RV016, RV042, RV042G 및 RV082 VPN Router에서 Mac OS용 Quick VPN Alternative 배포

목표

Mac OS에 적합한 Quick VPN 버전이 없습니다. 그러나 Mac OS용 Quick VPN 대안을 구축하려는 사용자가 늘고 있습니다. 이 문서에서는 IP Security를 Quick VPN의 대안으로 사용합니다.

참고: 구성을 시작하기 전에 MAC OS에 IP 보안을 다운로드하여 설치해야 합니다. 다음 링크에서 다운로드할 수 있습니다.

http://www.lobotomo.com/products/IPSecuritas/

이 문서에서는 Rv016, RV042, RV042G 및 RV082 VPN Router에서 Mac OS용 Quick VPN 대안을 구축하는 방법에 대해 설명합니다.

적용 가능한 디바이스

· RV016
· RV042
· RV042G
· RV082

소프트웨어 버전

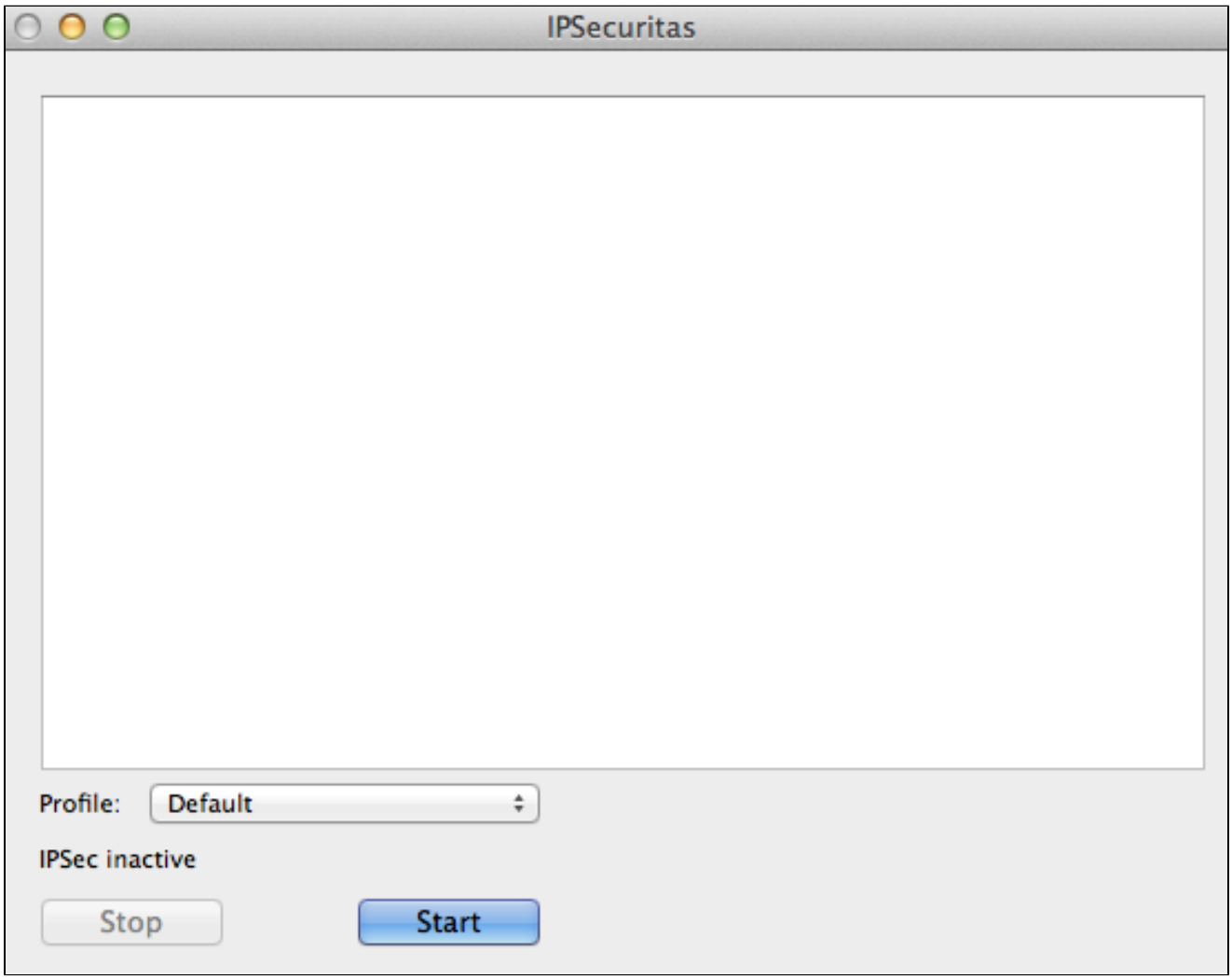
· v4.2.2.08

Mac OS용 Quick VPN 대안 구축

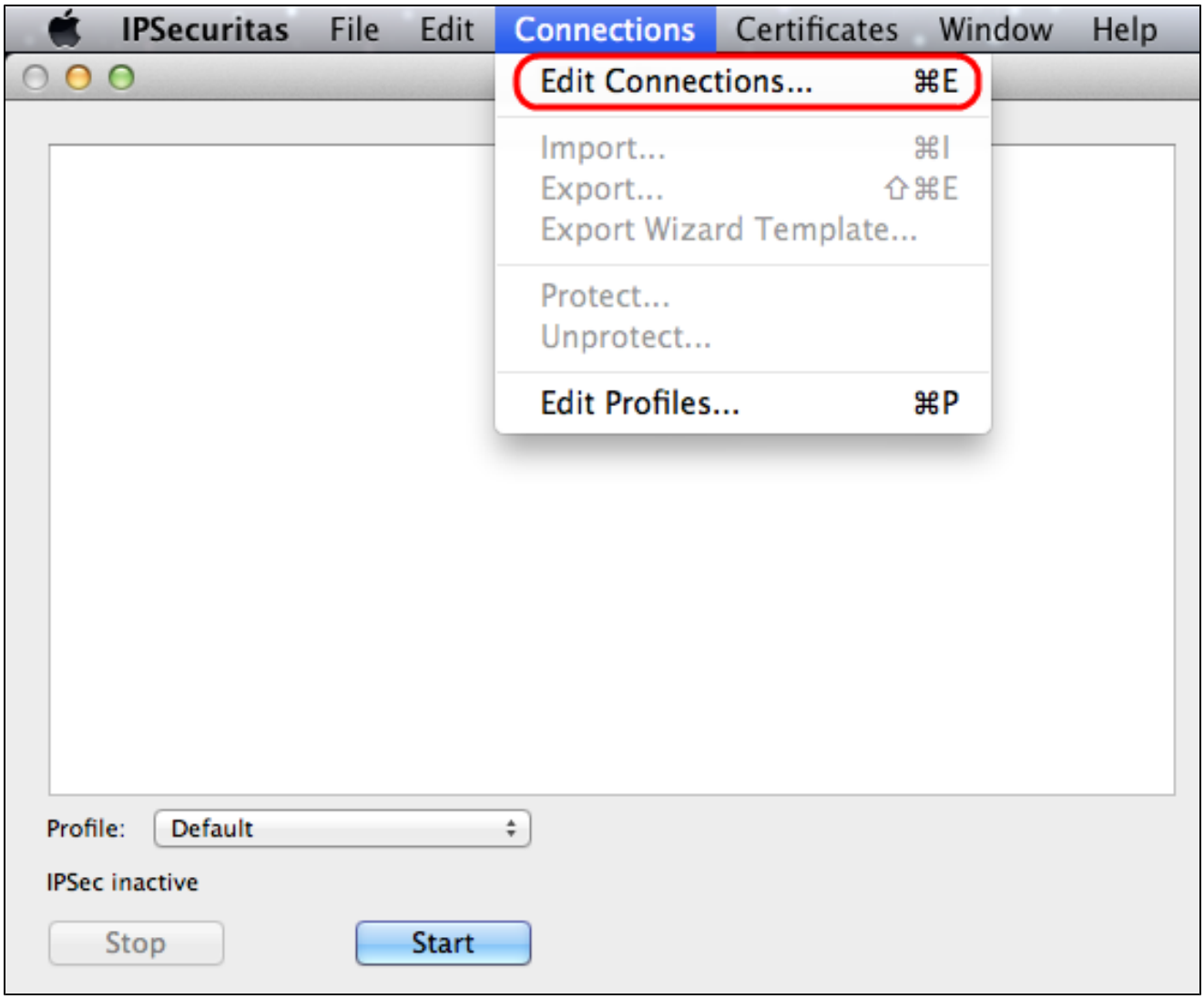
참고: 디바이스의 VPN 클라이언트-게이트웨이 컨피그레이션을 먼저 수행해야 합니다. VPN Client to Gateway를 구성하는 방법에 대한 자세한 내용은 RV016, RV042, RV042G 및 RV082 VPN Router의 VPN 클라이언트에 대한 원격 액세스 터널 설정(Client to Gateway)을

참조하십시오.

