ASA 8.x/ASDM 6.x: ASDM을 사용하여 기존 Site-to-Site VPN에 새 VPN 피어 정보 추가

목차

소개

이 문서에서는 ASDM(Adaptive Security Device Manager)을 사용하여 기존 사이트 간 VPN 컨피그레이션에 새 VPN 피어가 추가될 때 수행할 컨피그레이션 변경 사항에 대한 정보를 제공합니다. 이는 다음 시나리오에서 필요합니다.

- ISP(인터넷 서비스 공급자)가 변경되었으며 새로운 공용 IP 범위 집합이 사용됩니다.
- 사이트에서 네트워크를 완전히 재설계합니다.
- 사이트에서 VPN 게이트웨이로 사용되는 디바이스는 다른 공용 IP 주소의 새 디바이스로 마이그레이션됩니다.

이 문서에서는 사이트 대 사이트 VPN이 이미 올바르게 구성되었으며 정상적으로 작동한다고 가정합니다. 이 문서에서는 L2L VPN 컨피그레이션에서 VPN 피어 정보를 변경하기 위해 따라야 할 단계를 제공합니다.

사전 요구 사항

요구 사항

Cisco에서는 이 주제에 대해 알고 있는 것이 좋습니다.

- ASA Site-to-Site VPN 컨피그레이션 예

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Adaptive Security Appliance 5500 Series(소프트웨어 버전 8.2 이상)
- 소프트웨어 버전 6.3 이상이 포함된 Cisco Adaptive Security Device Manager

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

Site-to-Site VPN은 HQASA와 BQASA 간에 잘 작동합니다. BQASA에 완전한 네트워크 재설계가 있고 IP 스키마가 ISP 레벨에서 수정되었지만 모든 내부 하위 네트워크 세부 정보는 동일하게 유지됩니다.

이 샘플 컨피그레이션에서는 다음 IP 주소를 사용합니다.

- 기존 BQASA 외부 IP 주소 - 200.200.200.200
- 새 BQASA 외부 IP 주소 - 209.165.201.2

참고: 여기서 피어 정보만 수정됩니다. 내부 서브넷에 다른 변경 사항이 없으므로 암호화 액세스 목록은 동일하게 유지됩니다.

ASDM 컨피그레이션

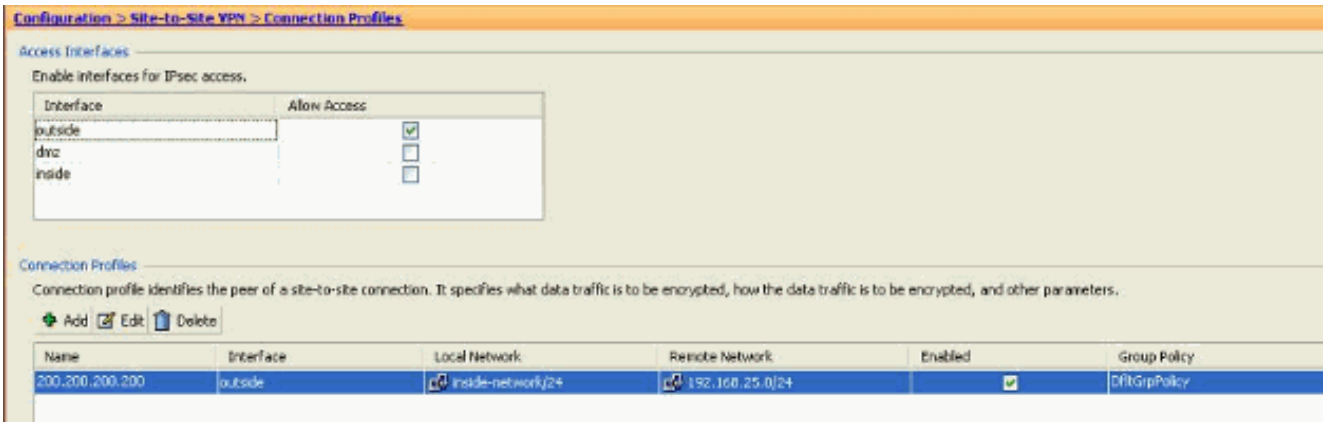
이 섹션에서는 ASDM을 사용하여 HQASA에서 VPN 피어 정보를 변경하는 데 사용할 수 있는 방법에 대한 정보를 제공합니다.

새 연결 프로파일 생성

기존 VPN 컨피그레이션을 방해하지 않고 새 VPN 피어 관련 정보로 새 연결 프로파일을 생성할 수 있으므로 이 방법이 더 쉽습니다.

