EVALUATION REPORT

VPN Performance **World Tour**

- CONSUMER
- MULTI PLATFORM
- GLOBAL - 5 ORIGINS
- AMTSO ALIGNED

2026 GLOBAL VPN PERFORMANCE RACE

VPN Performance

H1 2026

amtso
The cybersecurity industry's testing standard community
STANDARD

PRODUCTS IN TEST

ExpressVPN
Mullvad
NordVPN
ProtonVPN
Surfshark

Contents

ABOUT US

ARTIFACT SECURITY

Artifact Security is an independent testing firm in London focused on the real-world performance of consumer security and privacy products. Our methodology is built for reproducibility, not marketing benchmarks.

All evaluations run in isolated, repeatable environments. Products are acquired commercially. Methodology design in accordance with AMTSO VPN Guidelines.

TRANSPARENCY · INNOVATION · PARTNERSHIP

Core Team

Stefan Dumitrascu
Chief Executive Officer

Ana Maria Pricop
Chief Business Officer

Erica Marotta
Technical Lead

Dimitrios Tsarouchas
Offensive Test Lead

The race result

NordVPN tops the regional medal table — the only vendor to earn an overall Platinum, winning three of five regions outright. ExpressVPN, ProtonVPN and Surfshark follow on Gold, Mullvad trails, held back by inconsistent throughput. Category bests: NordVPN leads download and upload, while ProtonVPN owns latency and consistency (by far the lowest jitter).

From dimensions to medals

We analysed both individual scores for things such as download, upload, latency and jitter and also looked at an Olympics-style table that yields a clear overall standing while keeping every dimension visible.

