Subnet Authorization

This type of authorization allows you to create an authorization rule for a specific UTM user from a specific subnet

In order not to register each device as a separate UTM user and not to fix authorization factors for it, you can use Subnet Authorization.

This feature will allow a UTM user from the desired subnet to auto-authorize without being tied to a MAC and/or specific IP and will be useful if a large number of devices need to be auto-authorized.

> Traffic across the entire subnet will be recorded per user.
> In a network for which a Subnet Authorization rule has been created, DHCP can work.

For example, there is a WiFi subnet on the 192.168.10.0/24 subnet from which devices should be allowed to log in. Create an authorization rule:

1. Go to the **Users –> User & Group** section and click Add user

2. Fill in the fields Subnet name, Login, and click Save

3. Go to the section **Users –> Authorization –> Subnet authorization** and click **Add** in the upper left corner

4. Fill in the fields and click **Save**:

- User - select the user created in step 2
- Subnet - enter IP and subnet mask
- Comment - (optional)

Authorization

General   IP and MAC authorization   **Subnet authorization**

Adding an authorization rule

User
Subnet 1   ▼

Subnet
192.168.160.0/24

Comment
Guest subnet

Save   Cancel

Be careful when creating Subnet authorization rules
There will be problems with authorization if:
- There are overlapping networks for different users
- There are rules for authorizing users by IP addresses from a subnet in the Subnet authorization rule;
- Rules have been created in the **Fixed VPN IP addresses** subsection with binding to an IP address from the subnet of the Subnet authorization rule.

Revision #4
Created 24 August 2022 22:07:00 by Val Redman
Updated 13 October 2022 14:44:45 by Val Redman