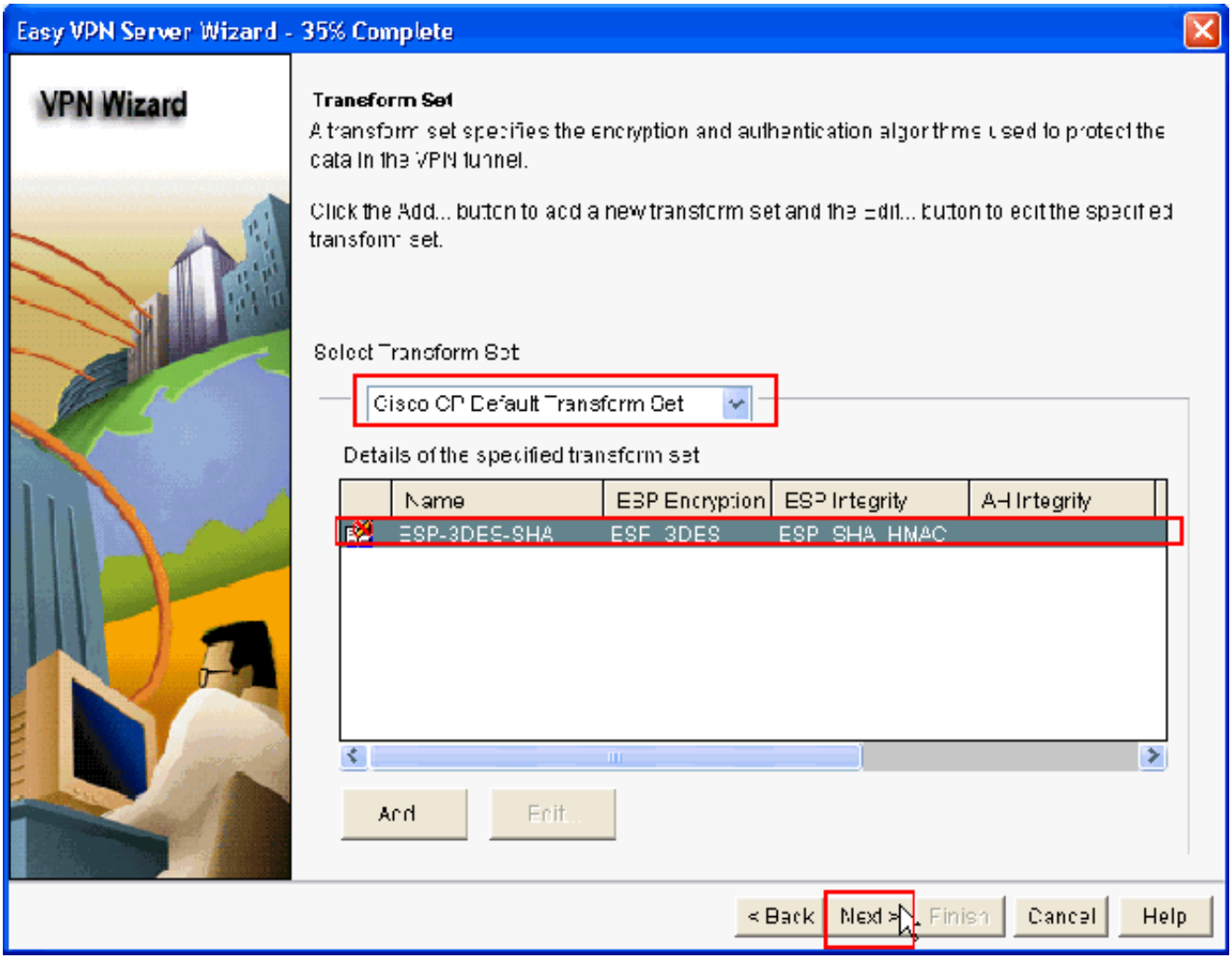


8. Transform **Set** 세부 정보(**Encryption and Authentication Algorithm**)를 제공하고 **OK**(확인)를 클릭합니다.

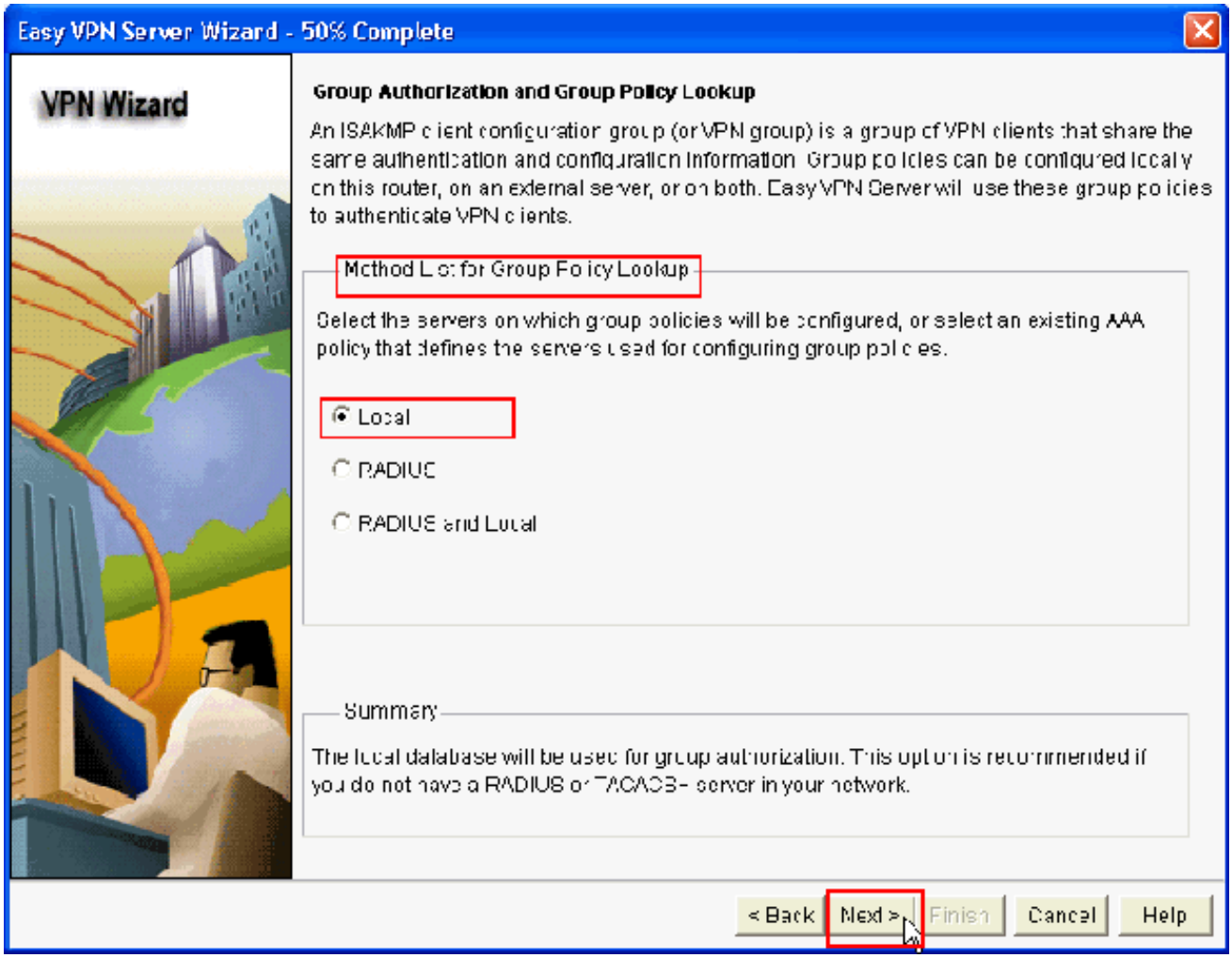


9. 이 예제에서는 **CP** Default **Transform Set라는 기본 변형 집합**이 사용됩니다.따라서 기본 변형 집합을 선택하고 **다음**을 클릭합니다

