RV016, RV042, RV042G 및 RV082 VPN Router의 일반 방화벽 설정

목표

방화벽은 인터넷과 같은 외부 네트워크로부터 내부 네트워크를 보호합니다. 방화벽은 네트워크 보안에 매우 중요합니다. 보안 요구 사항에 따라 특정 서비스를 활성화하거나 비활성화할 수 있는 여러 가지 설정이 제공됩니다.

이 문서의 목적은 RV016, RV042, RV042G 및 RV082 VPN Router에서 일반 방화벽 설정을 활성화하거나 비활성화하는 방법을 설명하는 것입니다.

적용 가능한 디바이스

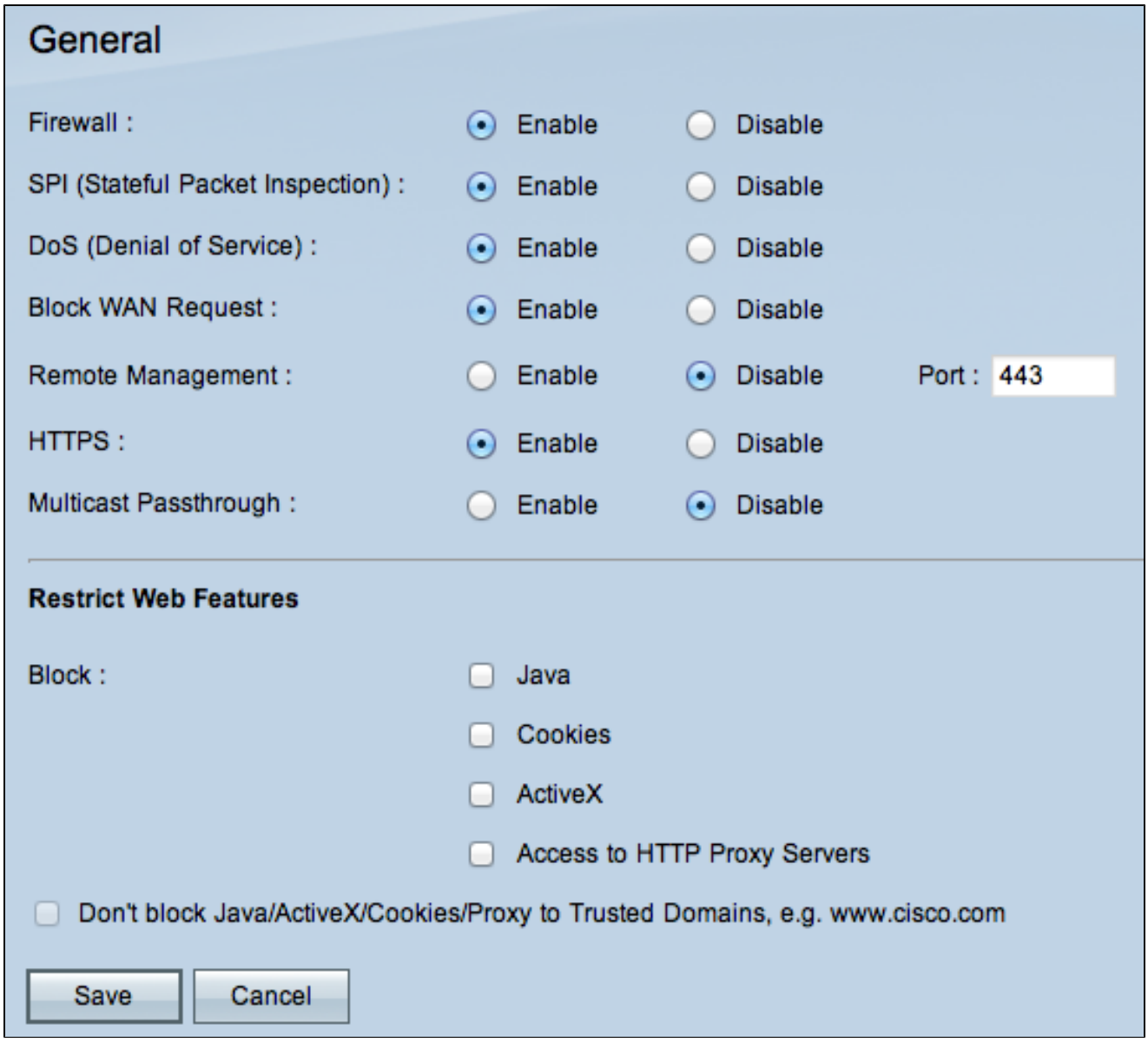
· RV016
· RV042
· RV042G
· RV082

소프트웨어 버전

· v4.2.1.02

일반 방화벽 설정

1단계. 라우터 컨피그레이션 유틸리티에 로그인하고 Firewall(방화벽) > General(일반)을 선택합니다. General(일반) 페이지가 열립니다.



2단계. 사용자 요구 사항에 따라 방화벽에서 사용 가능한 설정을 활성화 또는 비활성화하려면 활성화 또는 비활성화 라디오 버튼을 클릭합니다.

다음 필드는 다음과 같이 설명됩니다.

· 방화벽 — 이 기능이 활성화되면 라우터는 이 라우터를 통과하는 모든 트래픽에 대해 심층 패킷 검사를 수행하고 미리 정의된 프로토콜 동작을 따르지 않는 패킷을 삭제합니다.

