Congressional Research Service
Informing the legislative debate since 1914

MEMORANDUM August 14, 2026

To: Senator Ron Wyden
Attention: Chris Soghoian

From: [redacted]

Subject: **Consumer VPNs**

This memorandum responds to your request for information on virtual private network (VPN) services available to consumers. Specifically, you requested that this memorandum compare the security benefits and risks of VPN services, and that it discuss legacy technologies as well as modern implementations of VPNs, cybersecurity threats posed by vulnerable VPNs, risks of cryptanalysis in consumer VPNs, abilities of governments to access data encrypted by consumer VPNs, and effects of post-quantum cryptography (PQC) on consumer VPNs.

Information contained in this memorandum is of general interest to Congress and may be used in other CRS products. Your confidentiality as a requestor will be preserved in any event. If you have additional questions, please do not hesitate to contact me.

VPN Overview

A virtual private network creates an encrypted connection, between a user's device and a remote server (like a private tunnel), masking the user's internet protocol (IP) address and shielding the traffic's content from anyone positioned between the device and the VPN server.[1] With a VPN, an internet service provider, a public Wi-Fi operator, or a network-level surveillance system would not be able to see what a user is doing online. Information is encrypted at the client (the user's device), sent to the VPN provider's server, decrypted on the provider's server, assigned a new IP address for the VPN provider, and forwarded to its destination on the public internet (e.g., the server hosting the website that the user wants to visit)—this means the VPN provider itself becomes a trusted intermediary that can see unencrypted traffic unless additional protections added.[2]

A VPN could be set up for business or personal use. An enterprise VPN allows employees to remotely and securely connect to and access an organization's internal networks and resources. Third-party commercial

[1] Microsoft, "What is a VPN (virtual private network)?" https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn.

[2] Fortinet, "VPN: Keeping Sensitive Data Protected Everywhere," 2026, https://www.fortinet.com/resources/cyberglossary/what-is-a-vpn.

providers also offer consumer-level services to individual users who emphasize data "privacy, security, and unrestricted internet access."[3]

Consumer VPNs have evolved from a tool primarily used to facilitate corporate remote access to a mass-market privacy product used by over a billion people to shield browsing habits, evade censorship, and protect data on untrusted networks.[4] But VPN construction differs and its underlying technologies may introduce risk. For instance, legacy protocols written in memory-unsafe languages such as C carry a persistently higher vulnerability burden than modern, memory-safe languages. Traffic-analysis resistance varies sharply between single-hop commercial VPNs and multi-hop designs (i.e., how many servers data route through before arriving at the destination); the number of these hops may matter for users concerned about government collection of web traffic.[5] Additionally, advanced nation-state adversaries have engaged in "harvest-now, decrypt-later" attacks where encrypted data are downloaded today with the hope of decrypting them later using emerging technologies such as quantum computing.[6]

VPN Benefits and Risks

VPNs can give consumers a more private and secure connection to the public internet, particularly when they are attaching to an untrusted network (e.g., a public coffee shop's Wi-Fi, or while traveling to a country that is known to analyze web traffic). In these cases, the VPN could help to mitigate a *man-in-the-middle* attack whereby an eavesdropper on the network can steal sensitive information from the user. By replacing the user's IP address with the one associated with the VPN provider, the VPN provider may also enable a user to access material that would otherwise by restricted by their geography.

VPNs are not a total security solution. A VPN does not make a user totally anonymous to their destination service (e.g., a user can still sign into that service with an account attached to their identity). VPNs do not prevent phishing attacks or malware delivery. In practice, consumers using a VPN are shifting their trust from their internet service provider to the VPN operator. This may be beneficial in certain applications (e.g., accessing geographically restricted content or securing internet browsing on public Wi-Fi networks). But, a legacy single-hop commercial VPN gives one company—and by extension, any entity able to compel or intercept that company's data—visibility into which users are connecting to which destinations on the internet.[7]

Specific to VPNs, there are a few unique risks: memory compromises, cryptanalysis, traffic analysis, and encryption protocols, which are discussed further below.