FASTEST DOWNLOAD*

908 Mbps NordVPN

FASTEST UPLOAD*

920 Mbps NordVPN

LOWEST LATENCY*

183 ms ProtonVPN

*Highest category peaks achieved by vendors

OVERALL AWARDS

NordVPN

91 · Platinum

ExpressVPN

84 · Gold

ProtonVPN

83 Gold

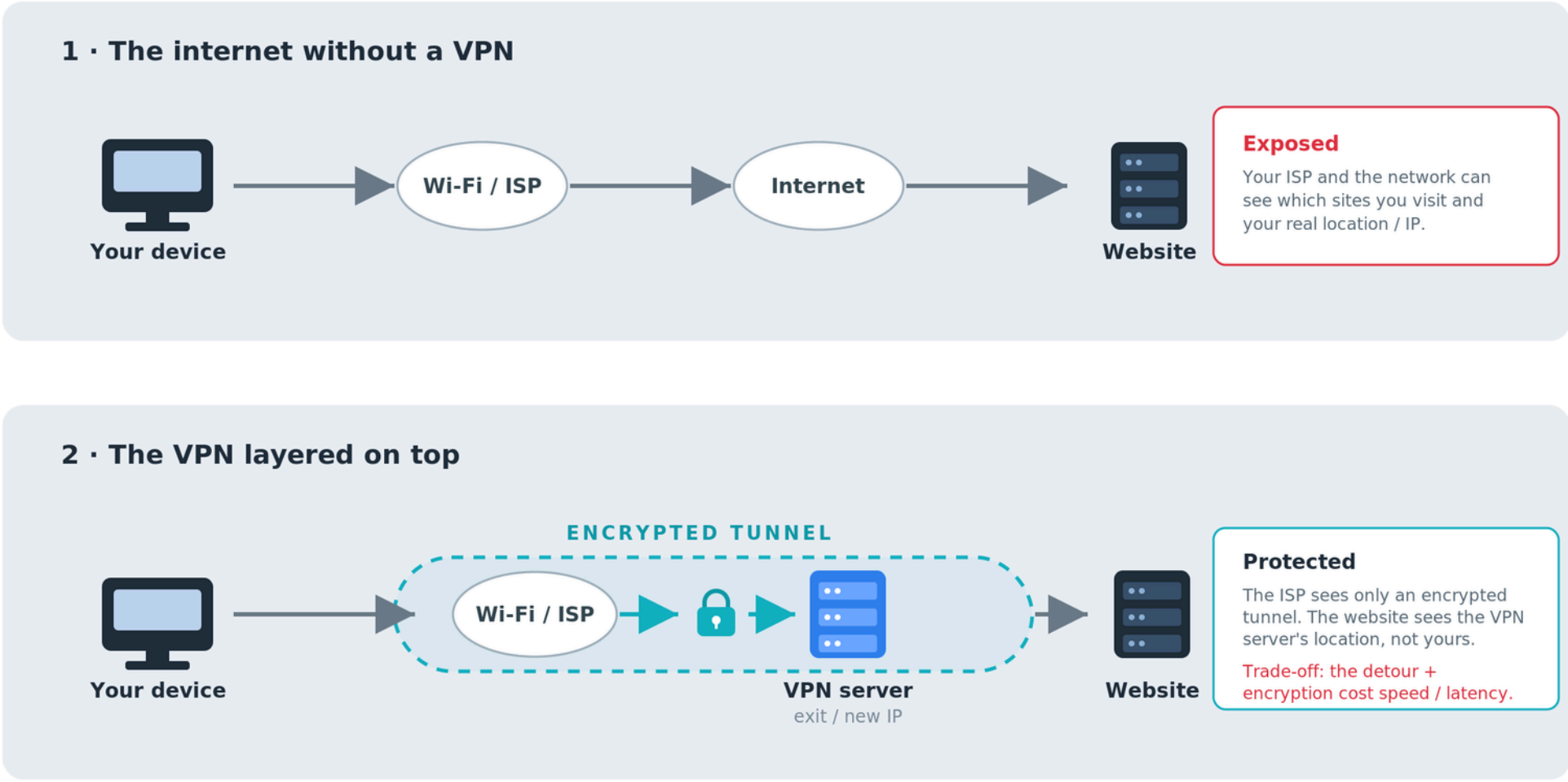
Surfshark

81 · Gold

Mullvad

70 Silver

A VPN routes your traffic through an **encrypted tunnel** to a remote server before it reaches the wider internet. The same path runs first without protection, then with the VPN layered on top.



Four numbers, not one

A fast download does not guarantee low latency. These four dimensions move independently, which is why we never collapse them into a single score.

DOWNLOAD

Throughput pulling data — the headline Mbps figure.

UPLOAD

Throughput pushing data — calls, backups, sharing.

LATENCY

Round-trip delay in ms — set by distance & routing.

JITTER / LOSS

Stability — variation and dropped packets under load.

What moves the numbers

- **Distance to the exit server** sets a latency floor — SF→Frankfurt is ~150 ms before any VPN overhead.
- **Encryption & packet processing** add load on both device and server.
- **Protocol** (WireGuard vs OpenVPN), server load and congestion all shift results.
- **Route quality** between VPN region and destination can matter more than the brand.

55 highways

Each pins the origin to a fixed destination test server via a chosen VPN region.

5 origin regions

Germany (Frankfurt), Singapore, US West (San Francisco), US East (New York), United Kingdom (London)

Targeted speed tests

Ookla is given the exact destination server ID — real SF→destination tunnel.

Outlier trim

We remove the single fastest and slowest run per vendor per highway.

Results that buyers, journalists and vendors can all reproduce.

TRANSPARENCY

Reproducible, isolated environments. Documented exclusion rules. Raw per-run data retained and shared on our Transparency Portal.

INNOVATION

The first real hardware on location testing. Real laptops and phones across the world, replicating real world conditions.

