# Configuration of an IPv6 Access Rule on RV016, RV042, RV042G and RV082 VPN Routers

## Objective

An access rule helps the router determine what traffic is allowed to pass through the firewall. This helps add security to the router.

This article explains how to add an IPv6 access rule on the RV016, RV042, RV042G, and RV082 VPN Routers.

## Applicable Devices

- RV016
- RV042
- RV042G
- RV082

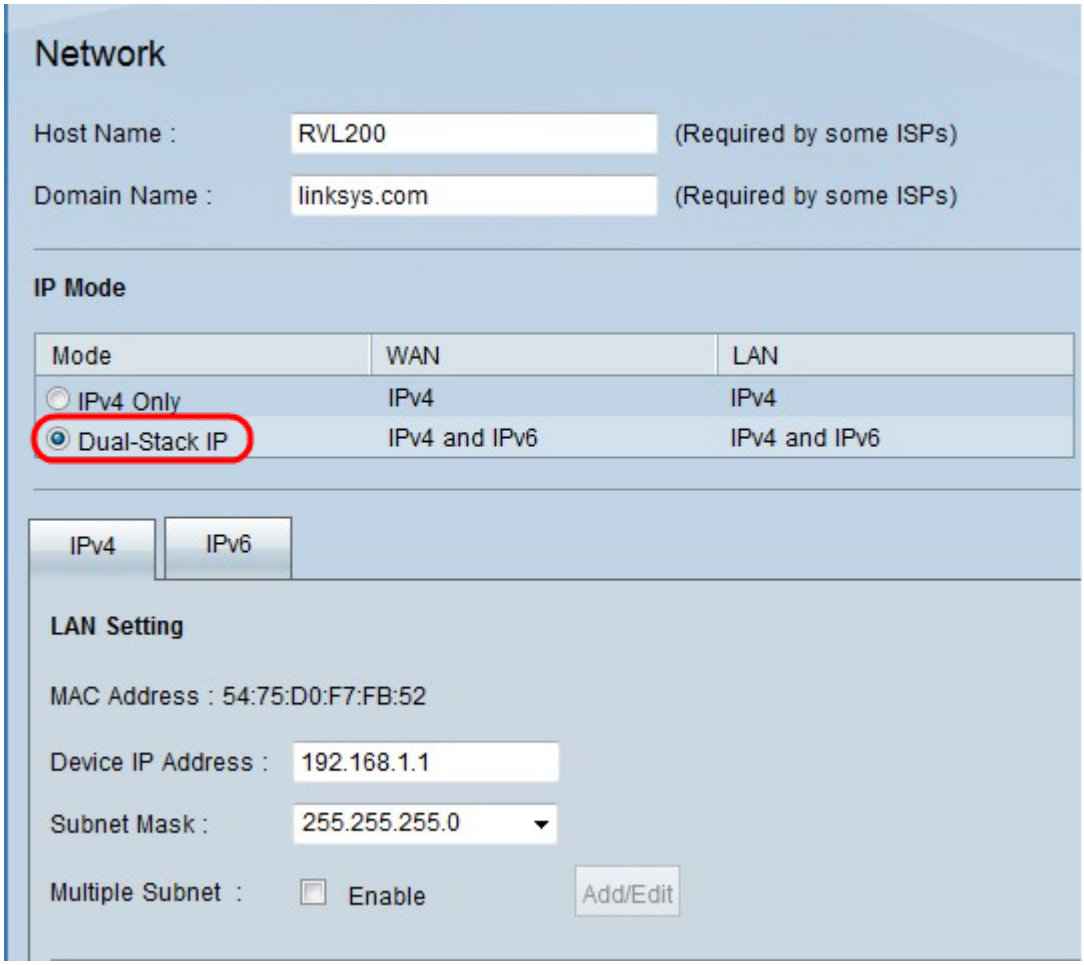
## Software Version

- v4.2.1.02

## Configuration of an IPv6 Access Rule

### Enable IPv6 Mode

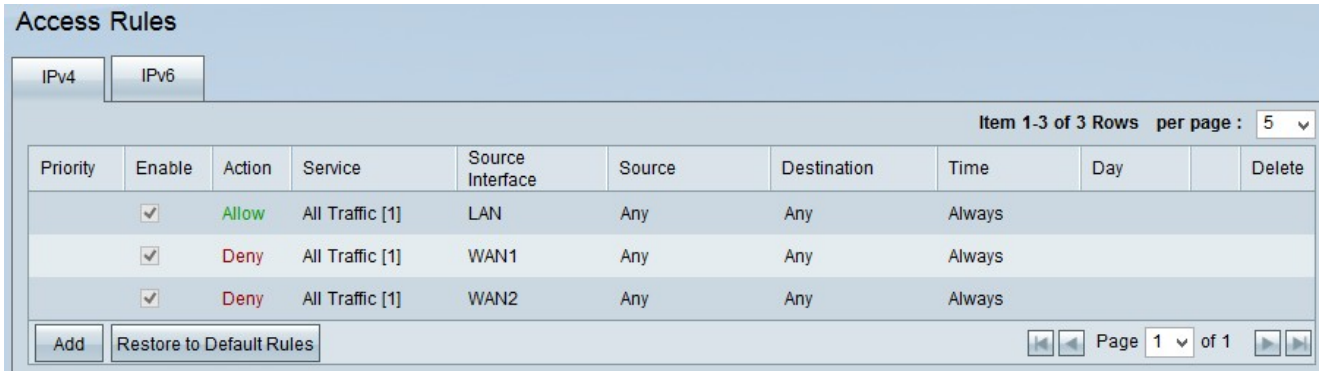
