정적으로 주소가 지정된 ASA와 CCP 컨피그레이션을 사용하는 동적으로 주소가 지정된 Cisco IOS 라우터 간의 동적 IPsec 터널 예

목차

소개

이 문서에서는 PIX/ASA Security Appliance가 Cisco IOS® 라우터에서 동적 IPsec 연결을 수락하도록 하는 방법에 대한 샘플 컨피그레이션을 제공합니다.이 시나리오에서는 IPsec 터널이 라우터 끝에서만 시작되는 시점을 설정합니다.동적 IPsec 컨피그레이션으로 인해 ASA에서 VPN 터널을 시작할 수 없습니다.

이 컨피그레이션을 통해 PIX Security Appliance는 원격 VPN 라우터를 사용하여 동적 IPsec LAN-to-LAN(L2L) 터널을 생성할 수 있습니다.이 라우터는 인터넷 서비스 공급자로부터 외부 공용 IP 주소를 동적으로 수신합니다.DHCP(Dynamic Host Configuration Protocol)는 제공자로부터 동적으로 IP 주소를 할당하기 위해 이 메커니즘을 제공합니다.이렇게 하면 호스트가 더 이상 필요하지 않을 때 IP 주소를 재사용할 수 있습니다.

라우터의 컨피그레이션은 CCP(Cisco Configuration Professional)를 사용하여 수행됩니다.CCP는 Cisco IOS 기반 라우터를 구성할 수 있는 GUI 기반 디바이스 관리 툴입니다.CCP로 라우터를 구성하는 방법에 대한 자세한 내용은 Cisco Configuration Professional을 사용하여 기본 라우터 컨피그레이션을 참조하십시오.

ASA 및 Cisco IOS 라우터를 사용하는 IPsec 터널 설정에 대한 자세한 내용과 컨피그레이션 예는 ASA가 포함된 Site-to-Site VPN(L2L)을 참조하십시오.

자세한 내용과 PIX 및 Cisco IOS 라우터를 사용하여 동적 IPSec 터널 설정에 대한 컨피그레이션 예는 IOS와 함께 사이트 간 VPN(L2L)을 참조하십시오.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 IPSEC 터널을 설정하기 위해 ASA와 라우터에 모두 인터넷 연결이 설정되어 있는지 확인하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 12.4를 실행하는 Cisco IOS Router1812
- Cisco ASA 5510 소프트웨어 릴리스 8.0.3

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 규칙을 참조하십시오.

배경 정보

이 시나리오에서는 192.168.100.0 네트워크가 ASA에 뒤쳐지고 192.168.200.0 네트워크가 Cisco IOS 라우터 뒤에 있습니다.라우터가 ISP에서 DHCP를 통해 공용 주소를 얻는다고 가정합니다.ASA 엔드에서의 정적 피어 컨피그레이션에 문제가 있으므로 ASA와 Cisco IOS 라우터 간에 사이트 간 터널을 설정하기 위해 동적 암호화 컨피그레이션 방식에 접근해야 합니다.

ASA 엔드에서의 인터넷 사용자는 외부 인터페이스의 IP 주소로 변환됩니다.NAT가 Cisco IOS 라우터 끝에 구성되지 않은 것으로 가정합니다.

다음은 동적 터널을 설정하기 위해 ASA 엔드에서 구성하는 주요 단계입니다.

1. 1단계 ISAKMP 관련 컨피그레이션
2. NAT 예외 컨피그레이션
3. 동적 암호화 맵 컨피그레이션

ASA에 고정 공용 IP 주소가 있는 것으로 간주되므로 Cisco IOS 라우터에는 고정 암호화 맵이 구성되어 있습니다.다음은 동적 IPSEC 터널을 설정하기 위해 Cisco IOS Router 엔드에서 구성할 기본 단계 목록입니다.

1. 1단계 ISAKMP 관련 컨피그레이션
2. 고정 암호화 맵 관련 컨피그레이션

이러한 단계는 이러한 컨피그레이션에서 자세히 설명합니다.

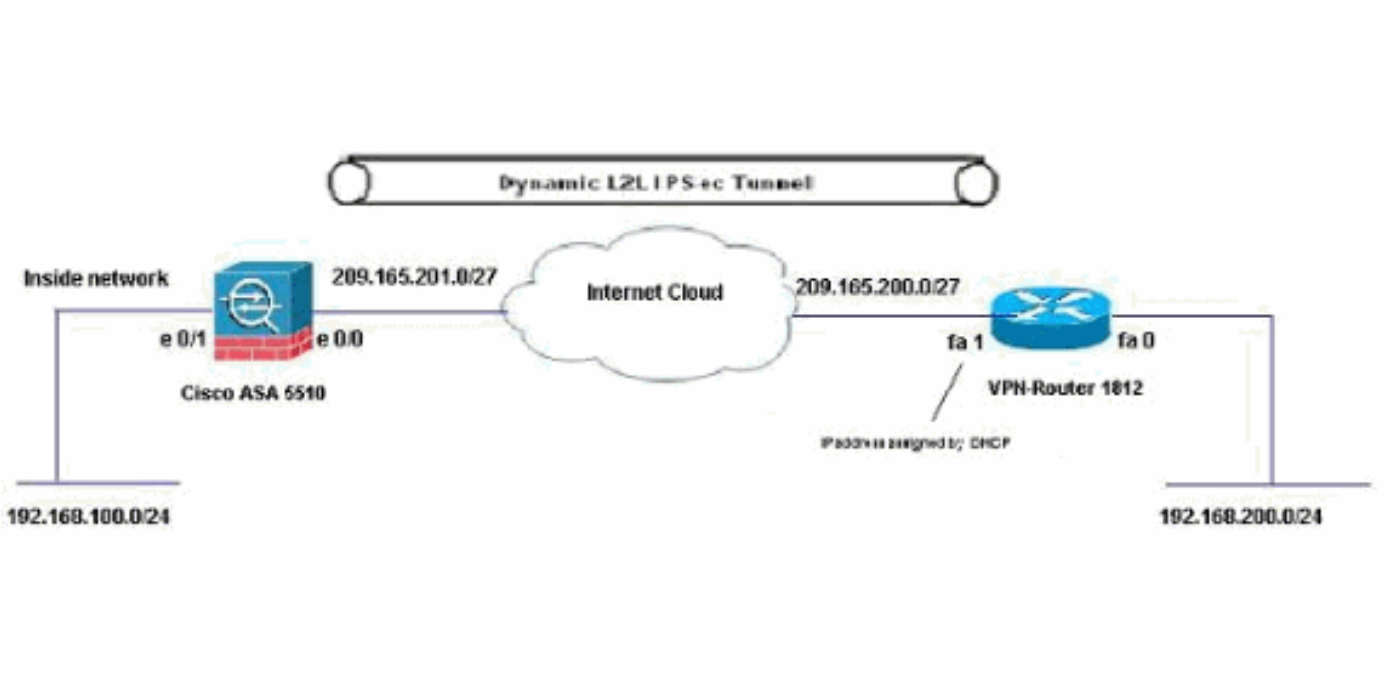
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

