ASDM 6.4:IKEv2 컨피그레이션을 사용하는 Site-to-Site VPN 터널 예

목차

소개

이 문서에서는 IKE(Internet Key Exchange) 버전 2를 사용하여 두 Cisco ASA(Adaptive Security Appliance) 간에 사이트 간 VPN 터널을 구성하는 방법에 대해 설명합니다. ASDM(Adaptive Security Device Manager) GUI 마법사를 사용하여 VPN 터널을 구성하는 데 사용되는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco ASA가 기본 설정으로 구성되어 있는지 확인합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.4 이상을 실행하는 Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco ASDM 소프트웨어 버전 6.4 이상

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

IKEv2는 다음과 같은 이점을 포함하는 기존 IKEv1 프로토콜의 향상된 기능입니다.

- IKE 피어 간 메시지 교환 수 감소
- 단방향 인증 방법
- DPD(Dead Peer Detection) 및 NAT-Traversal에 대한 내장 지원
- 인증을 위한 EAP(Extensible Authentication Protocol) 사용
- 안티클로깅 쿠키를 사용하여 간단한 DoS 공격의 위험 제거

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

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

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.

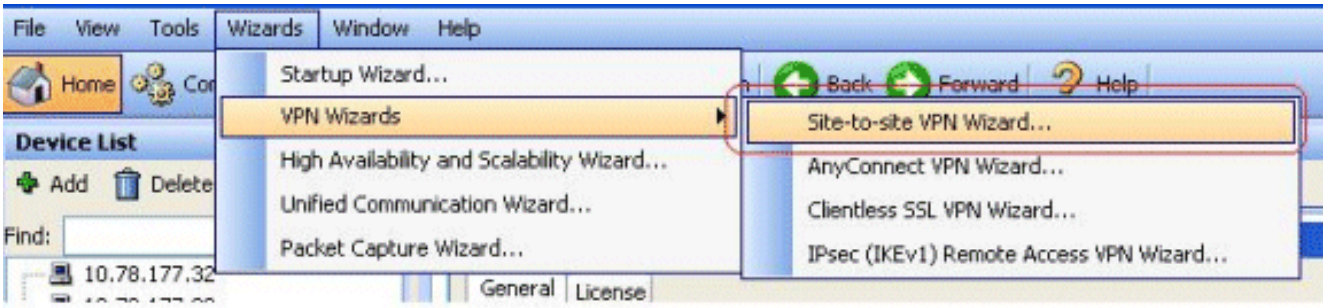
이 문서에서는 HQ-ASA에서 사이트 대 사이트 VPN 터널의 컨피그레이션을 보여줍니다.BQ-ASA에서 미러로 동일한 작업을 수행할 수 있습니다.

HQ-ASA의 ASDM 컨피그레이션

이 VPN 터널은 사용하기 쉬운 GUI 마법사를 사용하여 구성할 수 있습니다.

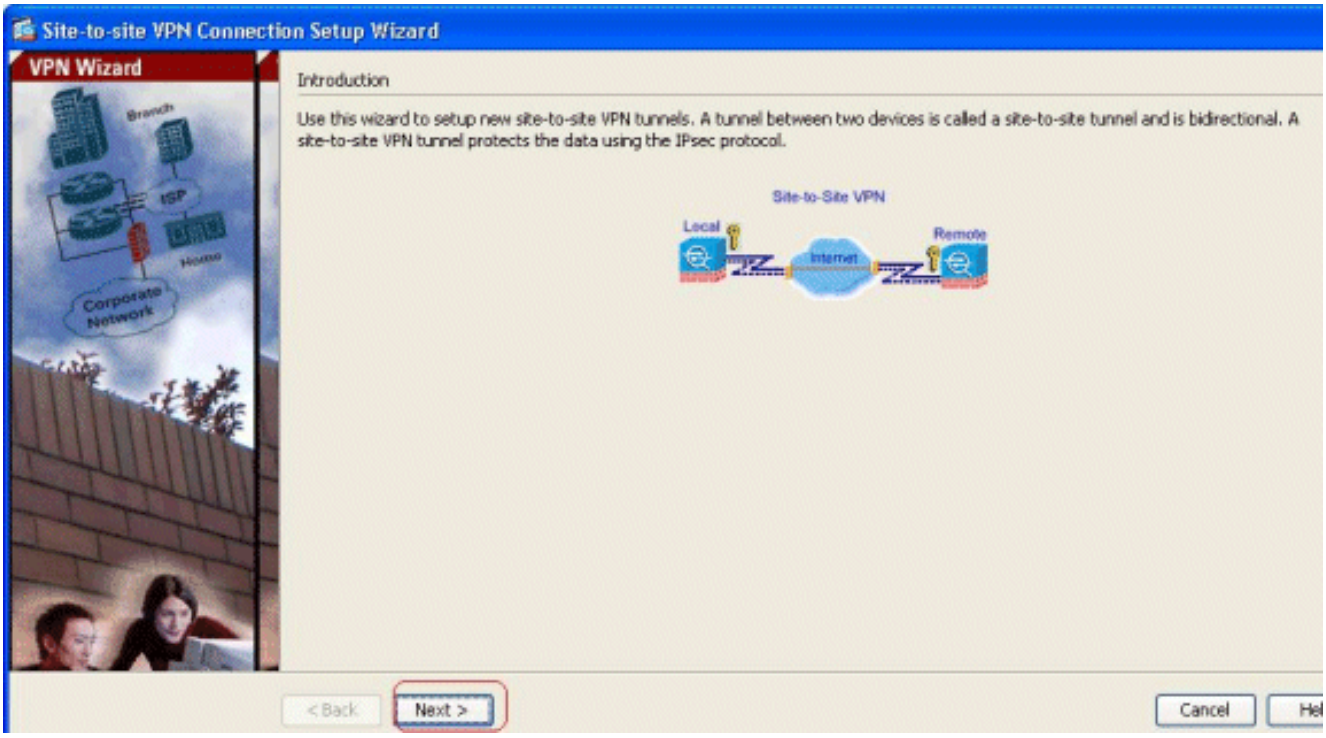
다음 단계를 완료하십시오.

