CISCO START
Simple Secure Smart

Cisco RV340 시리즈 보안 라우터

간편 설치 가이드

이 단계별 가이드에 따라 RV340 시리즈 보안 라우터를 간편하게 설치하실 수 있습니다.

1. 장비 연결
2. 로그인 및 암호 변경
3. 초기 설치 마법사 사용
4. VPN 설치 마법사 사용
5. 애플리케이션 제어 마법사 사용
6. 구성 적용

cisco

1 장비 연결

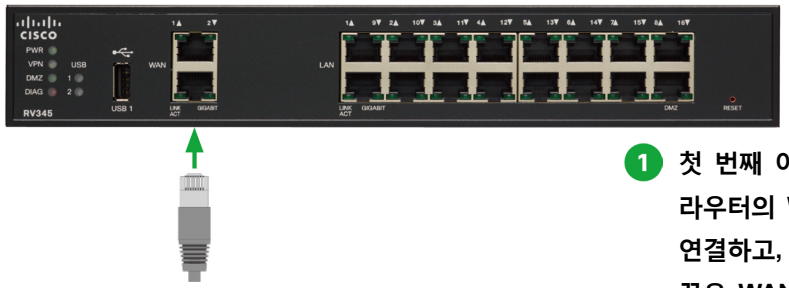
1-1 시작하기 전에

설치를 시작하기 앞서 아래와 같은 장비를 갖추고 있는지 확인하십시오.

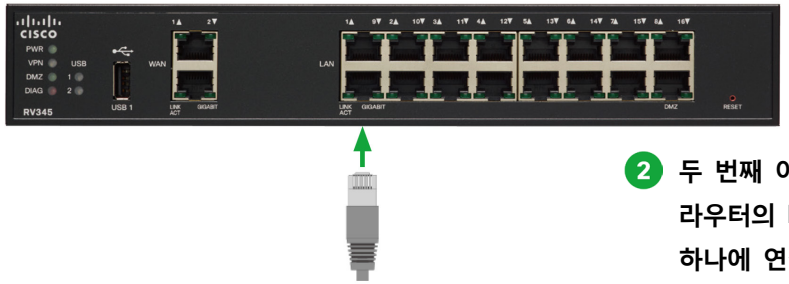
- RV340 Router (라우터)
- 이더넷 케이블 2개
- 전원 어댑터
- PC

라우터에 아무 것도 연결되어 있지 않은지 확인하고 DHCP를 사용할 수 있도록 PC를 설정합니다. 그리고 케이블 또는 DSL 모뎀, 컴퓨터, 라우터 등을 포함해 모든 장비의 전원을 끕니다.

1-2 장비 연결

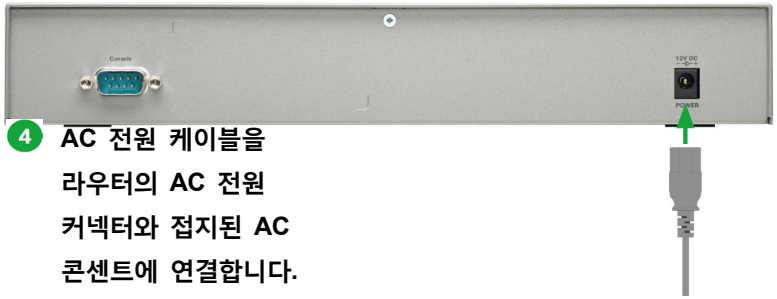


1 **첫 번째 이더넷 케이블을 라우터의 WAN 포트 1번에 연결하고, 케이블의 다른 끝은 WAN 장비의 이더넷 포트에 연결합니다.**



2 **두 번째 이더넷 케이블을 라우터의 LAN 포트 중 하나에 연결하고, 케이블의 다른 끝은 PC의 이더넷 포트에 연결합니다.**

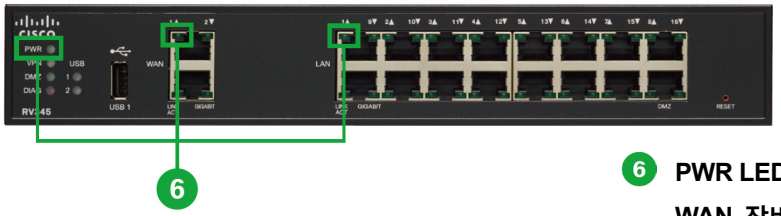
3 **WAN 장비의 전원을 켜고 연결이 될 때까지 기다립니다.**



4 **AC 전원 케이블을 라우터의 AC 전원 커넥터와 접지된 AC 콘센트에 연결합니다.**

전원 스위치는 "켜짐"으로 기본 설정되어 있습니다. 전원 어댑터가 제대로 연결이 되고 장비의 부팅이 완료되면 전면 패널의 전원등이 녹색이 됩니다.

5 **2단계에서 LAN 포트 중 하나에 연결한 PC의 전원을 켭니다.**



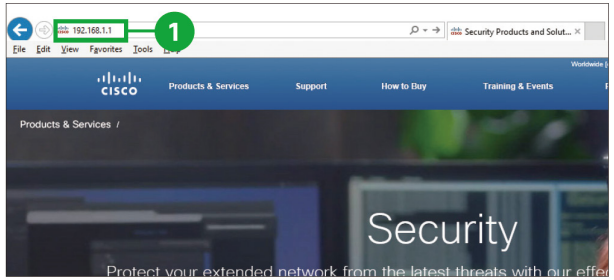
6 **PWR LED가 녹색이고 WAN 장비 및 PC에 연결한 포트 LED가 녹색이 되거나 녹색 깜박임이 나타나는지 확인합니다.**

메모

시스템이 부팅되는 동안 PWR LED는 시스템이 완전히 부팅될 때까지 계속해서 깜박입니다. 시스템이 시작되면 1번 LAN의 PWR, LINK/ACT 및 GIGIBIT LED가 점멸됩니다. 부팅이 25% 진행되면 1번 LAN과 2번 LAN의 PWR, LINK/ACT 및 GIGIBIT LED가 점멸됩니다. 부팅이 50 % 진행되면 1번 LAN, 2번 LAN, 3번 LAN의 PWR, LINK/ACT 및 GIGIBIT LED가 점멸됩니다. 부팅이 75% 진행되면 1번, 2번, 3번, 4번 LAN의 PWR, LINK/ACT 및 GIGIBIT LED가 점멸됩니다. 시스템 부팅은 보통 3분 이내에 완료됩니다. 라우터의 모든 기능이 구성되어있고 설정이 최대값인 경우에는 부팅하는 데 최대 7분의 시간이 소요됩니다.

