



ASSURED

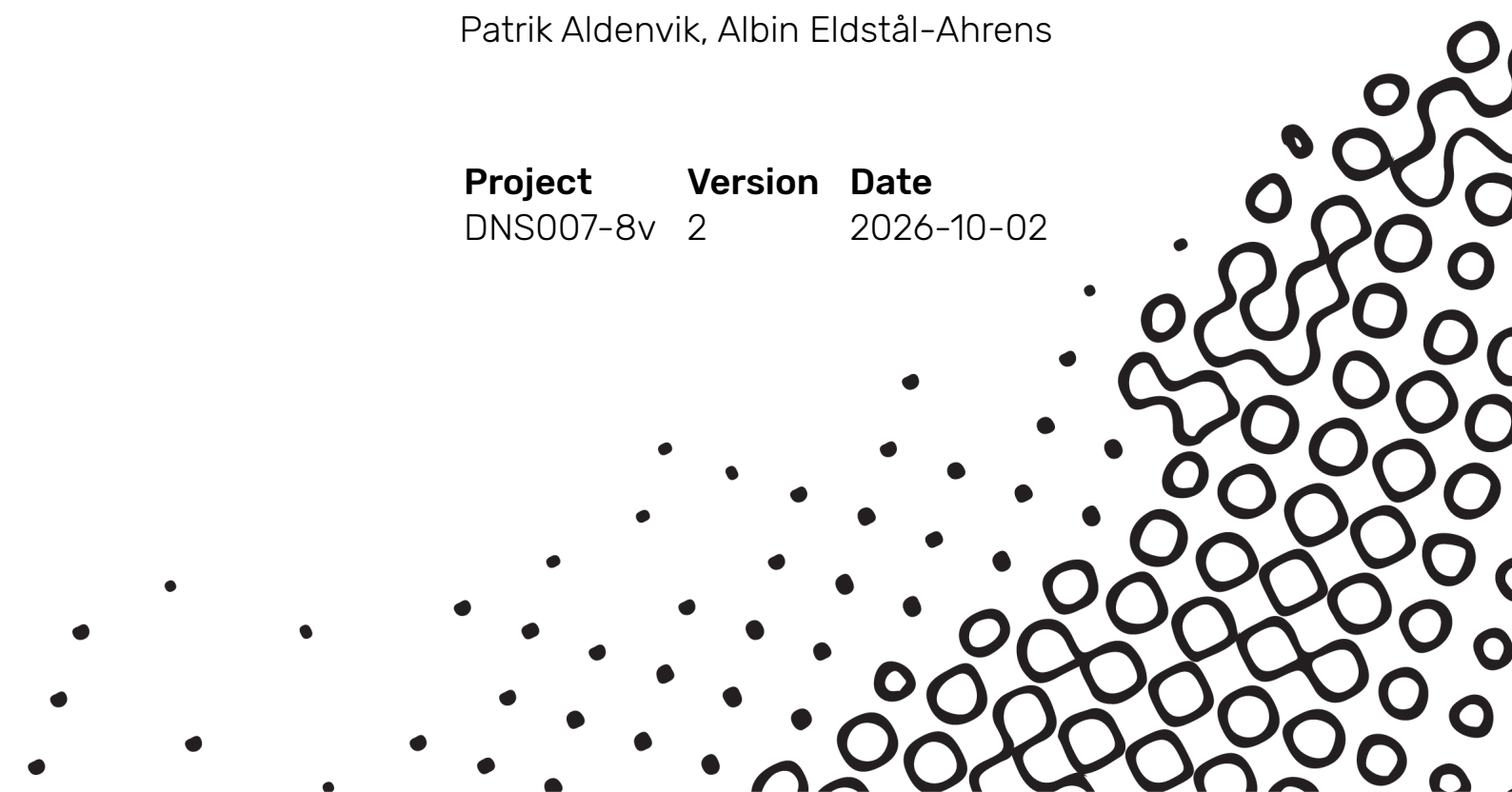
SECURITY CONSULTANTS

Report

DNSFilter Infrastructure Verification Test

Patrik Aldenvik, Albin Eldstål-Ahrens

Project	Version	Date
DNS007-8v	2	2026-10-02



Executive summary

Between 2026-05-20 and 2026-06-18 Assured Security Consultants performed an assessment covering DNSFilter's Guardian Connect VPN infrastructure environment hosted across Google Cloud Platform and a Proxmox hypervisor setup. Further, between 2025-09-21 and 2025-09-22 a verification test was performed, where the findings from the original report has been reassessed and given a status of:

FIXED, **PARTIALLY FIXED**, **ACCEPTED** or **REMAINING**.

