NetCommWireless

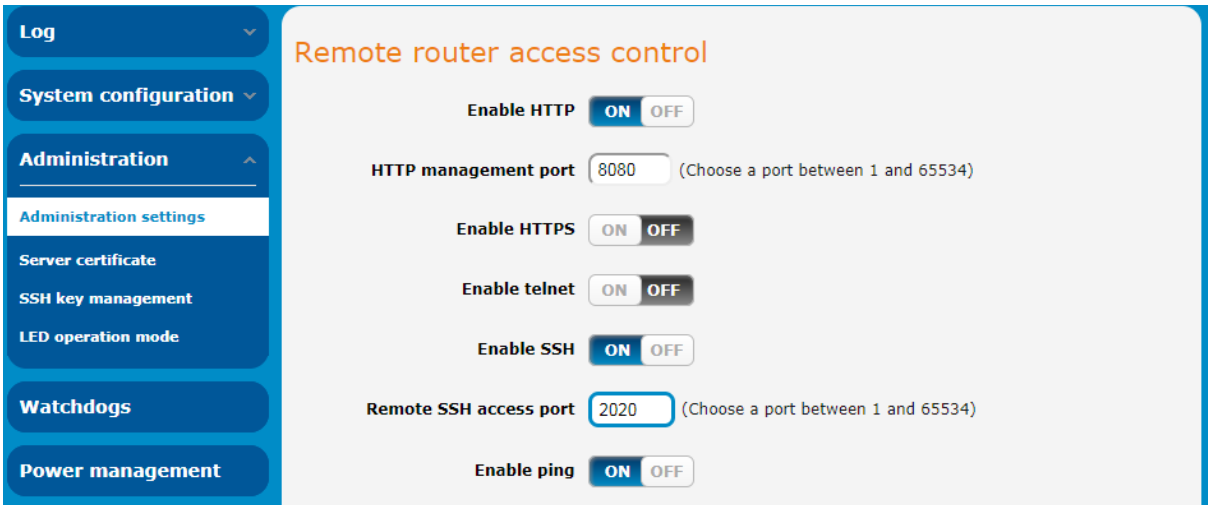
Securing Remote Administration

NetComm Wireless M2M Routers

Securing Remote administration on M2M Router

If you are using Public IP address on your M2M device, we highly recommend taking security measures to prevent your device from unauthorized access. Some security measures are listed below.

- Enable only the service that you intend to use and preferably open that through a non-default port. As an example, if you are planning to use HTTP and SSH remotely, enable them on port 8080 and 2020 instead of the default ports. To configure that, navigate to **System > Administration > Administration settings** and configure it as follows.



Remote router access control

Enable HTTP: ON

HTTP management port: 8080 (Choose a port between 1 and 65534)

