securitum

Security report

SUBJECT

Proton VPN’s No-Log policy – regarding VPN activity

DATE

24.04.2023 – 01.05.2023

LOCATION

Zürich, Switzerland

AUTHORS

Maciej Szymczak
Marek Rzepecki

VERSION

1.0

Executive summary

This document is a summary of work conducted by Securitum. The subject of the test was verification of compliance with **Proton VPN’s No-Log policy**, which is described in the following articles:

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

The scope of the audit included the following questions which were designed to provide a precise estimation of the VPN solution's security level in terms of the no-log, but was not limited to them:

- Does Proton VPN track user’s activity on the VPN servers (servers that handle traffic)?
- Does Proton VPN log the metadata related to activity on the VPN server such as DNS traffic?
- Does Proton VPN inspect or log the network traffic on its VPN servers?
- Does Proton VPN monitor or log information about the services to which the user connects?
- Does Proton VPN track which services (websites, servers) have been accessed from a specific VPN server?
- Does Proton VPN apply the same privacy policy to all servers across all regions and subscription tiers?
- Does Proton VPN have a specific process to ensure that any unauthorised configuration change (such as “log=false” to “log=true”) will be detected? Will it trigger an automatic alarm?
- Does Proton VPN have a proper Change Management process in place to ensure that any authorized changes applied to the logs-related configuration files are reviewed and approved by another employee (dual control)?
- Do Proton VPN configuration files have any logging enabled?
- Does Proton VPN log the information about which VPN server a user is connected to at any given time (and similarly – which user is connected to a specific VPN server)?

To verify compliance, Securitum assigned two senior security consultants to visit Proton’s office in Zurich, Switzerland. From April 24th to April 26th, 2023, the auditors spent a total of 6 man-days collaborating with Proton’s team to gather answers to the aforementioned questions.

The audit encompassed a comprehensive analysis of the no-logs policy, a technical assessment of VPN configuration files (as well as the configuration of underlying services), conversations with team members, a meticulous inspection of several randomly selected VPN servers by the auditors, and an evaluation of the VPN server deployment process. It is worth noting that the Proton Team was cooperative, providing detailed answers to highly technical questions related to the VPN service and its supporting services. All processes and configurations of the VPN service were explained and demonstrated transparently.

The audit did not cover the verification of the CI/CD environment, the examination of the source code, or the analysis of the resulting binaries for the VPN software (OpenVPN, WireGuard, strongSwan, and associated libraries and components). These aspects were considered out of the scope of the audit.

No traces of logging user-related data by the VPN service were found. Securitum can confirm that, as of April 26th, 2023, Proton VPN service is compliant with its no-log policy, provides high privacy, and is maintained by a team that is highly committed to safeguarding user data and developing the product in a manner that minimizes the processing and storage of user-related information.

The audit verifying compliance with the no-log policy was also conducted one year earlier, from February 21st to February 24th, 2022, and its results can be found below:

- https://protonvpn.com/blog/no-logs-audit/
- https://protonvpn.com/blog/wp-content/uploads/2022/04/securitum-protonvpn-nologs-20220330.pdf

Since the previous audit several solutions have been introduced to extend the functionalities of the VPN service and enhance user privacy. During this iteration of the audit, compliance with the no-log policy of both the new solutions and all other components of Proton VPN was verified.

Despite the implementation of changes, Securitum's opinion – based on a detailed analysis of the business and technical aspects of Proton VPN – is that the functionalities responsible for guaranteeing user privacy have remained unchanged.

Nonetheless, to guarantee that the solution adheres to best practices for ensuring user privacy, it is recommended to conduct such audits annually to maintain the same level of protection in future privacy approaches.

Contents

Change history

Document date	Version	Change description
01.05.2023	1.0	Final version of the document.

Audit conclusions

Does Proton VPN track user's activity on the VPN servers (servers that handle traffic)?

User activity is not tracked on the VPN servers. This fact was confirmed through a detailed analysis of the components that make up of Proton VPN:

- Logs generated by the services and the operating system,
- Files created and stored by the services,
- Configuration settings of these services.

A low-level analysis of the logic implemented in the services that constitute Proton VPN also revealed no discrepancies or traces of logging user-related data.

Does Proton VPN log metadata relate to activity on the VPN server such as DNS traffic?

No metadata related to user activity is logged by the VPN servers. The only data which may be stored and logged for statistical purposes is the type of VPN Client (Linux/Windows/iOS/Android) used by the user and the location of the Autonomous System (AS) from which the connection was made (only if from a country with strong Internet censorship to detect and bypass this censorship).

