RV340 또는 RV345 라우터에 Secure Sockets Layer SSL VPN(Virtual Private Network) 구성

특별 알림: 라이센스 구조 - 펌웨어 버전 1.0.3.15 이상 앞으로 AnyConnect는 클라이언트 라이센스에 대해서만 요금이 부과됩니다.

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

목표

SSL VPN(Secure Sockets Layer Virtual Private Network) 게이트웨이를 사용하면 원격 사용자가 웹 브라우저를 사용하여 보안 VPN 터널을 설정할 수 있습니다. 이 기능을 사용하면 SSL HTTPS(Hypertext Transfer Protocol Secure) 브라우저 지원을 통해 기본 HTTP(Hypertext Transfer Protocol)를 사용하는 광범위한 웹 리소스 및 웹 지원 애플리케이션에 쉽게 액세스할 수 있습니다.

SSL VPN을 사용하면 사용자가 네트워크 트래픽을 암호화하여 안전하고 인증된 경로를 사용하여 제한된 네트워크에 원격으로 액세스할 수 있습니다.

RV340 및 RV345 라우터는 Cisco AnyConnect VPN 클라이언트 또는 Anyconnect Secure Mobility Client를 지원합니다. 이러한 라우터는 기본적으로 2개의 SSL VPN 터널을 지원하며 사용자는 최대 50개의 터널을 지원하기 위해 라이센스를 등록할 수 있습니다. 설치 및 활성화되면 SSL VPN은 안전한 원격 액세스 VPN 터널을 설정합니다.

이 문서에서는 RV340 또는 RV345 라우터에서 SSL VPN을 구성하는 방법을 보여 줍니다.

적용 가능한 디바이스

- RV340
- RV345
- Cisco Secure Mobility Client

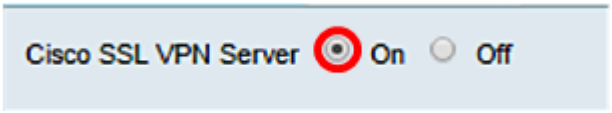
소프트웨어 버전

- 1.0.03.15 — RV340, RV345
- 4.4.01054 — AnyConnect Secure Mobility Client

SSL VPN 구성

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

2단계. Cisco SSL VPN Server를 활성화하려면 On 라디오 버튼을 클릭합니다.

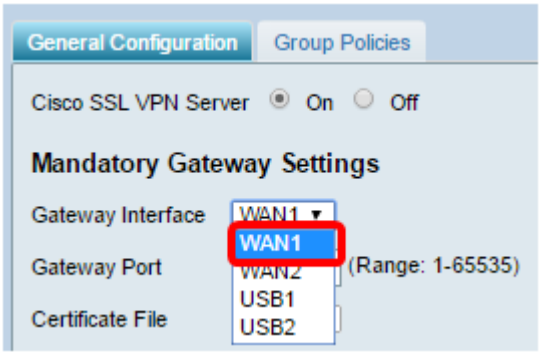


필수 게이트웨이 설정

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

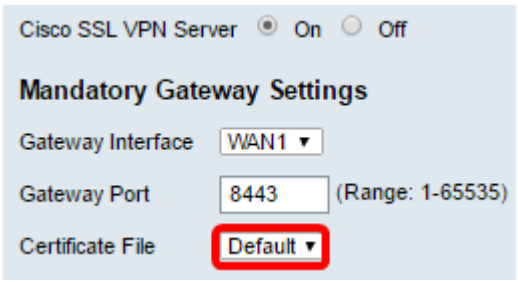


참고: 이 예에서는 WAN1을 선택합니다.

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

참고: 이 예에서는 포트 번호로 8443이 사용됩니다.

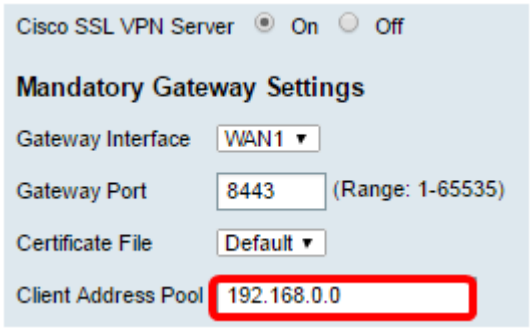
5단계. 드롭다운 목록에서 인증서 파일을 선택합니다. 이 인증서는 SSL VPN 터널을 통해 네트워크 리소스에 액세스하려는 사용자를 인증합니다. 드롭다운 목록에는 기본 인증서 및 가져온 인증서가 포함됩니다.



