Firewall-instellingen configureren op de RV34x Series router

Doel

Het doel van dit artikel is om te verklaren hoe te om de Basis Firewall Instellingen op de RV34x Series router te configureren.

Inleiding

Het primaire doel van een firewall is het inkomende en uitgaande netwerkverkeer te controleren door de gegevenspakketten te analyseren en te bepalen of dit al dan niet moet worden toegestaan op basis van een vooraf bepaalde set regels. Een router wordt beschouwd als een sterke hardware firewall vanwege functies die het filteren van inkomende gegevens mogelijk maken. Een netwerkfirewall bouwt een brug tussen een intern netwerk dat verondersteld wordt veilig en vertrouwd te zijn en een ander netwerk, gewoonlijk een extern internetwerk zoals Internet dat niet veilig en onbetrouwbaar wordt verondersteld.

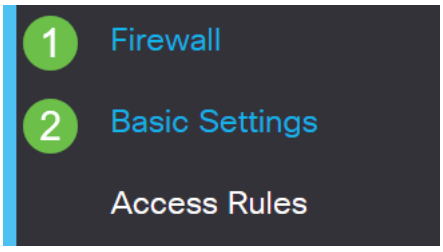
Toepasselijke apparaten | Versie firmware

- RV34x Series | 1.0.03.21 (Download de laatste versie)

Basisfirewallinstellingen configureren

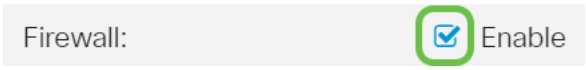
Stap 1

Meld u aan bij de Web User Interface (UI) en kiest u **Firewall >Basisinstellingen**.



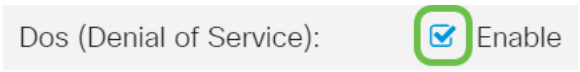
Stap 2

Controleer het dialoogvenster Firewall **inschakelen** om de functie Firewall te activeren. Dit is standaard ingeschakeld.



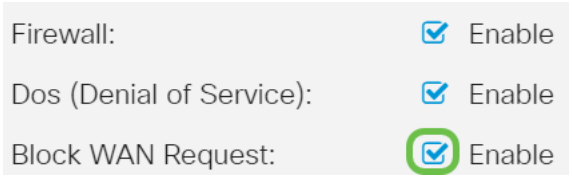
Stap 3

Controleer het dialoogvenster Dos **inschakelen** (Dialoogvenster Service **inschakelen**) om uw netwerk te beveiligen tegen DoS-aanvallen. Dit is standaard ingeschakeld.



Stap 4

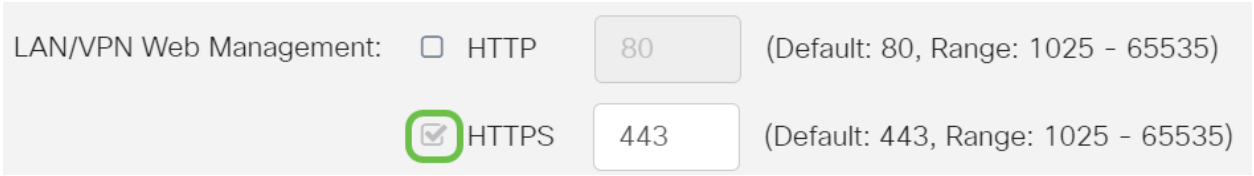
Controleer het dialoogvenster WAN-aanvraag blokkeren om ping-verzoeken aan de RV34x Series router te ontkennen. Dit is standaard ingeschakeld.



Stap 5

In het gebied LAN/VPN Web Management controleert u het vakje **HTTP** en/of **HTTPS** om verkeer van deze protocollen mogelijk te maken. Bij dit voorbeeld wordt het aanvinkvakje HTTPS ingeschakeld.

- HTTP — Hyper-Text Transfer Protocol is een protocol voor gegevensoverdracht dat op internet wordt gebruikt.
- HTTPS - Hyper-Text Transfer Protocol Secure is een beveiligde versie van HTTP die pakketten versleutelt voor verhoogde beveiliging.

