

The 'Point and Click' Home VPN HowTo Guide

contact: beakmyn <at> frontiernet <dot> net

The 'Point and Click' Home VPN HowTo Guide by [beakmyn](#) is licensed under a [Creative Commons Attribution-Share Alike 3.0 United States License](#)
Rev 1.6, March 26, 2009

This document is under peer review and as such may change and may not be 100% correct or complete.

Best viewed at 1024x768 or better, using a computer.

- [Background](#)
 - [Audience](#)
 - [Disclaimer](#)
 - [Software](#)
 - [Conventions Used](#)
 - [Prerequisites](#)
- [Let's Get Started: Installing Ubuntu](#)
- [Installing Webmin](#)
 - [Modify apt sources.list](#)
 - [Add the maintainer's GPG key](#)
 - [Update your apt sources](#)
 - [Install Webmin package](#)
- [Install OpenVPN](#)
- [Access Webmin](#)
- [Setup IP forwarding and masquerading](#)
- [Setting Firewall rule\(s\) to allow VPN web traffic to redirect out eth0](#)
 - [Packet filtering \(filter\)](#)
 - [Network address translation \(nat\)](#)
- [Install OpenVPN-admin module](#)
 - [Creating the Keys list](#)
 - [Create the Server Key](#)
 - [Create the Client Key\(s\)](#)
 - [Add VPN to the list](#)
 - [Add Clients to Server](#)
 - [Setup New Client on Server](#)
- [Start your VPN Server](#)
- [Setup Client Machine](#)
- [Testing the VPN Server using the OpenVPN client GUI from Windows](#)
- [Other things to try](#)

Background

I travel a lot and many times I'm connecting to wireless hotspots or I'm in a foreign country. As such I don't always want everyone to know what websites I'm surfing or what message boards I'm posting to. I also want to be able to troubleshoot any problems on the home network while away. There are many methods by which one can anonymize their web traffic or at the minimum control, to some extent, who sees it and what they see. For me, using a random proxy server or Tor doesn't look so good when you don't know who is controlling the end point server.

Audience

This guide is for those who want to quickly set up and administer a OpenVPN server. While the technical detail isn't high it does require some basic understanding of the Linux operating system. For those that are unsure, I have included screenshots in order to make things easier to understand. For those of you who refuse to acknowledge the existence of a GUI in Linux and swear by vi and ssh this guide isn't really for you. I've gone down that road and now I'm trying something different.

So, this guide is for those who want a straightforward 'point and click' solution that makes it very easy and gets you up and running with minimal effort. If you want to read about all the parameters, check the footnotes.

Disclaimer

The VPN in this guide is a Tun routed solution, aka "Road Warrior". While Tun is more efficient and easier to administer it only passes TCP/IP traffic. It will not route IPX or NetBEUI for that you need a TAP configuration. It will route all web traffic from your client through the VPN. This does come at some cost of bandwidth. Most residential broadband packages limit your upstream speed. This is important because your web traffic will need to be uploaded from your VPN back to you. So while I've found that services like Hulu and Skype are bearable, there is a noticeable decrease in performance.

Software

- **Free Dynamic DNS account** you can use one of your choosing I like [DynDNS](#) but there's also [No-IP](#) and probably others.
- **Computer running [Ubuntu Linux Server Edition](#)**, we'll only install a command line version of Linux. I'm running a 500MHz machine with 512MB of RAM
- We'll be administering the VPN server from another machine using **Webmin** which has a very nice VPN admin that makes administration 'point and click

- [OpenVPN 2.1 beta 7 and OpenVPN GUI](#) for Windows

Conventions Used

```
vpnuser@vpnserver:~$ This is command to type
This is text that was added to a file
```

Prerequisites

You'll want to set a static IP on your VPN server or at the very least set a permanent reservation in the DHCP pool for the VPN Server. You'll also want to create a port forward rule to forward all traffic on the WAN destined for Port 1194 of type UDP to the VPN Server.

Let's Get Started: Installing Ubuntu

Insert your Ubuntu server CD-ROM press F4 and select *Install a command-line system*.

You can choose any name you wish for the vpnserver however, since I'm not very creative I just call it **vpnserver**.