1. Configuration(*구성*) > *Site-to-Site VPN* > *Connection Profiles(연결 프로파일)*로 이동하고 Connection Profiles(연결 프로파일) 영역 아래 *Add(추가)*를 클릭합니다

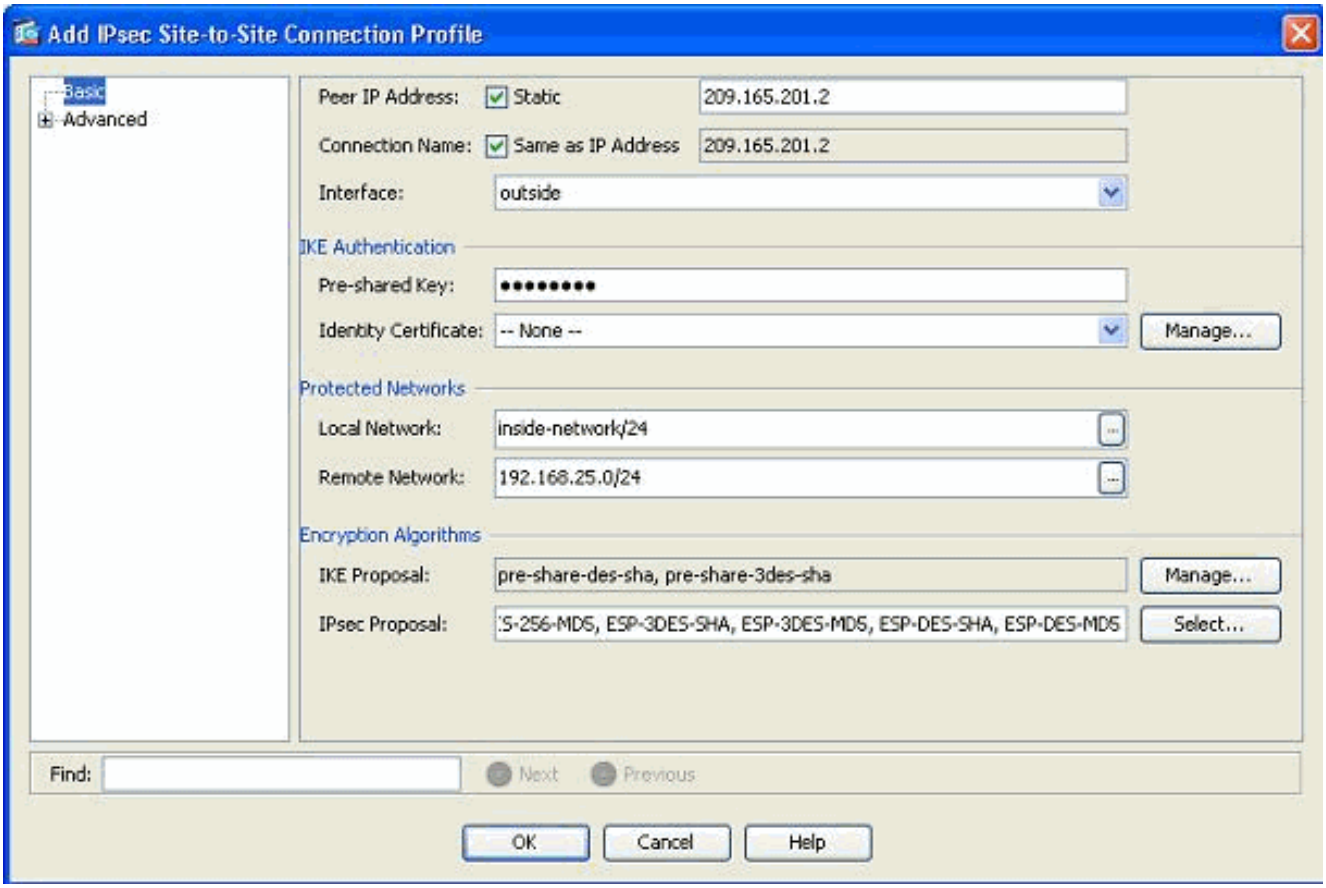
.



Add *IPSec Site-to-Site Connection Profile(IPSec 사이트 간 연결 프로파일 추가)* 창이 열립니다.