1. ASDM에 로그인하고 Wizards(마법사) > **VPN Wizards(VPN 마법사) > Site-to-site VPN Wizard(사이트 간 VPN 마법사)로** 이동합니다
.



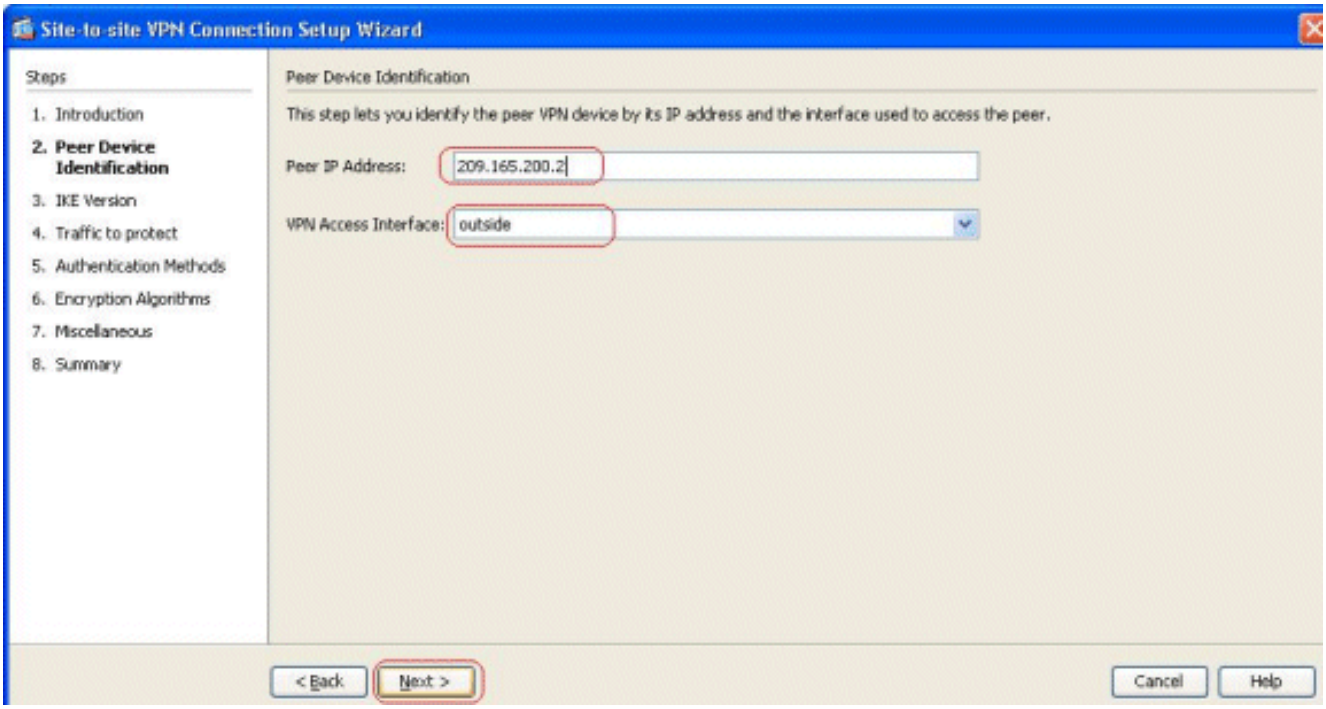
2. 사이트 대 사이트 VPN 연결 설정 창이 나타납니다.Next(**다음)를 클릭합니다**

.