· SPI(Stateful Packet Inspection) — 라우터의 방화벽은 SPI(Stateful Packet Inspection)를 사용하여 방화벽의 트래픽을 검토합니다. TCP 스트림 및 UDP 통신 등의 네트워크 연결 상태를 모니터링합니다. 방화벽은 서로 다른 유형의 연결에 대해 합법적인 패킷을 구별하며, 알려진 활성 연결과 일치하는 패킷만 방화벽에 의해 허용되며 나머지 패킷은 모두 거부됩니다.

· Dos(Denial of Service) — 이 기능이 활성화되면 라우터는 인터넷에서 오는 DOS(Denial of Service) 공격을 차단합니다. DOS 공격으로 인해 라우터의 CPU가 사용 중이어서 일반 트래픽에 서비스를 제공할 수 없습니다.

· WAN 요청 차단 — 이 기능을 활성화하면 라우터가 인터넷의 PING 요청을 무시하므로 숨겨진 것처럼 보입니다. 이렇게 하면 네트워크 포트를 숨겨 침입자가 네트워크에 쉽게 액세스할 수 없도록 하여 보안을 제공할 수 있습니다.

· 원격 관리 — 이 기능을 활성화하면 라우터를 통해 인터넷에서 웹 구성 유틸리티에 액세스할 수 있습니다. WAN 측의 호스트에 개방할 포트 번호를 입력합니다. 기본 설정은 443입니다. 사용자가 원격 연결을 설정할 때 이 포트를 지정해야 합니다.

· HTTPS — 이 옵션을 활성화하면 일반 HTTP가 아닌 WAN측에서 HTTPS 세션을 통해 웹 구성 유틸리티에 액세스할 수 있습니다. 이렇게 하면 SSL 암호화 알고리즘으로 원격 웹 세션이 보호됩니다. HTTPS 기능을 사용할 수 없는 경우 사용자는 QuickVPN을 사용하여 연결할 수 없습니다. 비활성화하면 보안 수준이 낮은 HTTP 연결을 사용합니다.

· 멀티캐스트 패스스루 — IGMP 프록시가 현재 라우터에서 실행되는 경우, 멀티캐스트 패스스루가 활성화되면 라우터는 인터넷에서 IP 멀티캐스트 트래픽이 들어오도록 허용합니다.

참고: 방화벽을 비활성화하려면 관리자 비밀번호를 기본값에서 변경해야 합니다.
SPI(Stateful Packet Inspection), DoS(Denial of Service), Block WAN Request 및 Remote Management(원격 관리) 필드는 회색으로 비활성화됩니다.

3단계. Restrict Web Features(웹 기능 제한) 영역에서 확인란의 일부 또는 전체를 선택하여 해당 기능을 제한합니다.

· Java — Java는 웹 사이트를 위한 프로그래밍 언어입니다. Java를 차단하려면 Java 확인란을 선택합니다. Java를 거부하면 이 프로그래밍 언어로 작성된 인터넷 사이트에 액세스하지 못할 수 있으므로 라우터에 연결된 디바이스가 Java로 생성된 웹 사이트에 액세스할 필요가 없는 경우 Java 애플릿을 차단해도 안전합니다. 반면 사이버 범죄자는 Java를 공격의 핵심 부분으로 사용합니다. 즉, 악성코드에 감염된 웹 사이트를 방문할 때 OS를 확인하고 OS에 지정된 공격을 실행합니다. 예를 들어, 해킹 된 웹 사이트를 방문 할 때, JAR (Java Archive) 파일이 트리거되어 기능을 수행하지만 몰래 컴퓨터의 OS를 확인하는 데 사용됩니다.

· 쿠키 — 쿠키는 PC에 저장되어 사용자가 쿠키와 상호 작용할 때 인터넷 사이트에서 사용하는 데이터입니다. 쿠키를 차단하려면 Cookies(쿠키) 확인란을 선택합니다. 쿠키를 차단하려는 경우 웹 사이트는 디바이스에서 액세스할 때 이전 방문 정보를 저장할 수 없습니다. 이점은 악성 쿠키(제3자 추적 쿠키)가 저장되지 않아 보안 위험이 있다는 것입니다.

· ActiveX — ActiveX는 Microsoft Windows의 소프트웨어 구성 요소로, 인터넷 사이트에서 사용되는 애드온과 같은 소규모 프로그램을 제어하거나 애플리케이션을 개발하는 데 사용

