

Configuratie van firewalltoegangsregels om pingpakketten van twee verschillende netwerken te blokkeren op RV016, RV042, RV042G en RV082 VPN-routers

Doel

Op een router kunnen twee verschillende netwerken nodig zijn om internettoegang te bieden aan apparaten die niet in hetzelfde netwerk als de router staan. Dit kan worden bereikt door middel van een toegangsregel op basis van verschillende criteria om toegang tot een netwerk of IP-adresbereik toe te staan of te weigeren. Een toegangsregel helpt de router bepalen welk verkeer door de firewall mag worden doorgegeven en helpt ook om beveiliging aan de router toe te voegen.

In dit artikel wordt uitgelegd hoe u pingpakketten van twee verschillende netwerken op RV016-, RV042-, RV042G- en RV082 VPN-routers kunt blokkeren via een toegangsregel.

Toepasselijke apparaten

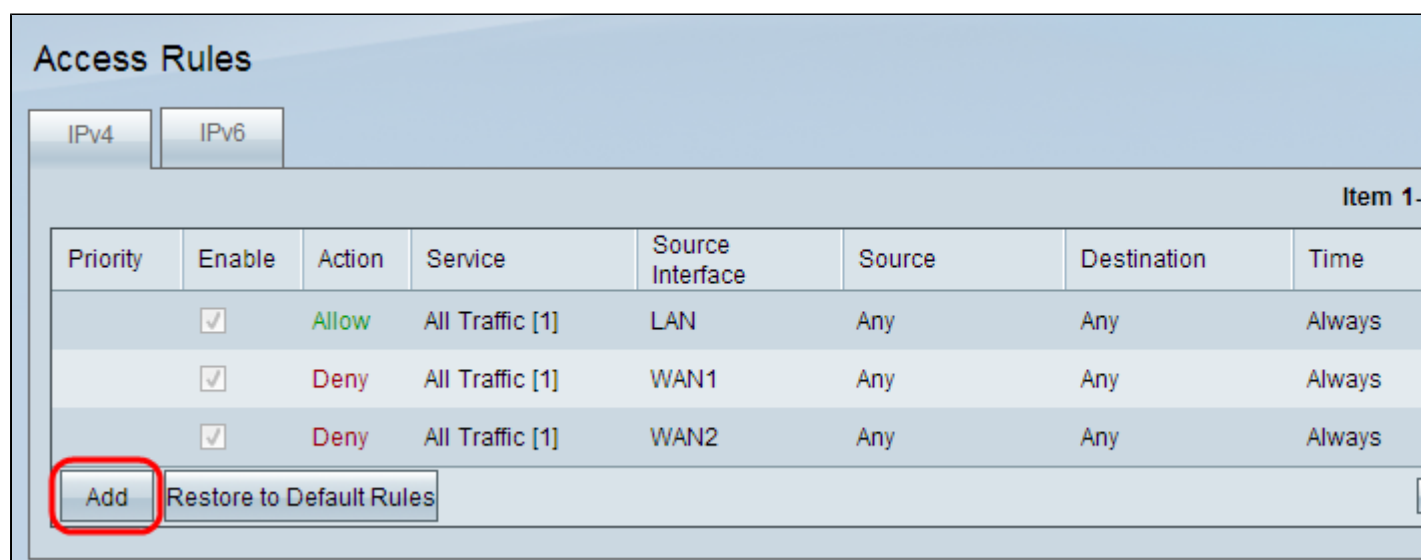
- RV016
- RV042
- RV042G
- RV082

Softwareversie

- v4.2.1.02

Configuratie van toegangsregels

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



The screenshot displays the 'Access Rules' configuration page. At the top, there are tabs for 'IPv4' and 'IPv6'. Below the tabs is a table with the following columns: Priority, Enable, Action, Service, Source Interface, Source, Destination, and Time. The table contains three rows of rules:

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always

At the bottom of the table, there is an 'Add' button (highlighted with a red circle) and a 'Restore to Default Rules' button.

Stap 2. Klik op **Add** om een toegangsregel toe te voegen. De pagina *Access Rules Services* wordt geopend:

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Stap 3. Kies de juiste actie in de vervolgkeuzelijst Actie zodat het verkeer kan worden doorgegeven als **Toestaan** is geselecteerd. Anders, kies **Deny** om het verkeer te ontkennen.

Stap 4. Kies de juiste service uit de vervolgkeuzelijst Service.

