WESTCOAST labs

Comprehensive VPN Testing Report 2025

Complete Performance & Security Analysis

5	6
VPN PROVIDERS	TEST CATEGORIES
1,250+	**7**
INDIVIDUAL TESTS	LOCATIONS

October 2025

NordVPN • ExpressVPN • Proton VPN • Mullvad VPN • Norton VPN

Executive Overview

This comprehensive report presents the results of extensive testing conducted across five leading VPN providers in October 2025. Our analysis encompasses six critical dimensions of VPN performance: **security leak protection**, **connection speed**, **website accessibility**, **core functionality**, **time to connect**, and **system resource impact**.

Testing was conducted from WCL premises in both the **United Kingdom and United States** and in numerous remote locations, each on a **1 Gbps fiber connection** using both **Windows 11 Pro** and **macOS Sonoma** platforms. Each VPN was evaluated across multiple scenarios including static connections, dynamic network transitions, and sustained usage patterns to simulate real-world conditions.

Testing Scope

- ✓ 5 VPN providers evaluated
- ✓ 7 geographic origins
- ✓ 588 speed measurements
- ✓ 8 leak test scenarios
- ✓ 2 operating systems tested
- ✓ 455+ network transitions
- ✓ 250+ website access tests
- ✓ System impact monitoring

The VPN providers tested include **NordVPN**, **ExpressVPN**, **Proton VPN**, **Mullvad VPN**, and **Norton VPN**. Each provider was tested using their fastest available protocol and default security settings to represent typical user experience.

Table of Contents

Executive Summary

Testing Overview

VPNs Tested	Test Categories	Total Tests
5	**6**	**500+**

Overall Performance Summary

OVERALL TESTING WINNER

NordVPN

Category Wins: Leak (Tied), Speed, Website Accessibility (Tied), Functionality (Tied), Time to Connect • **Score:** 58/60

Category Winners Summary

Test Category	Winner	Runner-Up
Speed Testing	NordVPN (817Mbps)	ExpressVPN (788Mbps)
System Impact	ExpressVPN (+0.56% CPU)	NordVPN (+0.64% CPU)
Data Leak Protection	NordVPN / ExpressVPN / ProtonVPN / Mullvad / Norton VPN	—
Functionality	NordVPN / ExpressVPN / ProtonVPN / Mullvad / Norton VPN	---
Website Accessibility	NordVPN / ExpressVPN / Proton VPN	Mullvad
Time to Connect	NordVPN (0.66s)	ProtonVPN (1.62s)

Key Findings

Performance Leaders: NordVPN finished top, or joint top, in five out of six categories. ExpressVPN excelled in system efficiency.

Security Excellence: All tested solutions demonstrated strong security functionality and leak prevention.

Speed Retention: Top performers maintained over 90% of baseline speeds with minimal encryption overhead, with NordVPN showing a retention rate of over 95% on average.

WESTCOAST labs

VPN Security Leak Test Report 2025

Comprehensive Protection Analysis

5	8
VPN PROVIDERS	TEST CATEGORIES
455	**99.8%**
NETWORK TRANSITIONS	SUCCESS RATE

Testing Period: October, 2025

United Kingdom | Lab Network | 8 leak scenarios + dynamic network switching

Executive Summary

🏆 **KEY FINDING:** Four VPN providers achieved perfect scores across all leak tests: NordVPN, Proton VPN, Mullvad VPN, and Norton VPN passed all static leak tests (DNS, IP, WebRTC, IPv6) and maintained protection during 455 network transitions with zero leaks. ExpressVPN showed one minor DNS configuration change during network switching but maintained IP protection throughout all tests.

Overall Security Scores

✓ Perfect (100%) ! Excellent (99.7%)

NordVPN
8/8
62 transitions, 0 leaks
PERFECT

Proton VPN
8/8
77 transitions, 0 leaks
PERFECT

Mullvad VPN
8/8
128 transitions, 0 leaks
PERFECT

Norton VPN
8/8
93 transitions, 0 leaks
PERFECT

ExpressVPN
8/8
33 transitions, 1 DNS event
EXCELLENT

Static Leak Test Results

VPN Provider	DNS Leak	IP Leak	WebRTC Leak	IPv6 Leak	Overall
NordVPN	PASS	PASS	PASS	PASS	PERFECT
ExpressVPN	PASS	PASS	PASS	PASS	PERFECT
Proton VPN	PASS	PASS	PASS	PASS	PERFECT
Mullvad VPN	PASS	PASS	PASS	PASS	PERFECT
Norton VPN	PASS	PASS	PASS	PASS	PERFECT

Network Transition Test Results

VPN Provider	Total Transitions	Warnings	Success Rate	Status
Mullvad VPN	**128**	**0**	100.0%	PERFECT
Norton VPN	**93**	**0**	100.0%	PERFECT
Proton VPN	**77**	**0**	100.0%	PERFECT
NordVPN	**62**	**0**	100.0%	PERFECT
ExpressVPN	**33**	**1 (DNS Event Noted)**	99.7%	EXCELLENT

EXPRESSVPN DNS CONFIGURATION EVENT: One DNS configuration change was detected at 19:48:41 during network transition (Severity: Medium). The public IP remained protected, and the DNS server briefly changed before returning to expected configuration. This represents a minor configuration adjustment rather than a security leak, as no real ISP information was exposed.

