Firewallconfiguratie op RV320 en RV325-routers

Doel

Dit artikel legt uit hoe u basisfirewallinstellingen kunt configureren op de RV32x VPN-routerserie.

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. Netwerkfirewalls beschermen een intern computernetwerk (huis, school, bedrijfsintranet) tegen kwaadaardige toegang van buitenaf. Netwerkfirewalls kunnen ook worden geconfigureerd om de toegang tot de buitenkant te beperken van interne gebruikers.

Toepasselijke apparaten

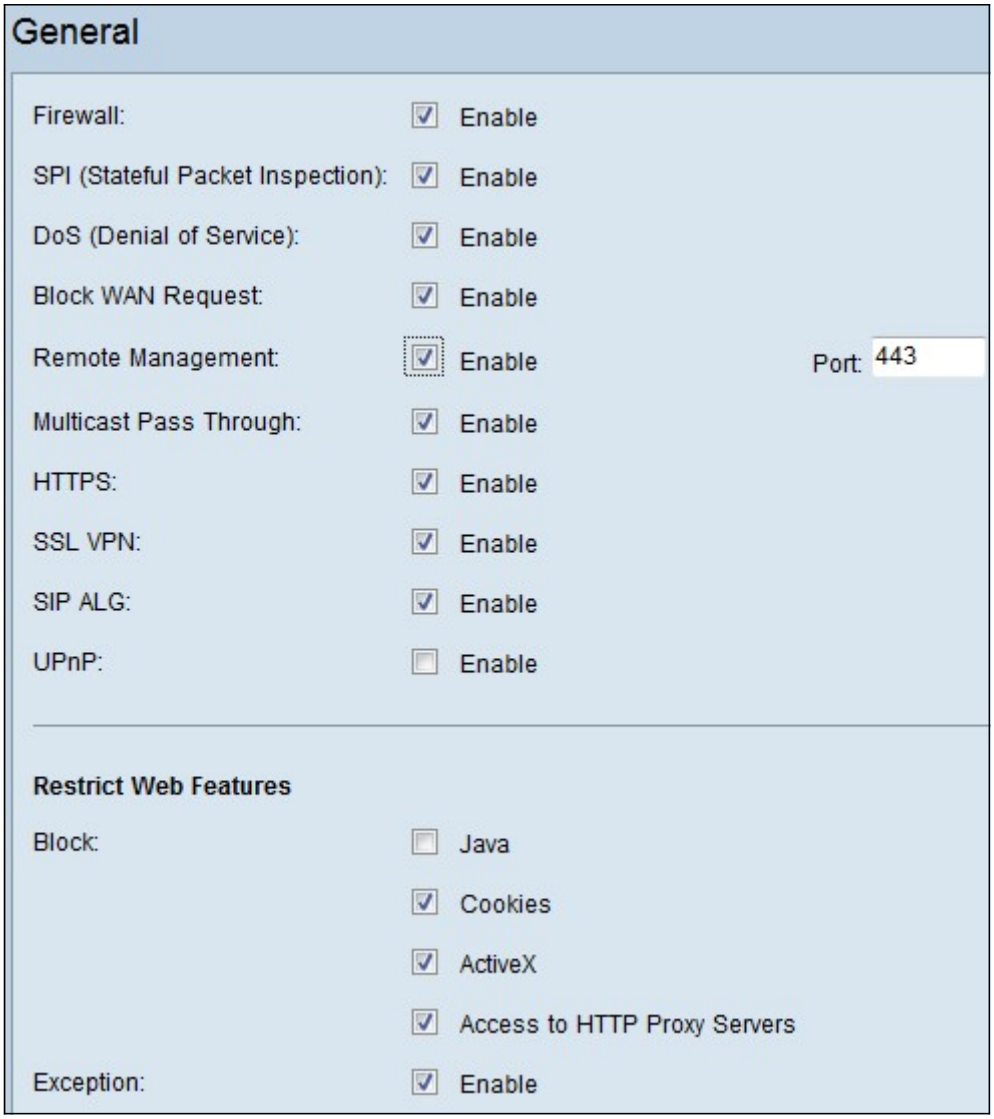
- RV320 VPN-router met dubbel WAN
- RV325 Gigabit VPN-router met dubbel WAN

Softwareversie

- v1.1.0.09

Basisinstellingen

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



Stap 2. Gebaseerd op uw vereisten, controleert u het vakje **Enable** waarmee u de functies wilt activeren.

