Access Control Configuration on the RV315W VPN Router

Objective

Access Control configuration allows for the ability to restrict access to a specific IP address. There are a variety of options to customize the restrictions. Time of day, days of the week, IP addresses, physical port, and type of protocol are examples of some of the customization features for the access control policy.

This article helps explain how to utilize and configure Access Controls on the RV315W VPN Router.

Applicable Device

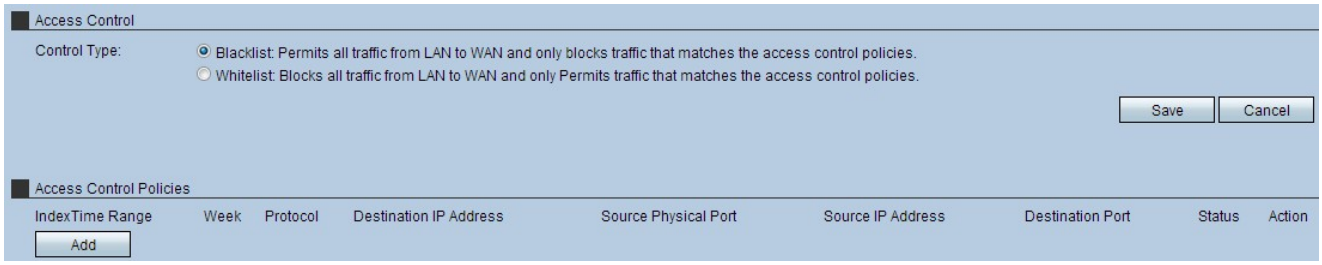
- RV315W

Software Version

- 1.01.03

Configuration Management

Step 1. Log into the web configuration utility and choose **Security > Access Control**. The *Access Control* page opens:



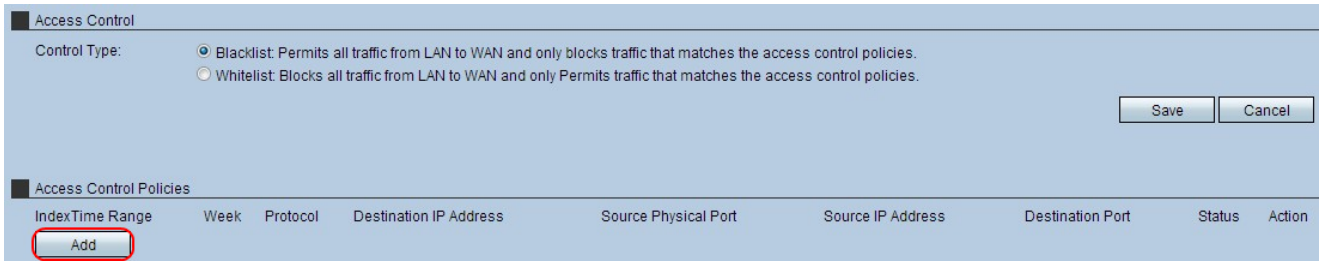
Step 2. Click either the Block list or Allow list radio button in the Control Type field.

- Block list — This option allows all traffic from the LAN to the WAN, except the traffic that is blocked through the access control settings.

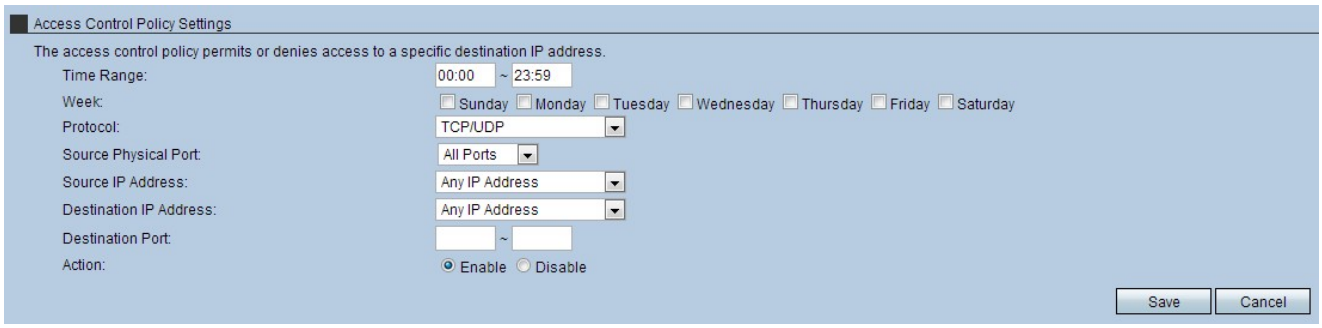
- Allow list — This option blocks all traffic from the LAN to the WAN, except the traffic that is allowed through the access control settings.