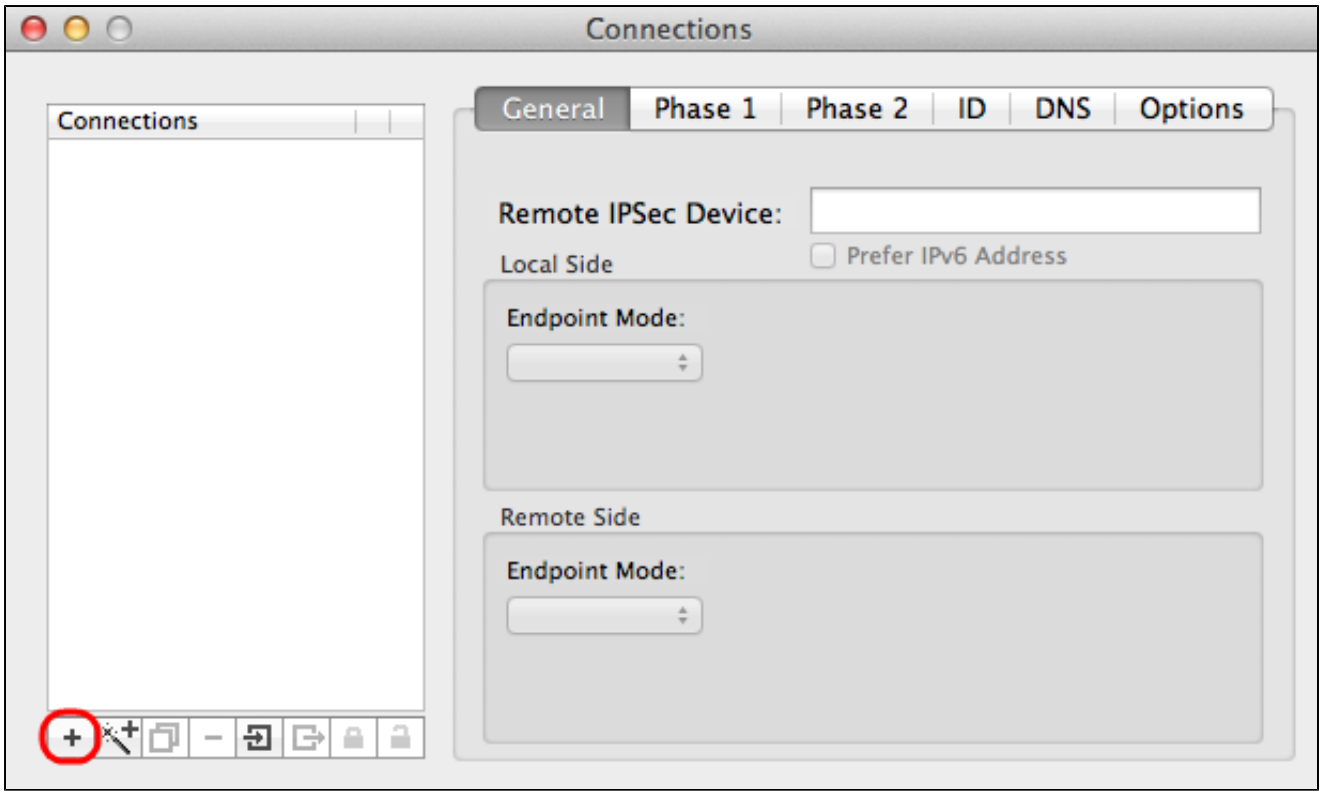
1단계. Mac OS에서 IP Security를 실행합니다. IPSecuritas 창이 나타납니다.



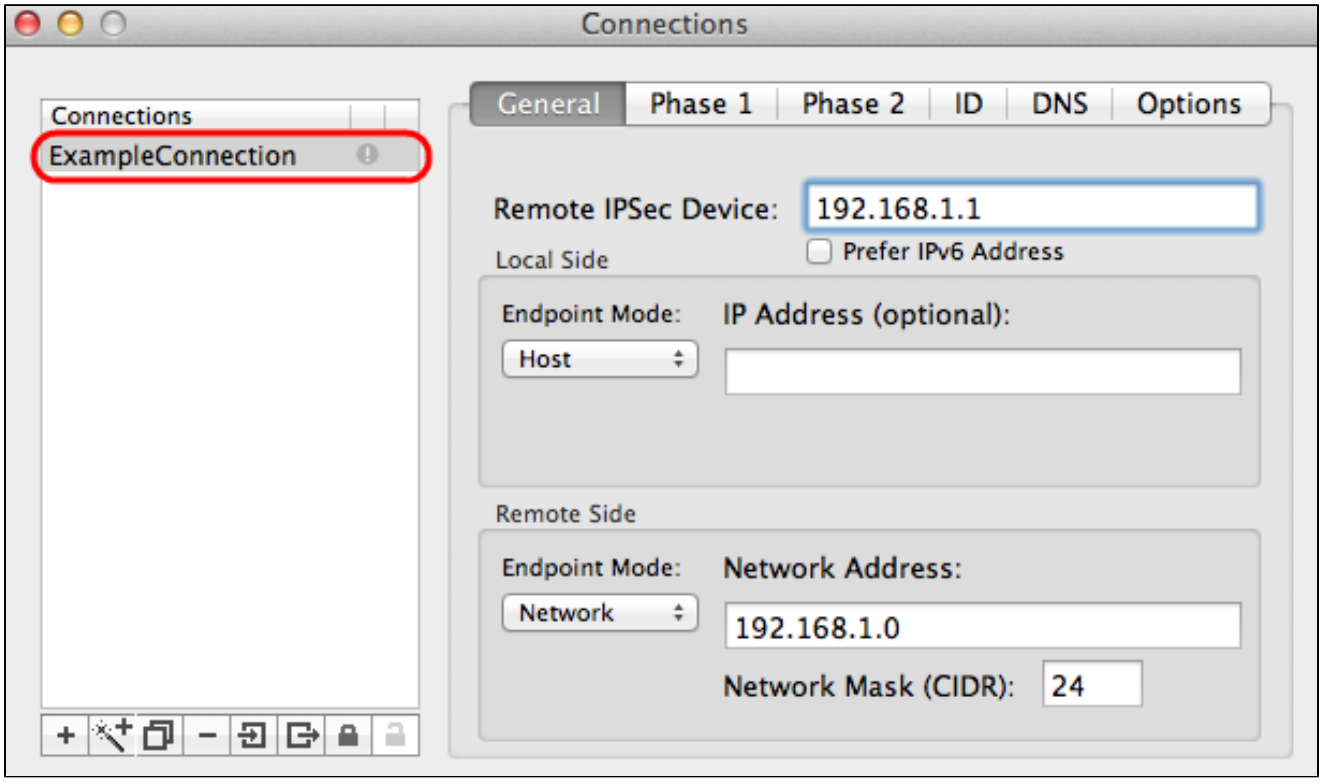
2단계. 시작을 클릭합니다.



