**ASSIGNMENT 1**

**1. What is a proxy?**

Normally when you browse the web, your computer connects to a website directly and begins downloading the pages for you to read. This process is simple and direct.

When you use a proxy server, your computer sends all web traffic to the proxy first. The proxy forwards your request to the target website, downloads the relevant information, and then passes it back to you.

Why would you do this? There’s a couple of reasons:

You want to browse a website anonymously – all traffic appears to come from the proxy server, not your computer.

You need to bypass a content restriction. Famously, your UK Netflix subscription won’t work in the USA. But if you connect to a UK proxy server it looks like you are watching TV from the UK and everything works as expected.

Although they work very well, there’s also a few problems with proxies:

All of the web traffic that passes through a proxy can be seen by the server owner. Do you know the proxy owner? Can they be trusted?

Web traffic between your computer and proxy, and proxy and website is unencrypted, so a skilled hacked can intercept sensitive data in transit and steal it.

**What is a VPN?**

A VPN is quite similar to a proxy. Your computer is configured to connect to another server, and it may be that your route web traffic through that server. But where a proxy server can only redirect web requests, a VPN connection is capable of routing and anonymising all of your network traffic.

But there is one significant advantage of the VPN – all traffic is encrypted. This means that hackers cannot intercept data between your computer and the VPN server, so your sensitive personal information cannot be compromised.

**VPNs are the most secure choice**

By encrypting and routing all of your network traffic, the VPN has a distinct advantage over a proxy server. And more than simply anonymising your web activities, a proxy server offers additional functionality too.

Take the Panda Dome VPN service. Not only does it anonymise your internet traffic and help you circumvent geographic filters, but traffic is also carefully inspected and filtered. Our VPN servers check every request and block anything that is known to be dangerous, like websites that host malware.

Routing your web traffic through an advanced VPN helps you avoid malware infections, phishing scams and fake websites. And because Panda’s servers are constantly updated, you are protected around the clock from sophisticated cybercrime attacks.

You can get started with the Panda VPN now – for free – here. And for more help and advice about staying safe online, take a look at the practical tips in the Panda Security blog.

**2. Can a server act as client?**

There are many types of servers, including web servers, mail servers, and virtual servers. An individual system can provide resources and use them from another system at the same time. This means that a device could be both a server and a client at the same time.