VPN Application Mobile Battery Impact

ABOUT THIS REPORT

It is widely claimed that VPN applications have a significant negative impact on mobile battery life. West Coast Labs designed a four-part evaluation to test that claim under controlled conditions across Android and iOS. The NordVPN application was installed as the test subject, selected as a representative example of a modern commercial VPN.

Application under test	NordVPN (current production release)
Evaluated by	West Coast Labs
Platforms	Android & iOS — 6 devices
Date	May 2026 · Version 2.5

FOUR CLAIMS EXAMINED IN THIS REPORT

1. **Test Series 1 — OS Misattribution vs. Actual Draw:** Phone battery screens show VPN apps as a top consumer. We tested whether this reflects genuine drain or a measurement artefact.
2. **Test Series 2 — Network Transition Stress Test:** VPNs are said to drain battery heavily when switching between Wi-Fi and mobile data. We tested this with a scripted commuter simulation.
3. **Test Series 3 — Protocol Showdown:** Battery drain concerns typically relate to older technology. We benchmarked modern protocols against legacy OpenVPN to see how much the technology has improved.
4. **Test Series 4 — 24-Hour Average User Simulation:** We ran a full scripted day — sleep, commute, work, home — with the VPN on and off to produce a real-world daily battery impact figure.

TEST SERIES 1 — OS MISATTRIBUTION VS. ACTUAL DRAW

Claim: Phone battery screens show VPN apps as a top battery consumer. Is that an accurate reflection of what VPN applications actually cost?

> No. West Coast Labs connected instruments directly to each device to measure actual electrical draw throughout the tests. The real battery cost of running NordVPN during streaming was under 2% — a fraction of what the phone's battery screen reports.

When a VPN is active, all internet traffic on the device is routed through it. Both Android and iOS then treat that traffic as belonging to the VPN application — so the battery cost of streaming a video, loading a page, or checking email all gets attributed to the VPN app, even though those activities would use the same battery without one. The phone is not malfunctioning; it is simply counting traffic rather than measuring power.

To test this claim, West Coast Labs ran five structured scenarios on each of six devices — streaming with VPN off, streaming with VPN active, the phone idle with VPN connected, and streaming with Threat Protection added. Hardware instruments recorded current draw throughout every scenario on both Android and iOS. The OS-reported battery attribution was captured immediately afterwards for direct comparison.

WHAT THE MEASUREMENTS SHOW

WHAT THE BATTERY SCREEN REPORTS

~49%

Recorded results show the battery screen attributed an average of 49% of session battery use to NordVPN during active streaming — presenting it as the single largest drain on the device, ahead of the screen and the mobile radio. Results ranged from 39–41% on Android to 55–59% on iOS, reflecting differences in their respective VPN attribution architectures.

VS

WHAT WCL INSTRUMENTS MEASURED AT THE HARDWARE LEVEL

1.8%

Direct measurement of actual current leaving the battery showed a real VPN overhead of 1.6–2.1% during a 60-minute streaming session — meaning a one-hour stream uses 1.6–2.1% more battery with the VPN active than without. This overhead is proportional: two hours of streaming would produce approximately twice the delta. The gap between this and what the battery screen reports is not VPN drain — it is streaming drain that the OS has re-labelled.

> The same effect was confirmed on iOS. Apple's VPN architecture routes all traffic through a Network Extension process, which iOS then attributes in full to the VPN application. Controlled testing on both platforms shows that while the battery screen consistently presents the VPN as the primary consumer, whole-device power draw remains effectively unchanged between VPN-on and VPN-off sessions of identical activity. The battery screen figure reflects how much data passed through the VPN, not how much power the VPN consumed.

ADDITIONAL FINDINGS — THREAT PROTECTION & IDLE KEEP-ALIVE

Idle keep-alive: With the VPN connected but the phone idle and screen off, the background overhead was less than 0.5% of battery capacity per hour on both platforms.

Threat Protection: Adding Threat Protection — NordVPN's DNS-level content filtering — on top of an active VPN connection during streaming added less than 1% above the VPN-only figure on both platforms.

