A **proxy server** is an **intermediary** between a client (you) and the internet (server).

Instead of:

User → Website

It works like:

User→ Proxy → Website

Website → Proxy → User

The website **does not see your real IP address**; it sees the **proxy's IP**.

A **VPN (Virtual Private Network)** creates a **secure, encrypted tunnel** between your device and a remote server.

Instead of:

User→ Internet → Website

With VPN:

User→ Encrypted Tunnel → VPN Server → Website

Website → VPN Server → User

The website sees the **VPN server's IP**, not your real IP.

Proxies and VPNs are essential tools in cybersecurity with dual uses: attackers exploit them to conceal their identity and location during malicious activities, while ethical hackers, investigators, and defenders rely on them to safeguard privacy, conduct safe research, and protect sensitive operations.
Both can mask IP addresses, but they differ significantly in scope, security, and reliability — VPNs generally offer stronger protection through full encryption, while proxies provide lighter, often faster IP masking.
Understanding this duality is key because the same technology that enables anonymity for legitimate privacy needs can also facilitate cybercrime if misused.

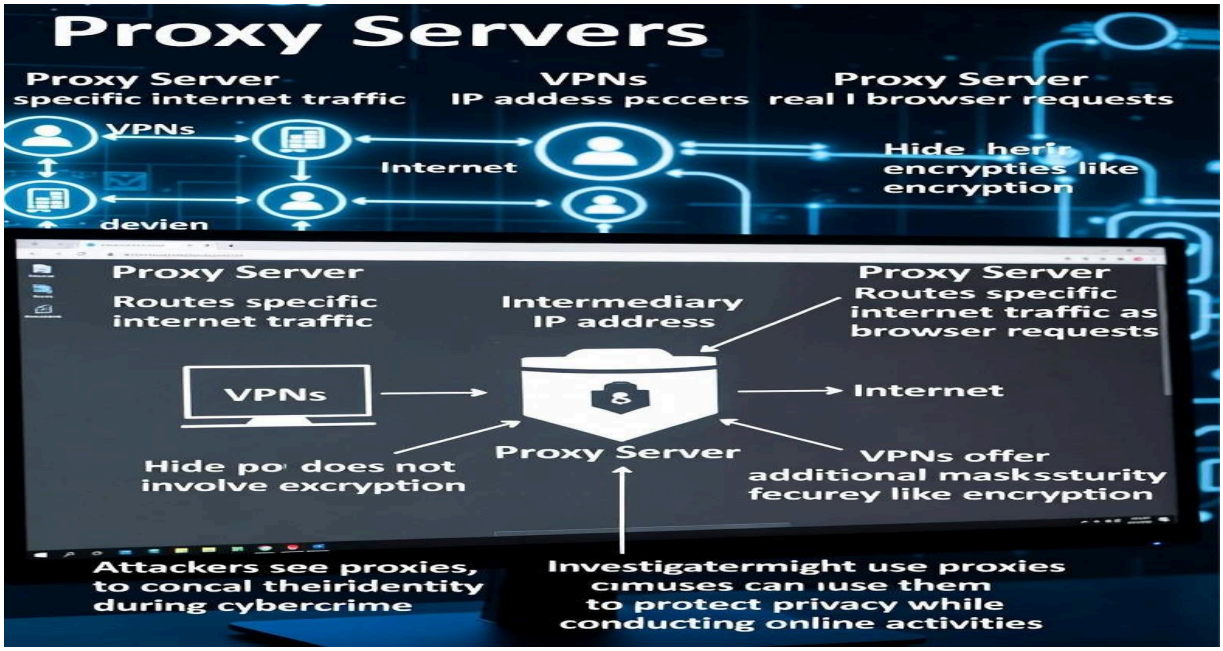
Main differences at a glance
Proxies route specific traffic (e.g., browser only) through an intermediary server to hide your IP — fast and simple but usually without encryption.
VPNs create an encrypted tunnel for all device traffic, hiding your IP and protecting data from interception — slower but far more secure.

Attackers favor chains of proxies/VPNs or residential proxies for evasion; investigators prefer audited no-logs VPNs for defensible privacy.

Why this matters
The line between offensive and defensive use is often blurry — the same tool can protect a whistleblower or hide a ransomware operator. Responsible use requires choosing reputable services, understanding logs policies, and combining tools with other security practices.

Proxies and VPNs in Cybersecurity: Dual-Use Tools for Anonymity, Evasion, and Protection
Proxies and Virtual Private Networks (VPNs) stand as two of the most widely deployed technologies for altering how your internet traffic appears to the world. They both obscure your real IP address, but they operate differently, provide varying levels of protection, and serve contrasting purposes depending on the user.

