## **What is a VPN?**

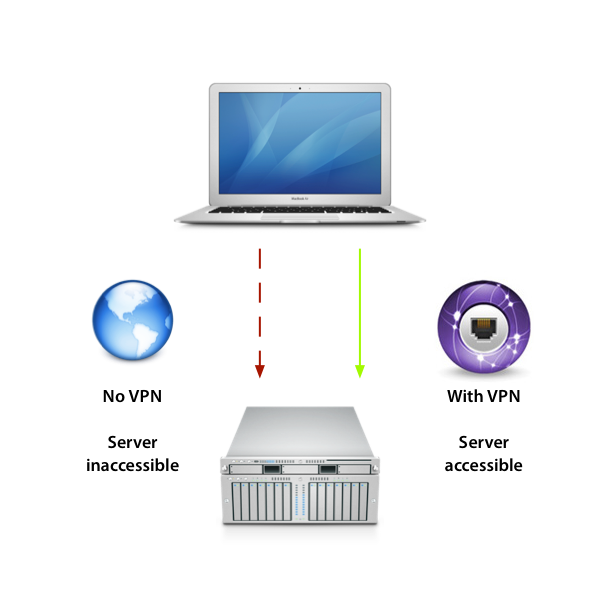
VPN stands for *Virtual Private Network*. If you have files on a server at work, that server is unlikely to be public facing (accessible over the Internet) and will no doubt be behind a firewall. Operating a VPN is far more secure than just opening ports on a firewall, which can be a security risk. Since more and more workers are traveling and/or working from home, companies require a way of allowing employees access to resources they need while still maintaining a high level of security.

Enter VPN, a way of securely connecting to a private network over the Internet. Using a VPN connection, it is just like you’re at the office. Imagine being at home and you realize there’s something you need from a server or internal website at the office. A VPN connection is just like having a *really* long ethernet cable that you plug into your Mac that’s connected to your work’s network.

## **Uses for a VPN**

### **Remotely Connecting to a Network at Work**

As we briefly touched upon, when you’re at work you’ll be able to access any file servers that are there. When you’re on the road or at home, you won’t be able to. With a VPN connection, it’s as though you’re on the same network. When it’s connected, you’ll be able to access any of the file servers using their normal IP address.

With a VPN connection, you can establish a secure connection to an otherwise private (and inaccessible) network

### **Encrypting Your Web Browsing**

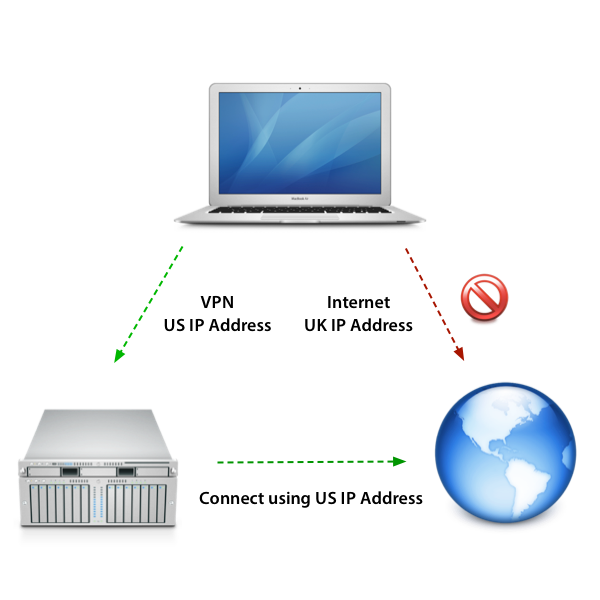
As a VPN connection is secure, any data going across it is encrypted. When you’re at a coffee shop and you’re browsing the web, your traffic could potentially be monitored. Most VPN Software (such as OS X) includes an option to have all your Internet traffic - not just when you’re accessing the VPN destination - to pass over a VPN connection, thus encrypting all your web browsing and increasing the security of anything you do online.