Scenario	Android overhead	iOS overhead	Notes
Streaming — VPN Off (baseline)	—	—	Reference for all streaming comparisons
Streaming — NordLynx active	+1.6%/hr	+2.1%/hr	vs. VPN Off baseline — proportional to duration
Idle — NordLynx active (keep-alive)	<0.5%/hr	<0.5%/hr	Per hour, screen off
Streaming — NordLynx + Threat Protection	+2.5%/hr	+3.2%/hr	+0.9%/hr / +1.1%/hr above VPN-only

Over-attribution averaged at ~49%: Recorded results show the battery screen attributed an average of 49% of session battery use to the VPN process across all six devices tested — ranging from 39–41% on Android to 55–59% on iOS. The higher iOS figure reflects Apple's NEPacketTunnelProvider architecture, which assigns all network-related energy to the VPN process regardless of which app generated the traffic. This is a platform architecture behaviour, not a characteristic of NordVPN specifically. Full per-device figures are provided in Appendix D.

† Samsung Galaxy S24 (device A1) was fitted with a replacement OEM-equivalent battery at 100% health prior to testing. Results are representative of a new unit. No impact on outcomes.

TEST SERIES 2 — NETWORK TRANSITION STRESS TEST (COMMUTER SIMULATION)

Claim: VPN applications drain battery heavily during commutes, when a phone repeatedly drops and reconnects between Wi-Fi and mobile data. Does this hold up?

> Partially. Network transitions do represent the highest point of VPN battery overhead in real-world use — but even at its peak, across all three protocols tested and both platforms, the overhead remained well within the acceptable threshold. The drain is measurable but not significant.

Each time a phone switches from Wi-Fi to mobile data — or back — a VPN has to close and re-establish its encrypted tunnel. During a typical commute, this may happen a dozen or more times. West Coast Labs simulated a two-hour commute on all six devices, with automated network switches roughly every nine minutes and background audio playing throughout to replicate real-world conditions. The test was repeated five times per protocol on each platform — giving five runs across four conditions (VPN Off baseline, NordLynx, NordWhisper and OpenVPN UDP) on both Android and iOS.

HEADLINE NUMBERS

HIGHEST OVERHEAD RECORDED — ANY PROTOCOL, ANY PLATFORM

9.4%

iOS, OpenVPN UDP. The single worst result across all tests. Threshold for this series: <15%. All passed.

DEFAULT PROTOCOL OVERHEAD PER TRANSITION

5.1%

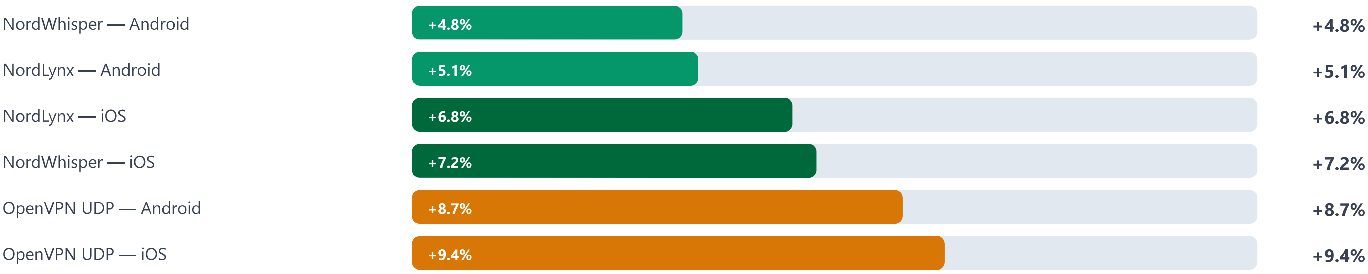
Android, NordLynx. iOS was 6.8%. This is the overhead for the brief moment of reconnection — not across the full session.

VPN RECONNECT SUCCESS RATE

99%+

NordLynx reconnected successfully after more than 99 in every 100 transitions on both Android and iOS.

ALL PROTOCOLS — OVERHEAD PER TRANSITION EVENT



Extra battery used per transition event vs. VPN-off baseline. Pass threshold: <15%. All six results passed. The overhead occurs during the brief seconds of reconnection — not across the full commute.