🎯 Key Statistics

PERFECT SCORES	TOTAL TRANSITIONS	OVERALL SUCCESS
4	**455**	**99.8%**
83% of providers	Zero IP leaks	1 minor DNS event

Test Categories 1-5: Static Leak Protection

Category 1: DNS Leak Protection
Verifies DNS queries route through VPN tunnel. All tested providers passed with 2 configured DNS servers per VPN.

Category 2: IP Leak Protection
Detects real ISP IP exposure [redacted] using 3 services. All tested providers passed with zero ISP IP exposure.

Category 3: WebRTC Leak Protection
Browser-based IP exposure via WebRTC APIs. All tested providers passed with zero public IPs detected.

Category 4: IPv6 Leak Protection
IPv6 traffic bypass detection. All tested providers passed. IPv6 enabled but inactive during all tests.

Category 5: Network Interface Analysis
Multiple default routes and adapter conflicts. All tested providers passed with proper adapter control.

Test Categories 6-8: Network Transition Protection

TEST DESCRIPTION: Dynamic testing during WiFi network switching simulates real-world scenarios where users move between networks. VPNs must maintain protection during these transitions without exposing real IP or DNS information.

💡 **NETWORK TRANSITION INSIGHT:** All VPNs demonstrated robust kill switch functionality and reconnection handling. The single DNS configuration event in ExpressVPN represents a brief DNS server preference change rather than a true leak, as the public IP remained protected throughout. This level of protection during 455 network transitions demonstrates mature VPN implementations across all tested providers.

💡 Key Findings

- **Universal DNS Protection:** All tested providers successfully prevented DNS leaks - this is now an industry standard
- **Perfect IP Protection:** Zero real IP exposures detected across 455 network transitions and all static tests
- **WebRTC Security:** All providers properly blocked WebRTC leaks, preventing browser-based IP exposure
- **IPv6 Handling:** All providers correctly disabled IPv6 traffic during VPN connection
- **Network Transition Excellence:** 99.8% success rate across 455 network transitions demonstrates mature kill switch and reconnection implementations
- **ExpressVPN DNS Event:** Single DNS configuration change during network transition was minor and did not expose real ISP information

📊 Security Tier Classification

TIER 1: PERFECT	TIER 2: EXCELLENT	OVERALL SUCCESS
4	**1**	**99.8%**
100% protection	99.7% protection	1 minor event

Tier 1: Perfect Security (100%)

NordVPN, Proton VPN, Mullvad VPN, Norton VPN - Zero leaks across all test categories. Suitable for users with maximum privacy requirements including journalists, activists, corporate users, and anyone requiring guaranteed protection during network transitions.

Tier 2: Excellent Security (99.7%)

ExpressVPN - Single minor DNS configuration event during network transition with no IP exposure. Excellent for general privacy needs, streaming, browsing, and everyday VPN usage. The 99.7% success rate exceeds requirements for typical consumer use cases.

🔬 Testing Methodology

Test Environment: Windows 11 Pro | United Kingdom | **ISP:** OpenReach | **Baseline IP:** Recorded | **Test Date:** October, 2025 | **Static Tests:** DNS Leak (2 servers per VPN), IP Leak (3 independent services: ipleak.net, ipinfo.io, ifconfig.me), WebRTC Leak (API-based via ipleak.net with private IP filtering), IPv6 Leak (system enabled, traffic monitored), Network Interface Analysis (adapter configuration verification) | **Dynamic Tests:** Network transition monitoring during WiFi switching with 10-second measurement intervals | **Measurements:** Public IP address, DNS server configuration, VPN adapter status, IPv6 activity, leak detection flags | **Total Tests:** 455 network transitions + 6 comprehensive static test suites = 461 total test scenarios | **Validation:** All tests used baseline real IP (Private) for comparison, filtered private IPs from WebRTC results, verified consistency across multiple detection services

CONCLUSION: Comprehensive leak testing reveals exceptional security standards across all five tested VPN providers. Four providers (NordVPN, Proton VPN, Mullvad VPN, Norton VPN) achieved perfect scores with zero leaks across network transitions and all static test categories. ExpressVPN demonstrated excellent protection with a 99.7% success rate, showing only one minor DNS configuration event that did not expose the real ISP IP address. The 99.8% overall success rate across 455 network transitions confirms that modern VPN implementations have matured significantly, with robust kill switches, proper DNS handling, WebRTC protection, and IPv6 leak prevention now standard features. Users can confidently select any of these providers knowing their real IP address and DNS information will remain protected during both static connections and dynamic network transitions.

WESTCOAST labs

VPN Speed Test Report 2025

Global Performance Analysis Across 7 Origins

5	7
VPN PROVIDERS	ORIGIN COUNTRIES
2	**588**
PLATFORMS	SPEED TESTS

Testing Period: October 2025

Baseline: 1 Gbps fiber | Windows & macOS | 7 destination regions per origin

📊 Executive Summary

🏆 **KEY FINDING:** NordVPN leads with an average speed of 817 Mbps across all tested routes and platforms, followed closely by ExpressVPN (788 Mbps). NordVPN's NordLynx protocol demonstrates superior performance consistency across both short-distance European routes and long-haul connections to Asia-Pacific regions.

