RV016, RV042, RV042G 및 RV082에서 일반 방화벽 설정 구성

목표

RV016, RV042, RV042G 및 RV082의 내장형 방화벽은 기본적으로 특정 종류의 트래픽을 차단합니다. HTTPS, TCP 및 ICMP 요청, 원격 관리 트래픽과 같이 차단되는 트래픽의 종류를 조정할 수 있습니다. 방화벽 자체도 활성화 또는 비활성화할 수 있습니다. 또한 보안 취약점이 될 수 있는 웹 사이트의 특정 부분도 차단할 수 있습니다. 이러한 웹 사이트 기능은 차단을 해제하면 잠재적으로 해로운 데이터를 컴퓨터에 저장할 수 있습니다.

이 문서의 목적은 RV016, RV042, RV042G 및 RV082에서 일반 방화벽 설정을 구성하는 방법을 설명하는 것입니다.

적용 가능한 디바이스

· RV016

· RV042

· RV042G

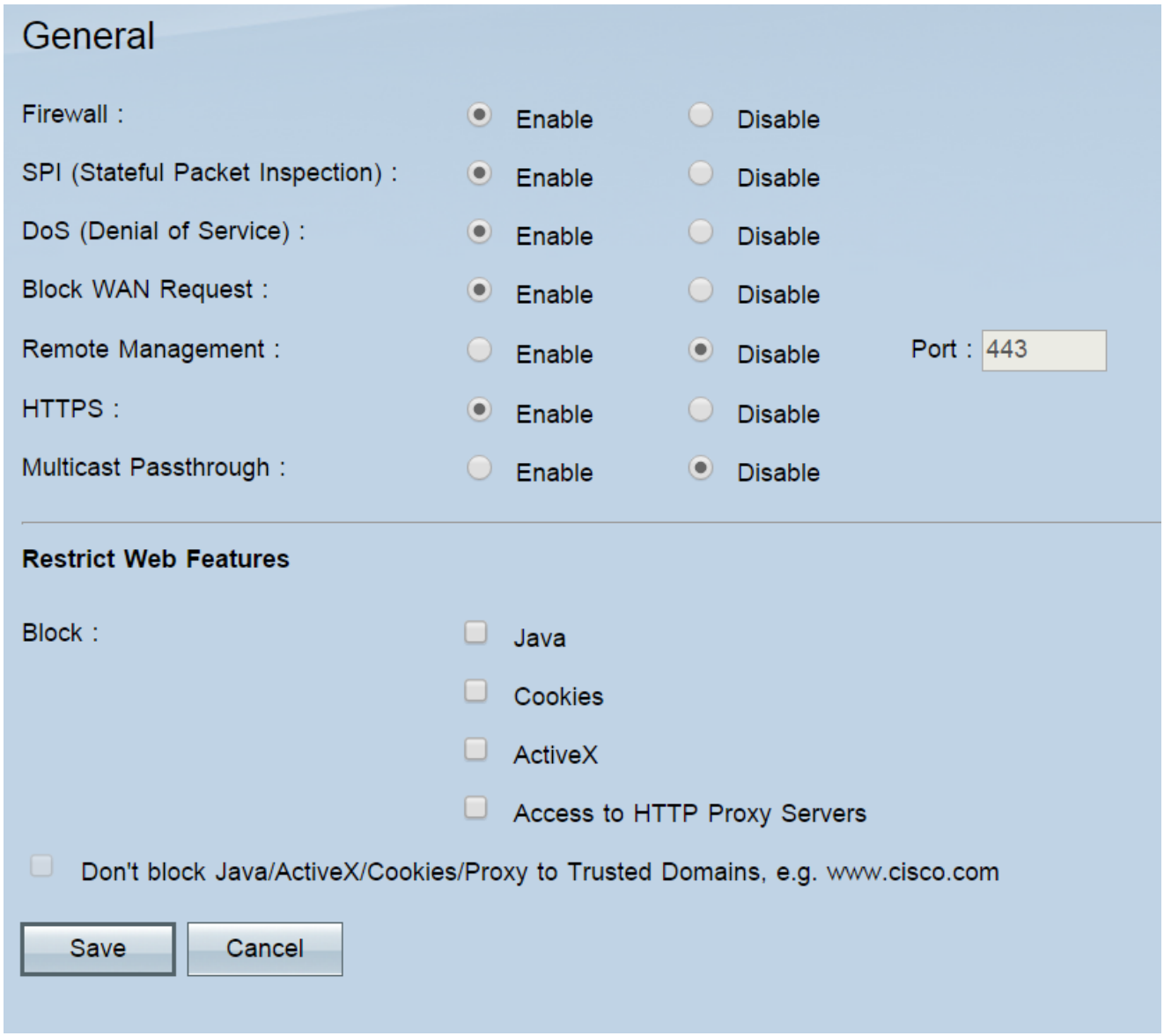
· RV082

소프트웨어 버전

· v4.2.3.06

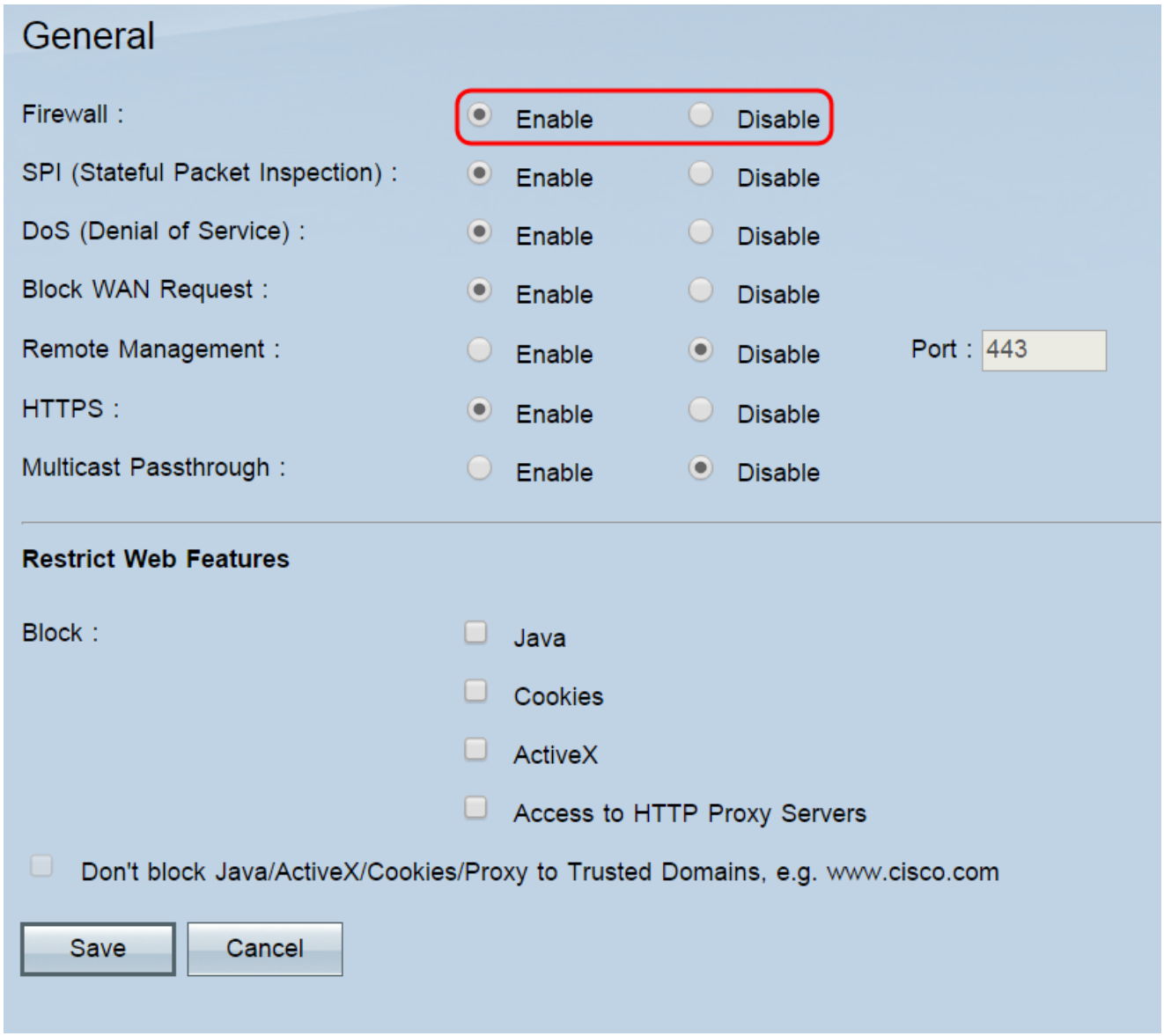
일반 방화벽 설정 구성

1단계. 웹 컨피그레이션 유틸리티에 로그인하고 Firewall > General을 선택합니다. General(일반) 페이지가 열립니다.



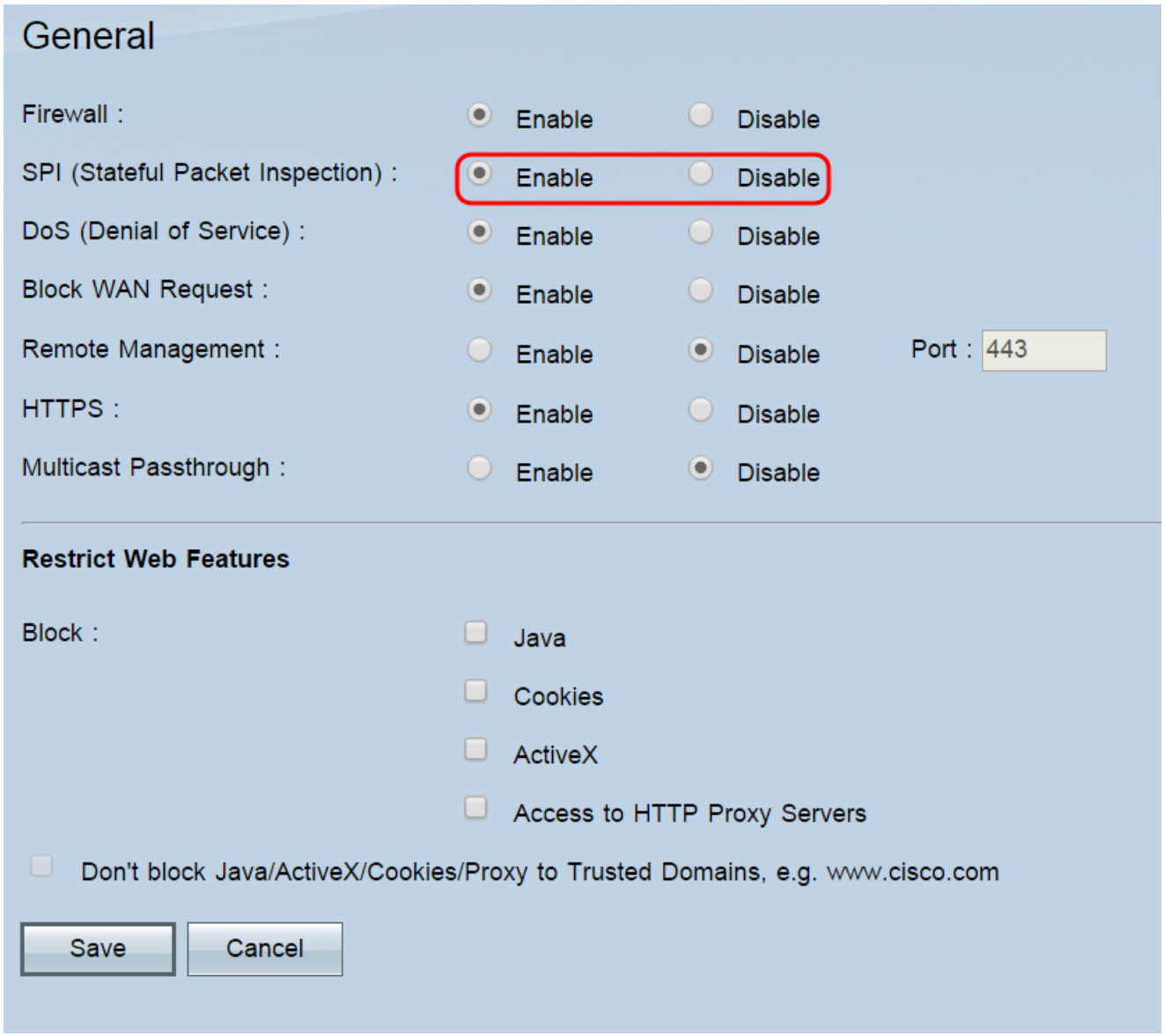
일반 기능

1단계. Firewall 필드에서 라디오 버튼을 선택하여 방화벽을 활성화 또는 비활성화합니다. 방화벽은 기본적으로 활성화되어 있습니다. 비활성화하는 것은 권장되지 않습니다. 방화벽을 비활성화하면 액세스 규칙 및 콘텐츠 필터도 비활성화됩니다.

