RV34x Series 라우터에서 AnyConnect VPN(Virtual Private Network) 연결 설정

목표

이 문서의 목적은 RV34x Series 라우터에서 AnyConnect VPN 연결을 구성하는 방법을 보여주는 것입니다.

AnyConnect Secure Mobility Client 사용의 장점:

1. 안전하고 지속적인 연결
2. 지속적인 보안 및 정책 시행
3. ASA(Adaptive Security Appliance) 또는 엔터프라이즈 소프트웨어 구축 시스템에서 구축 가능
4. 맞춤형 및 번역 가능
5. 손쉬운 구성
6. IPSec(Internet Protocol Security) 및 SSL(Secure Sockets Layer) 지원
7. IKEv2.0(Internet Key Exchange 버전 2.0) 프로토콜 지원

소개

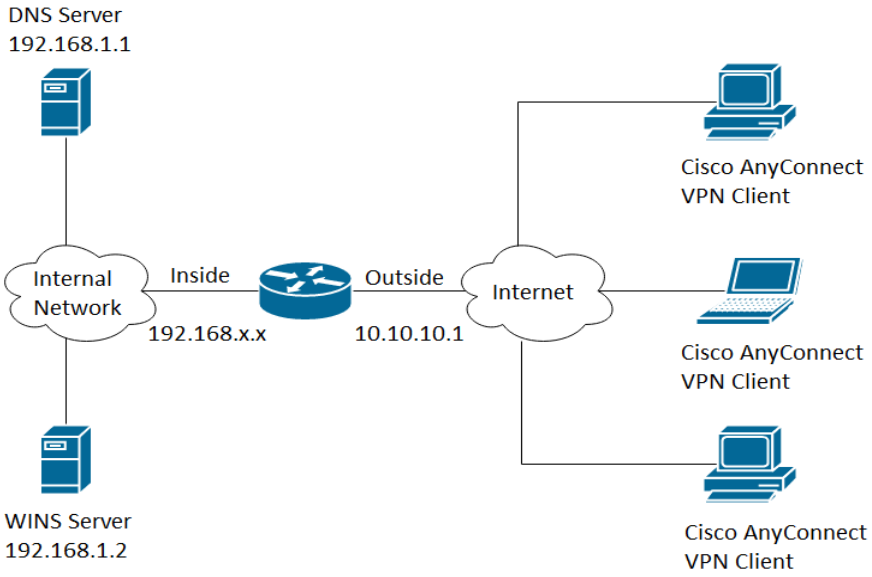
VPN(Virtual Private Network) 연결을 통해 사용자는 인터넷과 같은 공용 또는 공유 네트워크를 통해 사설 네트워크에서 데이터를 액세스하고 송수신할 수 있지만, 사설 네트워크와 리소스를 보호하기 위해 기본 네트워크 인프라에 대한 보안 연결은 여전히 보장됩니다.

VPN 클라이언트는 원격 네트워크에 연결하려는 컴퓨터에 설치되어 실행되는 소프트웨어입니다. 이 클라이언트 소프트웨어는 IP 주소 및 인증 정보와 같은 VPN 서버의 구성과 동일한 구성으로 설정해야 합니다. 이 인증 정보에는 데이터를 암호화하는 데 사용할 사용자 이름 및 사전 공유 키가 포함됩니다. 연결할 네트워크의 물리적 위치에 따라 VPN 클라이언트는 하드웨어 디바이스가 될 수도 있습니다. 이는 일반적으로 VPN 연결을 사용하여 서로 다른 위치에 있는 두 네트워크를 연결하는 경우에 발생합니다.

Cisco AnyConnect Secure Mobility Client는 다양한 운영 체제 및 하드웨어 구성에서 작동하는 VPN에 연결하기 위한 소프트웨어 애플리케이션입니다. 이 소프트웨어 애플리케이션은 사용자가 자신의 네트워크에 직접 연결된 것처럼 다른 네트워크의 원격 리소스에 액세스 할 수 있지만 안전한 방법으로. Cisco AnyConnect Secure Mobility Client는 컴퓨터 기반 또는 스마트폰 플랫폼에서 모바일 사용자를 보호할 수 있는 혁신적인 새로운 방법을 제공하여 최종 사용자에게 더욱 원활하고 항상 보호되는 환경을 제공하고 IT 관리자에게 포괄적인 정책 적용을 제공합니다.

RV34x 라우터에서 펌웨어 버전 1.0.3.15부터 시작하여 계속 진행하면 AnyConnect 라이센싱이 필요하지 않습니다. 클라이언트 라이센스에만 요금이 부과됩니다.

