

Toegangsregels voor RV130 en RV130W toevoegen en configureren

Doel

Netwerkapparaten bieden basisfuncties voor verkeersfiltering met toegangsregels. Een toegangsregel is één ingang in een Toegangscontrolelijst (ACL) die een vergunning specificeert of regel (om een pakket door te sturen of te laten vallen) ontkent die op het protocol, een bron en een bestemmingsIP adres, of netwerkconfiguratie wordt gebaseerd.

Het doel van dit document is u te tonen hoe u een toegangsregel op de RV130 en RV130W kunt toevoegen en configureren.

Toepasselijke apparaten

•RV130

RV130W

Softwareversies

·Versie 1.0.1.3

Een toegangsregel toevoegen en configureren

Standaard uitgaand beleid instellen

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

Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

No data to display

Add Row Edit Enable Disable Delete Reorder

Save Cancel

Stap 2. Klik in het gebied *Default Outbound Policy* op de gewenste radioknop om een beleid voor uitgaand verkeer te kiezen. Het beleid wordt toegepast wanneer er geen toegangsregels of geconfigureerd beleid voor internettoegang zijn. De standaardinstelling is **Allow**, waarmee al het verkeer naar internet kan worden doorgegeven.

Access Rules

Default Outbound Policy

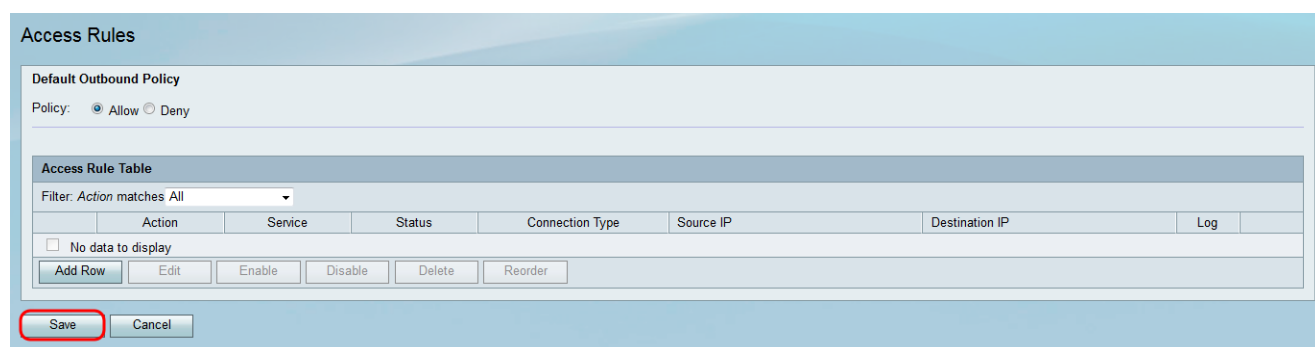
Policy: Allow Deny

Access Rule Table

De beschikbare opties zijn als volgt gedefinieerd:

- Toestaan — Laat alle soorten verkeer toe die van LAN naar Internet gaan.
- Ontken — blokkeer alle soorten verkeer die van LAN naar Internet gaan.

Stap 3. Klik op **Opslaan** om de instellingen op te slaan.



Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

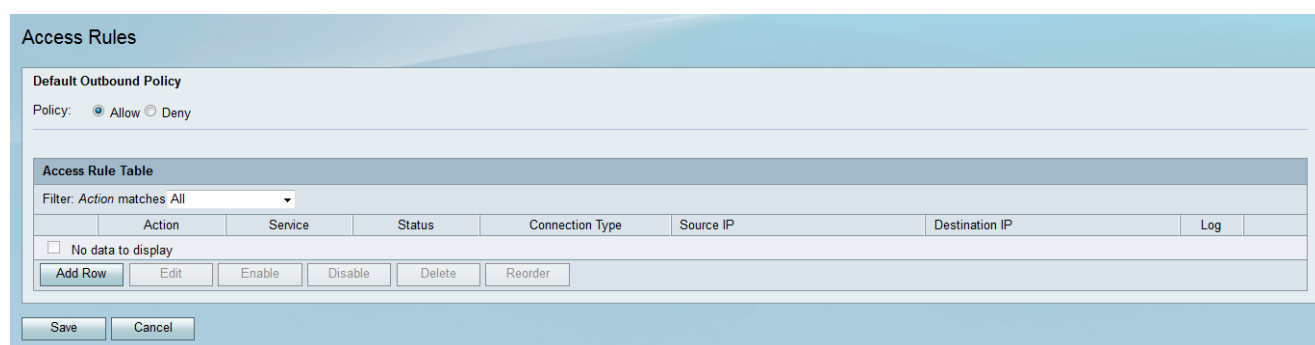
Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

No data to display

Een toegangsregel toevoegen

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



Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

No data to display

Stap 2. Klik op **Rij toevoegen** in de *tabel met toegangsregels* om een nieuwe toegangsregel toe te voegen.