.

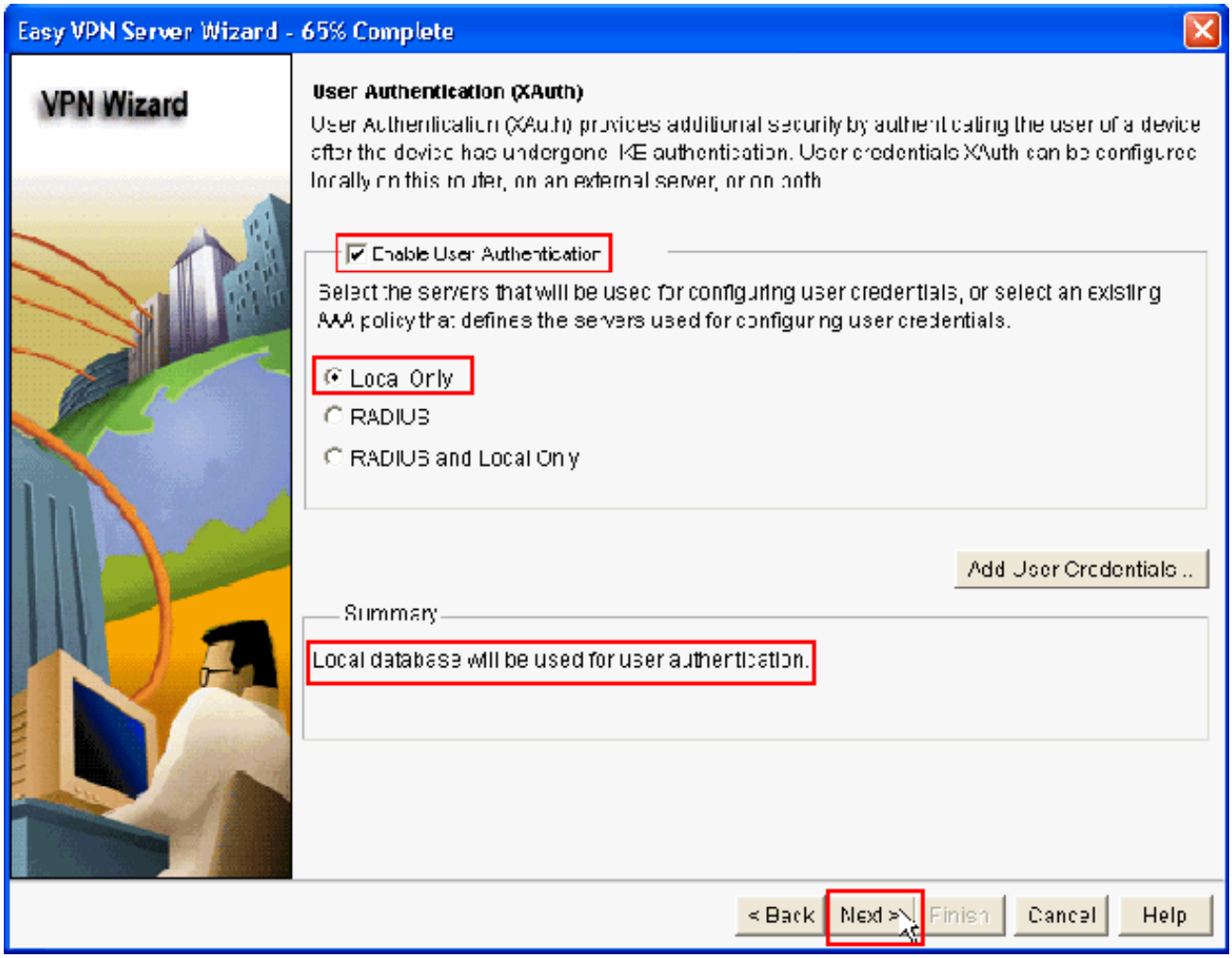


10. 새 창에서 그룹 정책을 구성할 서버를 선택합니다. 이 서버는 **로컬** 또는 **RADIUS** 또는 로컬 및 RADIUS**가** 될 수 있습니다.이 예에서는 **로컬 서버**를 사용하여 그룹 정책을 구성합니다 .Local(**로컬**)을 선택하고 **Next(다음)**를 클릭합니다
.