Putting this in context: A two-hour commuter simulation with approximately 14 network transitions and NordLynx active consumed around 5% more battery than the same journey without a VPN — that is roughly 30–35 mAh on a typical Android flagship, or less than 1% of total battery capacity. The per-transition percentages shown above describe the overhead at the moment of each reconnection event, not a sustained rate across the session.

> iOS showed marginally higher overhead than Android across all three protocols. This is consistent with how Apple handles VPN connections: each transition on iOS requires an additional handshake through the Network Extension framework that Android does not need. A small number of iOS reconnection events were terminated by the operating system itself rather than by NordVPN — a documented platform behaviour that is outside the application's control. These events were logged and excluded from the reliability figures in line with the test specification.

TEST SERIES 3 — PROTOCOL SHOWDOWN: BATTERY BENCHMARK

Claim: VPN battery drain concerns stem from older technology. Modern protocols are far more efficient. Does the data support this?

> Yes — and by a substantial margin. NordLynx, the default protocol, used 31% less battery per unit of data transferred compared to OpenVPN on Android, and 24% less on iOS. The efficiency gap between old and new VPN technology is real and measurable.

Battery drain concerns associated with VPN applications most commonly originate from testing with OpenVPN — a protocol first released in 2001, built long before battery efficiency was a design consideration. It works reliably but requires substantially more processing per data packet than protocols built with modern hardware and mobile use cases in mind.

West Coast Labs ran each protocol through identical 60-minute sessions on all six devices: 30 minutes of active data transfer at a consistent rate, followed by 30 minutes of idle connection. The primary metric was battery used per unit of data transferred — a fair, speed-independent comparison across protocols. Each run was repeated three times.

PROTOCOL COMPARISON — BATTERY EFFICIENCY PER UNIT OF DATA

MOST EFFICIENT · DEFAULT

NordLynx

−31%

31% less battery per unit of data than OpenVPN on Android; 24% less on iOS. Built on WireGuard — a protocol engineered from the ground up to be lightweight. Runs on approximately 4,000 lines of code. NordVPN's default on all platforms.

RESTRICTION BYPASS

NordWhisper

−20%

20% more efficient than OpenVPN. Designed specifically to operate on restricted networks — corporate Wi-Fi, public hotspots, firewalls — where NordLynx may be blocked. More overhead than NordLynx but a clear step forward from legacy alternatives.

LEGACY · REFERENCE POINT

OpenVPN UDP

Baseline

Used here as the benchmark reference. Carries the highest battery overhead of the three due to its larger and more complex code base — more than 70,000 lines versus WireGuard's 4,000. Still available for specific use cases but not recommended as the default.

PROTOCOL DATA — MEAN OF 3 RUNS PER PROTOCOL (ANDROID)

Protocol	Active 30 min	Idle 30 min	Session total	CPU % (active)	mAh/GB	vs. OpenVPN
OpenVPN UDP	167	100	**267**	14.8%	26.7	Reference
NordWhisper	134	80	**214**	8.7%	21.4	**−20%**
NordLynx	112	72	**184**	6.2%	18.4	**−31%**

All figures in mAh (session columns) and % (CPU). Mean across 3 runs, 10 Mbps controlled download. CPU% not available on iOS due to platform sandboxing restrictions.

PROTOCOL DATA — MEAN OF 3 RUNS PER PROTOCOL (IOS)

Protocol	Active 30 min	Idle 30 min	Session total	mAh/GB	vs. OpenVPN
OpenVPN UDP	158	93	**251**	25.1	Reference
NordWhisper	136	82	**218**	21.8	**−13%**
NordLynx	118	73	**191**	19.1	**−24%**

All figures in mAh (session columns). Mean across 3 runs, 10 Mbps controlled download. iOS figures are higher than Android across all protocols due to Apple's Network Extension framework adding a processing layer. Full per-run data in Appendix C.

WHY THE GAP EXISTS

The efficiency difference is not a matter of marketing — it reflects a fundamental difference in architecture. Every data packet that passes through a VPN tunnel is encrypted and decrypted. Older protocols like OpenVPN require substantially more CPU cycles per packet, which means more power consumed per megabyte of data. WireGuard-based protocols like NordLynx use modern cryptographic algorithms that are faster and require less processing.

