

Access Rules Configuration on RV215W

Objective

The RV215W allows for the configuration of access rules to increase security. These Access Control Lists (ACLs) are lists that block or allow traffic from being sent to and from certain users. They can be configured to be in effect all the time or based on defined schedules.

This article explains how to configure access rules on the RV215W.

Applicable Devices

- RV215W

Software Version

- 1.1.0.5

Access Rules

Step 1. Log in to the web configuration utility and choose **Firewall > Access Rules**. The *Access Rules* page opens:

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	Priority
<input type="checkbox"/> No data to display							

Step 2. Click the radio button that corresponds to the desired default outbound policy in the Policy field. The default outbound policy determines if outbound traffic is allowed or denied. It is used whenever there are no access rules or internet access policies configured to an IP address of a user.

Step 3. Click **Save**.

Add Access Rule

Step 1. Click **Add Row** to add a new access rule. The Add Access Rule page opens:

Add Access Rule

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100 or fec0::64)

Finish: (Hint: 192.168.1.200 or fec0::c8)

Destination IP:

Start:

Finish:

Log:

QoS Priority:

Rule Status: Enable

Step 2. From the Connection Type drop-down list choose the type of rule to create.

- Outbound (LAN > WAN) — The rule affects packets that come from the secure LAN and go to the unsecure WAN.
- Inbound (WAN > LAN) — The rule affects packets that come from the unsecure WAN and go to secure LAN.
- Inbound (WAN > DMZ) — The rule affects packets that come from the unsecure WAN and go to the DMZ. A DMZ is a network segment that separates the LAN from the WAN to provide an added layer of security.

Step 3. From the Action drop-down list choose the action that is to be applied to the rule.

- Always Block — Always blocks packets.
- Always Allow — Always allows packets.
- Block by schedule — Blocks packets based on a specified schedule.
- Allow by schedule — Allows packets based on a specified schedule.

Step 4. From the Schedule drop-down list choose a schedule to apply to the rule.

Step 5. From the Services drop-down list choose a service to allow or block.

Note: Click **Configure Services** to configure schedules on the *Service Management* page.

Step 6. From the Source IP drop-down list choose the source IP addresses to which the rule blocks or allows packets from.

- Any — The rule applies to all source IP addresses.
- Single Address — Enter a single IP address to which the rule applies in the Start field.
- Address Range — Enter a range of IP addresses to which the rule applies to in the Start and Finish fields.

Step 7. From the Destination IP drop-down list choose the destination IP addresses to which the rule blocks or allows packets to.

- Any — The rule applies to all destination IP addresses.
- Single Address — Enter a single IP address to which the rule applies to in the Start field.
- Address Range — Enter a range of IP addresses to which the rule applies to in the Start and Finish fields.

Step 8. From the Log drop-down list choose a log option. Logs are generated system records that are used for security management.

- Never — Disables Logs.
- Always — The RV215W creates a log whenever a packet matches the rule.

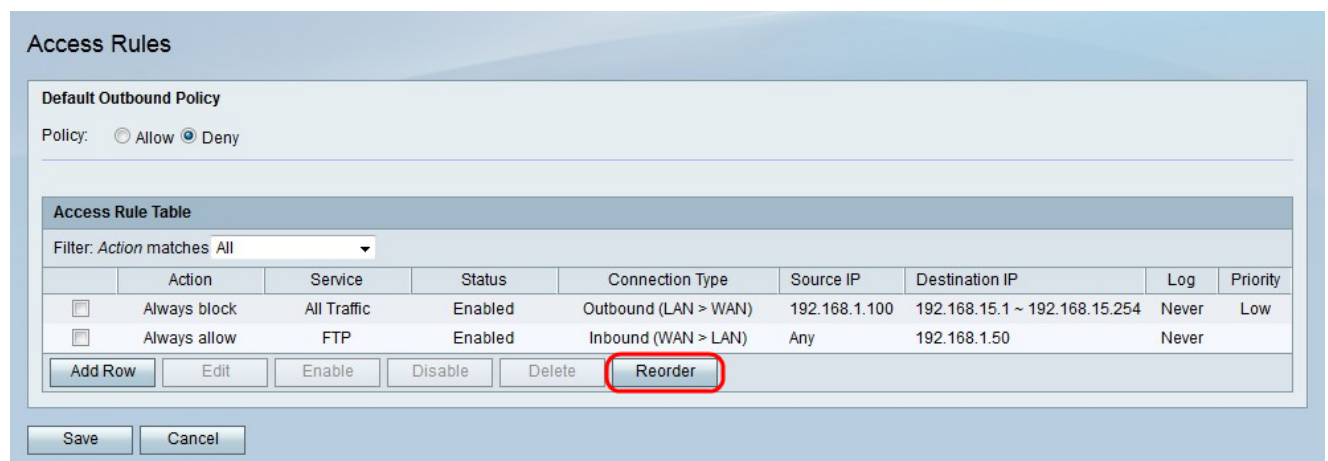
Step 9. From the QoS Priority drop-down list choose a priority for the outbound IP packets of the rule. Priority one is the lowest while priority four is the highest. Packets in higher priority queues will be sent before those in lower priority queues.