3단계. 메뉴 모음에서 Connections(연결) > Edit Connections(연결 수정)를 선택합니다. Connections 창이 나타납니다.

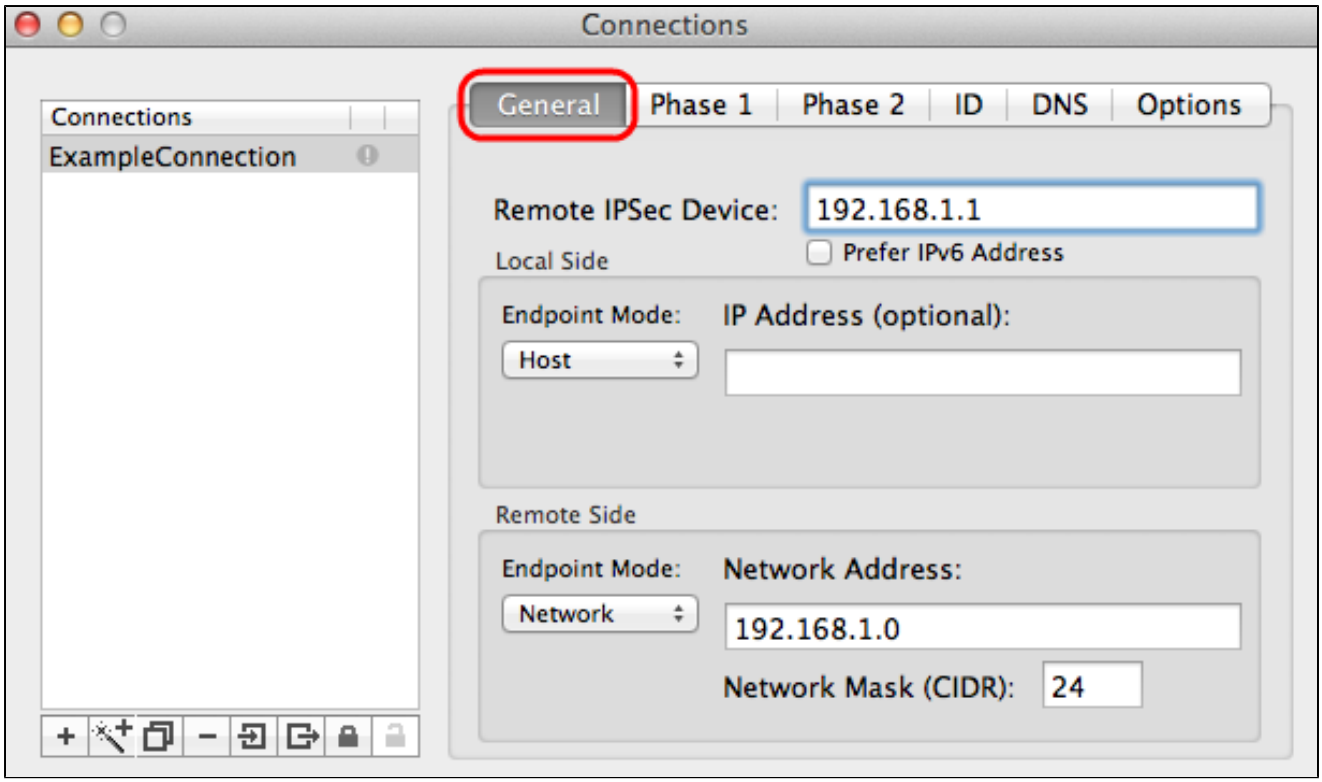


4단계. 새 연결을 추가하려면 + 아이콘을 클릭합니다.



