How to setup your own private, secure, free* VPN on the Amazon AWS Cloud in 10 minutes

UPDATE: 19 September 2016, Added the new AWS Mumbai region also.

So, we all know the benefits of using a VPN like privacy, anonymity, unblocking websites, security, overcoming geographical restrictions and so on. However, it has always been hard to trust a VPN provider who could potentially log and intercept your internet traffic! Launching a private VPN server will give us the best of what a VPN truly offers. This guide will walk you through all the steps to running your own VPN server in about 10 minutes.

Advantages of a Private VPN Server

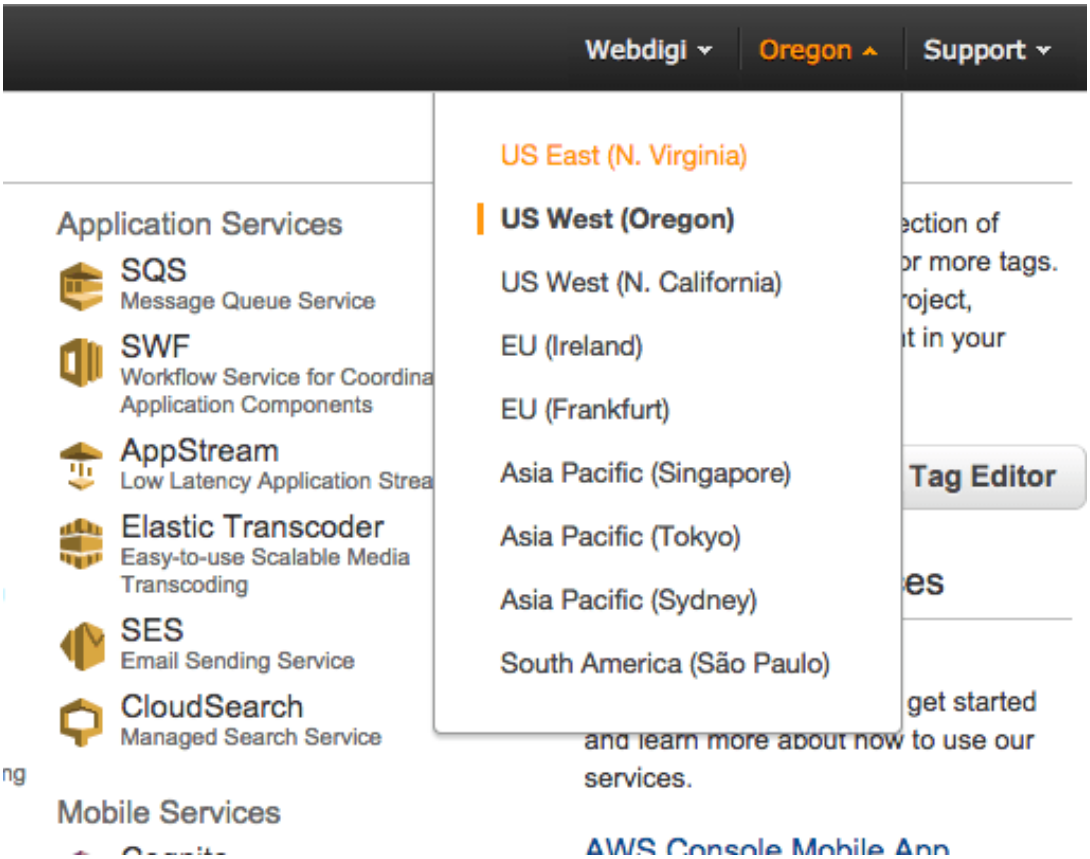
Simple: Non-techies should also be able to follow this guide easily.
Quick: 10 minutes is all it takes to follow this guide and create a private VPN server.
Private: Dedicated VPN server for your use only.
Secure: Encrypted & password enabled VPN server with no logs.
On demand: You can start / stop the VPN server as required.
Global: One or more VPN servers in 9 worldwide regions (including US, Tokyo, Singapore).
Device support: Supports PPTP and L2TP with IPSEC which means you can use the VPN server on your Android, iPhone, iPad, PC, MAC, and even most routers (to support Apple TV, Chromecast).
Open source: Review / contribute to this project https://github.com/webdigi/AWS-VPN-Server-Setup
Free: New Amazon AWS customers have a free tier server for the first year.

Creating your Private VPN Server

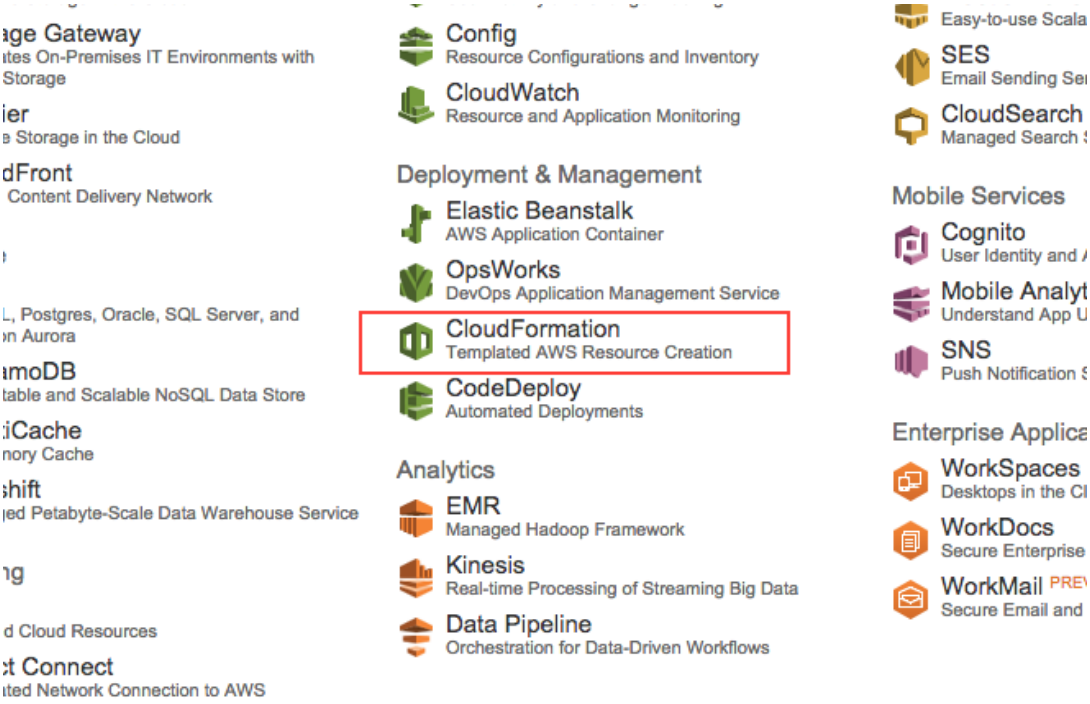
How to setup your own private, secure, free* VPN on the Amazon AW...

1. Setup a free Amazon (AWS) cloud account.
Visit http://aws.amazon.com/free/ and complete the signup. If you already have an Amazon AWS account then please login and follow on.

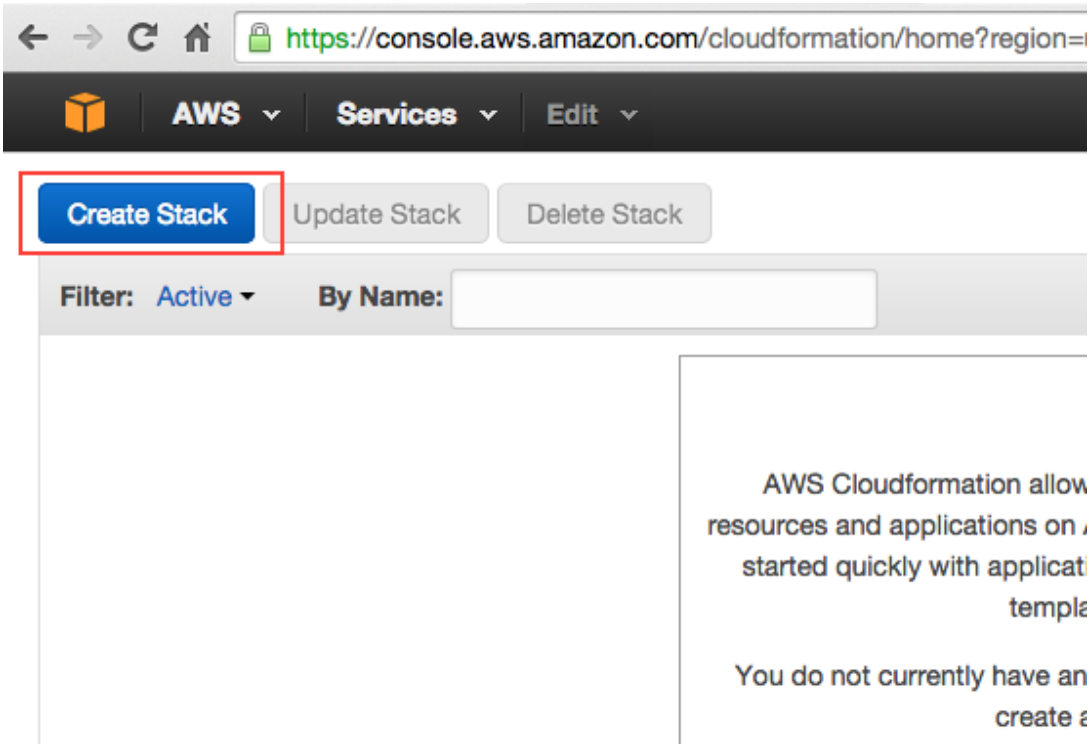
2. Select a region for your VPN server.
The VPN server can be in the following locations – North Virginia, Oregon, California, Ireland, Frankfurt, Singapore, Tokyo, Sydney, São Paulo. All your traffic will flow through the region that your VPN server is hosted. The selected region will appear in bold next to your name on the top header bar.



