

BingerVPN User Manual

Explanation of our system

One of the primary motivations for someone to use a VPN is to increase their privacy while being online. Whether an individual is attempting to protect their online activity from their ISP or simply trying to reduce their digital footprint for their own personal reasons, a VPN will do a competent job in keeping a user anonymous—for the most part. One thing that is not considered when using a VPN is the actual provider of that VPN and what information they have about you. Many VPN providers sell their users' data without them knowing. To avoid the potential infringements with VPN providers, we have decided to create our own VPN with the OpenVPN protocol.

BingerVPN, a self-hosted OpenVPN server, replicates the functionality of a commercial VPN provider. This is done by enabling clients to securely connect to the server through an encrypted tunnel and make it appear as if their internet traffic comes from a different location. Our server includes a web-based monitoring dashboard that displays important client and server information. It also includes tools to generate necessary client profiles to connect to the VPN, which facilitate user authentication and ensure that only authorized users can access the network securely.

Connecting to the VPN server

The first step required to connect to the VPN server is to create a client profile that contains necessary information that validates the client as an official one. The client profile must have the client's certificate, private key, the CA certificate, TLS authentication key, and connection settings made in the server configuration file. We created a bash script that embeds all of these things and creates a client profile once the client's certificate and private key are generated with easyRSA and then signed by the certificate authority.

```
BingerVPN@vultr:~/openvpn_scripts$ ./create_client_profile.sh client1
```

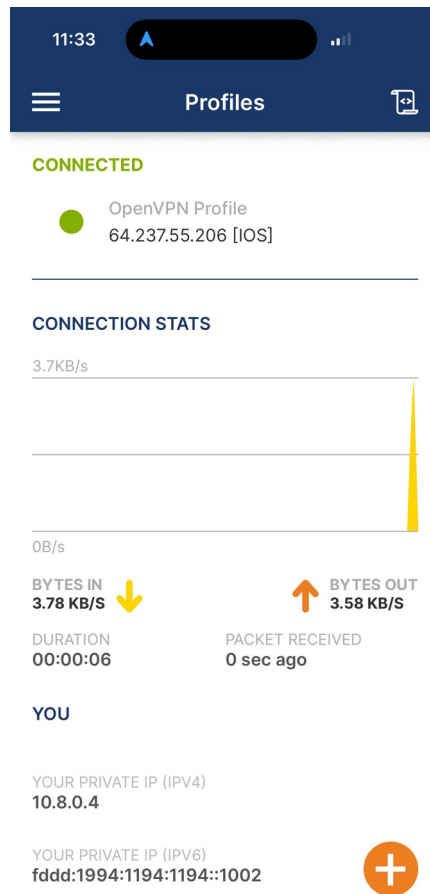
So once the client profile is created you must download it on the client's local machine and this can be achieved with the SSH File Transfer Protocol.

```
federico@federico-ThinkPad-T480:~$ sftp BingerVPN@64.237.55.206:openvpn-clients/Federico.ovpn ~/BingerVPN
```

After the client has downloaded their client profile on their local machine, they can connect to the VPN server in two different ways depending on their operating system. For Linux, all they have to do is open up a terminal and insert this command that points OpenVPN to the client profile.

```
federico@federico-ThinkPad-T480:~$ sudo openvpn --config ~/BingerVPN/Federico.ovpn
```

The second way is to use OpenVPN's client application which would apply to Windows, MacOS, Android, and IOS.



BingerVPN's client monitoring dashboard

It's very simple to use our client monitoring dashboard. The first step is to have Flask installed on the server and allow port 5000 in the server's dedicated firewall. After that, you must activate the virtual environment in the directory where the app.py file lies.

```
BingerVPN@vultr:~/testing_UI$ source venv/bin/activate
```

Once the virtual environment is activated, then you can run the application, and it will give you a link to our client monitoring dashboard that displays important information about the server and clients.

BingerVPN

Client VPN

VPN Mode	Status	Clients	Up Since	Server IP
Server	CONNECTED	2	0h 0m	64.237.55.206

Username	VPN IP Address	Remote IP Address	Bytes In	Bytes Out	Connected Since	Cipher
IOS	10.8.0.4	99.101.1.1	43442	52849	2026-04-27 18:29:18	AES-256-GCM
Federico	10.8.0.2	99.101.1.1	78602	45205	2026-04-27 18:28:50	AES-256-GCM

Map View



BingerVPN Server
Piscataway, New Jersey
64.237.55.206