

Toegangsregels configuratie voor RV320 en RV325 VPN-routers

Doel

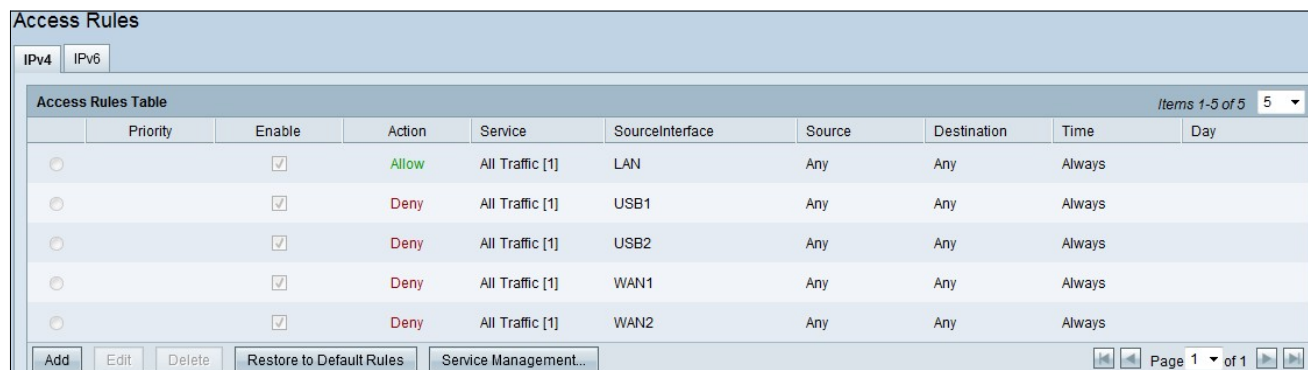
Toegangscontrolelijsten (ACL's) zijn lijsten die verkeer blokkeren of verhinderen dat er van en naar bepaalde gebruikers wordt verzonden. Toegangsregels kunnen zo worden ingesteld dat ze de hele tijd of op basis van een vastgesteld schema van kracht zijn. Een toegangsregel is op basis van verschillende criteria ingesteld om toegang tot het netwerk toe te staan of te weigeren. De toegangsregel is gepland op basis van het tijdstip waarop de toegangsregels op de router moeten worden toegepast. Dit artikel beschrijft de Wizard Instellen van de toegangsregel die wordt gebruikt om te bepalen of het verkeer in het netwerk mag binnengaan via de firewall van de router of niet om de veiligheid in het netwerk te verzekeren.

Toepasselijke apparaten | Versie firmware

- RV320 VPN-router met dubbel WAN | V 1.1.0.09 ([laatste download](#))
- RV325 Gigabit VPN-router met dubbel WAN | V 1.1.0.09 ([laatste download](#))

Configuratie van toegangsregels

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



	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

De tabel met toegangsregels bevat de volgende informatie:

- Prioriteit — Geeft de prioriteit van de toegangsregel weer
- Inschakelen — Geeft aan of de toegangsregel is ingeschakeld of uitgeschakeld
- Action — laat zien dat de toegangsregel is toegestaan of geweigerd.
- Service: toont het type service.
- SourceInterface - toont op welke interface de toegangsregel van toepassing is.
- Bron — Toont het IP-adres van het bronapparaat
- Bestemming — Geeft het IP-adres van het doelapparaat weer
- Tijd — Geeft aan wanneer de toegangsregel moet worden toegepast
- Dag — Geeft weer gedurende een week wanneer de toegangsregel van toepassing is

Servicebeheer

Stap 1. Klik op **Service Management** om een nieuwe service toe te voegen. De pagina *Service Management* wordt geopend:

<input type="checkbox"/>	Service Name	Protocol	Port Range	
<input type="checkbox"/>	All Traffic	TCP&UDP	1~65535	
<input type="checkbox"/>	DNS	UDP	53~53	
<input type="checkbox"/>	FTP	TCP	21~21	
<input type="checkbox"/>	HTTP	TCP	80~80	
<input type="checkbox"/>	HTTP Secondary	TCP	8080~8080	

Items 1-5 of 21 5 per page

Add Edit Delete Page 1 of 5

Save Cancel

Stap 2. Klik op **Add** om een nieuwe service toe te voegen.

