***Research Findings***

***Author: Vineeth M***

***Date: 24/10/2025***

***1.ISP (Internet Service Provider)***

*Internet Service Providers (ISPs) are companies that provide individuals and businesses with access to the internet. They connect users to the internet through various technologies such as DSL, fiber-optic cables, and wireless connections. Beyond basic connectivity, ISPs often offer additional services like email, web hosting, and online storage. Since ISPs enable Internet access, they have a big responsibility to make sure their networks are secure and that users can browse safely. By analyzing traffic patterns, ISPs can detect and mitigate potential threats more efficiently.*

*Internet Service Providers (ISPs) have several important duties to ensure smooth and secure internet access.* ***Providing internet access*** *involves connecting users through various technologies like dial-up, DSL, cable, wireless, and fiber-optic connections, each offering different speeds and coverage depending on the infrastructure.* ***Network infrastructure maintenance*** *requires ISPs to manage and repair routers, switches, cables, and servers, ensuring the network remains reliable and uninterrupted for all users.* ***Routing internet traffic*** *means ISPs direct data packets efficiently between devices and networks, making sure information reaches the correct destination quickly and accurately.* ***Resolving domain names*** *involves converting human-friendly website addresses into IP addresses that computers use to communicate, a crucial step for accessing online content.* ***Offering additional services*** *allows ISPs to provide value-added options like email accounts, domain registration, web hosting, and cloud storage, which support both individual and business users in managing their online presence.*

***How the ISP Provide Privacy and Security.***

### ***1. Private IP Addresses***

*ISPs assign* ***private IP addresses*** *to customer devices, such as those in the ranges 192.168.x.x or 10.x.x.x. These private IPs are not routable on the internet, which means that customer devices remain hidden from external access, providing an added layer of privacy and security.*

### ***2. Network Address Translation (NAT)***

*To enable these private devices to access the internet,* ***Network Address Translation (NAT)*** *is used. NAT allows multiple devices on a local network to share a single public IP address. When data is sent out to the internet, NAT translates the private IPs into the public IP, making all outbound traffic appear to come from one address.*

### ***3. Carrier-Grade NAT (CGNAT)***

*ISPs use something called* ***Carrier-Grade NAT (CGNAT)*** *to make the most out of the limited number of public IP addresses available. CGNAT allows a large number of customers to share just a few public IP addresses, helping the ISP serve many people without needing a huge number of public IPs. This method not only saves valuable IP resources but also provides an extra layer of* ***privacy and security****, since individual customer devices are hidden behind the shared public IP. As a result, it becomes much harder for outsiders to directly access or identify a specific user’s device on the internet.*

### ***4. Firewalling & Access Control Lists (ACLs)***

*ISPs use* ***firewalls*** *and* ***Access Control Lists (ACLs)*** *on their main routers to protect their internal network. These tools help* ***block any unauthorized access*** *to important systems such as DNS servers and management interfaces. Firewalls control what kind of traffic is allowed in or out of the network, while ACLs specify which IP addresses or ports can communicate.*

### ***5. MPLS VPNs for Enterprise Customers***

*For business clients, ISPs use* ***MPLS (Multiprotocol Label Switching)*** *to build* ***Virtual Private Networks (VPNs)*** *that keep company data separate and secure. In this system, data packets are given special* ***labels*** *that tell the network exactly where to send them. These labeled packets travel through the ISP’s backbone in a* ***private, isolated path****, ensuring that each company’s traffic stays separate from other companies. It works like having a* ***private tunnel inside the ISP’s network****, giving businesses the security and reliability of a private connection while still using the ISP’s shared infrastructure.*

### ***6. Encrypted Tunnels (IPsec, L2TP, WireGuard)***

*ISPs support* ***encrypted tunnels****, such as* ***IPsec, L2TP, or WireGuard****, to protect data sent over the internet. These tunnels create a* ***secure, private path*** *so that information cannot be intercepted by outsiders. For example,* ***remote workers*** *can safely connect to their company’s network from home using such a tunnel.*

