securitum

Security report

SUBJECT

Verification of Proton VPN's No-Log policy

DATE

03.07.2024 – 12.07.2024

LOCATION

Geneva, Switzerland

AUTHORS

Marek Rzepecki
Marcin Zięba

VERSION

1.0

securitum

Executive summary

This document is a summary of work conducted by Securitum. The subject of the test was the verification of Proton's consumer servers' compliance with the **Proton VPN's No-Log policy**, the goal of which is to ensure the users that no data related to their activity is being logged or stored. More details on Proton's No-Log policy may be found at the links below:

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

The audit aimed to verify compliance with the No-Log policy. To achieve this, Securitum assigned two senior security consultants to visit Proton's office in Geneva, Switzerland. From July 3rd to July 5th, 2024, the auditors dedicated a total of six man-days, working alongside Proton delegates responsible for VPN product development, to audit and verify the technical aspects of the VPN implementation. This was done to ensure that no user-related data, which could reveal their identity or track their activity, is collected, and that VPN ensures the highest level of privacy.

The audit comprised the following:

- A technical analysis of the solutions utilized by the VPN, based on the provided documentation.
- Discussions with the technical representatives of Proton to thoroughly understand the interdependencies among the individual VPN components.
- A practical verification, where the configuration of all key VPN server components was meticulously examined for potential user data collection. This was conducted on VPN servers randomly selected by the auditors.
- A practical verification to determine whether any user activity information was being collected or stored on the VPN servers. This was also performed on VPN servers randomly selected by the auditors.
- Verification of security practices related to configuration changes and the deployment of new servers (VPN development and VPN server deployment process).

To structure the process of verifying compliance with the No-Log policy, a series of control questions was prepared (though the audit was not limited to these) and is presented below:

- 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)?

The detailed answers to the above questions are included in the next part of this document.

The audit did not encompass the verification of the CI/CD environment, the examination of the source code, communication with other Proton's VPN components used in accounting/ account management process or the analysis of the resulting binaries for the VPN software (OpenVPN, WireGuard, strongSwan, and associated libraries and components). These aspects were deemed to be outside the scope of the audit.

It should be noted that the attitude of the Proton's delegates demonstrated a high level of cooperativeness. The responses provided to all inquiries were highly detailed and allowed for the collection of information necessary to clearly confirm that Proton's No-Log policy is fully adhered to as intended.

During the audit, it was confirmed that the Proton VPN product complies with the No-Log policy and offers the highest standards of security and privacy. No traces of user logs were detected, and user privacy is protected through both technical and organizational measures. All changes and additional features are developed based on the fundamental principle of maximizing user security and privacy.

The compliance with No-Log was also verified in 2022 and 2023, and one may read the reports from these audits at the below links:

- https://protonvpn.com/blog/no-logs-audit/
- Direct link to the 2023 report: https://res.cloudinary.com/dbulfrlrz/images/v1714481298/wp-vpn/securitum-proton-protonvpn-no-log-policy-20230517/securitum-proton-protonvpn-no-log-policy-20230517.pdf
- Direct link to the 2022 report: https://res.cloudinary.com/dbulfrlrz/images/v1714482825/wp-vpn/securitum-protonvpn-nologs-20220330/securitum-protonvpn-nologs-20220330.pdf

Since the time of previous iterations, Proton introduced multiple changes and additional mechanisms responsible for extending the product's functionality and enhancing user's security and convenience. It should be mentioned that current iteration of the audit included all these changes.

In Securitum's opinion, based on a detailed analysis of the business and technical aspects of Proton VPN, the functionalities responsible for ensuring user privacy have remained unchanged.

However, to ensure that the solution continues to adhere to best practices for safeguarding user privacy, it is recommended to conduct such audits annually. This will help maintain the same level of protection in future privacy measures.

Contents

Change history

Document date	Version	Change description
12.07.2024	1.0	Final version of the document.

Audit conclusions

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

It was confirmed that Proton does not track user's activity on the VPN servers.

This was verified through the following steps:

- Configuration analysis of the VPN solution components running on the VPN server.
- Verification of the files stored on the VPN server filesystem.
- Application and system logs of the VPN server components.
- A detailed, technical analysis concerning the implementation of various components comprising the VPN server.

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

Proton does not log metadata that can be uniquely associated with any user, their activities, or visited services. Information gathered solely for statistical purposes, as well as to ensure operational continuity and smoothness, includes data such as:

- The number of connections to a specific VPN server, from a given country.
- Device type (Android, iOS, macOS, Windows etc.).
- Connection type (IKEv2, OpenVPN UDP/TCP, Wireguard UDP/TCP, Stealth protocol, Browser Extension)

To further prevent the tracking of user activity, when only a little number of individuals connect from a particular country, this data is not included in the statistics. It should be noted that these data points cannot be correlated with individual users or linked to historical data.

This has been confirmed through the verification of log occurrences and the VPN server component's configuration on several randomly selected VPN servers by the auditors.