RV340 Series 라우터의 AnyConnect 라이센싱에 대한 자세한 내용은 RV340 Series 라우터의 AnyConnect Licensing 문서를 참조하십시오.



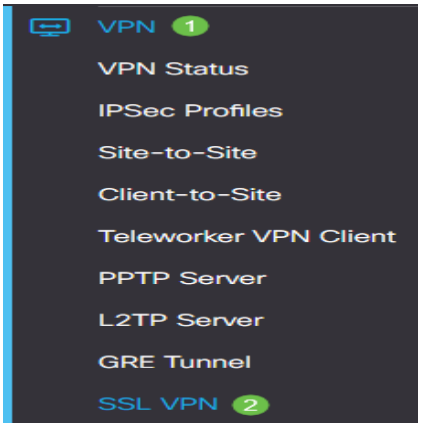
적용 가능한 장치 | 펌웨어 버전

- Cisco AnyConnect Secure Mobility Client | 4.4(최신 다운로드)
- RV34x Series | 1.0.03.15 (최신 다운로드)

RV34x에서 AnyConnect VPN 연결 구성

RV34x에서 SSL VPN 구성

1단계. 라우터 웹 기반 유틸리티에 액세스하고 **VPN > SSL VPN을 선택합니다**.



2단계. Cisco SSL VPN **Server**를 활성화하려면 On 라디오 버튼을 클릭합니다.

필수 게이트웨이 설정

다음 컨피그레이션 설정은 필수입니다.

3단계. 드롭다운 목록에서 게이트웨이 인터페이스를 선택합니다. 이 포트는 SSL VPN 터널을 통해 트래픽을 전달하는 데 사용됩니다. 옵션은 다음과 같습니다.

- WAN1
- WAN2
- USB1
- USB2

참고: 이 예에서는 WAN1이 선택됩니다.

4단계. SSL VPN 게이트웨이에 사용되는 포트 번호를 Gateway Port(게이트웨이 포트) *필드*에 1~65535 범위의 포트 번호를 입력합니다.

참고: 이 예에서는 8443이 포트 번호로 사용됩니다.

5단계. 드롭다운 목록에서 인증서 파일을 선택합니다. 이 인증서는 SSL VPN 터널을 통해 네트워크 리소스에 액세스하려는 사용자를 인증합니다. 드롭다운 목록에는 기본 인증서 및 가져온 인증서가 포함됩니다.

참고: 이 예에서는 기본값이 선택됩니다.

6단계. Client Address Pool 필드에 클라이언트 주소 풀의 IP 주소를 입력합니다. 이 풀은 원격 VPN 클라이언트에 할당될 IP 주소의 범위가 됩니다.

참고: IP 주소 범위가 로컬 네트워크의 IP 주소와 겹치지 않는지 확인하십시오.

참고: 이 예에서는 192.168.0.0이 사용됩니다.

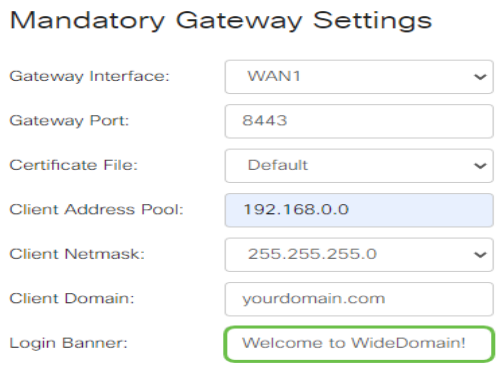
7단계. 드롭다운 목록에서 클라이언트 넷마스크를 선택합니다.

참고: 이 예제에서는 255.255.255.128을 선택합니다.

8단계. Client Domain(클라이언트 도메인) 필드에 *클라이언트 도메인 이름을* 입력합니다. SSL VPN 클라이언트에 푸시해야 하는 도메인 이름입니다.

참고: 이 예에서는 WideDomain.com이 클라이언트 도메인 이름으로 사용됩니다.

9단계. Login Banner(로그인 배너) 필드에 로그인 배너로 표시될 *텍스트를* 입력합니다. 이 배너는 클라이언트가 로그인할 때마다 표시됩니다.

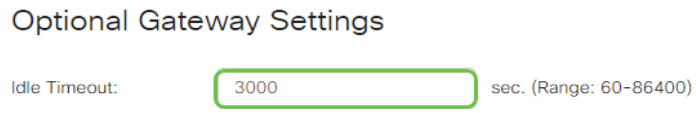


참고: 이 예에서는 Welcome to Widedomain!이 로그인 배너로 사용됩니다.