This was verified by inspecting the system and service logs of a randomly chosen VPN server by the auditors and conducting a low-level configuration analysis of Proton VPN components.

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

Network traffic passing through the Proton VPN servers is not inspected, with one exception: on the Free Tier subscription BitTorrent traffic is automatically detected using nDPI library and blocked for performance reasons.

It is important to note that this discovery result is not logged and only used to block user traffic, and in Securitum's opinion it does not pose a threat to user privacy.

It was confirmed that no logs containing user-related data (or data which could enable a malicious actor to track a user's VPN usage) are created or stored. This was verified by examining the system and service logs of a randomly chosen VPN server by the auditors and conducting a low-level configuration analysis of Proton VPN components.

Does Proton VPN monitor or log information about the services to which the user connects?

Proton VPN does not monitor or log any information about the services being used, with one exception – on the Free Tier subscription BitTorrent traffic is detected automatically using nDPI library and blocked for performance reasons.

No other mechanisms that monitor, track or log data about the services visited by the user are in use.

Does Proton VPN track which services (websites, servers) have been accessed from a specific VPN server?

The servers comprising Proton VPN do not monitor or log which services (or types of services) have been used by the servers in general or by a specific VPN server.

This was confirmed through an analysis of the system and service logs from a randomly chosen VPN server by the auditors, as well as an examination of the logic behind the process responsible for establishing the VPN connection.

Does Proton VPN apply the same privacy policy to all servers across all regions and subscription tiers?

All Proton VPN servers are configured identically and provide the same level of protection, without differentiating between the physical location of the server or the subscription tier. The only exception is that, in the free subscription tier BitTorrent traffic is blocked by default to prevent performance issues.

Does Proton VPN have a specific process to ensure that any unauthorised configuration change (such as “log=false” to “log=true”) will be detected? Will it trigger an automatic alarm?

No fully automated configuration change verification is implemented on the servers. However, software verification is performed by comparing the checksums (SHA-256) of the installed software against the checksums in the Ansible playbook, which verifies the checksums of all files present on the VPN server with a trusted source.

This process is not automated and must be initiated manually.

Does Proton VPN have a proper Change Management process in place to ensure that any authorized changes applied to the log-related configuration files are reviewed and approved by another employee (dual control)?

Each change in the configuration of the services comprising Proton VPN or the addition of new software is subject to a thorough, multi-stage Verification Process.

After extensive manual and automated testing, the changes are reviewed and approved by an independent team member before being published.

Furthermore, the details of each change are logged and tracked in an internal system, making it impossible for changes to be introduced without notice.

Do Proton VPN configuration files have any logging enabled?

During the audit, it was found that the services used to set up and manage the VPN connection do not collect logs. Certain system services necessary for the correct operation of the solution (but not related to user's VPN connection itself) collect truncated system logs.

The auditors verified the content of these logs and did not find any traces of data related to users or processed by them, or other information that could endanger users' privacy.

Does Proton VPN log information about which VPN server a user is connected to at any given time (and similarly, which user is connected to a specific VPN server)?

The Proton VPN does not track where which user is connected. However, due to accounting requirements, it is necessary to count the total VPN sessions per account to fit the limits of a given subscription tier. This process is triggered by a centralized accounting service, which operates separately from the VPN server that handles user traffic, and it is done in an automated way without revealing any user data to the VPN server.

Authentication to VPN servers is done either by using set of randomly server-side generated credentials (different from user's main set of credentials – e-mail address and user-defined password) or by a certificate. During VPN connection, the e-mail address used to register an account is not being sent to the server at any time. The randomly generated "VPN username" is being sent to the VPN server, but it is not being logged at any time, meaning Proton VPN does not log information about which VPN server the user is connected to. Analogically, Proton VPN does not log information about which user is connected to the specific VPN server.

This set of credentials (a random username and password) cannot be used to identify the user locally by the VPN server side; however, it is technically possible to do that on the API server, but – as declared by Proton VPN Team – such mechanism was not implemented at the time of the audit.

As an alternative method of authentication, the certificate can be used – this method is even more anonymous, as there is no technical way to link the certificate used during the authentication with a specific user.

Proton VPN Client is by default using WireGuard protocol, which is using certificate-based authentication. Credential-based authentication is a legacy authentication method still needed for technical reason only by IKEv2.

Proton VPN does not log information about the username or the IP address of the user connecting to VPN server.