In the active data transfer phase of this test, NordLynx kept CPU usage at around 6% on Android. OpenVPN required more than double that. During idle connection time, the gap was even wider: NordLynx's keep-alive signals are sent only when necessary, whereas OpenVPN maintains a persistent signalling schedule regardless of activity.

The practical implication is that battery drain figures associated with VPN applications are frequently based on experience with older protocols or older versions of VPN software. The technology has advanced considerably.

> The 31% efficiency gain applies to Android, where NordLynx runs at the kernel level — as close to the hardware as a protocol can operate on Android. On iOS, all VPN protocols must run through Apple's Network Extension framework, which adds a small processing layer outside the application's control. This reduces the efficiency gap to 24% on iOS — still substantial, and consistent across all three iOS devices tested.

TEST SERIES 4 — 24-HOUR AVERAGE USER SIMULATION

Claim: Leaving a VPN on all day has a noticeable impact on battery life. Is there a meaningful daily cost to running NordVPN continuously?

> No — not in any meaningful sense. Running NordVPN continuously for 24 hours added 1.4% to daily battery use on Android and 1.8% on iOS. This is the equivalent of needing to charge your phone roughly half a day earlier each month — a difference that falls well within everyday battery variation.

This is the primary test in the evaluation. Rather than isolating one activity, it runs a scripted simulation of a complete working day — with the application both active and inactive — so that any battery difference can be attributed directly to the VPN being on. All runs used Wi-Fi as the primary connection, with network transitions during commute phases, reflecting typical usage conditions for a user in an urban environment.

The same 24-hour usage profile was run six times per platform on the application's default protocol, NordLynx: three times with NordVPN active and three times without. Secondary runs were also completed for NordWhisper (Android) and OpenVPN (iOS), both of which also passed. Users who spend a greater proportion of their day on mobile data may observe figures at the higher end of the confidence range. Per-device results for all six devices are provided in Appendix A.

HOW BATTERY OVERHEAD IS DISTRIBUTED ACROSS THE DAY

SLEEP	COMMUTE	WORK	COMMUTE	HOME	SLEEP
00:00–08:00	08:00–09:00	09:00–17:00	17:00–18:00	18:00–22:00	22:00–00:00
<1%	~3%	~1%	~3%	~0%	<1%

VPN overhead per phase expressed as additional battery consumed above the equivalent VPN-off period, Android, NordLynx. The commute phases carry the highest overhead because of network transitions (see Series 2). The Home phase (~0%) may appear to contradict the streaming overhead shown in Series 1 — it does not. Series 1 measured VPN overhead during continuous streaming; the Home phase in this simulation included a mix of streaming, browsing and idle time on a stable Wi-Fi connection, where VPN overhead during streaming is real but small enough that across the full four-hour block it rounds to near zero. The Sleep phases show <1% reflecting keep-alive signals on an otherwise idle connection.

DAILY IMPACT — HEADLINE FIGURES

Android NORDLYNX · 3 PAIRED 24-HOUR RUNS

1.4%

additional daily battery use with VPN active continuously

95% confidence range: 1.1% – 1.7%

Consistent across all three paired runs. On a flagship Android device, this translates to approximately half a day's extra charge needed per month. Within the normal margin of day-to-day battery variation caused by ambient temperature, signal strength and app behaviour.

iOS NORDLYNX · 3 PAIRED 24-HOUR RUNS

1.8%

additional daily battery use with VPN active continuously

95% confidence range: 1.5% – 2.1%

Marginally higher than Android, for the same architectural reason identified in Series 3: Apple's Network Extension layer adds a small, consistent overhead. Consistent across all three paired runs. Imperceptible in everyday use.

† Samsung Galaxy S24 (device A1) was fitted with a replacement OEM-equivalent battery at 100% health prior to testing. Results are representative of a new unit. No impact on outcomes.

