Configure Access Rules on an RV34x Series Router

Objective

The RV340 Dual-WAN VPN Router is an easy-to-use, flexible, high-performance device well suited for small businesses. With added security features, such as Web Filtering, Application Control, and IP Source Guard. The new RV340 delivers highly secure, broadband, wired connectivity to small offices and remote employees. These new security features also provide the ease of fine tuning permitted activity on the network.

Access Rules or policies on the RV34x Series Router allow the configuration of rules to increase security in the network. A combination of rules, and you have an Access Control List (ACL). ACLs are lists that block or allow traffic from being sent to and from certain users. Access Rules can be configured to be in effect all the time or based on defined schedules.

ACLs have an implicit deny at the end of the list, so unless you explicitly permit it, traffic cannot pass. For example, if you want to allow all users to access a network through the router except for particular addresses, then you need to deny the particular addresses and then permit all others.

The objective of this article is to show you how to configure access rules on an RV34x Series Router.

Applicable Devices

- RV34x Series

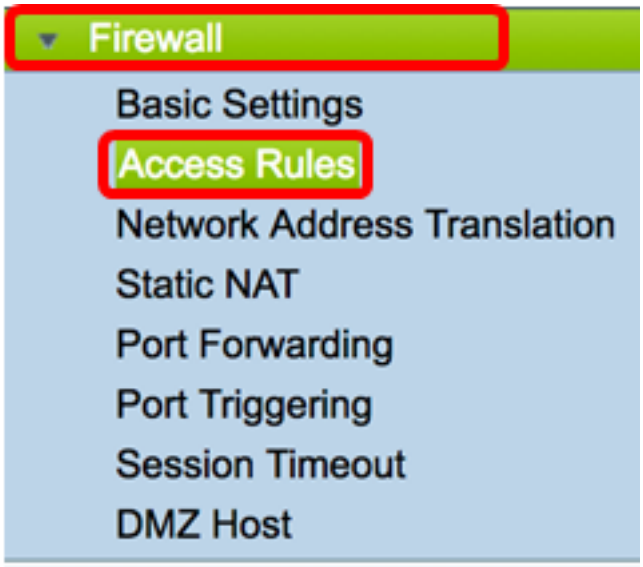
Software Version

- 1.0.1.16
  - A firmware updating the UI has become available since this article's publishing, click here to go to the downloads page, locate your specific product there.

Configure an Access Rule on an RV34x Series Router

Create an Access Rule

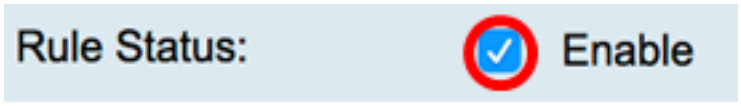
Step 1. Log in the web-based utility of the router and choose **Firewall > Access Rules**.



Step 2. In the IPv4 or IPv6 Access Rules table, click **Add** to create a new rule.

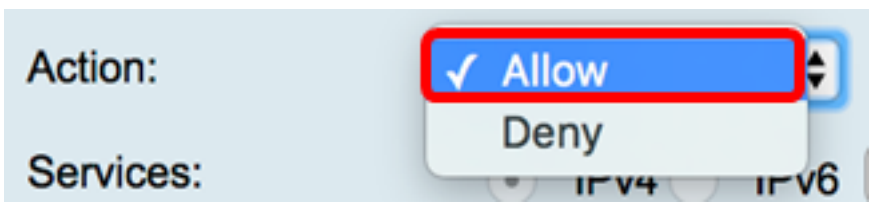
Note: On the RV34x Series Router, it is possible to configure up to 202 rules. In this example, IPv4 is used.

Step 3. Check the **Enable Rule Status** check box to enable the rule.



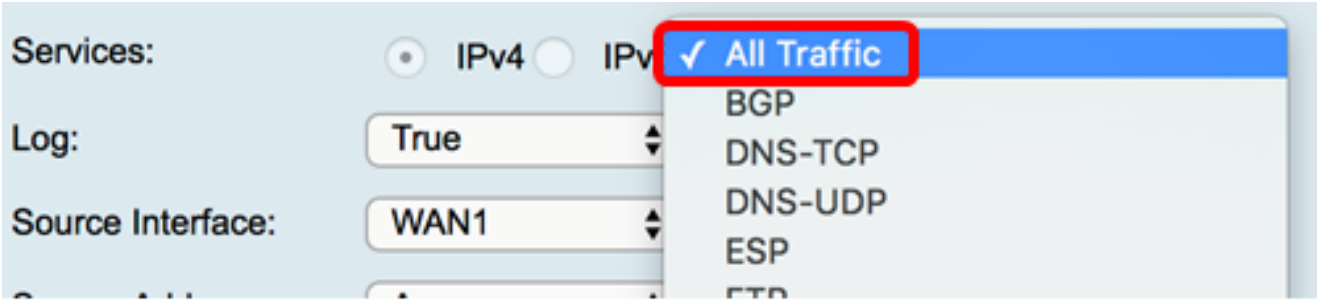
Step 4. In the Action drop-down menu, choose whether the policy will Allow or Deny data.

Note: In this example, Allow is chosen.



Step 5. From the Services drop-down menu, choose the kind of traffic that the router will either allow or deny.