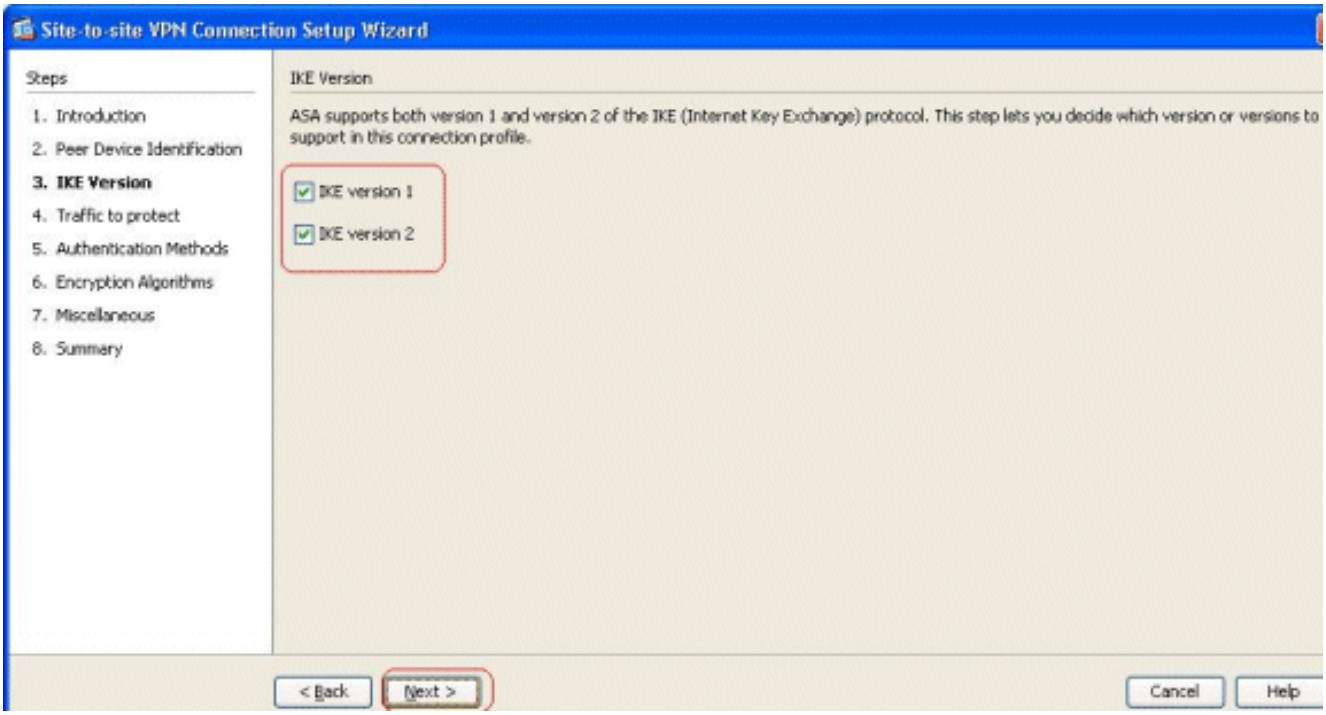
3. 피어 IP 주소 및 VPN 액세스 인터페이스를 지정합니다.Next(**다음)를 클릭합니다**

.



4. 두 IKE 버전을 모두 선택하고 Next(**다음**)를 클릭합니다

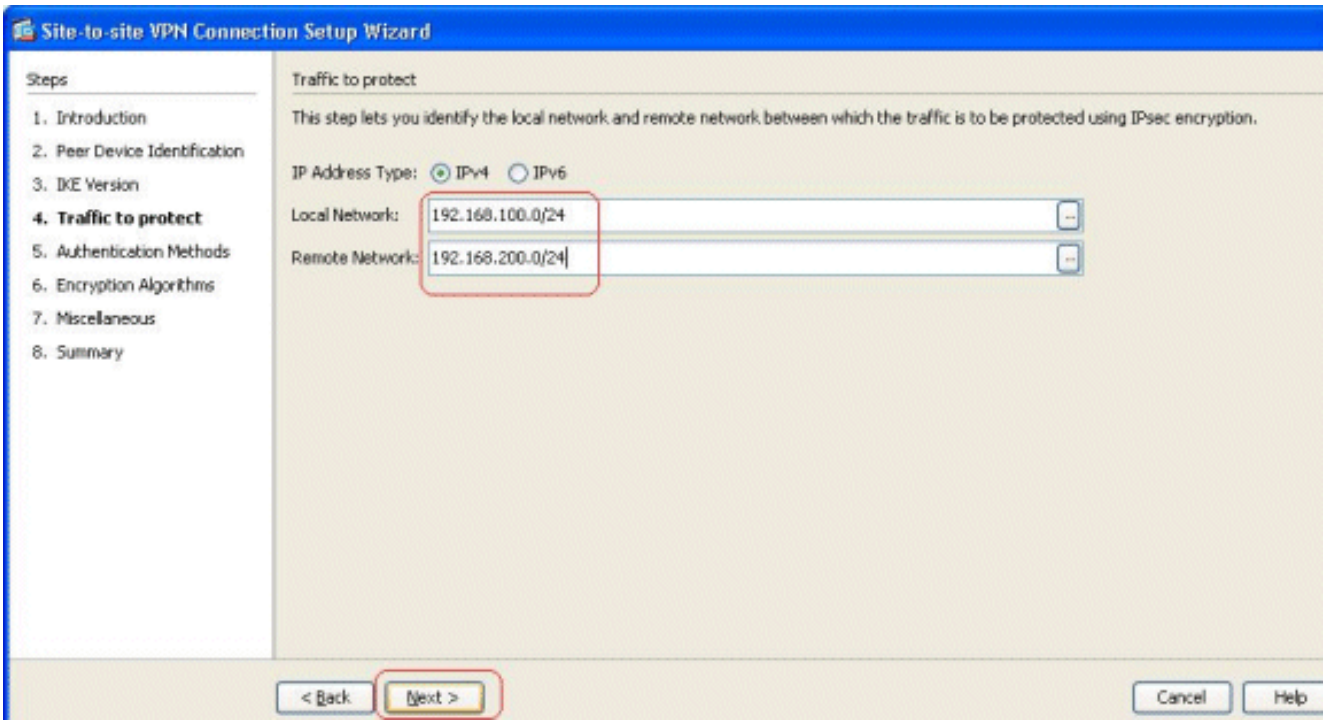
.



참고: IKEv2에 장애가 발생할 경우 이니시에이터가 IKEv2에서 IKEv1으로의 백업을 가질 수 있으므로 두 버전의 IKE가 모두 여기서 구성됩니다.