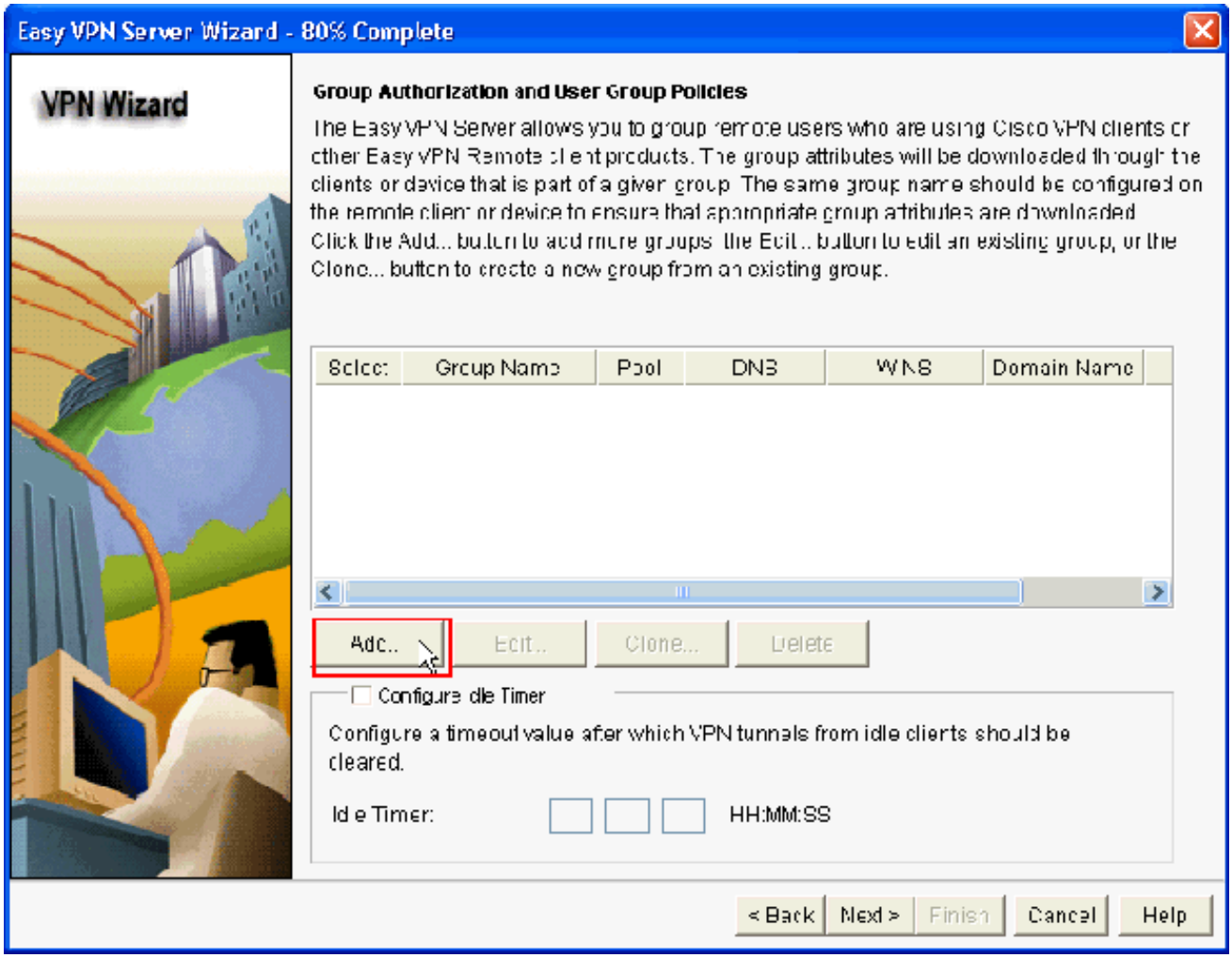
11. 이 새 창에서 User Authentication(사용자 인증)에 사용할 서버를 선택합니다. 이 창은 **Local Only(로컬 전용)** 또는 **RADIUS** 또는 Local Only(로컬 전용) **및 RADIUS일** 수 있습니다.이 예에서는 **로컬 서버**를 사용하여 인증을 위한 사용자 자격 증명을 구성합니다.Enable User Authentication(**사용자 인증 활성화**) 옆의 **확인란**이 선택되어 있는지 확인합니다.Local **Only(로컬 전용)**를 선택하고 **Next(다음)**를 클릭합니다

.