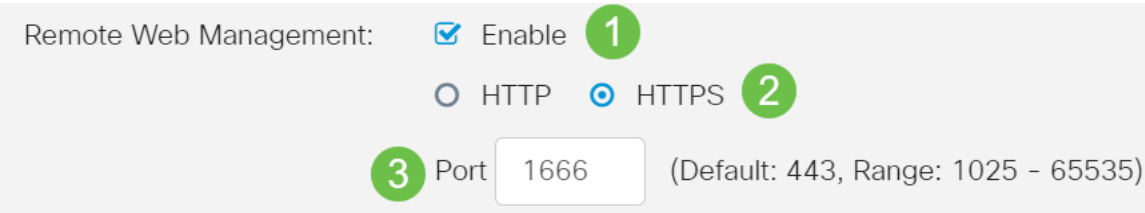


Stap 6 (optioneel)

Controleer het aanvinkvakje Afstandsbeheer **inschakelen** om het beheer op afstand in te schakelen. Anders slaat u over op Stap 8.

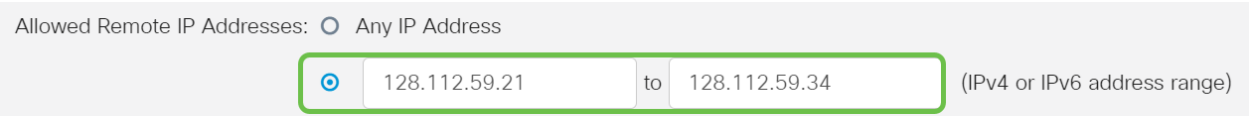
Kies het type protocol dat wordt gebruikt om verbinding te maken met de firewall door een radioknop te kiezen. De opties zijn **HTTP** en **HTTPS**.

Voer een poortnummer in dat varieert van 1025 tot 65535, wat afstandsbeheer is toegestaan. De standaardinstelling is 443. In dit voorbeeld wordt 1666 gebruikt.



Stap 7

In het gebied Toegestane Remote IP-adressen kiest u een radioknop om een IP-adres in te schakelen om het netwerk op afstand te bereiken of om een bereik van IPv4- of IPv6-adressen te specificeren. Bij dit voorbeeld werd een IP-bereik geselecteerd. In dit voorbeeld is het beginnende IP-adres 128.112.59.21 en het laatste IP-adres 128.112.59.34.



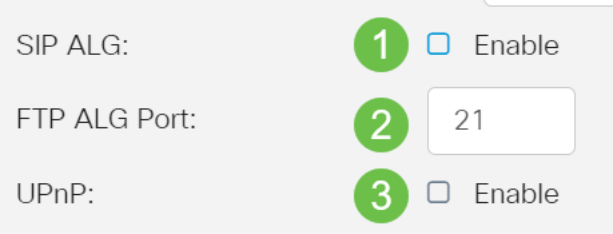
Stap 8 (optioneel)

Controleer het aanvinkvakje SIP ALG **inschakelen** om SIP-toepassingsgateway (SIP) aan te passen aan de firewall. Deze optie kan worden ingeschakeld om SIP-pakketten door de firewall te laten passeren. Een SIP-pakket wordt gebruikt om verbindingen van spraakverkeer te initiëren. Als uw VoIP-provider een ander NAT-reisprotocol (Network Address Translation) gebruikt, kan deze functie worden uitgeschakeld: de standaardinstelling.

Specificeer de FTP-poort (File Transfer Protocol) van SIP ALG in het veld *FTP ALG Port*. De standaardinstelling is 21.

Controleer het aanvinkvakje UPnP **inschakelen** om Universal plug-and-Play (UPnP) in te schakelen. Deze optie is standaard uitgeschakeld.

Deze opties worden bijvoorbeeld uitgeschakeld.



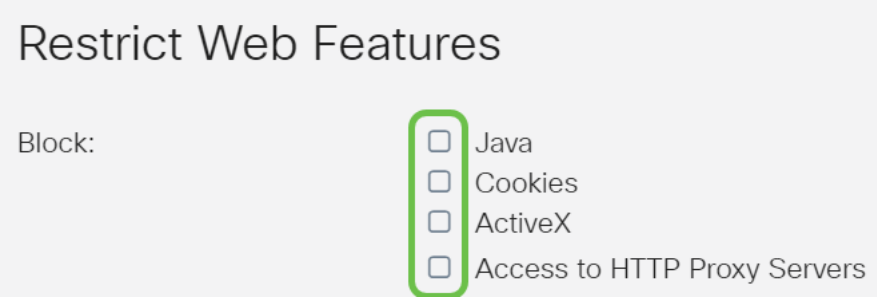
Stap 9 (optioneel)