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

네트워크 다이어그램

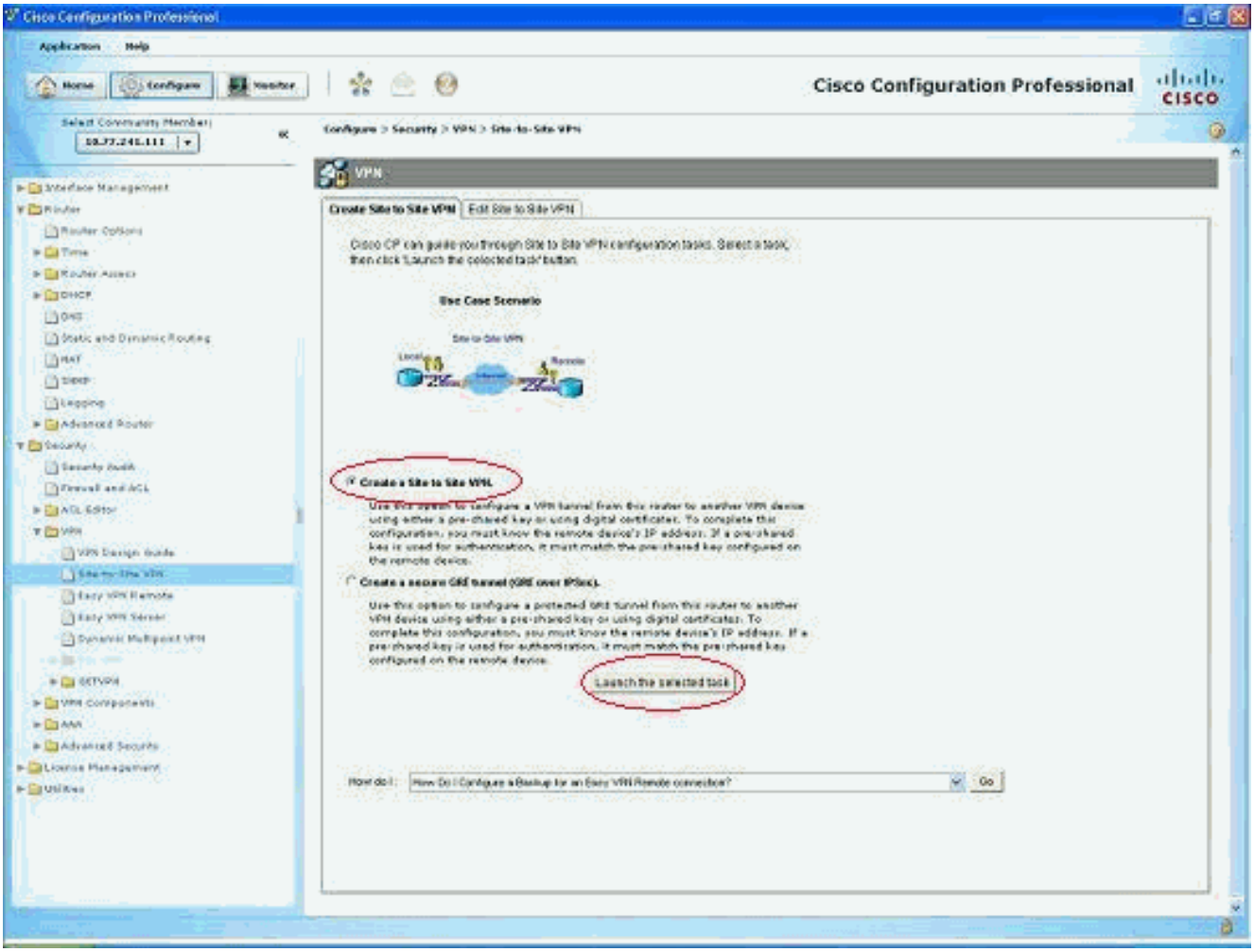
이 문서에서는 다음 네트워크 설정을 사용합니다.



