ASA-to-ASA Dynamic-to-Static IKEv1/IPsec 컨피그레이션 예

목차

소개

이 문서에서는 ASA(Adaptive Security Appliance)가 동적 피어(이 경우 ASA)에서 동적 IPsec 사이트 대 사이트 VPN 연결을 수락하도록 허용하는 방법에 대해 설명합니다. 이 문서의 네트워크 다이어그램에 나와 있는 것처럼, IPsec 터널은 Remote-ASA 끝에서만 터널이 시작될 때 설정됩니다.동적 IPsec 컨피그레이션으로 인해 Central-ASA가 VPN 터널을 시작할 수 없습니다.Remote-ASA의 IP 주소를 알 수 없습니다.

와일드카드 IP 주소(0.0.0.0/0)과 와일드카드 사전 공유 키로부터의 연결을 동적으로 수락하려면 Central-ASA를 구성합니다.그런 다음 crypto access-list에서 지정한 대로 로컬-중앙-ASA 서브넷에서 중앙-ASA 서브넷으로 트래픽을 암호화하도록 Remote-ASA가 구성됩니다.양측은 IPsec 트래픽에 대해 NAT를 우회하기 위해 NAT(Network Address Translation) 면제를 수행합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco ASA(5510 및 5520) Firewall Software Release 9.x 이상을 기반으로 합니다.

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.

구성

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

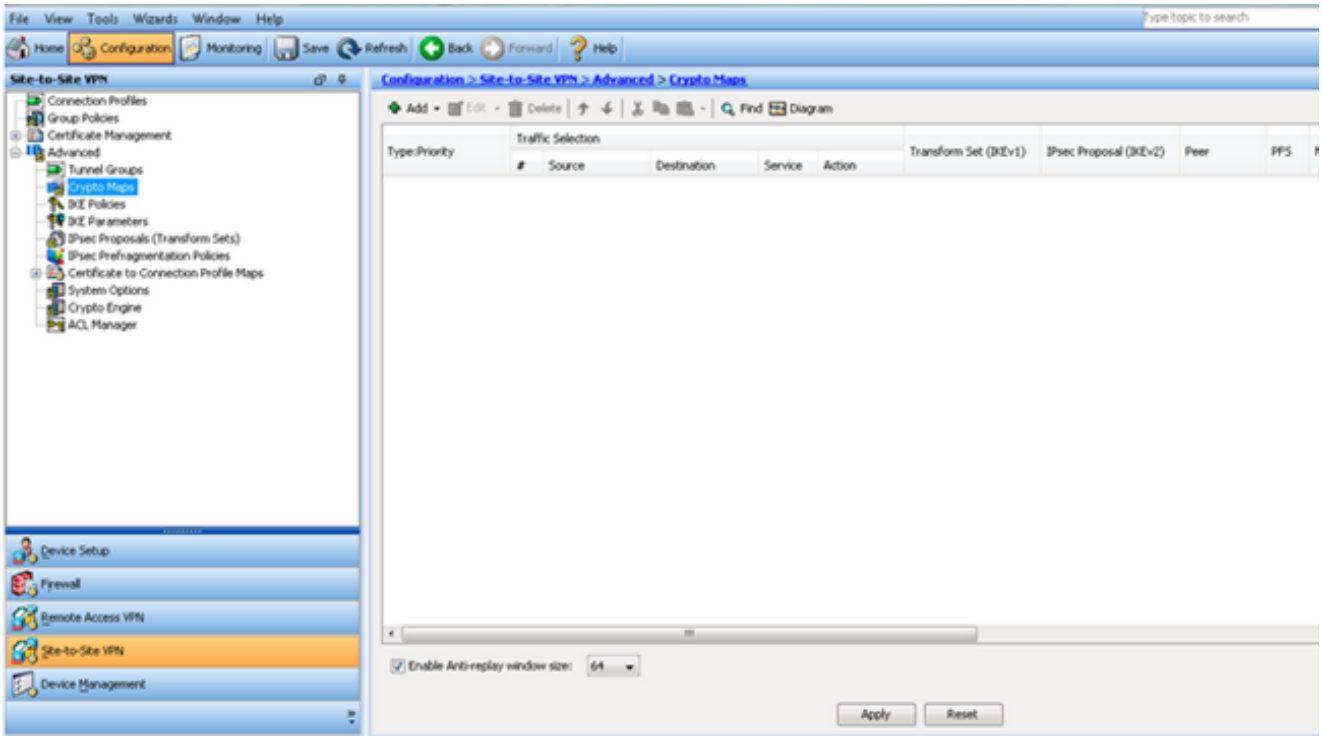
네트워크 다이어그램

ASDM 컨피그레이션

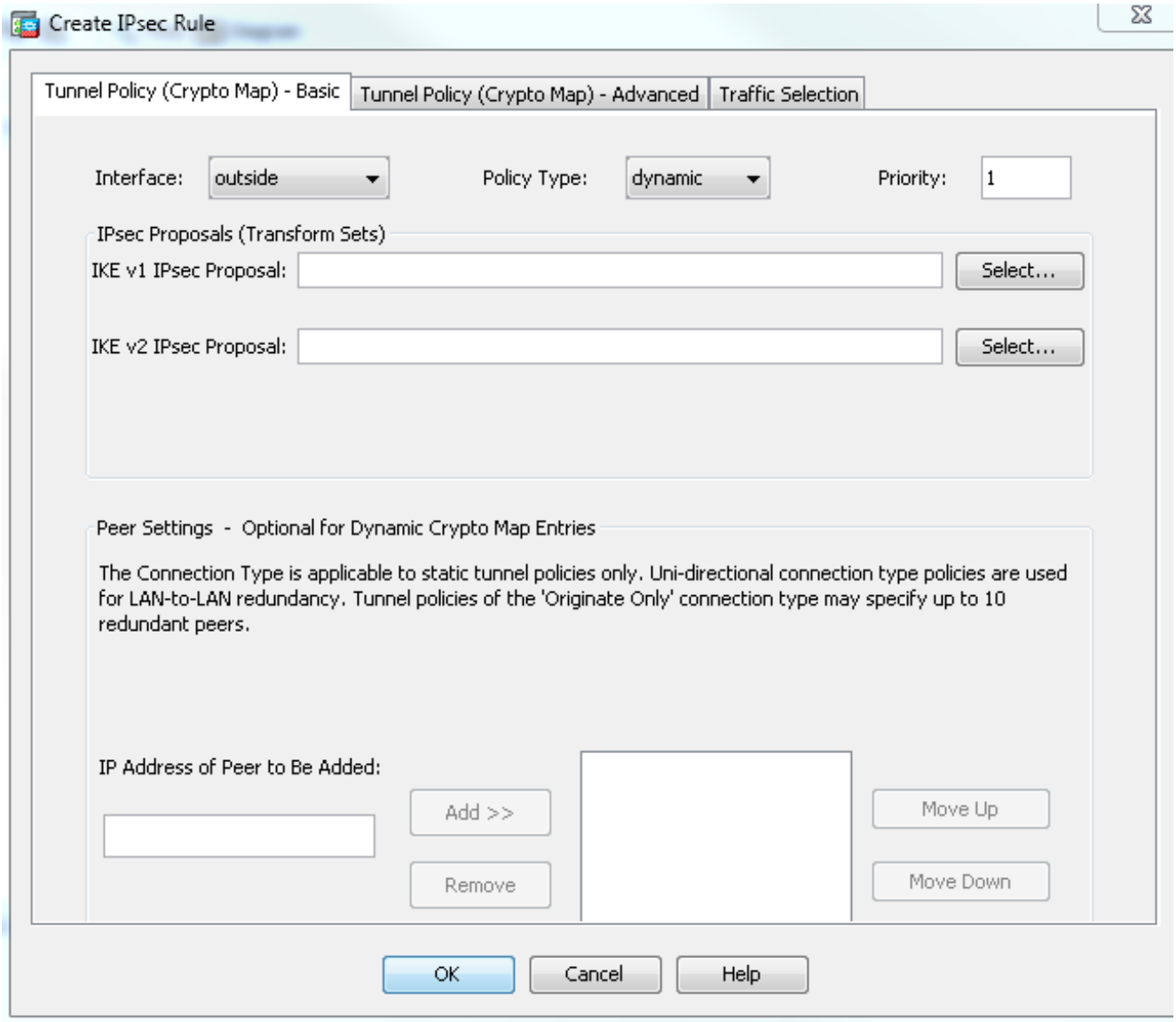
Central-ASA(정적 피어)

고정 IP 주소가 있는 ASA에서 IKEv1 사전 공유 키를 사용하여 피어를 인증하는 동안 알 수 없는 피어의 동적 연결을 수락하는 방식으로 VPN을 설정합니다.

1. Configuration **> Site-to-Site VPN > Advanced > Crypto Maps를 선택합니다.**창에는 이미 배치된 암호화 맵 항목 목록이 표시됩니다(있는 경우). ASA는 피어 IP 주소가 무엇인지 알지 못하기 때문에 ASA가 연결을 수락하려면 일치하는 변형 집합(IPsec 제안)을 사용하여 **동적 맵**을 구성합니다. Add(**추가)를 클릭합니다**
.