선택적 게이트웨이 설정

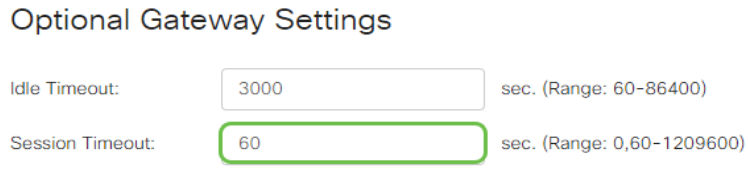
다음 컨피그레이션 설정은 선택 사항입니다.

1단계. 60~86400 범위의 유휴 시간 제한 값을 초 단위로 입력합니다. SSL VPN 세션이 유휴 상태로 유지될 수 있는 기간입니다.



참고: 이 예에서는 3000이 사용됩니다.

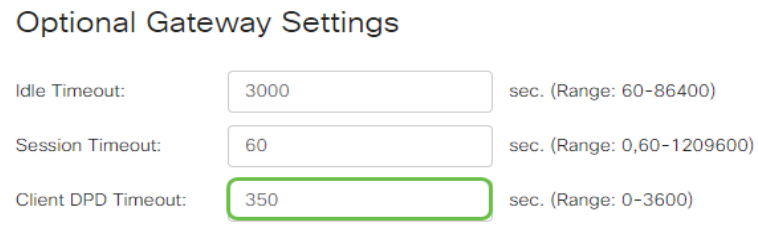
2단계. Session Timeout 필드에 값(초)을 입력합니다. 지정된 유휴 시간 이후에 TCP(Transmission Control Protocol) 또는 UDP(User Datagram Protocol) 세션이 시간 초과되는 데 걸리는 시간입니다. 범위는 60~1209600입니다.



참고: 이 예에서는 60이 사용됩니다.

3단계. ClientDPD Timeout(ClientDPD 시간 제한) 필드에 0~3600 범위의 값을 초 단위로 입력합니다. 이 값은 VPN 터널의 상태를 확인하기 위해 HELLO/ACK 메시지를 정기적으로 전송하도록 지정합니다.

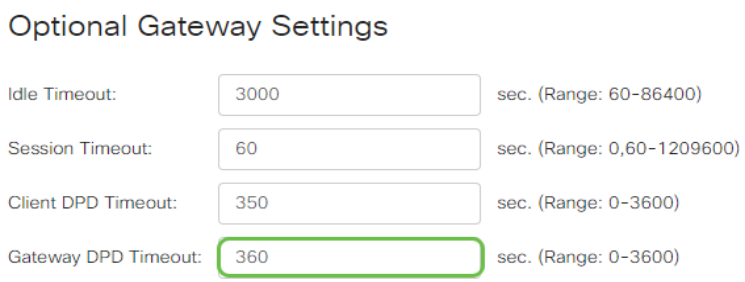
참고: 이 기능은 VPN 터널의 양쪽 끝에서 활성화해야 합니다.



참고: 이 예에서는 350이 사용됩니다.

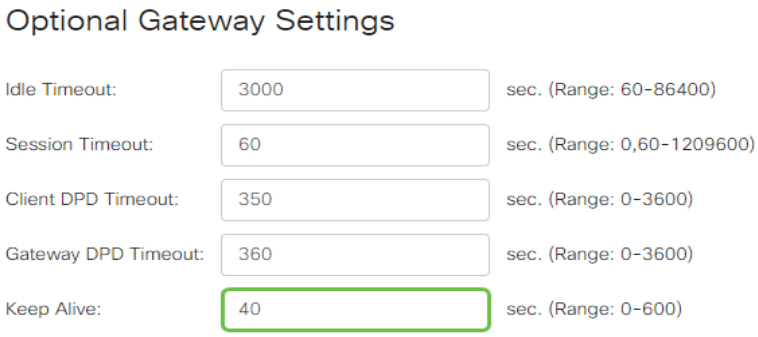
4단계. GatewayDPD Timeout(GatewayDPD 시간 제한) 필드에 0~3600 범위의 값을 초 단위로 입력합니다. 이 값은 VPN 터널의 상태를 확인하기 위해 HELLO/ACK 메시지를 정기적으로 전송하도록 지정합니다.

참고: 이 기능은 VPN 터널의 양쪽 끝에서 활성화해야 합니다.