For partitioning I chose to let Ubuntu use the entire disk and not use LVM or encryption. If you do use encryption on the disk bear in mind that this will require you to enter a password at boot, before the system will start.

Installing Webmin

For installation we'll be using the author's maintained apt repository, which will require some configuration to use as it's not part of the standard Ubuntu repository.

Modify apt sources.list

We need to add webmin's repository to apt in order to download. Webmin doesn't have a specific Ubuntu repository but that's not a problem the one provided is compatible. You can use vi or nano or any other text editor to make the necessary changes to your sources.list. In this guide I will be nano.

```
vpnuser@vpnserver:~$ sudo nano /etc/apt/sources.list

deb http://download.webmin.com/download/repository sarge contrib
```

Press **Ctrl+X** and **Y** to save. Press **<enter>** to use the current file name

Add the maintainer's GPG key

Next we need to get the GPG key for the repository so that apt will trust it.

```
vpnuser@vpnserver:~$ wget http://www.webmin.com/jcameron-key.asc
vpnuser@vpnserver:~$ sudo apt-key add jcameron-key.asc
```

Update your apt sources

```
vpnuser@vpnserver:~$ sudo apt-get update
```

Install Webmin package

```
vpnuser@vpnserver:~$ sudo apt-get install webmin
```

Now sit back and let Webmin install it'll take a little bit of time. All dependencies will automatically be included.

Once installed the Webmin server is accessible by using your web browser and navigating to <https://<your server name>:1000/>

We'll bring up the Webmin interface in a bit but first we need to install OpenVPN. If you don't have a local DNS then you'll need to access your VPN by using the IP address. If accessing it from a Windows OS then you add an entry to your host file.

Install OpenVPN

```
vpnuser@vpnserver:~$ sudo apt-get install openvpn
```

Access Webmin

It's not time to leave the console and remotely administer the server using Webmin. Fire up your browser of choice and head over to <https://vpnsrvr:10000> . If your browser asks about an invalid self certificate you can add an exception and allow it.



We can now log into the Webmin interface. Take a moment to look around and get acquainted. Go ahead and poke around. I'll still be here when you get back. Really, go ahead and click those little green arrows on the left.

Setup IP forwarding and masquerading

In the Webmin interface click on the green arrow for **Others** and select **File Manager**. Navigate to `/etc/sysctl.conf` and select **edit**. Uncomment the line:

```
net.ipv4.ip_forward=1
```

Click **Save and Close**

Setting Firewall rule(s) to allow VPN web traffic to redirect out eth0

First we'll assume that the firewall is not set up yet so click **Reset Firewall**. Now we need to add some rules. From Showing IPTables dropdown select **Packet filtering (filter)** we'll created the following rules

Packet filtering (filter)

Incoming Packets (INPUT)

Accept If state of connection is **ESTABLISHED, RELATED**

Connection states	Equals	Existing connection (ESTABLISHED)
(use Ctrl+Click to select multiple)		Related to existing (RELATED)

Accept If input interface is **eth0**

Incoming interface	equals	eth0
---------------------------	--------	------

Accept If input interface is **tun0**

Incoming interface	Equals	tun0
---------------------------	--------	------

Accept If input interface is **lo**

Incoming interface	Equals	lo
---------------------------	--------	----

Accept If protocol is **TCP** and destination ports are **10000**

Network Protocol	Equals	TCP
Destination TCP or UDP Port	Equals	10000

Accept If protocol is **UDP** and destination ports are **1194**

Network Protocol	Equals	UDP
Destination TCP or UDP Port	Equals	1194

Forwarded Packets (FORWARD)

Accept If input interface is **tun0**

Incoming interface	Equals	tun0
---------------------------	--------	------

Network address translation (nat)

This is the rule that goes along with the VPN "push redirect-gateway". This allows the VPN web traffic to be routed out through your connection.

Packets after routing (POSTROUTING)

[Masquerade](#) If source is 10.8.0.0/24 and output interface is **eth0**

Source address or network	Equals	10.8.0.0/24
Outgoing interface	Equals	eth0

Install OpenVPN-admin module

Click on the green arrow on the left to expand **Webmin** and select **Webmin Configuration**, then click on **Webmin modules**.

