Windows를 통한 RV042, RV042G 및 RV082 VPN 라우터에서 Shrew VPN 클라이언트 구성

목표

VPN(Virtual Private Network)은 원격 사용자가 인터넷을 통해 사설 네트워크에 가상으로 연결하는 방법입니다. 클라이언트-게이트웨이 VPN은 VPN 클라이언트 소프트웨어를 사용하여 사용자의 데스크톱 또는 랩톱을 원격 네트워크에 연결합니다. 클라이언트-게이트웨이 VPN 연결은 사무실 네트워크에 원격으로 안전하게 연결하려는 원격 직원에게 유용합니다. Shrew VPN 클라이언트는 쉽고 안전한 VPN 연결을 제공하는 원격 호스트 장치에 구성된 소프트웨어입니다.

이 문서의 목적은 RV042, RV042G 또는 RV082 VPN Router에 연결하는 컴퓨터에 대해 Shrew VPN Client를 구성하는 방법을 설명하는 것입니다.

참고: 이 문서에서는 Windows 컴퓨터에서 Shrew VPN 클라이언트를 이미 다운로드한 것으로 가정합니다. 그렇지 않으면 Shrew VPN 구성을 시작하기 전에 클라이언트-게이트웨이 VPN 연결을 구성해야 합니다. 클라이언트-게이트웨이 VPN을 구성하는 방법에 대한 자세한 내용은 RV042, RV042G 및 RV082 VPN 라우터에서 VPN 클라이언트에 대한 원격 액세스 터널 설정(클라이언트-게이트웨이)을 참조하십시오.

적용 가능한 디바이스

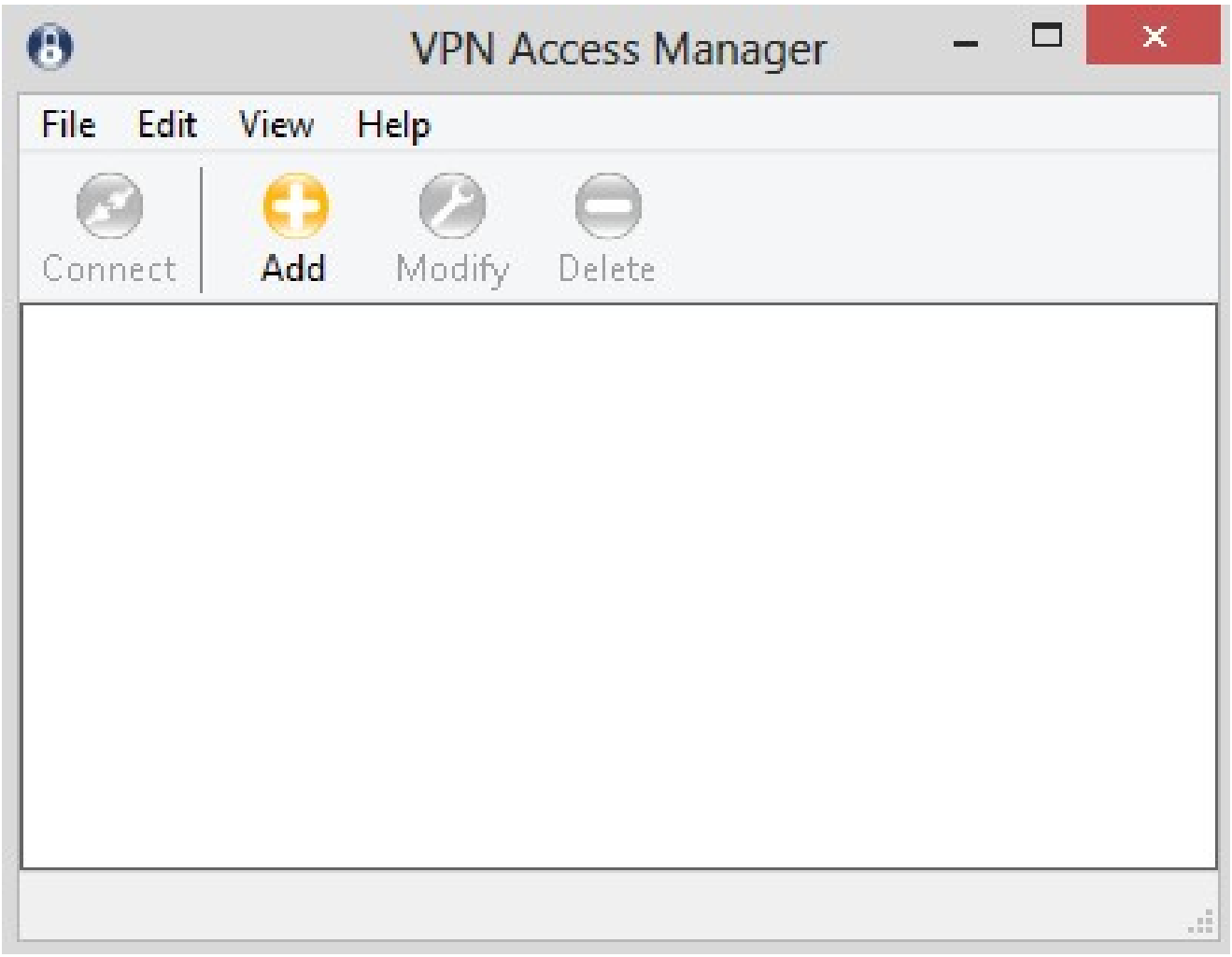
· RV042
· RV042G
· RV082

소프트웨어 버전

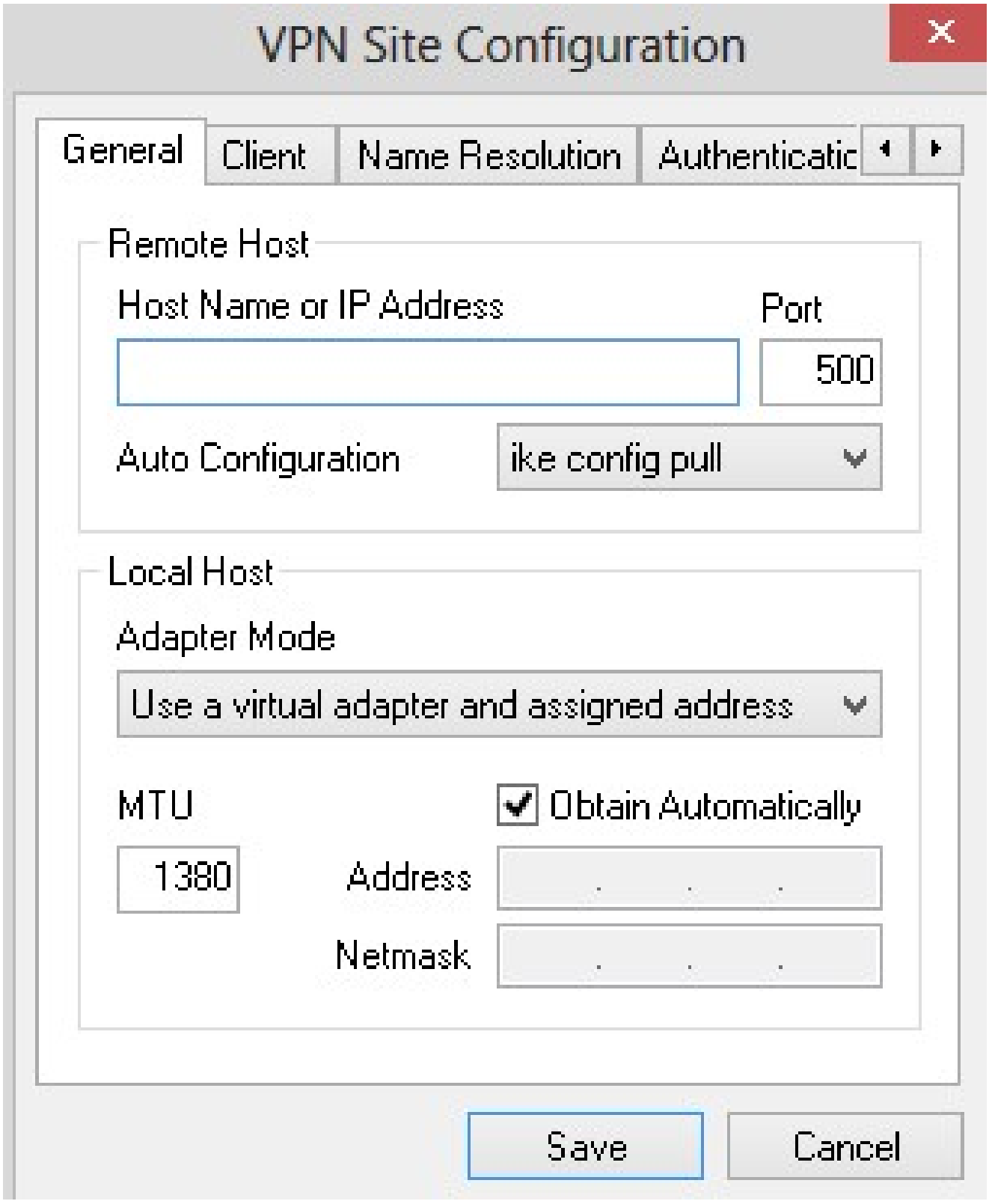
· v4.2.2.08

Windows에서 Shrew VPN 클라이언트 연결 구성

1단계. 컴퓨터에서 Shrew VPN 클라이언트 프로그램을 클릭하고 엽니다. Shrew Soft VPN Access Manager 창이 열립니다.

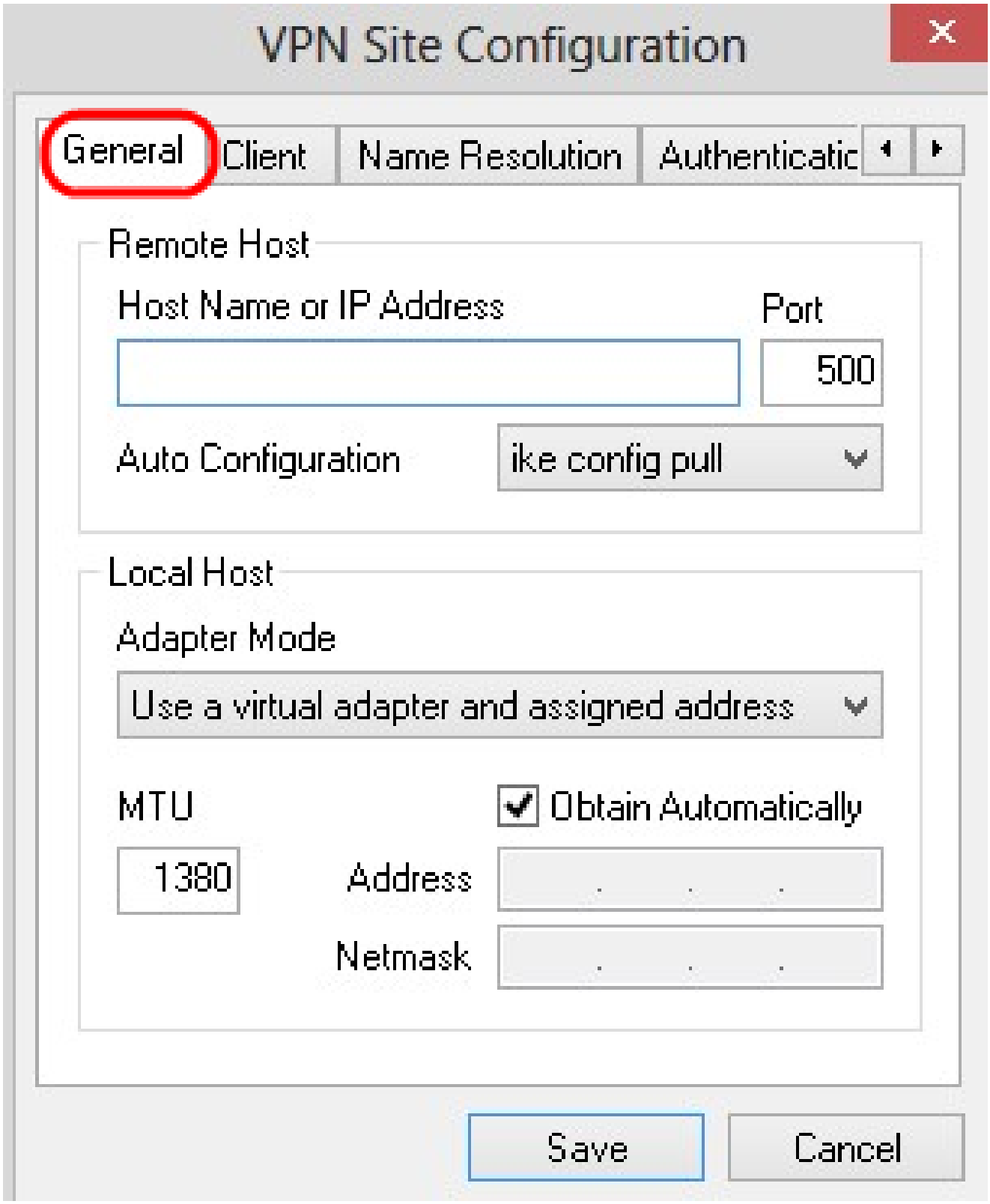


2단계. Add(추가)를 클릭합니다. VPN Site Configuration(VPN 사이트 컨피그레이션) 창이 나타납니다.



일반 컨피그레이션

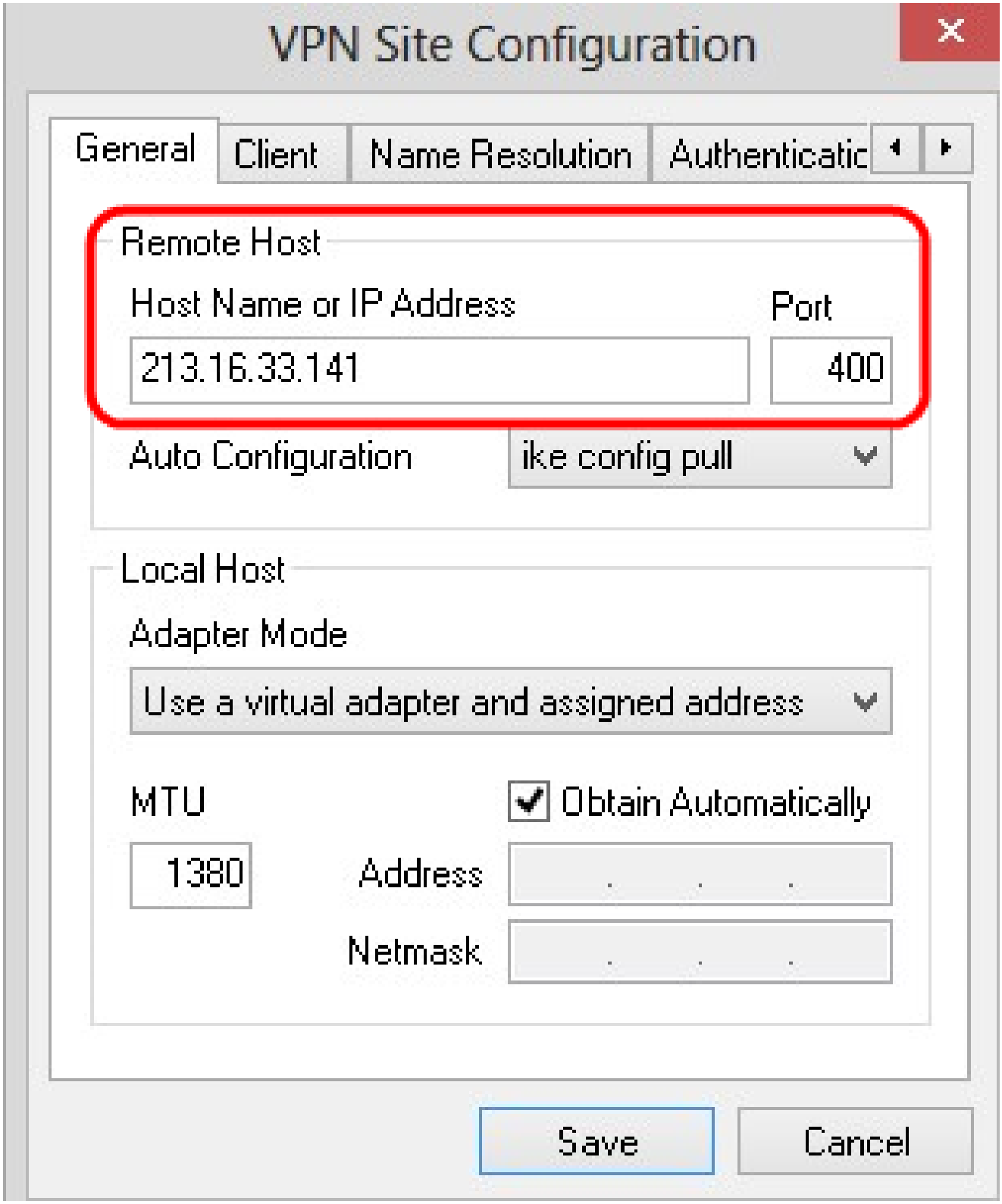
1단계. General(일반) 탭을 클릭합니다.



참고: General(일반) 섹션은 원격 및 로컬 호스트 IP 주소를 구성하는 데 사용됩니다. 이러한 매개변수는 클라이언트-게이트웨이 연결의 네트워크 매개변수를 정의하는 데 사용됩니다.

2단계. Host Name or IP Address 필드에 구성된 WAN의 IP 주소인 원격 호스트 IP 주소를 입력합니다.

3단계. 연결에 사용되는 포트의 번호를 Port 필드에 입력합니다. 그림에 표시된 예에서 사용되는 포트 번호는 400입니다.



4단계. Auto Configuration 드롭다운 목록에서 원하는 컨피그레이션을 선택합니다.

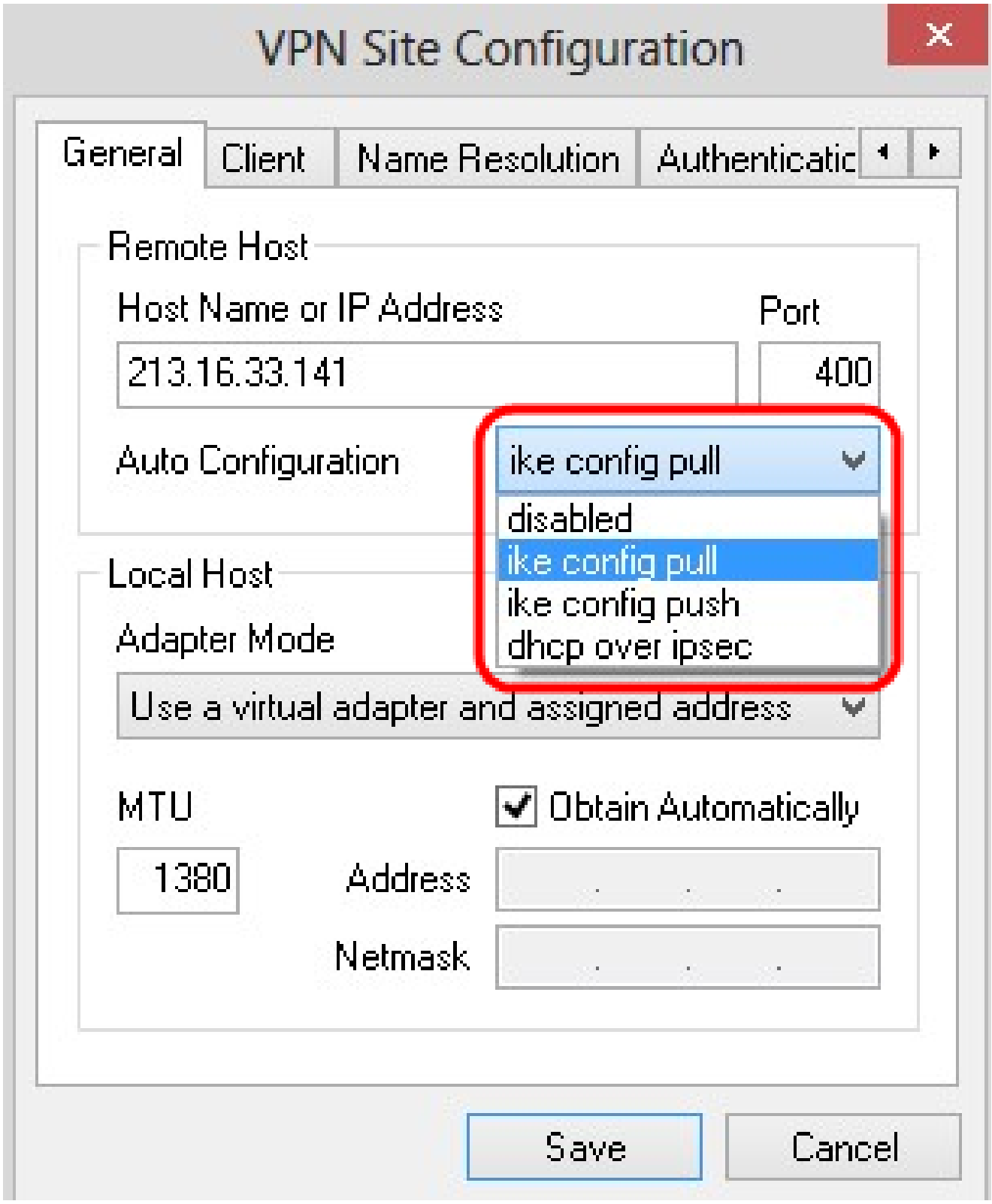
· Disabled(비활성화됨) — disabled 옵션은 모든 자동 클라이언트 컨피그레이션을 비활성화

합니다.

· IKE Config Pull — 클라이언트에서 컴퓨터의 요청을 설정할 수 있습니다. 컴퓨터에서 Pull 메서드를 지원하면 클라이언트에서 지원하는 설정 목록이 반환됩니다.

· IKE Config Push — 컴퓨터에 컨피그레이션 프로세스를 통해 클라이언트에 설정을 제공할 수 있는 기회를 제공합니다. 컴퓨터에서 Push 메서드를 지원하면 클라이언트에서 지원하는 설정 목록이 반환됩니다.

· DHCP Over IPSec — 클라이언트에서 DHCP over IPSec을 통해 컴퓨터의 설정을 요청할 수 있습니다.