Enable HTTPS: OFF

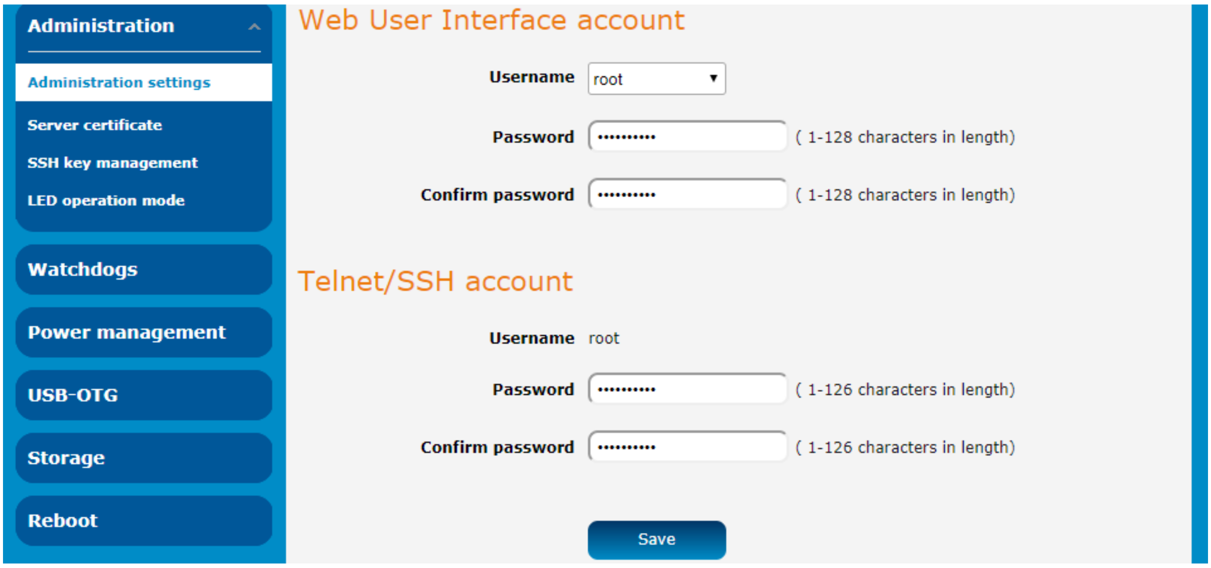
Enable telnet: OFF

Enable SSH: ON

Remote SSH access port: 2020 (Choose a port between 1 and 65534)

Enable ping: ON

- Change the default password for all users to something different which is easy for you to remember but tough for others to guess. A combination of alphanumeric characters, upper-lower case and special characters are suggested but not enforced. Those passwords can be changed from the same page. Change the passwords for both **root** and **admin** under “Web User Interface account” to secure web access and for **root** under “Telnet/SSH account” to secure CLI access.



Web User Interface account

Username: root

Password: •••••••••• (1-128 characters in length)

Confirm password: •••••••••• (1-128 characters in length)

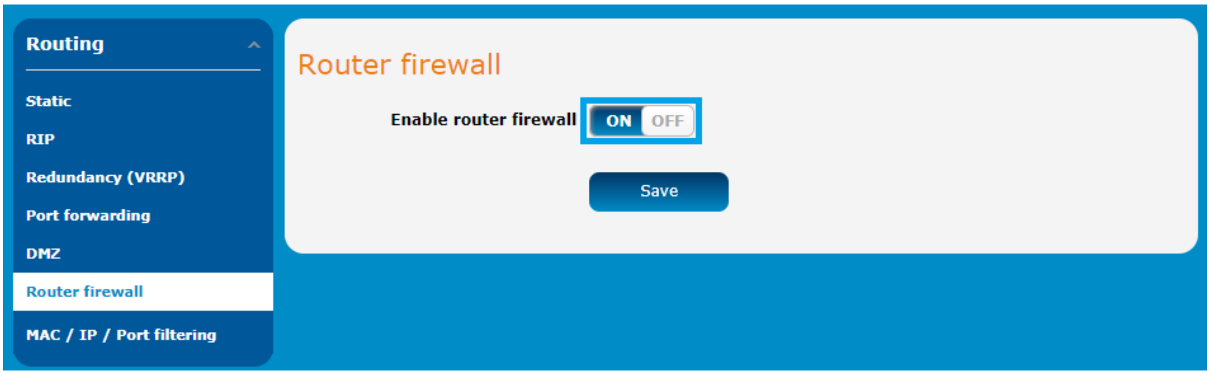
Telnet/SSH account

Username: root

Password: •••••••••• (1-126 characters in length)

Confirm password: •••••••••• (1-126 characters in length)

- Make sure that the “Router firewall” is turned on. To confirm that, navigate to **Networking > Routing > Router firewall**.