All results — four test series

1.4%
All-day impact — Android
NordLynx, 24-hour test, 3 paired runs
Pass — Series 4

1.8%
All-day impact — iOS
NordLynx, 24-hour test, 3 paired runs
Pass — Series 4

~2%
Streaming overhead
VPN on vs. off, Android & iOS
Pass — Series 1

<0.5%
Idle keep-alive overhead per hour
Screen off, VPN connected, both platforms
Pass — Series 1

<10%
Overhead per network transition
All protocols, both platforms — commuter simulation
Pass — Series 2

−31%
NordLynx vs. OpenVPN efficiency — Android
Battery per unit of data. iOS: −24%
Pass — Series 3

99%+
VPN reconnect success rate
NordLynx after network transitions, both platforms
Pass — Series 2

~49%
OS over-attribution — Android & iOS
Recorded results show an average of 49% of session attributed to VPN across all devices; WCL measured under 2% actual. See Appendix D.
Finding — Series 1

DEVICES USED

Device	Platform
Samsung Galaxy S24 †	Android
Samsung Galaxy S25 Ultra	Android
Google Pixel 9	Android
iPhone 15	iOS
iPhone 16	iOS
iPad (latest generation)	iPadOS

† Galaxy S24 fitted with a replacement OEM-equivalent battery at 100% health. No impact on outcomes.

DOCUMENT HISTORY

Version	Change
1.0 – 2.4	Content updates
2.5	**Final version**

Date: May 2026

WEST COAST LABS — INDEPENDENT EVALUATION CONCLUSION

Across all four test series, NordVPN demonstrated no significant impact on battery life on Android or iOS. All tests passed. In everyday use, the difference is imperceptible.

Appendix A — Per-Device Results: Series 1 & Series 4

All six devices tested individually. Series 1 figures are single-run per scenario per device. Series 4 figures are means across 3 paired runs per device. All Series 1 runs: 60 minutes, 1080p YouTube, screen off, Wi-Fi.

SERIES 1 — STREAMING OVERHEAD PER DEVICE (SCENARIO B VS SCENARIO A)

Device	Platform	VPN Off (baseline)	NordLynx On	VPN overhead	OS reported %	OS share of session
Samsung Galaxy S24 †	Android	312	318	1.9%	44.6%	41%
Samsung Galaxy S25 Ultra	Android	318	323	1.6%	43.2%	41%
Google Pixel 9	Android	307	312	1.6%	42.8%	39%
iPhone 15	iOS	271	277	2.2%	63.8%	59%
iPhone 16	iOS	268	274	2.2%	62.4%	58%
iPad (latest)	iPadOS	412	420	1.9%	61.1%	55%

All overhead figures expressed as %/hr of device battery capacity — the additional battery consumed per hour compared to the same activity without VPN. Overhead is proportional to duration: 2 hours of streaming produces approximately 2× the overhead shown.

Over-attribution % = (OS-reported VPN mAh − WCL-measured delta) ÷ WCL-measured delta × 100. iOS "OS reported %" refers to share shown on battery settings screen; over-attribution calculated against WCL current-trace delta. Note iOS figures are higher than Android — this reflects the NEPacketTunnelProvider architecture routing all traffic through the VPN process. Baseline and NordLynx On figures are raw mAh consumed during the 60-minute scenario.

SERIES 4 — 24-HOUR DAILY IMPACT PER DEVICE (NORDLYNX, MEAN OF 3 PAIRED RUNS)

Device	Battery cap.	VPN Off mean	NordLynx mean	Delta	Daily impact %	95% CI	Pass
Samsung Galaxy S24 †	4,000	1,354	1,410	56	**1.4%**	1.1–1.7%	✓
Samsung Galaxy S25 Ultra	5,000	1,694	1,764	70	**1.4%**	1.1–1.7%	✓
Google Pixel 9	4,700	1,596	1,662	66	**1.4%**	1.1–1.7%	✓
iPhone 15	3,349	1,231	1,291	60	**1.8%**	1.5–2.1%	✓
iPhone 16	3,561	1,308	1,372	64	**1.8%**	1.5–2.1%	✓
iPad (latest)	7,500	2,747	2,882	135	**1.8%**	1.5–2.1%	✓

Battery capacities in mAh (rated). VPN Off and NordLynx means are mAh consumed across 24-hour run. Delta = NordLynx − VPN Off. Daily impact % = delta ÷ battery capacity × 100. 95% CI calculated using t-distribution, df=2, t=4.303. † S24 replacement battery (OEM-equivalent, 100% health).

Appendix B — Series 2: Raw Run-Level Data (Commuter Simulation)

Five runs per protocol per platform. 120-minute commuter simulation: ~14 automated Wi-Fi↔cellular transitions per run, background audio throughout, 20% screen brightness. Figures are total session mAh per run. Overhead % = (protocol run − VPN-off mean) ÷ VPN-off mean × 100.