<input type="checkbox"/>	Service Name	Protocol	Port Range	
<input type="checkbox"/>	All Traffic	TCP&UDP	1~65535	
<input type="checkbox"/>	DNS	UDP	53~53	
<input type="checkbox"/>	FTP	TCP	21~21	
<input type="checkbox"/>	HTTP	TCP	80~80	
<input type="checkbox"/>	HTTP Secondary	TCP	8080~8080	
<input type="checkbox"/>	Database	TCP	520 ~520	

Items 1-5 of 21 5 per page

Add Edit Delete Page 1 of 5

Save Cancel

Stap 3. Configuratie van de volgende velden.

- Servicenaam - Op basis van uw vereisten een naam voor de service geven
- Protocol — Kies een protocol TCP of UDP voor uw service
- Poortbereik — Voer het poortnummerbereik in dat is gebaseerd op uw vereisten en het poortnummer moet binnen het bereik liggen (1-65536).

Stap 4. Klik op **Save** om de wijzigingen op te slaan

Configuratie van toegangsregels op IPv4

Access Rules

IPv4 IPv6

Access Rules Table Items 1-5 of 5 5 per page

	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

Page 1 of 1

Stap 1. Klik op **Add** om een nieuwe toegangsregel te configureren. Het venster *Toegangsregels bewerken* verschijnt.

Edit Access Rules

Services

Action:

Service: [TCP&UDP/1~65535]

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Stap 2. Kies de gewenste optie in de vervolgkeuzelijst Handeling om verkeer voor de regel toe te staan of te beperken die u wilt instellen. Toegangsregels beperken de toegang tot het netwerk op basis van verschillende waarden.

- Sta toe — staat al het verkeer toe.
- Jeans: beperkt al het verkeer.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From:

To:

Effective on:

Mon Tue Wed Thu Fri Sat

Stap 3. Kies de juiste service die u moet filteren in de vervolgkeuzelijst Service.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Stap 4. Kies de gewenste optie Log in de vervolgkeuzelijst Log. De logoptie bepaalt of het apparaat een logbestand van het verkeer bijhoudt dat overeenkomt met de ingestelde toegangsregels.

- Logpakketten die aan deze toegangsregel beantwoorden — de router houdt een logbestand bij dat de service bijhoudt die is geselecteerd.
- Niet Log - de router houdt geen logbestanden voor de toegangsregel.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Stap 5. Kies de gewenste broninterface in de vervolgkeuzelijst Interface. Deze interface is waar de toegangsregel zou worden afgedwongen.

- LAN — De toegangsregel heeft alleen gevolgen voor het LAN-verkeer.
- WAN 1 — De toegangsregel heeft alleen gevolgen voor WAN 1-verkeer.
- WAN 2 — De toegangsregel heeft alleen gevolgen voor WAN 2-verkeer.
- Alle — De toegangsregel beïnvloedt alle verkeer in elk van de interfaces van het apparaat.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Stap 6. Kies het juiste bron-IP-type waarop de toegangsregel wordt toegepast in de vervolgkeuzelijst Bron-IP.

- Elk — Elk IP adres van het netwerk van het apparaat heeft de regel op hen van toepassing.
- Enkel - slechts één enkel gespecificeerd IP adres op het netwerk van het apparaat heeft de regel toegepast op het. Voer het gewenste IP-adres in het aangrenzende veld in.
- Bereik - Slechts een gespecificeerd bereik van IP adressen op het netwerk van het apparaat heeft de regel op hen van toepassing. Als u Bereik kiest, moet u de eerste en laatste IP adressen voor het bereik in de aangrenzende velden invoeren.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP: To

Destination IP:

- ANY
- Single
- Range

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu

Stap 7. Kies het juiste bestemming-IP-type waarop de toegangsregel wordt toegepast in de beschikbare vervolgkeuzelijst.