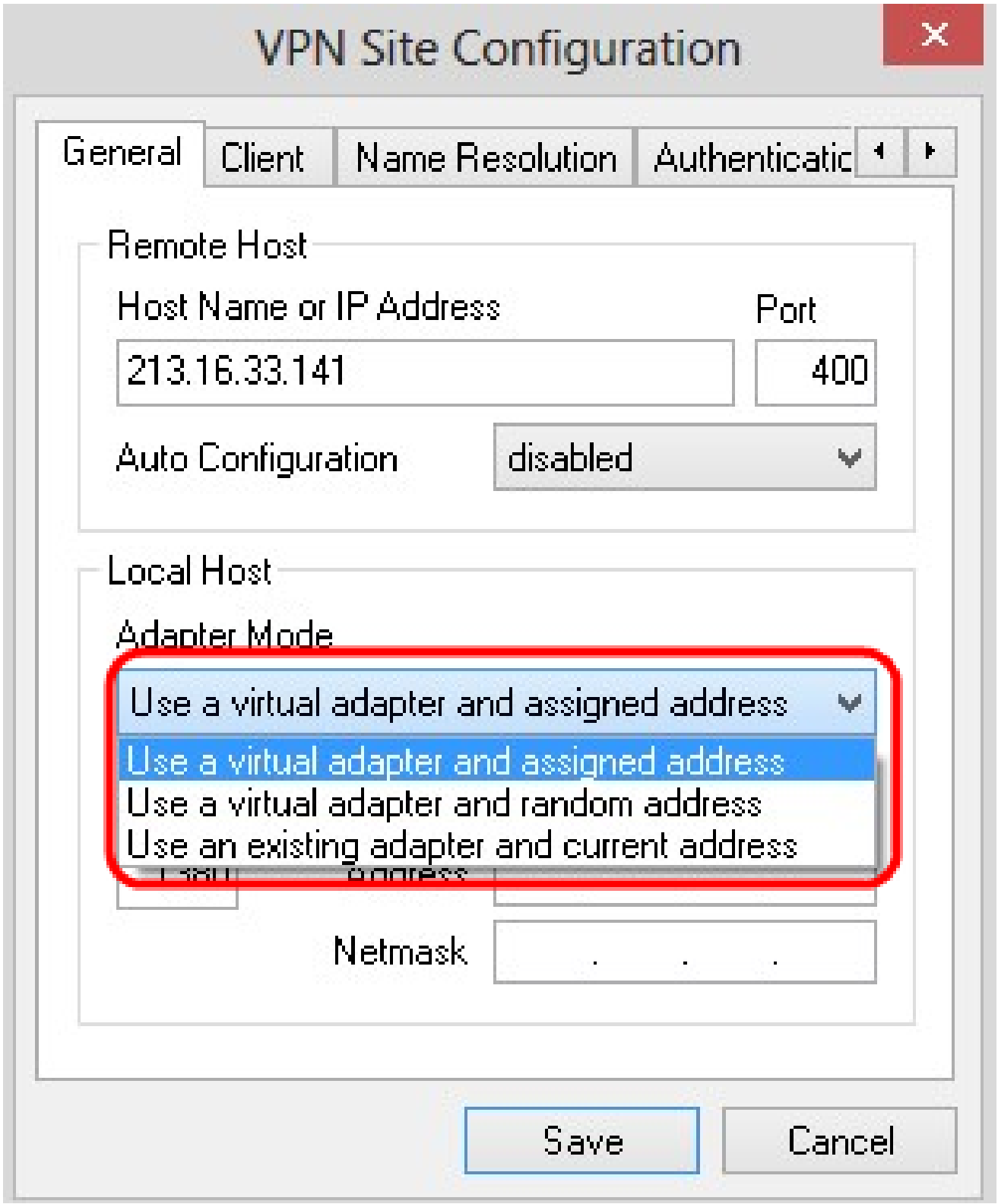


5단계. Adapter Mode 드롭다운 목록에서 Auto Configuration에 따라 로컬 호스트에 대해 원하는 어댑터 모드를 선택합니다.

· Use a Virtual Adapter and Assigned Address — 클라이언트가 지정된 주소의 가상 어댑터를 사용할 수 있도록 허용합니다.

· Use a Virtual Adapter and Random Address — 클라이언트가 임의의 주소로 가상 어댑터를 사용할 수 있도록 허용합니다.

· Use an Existing Adapter and Current Address — 기존 어댑터와 해당 주소를 사용합니다. 추가 정보를 입력할 필요가 없습니다.

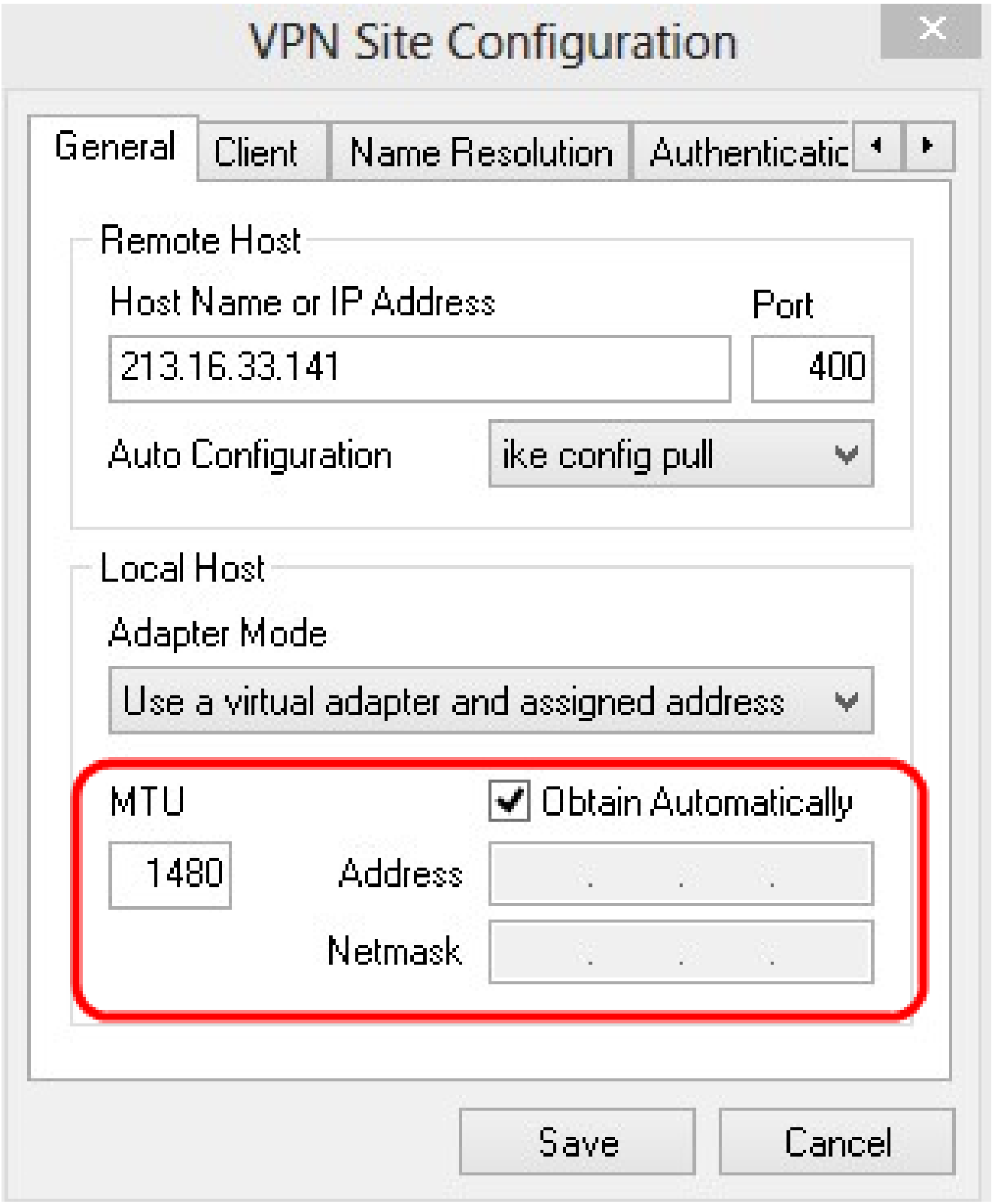


6단계. 5단계의 Adapter Mode(어댑터 모드) 드롭다운 목록에서 Use a Virtual Adapter and Assigned Address(가상 어댑터 및 할당된 주소 사용)를 선택한 경우 MTU 필드에 MTU(최대 전송 단위)를 입력합니다. 최대 전송 단위는 IP 프래그먼트화 문제를 해결하는 데 도움이 됩니다. 기본값은 1380입니다.

7단계(선택 사항) DHCP 서버를 통해 주소 및 서브넷 마스크를 자동으로 가져오려면 Obtain Automatically(자동으로 가져오기) 확인란을 선택합니다. 이 옵션은 일부 컨피그레이션에서는 사용할 수 없습니다.

8단계. 5단계의 Adapter Mode(어댑터 모드) 드롭다운 목록에서 Use a Virtual Adapter and Assigned Address(가상 어댑터 사용 및 할당된 주소)를 선택한 경우 Address(주소) 필드에 원격 클라이언트의 IP 주소를 입력합니다.

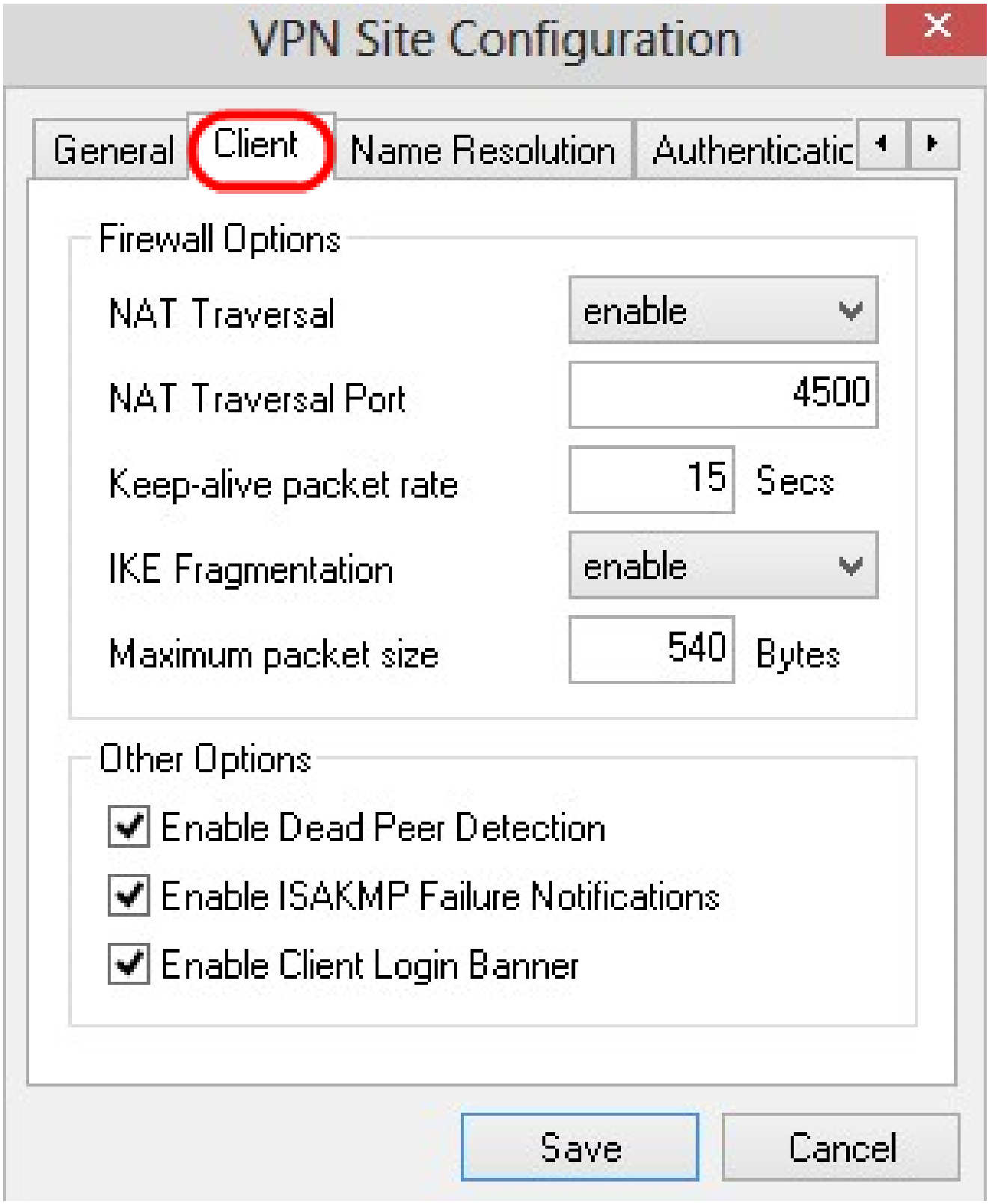
9단계. 5단계의 Adapter Mode(어댑터 모드) 드롭다운 목록에서 Use a Virtual Adapter and Assigned Address(가상 어댑터 사용 및 할당된 주소)를 선택한 경우 Netmask(넷마스크) 필드에 원격 클라이언트 IP 주소의 서브넷 마스크를 입력합니다.



10단계. Save(저장)를 클릭하여 설정을 저장합니다.

클라이언트 컨피그레이션

1단계. Client(클라이언트) 탭을 클릭합니다.



참고: Client(클라이언트) 섹션에서 방화벽 옵션, Dead Peer Detection(데드 피어 탐지) 및 ISAKMP(Internet Security Association and Key Management Protocol) Failure Notifications(ISAKMP(Internet Security Association and Key Management Protocol) 실패 알림을 구성할 수 있습니다. 이 설정은 수동으로 구성하고 자동으로 가져오는 컨피그레이션 옵션을 정의합니다.

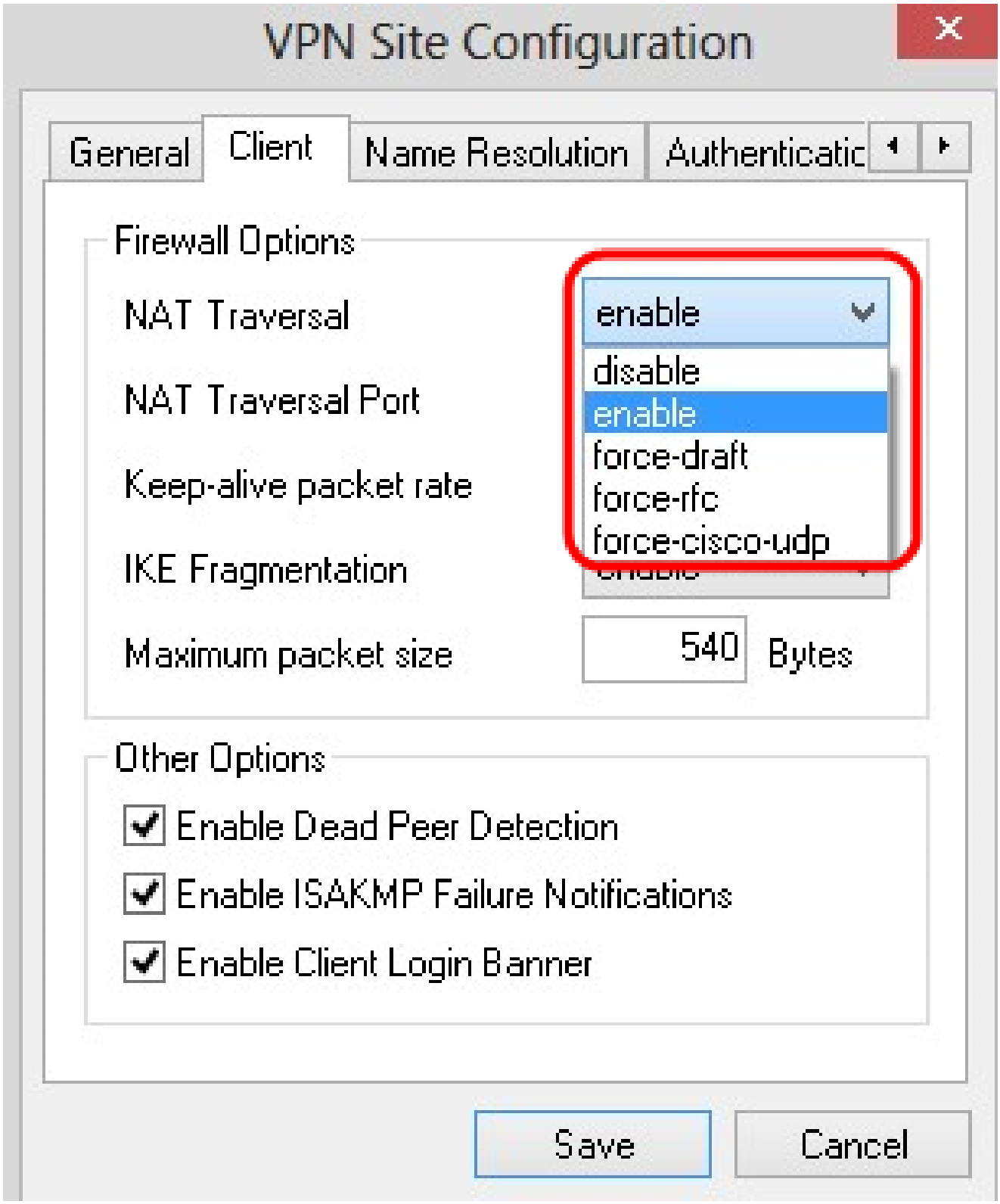
2단계. NAT Traversal 드롭다운 목록에서 적절한 NAT(Network Address Translation) traversal 옵션을 선택합니다.

· Disable — NAT 프로토콜이 비활성화됩니다.

· Enable — IKE 프래그먼트화는 게이트웨이가 협상을 통해 지원을 나타내는 경우에만 사용됩니다.

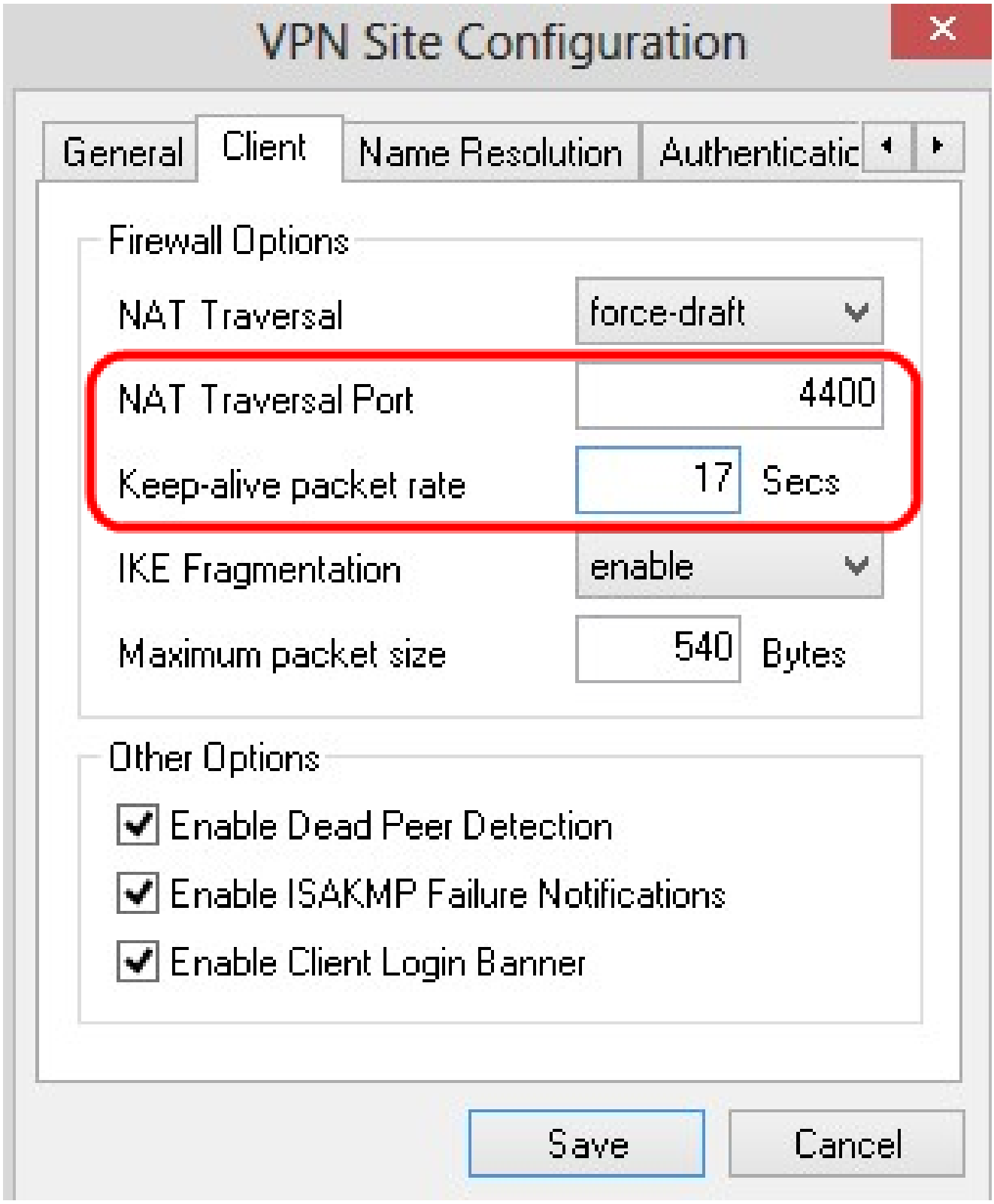
· Force Draft — NAT 프로토콜의 초안 버전입니다. 게이트웨이가 협상 또는 NAT 탐지를 통해 지원을 나타내는 경우에 사용됩니다.

· Force RFC — NAT 프로토콜의 RFC 버전입니다. 게이트웨이가 협상 또는 NAT 탐지를 통해 지원을 나타내는 경우에 사용됩니다.



3단계. NAT Traversal Port 필드에 NAT의 UDP 포트를 입력합니다. 기본값은 4500입니다.

4단계. Keep-alive packet rate 필드에 전송되는 keep-alive 패킷의 속도 값을 입력합니다. 값은 초 단위로 측정됩니다. 기본값은 30초입니다.