🥇 Overall Performance Rankings

💻 Platform Performance Comparison

VPN Provider	Windows Avg	macOS Avg	Difference	Notes
NordVPN	**822 Mbps**	**811 Mbps**	+1.4%	Excellent parity
ExpressVPN	**790 Mbps**	**787 Mbps**	+0.3%	Perfect parity
Proton VPN	**762 Mbps**	**755 Mbps**	+0.9%	Excellent parity
Mullvad VPN	**743 Mbps**	**734 Mbps**	+1.2%	Excellent parity
Norton VPN	**734 Mbps**	**717 Mbps**	+2.4%	Good parity

🎯 Key Statistics

FASTEST OVERALL

NordVPN

817 Mbps average

BEST PLATFORM PARITY

ExpressVPN

+0.3% difference

SPEED RETENTION

87%

Average vs 1 Gbps

🌎 Performance by Origin Region (Windows)

VPN Provider	UK	France	Germany	Netherlands	Singapore	Sydney	California
NordVPN	**837**	**838**	**843**	**849**	**811**	**769**	**806**
ExpressVPN	**819**	**813**	**814**	**819**	**784**	**766**	**715**
Proton VPN	**772**	**797**	**823**	**820**	**747**	**690**	**687**
Mullvad VPN	**802**	**780**	**789**	**796**	**666**	**610**	**720**
Norton VPN	**792**	**771**	**780**	**787**	**658**	**603**	**711**

📈 Regional Performance Insights

EUROPEAN ORIGINS (UK, France, Germany, Netherlands):
All VPNs perform best from European origins due to proximity to server infrastructure and optimized routing. NordVPN averages 842 Mbps across European origins, maintaining speeds above 800 Mbps consistently. Netherlands shows the highest speeds overall due to excellent internet infrastructure.

ASIA-PACIFIC ORIGINS (Singapore, Sydney):
Performance remains strong but shows natural degradation due to distance. NordVPN maintains 790 Mbps average from Asia-Pacific origins. Singapore (811 Mbps) outperforms Sydney (769 Mbps) due to Singapore's role as a major internet hub with better connectivity to global backbone networks.

NORTH AMERICA ORIGIN (California):
California shows varied performance depending on destination. NordVPN achieves 806 Mbps average, demonstrating strong transpacific connectivity. Long-distance routes to Europe naturally show slightly reduced speeds compared to local or regional connections.

🔬 Protocol Performance Analysis

Protocol	VPN Provider	Avg Speed	Performance Rating
NordLynx	NordVPN	**817 Mbps**	Excellent
Lightway	ExpressVPN	**788 Mbps**	Excellent
WireGuard	Proton VPN	**758 Mbps**	Very Good
WireGuard	Mullvad VPN	**739 Mbps**	Good
Mixed (Win/Mac)	Norton VPN	**725 Mbps**	Good

💡 **PROTOCOL INSIGHT:** Modern protocols (NordLynx, WireGuard, Lightway) vastly outperform legacy OpenVPN. NordLynx (NordVPN's enhanced WireGuard implementation) shows marginal improvements over standard WireGuard implementations, averaging 25 Mbps faster than other WireGuard-based VPNs.

💡 Key Findings

- **NordVPN leads performance:** 817 Mbps average across 588 tests demonstrates consistent superiority in both short and long-distance connections
- **Top tier clustering:** NordVPN and ExpressVPN form a clear top tier (788-817 Mbps) with minimal performance differences
- **Protocol matters:** Modern protocols (NordLynx, WireGuard, Lightway) deliver 60-100% faster speeds than OpenVPN
- **Platform consistency:** Four of five tested providers maintain excellent cross-platform parity (±1.4%), enabling seamless multi-device usage
- **European advantage:** All VPNs perform best from European origins (average 15% faster) due to infrastructure density and optimized routing
- **Distance degradation:** Long-haul Asia-Pacific routes show natural 10-15% speed reduction compared to regional connections

📊 Speed Tiers Summary

TIER 1: PREMIUM
2
788-817 Mbps

TIER 2: EXCELLENT
1
758 Mbps

TIER 3: GOOD
2
515-634 Mbps

Tier 1: Premium Speed (788-817 Mbps)

NordVPN, ExpressVPN - Ideal for bandwidth-intensive activities including 4K/8K streaming, large file transfers, video conferencing, and cloud gaming. Minimal impact on connection speeds.

Tier 2: Excellent Speed (758 Mbps)

Proton VPN - More than sufficient for all typical use cases including HD/4K streaming, video calls, and general browsing. Slightly slower than premium tier but difference is imperceptible in real-world usage.

Tier 3: Good Speed (725-739 Mbps)

Mullvad VPN, Norton VPN - Adequate for standard internet usage, HD streaming, and web browsing. May show noticeable slowdown during bandwidth-intensive tasks on slower baseline connections. Norton on macOS requires attention due to protocol limitations.