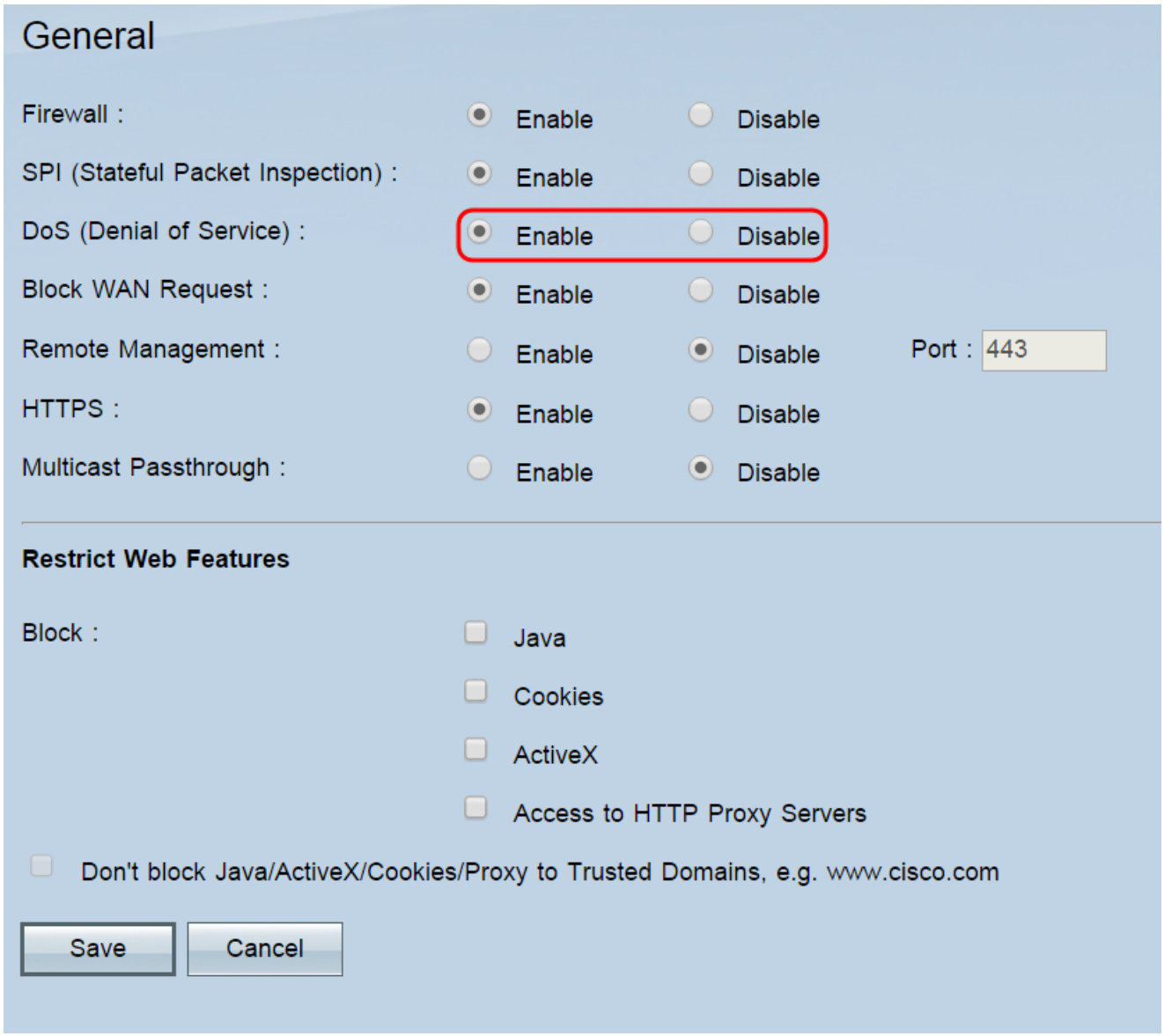


참고: 방화벽을 비활성화하려는 경우 기본 관리자 비밀번호를 계속 사용하고 있으면 비밀번호를 변경해야 한다는 경고 메시지가 표시됩니다. 비밀번호를 변경할 때까지 방화벽을 비활성화할 수 없습니다. OK(확인)를 클릭하여 비밀번호 페이지로 이동하거나, Cancel(취소)을 클릭하여 이 페이지를 계속 진행합니다.