The scope included multiple security components: Secure Gateway (SGW) relay servers, their virtualization host, the backend API server for user connectivity, an associated load balancer serving that API, and the User Database containing account information.

A primary objective of this engagement was to verify the operational design where Personally Identifiable Information (PII), such as login credentials and billing details, remains strictly segregated from network traffic logs or peer IP address data managed on relay nodes.

Six findings were identified as Medium severity focusing on privacy concerns, principle of least privilege and firewall configuration in the server environment. These include logging of client IP addresses when users bypass the API load balancer or when TLS errors occur towards the SGW. Additionally, specific firewall rulesets containing permissive source port allowances were observed that could allow traffic bypass. Also the database stores email addresses in plain text and an overprivileged Google Cloud Service Account was identified.

Observations were made with the following risk severity assessments (number of issues):

Critical **0** High **0** Medium **6** Low **4** Note **0** Good **1**

The main objective of this audit was to verify that users could not be identified and there are a couple of observations that contradict this. Email addresses are stored in plaintext and there is logging of client IPs on the SGW and API server under some specific circumstances. The load balancer allows for HTTP, which might be abused for a man in the middle attack by an adversary on the same local network.

The verification test shows that Guardian has prioritized mitigating issues in their infrastructure. A majority of the Medium findings has been fixed. The issues with status ACCEPTED is a work in progress or has been classified as a low risk issue by Guardian. No issues related to customer traffic integrity remains and issues with potential privacy impact was dealt with swiftly.

Assured would like to thank the Guardian team for their support during this assessment. We are happy to answer any questions and provide further advice.

Contents

3	Observations	2
3.1	Server-Audit	2
3.1.1	MED FIXED API logs client IP	2
3.1.2	MED FIXED SGW firewall bypass	2
3.1.3	MED FIXED SGW API Client IP logged on TLS errors	2
3.1.4	MED ACCEPTED DB plaintext storage of user email	3
3.1.5	MED FIXED LB/API/DB cross environment access	3
3.1.6	LOW ACCEPTED SGW and Hypervisor disk unencrypted	3
3.1.7	LOW FIXED LB accepts API traffic over insecure HTTP	4
3.2	GCP	5
3.2.1	GOOD Default resources	5
3.2.2	MED ACCEPTED Overprivileged service accounts	5
3.2.3	LOW ACCEPTED Rotation of service account keys	5
3.2.4	LOW ACCEPTED Publicly available management port	5
4	Privacy considerations	6
4.1	API load balancer (LB)	6
4.2	API server (API)	6
4.3	Database server (DB)	7
4.4	Secure Gateway (SGW)	7
4.5	Hypervisor	8
4.6	GCP hosting infrastructure	8

Verification state tagging

When we conduct a verification test, we tag the re-tested observation with the state depending on whether they are fixed, partially fixed, remaining or accepted, with the following corresponding tags:

- **FIXED** for verified fixed findings.
- **PARTIALLY FIXED** for findings where we found partial mitigation in effect.
- **REMAINING** where the finding was verified still valid.
- **ACCEPTED** where the finding was valid but will not be fixed by the customer for some reason.

3 Observations

3.1 Server-Audit

3.1.1 MED FIXED API logs client IP

Likelihood: LOW (2), Impact: HIGH (6)

The API server logs the IP address of the client that issues the HTTP request towards its listening ports 80 and 443.

A typical user, using the Guardian applications, will connect to the load balancer that in turn will forward traffic to the API server and in that scenario the load balancer's IP address will be logged. But if a user decides to connect directly to the API server, the client IP address will be logged by the API server.