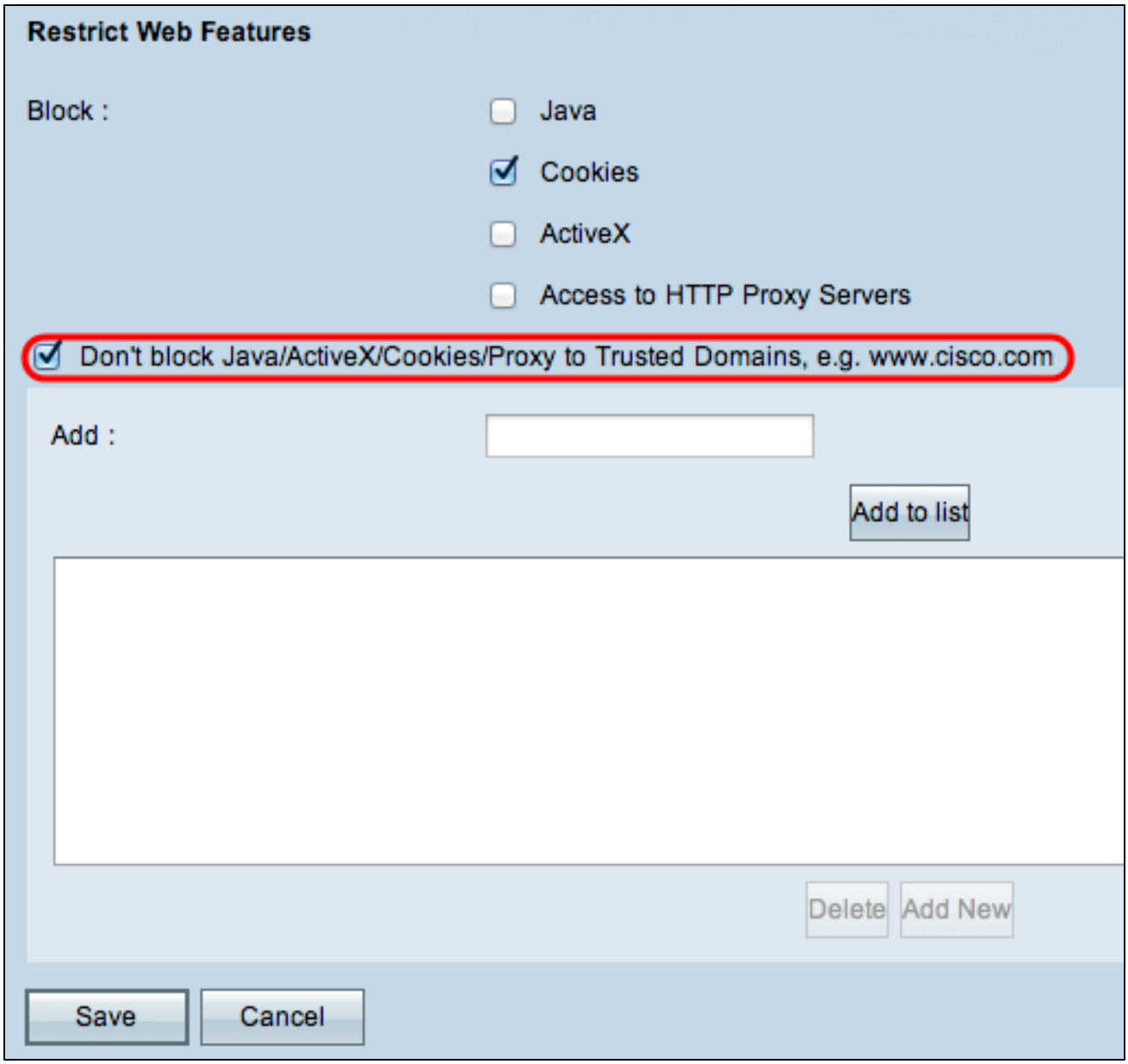
할 수 있습니다. ActiveX를 허용하면 웹 사이트에서 애니메이션 및 기타 유사한 프로그램을 실행할 수 있으므로 탐색 시 사용자 환경을 개선하는 데 도움이 됩니다. 반면 컴퓨터에 손상을 줄 수 있는 사이버 범죄자가 개발한 악성 ActiveX 소프트웨어가 포함된 웹 페이지를 방문할 경우 잠재적 위험이 있습니다. ActiveX를 차단하려면 ActiveX 확인란을 선택합니다. ActiveX를 차단하면 ActiveX를 사용하여 수행하는 특정 인터넷 사이트에 액세스하려는 경우 문제가 발생할 수 있습니다.

· 프록시 HTTP 서버에 액세스 — 프록시 서버를 통해 익명으로 서핑하고 프록시 서버에 대한 액세스를 거부하려면 Access to Proxy HTTP Server(프록시 HTTP 서버에 액세스) 확인란을 선택합니다. HTTP 프록시 서버는 해커로부터 최종 사용자의 세부 정보를 숨깁니다. 그들은 중개인 역할을 하므로 당신은 인터넷에 직접 접속하지 않습니다. 그러나 로컬 사용자가 WAN 프록시 서버에 액세스할 수 있는 경우, 라우터의 콘텐츠 필터를 살펴보고 라우터에 의해 차단된 인터넷 사이트에 액세스할 수 있습니다.

