

RV130 및 RV130W에서 기본 방화벽 설정을 구성하는 방법

목표

기본 방화벽 설정은 인바운드 및 아웃바운드 인터넷 트래픽을 선택적으로 차단 및 허용하는 데 사용하는 규칙을 생성하고 적용하여 네트워크를 보호할 수 있습니다. Universal Plug and Play와 같은 기능을 사용하면 추가 컨피그레이션 없이 네트워크에서 디바이스를 서로 쉽게 연결할 수 있습니다.

UPnP(Universal Plug and Play)를 사용하면 디바이스와 통신할 수 있는 디바이스를 자동으로 검색할 수 있습니다. 콘텐츠를 차단하면 특정 콘텐츠를 장치에 보내 보안을 손상시키거나 악성 소프트웨어로 컴퓨터를 감염시킬 수 있으므로 컴퓨터를 보호하는 데 도움이 됩니다. 선택한 포트의 특정 콘텐츠를 차단하는 기능은 방화벽 보안 강화에 유용합니다.

이 문서의 목적은 RV130 및 RV130W에서 기본 방화벽 설정을 구성하는 방법을 설명하는 것입니다.

적용 가능한 장치

- RV130
- RV130W

소프트웨어 버전

- v1.0.1.3

기본 방화벽 설정 구성

1단계. 웹 구성 유틸리티에 로그인하고 **Firewall > Basic Settings**를 선택합니다. 기본 설정 페이지가 열립니다.

Basic Settings

IP Address Spoofing Protection:	<input checked="" type="checkbox"/> Enable
DoS Protection:	<input checked="" type="checkbox"/> Enable
Block WAN Ping Request:	<input type="checkbox"/> Enable
LAN/VPN Web Access:	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
Remote Management:	<input checked="" type="checkbox"/> Enable
Remote Access:	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS
Remote Upgrade:	<input checked="" type="checkbox"/> Enable
Allowed Remote IP Address:	<input checked="" type="radio"/> Any IP Address <input type="radio"/> 0 . 0 . 0 . 0 - 0
Remote Management Port	443 (Range: 1 - 65535, Default: 443)
IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	<input type="checkbox"/> Enable
SIP ALG	<input type="checkbox"/> Enable

UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input type="checkbox"/> Enable

Block Java:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Proxy:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>

Save Cancel

2단계. *IP Address Spoofing Protection*(IP 주소 스푸핑 보호) 필드에서 Enable(활성화) 확인란을 선택하여 IP 주소 스푸핑으로부터 네트워크를 보호합니다. IP 주소 스푸핑은 권한이 없는 사용자가 자신의 IP 주소를 사용하여 다른 신뢰할 수 있는 디바이스를 가장하여 네트워크에 대한 액세스를 얻으려고 시도하는 경우를 말합니다. 을(를) 활성화하는 것이 좋습니다. *IP 주소 스푸핑 보호*.

IP Address Spoofing Protection:	<input checked="" type="checkbox"/> Enable
DoS Protection:	<input checked="" type="checkbox"/> Enable
Block WAN Ping Request	<input checked="" type="checkbox"/> Enable

3단계. *DoS Protection*(DoS 보호) 필드에서 Enable(활성화) 확인란을 선택하여 DoS 공격으로부터 네트워크를 보호합니다. Denial of Service Protection은 DDoS(Distributed Denial of Service) 공격으로부터 네트워크를 보호하는 데 사용됩니다. DDoS 공격은 네트워크의 리소스를 사용할 수 없는 지점까지 네트워크를 플러딩하기 위한 것입니다.

IP Address Spoofing Protection:	<input checked="" type="checkbox"/> Enable
DoS Protection:	<input checked="" type="checkbox"/> Enable
Block WAN Ping Request	<input checked="" type="checkbox"/> Enable

4단계. *Block WAN Ping Request*(WAN Ping 요청 차단) 필드에서 Enable(활성화) 확인란을 선택하여 외부 WAN 네트워크에서 디바이스에 대한 ping 요청을 중지합니다.

IP Address Spoofing Protection:	<input checked="" type="checkbox"/> Enable
DoS Protection:	<input checked="" type="checkbox"/> Enable
Block WAN Ping Request:	<input checked="" type="checkbox"/> Enable

5단계. 나열된 *LAN/VPN Web Access*(LAN/VPN 웹 액세스)에서 *Remote Management Port*(원격 관리 포트)까지의 필드는 LAN 및 Remote Management Web Access(원격 관리 웹 액세스)를 구성하는 데 사용됩니다. 이러한 구성에 대한 자세한 내용은 [RV130 및 RV130W에서 LAN 및 원격 관리 웹 액세스 구성을 참조하십시오](#).

IP Address Spoofing Protection:	<input checked="" type="checkbox"/> Enable
DoS Protection:	<input checked="" type="checkbox"/> Enable
Block WAN Ping Request:	<input checked="" type="checkbox"/> Enable
LAN/VPN Web Access:	<input type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS
Remote Management:	<input type="checkbox"/> Enable
Remote Access:	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Remote Upgrade:	<input type="checkbox"/> Enable
Allowed Remote IP Address:	<input checked="" type="radio"/> Any IP Address <input type="radio"/> 0 . 0 . 0 . 0 - 0
Remote Management Port:	443 (Range: 1 - 65535, Default: 443)
IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	<input checked="" type="checkbox"/> Enable
SIP ALG	<input checked="" type="checkbox"/> Enable

6단계. *IPv4 Multicast Passthrough:(IGMP Proxy)* 필드에서 Enable(활성화) 확인란을 선택하여 IPv4에 대한 멀티캐스트 패스스루를 활성화합니다. 이렇게 하면 그룹 IGMP 패킷이 외부 WAN 네트워크에서 내부 LAN으로 전달됩니다.

IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	<input checked="" type="checkbox"/> Enable
SIP ALG	<input checked="" type="checkbox"/> Enable

7단계. *IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)* 필드에서 Enable(활성화) 확인란을 선택하여 Multicast Immediate Leave를 활성화합니다. 즉각적인 휴지를 활성화하면 동시 멀티캐스트 그룹 사용 시에도 네트워크의 호스트에 최적의 대역폭 관리가 제공됩니다.

IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	<input checked="" type="checkbox"/> Enable
SIP ALG	<input checked="" type="checkbox"/> Enable

8단계. SIP(Session Initiation Protocol) ALG(Application Layer Gateway) 필드에서 **Enable**(활성화) 확인란을 선택하여 SIP 트래픽이 방화벽을 통과하도록 허용합니다. SIP(Session Initiation Protocol)는 IP 네트워크를 통해 음성 및 멀티미디어 통화의 설정을 알리는 플랫폼을 제공합니다. ALG(Application Layer Gateway) 또는 애플리케이션 레벨 게이트웨이라고도 하는 애플리케이션은 애플리케이션 패킷의 페이로드 내에서 IP 주소 정보를 변환하는 애플리케이션입니다.

IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	<input checked="" type="checkbox"/> Enable
SIP ALG	<input checked="" type="checkbox"/> Enable

참고: 디바이스는 최대 256개의 SIP ALG 세션을 지원합니다.

범용 플러그 앤 플레이 구성

1단계. UPnP 필드에서 Enable to enable the Universal Plug and Play (UPnP) 를 선택합니다.

UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input checked="" type="checkbox"/> Enable

2단계. Allow Users to Configure(사용자가 구성할 수 있도록 허용) 필드에서 Enable(활성화) 확인란을 선택하여 UPnP 포트 매핑 규칙을 컴퓨터 또는 다른 UPnP 지원 디바이스에서 UPnP 지원이 활성화된 사용자가 설정할 수 있도록 허용합니다. 비활성화된 경우 디바이스에서 애플리케이션이 전달 규칙을 추가할 수 없습니다.

UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input checked="" type="checkbox"/> Enable

3단계. Allow Users to Disable Internet Access(사용자가 인터넷 액세스를 비활성화하도록 허용) 필드에서 **Enable(활성화)** 확인란을 선택하여 사용자가 인터넷 액세스를 비활성화하도록 허용합니다.

UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input checked="" type="checkbox"/> Enable

콘텐츠 차단

1단계. 디바이스에서 차단하려는 콘텐츠에 해당하는 필드의 확인란을 선택합니다.

Block Java:	<input type="checkbox"/>	<input type="radio"/> Auto	<input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input type="checkbox"/>	<input type="radio"/> Auto	<input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input type="checkbox"/>	<input type="radio"/> Auto	<input type="radio"/> Manual Port: <input type="text"/>
Block Proxy:	<input type="checkbox"/>	<input type="radio"/> Auto	<input type="radio"/> Manual Port: <input type="text"/>

사용 가능한 옵션은 다음과 같이 정의됩니다.

- Java 차단 — Java 애플릿의 다운로드를 차단합니다.
- 쿠키 차단 — 디바이스가 웹 페이지에서 쿠키 정보를 수신하지 못하도록 차단합니다.
- ActiveX 차단 — Windows 운영 체제에서 Internet Explorer를 사용할 때 표시될 수 있는 ActiveX 애플릿을 차단합니다.
- Block Proxy — 디바이스가 프록시 서버를 통해 외부 디바이스로 통신하지 못하도록 차단합니다. 이렇게 하면 디바이스가 방화벽 규칙을 우회할 수 없습니다.

2단계. **자동** 라디오 버튼을 선택하여 특정 콘텐츠의 모든 인스턴스를 자동으로 차단하거나 **수동** 라디오 버튼을 클릭하고 콘텐츠를 차단할 특정 포트를 해당 필드에 입력합니다.

Block Java:	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Auto	<input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input checked="" type="checkbox"/>	<input type="radio"/> Auto	<input checked="" type="radio"/> Manual Port: <input type="text" value="500"/>
Block ActiveX:	<input type="checkbox"/>	<input type="radio"/> Auto	<input type="radio"/> Manual Port: <input type="text"/>
Block Proxy:	<input type="checkbox"/>	<input type="radio"/> Auto	<input type="radio"/> Manual Port: <input type="text"/>

참고: 원하는 숫자를 포트 값 범위(1~65535)에 입력할 수 있습니다.

3단계. **Save(저장)**를 클릭하여 설정을 저장합니다.

4단계. 라우터를 다시 시작하라는 창이 나타납니다. 변경 **사항**을 적용하려면 라우터를 다시 시작하려면 **Yes**를 클릭합니다.

Information ✖

 These configuration changes will only be applied after the router restarts. Would you like to restart the router now?

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.