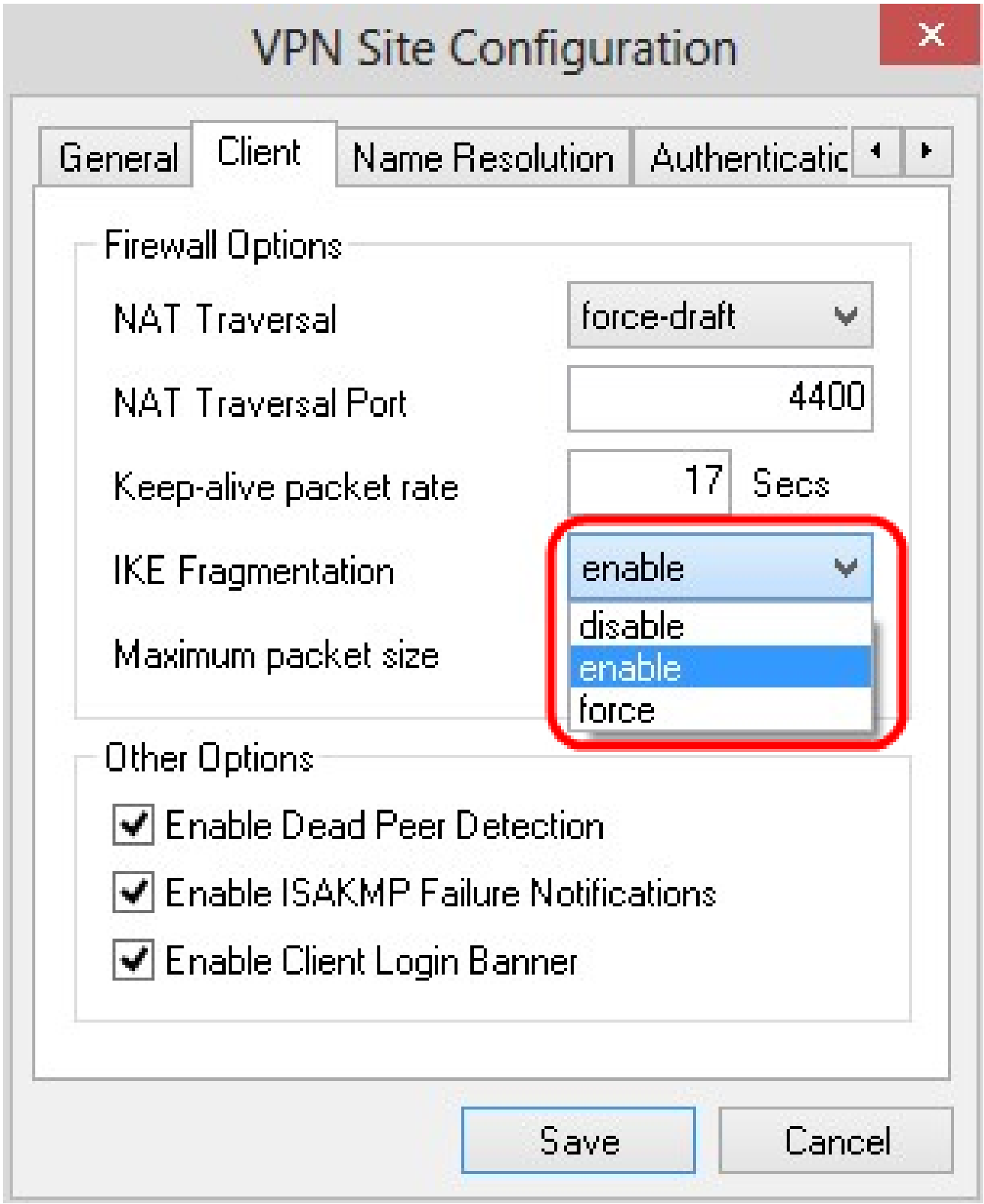


5단계. IKE Fragmentation(IKE 단편화) 드롭다운 목록에서 적절한 옵션을 선택합니다.

· Disable — IKE 프래그먼트화가 사용되지 않습니다.

· Enable — IKE 프래그먼트화는 게이트웨이가 협상을 통해 지원을 나타내는 경우에만 사용됩니다.

· Force — IKE 조각화는 표시나 탐지에 관계없이 사용됩니다.

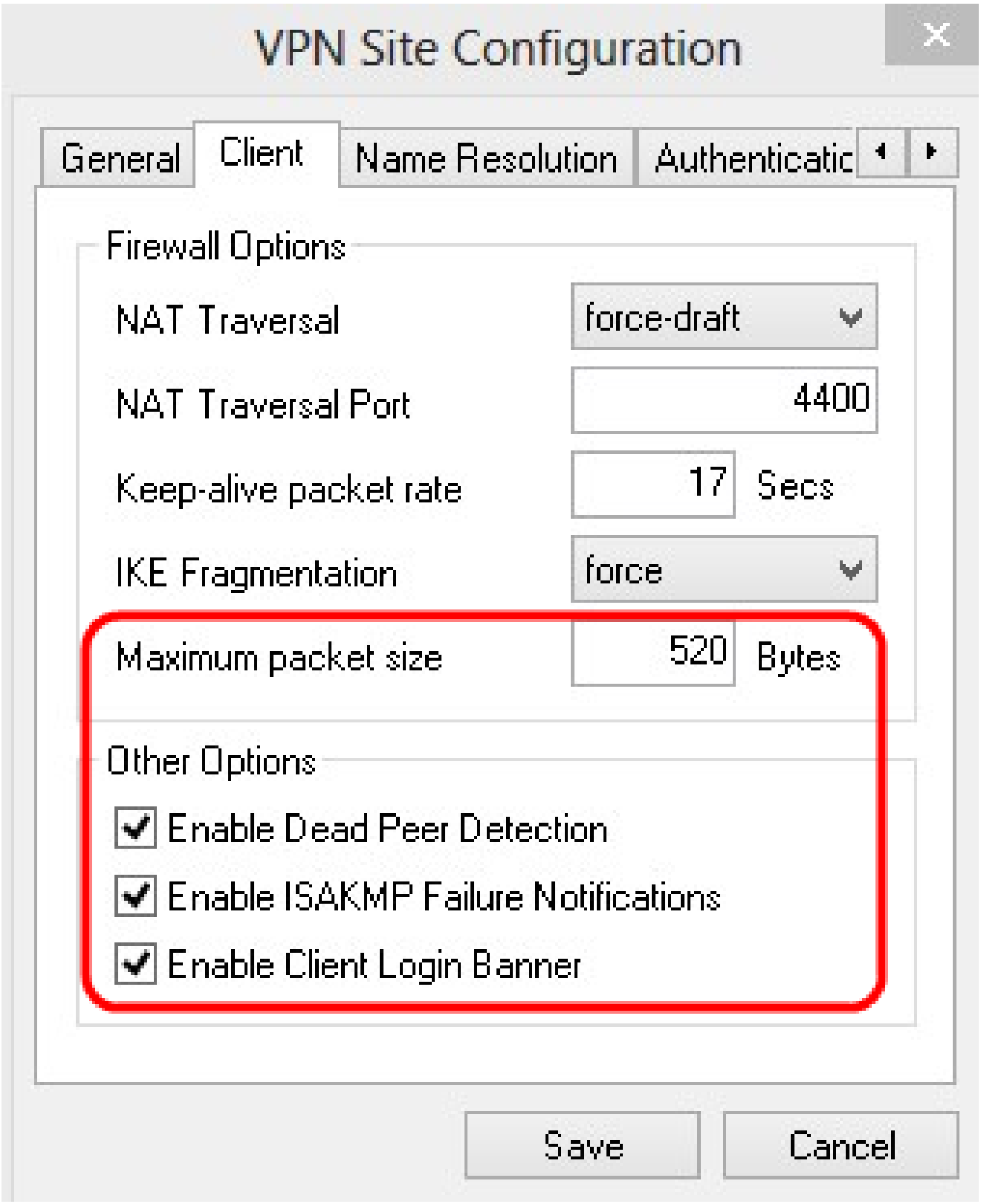


6단계. Maximum packet size(최대 패킷 크기) 필드에 최대 패킷 크기를 Bytes(바이트)로 입력합니다. 패킷 크기가 최대 패킷 크기보다 큰 경우 IKE 단편화가 수행됩니다. 기본값은 540바이트입니다.

7단계. (선택 사항) 다른 시스템이 더 이상 응답할 수 없는 경우 컴퓨터와 클라이언트가 이를 탐지하도록 허용하려면 Enable Dead Peer Detection 확인란을 선택합니다.

8단계. (선택 사항) VPN 클라이언트에서 장애 알림을 보내려면 Enable ISAKMP Failure Notifications(ISAKMP 장애 알림 활성화) 확인란을 선택합니다.

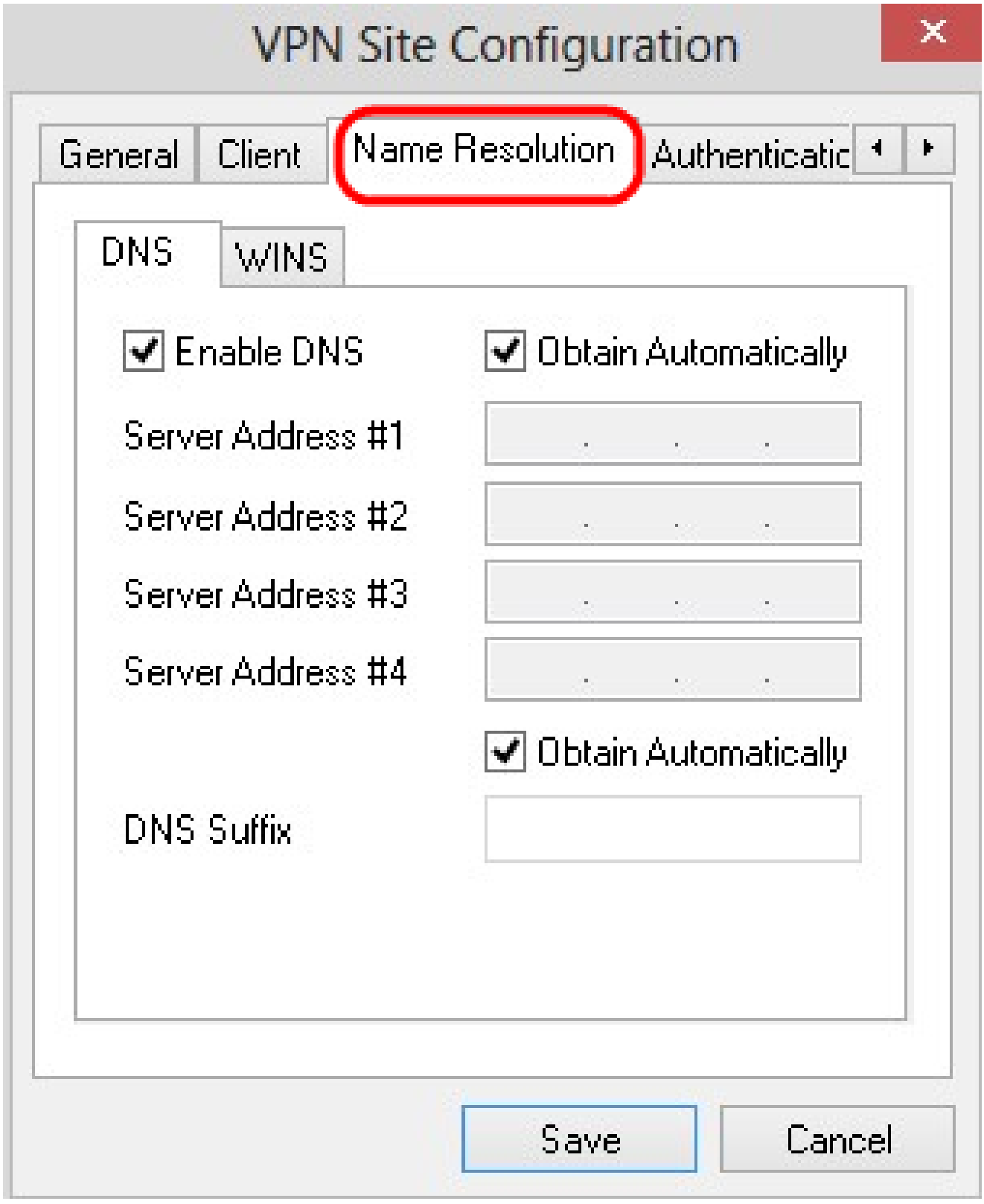
9단계(선택 사항) 게이트웨이와 연결이 설정된 경우 클라이언트에서 로그인 배너를 표시하려면 Enable Client Login(클라이언트 로그인 활성화) 확인란을 선택합니다.



10단계. Save(저장)를 클릭하여 설정을 저장합니다.

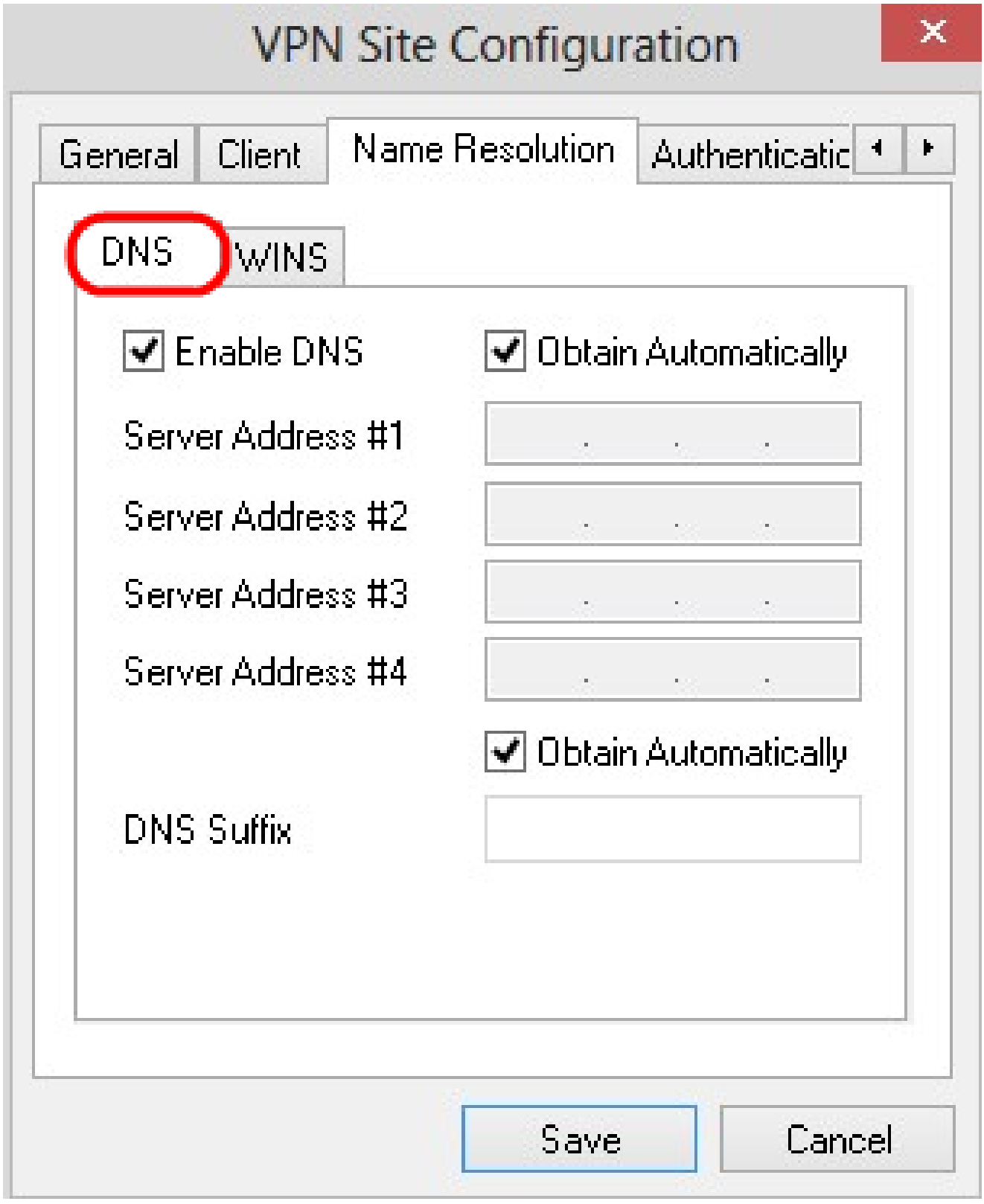
이름 확인 구성

1단계. 이름 확인 탭을 클릭합니다.



참고: Name Resolution(이름 확인) 섹션은 DNS(Domain Name System) 및 WIN(Windows Internet Name Service) 설정을 구성하는 데 사용됩니다.

2단계. DNS 탭을 클릭합니다.

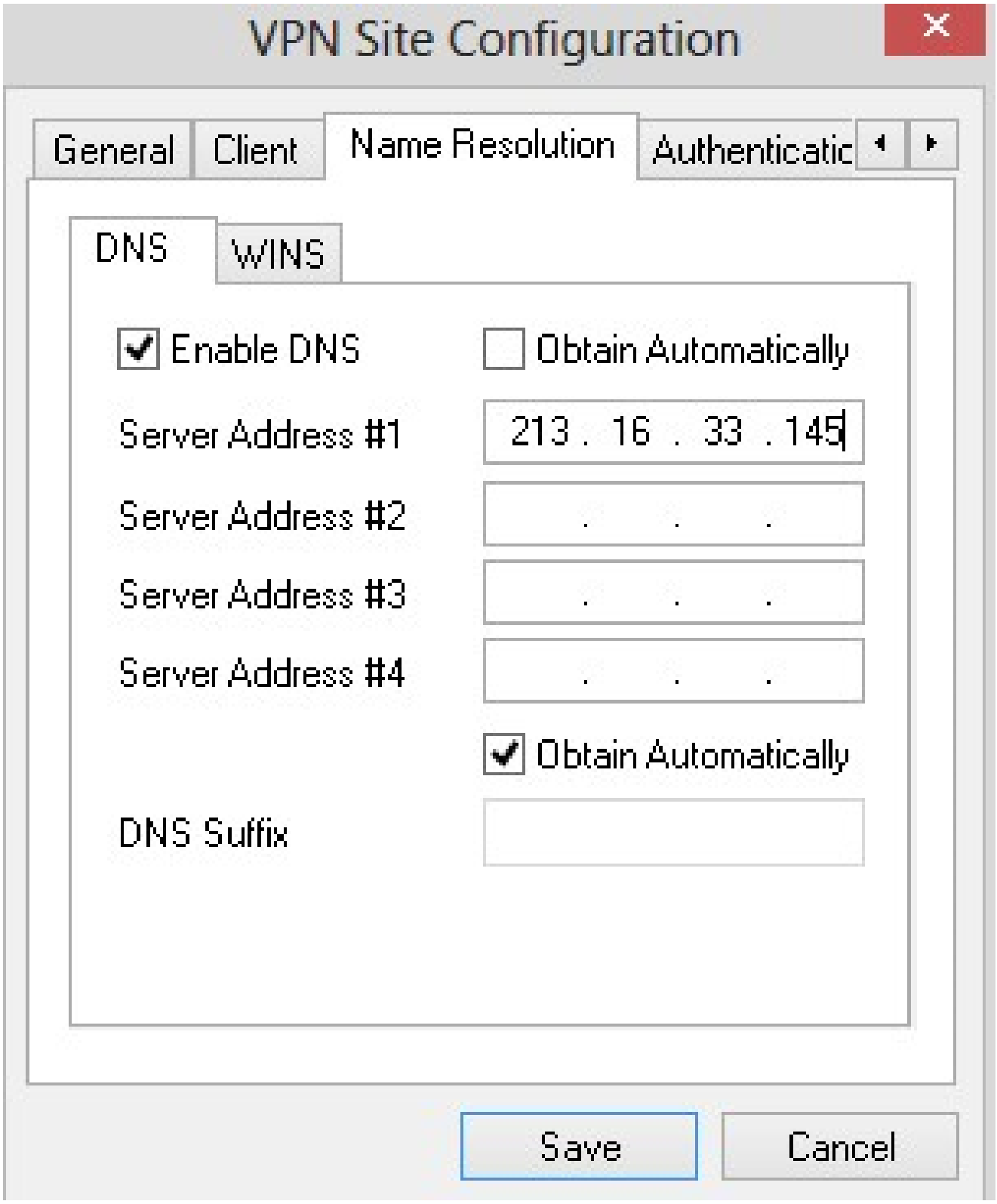


3단계. Enable DNS(DNS 활성화)를 선택하여 DNS(Domain Name System)를 활성화합니다.

4단계(선택 사항) DNS 서버 주소를 자동으로 가져오려면 Obtain Automatically(자동으로 가져오기) 확인란을 선택합니다. 이 옵션을 선택하는 경우 6단계로 건너뜁니다.

5단계. Server Address #1 필드에 DNS 서버 주소를 입력합니다. 다른 DNS 서버가 있는 경우

나머지 Server Address 필드에 해당 서버의 주소를 입력합니다.