참고: 이 예에서는 Default(기본값)가 선택됩니다.

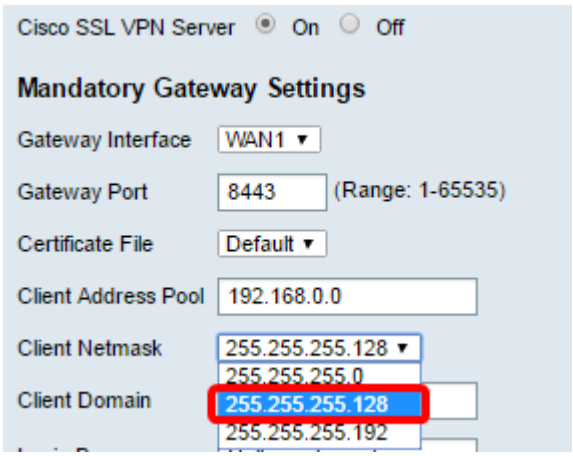
6단계. Client Address Pool(클라이언트 주소 풀) 필드에 클라이언트 주소 풀의 IP 주소를 입력합니다. 이 풀은 원격 VPN 클라이언트에 할당될 IP 주소의 범위가 됩니다.

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



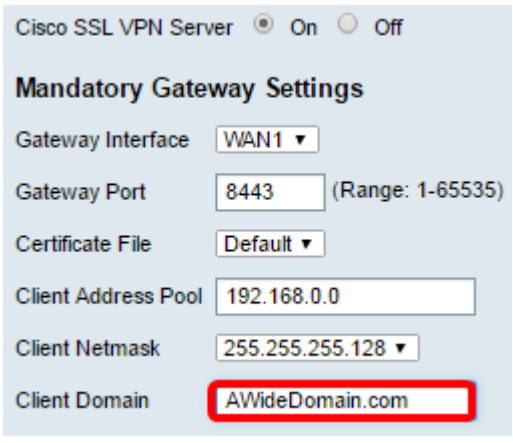
참고: 이 예에서는 192.168.0.0이 사용됩니다.

7단계. 드롭다운 목록에서 클라이언트 넷마스크를 선택합니다.



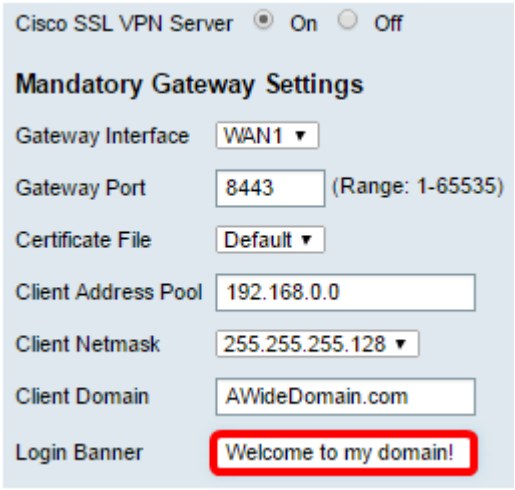
참고: 이 예제에서는 255.255.255.128을 선택합니다.

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



참고: 이 예에서는 AWideDomain이 클라이언트 도메인 이름으로 사용됩니다.

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



참고: 이 예에서는 내 도메인에 오신 것을 환영합니다! 로그인 배너로 사용됩니다.

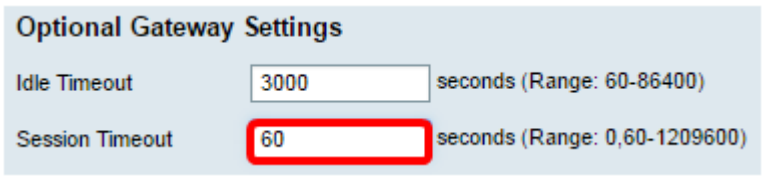
선택적 게이트웨이 설정

다음 컨피그레이션 설정은 선택 사항입니다.

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

참고: 이 예에서는 3000이 사용됩니다.