Advertisement

### **Be Somewhere Else in the World**

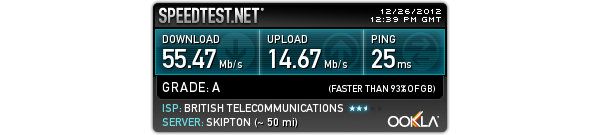
As you can pass your Internet traffic over the VPN connection, to most websites you will look like you’re accessing it from wherever the VPN server is. Confused? Let’s clear that up!

Let’s say you’re in London on a trip and stuck in a hotel room for a few hours. If you try and access a site that is only available in the US (such as Hulu), then you’ll be greeted with a message explaining that. If your VPN server is located in the US and you connect and make sure your Internet traffic passes through the VPN connection, then you’ll be able to access the site.

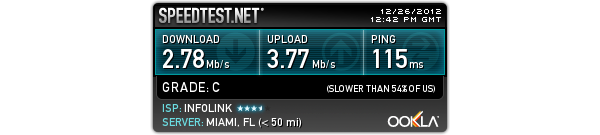
With a VPN connection, you can take on the network connection of the VPN server and browse the web as though you’re in a different country

The reason for this is that when you’re connected via VPN, you’re effectively *on that network*. You’ll have a local IP address on that network that’s assigned to your VPN connection and your Internet traffic effectively starts from where the VPN server is. As a result, to most sites, your location is actually wherever the VPN server is. I’ll explain this with an example.

There are plenty of speed test websites out there, one of the most popular ones is [Speedtest.net](https://www.speedtest.net/). If I run a speed test from my current location, I get feedback of my broadband speed and the closest testing server I connected to (in this case it was Skipton, UK).

The speed test shows the nearest testing server as well as ISP information

Now, when I connect via a VPN to a US server, ensure that all Internet traffic is sent via the VPN and run the test again, the site assumes that my closest server is in Miami! This is because it’s the *VPN server* the speed test is basing it from.

When using a VPN connection, the speed test believes I am located near Miami

Depending on the VPN server and your connection, you’ll notice that the speed drops dramatically.

**Tip:** For users in restricted countries such as China where many sites we take for granted (Twitter and Facebook) are blocked, some users “circumvent” this restriction by using services such as VPN.

## **Set up a VPN Connection**

There are a few things things you need to have before setting up a VPN connection:

### **VPN Server Address**

This is the IP address that we need of the VPN server. It can also be a fully qualified domain name (FQDN) such as *vpn.mycompany.com*, depending on how it’s been configured.

Advertisement

### **Username and Password**

All VPN connections have a username and password. These are usually set up for you by your IT administrator.

### **Connection Type**

There are two types of VPN connections, L2TP and PPTP. Both allow a secure connection, though L2TP is generally found to be the better of the two. This is because, in addition to a username and password, L2TP connections can require a *shared secret*. This is like a secret passphrase that any VPN users will need to add to their connection.

## **How to Connect Your Mac via VPN**

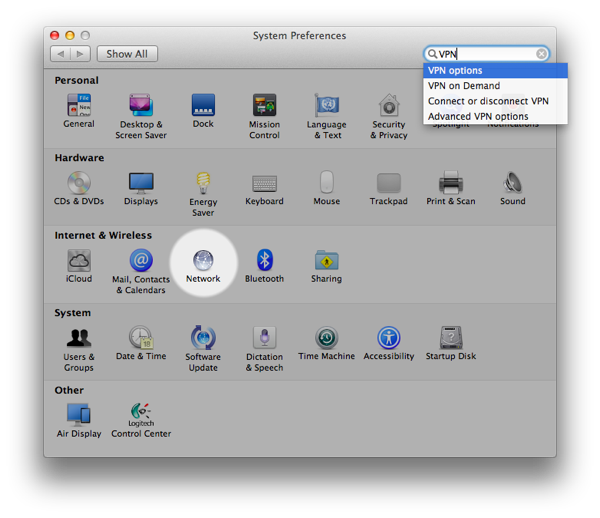
To set up a VPN connection on your Mac, you need the following details.