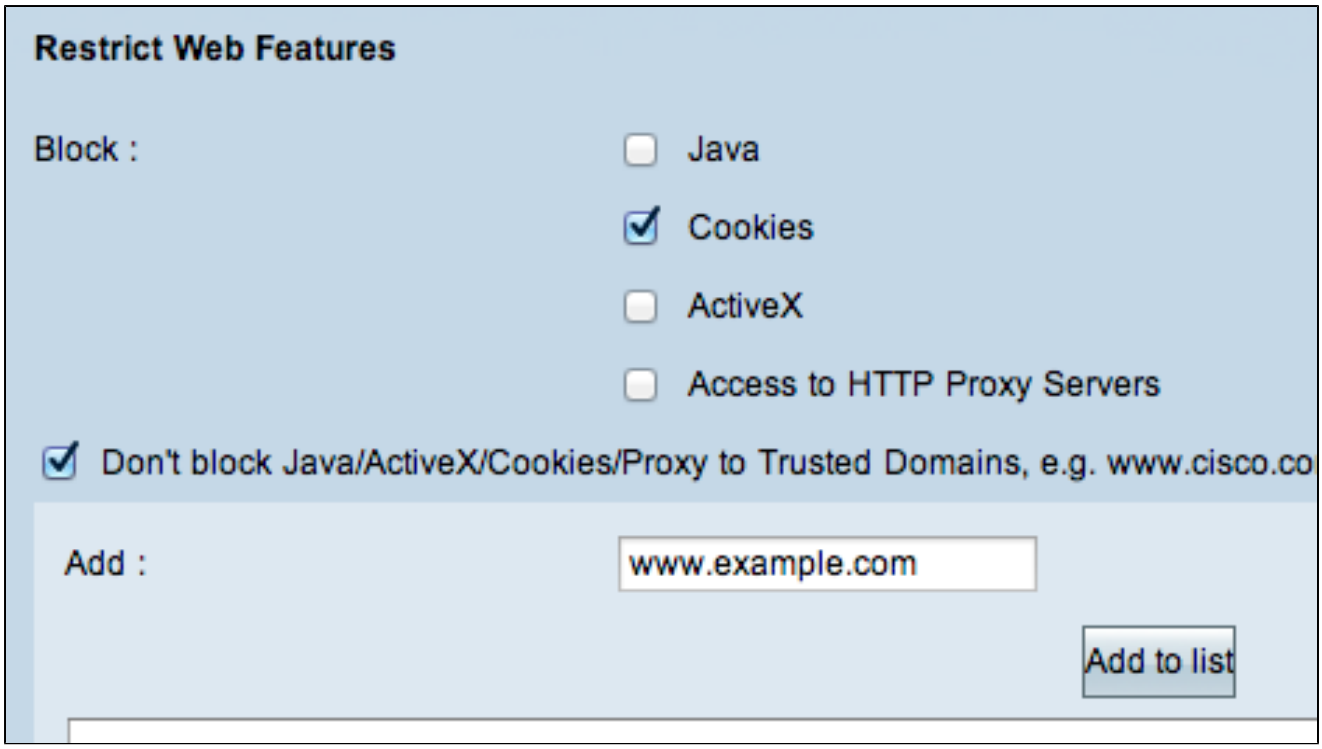
4단계. 설정을 저장하려면 Save(저장)를 클릭합니다.

트러스트된 도메인 추가

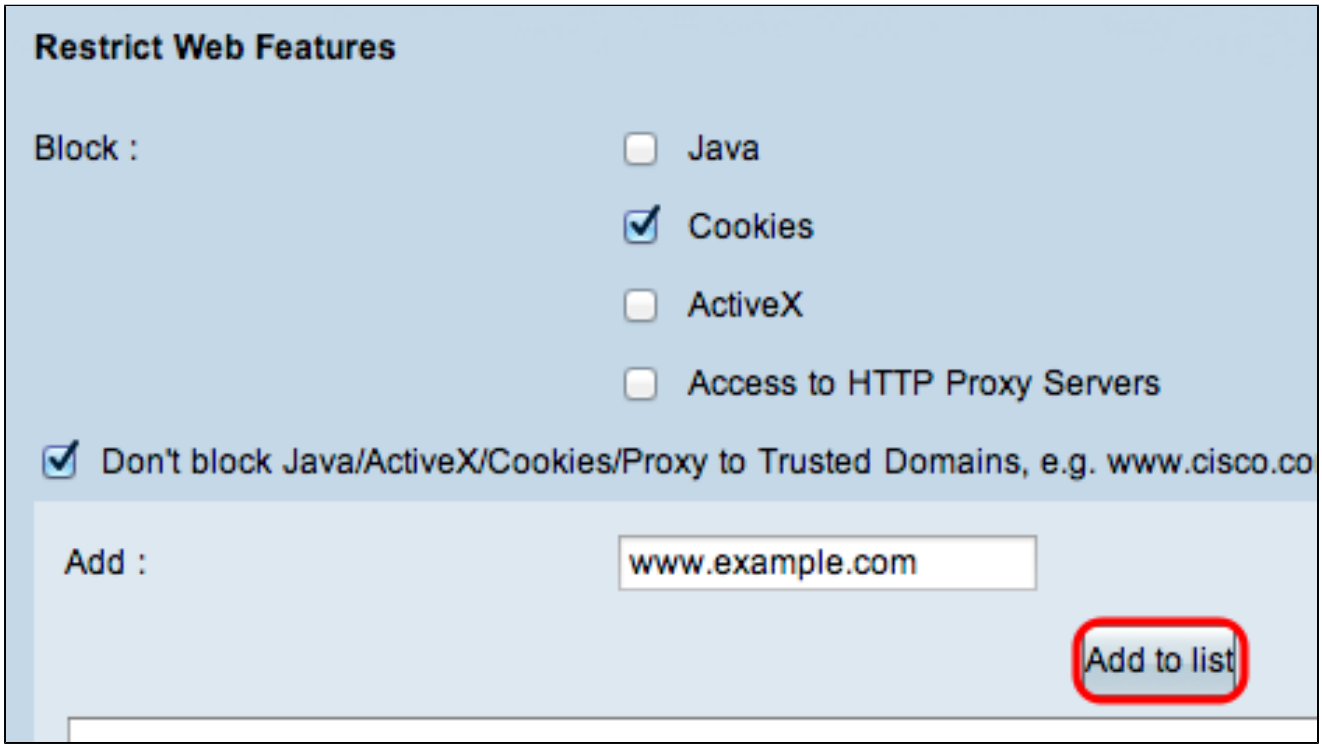
웹 기능 중 하나가 차단될 수 있지만 사용자는 지정된 트러스트된 도메인에 대해 이러한 기능을 사용하도록 허용할 수 있습니다.



