# Standaard toegangscontrolebeleid voor de CVR100W VPN-router

## Doel

Het Toegangsbeheerbeleid geeft de gebruiker de controle om te beslissen of de informatie van het apparaat al dan niet wordt gedeeld. Deze optie kan communicatie van het beveiligde LAN naar het onveilige WAN uitschakelen. Een gebruiker zou de toegang door dit beleid willen beperken als hij vindt dat de informatie die door WAN is doorgegeven niet veilig is.

Dit artikel legt uit hoe u het beleid voor standaard toegangscontrole op de CVR100W VPN-router kunt configureren.

## Toepassbaar apparaat

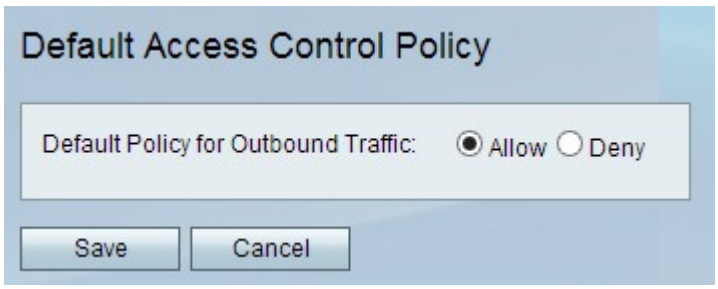
- CVR100W

## Softwareversie

•1.0.1.19

## Standaard toegangsbeheerbeleid

Stap 1. Meld u aan bij het programma voor webconfiguratie en kies **Firewall > Toegangsbeheer > Standaardtoegangsbeleid**. De pagina *Default Access Control Policy* wordt geopend:




Stap 2. Kies een van de volgende opties in het veld *Standaardbeleid voor uitgaande verkeer*:

- Laat — Dit maakt het mogelijk dat alle informatie door het WAN gaat en laat het systeem indien nodig achter. Klik op de radioknop **Toestaan** om informatie minder veilig maar makkelijker toegankelijk te houden.

- Ontken — Dit ontkent informatie om door de WAN-poort te gaan en laat het systeem om informatie onder de best mogelijke beveiliging te houden. De hosts vanaf de LAN poort kunnen nog steeds communiceren, zelfs als de WAN-poort is uitgeschakeld. Als er twijfels zijn over de beveiliging van uitgaande informatie, klik dan op de radioknop **Deny**.

Stap 4. Klik op **Opslaan**.