5단계. Connections 아래에 새 연결의 이름을 입력합니다.

일반



1단계. General(일반) 탭을 클릭합니다.

2단계. Remote IPSec Device 필드에 원격 라우터의 IP 주소를 입력합니다.

참고: 이 컨피그레이션은 원격 클라이언트를 위한 것이므로 로컬 측을 구성할 필요가 없습니다. 원격 모드를 구성하기만 하면 됩니다.

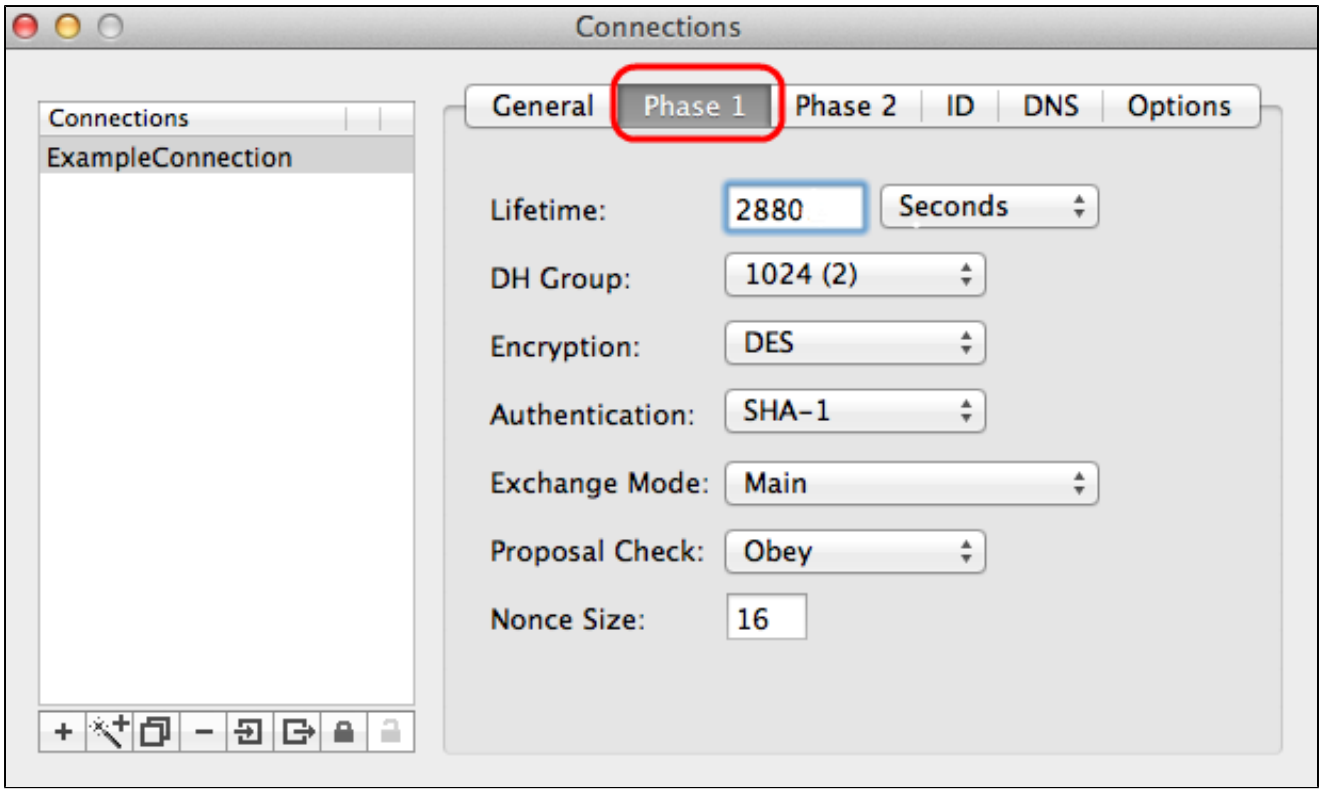
3단계. Remote Side(원격 측) 영역의 Endpoint Mode(엔드포인트 모드) 드롭다운 목록에서 Network(네트워크)를 선택합니다.

4단계. CIDR(네트워크 마스크) 필드에 서브넷 마스크를 입력합니다.

5단계. Network Address 필드에 원격 네트워크 주소를 입력합니다.

1단계

1단계는 안전한 인증 통신을 지원하기 위해 터널의 양단 사이에 있는 간단한 SA(Logical Security Association)입니다.