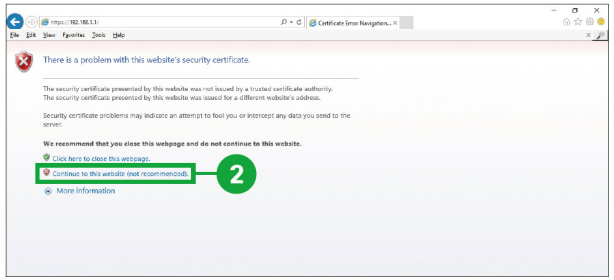
2 로그인 및 암호 변경

라우터는 기본 설정 상태로 출하됩니다. 그러나 ISP(Internet Service Provider)가 설정을 수정하도록 요구할 수 있습니다. Internet Explorer (버전 10 이상), Firefox, Chrome (PC용), Safari (Mac용)와 같은 웹 브라우저에서 설치 마법사와 장비 관리자를 사용해 라우터 설정을 수정할 수 있습니다. 웹 브라우저를 실행합니다.



1 웹 브라우저를 실행하고 주소 표시줄에 IP 주소 "https://192.168.1.1"을 입력한 다음, Enter 키를 누릅니다.

환경에 따라 보안 인증서 페이지가 나타납니다.

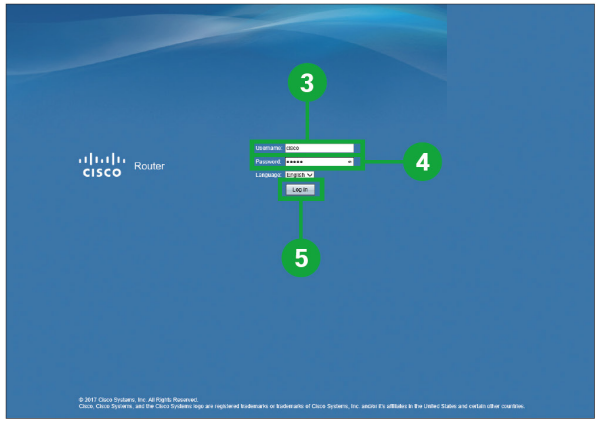


2 [Continue to this website (not recommended)]를 클릭합니다.

주의

로그인 페이지가 나타나지 않으면 다음을 확인하십시오.

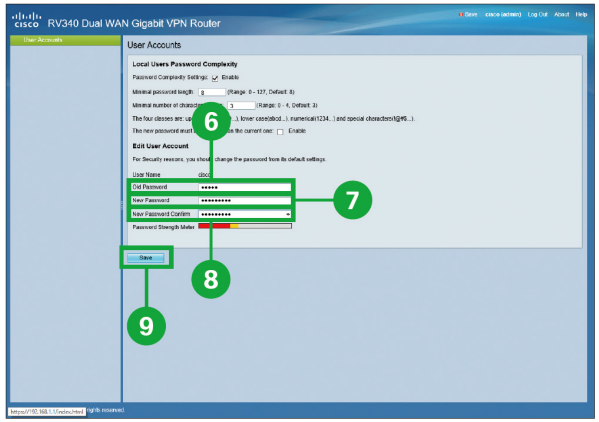
- PWR LED가 녹색이고 포트 LED가 녹색이 되거나 녹색 깜박임이 나타나는지
- 라우터의 이더넷 포트에 스트레이트 이더넷 케이블이 연결되어 있는지
- 브라우저의 모든 팝업 차단 기능이나 프록시 설정이 비활성화되어 있는지, 그리고 PC 또는 노트북에서 모든 무선 클라이언트가 비활성화되어 있는지
- DHCP를 사용하도록 PC가 설정되어 있는지, 라우터가 DHCP 서버 역할을 하고 있는지, PC가 정적 IP 주소를 가지고 있는 경우에 DHCP를 사용하도록 PC를 임시 설정하는지



3 [Username]에 "cisco"를 입력합니다.

4 [Password]에 "cisco"를 입력합니다.

5 [Log In]을 클릭합니다.

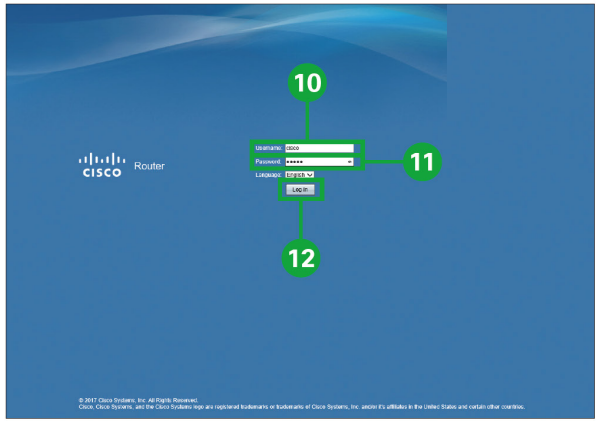


6 [Old Password]에 "cisco"를 입력합니다.

7 [New Password]에 암호를 입력합니다.

8 [New Password Confirm]에 암호를 다시 입력합니다.

9 [Save]를 클릭합니다.



10 [Username]에 "cisco"를 입력합니다.

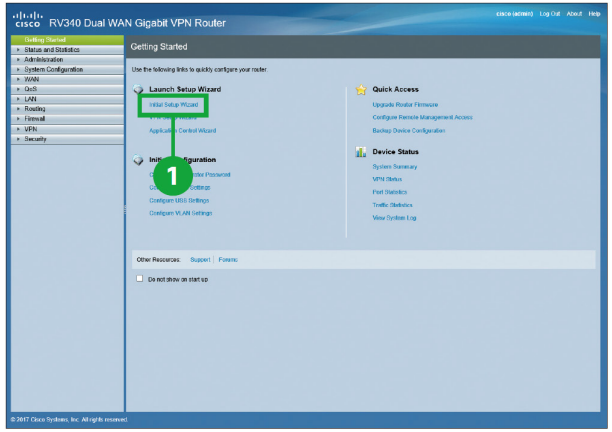
11 [Password]에 암호를 입력합니다.

12 [Log In]을 클릭합니다.