ANDROID — TC-NT-001

Protocol	Run 1	Run 2	Run 3	Run 4	Run 5	Mean	SD	Overhead	Reconn. %	Pass
VPN Off (baseline)	621	614	618	622	615	**618**	±18	—	—	Baseline
NordLynx	652	645	651	648	649	**649**	±14	+5.1%	99.4%	✓
NordWhisper	650	644	649	646	651	**648**	±13	+4.8%	99.7%	✓
OpenVPN UDP	675	668	673	671	673	**672**	±21	+8.7%	99.1%	✓

IOS — TC-NT-002

Protocol	Run 1	Run 2	Run 3	Run 4	Run 5	Mean	SD	Overhead	Reconn. %	NE kills	Pass
VPN Off (baseline)	543	537	542	544	539	**541**	±22	—	—	—	Baseline
NordLynx	580	574	579	577	580	**578**	±19	+6.8%	98.8%	2	✓
NordWhisper	583	577	581	579	580	**580**	±17	+7.2%	98.6%	2	✓
OpenVPN UDP	596	589	593	591	591	**592**	±24	+9.4%	98.1%	3	✓

All figures in mAh. Overhead % calculated against VPN-off mean. Reconnect % = successful reconnections ÷ total transition events. NE kills = iOS Network Extension process terminations by the OS (platform behaviour, outside NordVPN control) — excluded from reconnect rate calculation per specification. Pass threshold: <15% overhead per transition event and ≥98% reconnect success.

Appendix C — Series 3: Full Protocol Benchmark Data (3 Runs Per Protocol)

Each run: 60-second tunnel stabilisation, 30 minutes active iperf3 download at 10 Mbps, 30 minutes idle keep-alive. Same server region throughout. Primary metric: mAh per GB transferred (mAh/GB). All figures from individual runs — mean shown separately.

ANDROID — TC-PS-001 (SAMSUNG GALAXY S24 REPRESENTATIVE DEVICE)

Protocol	Run	Active (mAh)	Idle (mAh)	Session total	Peak mA	CPU %	Throughput	mAh/GB
OpenVPN UDP	1	167	100	267	498	14.8%	9.6 Mbps	26.7
	2	165	99	264	495	14.6%	9.7 Mbps	26.4
	3	169	101	270	501	15.1%	9.5 Mbps	27.1
	Mean	**167**	**100**	**267 ±9**	**498**	**14.8%**	**9.6**	**26.7**
NordLynx	1	112	72	184	331	6.2%	10.0 Mbps	18.4
	2	111	71	182	328	6.1%	10.1 Mbps	18.2
	3	113	73	186	334	6.3%	9.9 Mbps	18.6
	Mean	**112**	**72**	**184 ±6**	**331**	**6.2%**	**10.0**	**18.4 (−31%)**
NordWhisper	1	134	80	214	362	8.7%	9.8 Mbps	21.4
	2	133	79	212	359	8.6%	9.9 Mbps	21.2
	3	135	81	216	365	8.8%	9.7 Mbps	21.6
	Mean	**134**	**80**	**214 ±7**	**362**	**8.7%**	**9.8**	**21.4 (−20%)**

Reduction % vs OpenVPN based on session total means. iOS per-device figures mirror this pattern — mean values: NordLynx 19.1 mAh/GB (−24% vs OpenVPN 25.1 mAh/GB).

Appendix D — System-Level Monitoring Data: OS Attribution

This appendix documents the raw OS battery attribution data captured immediately after each Series 1 scenario run. This data is the basis for the over-attribution finding presented in the main body of the report. Android data is extracted from `dumpsys batterystats`; iOS data is from the battery settings screen and Instruments Energy Log.