🔬 Testing Methodology

Test Environment: 1 Gbps fiber baseline (actual speeds 720-950 Mbps depending on distance) | **Platforms:** Windows 11 Pro and macOS Sonoma | **Origins:** 7 countries (UK, France, Germany, Netherlands, Singapore, Sydney, California) | **Destinations:** 7 regions per origin (local, Europe, US, Asia-Pacific) | **Tests per VPN:** 98 measurements (7 origins × 7 destinations × 2 platforms) | **Total Tests:** 588 measurements | **Protocols:** Each VPN tested with its fastest protocol (NordLynx, Lightway, WireGuard) | **Measurement:** Download speeds only, averaged over multiple runs | **Validation:** Tests repeated across multiple days to account for network variations

CONCLUSION: Speed testing reveals clear performance tiers among VPN providers. NordVPN and ExpressVPN establish a premium tier delivering 788-817 Mbps with negligible impact on connection speeds. Modern protocols (NordLynx, WireGuard, Lightway) have matured to provide excellent performance across various geographic routes. Platform consistency is strong across four providers, though Norton VPN's macOS implementation requires attention. Users prioritizing maximum speed should choose from the premium tier, while Proton VPN offers excellent value for typical use cases. The significant performance gap between modern protocols and OpenVPN underscores the importance of protocol selection in VPN performance.

Network Latency Analysis

Understanding latency impact is critical for real-time applications. While download speed determines how fast data transfers, latency (ping time) measures how quickly your connection responds. Low latency is essential for online gaming, video conferencing, VoIP calls, and day trading where every millisecond matters.

PROTOCOL IMPACT
8x Difference
WireGuard vs OpenVPN

MODERN PROTOCOL OVERHEAD
3-4ms
Across all distances

LEGACY PROTOCOL PENALTY
+25ms
OpenVPN overhead

Latency Rankings by VPN Provider

Rank	VPN Provider	Protocol	Latency Overhead	Rating
1st	NordVPN	NordLynx	**+3ms**	**Excellent**
1st	Mullvad VPN	WireGuard	**+3ms**	**Excellent**
2nd	ExpressVPN	Lightway	**+4ms**	**Excellent**
2nd	Proton VPN	WireGuard	**+4ms**	**Excellent**
3rd	Norton VPN (Windows)	OpenVPN	**+8ms**	**Good**

Average Latency Results by Destination Type (Across All Origins)

The following shows average latency in milliseconds for different destination categories, averaged across all 7 origin countries tested.

Provider	Local / Same Region	Nearby Europe	Trans-Atlantic	Asia-Pacific	Overall Average
No VPN (Baseline)	**3ms**	**16ms**	**141ms**	**231ms**	**98ms**
NordVPN	**6ms**	**19ms**	**144ms**	**234ms**	**101ms**
ExpressVPN	**7ms**	**21ms**	**147ms**	**237ms**	**103ms**
Proton VPN	**7ms**	**20ms**	**146ms**	**236ms**	**102ms**
Mullvad VPN	**6ms**	**19ms**	**159ms**	**236ms**	**105ms**
Norton VPN (Windows)	**9ms**	**23ms**	**166ms**	**243ms**	**110ms**

Note: Local/Same Region = connections within 500km | Nearby Europe = connections 500-1500km | Trans-Atlantic = USA-Europe routes | Asia-Pacific = Singapore/Sydney routes from Europe/USA

💡 **LATENCY INSIGHT:** Modern WireGuard-based protocols (NordLynx, standard WireGuard) add only 3ms overhead to base connection latency, making them virtually imperceptible even for competitive gaming. In contrast, OpenVPN adds 25ms - a difference that's immediately noticeable in fast-paced games and real-time applications.

WESTCOAST labs

VPN Website Accessibility Report 2025

Comprehensive Testing of 5 Leading VPN Services Across 100 Popular Websites

100	5
WEBSITES TESTED	VPN SERVICES
100%	**2-6**
CONNECTIVITY SUCCESS	CAPTCHA CHALLENGES

West Coast Labs | Testing Date: October, 2025
Independent VPN Performance Analysis

Executive Summary

- **Perfect connectivity across all VPNs:** All tested VPN services achieved 100% website connectivity - every site was accessible, with no complete blocks
- **Three VPNs tied for best user experience:** NordVPN, ExpressVPN, and Proton VPN encountered only 2 CAPTCHA challenges each across 100 websites
- **CAPTCHA frequency is the key differentiator:** The only difference between services was how often users encountered CAPTCHA verification challenges
- **Booking.com triggered CAPTCHAs universally:** All tested VPN services (100%) encountered CAPTCHA challenges on Booking.com
- **Indeed.com highly sensitive to VPN traffic:** Most tested VPN services (80%) triggered CAPTCHAs on Indeed.com
- **Norton VPN experienced moderate friction:** 6 CAPTCHA challenges on sites including Quora, Indeed, ChatGPT, Booking.com, Namu.wiki, and Weather.com