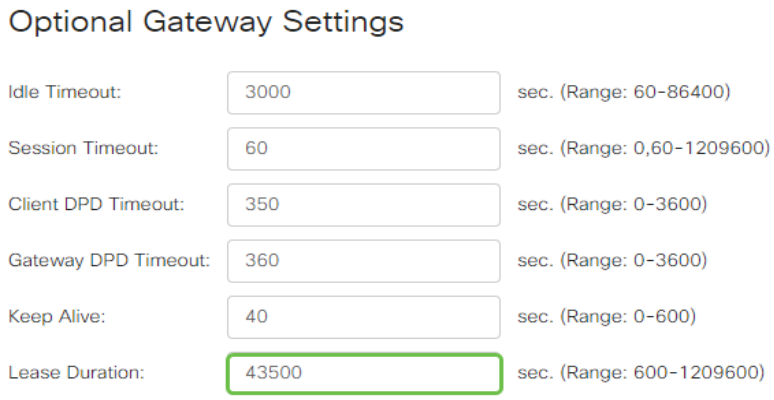
참고: 이 예에서는 360이 사용됩니다.

5단계. Keep Alive 필드에 0~600 *범위*의 값을 초 단위로 입력합니다. 이 기능을 사용하면 라우터가 항상 인터넷에 연결됩니다. 삭제된 경우 VPN 연결을 다시 설정하려고 시도합니다.



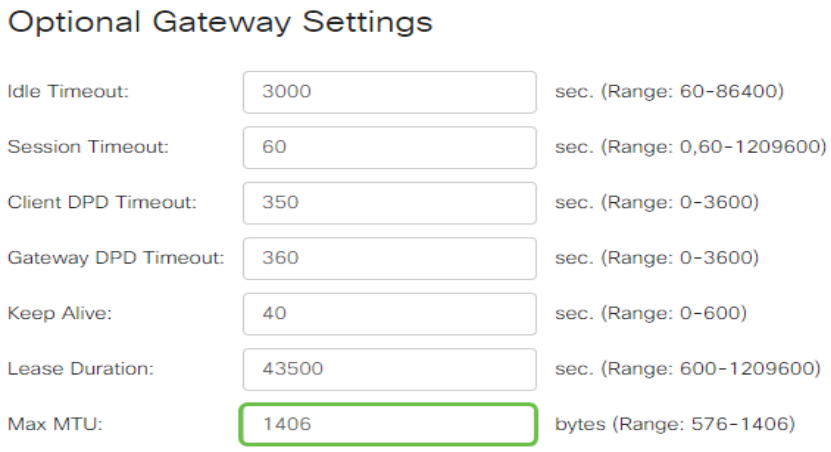
참고: 이 예에서는 40이 사용됩니다.

6단계. *Lease Duration(리*스 기간) 필드에 연결할 터널 기간의 값(초)을 입력합니다. 범위는 600~1209600입니다.



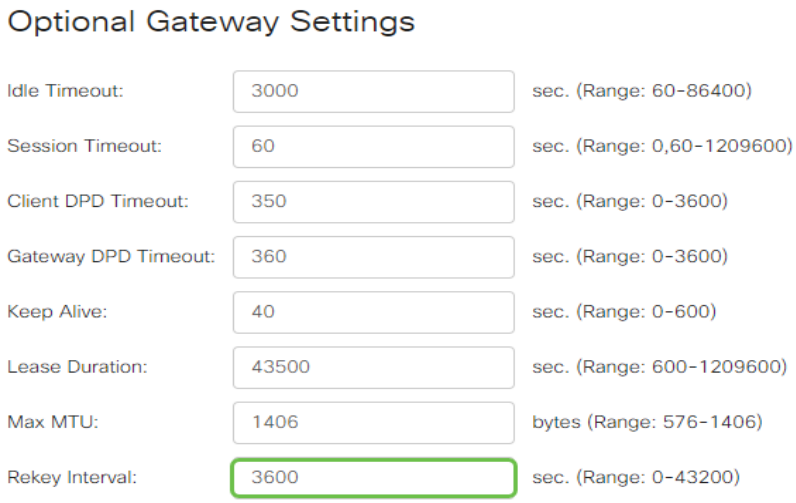
참고: 이 예에서는 43500이 사용됩니다.

7단계. 네트워크를 통해 전송할 수 있는 패킷 크기를 바이트 단위로 입력합니다. 범위는 576~1406입니다.



참고: 이 예에서는 1406이 사용됩니다.

8단계. Rekey Interval 필드에 릴레이 간격 *시간을* 입력합니다. Rekey 기능을 사용하면 세션이 설정된 후 SSL 키를 재협상할 수 있습니다. 범위는 0~43200입니다.

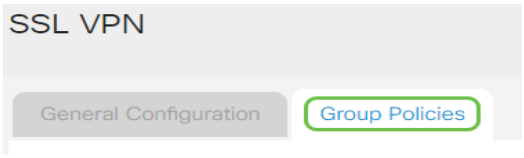


참고: 이 예에서는 3600이 사용됩니다.