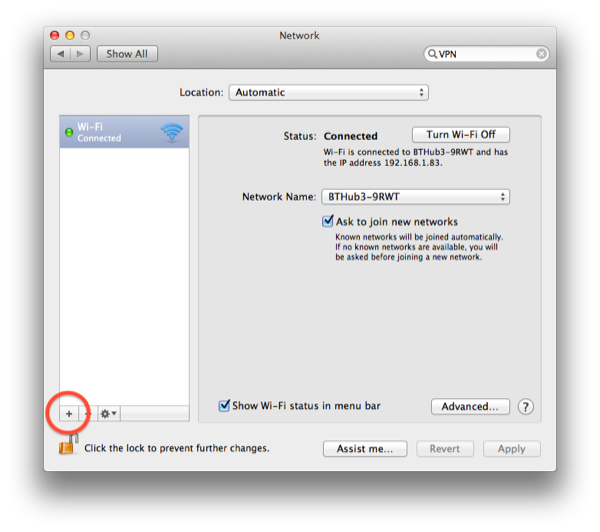
1. Server IP address or fully qualified domain name
2. Username and password
3. Connection type (L2TP or PPTP)

For the purposes of this tutorial, I’ll be using dummy information. While there are “free” VPN services out there we could use, I take the safety and security of your Mac (and mine) very seriously! If you would like to know more about commercial VPN services, I’ll be exploring these later.

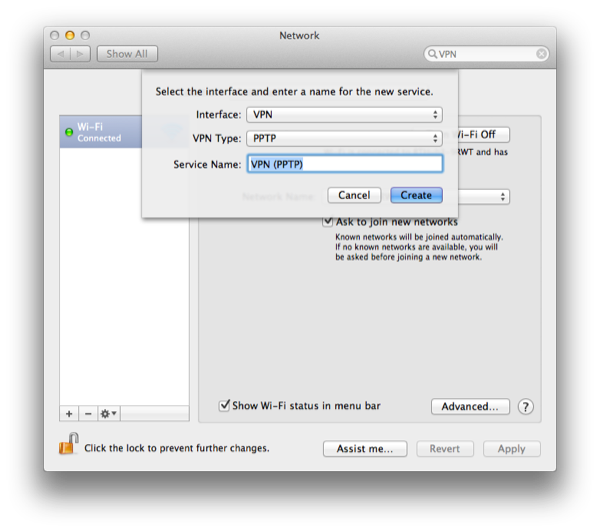
All VPN settings can be entered into *System Preferences*, under the *Network* preference pane.

**Step 1:** Open *System Preferences* and then select *Network*

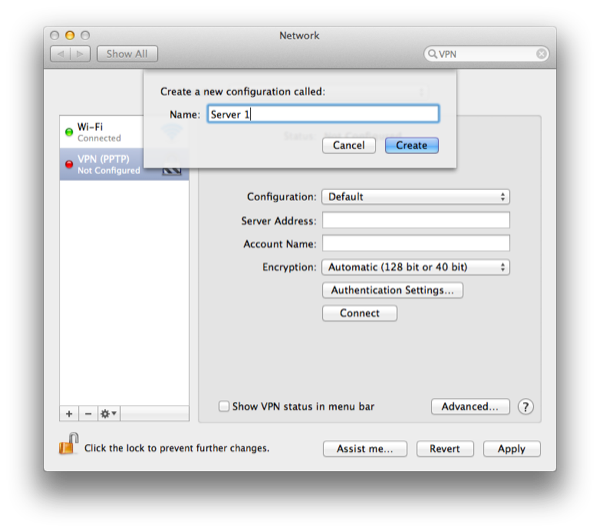
**Step 1: Open System Preferences and then select Network