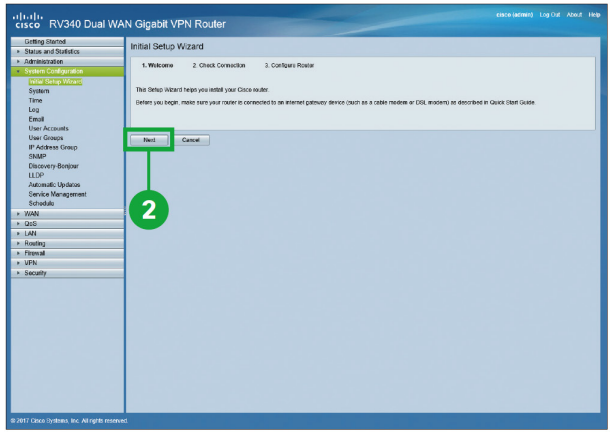
장치 관리자 시작 페이지가 나타납니다.

3 초기 설치 마법사 사용

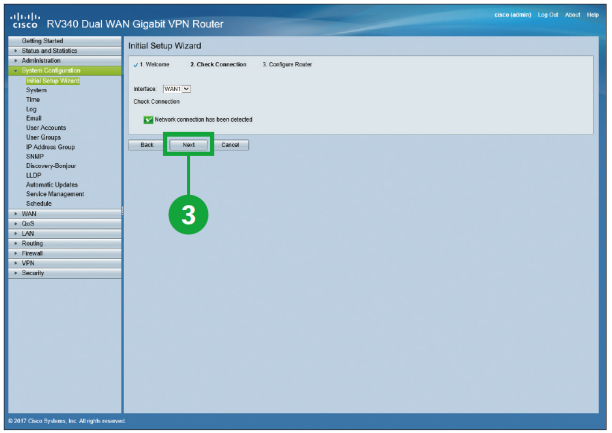
초기 설치 마법사 페이지에서 회선 연결성을 점검하고 라우터의 기본 설정을 구성할 수 있습니다. 인터넷 연결 설정에 필요한 정보는 ISP에게 문의하십시오.



1 시작하기 페이지에서 [Initial Setup- Wizard]를 클릭합니다.

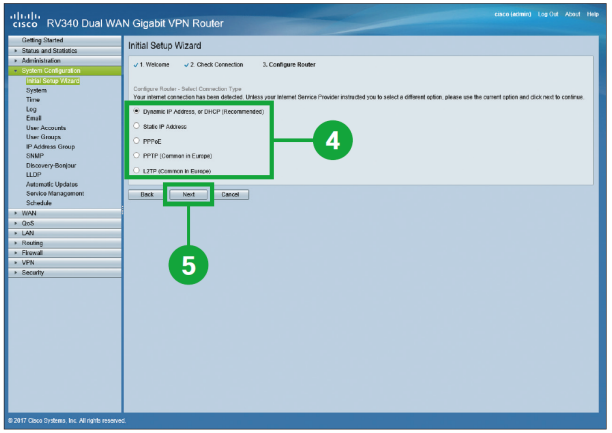


2 [Next]를 클릭합니다.



3 [Next]를 클릭합니다.

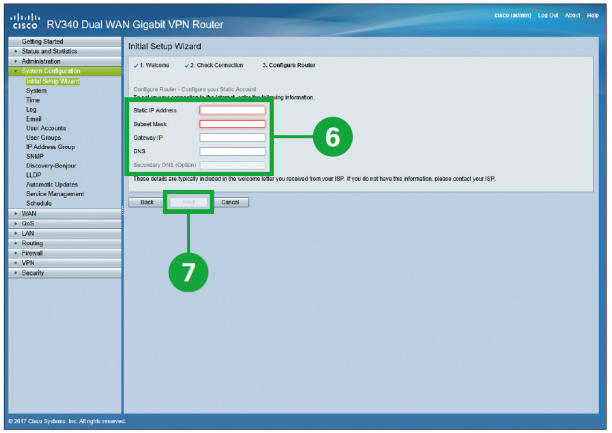
라우터가 연결을 감지하면 연결 상세 정보가 이 페이지에 표시됩니다.



4 인터넷 연결 유형을 선택합니다.

5 [Next]를 클릭합니다.

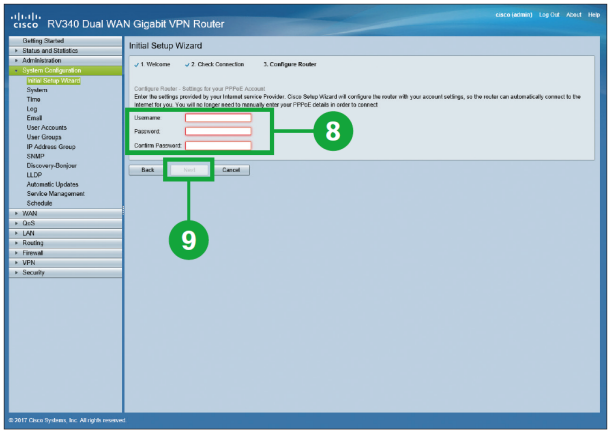
[Dynamic IP Address, or DHCP (Recommended)]를 선택하면 14로 건너뜁니다.



6 [Static IP Address]를 선택한 경우에는 필수 정보를 입력합니다.

7 [Next]를 선택하고 14로 건너뜁니다.

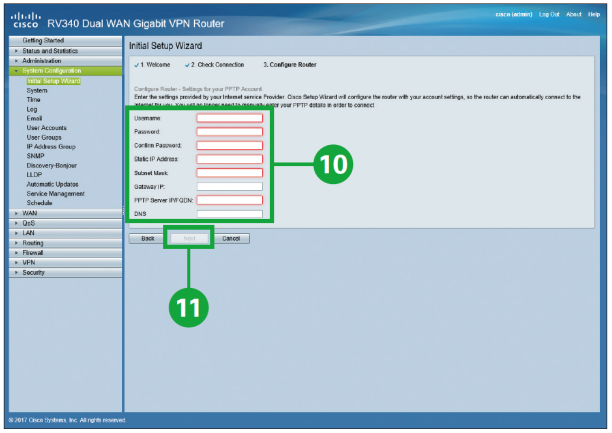
이러한 상세 정보는 ISP측에서 제공됩니다. 이 정보가 없는 경우에는 ISP에게 문의하시기 바랍니다.