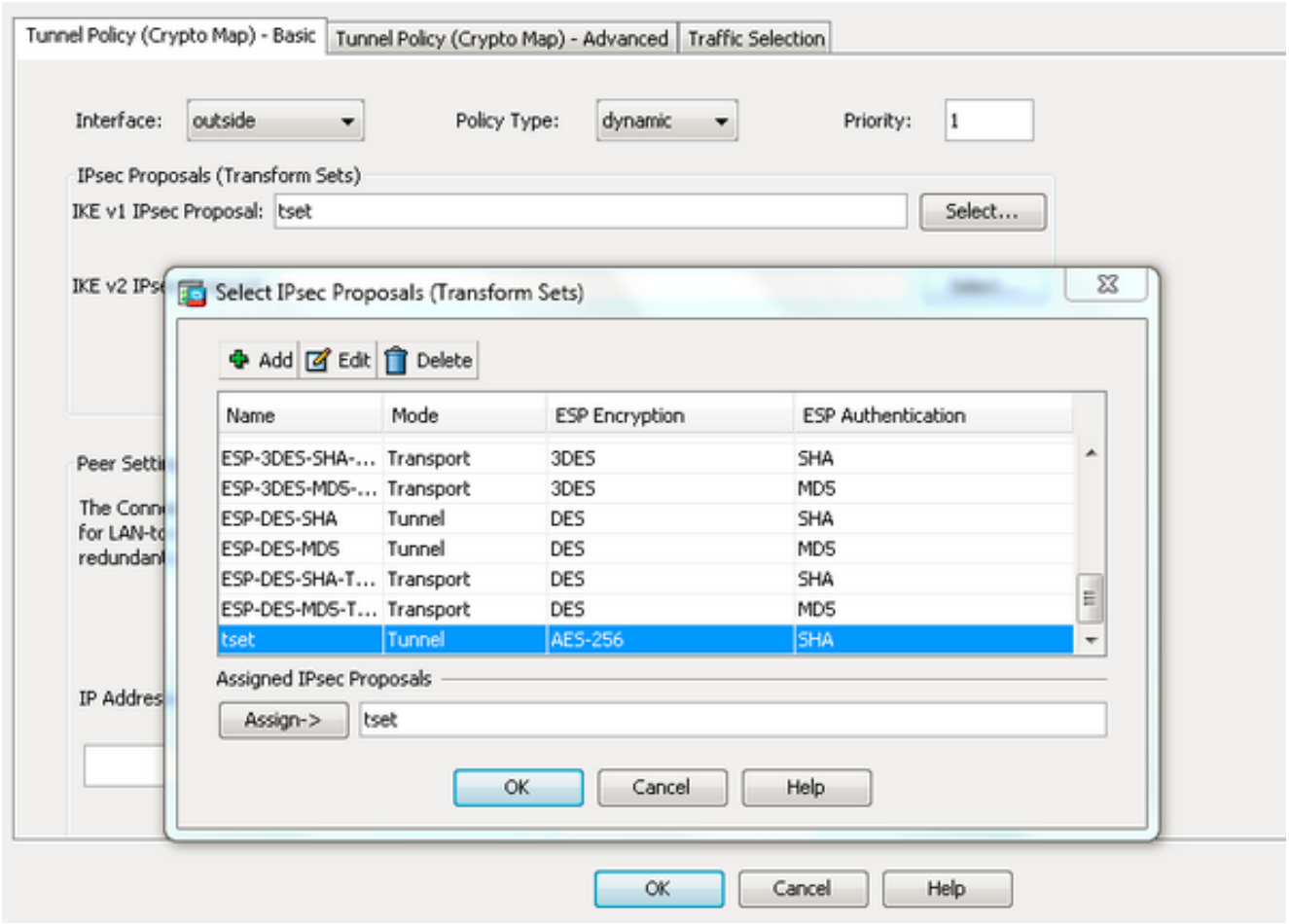


2. Create IPsec Rule(IPsec 규칙 생성) 창의 Tunnel Policy(Crypto Map) - Basic(터널 정책(암호화 맵) - Basic(기본) 탭의 Interface(인터페이스) 드롭다운 목록에서 **outside(외부)를** 선택하고 Policy Type(정책 유형) 드롭다운 목록에서 **dynamic(동적)**을 선택합니다.Dynamic-Map 아래에 항목이 여러 개 있는 경우 Priority 필드에서 이 항목의 우선순위를 지정합니다.그런 다음 IPsec 제안을 선택하려면 IKE v1 IPsec Proposal 필드 옆에 있는 **Select**(선택)를 클릭합니다 .

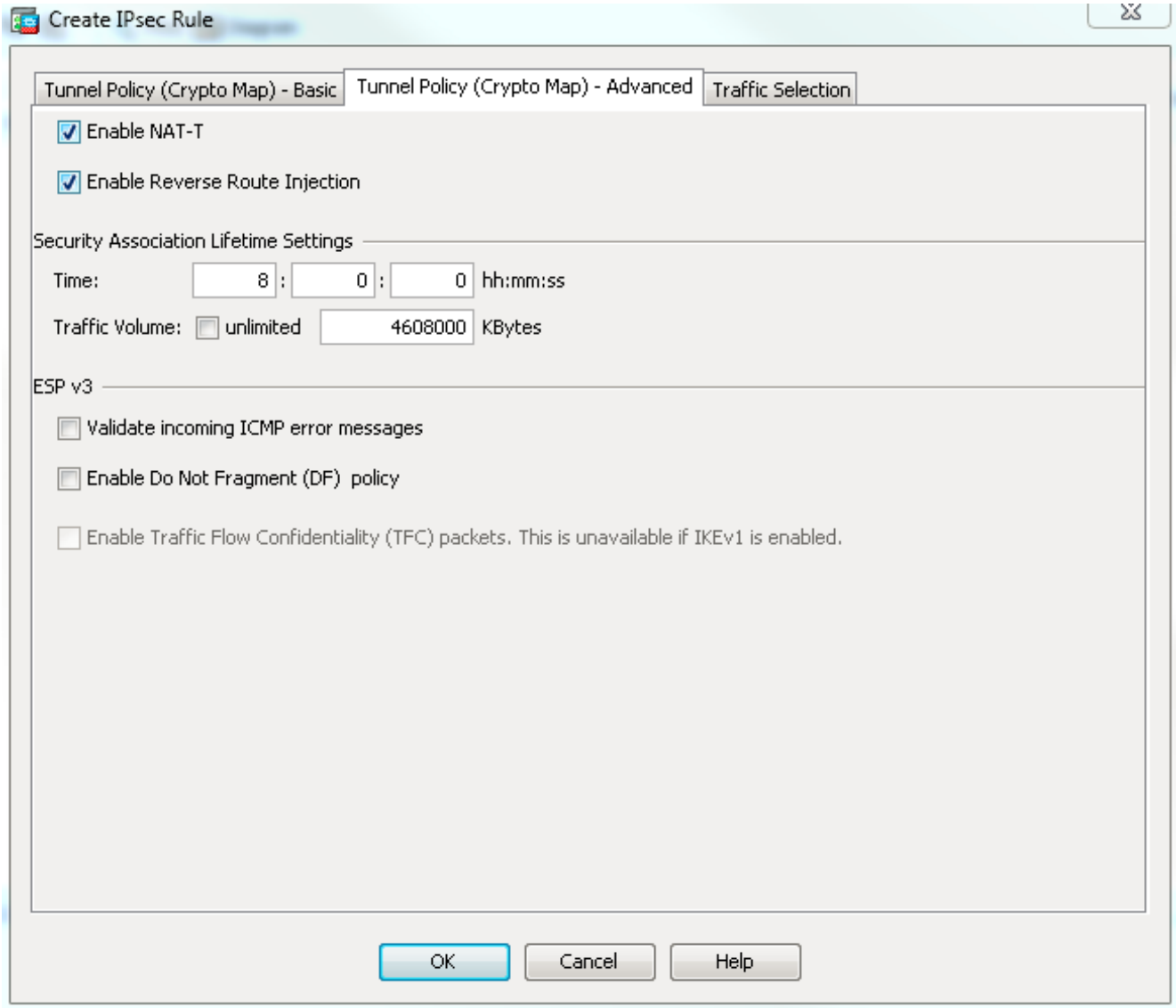


3. Select IPsec Proposals (Transform Sets)(IPsec 제안(변형 집합) 선택) 대화 상자가 열리면 현재 IPsec 제안 중에서 선택하거나 **Add(추가)**를 클릭하여 새 제안서를 작성하고 동일한 기능을 사용합니다.완료되면 **OK**(확인)를 클릭합니다

.