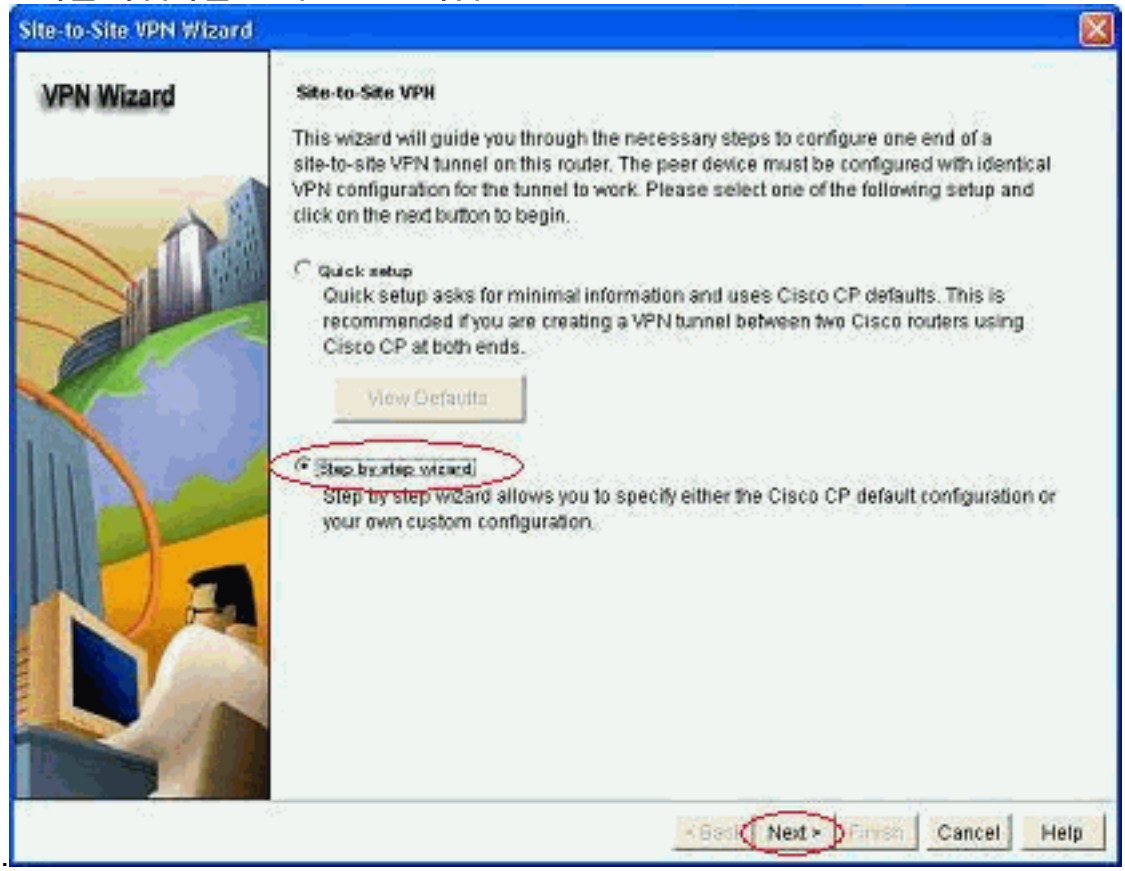
구성

CCP를 사용하는 VPN-라우터의 IPsec VPN 컨피그레이션입니다.다음 단계를 완료하십시오.

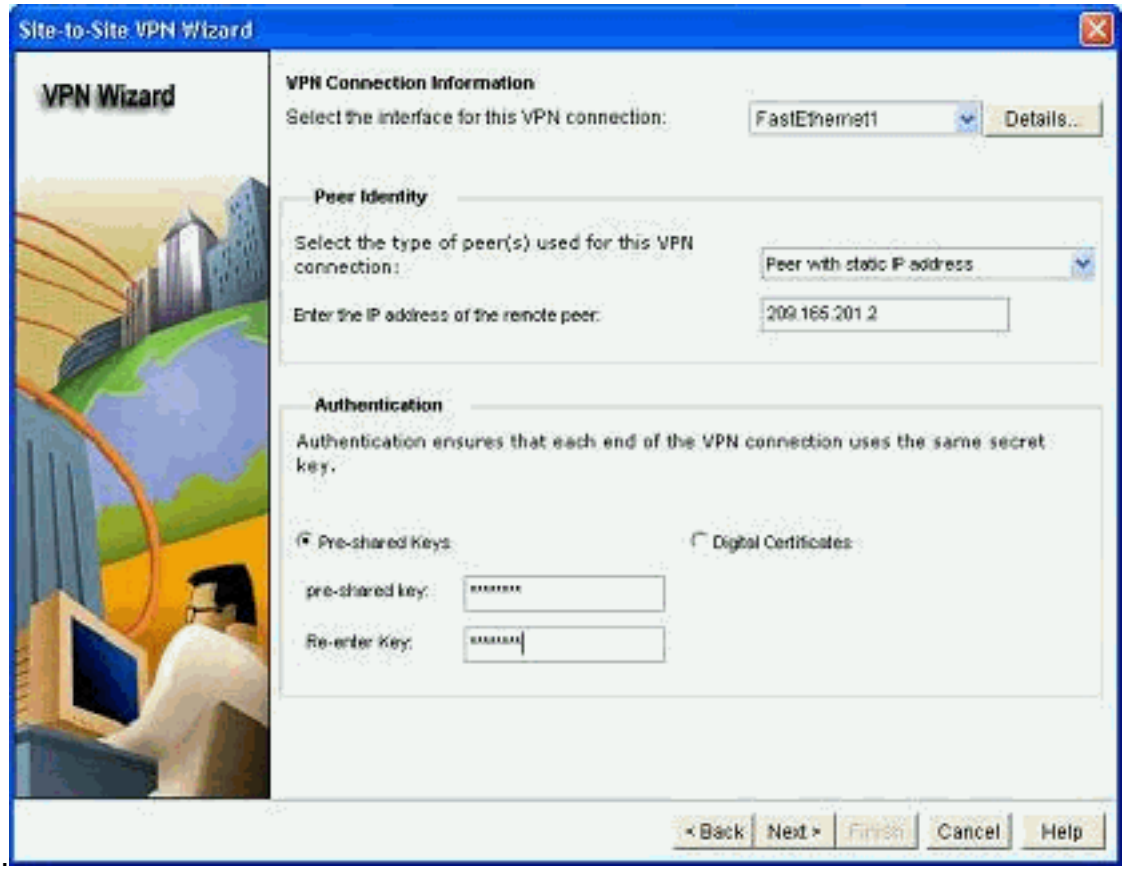
1. CCP 애플리케이션을 열고 Configure(구성) **> Security(보안) > VPN > Site to Site VPN을** 선택합니다.**선택한 탭 실행을 클릭합니다**
   .