[3] PaloAlto Networks, "What is a VPN? A Complete Guide to Virtual Private Networks," https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn.

[4] Sviat Soldatenkov, "VPN Usage Trends 2025: Which Countries Lead in VPN Adoption?" blog post, October 29, 2025, https://outbyte.com/blog/vpn-usage-trends-2025-which-countries-lead-in-vpn-adoption/; Statista, "Virtual Private Networks," statistics report, 2025, https://www.statista.com/study/110798/vpns/.

[5] *Network traffic analysis* is performed by collecting and analyzing data from a network in order to determine the operations of the network, but may also reveal information about specific users. For more information, see Mesh Flinders and Ian Smally, "What is Network Traffic Analysis," *IBM*, https://www.ibm.com/think/topics/network-traffic-analysis.

[6] Brandi Vincent, "Report: China May Steal Encrypted Government Data Now to Decrypt with Quantum Computers Later," *NextGov*, November 21, 2021, https://www.nextgov.com/emerging-tech/2021/11/report-china-may-steal-encrypted-government-data-now-decrypt-quantum-computers-later/187020/. See also section on "Protecting National Security Interests in Quantum Computing," CRS Report R47685, by Ling Zhu, https://www.crs.gov/Reports/R47685#_Toc145340310.

[7] Casey Ford and Ania M. Piotrowska, "What is a mixnet? Unparalleled online privacy with a VPN," NYM, January 12, 2024, https://nym.com/blog/what-is-a-mixnet.

Memory Compromises

A substantial share of VPN client and server vulnerabilities trace not to weaknesses in cryptographic algorithms themselves but to the programming languages used to implement them. Older VPN solutions (e.g., the OpenVPN platform, most Internet Protocol Security [IPsec] protocol implementations, and the OpenSSL cryptographic software) are written primarily in C, a memory-unsafe language that requires developers to manually manage memory allocation. The Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Advisory Committee found in a 2023 review that a disproportionate share of critical open-source infrastructure, including networking and cryptographic libraries, remains written in memory-unsafe languages. Also, it found that memory-safety defects—buffer overflows, use-after-free errors, and heap corruption—continue to represent the largest single class of exploitable vulnerabilities across the software ecosystem.[8] A broader 2024 survey of open-source repositories reinforced this finding by showing that memory-unsafe code and its dependencies remain pervasive in exactly the kind of low-level networking software upon which VPN protocols rely.[9]

Cryptanalysis

Cryptanalysis is the study of techniques to defeat cryptographic methods. Legacy VPN deployments support negotiable *cipher suites*, which are common sets of cryptographic algorithms.[10] These cipher suites are built into products to provide flexibility and improve compatibility across a variety of hardware (where some older hardware might be incapable of processing newer cipher suites). This flexibility created a class of attacks called *downgrade* attacks where an adversary could force a connection to fall back to weaker cryptographic standards such as Triple Data Encryption Algorithm (3DES) or the Rivest Cipher 4 (RC4).[11] Internet Key Exchange (version 2)/Internet Protocol Security (jointly referred to as IKEv2/IPsec) security architecture deployments, in particular, have a long history of configurable cipher suites, and a misconfigured or legacy deployment running outdated cipher key establishment and exchange, or weak pre-shared keys remain more susceptible to cryptanalytic or brute-force attack than fixed modern suites.[12]

Some VPN implementations eliminate this vulnerability by hard-coding a single, modern cipher suite for key exchange (e.g., ChaCha20-Poly1305 for authenticated encryption and Curve25519 for key exchange in the case of WireGuard).[13] This design choice reflects a broader shift in protocol philosophy; rather than maximizing flexibility, modern VPN protocols prioritize a small, secure configuration space that is easier for both defenders and independent auditors to review, understand, and implement.

[8] CISA Cybersecurity Advisory Committee, "Memory Safety," report to the CISA Director, December 5, 2023, https://www.cisa.gov/sites/default/files/2023-12/CSAC_TAC_Recommendations-Memory-Safety_Final_20231205_508.pdf.

