**Computer Science Internal Assessment**

How can a secure, free-to-use Virtual Private Network (VPN) be developed to ensure privacy and encryption for users while maintaining ease of use?

**Introduction:**

Hello, I’m an I.B. student from Barcelona, Spain and I have been taking computer science courses for the last 18months. My advisor for this project will be my computer science teaches, Mr. Nicolas Philippe.

My client is a good friend of mine, Sergi who is owner of a small team of freelancers who offer different type of freelancing such as video editing, photoshop editing, website design and etc. He and his team often work with different companies from all over the world, therefor they usually use applications and websites that clients give from their country, and the most of these websites and applications are blocked and only are accessible by being the citizen of the country the website is made in. So to bypass the country block, the team uses a free-to-use VPN with low speed and low security quality, with this information, my friend Sergi asked me for help as he already knew that I study computer science, and I could not help but agree.

So I got a idea to make a free-to-use VPN for Sergi’s team so they can access customer’s websites and applications without being scared to lose their data or having problems with low speed internet.

To make a successful and to solve my client’s problem, I will state four different potential solutions that can demonstrate success of my program:

1. Best case scenario – the program will be fully functional with all features listed below:

1. Best possible speeds of internet.
2. Secured connection (the VPN has to have a fire wall protection in case someone unethical would like to steal your data).
3. Being accessing to not only my client’s team but the rest of the world by making the program public.
4. Making the program as an open-source application

2. Likely case scenario – the program will be functional but may have some small bugs with features listed below:

a. A good internet speed

b. Will be secure for unethical hackers or malware programs.

c. People outside the project may have access to the program

d. Wont be an open source, could not be modified by users.

3. Minimal case scenario – the program will bootup and it may have a decent working VPN and will have way more bugs expected, won’t have it’s own server, the program will be using open VPN tunnels that have poor internet quality and poor connection security. Won’t have any design.

4. Lowest possible case scenario – Program won’t function at all, the VPN feature won’t work at all, won’t have any design at all, the program will be full of bugs and may not even bootup.

My program will have it own “server” which will be a personal computer system in which will connect the device with a VPN, by that I mean that it will be a middle program, which will get the open tunnel VPN (from different countries’ that have this open tunnel system) after that it will run the code, and decode it so no malware cannot get into the users machine/system.