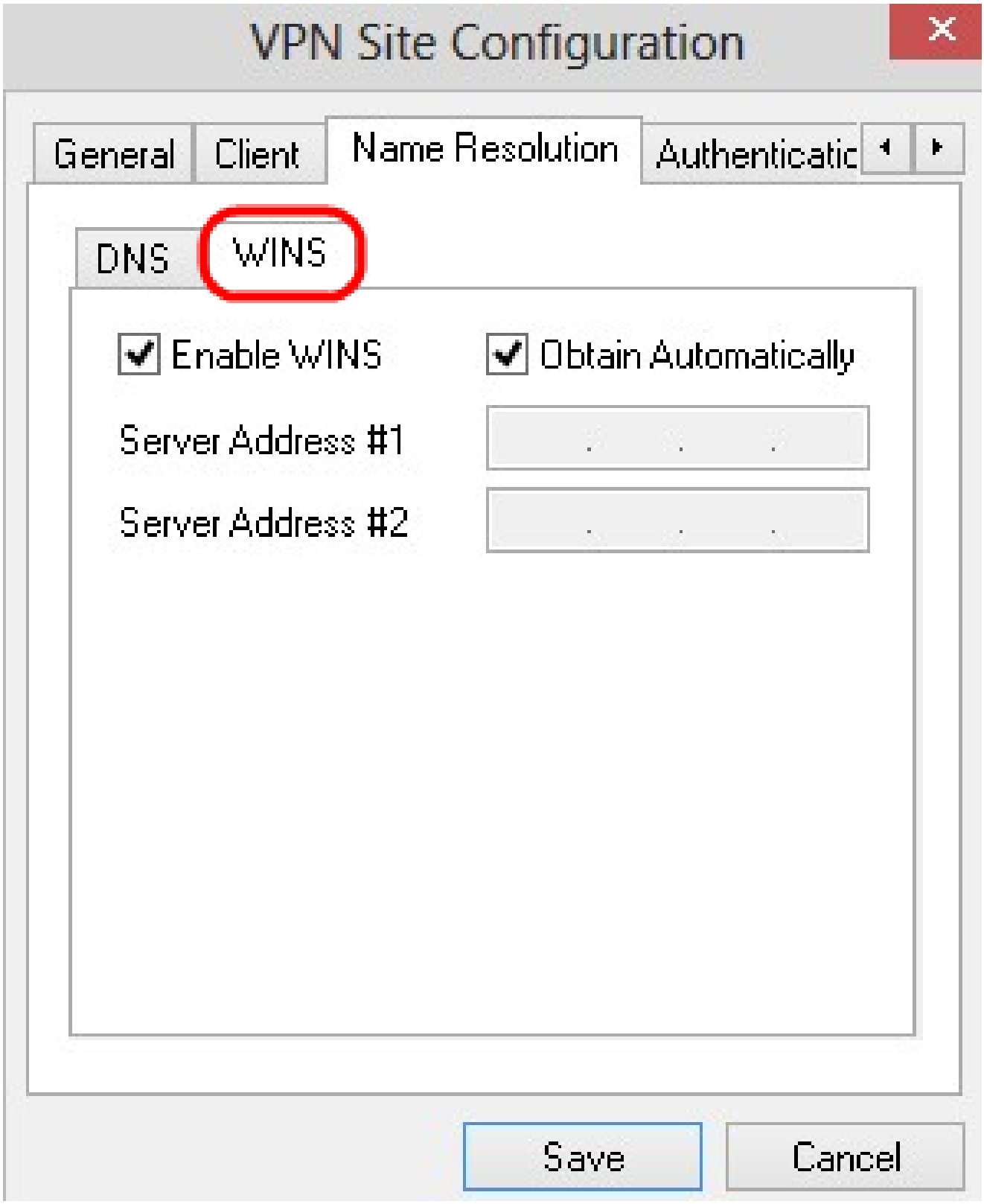


6단계. (선택 사항) DNS 서버의 접미사를 자동으로 가져오려면 Obtain Automatically(자동으로 가져오기) 확인란을 선택합니다. 이 옵션을 선택하는 경우 8단계로 건너뜁니다.

7단계. DNS Suffix 필드에 DNS 서버의 접미사를 입력합니다.

8단계. Save(저장)를 클릭하여 설정을 저장합니다.

9단계. WINS 탭을 클릭합니다.

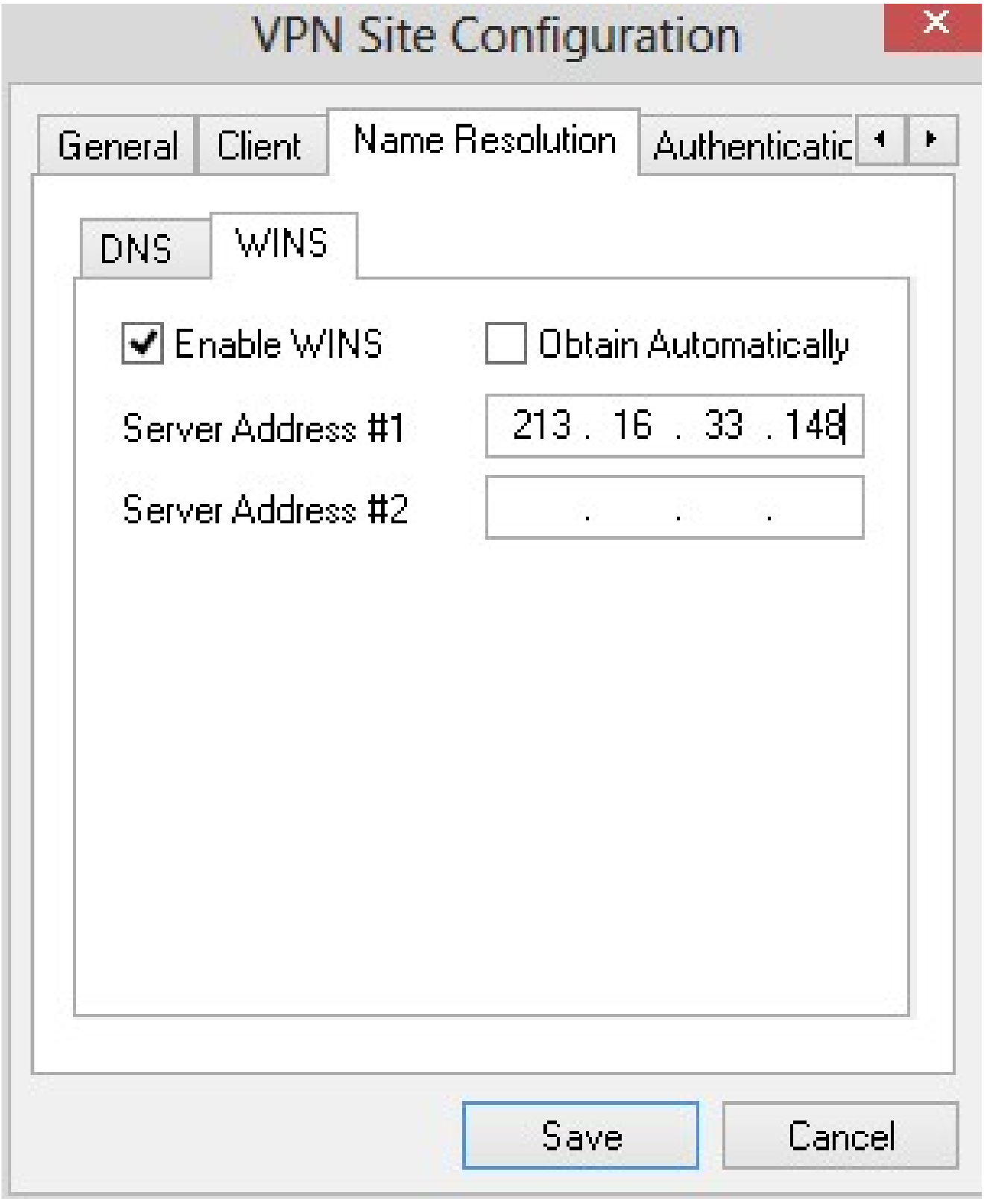


10단계. WINS(Windows Internet Name Server)를 활성화하려면 Enable WINS(WINS 활성화

)를 선택합니다.

11단계(선택 사항) DNS 서버 주소를 자동으로 가져오려면 Obtain Automatically(자동으로 가져오기) 확인란을 선택합니다. 이 옵션을 선택하는 경우 13단계로 건너뜁니다.

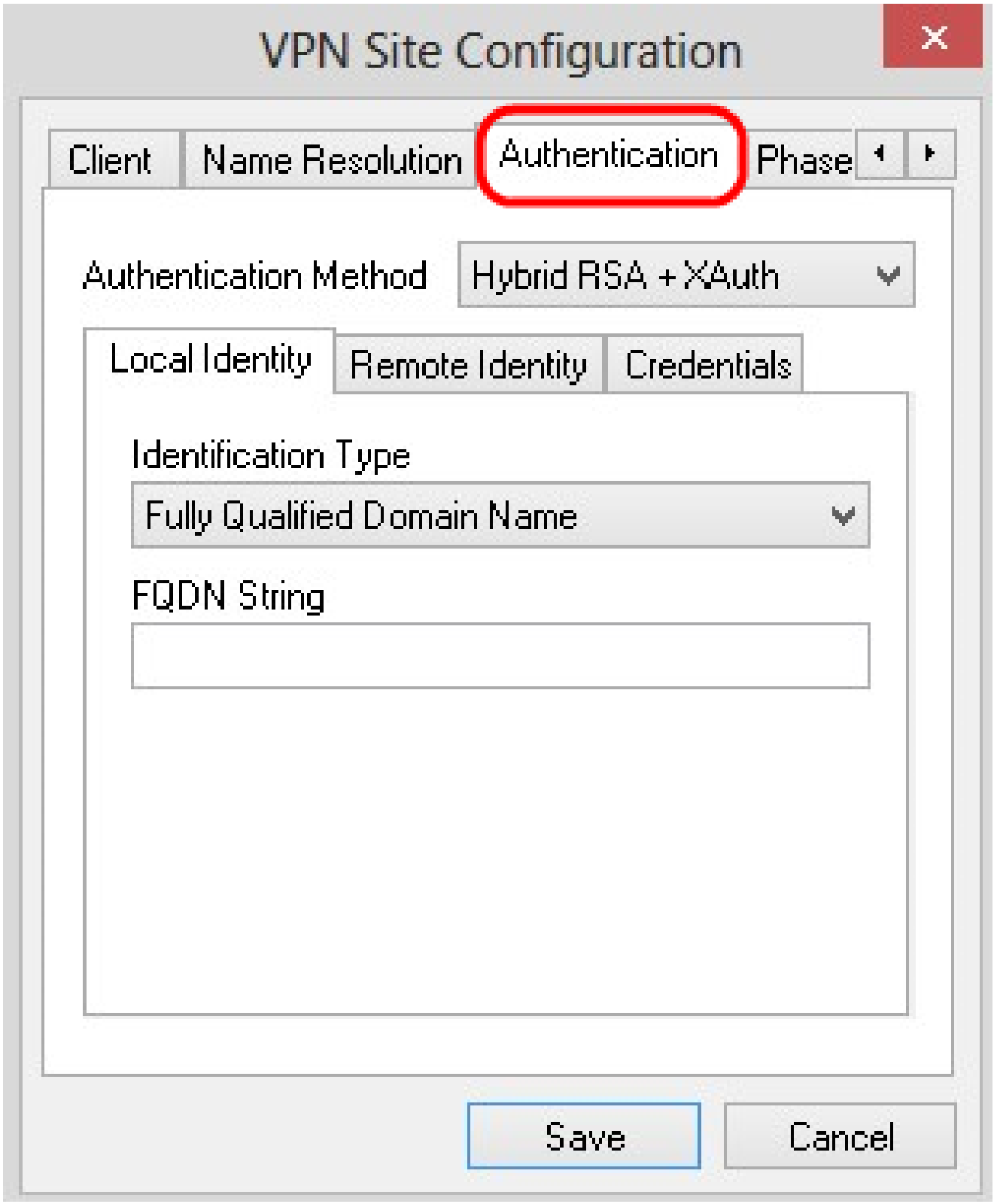
12단계. Server Address #1 필드에 WINS 서버의 주소를 입력합니다. 다른 DNS 서버가 있는 경우 나머지 Server Address 필드에 해당 서버의 주소를 입력합니다.



13단계. Save(저장)를 클릭하여 설정을 저장합니다.

인증

1단계. Authentication(인증) 탭을 클릭합니다.



참고: Authentication(인증) 섹션에서 클라이언트가 ISAKMP SA를 설정하려고 할 때 인증을 처리하도록 매개변수를 구성할 수 있습니다.

2단계. Authentication Method 드롭다운 목록에서 적절한 인증 방법을 선택합니다.

· 하이브리드 RSA + XAuth — 클라이언트 자격 증명이 필요하지 않습니다. 클라이언트가 게

이트웨이를 인증합니다. 자격 증명은 PEM 또는 PKCS12 인증서 파일 또는 키 파일 형식의 형태로 제공됩니다.

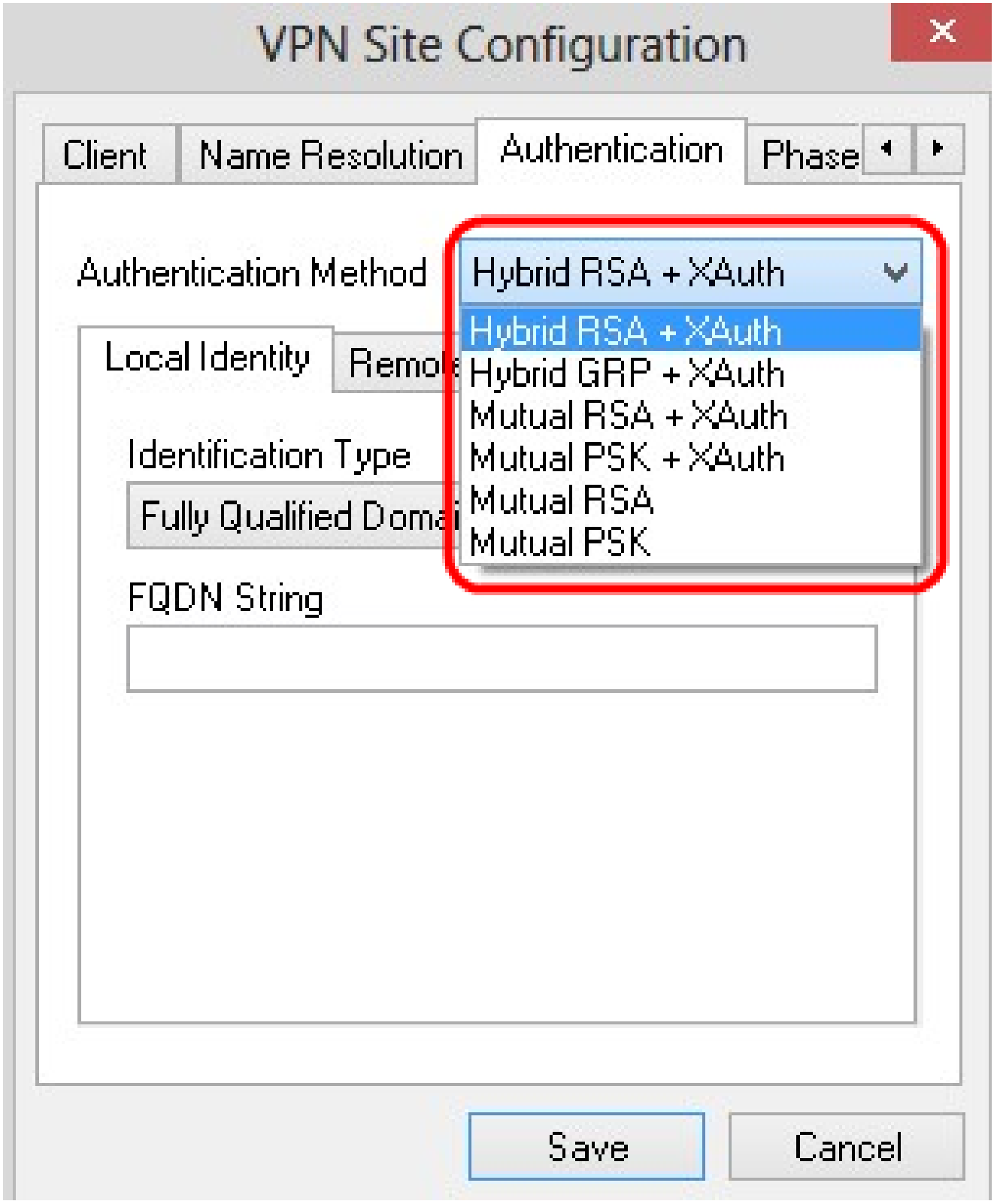
· 하이브리드 GRP + XAuth — 클라이언트 자격 증명이 필요하지 않습니다. 클라이언트가 게이트웨이를 인증합니다. 자격 증명은 PEM 또는 PKCS12 인증서 파일 및 공유 암호 문자열 형식입니다.

· 상호 RSA + XAuth — 클라이언트와 게이트웨이는 모두 인증을 위해 자격 증명이 필요합니다. 자격 증명은 PEM 또는 PKCS12 인증서 파일 또는 키 유형 형식입니다.

· 상호 PSK + XAuth — 인증하려면 클라이언트와 게이트웨이 모두에 자격 증명이 필요합니다. 자격 증명은 공유 암호 문자열 형식입니다.

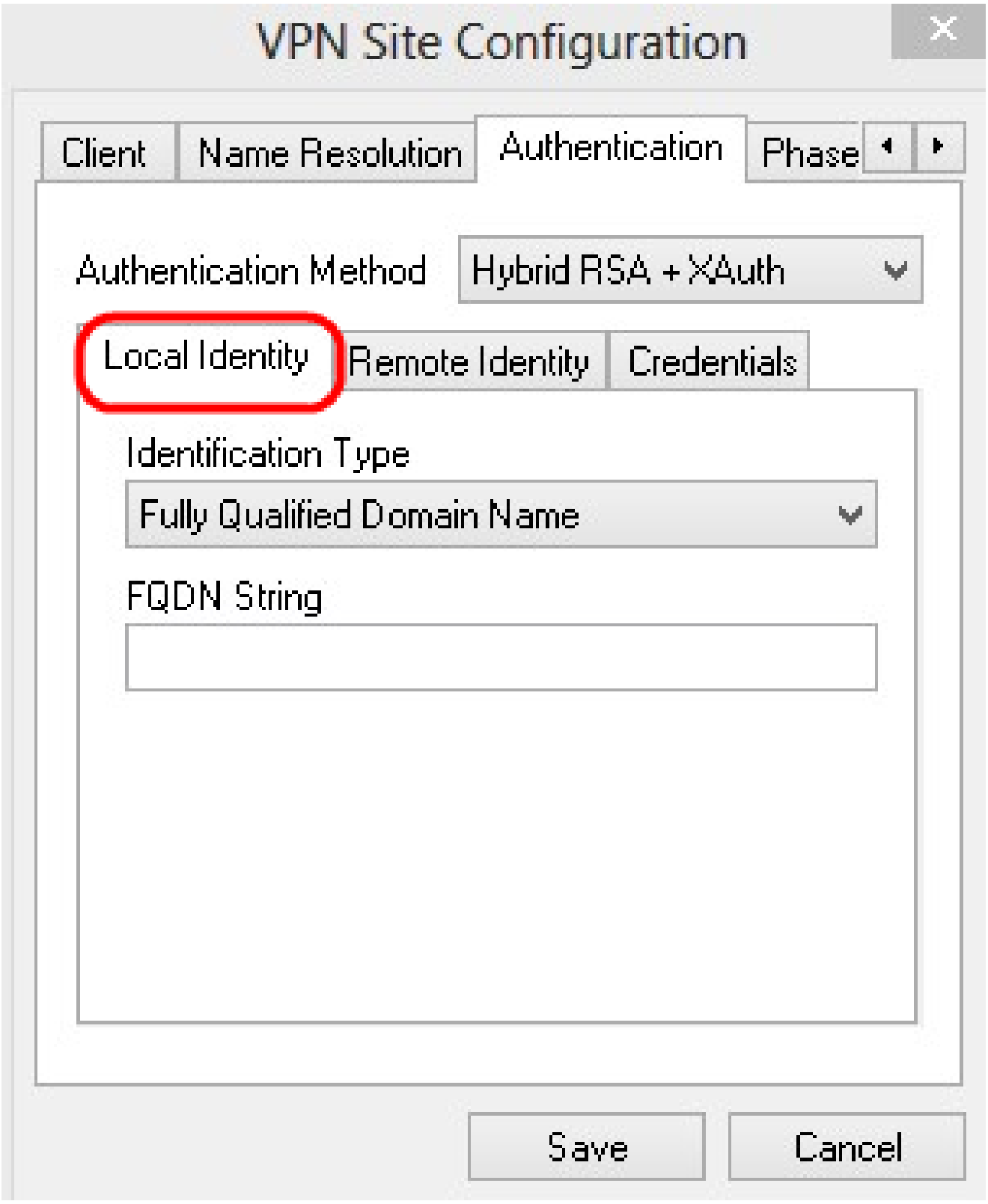
· 상호 RSA — 클라이언트와 게이트웨이 모두 인증을 위해 자격 증명이 필요합니다. 자격 증명은 PEM 또는 PKCS12 인증서 파일 또는 키 유형 형식입니다.

· 상호 PSK — 인증하려면 클라이언트와 게이트웨이 모두 자격 증명이 필요합니다. 자격 증명은 공유 암호 문자열 형식입니다.



로컬 ID 컨피그레이션

1단계. Local Identity(로컬 ID) 탭을 클릭합니다.



참고: 로컬 ID는 확인을 위해 게이트웨이로 전송되는 ID를 설정합니다. Local Identity(로컬 ID) 섹션에서 ID가 전송되는 방법을 확인하기 위해 Identification Type(식별 유형) 및 FQDN(Fully Qualified Domain Name) 문자열이 구성됩니다.