Access Rules

Default Outbound Policy
 Policy: Allow Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

De pagina *Toegangsregel toevoegen* wordt geopend:

Add Access Rule

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

[Stap 3. Kies in de vervolgkeuzelijst *Type verbinding* het type verkeer waarvoor de regel geldt.](#)

Connection Type: Outbound (LAN > WAN) ▾
 Outbound (LAN > WAN)
 Inbound (WAN > LAN)
 Inbound (WAN > DMZ)

Action:

Schedule: ▾ Configure Schedules

Services: All Traffic ▾ Configure Services

Source IP: Any ▾

Start:

Finish:

De beschikbare opties zijn als volgt gedefinieerd:

- Uitgaand (LAN > WAN) — De regel heeft invloed op pakketten die afkomstig zijn van het lokale netwerk (LAN) en naar het internet (WAN) gaan.
- Inkomende (WAN > LAN) — De regel heeft invloed op pakketten die van internet (WAN) komen en naar het lokale netwerk (LAN) gaan.
- Inkomende (WAN > DMZ) — De regel beïnvloedt pakketten die van Internet (WAN) komen en in de gedemilitariseerde zone (DMZ) subnetwork gaan.

Stap 4. Kies in de vervolgkeuzelijst *Actie* de actie die moet worden uitgevoerd wanneer een regel wordt aangepast.

Connection Type: Outbound (LAN > WAN) ▾

Action: Always block ▾
 Always block
 Always allow
 Block by schedule
 Allow by schedule

Schedule: ▾ Schedules

Services: ▾ Configure Services

Source IP: Any ▾

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

De beschikbare opties zijn als volgt gedefinieerd:

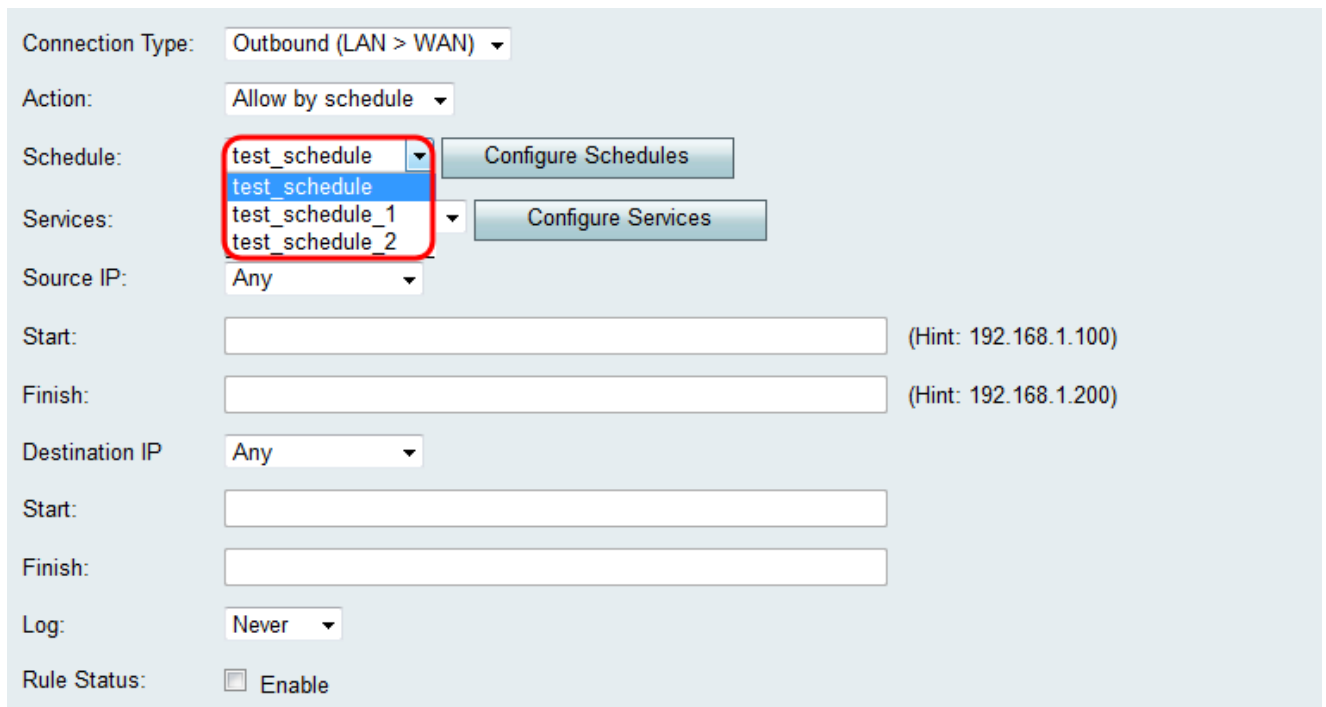
- Altijd Blokkeren — Altijd ontzeggen toegang als de voorwaarden worden aangepast. Naar stap 6.