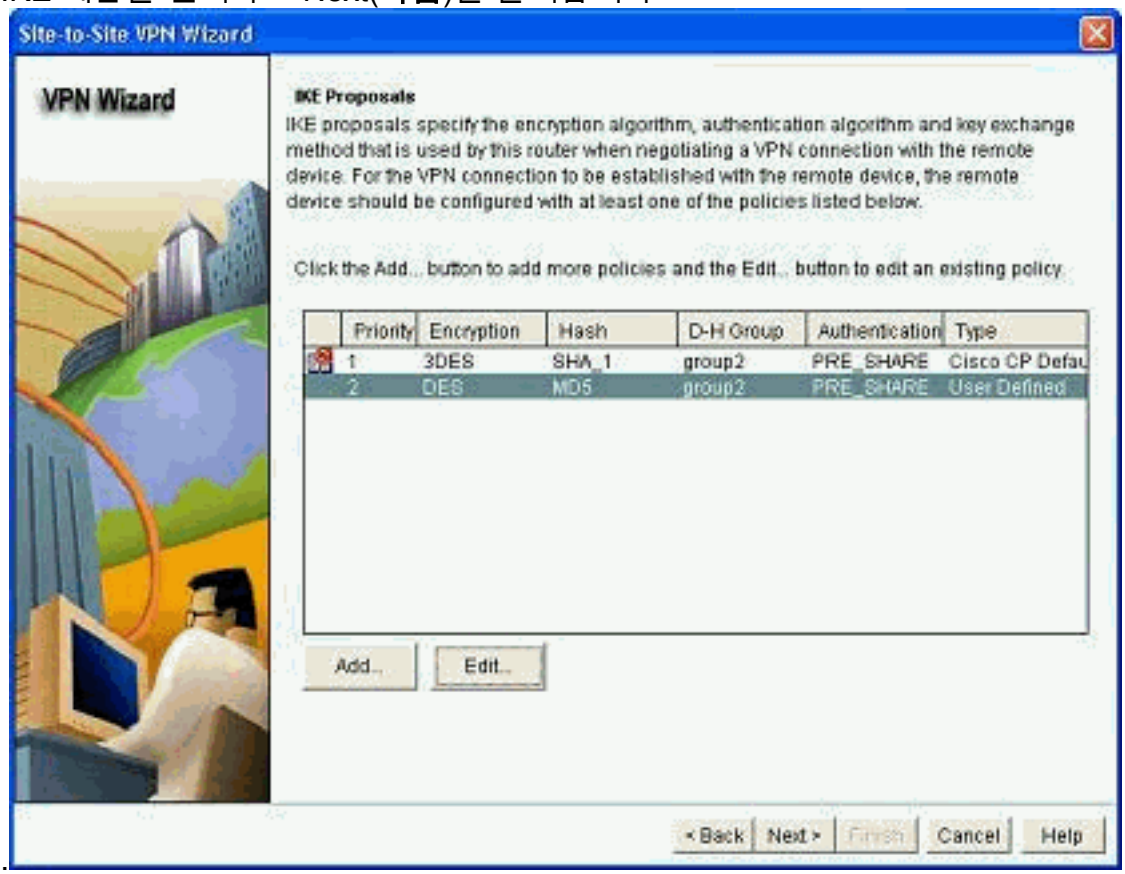
2. **단계별 마법사를 선택한** 다음 **다음**을 클릭합니다



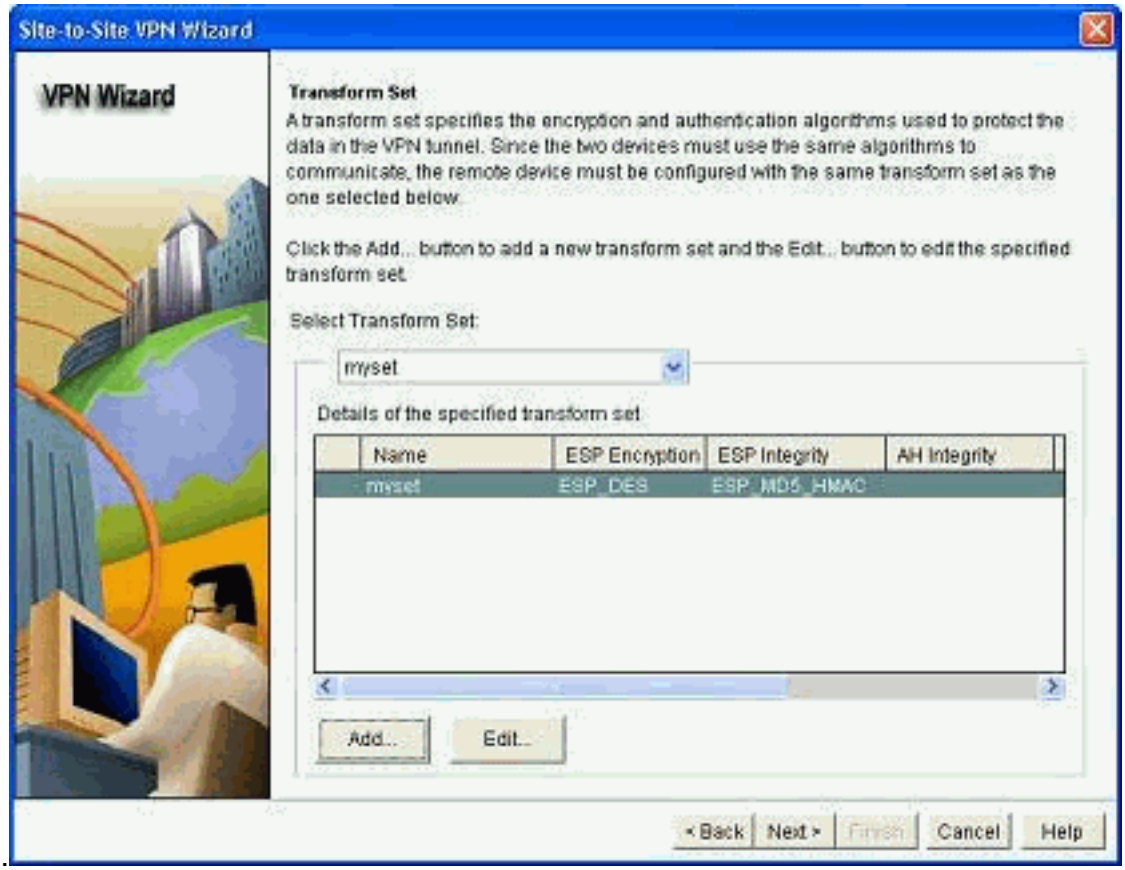
3. 인증 세부 정보와 함께 원격 피어 IP 주소를 입력합니다