PARTNERSHIP

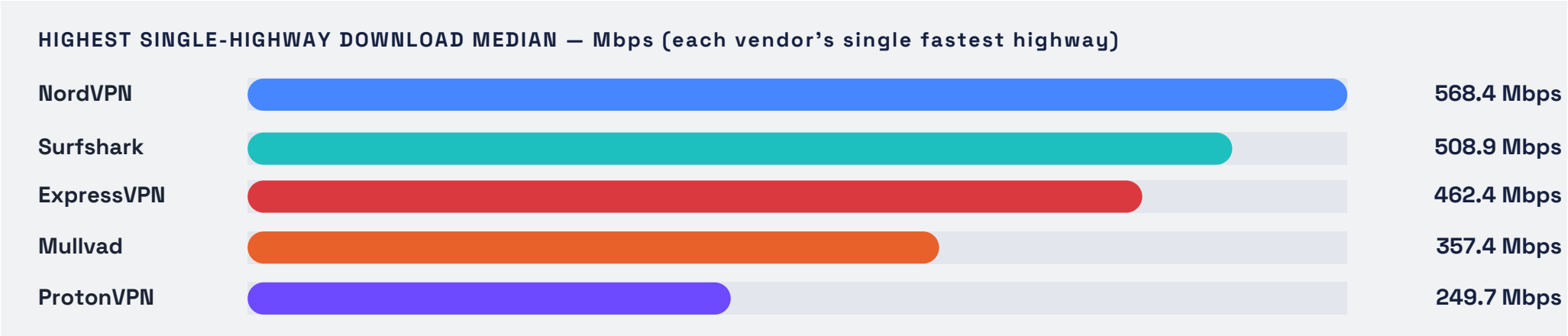
AMTSO-aligned testing. Products acquired commercially. Vendors given a right of reply.

OUTCOME — Independent, repeatable evidence that holds up to scrutiny from every side of the table.

VENDOR LEADERBOARD

Windows, route-pinned · ordered by average download

Vendor	Avg DL	Median DL	Highways /24	Avg Lat	Jitter	Loss
NordVPN	271.9	568.4	12	238.8	16.3	0.61%
ExpressVPN	257.4	462.4	9	227.5	18.78	0.48%
Surfshark	208.7	508.9	1	236.9	15.51	0.96%
Mullvad	192.0	357.4	0	237.8	9.15	0.92%
ProtonVPN	165.2	249.7	2	231.4	5.93	0.58%



RESULTS BY REGION

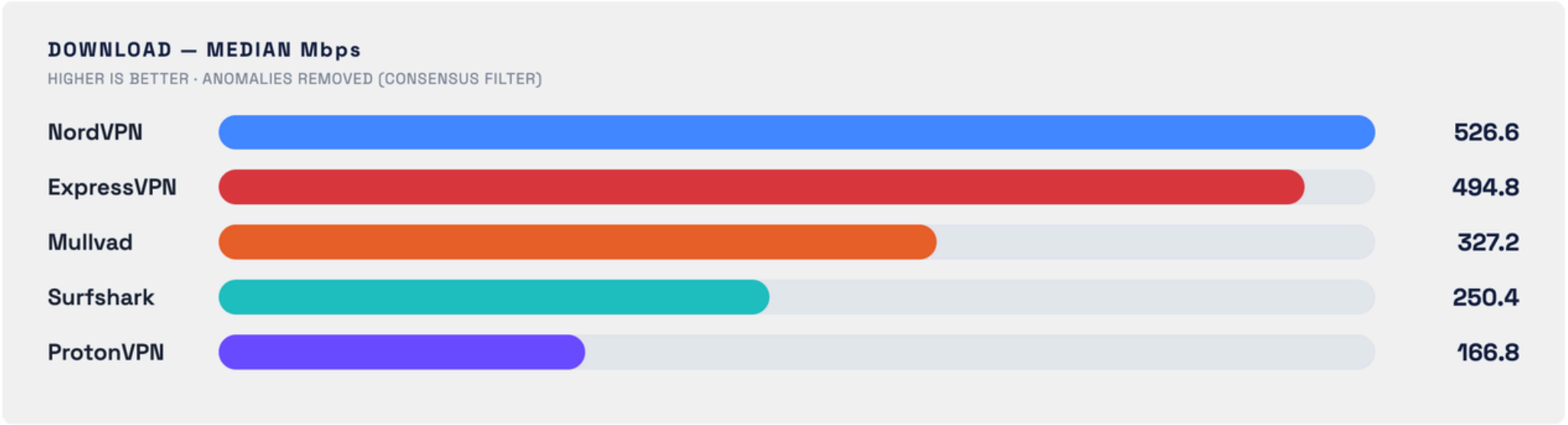
MEDIAN DOWNLOAD BY REGION — Mbps (route-pinned, per vendor) · highlighted = region winner

