Blocking Internet Access for LAN Clients

The information on this page is updated in accordance with the **00.07.4** firmware version .

□

Contents

Introduction

This article contains instructions o how to block Internet access for LAN clients using a Teltonika-Networks device.

Blocking WAN (Internet) access

Access between your end device and other networks is controlled by your network device's (router, gateway) firewall. Therefore, in order to set networks access limitations you will need to modify the firewall configuration. In the Teltonika-Networks devices this can be done over the **Network → Firewall** page.

- First, go to the **Network → Firewall → Traffic Rules** page.
- Scroll down to the 'Add New Forward Rule' section and create a rule such as this:
  1. Create a custom name for the rule.
  2. Set 'Source Zone' to *lan*.
  3. Set 'Destination Zone' to *wan*.
  4. Click 'Add'.

All clients

- To block all LAN clients from accessing the Internet, set up the rule like this:
  1. Set 'Protocol' to *Any*.
  2. Set 'Action' to *Drop*.

- If you later wish to undo the changes, you can delete the rule or turn it off.

Single client or range of clients

- To block a single LAN client from accessing the Internet, set up the rule like this:
  1. Set 'Protocol' to *Any*.
  2. Set 'Source address' to the the one that you wish to block.
  3. Set 'Action' to *Drop*.
- Alternatively, you can specify an IP address/netmask combination to include a range of addresses. For example, specifying *192.168.1.100/30* as the 'Source address' would denote a range of 192.168.1.100 to 192.168.1.103.
- If you later wish to undo the changes, you can delete the rule or turn it off.

Blocking a specific IP or network

- To block all LAN clients from accessing specific IP address, set up the rule like this:
  1. Set 'Protocol' to *Any*.
  2. Set 'Destination address' to the the one that you wish to block.
  3. Set 'Action' to *Drop*.
- Alternatively, you can specify an IP address/netmask combination to include a range of addresses. For example, specifying *10.0.0.0/8* as the 'Destination address' would denote a range of 10.0.0.0 to 10.255.255.255
- If you later wish to undo the changes, you can delete the rule or turn it off.

Blocking a specific site(s)

Note: On RUT and TRB series devices, Web Filter is additional software that can be installed from the **System → Package Manager** page.

- To block access to a website for LAN clients, go to Services → Web Filter.
- Set the main parameters of Web Filter under the 'Site Blocking Settings' section.
  1. Turn Web Filter on.
  2. Set 'Mode' to *Blacklist*.

  Alternatively, you can set 'Mode' to *Whitelist* to allow access only to specific sites and block access to all others.
- Specify sites that you wish to block under the 'Site Blocking Rules' section.
  1. Click 'Add' to create a new entry in the list. You may add as many entries as you wish.
  2. Specify a 'Hostname' that you wish to block.
  3. Don't forget to save the changes.