Now it's time to install the OpenVPN module. The Install tab should be select by default. Set the radio button to select **From ftp or http URL** and enter the following address to download the OpenVPN admin module.

http://www.openit.it/index.php/openit_en/content/download/3566/14487/file/openvpn-2.5.wbm.gz

Now click on **Install Module**. Once the module has installed you click on the green arrow on the left to expand Servers and you click on **OpenVPN + CA**. We'll be jumping around in here for the rest of the howto.

Creating the Certificate Authority

The first thing we need to do is create our Certificate Authority (CA)

Make the appropriate changes to

- Name
- State
- Province
- City
- Organization
- Email

Since this a home server you can really enter anything you want here. You can change the **Key size** to 1024 if you like. This pertains to the Diffie Hellman parameters key by which the server and client "can agree on a secret key over an insecure communication channel. Before a VPN connection is established, the channel is insecure, after all. "¹

New Certification Authority	
Name of Certification Authority	changeme
Complete path to openssl.cnf	/etc/openvpn/openvpn-ssl.cnf
Keys directory	/etc/openvpn/keys
Key size (bit)	2048
Expiration time of Certification Authority key (days)	3650
State	US
Province	NY
City	New York
Organization	My Org
Email	me@my.org

For this guide I'm going to leave everything at the default. Click on **Save** and the system will now create the Diffie Hellman file. This took 20 minutes on my machine. You'll see lots of ...+.....+ and finally some ****

Click on **Return to OpenVPN Administration** then click on the icon **Certificate Authority List** and you'll see you're new CA listed.

Certification Authority List				
Name	Notes	Info	Keys list	Remove
changeme		CA Info	Keys list	Remove

Creating the Keys list

Now we need to create our keys. At a minimum you will need to create one (1) server key and one (1) client key. Each client will need it's own key.

Create the Server Key

New key to Certification Authority: changeme

Key name	serverkey
Key password (min 4 chars)	
Server key doesn't need password!	
Key Server	server
Generate exportable PKCS#12 key	no
Password for exporting PKCS#12 (min 4 chars)	
Key expiration time (days)	3650
State	US
Province	NY
City	New York
Organization	My Org
Organization Unit	Office
Email	me@my.org

Save

Set the key name. In my case I chose the very creative **serverky**. Set the **Key Server** to server, then click **Save**.

Once the key is created, Click on **Return to Keys list of Certificate Authority changeme**, where changeme is the name you gave your CA.

Create the Client Key(s)

Each client will need it's own key. I suggest setting a password as this provides you with a two factor authentication. Just in case someone gets your key file they still need a password to authenticate and use the VPN.

NOTE: Minimum password and name length is four (4) characters

New key to Certification Authority: changeme

Key name	clientkey
Key password (min 4 chars)	••••••••
Server key doesn't need password!	
Key Server	client
Generate exportable PKCS#12 key	no
Password for exporting PKCS#12 (min 4 chars)	
Key expiration time (days)	3650
State	US
Province	NY
City	New York
Organization	My Org
Organization Unit	Office
Email	me@my.org

Save

Both keys should now be listed

Keys list of Certification Authority changeme

Name	Key Server	Verify	Export	Complete path of status log file	
serverkey	server	Verify	Export	active	Remove
clientkey	client	Verify	Export	active	Remove

Go back to the **Administration page** and click on icon name **VPN List**

Add VPN to the list

VPN server list:

VPN List is empty

ca (Certification Authority): changeme

New VPN server

Creation of new VPN Server: select the Certification Authority and click New VPN server

VPN server list with simmetric key
 VPN List is empty

New VPN Server with symmetrical key Creation of new VPN Server with symmetrical key

[Return to OpenVPN Administration](#)

Your CA should automatically be listed so all you need to do is click on the button labeled **New VPN Server**

Ok there's a lot of information here. Fortunately we don't need to change most of it. The image below has all the changing. Here's what was changed.

