Hoe de basisfirewall-instellingen op de RV130 en RV130W te configureren

Doel

Basisfirewallinstellingen kunnen uw netwerk beveiligen door regels te maken en toe te passen die het apparaat gebruikt om inkomend en uitgaand internetverkeer selectief te blokkeren en toe te staan.
Dankzij functies als Universal Plug and Play kunt u eenvoudig apparaten op uw netwerk met elkaar verbinden zonder extra configuraties.

Universal Plug and Play (UPnP) maakt automatische detectie van apparaten mogelijk die kunnen communiceren met het apparaat. Het blokkeren van de Inhoud kan helpen uw computer te beveiligen omdat bepaalde inhoud naar uw apparaat kan worden verzonden die veiligheid kan compromitteren of uw computer met kwaadaardige software kan besmetten. De mogelijkheid om specifieke inhoud op de poorten van uw keuze te blokkeren is nuttig voor een betere firewallbeveiliging.

Het doel van dit document is om u te tonen hoe u Basisfirewallinstellingen kunt configureren op de RV130 en RV130W.

Toepasselijke apparaten

•RV130

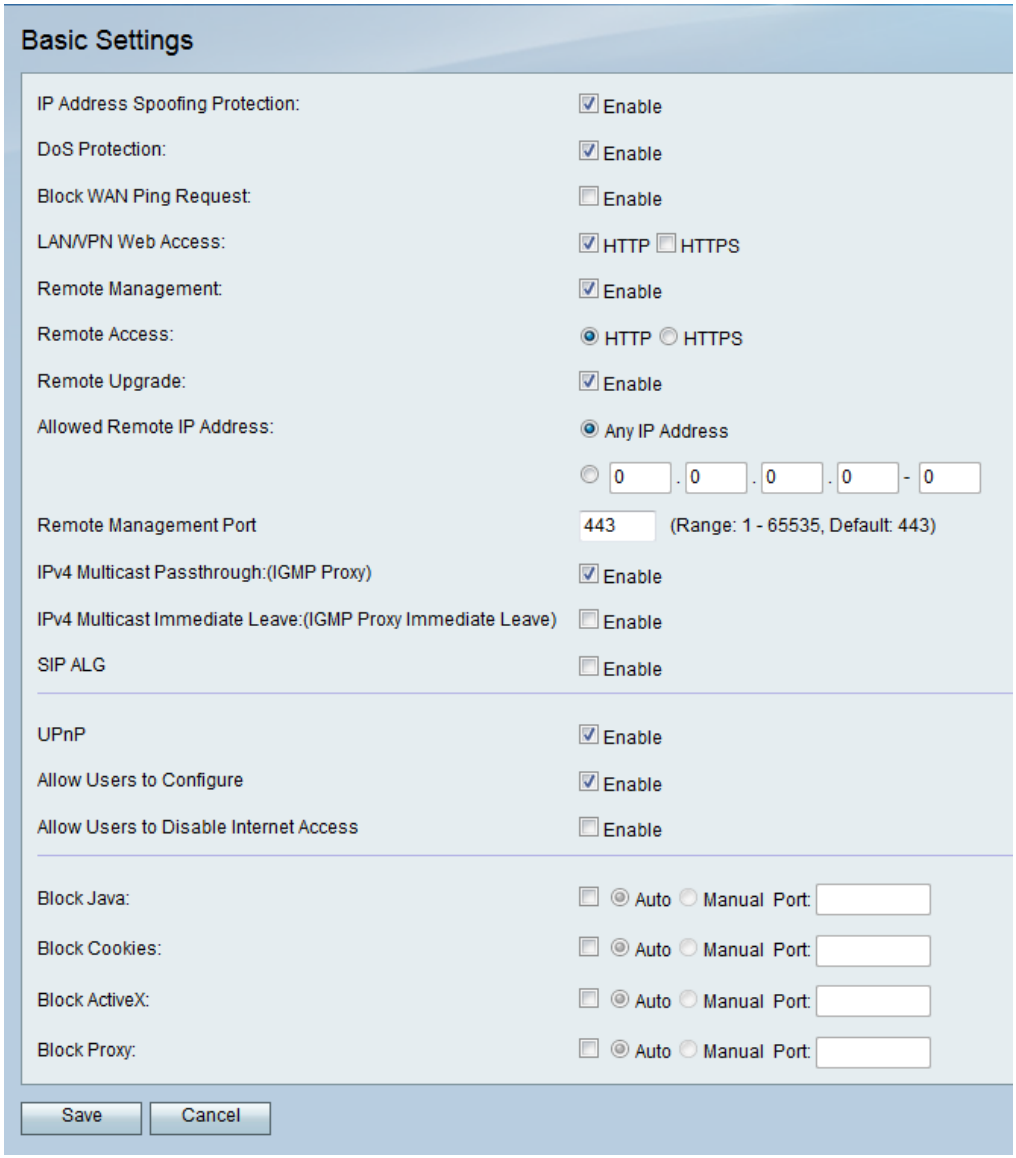
RV130W

Softwareversie

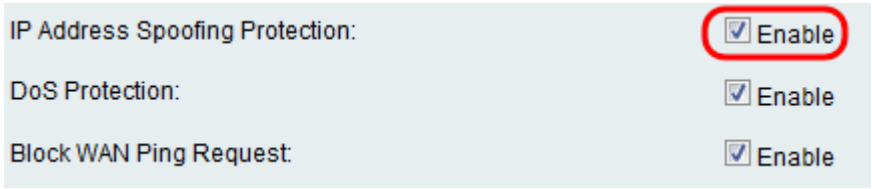
·v1.0.1.3

Basisfirewallinstellingen configureren

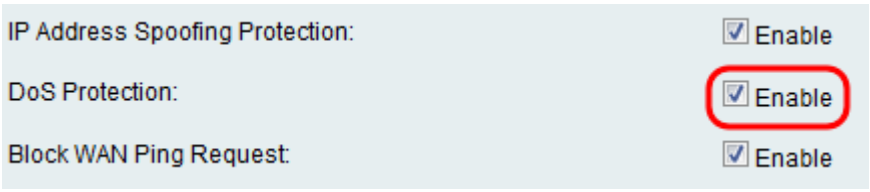
Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **Firewall > Basisinstellingen**. De pagina Basisinstellingen wordt geopend:



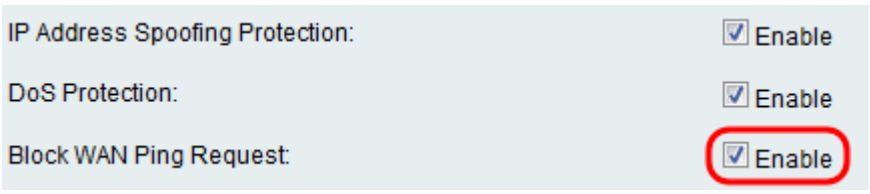
Stap 2. Selecteer in het veld *IP Address Spoofing Protection* het aanvinkvakje **Enable** om uw netwerk te beschermen tegen IP-adresspoofing. IP Address Spoofing is wanneer een onbevoegde gebruiker probeert toegang te krijgen tot een netwerk door een ander vertrouwd apparaat te imiteren met behulp van zijn IP-adres als zijn eigen. Aanbevolen wordt om *Bescherming tegen IP-adresspeling.*