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

It has been strictly confirmed and verified through detailed technical analysis of selected servers of all types that no data related to network traffic, user activity, or metadata that could in any way be used for user tracking is logged.

A preliminary inspection of network traffic is conducted on servers where BitTorrent traffic is not permitted (which is blocked for free users) as confirmed in the terms of service. However, it has been confirmed through detailed analysis that this traffic is not logged anywhere. Information that could potentially identify which specific user was using BitTorrent is also not logged, even in cases where access to the server or other techniques could allow for such analysis.

It should be noted that this analysis is performed only on the fly to maintain optimal device performance. Thus, there is no logging but only live monitoring.

In Securitum's opinion, this behavior does not pose any risk to user's privacy.

Network traffic passing through the Proton VPN servers is not inspected, with one exception: on the free account, BitTorrent traffic is automatically detected and blocked for performance reasons.

This has been confirmed through verification on several randomly selected VPN servers by the auditors.

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

It has been strictly confirmed that Proton does not log information regarding which services users utilize.

The only traces that could qualify as "monitoring" (rather than logging) involve verifying whether a user employing NetShield attempts to access a site deemed malicious or containing advertisements. This mechanism is based on DNS of specific domains. It detects and blocks attempts to resolve the domain, which is known as dangerous/malicious.

However, this information is not recorded or actively monitored in any way. NetShield mechanism is optional, and the entire process aims to enhance user security; without executing this operation, the process cannot be achieved.

With the introduction of NetShield, which blocks malware/advertisements, general statistics are maintained regarding the number of connections (but not a list of specific domains) to malicious addresses. This enables users to access information on how Proton's NetShield has protected them. This information (counter of visited unwanted domains) is immediately deleted upon the conclusion of the user's session.

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

Proton VPN does not retain records of which services were accessed from which server.

Proton gathers statistics on whether servers have access to specific Internet services (i.e., whether they have not been blocked) to ensure operational continuity. It is important to note that these statistics are solely related to server operations and do not pertain to individual users.

The only data collected for statistical purposes pertains to the frequency with which each category of blocked data was prevented from being accessed by a particular server (but not a specific user).

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

It has been strictly confirmed that all servers, in all regions and subscription types (free and premium accounts), are configured with the same privacy policies, and with the utmost care for aspects related to data and device (server) security.

This has been verified through an in-depth review of the technologies used from a configuration standpoint, and by searching for files that might contain any user-related data (logs), on several randomly selected servers of each type and tier by auditors. The only exception differentiating the policies for premium and free accounts is the blocking the BitTorrent protocol for free users where BitTorrent protocol is prohibited (on free servers).

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?

It has been confirmed that Proton has implemented advanced mechanisms to ensure that:

- Changes to configuration files/components have not been made, and no additional arguments have been added to executed system commands.
- VPN server component settings have not been altered, such as enabling logging.
- No unauthorized access to devices has occurred.
- All servers are configured identically, and any deviations from the norm are detected and subjected to individual analysis.
- There are additional procedures and components that allow for automatic verification to ensure no changes have been made. These procedures are initiated periodically by manual execution.
- No unauthorized actions have been performed on the system.
- All operations performed on the system are logged and subjected to both automatic and manual analysis by the appropriate team.

Access to the servers is limited to very restricted personnel and is strictly controlled.

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)?

An automatic and manual verification process is implemented for every change before it is deployed to production servers. Each change is reviewed by an additional engineer (dual control) as part of the Secure Software Development Life Cycle (SSDLC) process.

Changes are first introduced in a controlled environment and monitored before being rolled out across the entire infrastructure.

Do Proton VPN configuration files have any logging enabled?

Server-side configuration files for all VPN clients (IKEv2, OpenVPN, WireGuard, Browser Extension) do not contain any logging implemented.

Certain essential system services required for the proper functioning of the solution (unrelated to the user's VPN connection) gather diagnostic system logs. Auditors examined these logs and found no evidence of user-related data, data processed by users, or any other information that could compromise 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)?

Temporary, intermediate pseudonym (different from the user's email/ account registration data related credentials) is created to establish a final VPN connection. The only verification performed by Proton is to check whether the user is a paid user or not. The purpose of this action is to terminate excess sessions for free users if the limit is exceeded.

During the VPN connection, the e-mail address used to register an account is not being sent to the VPN 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 that Proton VPN does not log information about which VPN server the user is connected to. Similarly, Proton VPN does not log information about which user is connected to a specific VPN server.

Server monitors general, anonymised statistics which are related to the number of people from a given country connected to a specific server. However, to further prevent any possibility of user tracking or identifying individuals from less common regions, this statistic is not collected when the number of connections to VPN servers from small countries is too low.

There is an additional accounting service whose goal is to prevent abuses and ensure the continuity of the Proton VPN. Its actions are performed by a dedicated external system, owned, and managed solely by Proton Team. These servers are kept in a secure location in Switzerland. User data is not logged or stored there in redundant, unnecessary amount. The accounting service was outside the scope of the audit.

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.