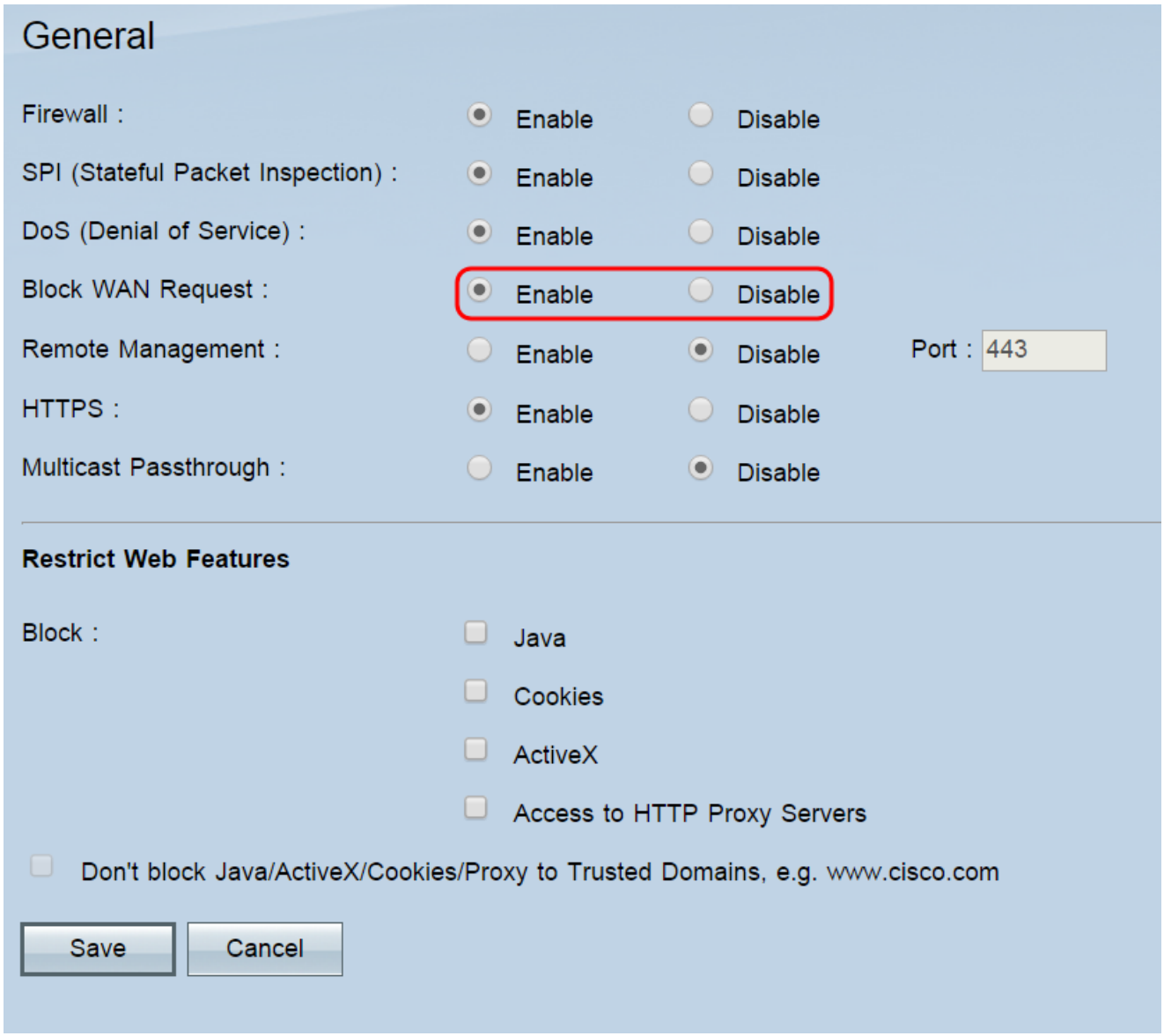
2단계. SPI(Stateful Package Inspection)에서 Enable 또는 Disable 라디오 버튼을 선택합니다. SPI는 기본적으로 활성화되어 있습니다. 이 기능을 사용하면 라우터가 처리할 패킷을 전송하기 전에 모든 패킷을 검사할 수 있습니다. 이는 방화벽이 활성화된 경우에만 활성화할 수 있습니다.



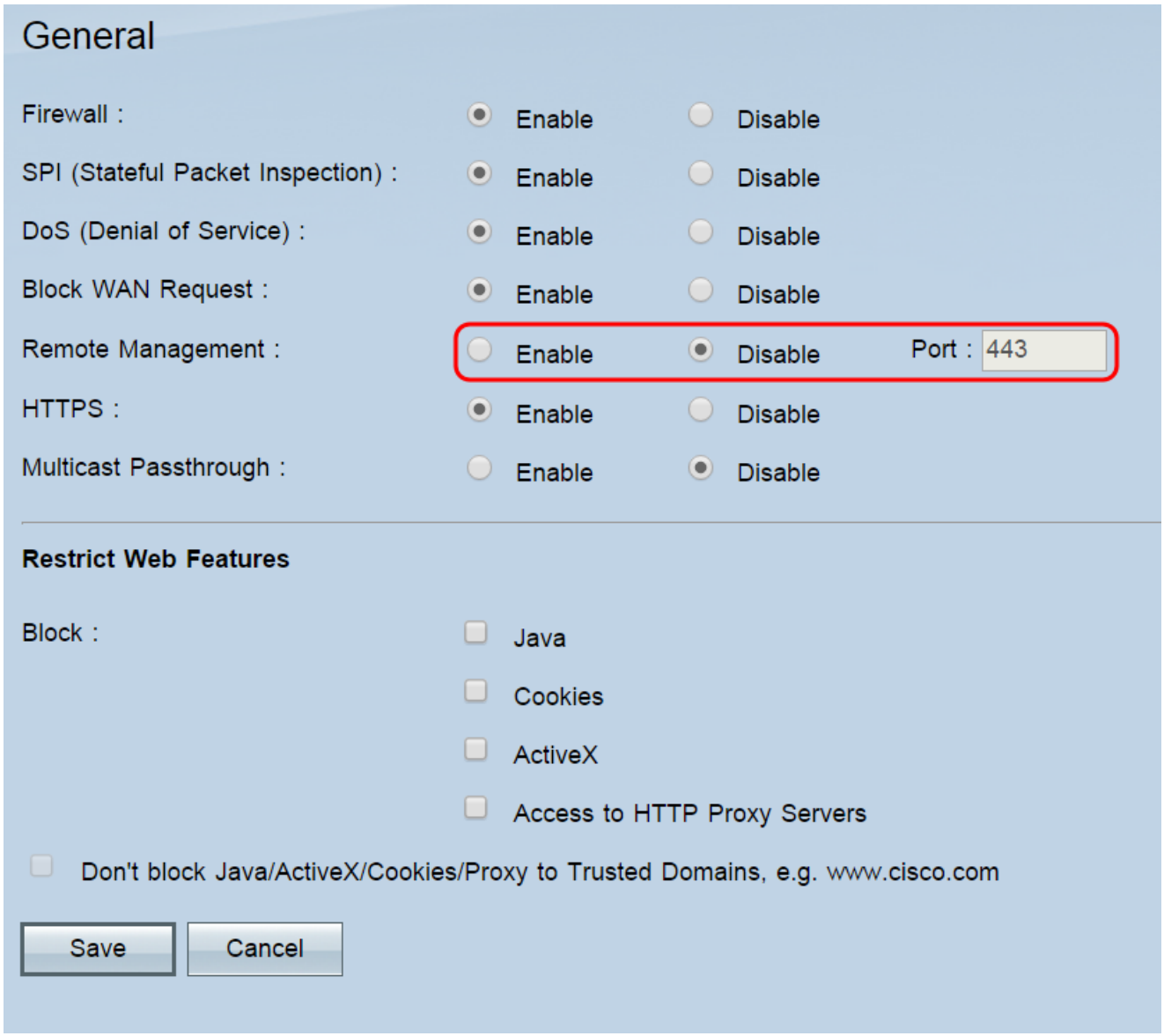
3단계. DoS(Denial of Service) 필드에서 Enable 또는 Disable 라디오 버튼을 선택합니다. DoS는 기본적으로 활성화되어 있습니다. 이 기능은 내부 네트워크에서 외부 공격(예: SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing 및 리어셈블리 공격)을 방지합니다. 이는 방화벽이 활성화된 경우에만 활성화할 수 있습니다.



