

Configure Service Management for Access Rules on RV160X/RV260X Routers

Objective

The objective of this article is to show you how to configure access rules on the RV160 and RV260 routers.

Introduction

Access rules define the rules that traffic must meet to pass through an interface. An access rule permits or denies traffic based on the protocol, a source and destination IP address or network, and optionally the source and destination ports.

When you deploy access rules to devices, they become one or more Access Control Entries (ACEs) to Access Control Lists (ACLs) that are attached to interfaces. Typically, these rules are the first security policy applied to packets; they are your first line of defense. Each packet that arrives at an interface is examined to determine whether to forward or drop the packet based on the criteria you specify. If you define access rules in the out direction, packets are also analyzed before they are allowed to leave an interface.

Applicable Devices

- RV160
- RV260

Software Version

- 1.0.00.15

Configure Access Rules

To configure access rules on the RV160/RV260, follow these steps.

Step 1. Log in to the web configuration page of your router.



Router

cisco **1**

•••••••• **2**

English ▾

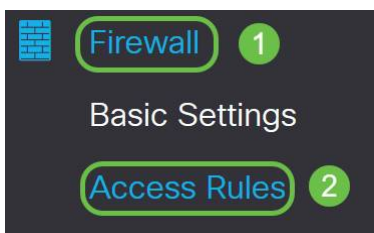
Login **3**

©2018 Cisco Systems, Inc. All Rights Reserved.

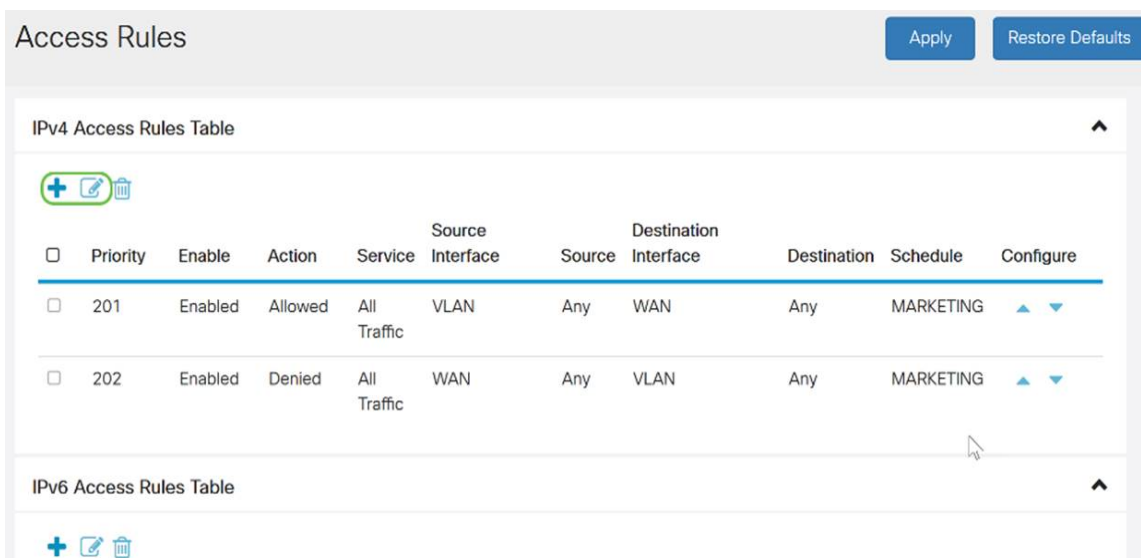
Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Note : In this article, we will be using the RV260W to configure access rules. The configuration may vary depending on the model you are using.

Step 2. Navigate to **Firewall > Access Rules**.



Step 3. In the *IPv4 or IPv6 Access Rules Table*, click **Add** or select the row and click **Edit**.



Step 4. In the *Add/Edit Access Rules* section, enter the following fields.

<i>Rule Status</i>	Check <i>Enable</i> to enable the specific access rule. Uncheck to disable.
<i>Action</i>	Choose <i>Allow</i> or <i>Deny</i> from the drop-down list.

<i>Services</i>	<ul style="list-style-type: none"> • <i>IPv4</i> – Select the service to apply IPv4 rule. • <i>IPv6</i> – Select the service to apply IPv6 rule. • <i>Services</i> – Select the service from the drop-down list.
<i>Log</i>	<p>Select an option from the drop-down list.</p> <ul style="list-style-type: none"> • <i>Always</i> – Logs appear for packet that matches the rules. • <i>Never</i> – No log required.
<i>Source Interface</i>	Select the source interface from the drop-down list.
<i>Source Address</i>	<p>Select the source IP address to which the rule is applied and enter the following:</p> <ul style="list-style-type: none"> • <i>Any</i> – Select to match all IP addresses. • <i>Single</i> – Enter an IP address. • <i>Subnet</i> – Enter a subnet of a network. • <i>IP Range</i> – Enter the range of IP addresses.
<i>Destination Interface</i>	Select the source interface from the drop-down list.
<i>Destination Address</i>	<p>Select the source IP address to which the rule is applied and enter the following:</p> <ul style="list-style-type: none"> • <i>Any</i> – Select to match all IP addresses. • <i>Single</i> – Enter an IP address. • <i>Subnet</i> – Enter a subnet of a network. • <i>IP Range</i> – Enter the range of IP addresses.
<i>Schedule Name</i>	Select <i>Always, Business, Evening hours, Marketing, or Work hours</i> from the drop-down list to apply the firewall rule. Then, click <i>here</i> to configure the schedules.

Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 v

Log: Always Never

Source Interface: v

Source Address: v

Destination Interface: v

Destination Address: v

Schedule

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

Step 5. (Optional) To configure schedules, click **here** next to *Schedule Name*.

Schedule

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

Step 6. (Optional) Click **Add** to add a schedule or select the row and click **Edit**.

Schedules Apply Cancel Back

[+](#) [✎](#) [🗑](#)

<input type="checkbox"/>	Name	Start (24h:mm:ss)	End (24h:mm:ss)	Days
<input 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

Note: For more information on configuration of schedule, click [here](#).

Step 7. (Optional) Click **Apply**.

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.

Step 8. (Optional) Click **Restore Defaults**, to restore the default settings.

Access Rules Apply Restore Defaults

IPv4 Access Rules Table [^](#)

[+](#) [✎](#) [🗑](#)

Service Management

Step 1. To add or edit an entry on the Service list, click on **Service Management**.

Access Rules Apply Restore Defaults

Traffic

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

IPv6 Access Rules Table ▲

+ ✎ 🗑

<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...

Step 2. To add a service, click **Add** under the Service table. To edit a service, select the row and click **Edit**. The fields open for modification.

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

Step 3. You can have many services in the list:

- *Name* - Name of the service or application.
- *Protocol* - Select a protocol from the drop-down list.
- *Port Start/ICMP Type/IP Protocol* - Range of port numbers reserved for this service.
- *Port End/ICMP Code* - Last number of the port, reserved for this 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

Step 4. If you've added or edited any settings, click **Apply**.

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

You should now have successfully configured access rules on your RV160/ RV260 router.