Verification Note: The API server no longer logs the client IP that issued the HTTP(s) request.

3.1.2 MED FIXED SGW firewall bypass

Likelihood: MEDIUM (3), Impact: MEDIUM (3)

The firewall on the SGW is configured to drop incoming traffic except for a set of allowed source ports. The ruleset includes rules which can be exploited to bypass the firewall and connect to any service listening on the internet interface, even if it would normally be blocked by the firewall.

Verification Note: The firewall allow rules that were based on source port have been removed.

3.1.3 MED FIXED SGW API Client IP logged on TLS errors

Likelihood: LOW (2), Impact: HIGH (6)

The relay servers expose an HTTPS API used by clients to register WireGuard/IKEv2 keys for new devices. When a client violates the TLS protocol in one of various ways, error messages are written to the system log which contain the client's public IP address.

Verification Note: The client IP is no longer logged when TLS errors occurs.

3.1.4 MED ACCEPTED DB plaintext storage of user email

Likelihood: LOW (2), Impact: HIGH (6)

User account emails exist in plaintext within the database. This was observed during data inspection using psql queries against the application database.

Verification Note: As for now it is possible to retrieve user account email addresses in plaintext from the database. Guardian looks for alternatives that also can handle business requirements.

3.1.5 MED FIXED LB/API/DB cross environment access

Likelihood: LOW (2), Impact: HIGH (6)

The load balancer, API servers and database instances maintained active connectivity to hosts outside their own environment via a mesh network.

Verification Note: Cross environment access is no longer possible from the assessed servers.

3.1.6 LOW ACCEPTED SGW and Hypervisor disk unencrypted

Likelihood: LOW (2), Impact: MEDIUM (5)

The root filesystem of the relay server hypervisor is unencrypted. An attacker with physical access to a powered-down server is able to both read the full contents of the filesystem and compromise the installation by installing their own authentication bypass mechanisms. This affects both the hypervisor (virtualization host) and guests (individual SGW relay servers).

Verification Note: Disk encryption was not present on the SGW or Hypervisor. This is a work in progress and at the time of the verification test the implementation had not reached its final state.

3.1.7 LOW FIXED LB accepts API traffic over insecure HTTP

Likelihood: LOW (1), Impact: MEDIUM (5)

The load balancer in front of the Connect API allows clients to connect using unencrypted HTTP and forwards the connections to the underlying API server. This means that a client which is mislead to connect via HTTP will transmit and receive credentials in clear-text. This would allow eavesdropping as well as correlating user credentials with a user's public IP address.

Verification Note: All HTTP connections made towards the load balancer are now redirected to HTTPS.

3.2 GCP

3.2.1 GOOD Default resources

The environment had configured default resources, such as networks and service accounts, according to the principle of least privilege. Also none of the default resources was utilized. This is a good pattern since the default resources are assigned at creation time unless anything else is specified and could provide accidental superfluous privileges or access.

3.2.2 MED ACCEPTED Overprivileged service accounts

Likelihood: LOW (2), Impact: HIGH (7)

A service account has been granted more privileges than it uses in its day-to-day task.

Verification Note: GCP does not provide an out-of-the box solution for this service account. A working solution is investigated.

3.2.3 LOW ACCEPTED Rotation of service account keys

Likelihood: LOW (2), Impact: MEDIUM (3)

There were service accounts with user-managed keys¹ that are older than the Google recommendation of 90 days.

Verification Note: There are service accounts with keys older than 90 days. The risk of not rotating keys every 90 days has been accepted by Guardian.

3.2.4 LOW ACCEPTED Publicly available management port

Likelihood: LOW (1), Impact: MEDIUM (5)

All hosts in scope expose the management service SSH to the Internet.

Verification Note: The verification confirms that SSH is still exposed publicly. At the time of the verification test Guardian finds SSH as the best solution.

¹<https://docs.cloud.google.com/iam/docs/service-account-creds#key-types>

4 Privacy considerations

This section provides an overview of factors audited on the relevant servers. In cases where observations were made with a potential privacy impact, issues are listed in Section 3 *Observations*.