4단계. Block WAN Request(WAN 요청 차단) 필드에서 Enable(활성화) 또는 Disable(비활성화) 라디오 버튼을 선택합니다. WAN 요청 차단은 기본적으로 활성화되어 있습니다. 이 기능을 사용하면 라우터가 WAN에서 승인되지 않은 TCP 및 ICMP 요청을 삭제할 수 있으므로 해커가 WAN IP 주소를 ping하여 라우터를 찾을 수 없습니다. 이는 방화벽이 활성화된 경우에만 활성화할 수 있습니다.



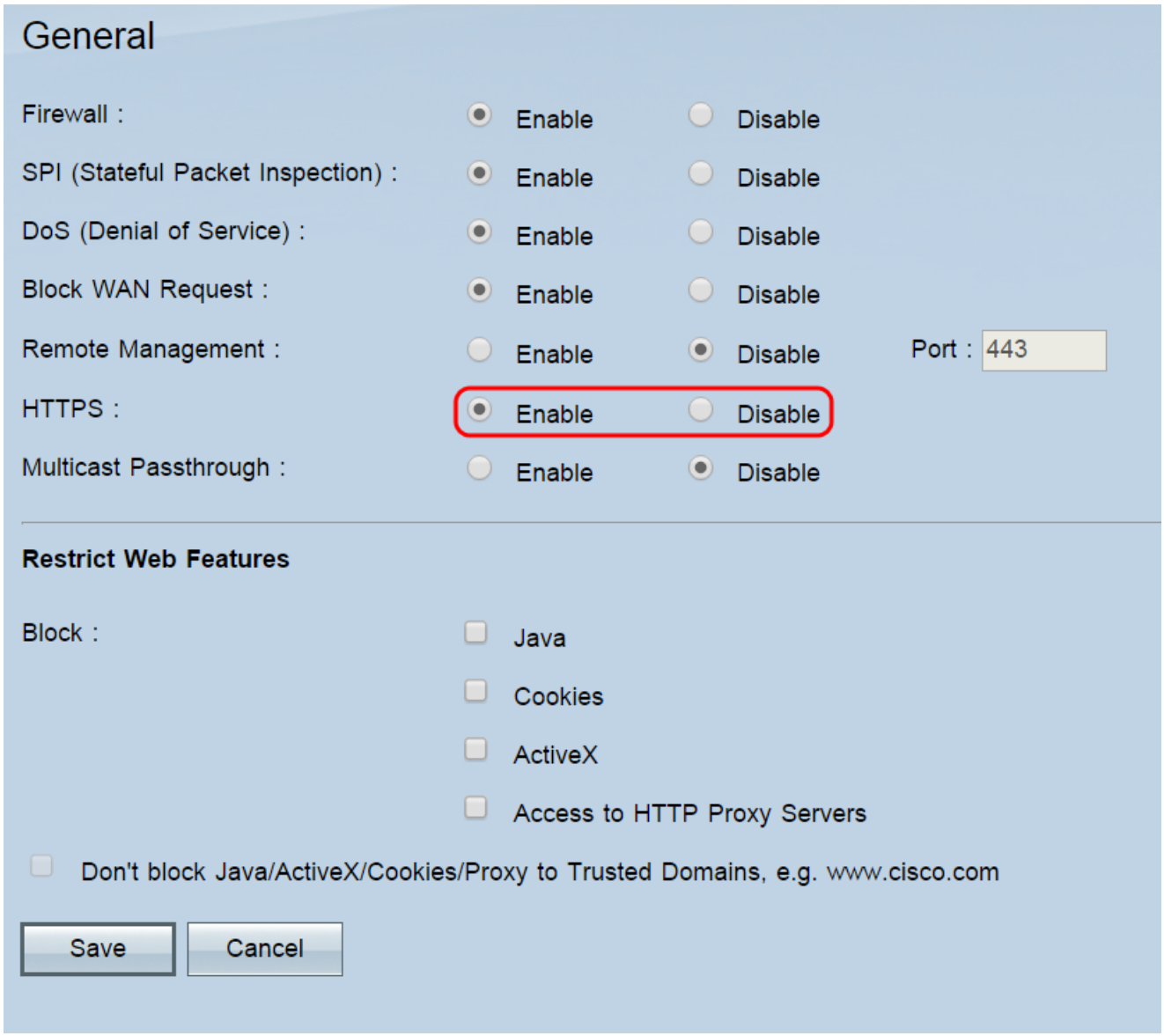
5단계. Remote Management(원격 관리) 필드에서 Enable(활성화) 또는 Disable(비활성화) 라디오 버튼을 선택합니다. 원격 관리는 기본적으로 비활성화되어 있습니다. 이 기능을 사용하면 인터넷 어디에서나 라우터의 웹 구성 유틸리티에 연결할 수 있습니다. 이 기능을 활성화한 경우 Port 필드에서 원격 연결에 사용되는 포트를 설정할 수 있습니다. 기본값은 443입니다.



참고: 기본 관리자 비밀번호를 사용하는 경우 비밀번호를 변경해야 한다는 경고 메시지가 표시됩니다. 비밀번호 페이지로 계속하려면 확인을 클릭하고 이 페이지를 유지하려면 취소를 클릭하십시오. 비밀번호를 변경하면 권한이 없는 사용자가 기본 비밀번호를 사용하여 라우터에 액세스하지 못하게 됩니다.