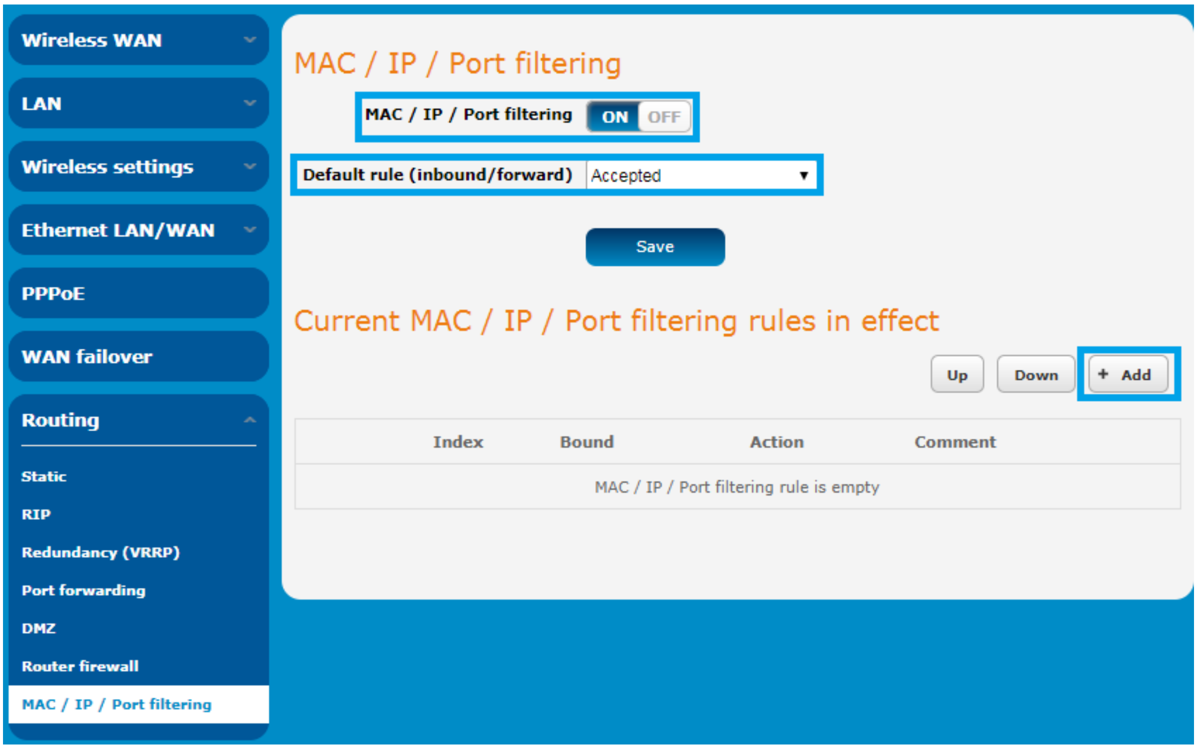
Router firewall

Enable router firewall: ON | OFF

- Enable access from the WAN for a specific IP address only. This can be configured from “Networking > Routing > MAC / IP / Port filtering” but requires caution. Follow the steps below to configure access from a specific IP address.

  a Navigate to **Networking > Routing > MAC / IP / Port filtering** and click on the **ON/OFF** button so that it is in the **ON** position.

  b By default, “Default rule (inbound/forward) is set to “Accepted”. Keep it as it is and click on **Add**.



