Firewall traffic rules

The information in this page is updated in accordance with **00.07.03.4** firmware version.

□

Contents

Introduction

This article contains instructions on how to configure firewall traffic rules to filter network traffic. Firewalls are a critical component of network security, and they act as a barrier between your network and the internet. By configuring traffic rules, you can gain granular control over what traffic should be allowed, blocked, or rejected. This can help to enhance network security by preventing unauthorized access and reducing the risk of malicious attacks. By following the instructions in this article, you can learn how to configure firewall traffic rules to enhance network security.

What is a traffic rule?

The **Traffic Rules** tab is a crucial feature of a firewall functionality that allows you to set rules to filter and control network traffic moving through the device. In essence, traffic rules determine which firewall rules will be applied to packets traveling through the network. These packets can be allowed, blocked, or rejected based on various criteria such as the source and destination IP addresses and port numbers specified in the packet headers. Additionally, traffic rules can be applied based on the specific firewall zone the packet is originating from and its intended

destination zone.

With traffic rules, you have the flexibility to choose which packets should be subject to specific firewall rules based on their characteristics. By allowing, blocking, or rejecting certain types of traffic, you can protect your network from malicious attacks and unauthorized access while ensuring that legitimate traffic flows smoothly.

Teltonika devices come equipped with preconfigured traffic rules that provide adequate security for basic scenarios. However, if your solution requirements demand additional unique changes to the firewall configuration, it's crucial to carefully configure traffic rules to ensure that your network operates efficiently and securely. You should analyze your network traffic patterns and security risks to determine which traffic should be allowed, blocked, or rejected. This process will help you create a custom traffic rule set tailored to your network's specific needs, thereby enhancing network security and efficiency.

It's worth noting that improperly configured traffic rules can cause network performance issues, such as delays or lost packets. Therefore, it's essential to test and verify the effectiveness of your traffic rules before implementing them in a production environment. Regularly reviewing and updating your traffic rules is also recommended to ensure that your network remains secure and optimized for performance.

Traffic Rules configuration specifics

This section aims to provide users with additional information that is crucial to know when configuring traffic rules. It not only answers some of the main questions that users may have, but also provides information that can make the configuration process smoother and more straightforward. By understanding this information, users can make more informed decisions and create effective traffic rule configurations that meet their network's specific needs.

Traffic Rules evaluation

Traffic rule settings can be found by navigating to **Network -> Firewall -> Traffic rules** via WebUI. The new rules are created in the **‘Add new instance’** section of the settings page.

The traffic is evaluated against each rule in the traffic rules from top to bottom. This means that if there are two distinct rules, one that allows traffic on a specific IP and another rule that blocks the traffic on that same IP, only the first rule will apply, and the traffic will be allowed.

It is important to be mindful of the order of traffic rules. The rules can always be rearranged by simply clicking on the symbol on the left side of the rule and dragging the rule where it is needed. You can also change the configuration of each rule by finding your rule in the traffic rules and pressing a **‘pencil’** button to edit settings.

Defining specific IP addresses and networks

It is possible to define both specific IP addresses to block hosts, as well as networks to block whole networks of devices. Examples are:

Full IP address for a host:

- 192.168.1.151

Network using CIDR notation:

- 192.168.1.0/24

Defining single ports and range of ports

It is also possible to define single ports, as well as a range of ports. To apply the rule for two ports, 22 and 443:

- Add port **22**
- Add port **443**

To apply the rule to all ports from 1200 to 1600:

- Add ports **1200-1600**

Resolving hostnames to IP addresses

A command **‘nslookup <hostname>’** can be utilized on both Windows and Linux machines to resolve a hostname to its corresponding IP address. This command can be particularly helpful when configuring network traffic rules because these rules require the use of IP addresses instead of hostnames. For instance, the following command can be used to resolve hostname '**www.wikipedia.org'** to its IP address:

```
nslookup www.wikipedia.org
```

It is worth noting that this command also functions on RutOS, as RutOS is based on OpenWRT, a Linux distribution.

Default ports for specific services

In the realm of networking, many services are assigned a default port number for communication. These default ports are typically well-known, reserved TCP/IP ports that range from 0 to 1023 and are specific to particular services. In addition to these ports, there are other well-known ports that fall outside of this range.

For example, the MQTT (Message Queuing Telemetry Transport) protocol, which is commonly used in Internet of Things (IoT) applications, uses port number 1883 as its default port. When configuring Teltonika devices to utilize the MQTT protocol, a rule is automatically created to permit traffic on port 1883.

However, if you encounter an issue with MQTT traffic being dropped, it is advisable to verify that the traffic rules are correctly configured to allow traffic on port 1883. You should confirm that the rule which permits traffic on this port exists and is enabled.

Furthermore, it is important to note that these default ports are not set in stone and can be changed. This can be necessary for security reasons, as attackers may target commonly used ports to exploit vulnerabilities in certain services. Therefore, it is crucial to periodically review and update the ports used by your organization's services to prevent security breaches.

