Task#7

Set up a proxy using an automatic configuration script

By default, Windows 10 is set to automatically detect proxy settings. However, this may not work when you're connected to your company's business network. One way to set up a proxy is to specify a script address that is given to you by the network administrator or by the company's IT department. When using a configuration script for a proxy server, note that its address is similar to a URL (the address of a website), such as http://my.proxy.server:8000/.

To set a proxy using an automatic configuration script, follow these steps:

Open Settings.

Click Network & Internet.

The list of network- and Internet-related settings appears.

Click Proxy.

The list of available proxy settings appears.

In the Automatic Proxy Setup section, set the Use Setup Script switch to On.

Enter the script address as it was given to you; then click Save.

Close Settings.

Set up a proxy manually

Another way to set a proxy is to manually enter its IP address and port number. The address of a proxy server is similar to that of any computer on the network, and it could be something like: 192.168.1.211. The port can be any combination of up to four figures. It can be any combination of digits, including 80 or 8080, depending on how its administrator(s) set it.

Task#7

The IP address and port of your company's proxy server are given to you by the network administrator or by the company's IT department. Here's how to set a proxy manually in Windows 10:

Open Settings.

Click Network & Internet.

The list of network- and Internet-related settings appears.

Click Proxy.

The list of available proxy settings appears.

In the Manual Proxy Setup section, set the Use a Proxy Server switch to On.

In the Address field, type the IP address.

In the Port field, type the port.

Click Save; then close the Settings window.

Task#7

In Internet Explorer: .

1. Go to **Tools** >> **Internet Options** >> **Connections** >> **LAN Settings**.

2. Then In Proxy Server Section, check **< Use Proxy Server for your LAN >** and **< Bypass proxy server for local addresses >** .

3. Set the desired proxy server address (**<< Click Here For Proxy Details >>**)

   Then, Click **< OK>**

4. Click on **Advanced Settings**.

In Mozilla: .

1. Go to **Tools** >> **Options** >> **Network** >> **Settings**.

2. Select **Manual Proxy Configuration** and set the desired proxy server details (**<< Click Here For Proxy Details >>**)

Task#7

In Google Chrome: .

1. Go to **Wretch** >> **Options** >> **Under the Hood** >> **Change Proxy Settings** >> **LAN Settings**.

2. Then check **< Use a Proxy Server for your LAN >** and **< Bypass proxy server for local addresses >** .

3. Set the desired proxy server address (**<< Click Here For Proxy Details >>**)

   Then, Click **< OK>**

4. Click on **Advanced Settings**.

Task#7

What is a proxy server?

Proxy servers act as relays between the website you're visiting and your device. Your traffic goes through a middle-man, a remote machine used to connect you to the host server. The proxy server hides your original IP address so that the website sees the IP of the proxy (in some cases, the computers of other proxy users are used for this). However, proxies only work on the application level, meaning it only reroutes the traffic coming from a single app you set your proxy up with. They also don't encrypt your traffic.

There are three main types of proxy servers:

- HTTP Proxies – These only cater to web pages. If you set up your browser with an HTTP proxy, all your browser traffic will be rerouted through it. They are useful for web browsing and accessing geo-restricted websites.
- SOCKS Proxies – These proxies are not limited to web traffic but still only work on the application level. For example, you can set it up on a game, video streaming app, or a P2P platform. Although they can handle all kinds of traffic, they are usually slower than HTTP proxies because they are more popular and often have a higher load.
- Transparent proxies – These are a different kind of proxy because their users are usually unaware of their existence. These proxies can be set up by employers or parents who want to monitor users' online activity and block access to specific websites. Hotels and cafes use them to

authenticate users on public Wi-Fi and companies or home users might also set them up to save bandwidth.

Task#7

What is a Virtual Private Network?

Like a proxy, a VPN also reroutes your internet traffic through a remote server and hides your IP address so websites can't see your original IP or location. However, it works on the operating system level, meaning that it redirects all your traffic, whether it's coming from your browser or a background app.

