TOTP Authentication in OPNSense

Time based One Time Password authentication Wikipedia has become more commonly used in Multi-Factor Authentication (MFA) for additional security in various areas. Generally used by authenticators such as FreeOTP, Microsoft Authenticator, Google Authenticator and many more. My preference is FreeOTP due to the ability to back up the configuration without having to use a proprietary system.

OPNSense has supported TOTP for several years, and we will discuss how to set it up. I will be using OPNSense v25.01.12, and offering a script we wrote to deploy the QR Codes most authenticators prefer.

We are mainly focused on using MFA, using TOTP with an authentication for Road Warrior VPN access.

Set up authentication in OPNSense

1. Log into your OPNSense router as a user with administrative permissions
2. Go to System | Access | Users
    1. For each user
        1. Edit Account
        2. Scroll down to OTP seed
        3. Click “Show” (older versions did not require this step)
        4. Click the gear box to (re)generate an OTP Seed
        5. Click Save
3. Go to System | Access | Users
    1. Select a user you know the password to
    2. Click “Show” on the OTP seed
    3. Scan the displayed QR Code into the authenticator app on your device
4. Go to System | Access | Servers
    1. Click plus sign to create new server
    2. Descriptive Name: Something that readily identifies this, such as TOTP
    3. Type: Local+Timebased One Time Password
    4. Token length: 6 (Microsoft compatible)
    5. Time Window: 30
        1. this is the default, but I like to see what the value is, so I enter it
        2. This defines what the window is. So, if your authenticator changes numbers in the middle of you typing it in, this defines if you have to reenter it
    6. Grace period: 10 (same as above, it is the default)
        1. this is the default, but I like to see what the value is, so I enter it
        2. Again, this is kind of like Time Window, but appears to be the difference in time between your authenticator and the server. Increasing this is less secure, but allows for an easier match
    7. Click Save
5. Go to System | Access | Tester
    1. Authentication Server: Select the one you just created
    2. Username: enter the username for an account
    3. Get a code from your authenticator
    4. Password: ######password

    1. ###### is the six (or eight, if you chose that) digit code given by the authenticator
    2. password is the normal password
5. Click Test

Implement TOTP in test mode

Assuming all is good, you have set up authentication. Now, you need to implement it.

1. Go to System | Settings | Administration
2. Near bottom, set Server to both your Local Database and the one you created earlier
3. (Optional) Set User OTP seed to the groups who should be able to request a new OTP seed
4. Click Save

Attempt to log in from a second session. If it all works, you are now authenticating with and without TOTP. Try logging in with just the password, and with the TOTP Authenticator token preceding the password (######*password*)

Full Testing

The QR Code is sensitive information. Anyone with access to the OTP Seed can use any Authenticator app to calculate the correct TOTP code. Treat this as the same level of sensitivity as you would passwords.

Ensure all of your users have their TOTP Authenticator working. There is no simple way I have found to get the QR Code to everyone. For just a few people, you can simply go to System | Access | Users, right click on their QR Code and put it where they can scan it into their Authenticator app.

For larger numbers of end users, I wrote a pair of scripts that will scan an OPNSense configuration file and create the QR Codes for each user. The user accesses the web page, enters their OPNSense username and password, and the QR Code is displayed for them.

Be aware of the security concerns if you use this script. Read the README.md file. The scripts can be downloaded via Subversion at

```
svn co http://svn.dailydata.net/svn/web_pages/trunk/totp_opnsense
```

The README.md file contains full instructions on usage.

Deployment

Warning: Once this step is done, you will not be able to access VPN or the WebUI without TOTP Authentication. You will, however, be able to ssh into the router and recover the

previous configuration file.

To deploy, simply remove (uncheck) Local Database for the Authentication Server.

1. Open System | Settings | Administration
2. Scroll to Authentication | Server
3. Click the server dropdown
4. uncheck *Local Database*
5. Click Save

Usage

Some VPN clients have configurations for TOTP, but each is different. All it does is prepend the TOTP code you enter to the password, so if your client does not have a separate field, you can simply prepend the six digit TOTP to your normal password. Once I have tested more, I may update this document for various OpenVPN clients.