Traffic rules configuration examples

In this section, we will discuss various types of traffic rule configurations that you can implement based on your specific needs. It's worth noting that traffic rules are highly flexible and allow you to create specific rules tailored to your network's unique requirements. Therefore, the following are merely examples of some possible configurations.

Allow a single host to access a web server in WAN network.

Let’s imagine that we would like to restrict traffic for this LAN network (192.168.1.0/24) and only one host needs to have access to the web server (185.xxx.xxx.xxx) on the internet.

Two traffic rules would be required for this scenario:

1. One traffic rule with lower priority to block all traffic from LAN to WAN network.
2. Another traffic rule with higher priority to allow a specific host (PC2) to access the web server.

All network traffic coming from the specified host (192.168.1.11) will match the first rule and will be allowed. All other traffic coming from other hosts on the local Network will not match the first rule, but will match the second rule and will be dropped.

In this scenario, only the host named ‘PC2’ on the **LAN** will be able to reach a web server in **WAN**.

Traffic rule to block all traffic to WAN

Create and configure the first rule to block all local traffic to WAN network.

- In the ‘Add type’ field choose **‘Add new forward rule’**.
- Enter a name of your choice for this rule.
- Choose **LAN** as source zone.
- Choose **WAN** as destination zone.
- Click **‘Add’**.

A new window will pop-out where you will be able to specify additional settings.

- In the action field choose **'Drop'**

Scroll down and press **'Save & Apply'**.

The new rule is created and enabled. To verify, go to the last page in **'Traffic rules'** and verify that the rule is configured correctly and is enabled.

Traffic rule to allow the host access

Create and configure the second rule to allow the host to access the web server:

- In the **'Add type'** field choose **'Add new forward rule'**.
- Enter a name of your choice for this rule.
- Choose **LAN** as source zone.
- Choose **WAN** as destination zone.
- Click **'Add'**.

A new window will pop-out where you will be able to specify additional settings.

- In the protocol field, choose **TCP+UDP**.
- In the source IP address enter the IP address of the host in **LAN** that you wish to allow to access the web server. In this example, the IP address of PC2 is **192.168.1.11**.
- In the destination address field, enter the IP address of the web server, which is **185.xxx.xxx.xxx** in this example.
- In the destination port field add ports **'80'** and **'443'**. These are **HTTP** and **HTTPS** port numbers that are used for communication with a web server.
- In the action field choose **'Accept'**.

You can specify additional settings as you wish. For example, you can set times when this rule should apply. This way, the host will be able to access the web server only at certain times.

Scroll down and press **'Save & Apply'**.

The new rule is created and enabled. To verify, go to the last page in **'Traffic rules'** and verify that the rule is configured correctly and is enabled. In addition, we need to move the second rule and ensure that the second rule is above the first rule.

These rules indicate that traffic from the host **192.168.1.11** in **LAN** destined to the IP address of **185.xxx.xxx.xxx** on ports **80** and **443** in **WAN** must be accepted. The **'Accept forward'** indicates the action (accept). The slider on the right side shows that the rule is enabled. The rule is above the Deny-LAN-WAN rule, so that traffic from host 192.168.1.11 (PC2) matches the first rule and is accepted. Traffic from other hosts in LAN will match the second rule and will be dropped.

Opening a port on the device.

To open a port on the device for WAN network:

- In the add type field select the **'Open ports on router'** option.
- Enter a name of your choice for this rule.
- Select a protocol that will be allowed to access the port. **TCP + UDP** by default
- Enter an external port that you want to open.
- Press the **'Add'** button.

A new window will pop-out where you will be able to specify additional settings. For the purpose of just opening a port, no additional settings are required. Scroll down and press **'Save & Apply'**.

The new rule is created and enabled. To verify, go to the last page in **'Traffic rules'** and verify that the rule is configured correctly and is enabled.

Here we can see that a new rule was created. It accepts **TCP, UDP** traffic from any host in **WAN** coming to the router on port **8080**. The slider on the right side is set to **'on'** indicating that the rule is enabled.

Open ports on the device for a specific LAN host.

To open a port for only one host on LAN you would need to create 2 traffic rules. One rule to block LAN traffic from accessing the port on device, and the second rule to allow only a single host to access that port. Both rules have similarities. The steps below describe how to create and configure both rules with differences mentioned.

Block traffic on a specific port from LAN

A traffic rule to block packets on a specific port from LAN:

- In the **'Add type'** field choose **'open ports on router'**.
- Enter a name of your choice for this rule.
- Select **'TCP+UDP'** as protocols.
- Enter an external port to block.
- Click **'Add'.**

A new window will pop-out where you will be able to specify additional settings.

- Choose **LAN** as the source zone.
- Leave the source IP field **‘any’** or specify a LAN network to block.
- In the action field choose **‘Drop’**.

Scroll down and press **‘Save & Apply’**.

The rule should not be created and enabled. The traffic coming from LAN to port 5000 on the device will now be dropped.

Allow traffic on a specific port from a single host in LAN

The second traffic rule to allow traffic on a specific port from a single host in LAN:

- In the **‘Add type’** field choose **‘open ports on router’**.
- Enter a name of your choice for this rule that allow host on a specified port.
- Select **'TCP+UDP'** as protocols.
- Enter an external port to allow.
- Click **‘Add’.**

- set the source IP address to the IP address of the host.
- In the action field choose **‘Accept’**.

