Firewall Access Rule Configuration to Block Ping Packets from two Different Networks on RV016, RV042, RV042G, and RV082 VPN Routers

Objective

Two different networks can be needed on a router to provide Internet access to devices which are not in the same network as the router. This can be achieved through an access rule based on various criteria in order to allow or deny access to any network or IP address range. An access rule helps the router determine what traffic is allowed to pass through the firewall and also helps to add security to the router.

This article explains how to block ping packets from two different networks on RV016, RV042, RV042G, and RV082 VPN Routers through an access rule.

Applicable Devices

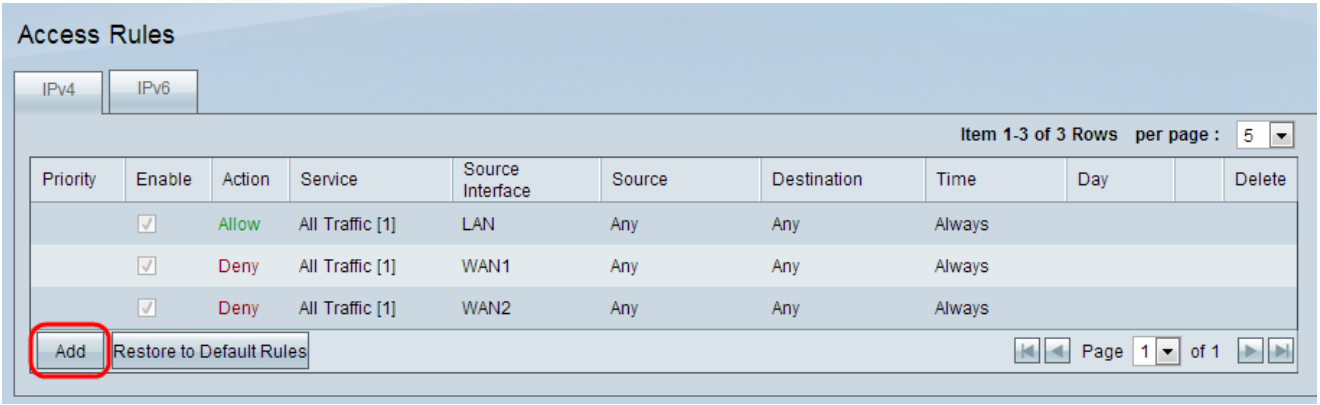
- RV016
- RV042
- RV042G
- RV082

Software Version

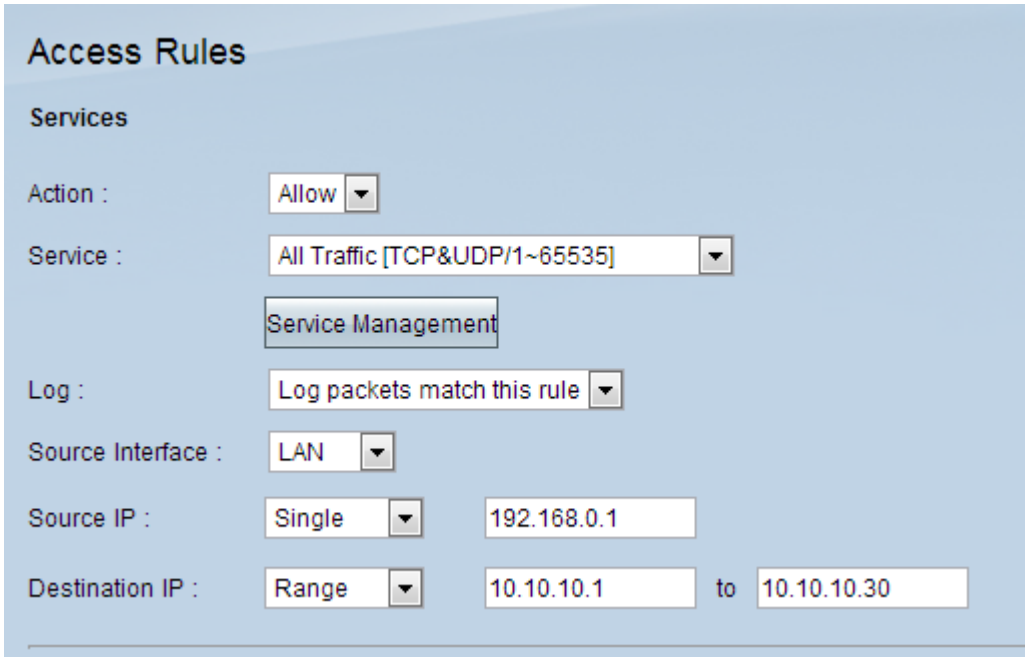
- v4.2.1.02

Access Rule Configuration

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



Step 2. Click **Add** to add an access rule. The *Access Rules Services* page opens:

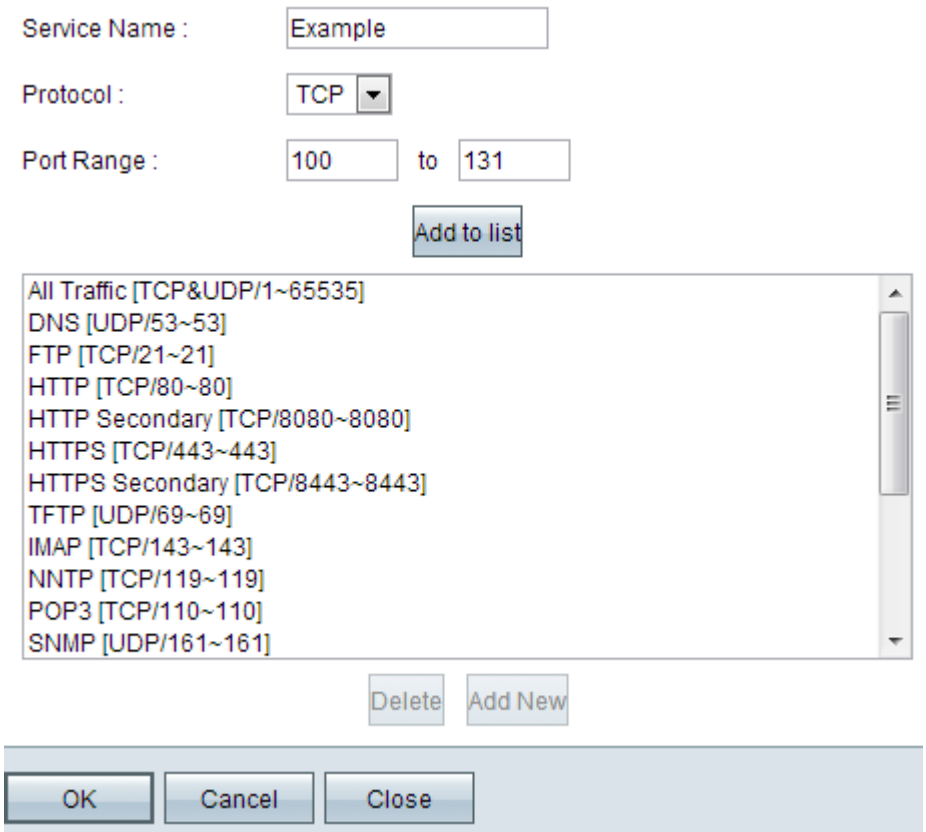


Step 3. Choose the appropriate action from the Action drop-down list that will allow the traffic to pass if **Allow** is chosen. Otherwise, choose **Deny** to deny the traffic.

Step 4. Choose the appropriate service from the Service drop-down list.

Note: If the desire service is available, skip to Step 10.

Step 5. If the appropriate service is not available, click **Service Management** and the *Service Management* window appears:



Step 6. Enter a desired service name in the Service Name field.

Step 7. Choose an appropriate protocol type from the Protocol drop-down list:

• TCP — Transmission Control Protocol is a protocol used by applications that require guaranteed delivery.

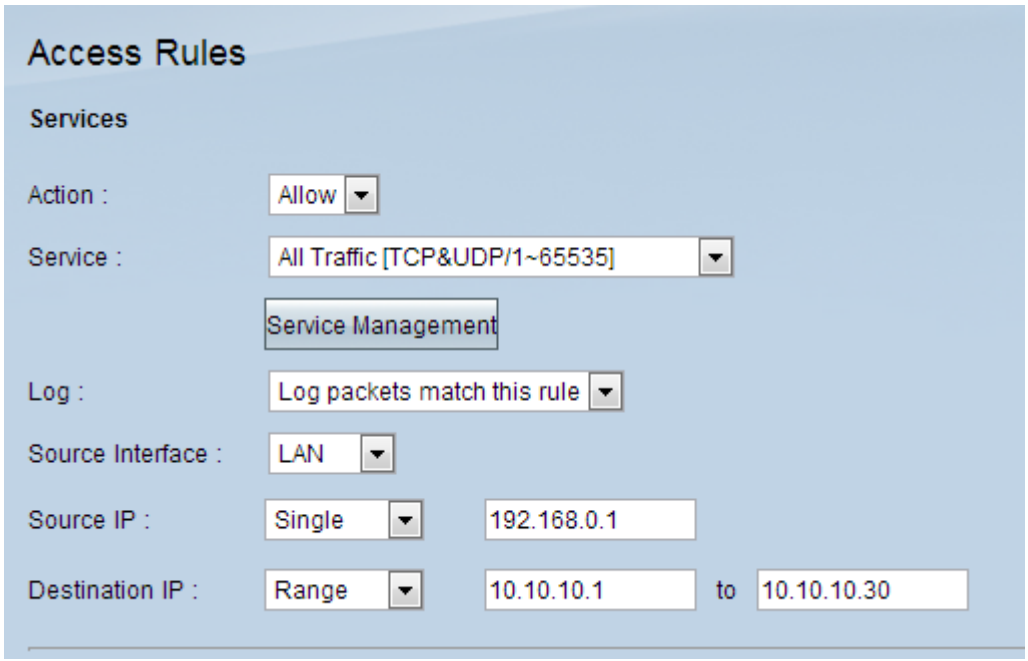
• UDP — User Datagram Protocol uses datagram sockets to establish host to host communications.