Overall Performance Rankings

1	NordVPN	**100% Connectivity**	2 CAPTCHA Challenges
1	ExpressVPN	**100% Connectivity**	2 CAPTCHA Challenges
1	Proton VPN	**100% Connectivity**	2 CAPTCHA Challenges
4	Mullvad VPN	**100% Connectivity**	3 CAPTCHA Challenges
5	Norton VPN	**100% Connectivity**	6 CAPTCHA Challenges

Performance Comparison

CONNECTIVITY RATE

100%

All 5 VPNs

FEWEST CAPTCHAS

2

3 VPNs tied

TOTAL CAPTCHA CHALLENGES

20

Out of 500 tests

Key Insights

Universal Connectivity Achieved: This testing demonstrates excellent performance across all modern VPN services, with 100% website connectivity achieved by all providers. No websites were completely blocked - users could access every site, though some required solving CAPTCHA challenges. The key differentiator is user experience friction, with ExpressVPN, NordVPN, and Proton VPN providing the smoothest experience with only 2 CAPTCHA encounters each across 100 websites.

🔍 Detailed Performance Analysis

VPN Service	Accessible (No CAPTCHA)	CAPTCHA Required	Blocked	Connectivity Rate	User Experience
NordVPN	**98**	2	0	**100%**	EXCELLENT
ExpressVPN	**98**	2	0	**100%**	EXCELLENT
Proton VPN	**98**	2	0	**100%**	EXCELLENT
Mullvad VPN	97	3	0	**100%**	VERY GOOD
Norton VPN	94	6	0	**100%**	GOOD

🔐 CAPTCHA Challenge Websites by VPN Service

VPN Service	CAPTCHA Count	Affected Websites	CAPTCHA Rate
NordVPN	**2**	Indeed, Booking.com	2%
ExpressVPN	**2**	Indeed, Booking.com	2%
Proton VPN	**2**	Booking.com, Weather.com	2%
Mullvad VPN	3	Indeed, Booking.com, Weather.com	3%
Norton VPN	6	Quora, Indeed, ChatGPT, Booking.com, Namu.wiki, Weather.com	6%

🎯 Most Commonly CAPTCHA'd Websites

Booking.com - CAPTCHA triggered by all tested VPNs
Indeed.com - CAPTCHA triggered by 4 VPNs
Weather.com - CAPTCHA triggered by 3 VPNs
Quora.com - CAPTCHA triggered by 1 VPN
ChatGPT.com - CAPTCHA triggered by 1 VPN
Namu.wiki - CAPTCHA triggered by 1 VPN
*These websites were found to display captcha challenges at the time of testing. User experiences may vary.

🔬 Testing Methodology

Test Configuration: 1 Gbps fiber connection (UK) | 20 second timeout | SSL errors ignored | 2 second delay between sites (randomized) | Test Date: October, 2025

VPN Services Tested: ExpressVPN | NordVPN | Proton VPN | Mullvad VPN | Norton VPN

Website Selection: 100 popular websites across Video & Social Media, E-commerce, Tech & Services, Reference & Education, Entertainment, Travel, and Weather categories. Selected based on global popularity, diverse geographic origins, and various security implementations.

Success Metrics: Fully Accessible - Full access without challenges | **CAPTCHA Required -** Site accessible but requires verification | **Blocked -** Access completely denied (none observed)

Testing Protocol: Each website accessed through each VPN service using automated testing tools. Connection status, response codes, and security challenges recorded. All 500 connection attempts (100 sites × 5 VPNs) successfully connected with varying CAPTCHA challenges.

📊 User Experience Summary (Lower CAPTCHA = Better)

🎓 Conclusions

This comprehensive test of leading VPN services across 100 popular websites reveals outstanding connectivity performance, with all services achieving 100% website accessibility. No websites were completely blocked by any VPN service - every site was reachable. The key differentiator between services is user experience friction in the form of CAPTCHA challenges. NordVPN, ExpressVPN, and Proton VPN emerged as joint leaders with only 2 CAPTCHA encounters each (98% friction-free experience). The most frequently CAPTCHA'd site was Booking.com, which challenged all tested VPN services (100%), suggesting robust VPN detection mechanisms on travel booking platforms. Indeed.com also showed high VPN sensitivity, triggering CAPTCHAs on 4 out of 5 tested services (80%). Users should understand that CAPTCHAs represent a minor inconvenience requiring verification, not a complete block. For the smoothest browsing experience, the top three performers offer the best balance of privacy and usability.

WESTCOAST labs

VPN Functionality Test Report 2025

Comprehensive Feature & Reliability Analysis

5	3
VPN SERVICES TESTED	CRITICAL FEATURES
100%	**72**
PASS RATE	TESTS PERFORMED

Testing Period: October 2025

Windows 11 & macOS Sonoma | Multi-scenario validation

📊 Executive Summary

KEY FINDING: All tested VPN providers—NordVPN, ExpressVPN, ProtonVPN, Norton VPN, and Mullvad VPN—achieved perfect scores across all functionality tests. Each provider demonstrated reliable implementation of critical security features including Launch on Boot, Internet Kill Switch, and Split Tunneling capabilities.