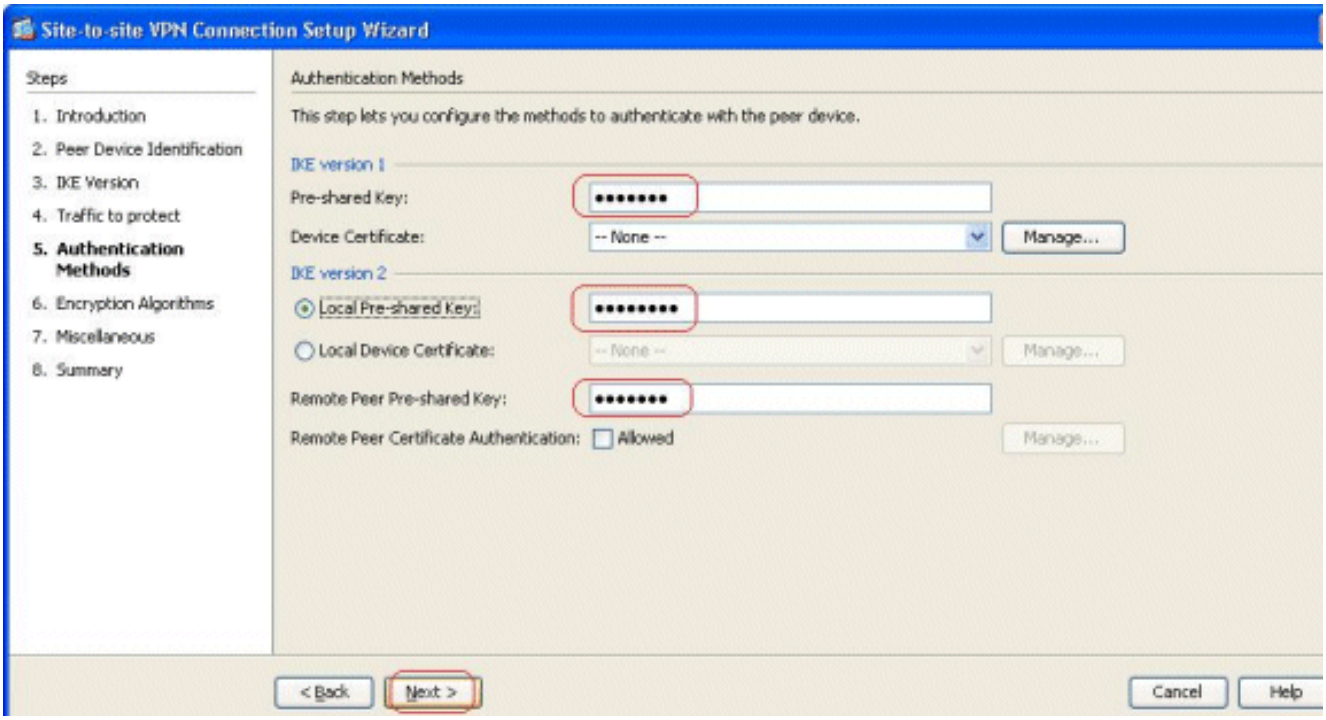
5. 이러한 네트워크 간의 트래픽이 암호화되어 VPN 터널을 통과하도록 로컬 네트워크 및 원격 네트워크를 지정합니다.Next(**다음)를 클릭합니다**

.



6. 두 버전의 IKE에 대해 사전 공유 키를 지정합니다

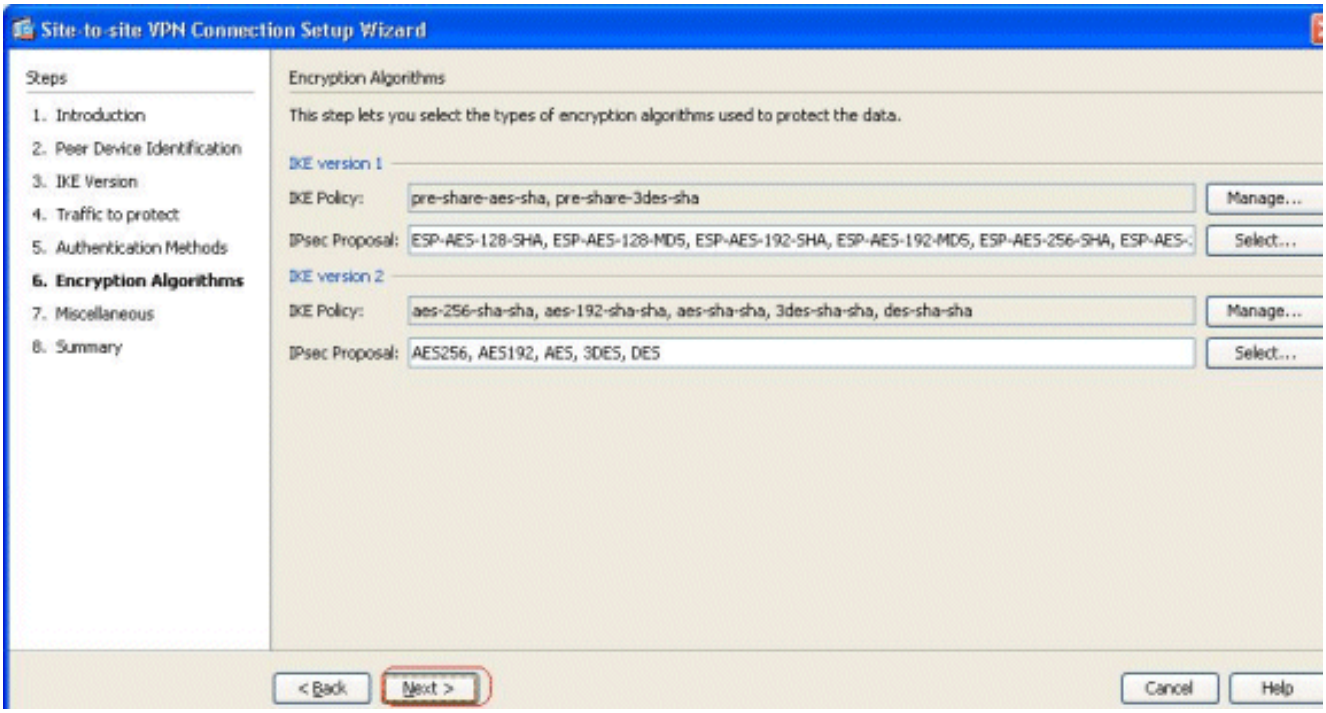
.



