securitum

Security report

SUBJECT

Verification of Proton VPN's No-Log policy

DATE

18.08.2025 – 19.09.2025

LOCATION

Zürich, Switzerland

AUTHORS

Martin Matyja,
Maciej Szymczak

VERSION

1.0

securitum

Executive summary

This report summarizes the findings of an independent security assessment conducted by **Securitum**, commissioned by **Proton AG**. The primary objective of this engagement was to validate that Proton's VPN server infrastructure strictly adheres to its publicly stated No-Logs policy. This policy asserts that no user activity or identifying metadata is logged or stored, thereby protecting user privacy and anonymity.

The full text of the **Proton VPN No-Logs policy** is available for review at the following locations:

- https://protonvpn.com/features/no-logs-policy
- https://protonvpn.com/support/no-logs-vpn/

To achieve this objective, Securitum dispatched two senior security consultants to the Proton AG office in Zürich, Switzerland. The on-site assessment occurred between August 18 and August 20, 2025, constituting six person-days of focused technical evaluation. Throughout the engagement, Securitum auditors worked directly with Proton's senior engineers responsible for the VPN infrastructure. The assessment involved technical inspection, configuration review, and system analysis to verify that the deployed environment contains no mechanisms capable of collecting or retaining user-identifiable data or internet activity logs.

Engagement scope and methodology

The assessment was designed to provide a comprehensive and practical validation of Proton VPN's No-Logs policy. Securitum's methodology combined documentation review, technical interviews, process evaluation, and direct, hands-on inspection of production systems.

It should be noted that throughout the engagement, Proton's engineering team demonstrated a high level of transparency and cooperativeness. All inquiries were answered with detailed technical explanations, and auditors were provided with the necessary access and demonstrations to verify the claims made in the No-Logs policy. This open and collaborative approach was essential for the successful completion of this assessment.

The scope of the audit covered Proton VPN's production server infrastructure. It was confirmed that this infrastructure runs on bare-metal servers fully owned and controlled by Proton AG. Some servers utilize lightweight, OS-level containerization, but the underlying physical hardware remains under Proton's exclusive control. This provides a strong foundation for security and privacy by eliminating reliance on third-party cloud infrastructure providers for the core VPN service.

Audit activities

The following activities were performed to achieve the engagement's objectives:

Documentation review and technical interviews

Analysis of technical architecture diagrams and system documentation, supplemented by in-depth discussions with Proton's senior engineers to establish a thorough understanding of the VPN infrastructure, data flows, and component interdependencies.

Live system inspection and configuration analysis

Direct, hands-on examination of production VPN server components. To ensure an unbiased sample, Securitum auditors independently and randomly selected production servers for each verification procedure. The analysis focused on system configurations, running processes, and storage to identify any mechanisms capable of collecting or retaining user data.

Change and deployment process review

Evaluation of the operational security practices governing configuration changes and new server deployments. This was done to verify that processes are in place to prevent the unauthorized or inadvertent introduction of logging mechanisms.

Data leakage analysis

Inspection of server storage and memory for evidence of out-of-band data persistence that could contravene the No-Logs policy, such as un-swapped memory blocks or temporary file caching.

Key areas of investigation

The audit was structured to answer critical questions derived directly from the assertions made in the No-Logs policy. The core focus was to verify the following:

1. Is user activity tracked or logged on the production VPN servers that handle user traffic?
2. Is connection metadata, such as DNS queries or session timestamps, logged on VPN servers?
3. Is user network traffic actively inspected, or its contents logged on VPN servers?
4. Is information monitored or logged regarding the specific services (e.g., websites, external servers) a user connects to?
5. Are aggregate logs maintained that correlate services accessed (e.g., websites, servers) with the specific VPN server used?
6. Is the No-Logs policy applied uniformly across all servers, in all geographic regions, and to all user subscription tiers?
7. Is an automated process in place to detect and generate alerts for unauthorized configuration changes that could enable logging (e.g., changing a "log" parameter from false to true)?
8. Is a formal Change Management process, incorporating a dual-control (four-eyes) principle, enforced for all authorized changes to logging-related configurations?
9. Do the active configuration files for the core VPN services contain any enabled logging directives?
10. Is information logged that associates a specific user with a specific VPN server they are connected to?

The detailed findings related to these investigation areas are presented in the subsequent sections of this report.

Scope exclusions

The scope of this engagement was specifically focused on the production VPN server environment and its adherence to the No-Logs policy. The following areas were explicitly excluded from the scope of this audit:

- The Continuous Integration/Continuous Deployment (CI/CD) pipeline.
- A formal source code review of the VPN software and its associated libraries.
- Ancillary Proton systems, such as accounting or account management platforms.
- Static or dynamic binary analysis of the VPN client or server software.