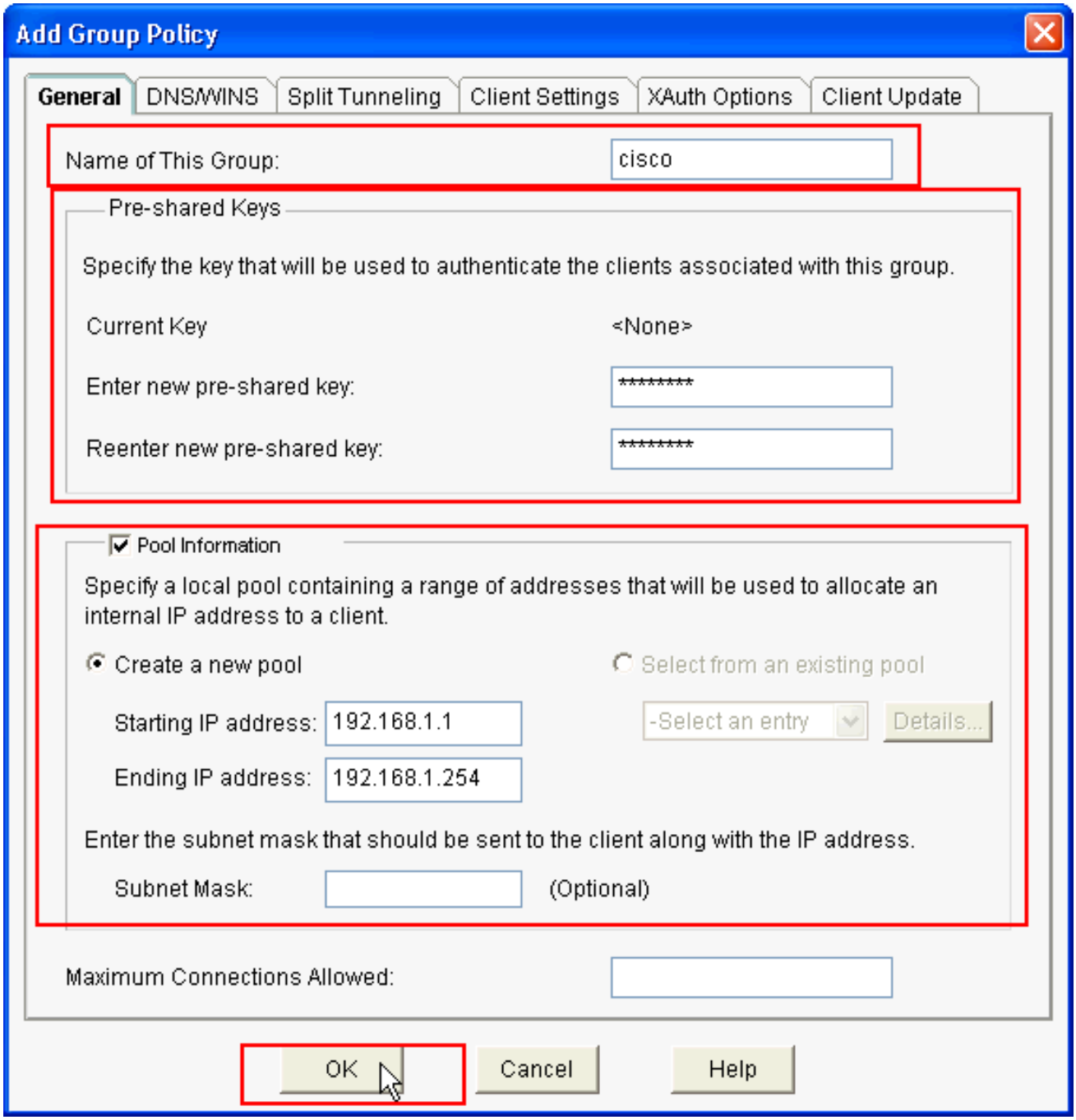
12. Add(**추가**)를 클릭하여 새 그룹 정책을 만들고 이 그룹에 원격 사용자를 추가합니다

.

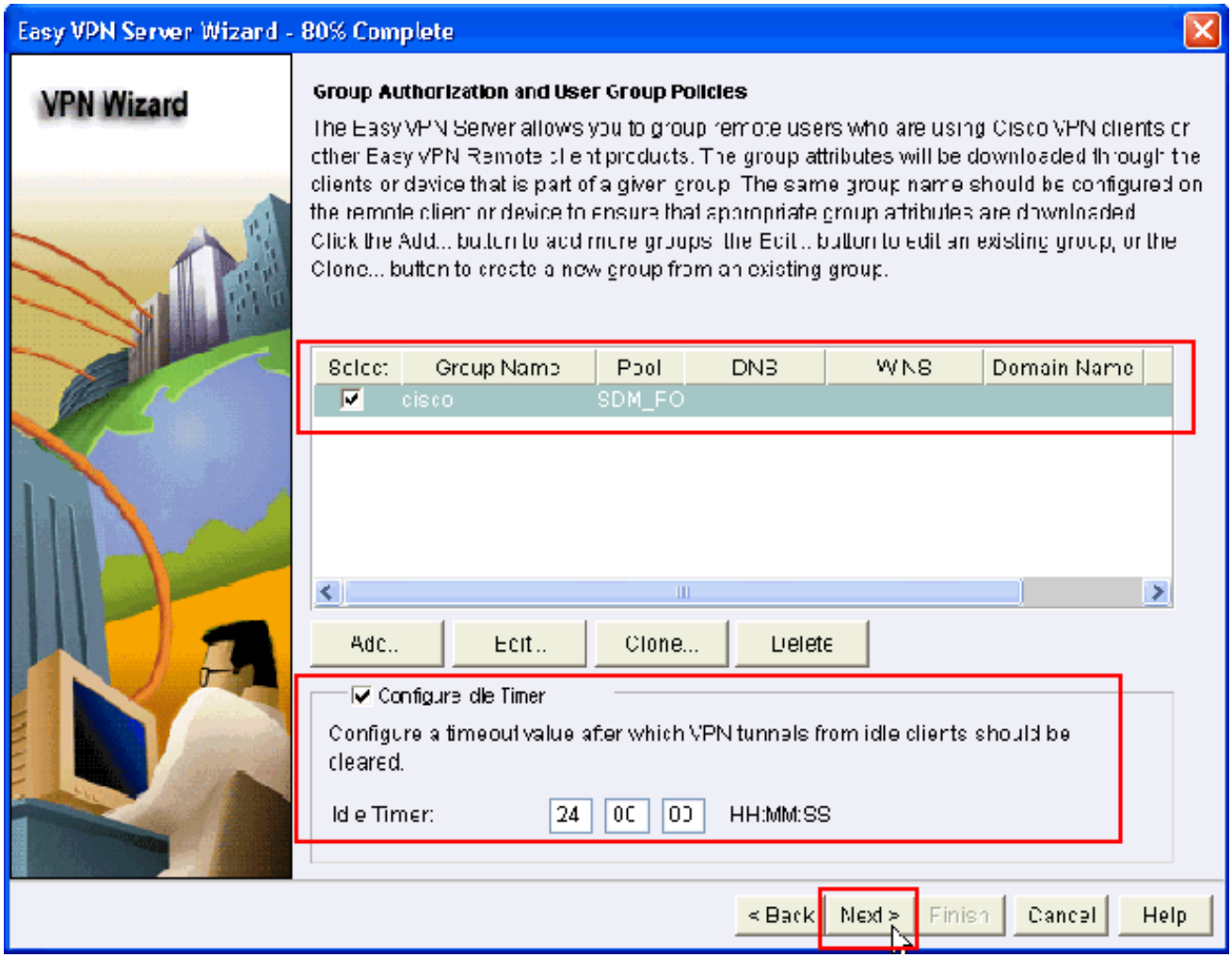


13. Add Group Policy(그룹 정책 추가) 창에서 이 그룹의 이름(이 예에서는 cisco)에 대한 그룹 이름을 사전 공유 키와 IP 풀(시작 IP 주소 및 **끝 IP 주소**) 정보를 제공하는 공간에 입력하고 **OK(확인)를 클릭합니다.참고:** 새 IP 풀을 생성하거나 기존 IP 풀이 있는 경우 사용할 수 있습니다

.