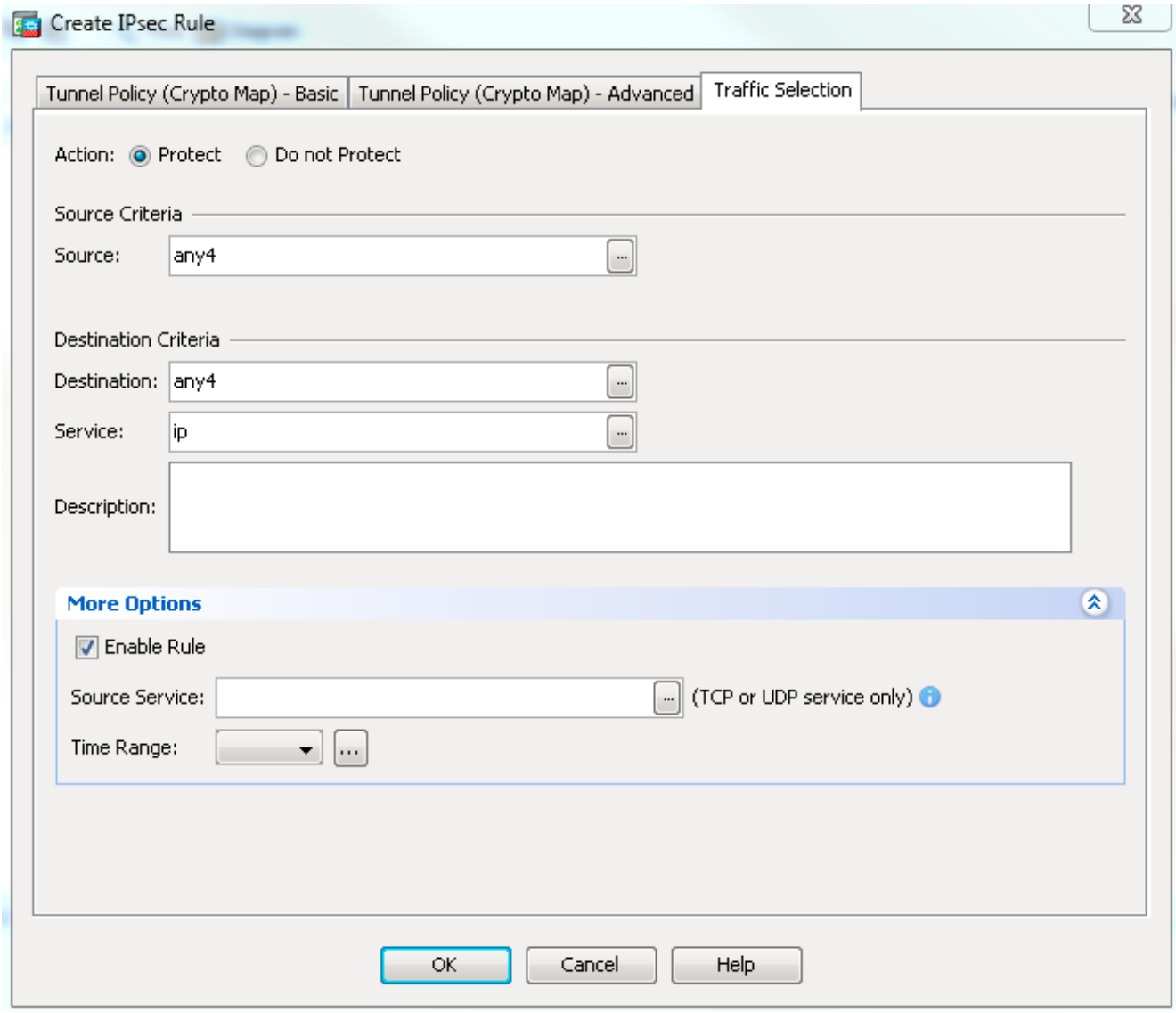


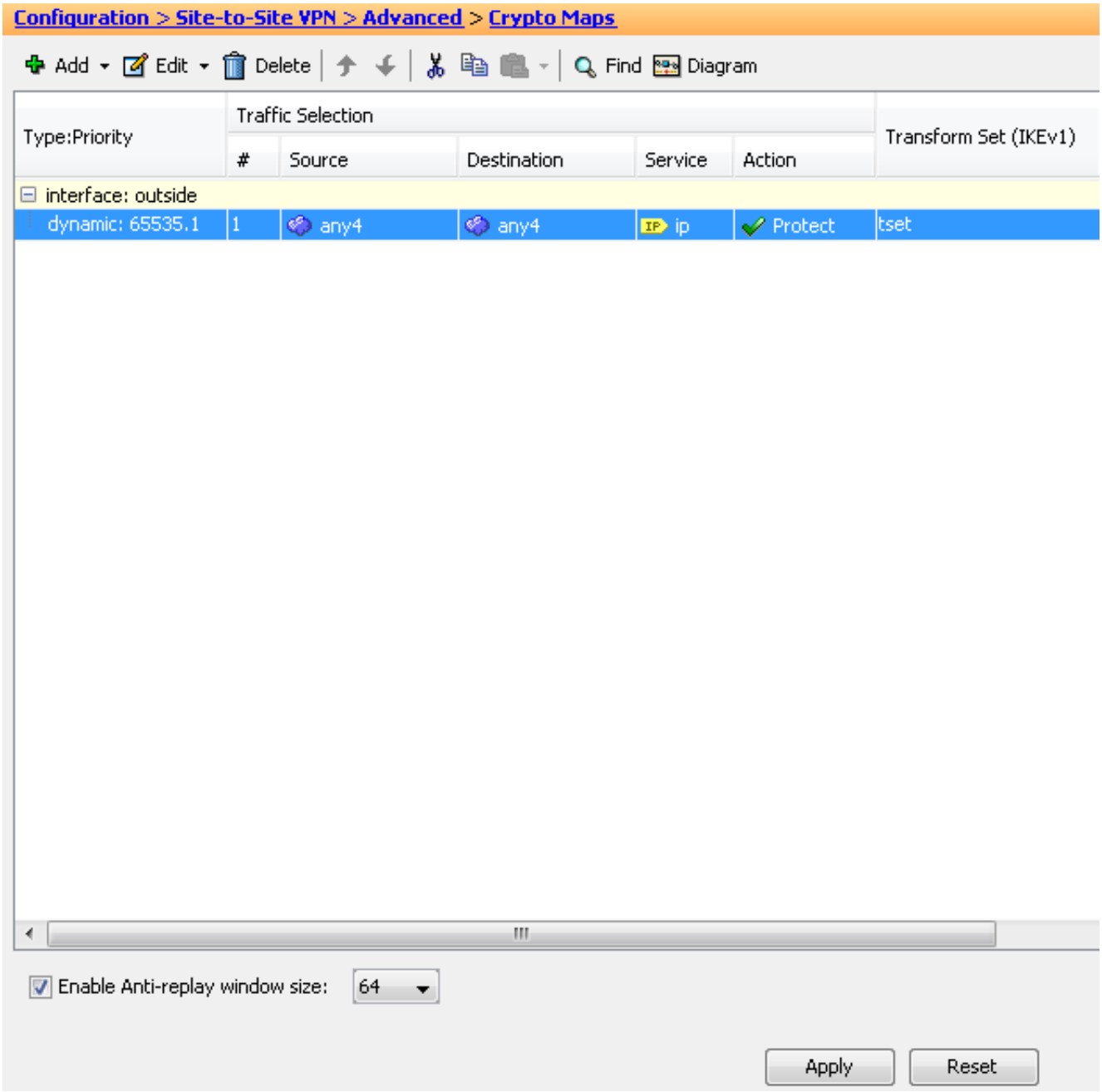
4. Tunnel Policy(Crypto Map)-Advanced(터널 정책(암호화 맵)-Advanced(고급) 탭에서 Enable NAT-**T(NAT-T 활성화**) 확인란(둘 중 한 피어가 NAT 디바이스 뒤에 있는 경우 필요) 및 Enable **Reverse Route Injection** 확인란을 선택합니다.동적 피어에 대해 VPN 터널이 작동하면 VPN 인터페이스를 가리키는 협상된 원격 VPN 네트워크에 대한 동적 경로가 ASA에 설치됩니다
.



선택적으로, Traffic Selection(트래픽 선택) 탭에서 동적 피어에 대한 흥미로운 VPN 트래픽을 정의하고 **OK**(확인)를 클릭할 수도 있습니다

.

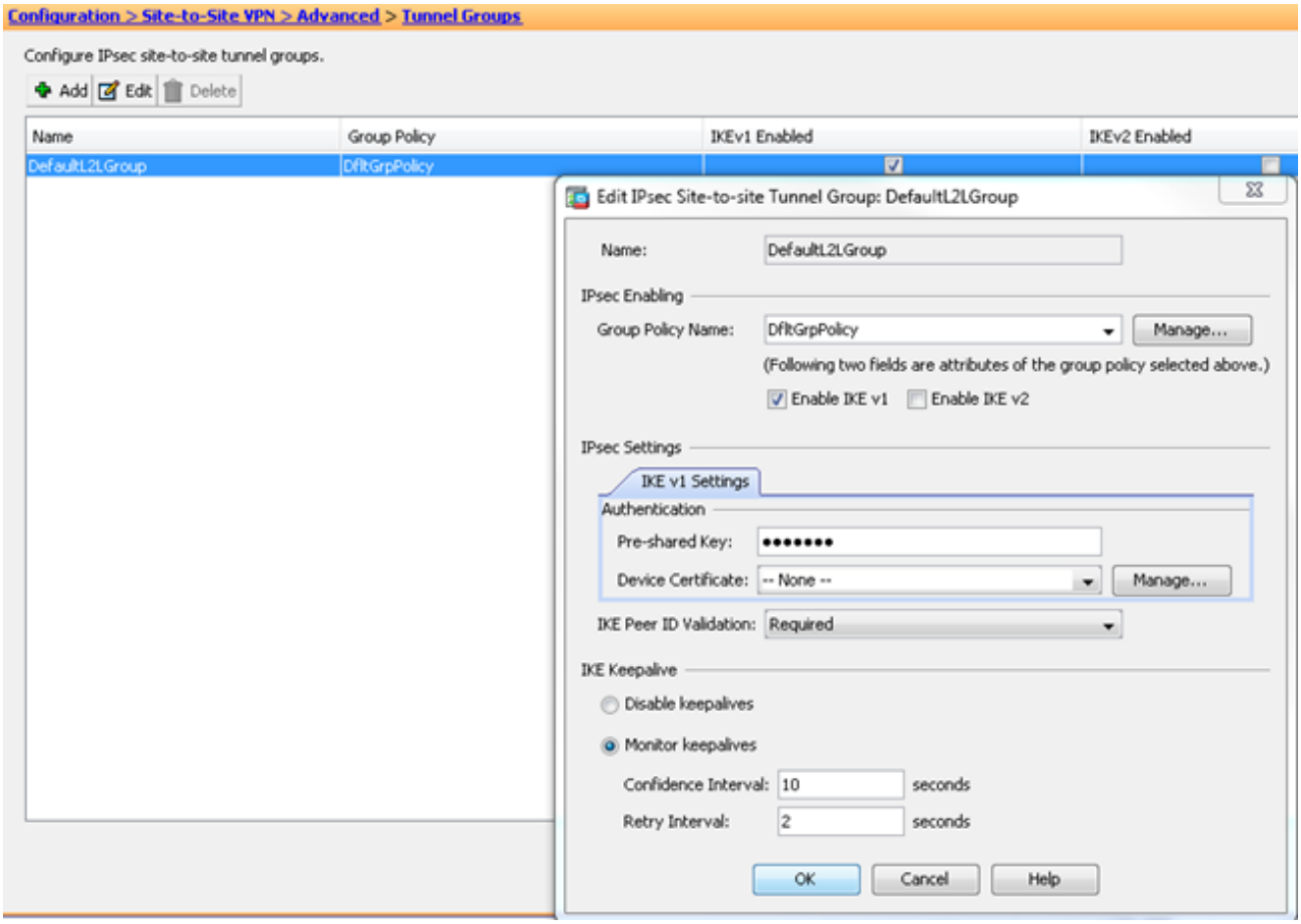

Create IPsec Rule
Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection
Action:
Protect
Do not Protect
Source Criteria
Source:
any4
Destination Criteria
Destination:
any4
Service:
ip
Description:
More Options
Enable Rule
Source Service:
(TCP or UDP service only)
Time Range:
OK
Cancel
Help



앞에서 언급한 대로, ASA는 원격 동적 피어 IP 주소에 대한 정보가 없으므로 알 수 없는 연결 요청은 기본적으로 ASA에 존재하는 DefaultL2LGroup 아래에 위치합니다.인증이 성공하려면 원격 피어에 구성된 사전 공유 키(이 예에서는 cisco123)를 DefaultL2LGroup의 키와 일치해야 합니다.

5. Configuration(**구성) > Site-to-Site VPN > Advanced(고급) > Tunnel Groups(터널 그룹)를** 선택하고 **DefaultL2LGroup을** 선택한 다음 Edit(수정)를 **클릭하고** 원하는 사전 공유 키를 구성합니다.완료되면 **OK**(확인)를 클릭합니다