A **proxy server** acts as an intermediary: your device sends requests to the proxy, which forwards them to the target website and returns the response. This hides your IP from the destination site, making it appear as though the proxy's IP is the origin. Proxies come in various types — HTTP/HTTPS (web-focused), SOCKS5 (more versatile), transparent (no hiding), anonymous (hide IP but reveal proxy use), and elite/high-anonymity (fully mask both). Most proxies do not encrypt traffic, meaning data remains visible to anyone monitoring the connection (e.g., ISPs, Wi-Fi owners, or potential interceptors). Speed is usually excellent because there's no encryption overhead, but security is limited — free/public proxies often log data, inject ads, or are controlled by malicious actors.



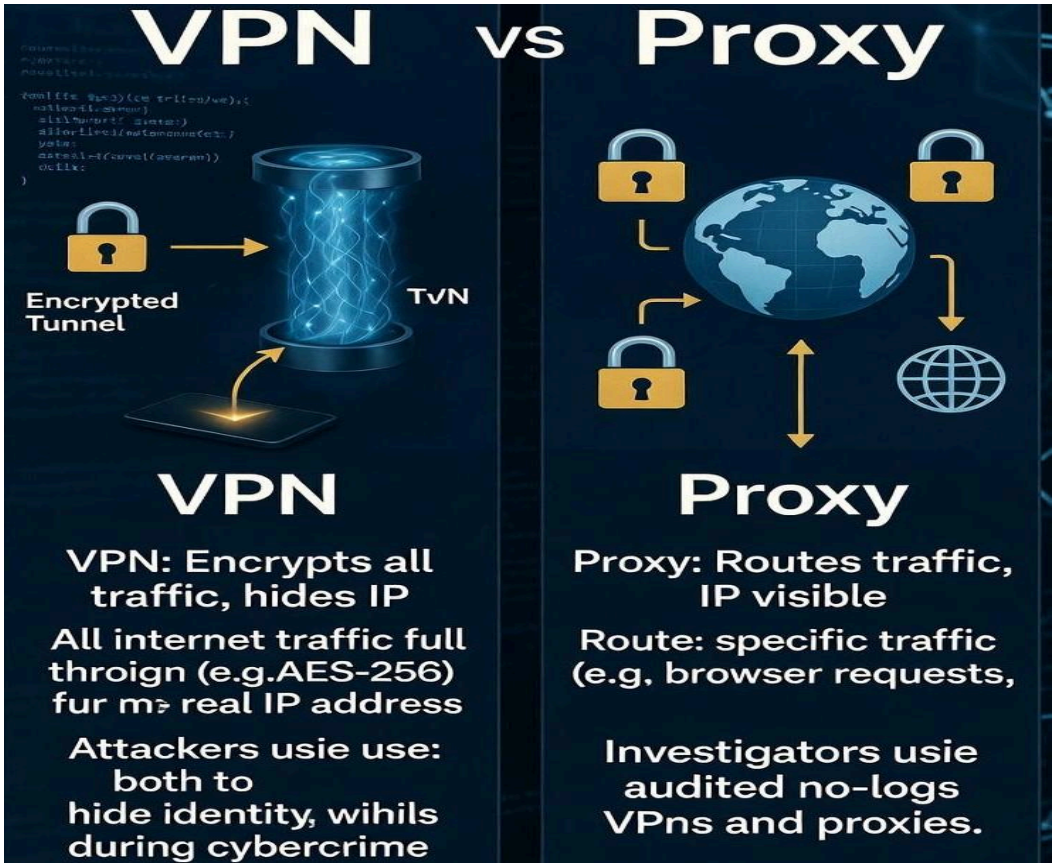
A **VPN**, in contrast, establishes a full encrypted tunnel between your device and a VPN server, routing all internet traffic (not just browser sessions) through it. Modern VPNs use strong protocols (WireGuard, OpenVPN, IKEv2) and ciphers (AES-256) to ensure confidentiality, integrity, and authenticity. The VPN server assigns you a new IP, and your ISP sees only encrypted traffic to the VPN provider. Reputable no-logs VPNs (audited by third parties) do not record browsing history, making it extremely difficult to trace activity back to you — even under legal pressure.