Step 1. Log in to the web configuration utility and choose **Setup > Network**. The *Network* page opens:



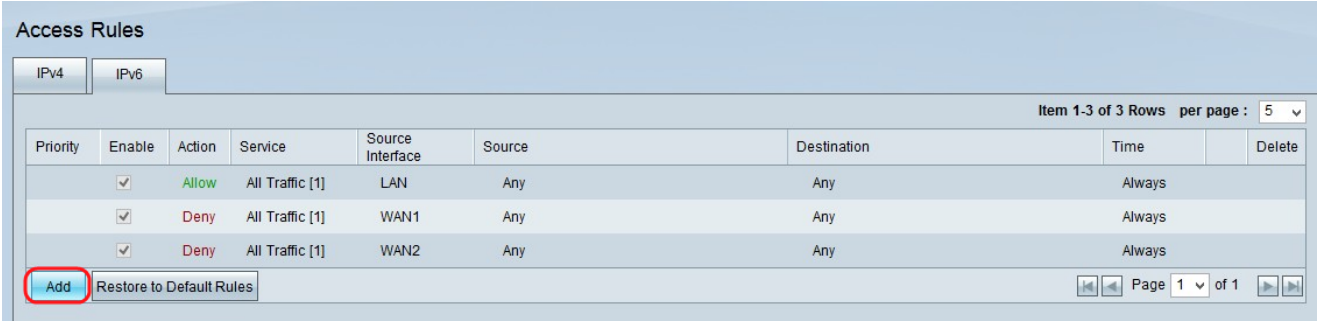

Step 2. Click the **Dual-Stack IP** radio button. This allows IPv4 and IPv6 to run at the same time. If IPv6 communication is possible then that is the preferred communication.

## IPv6 Access Rule Configuration

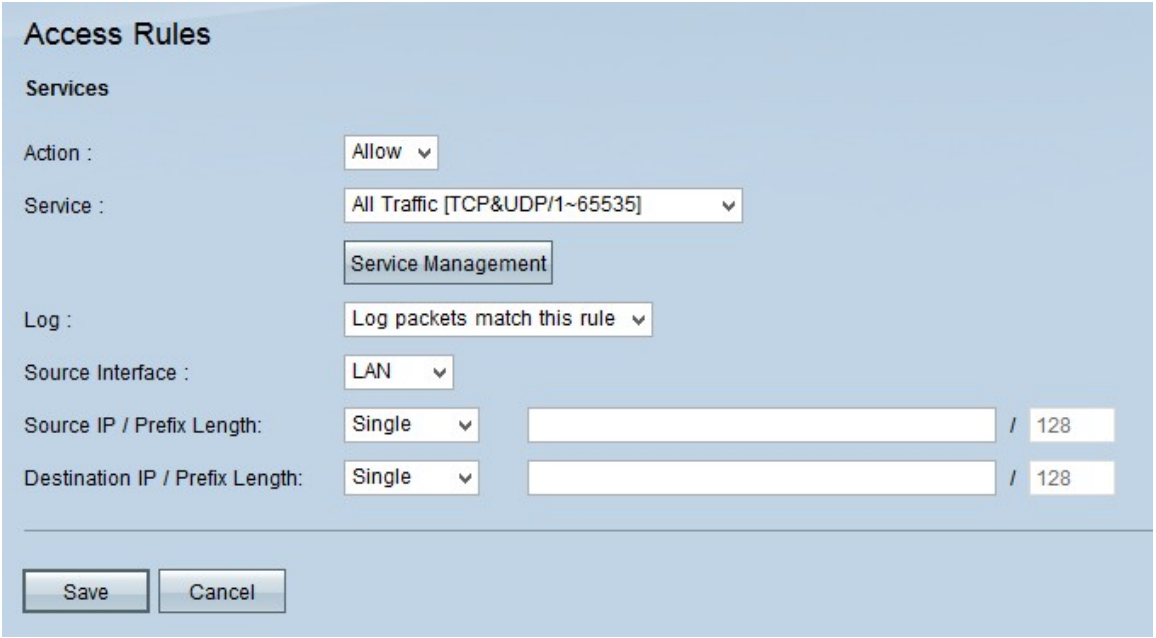
Step 1. Log in into the web configuration utility and choose **Firewall > Access Rules**. The *Access Rules* page opens:




Step 2. Click the IPv6 tab. This opens *IPv6 Access Rules* page.



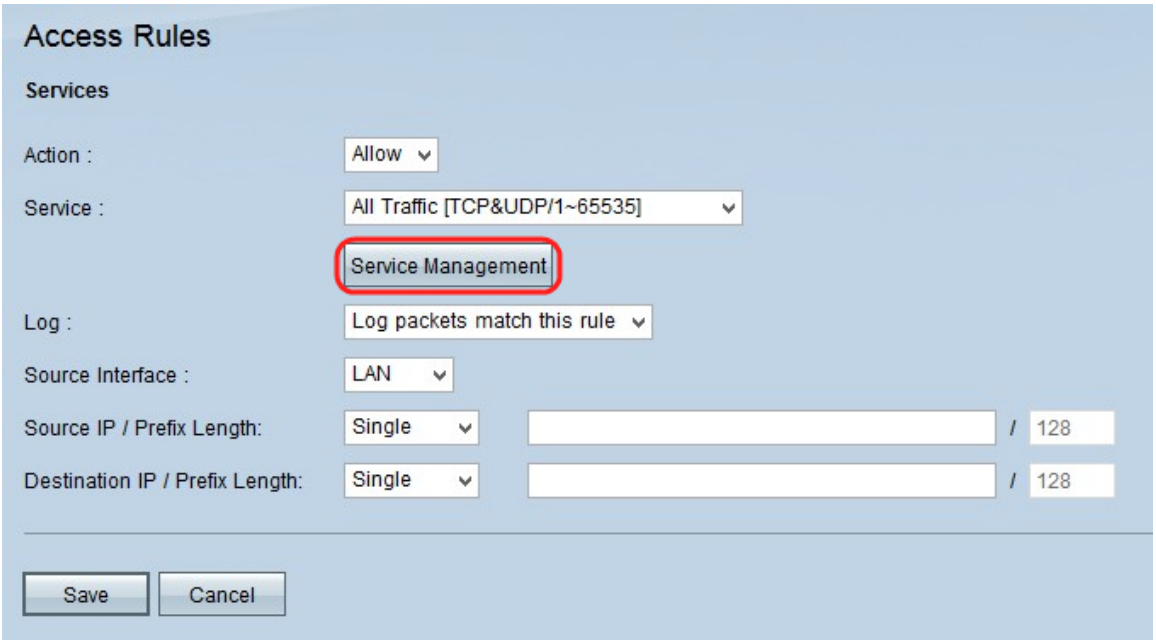

Step 3. Click **Add** to add the access rules. The *Access Rules* page is displayed to configure the access rules for IPv6.