[9] CISA, FBI, ACSC, and CSSS, "Exploring Memory Safety in Critical Open Source Projects," joint guidance, June 26, 2024, https://www.cisa.gov/sites/default/files/2024-06/joint-guidance-exploring-memory-safety-in-critical-open-source-projects-508c.pdf.

[10] A *cipher suite* is "[a] common set of cryptographic algorithms used for key establishment, signature generation, hash function computation, encryption, and/or data authentication." https://csrc.nist.gov/glossary/term/cipher_suite.

[11] The *triple data encryption standard* and *Rivest Cipher 4* are older cipher suites that are easily compromised and are no longer recommended for data protection.

[12] V. Smyslov, and C. Patton, "Prevention Downgrade Attacks on the Internet Ket Exchange Protocol Version 2 (IKEv2), July 30, 2025, https://www.ietf.org/archive/id/draft-smyslov-ipsecme-ikev2-downgrade-prevention-01.html.

[13] Willie Harris, "OpenVPN vs WireGuard: Which Protocol Should Developers Use in 2025?" *DEV*, October 13, 2025, https://dev.to/heintingla/openvpn-vs-wireguard-which-protocol-should-developers-use-in-2025-9n9.

Traffic Analysis

Encryption strength alone does not protect users from an advanced, persistent threat conducting bulk traffic collection. Even perfectly encrypted traffic reveals metadata (e.g., source, destination, timing, and volume) that can be correlated across a network to deanonymize users without ever breaking the cipher.[14]

Single-hop VPNs are most exposed to this kind of analysis because all of a user's traffic passes through one provider-operated server and anyone with visibility into that server (e.g., through compromise, subpoena, or direct collection) can correlate ingress and egress timing to unmask the user, even without decrypting payload content.[15] Multi-hop and mixnet architectures directly target and mitigate this weakness.[16] The Onion Router's (Tor) and NymVPN's multi-hop systems are engineered so that no single node possesses both the originating identity and the destination, and mixnets specifically add randomized timing delays and packet-mixing to defeat the timing-correlation techniques that make single-hop traffic analysis traceable.[17] Apple's Private Relay applies the same two-hop, split-knowledge principle at a narrower scope, splitting IP-address visibility and destination visibility between two independently operated relays to prevent any one party (including Apple) from performing this correlation.[18]

The practical implication is that resistance to bulk, passive collection scales with the number of independent hops and the unpredictability of timing across them. A single-hop VPN, however strongly encrypted, offers essentially no protection against an adversary who can compel (e.g., by government fiat) or infiltrate that one provider (e.g., by compromising the security of that provider). Multi-hop and mixnet designs raise the level of difficulty to correlate user information across multiple servers with different operators and, potentially, different jurisdictions.

Harvest-Now, Decrypt Later and Post-Quantum Cryptography

A long-term threat to VPN traffic confidentiality is not a flaw in current implementations but a mathematical one—sufficiently powerful quantum computers using Shor's algorithm could find the prime factors of a large composite number much faster than existing classical computers. Prime factorization is a very hard, time-consuming mathematical problem that underlies RSA (the common, federal standard for public-private key generation) and thus ensures the encryption security. The risk is that quantum computers could break the mathematical security used in most current VPN key exchange in moments, versus the thousands of years required by classical computers.[19] Also, adversaries with the capacity for bulk collection can record encrypted VPN sessions now and store them until a cryptographically relevant quantum computer becomes available—a strategy known as "harvest now, decrypt later," or HNDL.[20]

The National Institute of Standards and Technology (NIST) highlights this concern in NIST IR 8547:

> *Mosca's theorem* emphasizes the urgency of migrating to post-quantum algorithms by introducing a simple but powerful timeline: if "X" represents the number of years that data must be kept secure, and "Y" is the estimated time needed to complete the transition, then organizations must start

[14] For further information, see Privacy and Civil Liberties Oversight Board, "Report on Certain NSA Uses of XKEYSCORE for Counterterrorism Purposes," December 2020, https://documents.pclob.gov/prod/Documents/OversightReport/ee4c139b-1674-4bfa-9b6a-5b591b648090/NSA%20XKEYSCORE%20REPORT.pdf.