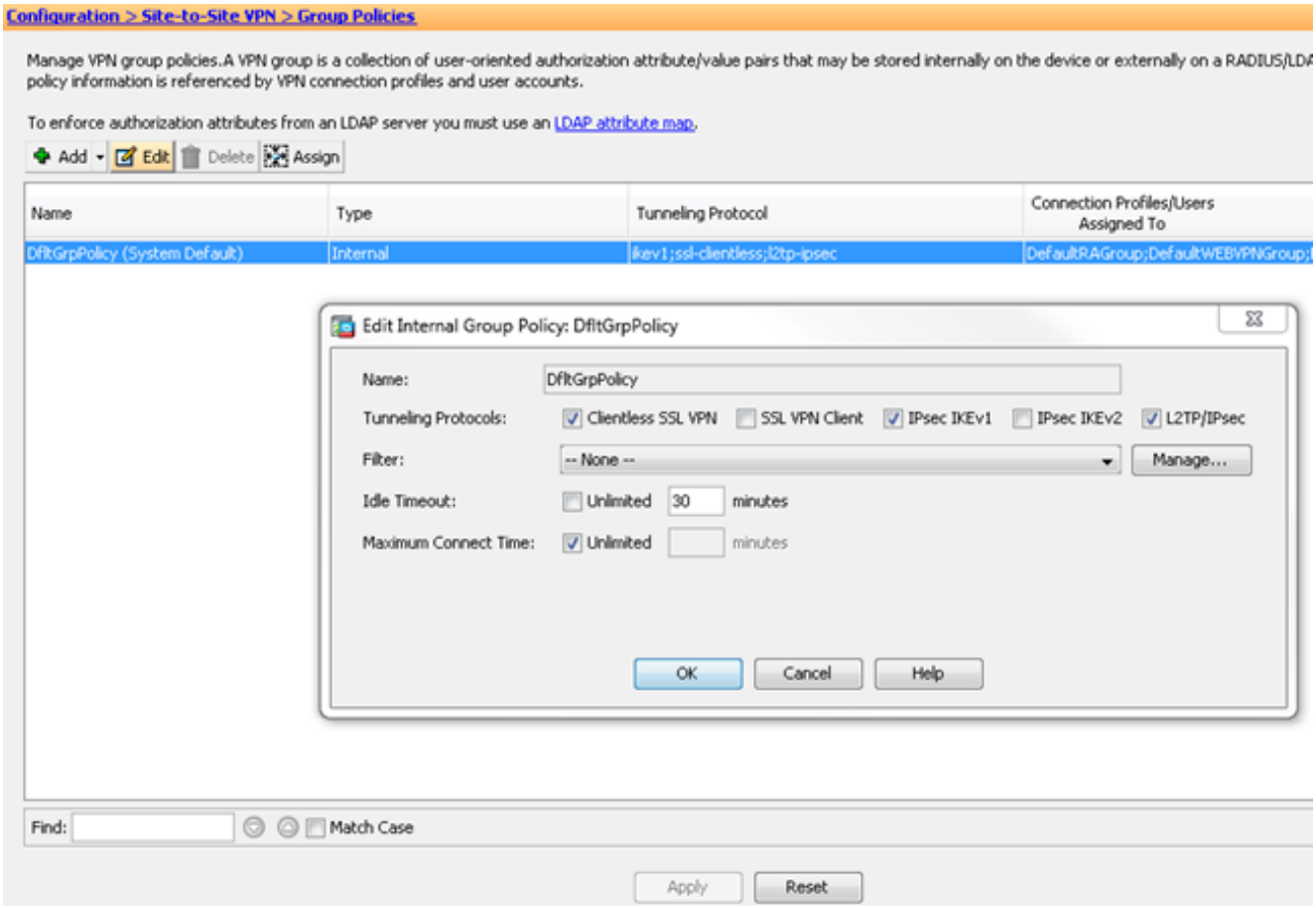
.



참고:이렇게 하면 고정 피어(Central-ASA)에 와일드카드 사전 공유 키가 생성됩니다. 이 사전 공유 키 및 관련 제안을 아는 모든 디바이스/피어는 VPN을 통해 VPN 터널 및 액세스 리소스를 성공적으로 설정할 수 있습니다.이 사전 공유 키가 알 수 없는 엔터티와 공유되지 않고 추측하기 쉽지 않은지 확인하십시오.

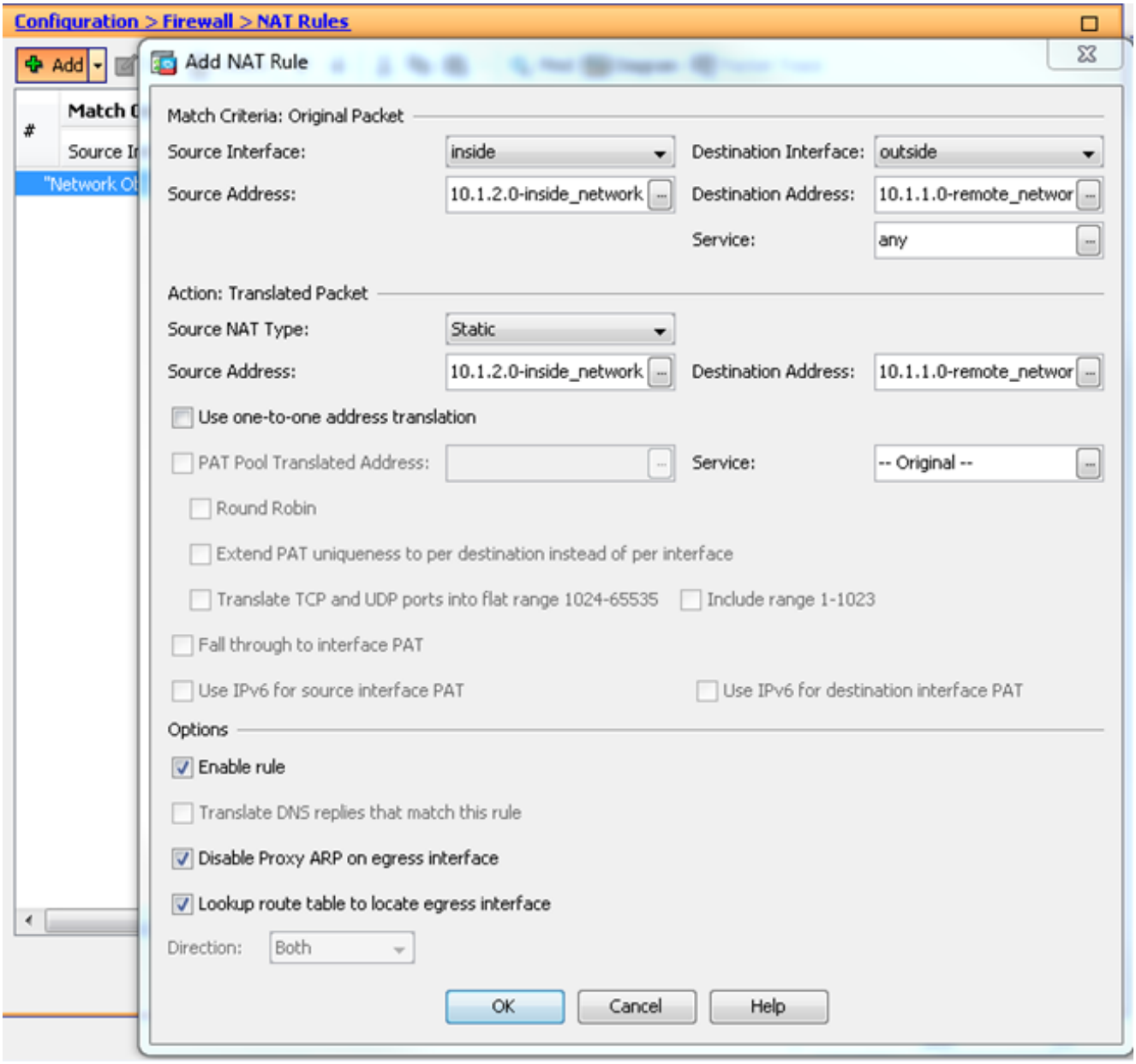
6. [**구성**] > [**사이트 대 사이트 VPN**] > [**그룹 정책**]을 선택하고 선택한 그룹 정책(이 경우 기본 그룹 정책)을 선택합니다. [내부 그룹 정책 편집] 대화 상자에서 그룹 정책을 편집하고 편집합니다.완료되면 **OK**(확인)를 클릭합니다

.



7. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > **NAT Rules(NAT 규칙)**를 선택하고 Add Nat Rule(NAT 규칙 추가) 창에서 VPN 트래픽에 대한 no nat(NAT-EXEMPT) 규칙을 구성합니다 .완료되면 **OK**(확인)를 클릭합니다

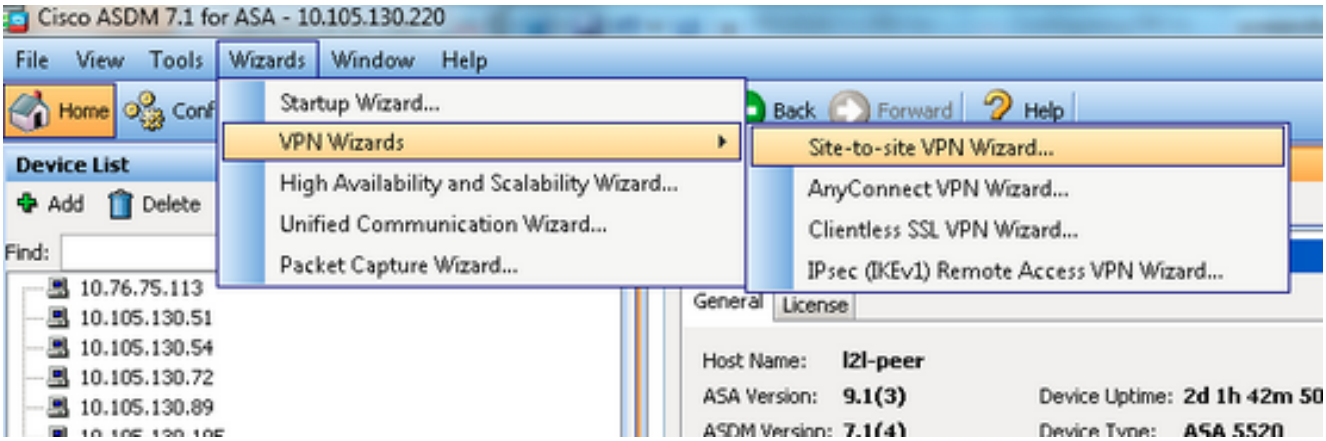
.



Remote-ASA(동적 피어)

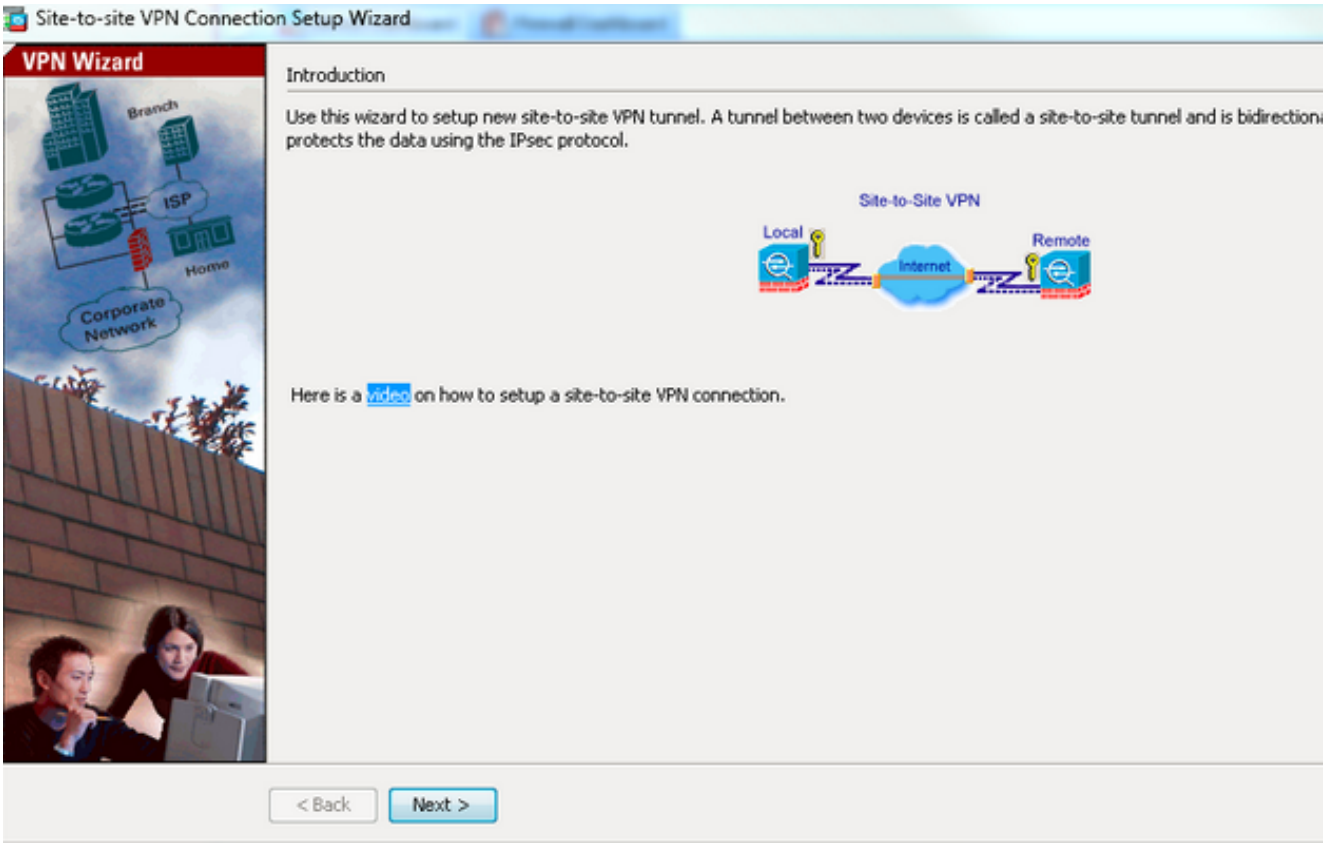
1. ASDM 애플리케이션이 ASA에 연결되면 **Wizards(마법사) > VPN Wizards(VPN 마법사) > Site-to-site VPN Wizard(사이트 대 사이트 VPN 마법사)**를 선택합니다

