RV34x Series 라우터에서 Client-to-Site VPN(Virtual Private Network) 연결 구성

목표

클라이언트-사이트 VPN(Virtual Private Network) 연결에서 인터넷의 클라이언트는 서버에 연결하여 서버 뒤에 있는 회사 네트워크 또는 LAN(Local Area Network)에 액세스할 수 있지만 네트워크 및 리소스의 보안을 유지합니다.이 기능은 개인 정보 보호 및 보안에 영향을 주지 않고 재택 근무자와 비즈니스 여행자가 VPN 클라이언트 소프트웨어를 사용하여 네트워크에 액세스할 수 있는 새로운 VPN 터널을 생성하므로 매우 유용합니다.

이 문서의 목적은 RV34x Series 라우터에서 Client-to-Site VPN 연결을 구성하는 방법을 보여주는 것입니다.

적용 가능한 디바이스

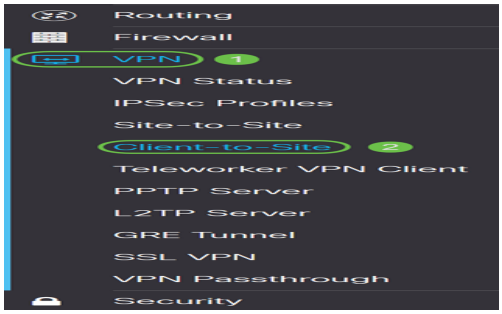
- RV34x 시리즈

소프트웨어 버전

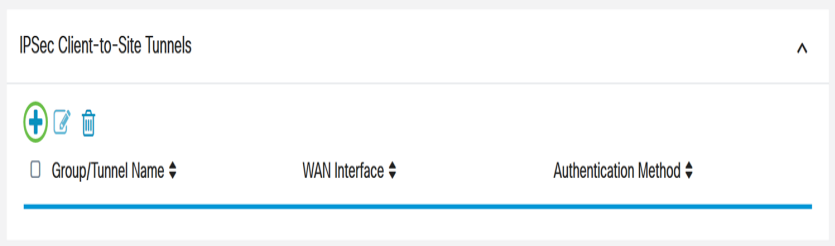
- 1.0.01.16

클라이언트-사이트 VPN 구성

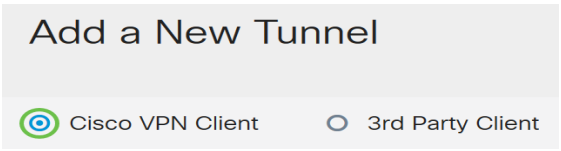
1단계. 라우터 웹 기반 유틸리티에 로그인하고 **VPN > Client-to-Site**를 선택합니다.



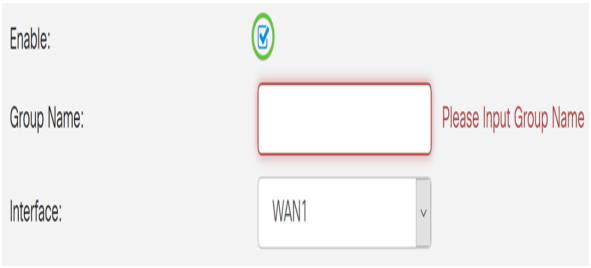
2단계. IPSec Client-to Site Tunnels 섹션 아래에서 **Add** 버튼을 클릭합니다.



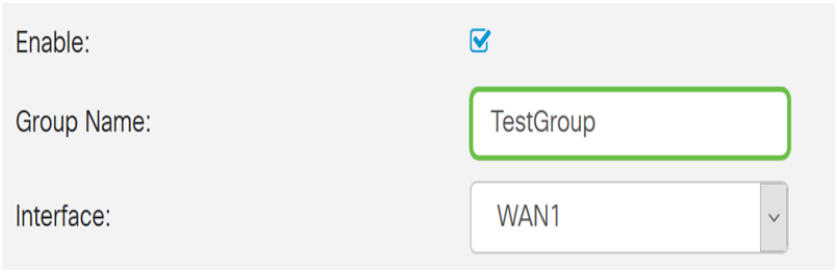
3단계. Add a *New Tunnel*(*새 터널 추가*) 영역에서 **Cisco VPN Client** 라디오 버튼을 클릭합니다.



4단계. **Enable** 확인란을 선택하여 컨피그레이션을 활성화합니다.