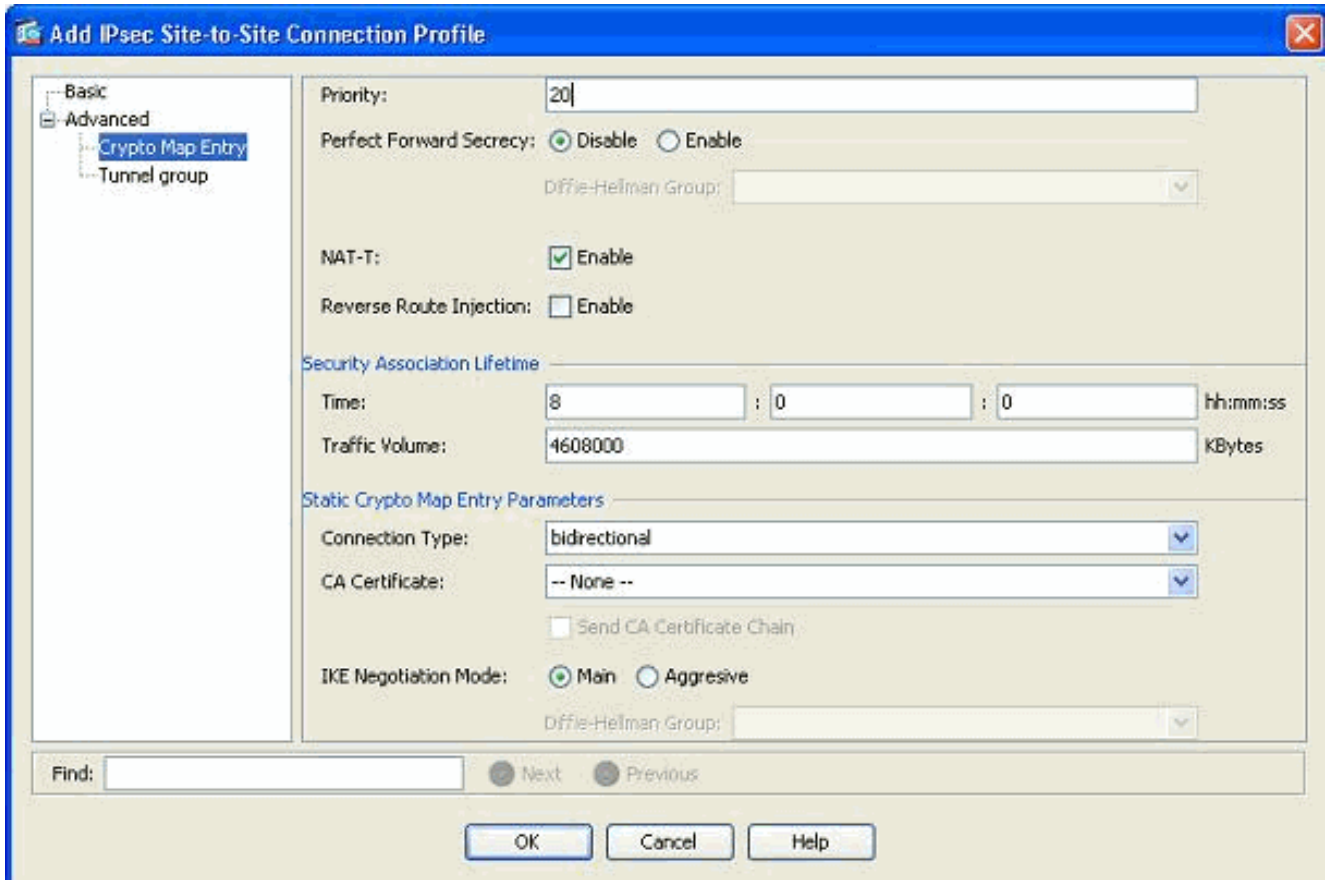
2. Basic(기본) 탭에서 *Peer IP Address(피어 IP 주소)*, Pre-shared Key(*사전 공유 키)* 및 Protected Networks(*보호된 네트워크)에* 대한 세부 정보를 *제공합니다*. 피어 정보를 제외하고 기존 VPN과 동일한 모든 매개변수를 사용합니다. *확인*을 *클릭합니다*

.



3. Advanced(고급) 메뉴에서 Crypto *Map Entry(암호화 맵 항목)를 클릭합니다*. 우선 순위 탭을 *참조하십시오*. 이 우선 순위는 해당 CLI 컨피그레이션의 시퀀스 번호와 같습니다. 기존 암호화 맵 엔트리보다 작은 번호가 할당되면 이 새 프로파일이 먼저 실행됩니다. 우선순위 번호가 높을수록 값이 낮습니다. 이는 특정 암호화 맵이 실행될 시퀀스 순서를 변경하는 데 사용됩니다. 확인을 클릭하여 새 연결 프로파일 생성을 완료합니다

.



그러면 연결된 암호화 맵과 함께 새 터널 그룹이 자동으로 생성됩니다. 이 새 연결 프로파일을 사용하기 전에 새 IP 주소로 BQASA에 연결할 수 있는지 확인합니다.