1단계. 1단계 탭을 클릭합니다.

2단계. 터널 구성 중에 입력한 수명을 Lifetime 필드에 입력합니다. 시간이 만료되면 새 키가 자동으로 재협상됩니다. 키 수명의 범위는 1081~86400초입니다. 1단계의 기본값은 28800초입니다.

3단계. Lifetime 드롭다운 목록에서 Lifetime에 적절한 시간 단위를 선택합니다. 기본값은 초입니다.

4단계. DH Group(DH 그룹) 드롭다운 목록에서 터널 컨피그레이션에 대해 입력한 것과 동일한 DH 그룹을 선택합니다. DH(Diffie-Hellman) 그룹은 키 교환에 사용됩니다.

5단계. 터널 컨피그레이션에 대해 입력한 암호화 드롭다운 목록에서 암호화 유형을 선택합니다. Encryption 메서드는 ESP(Encapsulating Security Payload) 패킷을 암호화/해독하는 데 사용되는 키의 길이를 결정합니다.

6단계. Authentication 드롭다운 목록에서 터널 컨피그레이션에 대해 입력한 인증 방법을 선택합니다. 인증 유형에 따라 ESP 패킷을 인증하는 방법이 결정됩니다.

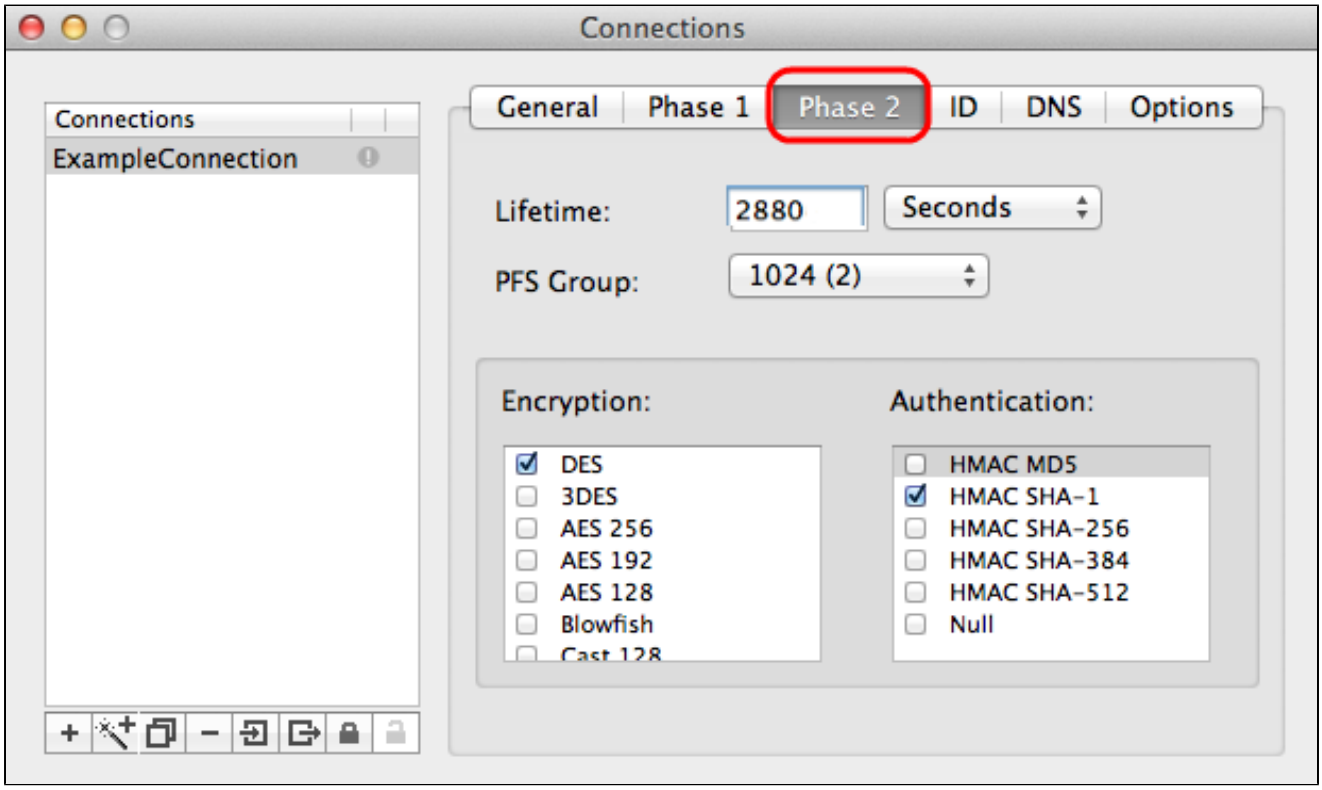
7단계. Exchange Mode(교환 모드) 드롭다운 목록에서 적절한 교환 모드를 선택합니다.