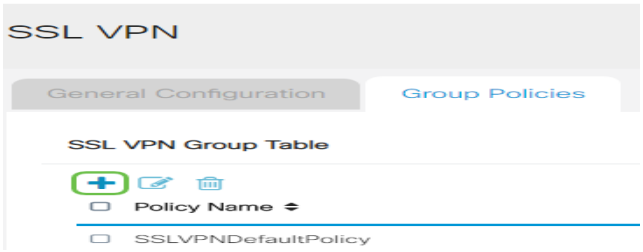
9단계. Apply를 **클릭합니다**.

그룹 정책 구성

1단계. Group Policies(**그룹 정책) 탭**을 클릭합니다.



2단계. SSL VPN Group Table(SSL VPN 그룹 테이블) 아래의 Add(추가) 버튼을 클릭하여 그룹 정책을 추가합니다.

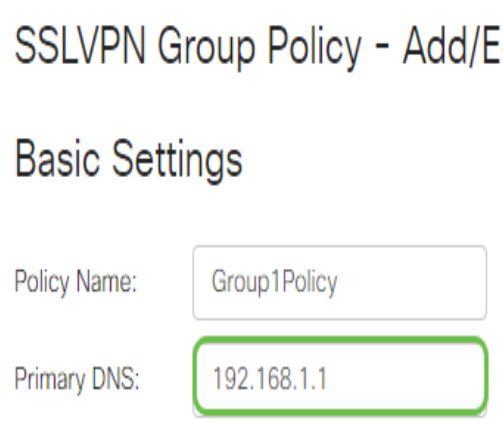


참고: SSL VPN Group(SSL VPN 그룹) 테이블에는 디바이스의 그룹 정책 목록이 표시됩니다. 목록의 첫 번째 그룹 정책(SSLVPNDefaultPolicy)을 수정할 수도 있습니다. 이는 디바이스에서 제공하는 기본 정책입니다.

3단계. Policy Name(정책 이름) 필드에 원하는 *정책 이름을* 입력합니다.

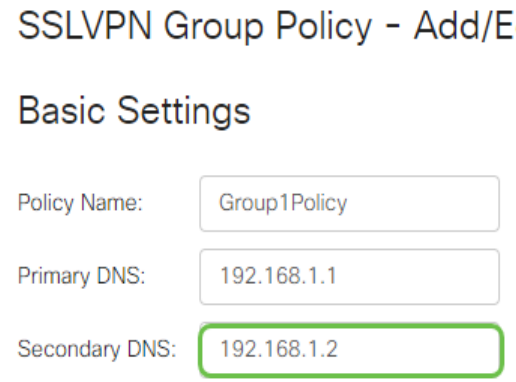
참고: 이 예에서는 그룹 1 정책이 사용됩니다.

4단계. 제공된 필드에 기본 DNS의 IP 주소를 입력합니다. 기본적으로 이 IP 주소는 이미 제공됩니다.



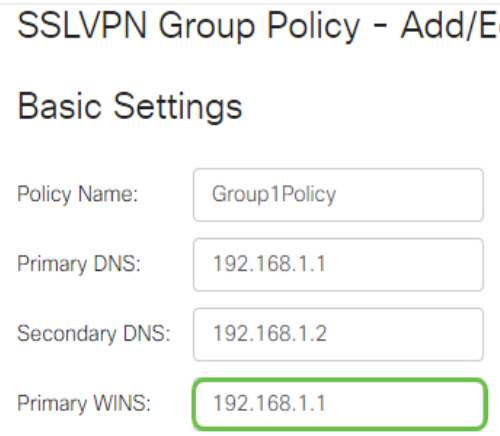
참고: 이 예에서는 192.168.1.1이 사용됩니다.

5단계. (선택 사항) 제공된 필드에 보조 DNS의 IP 주소를 입력합니다. 이는 기본 DNS가 실패할 경우 백업 역할을 합니다.



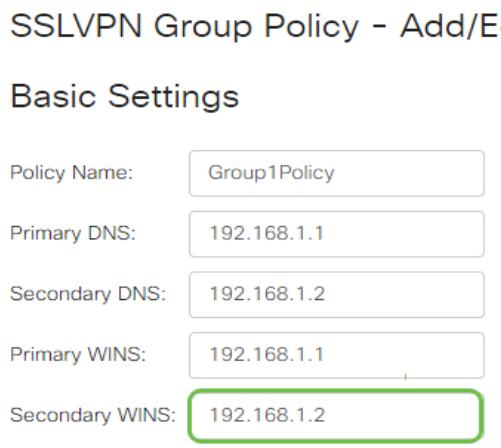
참고: 이 예에서는 192.168.1.2가 사용됩니다.

6단계. (선택 사항) 제공된 필드에 기본 WINS의 IP 주소를 입력합니다.