IKE 버전 1과 2의 주요 차이점은 허용되는 인증 방법의 조건에 있습니다.IKEv1은 두 VPN 종료(즉, 사전 공유 키 또는 인증서)에서 하나의 인증 유형만 허용합니다. 그러나 IKEv2에서는 별도의 로컬 및 원격 인증 CLI를 사용하여 비대칭 인증 방법을 구성할 수 있습니다(즉, 발신자에 대한 사전 공유 키 인증은 있지만 응답자에 대한 인증서 인증).또한 양쪽 끝에서 서로 다른 사전 공유 키를 가질 수 있습니다.HQ-ASA 끝의 로컬 사전 공유 키는 BQ-ASA 끝의 원격 사전 공유 키가 됩니다.마찬가지로 HQ-ASA 끝의 Remote Pre-shared 키는 BQ-ASA 끝의 Local Pre-shared 키가 됩니다.

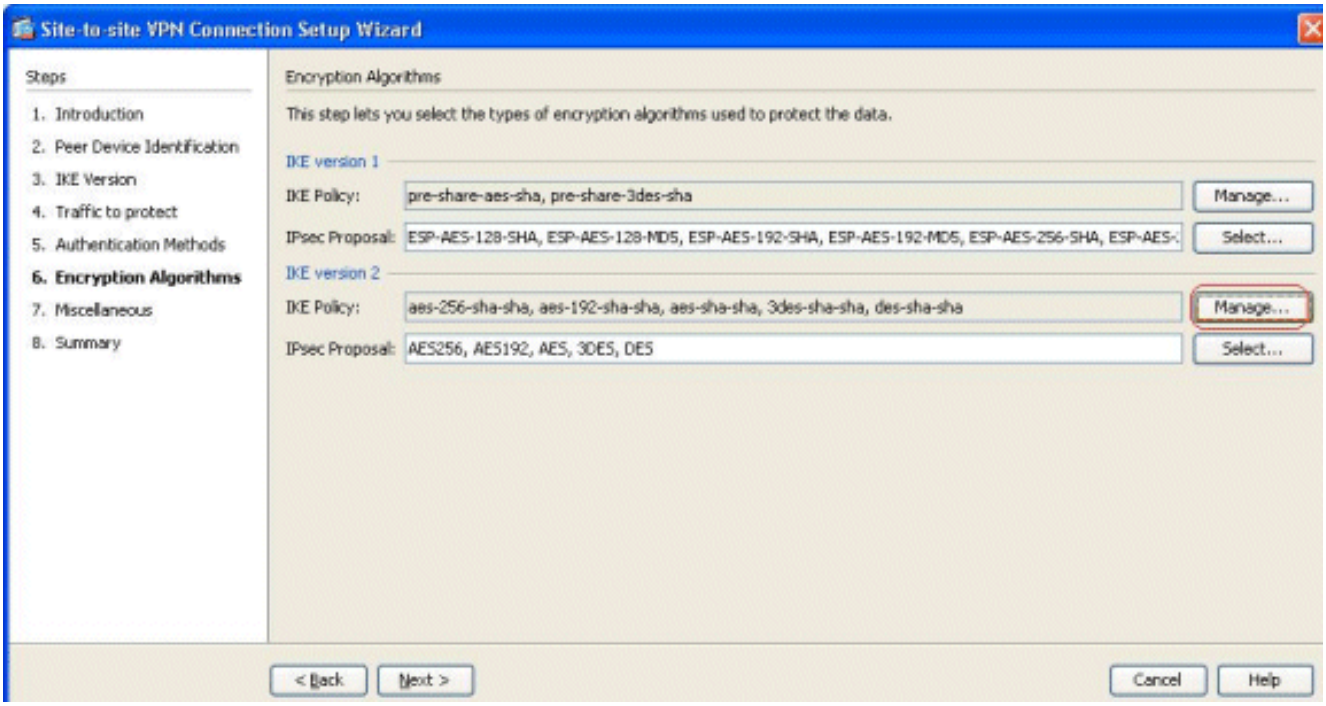
7. IKE 버전 1과 2의 암호화 알고리즘을 지정합니다. 여기서 기본값은 수락됩니다

.



8. IKE 정책을 수정하려면 **Manage..**를 클릭합니다

.