Name	MyVPN	
enable TLS and assume server role during TLS handshake	yes	
Net IP assigns (option server)	10.8.0.0 255.255.255.0	
Persisit/unpersist fconfig-pool data to file	yes	
Add an additional layer or HMAC authenticaion...	yes	
Limit server to a maximum of n concurrent clients	3	set your accordingly
Additional configurations	push "route 192.168.254.0 255.255.255.0"	To access all ressource on the server Lan
	push "redirect-gateway"	To redirect all your web traffic through your VPN
	push "dhcp-option DNS 192.168.254.254"	For Windows machines send DNS queries to VPN

When you're all done click **Save** and **return to VPN List**

You're almost done.

Add Clients to Server

Click on Client List. Now we'll add the clients we created early to the VPN. Click on the button **New VPN Client**

Setup New Client on Server

Yes, it's another long list of parameters. Remember how one of the requirements is a **DynDNS** account? Well this is where you put in the **hostname** of the DYNDNS account you created.

remote (Remote IP) myvpn.dyndns.com

Now click **Save**. Rinse, lather and repeat for each additional client, the remote will stay the same.

Start your VPN Server

On Actions click on the text **Start**

VPN server list:											
Name	management	CA	proto	port	local	Logs	Client List	Status	Remove	Actions	
MyVPN		changeme	udp	1194	ALL	Log	Client List	Disable	Remove	Start	

After a few moments the Name will turn black and the action will change to Stop. This means your VPN server is running and ready to start using it.

VPN server list:											
Name	management	CA	proto	port	local	Logs	Client List	Status	Remove	Actions	
MyVPN		changeme	udp	1194	ALL	Log	Client List	Disable		stop	

Setup Client Machine

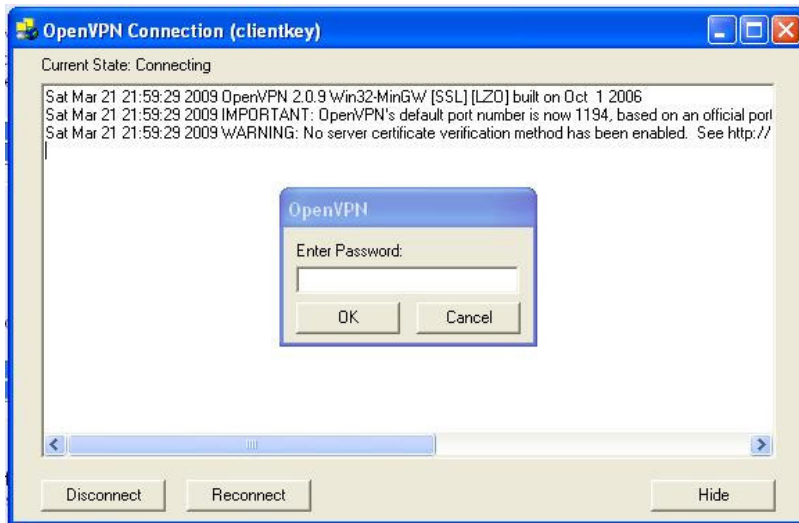
On the VPN Client list click on the **Export** text. This will allow you to download the <clientName>.tgz file. IT contains everything you need to put in the config directory of your OpenVPN config directory on your client machine. Isn't technology wonderful?!

VPN Client List MyVPN:						
Name	CA	proto	port	Export	Remove	
clientkey	changeme	udp		Export	Remove	

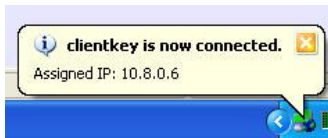
Testing the VPN Server using the OpenVPN client GUI from Windows

Be sure to install the "latest" development beta of OpenVPN (*OpenVPN 2.1_beta7* & *OpenVPN GUI 1.0.3*) as the push options we created are not valid for release 2.0.9

After uncompressing the .tgz file to your client conf directory. Start up your VPN Client program



You'll see a bunch of message fly by and after a few moments you'll see the ballon popup



You're Done!

Other things to try

Not that you've got the VPN up and running why not install and enable ssh. Then you can get a remote console using putty. Or perhaps you'd like some file storage, in that case then you'll want to install and enable SAMBA.



The 'Point and Click' Home VPN HowTo Guide by [beakmyn](#) is licensed under a [Creative Commons Attribution-Share Alike 3.0 United States License](#)

http://articles.techrepublic.com.com/5100-22_11-5687400.html