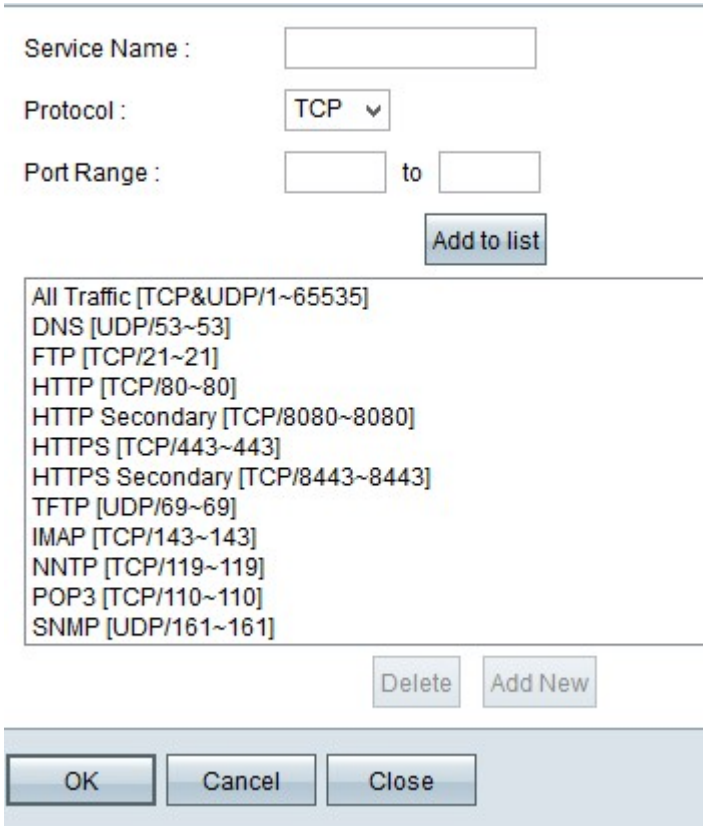

Step 4. Choose **Allow** from the Action drop-down list if the traffic is to be allowed. Choose **Deny** to deny the traffic.

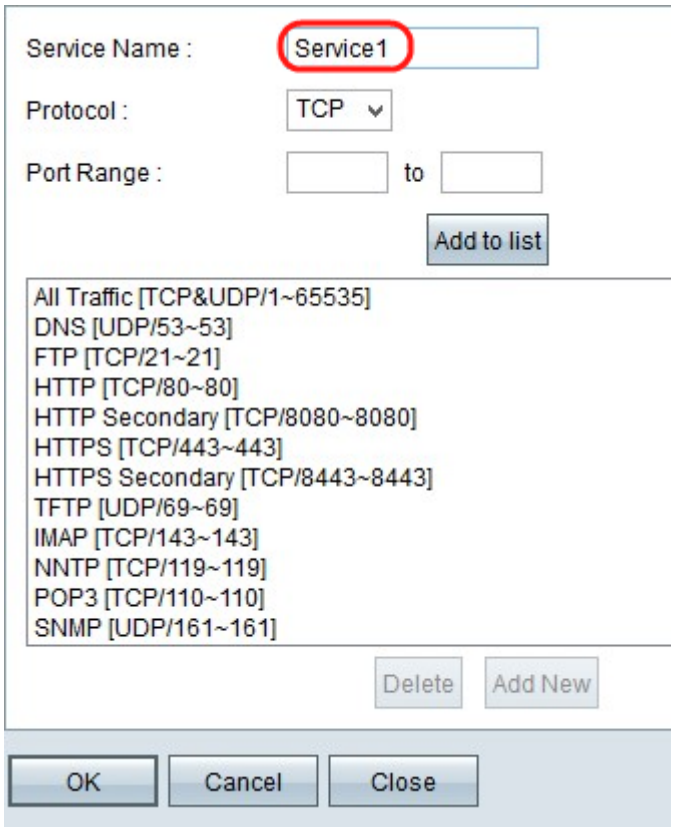
Step 5. Choose the appropriate service in the Service drop-down list.

**Timesaver:** If the desired service is available, skip to Step 12.

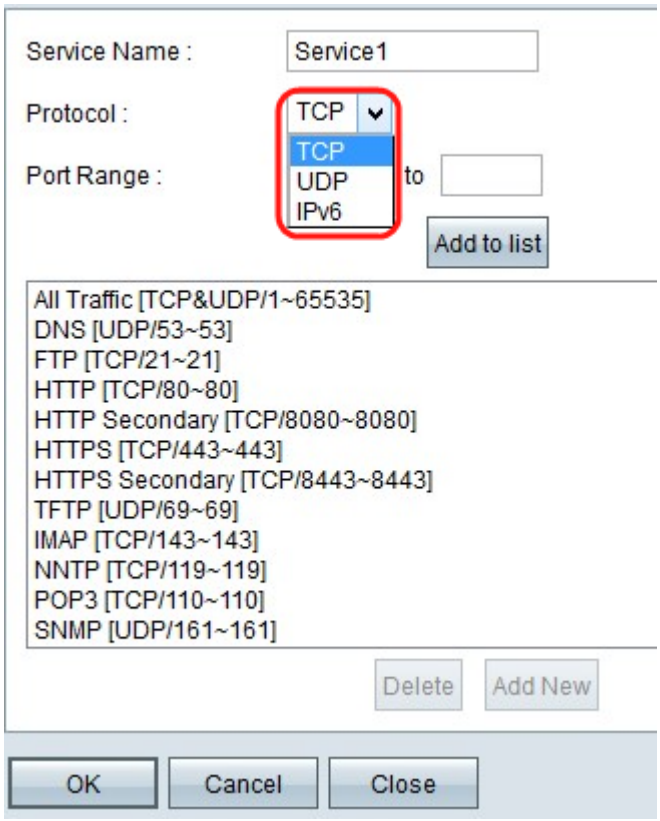


Step 6. If the appropriate service is not available, click **Service Management.** The *Service Management* window appears.