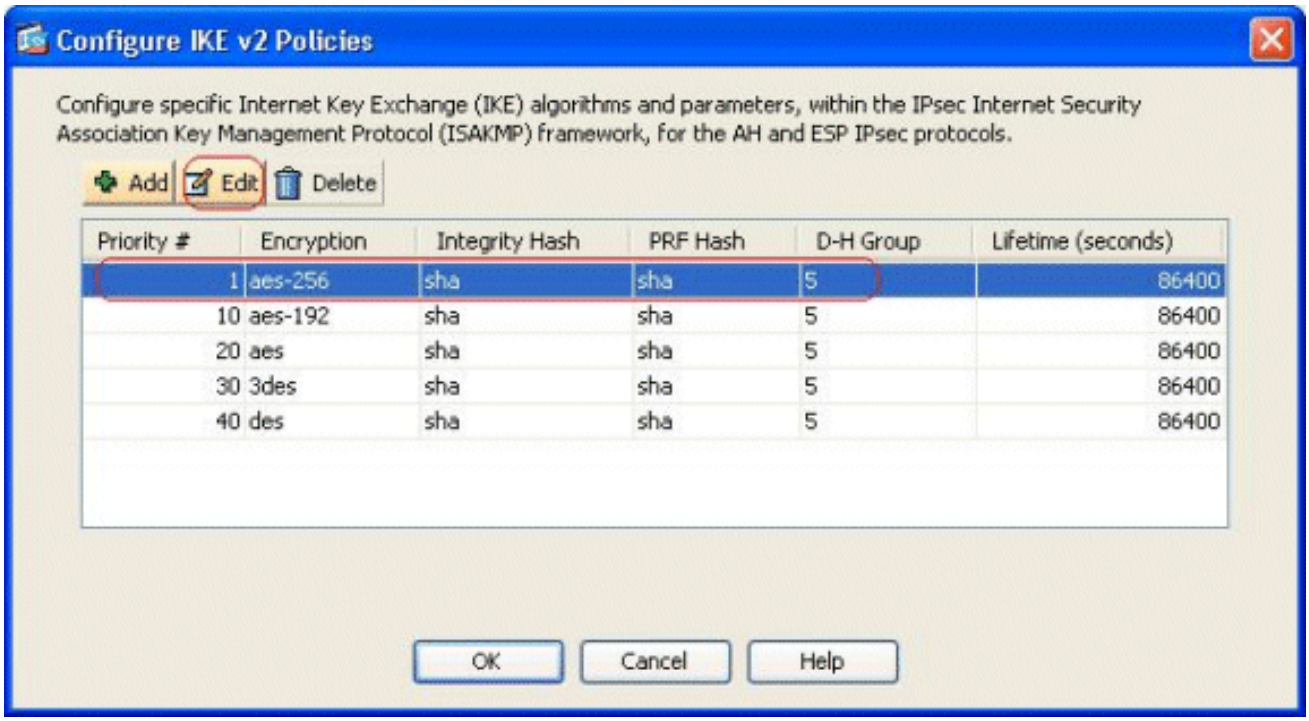
참고: IKEv2의 **IKE 정책**은 IKEv1의 **ISAKMP 정책**과 동일합니다.**IKEv2**의 IPsec 제안서는 IKEv1의 **변형 집합**과 동일합니다.

9. 이 메시지는 기존 정책을 수정하려고 할 때 나타납니다

. 계속하려면 **OK**(확인)를 클릭합니다.

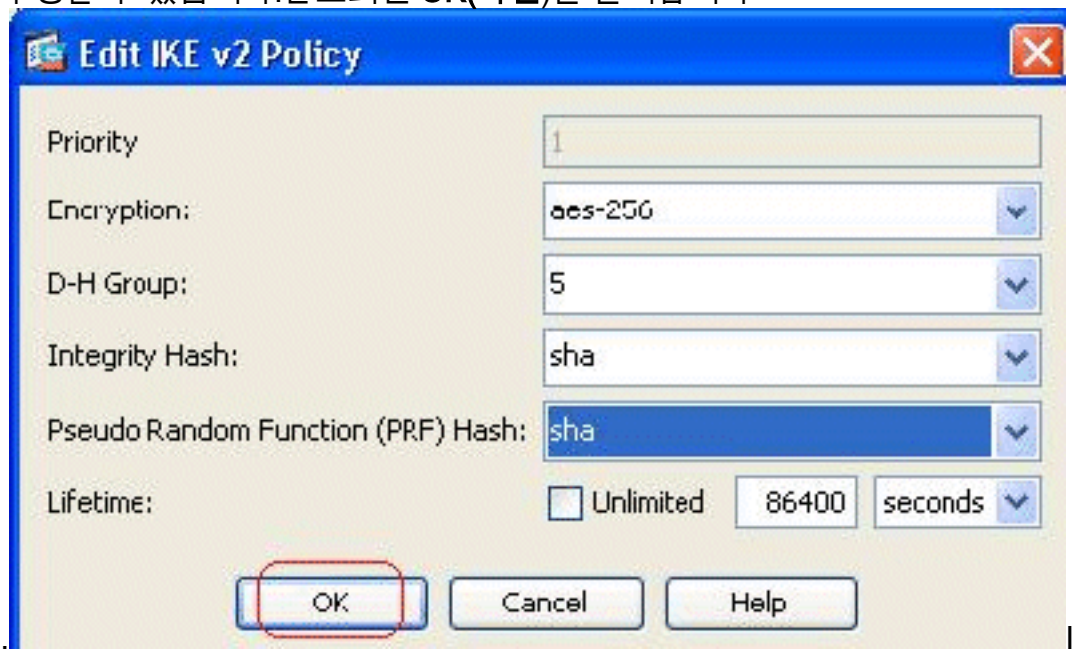
10. 지정된 IKE 정책을 선택하고 Edit를 **클릭합니다**

.