Limitations of the assessment

This assessment provides a point-in-time validation of Proton VPN's production environment as it existed during the on-site engagement. The findings are based on a guided review process, where Securitum auditors observed live systems as demonstrated by Proton's senior engineers. While this provides a high degree of assurance, it is distinct from an unsupervised, direct forensic investigation. The assessment was also conducted on a representative sample of production servers and did not encompass every server in Proton's global fleet. The conclusions in this report are based on the systems and evidence presented to the auditors during the defined engagement period.

Historical context and current scope

Securitum has previously conducted independent assessments of Proton VPN's No-Logs policy in 2022, 2023, and 2024. These audits serve as a consistent, year-over-year validation of Proton's commitment to user privacy. The public reports from these prior engagements are available for review:

- Consolidated blog post: https://protonvpn.com/blog/no-logs-audit/
- 2022 audit report: https://drive.proton.me/urls/521N34GHTM#PVwqewJVFgyS
- 2023 audit report: https://drive.proton.me/urls/TEGZZ53M28#lPz2jeVjV6Mp
- 2024 audit report: https://drive.proton.me/urls/ED8G4GC5MG#pM52Y8RMXIKn

Since the 2024 assessment, the Proton VPN platform has undergone significant evolution, including the introduction of new features and infrastructure enhancements. The scope of this 2025 audit was comprehensive and specifically included the verification of these new components and configurations to ensure they remain fully compliant with the No-Logs policy.

Recommendations

The technology landscape and the Proton VPN platform are in a constant state of evolution. To provide continuous assurance and maintain user trust, Securitum recommends that Proton AG maintain its commitment to commissioning annual, independent third-party audits. Regular verification ensures that infrastructure changes, new features, and evolving operational procedures continue to adhere to the strict principles of its No-Logs policy.

Contents

Change history

Document date	Version	Change description
19.09.2025	1.0	Final version of the security report.

Detailed findings

This section presents a comprehensive analysis of the key inquiries that guided this security assessment. The findings are the result of a direct, on-site inspection of Proton VPN's production infrastructure, where Proton's senior engineering staff demonstrated system configurations and processes to Securitum's auditors.

Does Proton VPN track user activity on its VPN servers?

No. Securitum confirmed that Proton does not track or log users' activities on its production VPN servers. The architecture is explicitly designed to process user traffic without maintaining any records of its content or destination. This design choice is fundamental to the No-Logs policy, ensuring that once a user's session is terminated, no historical record of their internet activity remains on the server infrastructure.

This conclusion was reached after a thorough, guided examination of randomly selected live servers where Proton engineers provided a detailed walkthrough of the server filesystem, demonstrating the contents of log directories and other storage locations. A technical review of the implementation and configuration of all services involved in handling user traffic was conducted in the same manner. Throughout this observed process, the configurations were shown to be set to minimal or no logging, and no evidence of user activity logging was found.

Does Proton VPN log connection metadata, such as DNS traffic?

No. User-attributable connection metadata is not logged. This includes sensitive data points such as a user's source IP address, specific connection timestamps, session duration, or their DNS queries. This approach adheres to the principle of data minimization, where only the absolute essential, non-identifiable data required for service maintenance is collected.

The audit confirmed the collection of a minimal set of fully anonymized, aggregate data used exclusively for statistical analysis and operational support. Proton engineers demonstrated the mechanisms that collect this data, which includes general device type based on operating system, the aggregate quantity of connections from a specific country, and the type of connection protocol used (such as Browser Extension, Stealth, WireGuard, OpenVPN, or IKEv2).

To support this, Proton operates its own private DNS infrastructure using the Knot Resolver software, which performs DNSSEC validation directly against the root DNS servers. This architecture gives them full control over the resolution process and reinforces the no-logging claim for DNS queries.

To protect user privacy, a threshold is enforced so that statistical data is only processed for countries with a sufficient volume of connections, making it impossible to correlate activity back to an individual.

Does Proton VPN inspect or log user network traffic on its VPN servers?

No. The audit confirmed that Proton VPN does not perform *Deep Packet Inspection* (DPI) or log the contents of user network traffic. An exception to this is the mechanism used on free-tier servers to enforce the publicly stated policy of blocking BitTorrent (P2P) traffic. Proton engineers demonstrated that this is accomplished through live, on-the-fly traffic identification for the sole purpose of blocking this specific protocol.

This process is a form of live monitoring, not logging; no data related to this inspection, including a user's IP address or the traffic's content, is ever written to a disk or any persistent storage. Proton engineers presented the live system's network stack configurations, confirming the absence of any generalized traffic inspection or content logging tools. In Securitum's professional opinion, this specific mechanism for traffic management is implemented in a way that does not pose a risk to user privacy.

Is information about services (websites, servers) a user connects to monitored or logged?

No. Proton does not log or monitor the specific services, websites, or servers that users connect to, ensuring that browsing history remains confidential. This was verified through a specific audit of the NetShield DNS filtering feature.