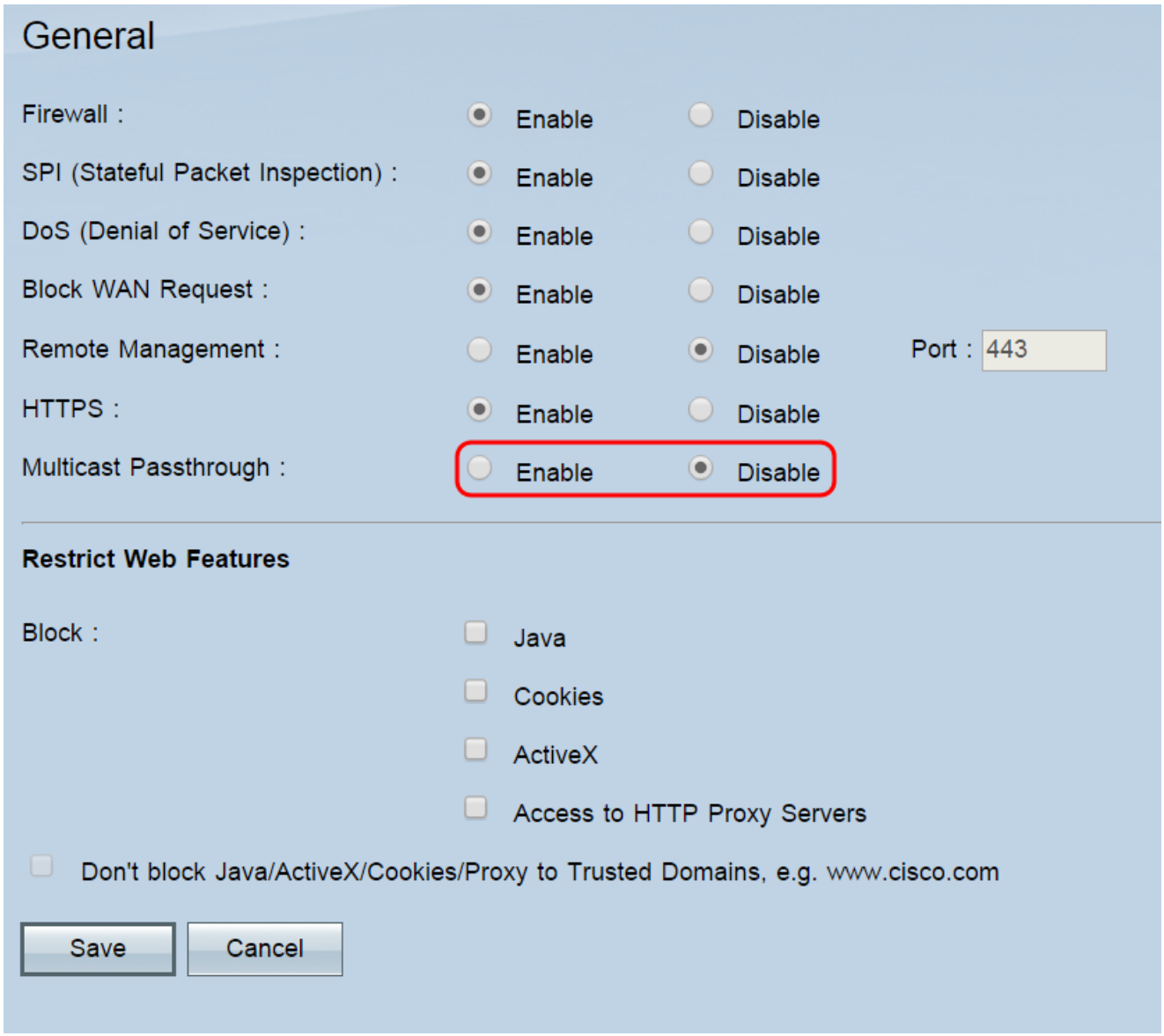
참고: 원격 관리가 활성화된 경우 http://<라우터의 WAN IP 주소>:<port>를 입력하여 모든 브라우저에서 웹 구성 유틸리티에 액세스할 수 있습니다. HTTPS가 활성화된 경우 https://<라우터의 WAN IP 주소>:<port>를 대신 입력합니다.

6단계. HTTPS 필드에서 Enable 또는 Disable 라디오 버튼을 선택합니다. HTTPS는 기본적으로 활성화되어 있습니다. 이 기능은 보안 HTTP 세션을 허용합니다.



참고: 이 기능이 비활성화되면 사용자는 QuickVPN을 사용하여 연결할 수 없습니다.

7단계. Multicast Passthrough 필드에서 Enable 또는 Disable 라디오 버튼을 선택합니다. 멀티캐스트 통과는 기본적으로 비활성화되어 있습니다. 이 기능을 사용하면 IP 멀티캐스트 패킷을 해당 LAN 디바이스에 브로드캐스트할 수 있으며, 인터넷 게임, 비디오 컨퍼런싱 및 멀티미디어 애플리케이션에 사용됩니다.