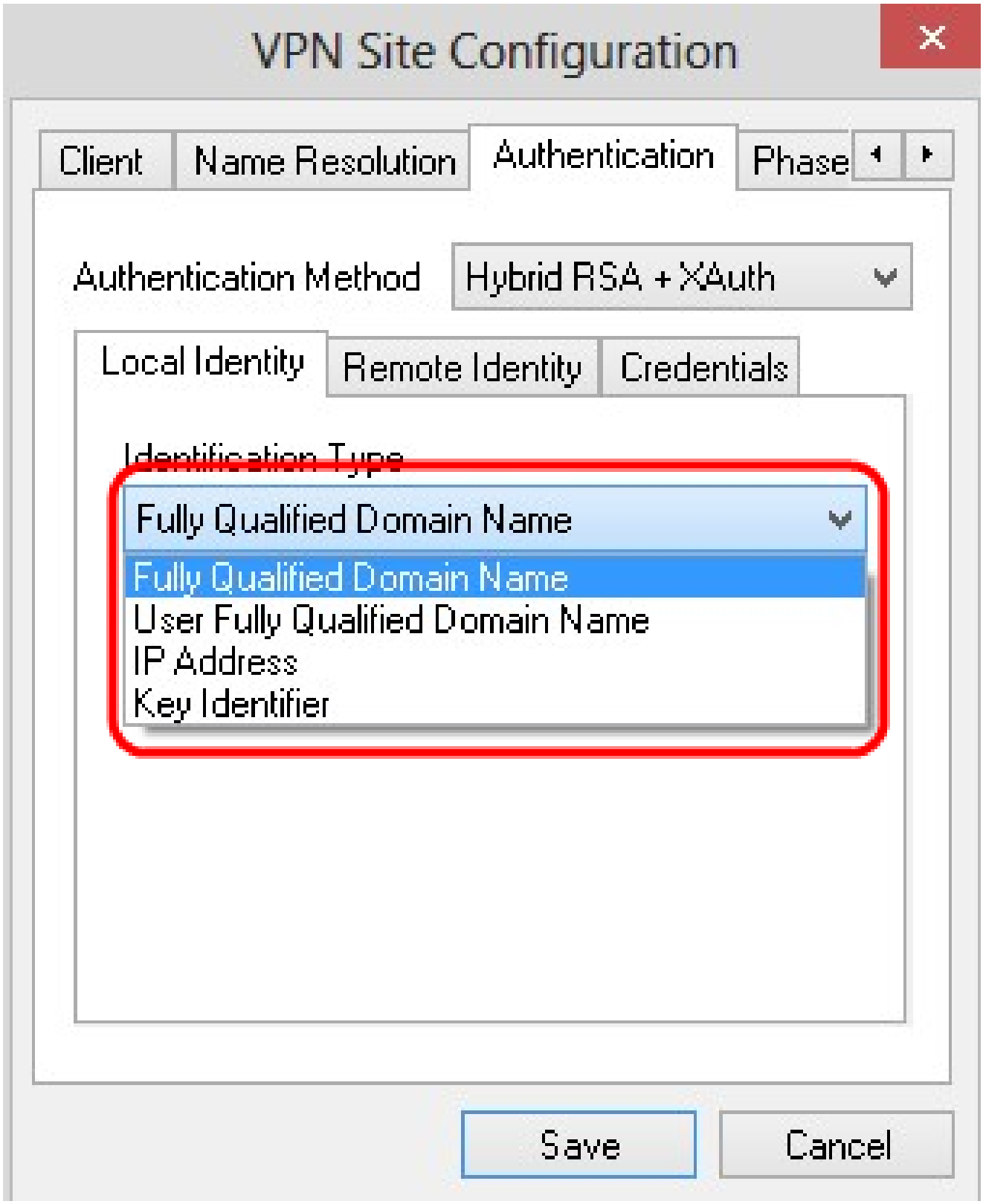
2단계. Identification Type 드롭다운 목록에서 적절한 식별 옵션을 선택합니다. 모든 인증 모드에 대해 일부 옵션을 사용할 수 있는 것은 아닙니다.

· FQDN(Fully Qualified Domain Name) — 로컬 ID의 클라이언트 ID는 FQDN(Fully Qualified Domain Name)을 기반으로 합니다. 이 옵션을 선택하는 경우 3단계를 수행한 다음 7단계로 건너뜁니다.

· 사용자 FQDN — 로컬 ID의 클라이언트 식별은 사용자 FQDN을 기반으로 합니다. 이 옵션을 선택하는 경우 4단계를 수행한 다음 7단계로 건너뜁니다.

· IP Address — 로컬 ID의 클라이언트 식별은 IP 주소를 기반으로 합니다. Use a discovered local host address(검색된 로컬 호스트 주소 사용)를 선택하면 IP 주소가 자동으로 검색됩니다. 이 옵션을 선택하는 경우 5단계를 수행한 다음 7단계로 건너뜁니다.

· 키 식별자 — 로컬 클라이언트의 클라이언트 식별은 키 식별자를 기반으로 식별됩니다. 이 옵션을 선택하는 경우 6단계와 7단계를 따릅니다.



3단계. FQDN String 필드에 DNS 문자열로 정규화된 도메인 이름을 입력합니다.

4단계. UFQDN String 필드에 DNS 문자열로 사용자 FQDN(정규화된 도메인 이름)을 입력합니다.

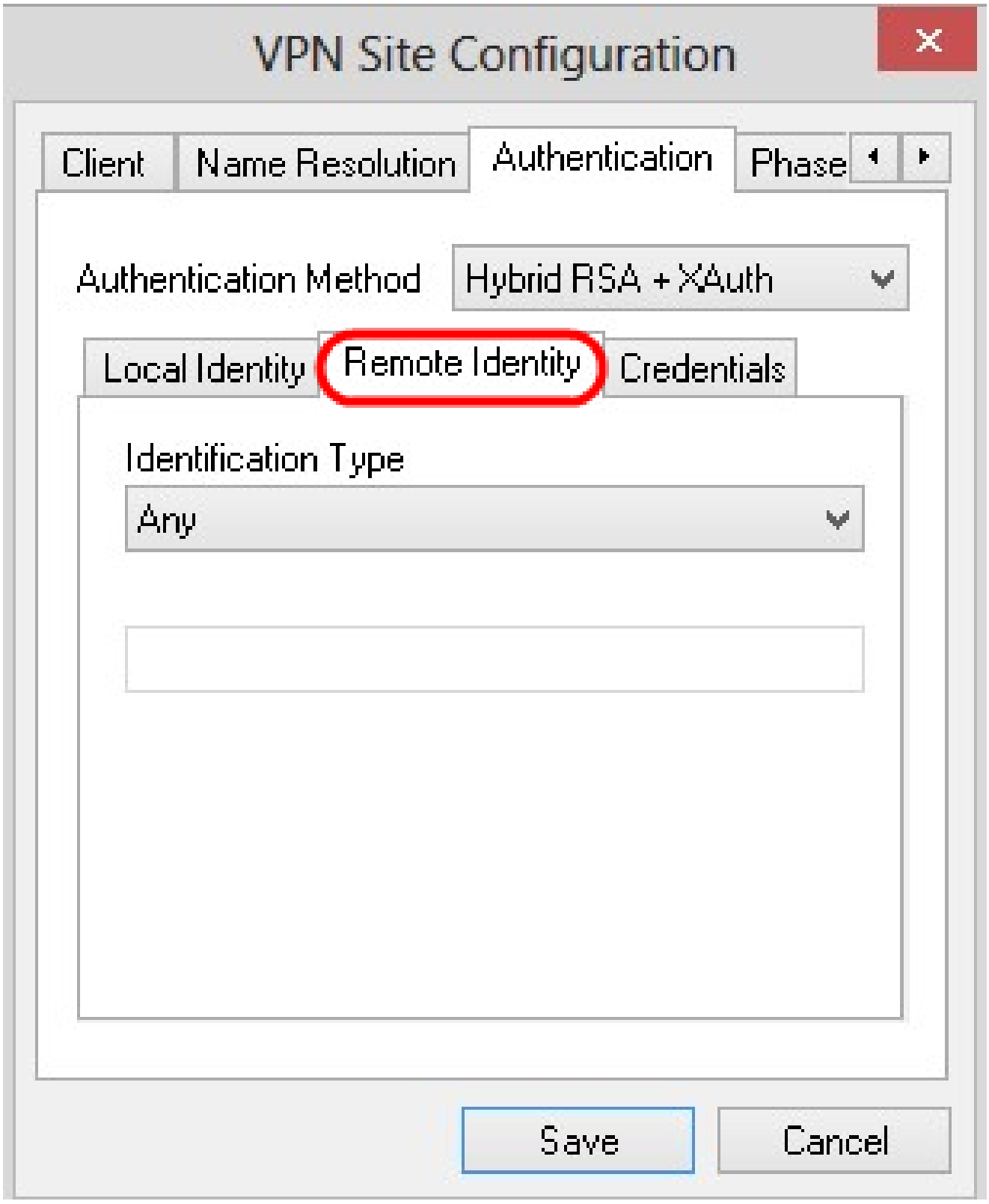
5단계. FQDN String 필드에 IP 주소를 입력합니다.

6단계. 키 ID 문자열에서 로컬 클라이언트를 식별하기 위한 키 식별자를 입력합니다.

7단계. Save(저장)를 클릭하여 설정을 저장합니다.

원격 ID 구성

1단계. 원격 ID 탭을 클릭합니다.



참고: 원격 ID는 게이트웨이에서 ID를 확인합니다. Remote Identity(원격 ID) 섹션에서 ID 확인 방법을 결정하도록 ID Type(식별 유형)이 구성됩니다.

2단계. Identification Type 드롭다운 목록에서 적절한 식별 옵션을 선택합니다.

· Any — 원격 클라이언트가 값 또는 ID를 승인하여 인증할 수 있습니다.

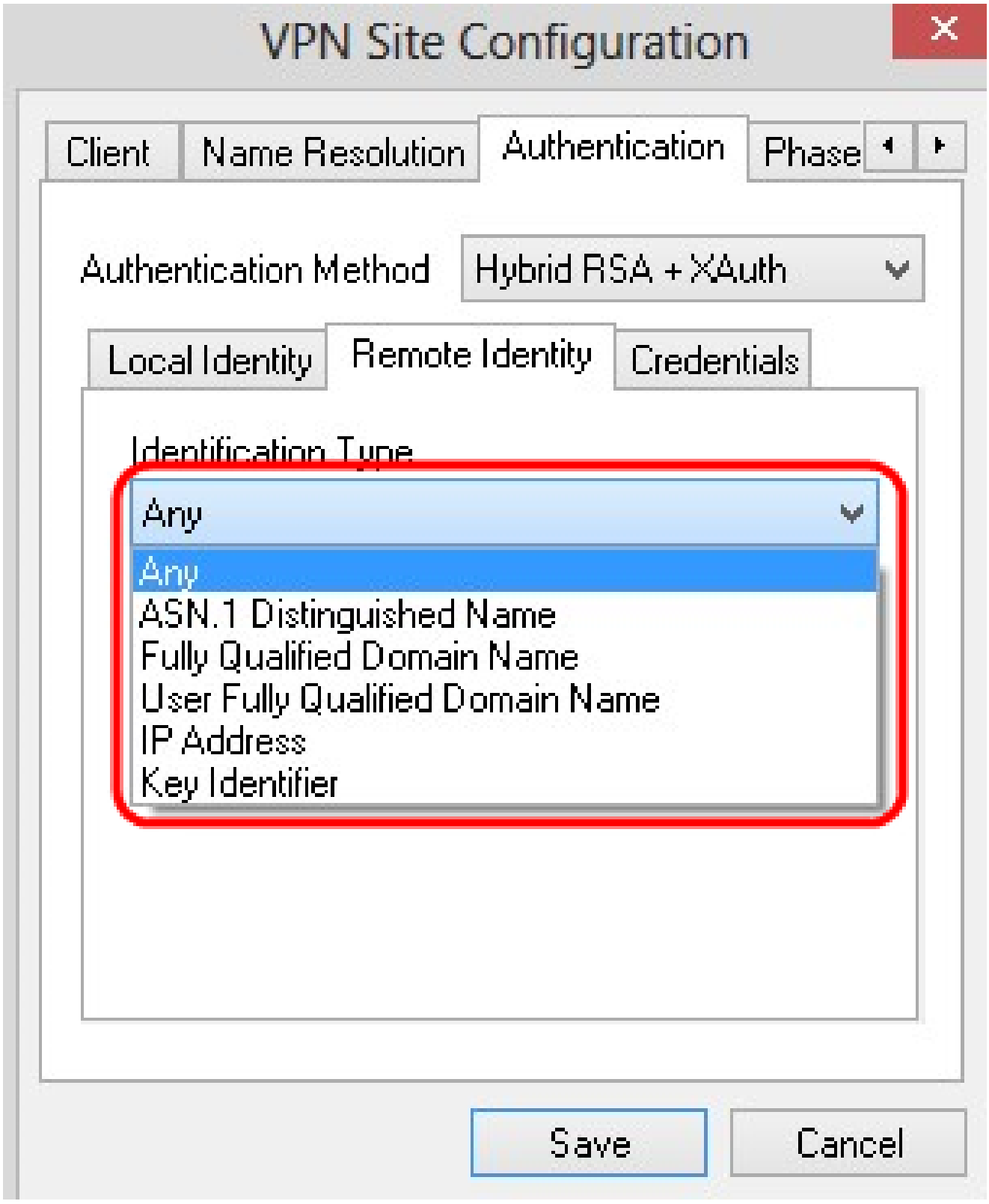
· ASN.1 Distinguished Name — 원격 클라이언트가 PEM 또는 PKCS12 인증서 파일에서 자동으로 식별됩니다. 인증 섹션의 2단계에서 RSA 인증 방법을 선택하는 경우에만 이 옵션을 선택할 수 있습니다. 인증서를 자동으로 수신하려면 Use the subject in the received certificate but don't compare with specific value 확인란을 선택하여 해당 인증서를 자동으로 수신합니다. 이 옵션을 선택하는 경우 3단계를 수행한 다음 8단계로 건너뜁니다.

· FQDN(Fully Qualified Domain Name) — 원격 ID의 클라이언트 식별은 FQDN(Fully Qualified Domain Name)을 기반으로 합니다. 인증 섹션의 2단계에서 PSK 인증 방법을 선택하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션을 선택하는 경우 4단계를 수행한 다음 8단계로 건너뜁니다.

· 사용자 FQDN(Fully Qualified Domain Name) — 원격 ID의 클라이언트 식별은 사용자 FQDN을 기반으로 합니다. 인증 섹션의 2단계에서 PSK 인증 방법을 선택하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션을 선택하는 경우 5단계를 수행한 다음 8단계로 건너뜁니다.

· IP Address — 원격 ID의 클라이언트 식별은 IP 주소를 기반으로 합니다. Use a discovered local host address(검색된 로컬 호스트 주소 사용)를 선택하면 IP 주소가 자동으로 검색됩니다. 이 옵션을 선택하는 경우 6단계를 수행한 다음 8단계로 건너뜁니다.

· Key Identifier — 원격 클라이언트가 식별하는 클라이언트 ID는 키 ID를 기반으로 합니다. 이 옵션을 선택하는 경우 7단계와 8단계를 따릅니다.



3단계. ASN.1 DN String 필드에 ASN.1 DN 문자열을 입력합니다.

4단계. FQDN String(FQDN 문자열) 필드에 DNS 문자열로 정규화된 도메인 이름을 입력합니다.

5단계. UFQDN String(FQDN 문자열) 필드에 DNS 문자열로 사용자 FQDN(Fully Qualified

Domain) 이름을 입력합니다.

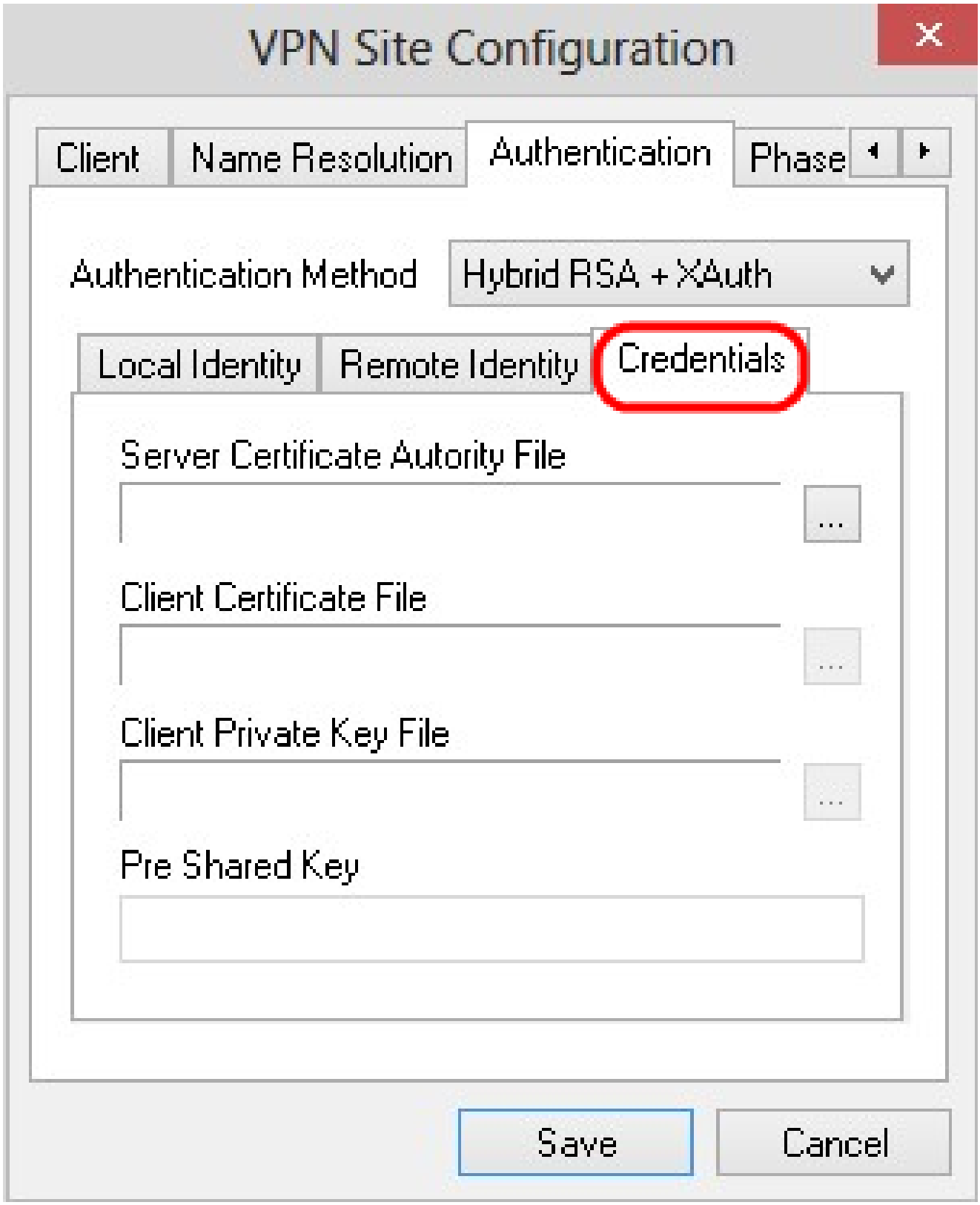
6단계. FQDN String 필드에 IP 주소를 입력합니다.

7단계. Key ID String 필드에 로컬 클라이언트를 식별하는 키 식별자를 입력합니다.

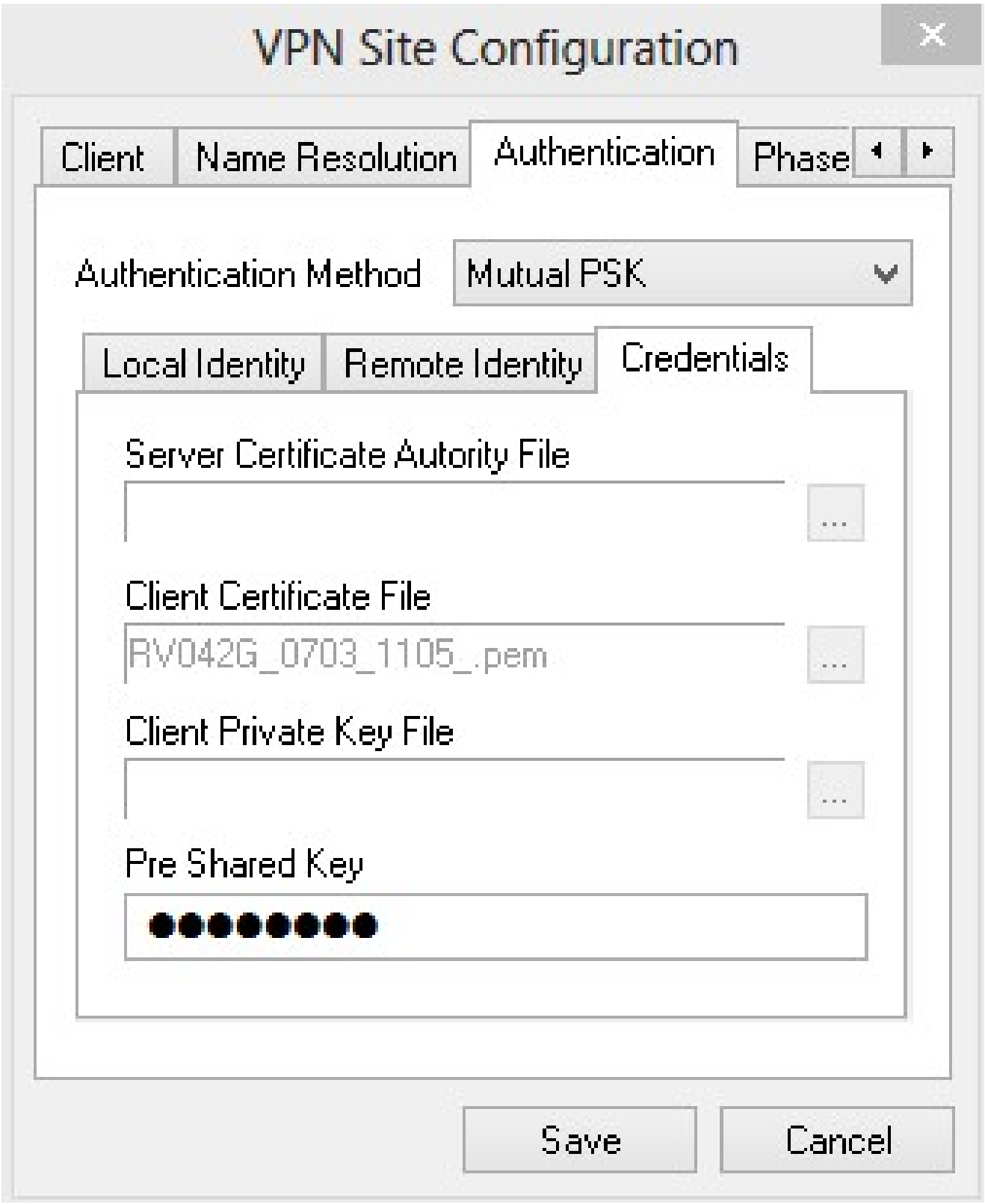
8단계. Save(저장)를 클릭하여 설정을 저장합니다.

자격 증명 구성

1단계. Credentials(자격 증명) 탭을 클릭합니다.



참고: Credentials(자격 증명) 섹션에서 Pre Shared Key(사전 공유 키)가 구성됩니다.



2단계. Server Certificate File(서버 인증서 파일)을 선택하려면 Server Certificate Authority File(서버 인증 기관 파일) 필드 옆에 있는 ... 아이콘을 클릭하고 서버 인증서 파일을 PC에 저장한 경로를 선택합니다.

