Firewallconfiguratie op de CVR100W VPN-router

Doel

Een firewall is een reeks functies die zijn ontworpen om een netwerk veilig te stellen. Een router wordt beschouwd als een sterke hardwarefirewall. Dit is te wijten aan het feit dat routers alle inkomende verkeer kunnen controleren en ongewenste pakketten kunnen drogen. Dit artikel legt uit hoe u basisfirewallinstellingen kunt configureren op de CVR100W VPN-router.

Toepassbaar apparaat

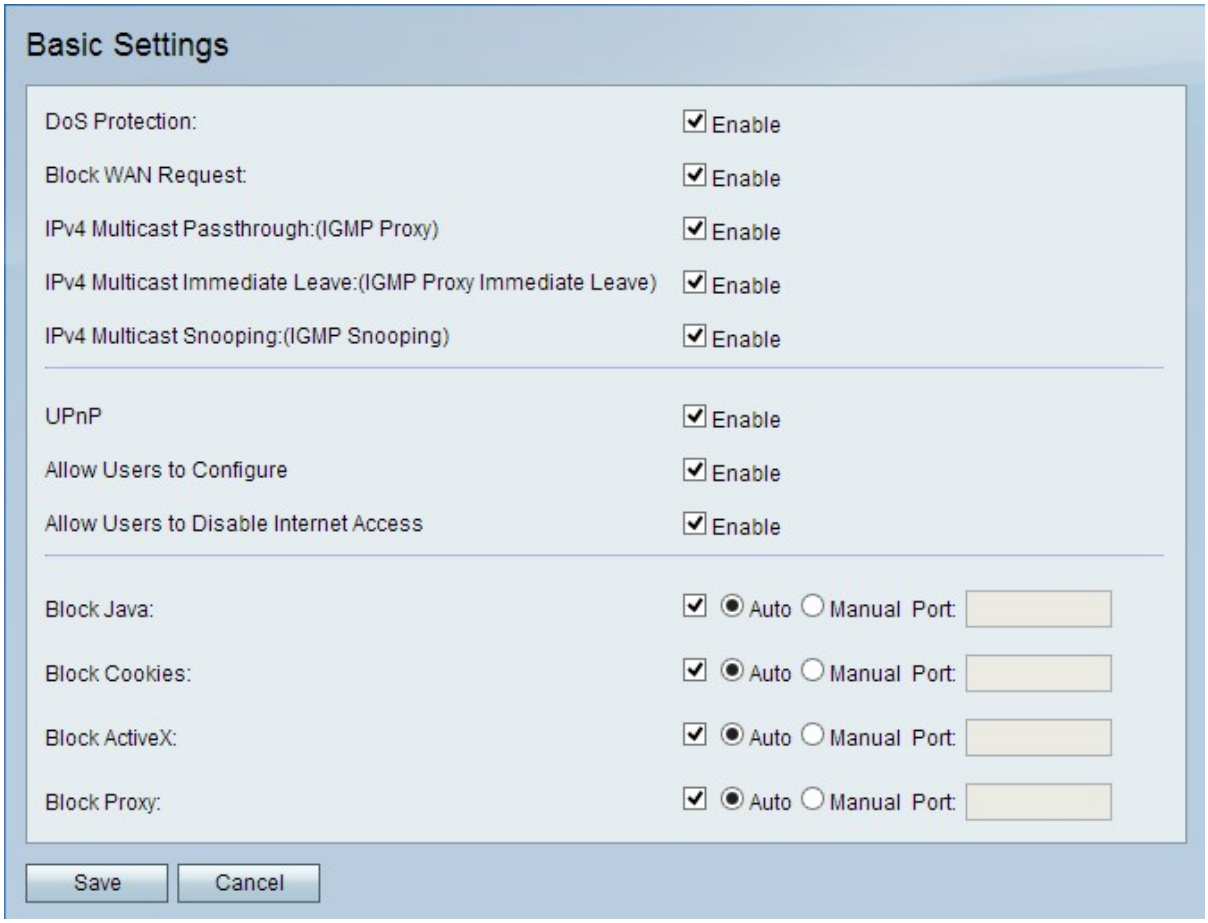
- CVR100W

Softwareversie

•1.0.1.19

Configuratie van basisfirewall

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



Opmerking: Stap 2 tot 13 is optioneel. U kunt deze opties instellen op basis van uw behoeften.

Stap 2. Controleer Schakel de**optie** in het veld DoS-**bescherming** (Denial of Service) op de CVR100W. Bescherm het netwerk wordt gebruikt om een netwerk van een gedistribueerde Denial of Service (DDoS) aanval te verhinderen. De aanvallen van DDoS zijn bedoeld om een netwerk te overspoelen tot het punt waar de middelen van het netwerk niet beschikbaar worden. De CVR100W gebruikt DoS-bescherming om het netwerk te beschermen door beperking en verwijdering van ongewenste pakketten.