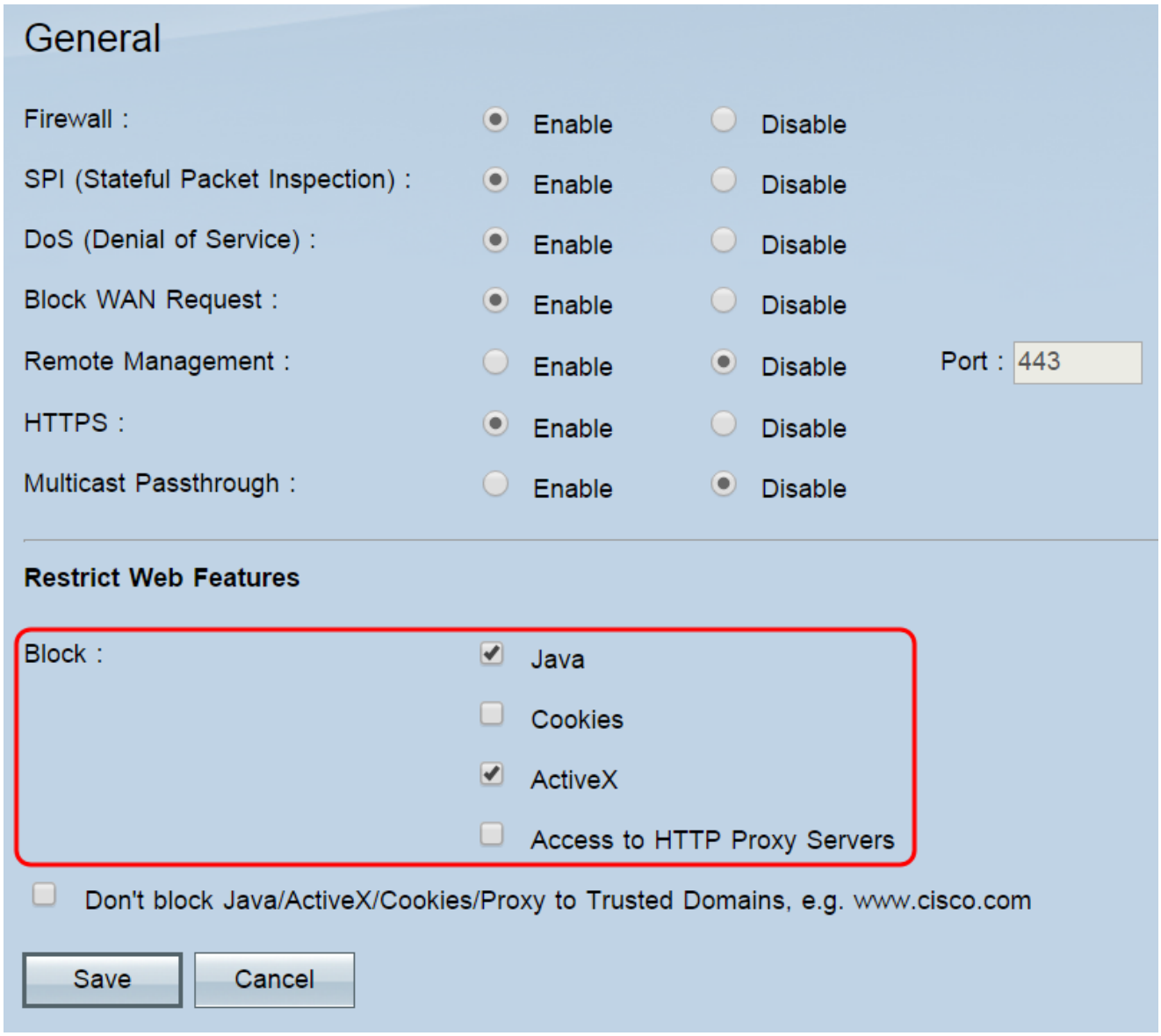


참고: RV016, RV042, RV042G 및 RV082는 IPSec 터널을 통한 멀티캐스트 트래픽 전달을 지원하지 않습니다.

8단계. 저장을 클릭합니다.

웹 기능

1단계. Block(차단) 필드에서 방화벽에서 차단하려는 웹 기능의 확인란을 선택합니다. 일부 도메인에 대해 차단된 기능을 허용하려면 2단계에서 해당 도메인을 예외 목록에 추가할 수 있습니다. 기본적으로 차단된 기능은 없습니다.



옵션은 다음과 같습니다.

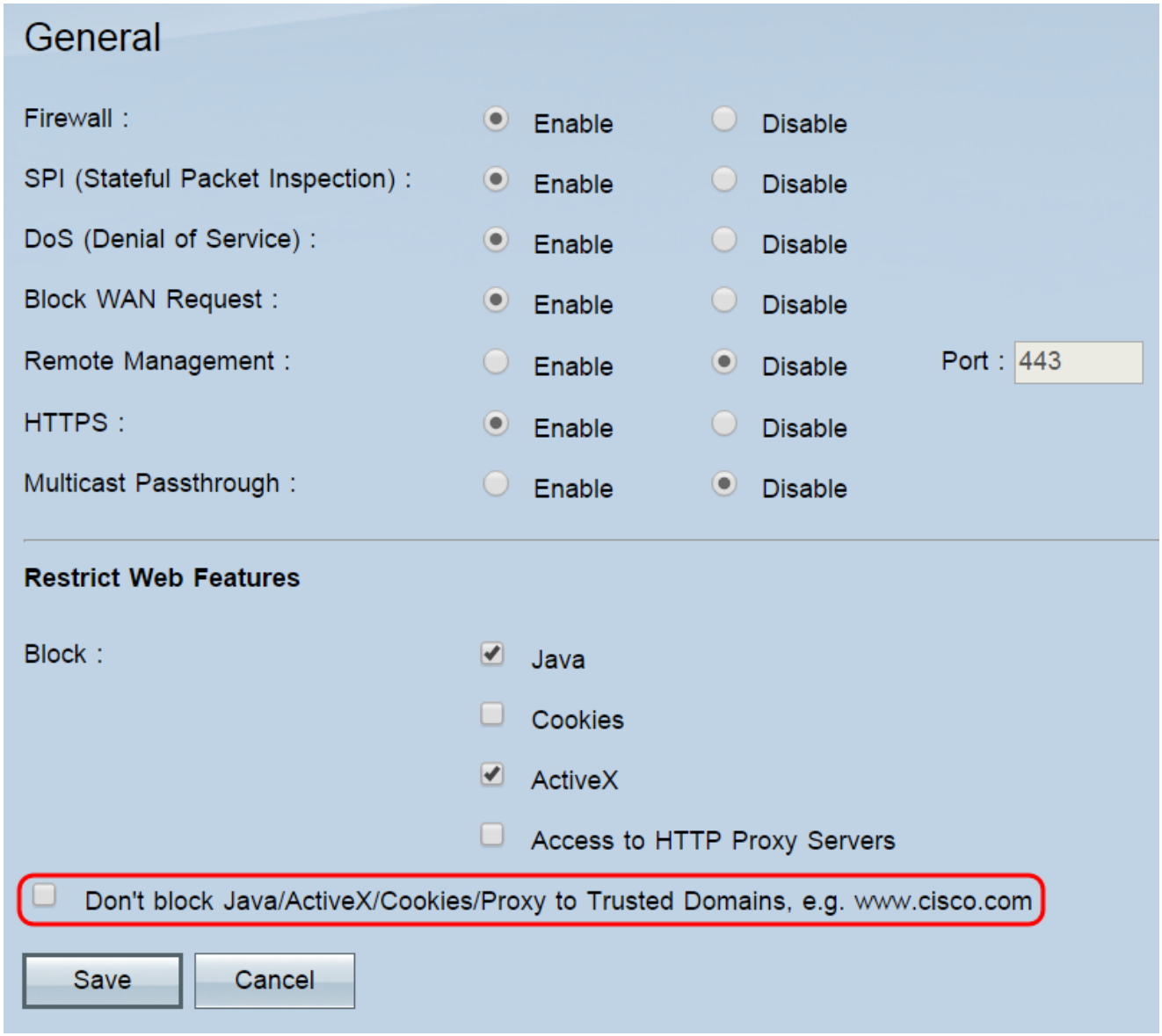
· Java — Java는 웹 사이트를 위한 프로그래밍 언어입니다. 이 확인란을 선택하면 Java 애플릿(웹 페이지에 포함되지만 웹 브라우저 외부에서 실행되는 소규모 프로그램)이 차단되지만 이 기능을 사용하는 웹 사이트가 잘못 작동할 수 있습니다.