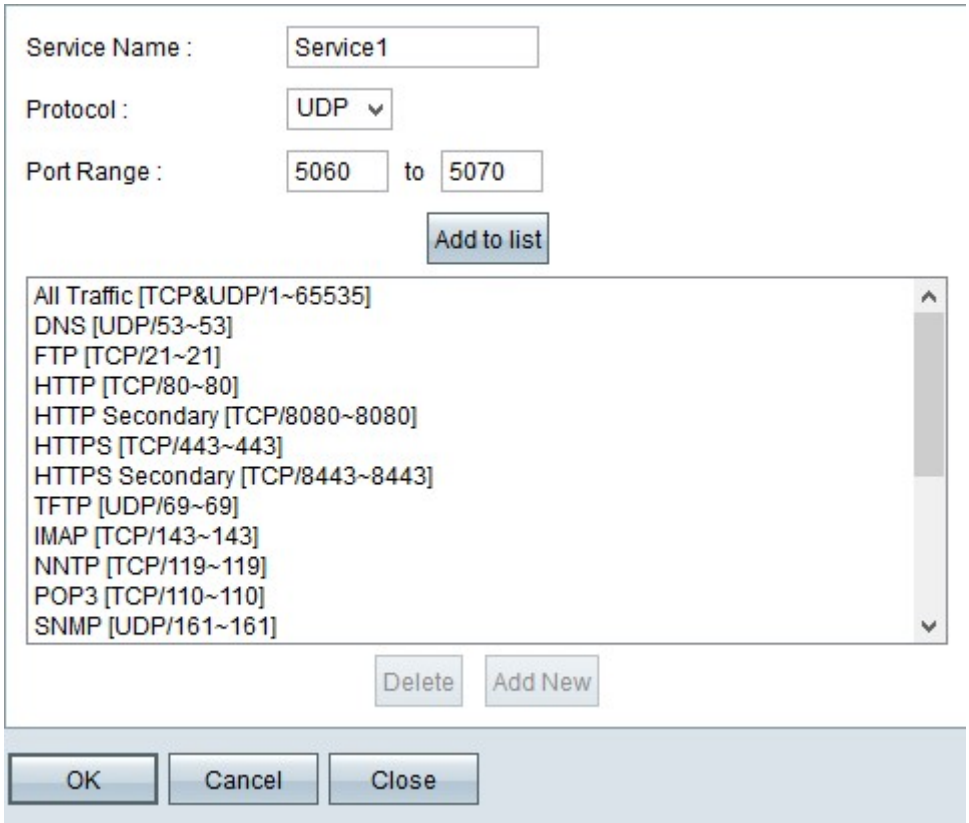




Step 7. Enter a name for the new service in the Service Name field.