3단계. 클라이언트 인증서 파일을 선택하려면 Client Certificate File(클라이언트 인증서 파일) 필드 옆에 있는 ... 아이콘을 클릭하고 PC에 클라이언트 인증서 파일을 저장한 경로를 선택합

니다.

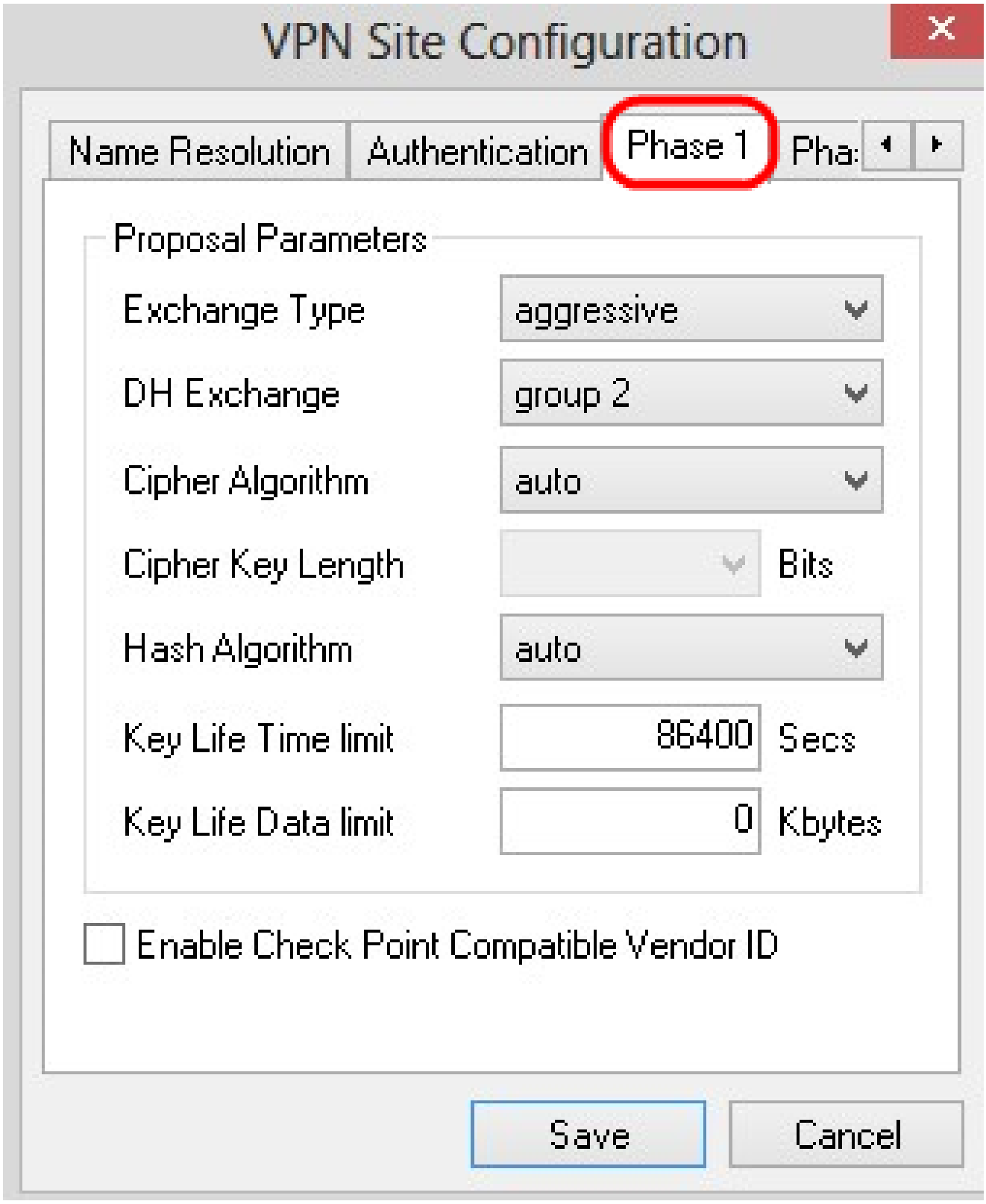
4단계. 클라이언트 개인 키 파일을 선택하려면 Client Private Key File(클라이언트 개인 키 파일) 필드 옆의 ... 아이콘을 클릭하고 PC에 클라이언트 개인 키 파일을 저장한 경로를 선택합니다.

5단계. PreShared Key(사전 공유 키) 필드에 사전 공유 키를 입력합니다. 이 키는 터널 컨피그레이션 중에 사용하는 키와 동일해야 합니다.

6단계. Save(저장)를 클릭하여 설정을 저장합니다.

1단계 컨피그레이션

1단계. 1단계 탭을 클릭합니다.

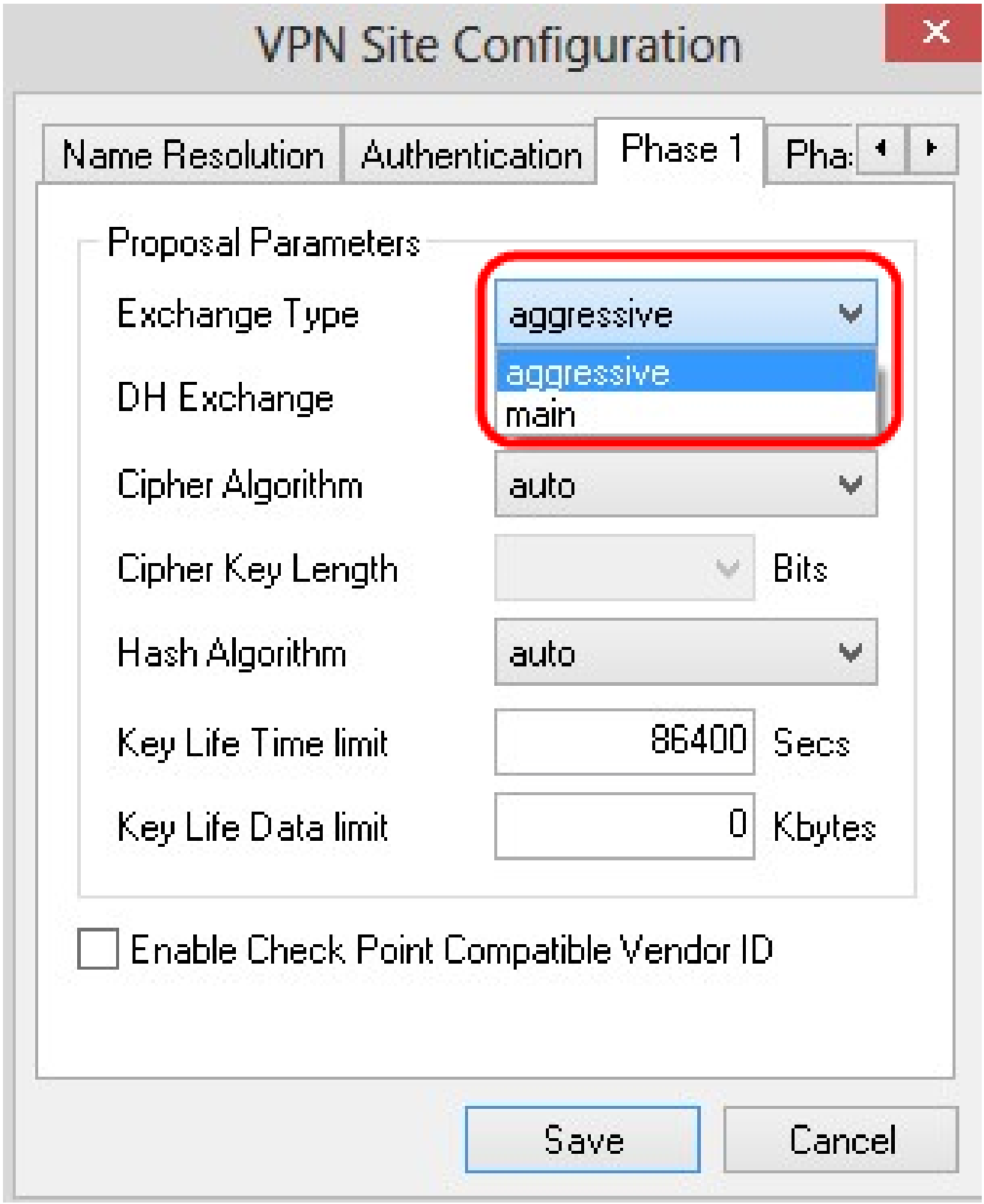


참고: 1단계 섹션에서 클라이언트 게이트웨이가 있는 ISAKMP SA를 설정할 수 있도록 매개변수를 구성할 수 있습니다.

2단계. Exchange Type 드롭다운 목록에서 적절한 키 교환 유형을 선택합니다.

· Main — 피어의 ID가 보호됩니다.

· Aggressive — 피어의 ID가 보호되지 않습니다.



3단계. DH Exchange 드롭다운 목록에서 VPN 연결을 구성하는 동안 선택한 적절한 그룹을 선택합니다.

4단계. Cipher Algorithm 드롭다운 목록에서 VPN Connection을 구성하는 동안 선택한 적절한

옵션을 선택합니다.

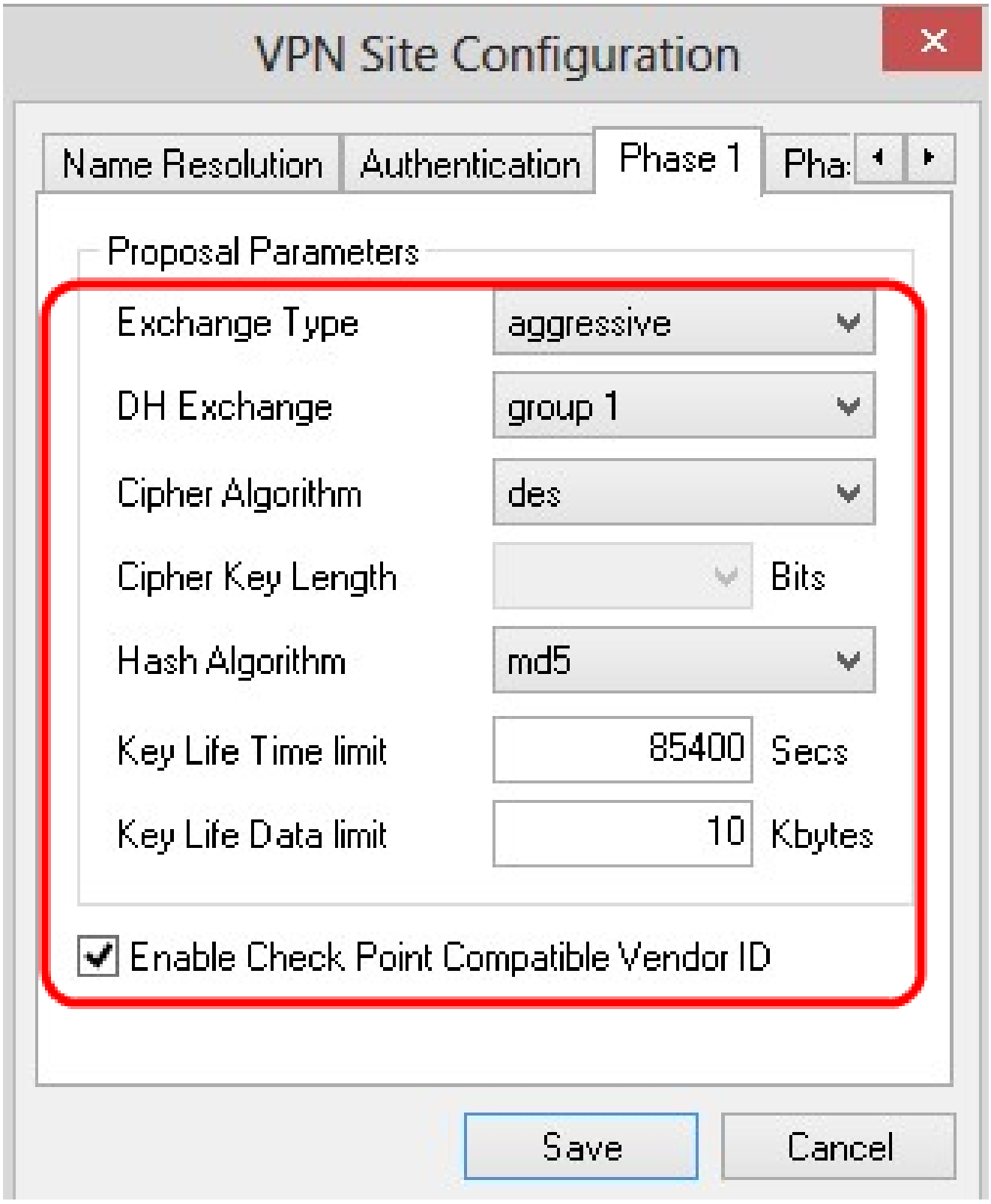
5단계. Cipher Key Length 드롭다운 목록에서 VPN 연결 구성 중에 선택한 옵션의 키 길이와 일치하는 옵션을 선택합니다.

6단계. Hash Algorithm(해시 알고리즘) 드롭다운 목록에서 VPN Connection(VPN 연결) 컨피그레이션 중에 선택한 옵션을 선택합니다.

7단계. Key Life Time limit(키 수명 제한) 필드에서 VPN 연결을 구성하는 동안 사용되는 값을 입력합니다.

8단계. Key Life Data limit(키 수명 데이터 제한) 필드에 보호할 값을 킬로바이트 단위로 입력합니다. 기본값은 0이며, 이 경우 기능이 해제됩니다.

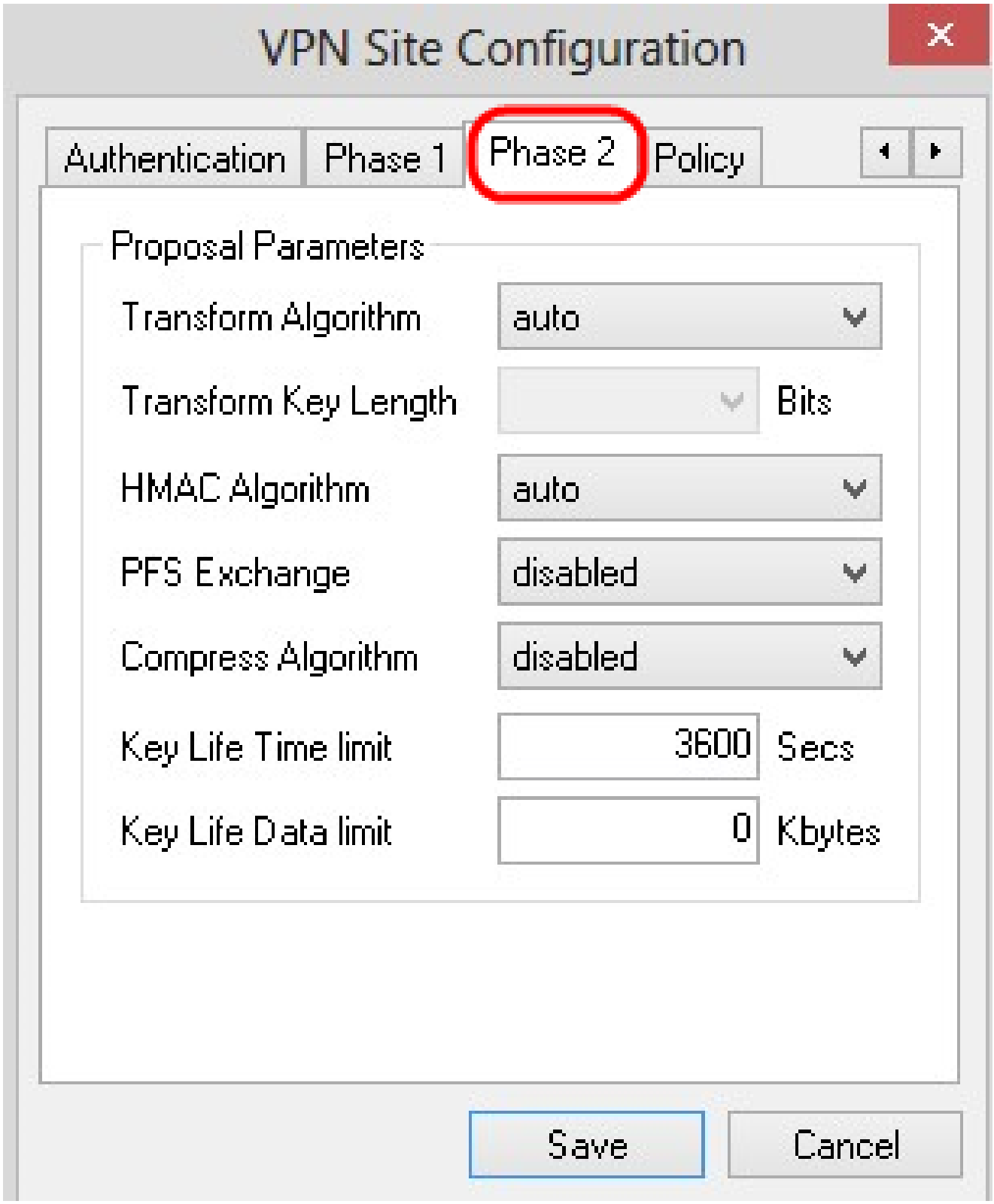
9단계. (선택 사항) Enable Check Point Compatible Vendor ID(Check Point 호환 벤더 ID 활성화) 확인란을 선택합니다.



10단계. Save(저장)를 클릭하여 설정을 저장합니다.

2단계 컨피그레이션

1단계. 2단계 탭을 클릭합니다.



참고: 2단계 섹션에서 원격 클라이언트 게이트웨이가 있는 IPsec SA를 설정할 수 있도록 매개 변수를 구성할 수 있습니다.

2단계. Transform Algorithm 드롭다운 목록에서 VPN 연결 구성 중에 선택한 옵션을 선택합니다.

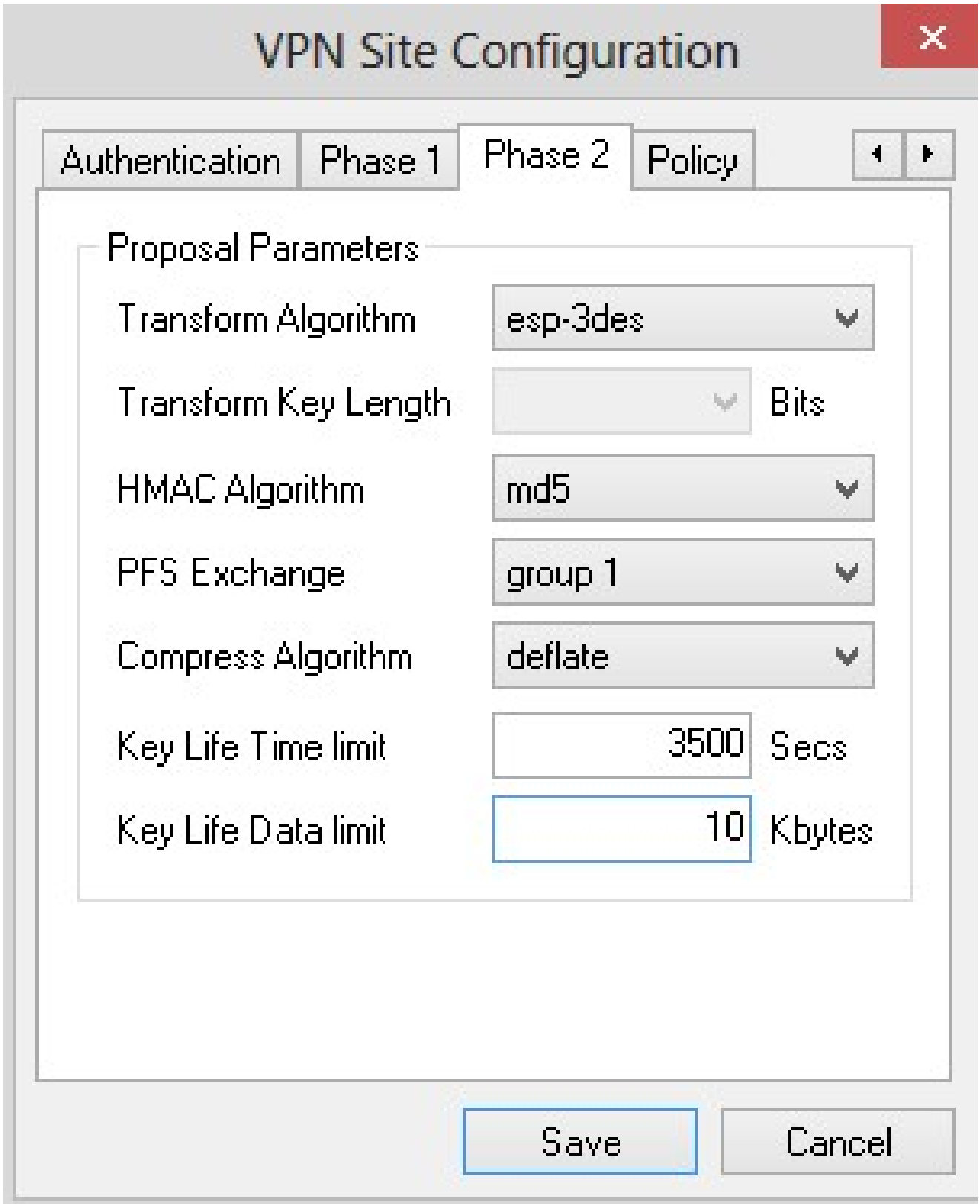
3단계. Transform Key Length 드롭다운 목록에서 VPN 연결을 구성하는 동안 선택한 옵션의 키 길이와 일치하는 옵션을 선택합니다.

4단계. HMAC Algorithm 드롭다운 목록에서 VPN 연결 구성 중에 선택한 옵션을 선택합니다.

5단계. PFS Exchange 드롭다운 목록에서 VPN 연결을 구성하는 동안 선택한 옵션을 선택합니다.

6단계. Key Life Time limit(키 수명 제한) 필드에 VPN 연결을 구성하는 동안 사용되는 값을 입력합니다.