·Altijd toestaan — altijd toegang verlenen als de voorwaarden worden aangepast. Naar stap 6.

·Blokken op schema — Toegang weigeren als de voorwaarden worden aangepast tijdens een vooraf ingesteld schema.

·Toestaan op schema — Toegang toestaan als de voorwaarden worden aangepast tijdens een vooraf ingesteld schema.

Stap 5. Als u **Blok door programma** koos of **door programma** in Stap 4 **toestaat**, kies het aangewezen programma van de vervolgkeuzelijst *Programma*.



Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: test_schedule_1 ▾

test_schedule_2

Source IP: Any ▾

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

Opmerking: Als u een schema wilt maken of bewerken, klikt u op **Schedules configureren**. Raadpleeg [Schedules voor configuratie op de RV130 en RV130W](#) voor meer informatie en richtlijnen.

Stap 6. Kies het type service waarop de toegangsregel van toepassing is uit de vervolgkeuzelijst *Services*.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: All Traffic ▾

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status:

All Traffic

All Traffic

DNS

FTP

HTTP

HTTP Secondary

HTTPS

HTTPS Secondary

TFTP

IMAP

NNTP

POP3

SNMP

SMT

TELNET

TELNET Secondary

TELNET SSL

Voice(SIP)

Opmerking: Als u een service wilt toevoegen of bewerken, klikt u op **Services configureren**. Raadpleeg [Servicebeheerconfiguratie op de RV130 en RV130W](#) voor meer informatie en richtlijnen.

IP-bron en -bestemming configureren voor uitgaand verkeer

Volg de stappen in deze sectie als **Uitgaand (LAN > WAN)** is geselecteerd als het verbindingstype in stap 3 van [het toevoegen van een toegangsregel](#).

Opmerking: Als een inkomend verbindingstype is geselecteerd in stap 3 van het toevoegen van een toegangsregel, gaat u naar de volgende sectie: [IP-bron en -bestemming configureren voor inkomend verkeer](#).

Stap 1. Kies hoe u de bron-IP wilt definiëren in de vervolgkeuzelijst *Bron-IP*. Voor uitgaand verkeer verwijst de bron-IP naar het adres of de adressen (in het netwerk) waarop de firewallregel van toepassing zou zijn.

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

De beschikbare opties zijn als volgt gedefinieerd:

- Alle — is van toepassing op verkeer vanaf elk IP-adres in het lokale netwerk. Laat daarom de velden *Start* en *Finish* leeg. Ga verder met Stap 4 als u deze optie kiest.
- Eén adres — is van toepassing op verkeer vanaf één IP-adres in het lokale netwerk. Voer in het veld *Start* het IP-adres in.
- Adresbereik — Van toepassing op verkeer afkomstig van een reeks IP-adressen in het lokale netwerk. Voer in het veld *Start* het eerste IP-adres van het bereik in en in het veld *Voltooien* het laatste IP-adres om het bereik in te stellen.

Stap 2. Als u in stap 1 **één adres** hebt gekozen, voert u het IP-adres in dat in het veld *Start* op de toegangsregel wordt toegepast en gaat u vervolgens naar stap 4. Als u **adresbereik** in stap 1 hebt gekozen, voert u een beginnend IP-adres in dat in het veld *Start op* de toegangsregel wordt toegepast.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Single Address ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

Stap 3. Als u in Stap 1 het **adresbereik** hebt gekozen, voert u het laatste IP-adres in dat het IP-adresbereik voor de toegangsregel in het veld *Voltoeien* inkapselt.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

Stap 4. Kies hoe u de bestemming IP wilt definiëren in de vervolgkeuzelijst *Bestemming IP*. Voor uitgaand verkeer verwijst Bestemming IP naar het adres of de adressen (in het WAN) waarnaar verkeer is toegestaan of geweigerd via het lokale netwerk.

