1..What is the difference between VPN and proxy? Which one should we go for if we want to have privacy strictly?

Ans:- Both VPNs and proxy servers are tools you can use to help keep your activity private when browsing the internet, sending emails, reading online message boards, streaming video, and downloading files. But both of these tools work in different ways.

A proxy server is a computer that sits between you and a server, acting as a gateway when you access the internet. When you connect to a specific website, video-streaming app, or file-sharing program from your laptop, tablet, smart phone, or any other device, you can first connect to a proxy. Once you do this, you’ll be connecting to the site or app through an outside host server.

There’s a clear benefit to this if you want to hide your identity. The website you are visiting or the streaming service you are accessing or file sharing site you are using will only see the IP address belonging to the proxy server. It won’t see your address. This will keep your identity and true location hidden from these sites and apps.

VPN encrypts the information :- The biggest benefit of a VPN is with VPN enabled, your browsing and any data you send or receive, will be encrypted. This is important: It means that hackers, government agencies, businesses, or anyone else won’t be able to see what you’re doing when online.

VPN providers promote online privacy :- If you want total privacy, work with a VPN provider that has a no-log policy. “No log” means the providers pledge not to track and store your activity while you are using the service to connect to the internet. This means that these providers won’t have any data to give to anyone else who wants information about what sites you browse or files you share. On the other hand, a free proxy may monitor traffic and sell data to third-parties.

VPN provider that charges a fee because paid services often offer more data privacy, more secure connections, and more reliable performance. Security of free VPN can be unreliable, as many providers use only one VPN connection, called point-to-point protocol (PTTP). A paid VPN service, on the other hand, can offer users data encryption which is more secure.

which one should we go for if we want to have privacy strictly?

If you want to hide your IP address, using either a proxy server or VPN will work. And if you’re worried about browsing speed, and you’re only worried about hiding your IP address from a single site or app, then a free proxy server will do the job.

If cost is an issue, then connecting to single sites, apps, or file-sharing services through a proxy server might be the smart move. It’s easy to find free proxy servers that will hide your IP address.

But if you want to keep your browsing activity hidden from snoops, logging onto the internet through a VPN is the better choice. Again, it comes down to encryption: VPNs encrypt your data while online. Proxy servers don’t.

If you plan to access several sites while online, especially if you’re connecting to sites such as your bank account or credit card portal, a VPN provides more security.

And while many of the preferred VPN providers will charge for their services, this price might be a small one to pay if it means that your most sensitive personal and financial information is shielded from the eyes of online snoops

2) can a server act as a client?

Ans:- No, a client can’t work as a server since Client cant host or stores large amount of data, it can read data only from the server, it can't act independently. Whereas the server can act as a client for example a server of FB can send a request to Google servers. The client and the server are always decoupled. If we want to change the UX alone we shall change the client code alone w/o the server code unaffected.