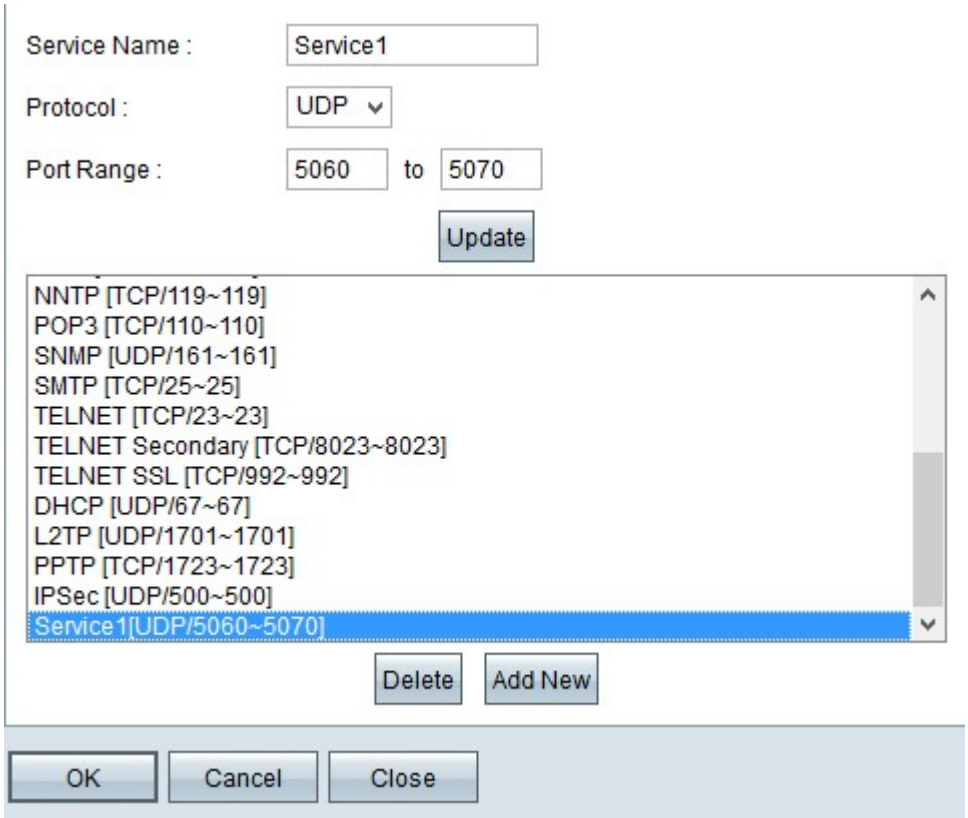

Step 8. Choose the appropriate protocol type from the Protocol drop-down list.

- TCP (Transmission Control Protocol) — A transport layer protocol used by applications that requires guaranteed delivery.
- UDP (User Datagram Protocol) — Uses datagram sockets to establish host to host communications. UDP delivery is not guaranteed.
- IPv6 (Internet Protocol version 6) — Directs Internet traffic between hosts in packets that are routed across networks specified by routing addresses.




Step 9. Enter the port range in the Port Range field. This range depends on the protocol chosen in the above step.

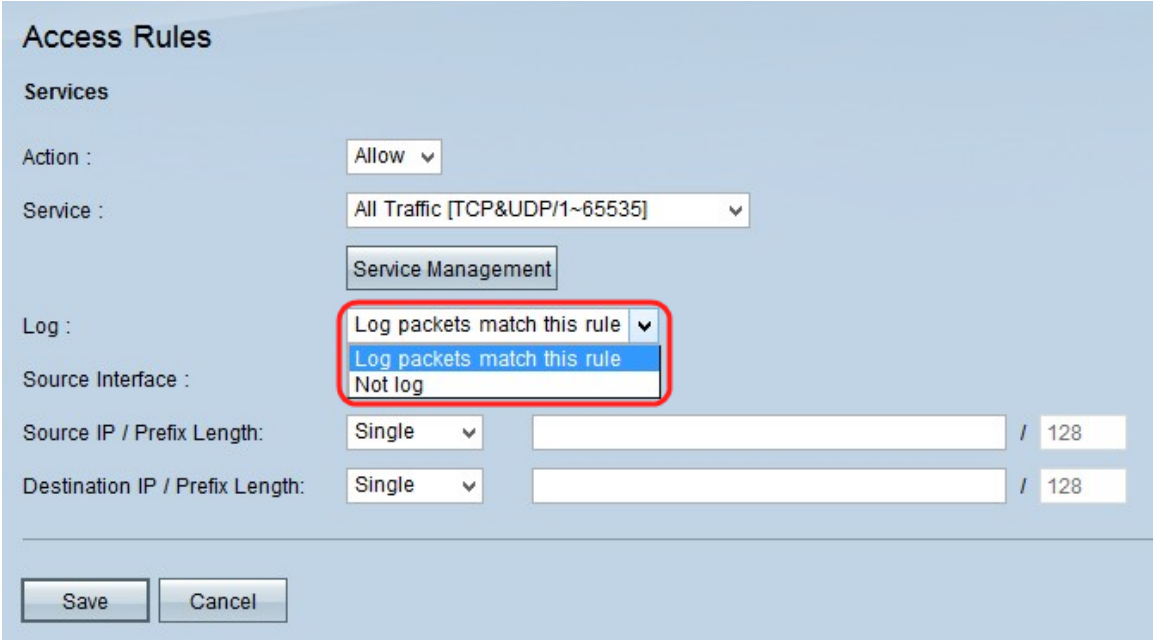
Step 10. Click **Add to List**. This adds the Service to the Service drop-down list.