Proton engineers demonstrated its architecture and live configuration, showing that it operates from static blocklists and does not log specific user DNS queries. For user feedback, the system maintains an ephemeral counter of the number of domains blocked during a session. It was explained that this data is displayed within the user's client interface specifically to demonstrate the effectiveness of the feature. This implementation demonstrates a privacy-by-design approach, as the counter exists only in the server's volatile memory, contains no specific domain information, and is permanently purged when the session terminates.

Are logs maintained that correlate services used with a specific VPN server?

No. Proton VPN does not track which external services are accessed by users through any given VPN server. It is critical to distinguish this internal, operational monitoring from any form of user activity tracking. Proton's engineering team demonstrated their internal monitoring systems, which conduct automated, synthetic health checks that are not linked to user traffic.

These checks are used only to ensure operational continuity and provide performance optimization - for example, by verifying that a server can reach major internet services. The guided review of these monitoring scripts and their outputs confirmed their complete isolation from any user session data, ensuring user activity cannot be correlated with server performance metrics.

Is the No-Logs policy applied uniformly across all servers, regions, and subscription tiers?

Yes. It has been verified that a consistent server configuration and the same strict No-Logs policy are deployed across all of Proton's servers, regions, and subscription tiers. This uniformity is a critical component of the policy's integrity, guaranteeing that a user's privacy protections are not dependent on their subscription level or geographic location.

Securitum auditors were shown the deployment configurations and base server images used for multiple geographic regions, and Proton engineers demonstrated that these templates were identical in their logging and data handling policies. The functional exception for BitTorrent traffic on free-tier servers was explained as a traffic filtering rule, not a logging exception, and was verified by reviewing the relevant firewall configurations as publicly disclosed.

Is there an automated process to detect and alert on unauthorized configuration changes?

Yes. Proton has implemented a robust, multi-layered strategy for ensuring configuration integrity. Proton engineers demonstrated their infrastructure-as-code deployment system, explaining how it automatically reverts "configuration drift". This is supplemented by a custom-built "Infra Audit" tool that periodically collects server state and uses automated analysis to detect divergence from the approved baseline.

Additionally, the monitoring system is configured to generate alerts on any unexpected increase in log volume, which could indicate that a logging parameter was illicitly enabled. It is important to note that while user activity is never logged, privileged administrative actions on the servers are logged for security and audit purposes.

Is a formal Change Management process with dual control enforced?

Yes. A formal Change Management process, incorporating the principle of dual control, is in place and strictly enforced for all modifications to logging-related configuration files. This process was verified through a guided review of merge request histories and branch protection rules within Proton's version control system.

The engineering team presented multiple examples of recent configuration changes, demonstrating the enforcement of the peer review and approval ("four-eyes") requirement before any change can be deployed. This process creates a clear, auditable trail for every modification, ensuring accountability and adherence to security best practices.

Do active VPN configuration files have any logging enabled?

No. A direct, observed review of the server-side configuration files for core services like OpenVPN and WireGuard confirmed that no logging directives are enabled. Proton engineers conducted a live inspection of the active configurations on production servers, and this walkthrough confirmed the absence of any parameters that would initiate user activity logging.

While standard OS-level logs are present as they are essential for basic server administration and troubleshooting (e.g., monitoring CPU usage, cron job execution, or SSH daemon activity), our guided review confirmed these logs are properly segregated from VPN services and do not contain any user-related IP addresses, traffic, or other privacy-sensitive data.

Is information logged that associates a user with a specific VPN server?

No. The system is architected with multiple layers to explicitly prevent the logging of any data that would map a specific user account to a VPN server. The process was demonstrated to our auditors and functions as follows: to establish a connection, a temporary, intermediate pseudonym (a randomly generated VPN username) is used. The user's actual registration email address or account identifier is never sent to the VPN server. Once authenticated, the active session is managed by an in-memory, ephemeral data store on the server.

This architecture is supported by a separate accounting service, located in Switzerland and outside the scope of this server audit, whose sole purpose is to prevent abuse, such as enforcing session limits for free users, without logging user-identifiable data. Furthermore, the primary connection protocol, WireGuard, uses certificate-based authentication, further minimizing the use of traditional credentials. By using these decoupling techniques, Proton ensures that no persistent data associating a user's identity with their VPN connection is ever stored on the VPN servers.

Conclusion

Securitum has completed its independent third-party assessment of the Proton VPN infrastructure and its adherence to its publicly stated No-Logs policy. The engagement, conducted from August 18-20, 2025, involved a direct, on-site review of production systems, operational procedures, and architectural documentation as demonstrated by Proton's senior engineering team.

The technical evidence reviewed showed no instances of user activity logging, connection metadata storage, or network traffic inspection that would contradict the No-Logs policy. Furthermore, the audit verified the implementation of robust administrative and technical controls, including automated configuration management and a formal dual-control change process, which are designed to ensure the continuous integrity of the no-logging environment.

Based on these findings, Securitum attests that the Proton VPN service, as configured at the time of the audit, fully complies with the privacy commitments outlined in its No-Logs policy.