Opmerking: Als de gewenste service beschikbaar is, gaat u naar Stap 10.

Stap 5. Als de juiste service niet beschikbaar is, klikt u op **Servicebeheer** en verschijnt het venster *Servicebeheer*:

Service Name :

Protocol :

Port Range : to

All Traffic [TCP&UDP/1~65535]
 DNS [UDP/53~53]
 FTP [TCP/21~21]
 HTTP [TCP/80~80]
 HTTP Secondary [TCP/8080~8080]
 HTTPS [TCP/443~443]
 HTTPS Secondary [TCP/8443~8443]
 TFTP [UDP/69~69]
 IMAP [TCP/143~143]
 NNTP [TCP/119~119]
 POP3 [TCP/110~110]
 SNMP [UDP/161~161]

Stap 6. Voer een gewenste servicenaam in het veld Servicenaam in.

Stap 7. Kies een geschikt protocoltype uit de vervolgkeuzelijst Protocol:

- TCP â€” Transmission Control Protocol is een protocol dat wordt gebruikt door toepassingen die een gegarandeerde levering vereisen.
- UDP â€” User Datagram Protocol gebruikt datagramsockets om host-to-host communicatie tot stand te brengen.
- IPv6 â€” leidt internetverkeer tussen hosts in pakketten die worden gerouteerd over netwerken die worden gespecificeerd door adressen te routeren.

Stap 8. Voer het bereik van poorten in dat van toepassing is op de service in het veld Poortbereik.

Stap 9. Klik op **Toevoegen aan lijst** om de service toe te voegen aan de vervolgkeuzelijst Service op de pagina *Toegangsregels*.

Stap 10. Klik op **OK** om het venster te sluiten. Hierdoor gaat de gebruiker terug naar de pagina *Toegangsregels*.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Stap 11. Kies **Logpakketten overeenkomen met deze regel** om de inkomende pakketten te registreren die overeenkomen met de toegangsregel in de vervolgkeuzelijst Log.

Stap 12. Kies een interface in de vervolgkeuzelijst Bron-interface die door deze regel wordt beïnvloed. De broninterface is de interface waarvan het verkeer in werking wordt gesteld.

- LAN â€” De lokale netwerkpoort sluit computers in de buurt aan op een netwerk zoals een kantoorgebouw of een school.
- WAN1 â€” De WAN-netwerkpoort sluit computers in een groot gebied op een netwerk aan. Dit kan elk netwerk zijn dat een regio of zelfs een land met elkaar verbindt. Het wordt gebruikt door bedrijven en de overheid om verbinding te maken met andere locaties.
- WAN2 â€” Hetzelfde als poort WAN1, behalve dat het een tweede netwerk is.
- DMZ â€” hiermee heeft buitenverkeer toegang tot een computer op het netwerk zonder het LAN bloot te stellen.
- OM HET EVEN WELKE â€” Laat om het even welke interface toe om worden gebruikt.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Stap 13. Kies een optie om het IP-bronadres op te geven dat het netwerk voor verkeer zal gebruiken via de interface in de vervolgkeuzelijst Bron:

- Om het even welk â€” Om het even welk IP adres zal worden gebruikt om verkeer door:sturen. Er zijn geen velden rechts van de vervolgkeuzelijst beschikbaar.
- Enkelvoudig â€” Er wordt één IP-adres gebruikt om verkeer door te sturen. Voer het gewenste IP-adres in het veld rechts van de vervolgkeuzelijst in.
- Bereik â€” Er wordt een IP-adres van het bereik gebruikt om verkeer door te sturen. Voer in de velden rechts van de vervolgkeuzelijst het gewenste IP-adresbereik in.

Stap 14. Kies een optie om het IP-adres van de bestemming op te geven dat het netwerk voor verkeer zal gebruiken via de interface in de vervolgkeuzelijst Bestemming:

- Om het even welk â€” Om het even welk IP adres zal worden gebruikt om verkeer door:sturen. Er zijn geen velden rechts van de vervolgkeuzelijst beschikbaar.
- Enkelvoudig â€” Er wordt één IP-adres gebruikt om verkeer door te sturen. Voer het gewenste IP-adres in het veld rechts van de vervolgkeuzelijst in.
- Bereik â€” Er wordt een IP-adres van het bereik gebruikt om verkeer door te sturen. Voer in de velden rechts van de vervolgkeuzelijst het gewenste IP-adresbereik in.

Stap 15. Klik op **Opslaan** om de instellingen 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.