3. Open CloudFormation in the Amazon AWS control panel.
You can follow this link or click on the cloud formation link from the AWS page.

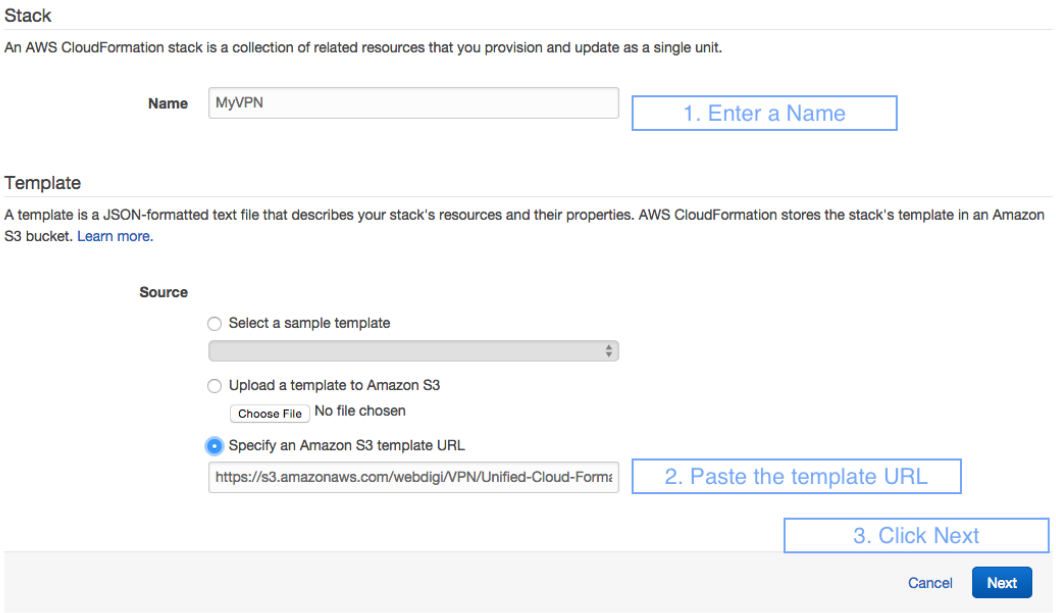


4. Start creating a stack with CloudFormation. Click on “Create Stack” button on top of the page.



5. Setting up the template for the stack

Enter a stack Name say MyVPN (you use what you like). Then under Template, Source, select “Specify an Amazon S3 template URL” and paste in this URL **https://s3.amazonaws.com/webdigi/VPN/Unified-Cloud-Formation.json** and then click Next.



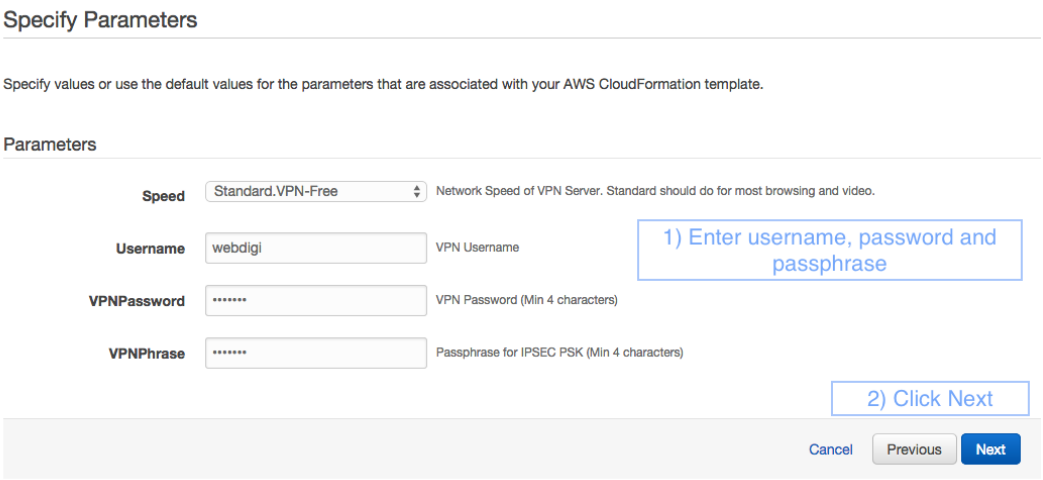
6. Setup VPN access details in the Specify Parameters page

Speed: Select Standard.VPN-Free and this should do for most use cases. We have also added faster server options if you ever require VPN with multiple simultaneous video streams and so on.

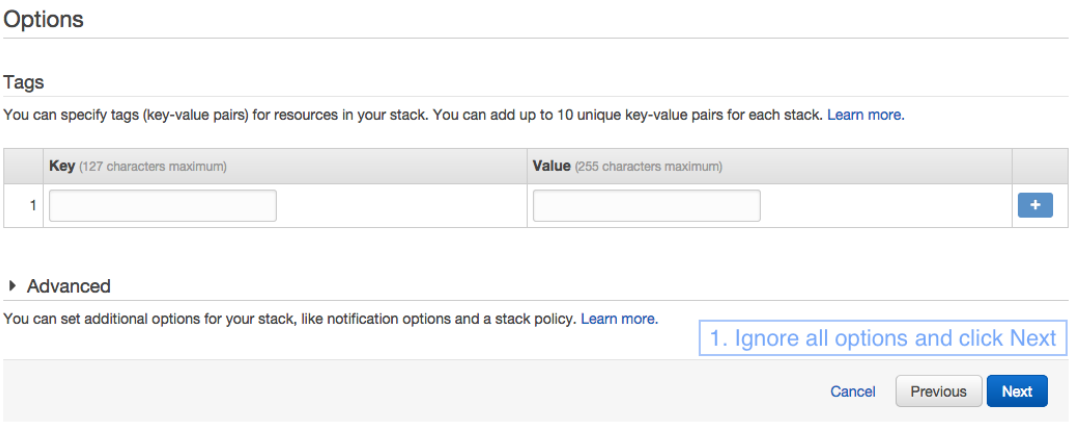
Username: VPN username for your VPN server.

VPNPassword: VPN password for your VPN server.

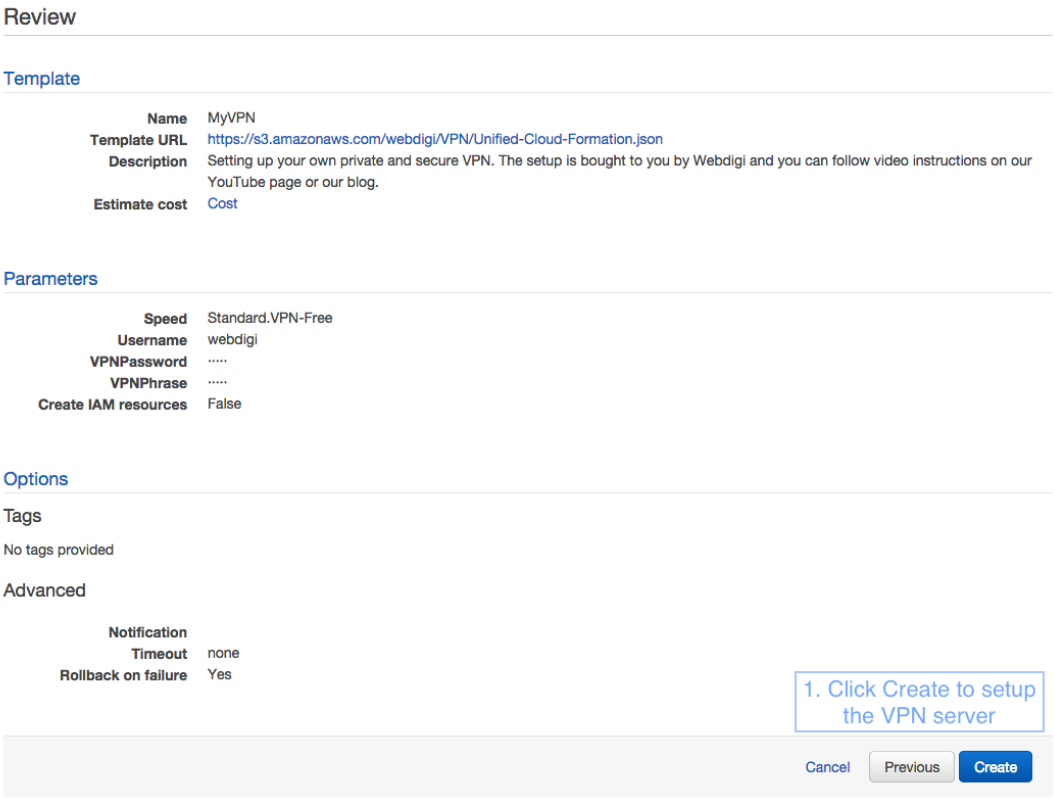
VPNPhrase: VPN passphrase the L2TP – IPSEC connections on your VPN server.