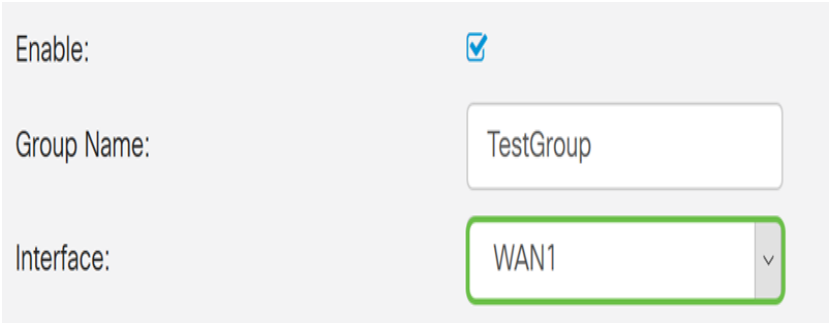
5단계. 제공된 필드에 그룹 이름을 입력합니다.이는 IKE(Internet Key Exchange) 협상 중에 이 그룹의 모든 구성원에 대한 식별자 역할을 합니다.



참고:A~Z 또는 0~9 사이의 문자를 입력합니다. 그룹 이름에는 공백과 특수 문자를 사용할 수 없습니다.이 예제에서는 TestGroup이 사용됩니다.

6단계. 드롭다운 목록을 클릭하여 인터페이스를 선택합니다.옵션은 다음과 같습니다.

- WAN1
- WAN2
- USB1
- USB2



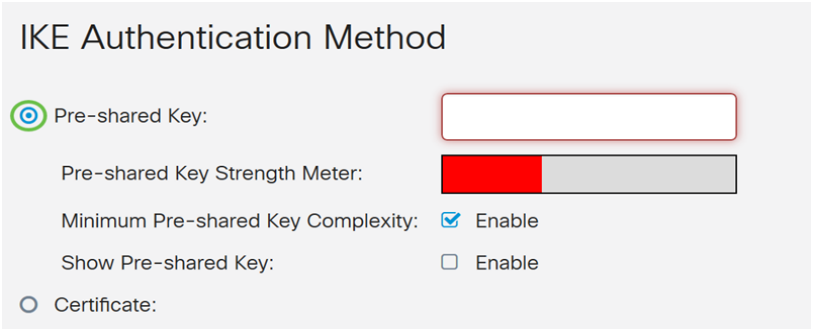
참고:이 예에서는 WAN1이 선택됩니다.이것이 기본 설정입니다.

7단계. IKE Authentication Method(IKE 인증 방법) 영역에서 IKE 기반 터널의 IKE 협상에 사용할 인증 방법을 선택합니다.옵션은 다음과 같습니다.

- 사전 공유 키 — IKE 피어는 사전 공유 키를 포함하는 키 해시를 컴퓨팅 및 전송하여 서로를 인증합니다.수신 피어가 Pre-shared 키를 사용하여 동일한 해시를 독립적으로 만들 수 있는 경우 두 피어가 동일한 암호를 공유해야 하므로 다른 피어를 인증해야 합니다.각 IPSec 피어는 세션을 설정하는 다른 피어의 사전 공유 키로 구성되어야 하므로 사전 공유

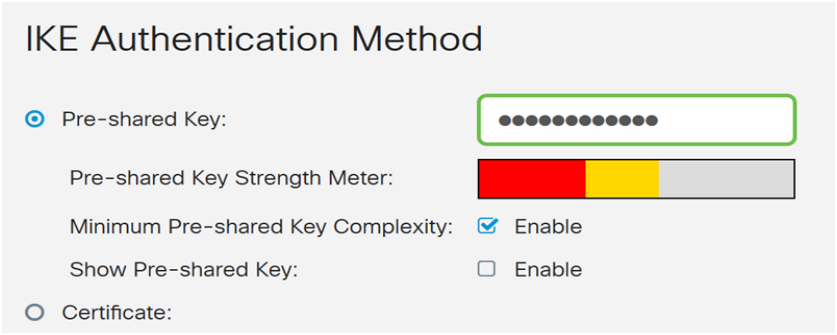
키는 제대로 확장되지 않습니다.