Network Preferences

**Step 2:** Click + and then select *VPN* under the interface option. Specify either *PPTP* or *L2TP*.

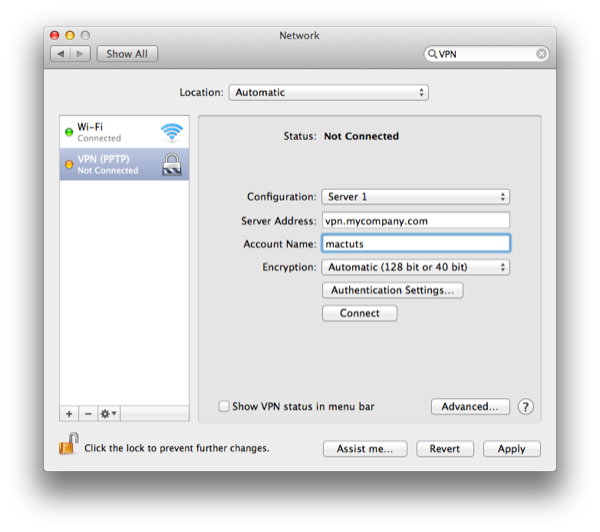
Step 2: Click + and then select VPN under the interface option. Specify either PPTP or L2TP

**Step 3:** Select *Configuration* and then *Add Configuration*. Name it “Server 1”.

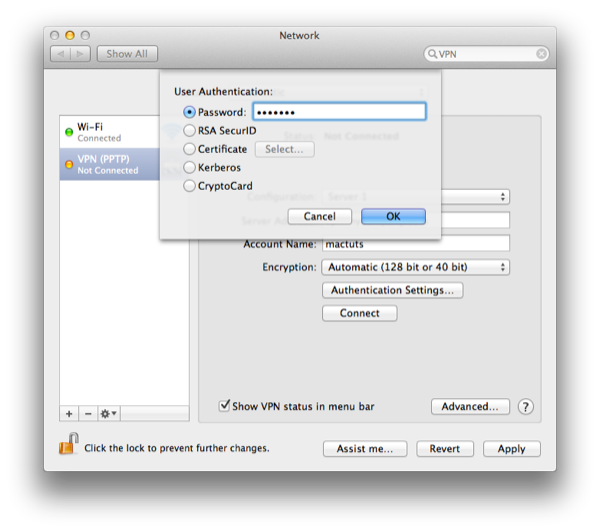
Step 3: Select Configuration and then Add Configuration. Name it "Server 1”

**Tip:** In the steps above, I asked you to add a configuration named “Server 1”. This step is actually optional and you can in fact just enter it under the *default* configuration. The reason for adding a configuration is that some users find they have multiple VPN settings. OS X can manage multiple VPN settings using the *configuration* option. For example, you may have a VPN profile (another name for a your VPN settings) for an office in the US and one in Australia.

**Step 4:** Enter the VPN server’s IP address (or FQDN) and user name.

Step 4: Enter the VPN server’s IP address (or FQDN) and user name.

**Step 5:** Select *Authentication Settings…* and then enter the password. Note: If you selected *L2TP* as the VPN type then this is panel is where you’d also enter the *shared secret*.

Step 5: Select Authentication Settings and then enter the password.

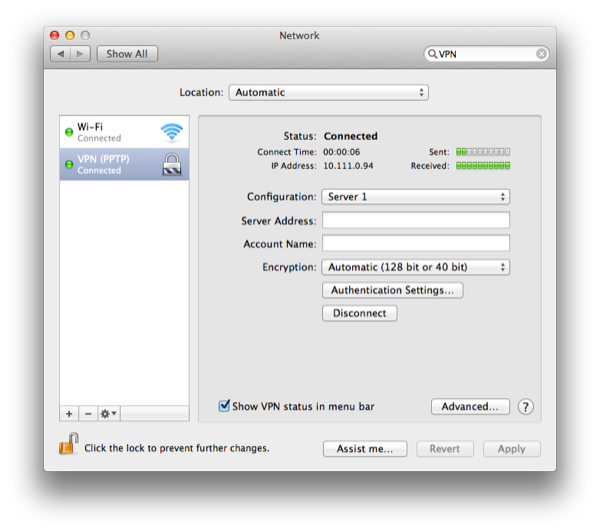
Note: If you selected L2TP as the VPN type then this is panel is where you’d also enter the shared secret

**Step 6:** Make sure *Show VPN status in menu bar* is selected, then click *Apply*.

That’s it, you’re ready to go! On your menu bar, you’ll see a new icon that looks like a luggage tag. Click this and then select *Connect VPN*. Once it’s connected, you’ll see a timer starting.