8 **[PPPoE]를 선택한 경우에는 필수 정보를 입력합니다.**

9 **[Next]를 선택하고 14로 건너뜁니다.**

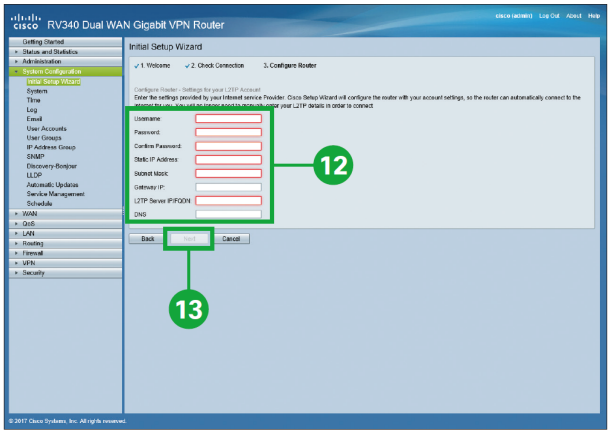
이러한 상세 정보는 ISP측에서 제공됩니다. 이 정보가 없는 경우에는 ISP에게 문의하시기 바랍니다.



10 **[PPTP (Common in Europe)]를 선택한 경우에는 필수 정보를 입력합니다.**

11 **[Next]를 선택하고 14로 건너뜁니다.**

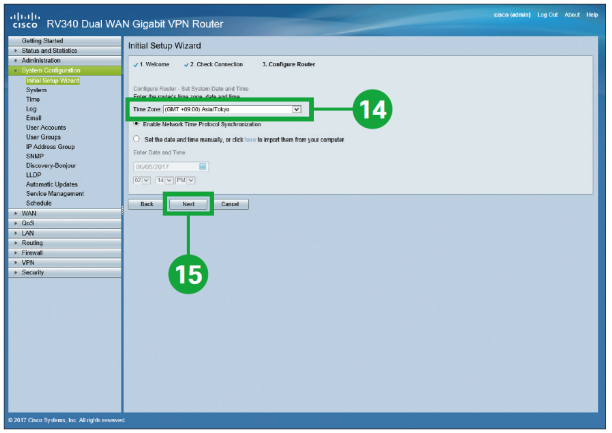
이러한 상세 정보는 ISP측에서 제공됩니다. 이 정보가 없는 경우에는 ISP에게 문의하시기 바랍니다.



12 **[L2TP (Common in Europe)]를 선택한 경우에는 필수 정보를 입력합니다.**

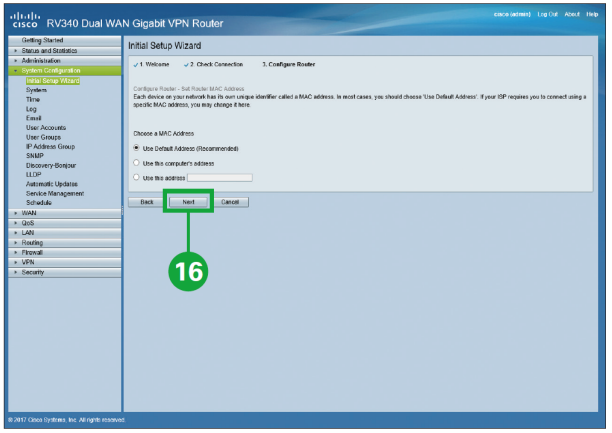
13 **[Next]를 클릭합니다.**

이러한 상세 정보는 ISP측에서 제공됩니다. 이 정보가 없는 경우에는 ISP에게 문의하시기 바랍니다.

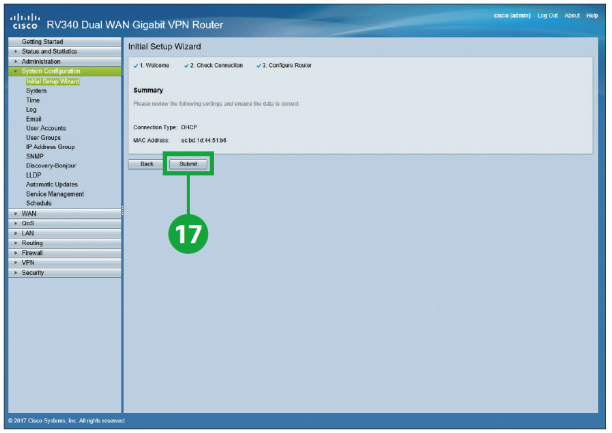


14 **[Time Zone] 드롭다운 목록에서 라우터의 시간대를 선택합니다.**

15 **[Next]를 클릭합니다.**



16 **[Next]를 클릭합니다.**

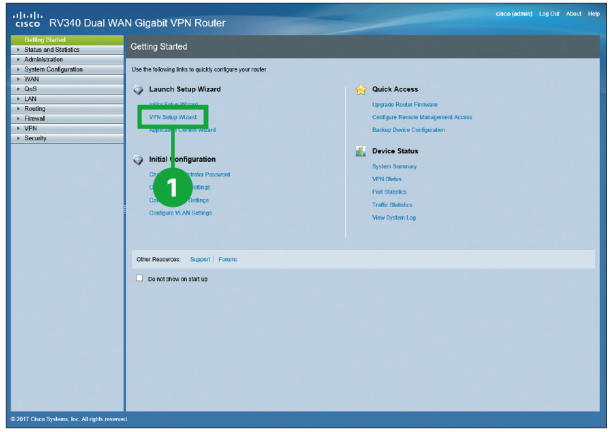


17 **[Submit]를 클릭합니다.**

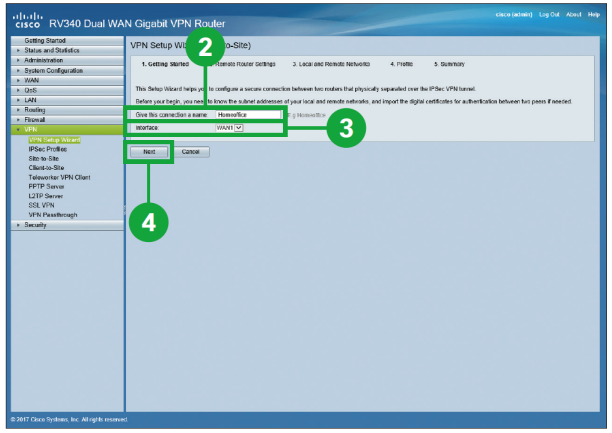
추가 WAN 설정이 필요한 경우에는 “부록 1, 추가 WAN 설정"로 가십시오.

