Two Factor Authentication at its Best Using OpenVPN

OpenVPN is a simple and true VPN solution. It is secure and simply configurable. You can install and run this software without relying on any third party tokens. The fact that it's open source and free really makes it stand out though. OpenVPN can be a little complicated to configure the first time you try, but once you get your configuration worked out, it's a pleasure to use. Once you have the software running, it's possible to seamlessly perform a great number of tasks.

For the purposes of this article I am going to demonstrate how to set up OpenVPN on a typical network. The below configuration will give your client PCs a secure access to your servers anywhere. The info contained in this tutorial will be aimed at Windows users.

Installing OpenVPN:

First, download the install file from <http://openvpn.se/download.html>(openvpn-2.0.5-gui-1.0.3-install.exe). This is the GUI version of OpenVPN. It's basically a handy OpenVPN with a minimal graphic interface that is accessible from the system tray.

Install it on the computer that is going to be your OpenVPN server first. This computer is going to need to be turned on and running OpenVPN at all times that you wish to have your virtual network/server accessible.

If you have any previous versions of OpenVPN installed, then shut down any running instance of it before installing.

Run the install program. During the installation, I recommend leaving all the options on default. All the instructions below assume that you have installed the program in the default directory. At the end of the install you may need to reboot the machine.

Creating certificates:

After rebooting you need to configure the OpenVPN files and create the necessary certificates on your server using the command prompt and a text editor like Notepad.

Go to Start - Run - and type **cmd** to open the command prompt.

Then, enter the command below to move to the correct directory:

```
cd C:\Program Files\OpenVPN\easy-rsa
```

Then, type this to run the batch file that will copy the configuration files:

```
init-config
```

Now, open the file **vars.bat** in a text editor. It should be located here: C:\Program Files\OpenVPN\easy-rsa\
You should change the values of the following variables at the bottom of the file with your requirements KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, and KEY_EMAIL. Make sure that none of these parameters are blank.

Back at the command prompt enter the following commands in order:

```
vars
```

```
clean-all
```

```
build-ca
```

When you run 'build-ca' you will be prompted for few entries. You can simply hit 'Enter' to accept the default values taken from the vars.bat file you customized. The only parameter that must be entered is the Common Name. Enter the name of your VPN Server for this entry. An example would be MyServer.

Here you are ready with your Certificate Authority, who is going to sign all of your certificates.

Now let's create the server certificates for that enter the following to generate a certificate and private key for the server:

```
build-key-server server
```

Make sure you enter **server** for the Common Name when asked by wizard. The rest of the settings can be left to defaults. You may leave the challenge password and optional company name blank if you wish. Type **y** for yes at the last queries, "Sign the certificate? [y/n]" and "1 out of 1 certificate requests certified, commit? [y/n]".

Here, you have created your server certificate. Now, to create clients certificates that will connect to the servers, you need to enter the following command one at a time changing the name for each client:

```
build-key client1

build-key client2

build-key client3

build-key client4
```

and so on……

Here, you will be prompted to enter data just like when you built the server key. Also, make sure if you typed the command **build-key client1** then you should enter **client1** for the Common Name. These entries much match.

Run the above commands for as many clients as you would like to have. Make sure that you use a unique common name for each client.

The final step in this process is to generate the Diffie Hellman parameters for the OpenVPN server. It helps in providing an extra layer of security.

Enter this command to begin the process:

```
build-dh
```

This will take a long time.

Sample network:

The provided config files and settings are configured for the following network scenario; you should change it as per your needs:

Your router's/Gateway's IP address is 192.168.100.1 and its subnet mask is 255.255.255.0

Your OpenVPN server attached to it has its network interface statically set to the IP address of 192.168.100.150 with the subnet mask 255.255.255.0 and a default gateway of 192.168.100.1.

1194 is the default port for OpenVPN. It's a good idea to change the port number 1194 to another for better security. If any aspect of your network is different, you will need to take that into consideration when following the rest of this guide.

Decide a new network range preferably in private IP stack to be used for VPN. Here it is 172.16.0.0/255.255.240.0.

Creating the config files:

Now it's time to create configuration files for the server and clients. Sample config files can be found in the config directory. For the above described network, sample files are provided herewith.

You need to create a separate config file for each client. The config file can be exactly the same for each client except for the network settings and file path of the .key and .crt files.

You need to change the IP addresses of the DNS servers and related network addresses in the server file.

These configuration files will be placed in the config directory (C:\Program Files\OpenVPN\config) of each corresponding computer. Each server needs one config file.

Server Configuration

Depending on version of Windows you have, you may need to make some changes on the server.

Disable the Windows firewall for you network connections.

The built-in Windows firewall (as well as some third party ones) causes problems if it is running on the server

Client configuration:

You are going to install OpenVPN on each of the client computers using the same install file you used above. You should leave all the install settings on their defaults for the clients. Once you rebooted, go ahead and copy the configuration file into the config directory (C:\Program Files\OpenVPN\config) of each client. Then, add the three necessary certificate files into the C:\Program Files\OpenVPN\easy-rsa\keys folder. The three required files are **ca.crt** (each client and the server share a copy of this), **client.key**, and **client.crt**.

Connecting:

If everything went well up to now, you should be able to start up OpenVPN and connect.

On the server:

Go to OpenVPN GUI in the system tray and click on connect. It should successfully connect and display that it has an IP address (VPN Address).

On the clients:

Once the server has been connected, you should be able to connect clients.

Using OpenVPN GUI:

When you want to connect to a Server, right-click the OpenVPN GUI and click connect. If you have more than one config file you will be able to choose between them. You may protect it using a password to protect it from unauthorized use, if you use a pass phrase protected key you will be prompted for the password.

OpenVPN GUI can start a connection automatically when it runs. To enable auto connect simply add this string to the command that starts the OpenVPN app:

```
--connect client.ovpn
```

Change **client** as needed for the name of each client config file.

Troubleshooting:

For the OpenVPN to work correctly, you need to change your DHCP Client service to started status and Automatic startup type. The above configuration has worked well for me in my situation. If you have any suggestions, feel free to comment.