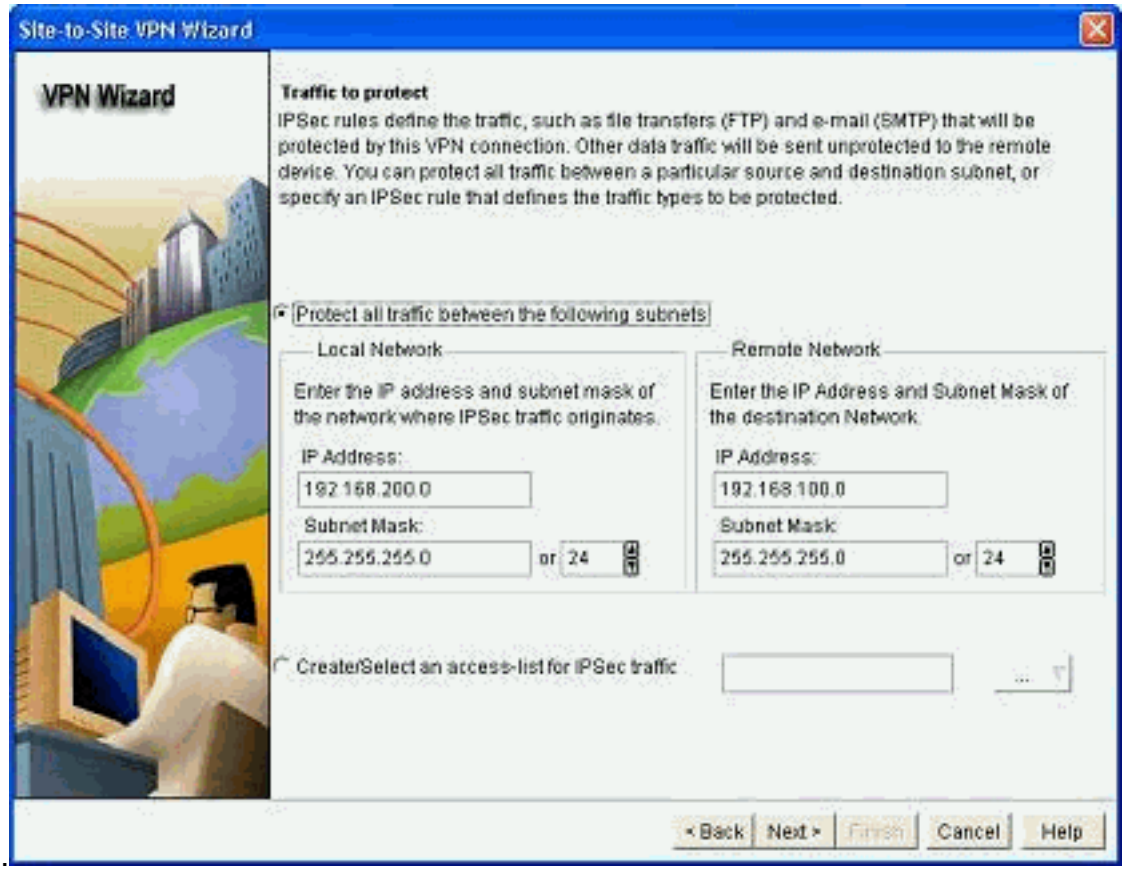
4. IKE 제안을 선택하고 Next(**다음**)를 클릭합니다



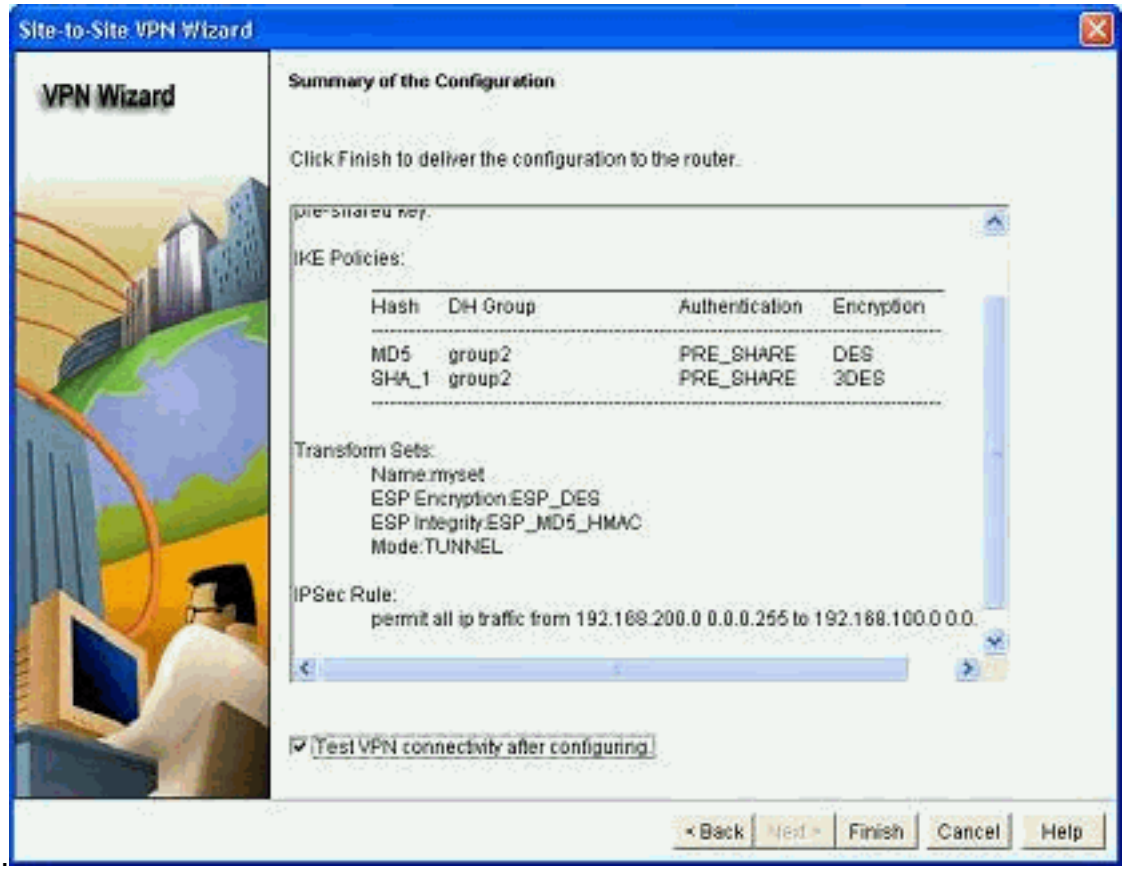
5. 변형 집합 세부 정보를 정의하고 Next(**다음**)를 클릭합니다