4 VPN 설치 마법사 사용

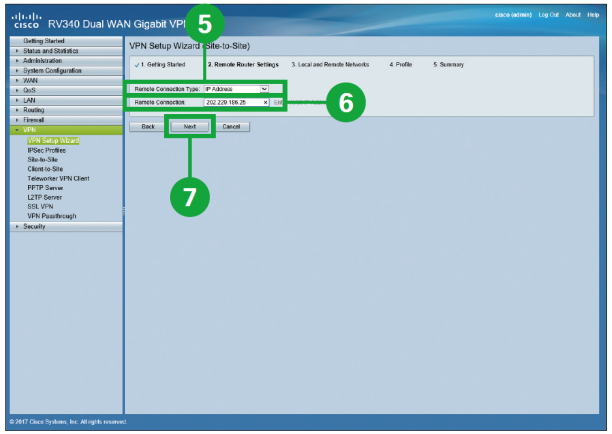
VPN은 원격 호스트가 마치 로컬 네트워크 상에 있는 것처럼 통신하도록 해줍니다. 라우터는 50개의 터널을 지원합니다. VPN 설치 마법사는 사이트 간 IPSEC 터널에서 안전하게 연결을 구성할 수 있도록 안내합니다. 사용자 누구라도 빠르고 효율적인 방식으로 IPSec 터널을 설치할 수 있도록 복잡한 파라미터 옵션을 제거하여 구성을 단순화합니다.



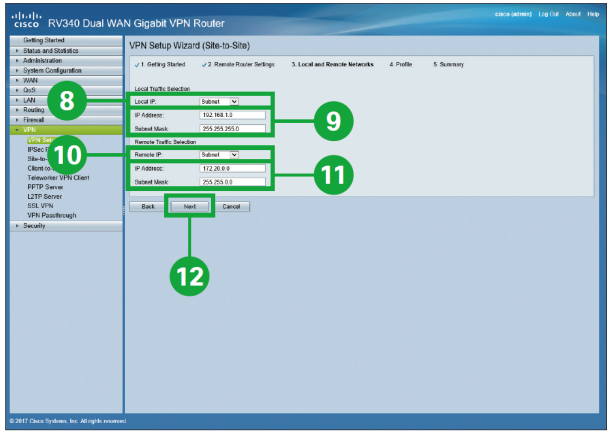
1. **시작하기 페이지에서 [VPN Setup- Wizard]를 클릭합니다.**



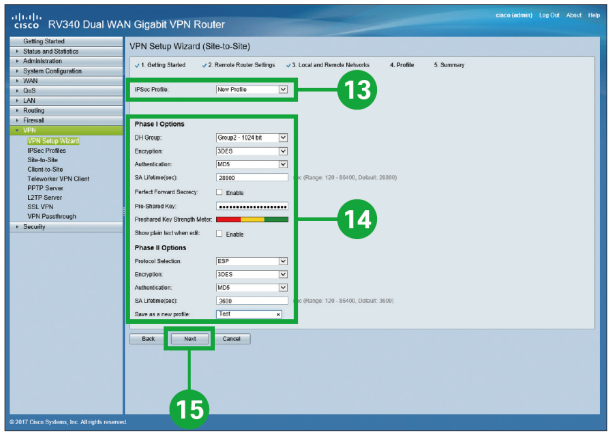
2. **[Give this connection a name] 필드에 연결 이름을 입력합니다.**
3. **드롭다운 목록에서 인터페이스를 선택합니다.**
4. **[Next]를 클릭합니다.**



5. **드롭다운 목록에서 [Remote Connection Type]을 선택합니다.**
6. **[IP Address]를 선택한 경우에는 IP 주소를, [FQDN]을 선택한 경우에는 이름을 입력합니다.**
7. **[Next]를 클릭합니다.**



8. **드롭다운 목록에서 [Local IP]를 선택합니다.**
9. **[IP Address]를 선택한 경우에는 IP 주소를, [Subnet]을 선택한 경우에는 IP 주소와 서브넷 마스크를 입력합니다.**
10. **드롭다운 목록에서 [Remote IP]를 선택합니다.**
11. **[IP Address]를 선택한 경우에는 IP 주소를, [Subnet]을 선택한 경우에는 IP 주소와 서브넷 마스크를 입력합니다.**
12. **[Next]를 클릭합니다.**



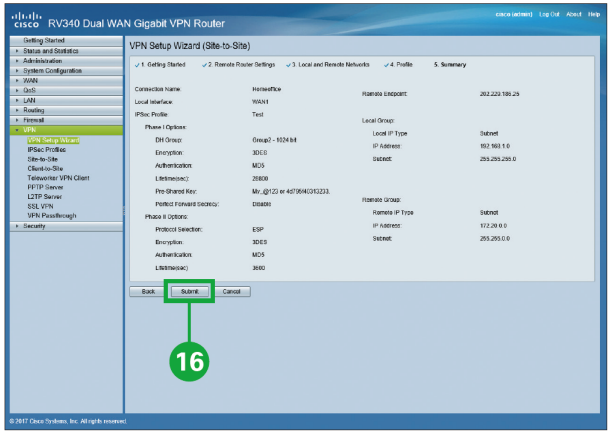
13 **드롭다운 목록에서 [IPSec profile]을 선택합니다.**

[Default]를 선택한 경우에는 15로 건너뜁니다.

14 **[New Profile]을 선택한 경우에는 필수 정보를 입력합니다.**

메모를 참조하십시오.