7. You will then be taken to the Options section and you can click Next without having to fill anything on this page.

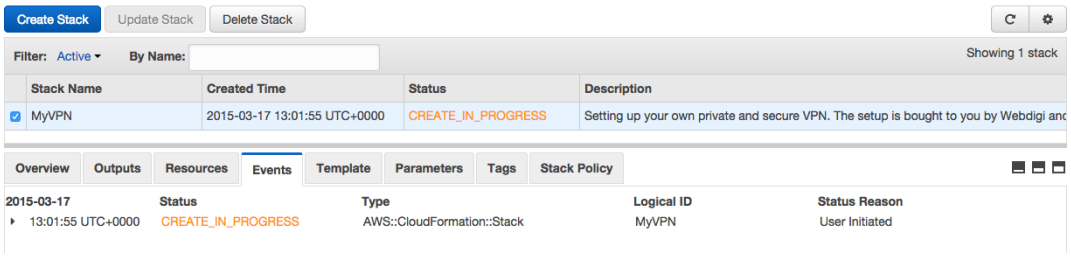


Finally, you will see a review page as in the screenshot below. Just click on Create and the VPN server will be created in a few minutes.

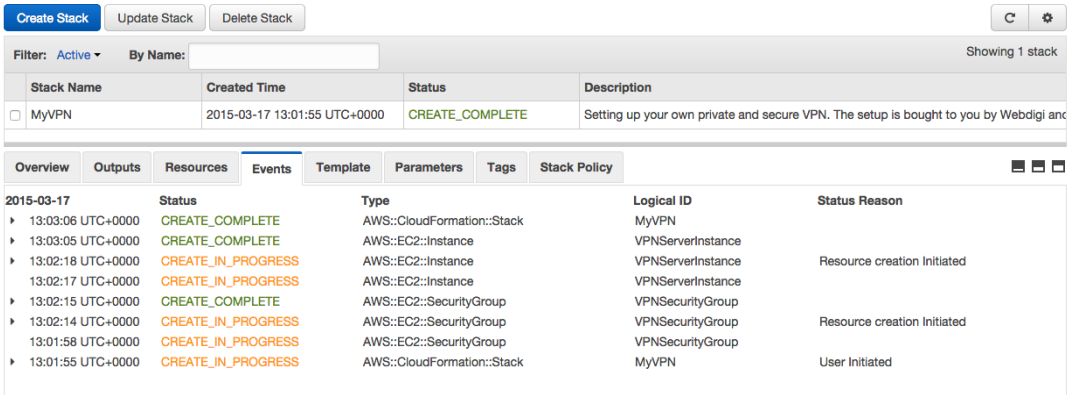


8. Monitoring the VPN server creation

You will see a page which shows that the status is Create in progress as below.

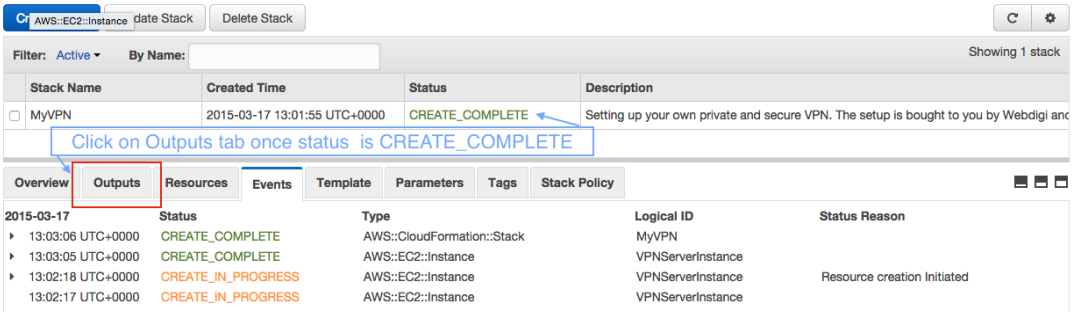


Within about 2 minutes you should see that the stack create in progress is complete as below.

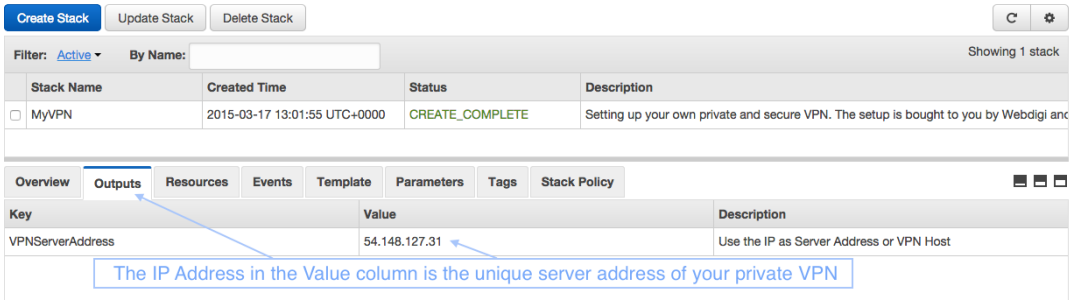


9. Obtain the private VPN server IP address

Once the stack status shows as CREATE_COMPLETE you can then click on the Outputs tab.



Now in the outputs tab you can see the server IP address as highlighted below.



Awesome, you should now have your private VPN server running in the IP address shown in the outputs tab. Please note that the IP address is unique for your server and you need it to connect your devices. **Now your VPN server is ready** and let us connect to it.