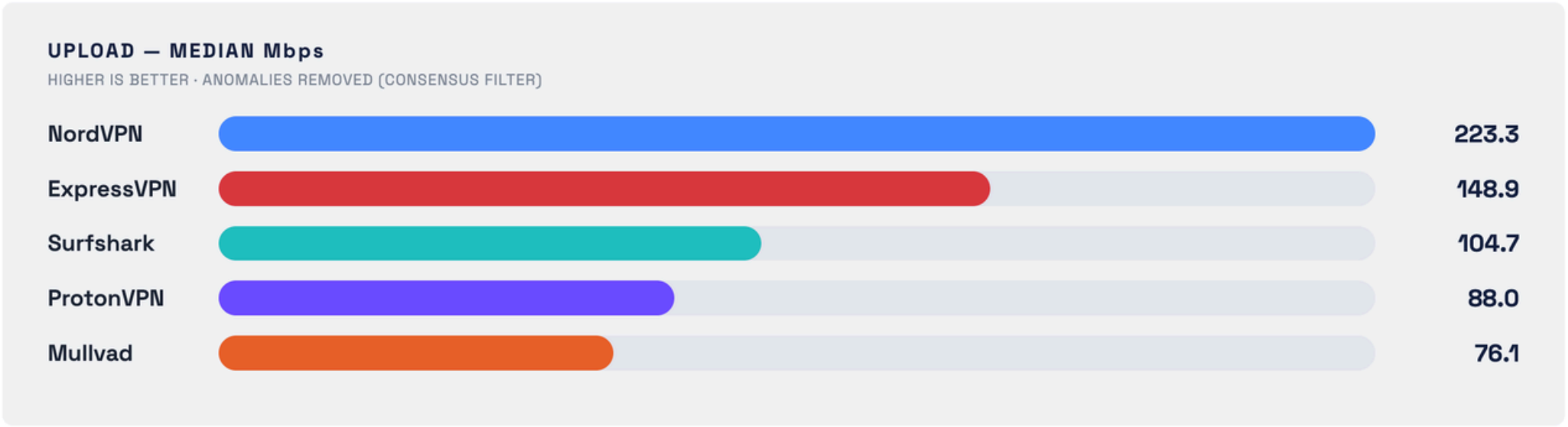
Vendor	Frankfurt	London 1G	Singapore	US East	US West
ExpressVPN	92	350	132	120	357
Mullvad	93	286	34	23	184
NordVPN	109	**483**	195	**140**	**548**
ProtonVPN	109	365	140	37	438
Surfshark	**142**	467	**215**	85	179

PEAK SINGLE-HIGHWAY DOWNLOAD — Mbps (each vendor's single fastest highway)

ANDROID RESULTS

Android throughput, measured speeds. Tests performed from **London**. Bars show **absolute download and upload** — the median of each vendor's per-highway medians.





TIME TO CONNECT & RELIABILITY · METHODOLOGY

What we measure. Time to Connect (TTC) is the gap between starting a connection and having a usable, encrypted tunnel. We capture it at the network level — not by trusting the app's on-screen timer.

Two numbers, on purpose. The **protocol** time is when the secure handshake finishes (measured from packet timestamps). The **real-world** time is when a live web request actually gets a reply. The gap between them exposes a VPN whose app says "Connected" before traffic is truly routing — a delay the interface hides.

Reliability too. Alongside speed, we run repeated connection attempts and record how many succeed. A connection that never establishes within 30 seconds counts as a failure. Any vendor below 95% success on a route is flagged.

Handshake: the brief back-and-forth where your device and the VPN server agree on encryption keys before any of your data is sent.