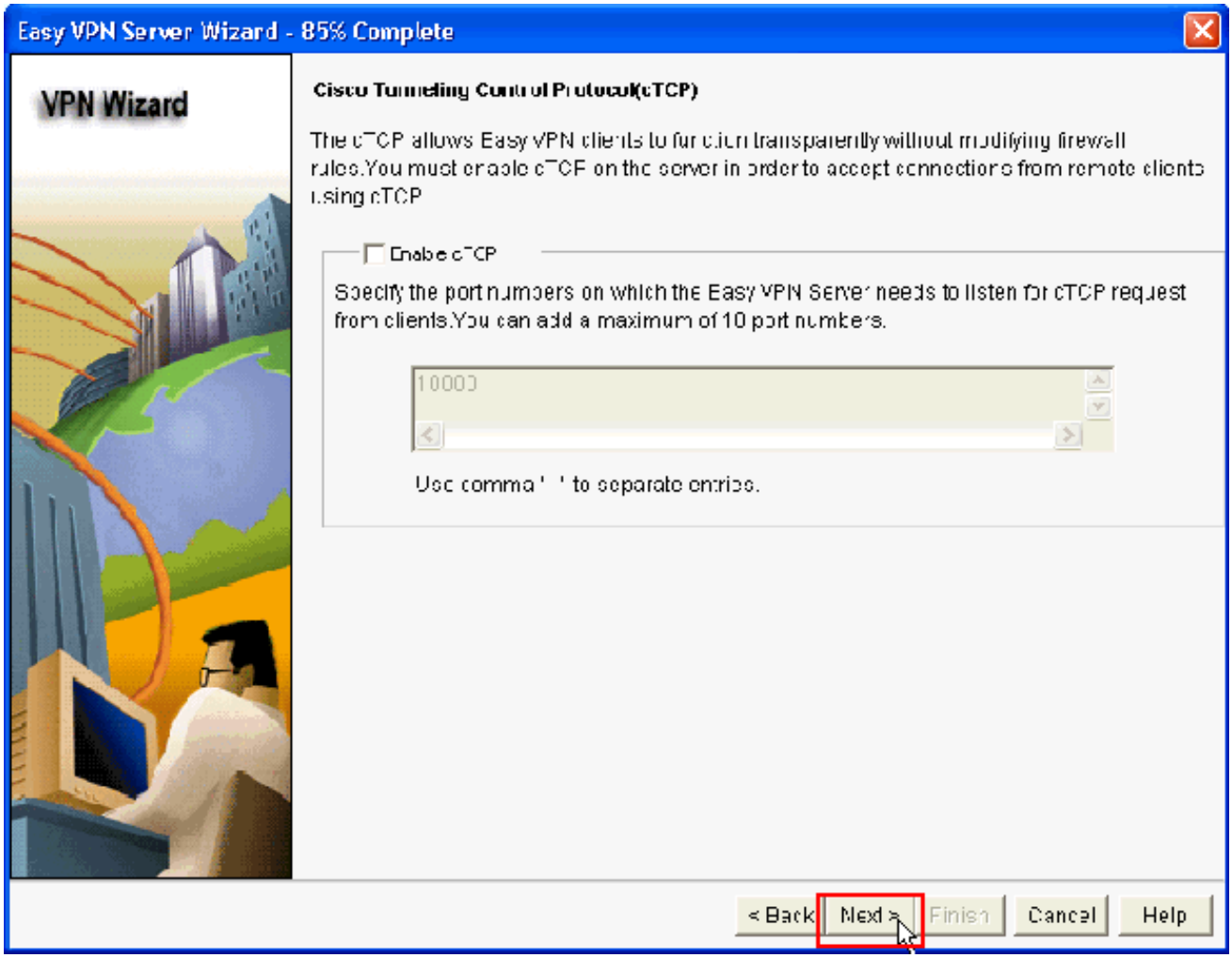


14. 이제 **cisco** 이름**으로** 생성된 새 **그룹 정책**을 선택한 다음 Configure Idle Timer(유휴 타이머 구성) 옆에 있는 확인란을 클릭하여 **유휴 타이머**를 구성합니다.Next(**다음)를 클릭합니다**
.