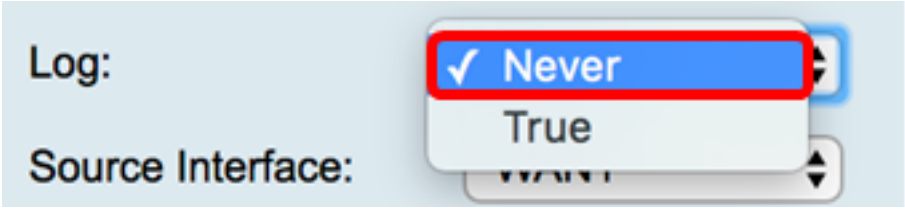
Note: For this example, All traffic is chosen. All traffic will be permitted.



Step 6. From the Log drop-down menu, choose an option to determine if the router will log the traffic that was permitted or denied. The options are:

- Never — Router will never log any traffic that was permitted and denied.
- True — Router will log traffic that matches the policy.

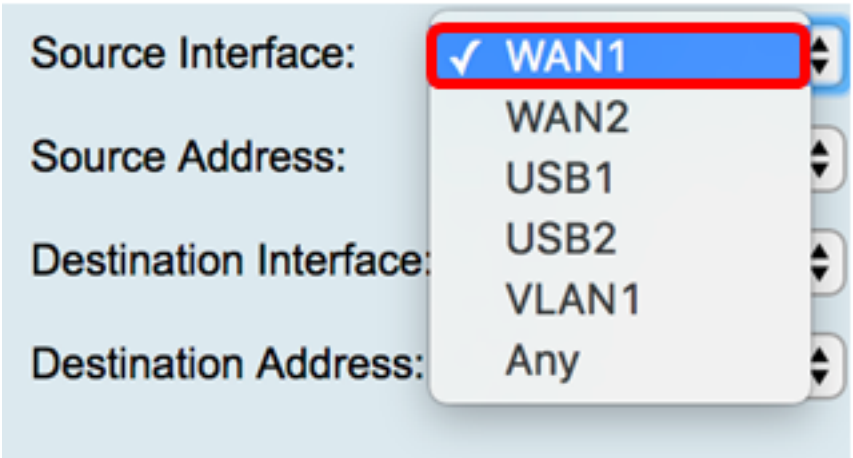
Note: In this example, Never is chosen.



Step 7. From the Source Interface drop-down menu, choose an interface for the incoming or inbound traffic where the access policy should be applied. The options are

- WAN1 — The policy applies only to the traffic from WAN1.
- WAN2 — The policy applies only to the traffic from WAN2.
- USB1 — The policy applies only to the traffic from USB1.
- USB2 — The policy applies only to the traffic from USB2.
- VLAN1 — The policy applies only to the traffic VLAN1.
- Any — The policy applies to any interface.

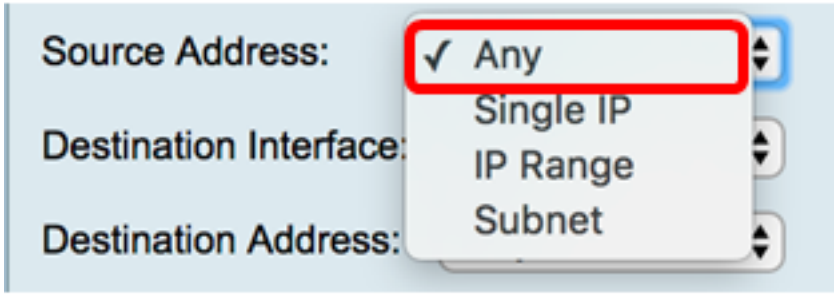
Note: If an additional Virtual Local Area Network (VLAN) has been configured, the VLAN option will appear on the list. In this example, WAN1 is chosen.



Step 8. From the Source Address drop-down menu, choose a source to apply the policy. The options are:

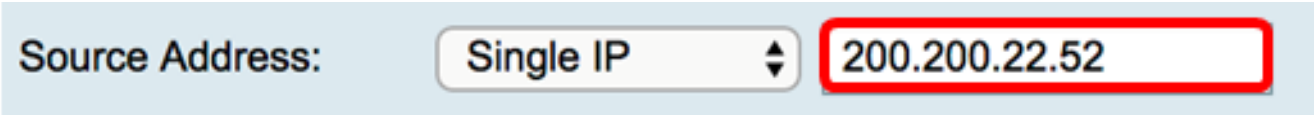
- Any — The policy will apply to any IP address on the network. If this is chosen, skip to Step 12 .
- Single IP — The policy applies to a single host or IP address. If this is chosen, skip to Step 9.
- IP Range — The policy applies to a set or range of IP addresses. If this is chosen, skip to Step 10.
- Subnet — The policy applies to an entire subnetwork. If this is chosen, skip to Step 11.

Note: In this example, Any is chosen.



Step 9. (Optional) Single IP was chosen in Step 8, enter a single IP address for the policy to be applied then skip to Step 12.

Note: For this example, 200.200.22.52 is used.



Step 10. (Optional) If IP Range was chosen in Step 8, enter the beginning and ending IP addresses in the respective IP address fields.

Note: In this example, 200.200.22.22 is used as the beginning IP address and 200.200.22.34 as the ending IP address.

