How to Install OpenVPN with MFA in OPNsense?

OpenVPN is an open-source VPN protocol that creates secure point-to-point or site-to-site connections using virtual private network (VPN) techniques. It was created by James Yonan in 2001 and is now one of the most popular VPN protocols among VPN users. It is distributed under the GNU General Public License (GPL). The project is being worked on by OpenVPN Inc. and a large number of open-source developers.

It supports all major operating systems, including macOS, FreeBSD, Windows, Linux, iOS, and Android.

The OpenVPN protocol has a high level of security. It comes with 256-bit encryption via OpenSSL. OpenVPN can use two different protocols for data transmission: TCP and UDP. The more widely used and recommended protocol is UDP. Pre-shared keys, certificate-based authentication, username/password authentication, and MFA are all supported by OpenVPN.

The factors username/password and a token are required for two-factor authentication. Another layer, namely a user certificate, is supported by OPNsense. This means that the user certificate will uniquely identify each user.

In this tutorial, we will explain to you how to install and configure the OpenVPN server on your OPNsense firewall that will allow your remote clients to safely access the Internet through your VPN tunnel. We'll also configure MFA for VPN user authentication by using the following multi factors:

- User certificate
- Username/Password
- Token (TOTP)

> **TIP**
>
> It is strongly advised that you install Zenarmor on your OpenVPN server to increase the security of your network. You can block security threats coming from your OpenVPN tunnel interface by configuring the Zenarmor, using web filtering, and applying application control.

The OpenVPN configuration is very simple. You can set up the OpenVPN tunnel with MFA i OPNsense firewall by simply following the seven steps outlined below.

1. Create a Certificate Authority
2. Configure OpenVPN in OPNsense
3. Create a VPN User
4. Add TOTP Access Server
5. Create SSL VPN Service
6. Add Firewall Rules
7. Export OpenVPN Client

To be able to follow this OpenVPN installation in the OPNsense firewall tutorial, you must have the following devices and root privileges.

- OPNsense 21.7.6 Firewall, configured as an OpenVPN VPN server.
- As an OpenVPN VPN client, a Windows PC or an Android device will be set up.
- Installed Google Authenticator Application.

1. Creating a Certificate Authority

OpenVPN requires certificates to protect the VPN service through encryption and authentication. The first step in configuring OPNsense is to create a Certificate Authority. To proceed, each option on this page must be selected, and all forms must be correctly completed. If you already have one, you can skip this step.

You may create a new Certificate Authority by following the steps below:

1. Navigate to `System` → `Trust` → `Authorities`.

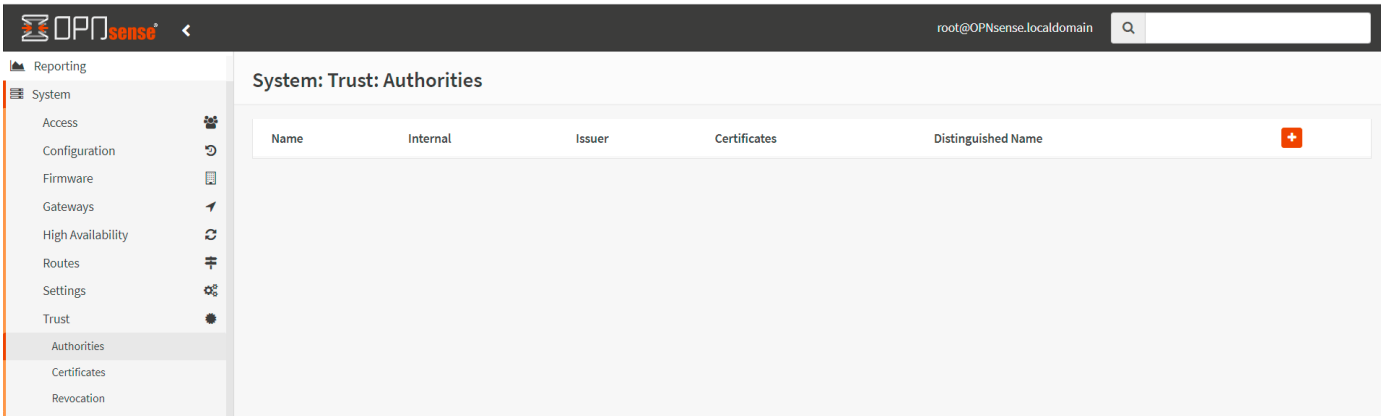

Figure 1. *Managing Certificate Authorities in OPNsense*

2. Click on the add button with the `+` icon at the top right corner of the form to create a new one.
3. Fill in the **Descriptive Name** field for the Certificate Authority, such as `OPNsenseOpenV`

4. Select `Create an internal Certificate Authority` for the **Method** option.
5. Select `RSA` for **Key Type**.
6. Set **Key length (bits)** to `4096`. A longer bit length increases the security of the key, but it also increases processing time. It is not recommended that the key length be less than 2048 bits.
7. **Digest Algorithm** to `SHA512`.
8. Set **Lifetime (days)** to 365 which means that any certificates that are signed by this CA will become invalid after one year. For a home network firewall, you may set a longer lifetime.
9. Set **Country Code**, such as `US`.
10. Set **State**, such as `California`.
11. Set **City**, such as `Sunnyvale`.
12. Set **Organization**, such as `MyCompany`.
13. Set the **Email Address**.
14. Set **Common Name** to `internal-openvpn-ca`.
15. Click `Save`.

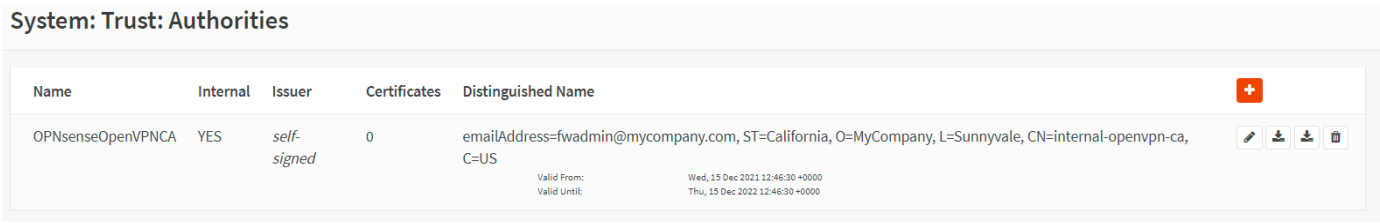

Figure 2. *Created Certificate Authorities on OPNsense*

2. Creating a Server Certificate

You may create a new Server Certificate that clients will use to verify the identity of the server when connecting to it by following the steps below:

1. Navigate to `System` → `Trust` → `Certificates`.

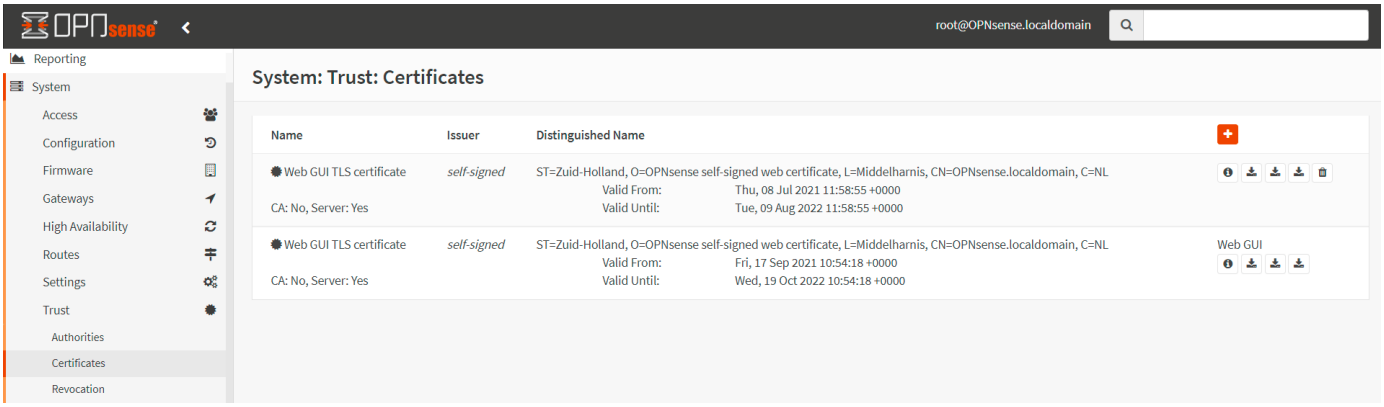

Figure 3. *Created Server Certificates in OPNsense*

> **INFO**
>
> There are already some certificates in the list, as you may have noticed. That certificate is currently being used by the web admin page you are viewing. Because HTTPS is enabled by default, it was created during the OPNsense installation.

2. Click on the add button with the `+` icon at the top right corner of the form to create a new one.
3. Select `Create an internal Certificate` for the **Method** option.
4. Fill in the **Description** field for the Server Certificate, such as `OpenVPN Server Certificate`.
5. Set **Certificate Authority** to `OPNsenseOpenVPNCA`.
6. Set **Type** to `Server Certificate`.
7. Set **Key length (bits)** to `4096`.
8. **Digest Algorithm** to `SHA512`.
9. Set **Lifetime (days)** to 365.
10. Set **Private key** location to `Save on this firewall`,

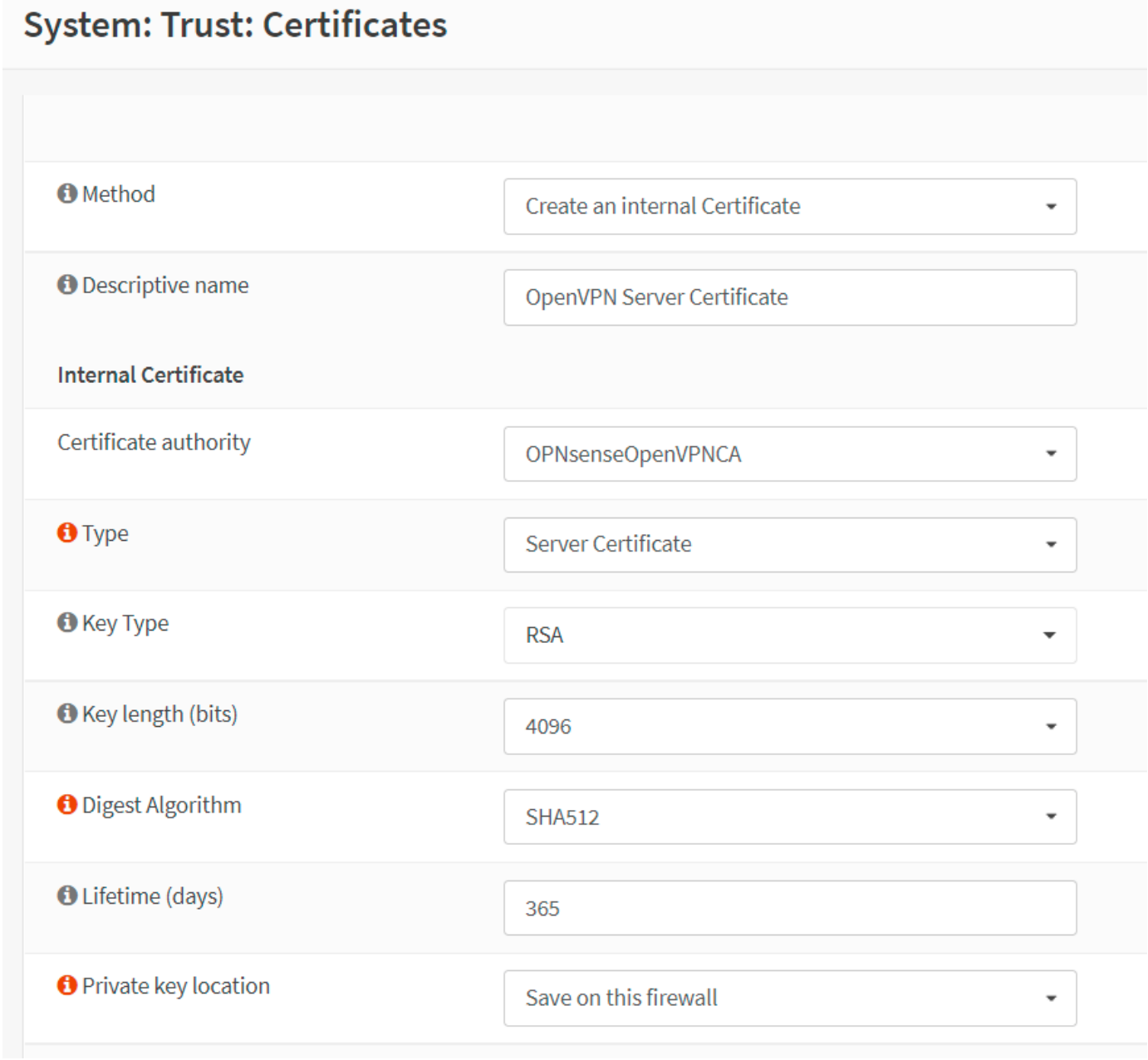

Figure 4. *Setting Server Certificate options in OPNsense-1*

11. Set **Country Code**, such as `US`.
12. Set **State**, such as `California`.
13. Set **City**, such as `Sunnyvale`.
14. Set **Organization**, such as `MyCompany`.
15. Set the **Email Address**.
16. Set **Common Name** to `OpenVPN Server Certificate`.
17. Leave other settings as default.

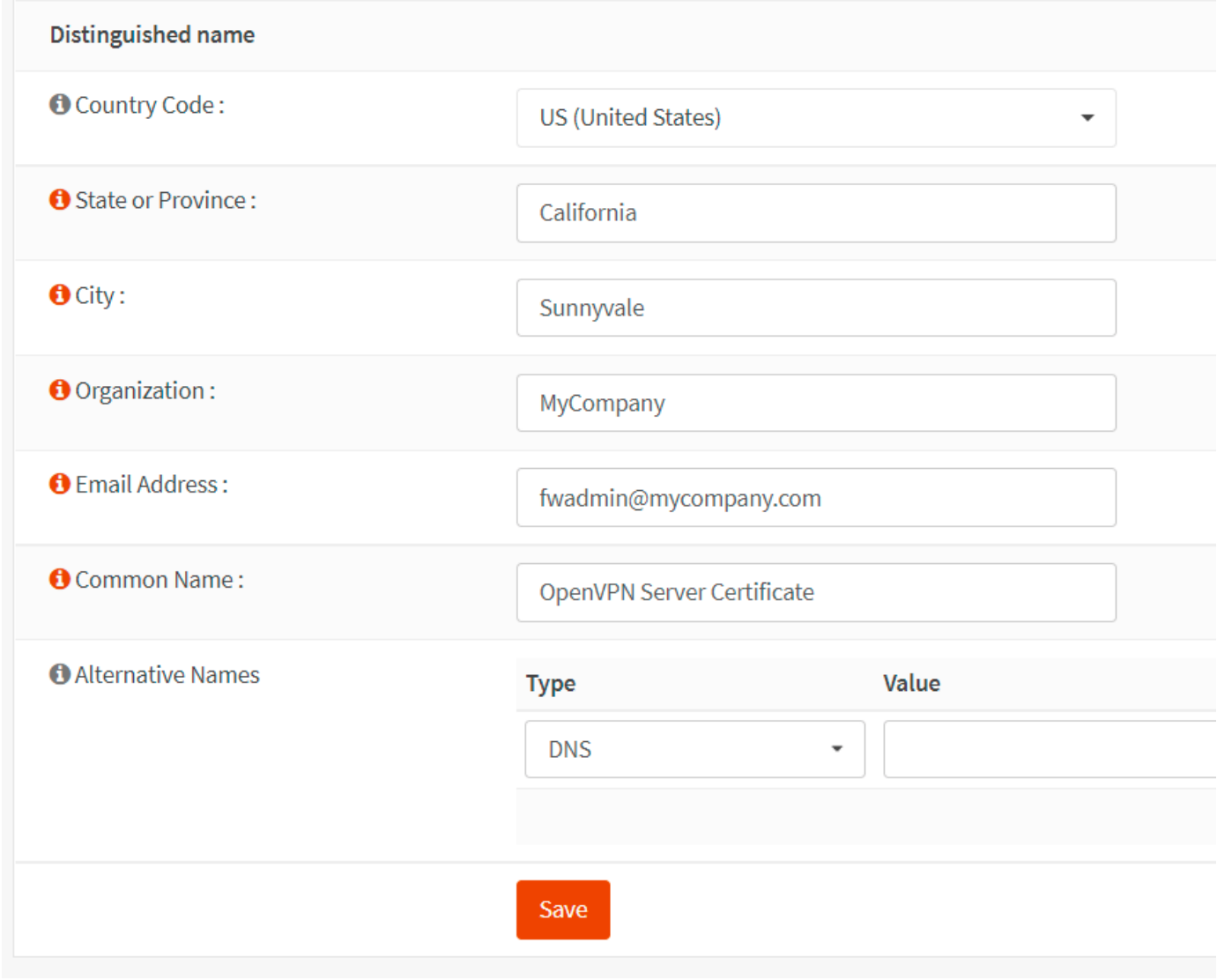

Figure 5. *Setting Server Certificate options in OPNsense-2*

18. Click `Save`.

You may manage your server certificates on the `Certificates` page of your OPNsense firewall. It allows you to view, delete, export user certificates and user keys by using the action buttons at the end of the certificate row.