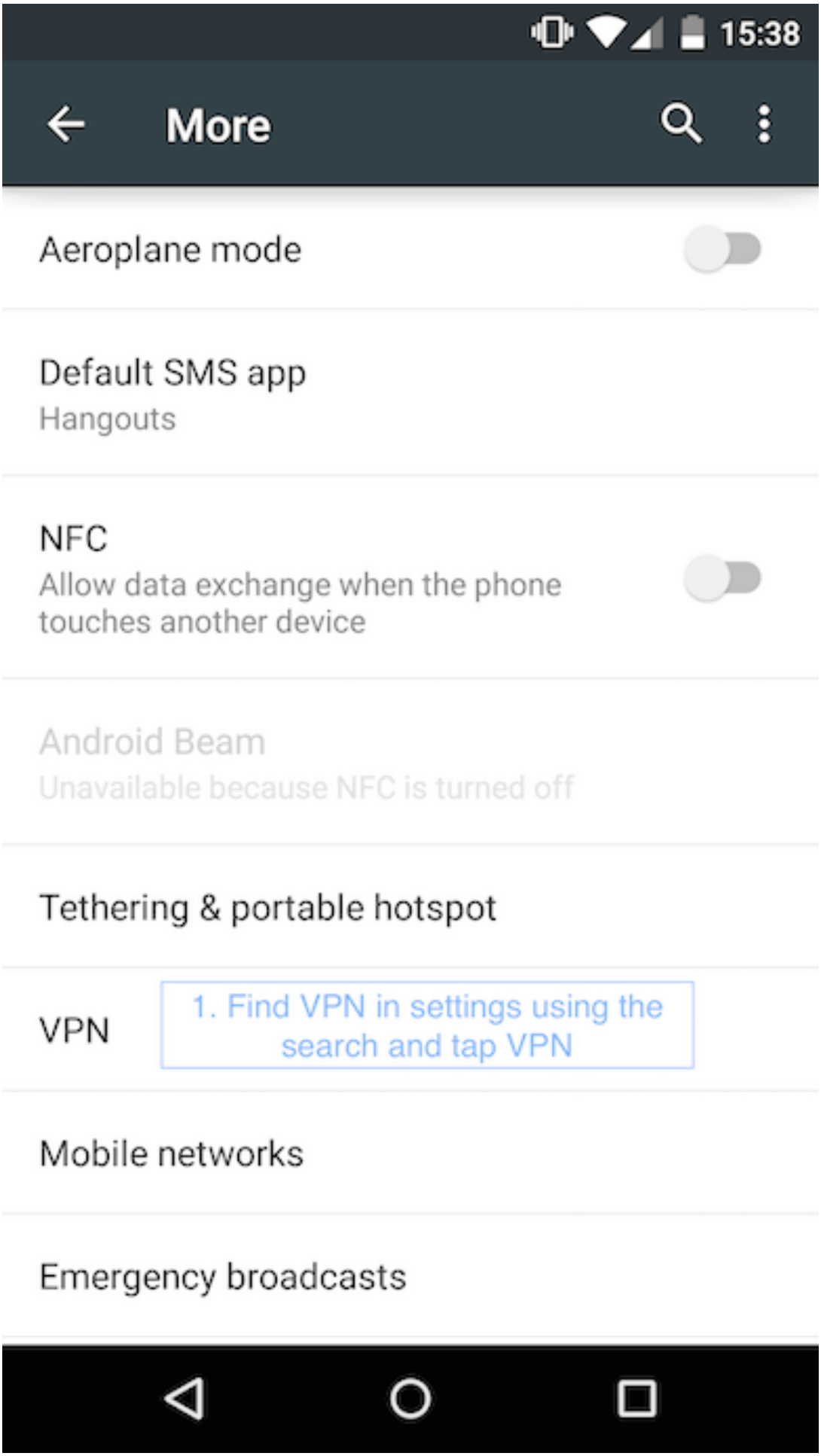
Connecting to your private VPN server

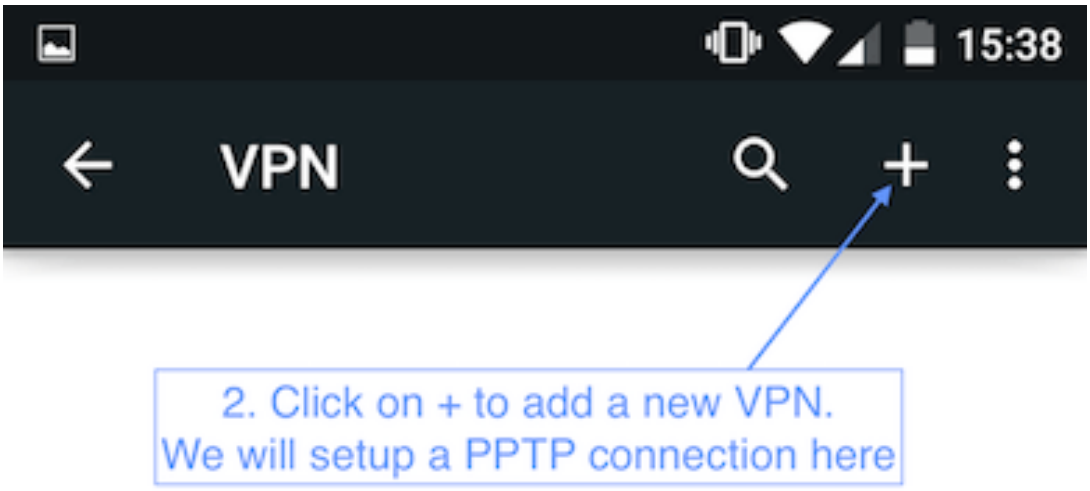
Each device has its own configuration to connect to a VPN server. We have added a how to for a few popular devices below. Please note that your private VPN server **supports both PPTP and L2TP** with IPSEC. This means that your VPN server supports most devices out there including older routers. You can connect to your VPN server with either PPTP or L2TP as supported by your device.

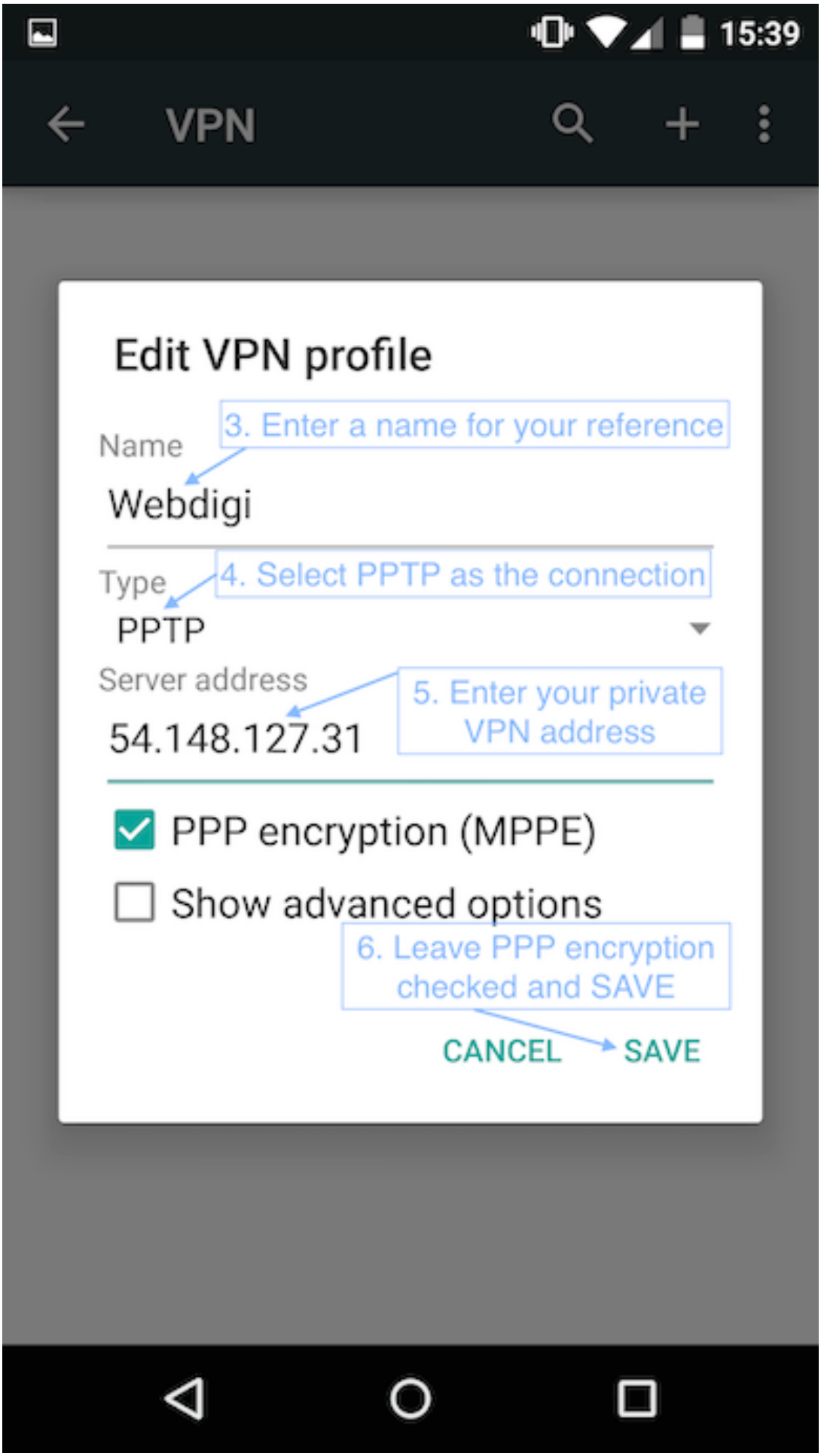
The parameters for your VPN connection are
Server Address: The IP address from step 9 and this is unique for your VPN server.
VPN Username & Password: From step 6 above. Same username & password for PPTP / L2TP VPN.
VPN Passphrase: You set this up on step 6 above and only have to be used with an L2TP connection.

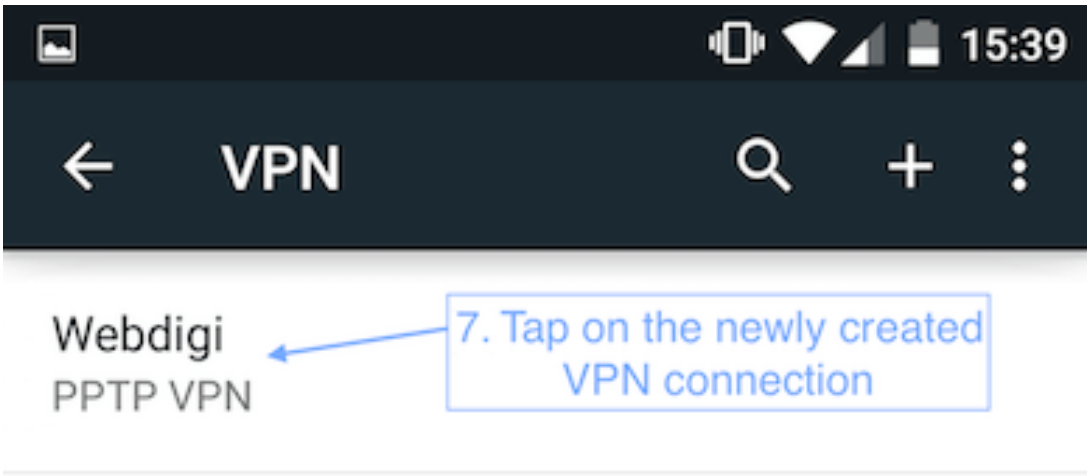
Examples below use PPTP but you can also find out how to setup L2TP with IPSEC on various websites.