Step 11. (Optional) If Subnet was chosen in Step 8, enter the network ID and its respective subnet mask to apply the policy.

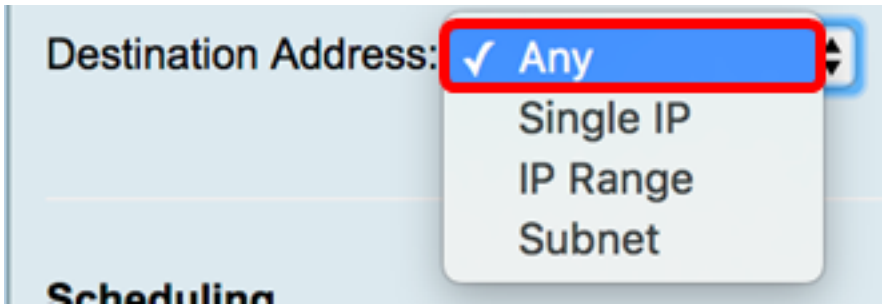
Note: In this example, 200.200.22.1 is used as the subnet ID and 24 as the subnet mask.

Step 12. From the Destination Interface drop-down menu, choose an interface for the outgoing or outbound traffic where the access policy should be applied. The options are WAN1, WAN2, USB1, USB2, VLAN1, and Any.

Note: For this example, WAN1 is chosen.

Step 13. From the Destination Address drop-down menu, choose a destination to apply the policy. The options are Any, Single IP, IP Range, Subnet.

Note: In this example, Any is chosen. Skip to Step 17.



Step 14. (Optional) If Single IP was chosen in Step 13, enter a single IP address for the policy to be applied.

Note: For this example, 210.200.22.52 is used.

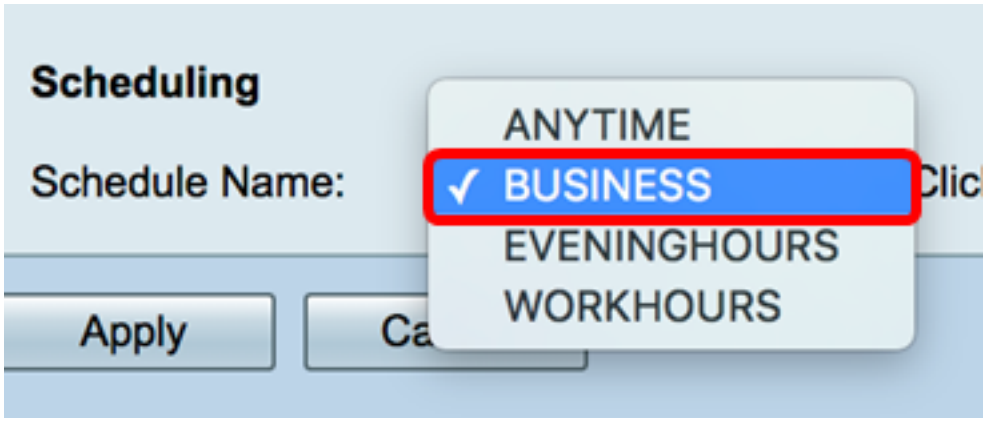
Step 15. (Optional) If IP Range was chosen in Step 13, enter the beginning and ending IP addresses in the respective IP address fields.

Note: In this example, 210.200.27.22 is used as the beginning IP address and 210.200.27.34 as the ending IP address. Skip to Step 17.