· 쿠키 — 쿠키는 웹 사이트가 사용자의 PC에 로컬로 저장하는 데이터입니다. 쿠키를 차단하면 쿠키에 의존하는 웹 사이트가 잘못 작동할 수 있습니다.

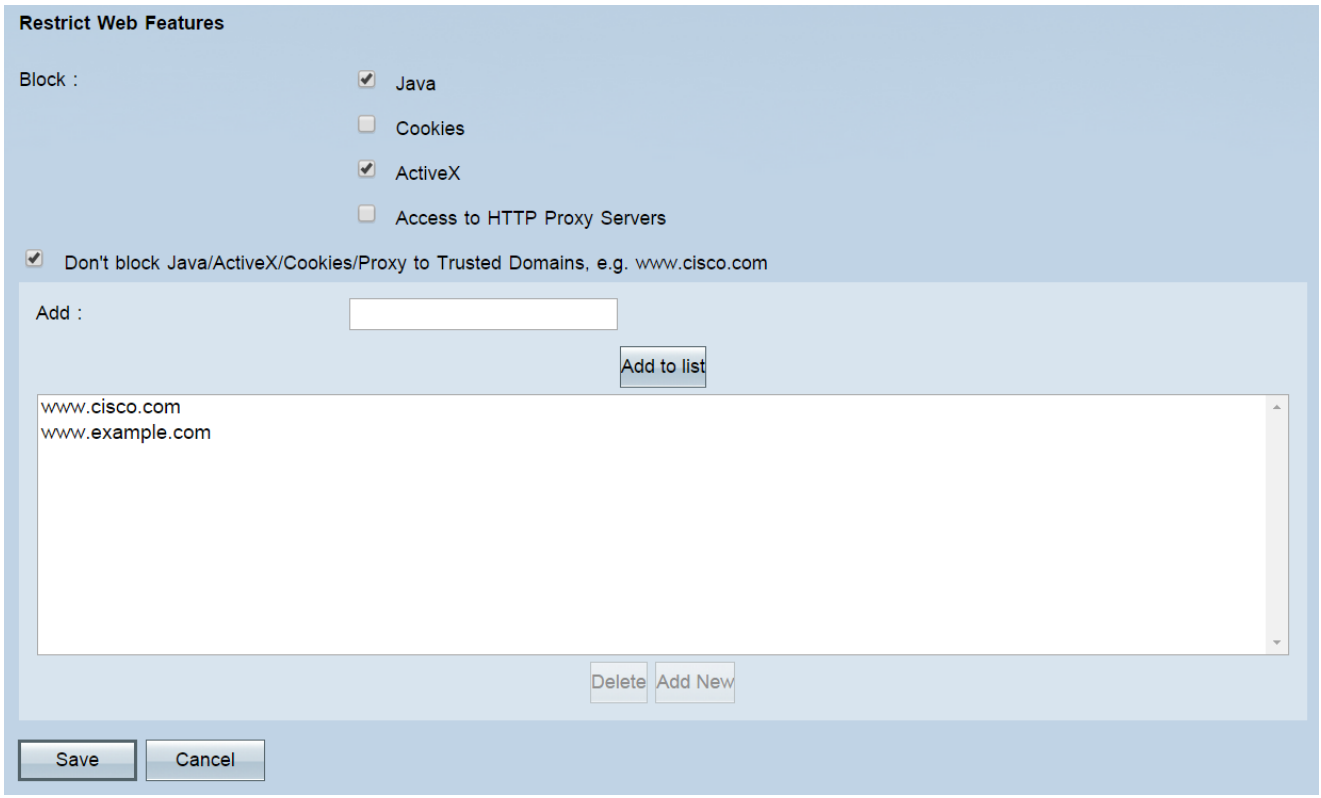
· ActiveX — ActiveX는 Microsoft에서 개발한 소프트웨어 프레임워크입니다. 이 프레임워크는 웹 페이지의 특정 부분을 실행하는 데 사용할 수 있습니다. 이 확인란을 선택하면 이러한 구성 요소가 차단되지만 ActiveX를 사용하는 웹 사이트가 잘못 작동할 수 있습니다.

· HTTP 프록시 서버에 액세스 — HTTP 프록시 서버에 대한 액세스를 차단하려면 이 확인란을 선택합니다. WAN 프록시 서버를 사용하면 라우터의 보안이 손상될 수 있습니다.

2단계. Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains(신뢰할 수 있는 도메인에 Java/ActiveX/Cookies/프록시 차단 안 함) 확인란을 선택하여 신뢰할 수 있는 도메인 목록을 엽니다. 이 목록에서 차단된 웹 기능이 허용되는 도메인을 추가하거나 제거할 수 있습니다. 이 필드는 기본적으로 선택되지 않으며 기능을 차단하기 위해 이전 상자를 선택한 경우에만 사용할 수 있습니다. 선택하지 않으면 모든 웹 사이트에서 기능이 차단됩니다.



3단계. (선택 사항) Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains(Java/ActiveX/Cookies/Proxy to Trusted Domains(신뢰할 수 있는 도메인에 대한 Java/ActiveX/Cookies/프록시 차단 안 함) 확인란을 선택하면 신뢰할 수 있는 도메인 목록이 나타납니다. 목록에 도메인을 추가하려면 Add 필드에 도메인을 입력하고 Add to List를 클릭합니다. 기존 도메인을 수정하려면 목록에서 해당 도메인을 클릭한 다음 Add(추가) 필드에서 수정한 다음 Update(업데이트)를 클릭합니다. 목록에서 도메인을 삭제하려면 목록에서 도메인을 클릭한 다음 Delete를 클릭합니다.



4단계. 저장을 클릭합니다.

General

Firewall :	Enable	Disable	
SPI (Stateful Packet Inspection) :	Enable	Disable	
DoS (Denial of Service) :	Enable	Disable	
Block WAN Request :	Enable	Disable	
Remote Management :	Enable	Disable	Port : 443
HTTPS :	Enable	Disable	
Multicast Passthrough :	Enable	Disable	

Restrict Web Features

Block :

- [x] Java
- [ ] Cookies
- [x] ActiveX
- [ ] Access to HTTP Proxy Servers

[ ] Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains, e.g. www.cisco.com

Save Cancel

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.