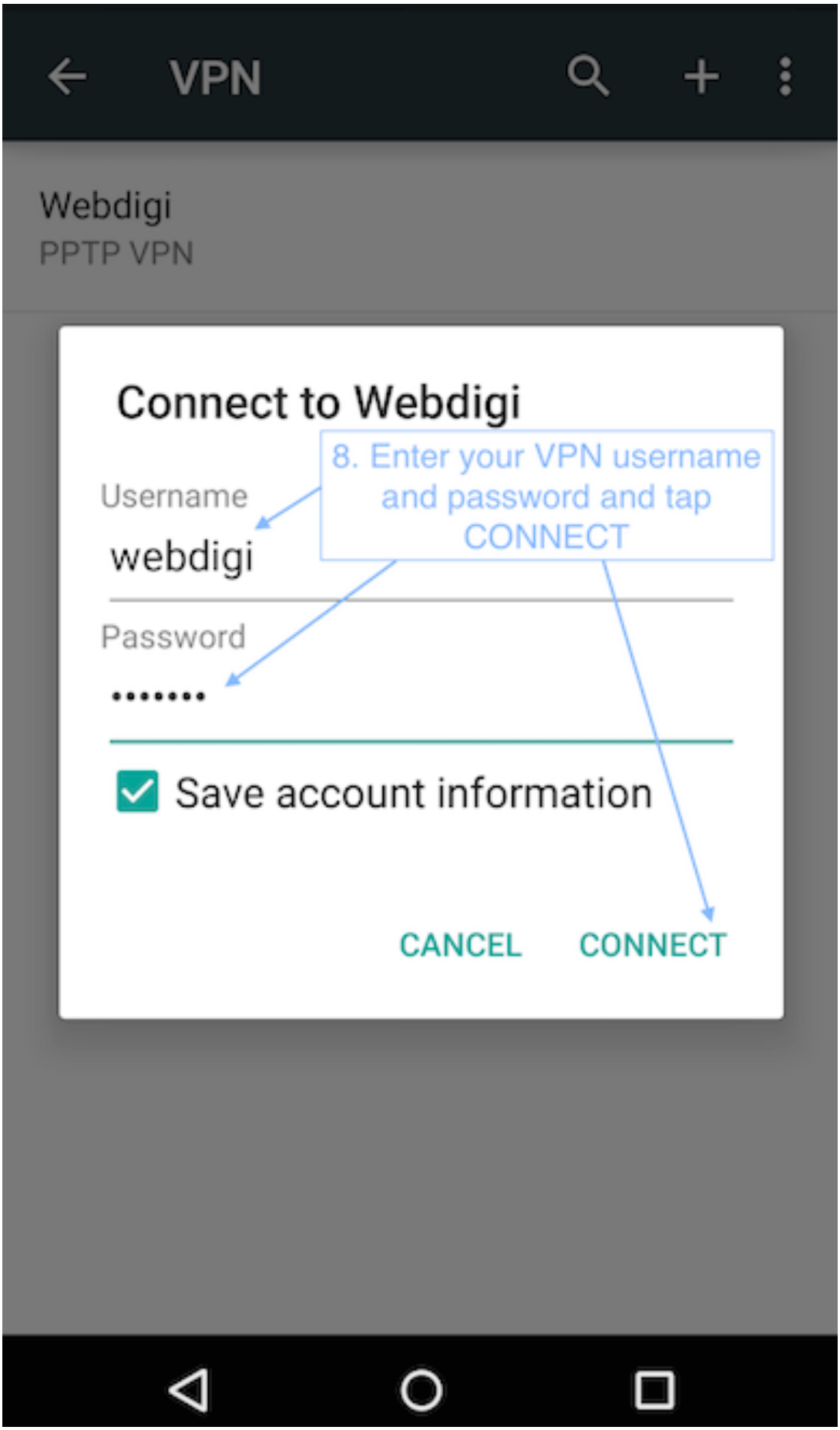
1. Setting up VPN on an Android 5.0


15:38
More
Aeroplane mode
Default SMS app
Hangouts
NFC
Allow data exchange when the phone touches another device
Android Beam
Unavailable because NFC is turned off
Tethering & portable hotspot
VPN
1. Find VPN in settings using the search and tap VPN
Mobile networks
Emergency broadcasts