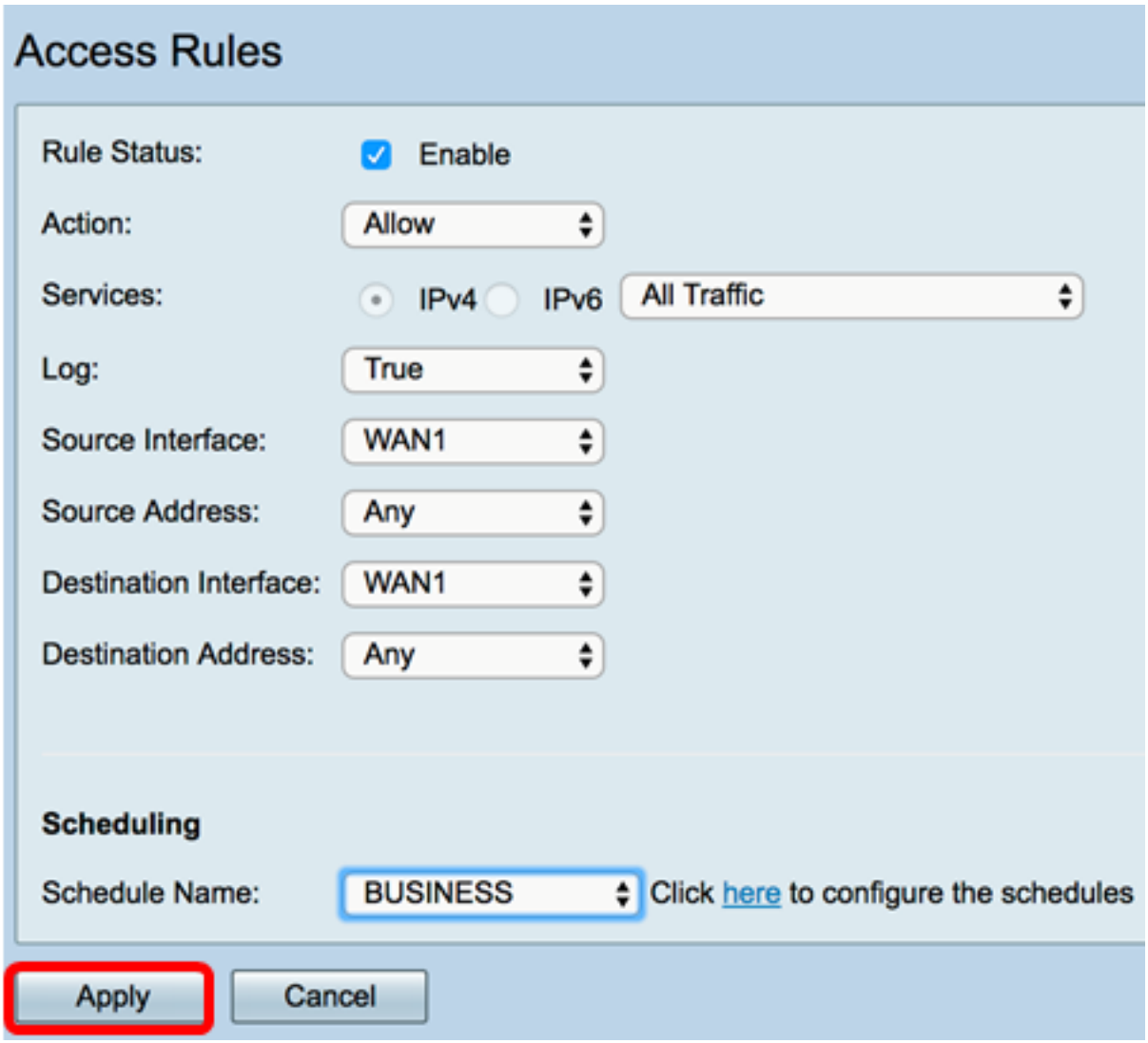
Step 16. (Optional) If Subnet was chosen in Step 13, enter the network address and its respective subnet mask to apply the policy.

Note: In this example, 210.200.27.1 is used as the subnet address and 24 as the subnet mask.

Step 17. From the Schedule Name drop-down list, choose a schedule to apply this policy. To learn how to configure a schedule, click here.



Step 18. Click **Apply**.

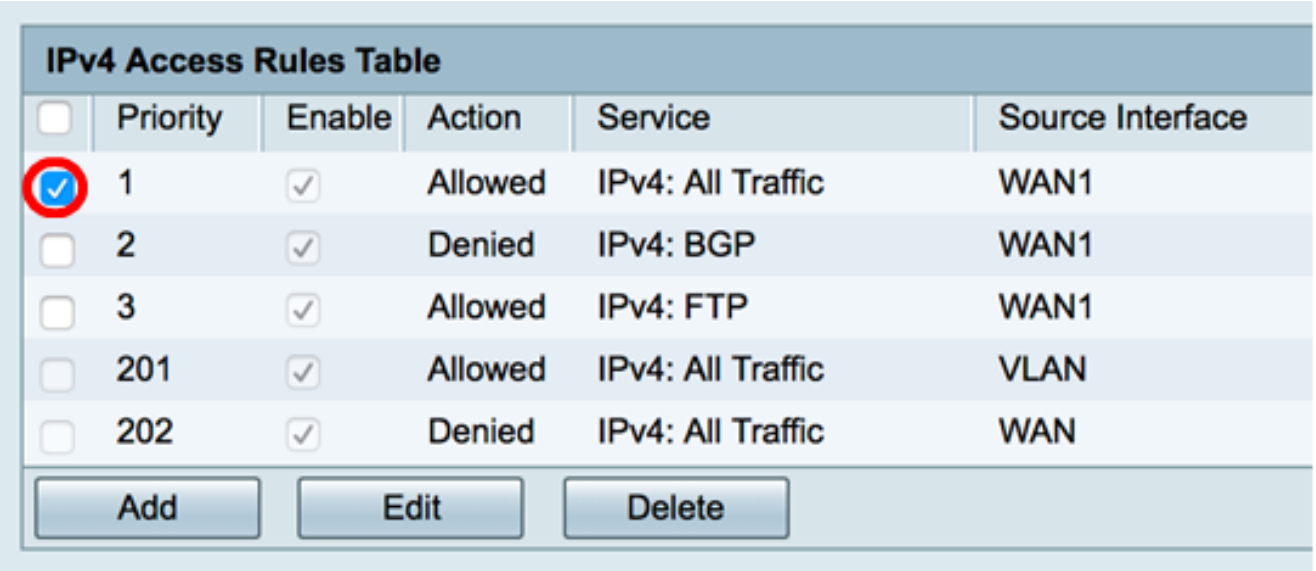


You should have now successfully created an access rule on an RV Series Router.