- 인증서 — 디지털 인증서는 전달자의 인증서 ID와 같은 정보를 포함하는 패키지입니다.이름 또는 IP 주소, 인증서의 일련 번호 만료 날짜 및 인증서 전달자의 공개 키 사본표준 디지털 인증서 형식은 X.509 사양에 정의되어 있습니다.X.509 버전 3은 인증서의 데이터 구조를 정의합니다.



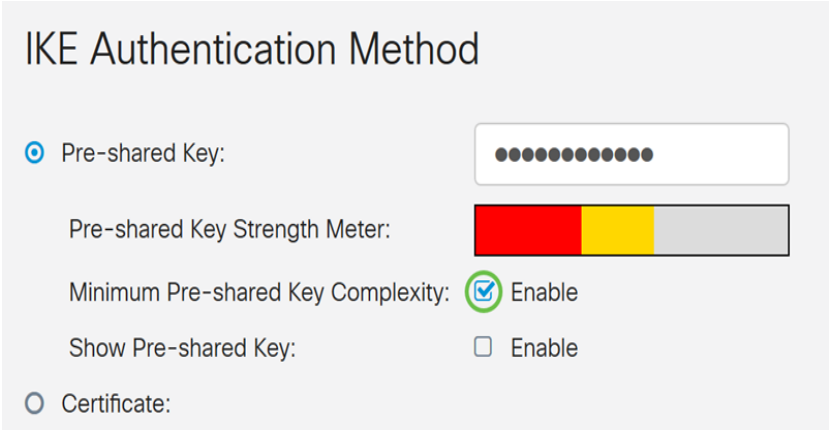
참고:이 예에서는 사전 공유 키가 선택됩니다.이것이 기본 설정입니다.

8단계. 제공된 필드에 사전 공유 키를 입력합니다.이는 IKE 피어 그룹 중 인증 키입니다.

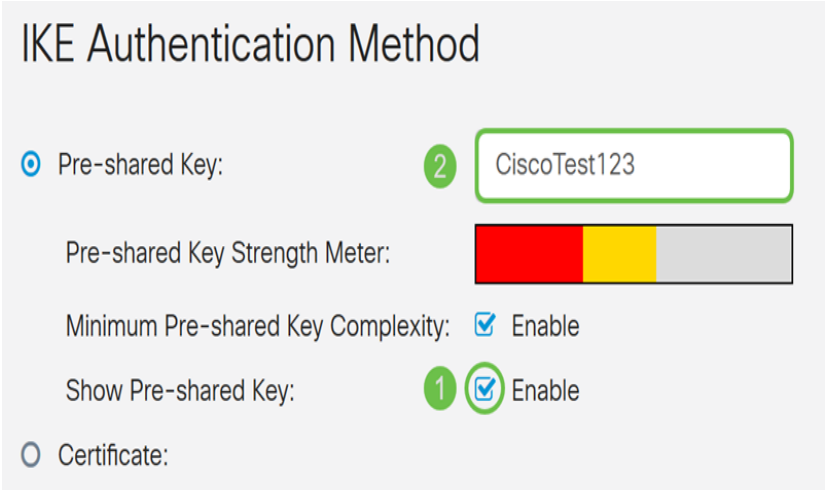


9단계. (선택 사항) Enable(활성화) 확인란을 선택하여 Minimum Pre-shared Key Complexity(사전 공유 키 복잡성 최소) Pre-shared Key Strength Meter를 보고 키의 강도를 확인합니다.키의 강도는 다음과 같이 정의됩니다.

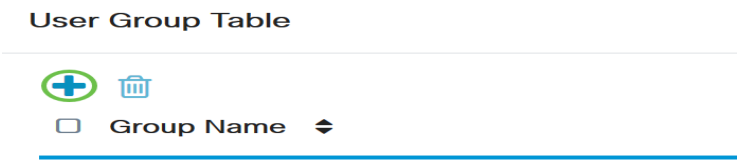
- 빨간색 - 암호가 약합니다.
- 주황색 - 비밀번호가 상당히 강력합니다.
- 녹색 — 암호가 강력합니다.



참고: Show *Pre-shared Key(사전 공유 키 표시)* 필드에서 Enable(활성화) 확인란을 선택하여 일반 텍스트로 비밀번호를 확인할 수 있습니다.