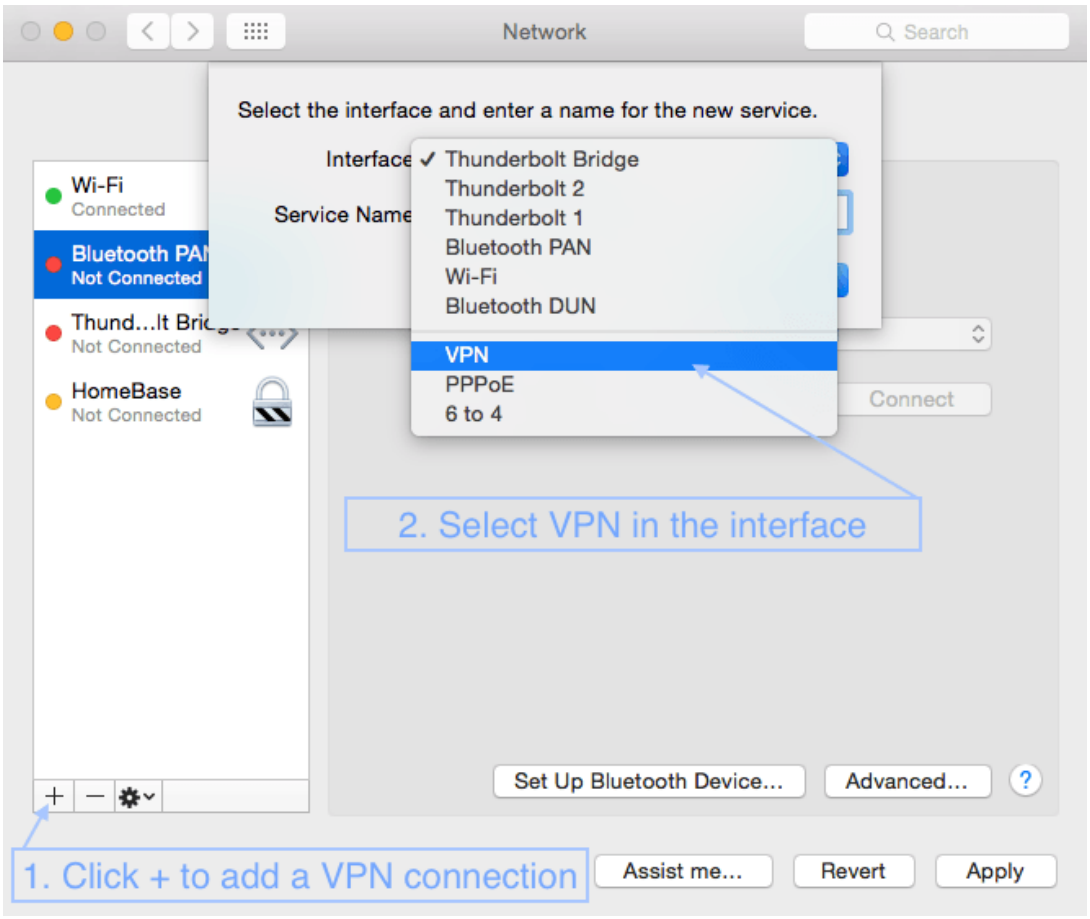

15:38
VPN
2. Click on + to add a new VPN.
We will setup a PPTP connection here

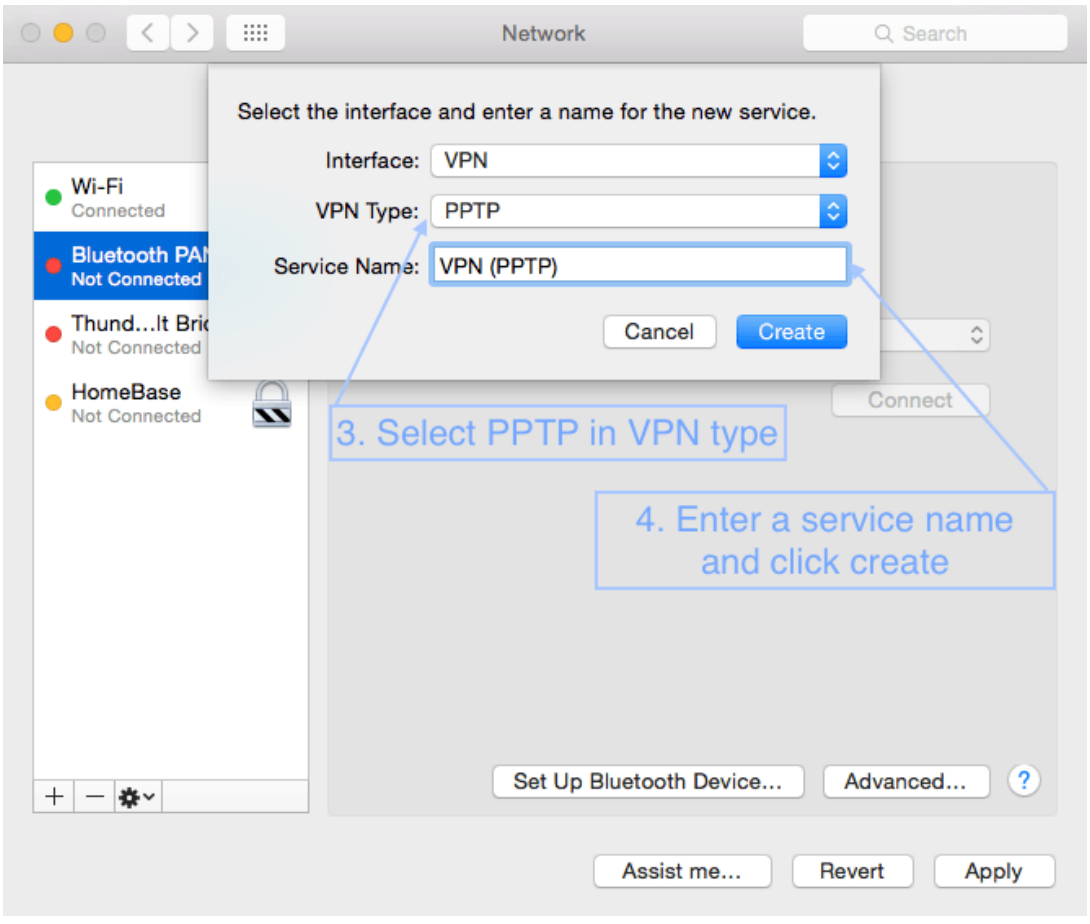

15:39
VPN
Edit VPN profile
3. Enter a name for your reference
Name
Webdigi
4. Select PPTP as the connection
Type
PPTP
Server address
5. Enter your private VPN address
54.148.127.31
PPP encryption (MPPE)
Show advanced options
6. Leave PPP encryption checked and SAVE
CANCEL
SAVE