[See glossary for additional information.]

Step 3. Click **Save** to apply settings.



Step 4. Click **Add** to add a new access control policy. The *Access Control Policy Settings* page opens:



Step 5. Enter a range in the Time Range field. This option is the time that the access control policy is effective.

Step 6. Select days of the week to allow or restrict access. This option is the days of the week that the access control policy is effective.

Step 7. From the Protocol drop-down list, choose the protocol for which the access control applies to.

- TCP — This protocol is used to transmit data from an application to the network. TCP is typically used for applications where information transfer must be complete and packets are not dropped.

- UDP — This protocol is for client/server network applications based on the Internet Protocol (IP). The main purpose of this protocol is for live applications. (VOIP, games etc.)

- TCP/UDP — Select this protocol to utilize both TCP and UDP. This is the default protocol.

- ICMP — This protocol sends errors messages and is responsible for error-handling in the network. Use this protocol to get a notification when the network has issues with the delivery of packets.

- HTTP — This protocol provides secure communication between a web server and browser. Use this protocol when there is a need to securely transfer packets between a server and browser.

- FTP — This protocol transmits the files between computers. Select this protocol when files are exchanged between multiple devices.

- SMTP — This protocol handles the transmission of e-mails. Select this protocol when exchanging e-mails.

- POP3 — This protocol combines with SMTP in regards to e-mail. POP3 downloads e-mails from an e-mail server to a personal computer. Select this protocol when downloading e-mails.

Step 8. From the Source Physical Port drop-down list, choose the port to which the access control applies.

Step 9. From the Source IP Address drop-down list, choose the IP address(es) to which the access control applies.

- Any IP Address — Choose this option to allow or deny all IP addresses. Select the enable or disable radio button for this option.
- Single IP Address — Choose this option to allow or deny individual IP addresses. Enter the applicable IP address in the Source IP Address field.
- IP Address Range — Choose this option to allow or deny IP addresses based on a selected range. Enter the applicable IP address range in the first and second Source IP Address field.

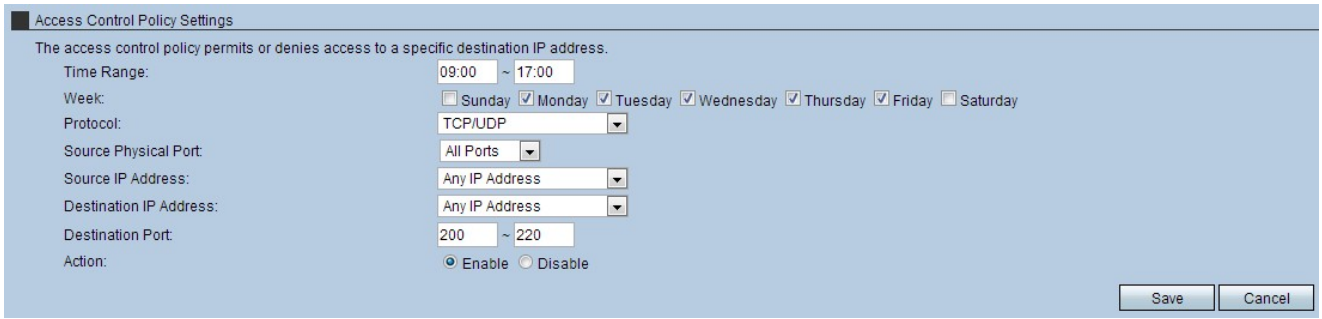
Step 10. From the Destination IP Address drop-down list, choose the IP address(es) to which the access control applies.

- Any IP Address — Choose this option to allow or deny all IP addresses. Click the enable or disable radio button for this option.
- Single IP Address — Choose this option to allow or deny an individual IP address. Enter the applicable IP address in the Destination IP Address field.
- IP Address Range — Choose this option to allow or deny IP addresses based on a selected range. Enter the applicable IP address range in the first and second Destination IP Address field.

Step 11. In the Destination Port fields, enter the port range of a protocol or application to which the access control applies.

Step 12. Click the **Enable** radio button to enable the access control policy.

Step 13. Click **Save** to apply settings.



Step 14. (Optional) In order to delete an Access Control policy, click the trash can icon under the Action header.

Step 15. (Optional) In order to edit an Access Control policy, click the envelope icon under the Action header.