MAC / IP / Port filtering

MAC / IP / Port filtering: ON OFF

Default rule (inbound/forward): Accepted

Current MAC / IP / Port filtering rules in effect

Index	Bound	Action	Comment
MAC / IP / Port filtering rule is empty			

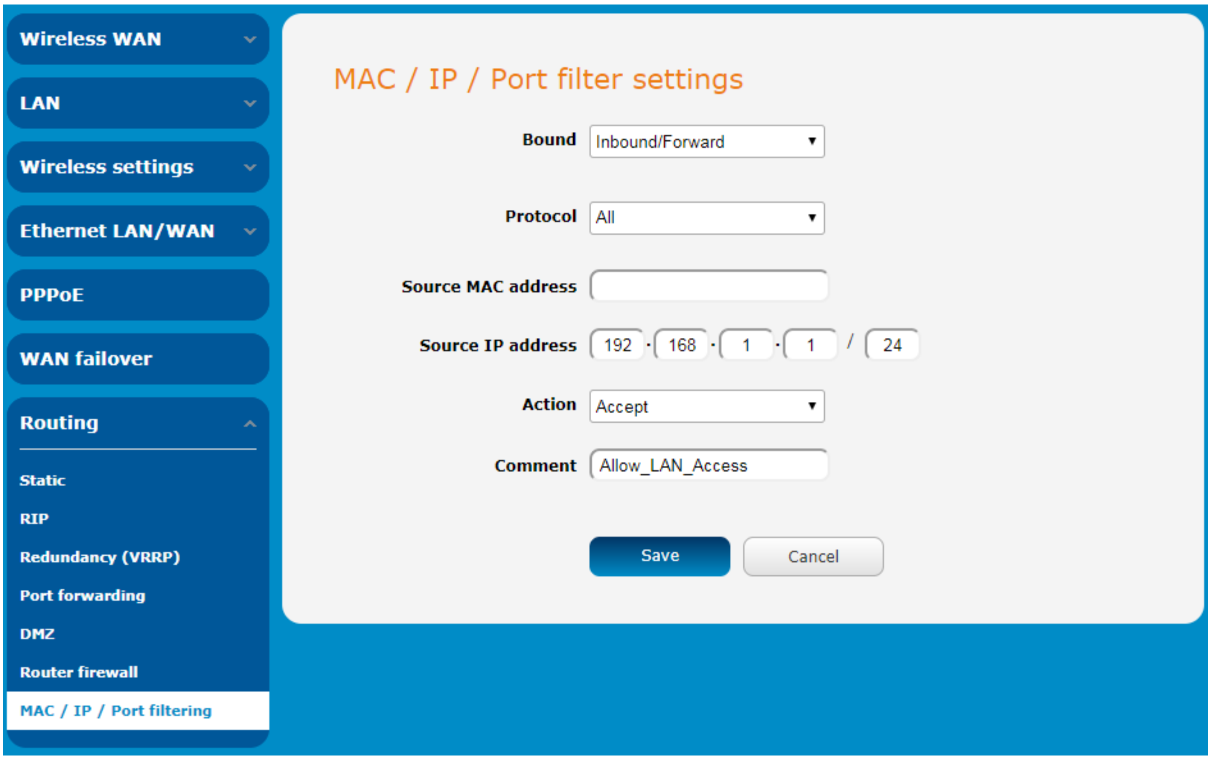
- In the next appearing window, we'll configure a default rule for our LAN traffic.

  Bound: Inbound/Forward

  Protocol: All

  Source IP address: 192.168.1.1/24 (Provide your LAN IP block)

  Action: Accept



MAC / IP / Port filter settings

Bound: Inbound/Forward

Protocol: All

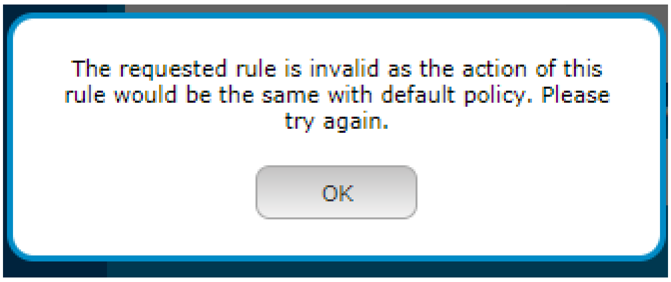
Source MAC address:

Source IP address: 192 . 168 . 1 . 1 / 24

Action: Accept

Comment: Allow_LAN_Access

This will show up a message that the configured rule is the same as the default. Ignore that message as we'll change the default rule later. Remember, the sequence is important. Proceed by clicking the **Save** button.