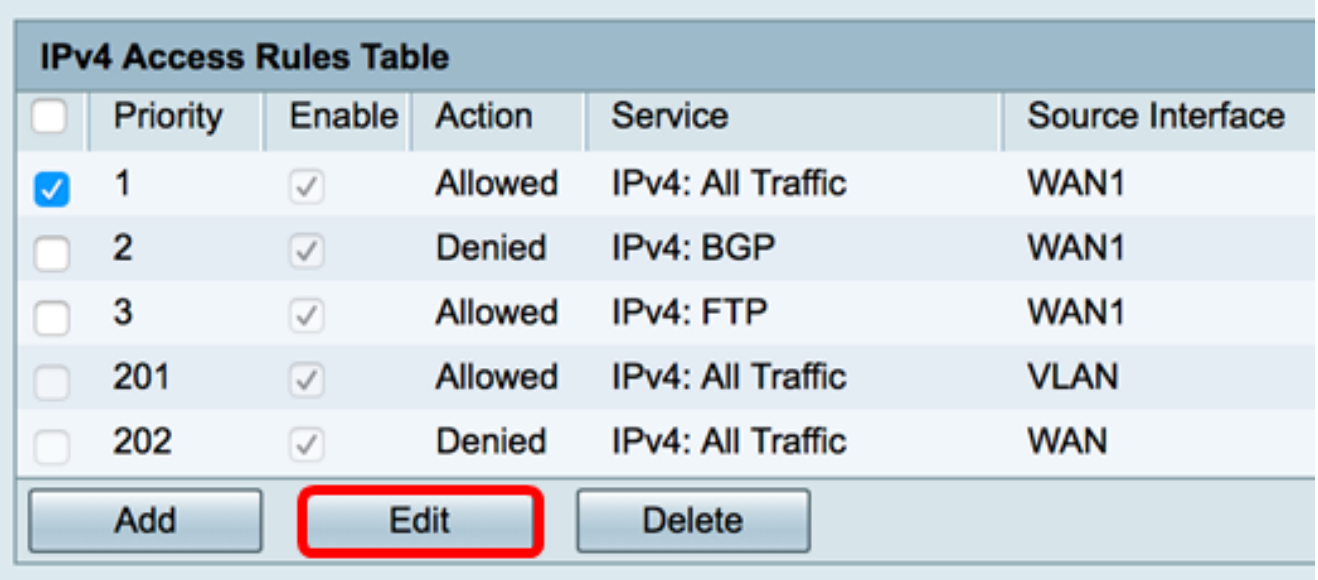
Edit an Access Rule

Step 1. In the IPv4 or IPv6 Access Rules Table, check the check box beside the access rule you want to configure.

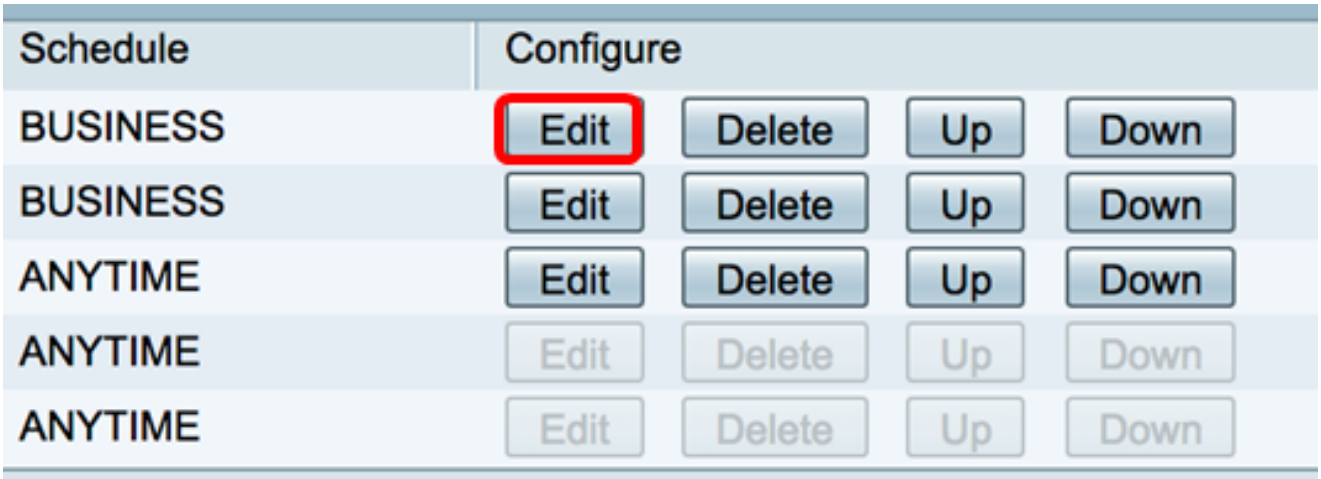
Note: In this example, in the IPv4 Access Rules Table, Priority 1 is chosen.