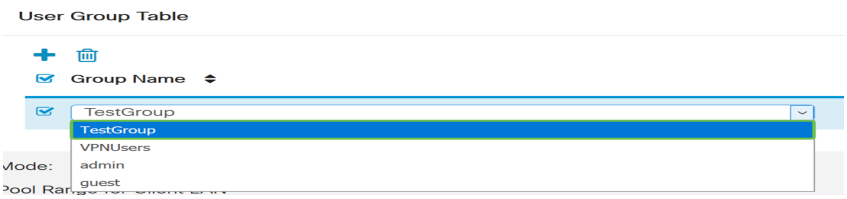


10단계. (선택 사항) User Group(사용자 그룹) 테이블에서 **더하기** 아이콘을 클릭하여 그룹을 추가합니다.



11단계(선택 사항) 드롭다운 목록에서 사용자 그룹이 관리자용인지 게스트용인지를 선택합니다.사용자 계정으로 사용자 그룹을 생성한 경우 선택할 수 있습니다.이 예제에서는 TestGroup을 선택하겠습니다.

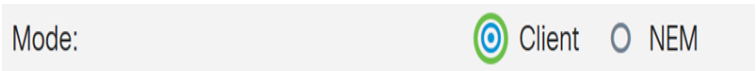
참고: TestGroup은 System Configuration(시스템 컨피그레이션) > User Groups(**사용자 그룹**)에서 생성한 사용자 **그룹입니다**.



참고:이 예제에서는 TestGroup을 선택합니다.사용자 그룹을 삭제하려면 사용자 그룹 옆의 상자를 선택한 다음 **삭제** 버튼을 클릭할 수도 있습니다.

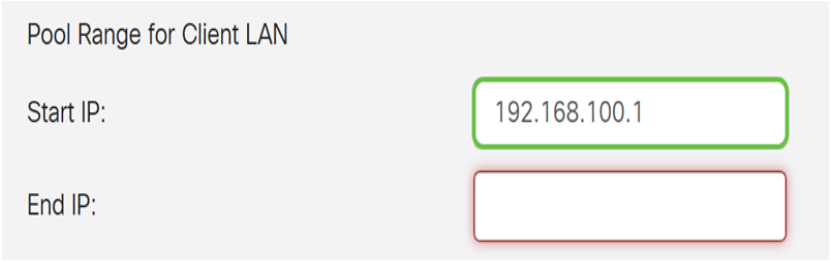
12단계. 라디오 버튼을 클릭하여 모드를 선택합니다.옵션은 다음과 같습니다.

- 클라이언트 — 이 옵션을 사용하면 클라이언트가 IP 주소를 요청할 수 있으며 서버는 구성된 주소 범위의 IP 주소를 제공합니다.
- NEM(Network Extension Mode) — 이 옵션을 사용하면 클라이언트가 서버 뒤에 있는 LAN 및 클라이언트가 제안하는 서브넷 간 트래픽에 VPN 서비스를 적용해야 하는 서브넷을 제안할 수 있습니다.



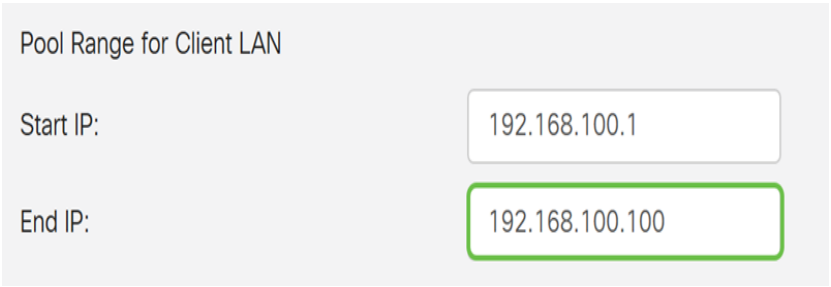
참고:이 예에서는 Client가 선택됩니다.

13단계. 시작 *IP* 필드에 시작 IP 주소를 입력합니다.이는 풀에 있는 첫 번째 IP 주소로서 클라이언트에 할당할 수 있습니다.