The requested rule is invalid as the action of this rule would be the same with default policy. Please try again.

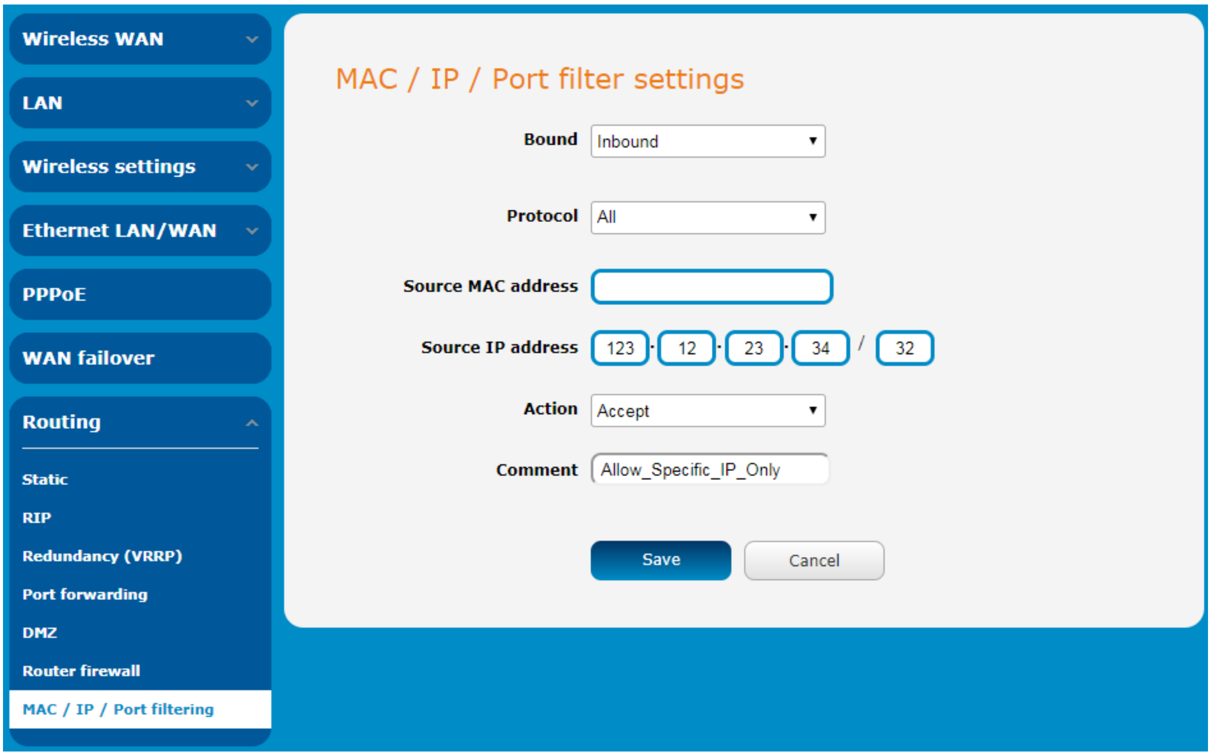
- Next configure the inbound rule allowing the specific IP address.

  Bound: Inbound

  Protocol: All

  Source IP address: X.X.X.X/24 (Provide the public IP that you'll be using to connect. For example, if you are planning to access the router from the office, check with your IT team about the public IP addresses that your office uses. Here you may configure a block in a single rule or individual IP addresses in individual rules. You may also search for "what is my ip" in google to find your IP address, just make sure that you have a fixed public IP)

  Action: Accept



MAC / IP / Port filter settings

Bound: Inbound

Protocol: All

Source MAC address:

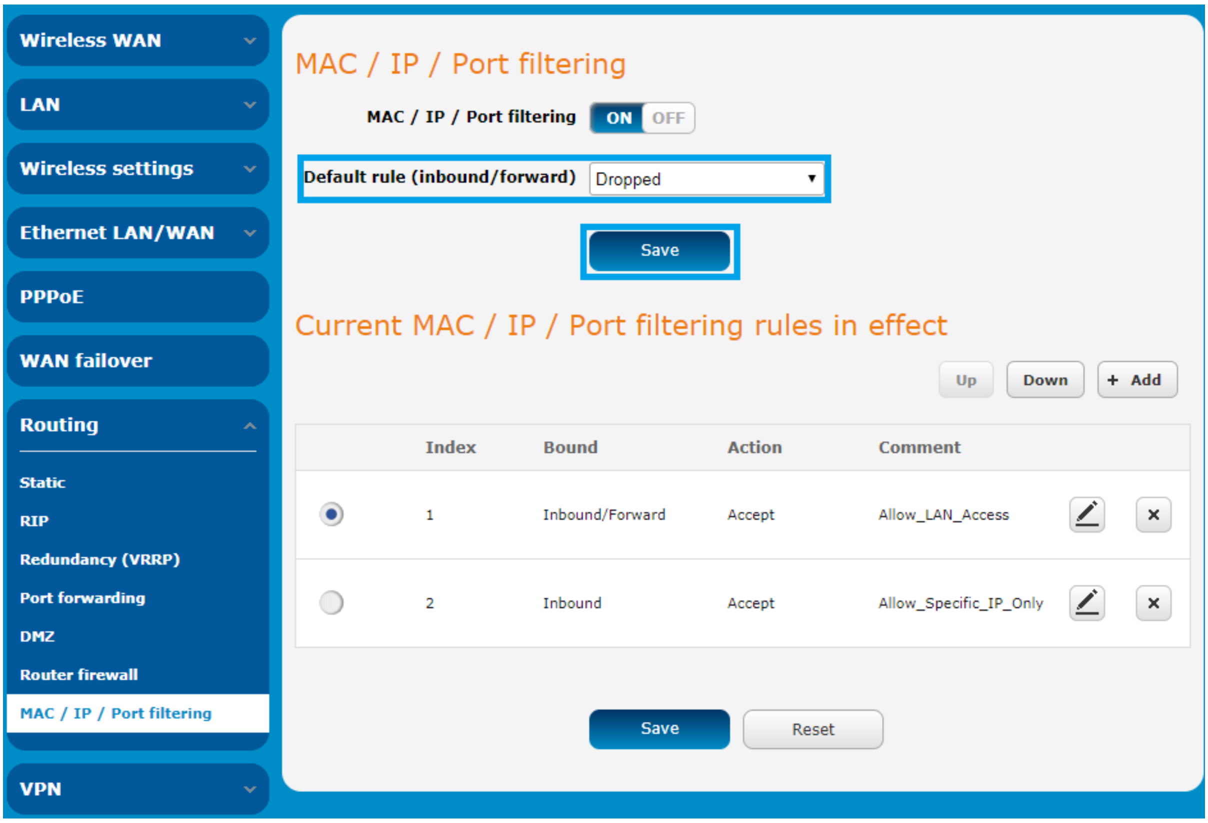
Source IP address: 123 . 12 . 23 . 34 / 32

Action: Accept

Comment: Allow_Specific_IP_Only

The same message will appear again, ignore it and press **OK**. Click **Save** to save the new rule.

2 Change the "Default rule (inbound/forward)" to "Dropped" and save the configuration.



MAC / IP / Port filtering

MAC / IP / Port filtering: ON

Default rule (inbound/forward): Dropped

Current MAC / IP / Port filtering rules in effect

	Index	Bound	Action	Comment
●	1	Inbound/Forward	Accept	Allow_LAN_Access
○	2	Inbound	Accept	Allow_Specific_IP_Only

From now on, only the configured IP address(es) will be able to access through open services from WAN, while any host on LAN side will have the same privilege as earlier.