

Configuratie van een IPv6-toegangsregel voor RV016, RV042, RV042G en RV082 VPN-routers

Doel

Een toegangsregel helpt de router te bepalen welk verkeer door de firewall mag passeren. Dit helpt veiligheid aan de router toe te voegen.

Dit artikel legt uit hoe een IPv6-toegangsregel op de RV016, RV042, RV042G en RV082 VPN-routers moet worden toegevoegd.

Toepasselijke apparaten

- RV016
- RV042
- RV042G
- RV082

Softwareversie

- v4.2.1.02

Configuratie van een IPv6-toegangsregel

IPv6-modus inschakelen

Stap 1. Meld u aan bij het programma voor webconfiguratie en kies **Setup > Netwerk**. De pagina *Netwerk* opent:

Network

Host Name : (Required by some ISPs)

Domain Name : (Required by some ISPs)

IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

IPv4 IPv6

LAN Setting

MAC Address : 54:75:D0:F7:FB:52

Device IP Address :

Subnet Mask :

Multiple Subnet : Enable

Stap 2. Klik op de radioknop **Dual-Stack IP**. Hiermee kunnen IPv4 en IPv6 tegelijkertijd worden uitgevoerd. Als IPv6-communicatie mogelijk is, dan is dat de geprefereerde communicatie.

IPv6-configuratie van toegangsregels

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

Access Rules

IPv4 IPv6

Item 1-3 of 3 Rows per page : 5

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<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		

Page 1 of 1

Stap 2. Klik op het tabblad IPv6. Dit opent de pagina *met IPv6-toegangsregels*.

Access Rules

IPv4 IPv6

Item 1-3 of 3 Rows per page : 5

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Delete
	<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	

Add Restore to Default Rules

Page 1 of 1

Stap 3. Klik op **Add** om de toegangsregels toe te voegen. De pagina *Toegangsregels* wordt weergegeven om de toegangsregels voor IPv6 te configureren.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP / Prefix Length: /

Destination IP / Prefix Length: /

Stap 4. Kies de vervolgkeuzelijst **toestaan** van de actie als het verkeer is toegestaan. Kies **Deny** om het verkeer te ontkennen.

Stap 5. Kies de juiste service in de vervolgkeuzelijst Service.

Timesaver: Als de gewenste service beschikbaar is, slaat u de stekker in op Stap 12.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP / Prefix Length: /

Destination IP / Prefix Length: /

Stap 6. Als de juiste service niet beschikbaar is, klikt u op **Servicebeheer**. Het venster *Service Management* verschijnt.

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]

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 7. Voer een naam in voor de nieuwe service in het veld Service Name.

Service Name :

Protocol : TCP ▼
TCP
UDP
IPv6

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 8. Kies het juiste protocoltype in de vervolgkeuzelijst Protocol.

- TCP (Transmission Control Protocol) — Een transportlaagprotocol dat wordt gebruikt door toepassingen waarvoor gegarandeerde levering vereist is.
- UDP (User Datagram Protocol) — Gebruikt datagram-camera's om host-communicatie op te zetten. UDP-levering is niet gegarandeerd.
- IPv6 (Internet Protocol versie 6) - leidt internetverkeer tussen hosts in pakketten die over netwerken worden routeerd die door het verzenden van adressen worden gespecificeerd.

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 9. Voer het poortbereik in het veld Poortbereik in. Dit bereik is afhankelijk van het protocol dat in de bovenstaande stap is geselecteerd.

Stap 10. Klik op **Toevoegen aan lijst**. Dit voegt de Service toe aan de vervolgkeuzelijst Service.

Service Name :

Protocol :

Port Range : to

NNTP [TCP/119~119]

POP3 [TCP/110~110]

SNMP [UDP/161~161]

SMTP [TCP/25~25]

TELNET [TCP/23~23]

TELNET Secondary [TCP/8023~8023]

TELNET SSL [TCP/992~992]

DHCP [UDP/67~67]

L2TP [UDP/1701~1701]

PPTP [TCP/1723~1723]

IPSec [UDP/500~500]

Service1[UDP/5060~5070]

Opmerking: Als u de service uit de servicelijst wilt verwijderen, kiest u de service uit de servicelijst en vervolgens klikt u op **Verwijderen**. Als u de service wilt bijwerken, kiest u de service die u vanuit de servicelijst wilt bijwerken en vervolgens klikt u op **Update**. Als u een

andere nieuwe service aan de lijst wilt toevoegen, klikt u op **Nieuw toevoegen**.

Stap 1. Klik op **OK**. Dit sluit het venster en voert de gebruiker terug naar de pagina *Toegangsregel*.

Opmerking: Als u op **Add New** klikt, volgt u de stappen 7 tot en met 11.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP / Prefix Length: / 128

Destination IP / Prefix Length: / 128

Stap 12. Als u de pakketten wilt loggen die overeenkomen met de toegangsregel, **kiezen u voor de pakketten** in de vervolgkeuzelijst **Log op deze regel**. Kies anders **niet loggen**.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP / Prefix Length: / 128

Destination IP / Prefix Length: / 128

Stap 13. Kies de interface die door deze regel wordt beïnvloed in de vervolgkeuzelijst Bron-interface. De broninterface is de interface waarvan het verkeer wordt gestart.

- LAN — Het lokale netwerk van de router.
- WAN1 - Het brede gebiedsnetwerk of het netwerk waarvan de router internet krijgt van de ISP of de volgende hoprouter.
- WAN2 — Dit is hetzelfde als WAN1, behalve dat het een secundair netwerk is.

- ALLE — Hiermee kan elke interface worden gebruikt.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP / Prefix Length: /

Destination IP / Prefix Length: /

Stap 14. In de vervolgkeuzelijst Bron IP kies een optie om het bron IP-adres te specificeren dat de toegangsregel wordt toegepast.

- Alle — toegangsregels worden toegepast op al het verkeer vanaf de broninterface. Er zullen geen velden rechts van de vervolgkeuzelijst beschikbaar zijn.
- Single-Access Rule zal op één IP adres van de broninterface worden toegepast. Voer het gewenste IP-adres in het adresveld in.
- Subnet - de toegangsregel zal op een netwerk van het broninterface worden toegepast. Voer het IP-adres en de lengte van het prefix in.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP / Prefix Length:

Destination IP / Prefix Length: /

Stap 15. In de vervolgkeuzelijst Bestemming IP; kies een optie om het IP-adres van de bestemming te specificeren dat de toegangsregel wordt toegepast.

- Alle — Toegangsregels worden toegepast op al het verkeer naar de doelinterface. Er zullen geen velden rechts van de vervolgkeuzelijst beschikbaar zijn.

- Enkelvoudig — Toegangsregel wordt toegepast op één IP-adres naar de doelinterface. Voer het gewenste IP-adres in het adresveld in.
- Subnet - de toegangsregel zal op een netwerk van het subnetwerk op de bestemmingsinterface worden toegepast. Voer het IP-adres en de lengte van het prefix in.

Stap 16. Klik op **Save** om alle wijzigingen op de IPv6-toegangsregel op te slaan.

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.