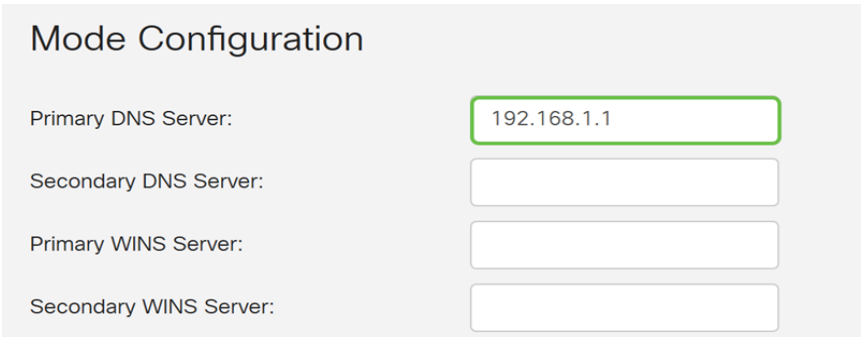
참고:이 예에서는 192.168.100.1이 사용됩니다.

14단계. End *IP* 필드에 끝 IP 주소를 입력합니다.이는 클라이언트에 할당할 수 있는 풀의 마지막 IP 주소입니다.



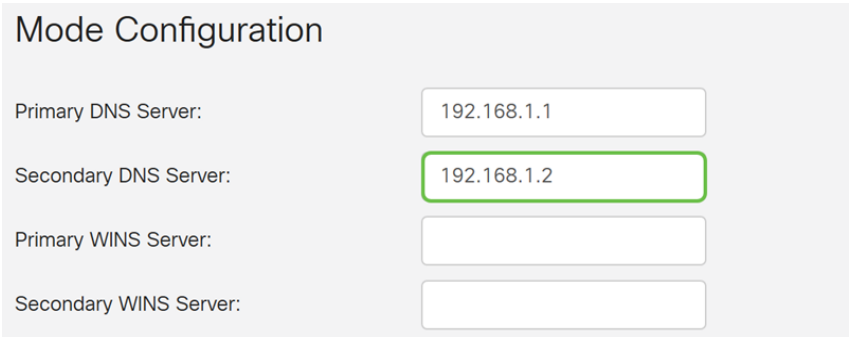
참고:이 예에서는 192.168.100.100이 사용됩니다.

15단계. (선택 사항) *Mode Configuration*(*모드 컨피그레이션*) 영역 아래 제공된 필드에 기본 DNS 서버의 IP 주소를 입력합니다.



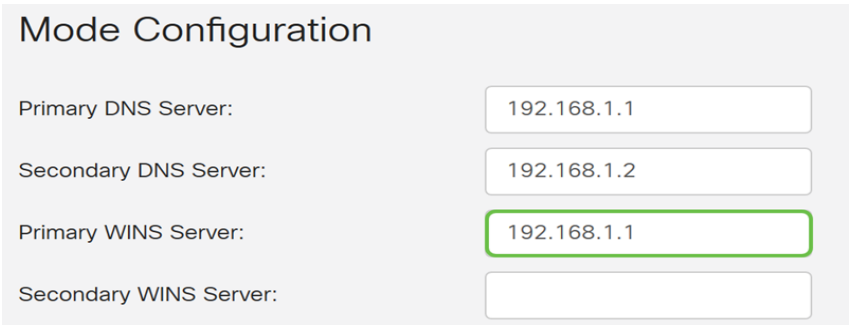
참고:이 예에서는 192.168.1.1이 사용됩니다.

16단계(선택 사항) 제공된 필드에 보조 DNS 서버의 IP 주소를 입력합니다.



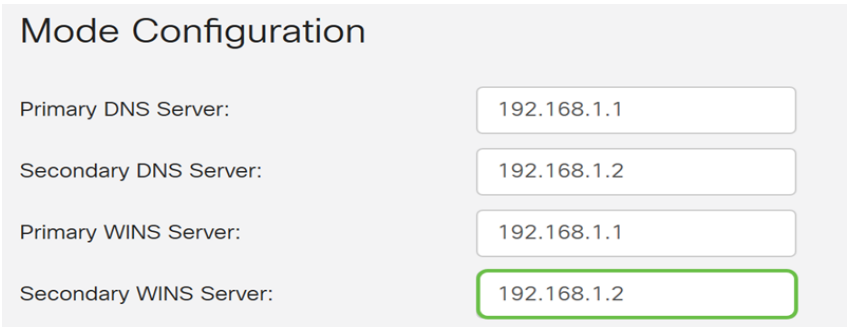
참고:이 예에서는 192.168.1.2이 사용됩니다.

17단계(선택 사항) 제공된 필드에 기본 WINS 서버의 IP 주소를 입력합니다.