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

De beschikbare opties zijn als volgt gedefinieerd:

- Alle — is van toepassing op verkeer naar een IP-adres in het openbare internet. Laat daarom de velden *Start* en *Finish* leeg.
- Eén adres — is van toepassing op verkeer dat naar één IP-adres in het openbare internet gaat. Voer in het veld *Start* het IP-adres in.
- Adresbereik — Dit is van toepassing op verkeer naar een reeks IP-adressen in het openbare internet. Voer in het veld *Start* het eerste IP-adres van het bereik in en in het veld *Voltoeien* het laatste IP-adres om het bereik in te stellen.

Stap 5. Als u in Stap 4 **één adres** hebt gekozen, voert u het IP-adres in dat in het veld *Start* op de toegangsregel wordt toegepast. Als u in Stap 4 het **adresbereik** hebt gekozen, voert u een beginnend IP-adres in dat in het veld *Start* op de toegangsregel wordt toegepast.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Single Address ▾

Start: 192.168.1.100

Finish:

Log: Never ▾

Rule Status: Enable

Stap 6. Als u in Stap 4 **Adresbereik** hebt gekozen, voert u het laatste IP-adres in dat het IP-adresbereik voor de toegangsregel in het veld *Voltooien* inkapselt.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status: Enable

[IP-bron en -bestemming configureren voor inkomend verkeer](#)

Volg de stappen in deze sectie als **Inbound (WAN > LAN)** of **Inbound (WAN > DMZ)** was geselecteerd als verbindingstype in stap 3 van [het toevoegen van een toegangsregel](#).

Stap 1. Kies hoe u de bron-IP wilt definiëren in de vervolgkeuzelijst *Bron-IP*. Voor inkomend verkeer verwijst de bron-IP naar het adres of de adressen (in het WAN) waarop de

firewallregel van toepassing zou zijn.

Connection Type: Inbound (WAN > LAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: All Traffic ▾

Source IP: Any ▾

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

De beschikbare opties zijn als volgt gedefinieerd:

- Alle — is van toepassing op verkeer afkomstig van een IP-adres in het openbare internet. Laat daarom de velden *Start* en *Finish* leeg. Ga verder met Stap 4 als u deze optie kiest.
- Eén adres — is van toepassing op verkeer dat afkomstig is van één IP-adres op het openbare internet. Voer in het veld *Start* het IP-adres in.
- Adresbereik — Van toepassing op verkeer afkomstig van een reeks IP-adressen op het openbare internet. Voer in het veld *Start* het eerste IP-adres van het bereik in en in het veld *Voltooien* het laatste IP-adres om het bereik in te stellen.

Stap 2. Als u in stap 1 **één adres** hebt gekozen, voert u het IP-adres in dat in het veld *Start* op de toegangsregel wordt toegepast en gaat u vervolgens naar stap 4. Als u in stap 1 **adresbereik** hebt gekozen, voert u een beginnend IP-adres in dat in het veld *Start* op de toegangsregel wordt toegepast.

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

Stap 3. Als u in Stap 1 het **adresbereik** hebt gekozen, voert u het laatste IP-adres in dat het IP-adresbereik voor de toegangsregel in het veld *Voltooien* inkapselt.

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

Stap 4. Voer in het veld *Start* onder de vervolgkeuzelijst *Bestemming IP* een enkel adres voor de bestemming IP in. Voor inkomend verkeer verwijst Bestemming IP naar het adres (in LAN) waarnaar verkeer vanaf het openbare internet is toegestaan of geweigerd.

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

Opmerking: Als **Inbound (WAN > DMZ)** was geselecteerd als het verbindingstype in stap 3 van het *toevoegen van een toegangsregel*, wordt het enige adres voor de bestemming IP automatisch geconfigureerd met het IP-adres van de ingeschakelde DMZ-host.

Vastlegging en inschakelen van de toegangsregel

Stap 1. Selecteer **altijd** in de vervolkeuzelijst *Log* als u wilt dat de router logbestanden maakt wanneer een pakket aan een regel voldoet. Selecteer **Nooit** als u wilt dat vastlegging nooit plaatsvindt wanneer een regel wordt aangepast.

Start:

Finish:

Log:

Rule Status: Enable

Stap 2. Controleer **het** aanvinkvakje **Enable** om de toegangsregel in te schakelen.

Add Access Rule

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status: Enable

Stap 3. Klik op **Opslaan** om de instellingen op te slaan.

Add Access Rule

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status: Enable

De *tabel met toegangsregels* wordt bijgewerkt met de nieuwe toegangsregel.

Access Rules



Configuration settings have been saved successfully

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

	Action	Service	Status	Connection Type	Source IP	Destination IP	Log
<input type="checkbox"/>	Allow by schedule	VOIP	Enabled	Outbound (LAN > WAN)	10.10.14.100 ~ 10.10.14.175	192.168.1.100 ~ 192.168.1.170	Never

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.