When a VPN connection is established you will see a timer on the menu barWhen a VPN connection is established, you will see a timer on the menu bar

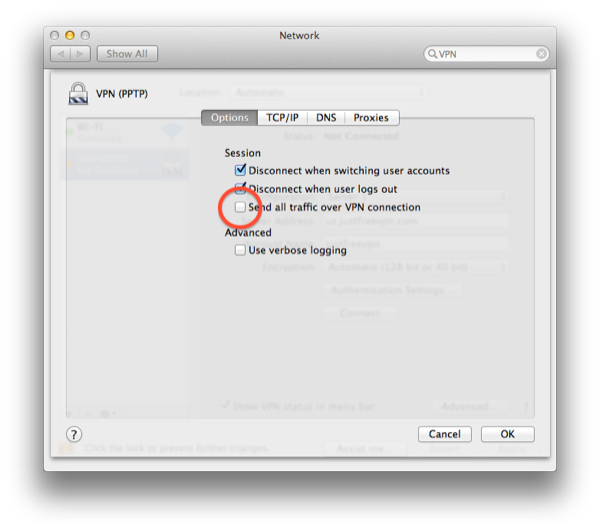
Now we’ve established a VPN connection, go back to System Preferences and you’ll see some connection information, including your VPN’s IP address.

System Preferences will also display connection details such as IP address and time connected

### **Sending All Traffic Over VPN**

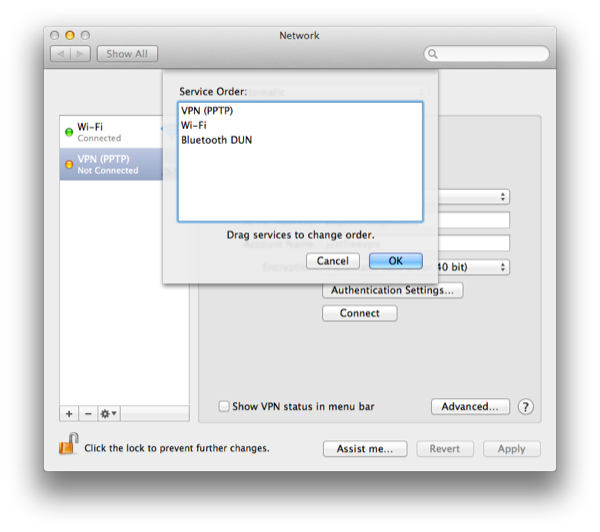
By default, your Mac will only pass necessary traffic via VPN, such as accessing a file server or other machines or sites that are on the same network as the VPN server. This is because most VPN connections can be quite slow, so your Mac doesn’t want to slow your Internet experience down needlessly. However, we can override this.

Go back in *System Preferences* and select *Advanced…*.

Go back in System Preferences and select Advanced.

Straight away, we see an option to *Send all traffic over VPN connection*. Ticking this and then saving the changes will mean your Mac will pass **all** network traffic over the VPN. It is generally not recommended since it can make your Internet connection appear very slow and you may also find accessing servers and printers on the network you’re physically on is stopped.

For all the data to be passed over the VPN once the option is enabled, we need to set the *service order*. This is the order that your Mac passes data over the network. We must have the VPN as the first service in the list. To do this, select the drop down cog menu and select *Set Service Order...* From here, you can drag the services into the required order, making sure the VPN is at the top.

Set the VPN to be the highest in the list of services

However, this is necessary if you need to access a site as we discussed earlier that’s only available in the country where your VPN server is located. Going back to our earlier example, if you were in the UK and you needed to access a US only site, enabling this option will allow you access to that site.