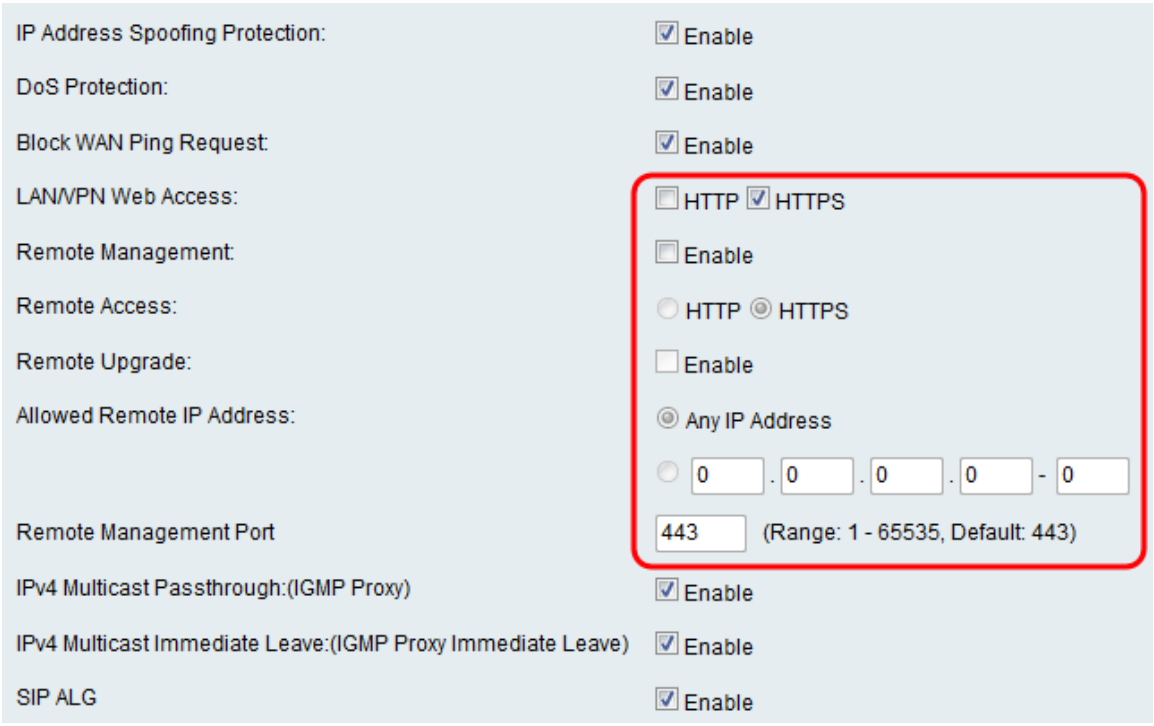
Stap 3. Schakel in het veld *DoS Protection* het aanvinkvakje **Enable** in om uw netwerk te beschermen tegen Denial of Service-aanvallen. De Bescherming van de ontkenning van de Dienst wordt gebruikt om een netwerk tegen een Gedistribueerde aanval van de Ontkenning van de Dienst (DDoS) te beschermen. DDoS-aanvallen zijn bedoeld om een netwerk te laten overstromen naar het punt waar de bronnen van het netwerk niet beschikbaar komen.



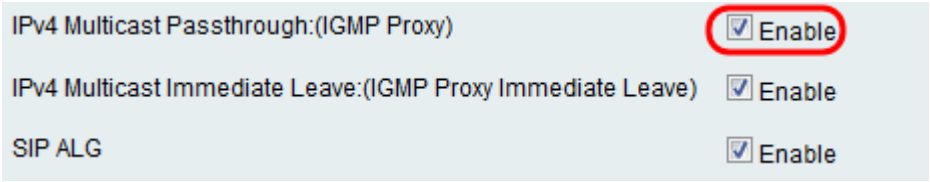
Stap 4. In het veld *Block WAN Ping request* (*WAN-pingverzoek blokkeren*) schakelt u het aanvinkvakje **Enable** in om pingverzoeken naar uw apparaat vanaf het externe WAN-netwerk te stoppen.



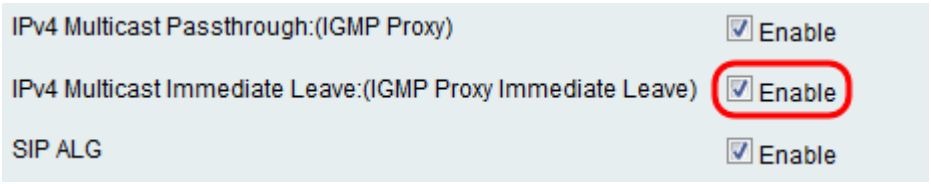
Stap 5. De genoemde velden van *LAN/VPN Web Access to Remote Management Port* worden gebruikt om LAN en Remote Management Web Access te configureren. Raadpleeg voor meer informatie over deze configuraties Configuration of LAN and Remote Management Web Access op de RV130 en RV130W.