### ***7. DNS Privacy (DoH/DoT)***

*Modern ISPs support* ***DNS privacy*** *using protocols like* ***DNS over HTTPS (DoH)*** *and* ***DNS over TLS (DoT)****. Normally, when you type a website address, your device asks a DNS server to find the site’s IP, and these queries are usually* ***sent in plain text****, which means anyone monitoring the network (including the ISP) can see which sites you visit. DoH and DoT* ***encrypt these DNS queries****, keeping them private so that outsiders cannot easily snoop on your browsing activity. This adds an extra layer of* ***security and privacy*** *while using the internet.*

### ***8. BGP Routing Control (Keeping Internal Networks Private)***

*ISPs use* ***BGP (Border Gateway Protocol)*** *to tell the internet which public IP addresses they own. They* ***only share public IPs****, while private internal addresses (like 10.10.10.0/24 used inside their network) are* ***kept hidden****. Using* ***route filtering****, ISPs make sure these internal addresses are never sent to the internet. This way,* ***the outside world cannot see the ISP’s internal network****, keeping their systems and customer data safe.*

***2.Virtual Private Network – VPN***

*A* ***VPN (Virtual Private Network)*** *is a tool that protects your internet connection by creating a* ***secure tunnel*** *between your device and the internet. It* ***hides your IP address****, encrypts your data, and prevents hackers or ISPs from tracking your online activity. VPNs also allow you to* ***access websites or content*** *that might be blocked in your area, keeping your browsing private and anonymous.*

*When you use a VPN, your device connects to a* ***remote server*** *operated by the VPN provider. All your internet traffic is* ***encrypted*** *and routed through this server, making it appear as if you are browsing from the server’s location rather than your real IP. The server then decrypts your data and sends it to its destination, while responses return through the same secure tunnel. This ensures that your online activity remains* ***private, secure, and anonymous****.*

***How the VPN Provide Privacy and Security.***

### ***1. Encryption (The Core of Privacy)***

*VPNs use* ***encryption*** *to protect your data by scrambling it so that anyone trying to intercept it cannot read it. This includes everything you send or receive online. Strong encryption ensures that even if someone gets access to your data, it would appear as* ***unreadable gibberish*** *without the correct decryption key. This is the* ***core feature*** *of a VPN that keeps your online activity private and secure.*

### *****2. Tunneling (Hides Your Real Path)*****

*A VPN wraps your data inside a* ***secure tunnel*** *that goes from your device to the VPN server before reaching the internet. Your ISP only sees that you’re connected to the VPN server, while websites see the server’s IP instead of your real one. This* ***hides your real IP address and browsing activity****, keeping your online path private.*

### *****3. IP Address Masking*****

*A VPN* ***hides your real IP address*** *by replacing it with the IP of the VPN server. Without a VPN, websites can see your home IP, but with a VPN, they see the server’s IP instead. This makes it appear as if you are browsing from a* ***different location****, protecting your privacy and location.*

### *****4. No Logs (Optional but Critical for Privacy)*****

*Some VPNs, especially privacy-focused ones, follow a* ***no-logs policy****, meaning they do not record your activity, timestamps, or original IP address. These policies are often* ***audited by third parties*** *to verify compliance. Even if required by law, such VPNs* ***cannot reveal your browsing history****, keeping your online activity private.*

### *****5. DNS Leak Protection*****

*Sometimes, DNS requests can bypass the VPN tunnel and reveal your real ISP. VPNs prevent this by* ***forcing all DNS queries to go through their encrypted DNS servers*** *instead of your ISP. They also use secure protocols like* ***DoH or DoT****. This ensures that* ***no one, including your ISP, can see which websites you are visiting****, keeping your browsing fully private.*

### *****6. Kill Switch (Prevents Leaks)*****

*A VPN* ***kill switch*** *protects you if the VPN connection suddenly drops. It* ***instantly blocks all internet traffic*** *until the VPN reconnects, preventing your real IP address or data from being accidentally exposed. This ensures that your* ***online activity stays private*** *at all times.*