15 **[Next]를 클릭합니다.**



16 **[Submit]를 클릭합니다.**

메모: 단계 2 옵션

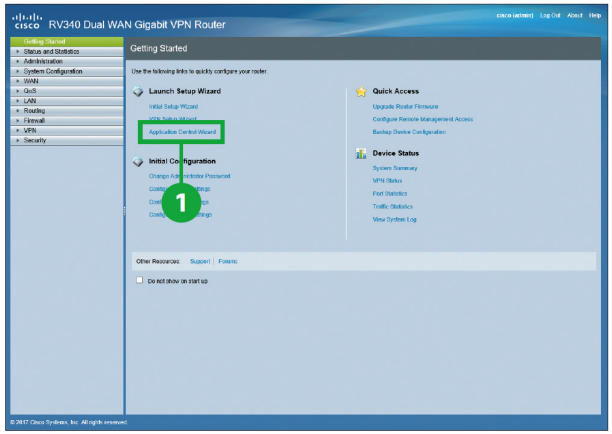
- **DH(Diffie-Hellman) 그룹**
  드롭다운 메뉴에서 DH 그룹을 선택합니다. PFS(Perfect Forward Secrecy)가 단계 1 옵션에서 활성화된 경우에만 이 그룹이 활성화됩니다.
- **프로토콜 선택**
  드롭다운 메뉴에서 프로토콜을 선택합니다.
- **암호화**
  드롭다운 목록에서 암호화 옵션을 선택합니다.
- **인증**
  인증을 선택합니다.
- **SA 갱신시간 (초)**
  이 단계에서 VPN 터널(IPSec SA)이 활성 상태인 기간입니다. 단계 2의 기본 값은 3600초입니다.

메모: 단계 1 옵션

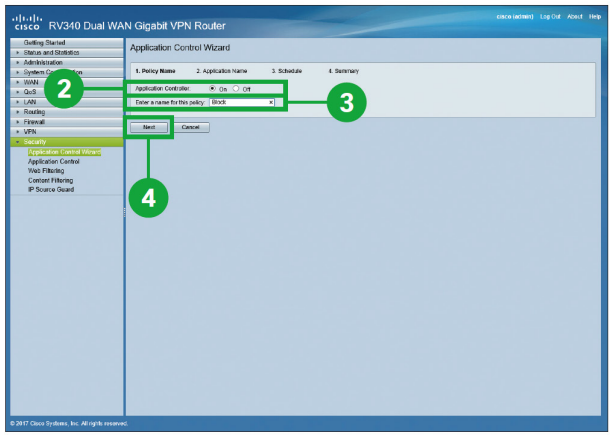
- **DH(Diffie-Hellman) 그룹**
  드롭다운 메뉴에서 DH 그룹(그룹 2 또는 그룹 5)을 선택합니다. DH는 키 교환 프로토콜로서 기본 키 길이가 서로 다른 2개의 그룹으로 구성되어 있습니다. 그룹 2는 최대 길이가 1,024비트이고, 그룹 5는 최대 길이가 1,536비트입니다. 보안 수준은 낮지만 더 빠른 속도를 원하다면 그룹 2를, 속도는 느려도 더 높은 보안 수준을 원한다면 그룹 5를 선택하십시오. 그룹 2가 기본적으로 선택되어 있습니다.
- **암호화**
  드롭다운 목록에서 암호화 옵션 (3DES, AES-128, AES-192 또는 AES-256)을 선택합니다. 암호화 방법에 따라 ESP/ISAKMP 패킷을 암호화 또는 암호 해제하는 데 사용될 알고리즘이 결정됩니다.
- **인증**
  인증 방법에 따라 ESP(Encapsulating Security Payload Protocol) 헤더 패킷이 검증되는 방법이 결정됩니다. MD5는 128비트 다이제스트를 생성하는 일방향 해싱 알고리즘입니다. SHA1은 160비트 다이제스트를 생성하는 일방향 해싱 알고리즘입니다. SHA1가 더 안전하다는 점에서 권장됩니다. VPN 터널의 양쪽 끝에서 동일한 인증 방법을 사용하는지 확인합니다. 인증 방법(MD5, SHA1 또는 SHA2-256)을 선택합니다.
- **SA 갱신시간 (초)**
  이 단계에서 IKE SA가 활성 상태인 기간입니다. 단계 1의 기본 값은 28,800초입니다.
- **PFS(Perfect Forward Secrecy)**
  Enable을 선택하여 PFS를 활성화하고 시간단위를 초 단위로 입력하거나 Enable의 선택을 해제하여 비활성화합니다. PFS가 활성화되면 IKE 단계 2 협상을 통해 IPSec 트래픽 암호화 및 인증을 위한 새로운 키가 생성됩니다. 이 기능을 활성화할 것을 권장합니다.
- **사전 공유 키**
  사전 공유 키를 사용해 원격 IKE 피어를 인증합니다. 최대 30개의 키보드 문자나 16진수 값(예: My_@123 또는 4d795f40313233)을 입력할 수 있습니다. VPN 터널의 양쪽 끝에서 반드시 동일한 사전 공유 키를 사용해야 합니다. VPN 보안을 극대화하려면 사전 공유 키를 정기적으로 변경할 것을 권장합니다.

5 애플리케이션 제어 마법사 사용

애플리케이션 제어 마법사를 통해 특정하게 지정된 원치 않는 애플리케이션이 클라이언트에 접근하지 못하도록 액세스를 제한할 수 있습니다. 카테고리 및 이름에 따라 애플리케이션에 대한 액세스를 허용 및 로깅하거나 차단할 수 있습니다. 또한 애플리케이션 제어 마법사가 활성 상태가 되는 시간을 예약할 수 있습니다.



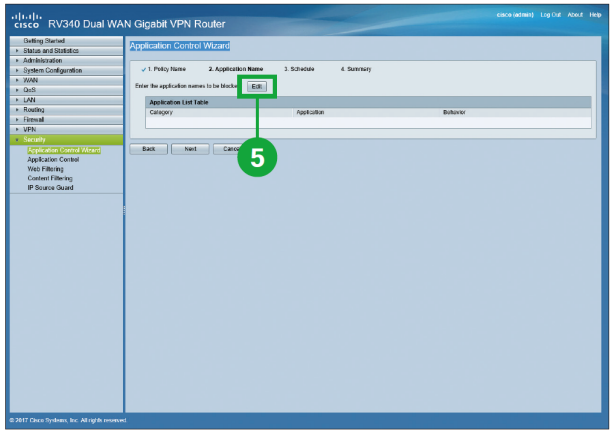
1 **시작하기 페이지에서 [Application Control Wizard]를 클릭합니다.**