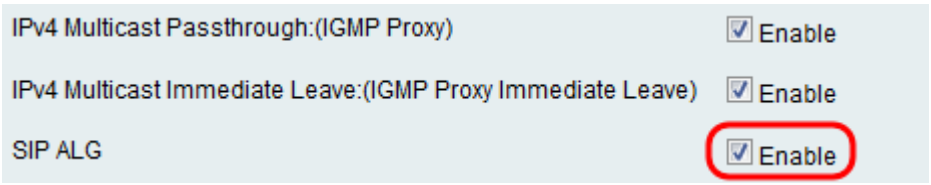
Stap 6. In het veld *IPv4 Multicast Passthrough: (IGMP Proxy)* vinkt u het aanvinkvakje **Enable** aan om de multicast-passthrough voor IPv4 in te schakelen. Hiermee worden IGMP-pakketten van het externe WAN-netwerk naar uw interne LAN doorgestuurd.



Stap 7. In het veld *IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)* vinkt u het aanvinkvakje **Enable aan** om Multicast Immediate Leave in te schakelen. Het toelaten van direct verlof zorgt ervoor dat optimaal bandbreedtebeheer wordt verstrekt aan hosts op uw netwerk, zelfs tijdens tijden van gelijktijdig multicast groepsgebruik.



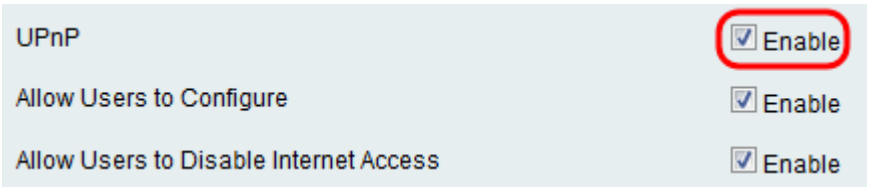
Stap 8. Selecteer in het veld *Session Initiation Protocol (SIP) Application Layer Gateway (ALG)* het aanvinkvakje **Enable** om het SIP-verkeer (Session Initiation Protocol) toe te staan om de firewall te passeren. Session Initiation Protocol (SIP) stelt platforms in staat om de installatie van spraak- en multimediatoepassingen via IP-netwerken te signaleren. Application Layer Gateway (ALG), ook bekend als Application Level Gateway, is een toepassing die IP-adresinformatie vertaalt binnen de payload van een applicatiepakket.



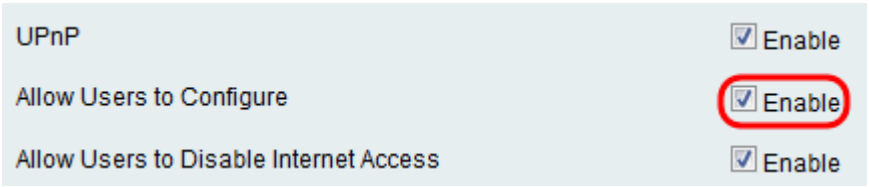
Opmerking: Het apparaat ondersteunt maximaal 256 SIP ALG sessies.

Universele plug-and-play configureren

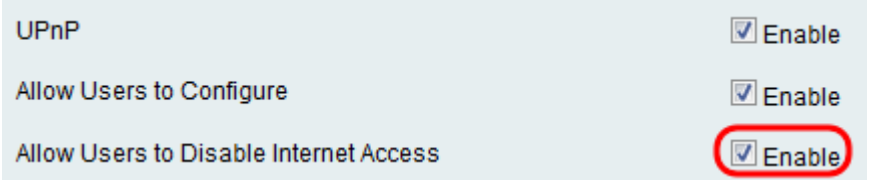
Stap 1. Selecteer in het veld *UPnP* de optie **Enable** om Universal plug and play (UPnP) in te schakelen.