참고:이 예에서는 192.168.1.1이 사용됩니다.

18단계(선택 사항) 제공된 필드에 보조 WINS 서버의 IP 주소를 입력합니다.

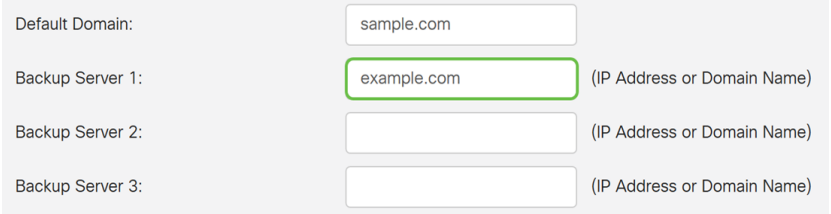


참고:이 예에서는 192.168.1.2이 사용됩니다.

19단계(선택 사항) 제공된 필드에 원격 네트워크에서 사용할 기본 도메인을 입력합니다.

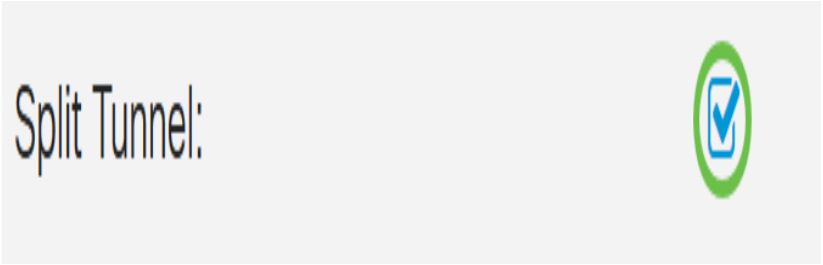
참고:이 예에서는 sample.com이 사용됩니다.

20단계. (선택 사항) *Backup Server 1* 필드에 백업 서버의 IP 주소 또는 도메인 이름을 입력합니다.기본 IPSec VPN 서버에 장애가 발생할 경우 디바이스가 VPN 연결을 시작할 수 있습니다.제공된 필드에 최대 3개의 백업 서버를 입력할 수 있습니다.Backup Server 1은 세 서버 중 우선 순위가 가장 높고 Backup Server 3은 가장 낮은 서버입니다.

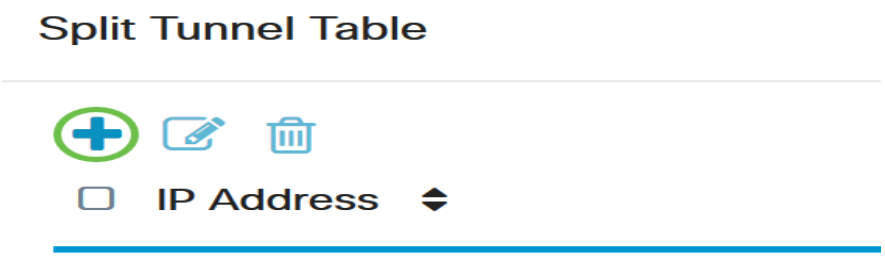


참고:이 예에서는 Example.com이 백업 서버 1에 사용됩니다.

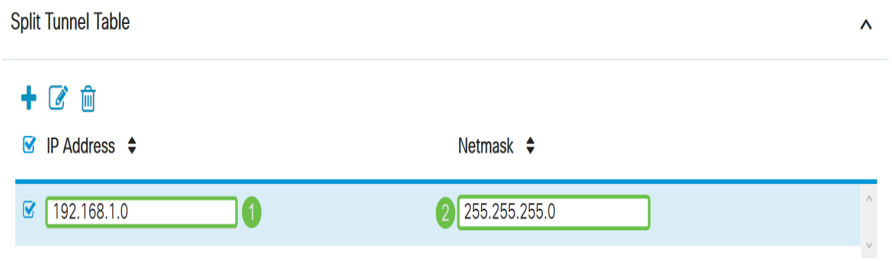
21단계. (선택 사항) Split **Tunnel** 확인란을 선택하여 스플릿 터널을 활성화합니다.스플릿 터널링을 사용하면 프라이빗 네트워크와 인터넷의 리소스에 동시에 액세스할 수 있습니다.



22단계(선택 사항) Split *Tunnel Table(터널 분할 테이블)* 아래에서 **더하기** 아이콘을 클릭하여 스플릿 터널의 IP 주소를 추가합니다.

