

Servicebeheer voor toegangsregels voor RV160X/RV260X routers

Doel

Het doel van dit artikel is om u te tonen hoe u de toegangsregels op de routers RV160 en RV260 kunt configureren.

Inleiding

De toegangsregels definiëren de regels die het verkeer moet naleven om door een interface te bladeren. Een toegangsregel staat of ontkent verkeer toe op basis van het protocol, een bron- en doeladres of -netwerk en naar keuze de bron- en doelpoorten.

Wanneer u toegangsregels naar apparaten implementeert, worden ze een of meer toegangscontrolelijsten (ACE's) naar toegangscontrolelijsten (ACL's) die aan interfaces zijn gekoppeld. Meestal zijn deze regels het eerste beveiligingsbeleid dat op pakketten wordt toegepast; zij zijn uw eerste verdedigingslinie. Elk pakket dat op een interface aankomt wordt onderzocht om te bepalen of het pakket door te sturen of te laten vallen gebaseerd op de criteria die u specificeert. Als u toegangsregels in de uitrichting definieert, worden de pakketten ook geanalyseerd voordat ze een interface mogen verlaten.

Toepasselijke apparaten

- RV160
- RV260

Softwareversie

- 1.0.00.15

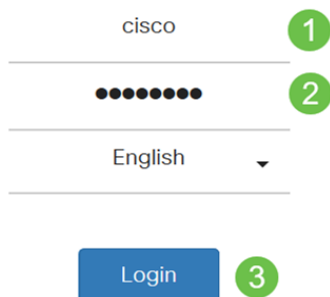
Toegangsregels instellen

Om de toegangsregels op de RV160/RV260 te configureren volgt u deze stappen.

Stap 1. Meld u aan bij de webconfiguratie van uw router.



Router

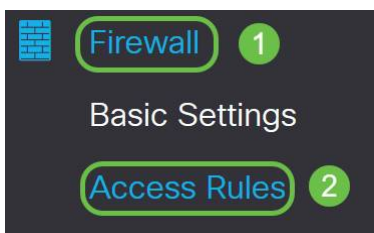


©2018 Cisco Systems, Inc. All Rights Reserved.

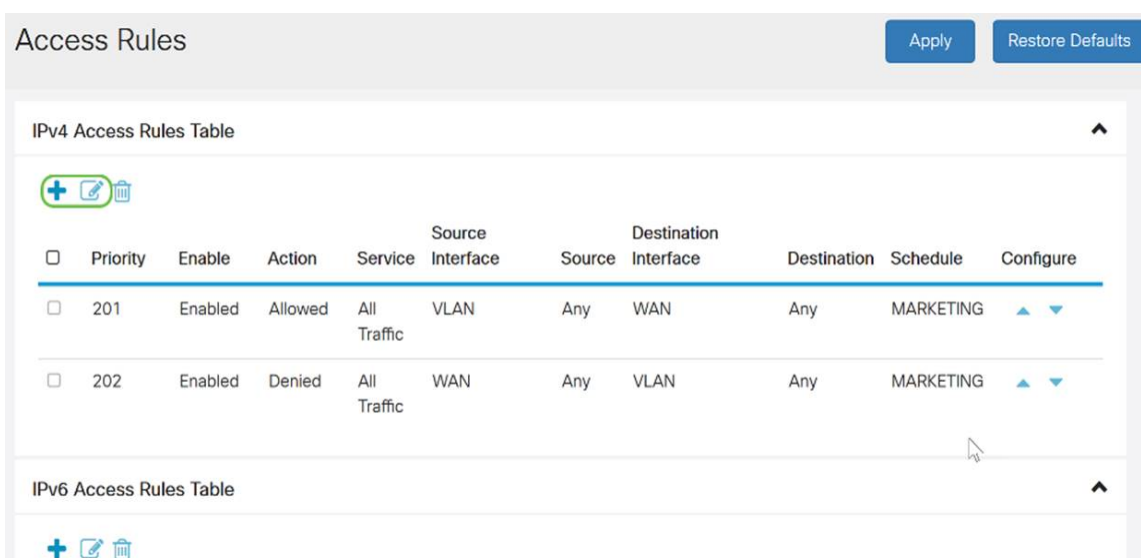
Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Opmerking: In dit artikel zullen we de RV260W gebruiken om toegangsregels te configureren. De configuratie kan variëren afhankelijk van het model dat u gebruikt.