.



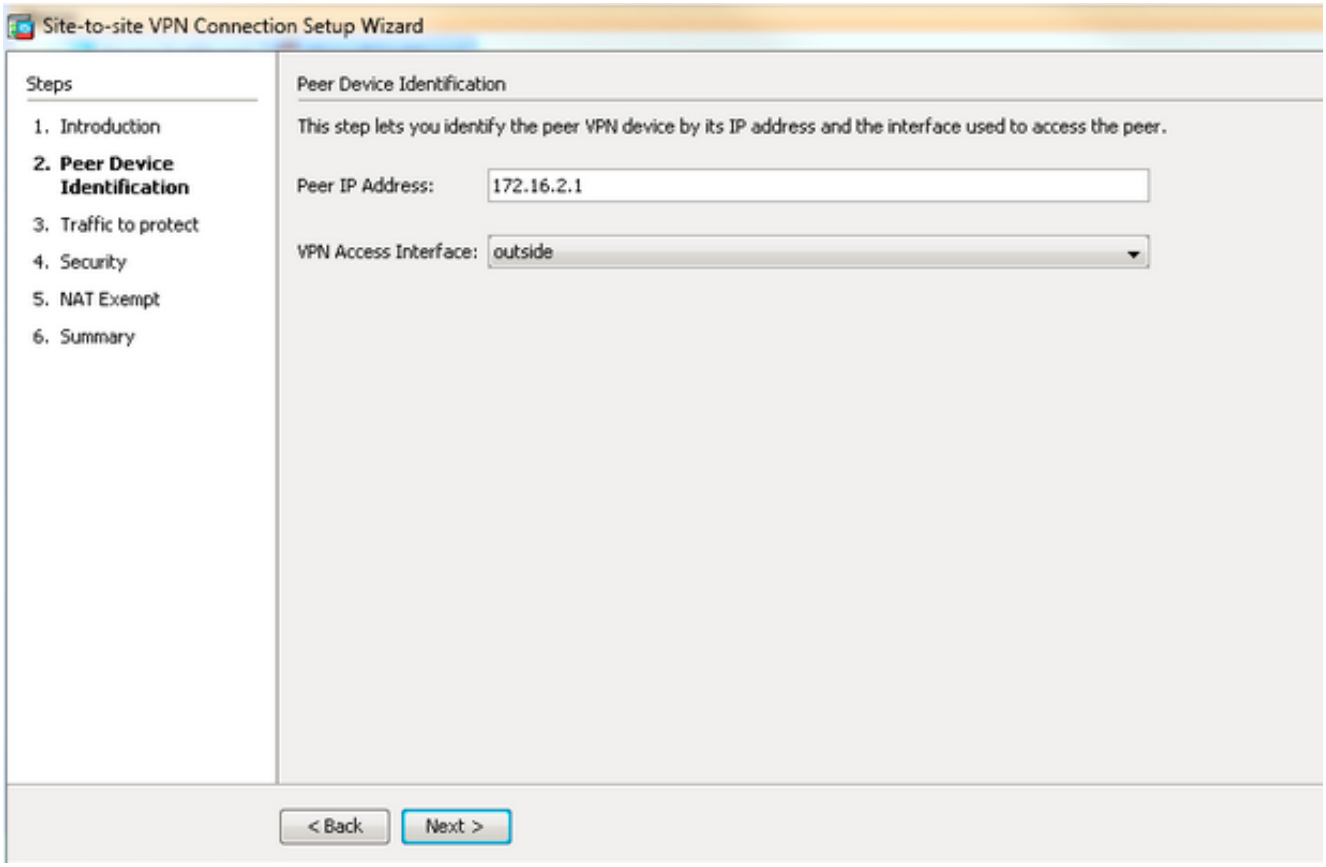
2. Next(**다음**)**를 클릭합니다**

.



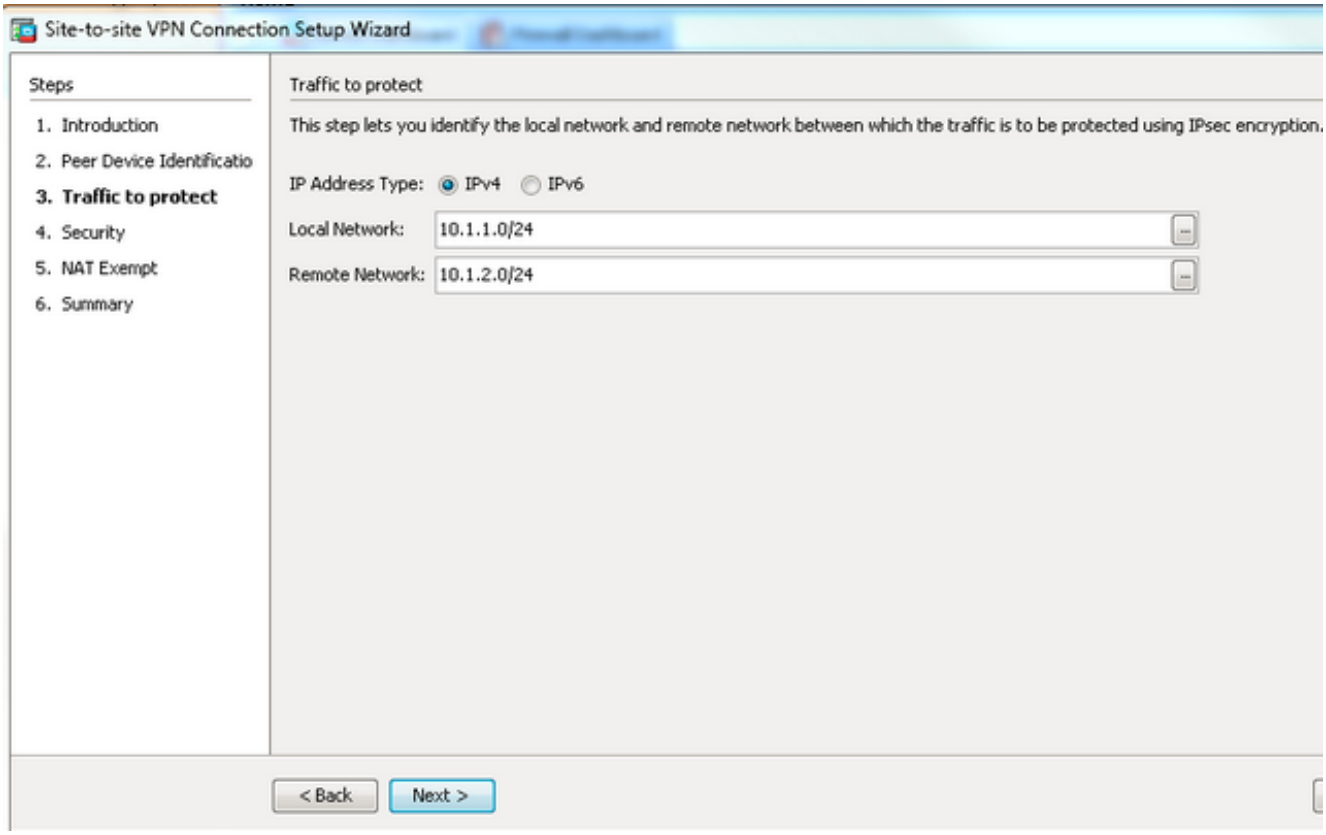
3. 원격 피어의 외부 IP 주소를 지정하려면 VPN Access Interface 드롭다운 목록에서 **outside**를 선택합니다.암호화 맵이 적용되는 인터페이스(**WAN**)를 선택합니다.Next(**다음**)**를 클릭합니다**

.