Selecteer onder het gebied Webeigenschappen beperken de selectieteksten van de types van web eigenschappen om in het gebied van het Blok te blokkeren. Deze selectietekens zijn standaard uitgeschakeld. De opties zijn:

Java — Alle webelementen die dit soort web-element bevatten, worden geblokkeerd. Deze instelling kan Java-gebaseerde webaanvallen helpen voorkomen.
Cookies — Cookies zijn gegevens die opgeslagen worden in de computer om websites te helpen begrijpen wie er toegang tot heeft. Door ze te blokkeren kan worden

voorkomen dat kwaadaardige koekjes toegang krijgen tot gegevens.
ActiveX - Dit is een plug-in die door Microsoft is ontwikkeld om een browservaring te verbeteren. Het blokkeren kan verhinderen dat kwaadaardige ActiveX plug-ins netwerkapparaten beschadigen.
Toegang tot Proxy HTTP Server — HTTP Proxy servers verstopt details van eindgebruikers van hackers. Ze werken als tussenpersonen zodat een klant niet direct op het internet komt. Als lokale gebruikers echter toegang hebben tot WAN-proxy-servers, kunnen ze een manier vinden rond de inhoud-filters in de router om toegang te krijgen tot internetsites die door de router zijn geblokkeerd.

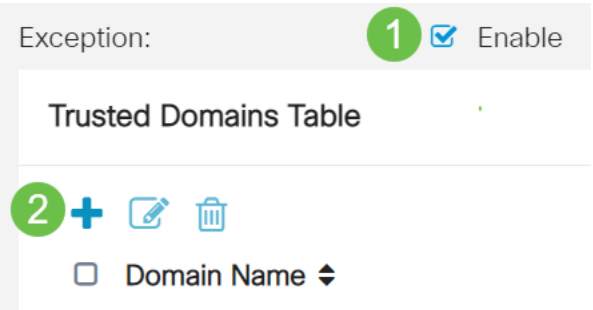
Dit voorbeeld, de selectietekens blijven uitgeschakeld.



Stap 11 (optioneel)

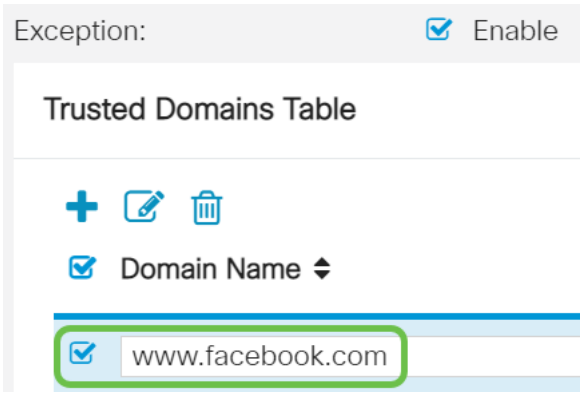
Controleer het aanvinkvakje Exception **Enable** Exception om alleen geselecteerde webfuncties zoals Java, Cookies, ActiveX of Access to HTTP Proxy Server toe te staan en alle anderen te beperken. Dit wordt standaard uitgeschakeld. Dit voorbeeld wordt uitgeschakeld.

In de tabel Betrouwbare velden klikt u op het **pictogram** toevoegen om domeinen toe te voegen die u kunt vertrouwen of die u op het netwerk kunt gebruiken.



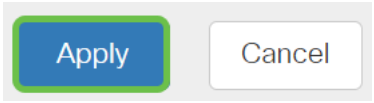
Stap 12

Voer in het veld *Domain Name* een domeinnaam in om toegang tot het netwerk te krijgen. Bijvoorbeeld, www.facebook.com wordt gebruikt.



Stap 13

Klik op Apply (Toepassen).



Stap 14 (optioneel)

Als u de configuratie permanent wilt opslaan, gaat u naar de pagina Configuration kopiëren/opslaan of klikt u op het **pictogram** voor het **opslaan** in het bovenste gedeelte van de pagina.

Conclusie

U had nu met succes de Firewall-instellingen op uw RV34x Series router moeten configureren.