11. Priority, Encryption, D-H Group, Integrity Hash, PRF Hash, Lifetime 값과 같은 매개변수를

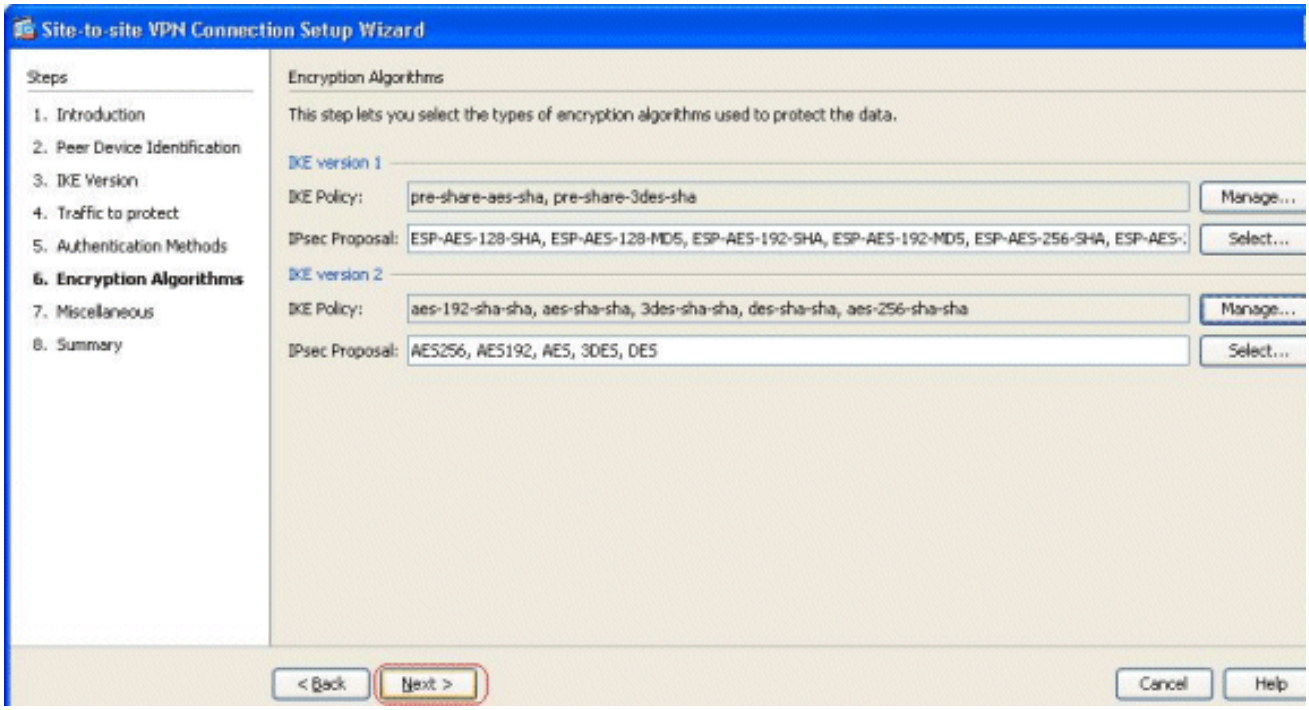
수정할 수 있습니다.완료되면 **OK(확인)**를 클릭합니다



IKEv2에서는 무결성 알고리즘을 PRF(Pseudo Random Function) 알고리즘과 별도로 협상할 수 있습니다.이는 현재 사용 가능한 옵션이 SHA-1 또는 MD5인 IKE 정책에서 구성할 수 있습니다.기본적으로 정의된 IPsec 제안 매개변수는 수정할 수 없습니다.새 매개 변수를 추가하려면 IPsec Proposal 필드 옆에 있는 Select(선택)를 클릭합니다.IKEv1과 IKEv2의 주요 차이점은 IPsec 제안의 관점에서 IKEv1은 암호화 및 인증 알고리즘의 조합 측면에서 변형 집합을 수락한다는 것입니다.IKEv2는 암호화 및 무결성 매개변수를 개별적으로 수락하고, 마지막으로 이러한 모든 OR 조합을 가능하게 합니다.이 마법사의 맨 끝에 있는 요약 슬라이드에서 볼 수 있습니다.