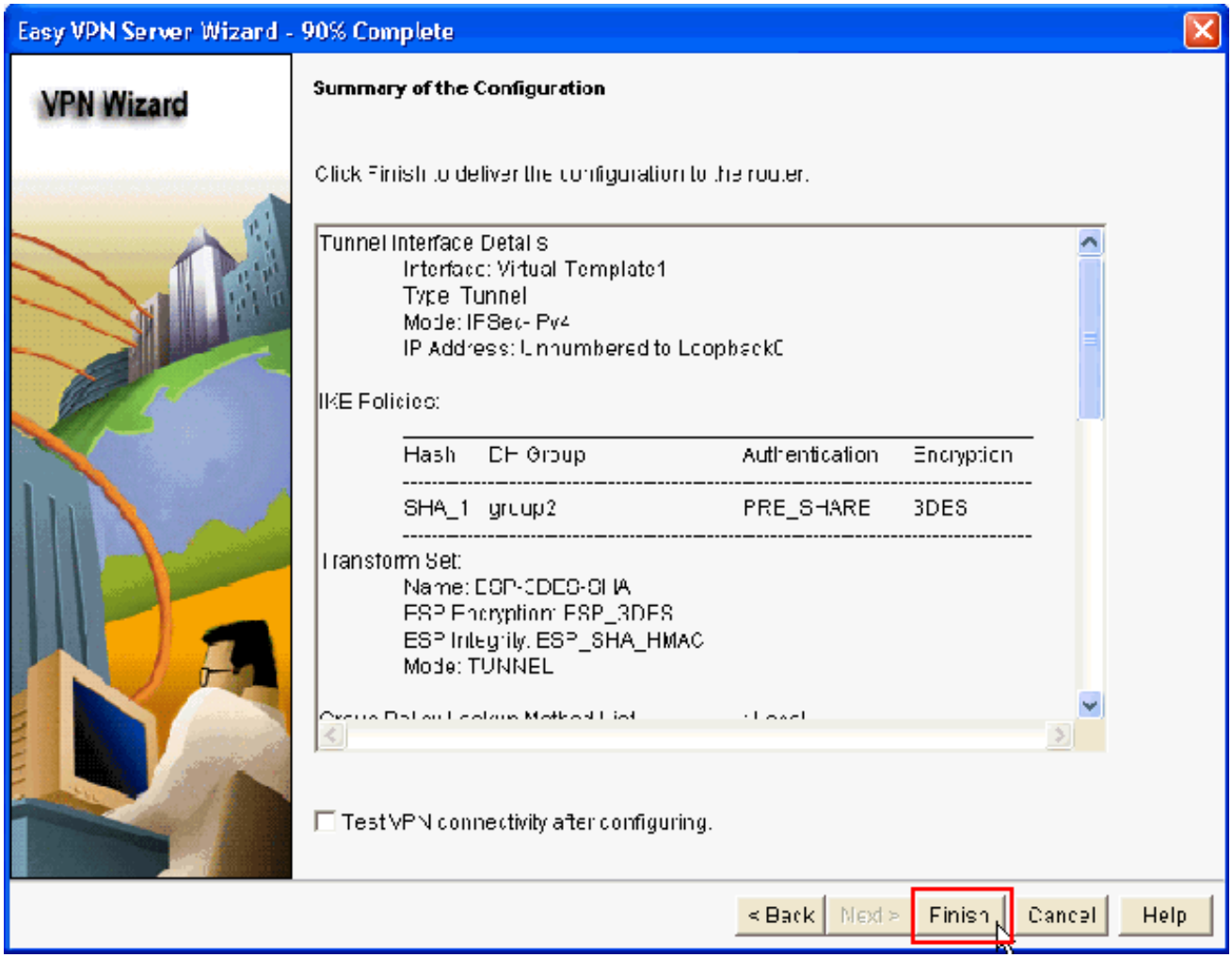
15. 필요한 경우 **Cisco Tunneling Control Protocol**(cTCP)을 활성화합니다.그렇지 않으면 **다음**을 클릭합니다

.



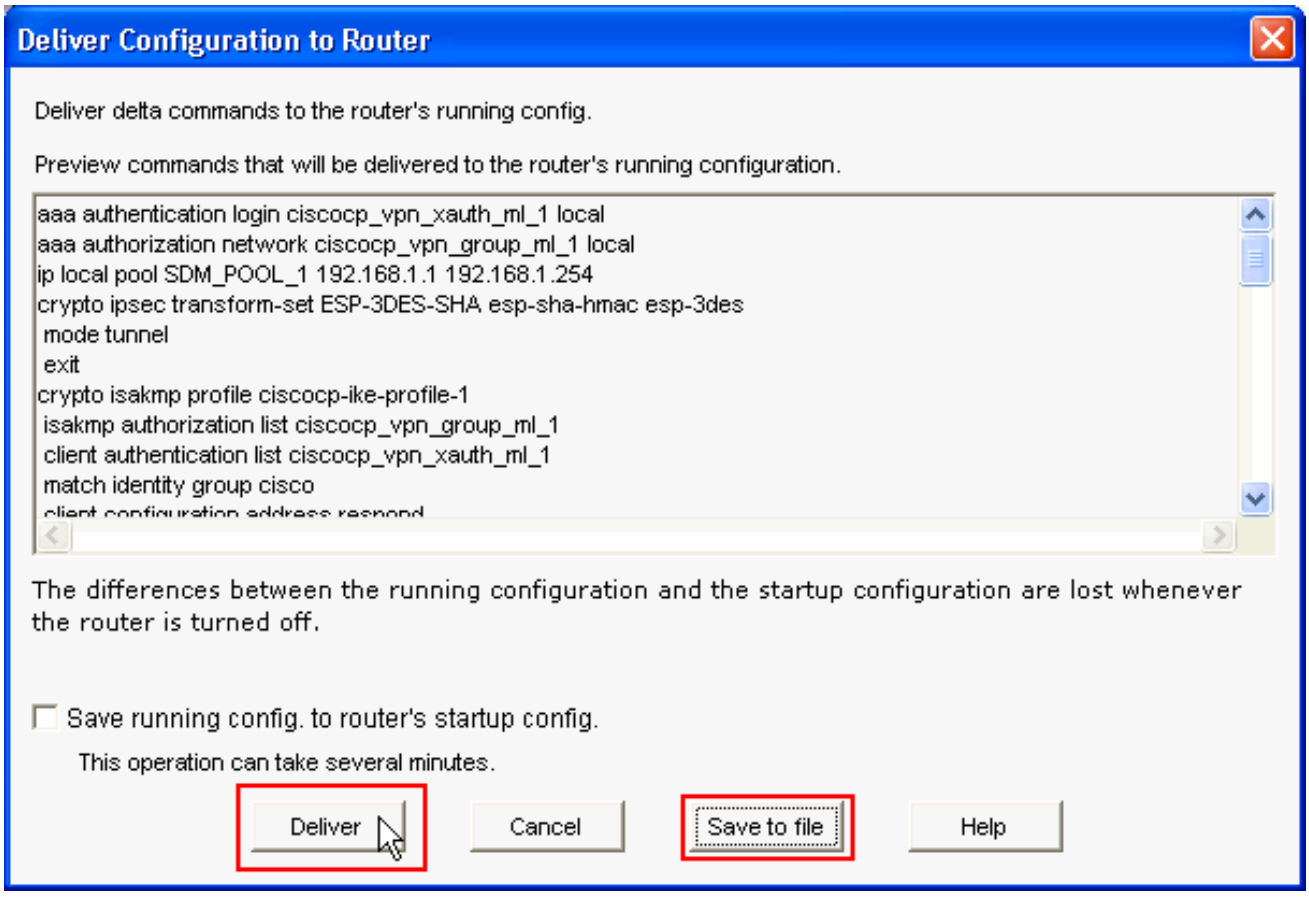
16. 구성 **요약을 검토합니다.마침을 클릭합니다**

.

