https://wiki.teltonika-networks.com/view/VLAN_Inter-Zone_accessibility_control_configuration_example

VLAN Inter-Zone accessibility control configuration example

The information in this page is updated in accordance with firmware version **00.07.03**.

☐

Contents

Introduction

In this example we will show how to manage VLAN to VLAN communication with either **one** firewall zone or **multiple** firewall zones.

If you're having trouble finding any page or some of the parameters described here on your device's WebUI, you should turn on **"Advanced WebUI"** mode. You can do that by clicking the **"Basic"** button under **"Mode"** which is located at the top-right corner of the WebUI.

Setting up VLANs

In this example, we are assuming that the VLANs are already set up, we will configure the firewall accordingly. If you need information on how to create VLANs on your device please refer to this artice: VLAN set up. For this article we have 3 separate VLANs created:

- lan | IP 192.168.1.1/24
- lan2 | IP 192.168.2.1/24
- lan3 | IP 192.168.3.1/24

Created VLANs in the WebUI should look similar to this:

VLAN to VLAN communication with one firewall zone

Once VLANs are created - they lay under one firewall zone, here is a Topology of the network and the zone which covers all 3 of VLANs:

Initially, when we create VLAN interfaces, all VLANs are able to communicate with each other, for example pinging from lan to lan2:

To disable VLAN to VLAN communication, navigate to **Network -> Firewall -> General Settings**. Press **Edit** on the **LAN** zone (lan -> wan), click on **Forward** and select **Drop or Reject**. Make sure that all created VLANs are added in the Covered networks tab:

Now if we try to reach lan2 from lan, the devices are not able to communicate:

VLAN to VLAN communication with inter-zone forwarding

In order to get more control over VLANs, an **inter-zone** forwarding functionality should be used. Here is a network topology with firewall zones and an explanation.

To start with, we will need to create new firewall zones: LAN1, LAN2 and LAN3. To add new zones, navigate to **Network -> Firewall -> General Settings**. In the Zones section, press ADD button to add a new zone.

A new window will open, there configure the settings according to the points below and press Save & Apply.:

- Name: lan1
- Input: Accept
- Output: Accept
- Forward: Reject
- Covered networks: lan

Note: By setting the Input and Output zones to **Accept** traffic is allowed to enter and leave the zone. **Forward: Reject** blocks communication between zones - this is a default policy. **Inter-zone forwarding** section can be used to modify the default behavior of the Forward zone and allow communication between zones.

Follow the same steps to create Firewall Zones **lan2** and **lan3**. **Lan2** zone settings:

- Name: lan2
- Input: Accept
- Output: Accept
- Forward: Reject

- Covered networks: lan2

Lan3 zone settings:

- Name: lan3
- Input: Accept
- Output: Accept
- Forward: Reject
- Covered networks: lan3

Newly created firewall zones should look like this:

Now, to attach these zones to the corresponding interfaces, we need to go back to the Network Interfaces tab (**Network -> Interfaces -> General**). Click edit on the lan interface and navigate to Firewall settings. In Create / Assign firewall-zone section, select lan1:

Follow these steps to attach the corresponding zone to the interfaces:

- lan2 interface – firewall zone lan2
- lan3 interface – firewall zone lan3

Inter-zone forwarding use examples

To customize communication between VLANs, we will need to edit Inter-zone forwarding rules. Navigate back to the firewall settings (**Network -> Firewall -> General settings**) and edit zones according to your needs.

Example: **lan1** wants to communicate only with **lan2**:

- lan1 settings: allow forward to destination zones: lan2
- lan1 settings: allow forward from source zones: lan2
- No need to change settings for the lan2 zone

If **lan1** to **lan2** communication is allowed, zone settings should look like this:

Testing the communication between **lan1** and **lan2**:

If we try to reach **lan3** from **lan1**, where the forwarding is not set, the result would be this:

To reach **lan3** from **lan1**, edit **lan3** zone accordingly:

- allow forward to destination zones: lan1
- allow forward from source zones: lan1

Zone settings after these changes should look like this:

Now the communication between **lan1** and **lan3** works:

Using these examples as a base, you can allow / reject VLAN to VLAN communication between different VLANs according to your needs.