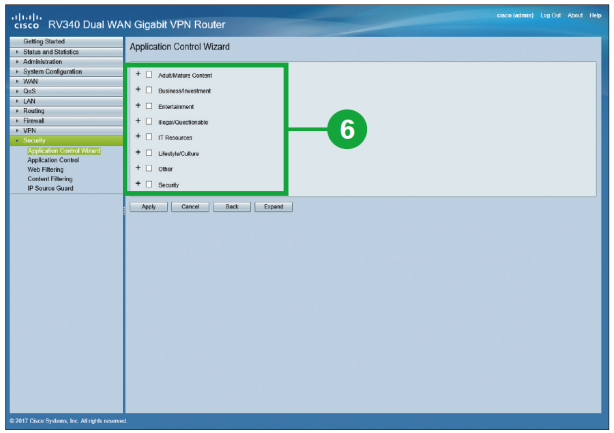
2 **[On]을 선택합니다.**

3 **[Enter a name of this policy] 필드에 정책 이름을 입력합니다.**

4 **[Next]를 클릭합니다.**

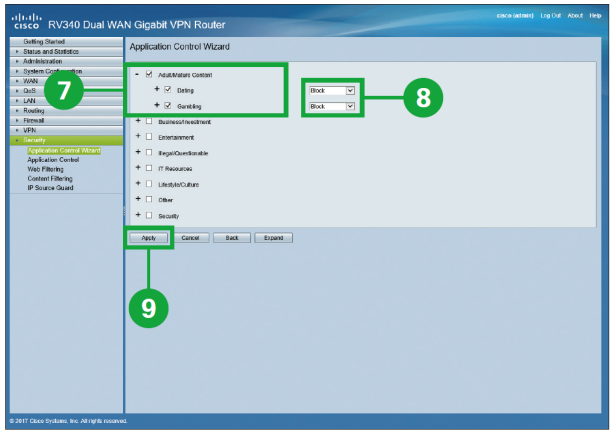


5 **[Edit]를 클릭합니다.**



6 **1개 이상의 카테고리 이름을 선택하거나 + 아이콘을 클릭해서 필터링할 서브 카테고리까지 확장합니다.**

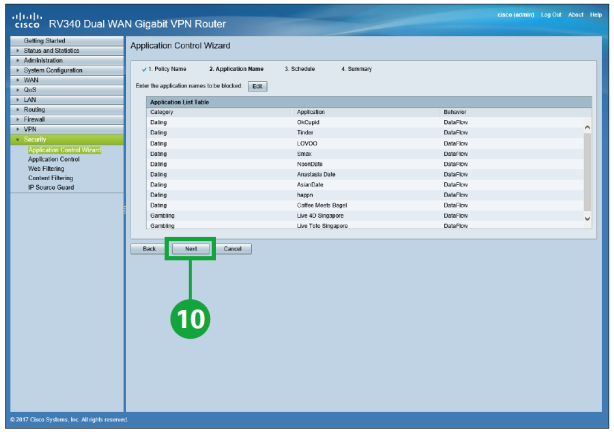
+ 아이콘을 클릭해서 필터링할 애플리케이션까지 확장할 수 있습니다.



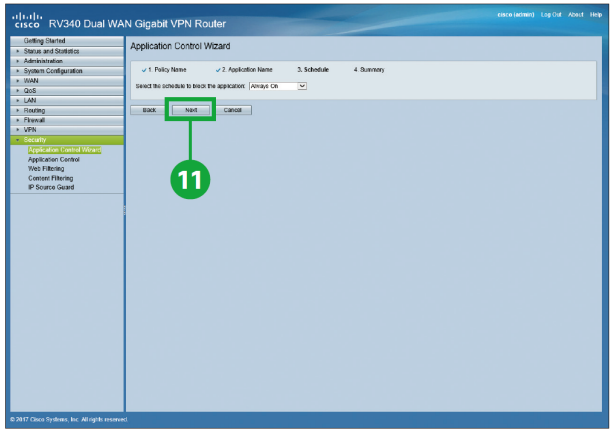
7 **1개 이상의 카테고리 이름, 서브 카테고리 이름 또는 필터링할 애플리케이션을 선택합니다.**

8 **드롭다운 목록에서 각 서브 카테고리 이름이나 애플리케이션에 대한 조치(허용 또는 차단 등)를 선택합니다.**

9 **[Apply]를 클릭합니다.**

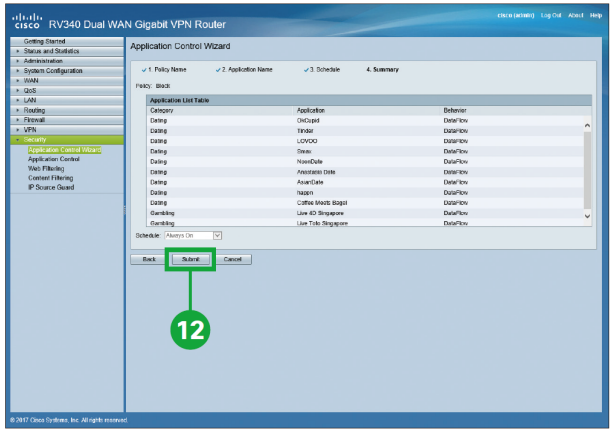


10 **[Next]를 클릭합니다.**



11 **[Next]를 클릭합니다.**

[Select the schedule to block the application] 드롭다운 목록에서 애플리케이션 차단 일정을 선택할 수 있습니다.

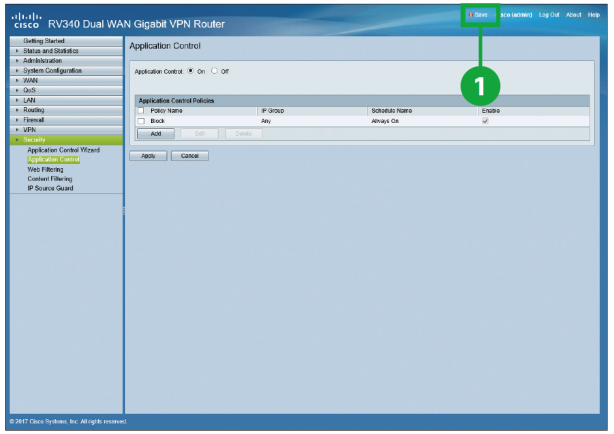


12 **[Submit]를 클릭합니다.**

애플리케이션 카테고리 또는 애플리케이션마다 서로 다른 조치를 취하도록 각기 애플리케이션 제어 정책을 설정할 수 있습니다. 그렇게 하려면 단계를 여러 번 반복합니다.

6 구성 적용

라우터가 현재 사용하고 있는 모든 구성들은 휘발성 메모리상에서 실행 구성 파일로 저장되어있기 때문에 재부팅을 하면 구성이 지워져 버립니다. 재부팅을 하는 동안 현재 구성 파일이 저장되도록 하려면 설정 변경 후 실행 구성 파일을 시작 구성 파일로 복사해야 합니다.