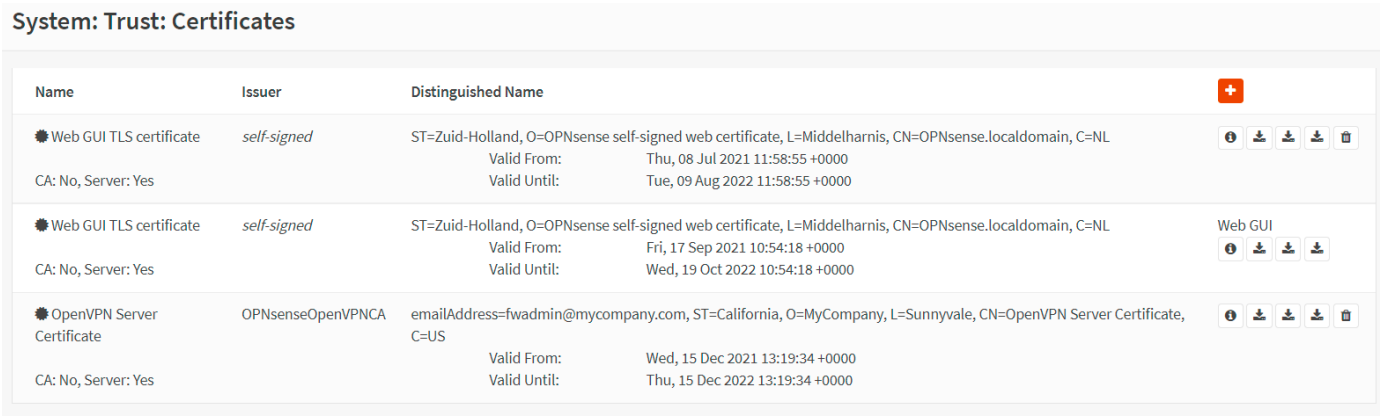

Figure 6. *Managing Server Certificates in OPNsense*

3. Creating a VPN User

OPNsense provides the following options for user authentication:

- **Local User Access:** You may manage VPN users using the OPNsense local user manager.
- **RADIUS:** You may manage users on an external RADIUS authentication server.
- **LDAP:** You may manage user access using Windows Active Directory Services.

For authentication in this tutorial, we will use `Local User Access`. When using Local User Access, per-user certificates can be easily used and managed in the OPNsense GUI. This is far more secure, but depending on the number of people who will access the service, it may be less convenient than using a central authentication system.

To manage VPN users, passwords, and certificates in the OPNsense firewall, you may follow the next two main steps given below:

1. *Adding OPNsense Local User*
2. *Creating Certificate for the VPN User*

1. Adding OPNsense Local User

We will only create one user account in this tutorial, but the procedure applies to as many users as we want. You may follow the steps listed below to add a local user to your OPNsense firewall:

1. Navigate to the `System` → `Access` → `Users` in your OPNsense firewall.
2. Enter a unique `Username` for the VPN account, such as `vpnuser1`.
3. Enter a strong `Password` for the VPN user.
4. Fill in the `Full Name` field.
5. You may enter an `E-Mail`.

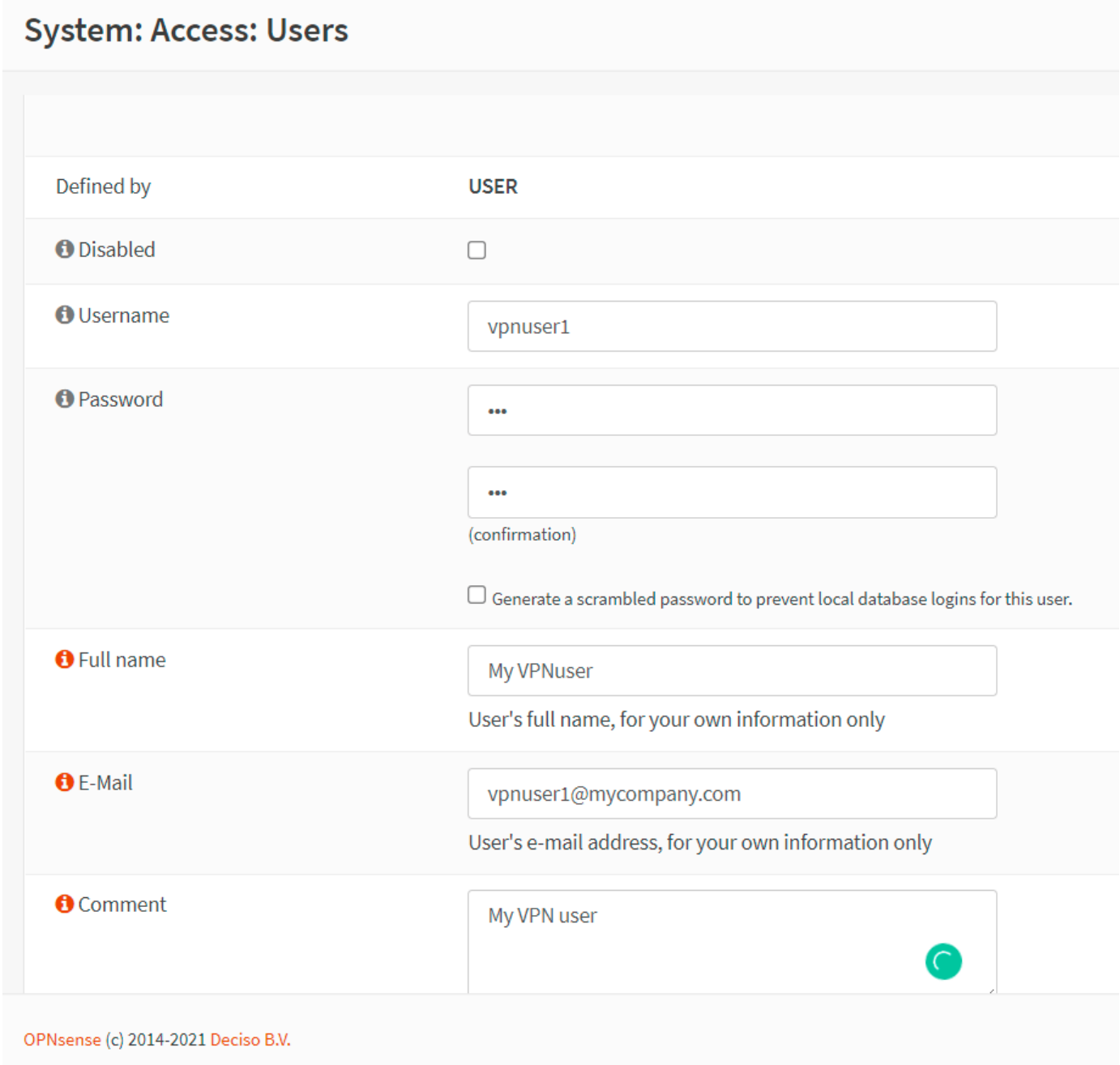

Figure 7. *Creating VPN user account in OPNsense-1*

6. You may leave the **Login shell** as `/sbin/nologin` if the VPN account is only going to be used for VPN access. This option prevents the user from logging into the OPNsense web UI.
7. You may enter an `Expiration date` or leave blank if the account shouldn't expire.
8. Check `Click to create a user certificate` for the **Certificate** option. So that a user certificate can be created at the same time creating the user account automatically.
9. Check `Generate new secret` for the **OTP seed** option to enable MFA for your VPN users.
10. You may leave other settings as default.
11. Click the `Save` button to apply the settings. This will redirect you to the certificate page to create the VPN user certificate. Certificate creation for the VPN user account is explained in the next section.

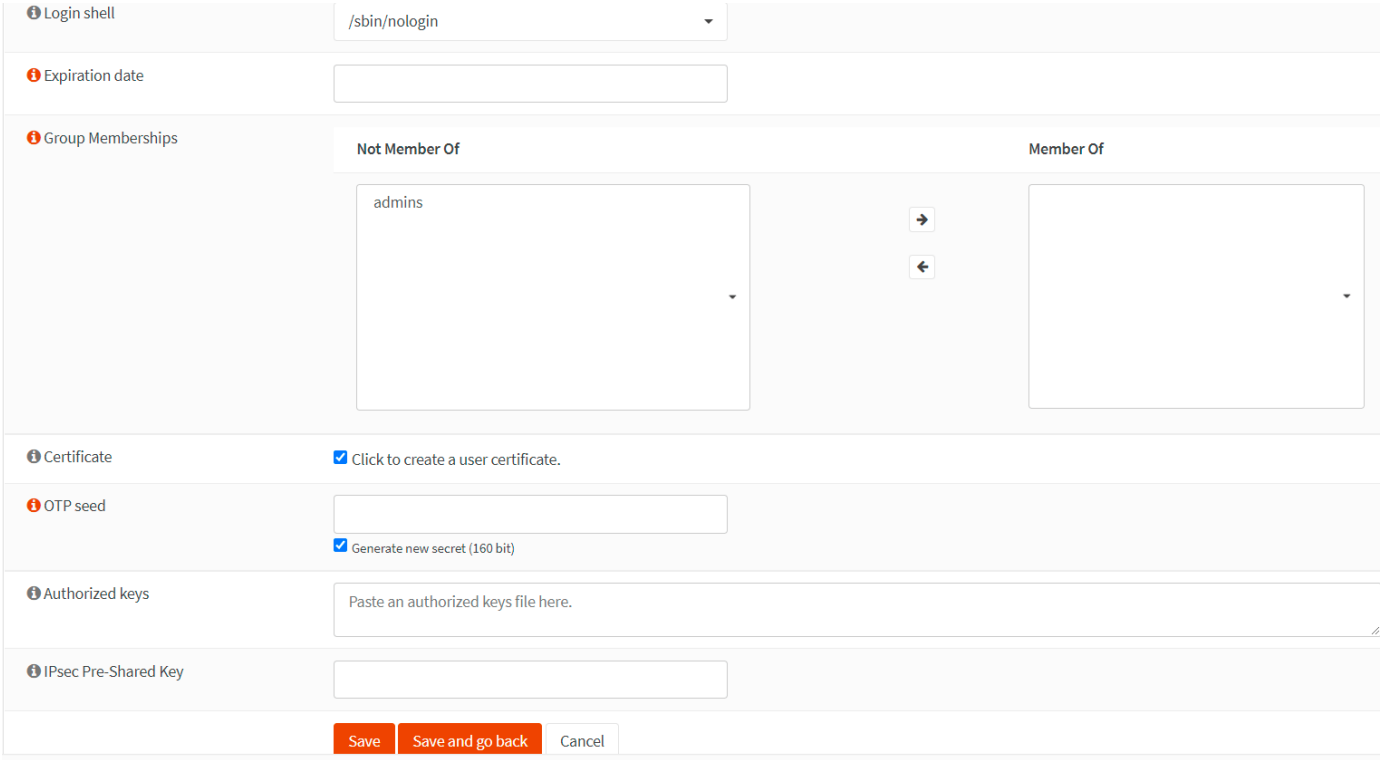

Figure 8. *Creating VPN user account in OPNsense-2*

2. Creating Certificate for the VPN User

We will only create a certificate for the user we have created in the previous section. You may apply the same procedure for all users you want. Follow the next steps listed below to add a certificate for the VPN user you've previously created in your OPNsense firewall:

1. Select `Create an internal Certificate` for the **Method** option.
2. You may leave the **Descriptive Name** field as it is, in our example `vpnuser1`.
3. Set **Certificate** authority to `OPNsenseOpenVPNCA`.
4. Set **Type** to `Client Certificate`.
5. Set **Key length (bits)** to `4096`.
6. Set **Digest Algorithm** to `SHA512`.
7. Set **Lifetime (days)** to 365.
8. Set **Private key** location to `Save on this firewall`,