HOW EACH RUN WORKS

1. **Start clean.** Confirm the app is fully disconnected, with a packet capture already running on the real network adapter.
2. **Connect & time it.** The clock starts, the operator hits Connect, and the handshake is timed from the captured packets.
3. **Prove it routes.** The instant the app says "Connected," a web request fires to confirm traffic is genuinely flowing.
4. **Repeat & trim.** Five attempts per route; the fastest and slowest are dropped and the rest averaged.

RATING SCALE

NEGLIGIBLE	2 seconds or less — you'd barely notice.
MINOR	2–4 seconds — a short, tolerable wait.
DISRUPTIVE	4–10 seconds — long enough to annoy.
CRITICAL	Over 10 seconds — frustrating every time.

THE BOTTOM LINE

Measuring at the packet level — and confirming traffic actually flows — gives an honest connect time that an app's own "Connected" label can't. It's the difference a user feels every time they switch their VPN on.

How long from clicking **Connect** to a working tunnel — and how often does it fail? **50 scripted connect/disconnect cycles per vendor** (SC-CP-01/02) · Windows, run from London — the fastest connection in the test at 1 Gbps, showing the best-case scenario. Operator-timed with a packet capture behind every attempt.

Vendor	TIME TO CONNECT s (user-experienced · wire)	CSR ≤30 s wire-verified	CSR ≤30 s test-rig loop	Loop TTC s incl. verification lag	Pure handshake ms (wire only)
● NordVPN	1.8	98%	98%	2.19	10
● ExpressVPN	14.6‡	98%	54%	18.83	15‡
● Mullvad	2.5	100%	100%	3.55	6
● Surfshark	2.9†	100%	100%	2.87	—
● ProtonVPN	2.9	98%	90%	15.02	12

Does anything escape the tunnel? Three tiers: **standard** steady-state checks, **split-tunneling** isolation, and **advanced** stress cases. All run inside the same evidenced live sessions. Windows · all five vendors complete.

Test case	Scenario	What a pass looks like	NordVPN	ExpressVPN	Mullvad	Surfshark	ProtonVPN
STANDARD LEAK CASES — STEADY STATE							
IP leak	SC-LR-01	Exit IP is a VPN server address; real ISP IP never observed at the exit	NO LEAK	NO LEAK	NO LEAK	NO LEAK	NO LEAK
DNS leak	SC-LR-02	Extended DNS test: every resolver inside the provider's network — zero ISP resolvers	NO LEAK	NO LEAK	NO LEAK	NO LEAK	NO LEAK
IPv6 leak	SC-LR-03	No IPv6 path present while connected — nothing to leak over IPv6	NO LEAK	NO LEAK	NO LEAK	NO LEAK	NO LEAK
WebRTC leak	SC-LR-04	Browser WebRTC exposes neither the real public IP nor local candidates	NO LEAK	NO LEAK	NO LEAK	NO LEAK	NO LEAK
Server-switch leak	SC-LR-05	Live UK→DE server switch under capture — no traffic from the real IP during transition	NO LEAK	NO LEAK	NO LEAK	NO LEAK	NO LEAK
SPLIT-TUNNELING CASES							
Cross-tunnel isolation	SC-LR-08	Excluded browser off-tunnel, tunneled browser inside — no cross-leak either way	NO LEAK	NO LEAK	NO LEAK	NO LEAK	NO LEAK
ADVANCED CASES							
Kill-switch drop window	SC-MF-03	Pcap review, all vendors: block never hit the tunnel endpoint	NO LEAK	NO LEAK	NO LEAK	NO LEAK	NO LEAK

We disclose what we did not test and why. Deferred to Round 2 on the isolated lab VLAN: SC-LR-07 (dual-AP handover) and SC-LR-09 (TunnelVision, rogue-DHCP option-121 . Findings are IPv4-scope, each backed by probe JSON, screenshot and hashed capture.