### *****8. Server-Side Privacy Techniques*****

*Privacy-focused VPN providers take extra steps to protect users. They often* ***run servers on RAM only****, so all data is wiped when the server reboots. They allow* ***anonymous sign-ups and cryptocurrency payments*** *to minimize personal information collection. Many are also* ***based in privacy-friendly countries****, such as Switzerland or Panama, where laws better protect user privacy. These measures keep your data secure even on the provider’s side.*

### ***9. Split Tunneling (Optional Control)***

***Split tunneling*** *lets you decide which internet traffic goes through the VPN. You can route* ***all traffic*** *through the VPN for maximum privacy, or only* ***specific apps or websites*** *(like streaming services) to balance* ***speed and privacy****. This gives you* ***flexible control*** *over your connection.*

*****3.Proxy Server*****

*A* ***proxy server*** *is an intermediary between your device and the internet. Instead of connecting directly to a website, your requests go through the proxy, which forwards the responses back to you. Proxy servers can* ***act as a firewall*** *to block threats,* ***filter web content****,* ***share network connections****, and* ***cache data*** *to make frequently visited websites load faster. They also provide an extra layer of* ***privacy*** *by hiding your real IP address and protecting your internal network from potential online threats.*

### ***How a Proxy Server Operates***

*Every device on the internet has a unique* ***IP address****, like a street address, so data knows where to go. A proxy server has its own IP address and sits between your device and the internet. When you send a web request, it goes to the proxy first. The proxy makes the request on your behalf, collects the response, and sends it back to you. While doing this, it can* ***hide your location by changing your IP****,* ***encrypt your data****, or* ***block access to certain websites****, helping to protect your privacy and improve security.*

*****How the VPN Provide Privacy and Security.*****

***Hide your real IP  
A proxy hides your real IP address, so websites see the proxy’s IP instead of yours. This helps keep your location and identity more private.***

***Act as a middleman*** *When a proxy* ***acts as a middleman****, your device sends requests to the proxy instead of directly to the website. The proxy then makes the request to the website using its own connection or session. The website responds to the proxy, which forwards the data back to your device. This way, the website sees the proxy as the client, not you, and your browser receives the page through the proxy. In simple terms, the proxy* ***loads the website on its side first*** *and then sends it to you, keeping your real IP hidden.*

***Support IP rotation******IP rotation*** *means that a proxy automatically changes the IP address it uses for your requests. Without rotation, a website sees the same IP every time you visit, making it easier to track your activity. With rotation, each request can come from a different IP, so websites see multiple addresses instead of just one. This makes it much harder for sites to identify or follow you, helping you stay more* ***anonymous online****.*

***Bypass geo-restrictions*** *Proxies can make it appear as if you are browsing from a different country, allowing access to content that might be restricted in your region.*

***SOCKS5 proxies support both TCP and UDP***

***trafficSOCKS5 proxies support both TCP and UDP traffic, making them more flexible than standard HTTP proxies. TCP is used for most web activities like browsing and downloading files, while UDP is used for faster, real-time applications like online gaming, video calls, or streaming. Because SOCKS5 can handle both types of traffic, it works for a wider range of applications, not just web browsing, making it a versatile choice for privacy and performance.***

### *****What Proxies Don’t Do (Limitations)*****

*Proxies do* ***not provide full privacy by default****. They usually* ***don’t encrypt your data****, so your ISP and the proxy provider can see your activity unless you use HTTPS sites. The proxy provider can also see your* ***real IP, full URLs, headers, and unencrypted traffic****. Your ISP knows you’re using a proxy and may see some traffic in plain text. Proxies often* ***don’t prevent DNS leaks****, meaning your ISP can still see which websites you visit unless you change DNS settings. They have* ***no kill switch****, so if the proxy fails, your real IP can be exposed. Most proxies work* ***only per app****, like a browser, and* ***transparent proxies don’t hide your IP at all****, so websites can still see your real address.*