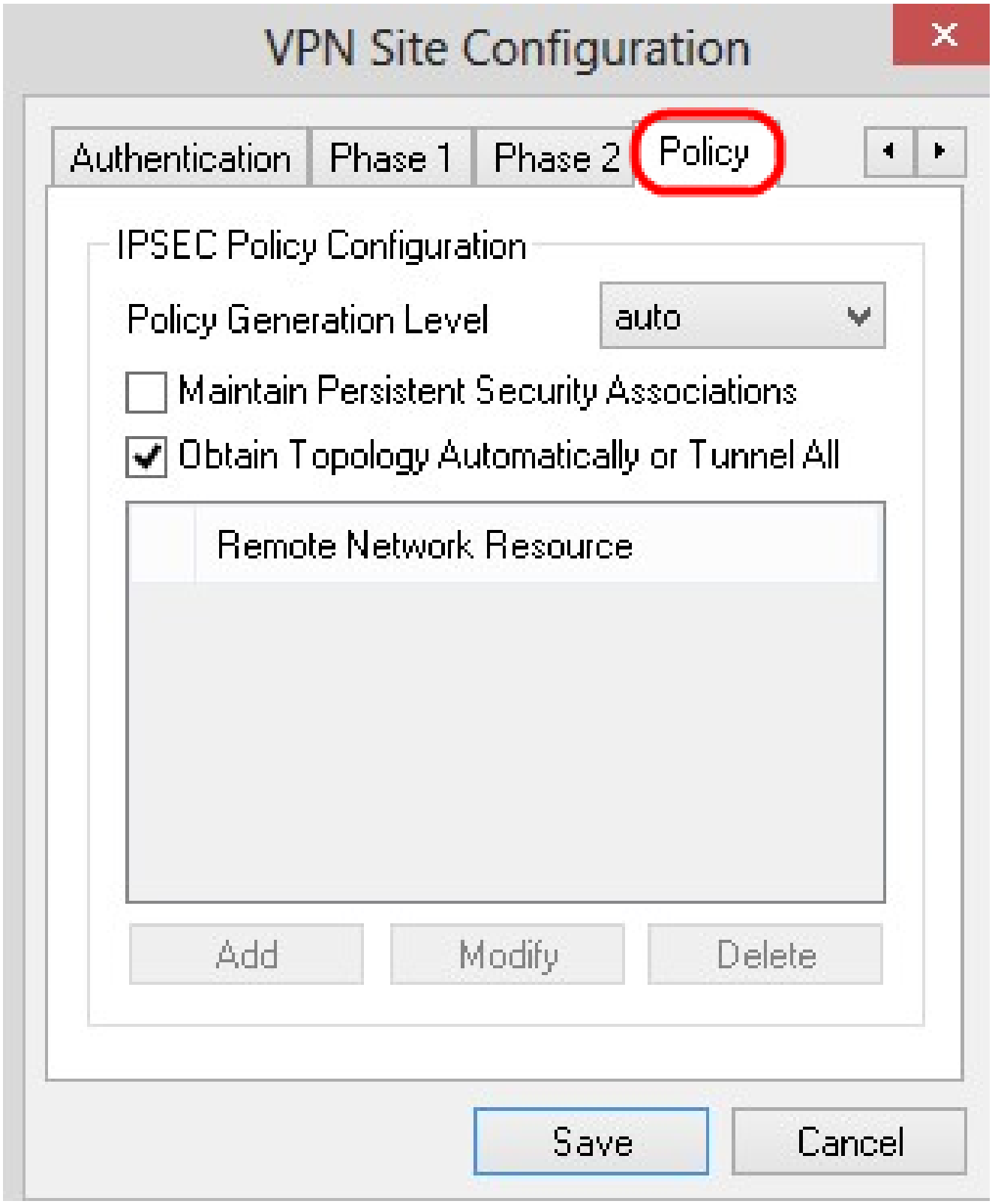
7단계. Key Life Data limit(키 수명 데이터 제한) 필드에 보호할 값을 킬로바이트 단위로 입력합니다. 기본값은 0이며, 이 경우 기능이 해제됩니다.



8단계. Save(저장)를 클릭하여 설정을 저장합니다.

정책 컨피그레이션

1단계. Policy(정책) 탭을 클릭합니다.



참고: Policy(정책) 섹션에서 IPSEC 정책이 정의되며, 이는 클라이언트가 사이트 컨피그레이션을 위해 호스트와 통신하는 데 필요합니다.

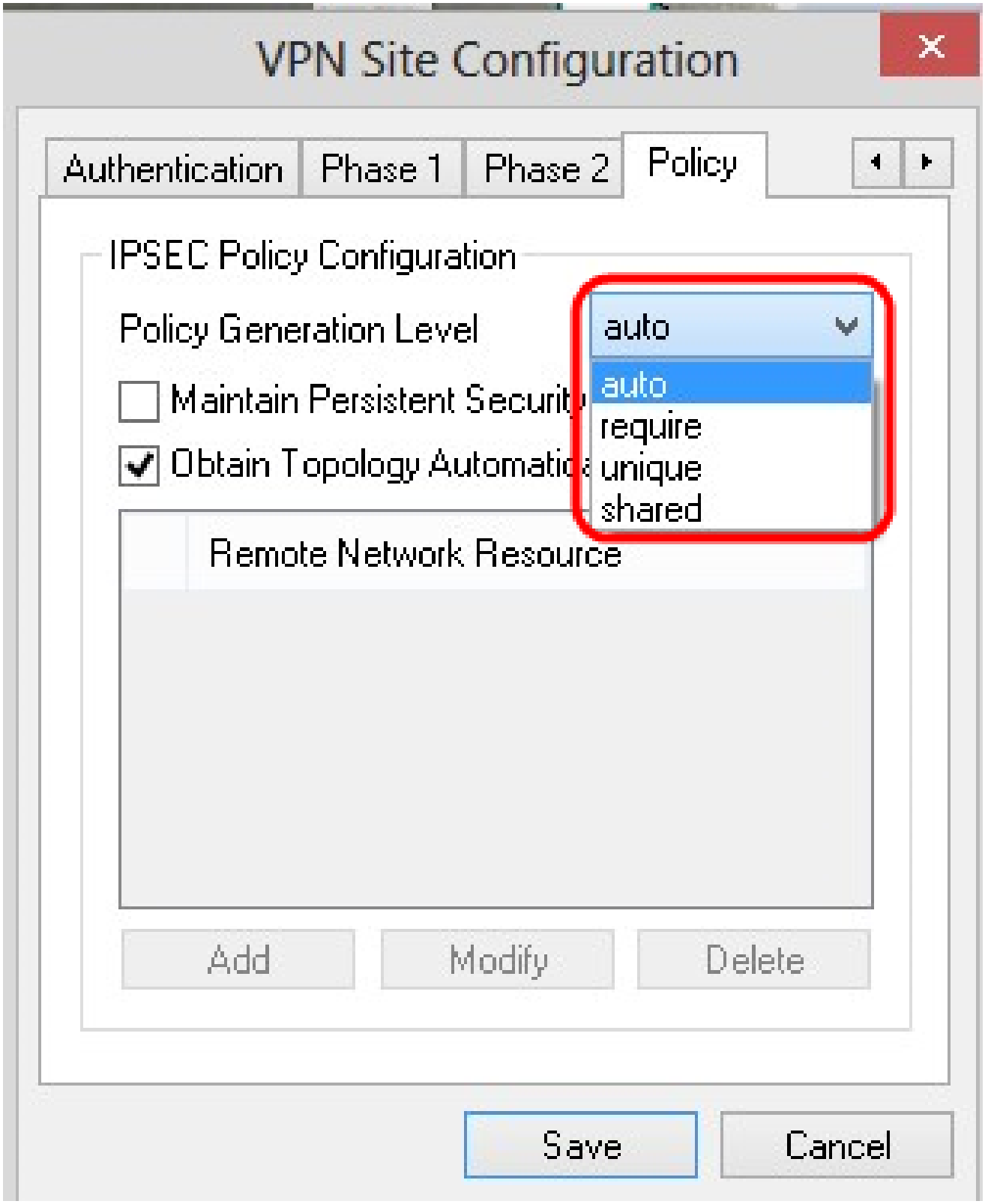
2단계. Policy Generation Level 드롭다운 목록에서 적절한 옵션을 선택합니다.

· Auto — 필요한 IPsec 정책 레벨이 자동으로 결정됩니다.

· Require — 각 정책에 대한 고유한 보안 연결은 협상되지 않습니다.

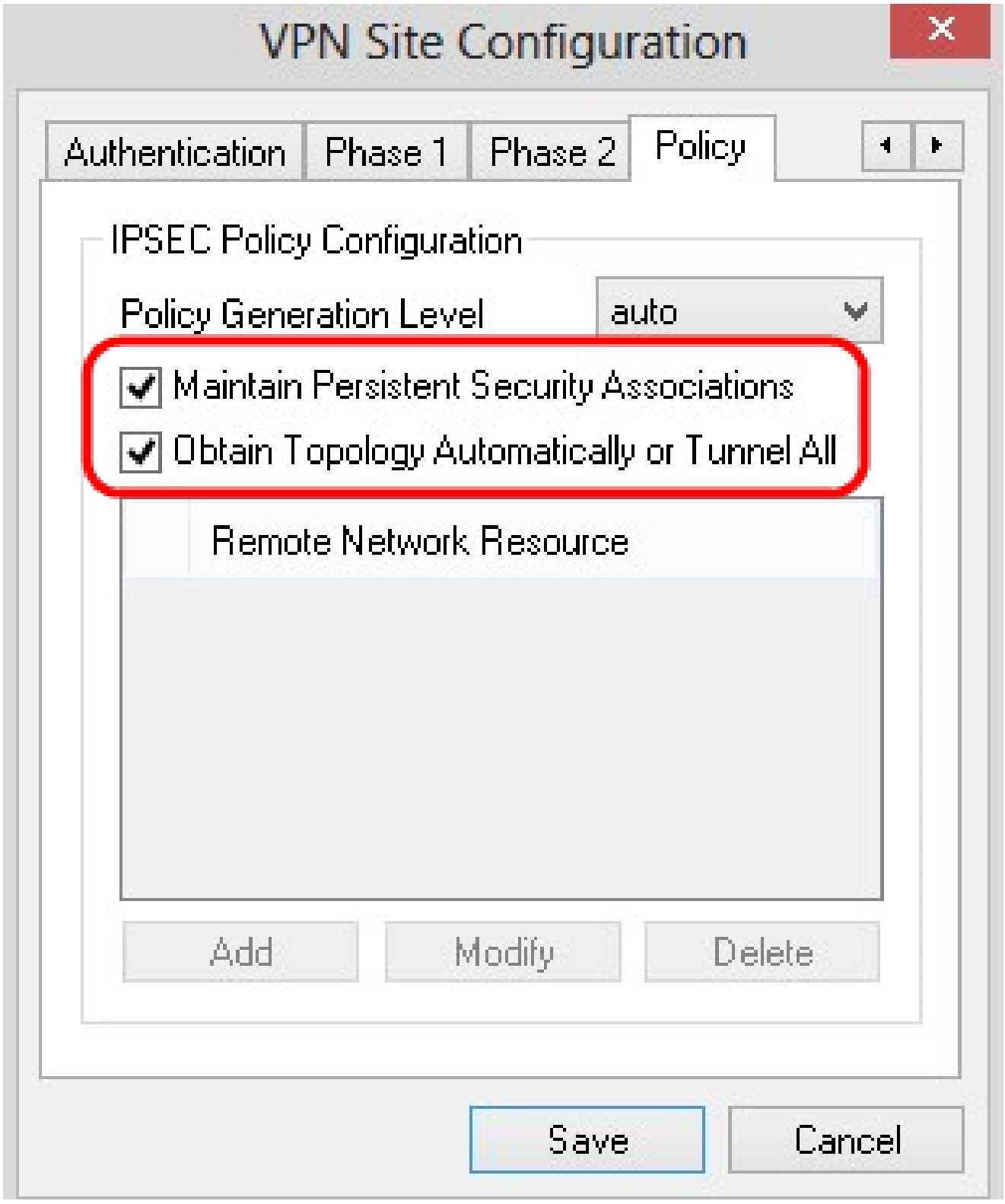
· Unique — 각 정책에 대한 고유한 보안 연결이 협상됩니다.

· 공유 — 필요한 레벨에서 적절한 정책이 생성됩니다.

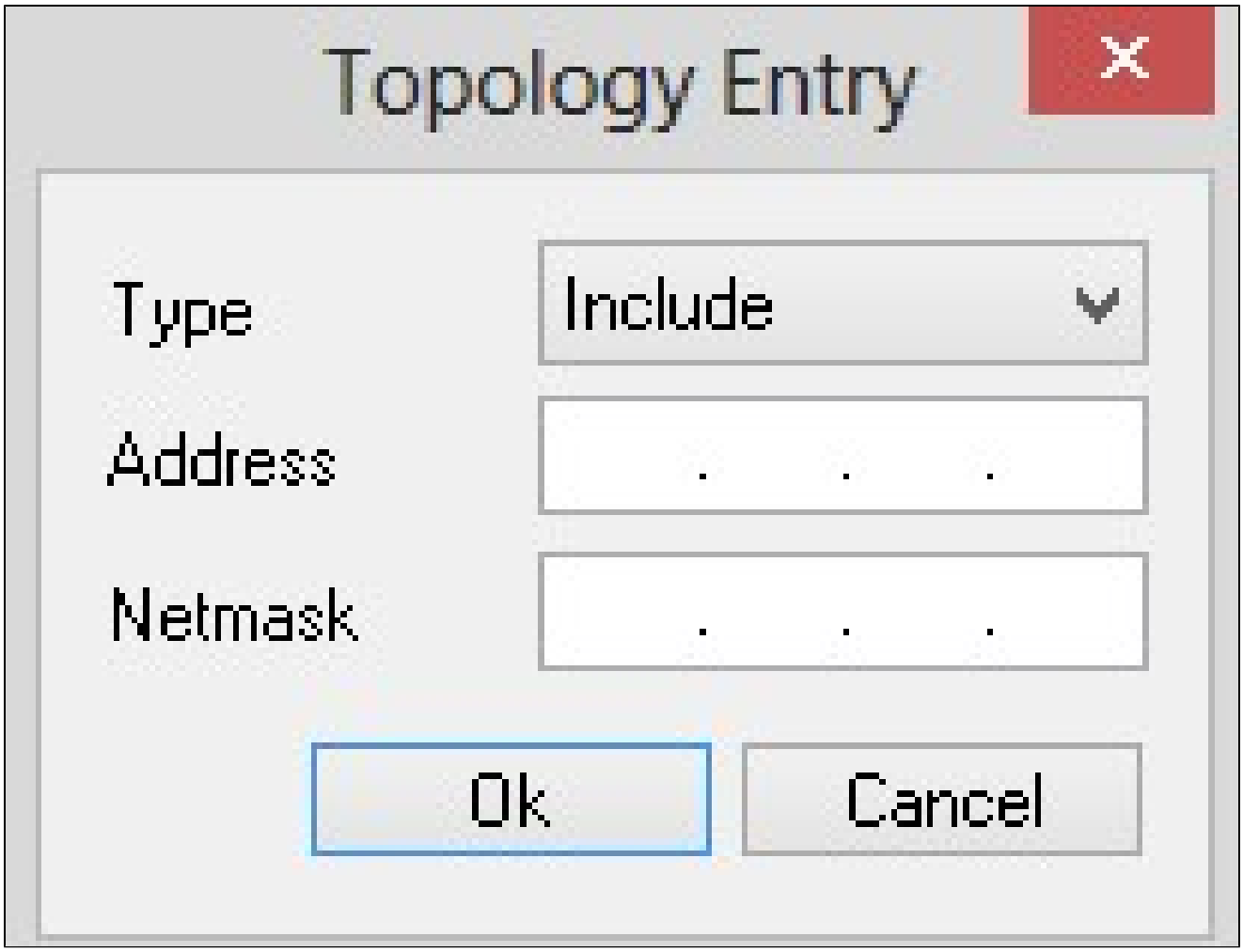


3단계. (선택 사항) IPSec 협상을 변경하려면 Maintain Persistent Security Associations 확인란을 선택합니다. 활성화된 경우 각 정책에 대한 협상이 연결된 후에 직접 이루어집니다. 비활성화된 경우 필요에 따라 협상이 이루어집니다.

4단계(선택 사항) 디바이스에서 자동으로 제공된 네트워크 목록을 수신하거나 기본적으로 모든 패킷을 RV0XX로 전송하려면 Obtain Topology Automatically or Tunnel All 확인란을 선택합니다. 선택하지 않으면 수동으로 컨피그레이션을 수행해야 합니다. 이 확인란을 선택한 경우 10단계로 건너뜁니다.



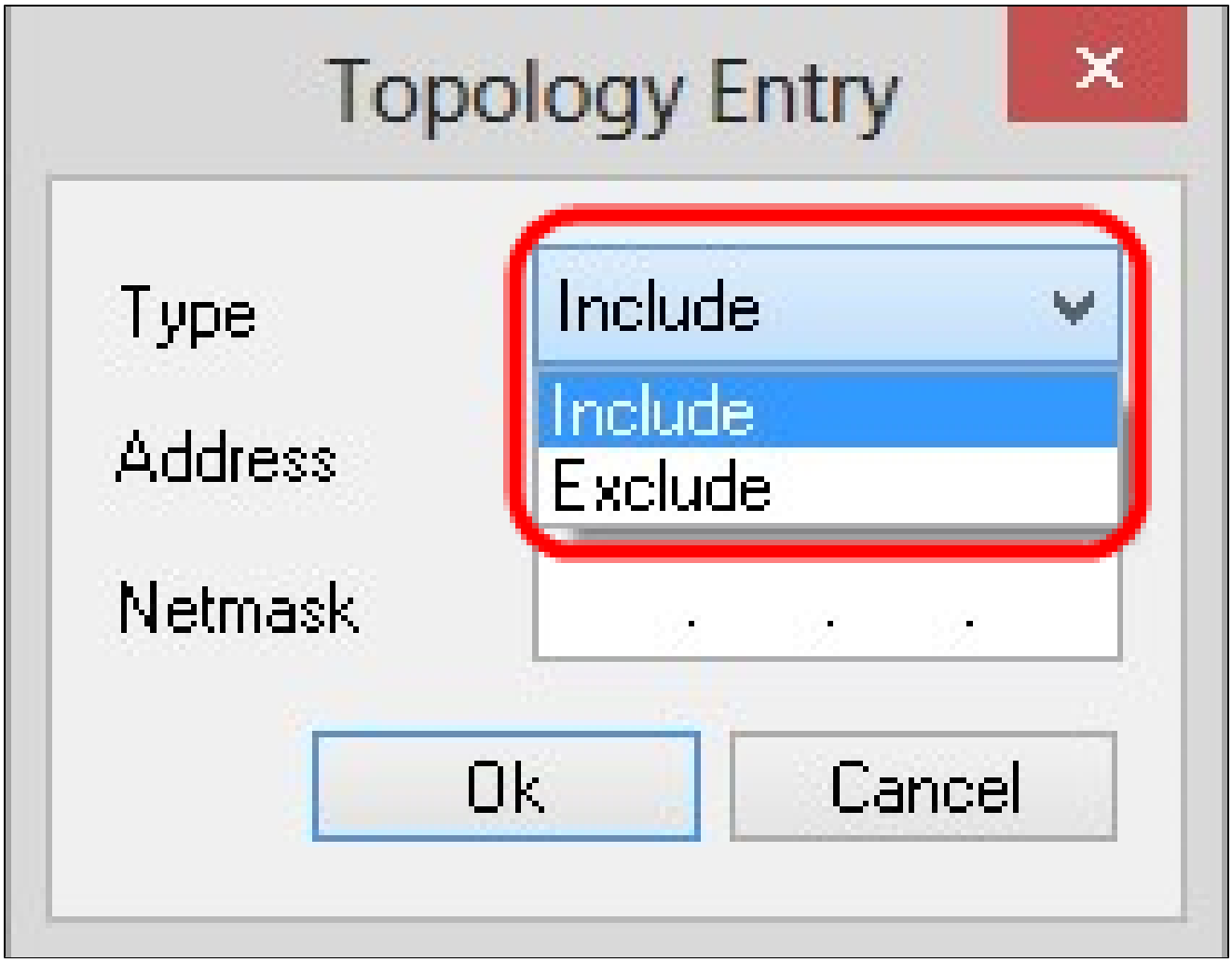
5단계. Add(추가)를 클릭하여 테이블에 토폴로지 항목을 추가합니다. Topology Entry 창이 나타납니다.



6단계. Type 드롭다운 목록에서 적절한 옵션을 선택합니다.