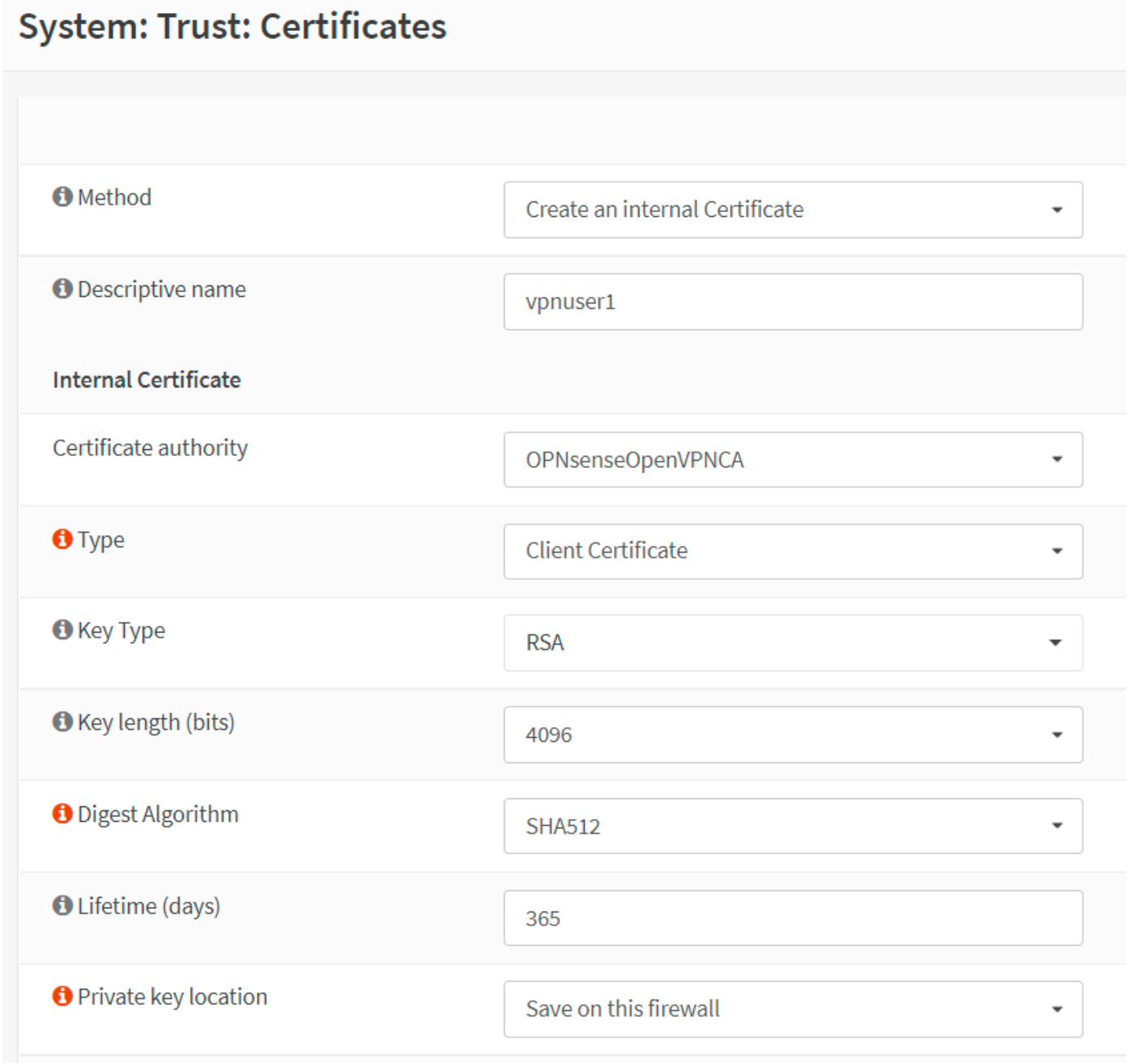

Figure 9. *Setting Client Certificate options in OPNsense-1*

9. Leave other settings as default.

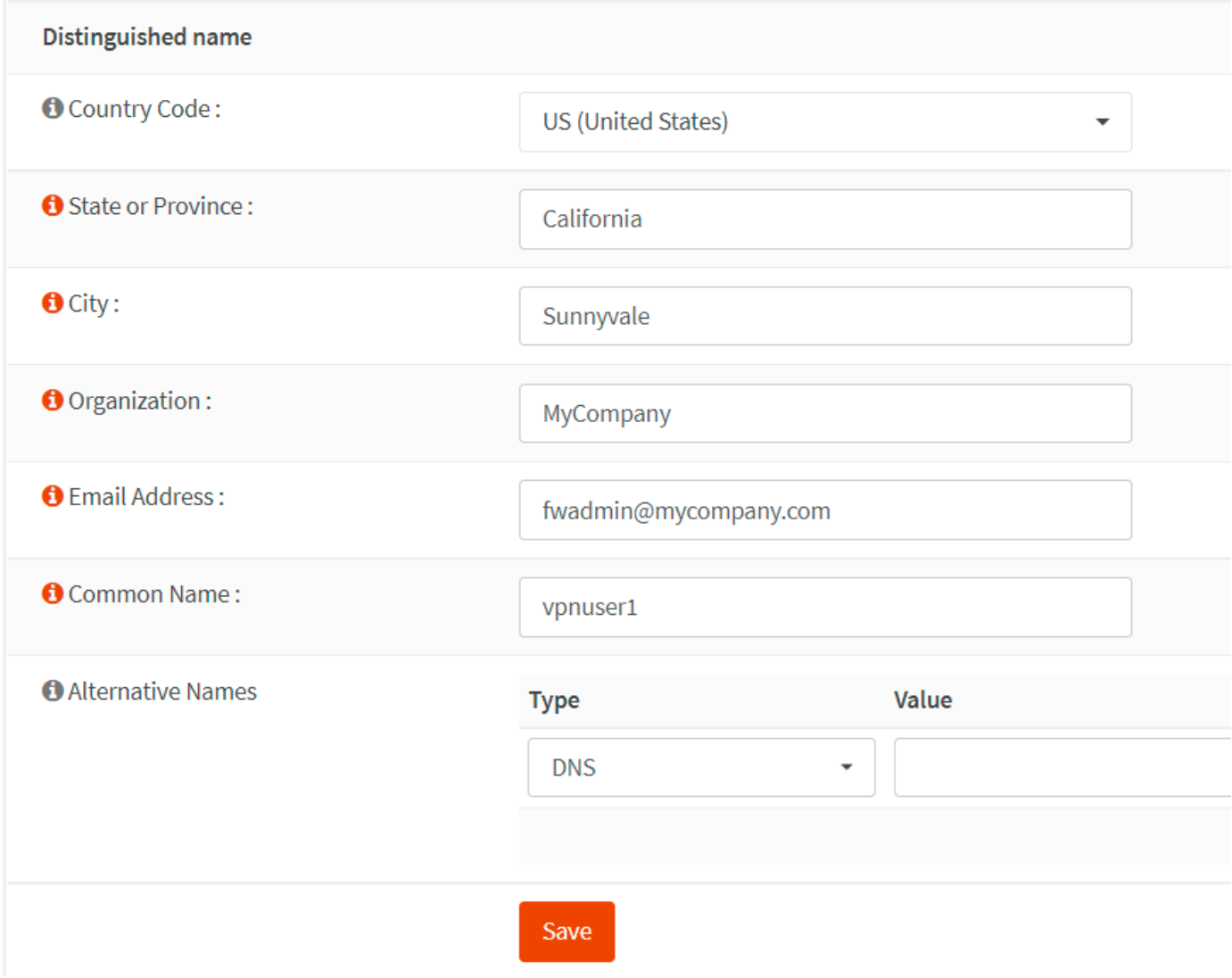

Figure 10. *Setting Client Certificate options in OPNsense-2*

10. Click the `Save` button. This will redirect you to the User page.
11. Scroll down to the **OTP QR code** option.
12. Click on the `Click to unhide` button to activate your newly created seed with your Google Authenticator compatible app. You will be given a QR code that you can scan with your mobile phone.

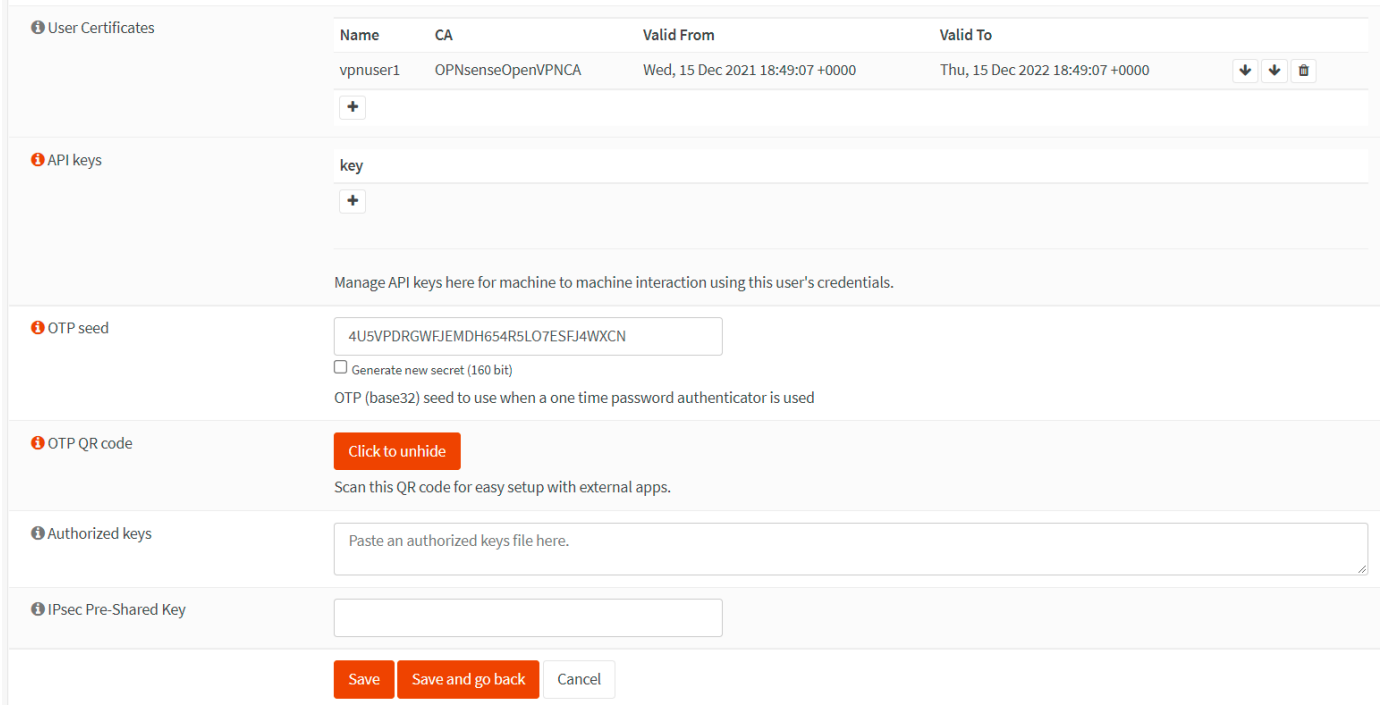

Figure 11. *Activating OTP seed in OPNsense*

13. Send the QR code to the user in a secure way.

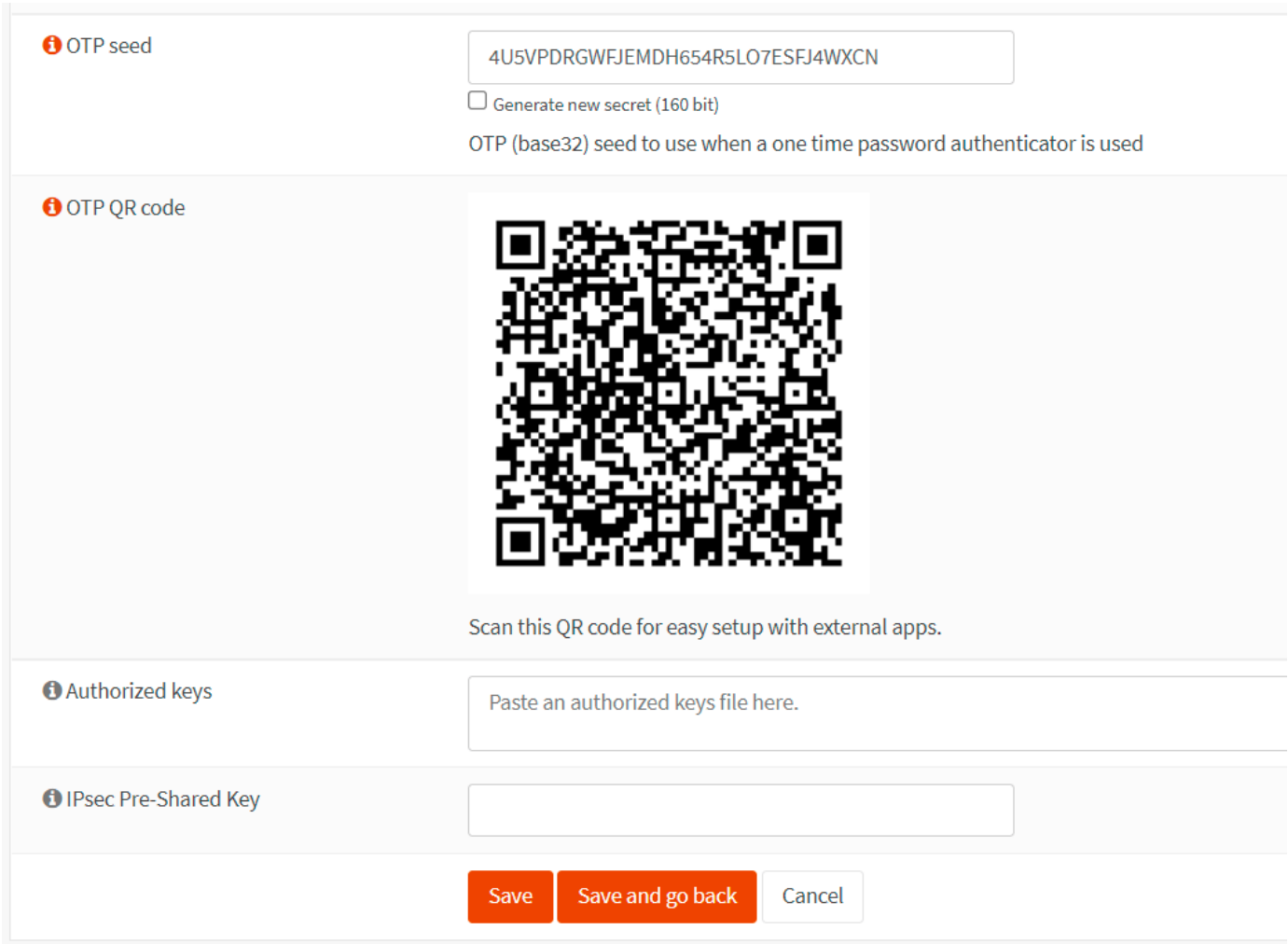

Figure 12. *Obtaining OTP QR code in OPNsense*

14. Click the `Save` button to activate the settings.
15. You may view the certificate created for the VPN user by navigating to the `System` > `Trust` > `Certificates` in your OPNsense firewall.

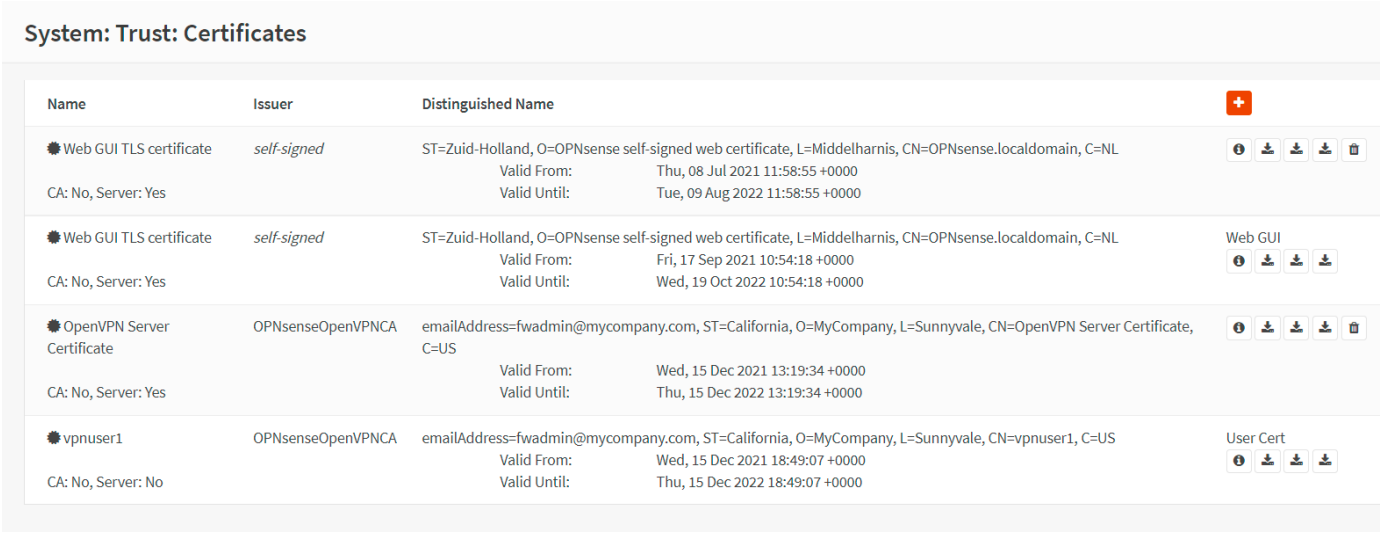

Figure 13. *Viewing the VPN client certificate in OPNsense*

> **CAUTION**
>
> Don't forget to send the newly generated OTP QR code to the VPN user, here `vpnuser1`, in a secure way.

4. Add TOTP Access Server

Since we'll configure an OpenVPN service with MFA in this tutorial, we must create a TOTP(Time-based One Time Password) server in the OPNsense firewall.

> **INFO**
>
> If you are installing the OpenVPN server to access your home network and you may not need an additional layer of security by implementing MFA for your VPN connection, you may skip this step.

To add a TOTP server in your OPNsense system, you may follow the instructions below:

1. Navigate to `System` > `Access` > `Servers` in your OPNsense web UI.

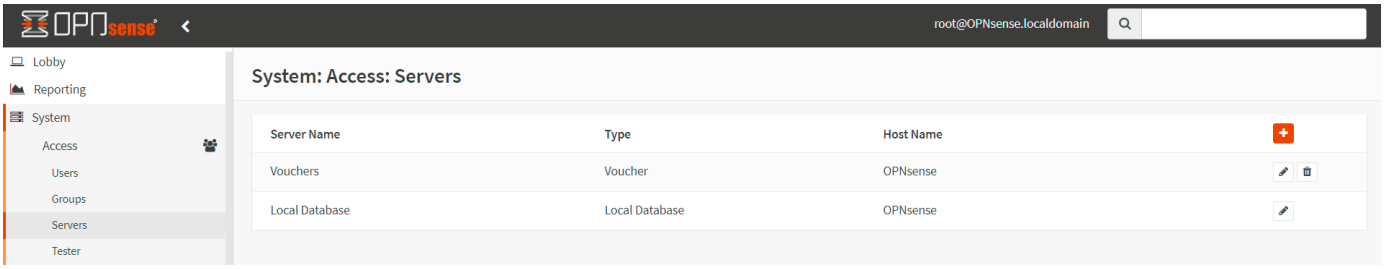

Figure 14. *Access Servers in OPNsense*

2. Click on the add button with the `+` icon at the top right corner of the form to create a new one.
3. Fill in the **Descriptive name** field for the Server, such as `TOTP VPN Access Server`.
4. Set the **Type** to `Local + Timebased One time Password`.
5. Leave other options as default if you use `Google Authenticator` as in our tutorial. For other tokens, you may need to change the `Token Length` option.
6. Click `Save` to add the TOTP server.