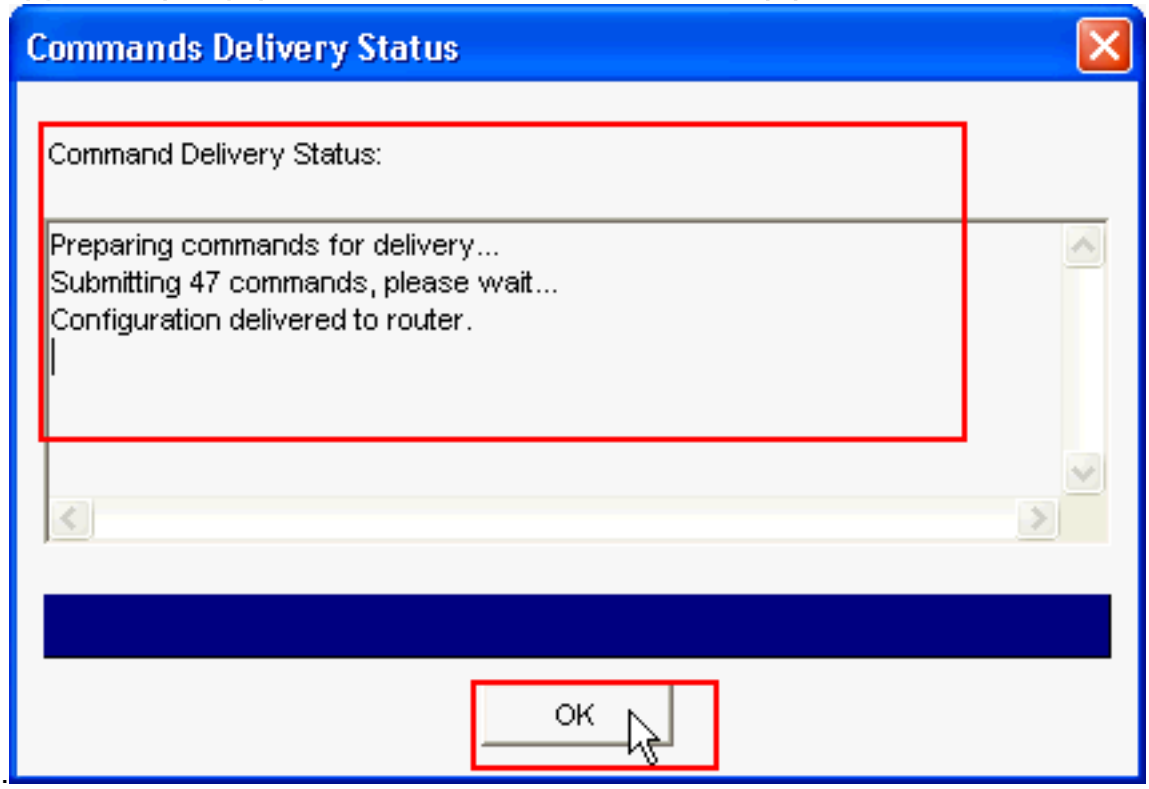


17. Deliver Configuration to **Router** 창에서 **Deliver**를 클릭하여 라우터에 컨피그레이션을 전달합니다.Save to file(**파일에 저장)을** 클릭하여 PC에 컨피그레이션을 파일로 저장할 수 있습니다

.



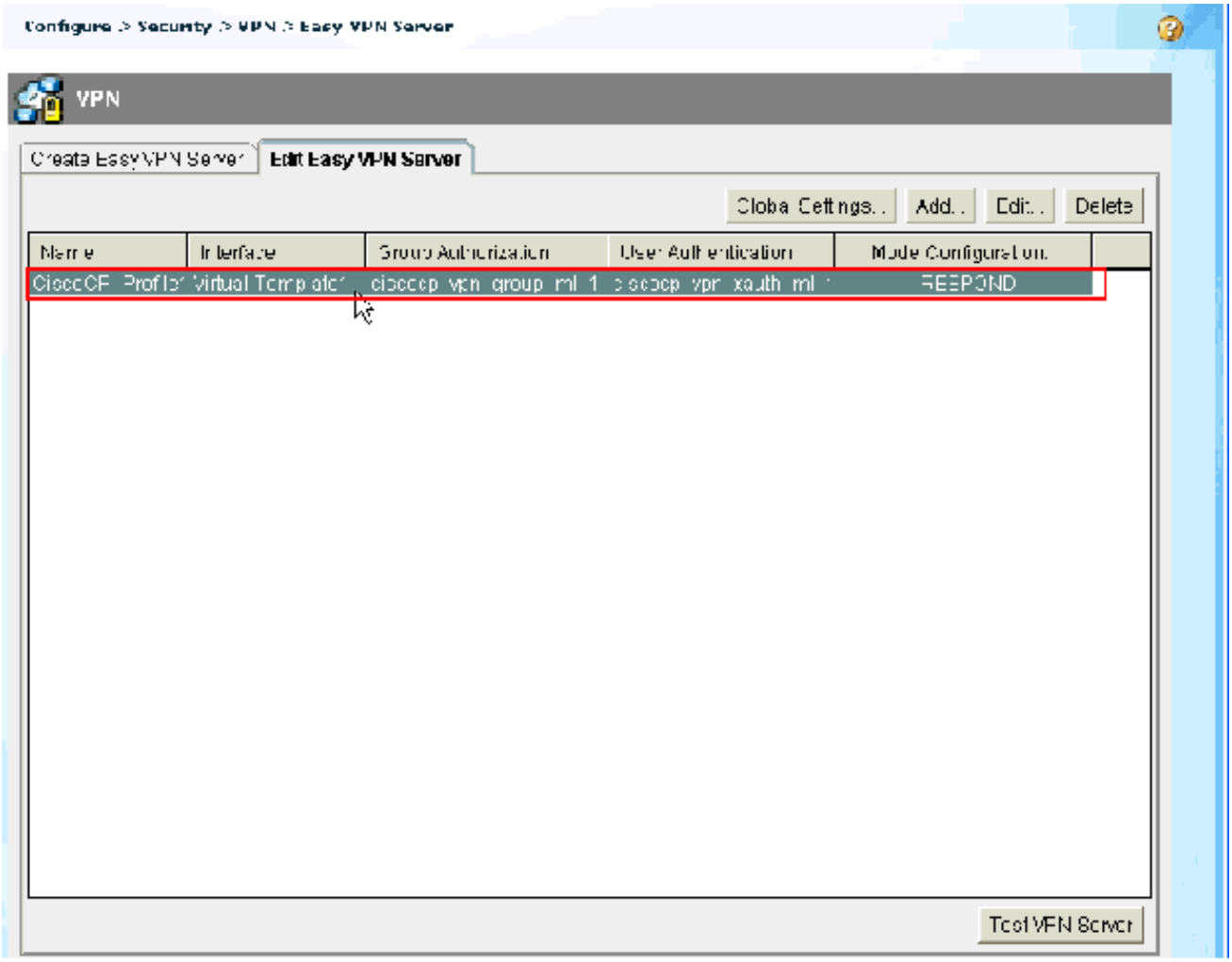
18. Command **Delivery Status** 창에는 라우터에 대한 명령의 전달 상태가 표시됩니다.**라우터에 제공된 컨피그레이션으로** 나타납니다.**확인**을 **클릭합니다**