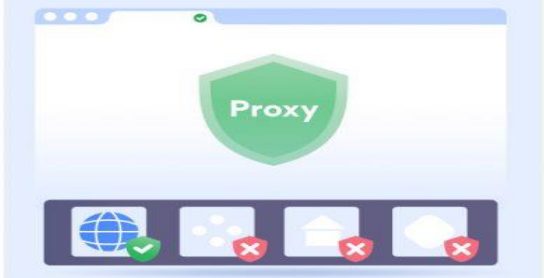
A VPN also encrypts your traffic between the internet and your device. That means the Internet Service Provider (ISP) monitoring your internet activity and collecting data about you can no longer see what you're doing online – just that you're connected to a VPN server. The encryption also protects you from government surveillance, website tracking, and any snoopers or hackers who might try to intercept your device. A VPN provides you ultimate online privacy and security.

It's important to note that both VPN and proxy providers can log user data such as user IP addresses, DNS requests, and other details. You should avoid such providers because they can give this information to law enforcement agencies, advertisers, or hackers if their servers get breached. To keep your activity online truly private, look for a provider that has a strict no-logs policy.

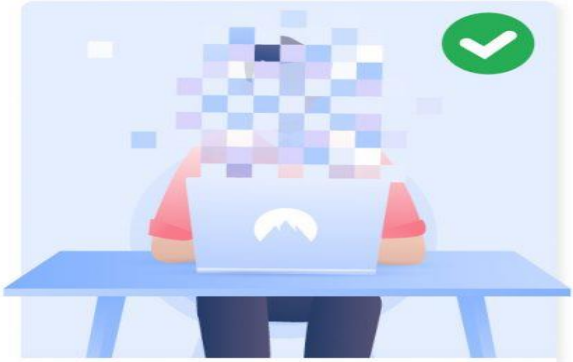
Task#7

VPN vs Proxy

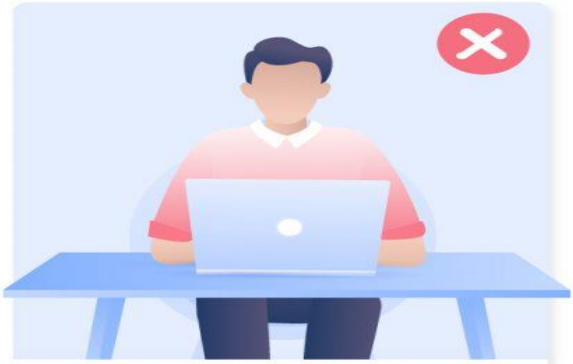
Protects all your internet traffic



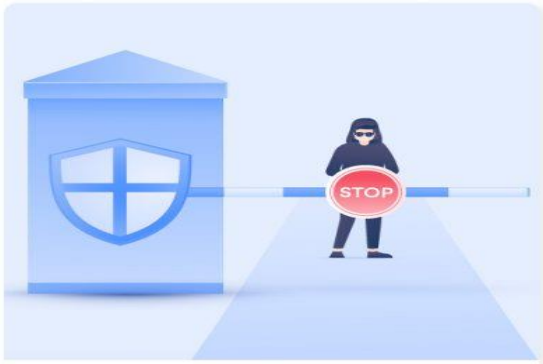
Protects only your browser or a certain app



Encryption



Encryption



Good for:

- Anonymous web browsing
- Viewing geo-blocked content
- Protecting yourself from hackers
- Preventing ISP tracking

Good for:

- Anonymous web browsing
- Viewing geo-blocked content

Task#7

Here is a quick comparison between the two:

- VPNs encrypt your traffic while proxy servers don’t. A VPN service protects you from ISP tracking, government surveillance, and hackers. Proxies don’t, so they should never be used to handle sensitive information;
- VPNs work on the operating system level and reroute all your traffic while proxies work on the application level and only reroute the traffic of a specific app or browser;
- VPNs can be slower than proxies as they need to encrypt your data; however, there are ways you can improve your connection and browsing speeds;
- VPNs are usually paid (you shouldn’t trust free VPN services as they have limitations and tend to mine your data) while many proxy servers are free;
- A VPN connection is more reliable while proxy server connections drop more frequently.