1단계. Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains(Java/ActiveX/Cookies/Proxy to Trusted Domains(신뢰할 수 있는 도메인에 대한 Java/ActiveX/쿠키/프록시 차단 안 함) 버튼을 선택합니다. 이는 사용자가 일반 방화벽 설정의 3단계에서 웹 기능을 차단하도록 선택한 경우에만 사용할 수 있습니다.



2단계. Add(추가) 필드에 트러스트된 도메인 목록에 추가할 도메인을 입력합니다.

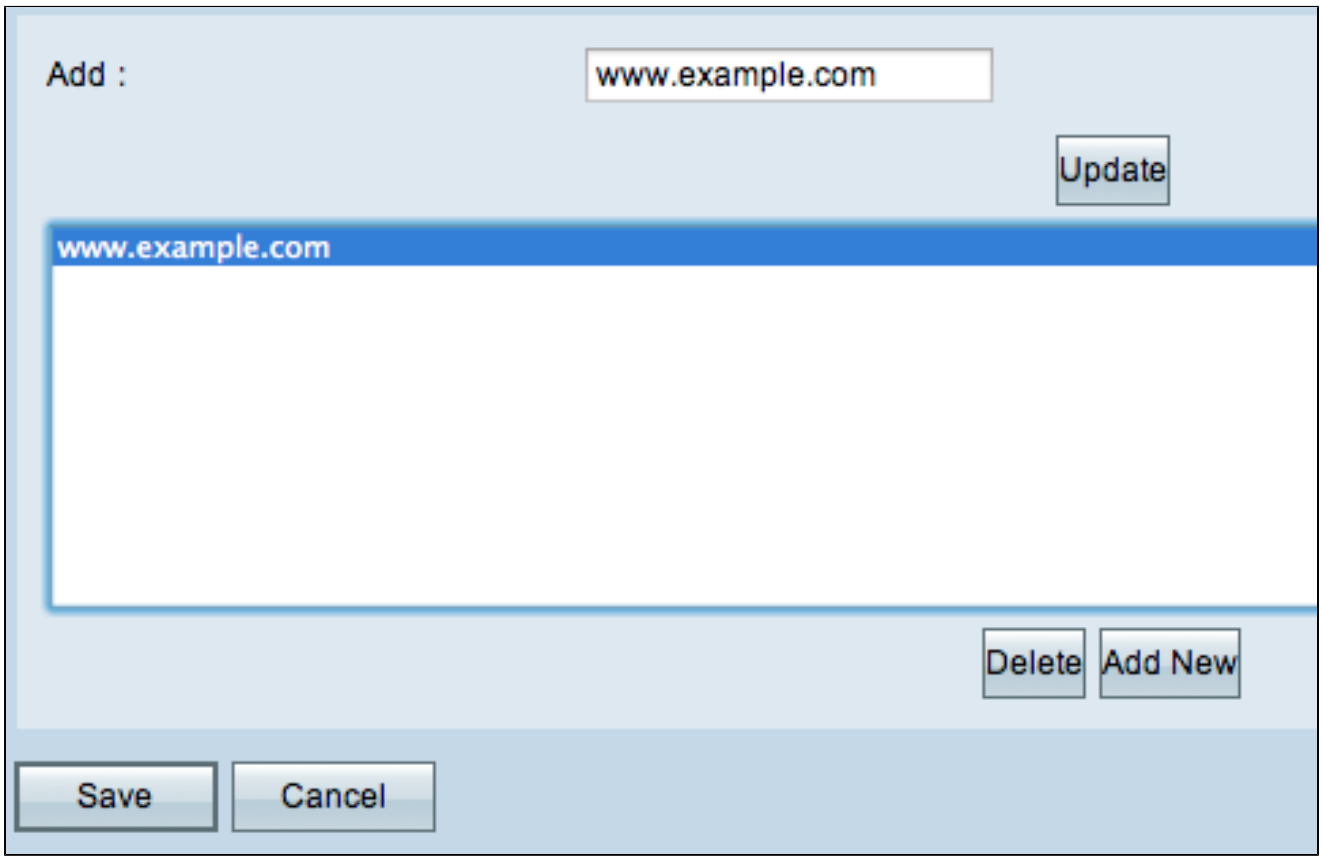


3단계. 목록에 추가를 클릭합니다. 도메인이 신뢰할 수 있는 목록에 추가됩니다.