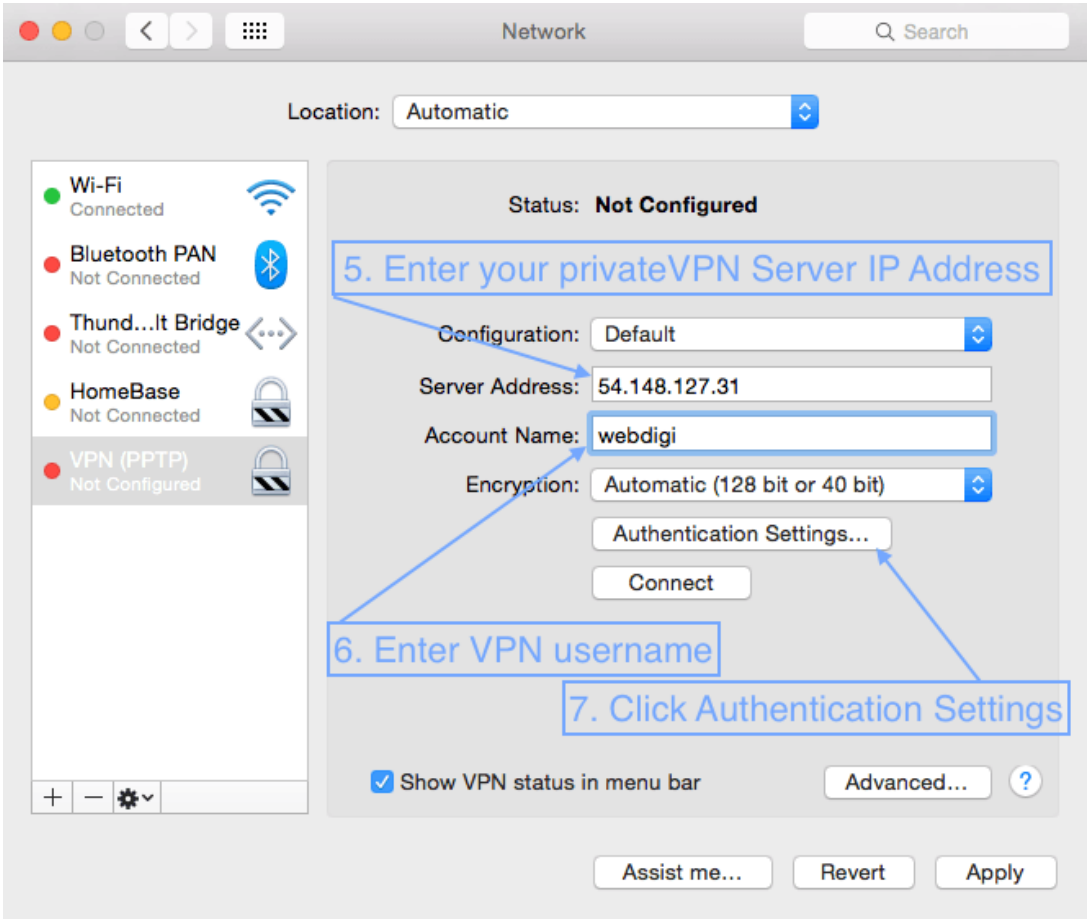

15:39
VPN
Webdigi
PPTP VPN
7. Tap on the newly created VPN connection

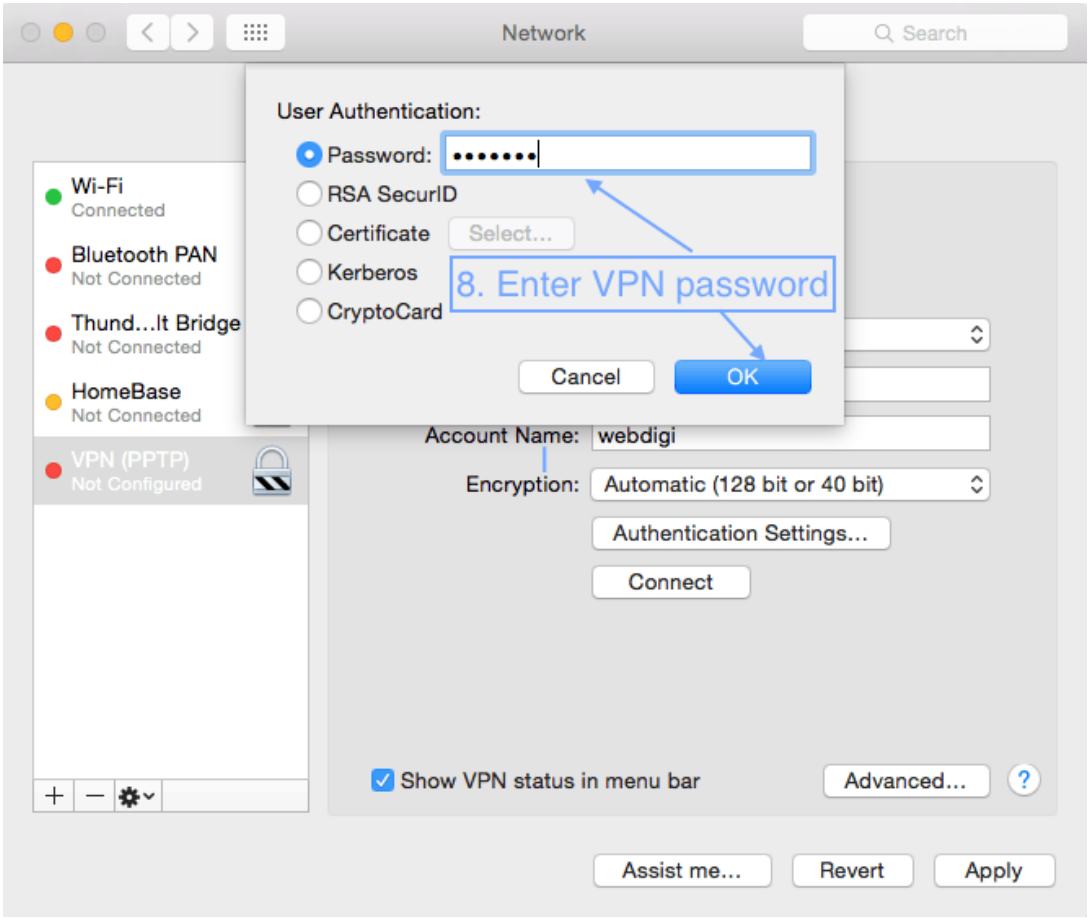


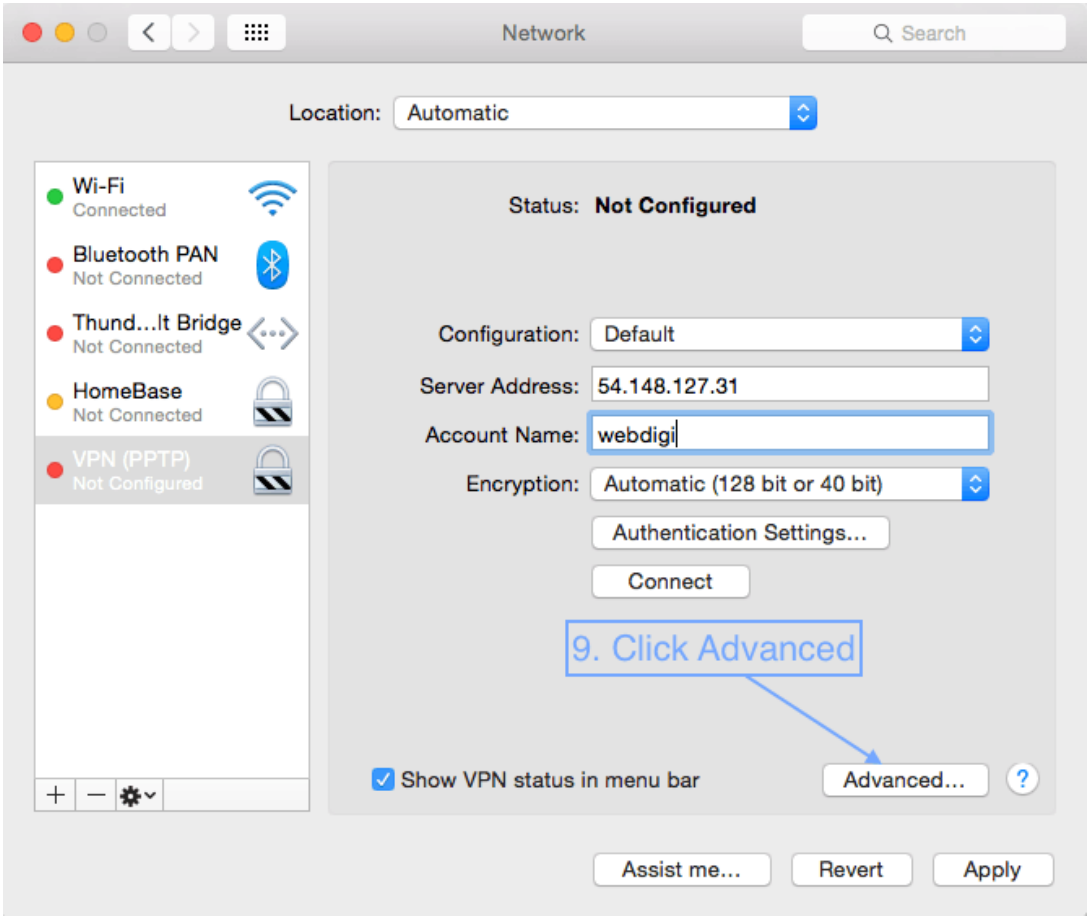
2. Setting up VPN on a MAC with the PPTP connection.
First open System Preferences, then Network and follow the screenshots below.

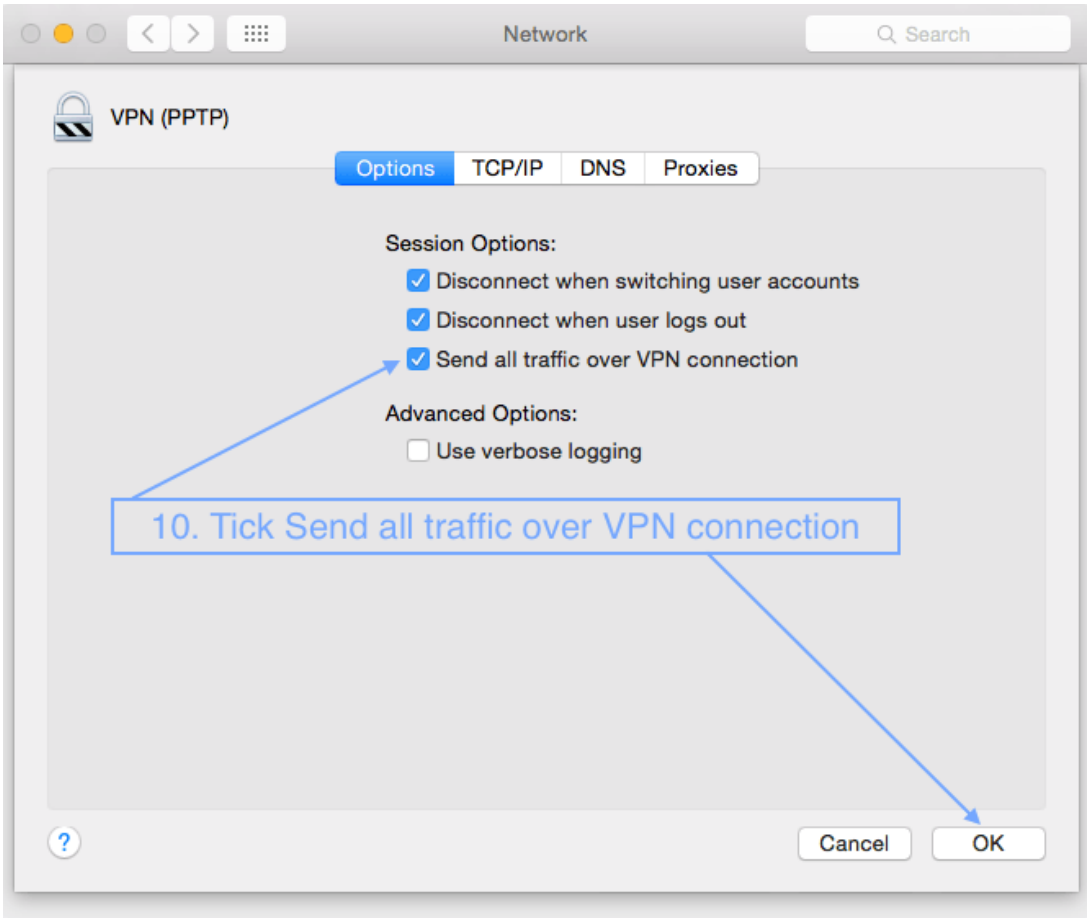

Network
Search
Select the interface and enter a name for the new service.
Interface
Service Name
Thunderbolt Bridge
Thunderbolt 2
Thunderbolt 1
Bluetooth PAN
Wi-Fi
Bluetooth DUN
VPN
PPPoE
6 to 4
Wi-Fi
Connected
Bluetooth PAN
Not Connected
Thund...lt Bridge
Not Connected
HomeBase
Not Connected
Connect
2. Select VPN in the interface
Set Up Bluetooth Device...
Advanced...
1. Click + to add a VPN connection
Assist me...
Revert
Apply

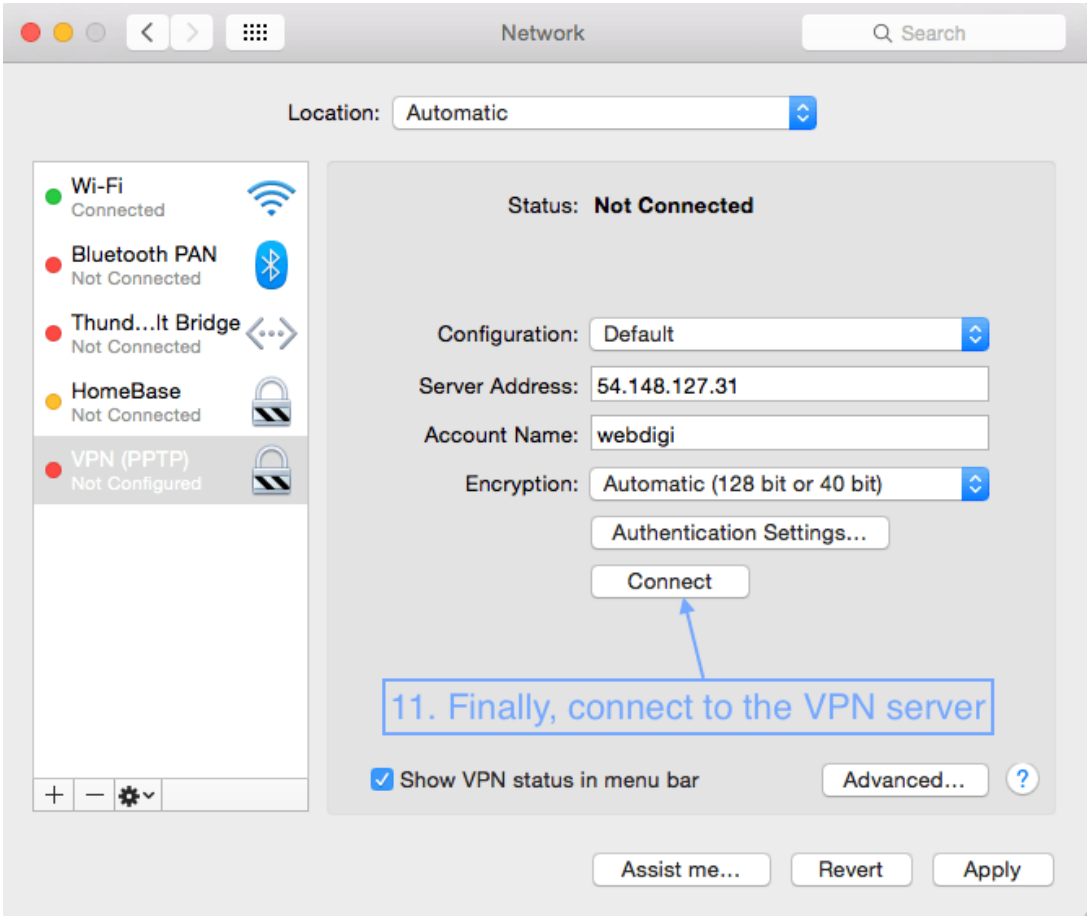

Network
Search
Select the interface and enter a name for the new service.
Interface: VPN
VPN Type: PPTP
Service Name: VPN (PPTP)
Cancel
Create
Wi-Fi
Connected
Bluetooth PAN
Not Connected
Thund...lt Bridge
Not Connected
HomeBase
Not Connected
Connect
3. Select PPTP in VPN type
4. Enter a service name and click create
Set Up Bluetooth Device...
Advanced...
Assist me...
Revert
Apply