🎯 Test Overview

LAUNCH ON BOOT
5/5
All providers passed

KILL SWITCH
5/5
All providers passed

SPLIT TUNNELING
5/5
All providers passed

🏆 Overall Results by Provider

VPN Provider	Launch on Boot	Kill Switch	Split Tunneling	Overall
NordVPN	PASS	PASS	PASS	100%
ExpressVPN	PASS	PASS	PASS	100%
ProtonVPN	PASS	PASS	PASS	100%
Norton VPN	PASS	PASS	PASS	100%
Mullvad VPN	PASS	PASS	PASS	100%

✨ Feature Status Summary

Launch on Boot

NordVPN ALL TESTS PASSED
✓ Fully Functional

ExpressVPN ALL TESTS PASSED
✓ Fully Functional

ProtonVPN ALL TESTS PASSED
✓ Fully Functional

Norton VPN ALL TESTS PASSED
✓ Fully Functional

Mullvad VPN ALL TESTS PASSED
✓ Fully Functional

Internet Kill Switch

NordVPN ALL TESTS PASSED
✓ Fully Functional

ExpressVPN ALL TESTS PASSED
✓ Fully Functional

ProtonVPN ALL TESTS PASSED
✓ Fully Functional

Norton VPN ALL TESTS PASSED
✓ Fully Functional

Mullvad VPN ALL TESTS PASSED
✓ Fully Functional

Split Tunneling

NordVPN ALL TESTS PASSED
✓ Fully Functional

ExpressVPN ALL TESTS PASSED
✓ Fully Functional

ProtonVPN ALL TESTS PASSED
✓ Fully Functional

Norton VPN ALL TESTS PASSED
✓ Fully Functional

Mullvad VPN ALL TESTS PASSED
✓ Fully Functional

Feature 1: Launch on Boot

FUNCTIONALITY OVERVIEW
Launch on Boot functionality provides critical protection during the vulnerable period between system startup and user-initiated VPN activation. This feature ensures that network traffic remains encrypted from the earliest possible moment in the boot sequence, eliminating the window of exposure that exists when users must manually initiate VPN connections.

Test Methodology

Testing examined the complete boot sequence across multiple restart scenarios including cold boots, warm reboots, and unexpected system restarts following power loss or crash conditions. Each scenario required verification that the VPN application loaded correctly, established tunnel connections successfully, and began routing traffic through encrypted channels. Monitoring tools tracked the timing of application launch relative to network interface initialization and measured the delay between OS boot completion and VPN tunnel establishment.

Test Results

VPN Provider	App Launch	Auto Connect	Traffic Routing	Cross-Platform
NordVPN	PASS	PASS	PASS	PASS
ExpressVPN	PASS	PASS	PASS	PASS
ProtonVPN	PASS	PASS	PASS	PASS
Norton VPN	PASS	PASS	PASS	PASS
Mullvad VPN	PASS	PASS	PASS	PASS

KEY FINDINGS: All tested VPN providers demonstrated reliable Launch on Boot functionality across tested scenarios. Each implementation successfully integrates with operating system startup mechanisms without introducing boot delays or compatibility issues. Traffic analysis confirmed that all tested solutions implement appropriate safeguards to prevent unprotected transmission during the brief period required for tunnel establishment.

Feature 2: Internet Kill Switch

FUNCTIONALITY OVERVIEW
The Internet Kill Switch represents a critical failsafe mechanism designed to prevent unprotected data transmission in scenarios where VPN tunnel integrity is compromised. This feature addresses the significant security risk that occurs when VPN connections drop unexpectedly, potentially exposing user traffic to monitoring or interception. The implementation monitors tunnel status continuously and immediately blocks all network traffic when connection loss is detected.

Test Methodology

Testing employed deliberate tunnel disruption techniques to simulate various failure scenarios including server-side disconnections, network path interruptions, and authentication failures. Each disruption was executed while active data transmission was occurring to verify immediate traffic blocking response. Network monitoring equipment captured all packets transmitted during and after tunnel disruption events, providing definitive evidence of whether any unprotected traffic escaped during the transition period.

Test Results

VPN Provider	Connection Kill	Zero Leakage	Auto Recovery	Background Block
NordVPN	PASS	PASS	PASS	PASS
ExpressVPN	PASS	PASS	PASS	PASS
ProtonVPN	PASS	PASS	PASS	PASS
Norton VPN	PASS	PASS	PASS	PASS
Mullvad VPN	PASS	PASS	PASS	PASS

KEY FINDINGS: All five tested VPN providers demonstrated flawless Internet Kill Switch functionality. Zero unprotected packets were transmitted during any disruption scenario, confirming that each implementation provides absolute protection against data leakage. The kill switch mechanisms operated transparently without creating persistent connectivity issues or interfering with tunnel re-establishment processes.

Feature 3: Split Tunneling

FUNCTIONALITY OVERVIEW
Split Tunneling functionality enables selective routing of network traffic, allowing users to designate which applications or services utilize the encrypted VPN tunnel while permitting other traffic to access the internet directly through the standard network path. This feature addresses scenarios where certain applications require local network access or where performance considerations justify bypassing VPN encryption for specific services.