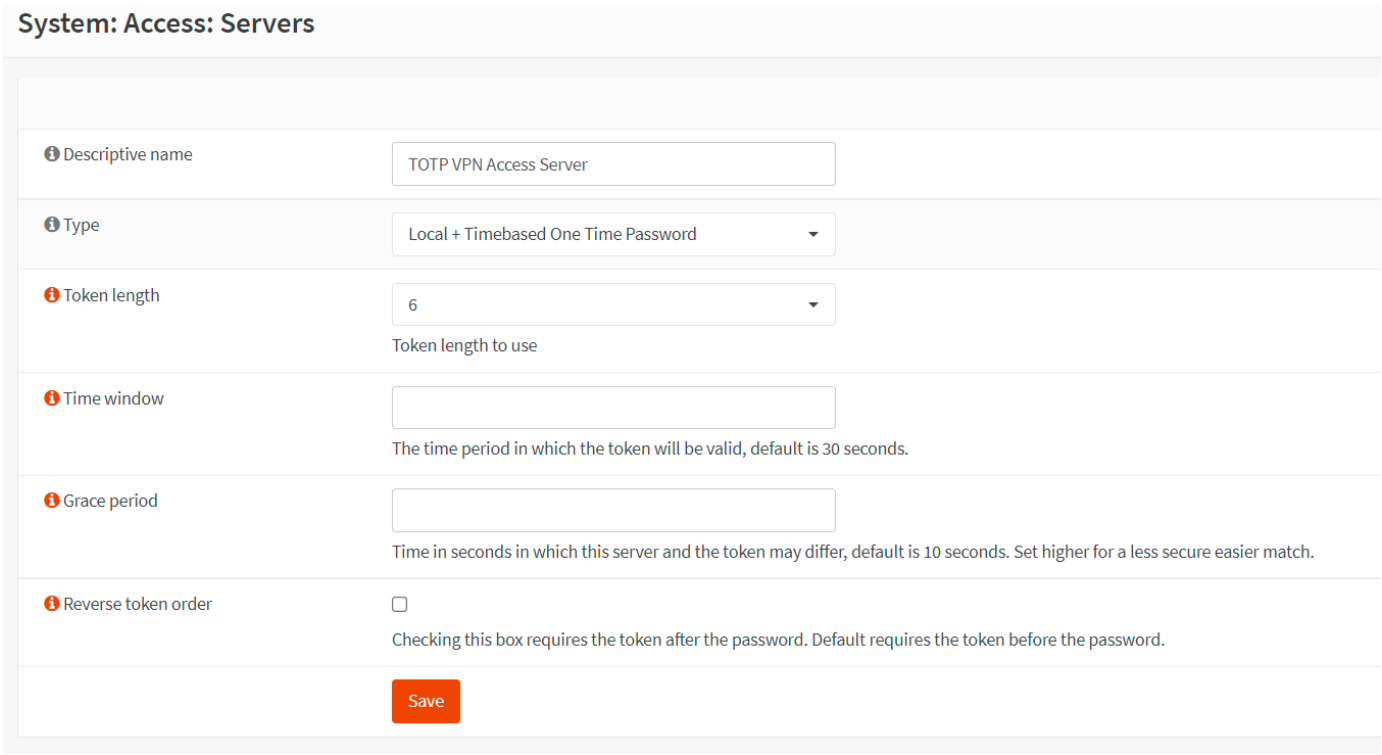

Figure 15. *Adding TOTP Access Server in OPNsense*

5. Add OpenVPN Server

After you've created the VPN users and certificates, you may start to set up the OpenVPN server in your OPNsense firewall. Adding a new OpenVPN server is a straightforward process. In this tutorial, we'll add one that makes use of multi-factor authentication. This configuration pro

adequate protection and is simple to implement on clients, as each can use the same configuration.

There are five sections in the OpenVPN server configuration in OPNsense:

1. *General Information*
2. *Cryptographic Settings*
3. *Tunnel Settings*
4. *Client Settings*
5. *Advanced configuration*

To set up an OpenVPN server in your OPNsense firewall, you may follow the next steps given below:

1. Navigate to `VPN` > `OpenVPN` > `Servers` in your OPNsense web UI.

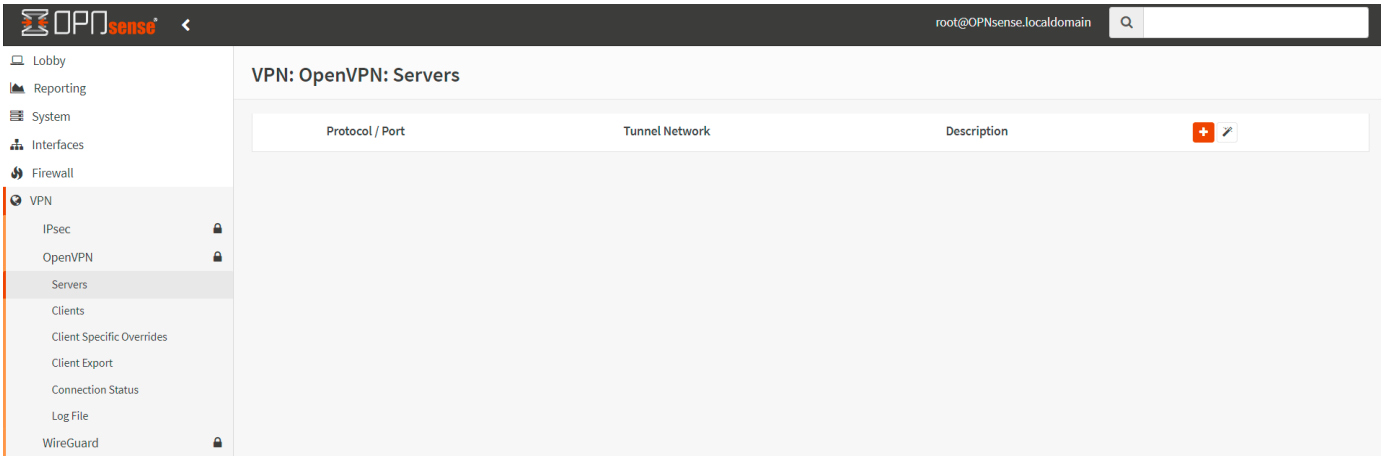

Figure 16. *OpenVPN servers in OPNsense*

2. Click on the add button with the `+` icon at the top right corner of the form to create a new one.

> **TIP**
>
> There is a wizard icon next to the `+` icon on the OpenVPN Servers page. By clicking on the wizard icon you may use the setup wizard to configure an OpenVPN server. It may be more convenient for some users.

3. Fill in the **Descriptive name** field for the Server, such as `My OpenVPN Server`.
4. Select `Remote Access (SSL/TLS + User Auth)` for the **Server Mode** since we'll use MFA.
5. Select `TOTP VPN Access Server` for **Backend for authentication**.

> **TIP**
>
> If you are installing the OpenVPN server to access your home network and you don't need an additional security layer by implementing MFA for your VPN connection, you may select `Local Database` for the Backend for Authentication. Then, your VPN clients are authenticated with 2FA by using local usernames, passwords, and certificates which are secure enough for a home network.

6. Set **Protocol** to `UDP`.
7. Select `tun` for the **Device Mode**.
8. Set **Interface** to `WAN`. If you have multiple WAN interfaces, you may select `any`.
9. You may leave the **Local Port** as default, `1194`. Or, you may change it as you wish for security reasons.

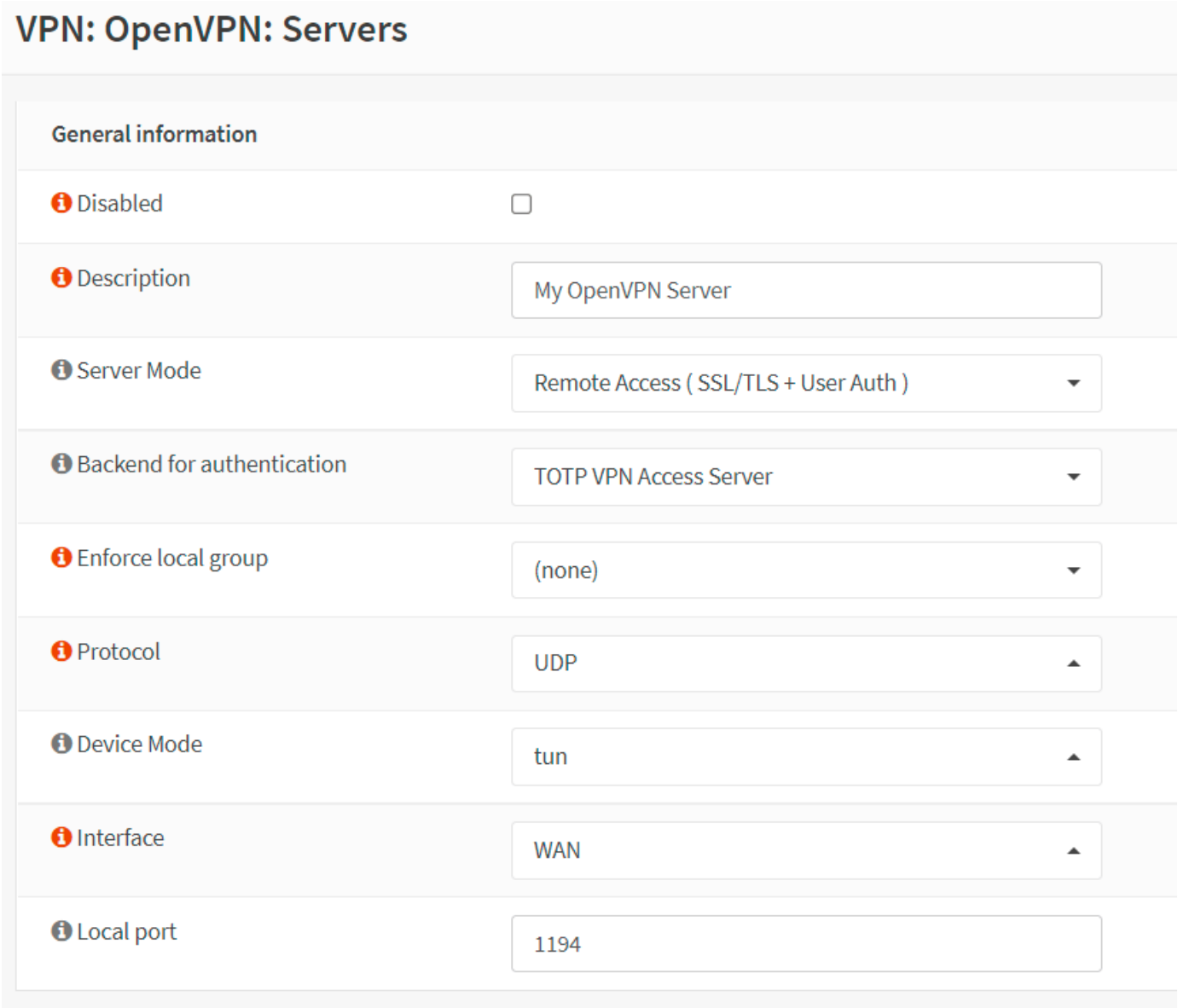

Figure 17. *Setting the General Information options for an OpenVPN server with MFA in OP*

10. Set **TLS Authentication** to `Enabled-Authentication & encryption`.
11. Check `Automatically generate a shared TLS authentication key` for the **TLS Shared Key** option.
12. Set **Peer Certificate Authority** to `OPNsenseOpenVPNCA`.
13. Set **Server Certificate** to `Open VPN Server Certificate`
14. Set **DH Parameters Length** to `4096 bit`.
15. You may set the **Encryption algorithm** to `AES-256-GCM (256-bit key, 128-bit block)`
16. Set the **Auth Digest Algorithm** to `SHA512`.
17. Set **Certificate Depth** to `One (Client+Server)`.
18. You may check the `Strict User/CN Matching` option to enforce a match between the **Common Name** of the client certificate and the username given at login for more security.

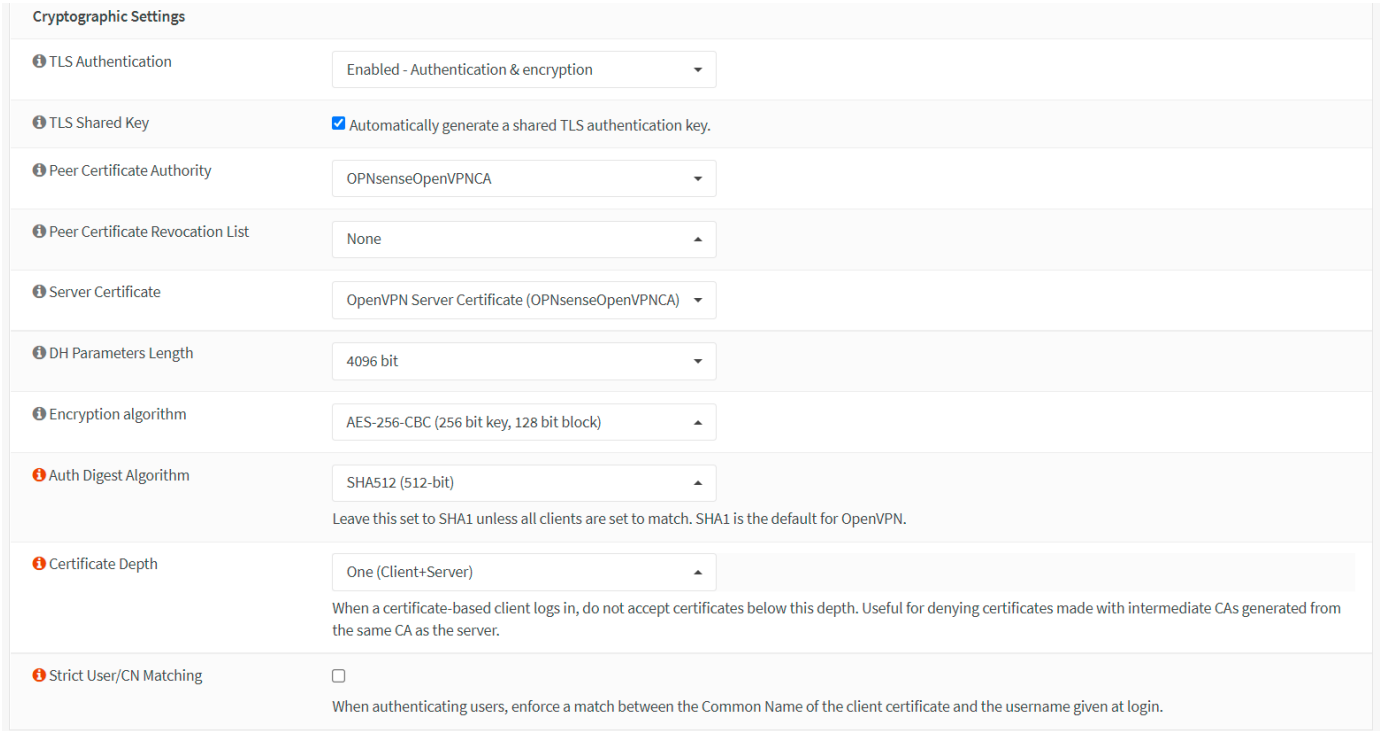

Figure 18. *Cryptographic Settings for an OpenVPN server with MFA in OPNsense*

19. Enter the IP address range in the CIDR format for the **IPv4 Tunnel Network**. This is the IP address range that will be used by your VPN clients. As your Tunnel Network, select an IP range that is not currently in use on your network. In this tutorial, we'll choose `192.168.10.0/24` as the tunnel network.
20. Select the **Redirect Gateway** option to force clients to access the Internet through your firewall. If you don't want to enable this option, you may enter your LAN address for the **IPv4 Local Network**. So that, your VPN clients are accessible from your local network, such as `10.10.10.0/24`.
21. You may set **IPv4 Remote Network** by entering the remote LAN/s to set up a `site-tc VPN`. You may leave this blank if you don't need to set up a site-to-site VPN.

22. You may set a value for the **Concurrent Connection**s option. This option specifies the *maximum* number of clients that can connect to this OpenVPN server instance *at the same time*. This is a global restriction that applies to all connected clients, not a per-user limit. The OpenVPN server will allow an unlimited number of connections to your server by default. Setting this to a reasonable value is advised, even if only for sanity purposes.
23. Select `legacy LZO algorithm with adaptive compression` for **Compression**. If OpenVPN detects that the data in the packets are not being compressed efficiently, this mode will dynamically disable compression for a period of time.
24. You may check the **Inter-client communication** option to allow communication between VPN clients connected to your OpenVPN server. Most of the time, you don't need to enable this option.
25. You may check the **Duplicate Connections** option to allow multiple concurrent connections from VPN clients using the same Common Name. Although this option is not recommended, you may need to enable it in some cases.