.

19. 새로 생성된 Easy VPN Server를 볼 수 있습니다.Edit Easy **VPN Server(Easy VPN 서버 수정)**를 선택하여 기존 서버를 편집할 수 있습니다.이렇게 하면 Cisco IOS 라우터에서 Easy VPN Server 컨피그레이션이 완료됩니다

.



CLI 컨피그레이션

라우터 컨피그레이션

```
Router#show run
Building configuration...

Current configuration : 2069 bytes
! version 12.4 service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption hostname Router boot-start-marker
boot-end-marker no logging buffered enable password
cisco !---AAA enabled using aaa newmodel command. Also
AAA Authentication and Authorization are enabled---! aaa
new-model
!
!
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization network ciscocp_vpn_group_ml_1 local
!
!
aaa session-id common
ip cef
!
!
!
!
ip domain name cisco.com
!
```

```
multilink bundle-name authenticated
!
!
!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
used during an IKE negotiation. Encryption and Policy
details are hidden as the default values are chosen.
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10
!
crypto isakmp client configuration group cisco
 key cisco123
 pool SDM_POOL_1
crypto isakmp profile ciscocp-ike-profile-1
   match identity group cisco
   client authentication list ciscocp_vpn_xauth_ml_1
   isakmp authorization list ciscocp_vpn_group_ml_1
   client configuration address respond
   virtual-template 1
!
!
!--- Configuration for IPsec policies. !--- Enables the
crypto transform configuration mode, !--- where you can
specify the transform sets that are used !--- during an
IPsec negotiation. crypto ipsec transform-set ESP-3DES-
SHA esp-3des esp-sha-hmac
!
crypto ipsec profile CiscoCP_Profile1
 set security-association idle-time 86400
 set transform-set ESP-3DES-SHA
 set isakmp-profile ciscocp-ike-profile-1
!
!
!
!--- RSA certificate generated after you enable the !---
ip http secure-server command.

crypto pki trustpoint TP-self-signed-1742995674
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1742995674
 revocation-check none
 rsakeypair TP-self-signed-1742995674

!--- Create a user account named cisco123 with all
privileges.

username cisco123 privilege 15 password 0 cisco123
archive
 log config
  hidekeys
!
!
!--- Interface configurations are done as shown below---
! interface Loopback0 ip address 10.10.10.10
255.255.255.0 ! interface FastEthernet0/0 ip address
10.77.241.111 255.255.255.192 duplex auto speed auto !
interface Virtual-Template1 type tunnel ip unnumbered
Loopback0 tunnel mode ipsec ipv4 tunnel protection ipsec
profile CiscoCP_Profile1 ! !--- VPN pool named
SDM_POOL_1 has been defined in the below command---! ip
```

```
local pool SDM_POOL_1 192.168.1.1 192.168.1.254

!--- This is where the commands to enable HTTP and HTTPS
are configured. ip http server ip http authentication
local ip http secure-server ! ! ! ! control-plane ! line
con 0 line aux 0 !--- Telnet enabled with password as
cisco. line vty 0 4 password cisco transport input all
scheduler allocate 20000 1000 ! ! ! ! end
```

다음을 확인합니다.

Easy VPN Server - show 명령

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

- **show crypto isakmp sa** - 피어의 현재 IKE SA를 모두 표시합니다.

```
Router#show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.77.241.111   172.16.1.1     QM_IDLE           1003    0 ACTIVE
```

- **show crypto ipsec sa** - 피어에 있는 모든 현재 IPsec SA를 표시합니다.

```
Router#show crypto ipsec sa
interface: Virtual-Access2
    Crypto map tag: Virtual-Access2-head-0, local addr 10.77.241.111

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0)
   current_peer 172.16.1.1 port 1086
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
    #pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 2

     local crypto endpt.: 10.77.241.111, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x186C05EF(409732591)

     inbound esp sas:
      spi: 0x42FC8173(1123844467)
        transform: esp-3des esp-sha-hmac
```

문제 해결

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: 디버그 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

관련 정보

- IPSec 협상/IKE 프로토콜
- Cisco Configuration Professional 빠른 시작 가이드
- Cisco 제품 지원 페이지 - 라우터
- 기술 지원 및 문서 – Cisco Systems