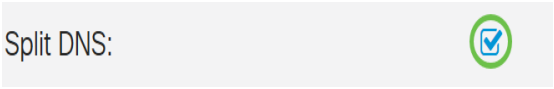


23단계(선택 사항) 제공된 필드에 스플릿 터널의 IP 주소와 넷마스크를 입력합니다.

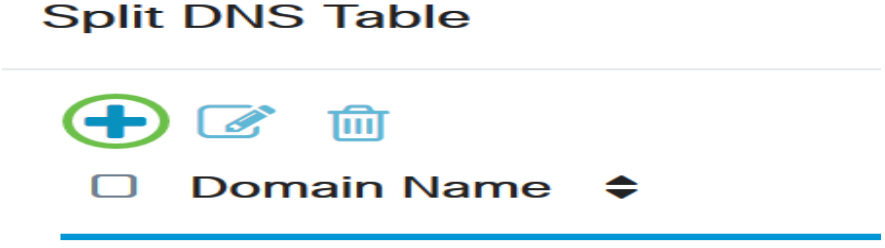


참고:이 예에서는 192.168.1.0 및 255.255.255.0이 사용됩니다.확인란을 선택하고 **Add**, **Edit** 및 **Delete** 버튼을 클릭하여 분할 터널을 각각 추가, 편집 또는 삭제할 수도 있습니다.

24단계. (선택 사항) **Split DNS** 확인란을 선택하여 스플릿 DNS를 활성화합니다.스플릿 DNS를 사용하면 내부 및 외부 네트워크에 대해 별도의 DNS 서버를 생성하여 네트워크 리소스의 보안 및 개인 정보를 유지할 수 있습니다.



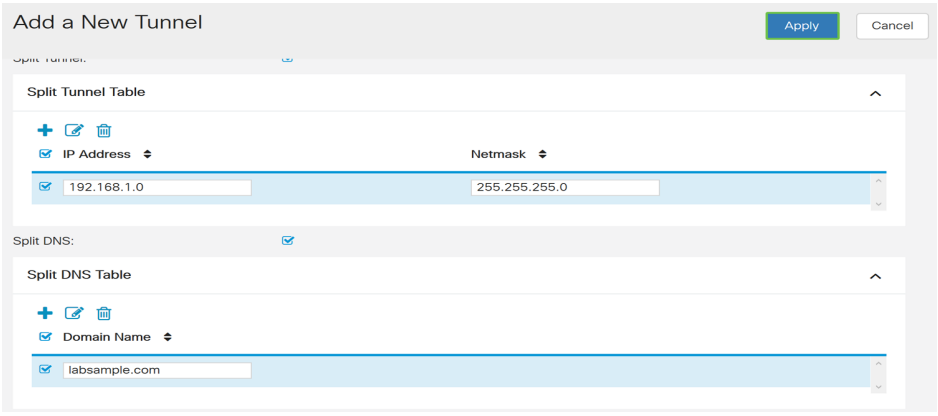
25단계. (선택 사항) *Split DNS Table(DNS 테이블 분할)*에서 **더하기** 아이콘을 클릭하여 스플릿 DNS에 대한 도메인 이름을 추가합니다.



26단계(선택 사항) 제공된 필드에 스플릿 DNS의 도메인 이름을 입력합니다.

참고:이 예에서는 labsample.com이 사용됩니다.확인란을 선택하고 **Add**, **Edit** 및 **Delete** 버튼을 클릭하여 분할 DNS를 각각 추가, 편집 또는 삭제할 수도 있습니다.

27단계. 적용을 **클릭합니다**.



결론

이제 RV34x Series 라우터에서 Client-to-Site 연결을 성공적으로 구성해야 합니다.

다음 항목에 대해 자세히 알아보려면 다음 문서를 클릭하십시오.

- RV34x Series 라우터에서 Teleworker VPN 클라이언트 구성
- GreenBow VPN 클라이언트를 사용하여 RV34x Series 라우터와 연결
- RV34x 라우터에서 VPN 클라이언트 설정을 위한 사용자 계정 생성
- RV34x 라우터에서 VPN 설정을 위한 사용자 그룹 생성

이 문서와 관련된 비디오 보기...

여기를 클릭하여 Cisco의 다른 기술 대화를 확인하십시오.