[15] Casey Ford and Ania M. Piotrowska, "What is a mixnet? Unparalleled online privacy with a VPN," NYM, January 12, 2024, https://nym.com/blog/what-is-a-mixnet. (Hereafter: "Mixnet").

[16] Mixnet.

[17] Mixnet.

[18] Private Relay.

[19] NIST IR 8547 ipd.

[20] PaloAlto Networks, "What is Harvest Now, Decrypt Later (HNDL)?" https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl.

> transitioning to post-quantum algorithms before X + Y exceeds the expected time Z for a cryptographically relevant quantum computer to be built. This means that even if quantum computers are a decade away, organizations must begin the migration to post quantum cryptography today to avoid having their encrypted data exposed once quantum computers become operational in the future.[21]

NIST finalized three post-quantum standards in August 2024: the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM, FIPS 203), the Module-Lattice-Based Digital Signature Algorithm (ML-DSA, FIPS 204), and the Stateless Hash-Based Signature Algorithm (SLH-DSA, FIPS 205).[22] NIST is continuing to investigate potential post-quantum cryptography (PQC) standards. Current federal guidance has advanced requirements for agency adoption of PQC to 2030 for establishing keys for high impact systems and 2031 for digital signatures for high impact systems—highlighting the growing urgency to transition systems to PQC standards.[23]

Some VPN implementations have begun deploying hybrid classical/post-quantum key exchange as an interim measure, combining a traditional algorithm with a post-quantum one so that breaking either alone is insufficient to compromise the session.[24] NIST cautions that hybrid schemes add complexity and should be viewed as a bridge rather than a permanent solution.[25] Notably, symmetric cryptographic ciphers (such as AES) are considered far less vulnerable to quantum attack than public-key exchange when using a sufficiently large block size (e.g., 256).[26] This means that most post-quantum risk is in how VPNs establish session keys, not in how they encrypt data once a session is established.

VPN Tools and Products

VPN providers have a variety of technologies to choose from when implementing their products. These technologies are the protocols used to enable the encrypted connection between the user and the VPN provider. The VPN protocol is the collection of decisions the provider makes, and technologies they implement, to enable their product. These include the encryption standards used, how a user is authenticated, how connections are established, and how a user's internet traffic is routed.[27] Some of those technologies, such as Open VPN and IPsec, have existed for decades. While older technologies often have a long history of stability, they are also susceptible to known vulnerabilities in their coding languages or have a recorded history of attacks over time. Newer technologies like WireGuard and mixnet seek to improve security and privacy of their users in novel ways. This section discusses a sample of protocols to illuminate strengths and vulnerabilities in VPN devices.

[21] Dustin Moody, Ray Perlner, Andrew Regenscheid, et al., "Transition to Post-Quantum Cryptography Standards" *NIST Internal Report 8547 ipd*, November 2024, https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf. (Hereafter "NIST IR 8547 ipd").

[22] These standards are available at https://csrc.nist.gov/publications/fips.

[23] The President, "Securing the Nation Against Advanced Cryptographic Attacks," 91 *Federal Register* 38483-38486, June 25, 2026.

[24] Murad Ragab and Bahareh Pahlevanzade, "OpenVPN with Hybrid Post-Quantum Cryptography on Constrained Devices," *IEEE*, 2025, https://ieeexplore.ieee.org/document/11385021/similar.

[25] NIST IR 8547.

[26] Block size is the number of bits in the input of a cipher block. For more information, see NIST IR 8547 ipd.

[27] Lukas Tamašiūnas, "VPN Protocols Explained: How to Choose the Best One," *NordVPN*, May 6, 2026, https://nordvpn.com/blog/vpn-protocols/.

Survey of Commercial VPN Providers

Commercial VPN offerings for consumers fall into several architectural categories, each with distinct cryptographic underpinnings. **Table 1** provides a survey of selected commercial VPN providers.