Does the VPN exit trigger **CAPTCHAs or block pages** on everyday browsing? All five vendors · London (UK) exit · Windows · SimilarWeb Top-100 corpus, walked step-by-step (homepage → login/auth → sub-pages).

HARD BLOCK PAGES

0

No outright denials of service, any vendor

CLEAN-SITE RATE

98% no challenge at any step

246 of 250 vendor-site walks clean

CAPTCHAs by vendor

Vendor	CAPTCHAs	Sites challenged	Hard blocks
Mullvad	1	1	0
Surfshark	2	1	0
ExpressVPN	2	2	0
NordVPN	2	2	0
ProtonVPN	4	4	0

Every recorded CAPTCHA is backed by a screenshot and the session HAR (SC-WA-01/02/03). All challenges were solvable in-session — none was a hard block.

WHERE FRICTION CLUSTERS

- fandom.com — 3 of 5 vendors
- claude.ai · mail.ru — 2 vendors each
- temu · github · bet.br — 1 vendor each

WHAT WE COUNT

- reCAPTCHA / hCaptcha / Turnstile
- Cloudflare interstitial
- 403 / 429 block page

READ WITH CARE

- Site-side bot defences, not vendor weakness
- CAPTCHA frequency is a usability signal
- Not a speed metric

The same handful of sites challenge several VPNs — fandom.com, claude.ai and mail.ru account for most of the friction — which points to site-side bot defences rather than a vendor-specific weakness. No vendor was hard-blocked on any site.

Do the headline features actually work? Each vendor walks a **scripted live session under continuous packet capture** — every step evidenced by an API probe, a screenshot and a SHA-256-hashed pcap.

Feature	Scenario	What a pass looks like	ExpressVPN	Mullvad	NordVPN	ProtonVPN	Surfshark
Auto-connect on launch	SC-MF-01	Quit app → relaunch → tunnel re-establishes with no manual action	PASS	PASS	PASS	PASS	PASS
Launch on boot	SC-MF-02	Reboot → tunnel established before any user-initiated traffic	PASS	PASS	PASS	PASS	PASS
Kill switch — drop	SC-MF-03	Tunnel forcibly dropped (transport endpoint firewall-blocked) → all outbound traffic halts	PASS	PASS	PASS	PASS	PASS
Kill switch — reconnect	SC-MF-04	From kill-switch state, reconnect → internet resumes cleanly on the new tunnel	PASS	PASS	PASS	PASS	PASS
Split tunneling	SC-MF-05	Excluded browser exits on real IP, tunneled browser on VPN IP — verified independently	PASS	PASS	PASS	PASS	PASS

HOW WE TEST

- One continuous packet capture per session
- Fixed scripted walk — same order, every vendor
- Forced drops, real reboots, real relaunches

EVIDENCE TRAIL

- ipleak / ipinfo / DNS probe JSON per step
- Screenshot at every verification point
- Pcap manifest with SHA-256 hash

What each vendor **says** its Windows app can do. Every cell is a vendor claim — official feature/support pages, July 2026 — not a test result. Names retained: these are public marketing claims. Each claim feeds the hands-on lab verification pass. Full register in the Appendix.

Claimed capability	ExpressVPN	Mullvad	NordVPN	ProtonVPN	Surfshark
Kill switch	Network Lock	Lockdown Mode — no internet unless tunnel up	Internet Kill Switch — two modes	Kill Switch + Advanced (permanent)	Kill Switch
Split tunneling	Per-app	Per-app exclusion	Per-app, standard + inverse	Per-app; works with kill switch + NetShield	Bypasser — apps + websites
Ad/tracker/malware blocking	Threat Manager (Advanced Protection)	DNS content blocking	Threat Protection Pro	NetShield (DNS-level)	CleanWeb
Multi-hop / double VPN	— no claim found	Multihop — user picks entry + exit	Double VPN servers	Secure Core (hardened entry nodes)	Dynamic MultiHop (Nexus)
Obfuscation / stealth	Automatic — no user toggle	WG over TCP / Shadowsocks / QUIC	Obfuscated servers + NordWhisper web-tunnel	Stealth protocol (WG over TLS)	NoBorders + Camouflage mode
Protocols (Windows app)	Lightway (+ Turbo) · OpenVPN fallback	WireGuard only	NordLynx · OpenVPN · NordWhisper	WireGuard · OpenVPN · Stealth	WireGuard · OpenVPN · IKEv2
Post-quantum encryption	Lightway ML-KEM	Quantum-resistant tunnels toggle	Default on NordLynx (X25519 + ML-KEM)	— no claim found	— no claim found
Dedicated IP	Pro plan	Not offered — by design	Paid add-on	Business plans only	Paid add-on
Port forwarding	Not offered	Removed 2023	Not offered	On P2P servers	Not offered