6. 암호화해야 하는 트래픽을 정의하고 **Next**를 클릭합니다



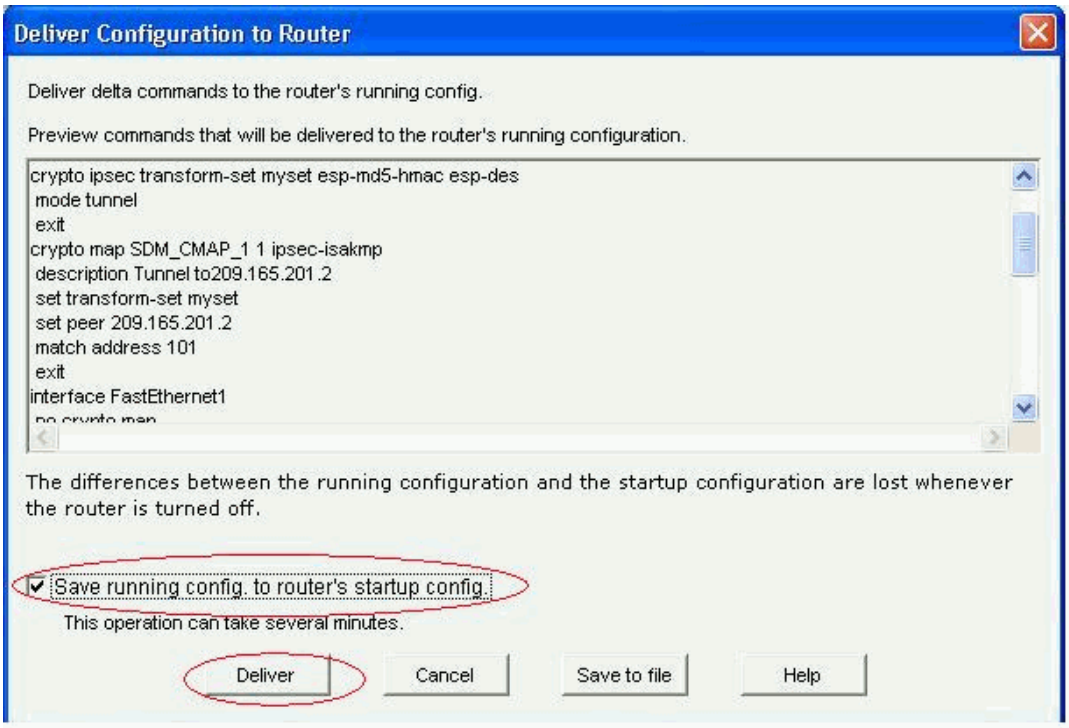
7. 암호화 IPsec 컨피그레이션의 요약을 확인하고 Finish를 **클릭합니다**



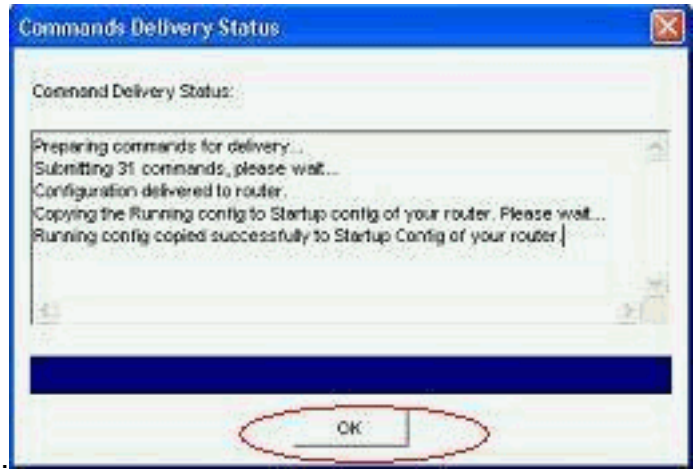
.

8. 컨피그레이션을 VPN-Router로 전송하려면 Deliver를 클릭합니다

.



9. **확인**을 **클릭합니다**.



CLI 컨피그레이션

- 시스코아사
- VPN-라우터

시스코아사

```
ciscoasa(config)#show run
: Saved
:
ASA Version 8.0(3)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.224
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
!--- Output suppressed access-list nonat extended permit
```

```
ip 192.168.100.0 255.255.255.0 192.168.200.0
255.255.255.0

no pager
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-613.bin
no asdm history enable
arp timeout 14400
!!--- Define the nat-translation for Internet users
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
!
!!--- Define the nat-exemption policy for VPN traffic
nat (inside) 0 access-list nonat
!
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
!!--- Configure the IPsec transform-set crypto ipsec
transform-set myset esp-des esp-md5-hmac
!
!!--- Configure the dynamic crypto map crypto dynamic-
map mymap 1 set transform-set myset
crypto dynamic-map mymap 1 set reverse-route
crypto map dyn-map 10 IPSec-isakmp dynamic mymap
crypto map dyn-map interface outside
!!--- Configure the phase I ISAKMP policy crypto isakmp
policy 10
 authentication pre-share
 encryption des
 hash md5
 group 2
 lifetime 86400
!
!!--- Configure the default L2L tunnel group parameters
tunnel-group DefaultL2LGroup IPSec-attributes
 pre-shared-key *
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
```

```
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
ciscoasa(config)#
```

CCP는 VPN-라우터에 이 컨피그레이션을 생성합니다.