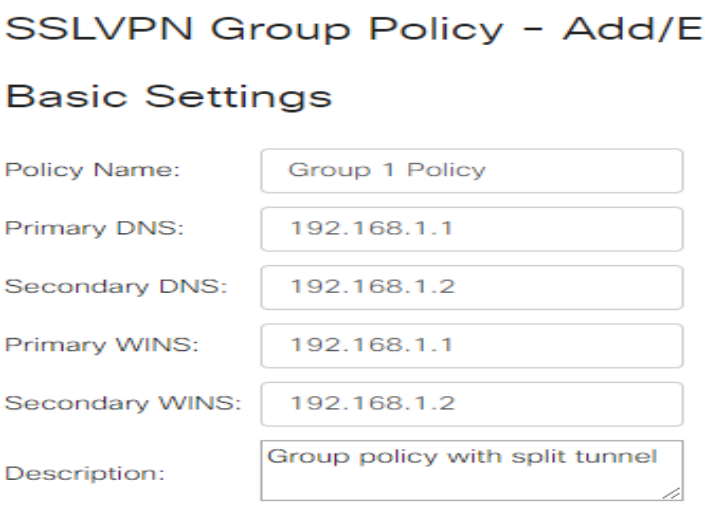
참고: 이 예에서는 192.168.1.1이 사용됩니다.

7단계. (선택 사항) 제공된 필드에 보조 WINS의 IP 주소를 입력합니다.



참고: 이 예에서는 192.168.1.2가 사용됩니다.

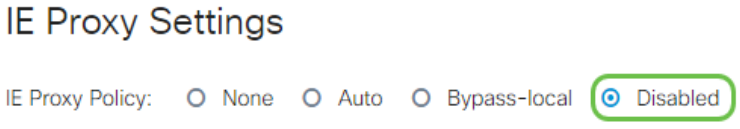
8단계. (선택 사항) Description(설명) 필드에 정책에 대한 *설명을* 입력합니다.



참고: 이 예에서는 스플릿 터널이 있는 그룹 정책이 사용됩니다.

9단계. (선택 사항) 라디오 버튼을 클릭하여 IE 프록시 정책을 선택하여 MSIE(Microsoft Internet Explorer) 프록시 설정에서 VPN 터널을 설정하도록 활성화합니다. 옵션은 다음과 같습니다.

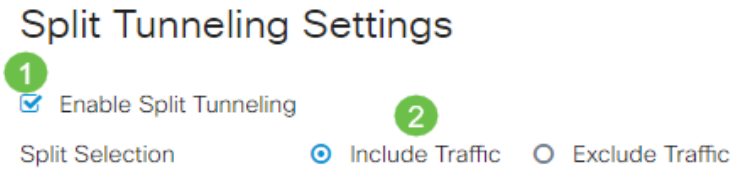
- None(없음) - 브라우저에서 프록시 설정을 사용하지 않도록 허용합니다.
- Auto(자동) - 브라우저에서 프록시 설정을 자동으로 탐지할 수 있습니다.
- Bypass-local - 브라우저가 원격 사용자에 구성된 프록시 설정을 우회하도록 허용합니다.
- Disabled(비활성화됨) - MSIE 프록시 설정을 비활성화합니다.



참고: 이 예에서는 Disabled(비활성화됨)가 선택됩니다. 이것이 기본 설정입니다.

10단계(선택 사항) Split Tunneling Settings(스플릿 터널링 설정) 영역에서 Enable **Split Tunneling(스플릿 터널링 활성화**) 확인란을 선택하여 인터넷으로 향하는 트래픽을 암호화되지 않고 직접 인터넷으로 전송하도록 허용합니다. 전체 터널링은 모든 트래픽을 최종 디바이스로 보낸 다음 이를 대상 리소스로 라우팅하여 웹 액세스 경로에서 기업 네트워크를 제거합니다.

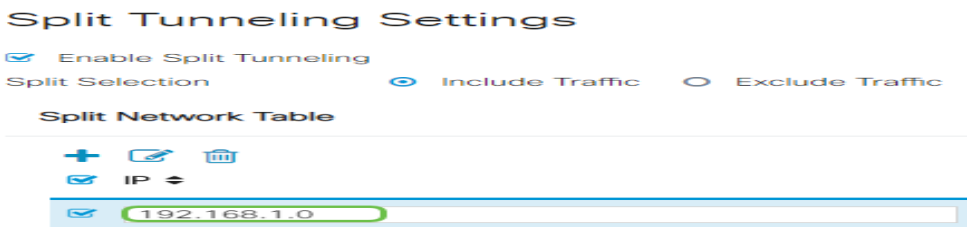
11단계. (선택 사항) 라디오 버튼을 클릭하여 스플릿 터널링을 적용할 때 트래픽을 포함할지 또는 제외할지를 선택합니다.