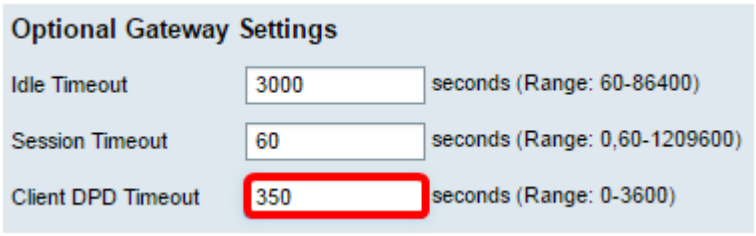
2단계. Session Timeout(세션 시간 초과) 필드에 초 단위의 값을 입력합니다. 지정된 유휴 시간 이후에 TCP(Transmission Control Protocol) 또는 UDP(User Datagram Protocol) 세션이 시간 초과되는 데 걸리는 시간입니다. 범위는 60~1209600입니다.



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.

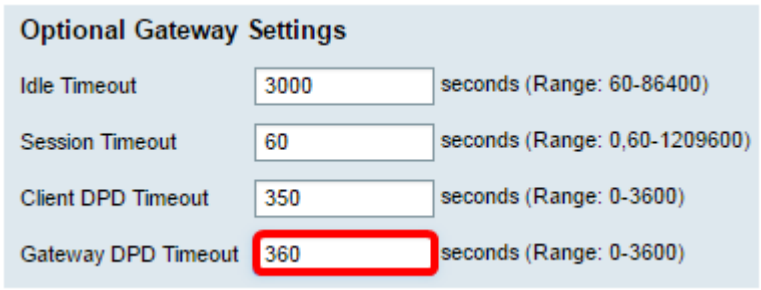
참고: 이 기능은 VPN 터널의 양쪽 끝에서 활성화해야 합니다.



참고: 이 예에서는 350이 사용됩니다.

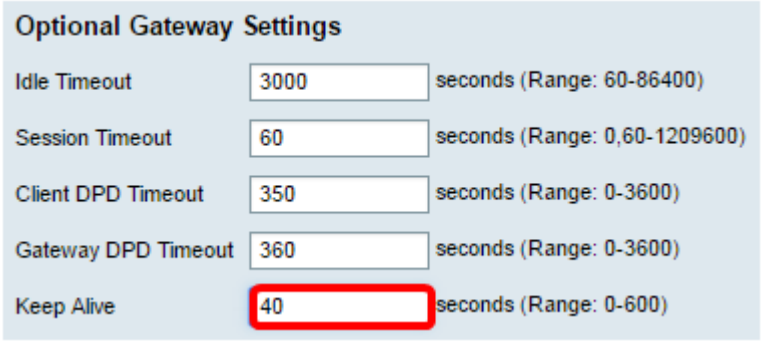
4단계. GatewayDPD Timeout(GatewayDPD 시간 초과) 필드에 0~3600 범위의 값을 초 단위로 입력합니다. 이 값은 VPN 터널의 상태를 확인하기 위해 HELLO/ACK 메시지를 정기적으로 전송하도록 지정합니다.

참고: 이 기능은 VPN 터널의 양쪽 끝에서 활성화해야 합니다.



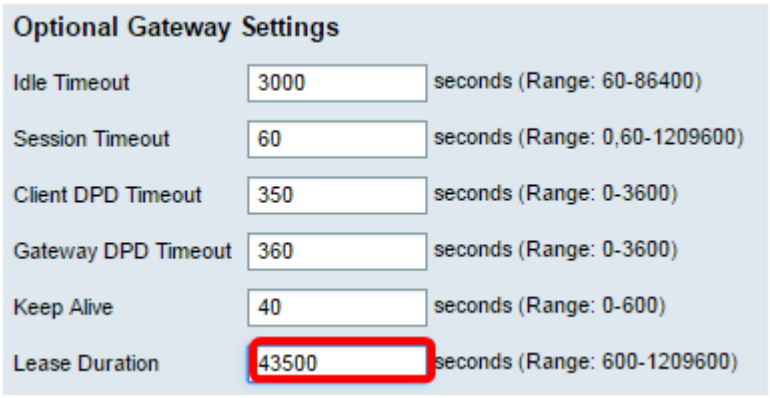
참고: 이 예에서는 360이 사용됩니다.