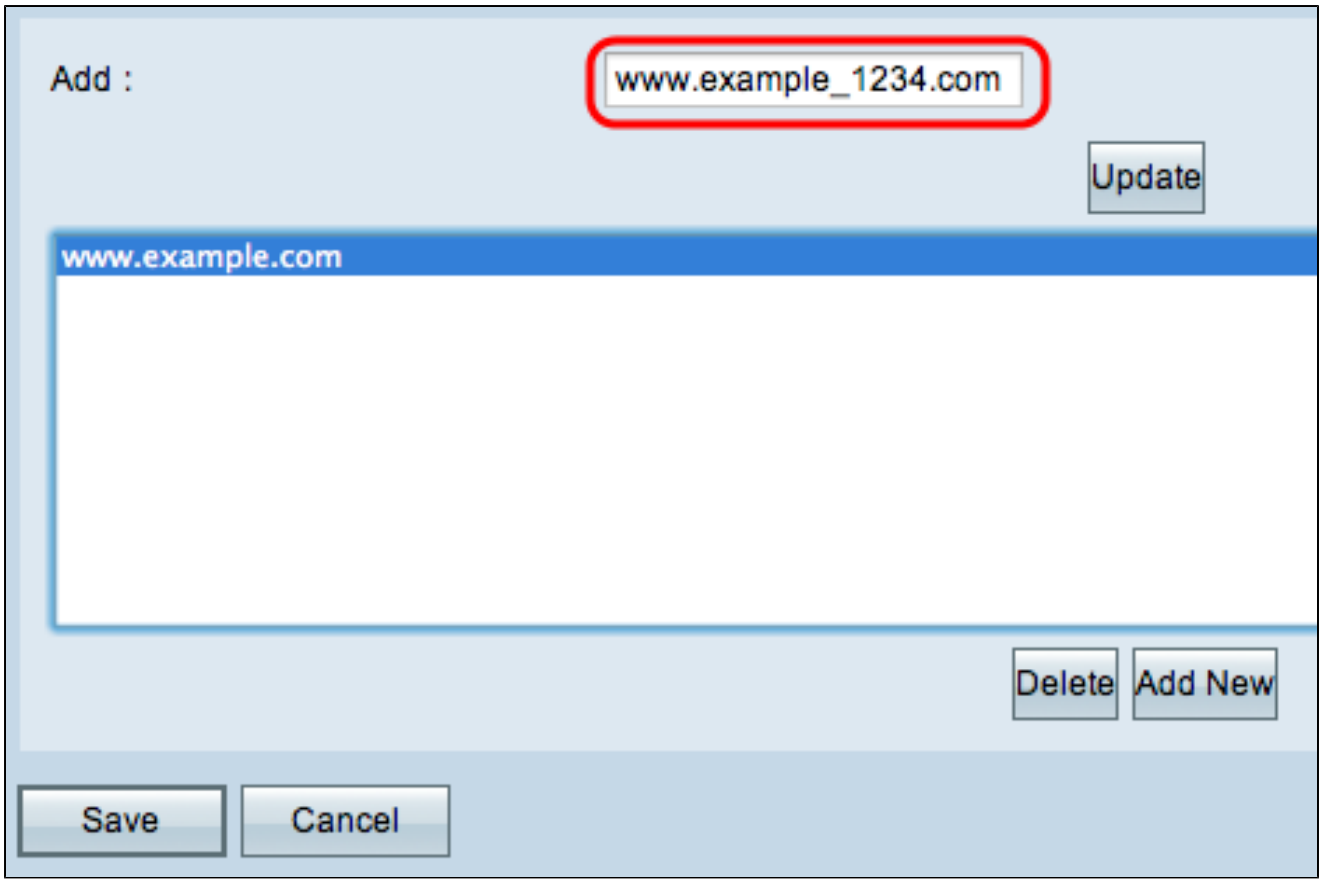
4단계. Save(저장)를 클릭하여 변경 사항을 저장합니다.