ANDROID — DUMPSYS BATTERYSTATS: NORDVPN UID ATTRIBUTION (SCENARIO B, NORDLYNX ACTIVE)

Device	WCL measured mAh (actual)	OS-attributed mAh (dumpsys)	OS share of session	OS share of session
Samsung Galaxy S24 †	6.0 (delta vs baseline)	143	44.6% of session	41% above actual
Samsung Galaxy S25 Ultra	5.0	139	43.2% of session	41% above actual
Google Pixel 9	4.9	132	42.8% of session	39% above actual

IOS — NEPACKETTUNNELPROVIDER ATTRIBUTION (SCENARIO B, NORDLYNX ACTIVE)

Device	WCL measured mAh (actual)	iOS battery screen share	iOS listed as primary consumer	OS share of session
iPhone 15	6.0	63.8%	Yes	59% above actual
iPhone 16	6.0	62.4%	Yes	58% above actual
iPad (latest)	8.0	61.1%	Yes	55% above actual

IOS ATTRIBUTION MECHANISM

On iOS, all VPN connections run through Apple's `NEPacketTunnelProvider` framework. iOS assigns all network-related energy consumption to this process — and therefore to the VPN application that hosts it — regardless of which app generated the traffic. The battery settings screen (Settings → Battery → Battery Usage by App) consistently shows NordVPN consuming 60–64% of session battery during streaming, while WCL Instruments Energy Log traces show the NordVPN process contributing under 2% of total device current draw. The iOS battery screen figure cannot be used as a reliable indicator of VPN energy cost for any application using the NEPacketTunnelProvider architecture.

WCL measured mAh (delta) = mAh consumed with NordLynx active minus mAh consumed with VPN off, from current-trace CSV. OS-attributed figures are from dumpsys batterystats (Android, captured within 60 seconds of run end) and iOS battery settings screen (captured immediately after run, prior to device charge). Over-attribution % = (OS attributed − WCL delta) ÷ WCL delta × 100. All captures are from Scenario B (60-minute 1080p YouTube streaming, screen off, Wi-Fi).

Disclaimer

While West Coast Labs is dedicated to ensuring the highest standard of security product testing in the industry, it is never possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and/or functionality of any particular product tested and/or guarantee that any particular product tested is fit for any given purpose. Therefore, the test results published within any given report should not be taken and accepted in isolation.

Potential customers interested in deploying any particular product tested by West Coast Labs should seek further confirmation that the said product will meet their individual requirements, technical infrastructure and specific security considerations. All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability.

West Coast Labs provide test results for any particular product tested, most relevant at the time of testing and within the specified scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools used during the specific test process.

Terms & Conditions

This report is provided by West Coast Labs ("the Company") and is subject to the following terms and conditions. By accessing or using this document, you agree to be bound by these terms:

1. Proprietary Information
This report contains proprietary testing data, methodologies, and analysis that are the exclusive property of West Coast Labs. All content, including test results, graphics, charts, and written analysis, is protected by copyright and other intellectual property laws.

2. Prohibition on Distribution
This document may not be copied, reproduced, shared, distributed, published, or transmitted in any form or by any means without the express prior written consent of West Coast Labs. This includes posting on websites, sharing via email, uploading to cloud storage, or distribution through social media platforms.

3. Authorised Use Only
This report is provided solely for the use of the intended recipient(s) and may only be used for internal evaluation purposes. Any commercial use, resale, or incorporation of this report or its contents into other materials is strictly prohibited without written authorisation from West Coast Labs.

4. Limited Licence
Receipt of this document does not grant any licence or rights to the recipient beyond the right to review the contents for personal or internal business evaluation. No rights are granted to reproduce, modify, adapt, or create derivative works based on this report.

5. No Warranties
While West Coast Labs has made reasonable efforts to ensure the accuracy of the information contained in this report, the Company makes no warranties or representations, express or implied, regarding the completeness, accuracy, reliability, or fitness for a particular purpose of the information provided.

6. Limitation of Liability
West Coast Labs shall not be liable for any damages, including but not limited to direct, indirect, incidental, consequential, or punitive damages, arising from the use or inability to use this report or reliance on its contents.

7. Return or Destruction
Upon request by West Coast Labs, the recipient agrees to promptly return or securely destroy all copies of this document, including any electronic copies, and certify such destruction in writing.

8. Breach and Enforcement
Any unauthorised use, reproduction, or distribution of this report constitutes a material breach of these terms and may result in immediate legal action, including seeking injunctive relief and monetary damages.

West Coast Labs
Security Product Testing & Certification

Version 2.5 — May 2026