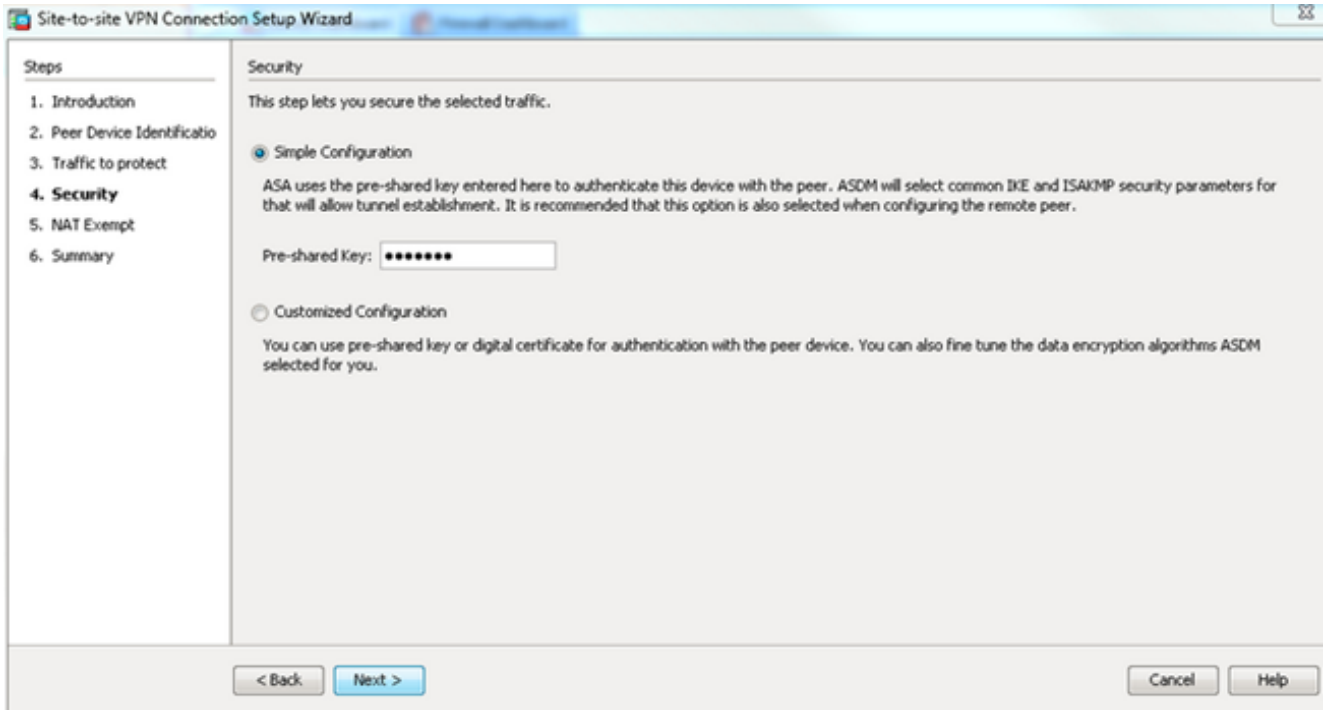
4. VPN 터널을 통과하도록 허용해야 하는 호스트/네트워크를 지정합니다.이 단계에서는 VPN 터널을 위한 로컬 네트워크 및 원격 네트워크를 제공해야 합니다.Local Network(로컬 네트워크) 및 Remote Network(원격 네트워크) 필드 옆의 버튼을 클릭하고 필요에 따라 주소를 선택합니다.완료되면 **Next**(다음)를 클릭합니다

.



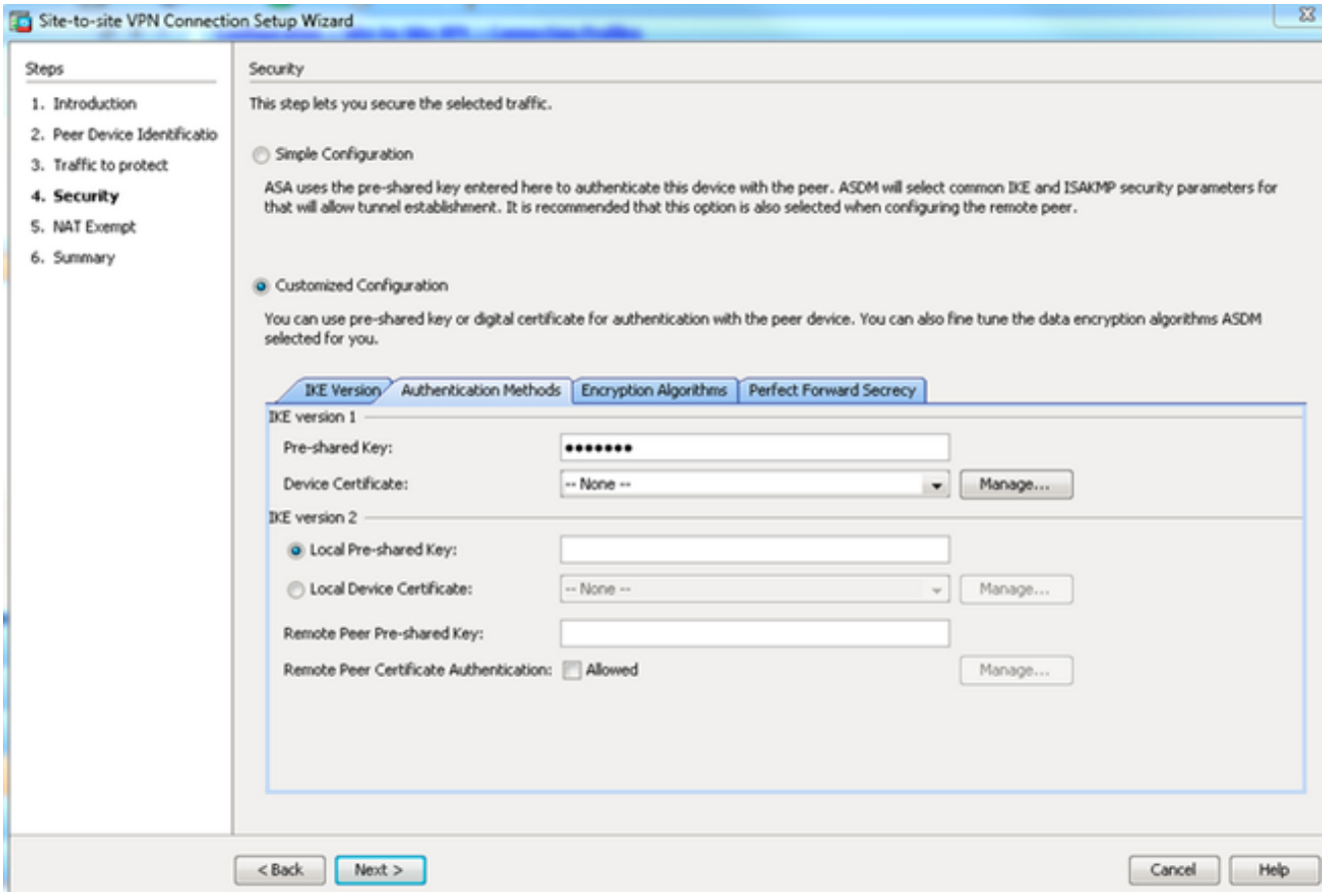
5. 이 예에서 사전 공유 키인 사용할 인증 정보를 입력합니다.이 예에서 사용되는 사전 공유 키는 cisco123입니다. L2L(LAN-to-LAN) VPN을 구성하는 경우 기본적으로 터널 그룹 이름은 원격 피어 IP 주소입니다

.



또는원하는 IKE 및 IPsec 정책을 포함하도록 컨피그레이션을 사용자 지정할 수 있습니다.피어 간에 하나 이상의 일치하는 정책이 있어야 합니다.Authentication Methods(인증 방법) 탭의 Pre-shared Key(사전 공유 키) 필드에 IKE 버전 1 사전 공유 키를 입력합니다.이 예에서는 **cisco123입니다**

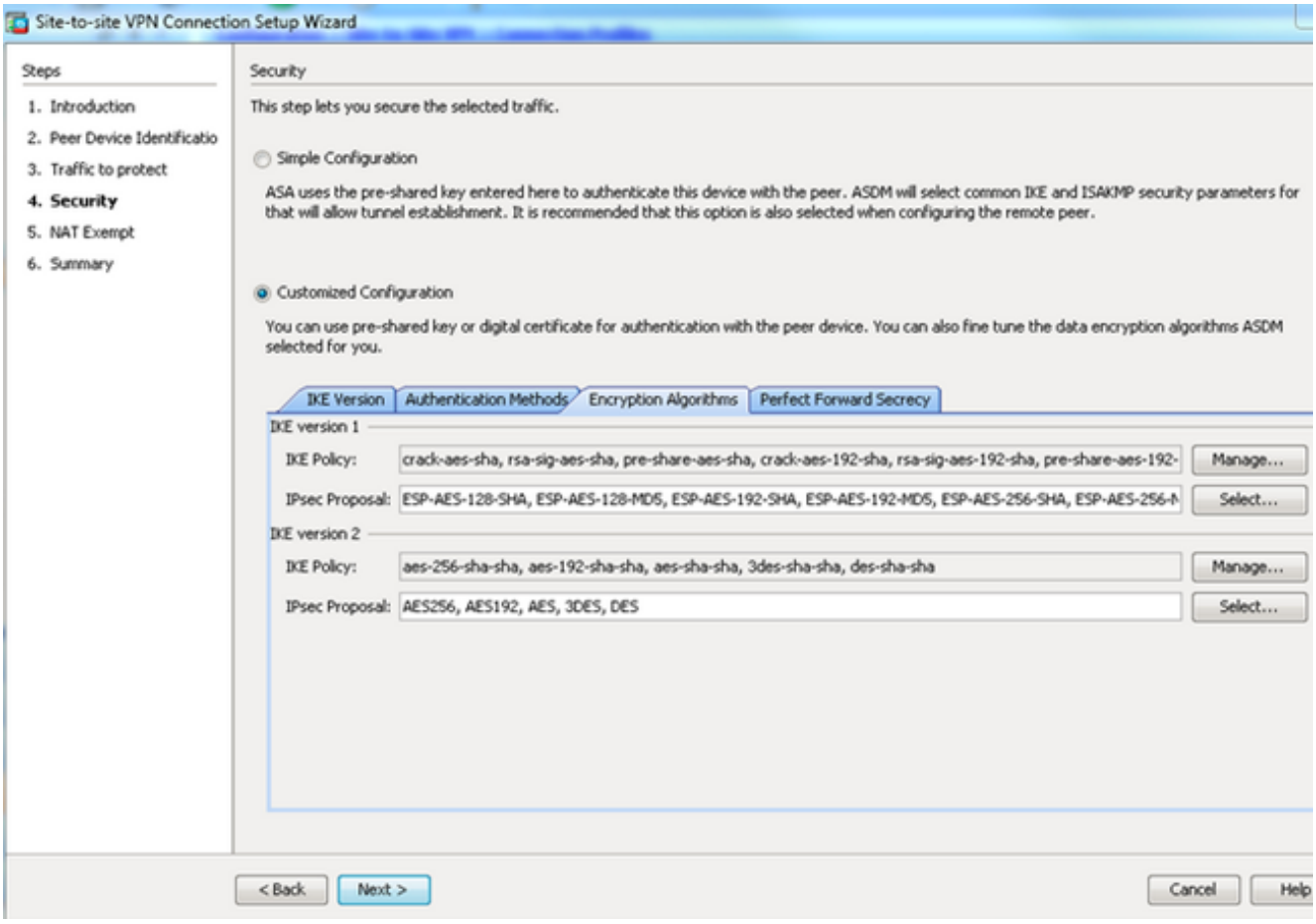
.



Encryption **Algorithms(암호화 알고리즘)** 탭을 클릭합니다.