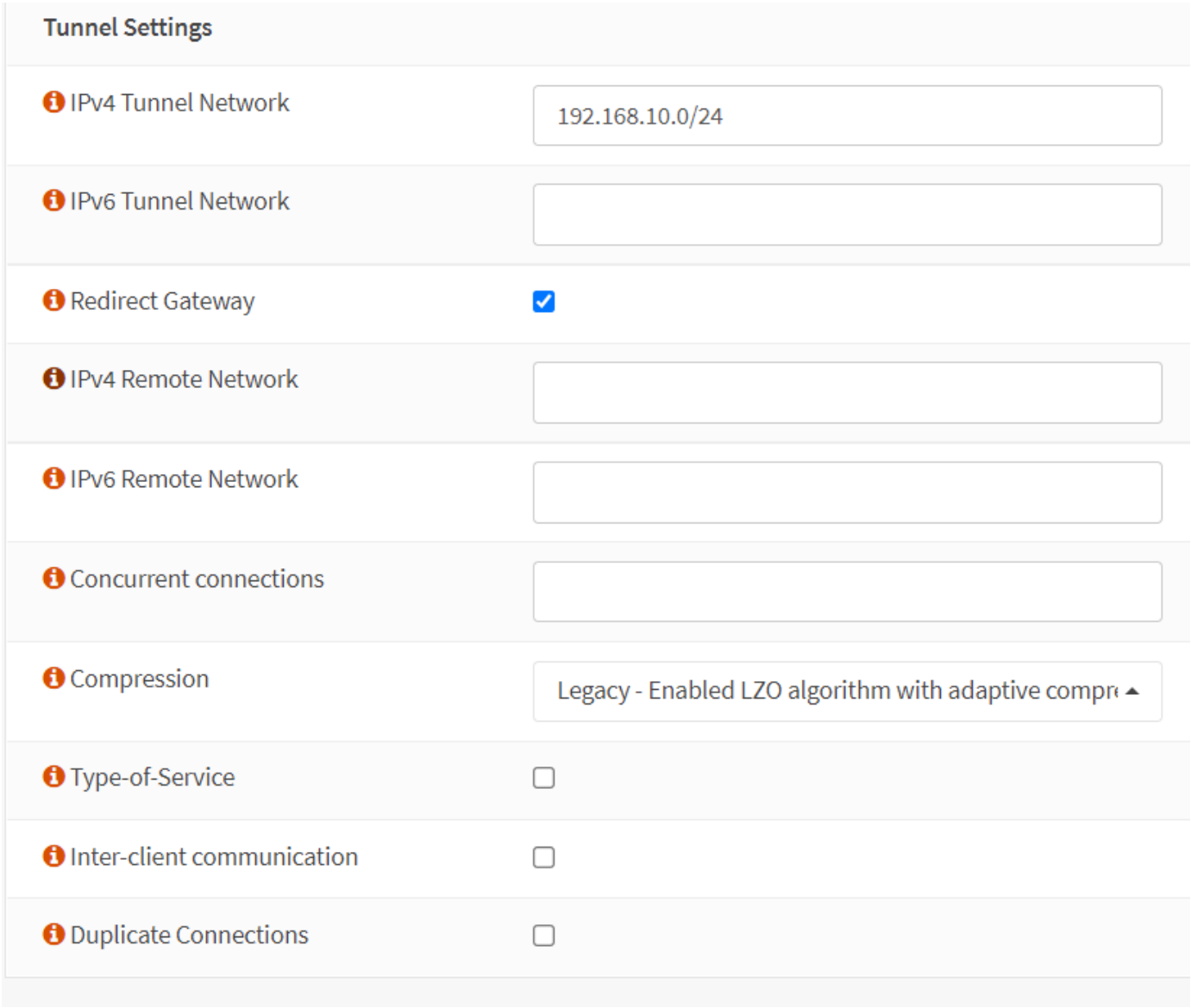

Figure 19. *Tunnel Settings for an OpenVPN server with MFA in OPNsense*

26. You may enable the **Dynamic IP** option which allows a client that is already connected to change its IP address without reconnecting.
27. Check the **Address Pool** option to provide a virtual adapter IP address to VPN clients.
28. Enable the **Topology** option so that VPN clients only receive a single IP and not an isolated IP subnet. For compatibility with older Windows OpenVPN clients, it is disabled by default.
29. If you specify a **DNS Default Domain**, this value will be used as the DNS suffix for your VPN clients. If your clients want to look up your internal hostnames without using an FQDN, this can be useful.
30. You may check **DNS Servers** and then enter DNS servers' IP addresses if you wish. If you have an internal DNS server, then you should enter its IP address here.
31. You may check the **Force DNS cache update** option to kick Windows clients into recognizing pushed DNS servers if you wish.
32. You may check the **Prevent DNS leaks** option to block DNS servers on other network adapters if you wish.
33. You may check **NTP Servers** and then enter NTP servers' IP addresses if you wish.
34. You may check **NetBIOS Options** to enable NetBIOS over TCP/IP if you wish.

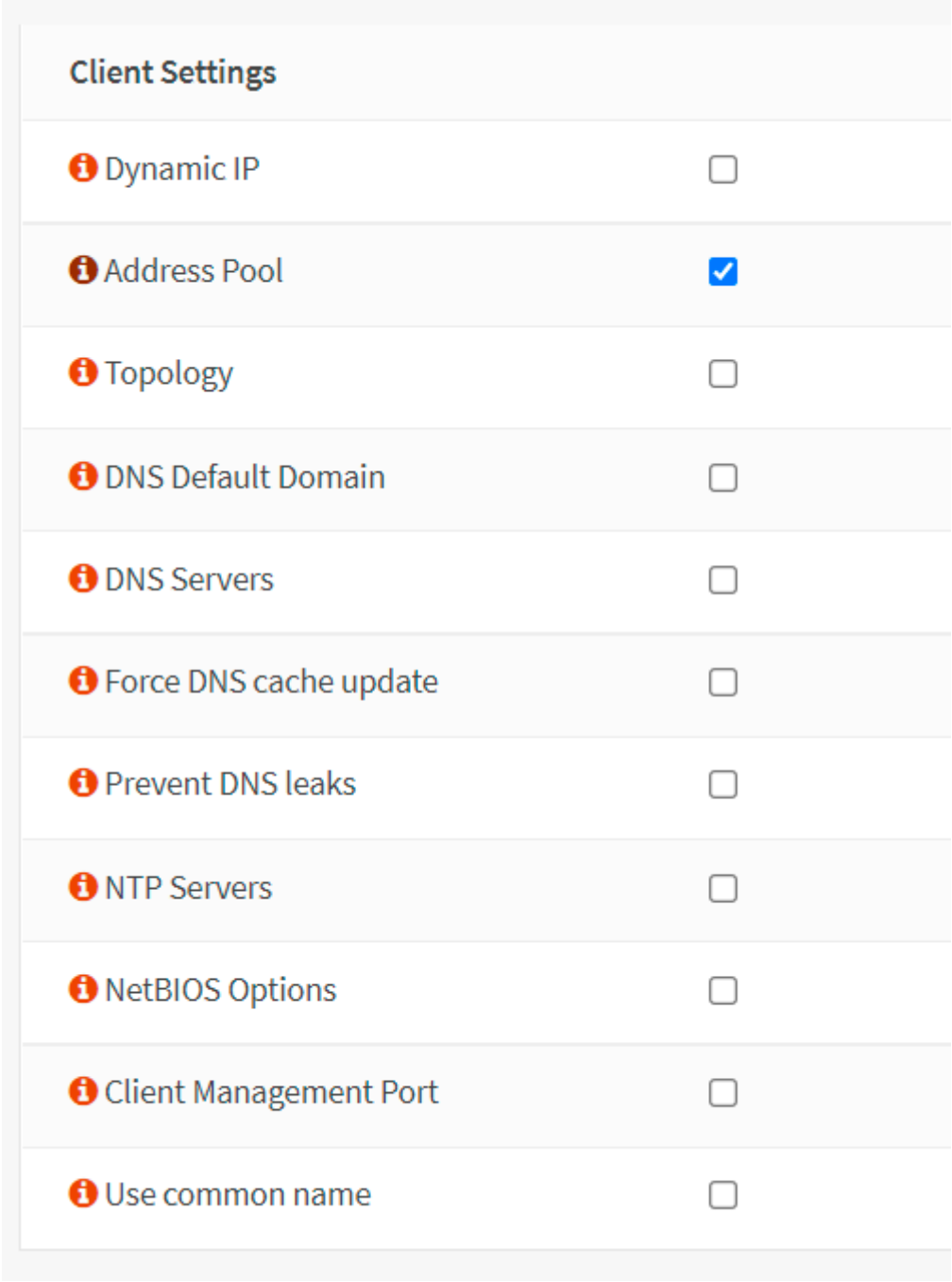

Figure 20. *Client Settings for an OpenVPN server with MFA in OPNsense*

35. Select `3` for the **Verbosity** level to show *TLS negotiations & route info*.
36. Set **Renegotiate time** to `0` to disable the renegotiate data channel key since we'll use OTP in our tutorial.
37. Leave other options as default.

> **TIP**
>
> The `Strict User/CN Matching` option is used to force the use of the same username as the certificate CN, preventing people from logging in with credentials other than the certificate name supplied. (For example, `vpnuser1` cannot log in as root.)

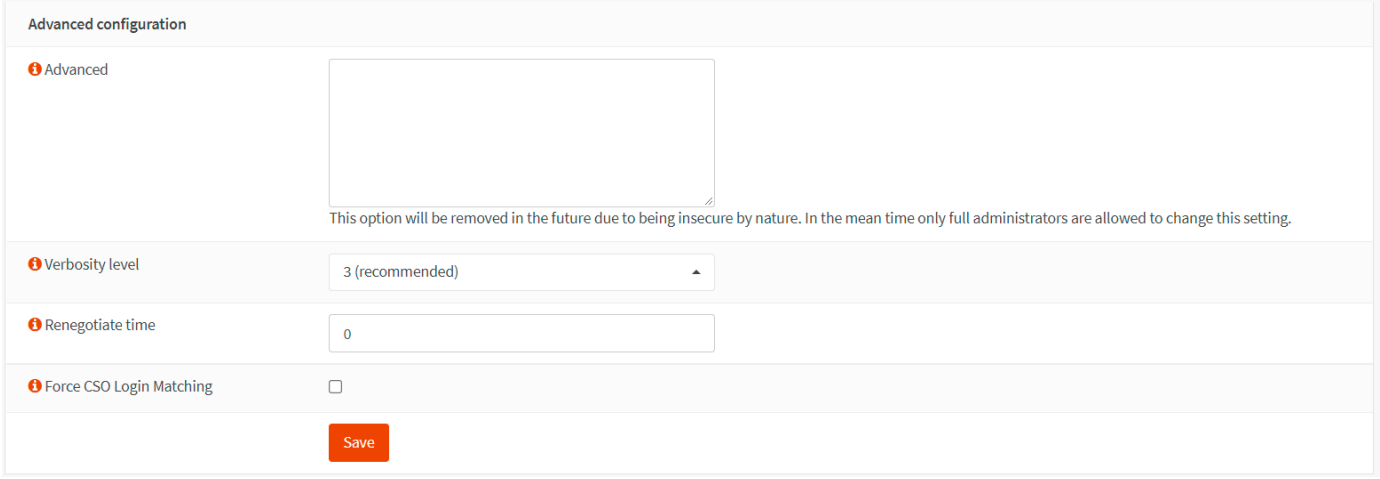

Figure 21. *Advanced configuration for an OpenVPN server with MFA in OPNsense*

38. Click `Save` at the bottom of the page to activate the settings.

You may view and manage your new VPN server on the OpenVPN servers page of the OPNsense firewall.

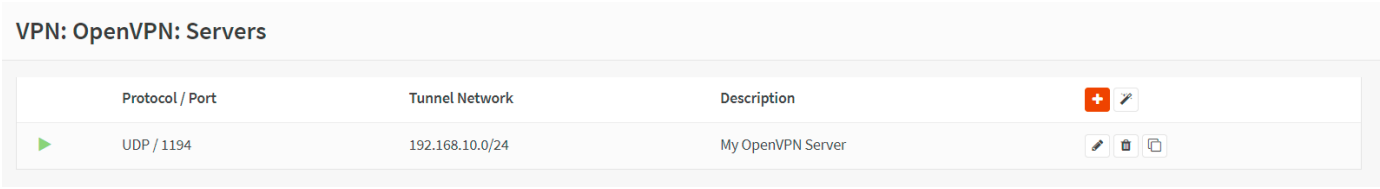

Figure 22. *OpenVPN servers in OPNsense*

6. Add Firewall Rules

By default, all traffic connecting to an OpenVPN server or flowing through VPN tunnels is forbidden. Therefore, you must define the following firewall rules in your OPNsense:

1. *Allow traffic from clients to VPN server*
2. *Allow VPN clients access to the Internet through VPN.*

1. Allow traffic from clients to VPN server

Allowing access to the OpenVPN server port, default UDP/1194, on the WAN interface is required to allow SSL VPN client connections. You should define a firewall rule that allows VPN clients to access to your OpenVPN server.

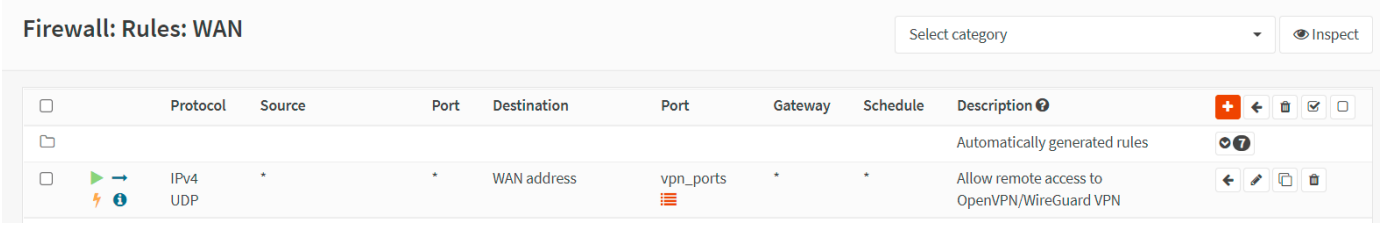

Figure 23. *OpenVPN servers access rule in OPNsense*

2. Allow VPN clients access to Internet through VPN

To allow VPN clients to the internet through the VPN tunnel, you may follow the next steps given below:

1. Navigate to the `Firewall` > `Rules` > `OpenVPN` in your OPNsense web UI.

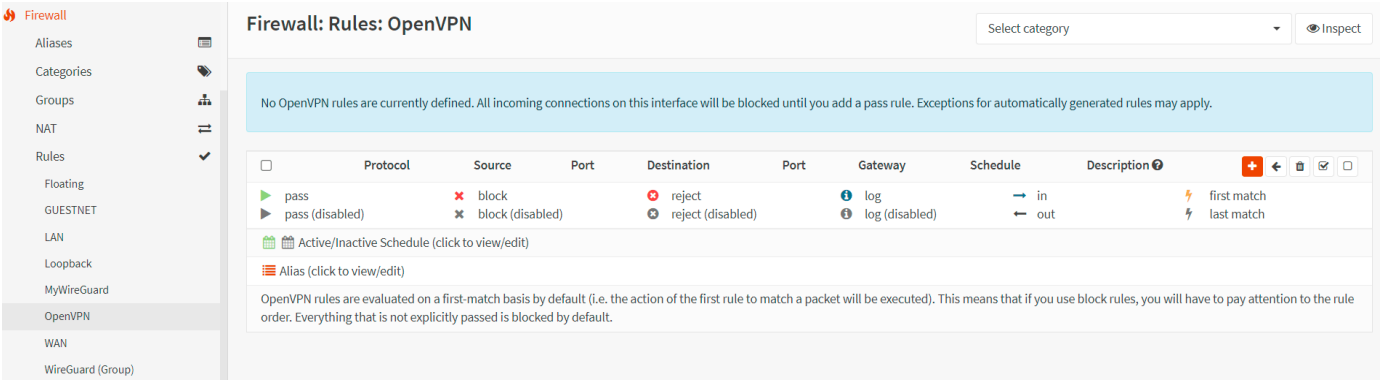

Figure 24. *OpenVPN interface firewall rules in OPNsense*

2. Click on the add button with the `+` icon at the top right of the page.
3. Set **Action** to `Pass`.
4. Set **Interface** to `OpenVPN`.
5. Set **Direction** to `in`.
6. Select `Single Host or Network` for the **Source** and set VPN IP address range such as `192.168.10.0/24`.