Offensive Use: How Attackers Exploit Proxies and VPNs

Cybercriminals rely heavily on these tools to break the chain of attribution. Residential proxies (IPs from real home ISPs) and rotating proxy networks make malicious traffic appear as normal user behavior from diverse locations, evading rate-limiting, IP bans, and fraud detection. Attackers chain multiple proxies/VPNs (multi-hop) or combine them with Tor for added layers. Commercial VPNs with no-logs policies or jurisdictions resistant to cooperation (e.g., certain offshore locations) are popular for launching phishing, credential stuffing, ransomware deployment, botnet C2, and fraud (e.g., account takeovers, promo abuse). In high-profile cases like the 911 S5 botnet or ransomware operations, attackers used VPNs/proxies to mask origins, complicating investigations until advanced techniques (e.g., Canarytokens, honeypots) partially defeated the anonymity.

Defensive/Legitimate Use: How Investigators and Ethical Hackers Employ Them
On the blue-team side, proxies and VPNs are indispensable for privacy and operational security (OPSEC). Ethical hackers (penetration testers) use residential proxies or VPNs to simulate real-world attacker infrastructure during red-team exercises, test detection rules without exposing their real IP, or bypass geo-blocks for reconnaissance. Investigators (DFIR teams, threat hunters, law enforcement cyber units) rely on audited no-logs VPNs when conducting open-source intelligence (OSINT), accessing threat intelligence portals, or researching malicious sites — preventing retaliation (e.g., DDoS against their home IP) or doxxing. Corporate security teams deploy VPNs for remote workers on public Wi-Fi, and researchers use them to avoid fingerprinting/tracking by malicious actors. Best practices include:

Choose audited no-logs providers (e.g., Mullvad, ProtonVPN, NordVPN — frequently audited in 2025–2026).
Prefer WireGuard for speed/security balance.
Use kill-switches and leak protection.
Combine with browser hardening (e.g., uBlock Origin, NoScript).
Avoid free proxies/VPNs — they often log/sell data or are honeypots.



Comparison Table: Proxies vs VPNs in Offensive & Defensive Contexts

Aspect	Proxies	VPNs	Attacker Preference	Defender/Investigator Preference
Encryption	Usually none (except SOCKS5 with added layers)	Full (AES-256, ChaCha20, etc.)	High (for speed/evasion)	High (for data protection)
Scope	App-specific (e.g., browser only)	Entire device	High (targeted tasks like scraping)	High (full OPSEC)
Speed	Very fast	Fast to moderate	Preferred	Acceptable
Anonymity Level	Low to medium (easy to detect many types)	Medium to high (with no-logs)	High (especially residential/rotating)	High (audited no-logs)
Detection Difficulty	Often detected (datacenter IPs flagged)	Harder (shared residential-like IPs)	High	High
Common Dual-Use Risks	Logging, MITM, injection	Provider cooperation, endpoint compromise	Exploitation for evasion	Trust in provider, potential leaks
2025–2026 Trends	Rise of residential/rotating proxies for fraud	Audits, post-quantum prep, multi-hop features	Increasing sophistication	Stronger emphasis on audited services

Tor as a Related Tool

Tor (The Onion Router) deserves mention for extreme anonymity: it routes traffic through multiple volunteer nodes with layered encryption, offering stronger unlinkability than most VPNs/proxies. Attackers sometimes use Tor for C2 or access; defenders/investigators use it for high-risk OSINT (e.g., accessing dark web intel). However, Tor is slower, exit nodes can see unencrypted traffic, and many sites block Tor IPs.

Broader Implications in 2026

The dual-use nature creates tension: governments and platforms increasingly target VPN/proxy traffic for blocking or surveillance, while privacy advocates push for stronger protections. Recent research (2025 papers) shows techniques like Canarytokens/honeypots can unmask 40–70% of VPN/proxy/Tor users in specific scenarios, underscoring that no tool guarantees perfect anonymity. Responsible cybersecurity requires balancing privacy needs with accountability — choosing transparent, audited services, and understanding that misuse can have severe legal consequences.

Key Citations

https://us.norton.com/blog/privacy/proxy-vs-vpn
https://www.bitdefender.com/en-gb/blog/hotforsecurity/vpn-vs-proxy-understanding-different-privacy-protection-tools
https://www.cherryservers.com/blog/vpn-vs-proxy-differences
https://trueguard.io/blog/how-fraudsters-use-vpns-proxies-exploit-products
https://www.scworld.com/feature/novel-technique-can-unmask-up-to-70-of-crooks-hiding-behind-vpns-proxies-tor
https://www.mdpi.com/2078-2489/16/2/126
https://www.freecodecamp.org/news/vpns-vs-proxies-what-are-the-differences/
https://nordvpn.com/blog/vpn-vs-proxy/
https://kelvpn.com/blog/vpn-proxy-tor-anonymity-comparison
https://www.pcmag.com/comparisons/tor-vs-vpn-the-battle-for-online-anonymity