트러스트된 도메인 업데이트

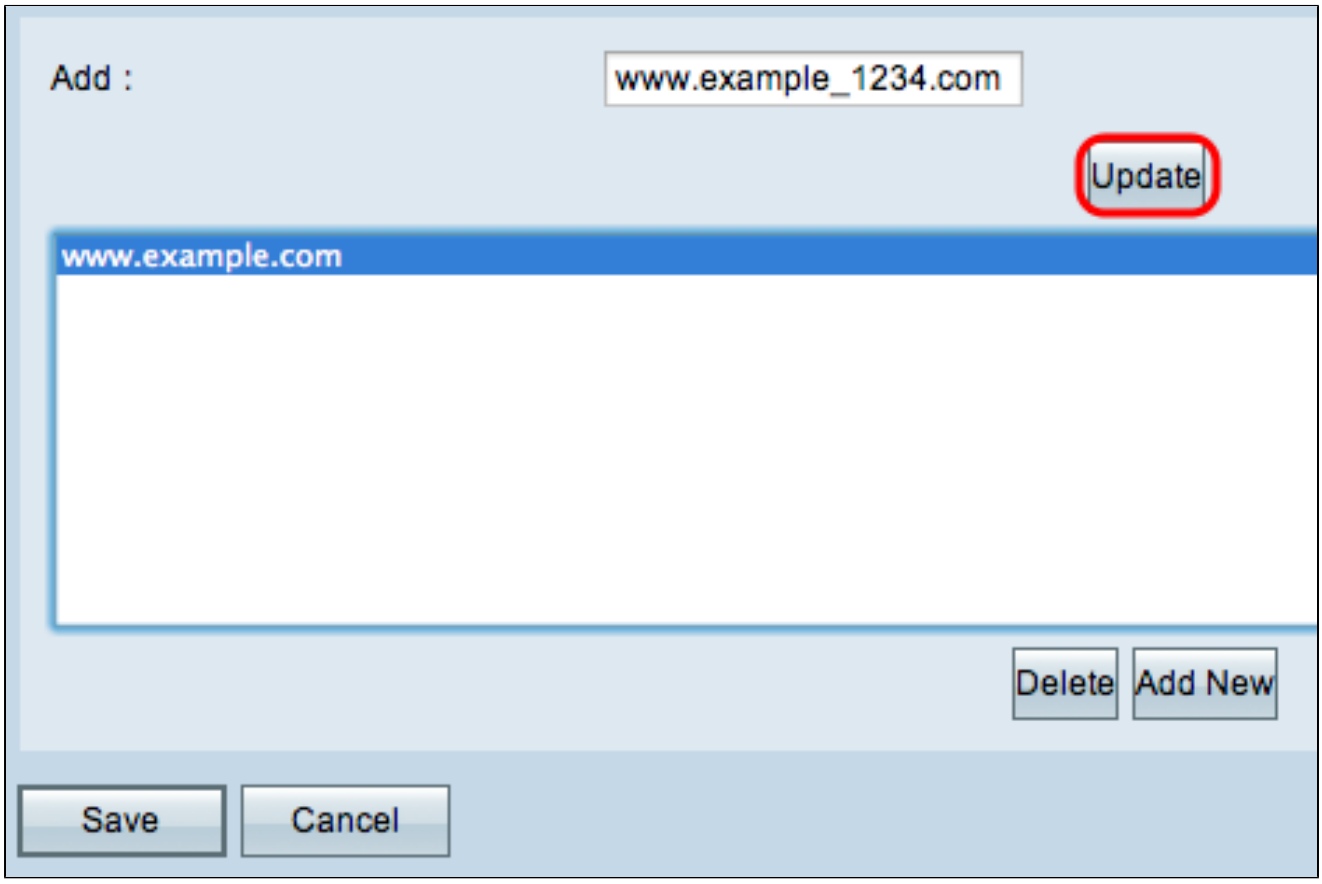
이 섹션에서는 사용자에게 트러스트된 도메인을 수정하는 방법을 안내합니다.



1단계. 신뢰할 수 있는 도메인 목록에서 편집할 도메인을 선택합니다.



2단계. Add(추가) 필드에 필요한 도메인에 대해 업데이트된 도메인 이름을 입력합니다.