· Main — FQDN(Full Qualified Domain Name)을 제외한 모든 게이트웨이 유형의 교환 모드를 나타냅니다.

· Aggressive — FQDN(Full Qualified Domain Name) 게이트웨이의 교환 모드를 나타냅니다.

2단계

2단계는 데이터 패킷이 두 엔드포인트를 통과하는 동안 데이터 패킷의 보안을 결정하는 보안 연계입니다.



1단계. 2단계 탭을 클릭합니다.

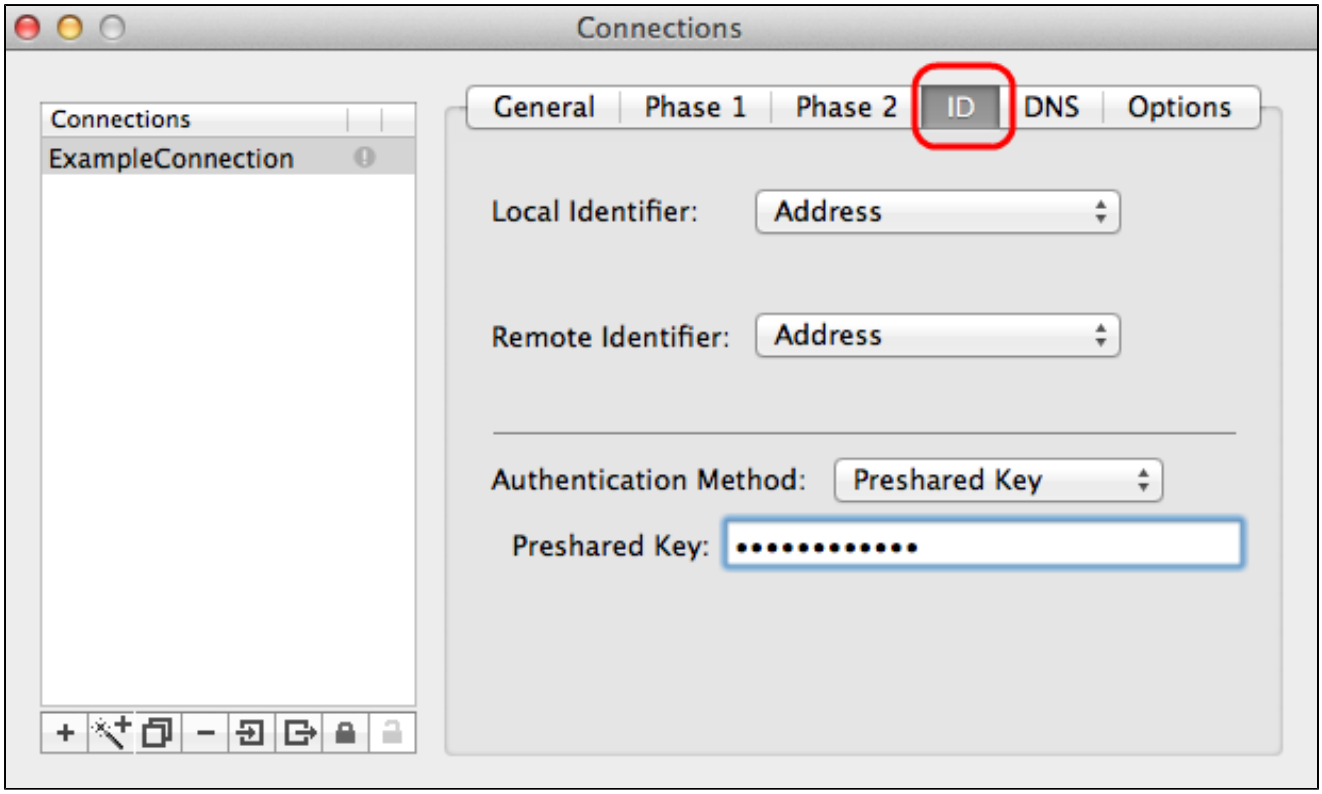
2단계. 터널 컨피그레이션에 대해 입력한 수명 필드와 1단계에도 동일한 수명을 입력합니다.

3단계. 터널 및 1단계 컨피그레이션에 대해 입력한 수명 드롭다운 목록에서 수명의 동일한 시간 단위를 선택합니다.

4단계. 터널 컨피그레이션을 위해 입력한 PFS(Perfect Forwarding Secrecy) Group(PFS(Perfect Forwarding Secrecy) 그룹) 드롭다운 목록에서 동일한 DH 그룹을 선택합니다.

5단계. 사용하지 않는 모든 암호화 및 인증 방법을 선택 취소합니다. 1단계 탭에 정의된 것만 확인합니다.

ID



1단계. ID 탭을 클릭합니다.