VPN-라우터

```
VPN-Router#show run
Building configuration...
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Router
!
!
username cisco privilege 15 secret 5
$1$UQxM$WvwDZbfDhK3wS26C9xYns/
username test12 privilege 15 secret 5
$1$LC0U$ex3tp4hM8CYD.HJSRDfQO1
!
!!--- Output suppressed no aaa new-model ip subnet-zero
! ip cef ! crypto isakmp enable outside
!
crypto isakmp policy 1
 encrypt 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 hash md5
 authentication pre-share
 group 2
!
!
crypto isakmp key cisco123 address 209.165.201.2
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
!
crypto map SDM_CMAP_1 1 IPSec-isakmp
 description Tunnel to209.165.201.2
 set peer 209.165.201.2
 set transform-set myset
```

```
 match address 101
!
!
!
interface BRI0
 no ip address
 shutdown
!
interface Dot11Radio0
 no ip address
 shutdown
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0
12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
!
interface Dot11Radio1
 no ip address
 shutdown
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
48.0 54.0
 station-role root
!
interface FastEthernet0
 ip address 192.168.200.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1
 ip address dhcp
 duplex auto
 speed auto
 crypto map SDM_CMAP_1
!
interface FastEthernet2
 no ip address
 shutdown
!
interface FastEthernet3
 no ip address
 shutdown
!
interface FastEthernet4
 no ip address
 shutdown
!
interface FastEthernet5
 no ip address
 shutdown
!
interface FastEthernet6
 no ip address
 shutdown
!
interface FastEthernet7
 no ip address
 shutdown
!
interface FastEthernet8
 no ip address
 shutdown
!
interface FastEthernet9
 no ip address
 shutdown
```

```
!
interface Vlan1
 no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1
!
!!--- Output suppressed ! ip http server ip http
authentication local ip http secure-server ! access-list
100 permit ip 0.0.0.0 255.255.255.0 0.0.0.0
255.255.255.0
access-list 101 remark CCP_ACL Category=4
access-list 101 remark IPSEC Rule
access-list 101 permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
!
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
line vty 5 15
 privilege level 15
 login local
 transport input telnet ssh
!
no scheduler allocate
end
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

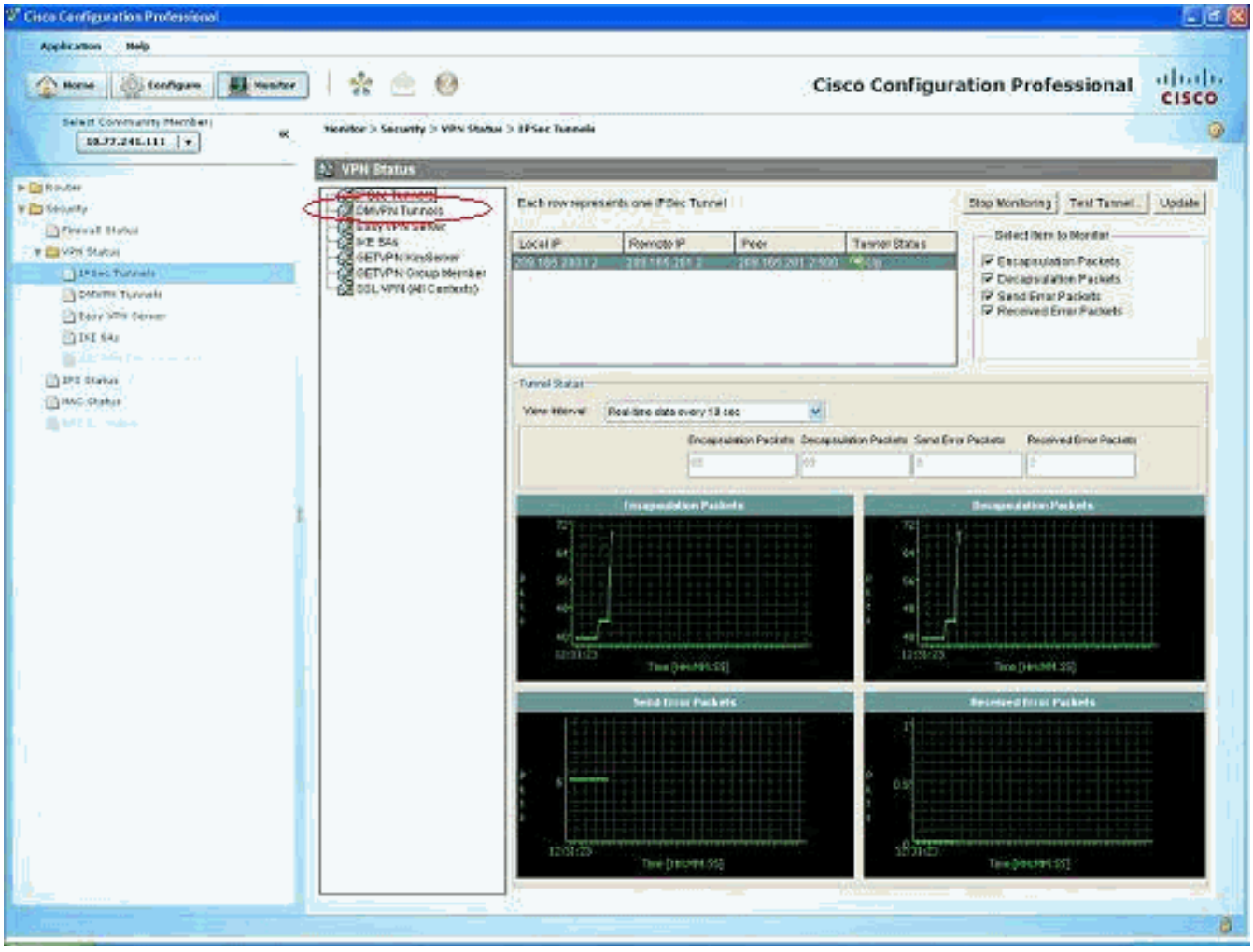
Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- CCP를 통해 터널 매개변수 확인
- ASA CLI를 통해 터널 상태 확인
- 라우터 CLI를 통해 터널 매개변수 확인

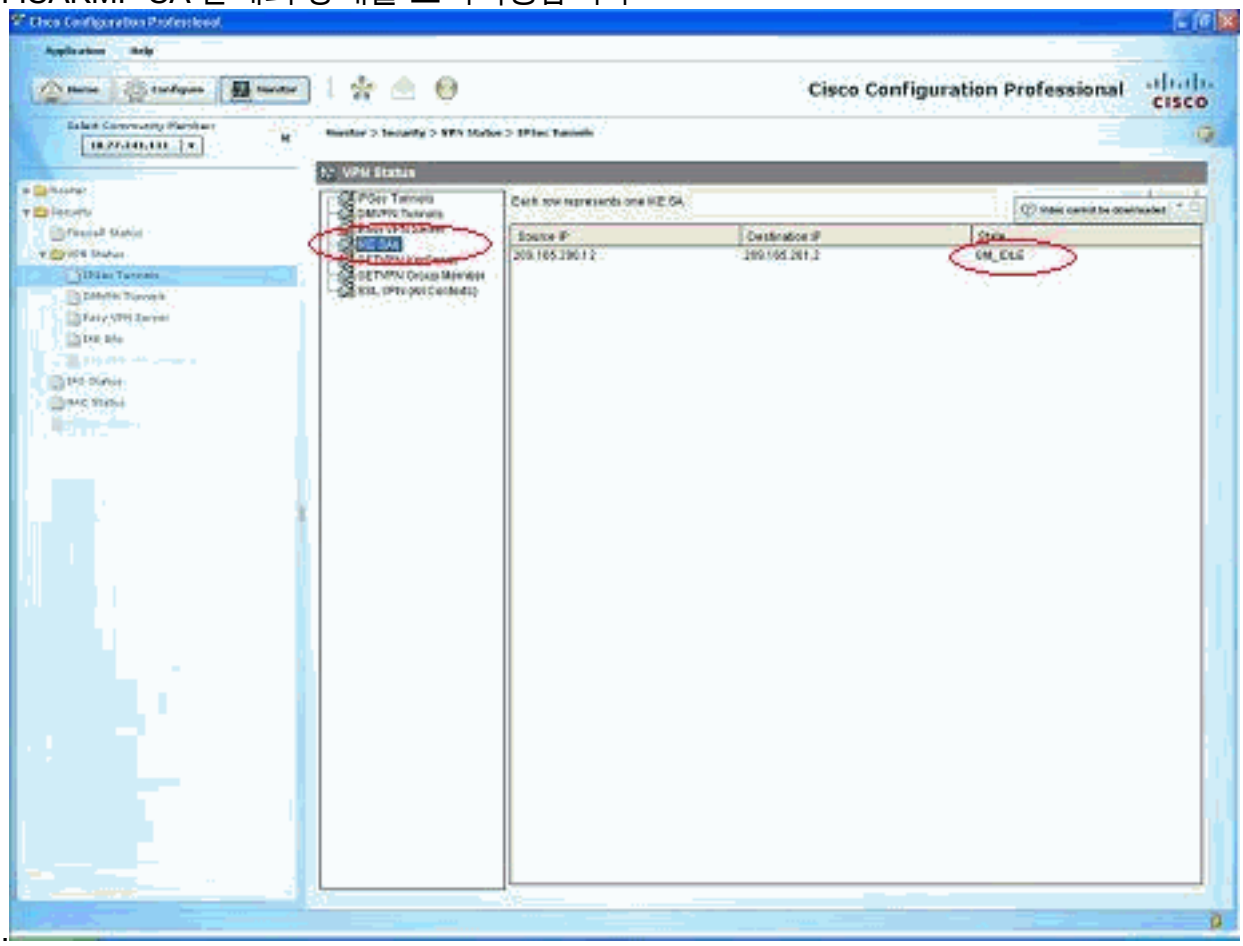
CCP를 통해 터널 매개변수 확인

- 트래픽이 IPsec 터널을 통과하도록 모니터링합니다

  .



- I ISAKMP SA 단계의 상태를 모니터링합니다



ASA CLI를 통해 터널 상태 확인

- I ISAKMP SA 단계의 상태를 확인합니다.