Stap 2. navigeren naar **firewall > toegangsregels**.



Stap 3. In de *tabel met IPv4- of IPv6-toegangsregels*, klikt u op **Toevoegen** of selecteert u de rij en vervolgens klikt u op **Bewerken**.



Stap 4. Voer in het gedeelte *Toegangsregels toevoegen/bewerken* de volgende velden in.

<i>Regelstatus</i>	Controleer <i>Schakel</i> de specifieke toegangsregel in. Uitschakelen om uit te schakelen
<i>Handeling</i>	Kies <i>toestaan</i> of <i>ontkennen</i> in de

	vervolgkeuzelijst.
<i>Services</i>	<i>IPv4</i> - Selecteer de service die u wilt toepassen op IPv4-regel. <i>IPv6</i> - Selecteer de service die u wilt toepassen op IPv6-regels. <i>Services</i> - Selecteer de service in de vervolgkeuzelijst.
<i>Log</i>	Selecteer een optie in de vervolgkeuzelijst. <i>Altijd</i> - er worden formulieren weergegeven die overeenkomen met de regels. <i>Nooit</i> - Geen logbestand vereist.
<i>Bron-interface</i>	Selecteer de broninterface in de vervolgkeuzelijst.
<i>Bronadres</i>	Selecteer het bron IP-adres waarop de regel van toepassing is en voer het volgende in: <i>Any</i> - selecteer deze optie om alle IP-adressen aan te passen. <i>Enkelvoudig</i> - Voer een IP-adres in. <i>Subnet</i> - Voer een subtype van een netwerk in. <i>IP-bereik</i> - Voer het bereik van IP-adressen in.
<i>Bestemmingsinterface</i>	Selecteer de broninterface in de vervolgkeuzelijst.
<i>Doeladres</i>	Selecteer het bron IP-adres waarop de regel van toepassing is en voer het volgende in: <i>Any</i> - selecteer deze optie om alle IP-adressen aan te passen. <i>Enkelvoudig</i> - Voer een IP-adres in. <i>Subnet</i> - Voer een subtype van een netwerk in. <i>IP-bereik</i> - Voer het bereik van IP-adressen in.
<i>Naam schema</i>	Selecteer <i>Altijd, Business, evening hour, marketing of werktijd</i> in de vervolgkeuzelijst om de firewallregel toe te passen. Klik vervolgens <i>hier</i> om de schema's te configureren.

Add/Edit Access Rules

Apply

Cancel

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 ▾

Log: Always Never

Source Interface: ▾

Source Address: ▾

Destination Interface: ▾

Destination Address: ▾

Schedule

Stap 5. (Optioneel) Klik om de schema's te configureren **hier** naast *Schedule Name*.

Schedule

Schedule Name: Click [here](#) to configure the schedules.

Stap 6. (Optioneel) Klik op **Add** om een programma toe te voegen of selecteer de rij en klik op **Bewerken**.

Schedules Apply Cancel Back

[+](#) [✎](#) [🗑](#)

<input type="checkbox"/>	Name	Start (24hh:mm:ss)	End (24hh:mm:ss)	Days
<input checked="" type="checkbox"/>	Always	00:00:00	23:59:59	Everyday
<input type="checkbox"/>	BUSINESS	09:00:00	17:30:00	Weekdays
<input type="checkbox"/>	EVENINGHOURS	18:01:00	23:59:59	Everyday
<input type="checkbox"/>	MARKETING	00:00:00	23:59:59	Everyday
<input type="checkbox"/>	WORKHOURS	08:00:00	18:00:00	Weekdays

Opmerking: Klik [hier](#) voor meer informatie over de configuratie van het schema.