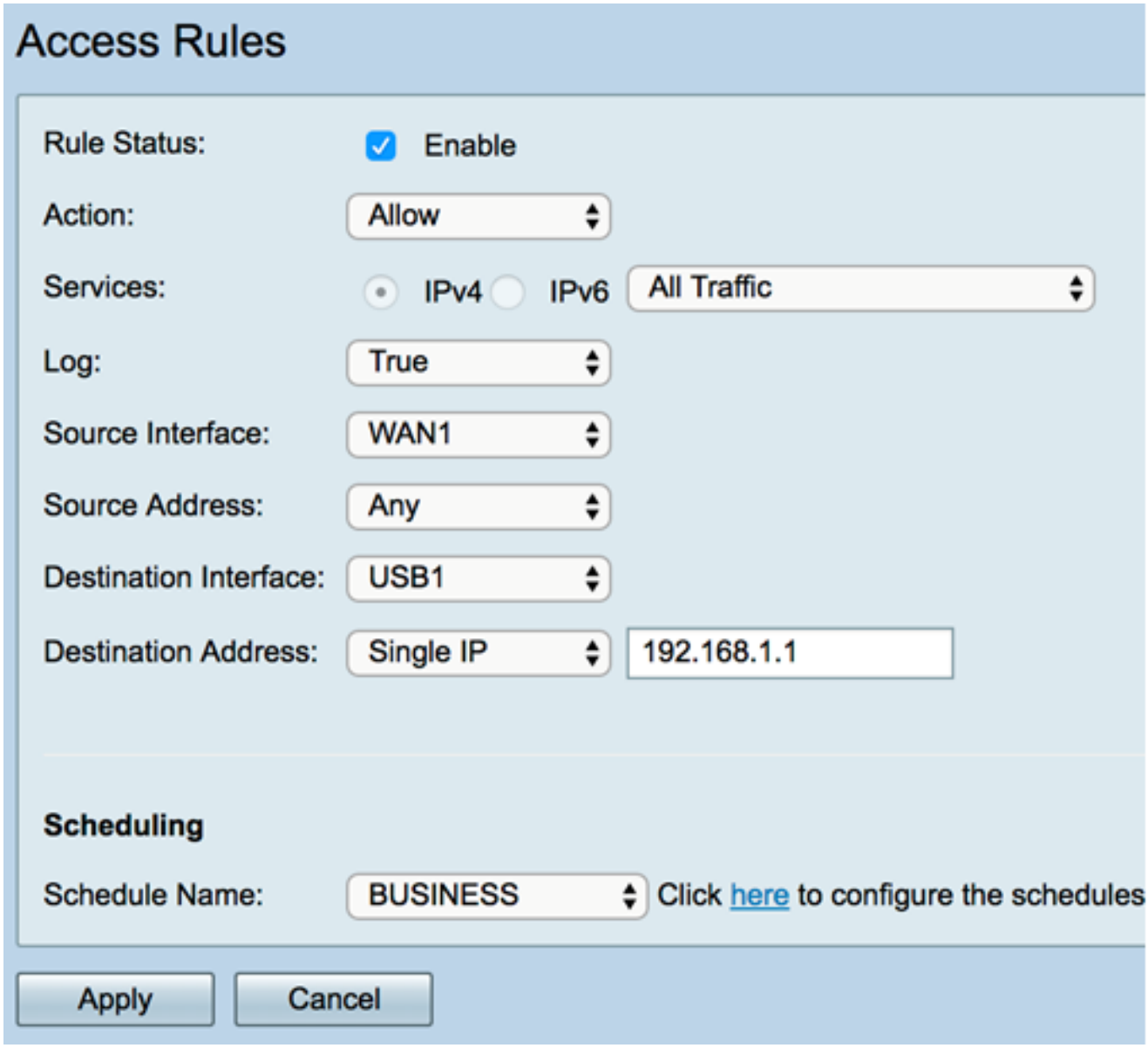
Step 2. Click **Edit**.



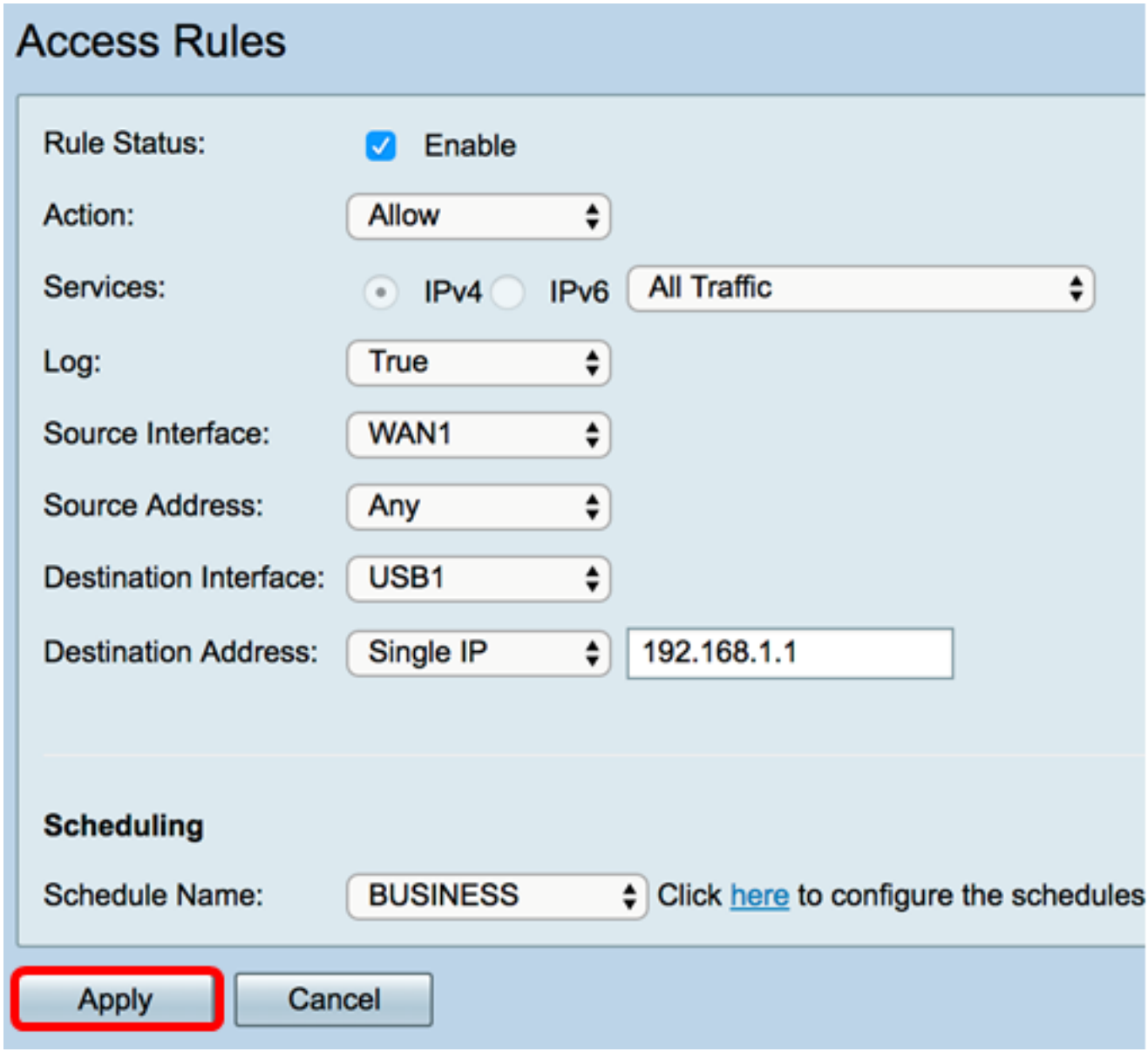
Step 3. (Optional) In the Configure column, click on the **Edit** button in the row of the desired access rule.



