securitum

Security report

SUBJECT

CactusVPN No-Log Policy Audit

DATE

20.04.2026 – 08.05.2026

LOCATION

Warsaw, Poland

AUTHOR

Martin Matyja (remote)

VERSION

1.0

securitum

Executive summary

This report summarizes the findings of an independent security assessment conducted by Securitum, commissioned by Cactus VPN LLC. The primary objective of this engagement was to validate that CactusVPN's server infrastructure strictly adheres to its publicly stated No-Logs policy.

The policy asserts that no user activity, network traffic or connection metadata - including IP addresses and DNS queries - is logged, monitored or stored on the servers. Furthermore, the infrastructure is purposefully built to ensure absolutely no identifiable data is ever collected or retrievable, thereby guaranteeing complete user privacy.

The text of the No-Logs policy is available for review at the following location:

- https://www.cactusvpn.com/terms-conditions/

To achieve this objective, Securitum dispatched a security consultant to engage directly with the Cactus VPN representatives. The assessment occurred between April 20, 2026, and May 7, 2026, constituting nine person-days of focused technical evaluation.

The assessment involved technical inspection of proprietary components and live system analysis to verify that the deployed environment contains no mechanisms or misconfigurations of collecting or retaining user-identifiable data.

Engagement Scope and Methodology

The assessment was designed to provide a whitebox validation of Cactus VPN's privacy claims. The Securitum's methodology combined policy verification with a focus on the VPN client's interaction, process evaluation and hands-on inspection of production systems.

It should be notice that the Cactus VPN team provided full requested transparency, granting the auditor access to the production instances, required permissions, access to different types of clients' accounts and answers all the questions issued.

The scope of the audit covered:

1. The VPN instances – running instances responsible for network traffic, supporting multiple protocols (e.g., WireGuard).
2. VPN clients – multiple types of VPN clients (e.g., Firefox extension, Linux app) running on the customer devices.

Audit Activities

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

Configuration Analysis

The engagement included a review of the configuration files regarding various services deployed on production instances. Auditors verified that the logic governing traffic handling does not contain instructions to log user activity.

Live System Inspection

The direct and hands-on examination of production servers were performed. Securitum auditor independently examined all four provided production servers across four locations. The analysis focused on file system integrity, running processes, configurations to identify any mechanisms or their configurations capable of storing and collecting user data.

Client Interaction with Infrastructure

Evaluation of production connection to the servers using a dedicated VPN client were performed. The auditor had access to execute a valid VPN service connection from the controlled device and VPN server to which the connection was created. It allowed to examine, in real time, the potential ways of logging user data.

Key Areas of Investigation

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

1. User activity tracking – verification that user activity is not tracked or logged on production egress servers.
2. Metadata logging - verification that connection metadata, such as DNS traffic, is not logged.
3. Network traffic inspection – verification that user network traffic is not inspected or logged.
4. Service monitoring - verification that services a user connects to are not monitored.
5. Policy uniformity - verification that the No-Logs policy is applied uniformly across all regions.
6. Configuration Files - verification that active configuration files have no logging enabled.

Contents

Change history

Document date	Version	Change description
08.05.2026	1.0	The final version of the security report.

Detailed Findings

This section presents a comprehensive analysis of the privacy and security claims made by CactusVPN. The findings below are the result of a direct inspection of CactusVPN's production servers and live system and connection inspection.

CactusVPN does not track or log user activity within VPN servers

Status: Confirmed

Securitum confirmed that Cactus VPN does not track or log user activity on its VPN servers. A live server inspection, incorporating a forensic approach across all four servers, revealed no user data stored in memory or transmitted to external systems. The analysis also included a comprehensive review of all processes running on the instances. Ultimately, no evidence of activity tracking was found.

CactusVPN does not log user-attributable connection metadata, such as DNS traffic

Status: Confirmed

Securitum confirmed that connection metadata is not logged. The configuration of metadata services, such as the DNS resolver, does not reveal any enforced logging mechanisms. The DNS cache mechanism revealed a default configuration that stores a specified number of records entirely in memory, and these records are not saved to disk. To deliver a higher level of performance, the Time-to-Live (TTL) option was set to its default value.

The auditor verified that this cache exists in memory and is not written to persistent logs that could be analyzed post-mortem. Searches for raw log files on the egress servers yielded no metadata that could be linked to individual users or their specific activities. The risk of correlating a domain to a specific user is assessed as negligible due to the high volume of shared traffic and the lack of user identifiers in the DNS requests.

CactusVPN does not inspect or log user network traffic on its VPN servers

Status: Confirmed

The audit confirmed that CactusVPN does not inspect or log the payload of network traffic. The VPN stack consists of multiple components supporting various methods of traffic routing, but its core relies on a WireGuard-based stack.

All components were verified against their configurations, execution methods, and custom process modifications. No evidence of inspecting or logging user network traffic was found across all four production servers.

Active VPN configuration files do not have logging directives enabled

Status: Confirmed

During a live system inspection of the production instances, server-side configuration files were confirmed to have logging directives explicitly disabled or left unconfigured if the default behavior of the components does not activate logging. The auditor inspected the configurations of various services, such as WireGuard, DNS resolvers, and additional proxies, alongside system-level daemons and components (e.g., `journald`).

No parameters were found that would lead to the logging of user traffic, associated metadata, or IP addresses.

The No-Logs policy is applied uniformly across all servers and geographic regions

Status: Confirmed

During the review of four production servers across different locations, it was found that identical or similar configurations - or configuration principles - were applied to every server instance. Manual verification confirmed that servers in different locations consistently adhered to the same strict no-logging policy for user data.

Conclusion

Securitum has completed its independent third-party assessment of the CactusVPN infrastructure and its adherence to its publicly stated No-Logs policy. The engagement involved a direct review of production systems and client software interaction.

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.

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