Table 1. Selected Commercial VPN Providers

Provider / Service	Core Protocol	Architecture	Notable Cryptographic Feature
Open VPN-based VPN providers	OpenVPN	Single-hop, client-to-server	Supports AES, OpenSSL, and TLS.
IPsec-based VPN providers	IKEv2/IPSec	Single-hop, client-to-server	AES or 3DES with Diffie-Hellman key exchange, kernel-level IPsec stack.
Mullvad	WireGuard (default) or OpenVPN	Single-hop by default; supports multi-hop	Anonymous and ephemeral user sessions.
Proton VPN	WireGuard, OpenVPN	Optional "Secure Core" multi-hop through hardened, Proton-owned servers	Tunnel-within-tunnel routing through Switzerland, Iceland, and Sweden.
Tailscale	WireGuard	Peer-to-peer mesh; not a traditional exit-node VPN	Per-device key pairs; control plane separated from data plane.
NymVPN	Sphinx-packet mixnet, WireGuard option	Decentralized mixnet with independent node operators	Layered Sphinx encryption designed to defeat traffic-pattern correlation.
Apple iCloud Private Relay	QUIC/TLS 1.3 over a two-hop relay	Multi-hop, split-knowledge design (Apple and third-party partner)	Neither hop can see both identity and destination; tokens for anonymous authentication.
Tor	Onion routing	Multi-hop, volunteer-operated relay network	Layered (onion) encryption; circuit-based hop selection.

Source: CRS analysis; Brett Cruz and Gene Petrino, "Is a VPN Encrypted?" security.org, November 5, 2025, https://www.security.org/vpn/encryption/; Becky McCarty, "What are the Benefits of Using VPN Encryption?" Linford & Co. LLP, May 17, 2023, https://linfordco.com/blog/vpn-encryption/; Tailscale, "About WireGuard," technical overview, January 5, 2026, https://tailscale.com/docs/concepts/wireguard; Casey Ford and Ania M. Piotrowska, "What is a mixnet? Unparalleled online privacy with a VPN," NYM, January 12, 2024, https://nym.com/blog/what-is-a-mixnet; Apple, "iCloud Private Relay Overview," December 2021, https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF; Roger Dingledine, Nick Mathewson, Paul Syverson, "Tor: The Second-Generation Onion Router," Proceedings of the 13th USENIX Security Symposium," August 9-13, 2004, https://www.usenix.org/legacy/events/sec04/tech/full_papers/dingledine/dingledine.pdf.

Notes: Abbreviations used: Virtual Private Network (VPN). Advanced Encryption Standard (AES). Triple Data Encryption Algorithm (3DES). Transportation-Layer Security (TLS). Internet Key Exchange (version 2)/Internet Protocol (IP) Security (IKEv2/IPsec). The Onion Router (Tor).

Selected Legacy Protocols

OpenVPN

OpenVPN remains the most widely deployed open-source VPN protocol and relies on the OpenSSL (secure socket layer) library for its Transport Layer Security-based (TLS) handshake and Advanced

Encryption Standard (AES) symmetric encryption.[28] Its longevity is both a strength and a liability: OpenVPN has accumulated a large, mature codebase, and is cited as having more than 70,000 lines of code.[29] The large codebase carries a correspondingly large attack surface, making the product more vulnerable to attack than newer, leaner counterparts. In August 2024, Microsoft security researchers disclosed a chain of OpenVPN vulnerabilities, including a plugin-loading flaw that could permit remote code execution and local privilege escalation when combined with other bugs.[30] Separate advisories have documented use-after-free memory bugs and heap leaks tied to TLS renegotiation handling, as well as an authentication-bypass flaw (CVE-2020-15078) affecting misconfigured servers.[31]

IKEv2/IPsec

IKEv2/IPsec is widely used for both corporate remote-access VPNs and native mobile-device VPN clients. It pairs the Internet Key Exchange protocol with the IPsec suite for packet-level encryption and authentication.[32] IKEv2/IPsec is generally regarded as fast and resilient to network changes; for example, it can survive a shift from transmitting information across Wi-Fi to cellular data without dropping the tunnel.[33] But, IKEv2/IPsec is typically executed deep in the operating-system kernel, where a memory-safety bug carries outsized consequences because kernel code runs with the highest system privileges.