기존 VPN 컨피그레이션 수정

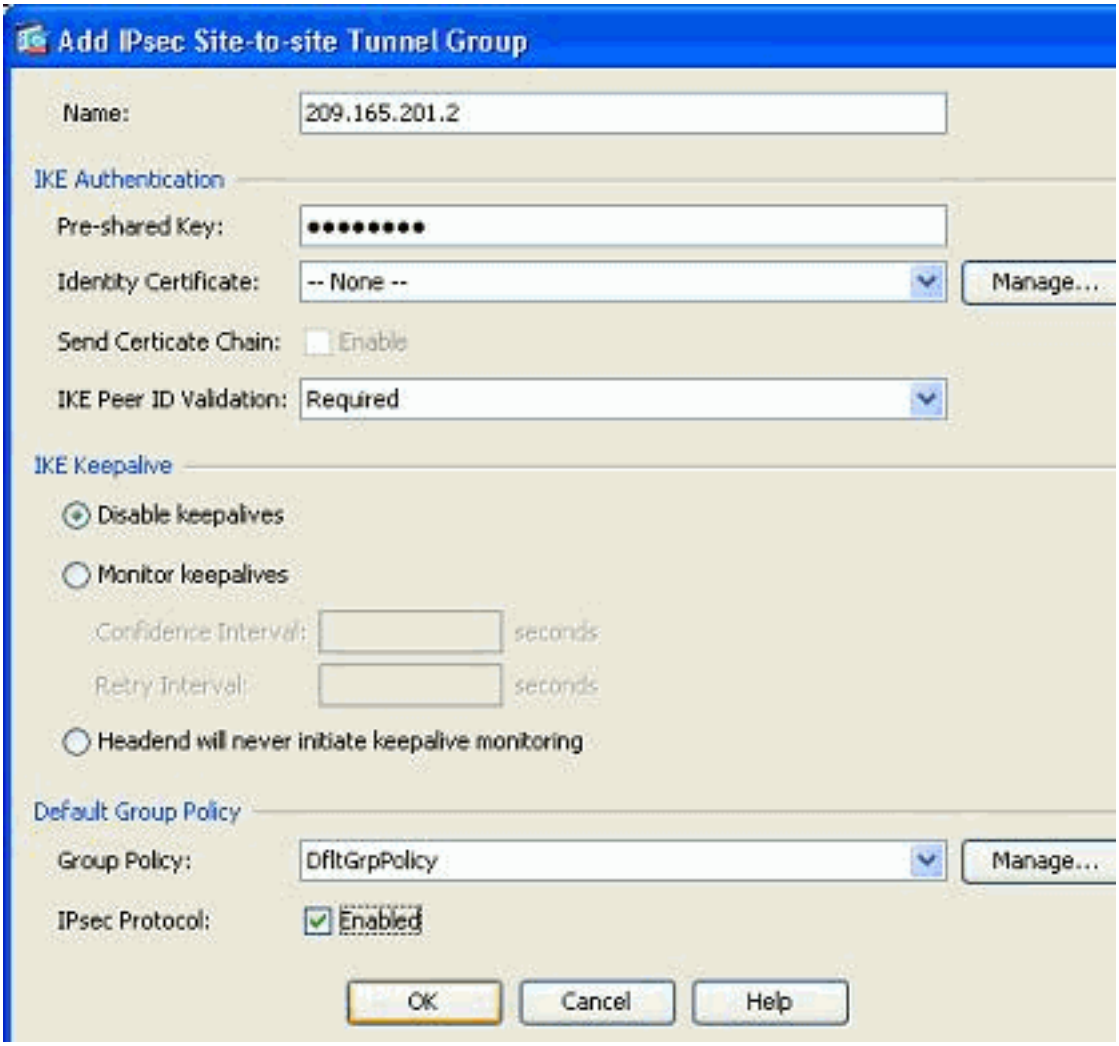
새 피어를 추가하는 또 다른 방법은 기존 컨피그레이션을 수정하는 것입니다. 기존 연결 프로파일은 특정 피어에 바인딩되어 있으므로 새 피어 정보에 대해 편집할 수 없습니다. 기존 컨피그레이션을 수정하려면 다음 단계를 수행해야 합니다.