Step 4. Update the necessary parameters.



Step 5. Click **Apply**.



Step 6. (Optional) To change the priority of an access rule in the Configure column, click on the **Up** or **Down** button of the access rule you want to move.

Note: When an access rule is moved up or down, it moves one step above or below its original placement. In this example, Priority 1 will be moved down.

Note: In this example, Priority 1 is now Priority 2.

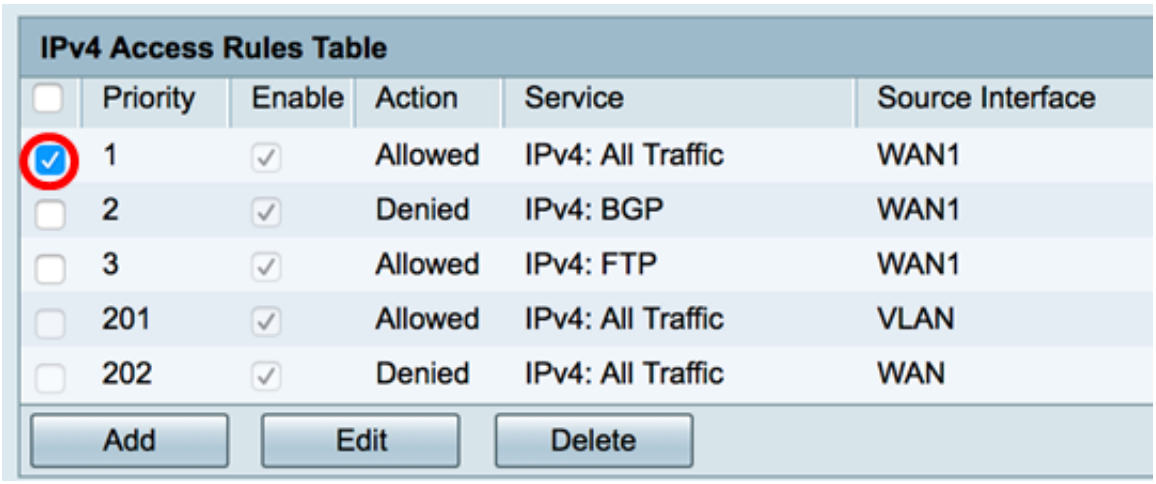
Step 7. Click **Apply**.

You should now have successfully edited an access rule on an RV34x Series Router.