"No claim found" means the capability is not advertised for the Windows app as of July 2026 — not an assertion the feature is absent. Sources: vendor feature & support pages and Windows release notes, accessed 5 July 2026.

Round 1 of our World Tour

This is Round 1 of an ongoing programme. Logistically, it was one of the most difficult tests to pull of. We wanted to design the most realistic test possible for an average buyer that reflects what a VPN performs like across the world. We would like to thank all participants in this round.

We plan to follow up the testing with a further expansion later in H2 of this year with more platforms in the test.

Our highlighted Winners:

- **NordVPN —** fastest average download and winner in most of our locations.
- **ProtonVPN —** consistency (lowest jitter) & latency.

Performance is only one axis — pair these numbers with privacy, security and price.

NEXT ROUNDS

Later rounds broaden coverage across regions, highways and platforms, and will revisit any provisional call.

DATA AVAILABLE

Methodology identifier VPNPerf2026v1 available on our website here.

Full per-run dataset available on our Transparency Portal.

Stefan Dumitrascu
Chief Executive Officer

Ana Maria Pricop
Chief Business Officer

TRANSPARENCY · INNOVATION · PARTNERSHIP

APPENDIX — FULL CLAIMS REGISTER

The complete register of vendor claims behind the Claimed Features page — the working checklist for the lab verification pass. ✓ = claimed by the vendor · — = no claim found (July 2026) · every ✓ is scheduled for hands-on verification on the test machines.

Claim	NordVPN	ExpressVPN	Surfshark	ProtonVPN	Mullvad
CONNECTION & TUNNEL					
Auto-connect on app launch	✓	✓	✓	✓	✓
Launch / connect on OS boot	✓	✓	✓	✓	✓
Auto-connect on untrusted Wi-Fi	✓	✓	✓	—	—
Kill switch (drop protection)	✓	✓	✓	✓	✓
Always-on / permanent kill switch	✓	—	—	✓	✓
Post-quantum key exchange	✓	✓	—	—	✓
Obfuscation / censorship circumvention	✓	✓	✓	✓	✓
Multi-hop routing	✓	—	✓	✓	✓

Vendor extras (claimed): NordVPN — Meshnet (60 devices), Dark Web Monitor, Onion over VPN · ExpressVPN — Lightway Turbo (Windows), TrustedServer RAM-only · Surfshark — Rotating IP, Nexus SDN, 100% RAM-only · ProtonVPN — VPN Accelerator, Tor servers, Moderate NAT · Mullvad — DAITA, numbered accounts (no email). Sources: vendor sites, accessed 5 July 2026.

Claim	NordVPN	ExpressVPN	Surfshark	ProtonVPN	Mullvad
TRAFFIC CONTROLS					
Split tunneling (per-app)	✓	✓	✓	✓	✓
Split tunneling (per-website/IP)	via Browser Extension	✓	✓	via Browser Extension	—
Ad / tracker / malware blocking	✓	✓	✓	✓	✓
Custom DNS	✓	—	—	✓	✓
Local network (LAN) access toggle	✓	✓	—	✓	✓
Port forwarding	—	—	—	✓	—
DIFFERENTIATORS & ACCOUNT					
Simultaneous devices	10	14	Unlimited	10	5
Independent no-logs audit	✓	✓	✓	✓	✓