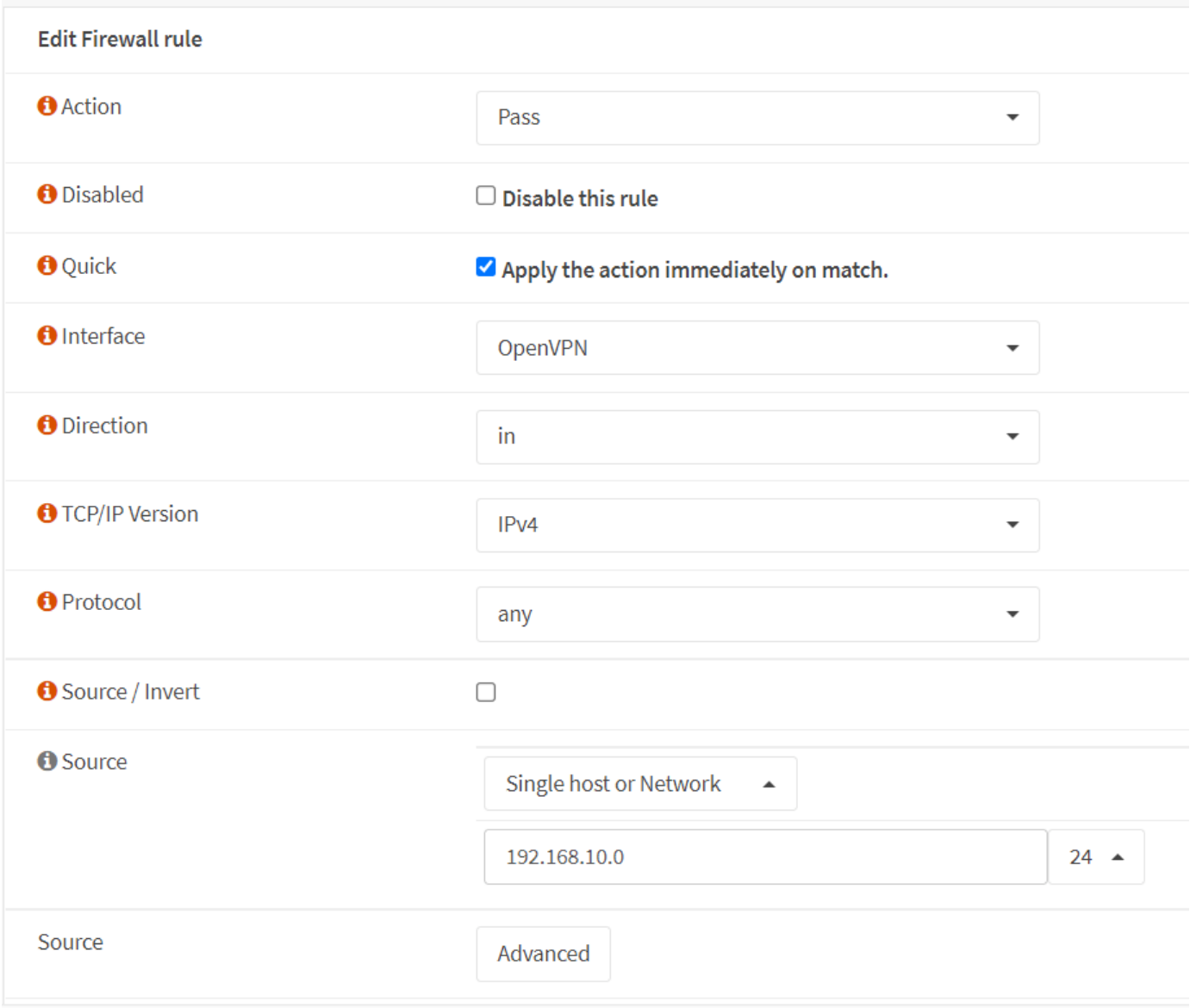

Figure 25. *Defining OpenVPN firewall rules in OPNsense-1*

7. Select `any` for the **Destination**.
8. You may type `VPN Rules` in the **Category** field.
9. Fill in the **Description** field, like `Allow VPN clients access`.
10. You may leave other settings as default.

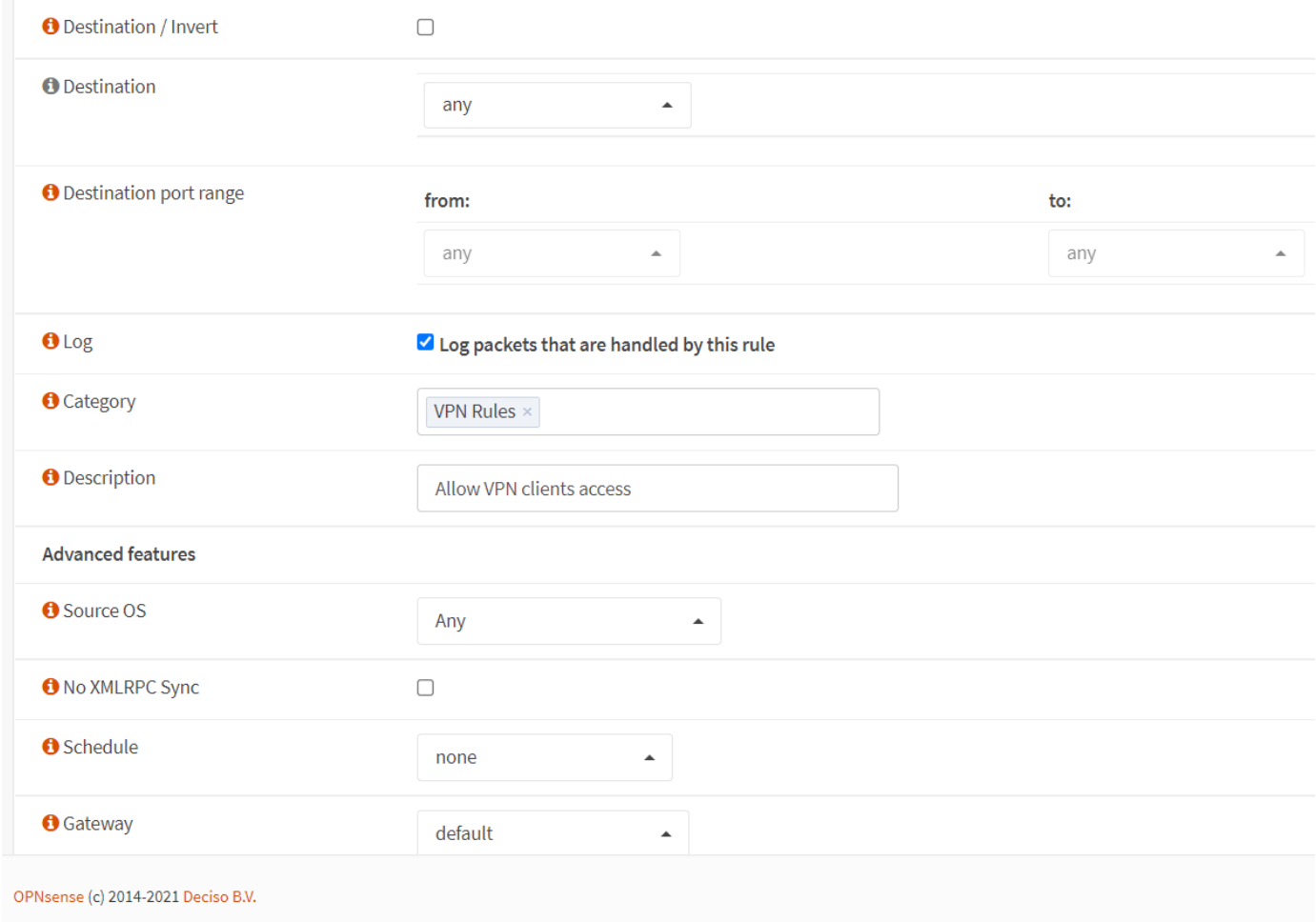

Figure 26. *Defining OpenVPN firewall rules in OPNsense-2*

11. Click the `Save` button at the bottom of the page to save the rule.
12. Click `Apply Changes` to activate the new firewall rule.

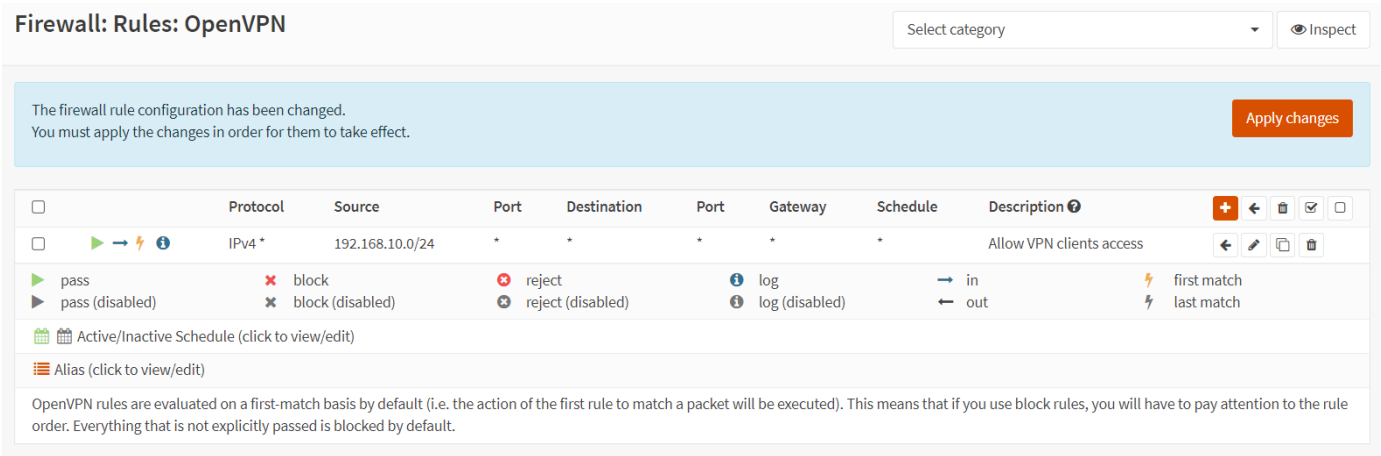

Figure 27. *Activating OpenVPN firewall rules in OPNsense*

The firewall configuration for the OpenVPN tunnel connection is complete. You must now export the configuration files so that they can be fed into the OpenVPN client that the user will install on his or her device.

7. Export OpenVPN Client

You can easily export the OpenVPN client configuration file as you need. To download the OpenVPN Client Configuration, you may follow the next steps:

1. Navigate to the `VPN` > `OpenVPN` > `Client Export` in your OPNsense web UI.
2. Select the newly created VPN server from the list, such as `My OpenVPN Server UDP:1194`, for the **Remote Access Server**.
3. Select the `File only` for the **Export Type**. Since you can easily import this text-based configuration file into OpenVPN client applications on different platforms, such as Windows, macOS, Android, and iOS.

> **TIP**
>
> You may also select `Archie` for the Export Type, if your VPN client runs in Windows or macOS. In this case, `Archie` file, such as `My_OpenVPN_Server_vpnuser1.zip` includes a directory that contains the configuration file (`.ovpn`), user certificate(`.p12`), and tls key(`.key`).

4. Leave other settings as default. For most cases, `Hostname` must be the public IP address of your OPNsense firewall and `Port` must be the port number you have set for the VPN service, default 1194.

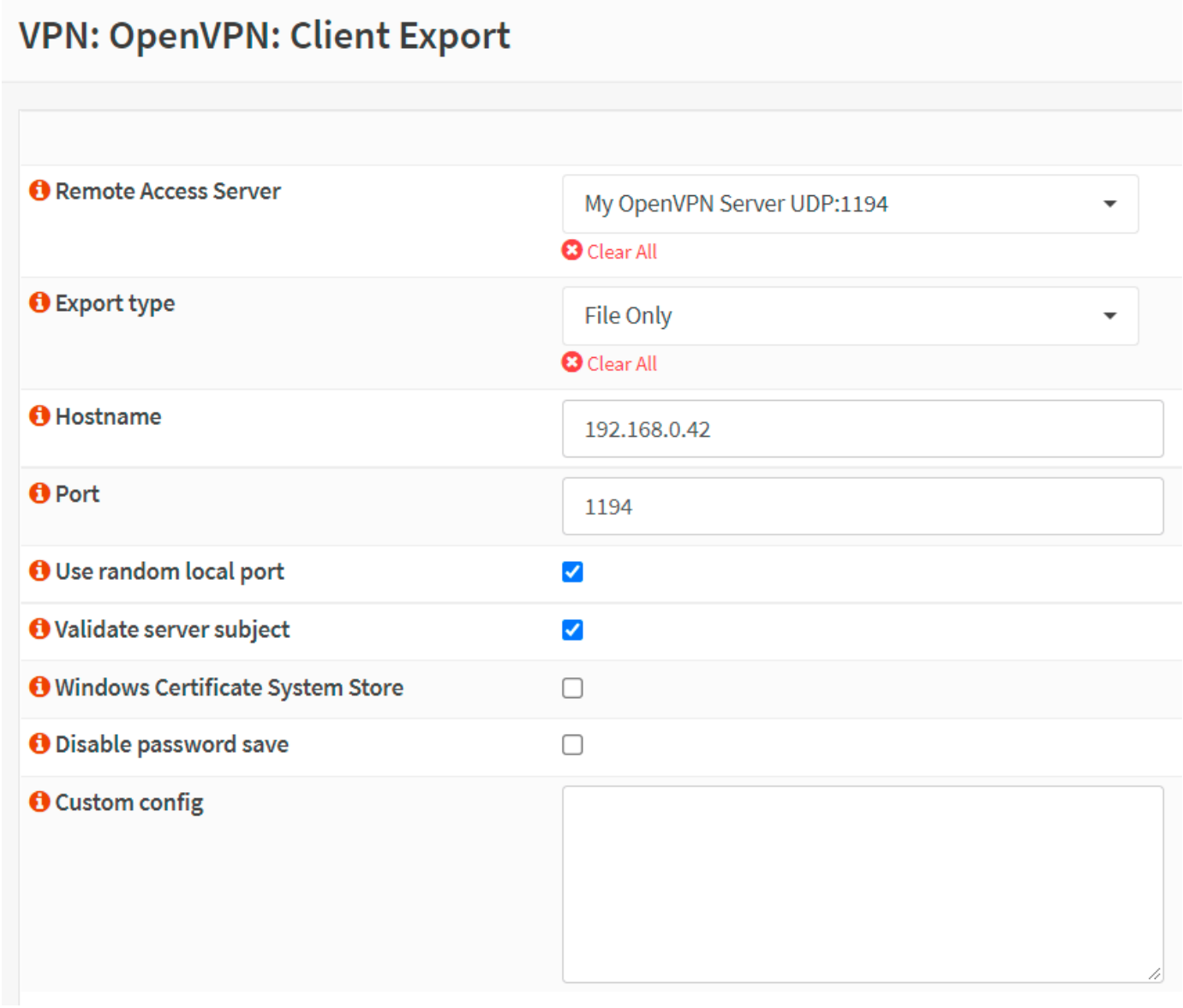

Figure 28. *Exporting OpenVPN client in OPNsense*

5. Scroll down to the bottom of the page. The list of users you have configured is in the `Accounts / certificates` pane, and the download button with a small cloud icon is on the right side of the corresponding row.
6. Click on the download button next to the VPN client user, `vpnuser1`.

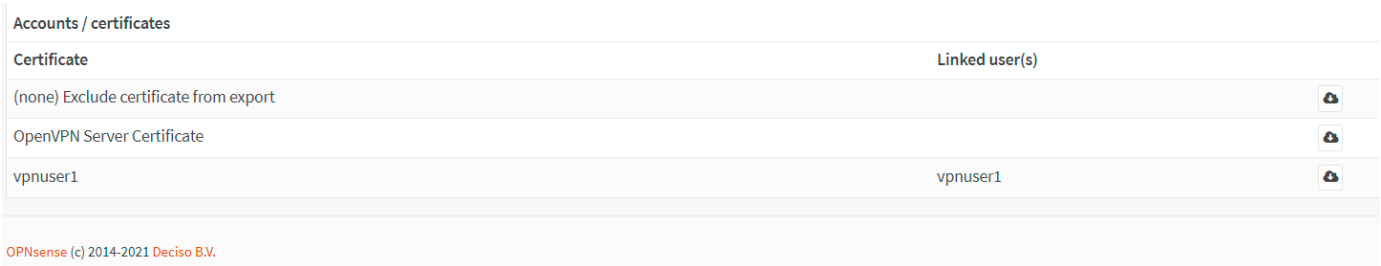

Figure 29. *Downloading OpenVPN client in OPNsense*

After exporting the OpenVPN client configuration file, such as `My_OpenVPN_Server_vpnuser1.ovpn`, you should send it to the user. So that, the user cai

import it into the OpenVPN client app in his/her device to connect to the LAN through the OpenVPN tunnel.

How do I connect to OPNsense OpenVPN?

In this section, we will explain how to connect the OPNsense OpenVPN server with MFA using a Windows PC or an Android device. We assume that you've already downloaded and sent the OpenVPN client configuration file to the VPN user.

Connecting from a Windows PC client

You can easily connect your OPNsense OpenVPN server with MFA from a remote Windows client by following the instructions given below:

1. Download the latest OpenVPN GUI installer file from the `openvpn.net` official website.
2. Install the OpenVPN installer, leaving everything at the default settings and agreeing to everything with `Yes`. Installing a TAP network driver may be required; do so if prompted.
3. After finishing OpenVPN installation on a Windows client machine, A small monitor icon with a locker on it appears in your taskbar. Right-click on it and select `Import file` to import the client configuration file.