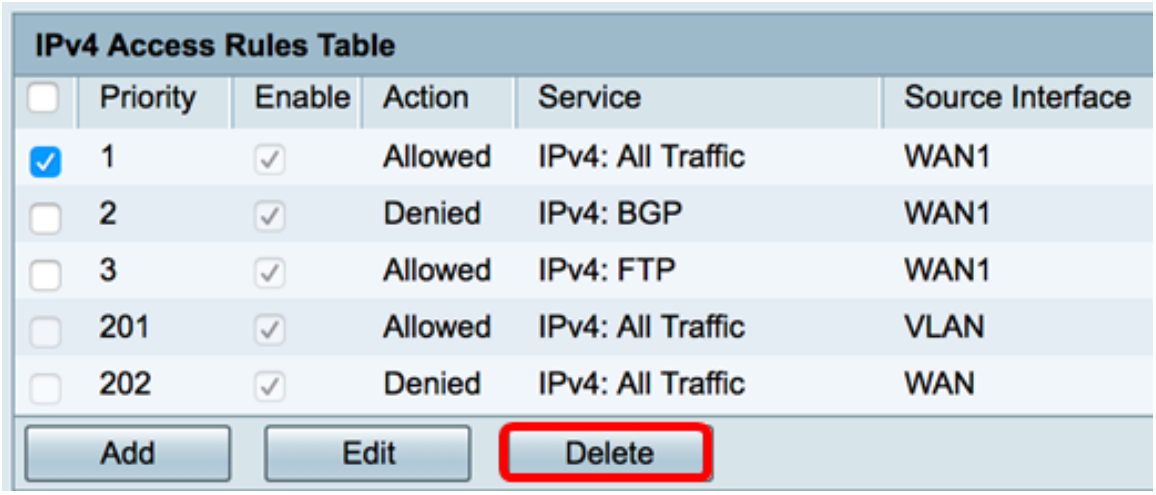
Delete an Access Rule

Step 1. In the IPv4 or IPv6 Access Rules Table, check the check box beside the access rule you want to delete.

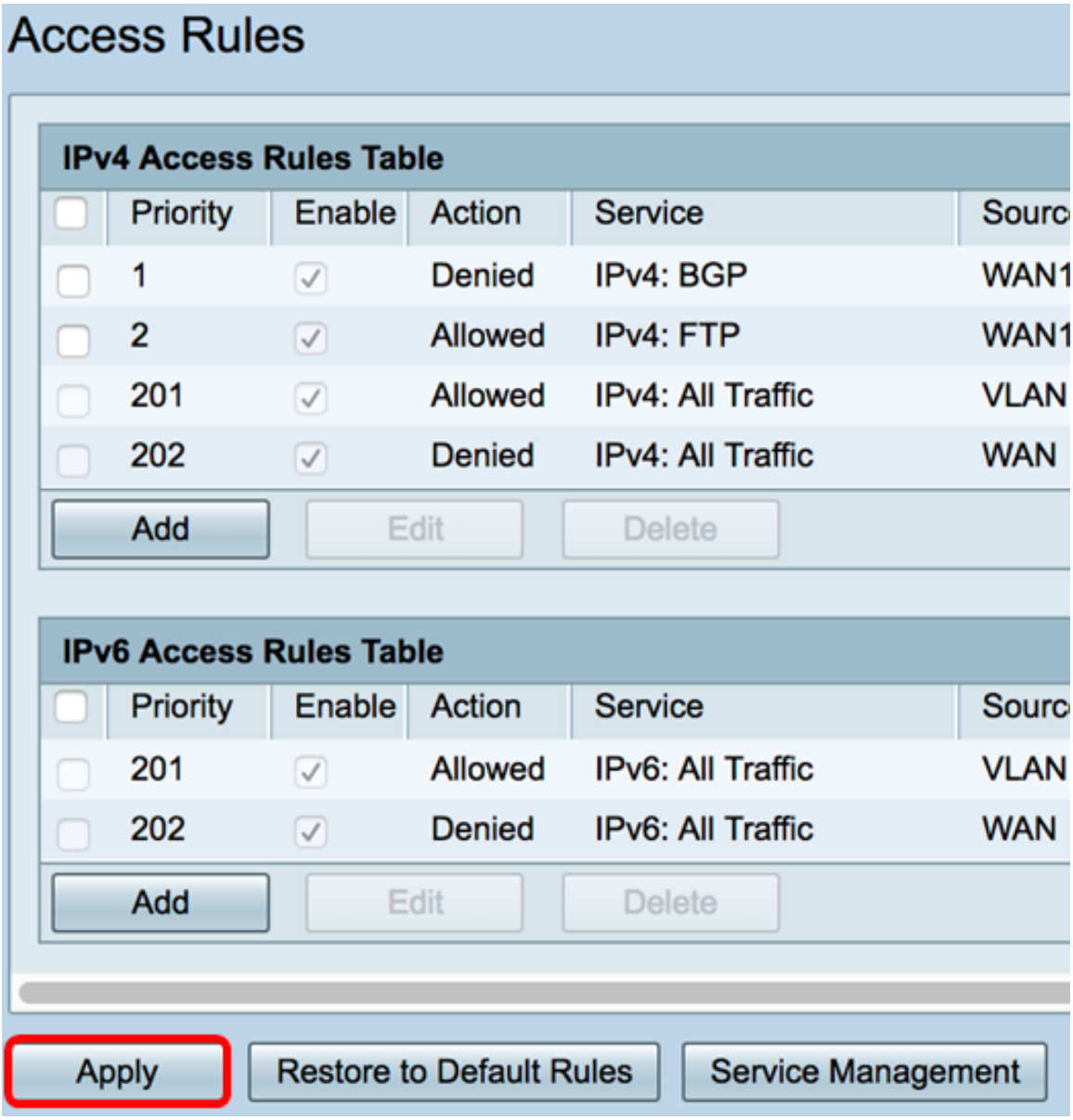
Note: In this example, in the IPv4 Access Rules Table, Priority 1 is chosen.



Step 2. Click **Delete** located below the table or click the delete button in the Configure column.



Step 3. Click **Apply**.



You should now have successfully deleted an access rule on the RV34x Series Router.

View a video related to this article...

Click here to view other Tech Talks from Cisco