1. 새 터널 그룹 생성
2. 기존 암호화 맵 편집

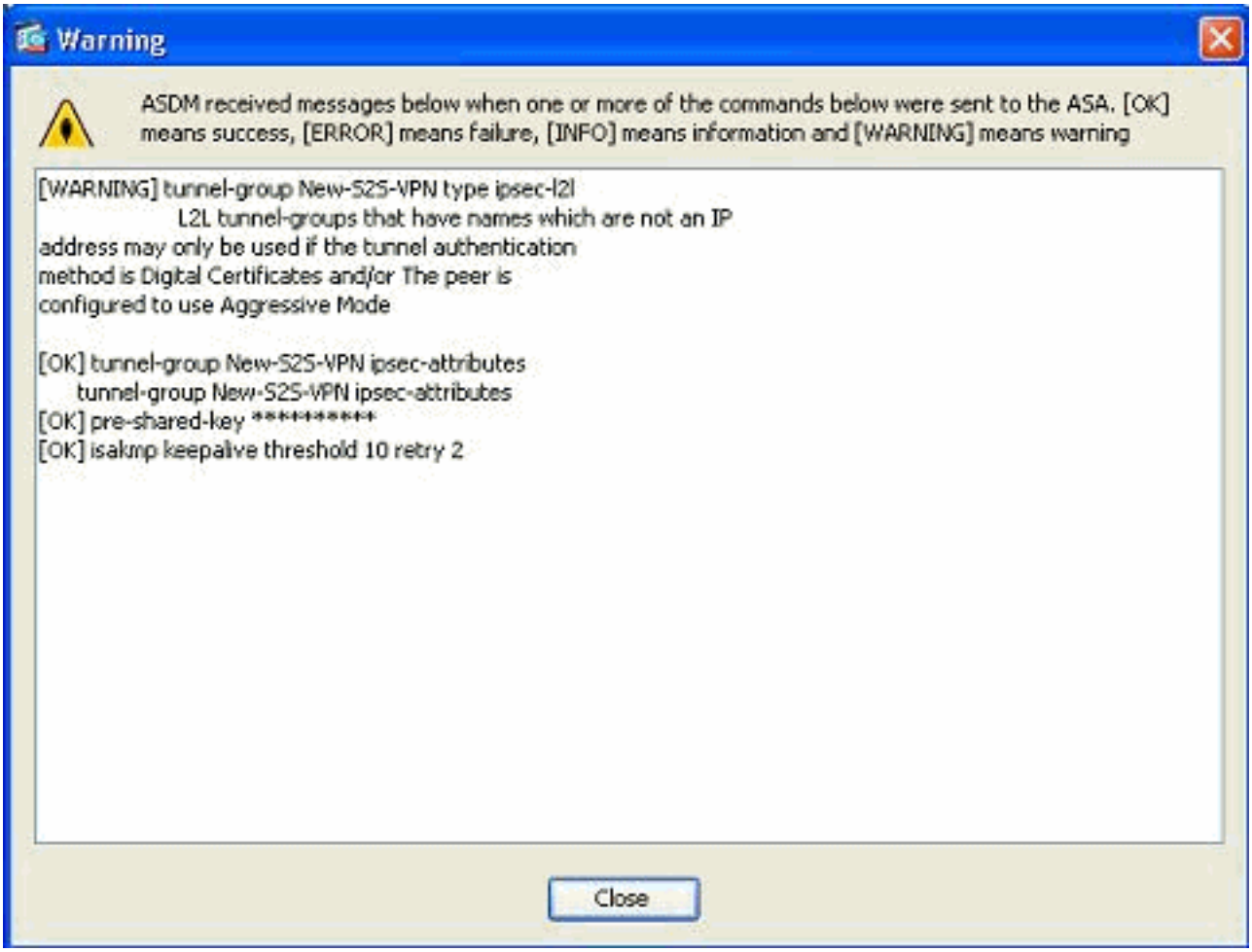
새 터널 그룹 생성

Configuration(*구성*) > *Site-to-Site VPN* > *Advanced(고급)* > *Tunnel groups(터널 그룹)*로 이동하여 *Add(추가)*를 클릭하여 새 VPN 피어 정보를 포함하는 새 터널 그룹을 생성합니다. Name(*이름*) 및 *Pre-shared Key(사전 공유 키)* 필드를 지정한 다음 *OK(확인)*를 클릭합니다.

참고: 사전 공유 키가 VPN의 다른 끝과 일치하는지 확인합니다.



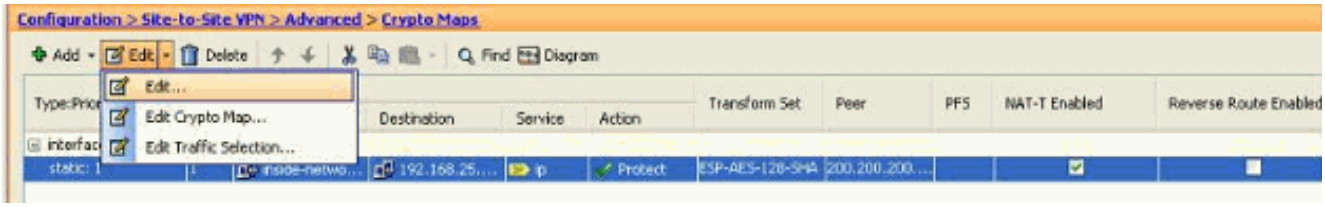
참고: 인증 모드가 사전 공유 키인 경우 Name(이름) 필드에 원격 피어의 IP 주소만 입력해야 합니다. 인증 방법이 인증서를 통할 때만 모든 이름을 사용할 수 있습니다. 이 오류는 Name 필드에 이름이 추가되고 인증 방법이 미리 공유될 때 나타납니다.