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



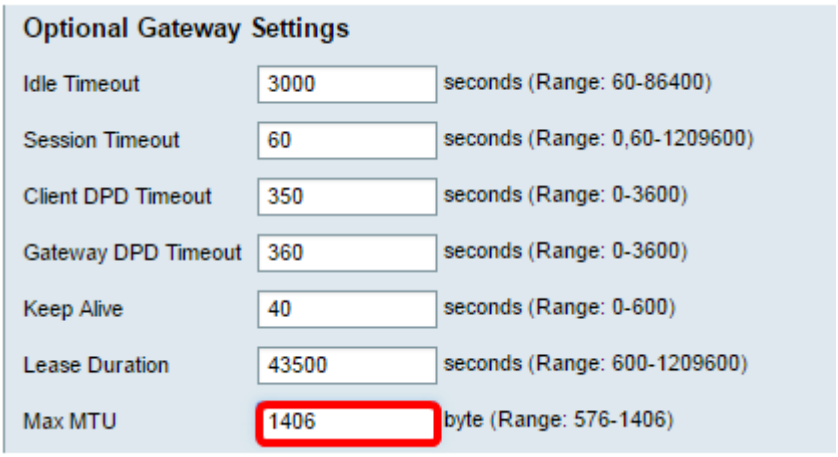
참고: 이 예에서는 40이 사용됩니다.

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



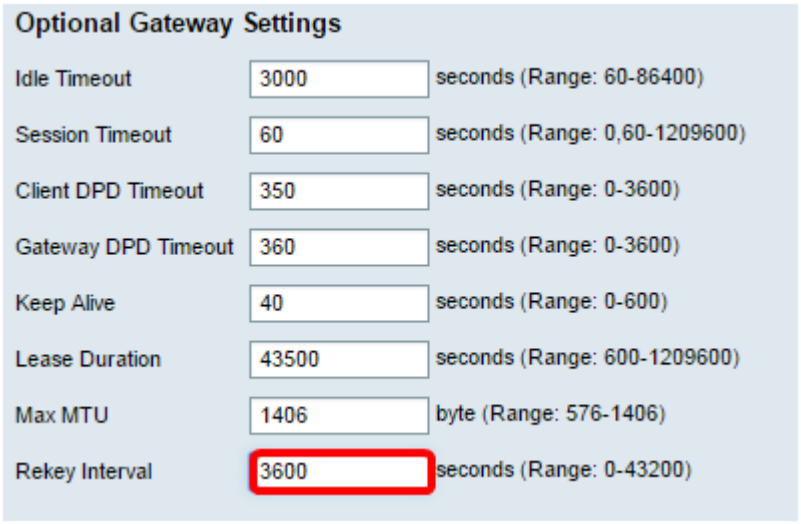
참고: 이 예에서는 43500이 사용됩니다.

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



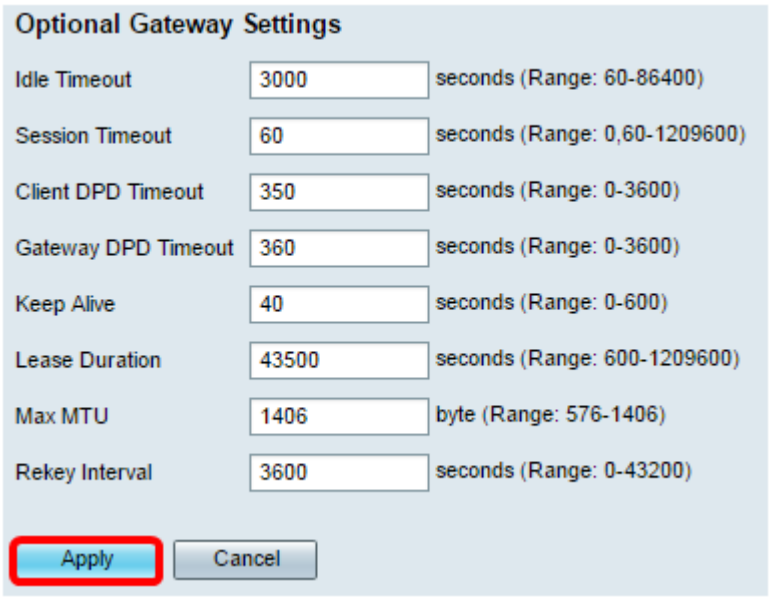
참고: 이 예에서는 1406이 사용됩니다.

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. 적용을 클릭합니다.



10단계(선택 사항) 구성을 영구적으로 저장하려면 깜박이는 아이콘을 

클릭합니다.

이제 RV34x 라우터에서 SSL VPN을 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.