참고: 이 예에서는 Include Traffic이 선택됩니다.

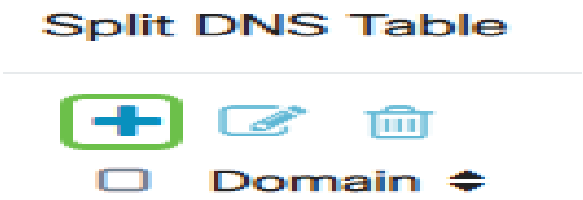
12단계. Split Network Table(스플릿 네트워크 테이블)에서 Add(추가) **버튼**을 클릭하여 스플릿 네트워크 예외를 추가합니다.

13단계. 제공된 필드에 네트워크의 IP 주소를 입력합니다.



참고: 이 예에서는 192.168.1.0이 사용됩니다.

14단계. Split DNS Table(스플릿 DNS 테이블)에서 **Add(추가)** 버튼을 클릭하여 스플릿 DNS 예외를 추가합니다.

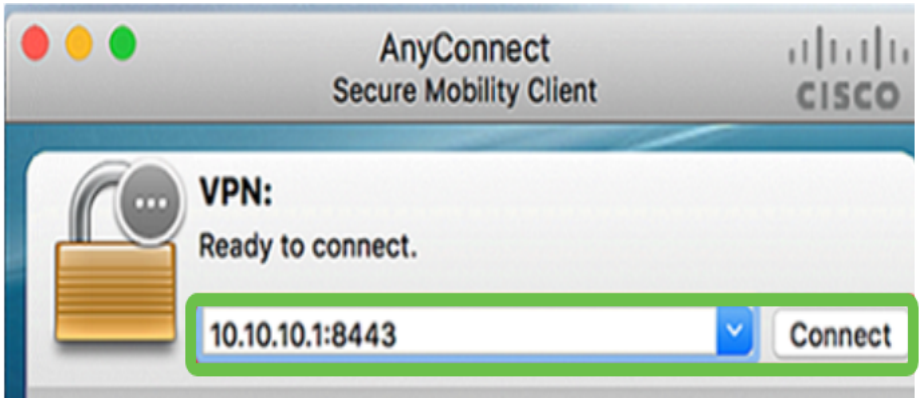


15단계. 제공된 필드에 도메인 이름을 입력한 다음 Apply(적용)를 **클릭합니다**.

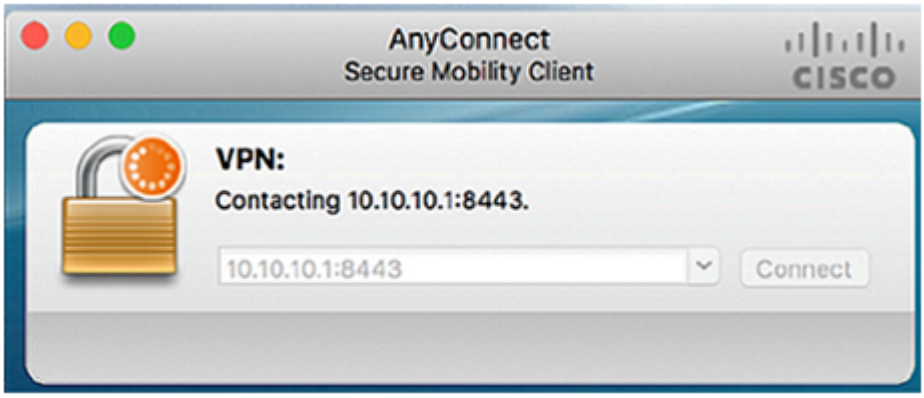
AnyConnect VPN 연결 확인

1단계. AnyConnect **Secure Mobility Client 아이콘을** 클릭합니다.

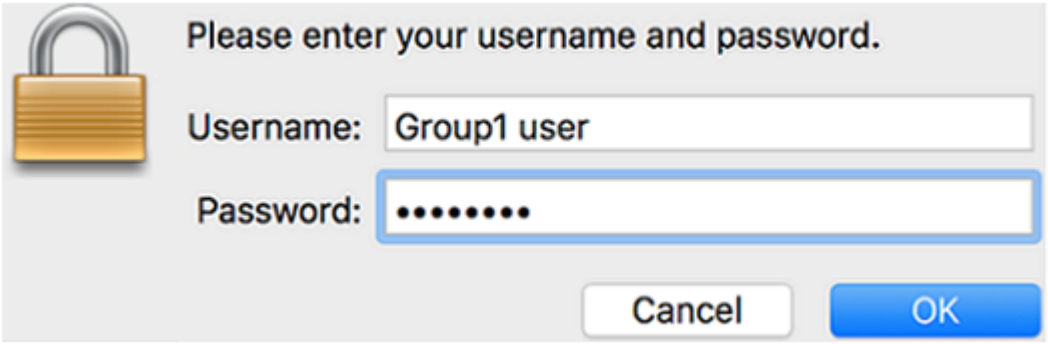
2단계. AnyConnect Secure Mobility Client(AnyConnect Secure Mobility Client) 창에서 콜론(:)으로 구분된 게이트웨이 IP 주소 및 게이트웨이 포트 번호를 입력한 다음 Connect(연결)를 **클릭합니다**.