Step 10. Check **Enable** in the Rule Status field to enable the rule.

Step 11. Click **Save**.

Reorder Access Rules

The reorder feature is an important option on the RV215W. The order in which the access rules are displayed in the access rule table indicates the order in which the rules are applied. The first rule in the table is the first rule to be applied.



The screenshot shows the 'Access Rules' configuration interface. At the top, there is a 'Default Outbound Policy' section with radio buttons for 'Allow' and 'Deny' (selected). Below this is the 'Access Rule Table' with a filter set to 'Action matches All'. The table contains two rules:

	Action	Service	Status	Connection Type	Source IP	Destination IP	Log	Priority
<input type="checkbox"/>	Always block	All Traffic	Enabled	Outbound (LAN > WAN)	192.168.1.100	192.168.15.1 ~ 192.168.15.254	Never	Low
<input type="checkbox"/>	Always allow	FTP	Enabled	Inbound (WAN > LAN)	Any	192.168.1.50	Never	

Below the table are buttons for 'Add Row', 'Edit', 'Enable', 'Disable', 'Delete', and 'Reorder' (highlighted with a red circle). At the bottom are 'Save' and 'Cancel' buttons.

Step 1. Click **Reorder** to reorder the access rules.

Step 2. Check the box of the access rule you want to reorder.

Access Rule Table								
	Priority	Action	Service	Status	Connection Type	Source IP	Destination IP	Log
<input type="checkbox"/>	Low	Always block	All Traffic	Enabled	Outbound (LAN > WAN)	192.168.1.100	192.168.15.1 - 192.168.15.254	Never
<input checked="" type="checkbox"/>		Always allow	FTP	Enabled	Inbound (WAN > LAN)	Any	192.168.1.50	Never

Move to: 1

Save Cancel Back

Step 3. From the drop-down list choose a position you want to move the specified rule to.

Step 4. Click **Move to** to reorder the rule. The rule moves to the specified position in the table.

Note: The up and down arrow buttons can also be used to reorder the access rules.

Step 5. Click **Save**.

Schedule Management Configuration

Step 1. Log in to the web configuration utility and choose **Firewall > Schedule Management**. The *Schedule Management* page opens:

Schedule Management

<input type="checkbox"/>	Name	Days	Start Time	End Time
<input type="checkbox"/>	No data to display			

Add Row Edit Delete

Save Cancel

Step 2. Click **Add Row** to add a new schedule. The *Add/Edit Schedules* page opens:

Add/Edit Schedules

Add/Edit Schedules Configuration

Name:

Scheduled Days

Do you want this schedule to be active on all days or specific days?

▼

Monday:

Tuesday:

Wednesday:

Thursday:

Friday:

Saturday:

Sunday:

Scheduled Time of Day

Do you want this schedule to be active on all days or at specific times during the day?

▼

Start time: Hours Minutes

End time: Hours Minutes

Save

Cancel

Back

Step 3. Enter a name for the schedule in the Name field.

Step 4. From the Scheduled Days drop-down list choose the days the schedule is active.

- All Days — The schedule is active for every day of the week.
- Specific Days — Check the check boxes of the days for the schedule to be active.

Step 5. From the Scheduled Time of Day drop-down list choose the time the schedule is active.

- All Times — The schedule is active at all times of the day.

- Specific Times — From the Start Time and End Time drop-down list choose the time the schedule starts and the time the schedule ends.

Step 6. Click **Save**.