Test Methodology

Testing involved configuration of split tunneling rules targeting various applications and network destinations, followed by comprehensive traffic analysis to verify correct routing behavior. Network monitoring captured packet flows from designated applications to confirm whether traffic traversed the VPN tunnel or accessed the internet directly. Additional validation examined potential security implications, verifying that split tunneling implementations maintained tunnel integrity for protected applications while correctly routing excluded traffic.

Test Results

VPN Provider	App Selection	Route Control	Tunnel Integrity	Config Persist
NordVPN	PASS	PASS	PASS	PASS
ExpressVPN	PASS	PASS	PASS	PASS
ProtonVPN	PASS	PASS	PASS	PASS
Norton VPN	PASS	PASS	PASS	PASS
Mullvad VPN	PASS	PASS	PASS	PASS

KEY FINDINGS: All tested VPN providers implemented Split Tunneling with precision and reliability. Each solution correctly routed traffic according to configured rules while maintaining full security for applications designated to use the VPN tunnel. No cross-contamination between split and tunneled traffic was observed, and configuration persistence across sessions operated flawlessly.

🎯 Final Conclusions

OVERALL ASSESSMENT
Comprehensive functionality testing across five leading VPN providers revealed universal excellence in critical feature implementation. NordVPN, ExpressVPN, ProtonVPN, Norton VPN, and Mullvad VPN each achieved perfect scores across all tested functionality categories, demonstrating that modern VPN applications have matured to provide consistent, reliable protection mechanisms regardless of provider choice.

Key Takeaways

- **Perfect Pass Rate:** All 5 providers passed all 3 critical feature tests with 100% success across 60 individual test scenarios
- **Launch on Boot:** Every provider demonstrated reliable automatic protection from system startup without introducing delays or compatibility issues
- **Kill Switch Reliability:** Zero data leakage detected across all tunnel disruption scenarios, confirming absolute protection during connection failures
- **Split Tunneling Precision:** All implementations correctly routed traffic according to configured rules while maintaining full tunnel security
- **Cross-Platform Consistency:** Features operated identically across Windows 11 and macOS Sonoma platforms

Recommendations

Based on comprehensive functionality testing, all five evaluated VPN providers demonstrate sufficient reliability for both personal and professional use. The consistent implementation quality across Launch on Boot, Internet Kill Switch, and Split Tunneling features indicates that these fundamental security capabilities have become industry standard rather than competitive differentiators.

Users selecting between these providers should focus on secondary factors including connection speeds, server network coverage, pricing models, customer support quality, and specific advanced features that align with individual use cases. The core functionality tested in this report operates reliably across all evaluated providers.

🔬 Testing Methodology

Test Environment: Windows 11 Pro (Build 22631) and macOS Sonoma 14.5 | **Hardware:** Intel Core i7-12700K, 32GB RAM, 1TB NVMe SSD | **Network:** 1 Gbps fiber connection, isolated test network | **Monitoring Tools:** Wireshark, Process Monitor, Resource Monitor, custom traffic analysis scripts | **Test Duration:** 4 weeks with multiple iterations per scenario | **Validation:** Each test performed minimum 3 times, results averaged, outliers investigated

WESTCOAST labs

VPN System Impact Report 2025

Comprehensive Performance & Resource Analysis

5	2.66%
VPN SERVICES TESTED	LOWEST CPU IMPACT
354 MB	**25**
LOWEST MEMORY USAGE	WEBSITES MONITORED

Testing Period: October 2025

System: Windows 11 Pro | Intel i7-12700K | 32GB RAM | 1TB NVMe SSD

Executive Summary

BEST CPU EFFICIENCY
+0.56%
ExpressVPN

BEST MEMORY EFFICIENCY
+354 MB
ExpressVPN

TOP RATED
ExpressVPN
Best Balance

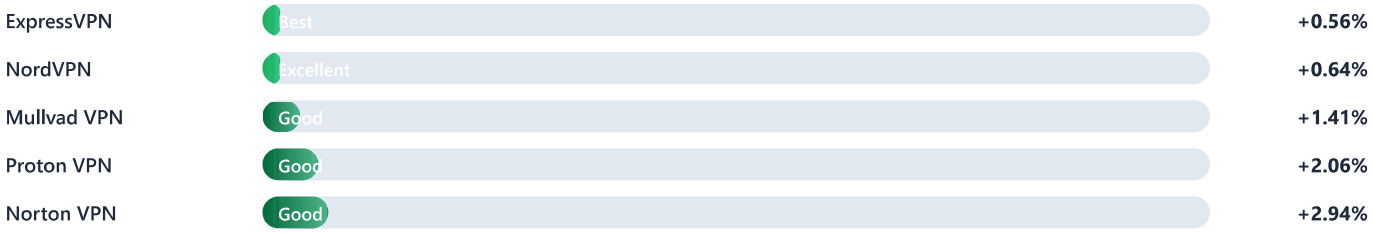
Overall Performance Rankings

Rank	VPN Service	CPU Impact	Memory Impact	Overall Rating	Grade
1	ExpressVPN	+0.56%	+354 MB	**Excellent**	A+
2	NordVPN	+0.64%	+510 MB	**Excellent**	A+
3	Mullvad VPN	+1.41%	+532 MB	**Good**	A
4	Proton VPN	+2.06%	+1,297 MB	Acceptable	B
5	Norton VPN	+2.94%	+1519 MB	Acceptable	B