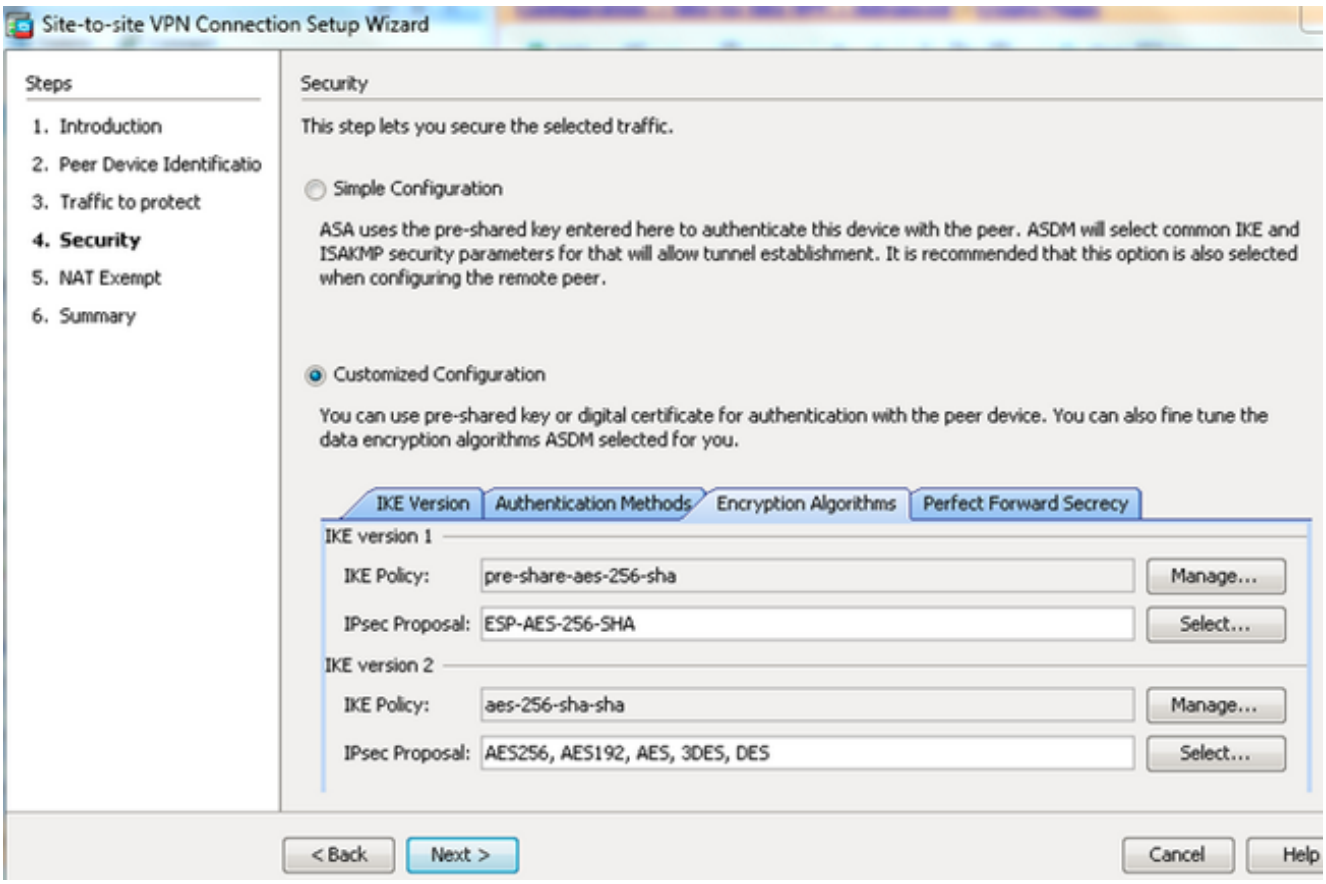
6. IKE **Policy**(IKE 정책) 필드 옆에 있는 Manage(관리)를 클릭하고 **Add** and configure a custom IKE Policy(사용자 지정 IKE 정책 추가 및 구성)**를** 클릭합니다(1단계). 완료되면 **OK**(확인)를 클릭합니다

.



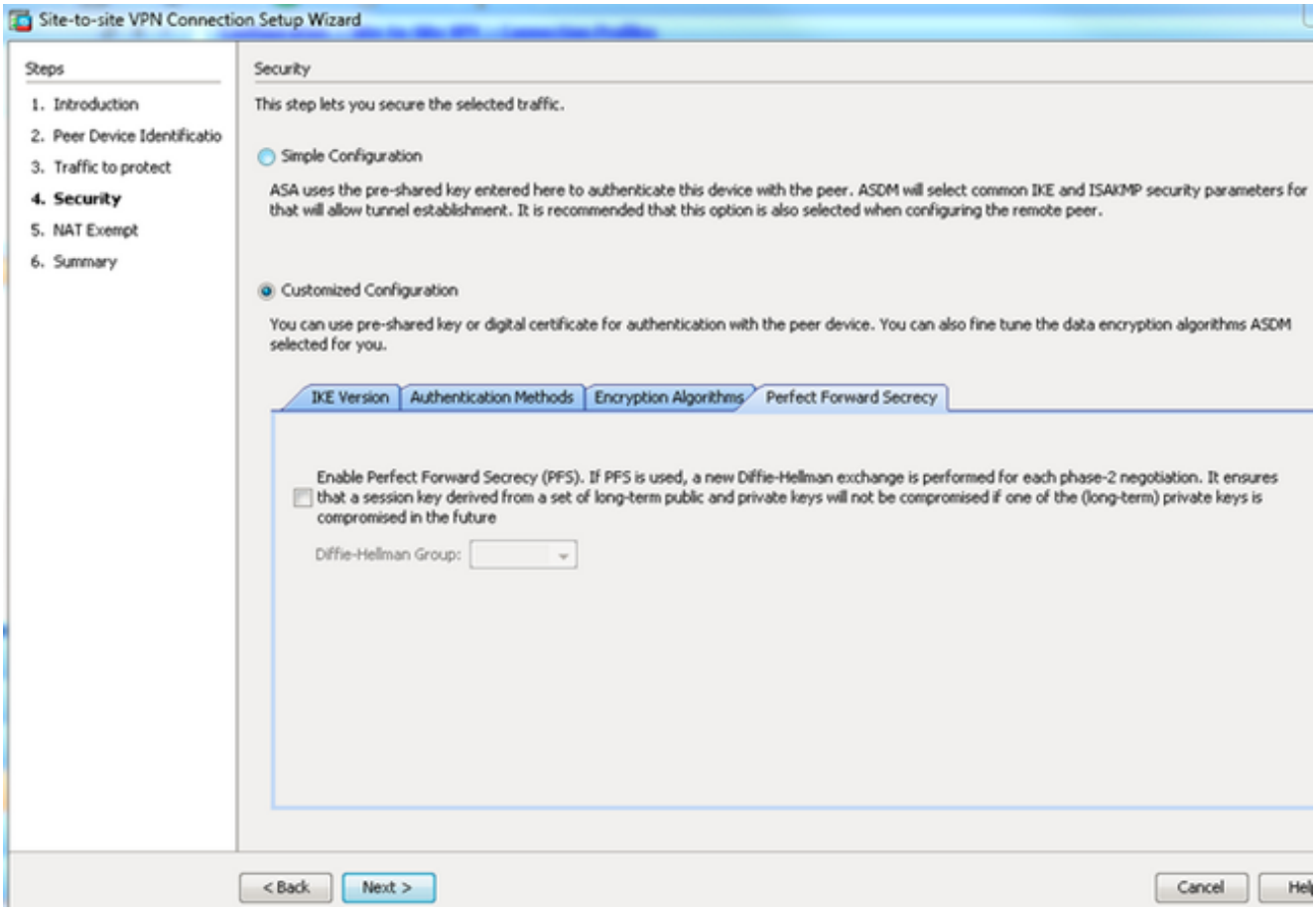
7. IPsec Proposal 필드 옆에 있는 Select(선택)를 클릭하고 원하는 IPsec Proposal(IPsec 제안)을 선택합니다.완료되면 **Next**(다음)를 클릭합니다

.



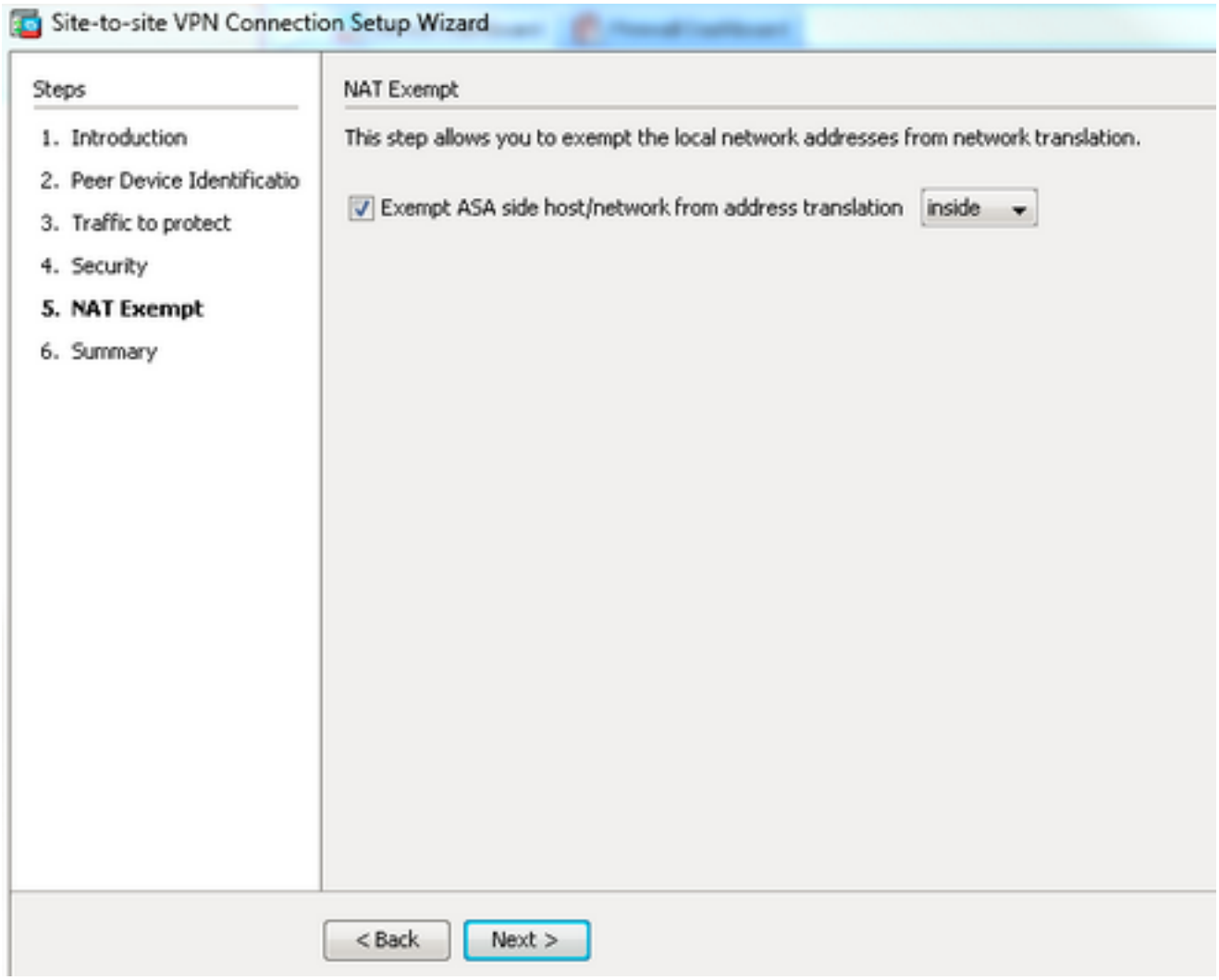
Perfect Forward Secrecy(PFS) 탭으로 이동하여 Enable Perfect Forward Secrecy**(PFS)** 확인란을 선택할 수도 있습니다.완료되면 **Next**(다음)를 클릭합니다

.