- Elk — Elk IP-adres van het bestemming heeft de regel op hen van toepassing.
- Enkel - slechts één enkel opgegeven IP-adres is van toepassing op deze regel. Voer het gewenste IP-adres in het aangrenzende veld in.
- Bereik - Slechts een gespecificeerd bereik van IP adres buiten het netwerk van het apparaat heeft de regel op hen van toepassing. Als u Bereik kiest, moet u de eerste en laatste IP adressen voor het bereik in de aangrenzende velden invoeren.

Scheduling

Time:

- Always
- Interval

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Timesaver: Standaard wordt de tijd ingesteld op Altijd. Als u de toegangsregel op een bepaalde tijd of dag wilt toepassen, volgt u Stap 8 naar Stap 1. Als u deze niet wilt toepassen, slaat u de

Stap 12 over.

Stap 8. Kies **Interval** in de vervolgkeuzelijst en de toegangsregels zijn actief voor bepaalde tijden. u moet het tijdsinterval invoeren voor de handhaving van de toegangsregel.

Scheduling

Time: Interval ▾

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

Stap 9. Voer het tijdstip in waarop u de toegangslijst wilt toepassen in het veld Van. De notatie voor de tijd is hh:mm.

Stap 10. Voer de tijd in waarop u de toegangslijst niet langer wilt toepassen in het veld Aan. De notatie voor de tijd is hh:mm.

Scheduling

Time: Interval ▾

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

Stap 1. Controleer het aankruisvakje van de specifieke dagen wanneer u de toegangslijst wilt toepassen.

Stap 12. Klik op **Opslaan** om de wijzigingen op te slaan.

Access Rules

IPv4 IPv6

Access Rules Table Items 1-5 of 6 5 ▾

Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
1 ▾	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	192.168.1.10 ~ 192.168.1.100	Any	03:00 ~ 07:00	All week
<input type="radio"/>	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	

Add Edit Delete Restore to Default Rules Service Management...

Page 1 of 2

Stap 13. (Optioneel) Als u de standaardregels wilt herstellen, klikt u op **Terugzetten op standaardregels**. Alle toegangsregels die door u zijn ingesteld, gaan verloren.

Configuratie van toegangsregels op IPv6

The screenshot shows the 'Access Rules' configuration page. At the top, there are two tabs: 'IPv4' and 'IPv6'. The 'IPv6' tab is selected and highlighted with a red circle. Below the tabs is the 'Access Rules Table' with a table of rules. The table has columns for Priority, Enable, Action, Service, SourceInterface, Source, Destination, Time, and Day. There are five rows of rules, all with 'All Traffic [1]' as the service and 'Always' as the time. The actions are 'Allow' for the first row and 'Deny' for the others. At the bottom, there are buttons for 'Add', 'Edit', 'Delete', 'Restore to Default Rules', and 'Service Management...'. The 'Add' button is highlighted with a red circle.

Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	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	

Stap 1. Klik op het tabblad IPv6 om IPv6-toegangsregels te configureren.

This screenshot is identical to the previous one, but the 'Add' button at the bottom left is highlighted with a red circle.

Stap 2. Klik op Add om een nieuwe IPv6-toegangsregel toe te voegen. Het venster *Toegangsregels bewerken* verschijnt.

The screenshot shows the 'Edit Access Rules' dialog box. It has a 'Services' section with several fields: 'Action' (set to 'Allow'), 'Service' (set to 'Allow' and highlighted with a red circle), 'Log' (set to 'No Log'), 'Source Interface' (set to 'LAN'), 'Source IP / Prefix Length' (set to 'ANY'), and 'Destination IP / Prefix Length' (set to 'ANY'). At the bottom, there are buttons for 'Save', 'Cancel', and 'Back'.