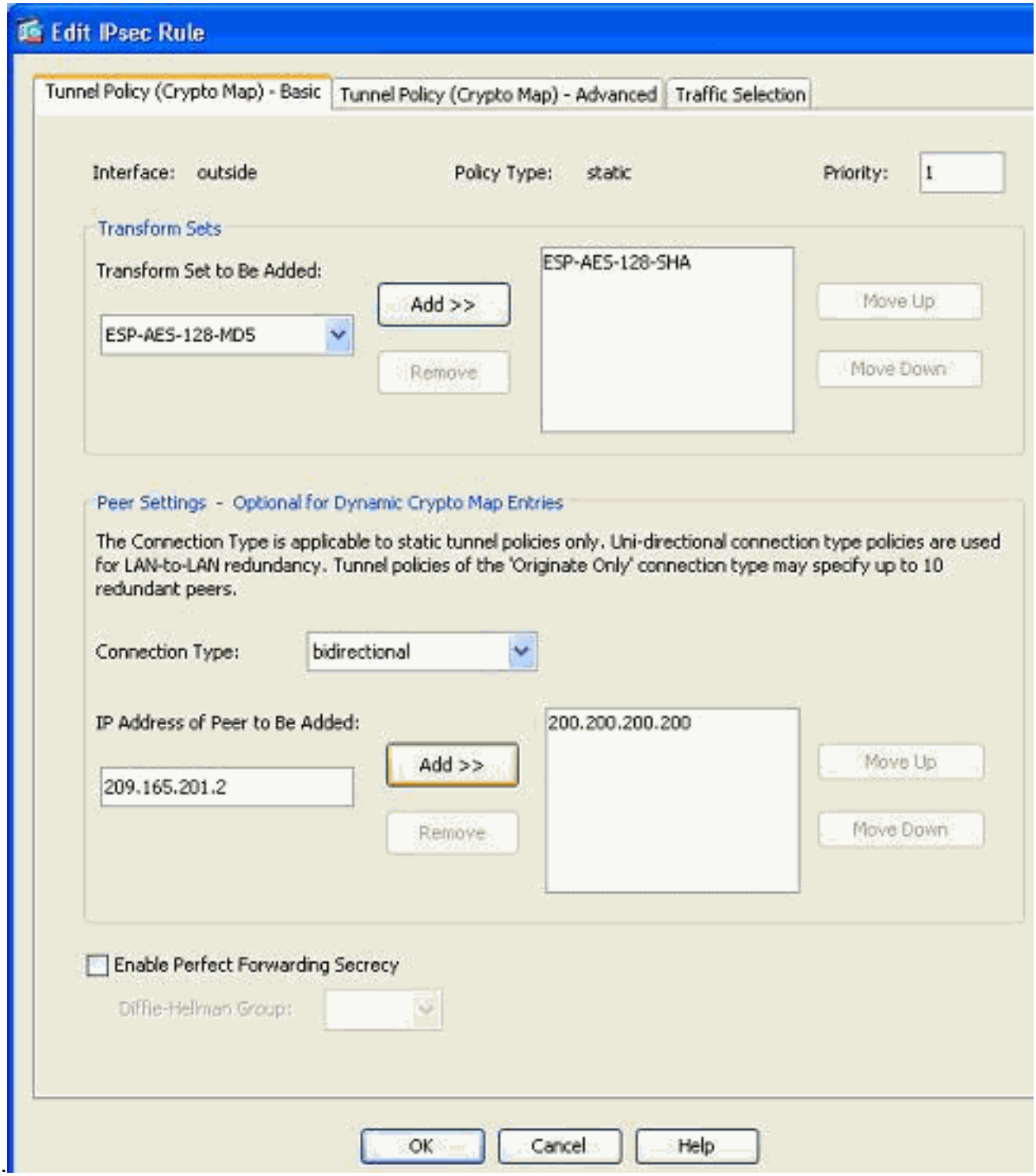
기존 암호화 맵 편집

새 피어 정보를 연결하기 위해 기존 암호화 맵을 수정할 수 있습니다.