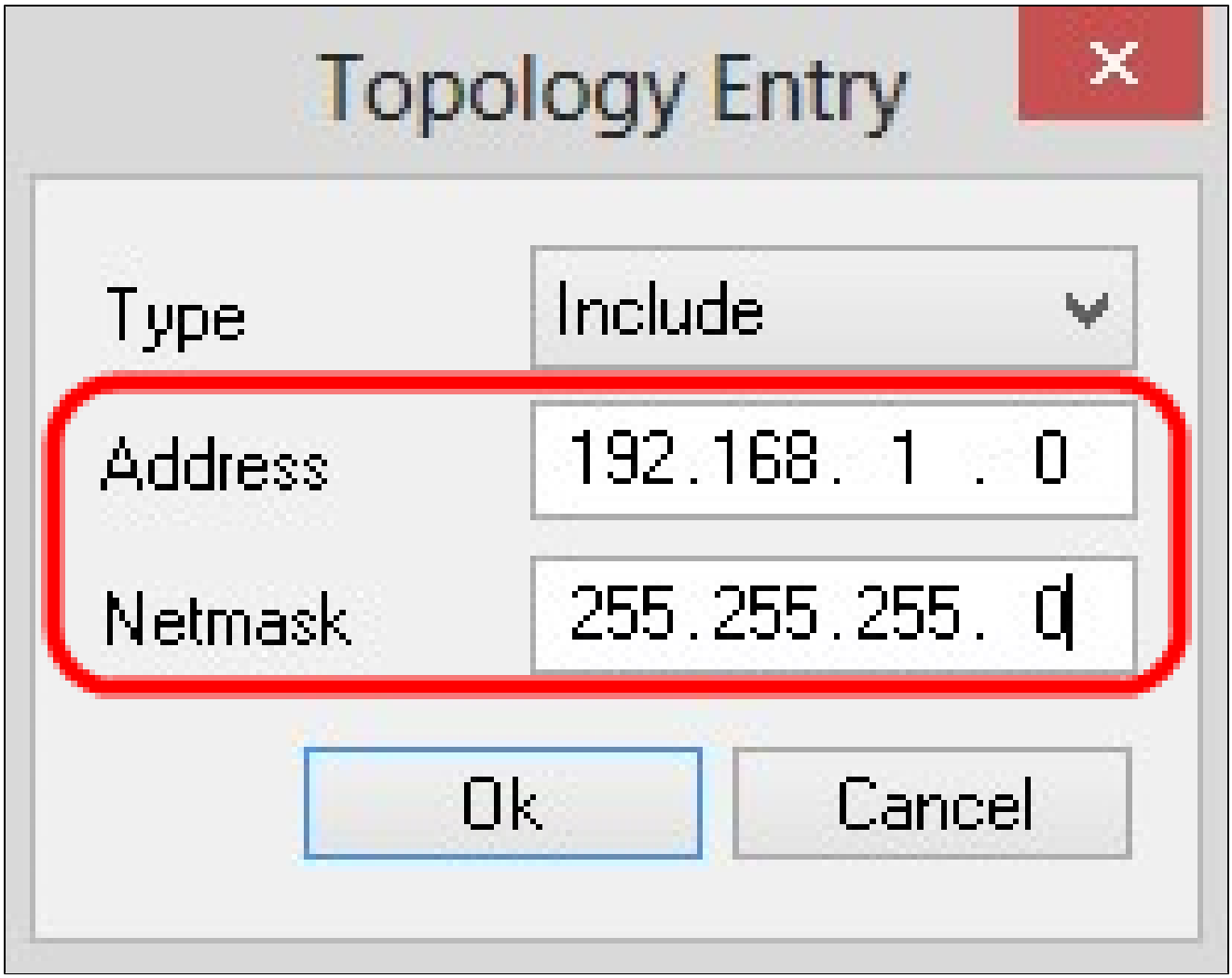
· 포함 — VPN 게이트웨이를 통해 네트워크에 액세스합니다.

· Exclude — 로컬 연결을 통해 네트워크에 액세스합니다.

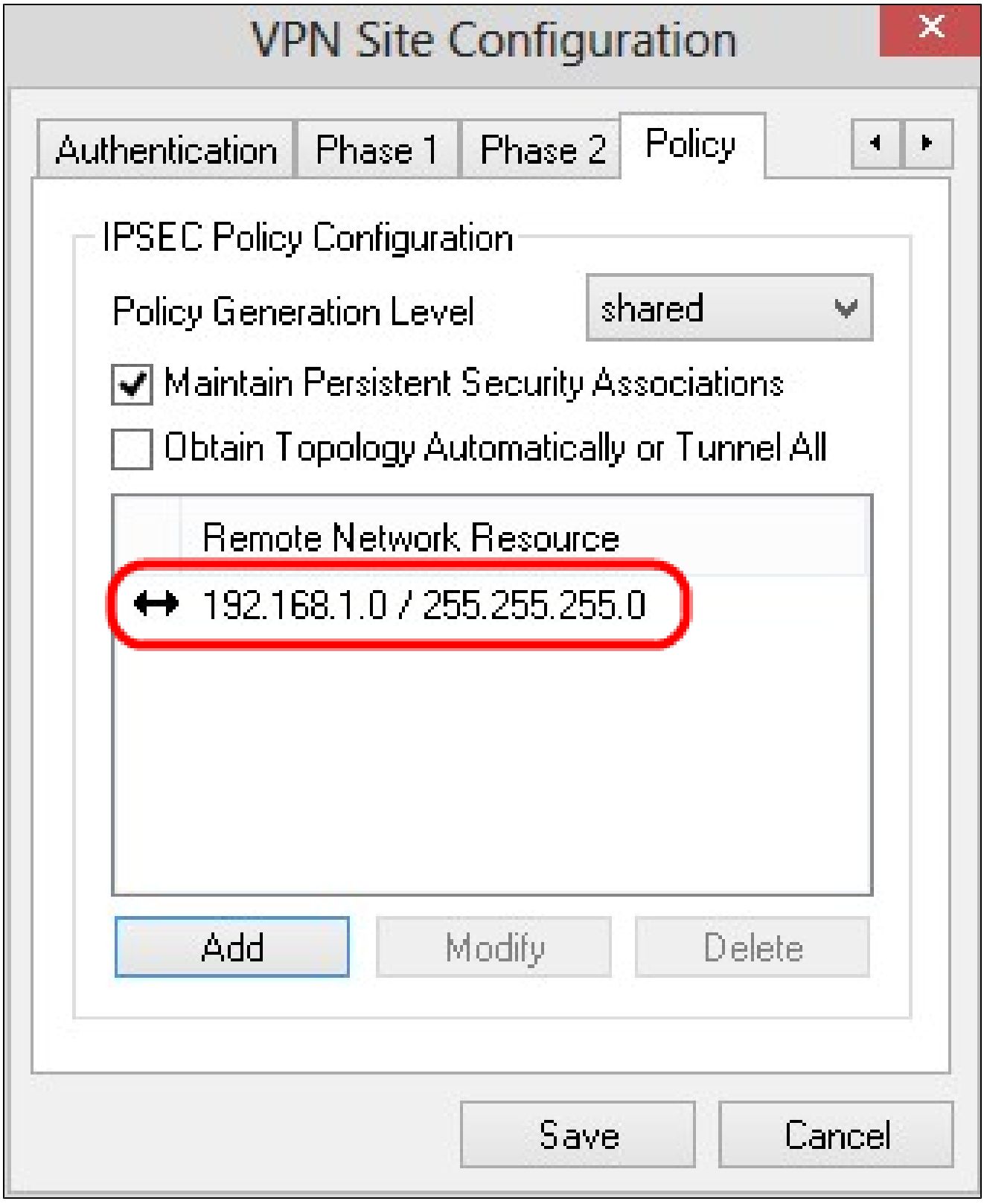


7단계. Address(주소) 필드에 RV0XX의 IP 주소를 입력합니다.

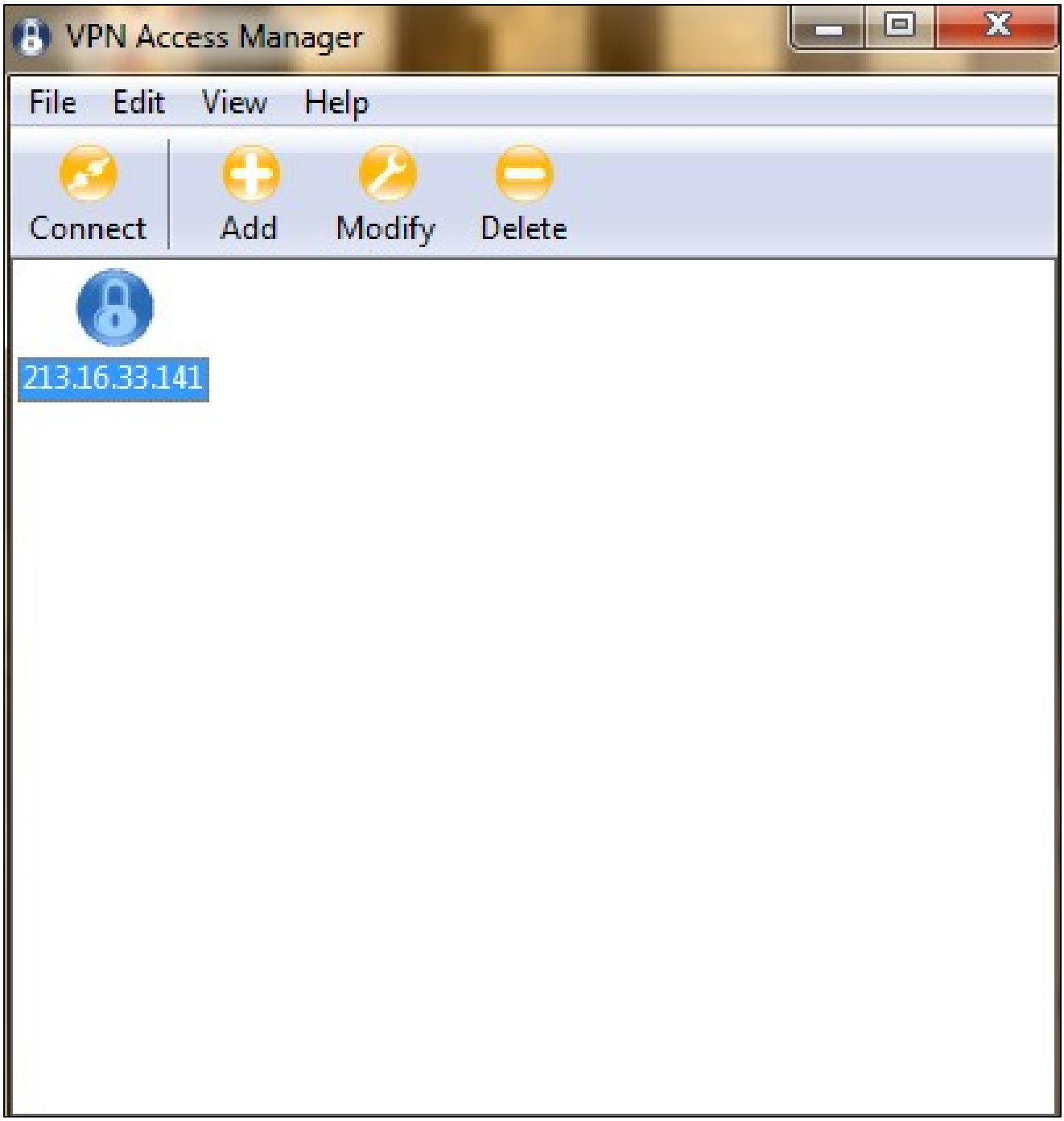
8단계. Netmask 필드에 디바이스의 서브넷 마스크 주소를 입력합니다.



9단계. OK(확인)를 클릭합니다. RV0XX의 IP 주소 및 서브넷 마스크 주소가 Remote Network Resource(원격 네트워크 리소스) 목록에 표시됩니다.



10단계. Save(저장)를 클릭하면 새 VPN 연결이 표시된 VPN Access Manager 창으로 사용자를 되돌립니다.

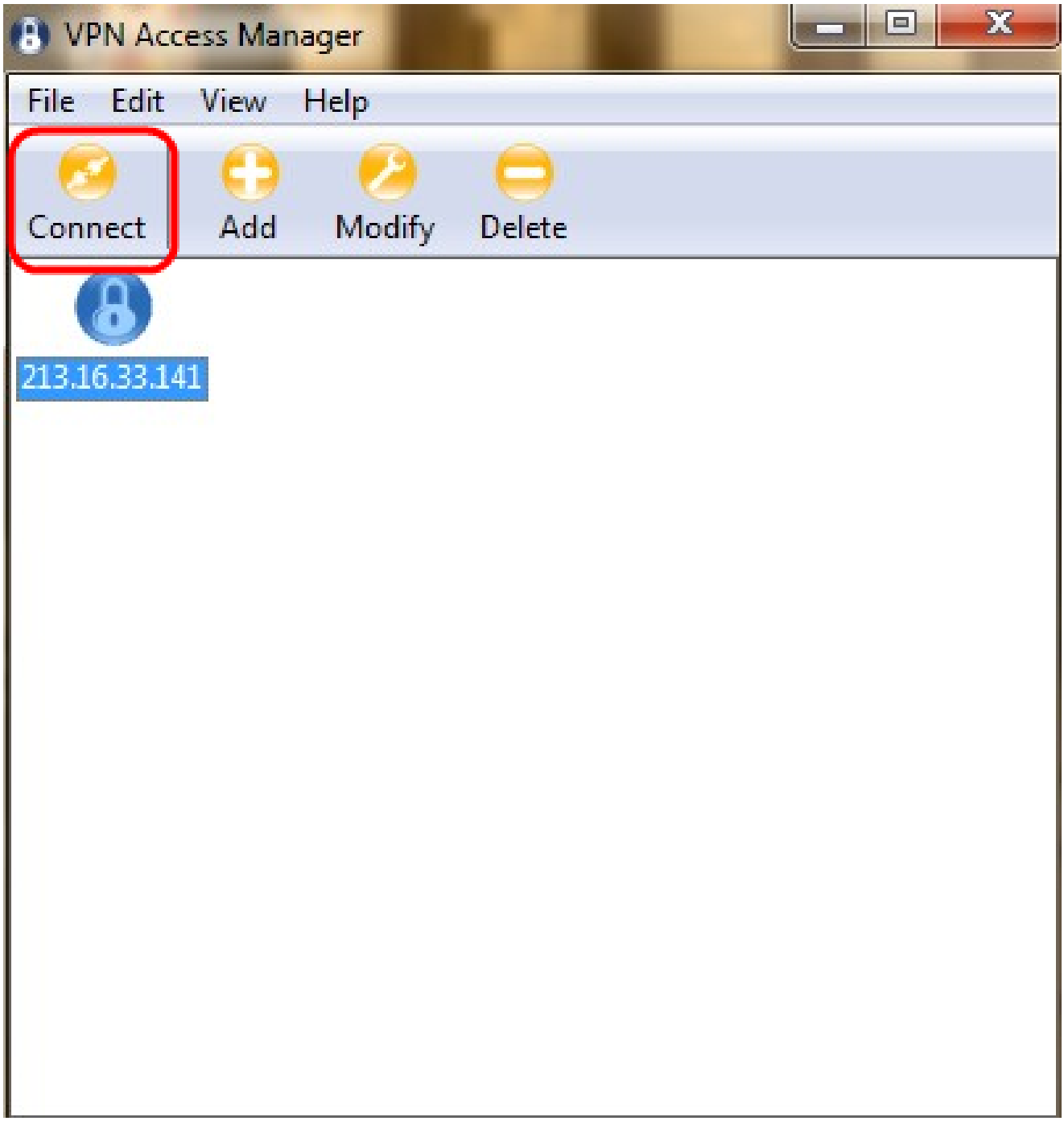


연결

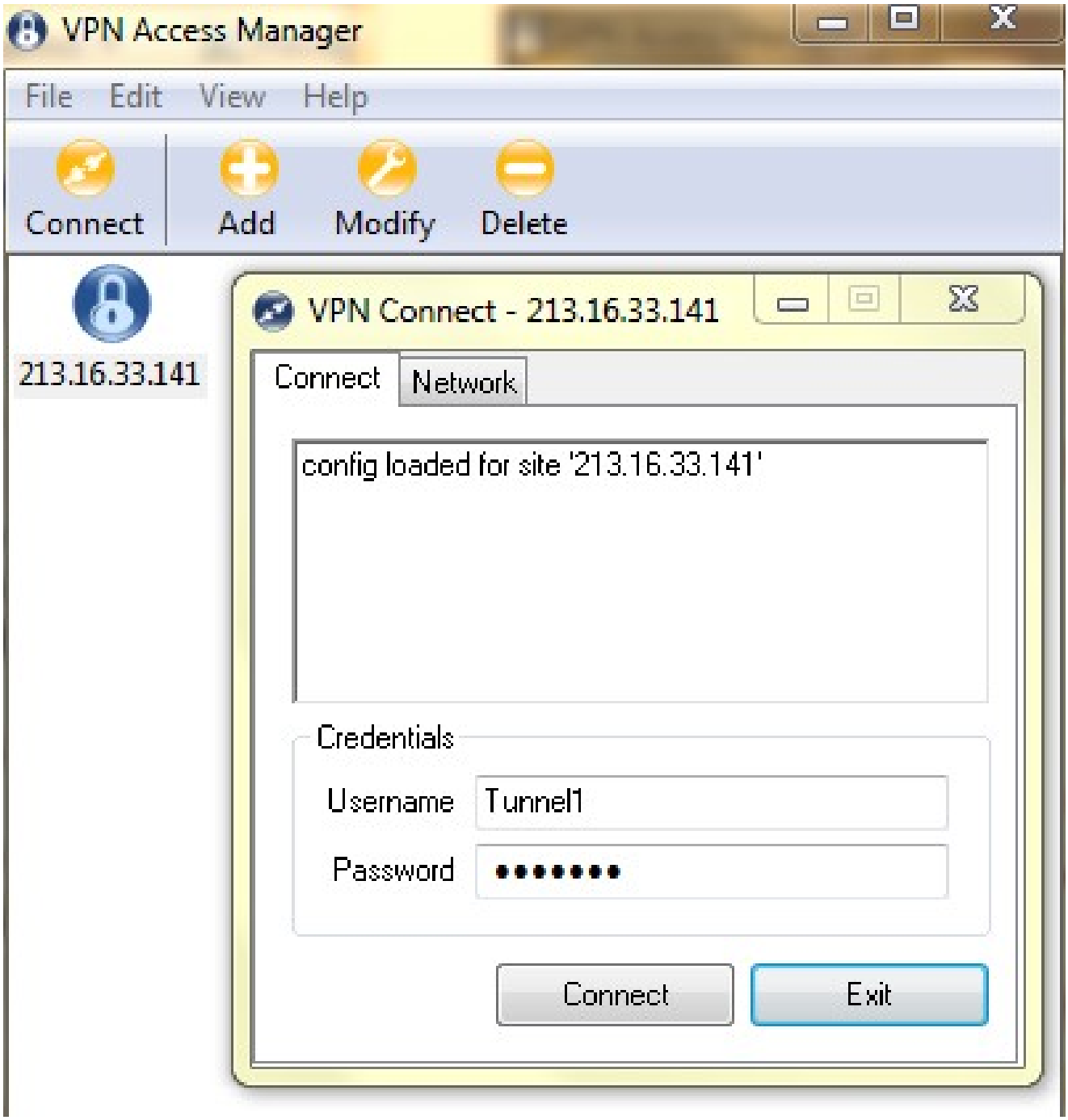
이 섹션에서는 모든 설정이 구성된 후 VPN 연결을 설정하는 방법에 대해 설명합니다. 필수 로그인 정보는 디바이스에 구성된 VPN 클라이언트 액세스와 동일합니다.

1단계. 원하는 VPN 연결을 클릭합니다.

2단계. 연결을 클릭합니다.



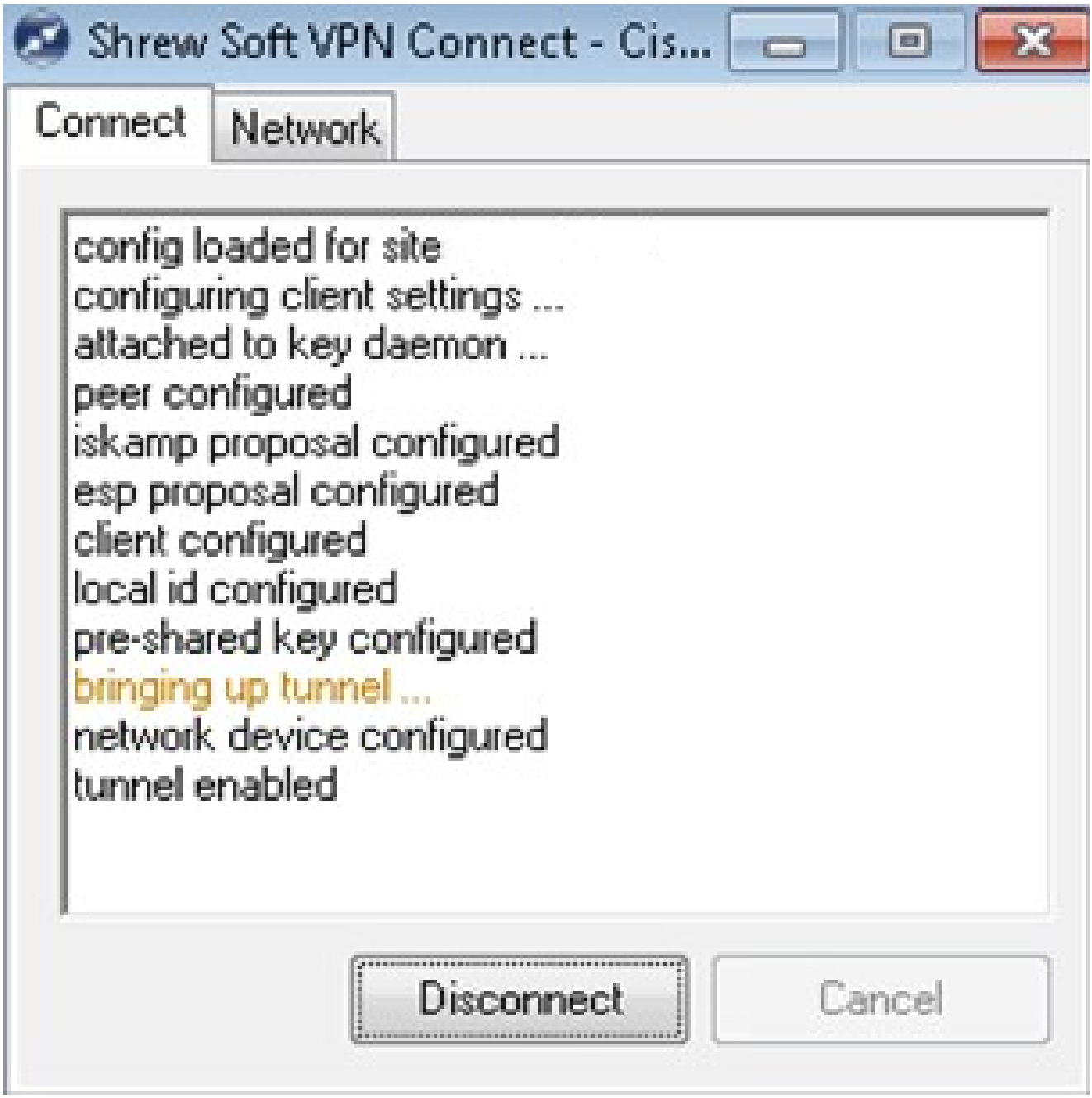
VPN Connect(VPN 연결) 창이 나타납니다.



3단계. Username(사용자 이름) 필드에 VPN의 사용자 이름을 입력합니다.

4단계. Password(비밀번호) 필드에 VPN 사용자 계정의 비밀번호를 입력합니다.

5단계. 연결을 클릭합니다. Monitoring Soft VPN Connect(Shrew 소프트 VPN 연결) 창이 나타납니다.



6단계(선택 사항) 연결을 비활성화하려면 Disconnect(연결 끊기)를 클릭합니다.

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.