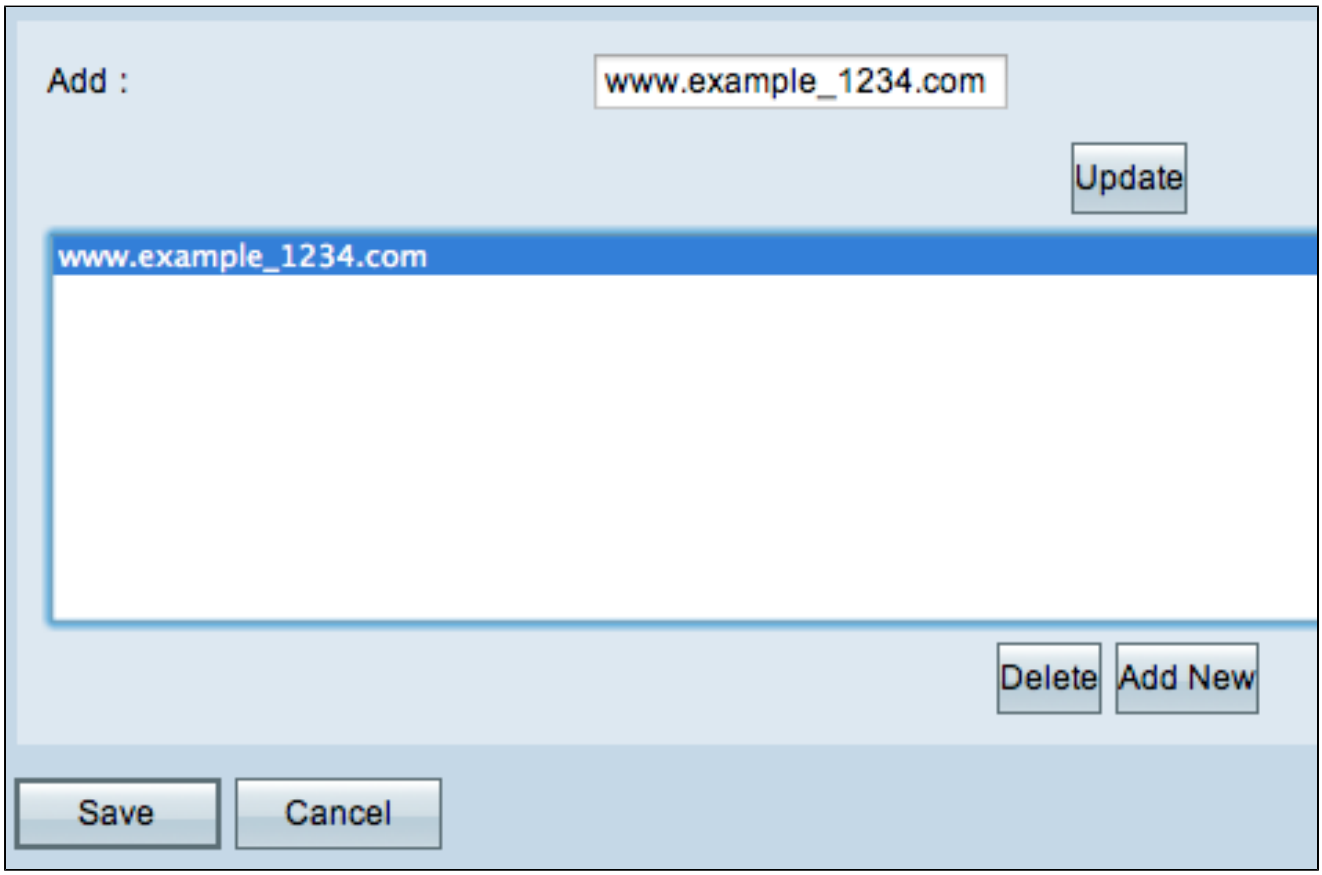


3단계. 업데이트를 클릭합니다.

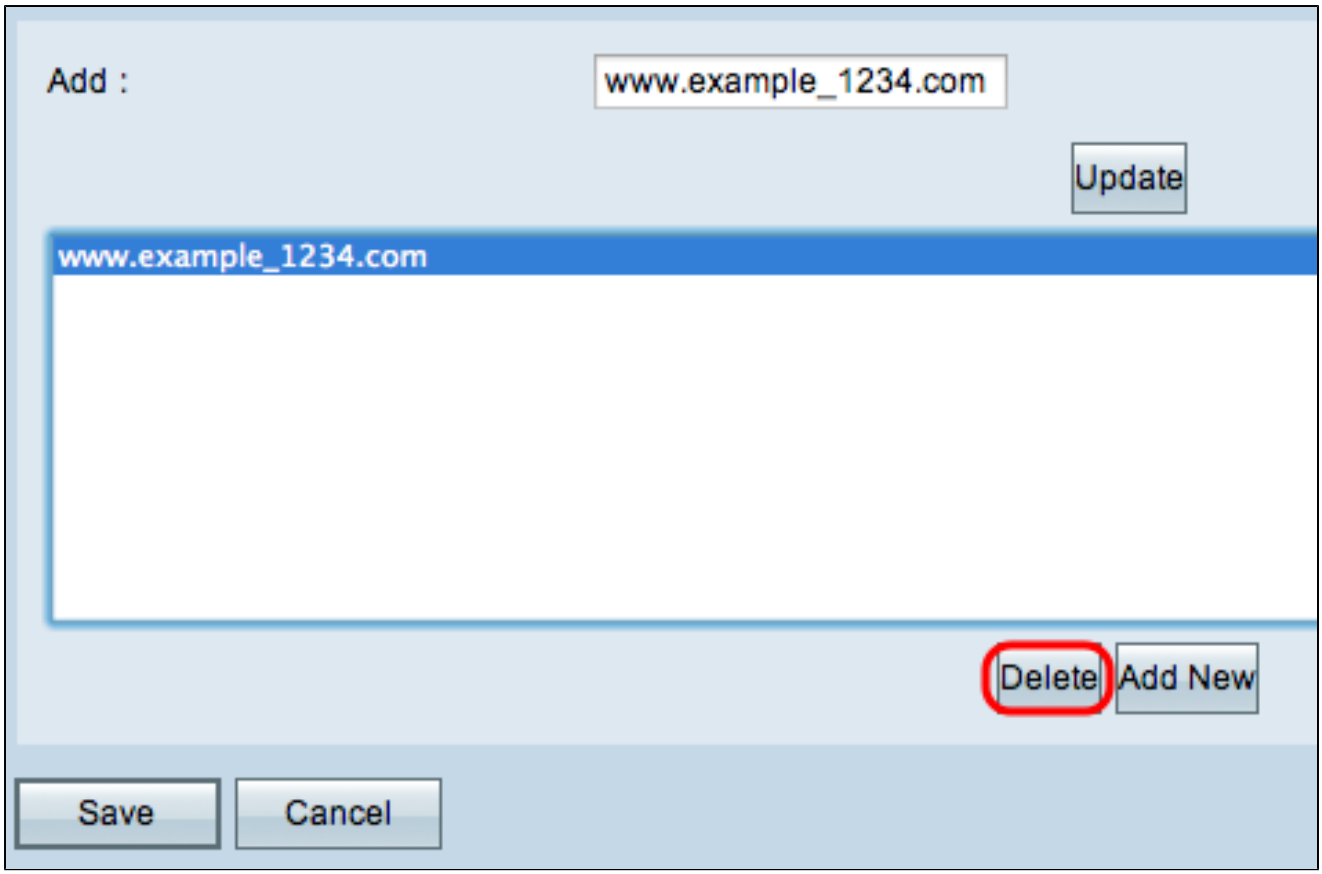
4단계. Save(저장)를 클릭하여 변경 사항을 저장합니다.

트러스트된 도메인 삭제

이 섹션에서는 사용자에게 트러스트된 도메인을 삭제하는 방법을 안내합니다.



1단계. 삭제할 도메인을 선택합니다.



2단계. 삭제를 클릭합니다. 도메인이 삭제됩니다.

3단계. Save(저장)를 클릭하여 변경 사항을 저장합니다.