Scroll down and press **‘Save & Apply’**.

The new rules are created and enabled. To verify, go to the last page in **‘Traffic rules’** and verify that the rule is configured correctly and is enabled. These rules indicate that any traffic coming from host **192.168.1.11** in the **LAN** to port **5000** on the device will be accepted. The slider on the right side shows that the rule is enabled. Drag the second rule to be above the first rule, so the traffic from the host is matched against it and is allowed to access the device on port 5000. All other traffic from the local network coming to port 5000 on the router will be dropped because it will match the second rule. For example, if port is set to 53 (a port used by DNS), only this host would be allowed to use DNS service running on the device. Similarly, if the ports are set to 80 and 443, only that specific IP address will be able to access the WebUI of the device.

Allow to remotely access the WebUI.

By default, all the traffic from WAN network to the router is rejected. A traffic rule can be configured to allow a specific IP address to access the WebUI of the router. It is a bad practice to allow all devices on the internet to be able to connect to the router, so only a single IP address will be able to do that in this example.

- In the **'Add type'** field choose **'Open ports on router'**.
- Enter a name of your choice for this rule.
- Choose **TCP** as the protocol.
- In the external port field, enter ports **80** and **443 (HTTP(S))** so that only the access to the WebUI is allowed. Click **'Add'**.

A new window will pop-out where you will be able to specify additional settings.

- In the source IP enter the IP address from which you want to be able to access the WebUI.
- Destination zone should be set to Device (input).
- In the destination IP address choose the IP address of the router.
- In the action field choose **'Accept'**.

You can specify additional settings as you wish.

Scroll down and press **'Save & Apply'**.

The new rule is created and enabled. To verify, go to the last page in **'Traffic rules'** and verify that the rule is configured correctly and is enabled.

The rule indicates that TCP traffic coming from the host **84.xxx.xxx.xxx** in the **WAN** to the device (router) on ports **80** and **443** will be accepted. The **'Accept input'** indicates the action (accept). The slider on the right side shows that the rule is enabled.

In this scenario, only the host **84.xxx.xxx.xxx** will be able to access the WebUI of the router via it's public IP. Similarly, if the port is set to 22 instead of 80 and 443, the remote host would be able to connect to the device via SSH, but not WebUI.

Block LAN network from accessing WAN on selected ports.

In this scenario devices on the **LAN** will not be able to send traffic to **WAN** on selected ports.

- In the **'Add type'** field choose **'Add new forward rule'**.
- Enter a name of your choice for this rule.
- Choose **LAN** as the source zone.

- Choose **WAN** as the destination zone.
- Click **‘Add’**.

A new window will pop-out where you will be able to specify additional settings.

- Select **'TCP+UDP'** as protocol.
- In the destination port field enter the range of ports you wish to deny (For example, **‘1500-1700’**), or list specific ports by leaving spaces in-between port numbers (For example, **‘80 443**’).
- In the action field choose **‘Drop’**.

You can specify additional settings as you wish. Scroll down and press **‘Save & Apply’**.

The new rule is created and enabled. To verify, go to the last page in **‘Traffic rules’** and verify that the rule is configured correctly and is enabled.

In this scenario, the traffic coming from the **LAN** devices to **WAN** on any port from a range of **1500-1700** will be dropped. The **‘Discard forward’** indicates the action (drop). The slider on the right side shows that the rule is enabled.

Block specific host on the LAN from accessing WAN on certain times.

In this scenario, a specific PC will not be able to send traffic to **WAN** during specified time periods. To block a certain PC, a **MAC** address is used. This is an address of a physical device and can belong to that device only. This is opposed to IP addresses, which can be easily changed.

- In the **‘Add type’** field choose **‘Add new forward rule’**.
- Enter a name of your choice for this rule.
- Choose **LAN** as source zone.
- Choose **WAN** as destination zone.
- Click **‘Add’**.

A new window will pop-out where you will be able to specify additional settings.

- In the source **MAC** address choose the **MAC** address of the host to who the rule will apply. You can enter a custom MAC address.
- In the action field choose **‘Drop’**.
- On weekdays you can choose on which days the rule will apply (The device will not be able to communicate). You can choose days of the month, start and stop times, and other time settings.

You can specify additional settings as you wish.
Scroll down and press **‘Save & Apply’**.

The new rule is created and enabled. To verify, go to the last page in **‘Traffic rules’** and verify that the rule is configured correctly and is enabled.

This rule indicates that the PC with mac address of **00:00:5e:xx:xx:xx** will not be able to send traffic to **WAN**. The **‘Discard forward’** indicates the action (drop). The rule does not show the times at which this rule is applied, but the times can be found on the settings page (**‘Pencil’** button). This rule will be applied for the first time on the 12th of February, 2023. Then, every Monday, Tuesday, Wednesday, Thursday, and Friday, from 8 AM to 4 PM this PC will not be able to send traffic to **WAN**.