- Firewall — Routerfirewalls kunnen worden uitgeschakeld (uitgeschakeld), of ze kunnen worden ingeschakeld om bepaalde typen netwerkverkeer te filteren via de zogeheten firewallregels. Een firewall kan worden gebruikt om al het inkomende en uitgaande verkeer te filteren en gebaseerd te zijn.
- SPI (Stateful Packet Inspection) - Hiermee controleert u de staat van netwerkverbindingen zoals TCP-stromen en UDP-communicatie De firewall onderscheidt u legitieme pakketten voor verschillende typen verbindingen. Alleen pakketten die overeenkomen met een bekende actieve verbinding worden door de firewall toegestaan en alle andere pakketten worden verworpen.
- DoS (Denial of Service) — gebruikt om een netwerk te beveiligen tegen een aanval met gedistribueerde Denial of Service (DDoS). De aanvallen van DDoS zijn bedoeld om een netwerk te overspoelen tot het punt waar de middelen van het netwerk niet beschikbaar worden. De RV320 gebruikt VoS bescherming om het netwerk te beschermen door de beperking en verwijdering van ongewenste pakketten.
- Blokkeer WAN-aanvraag - blokkeert alle ping-verzoeken naar de router vanuit de WAN-poort.
- Afstandsbeheer — Hiermee kunt u toegang tot de router krijgen via een WAN-netwerk op afstand.
    - Port - Voer een poortnummer in om extern te beheren.

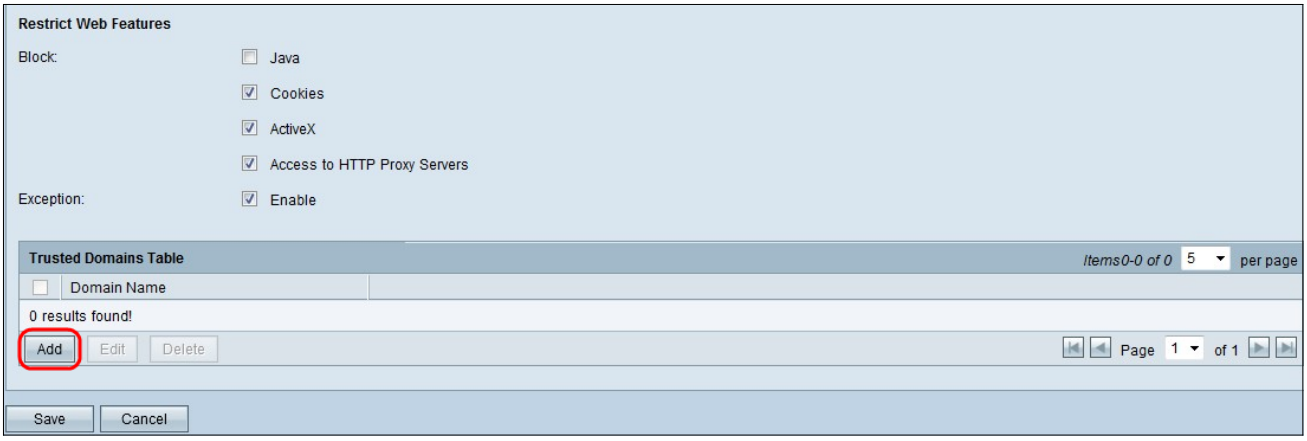
- Multicast Pass Through - Hiermee kunnen IP-multicast berichten door het apparaat stromen.
- HTTPS (Hypertext Transfer Protocol Secure) — is een communicatieprotocol voor beveiligde communicatie via een computernetwerk. Het verstrekt bidirectionele encryptie van client en server.
- SSL VPN - Hiermee kan een SSL VPN-verbinding worden gemaakt via de router.
- SIP ALG — SIP ALG biedt functionaliteit die Voice-over-IP verkeer mogelijk maakt dat zowel van de particuliere naar openbare als van de openbare naar privé kant van de firewall gaat wanneer het netwerkadres en de poortvertaling (NAPT) worden gebruikt. NAPT is het meest voorkomende type van netwerkadresomzetting.
- UPnP (Universal Plug and Play) - Hiermee kan apparaten automatisch worden ontdekt die kunnen communiceren met de router.