4.1 API load balancer (LB)

The HAProxy access logs are prevented from including the API client's IP address by two mechanisms: an `error-log-format` string which does not include `%ci`, and the directive `http-request set-src src,ipmask(0,0)` which rewrites the source IP address to `0.0.0.0` or `0::0`. Consequently, the log files contain either the string `<redacted>` or `0.0.0.0` in place of the client's IP address.

The HAProxy configuration includes the option `forwardfor` directive, which enables the X-Forwarded-For header. Due to the `ipmask` described above, the user's actual IP address is **not** included in the header.

Connection failures and TLS errors follow the same logging rules.

The firewall is configured to log the IP address of clients who attempt to connect on unexpected ports. This does not include connections to the API itself, but captures port scans and intrusion attempts targeting the load balancer host.

The default GCP full disk encryption is enabled for this host.

4.2 API server (API)

The Guardian-developed housekeeping daemon logs to `stdout/stderr` and during the course of the test no PII has been identified in this output.

Nginx was configured to anonymize the IP in the X-Forwarded-For header sent by the LB. It was found to also be possible to access the API server directly, and in that scenario the client IP was stored in the access log. This is not the behavior of the Guardian client, which always connects via LB.

The firewall is configured to log the IP address of clients connecting on unexpected ports. This does not include connections to the API itself, but captures port scans and intrusion attempts targeting the API host directly.

The default GCP full disk encryption is enabled for this host.

4.3 Database server (DB)

The database has no direct client contact but stores information for the API. The logs as well as the database have been audited for PII and the user accounts' email addresses were found in plaintext in the database. It is possible to create an account and use the service without registering an email address.

The firewall is configured to log the IP address of clients who connect on unexpected ports. This does not include users, as users do not directly connect to the DB server.

The default GCP full disk encryption is enabled for this host.

4.4 Secure Gateway (SGW)

SGW is not subject to automatic backups or data retention, and the host is considered disposable. SGWs are rebooted at least once per 30 day period, at which point any journald logs are lost.

Dynamic debug logs (dyndbg) are not enabled for the kernel wireguard subsystem. This means that built-in debug log calls are bypassed, and wireguard activity is not written to the kernel log.

The Strongswan Charon IPsec daemon is configured with no `filelog` or `syslog` configurations. The `charon-systemd` service is configured with only a default `journal` loglevel of `-1`, which prevents any logging to the `systemd` journal.

No logging firewall rules are configured.

Authentication failures (e.g. mistyped password, misregistered device, expired credentials, ...) from VPN clients and API clients are not logged to disk.

The Guardian-developed `relay-rs` daemon has logging to file enabled by default, with a hard-coded log level of `ERROR` and above. The source code was audited for configured log calls, and none were found to contain user information such as public IP addresses or activity. No log was written during testing.

The Guardian-developed `zoe-agent` daemon has logging centralized to a single class. Log calls in the codebase have been inspected, and do not include any user PII such as IP addresses or activity. Anonymized device IDs (i.e. ID of an ephemeral wireguard key pair or ephemeral IKEv2 credentials) are present, but these cannot be correlated to users or IP addresses.

API client IP addresses were found to be logged by `zoe-agent` under rare error conditions, caused by library code included in the Go standard library `net/http`. This is triggered by TLS malfunctions such as connection failure during handshake or a client connecting with invalid parameters. The logged IP address is not linked to any user account or VPN traffic,

and may not belong to any DNSFilter user.

VPN connection failures are not logged.

Usernames of VPN users were not found on the relay server.

4.5 Hypervisor

No further PII has been detected on the filesystem compared to the SGWs.

The firewall is configured to log the IP address of clients who connect on unexpected ports. This does not include normal user traffic, but captures port scans and intrusion attempts targeting the hypervisor host directly.

4.6 GCP hosting infrastructure

The virtual machines running the LB, API and DB servers do log to the Google Cloud Platform, such as the boot sequence and daemon events. No PII has been identified in the GCP logs.

The virtual machines are backed up every 8 hours and the backups are stored for 14 days.

There are no network flow logs recorded in the GCP Virtual Private Cloud where the virtual machines are located.

