securitum

Security report

SUBJECT

ProtonVPN's No-Logs policy – regarding VPN activity

DATE

21.02.2022 – 24.03.2022

RETEST DATE

N/A

LOCATION

Geneva, Switzerland

AUDITORS

Maciej Szymczak
Jakub Darecki

VERSION

1.0

securitum

Executive summary

This document is a summary of work conducted by Securitum. The subject of the test was a verification of compliance with the No-Logs policy.

The scope of the audit included the following questions, but was not limited to them only:

- Does ProtonVPN track user's activity on the VPN servers (servers which are passing the traffic)?
- Does ProtonVPN log the metadata about the activity on the VPN server such as DNS traffic?
- Does ProtonVPN inspect or log the network traffic on the VPN servers?
- Does ProtonVPN monitor or log information about which services (websites, servers) the user is connecting to?
- Does ProtonVPN monitor which services (websites, servers) have been used by the specific VPN server?
- Does ProtonVPN apply the same privacy policy to all servers, in all regions and to all subscription tiers?
- Does ProtonVPN have a specific process to ensure that any unauthorised configuration change (such as "log=false" → "log=true") will be detected? Will it trigger an automatic alarm?
- Does ProtonVPN 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)?
- Does VPN configuration files have any logging enabled?
- Does ProtonVPN log the information about which VPN server is the user connected to at the time (and analogically - which user is connected to the specific VPN server)?

To answer the above questions, Securitum delegated two senior security consultants for 8MD (man days) to arrive in ProtonVPN's headquarters between 21.02.2022 – 24.02.2022 to conduct a security audit, cooperating with ProtonVPN Team. The audit was based on the threat modelling, high level review of the No-Logs policy, low level technical audit of VPN configuration files, interviews with the ProtonVPN Team, technical audit of a few (randomly selected by the auditing team) VPN servers, and review of the deployment process of the VPN servers. During the audit, ProtonVPN Team was cooperative and helpful. They were providing detailed answers to all Securitum's questions and supporting their answers with evidence samples that were manually reviewed by Securitum's auditing team. The verification of the CI/CD environment, the audit of the source code and resulting binaries of the VPN software (OpenVPN, WireGuard, strongSwan and used libraries) were out of the scope of the audit.

As a result of the audit, it was confirmed that ProtonVPN offers high privacy with its No-Logs approach, and the audit did not detect any issues that could make a negative effect on the user's privacy. It should be stated that the audit addressed the state of the ProtonVPN product, as of 24.02.2022, and annual audits may be needed to ensure that future privacy approach offers the same protection level.

It should be noted, that purpose of this report is not to describe technical mechanism and software configuration to achieve No-Logs policy, but to confirm that it (ProtonVPN technology stack) was manually audited searching for all possible No-Logs policy critical points, showing specific questions auditors were trying to find answers for, during the course of the audit.

Contents

Change history

Document date	Version	Change description
24.03.2022	1.0	Final version of the report.

Audit conclusions

Does ProtonVPN log the metadata about the activity on the VPN server such as DNS traffic?

ProtonVPN does not log data related to DNS traffic or any metadata on the VPN servers. It was confirmed by manual inspection of processes running on the server that might potentially capture and analyse the network traffic (including the DNS).

Does ProtonVPN inspect or log the network traffic on the VPN servers?

ProtonVPN does inspect the network traffic on the Free VPN servers. The inspection is conducted in order to block BitTorrent network that is negatively affecting the performance on Free Servers. In order to detect the BitTorrent traffic, nDPI library is being used and upon detection the connection is automatically dropped. No further actions are performed (no logging, no alerting, just dropping). ProtonVPN does not log the information about the detected or dropped connections. In Securitum's opinion such inspection does not affect the privacy of the user as the inspection is done blindly without logging which user attempted to use the BitTorrent traffic.

It should be noted that ProtonVPN does not inspect the network traffic on all other subscription tiers' VPN servers.

Does ProtonVPN monitor or log information about which services (websites, servers) the user is connecting to?

ProtonVPN does not monitor or log any information about which services (websites, servers) the user is connecting to. One exception is detection and blocking of bit-torrent network traffic on Free Servers. However, it does not affect the privacy of the users. The BitTorrent traffic is being detected by the nDPI library and if the connection is recognized as BitTorrent traffic, it will be automatically dropped. The whole mechanism is working fully locally on the specific ProtonVPN server serving the connection, without notifying any central database. The restriction will be lifted when the BitTorrent traffic will stop. There is no deep traffic inspection of such connections, just the type of traffic is detected. The packet content (e.g. a torrent name) is not being analysed or logged.

Does ProtonVPN monitor which services (websites, servers) have been used by the specific VPN server?

ProtonVPN does not monitor such activities – there is no logging and no monitoring of the user's activity. One exception is detection and blocking of BitTorrent network traffic on Free Servers. However, it does not affect the privacy of the users. The BitTorrent traffic is being detected by the nDPI library and if the connection is recognized as BitTorrent traffic, it will be automatically dropped. The whole mechanism is working fully locally, on the specific ProtonVPN server serving the connection, without notifying any central database. The restriction will be lifted when the BitTorrent traffic will stop. There is no deep traffic inspection of such connections, just the type of traffic is detected. The packet content (e.g. a torrent name) is not being analysed or logged.

Does ProtonVPN apply the same privacy protection to all servers, in all regions and to all subscription tiers?

ProtonVPN applies the same privacy policy to all servers, in all regions, to all subscriptions tiers. The only difference between the Premium and Free servers is that on Free subscription, a BitTorrent traffic is disabled to minimize performance issues, but in our opinion it is not affecting the privacy of the ProtonVPN users.

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

ProtonVPN has a semi-automatic mechanism to verify potentially malicious changes. The files checksums (SHA265 algorithm) are being compared by the Ansible playbook, which is verifying the checksums of all files present on the VPN server with a trusted source (official Debian's repository checksum list and the internal file checksums as well). It's done regularly but triggered manually.

Does ProtonVPN 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)?

Yes, ProtonVPN has proper Change Management process in place – changes are stored in internal CI/CD software and must be approved by two employees, from different departments (one member of VPN Team and one member of Infrastructure Team).

Does VPN configuration files have any logging enabled?

ProtonVPN VPN's configuration files which were verified do not have any logging enabled.

List of assets which configuration was verified were:

- OS kernel logging
- any hosts level logging solutions (rsyslog and journald)
- all VPN software configuration files installed on the server:
    - OpenVPN configuration files (/etc/openvpn/*)
    - WireGuard configuration file (/etc/wireguard/wg0.conf)
    - strongSwan configuration files (/etc/strongswan/*)

Does ProtonVPN log the information about which VPN server is the user connected to at the time (and analogically - which user is connected to the specific VPN server)?

ProtonVPN does not log such information. 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 ProtonVPN does not log information about which VPN server the user is connected to. Analogically, ProtonVPN does not log the 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 ProtonVPN 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.

ProtonVPN 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.

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