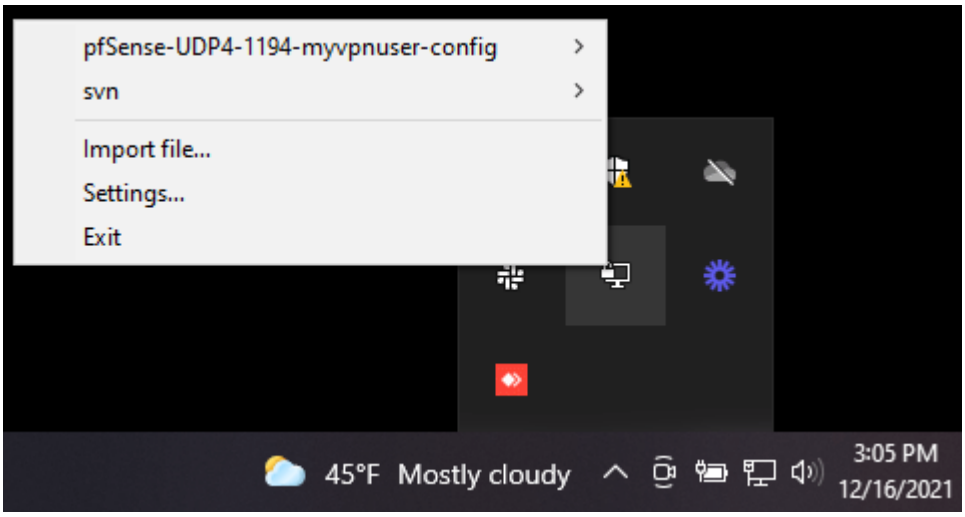

Figure 30. *Importing OpenVPN client configuration on Windows 10*

> **CAUTION**
>
> If you've downloaded an `Archie` file, such as `My_OpenVPN_Server_vpnuser1.zip` in the previous section, you must extract it into the OpenVPN config directory, such as `C:\Users\Administrator\OpenVPN\config`, for import.

4. After importing the OpenVPN client configuration successfully, right-click on the OpenVPN icon on the taskbar and select the newly imported configuration file.

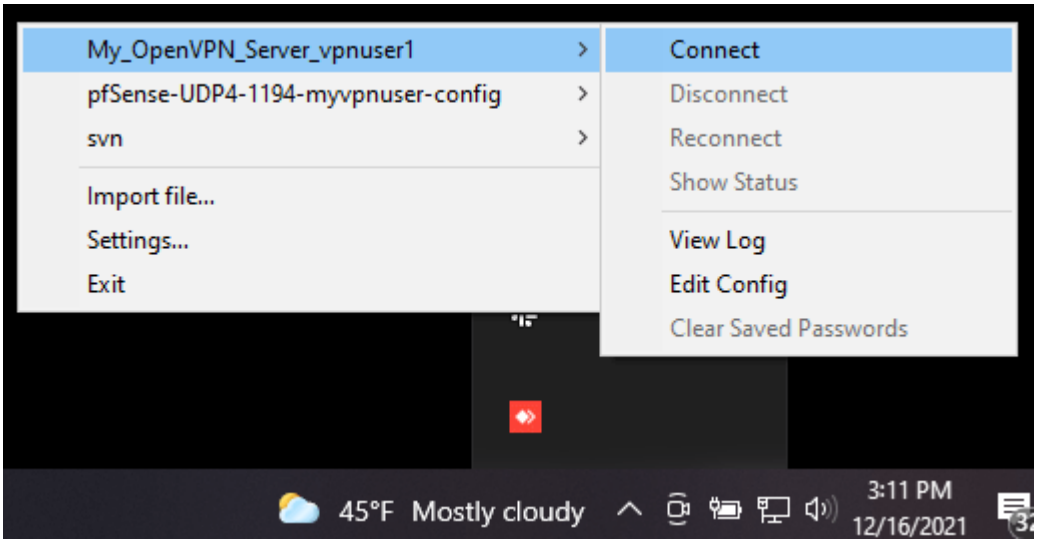

Figure 31. *Connecting to the OPNsense OpenVPN server from Windows 10 client*

5. Click `Connect` to start the VPN connection.
6. Enter your `VPN Username`.
7. Launch the Google Authenticator application on your mobile device.
8. Grab the token for your VPN account, such as `vpnuser1`.

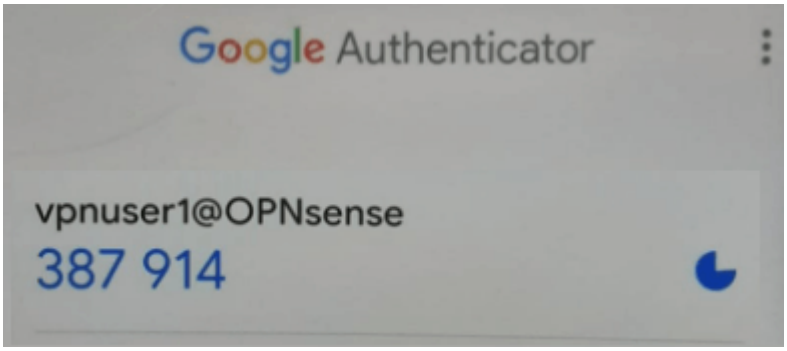

Figure 32. *Token generated by Google Authenticator for OpenVPN client user*

9. Return back to the OpenVPN GUI in your Windows PC.
10. Fill in the `Password` field using both the token and OPNsense local user password you defined.

> **INFO**
>
> Remember, you need to enter the token before or after your password (depending on your configuration). For example, if the Google Authenticator token is `387914` and your local

password is `MyPassword`, then you should enter `387914MyPassword` in the Password field of the OpenVPN GUI application.

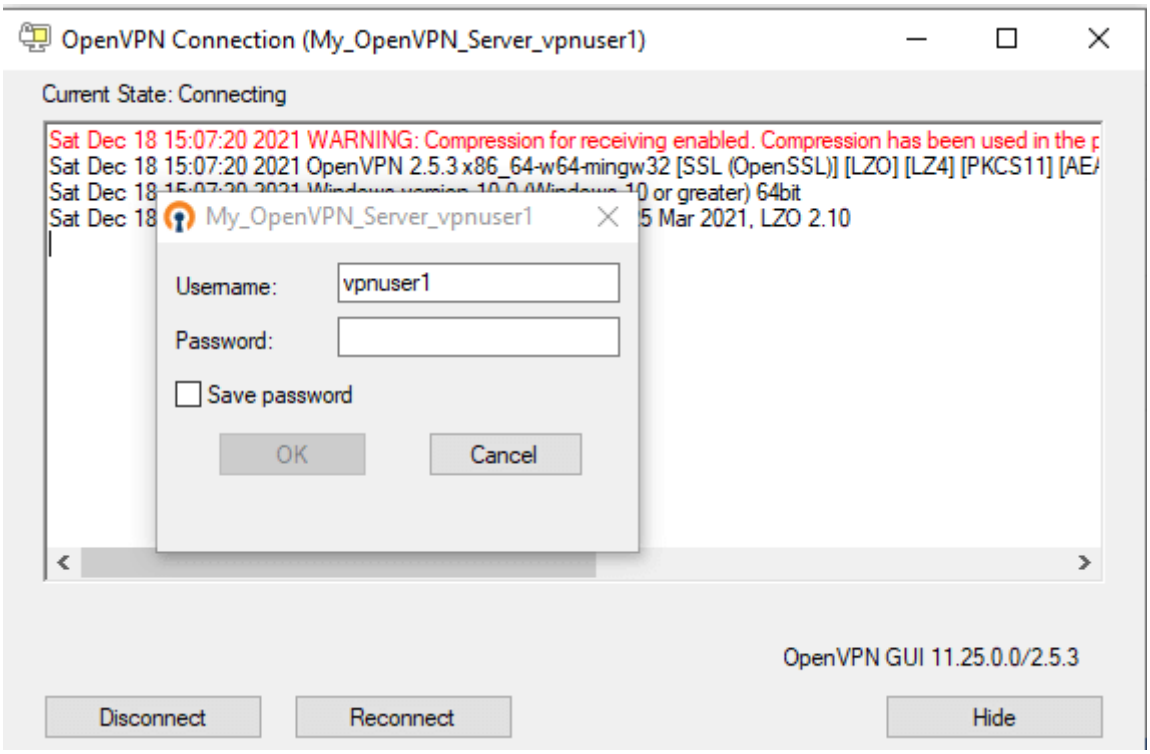

Figure 33. *OpenVPN client authentication with MFA on Windows 10*

11. Click on `OK` to connect.

You will be notified on the bottom right of the screen and the OpenVPN icon on the taskbar will change to `green` when the connection is successful.

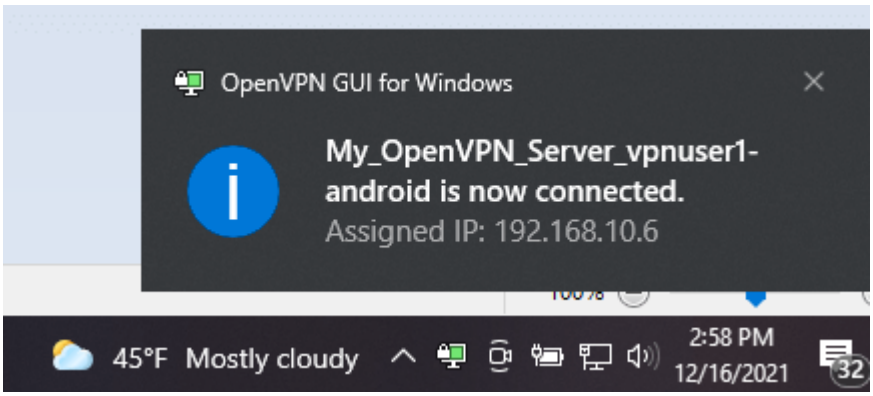

Figure 34. *OpenVPN Windows 10 client connected with MFA*

Connecting from an Android Device

You can easily connect your OPNsense OpenVPN server from an Android client by following the instructions given below:

1. Install the official OpenVPN application from the Google Play Store on your Android device.

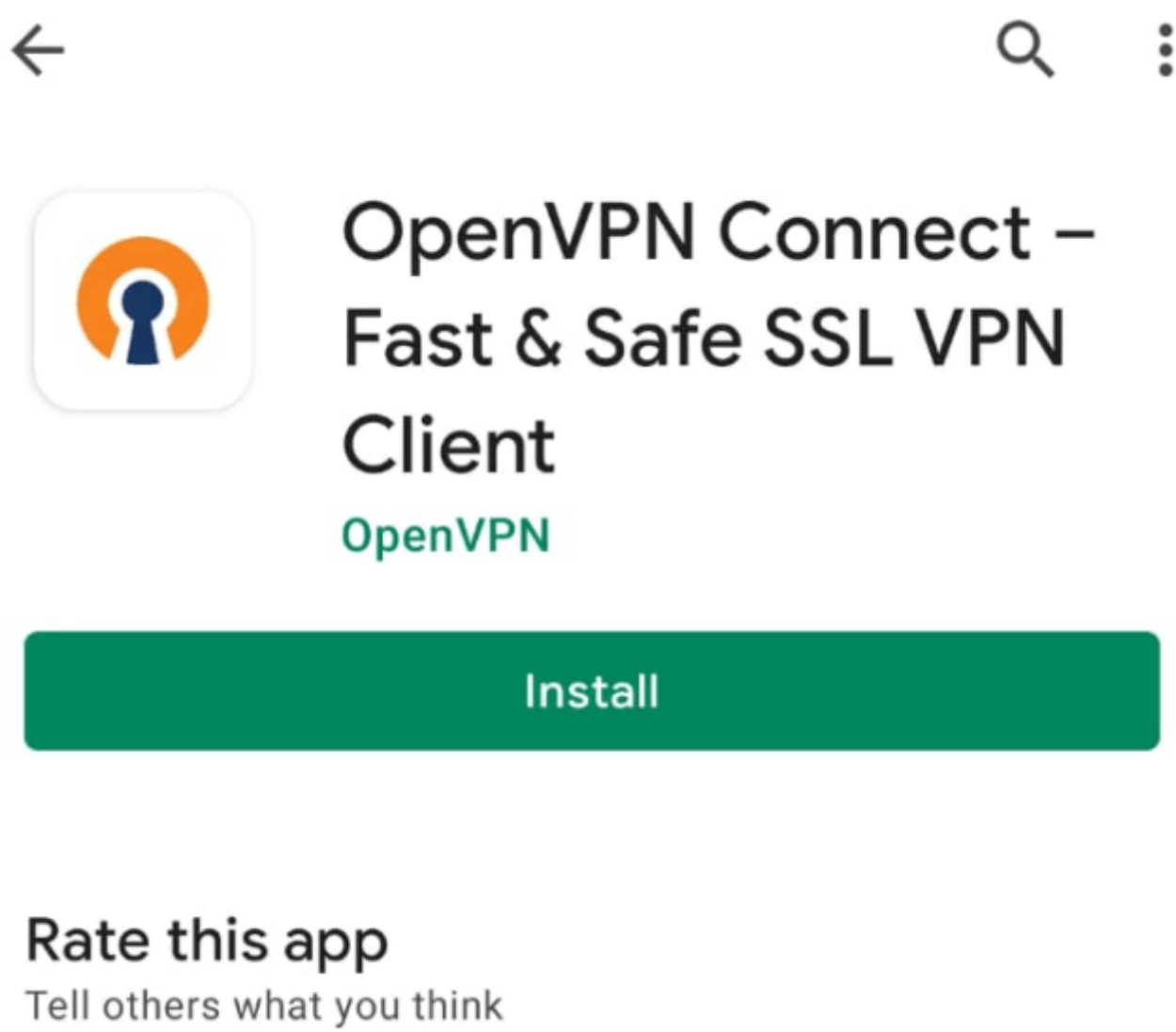

Figure 35. *Installing OpenVPN Connect client on an Android*

2. Launch the application and import the configuration file by selecting the file under the `FILE` tab `Import Profile` menu.