참고: 이 예에서는 10.10.10.1:8443이 사용됩니다. 이제 소프트웨어가 원격 네트워크에 연결 중임을 표시합니다.

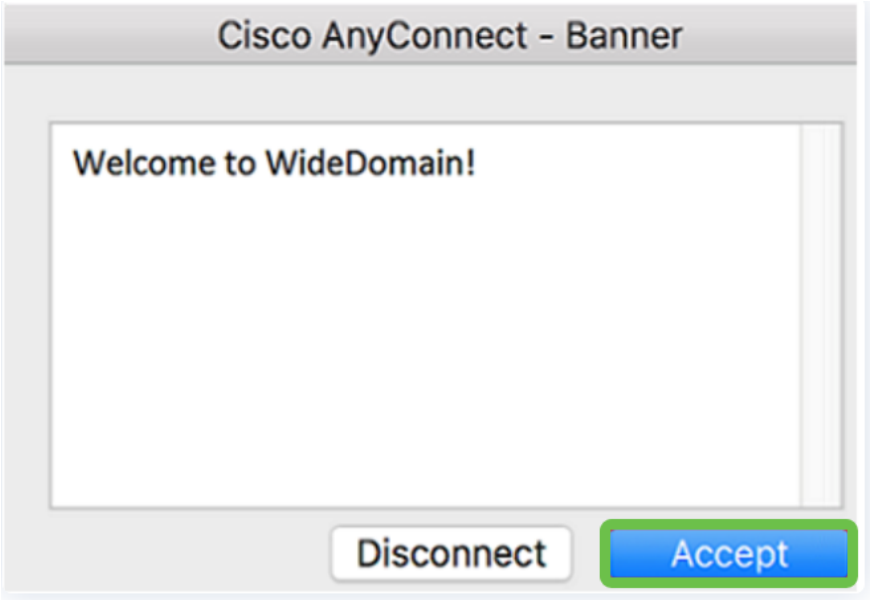


3단계. 각 필드에 서버 사용자 이름 및 비밀번호를 입력한 다음 **OK**(확인)를 클릭합니다.

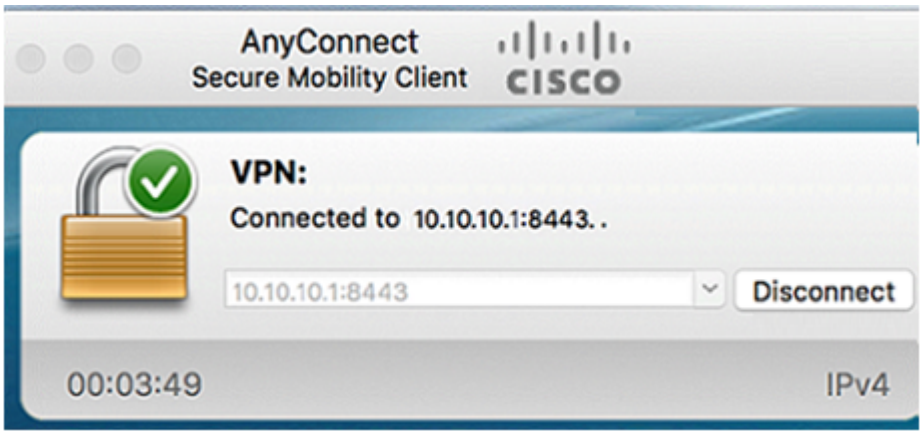


참고: 이 예에서는 Group1 사용자가 사용자 이름으로 사용됩니다.

4단계. 연결이 설정되는 즉시 로그인 배너가 나타납니다. Accept를 **클릭합니다**.



이제 AnyConnect 창에 네트워크에 대한 성공적인 VPN 연결이 표시됩니다.



5단계. (선택 사항) 네트워크 연결을 끊으려면 Disconnect를 **클릭합니다**.

이제 RV34x Series Router를 사용하여 AnyConnect VPN 연결을 성공적으로 구성했어야 합니다.

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.