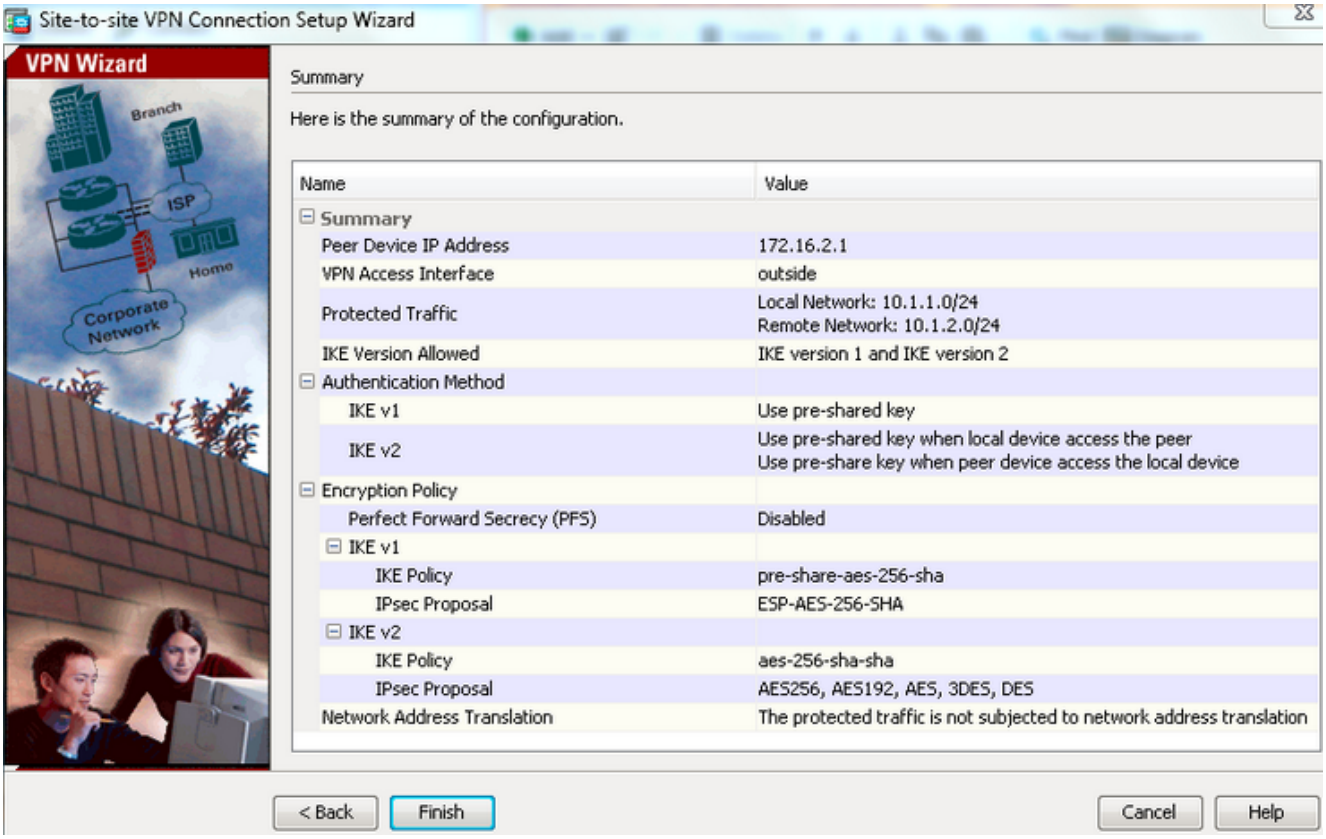
8. Exempt **ASA side host/network from address translation(ASA 측 호스트/네트워크에서 주소 변환 제외)** 확인란을 선택하여 터널 트래픽이 Network Address Translation(네트워크 주소 변환)을 시작할 수 없게 합니다.드롭다운 목록에서 **로컬 또는 내부**를 선택하여 로컬 네트워크에 연결할 수 있는 인터페이스를 설정합니다.Next(**다음)를 클릭합니다**

.



9. ASDM은 방금 구성한 VPN의 요약을 표시합니다.확인하고 **마침**을 클릭합니다

.



CLI 컨피그레이션

중앙 ASA(정적 피어) 컨피그레이션

1. 다음 예에서는 다음과 같이 VPN 트래픽에 대한 NO-NAT/NAT-EXEMPT 규칙을 구성합니다.
```
object network 10.1.1.0-remote_network
subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-inside_network
 subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
no-proxy-arp route-lookup
```
2. 원격 Dynamic-L2L-peer를 인증하려면 DefaultL2LGroup에서 사전 공유 키를 구성합니다.
```
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123
```
3. 2단계/ISAKMP 정책을 정의합니다.
```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```
4. 2단계 변환 세트/IPsec 정책을 정의합니다.
```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```
5. 다음 매개 변수를 사용하여 동적 맵을 구성합니다. 필요한 변형 집합보안 어플라이언스에서 연결된 클라이언트에 대한 라우팅 정보를 학습할 수 있는 RRI(Reverse Route Injection)를 활성화합니다(선택 사항).
```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset
crypto dynamic-map outside_dyn_map 1 set reverse-route
```

6. 동적 맵을 암호화 맵에 바인딩하고 암호화 맵을 적용하고 외부 인터페이스에서 ISAKMP/IKEv1을 활성화합니다.
```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

crypto map outside_map interface outside
crypto ikev1 enable outside
```

Remote-ASA(동적 피어)

1. VPN 트래픽에 대한 NAT 예외 규칙을 구성합니다.
```
object network 10.1.1.0-inside_network
subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-remote_network
subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
no-proxy-arp route-lookup
```
2. 고정 VPN 피어 및 사전 공유 키에 대한 터널 그룹을 구성합니다.
```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```
3. PHASE-1/ISAKMP 정책 정의:
```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```
4. 2단계 변형 집합/IPsec 정책을 정의합니다.
```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```
5. 흥미로운 VPN 트래픽/네트워크를 정의하는 액세스 목록을 구성합니다.
```
access-list outside_cryptomap extended permit ip object
10.1.1.0-inside_network object 10.1.2.0-remote_network
```
6. 다음 매개 변수를 사용하여 고정 암호화 맵을 구성합니다. 암호화/VPN 액세스 목록원격 IPsec 피어 IP 주소필요한 변형 집합
```
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set peer 172.16.2.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-256-SHA
```
7. 암호화 맵을 적용하고 외부 인터페이스에서 ISAKMP/IKEv1을 활성화합니다.
```
crypto map outside_map interface outside
crypto ikev1 enable outside
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

- **show crypto isakmp sa** - 피어의 현재 IKE SA(Security Associations)를 모두 표시합니다.
- **show crypto ipsec sa** - 현재 모든 IPsec SA를 표시합니다.

이 섹션에서는 두 ASA에 대한 확인 결과의 예를 보여줍니다.

중앙 ASA

```
Central-ASA#show crypto isakmp sa

  IKEv1 SAs:

     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: 172.16.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

    Central-ASA# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1

        local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      current_peer: 172.16.1.1

        #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #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
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

        local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 30D071C0
      current inbound spi : 38DA6E51

      inbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

원격-ASA

```
Remote-ASA#show crypto isakmp sa

  IKEv1 SAs:

     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: 172.16.2.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

  Remote-ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

        access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      current_peer: 172.16.2.1

        #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #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
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

        local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 38DA6E51
      current inbound spi : 30D071C0

      inbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

문제 해결

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

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

참고:debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

다음과 같이 다음 명령을 사용합니다.

```
clear crypto ikev1 sa <peer IP address>
Clears the Phase 1 SA for a specific peer.
```

주의:clear crypto **isakmp sa** 명령은 모든 활성 VPN 터널을 삭제하므로 방해가 됩니다.

PIX/ASA 소프트웨어 릴리스 8.0(3) 이상에서 **clear crypto isakmp sa** *<peer ip address>* 명령을 사용하여 개별 IKE SA를 지울 수 있습니다.8.0(3) 이전 소프트웨어 릴리스에서는 단일 터널에 대한 IKE 및 IPsec SA를 지우려면 **vpn-sessiondb logoff tunnel-group** *<tunnel-group-name>* 명령을 사용합니다.

```
Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1

clear crypto ipsec sa peer <peer IP address>
!!! Clears the required Phase 2 SA for specific peer.
debug crypto condition peer < Peer address>
!!! Set IPsec/ISAKMP debug filters.
debug crypto isakmp sa <debug level>
!!! Provides debug details of ISAKMP SA negotiation.
debug crypto ipsec sa <debug level>
!!! Provides debug details of IPsec SA negotiations
undebug all
!!! To stop the debugs
```

사용된 디버그:

```
debug cry condition peer <remote peer public IP>
debug cry ikev1 127
debug cry ipsec 127
```

Remote-ASA(개시자)

터널을 **시작하려면** 다음 packet-tracer 명령을 입력합니다.

```
Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed

IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple:
Prot=1, saddr=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
10.1.2.0, Crypto map (outside_map)
```

```
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
<skipped>...
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
+ VENDOR (13) + NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR ID received 172.16.2.1
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,
Oakley begin quick mode
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED


Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, IKE Initiator
starting QM: msg id = c45c7b30
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, Transmitting Proxy Id:
 Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
 Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +
ID (5) + ID (5) + NONE (0) total length : 172
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0
:
```

```
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Security negotiation complete for LAN-to-LAN Group (172.16.2.1)
Initiator, Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
```

Central-ASA(Responder)

```
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length
:
132
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, Connection landed on tunnel_group
DefaultL2LGroup
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Generating keys for Responder...
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) +
NONE (0) total length : 304
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8)
+ IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,
ID_IPV4_ADDR ID received172.16.1.1
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +
VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED
:
.
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, IKE Responder starting QM:
msg id = c45c7b30
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Received remote
IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,
Protocol 0, Port 0:
.
```

```
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,
IP = 172.16.1.1, Received local
IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0,
Protocol 0, Port 0Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map
check, map outside_dyn_map, seq = 1 is a successful match
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
:
.
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Transmitting Proxy Id:  Remote subnet: 10.1.1.0  Mask 255.255.255.0 Protocol 0  Port 0
Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE
(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED
Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security
negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) Responder,
Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Adding static
route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0
```

관련 정보

- Cisco ASA Series 명령 참조
- IPsec 협상/IKE 프로토콜 지원 페이지
- RFC(Request for Comments)
- 기술 지원 및 문서 - Cisco System