Stap 3. Gebaseerd op uw vereisten, controleer het aanvinkvakje **Enable** die overeenkomt met de functies die u wilt blokkeren.

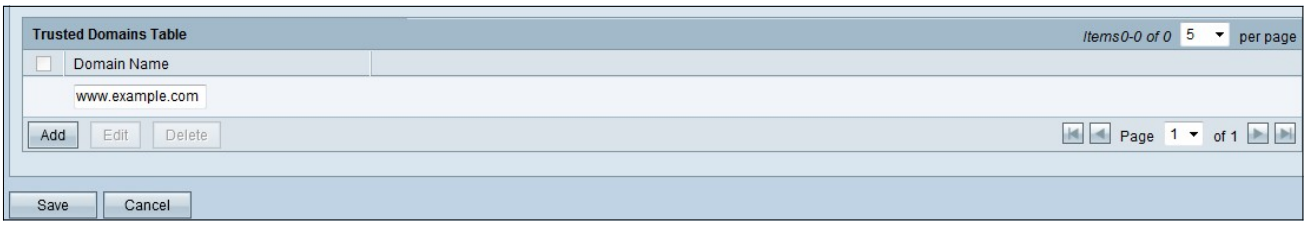
- Java — Door dit vakje in te schakelen worden Java-applets niet gedownload en uitgevoerd. Java is een gemeenschappelijke programmeertaal die door veel websites wordt gebruikt. Maar java-applets die gemaakt worden voor kwaadaardige bedoelingen kunnen een veiligheidsbedreiging voor een netwerk vormen. Wanneer je het hebt gedownload, kan een vijandige java-applet netwerkbronnen exploiteren.
- Cookies — Cookies worden gemaakt door websites om informatie over gebruikers op te slaan. Cookies kunnen de webgeschiedenis van de gebruiker volgen, wat kan leiden tot een inbreuk op de privacy.
- ActiveX - ActiveX is een type applet dat door veel websites wordt gebruikt. Hoewel over het algemeen veilig, kan een kwaadaardige ActiveX-applicatie die op een computer is geïnstalleerd, 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.
- Toegang tot HTTP Proxyservers — 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.
- Uitzondering - hiermee kunnen de geselecteerde functies worden geselecteerd (Java, Cookies, ActiveX of Access to HTTP Proxy Server) maar dit beperkt alle niet-geselecteerde functies op geconfigureerde vertrouwde domeinen. Een domein dat vertrouwd is en toegang heeft tot het vertrouwde netwerk. U kunt een betrouwbaar domein instellen dat gebruikers van een extern domein toegang geeft tot uw netwerkbronnen. Als deze optie uitgeschakeld is, kan een vertrouwd domein alle functies toestaan.

Opmerking: Time Saver: Als u de optie Exception niet hebt ingeschakeld, sla dan stap 4 over.

Stap 4. Klik op Toevoegen, voer een nieuw Trusted-domein in en klik op Opslaan om een betrouwbaar domein te maken.

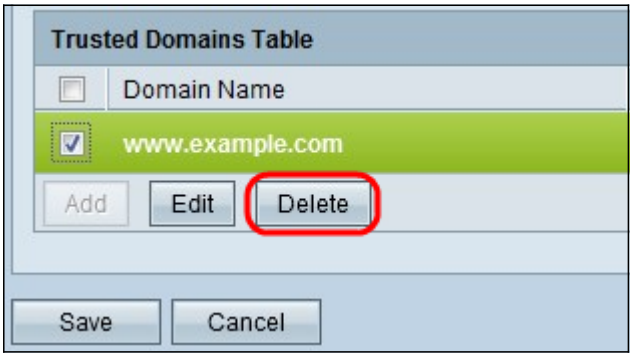


Stap 5. Klik op Opslaan om de wijzigingen bij te werken.



Stap 6. (Optioneel) Om de naam van het vertrouwde domein te bewerken, controleert u het aankruisvakje van het vertrouwde domein dat u wilt bewerken, klikt u op Bewerken, bewerkt u de domeinnaam en klikt u op Opslaan.

Stap 7. (Optioneel) Om een domein in de lijst Betrouwbaar domein te verwijderen, schakelt u het aankruisvakje in het vertrouwde domein in dat u wilt verwijderen en op Verwijderen klikt.



Bekijk een video gerelateerd aan dit artikel...

Klik hier om andere Tech Talks uit Cisco te bekijken