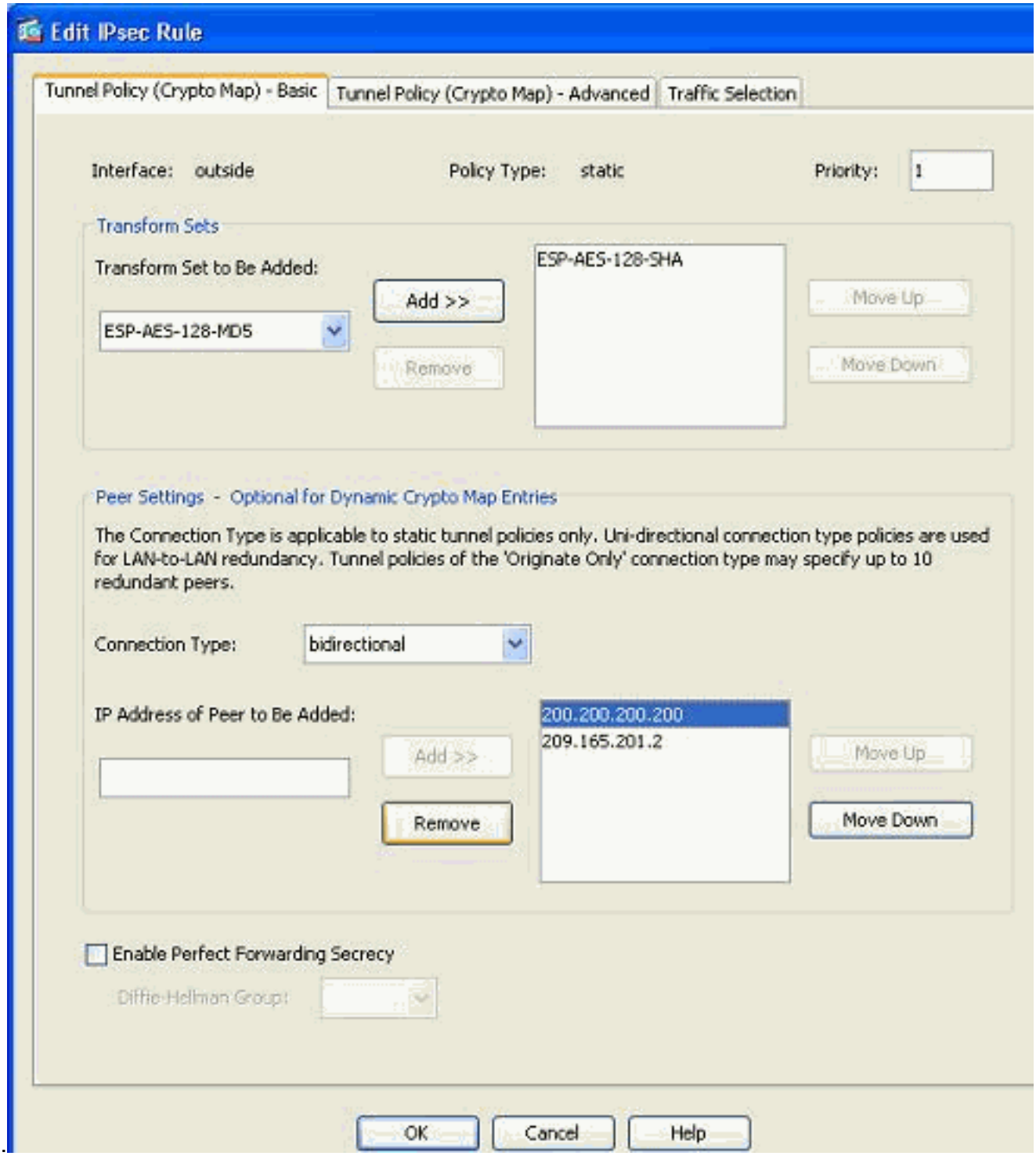
다음 단계를 완료하십시오.

1. Configuration(*구성*) > *Site-to-Site VPN* > *Advanced(고급)* > *Crypto Maps(암호화 맵)로* 이동한 다음 필요한 암호화 맵을 선택하고 Edit(수정)를 *클릭합니다*
.


Edit *IPSec Rule* 창이 나타납니다.
2. Tunnel Policy (Basic)(터널 정책(기본)) 탭의 Peer Settings(피어 설정) 영역에서 추가할 피어의 IP 주소 필드에 새 피어를 지정합니다. 그런 다음 Add(*추가)를* 클릭합니다