Stap 3. Kies de gewenste optie in de vervolgkeuzelijst Actie om de regel die u wilt instellen toe te staan of te beperken. Toegangsregels beperken de toegang tot het netwerk door de toegang tot het verkeer van specifieke diensten of apparaten toe te staan of te weigeren.

- Sta toe — staat al het verkeer toe.
- Jeans: beperkt al het verkeer.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP / Prefix Length:

Destination IP / Prefix Length:

Stap 4. Kies de juiste service die u moet filteren uit de vervolgkeuzelijst Service.

Opmerking: Wilt u alle verkeer toestaan, dan kiest u **al verkeer [TCP&UDP/1~65535]** uit de vervolgkeuzelijst voor de service als er actie is ingesteld om dit toe te staan. De lijst bevat alle soorten services die u zou willen filteren.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP / Prefix Length:

Destination IP / Prefix Length:

Stap 5. Kies de gewenste optie Log in de vervolgkeuzelijst Log. De logoptie bepaalt of het apparaat een logbestand van het verkeer bijhouden dat overeenkomt met de ingestelde toegangsregels.

- Ingeschakeld — Hiermee kan de router logtracking voor de geselecteerde service behouden.
- Niet Log - schakelt de router uit om log tracking te behouden.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: LAN
WAN1
WAN2
ANY

Destination IP / Prefix Length:

Save Cancel Back

Stap 6. Klik op de vervolgkeuzelijst Interface en kies de juiste broninterface. Deze interface is waar de toegangsregel zou worden afgedwongen.

- LAN — De toegangsregel heeft alleen gevolgen voor het LAN-verkeer.
- WAN 1 — De toegangsregel heeft alleen gevolgen voor WAN 1-verkeer.
- WAN 2 — De toegangsregel heeft alleen gevolgen voor WAN 2-verkeer.
- Alle — De toegangsregel beïnvloedt alle verkeer in elk van de interfaces van het apparaat.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: ANY ▾

Destination IP / Prefix Length: ANY
Single
Subnet

Save Cancel Back

Stap 7. Kies het juiste bron-IP-type waarop de toegangsregel van toepassing is, in de vervolgkeuzelijst Bron-IP/Prefixlengte.

- ALLE — Alle pakketten die van een netwerk van het apparaat worden ontvangen hebben de regel op hen van toepassing.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Single ▾ 2607:f0d0:1002:51::4 / 128

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- Enkel - slechts één enkel gespecificeerd IP adres in het netwerk van het apparaat heeft de regel toegepast op het. Voer het gewenste IPv6-adres in het aangrenzende veld in.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- Subnet — Alleen de IP adressen van een net hebben de regel op toegepast. Voer het IPv6-netwerkadres en de prefixlengte van het gewenste subtype in de aangrenzende velden in.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

- ANY
- Single
- Subnet

Save Cancel Back

Stap 8. Kies het juiste IP-type voor bestemming waarop de toegangsregel wordt toegepast, in de vervolgkeuzelijst Lengte bestemming / Voorvoegsel

- Elk — Elk IP-adres van het bestemming heeft de regel op hen van toepassing.
- Enkel - slechts één enkel gespecificeerd IP adres op het netwerk van het apparaat heeft de regel toegepast op het. Voer het gewenste IPv6-adres in.
- Subnet — Alleen de IP adressen van een net hebben de regel op toegepast. Voer het IPv6-netwerkadres en de prefixlengte van het gewenste subtype in de aangrenzende velden in.

Stap 9. Klik op **Opslaan** om de wijzigingen effectief te maken.

Bekijk een video gerelateerd aan dit artikel...

[Klik hier om andere Tech Talks uit Cisco te bekijken](#)