Modern Implementations

WireGuard

WireGuard was designed from the outset to minimize the VPN's attack surface: its complete implementation runs to roughly 4,000 lines of code (lean, compared with tens of thousands of lines for OpenVPN's full stack).[34] It uses a fixed, modern cryptographic suite (ChaCha20 for symmetric encryption, Poly1305 for authentication, and Curve25519 for key exchange) eliminating the algorithm-negotiation complexity that has historically created downgrade-attack opportunities in older protocols.[35] Despite its newer design, WireGuard is still vulnerable to cyberattacks. For example, there is a known vulnerability in the WireGuard Portal that allows a non-administrative user connecting via WireGuard to escalate their privileges to full administrator on the connecting network.[36]

---

[28] Becky McCarty, "What are the Benefits of Using VPN Encryption?" Linford & Co. LLP, May 17, 2023, https://linfordco.com/blog/vpn-encryption/.

[29] JP Jones, "WireGuard vs OpenVPN," Top 10 VPN, March 27, 2026, https://www.top10vpn.com/guides/wireguard-vs-openvpn/.

[30] Microsoft Threat Intelligence, "Chained for Attack: OpenVPN Vulnerabilities Discovered Leading to RCE and LPE," blog, August 8, 2024, https://www.microsoft.com/en-us/security/blog/2024/08/08/chained-for-attack-openvpn-vulnerabilities-discovered-leading-to-rce-and-lpe/.

[31] SentinelOne, "CVE-2020-15078: OpenVPN Auth Bypass Vulnerability," vulnerability database, March 4, 2026, https://www.sentinelone.com/vulnerability-database/cve-2020-15078/; "OpenVPN Security Advisories," https://openvpn.net/security-advisories/.

[32] "PaloAlto Networks, "What is IKEv2 (Internet Key Exchange Version 2)?" https://www.paloaltonetworks.com/cyberpedia/what-is-ikev2. (Hereafter "IKEv2").

[33] IKEv2.

[34] PaloAlto Networks, "WireGuard vs. OpenVPN | What are the Differences?" https://www.paloaltonetworks.com/cyberpedia/wireguard-vs-openvpn. (Hereafter "WireGuard vs. OpenVPN").

[35] WireGuard vs. OpenVPN.

[36] SentinelOne, "CVE-2026027899: WireGuard Portal Privilege Escalation Flaw," February 27, 2026, https://www.sentinelone.com/vulnerability-database/cve-2026-27899/.

Apple iCloud Private Relay

Private Relay is bundled with an iCloud+ subscription.[37] It routes Safari, Domain Name System (DNS), and unencrypted Hypertext Transfer Protocol (HTTP) traffic through two separate relays: the user's IP address is visible only to the first hop (operated by Apple), while the destination website is visible only to the second hop (operated by a third party), so no single entity—including Apple—can link the identity of the sender to the information's destination.[38] This two-hop, "split-knowledge" design was formally presented to the Internet Engineering Task Force as a multi-hop Multiplexed Application Substrate over QUIC Encryption (MASQUE) proxy architecture using TLS 1.3 and Quick User Datagram Protocol (UDP) Internet Connection (collectively referred to as QUIC), explicitly built to resist single-party surveillance (rather than to provide full-device VPN coverage).[39] Its scope is deliberately narrow—it does not protect non-Safari application traffic—which limits its value as a general-purpose VPN substitute.

Tailscale

Tailscale layers a coordination service atop WireGuard to build a peer-to-peer mesh network to protect information transfer rather than establish a traditional client-to-gateway tunnel.[40] Because the coordination server exchanges only public keys and policy metadata, not traffic content, the architecture separates a centralized control plane from a decentralized data plane.[41] This architecture would help to ensure actual traffic between two devices remains end-to-end encrypted and inaccessible in the event Tailscale's servers were compromised.[42] This is a different threat model from a commercial exit-node VPN, since Tailscale is designed for connecting a user's own devices rather than anonymizing traffic to third-party websites.