Network
Search
Location: Automatic
Wi-Fi
Connected
Bluetooth PAN
Not Connected
Thund...lt Bridge
Not Connected
HomeBase
Not Connected
VPN (PPTP)
Not Configured
Status: Not Configured
5. Enter your privateVPN Server IP Address
Configuration: Default
Server Address: 54.148.127.31
Account Name: webdigi
Encryption: Automatic (128 bit or 40 bit)
Authentication Settings...
Connect
6. Enter VPN username
7. Click Authentication Settings
Show VPN status in menu bar
Advanced...
Assist me...
Revert
Apply

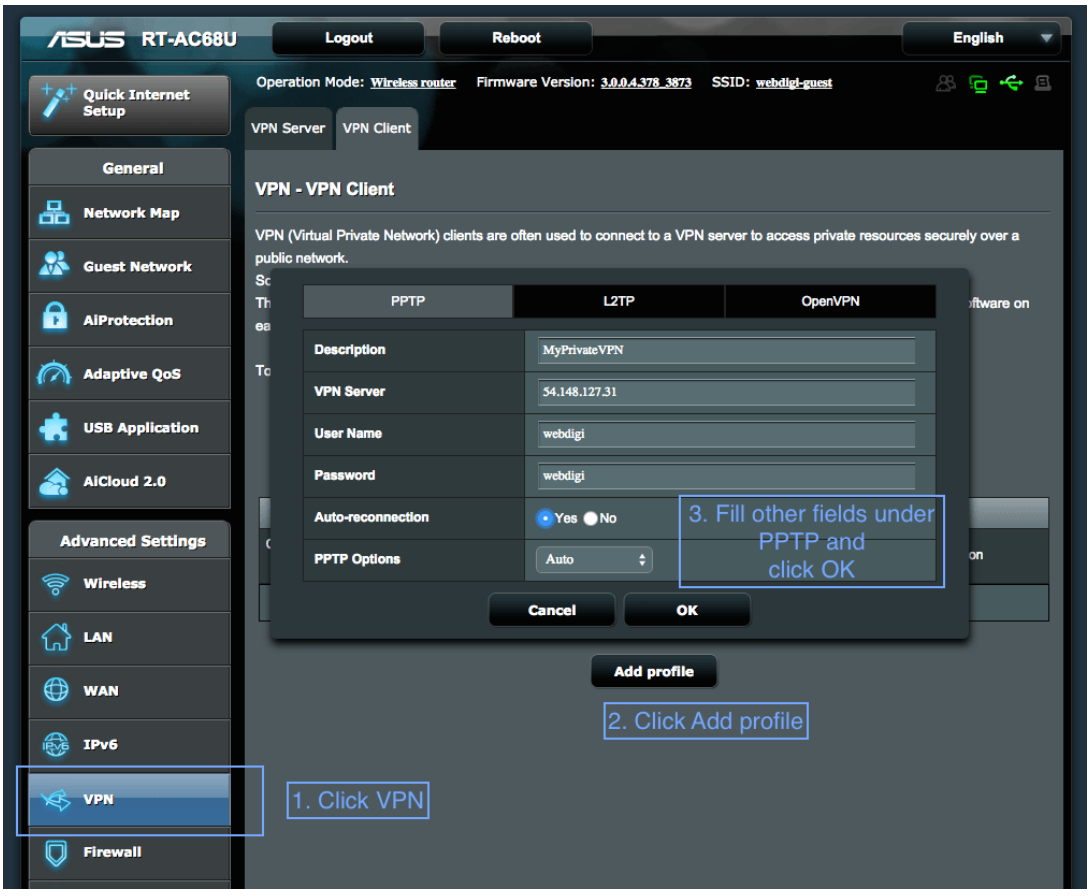

Network
Search
User Authentication:
Password:
RSA SecurID
Certificate
Select...
Kerberos
CryptoCard
8. Enter VPN password
Cancel
OK
Wi-Fi
Connected
Bluetooth PAN
Not Connected
Thund...lt Bridge
Not Connected
HomeBase
Not Connected
VPN (PPTP)
Not Configured
Account Name: webdigi
Encryption: Automatic (128 bit or 40 bit)
Authentication Settings...
Connect
Show VPN status in menu bar
Advanced...
Assist me...
Revert
Apply


Network
Search
Location: Automatic
Wi-Fi
Connected
Bluetooth PAN
Not Connected
Thund...lt Bridge
Not Connected
HomeBase
Not Connected
VPN (PPTP)
Not Configured
Status: Not Configured
Configuration: Default
Server Address: 54.148.127.31
Account Name: webdigi
Encryption: Automatic (128 bit or 40 bit)
Authentication Settings...
Connect
9. Click Advanced
Show VPN status in menu bar
Advanced...
Assist me...
Revert
Apply


Network
Search
VPN (PPTP)
Options
TCP/IP
DNS
Proxies
Session Options:
Disconnect when switching user accounts
Disconnect when user logs out
Send all traffic over VPN connection
Advanced Options:
Use verbose logging
10. Tick Send all traffic over VPN connection
Cancel
OK



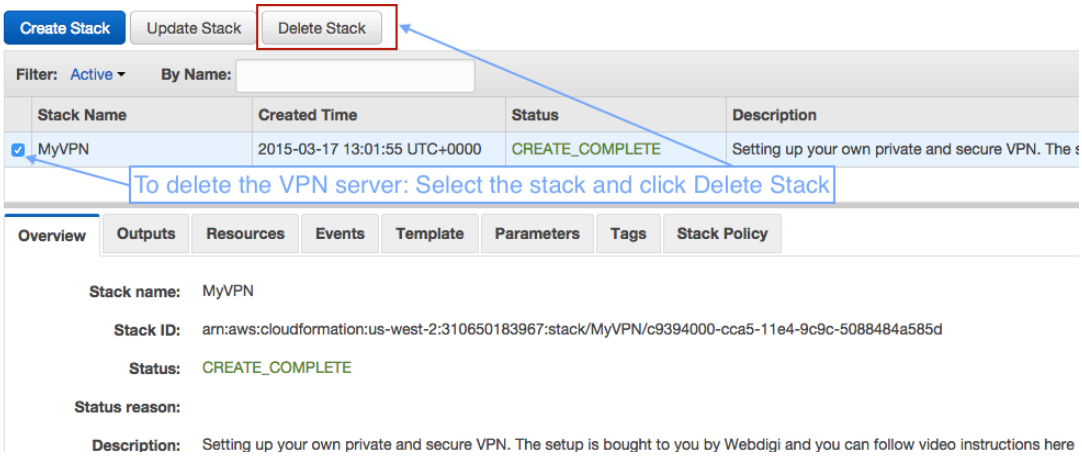
3. Setting up VPN on Asus RT-AC68U router



4. For all other devices please search for Setting up PPTP VPN on my iphone and so on. You can also setup an L2TP IPSEC VPN which is more secure but might not be supported on all devices.

Tips / Suggestions

1. If you want to delete your VPN server then just open CloudFormation on AWS. Make sure you select the same region that you created your VPN server. Then just click on Delete Stack button and your private VPN server will be removed.



2. You can have multiple VPN servers all over the world. You just have to repeat the setup steps in this guide by selecting different regions. Please note that AWS free tier gives you a total of 750 hours a month free. You can also delete and create VPN servers as frequently as you want.

3. Setting up a VPN connection on your router will allow all devices on its network to use the VPN server. This could be beneficial for use with AppleTV / Chromecast and any device that does not support a VPN.

4. You can test if your VPN connection is active by just searching for “what is my ip address” on your favourite search engine. The IP address reported will be that of your private VPN server if everything is your connection is enabled. If your VPN connection is not enabled or if the VPN server settings are not complete then it will report your ISP’s IP address.

5. We love your feedback and let us know if you face any issues in the comments section below or on our github page for setting up your private VPN on AWS.

46
COMMENTS

Also read...

113 **How to check if an email address exists without sending an email?**

1 **A single kill switch for 90% of the top ten websites**