Stap 7. (Optioneel) Klik op **Toepassen**.

Add/Edit Access Rules Apply Cancel

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6

Log: Always Never

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Schedule

Schedule Name: Click [here](#) to configure the schedules.

Stap 8. (Optioneel) Klik op **Standaardinstellingen herstellen** om de standaardinstellingen te herstellen.

Access Rules Apply Restore Defaults

IPv4 Access Rules Table [↑](#)

[+](#) [✎](#) [🗑](#)

Servicebeheer

Stap 1. Klik op **Service Management** om een item in de servicelijst toe te voegen of te

bewerken.

Access Rules

Apply Restore Defaults

Traffic

<input type="checkbox"/>	202	Enabled	Denied	All Traffic	WAN	Any	VLAN	Any	MARKETING	▲ ▼
--------------------------	-----	---------	--------	-------------	-----	-----	------	-----	-----------	-----

IPv6 Access Rules Table

+ [edit] [delete]

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input type="checkbox"/>	201	Enabled	Allowed	All Traffic	VLAN	Any	WAN	Any	MARKETING	▲ ▼
<input type="checkbox"/>	202	Enabled	Denied	All Traffic	WAN	Any	VLAN	Any	MARKETING	▲ ▼

Service Management...

Stap 2. Als u een service wilt toevoegen, klikt u op **Add** onder de servicetabel. U kunt een service bewerken door de rij te selecteren en op **Bewerken** te klikken. De velden kunnen worden gewijzigd.

Service Management

Apply Cancel Back

+ [edit] [delete] [download] [upload]

<input type="checkbox"/>	Name	Protocol	Port Start/ICMP Type/IP Protocol	Port End/ICMP Code
<input type="checkbox"/>	All Traffic	ALL	--	--
<input type="checkbox"/>	BGP	TCP	179	179
<input type="checkbox"/>	DNS-TCP	TCP	53	53
<input type="checkbox"/>	DNS-UDP	UDP	53	53
<input type="checkbox"/>	ESP	IP	50	--
<input type="checkbox"/>	FTP	TCP	21	21
<input type="checkbox"/>	HTTP	TCP	80	80

Stap 3. U kunt veel services in de lijst uitvoeren:

- *Naam* - Naam van de dienst of de toepassing.
- *Protocol* - Selecteer een protocol in de vervolgkeuzelijst.
- *Port Start/ICMP Type/IP Protocol* - Bereik van poortnummers gereserveerd voor deze service.
- *Port End-of-ICMP-code* - Het laatste nummer van de poort, gereserveerd voor deze service.

Service Management

Apply

Cancel

Back



<input type="checkbox"/>	Name	Protocol	Port Start/ICMP Type/IP Protocol	Port End/ICMP Code
<input type="checkbox"/>	All Traffic	ALL	--	--
<input type="checkbox"/>	BGP	TCP	179	179
<input type="checkbox"/>	DNS-TCP	TCP	53	53
<input type="checkbox"/>	DNS-UDP	UDP	53	53
<input type="checkbox"/>	ESP	IP	50	--
<input type="checkbox"/>	FTP	TCP	21	21
<input type="checkbox"/>	HTTP	TCP	80	80

Stap 4. Als u een of meer instellingen hebt toegevoegd of bewerkt, klikt u op **Toepassen**.

Service Management

Apply

Cancel

Back



<input type="checkbox"/>	Name	Protocol	Port Start/ICMP Type/IP Protocol	Port End/ICMP Code
<input type="checkbox"/>	All Traffic	ALL	--	--
<input type="checkbox"/>	BGP	TCP	179	179
<input type="checkbox"/>	DNS-TCP	TCP	53	53
<input type="checkbox"/>	DNS-UDP	UDP	53	53
<input type="checkbox"/>	ESP	IP	50	--
<input type="checkbox"/>	FTP	TCP	21	21
<input type="checkbox"/>	HTTP	TCP	80	80

U moet nu met succes de toegangsregels voor uw RV160/RV260-router hebben ingesteld.