```
ciscoasa#show crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 209.165.200.12
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
ciscoasa#
```

참고: 이 터널의 개시자가 반대쪽 끝에 있음을 나타내는 responder일 역할을 관찰합니다(예: VPN-라우터).

- II IPSEC SA 단계의 매개변수를 확인합니다.

```
ciscoasa#show crypto ipsec sa
interface: outside
    Crypto map tag: mymap, seq num: 1, local addr: 209.165.201.2

      local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
      current_peer: 209.165.200.12

      #pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29
      #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.201.2, remote crypto endpt.: 209.165.200.12

      path mtu 1500, IPSec overhead 58, media mtu 1500
      current outbound spi: E7B37960

    inbound esp sas:
      spi: 0xABB49C64 (2880740452)
         transform: esp-des esp-md5-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 4096, crypto-map: mymap
         sa timing: remaining key lifetime (kB/sec): (4274997/3498)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xE7B37960 (3887298912)
         transform: esp-des esp-md5-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 4096, crypto-map: mymap
         sa timing: remaining key lifetime (kB/sec): (4274997/3498)
         IV size: 8 bytes
         replay detection support: Y
```

라우터 CLI를 통해 터널 매개변수 확인

- I ISAKMP SA 단계의 상태를 확인합니다.

```
VPN-Router#show crypto isakmp sa
dst             src             state          conn-id slot status
209.165.201.2   209.165.200.12  QM_IDLE              1    0 ACTIVE
```

- II IPSEC SA 단계의 매개변수를 확인합니다.

```
VPN-Router#show crypto ipsec sa

interface: FastEthernet1
    Crypto map tag: SDM_CMAP_1, local addr 209.165.200.12

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
   current_peer 209.165.201.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39
    #pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 6, #recv errors 0

     local crypto endpt.: 209.165.200.12, remote crypto endpt.: 209.165.201.2
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xABB49C64(2880740452)

     inbound esp sas:
      spi: 0xE7B37960(3887298912)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4481818/3375)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xABB49C64(2880740452)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4481818/3371)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- 기존 암호화 연결을 해제합니다.

```
ciscoasa#clear crypto ipsec sa
ciscoasa#clear crypto isakmp sa

VPN-Router#clear crypto isakmp
```

- VPN 터널 문제를 해결하려면 debug 명령을 사용합니다.**참고:** 디버깅을 활성화하면 인터네트워크에서 로드가 많은 상태가 발생하는 경우 라우터 작업이 중단될 수 있습니다.**debug 명령을 주의하여 사용하십시오.일반적으로 이러한 명령은 특정 문제를 해결할 때 라우터 기술 지원 담당자의 지시에 따라서만 사용하는 것이 좋습니다.**

```
ciscoasa#debug crypto engine
ciscoasa#debug crypto isakmp
ciscoasa#debug crypto IPSec
ciscoasa#

VPN-Router#debug crypto engine
Crypto Engine debugging is on
VPN-Router#debug crypto isakmp
Crypto ISAKMP debugging is on
VPN-Router#debug crypto ipsec
Crypto IPSEC debugging is on
VPN-Router#
```

debug 명령에 대한 자세한 내용은 debug 명령 이해 및 사용의 debug crypto isakmp를 참조하십시오.

관련 정보

- IPSEC 협상/IKE 프로토콜 지원 페이지
- Cisco ASA Security Appliance OS 소프트웨어 설명서
- 가장 일반적인 IPSEC VPN 트러블슈팅 솔루션
- RFC(Request for Comments)