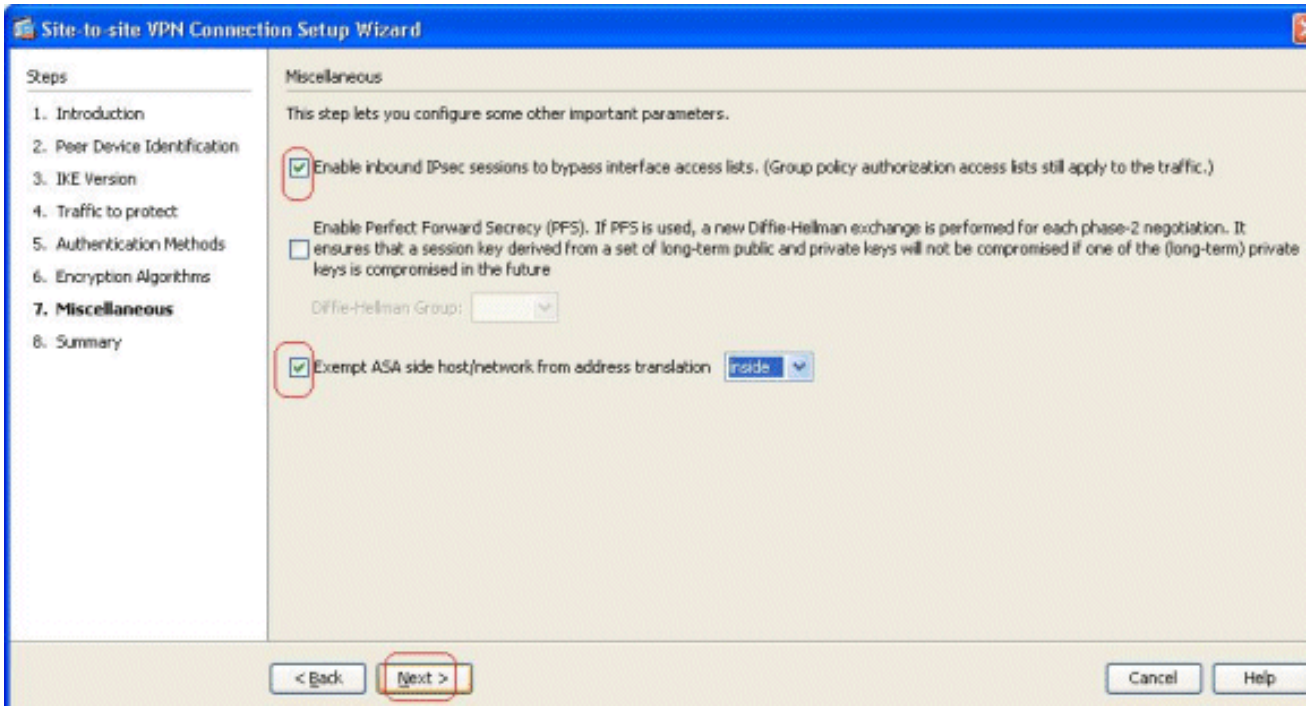
12. Next(**다음)를 클릭합니다**

.



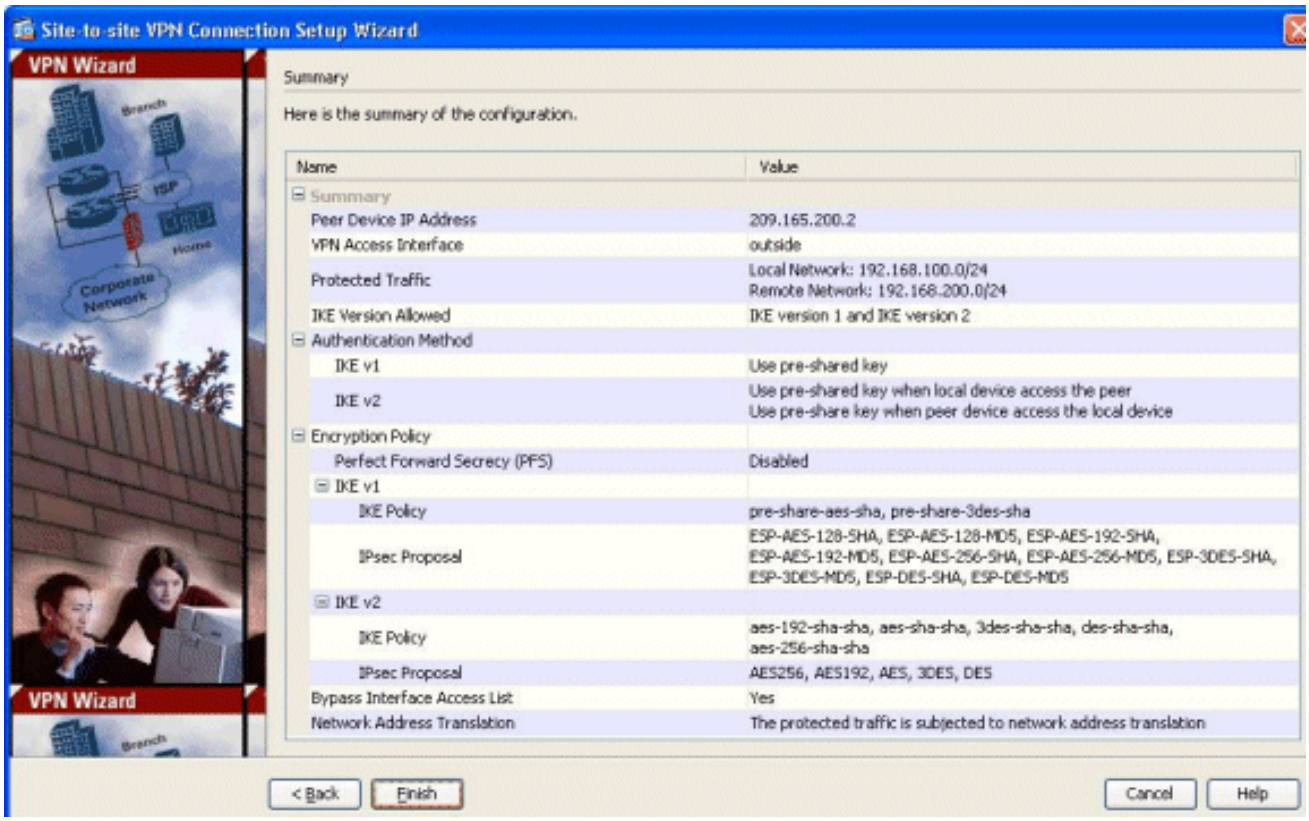
13. NAT 면제, PFS, 인터페이스 ACL 우회 등의 세부 정보를 지정합니다.**다음**을 **선택합니다**

.



14. 컨피그레이션의 요약은 여기에서 확인할 수 있습니다

.



Finish(마침)를 클릭하여 Site-to-Site VPN 터널 마법사를 완료합니다.구성된 매개변수를 사용하여 새 연결 프로파일이 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.

- show crypto ikev2 sa - IKEv2 런타임 SA 데이터베이스를 표시합니다.
- show vpn-sessiondb detail l2l - 사이트 간 VPN 세션에 대한 정보를 표시합니다.

문제 해결

문제 해결 명령

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

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- debug crypto ikev2 - IKEv2에 대한 디버그 메시지를 표시합니다.

관련 정보

- Cisco ASA 5500 Series 어플라이언스 기술 지원
- 기술 지원 및 문서 – Cisco Systems