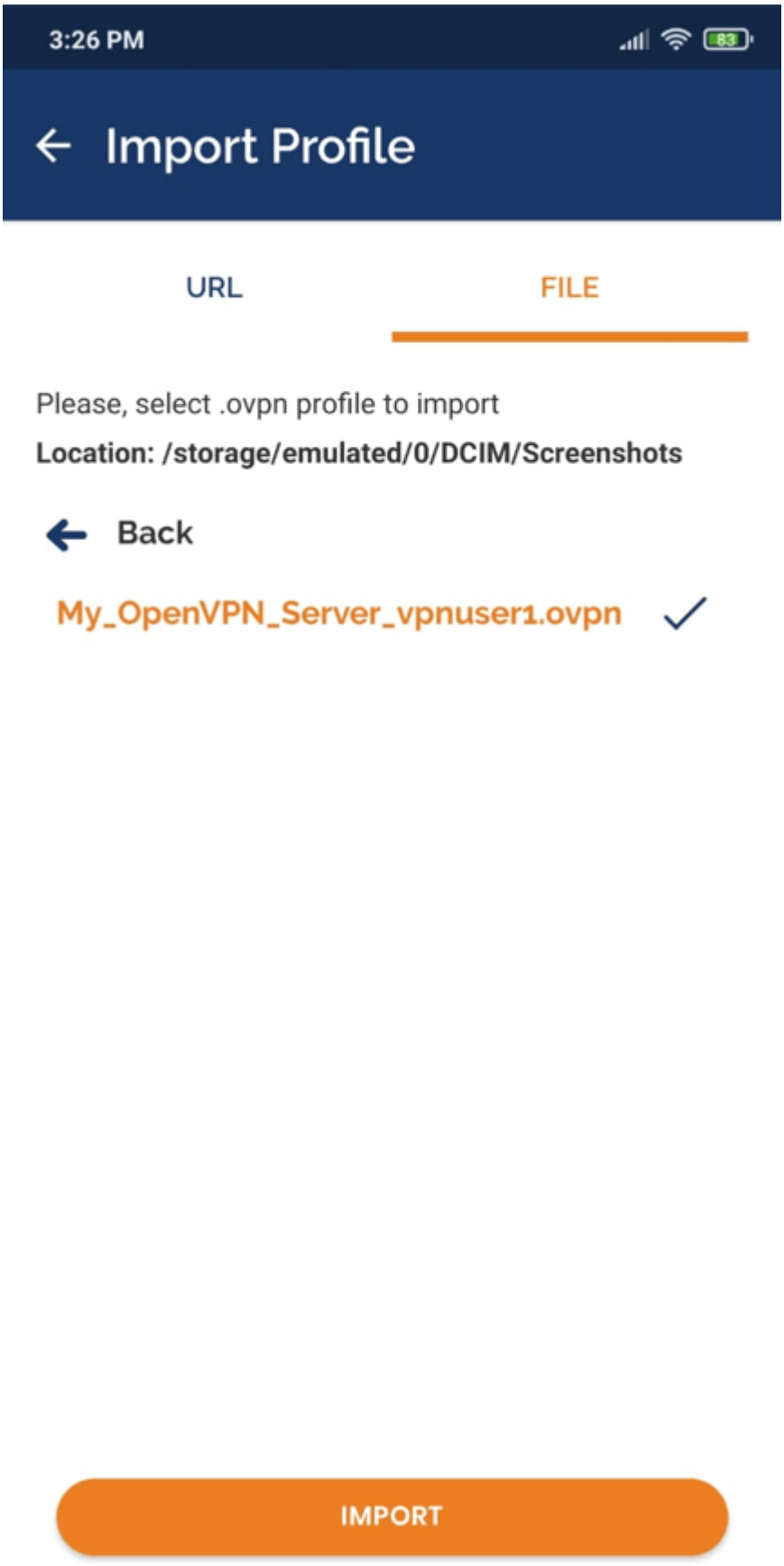

Figure 36. *Importing OpenVPN client configuration on an Android*

5. Enter the VPN user name.

6. Selecting the `Connect after import` option.

7. Tap on the `ADD` button.

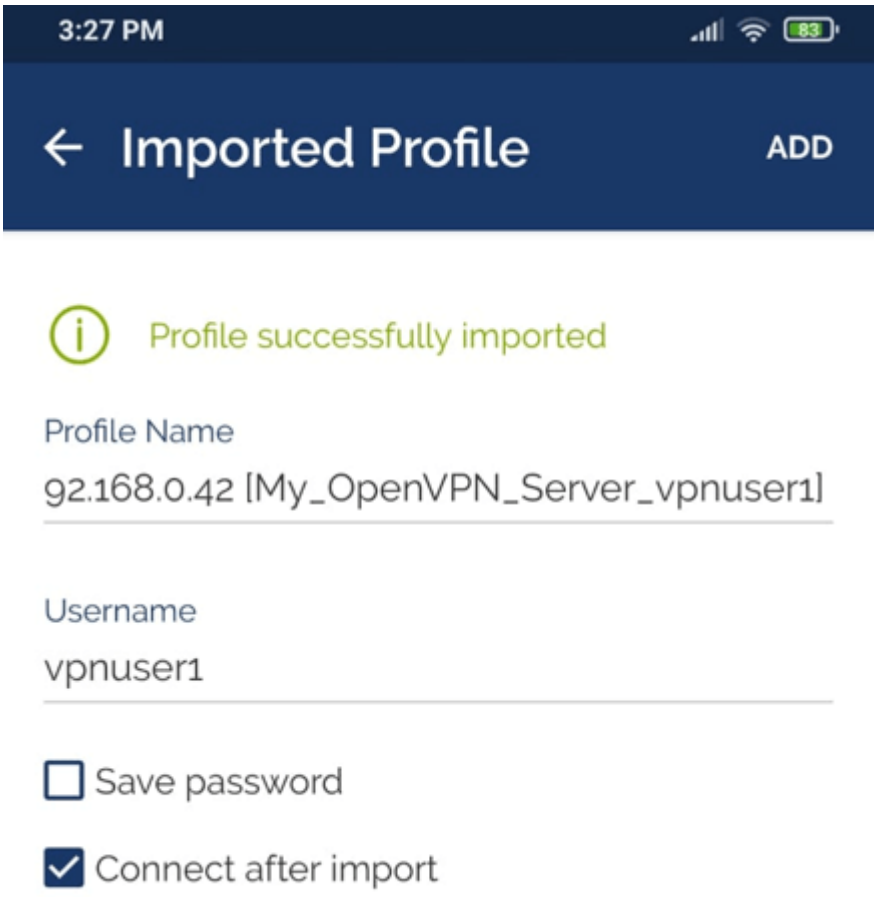

Figure 37. *Importing OpenVPN client configuration on an Android-2*

8. Launch the Google Authenticator application on your mobile device.

9. Grab the token for your VPN account, such as `vpnuser1`.

11. Enter the VPN password using both the token and OPNsense local user password you defined to connect to the VPN server. Then, tap on `OK`.

> **INFO**
>
> Remember, you need to enter the token before or after your password (depending on your configuration). For example, if the Google Authenticator token is `085256` and your local password is `MyPassword`, then you should enter `085256MyPassword` in the Password field of the OpenVPN GUI application.

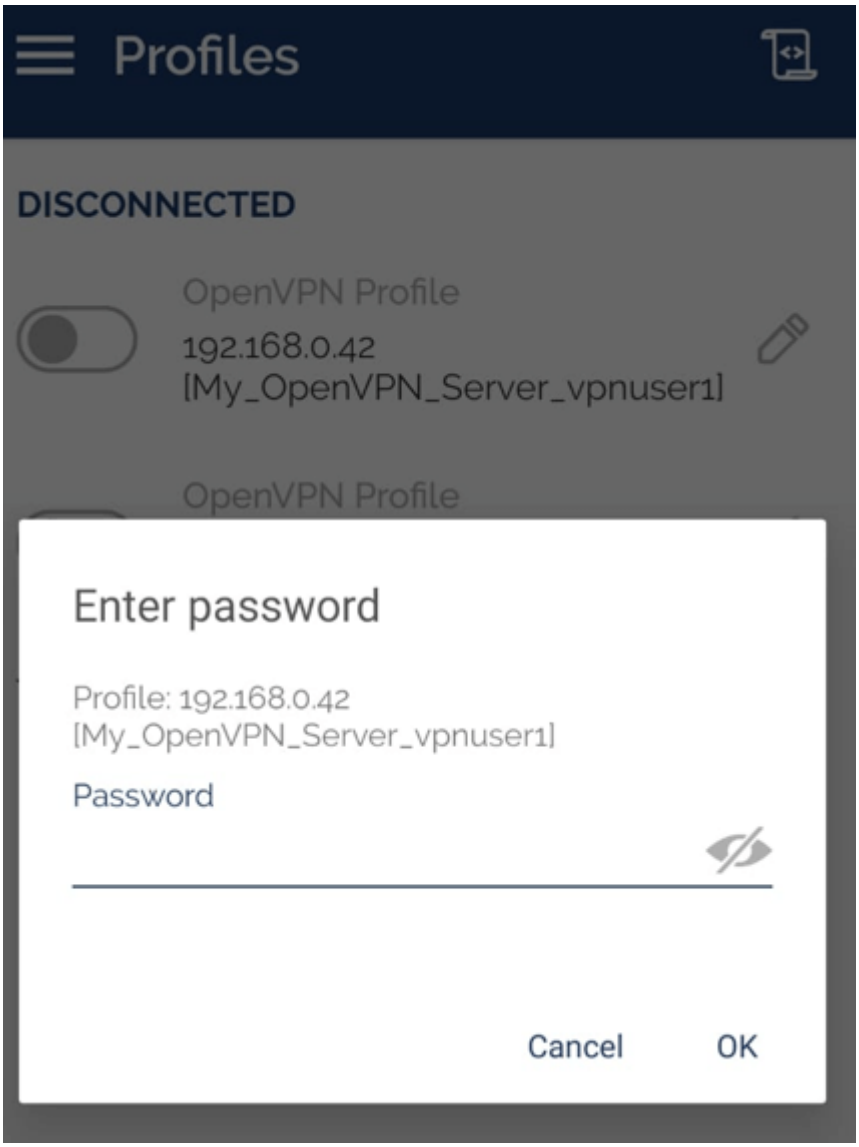

Figure 38. *Entering VPN password for OpenVPN connection in Android device*

12. Now, you should be connected to a VPN server from your Android device.

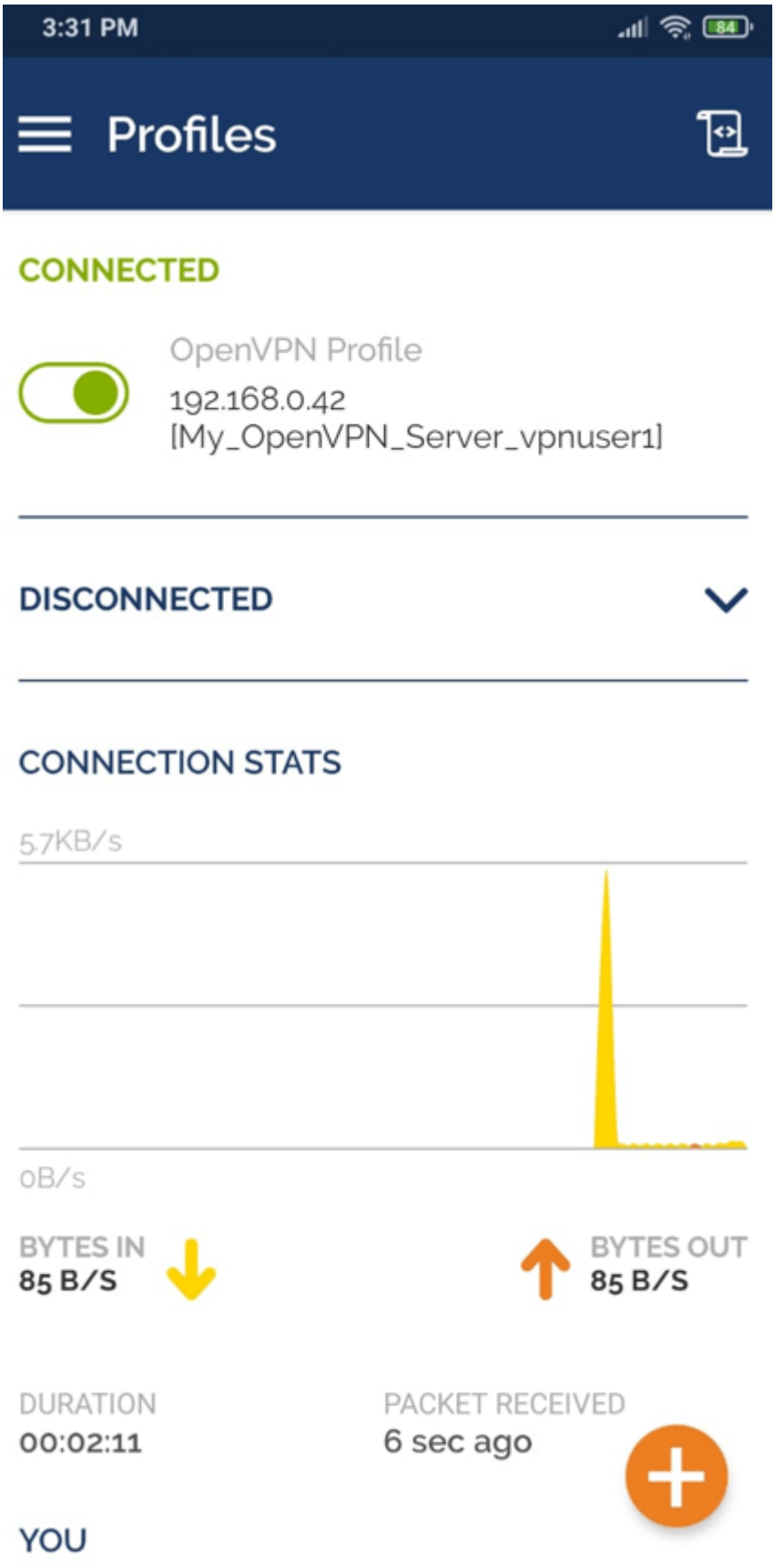

Figure 39. *Connected OpenVPN Client on Android*

13. To disconnect from the VPN, you may tap on the green toggle button at the top.

Verifying the VPN connection

OpenVPN server configuration and client configurations are completed. To test the configurations, you may follow the steps given below.

1. Viewing VPN connections on OPNsense: Navigate to the `VPN` -> `OpenVPN` > `Connection Status` in your OPNsense web UI. You should be able to see information about the connected VPN clients. The following details are displayed:

- Vpn username,
- the real IP address of the connected client,
- the VPN IP address of the connected client,
- the time since the last connection,
- the amount of data transferred and received.
- Status of the OpenVPN server

Also, you may perform the following task:

- Restart or stop the OpenVPN service by using the Action buttons at the upper right corner of the page.
- Kill the VPN client connection by using the `X` button at the end of the VPN client connection.

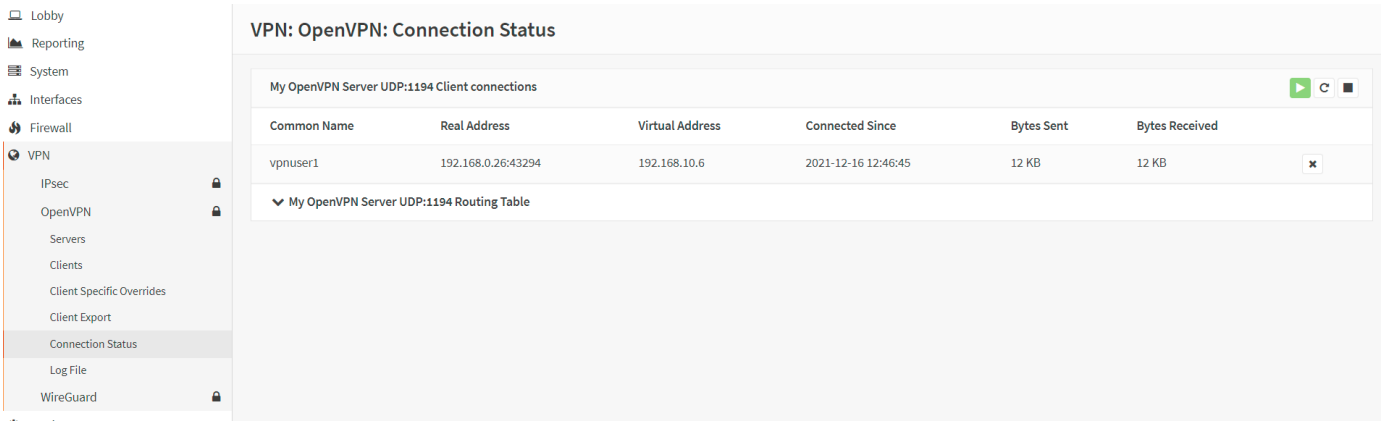

Figure 40. *OpenVPN status in OPNsense*

2. Ping Test: You should be able to successfully ping your OpenVPN server from the client and vice versa:

```
ping 192.168.10.1
```

3. IP Control

On your client machine go to this website `https://www.whatismyip.com` to check your public IP address. If your OpenVPN tunnel works well, you should see your VPN server's public IP address instead of your client computer's public IP address in the browser.

4. Traceroute Test

You should see the OpenVPN Server VPN IP address in the traceroute command output.

5. Viewing Firewall Logs

You should see that your VPN clients with 192.168.10.X IP addresses are accessing the internet via VPN tunnel interface, such as `ovpns` in firewall live view by navigating to `Firewall` > `Log Files` > `Live View` and filtering src by VPN client IP, such as `192.168.10.6`.

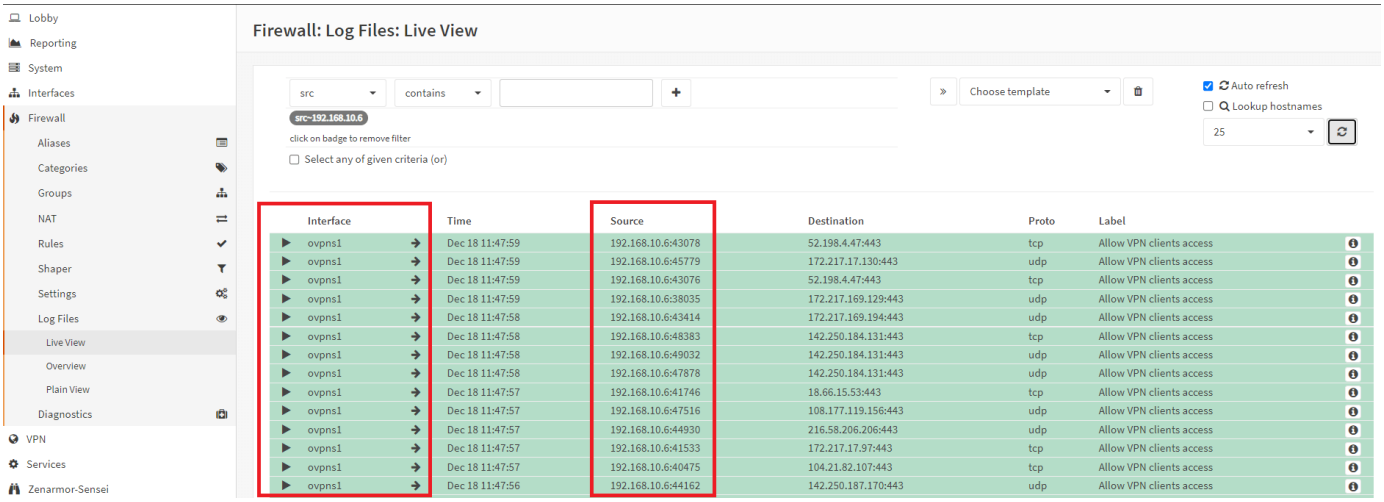

Figure 41. *Viewing firewall logs for OpenVPN client internet traffic in OPNsense*