• IPv6 — Directs Internet traffic between hosts in packets that are routed across networks specified by routing addresses.

Step 8. Enter the range of ports that will apply to the service in the Port Range field.

Step 9. Click **Add to List** to add the Service to the Service drop-down list on the *Access Rules* page.

Step 10. Click **OK** to close the window and this takes the user back to the *Access Rules* page.



Step 11. Choose **Log packets match this rule** to log the incoming packets that match the access rule in the Log drop-down list.

Step 12. Choose an interface from the Source Interface drop-down list that is affected by this rule. Source interface is the interface from which the traffic is initiated.

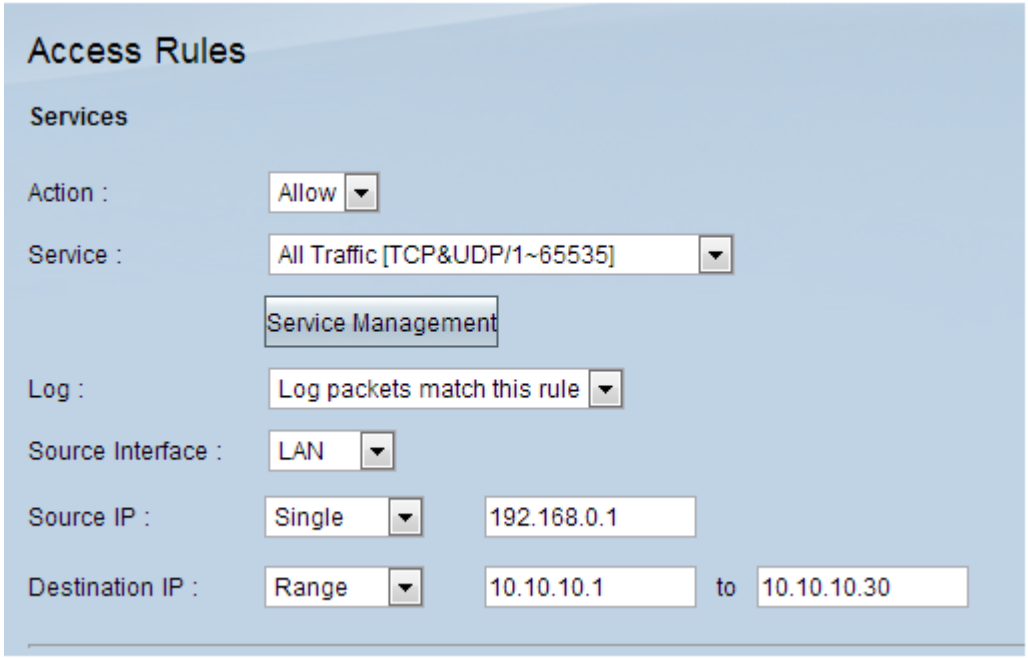
• LAN — The local area network port connects computers in close proximity on a network such as an office building or school.

• WAN1 — The wide area network port connects computers in a large area on a network. This could be any network that connects a region or even a country. It is used by businesses and the government to connect to other locations.

• WAN2 — Same as port WAN1 except that it is a second network.

• DMZ — Allows outside traffic to access a computer on the network without exposing the LAN.

• ANY — Allows any interface to be used.



Step 13. Choose an option to specify the source IP address that the network will use for traffic through the interface from the Source IP drop-down list:

- Any — Any IP address will be used to forward traffic. There will not be any fields to the right of the drop-down list available.
- Single — A single IP address will be used to forward traffic. Enter the desired IP address in the field to the right of the drop-down list.
- Range — A range IP address will be used to forward traffic. Enter the desired IP addresses range in the fields to the right of the drop-down list.

Step 14. Choose an option to specify the destination IP address that the network will use for traffic through the interface from the Destination IP drop-down list:

- Any — Any IP address will be used to forward traffic. There will not be any fields to the right of the drop-down list available.
- Single — A single IP address will be used to forward traffic. Enter the desired IP address in the field to the right of the drop-down list.
- Range — A range IP address will be used to forward traffic. Enter the desired IP addresses range in the fields to the right of the drop-down list.

Step 15. Click **Save** to apply settings.