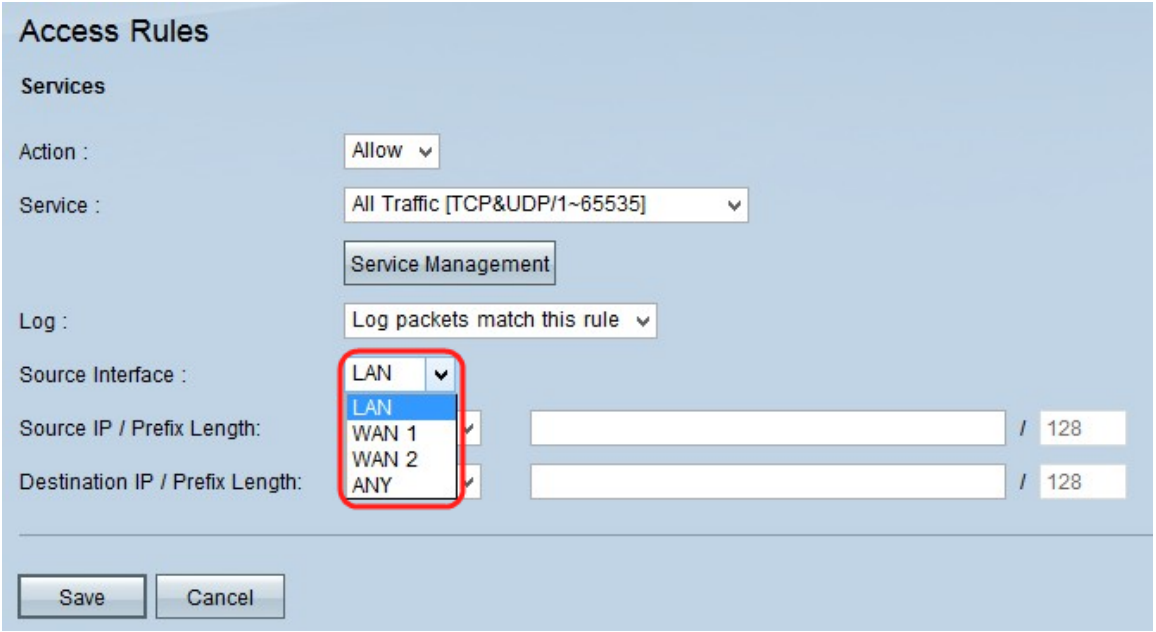

**Note:** If you want to delete service from the service list chose the service from the service list and click **Delete**. If you want update the service entry then choose the service to be updated from the service list and then click **Update**. To add another new service to the list click **Add New**.

Step 11. Click **OK**. This closes the window and takes the user back to the *Access Rule* page.