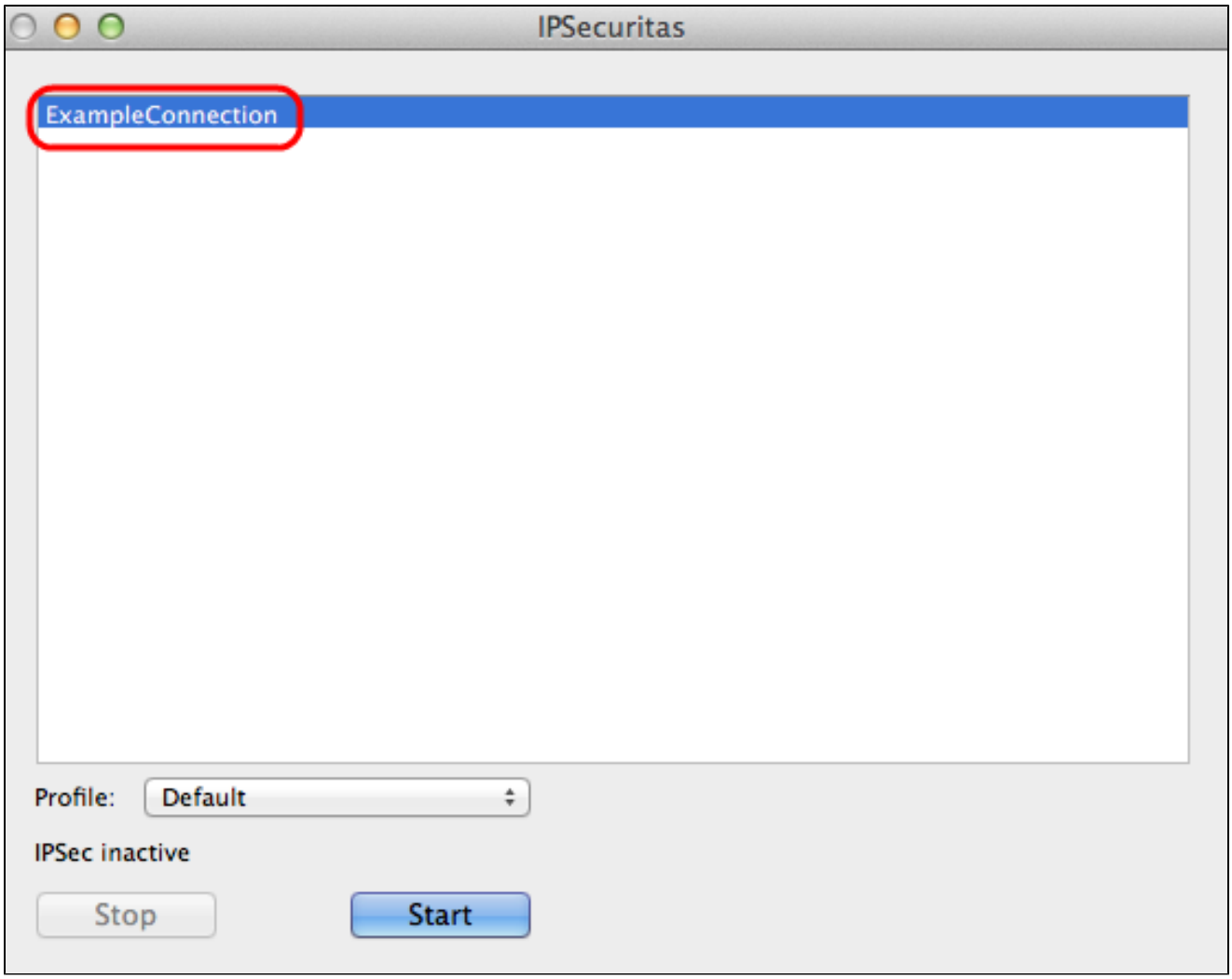
2단계. Local Identifier 드롭다운 목록에서 터널과 동일한 로컬 식별자 방법을 선택합니다. 필요한 경우 로컬 식별자 유형에 따라 적절한 값을 입력합니다.

3단계. Remote Identifier(원격 식별자) 드롭다운 목록에서 터널과 동일한 원격 식별자 방법을 선택합니다. 필요한 경우 원격 식별자 유형에 따라 적절한 값을 입력합니다.

4단계. Authentication Method 드롭다운 목록에서 터널과 동일한 인증 방법을 선택합니다. 필요한 경우 인증 방법 유형에 따라 적절한 인증 값을 입력합니다.

5단계. x 아이콘(빨간색 원)을 클릭하여 연결 창을 닫습니다. 그러면 설정이 자동으로 저장됩니다. IPSecuritas 창이 나타납니다.

연결



1단계. IPSecuritas 창에서 Start(시작)를 클릭합니다. 그런 다음 사용자는 VPN에 액세스하기 위해 연결됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.