Stap 3. Om alle ping-verzoeken naar de CVR100W vanuit WAN te blokkeren, **schakelt** u in het veld WAN-aanvraag blokkeren in.

Stap 4. Om IPv4-multicast verkeer via de CVR100W vanuit het internet te laten verlopen, **schakelt** u in het veld IPv4-multicast passthrough in **om**. IP multicast is een methode die wordt gebruikt om IP-datagrammen naar een aangewezen groep ontvangers in één transmissie te verzenden.

Stap 5. IGMP-proxy is een manier waarop de router met andere apparaten kan communiceren via IGMP-berichten. Met onmiddellijke vakantie kan de CVR100W de multicast groep op optimale snelheid verlaten. Schakel IGMP Proxy onmiddellijk uit door te controleren of het IPv4-multicast veld **onmiddellijk** verlaten **is** ingeschakeld.

Stap 6. Om IGMP Snooping mogelijk te maken, waardoor andere switches op het netwerk kunnen luisteren naar de berichten die heen en weer gaan tussen de computer en de CVR100W, **schakelt** u **in** het veld IPv4 Multicast Snooping in.

Stap 7. Controleer Universal Plug and Play (UPnP) op **Schakel** in het UPnP-veld. UPnP maakt automatische ontdekking mogelijk van apparaten die met de CVR100W kunnen communiceren.

Stap 8. Om gebruikers met UPnP-compatibele apparaten toe te staan om de regels van UPnP-poortselectie te configureren **schakelt** u de optie in het veld **toestaan** in. Port-mapping of poorttransport wordt gebruikt om communicatie tussen externe hosts en services mogelijk te maken die binnen een privaat LAN worden geleverd.

Stap 9. Om gebruikers toe te staan om internettoegang tot het apparaat uit te schakelen, controleert u in het veld Toegang voor gebruikers toestaan om internet uit te schakelen.

Stap 10. Om te voorkomen dat er javepauzen worden gedownload, controleert u **BlokJava** in het veld BlokJava. Java-applets die voor een kwaadaardige bedoeling zijn gemaakt, kunnen een beveiligingsbedreiging voor een netwerk vormen. Wanneer je het hebt gedownload, kan een vijandige java-applet netwerkbronnen exploiteren. Klik op de radioknop die overeenkomt met de gewenste blokmethode.

- Auto — blokkeert automatisch java.
- Handmatige poort — Voer een specifieke poort in waarop u java wilt blokkeren.

Stap 11. Als u niet wilt dat een website cookies maakt, controleert u **Cookies** in het veld Cookies blokkeren. Cookies worden gemaakt door websites om informatie van deze gebruikers op te slaan. Cookies kunnen de webgeschiedenis van de gebruiker volgen, wat kan leiden tot een inbreuk op de privacy. Klik op de radioknop die overeenkomt met de gewenste blokmethode.

- Auto - blokkeert koekjes automatisch.
- Handmatige poort — Voer een specifieke poort in waarop je koekjes moet blokkeren.

Stap 12. Om ActiveX-applets te blokkeren nadat u deze hebt gedownload, controleert u **Blok ActiveX** in het veld Blok ActiveX. ActiveX is een type applet dat geen beveiliging heeft. Nadat een ActiveX-applet op een computer is geïnstalleerd, kan deze alles doen wat een gebruiker kan doen. Het kan schadelijke code in het besturingssysteem invoegen, op een beveiligd intranet surfen, een wachtwoord wijzigen of documenten herstellen en verzenden. Klik op de radioknop die overeenkomt met de gewenste blokmethode.

- Auto — Blokkeer automatisch ActiveX.
- Handmatige poort - Voer een specifieke poort in waarop u ActiveX wilt blokkeren.

Stap 13. Controleer **Blokproxy**-servers in het veld Blokproxy om deze te blokkeren. Proxyservers zijn servers die een link tussen twee afzonderlijke netwerken bieden. Kwaadaardige proxy-servers kunnen alle niet-versleutelde gegevens die naar ze worden verzonden, zoals logins of wachtwoorden, opslaan. Klik op de radioknop die overeenkomt met de gewenste blokmethode.

- Auto — Blokkeer automatisch proxyservers.
- Handmatige poort — Voer een specifieke poort in waarop u proxy-servers wilt blokkeren.

Stap 14. Klik op **Opslaan** om de door u aangebrachte wijzigingen op te slaan.