**Note:** If you click **Add New**, follow Steps 7 through 11.

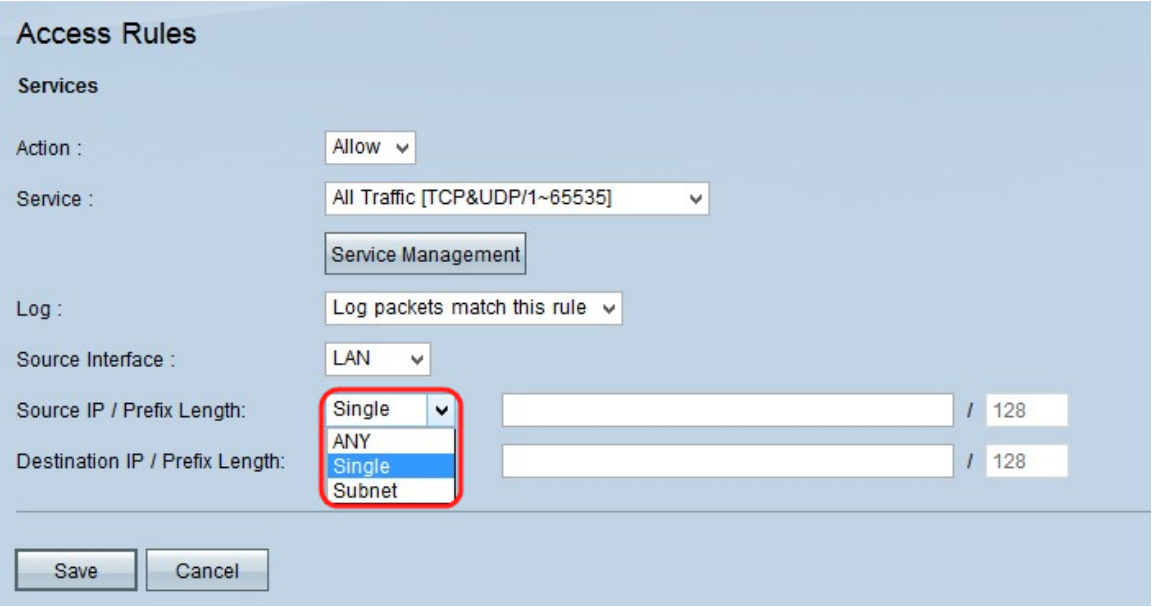



Step 12. If you want to log the packets that match the access rule choose **Log packets match this rule** in the Log drop-down list. Otherwise choose **Not Log**.



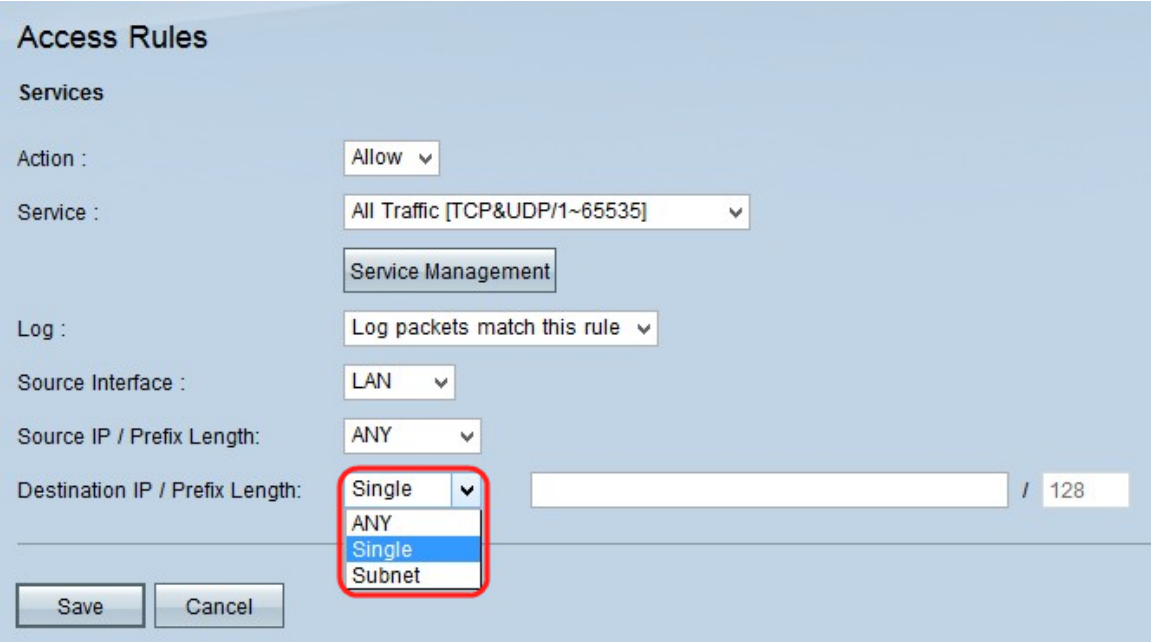

Step 13. Choose the interface that is affected by this rule from the Source Interface drop-down list. The source interface is the interface from which the traffic is initiated.

- LAN — The local area network of the router.
- WAN1 — The wide area network or the network from which router gets internet from the ISP or next hop router.
- WAN2 — The same as WAN1 except that it is a secondary network.
- ANY — Allows any interface to be used.




Step 14. In the Source IP drop-down list, choose an option to specify the source IP address that the access rule is applied.

- Any — Access rule will be applied on all the traffic from the source interface. There wont be any fields to the right of the drop-down list available.
- Single — Access rule will be applied on a single IP address from the source interface. Enter the desired IP address in the address field.
- Subnet — Access rule will be applied on a subnet network from the source interface. Enter the IP address and the prefix length.




Step 15. In the Destination IP drop-down list; choose an option to specify the destination IP address that the access rule is applied.

- Any — Access rule will be applied on all the traffic to the destination interface. There wont be any fields to the right of the drop-down list available.
- Single — Access rule will be applied on a single IP address to the destination interface. Enter the desired IP address in the address field.

- Subnet — Access rule will be applied on a subnet network to the destination interface. Enter the IP address and the prefix length.

Step 16. Click **Save** to save all changes made on the IPv6 access rule.