Stap 2. In het veld *Toestaan aan gebruikers om* het veld *te configureren*, schakelt u het aanvinkvakje **Inschakelen in** om toe te staan dat de UPnP-poorttoewijzingsregels worden ingesteld door gebruikers die UPnP-ondersteuning hebben ingeschakeld op hun computers of andere UPnP-apparaten. Indien uitgeschakeld, staat het apparaat de toepassing niet toe om de verzendregel toe te voegen.



Stap 3. In het veld *Toestaan dat gebruikers internettoegang kunnen uitschakelen*, schakelt u het aanvinkvakje **Enable** in om gebruikers de internettoegang uit te schakelen.



Inhoud blokkeren

Stap 1. Controleer het aankruisvakje in het veld dat overeenkomt met de inhoud die u van het apparaat wilt blokkeren.

De beschikbare opties zijn als volgt gedefinieerd:

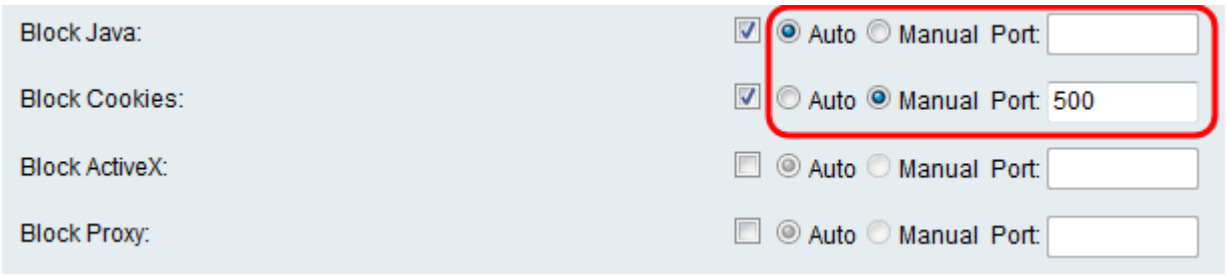
·Blokkeer Java — blokkeert het downloaden van Java-applets.

·Blokkeer Cookies — blokkeert het apparaat om cookie-informatie van webpagina's te ontvangen.

·Blokkeer ActiveX — blokkeert ActiveX-applets die aanwezig kunnen zijn wanneer u Internet Explorer op het Windows-besturingssysteem gebruikt.

·Blokkeer Proxy — blokkeert het apparaat van communicatie via een proxyserver naar externe apparaten. Dit voorkomt dat het apparaat firewallregels omzeilt.

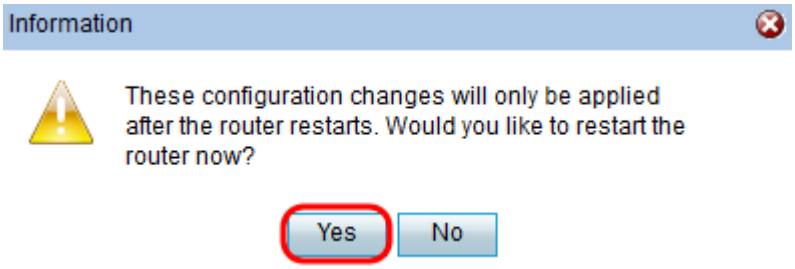
Stap 2. Selecteer de knop **Auto** om alle exemplaren van die bepaalde inhoud automatisch te blokkeren of klik op de knop **Handmatig** en voer een specifieke poort in het corresponderende veld in waarop de inhoud wordt geblokkeerd.



Opmerking: U kunt elk gewenst nummer in het bereik (1-65535) invoeren voor uw poortwaarde.

Stap 3. Klik op **Opslaan** om de instellingen op te slaan.

Stap 4. Er verschijnt een venster waarin u wordt gevraagd de router opnieuw te starten. Klik **Ja** om uw router opnieuw te starten om de wijzigingen toe te passen.



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.