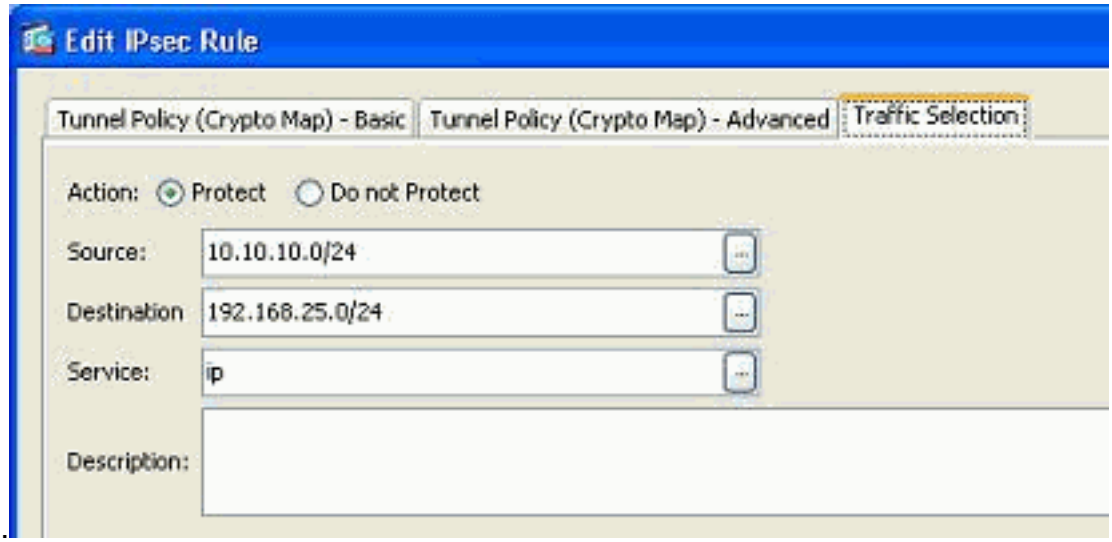


3. 기존 피어 IP 주소를 선택하고 *Remove(제거)*를 클릭하여 새 피어 정보만 유지합니다. *확인*을 *클릭합니다*

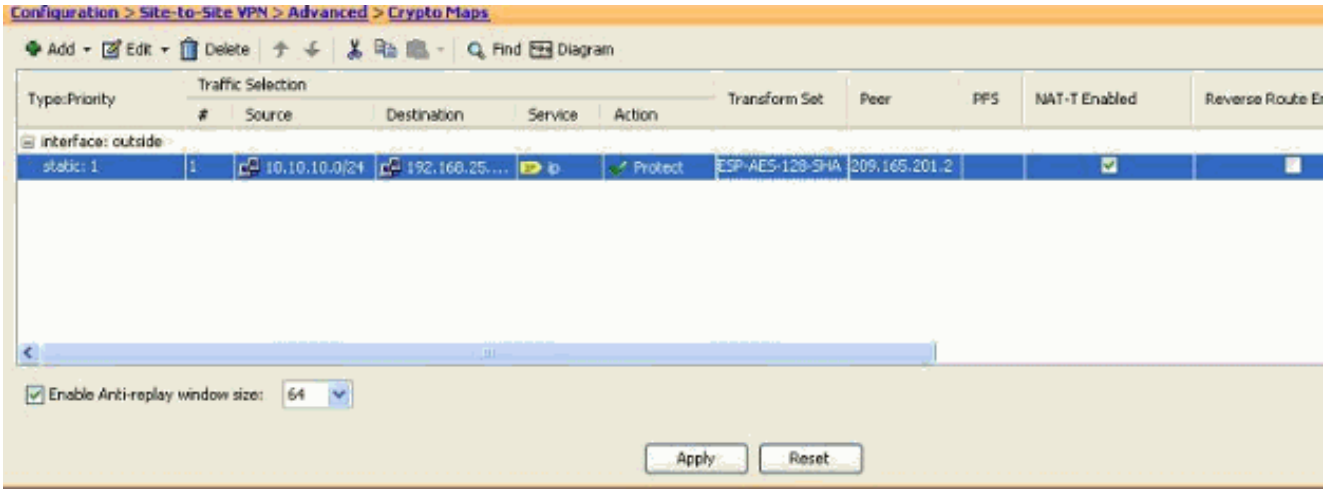


참고: 현재 암호화 맵에서 피어 정보를 수정하면 이 암호화 맵과 연결된 연결 프로파일이 ASDM 창에서 즉시 삭제됩니다.

4. 암호화된 네트워크의 세부 사항은 동일하게 유지됩니다. 이를 수정해야 하는 경우 *Traffic Selection* 탭으로 이동합니다



5. 수정된 암호화 맵을 보려면 *Configuration > Site-to-Site VPN > Advanced > Crypto Maps* 창으로 이동합니다. 그러나 이러한 변경 사항은 *적용*을 클릭해야 적용됩니다. Apply(*적용*)를 클릭한 후 Configuration(컨피그레이션) > *Site-to-Site VPN > Advanced(고급) > Tunnel groups(터널 그룹)* 메뉴로 이동하여 연결된 터널 그룹이 있는지 확인합니다. 대답이 "예"인 경우 연결된 *연결 프로파일*이 생성됩니다



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.

- 단일 피어에 대한 보안 연결 매개변수를 보려면 다음 명령을 사용합니다.show crypto ipsec sa peer <Peer IP address>

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

IKE Initiator가 정책을 찾을 수 없음: intf test_ext, 소스: 172.16.1.103, Dst: 10.1.4.251

이 오류는 VPN Concentrator에서 ASA로 VPN 피어를 변경하려고 할 때 로그 메시지에 표시됩니다.

해결책:

이는 마이그레이션 중에 발생한 구성 단계가 잘못되었기 때문일 수 있습니다. 새 피어를 추가하기 전에 인터페이스에 대한 암호화 바인딩이 제거되었는지 확인합니다. 또한 터널 그룹에서 피어의 IP 주소를 사용했지만 이름은 사용하지 않았는지 확인합니다.

관련 정보

- ASA를 사용하는 L2L(Site to Site) VPN
- 가장 일반적인 VPN 문제
- ASA 기술 지원 페이지
- 기술 지원 및 문서 – Cisco Systems