Mixnet (NymVPN)

NymVPN routes traffic through a five-hop Sphinx-packet mixnet, a design that deliberately introduces timing variation and packet-mixing strategies to defeat traffic-correlation attacks rather than relying purely on encryption strength.[43] Some have argued that gateway discovery is still possible with the mixnet as the system depends on a centralized API endpoint, a design choice that may partially undercut the mixnet's decentralization claims and could create a single point of observation for gateway-selection traffic.[44]

Mullvad

Mullvad has built its reputation on both minimal-data account creation (e.g., numeric accounts with no email or personal information required) and public third-party audits. A 2024 penetration test and source-

[37] Apple, "About iCloud Private Relay," support document, August 31, 2023, https://support.apple.com/en-us/102602.

[38] Apple, "iCloud Private Relay Overview," December 2021, https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF. (Hereafter "Private Relay").

[39] Private Relay.

[40] Tailscale, "How Tailscale Works," blog, March 20, 2020, https://tailscale.com/blog/how-tailscale-works. (Hereafter: "How Tailscale Works").

[41] How Tailscale Works.

[42] How Tailscale Works.

[43] Mixnet.

[44] "Centralized nym-vpn-api Dependency Compromises Decentralized Mixnet Integrity," GitHub, February 21, 2025, https://github.com/nymtech/nym-vpn-client/issues/2237.

code review found no critical vulnerabilities.[45] A 2025 web-application audit also found no major vulnerabilities.[46] A 2024 Swedish police raid on Mullvad's offices reportedly failed to produce customer data, consistent with the company's no-logs claims, though this remains anecdotal rather than a formal cryptographic proof.[47]

Proton

Proton VPN offers a "secure core" feature that tunnels traffic through a second, Proton-operated server in a jurisdiction with strong privacy protections before it exits to the destination.[48] This tunnel-within-a-tunnel multi-hop model is intended to blunt the impact of a compromised exit server.

Tor

Tor network encrypts traffic in successive layers and routes it through three volunteer-operated relays by default, such that no single relay knows both the originating user and the final destination.[49] However, because of Tor's design, users face a risk with potentially malicious *exit nodes* (the last traffic hop in the network, where data are decrypted). Malicious users operating exit nodes may inject malware or other content into HTTP traffic, or conduct a man-in-the-middle attack against the user and the internet destination to steal data.[50]

[45] X41 D-Sec, "Security Review for Mullvad VPN AB," final report and management summary, December 10, 2024, https://www.x41-dsec.de/static/reports/X41-Mullvad-Audit-Public-Report-2024-12-10.pdf.

[46] Assured Security Consultants, "Mullvad VPN Web Application Penetration Test," report, September 20, 2025, https://www.assured.se/publications/Assured_Mullvad_Web_App_Pentest_2025.pdf.

[47] Mark Gill, "Another Audit, Same Result – Mullvad Proven Secure and Log-Free in Latest Audit Check," *TechRadar*, October 29, 2025, https://www.techradar.com/vpn/vpn-services/another-audit-same-result-mullvad-proven-secure-and-log-free-in-latest-audit-check.

[48] Proton VPN, "What is Secure Core?" https://protonvpn.com/support/secure-core-vpn.

[49] Roger Dingledine, Nick Mathewson, Paul Syverson, "Tor: The Second-Generation Onion Router," Proceedings of the 13th USENIX Security Symposium," August 9-13, 2004, https://www.usenix.org/legacy/events/sec04/tech/full_papers/dingledine/dingledine.pdf.

[50] Nethaniel Ribco, "An Analysis of the Security Risks Posed by TOR Browser," *CyberProof*, November 15, 2023, https://www.cyberproof.com/blog/an-analysis-of-the-security-risks-posed-by-tor-browser/.