TACACS+

☐

Contents

Introduction

This article contains instructions on configuring a RUTX router to start using the TACACS+ function. TACACS+ (Terminal Access Controller Access Control System) is a security protocol that provides centralized validation of users who are attempting to gain access to a router or other devices. TACACS+ provides separate authentication, authorization, and accounting services. The TACACS+ will work on our **newest firmware version which currently is 7.3**, unfortunately, older firmware versions does not support this function.

Prerequisites

- Docker Desktop
- RUTX router
- Firmware version that is **not older than 7.3**

Docker Desktop instructions

Visit https://www.docker.com/products/docker-desktop/ and choose an appropriate version of the Docker Desktop for your operating system. Create yourself a free account to start with.

Creating Docker Containers

After completing the installation, and creating a new account, open up the terminal supported by your operating system and run the following command:

```
docker run --name tac_plus -it -d -p 49:49 lfkeitel/tacacs_plus:latest
```

The result should be:

- In console:

- In Docker Desktop:

- After successfully creating a container, copy the **CONTAINER ID** from the Docker Desktop application or console terminal.

Configuring the Docker container

- Let's execute a command using a console terminal that will log in us into the Docker Container.

```
docker exec -it <CONTAINER ID> /bin/bash
```

The result should look similar to this:

Now we need to make some adjustments to the configuration file of our container. To be able to edit the files, let's install a new application by using the following command in our console terminal:

```
apt install nano
```

After installing the nano editor, enter the following command to edit the container configuration file:

```
nano etc/tac_plus/tac_plus.cfg
```

Edit the original **user = admin** to **user = root** and change the password, the password will override the original router password for the configured root user. Please **do not** delete the word "**clear**" (underlined in green in the example below) in front of the password. You can also edit the secret key in the **host = world** section, this variable is called a key, and by default, it's set to **tac_plus_key**. After you finish the editing to save the configuration file click CTRL+X, then choose YES (Y button on the keyboard) and ENTER.

- Make sure that **port number 49** (TACACS) is accessible. Depending on your operating system make the required adjustments to the firewall. Restart the Docker container to start it with the new configuration settings.

Router configuration

- Install the PAM package from the package manager or you can find it and download it at the following link: https://wiki.teltonika-networks.com/view/RUTX11_Package_Downloads
- Navigate to WebUI → Administration → Access control → General
- Switch from General to the PAM tab.
- Click edit on **SSH** service.
- Change the settings:

Testing the configuration

- Open the SSH client you are using.
- Connect to the router via SSH as usual.
- Enter the password you set in the **tac_plus.cfg** configuration file.
- If you check the logs (logread command), you should see something like this:

- Keep in mind that you **wouldn't be able to access the router** via SSH using the **default router password** unless you turn off the PAM authentication in the router's WEBUI.