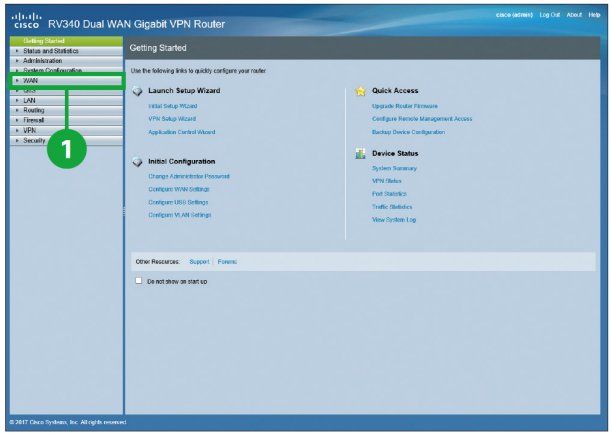


1 **깜박이는 [Save]를 클릭합니다.**

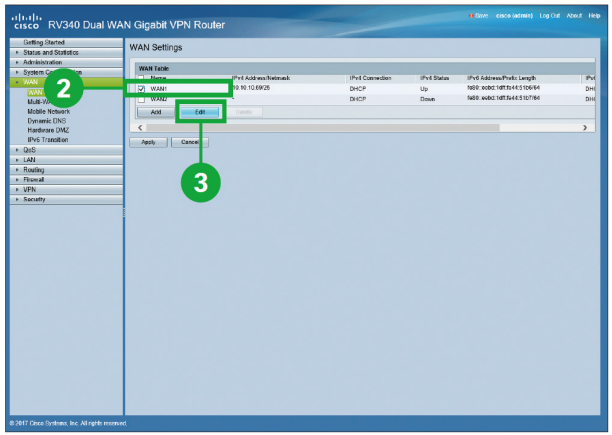
2 **[Apply]를 클릭합니다.**

부록 1 추가 WAN 설정

추가 WAN 설정을 원하면 아래 단계를 따릅니다.

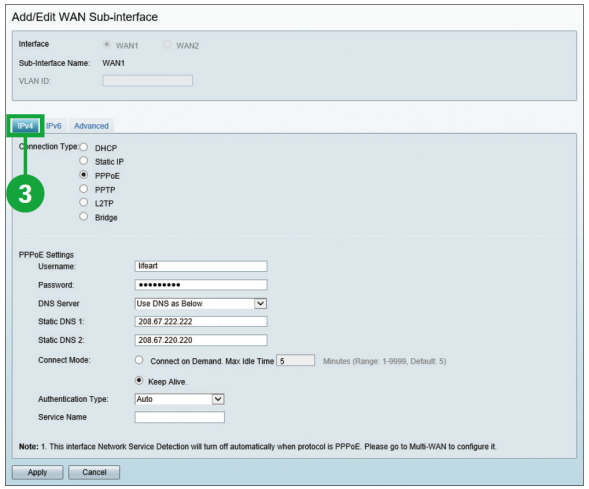


1 [WAN]을 클릭합니다.



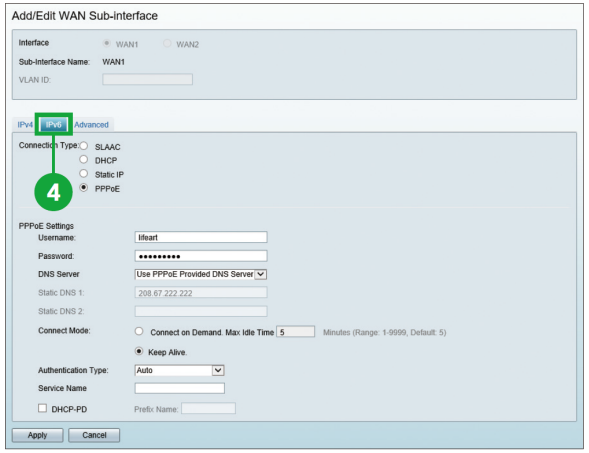
2 인터페이스를 선택합니다.

3 [Edit]를 클릭합니다.



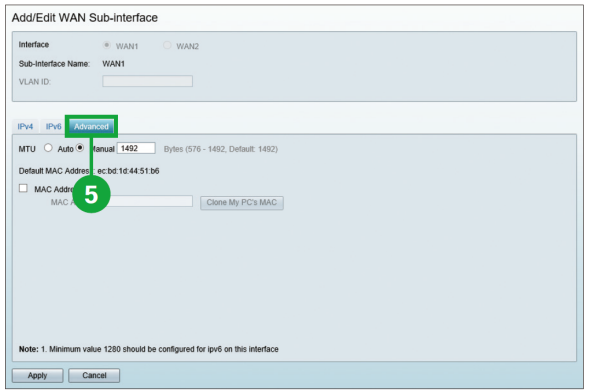
3 [IPv4] 탭을 클릭해서 IPv4에 대한 추가 설정을 구성합니다.

예를 들어 수동으로 [DNS Server]를 구성할 수 있습니다.



4 [IPv6] 탭을 클릭해서 IPv6에 대한 추가 설정을 구성합니다.

예를 들어 [DHCP-PD]를 구성할 수 있습니다.



5 [Advanced] 탭을 클릭해서 추가 고급 설정을 구성합니다.

예를 들어 수동으로 [MTU]를 구성할 수 있습니다.

부록 2 기타 참조 위치

■ 지원

- **시스코 지원 커뮤니티**
  http://www.cisco.com/go/smallbizsupport
- **시스코 지원 및 리소스**
  http://www.cisco.com/go/smallbizhelp
- **전화 지원 연락처**
  http://www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
- **시스코 펌웨어 다운로드**
  http://www.cisco.com/go/smallbizfirmware
- **시스코 오픈 소스 요청**
  http://www.cisco.com/go/smallbiz_opensource_request
- **시스코 파트너 센트럴**
  http://www.cisco.com/web/partners/sell/smb
- **시스코 온라인 장비 에뮬레이터**
  http://www.cisco.com/go/onlinedevicemanagers

■ 제품 문서

- **Cisco RV340 시리즈 보안 라우터 관리 가이드**
  http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/RV340/Administration/EN/b_RV340_AG.pdf