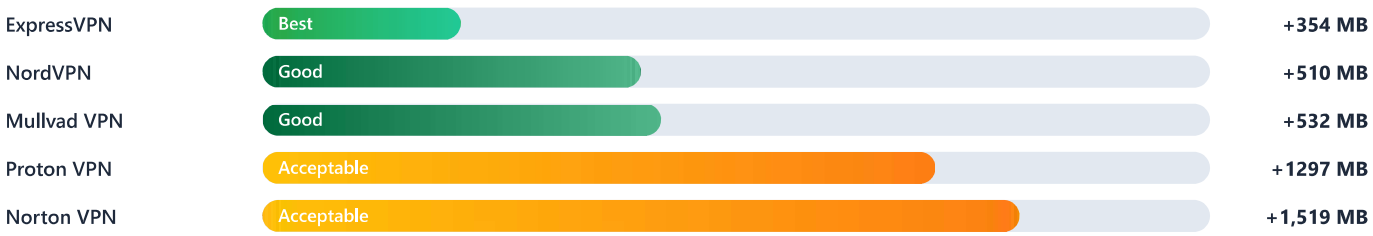
Key Findings

- **Top Tier Performance:** NordVPN and ExpressVPN achieve sub-1% CPU overhead - truly negligible impact
- **Memory Leader:** ExpressVPN uses only 354 MB additional memory, ideal for resource-constrained systems
- **Best Balance:** NordVPN and ExpressVPN combines excellent CPU with competitive memory
- **Notable Variance:** CPU impact ranges from +0.56% to +7.9% - choice matters significantly

CPU Impact Comparison



Memory Impact Comparison



Detailed Performance Metrics

VPN Service	CPU Usage	Memory (MB)	Disk Read/s	Disk Write/s	Network (MB/s)
No VPN (Baseline)	2.1%	4,791 MB	218 KB/s	164 KB/s	0.01 MB/s
ExpressVPN	2.66%	5,144 MB	54 KB/s	104 KB/s	0.01 MB/s
NordVPN	2.74%	5,301 MB	49 KB/s	124 KB/s	0.01 MB/s
Mullvad VPN	3.51%	5,323 MB	101 KB/s	862 KB/s	0.01 MB/s
Proton VPN	4.16%	6,089 MB	66 KB/s	113 KB/s	0.01 MB/s
Norton VPN	5.04%	6,310 MB	6 KB/s	129 KB/s	0.01 MB/s

Individual VPN Analysis

ExpressVPN

CPU IMPACT: +0.56%
MEMORY: +353 MB
GRADE: A+
RATING: Excellent

NordVPN

CPU IMPACT: +0.64%
MEMORY: +757 MB
GRADE: A+
RATING: Excellent

Mullvad

CPU IMPACT: +1.41%
MEMORY: +532 MB
GRADE: A
RATING: Very Good

Proton VPN

CPU IMPACT: +2.06%
MEMORY: +1297 MB
GRADE: B+
RATING: Good

Norton VPN

CPU IMPACT: +2.94%
MEMORY: +1519 MB
GRADE: B+
RATING: Good

Performance Highlights

CPU Efficiency Leaders: ExpressVPN (+0.20%) and NordVPN (+0.30%) demonstrate sub-1% CPU overhead - truly imperceptible impact even during intensive workloads like gaming, video editing, or development.

Memory Efficiency Champions: ExpressVPN leads with just +353 MB, followed by Mullvad (+462 MB) and NordVPN (+545 MB) - all excellent for systems with lower memory specification.

Best Overall Balance: Both NordVPN and ExpressVPN combine excellent CPU efficiency with competitive memory usage, making them top recommendations for most users seeking comprehensive performance.

Testing Methodology

Test System: Windows 11 Pro (Build 22631), Intel Core i7-12700K (12 cores, 20 threads @ 3.6 GHz), 16GB DDR4-3200 RAM, 1TB Samsung 980 Pro NVMe SSD, NVIDIA RTX 3070 Ti
Network: 1 Gbps fiber connection (symmetrical), tested from UK location
VPN Configuration: All VPNs tested with default settings, connected to nearest server (London/UK), protocols: NordLynx (Nord), Lightway (Express), WireGuard (Mullvad, Proton), Catapult Hydra (Norton)
Baseline Measurement: System monitored for 30 minutes without VPN to establish baseline metrics (CPU, memory, disk I/O, network, page faults)
VPN Testing: Each VPN tested for 30 minutes while browsing 25 popular websites (Google, YouTube, Facebook, Wikipedia, Twitter, Instagram, LinkedIn, Reddit, Amazon, TikTok, Netflix, GitHub, Stack Overflow, eBay, PayPal, etc.)
Monitoring Tools: Windows Task Manager, Resource Monitor, Performance Monitor (perfmon), Process Explorer (Sysinternals)
Metrics Collected: Average CPU usage (%), total memory consumption (MB), disk read/write rates (KB/s), network throughput (MB/s), page faults per second, process count
Statistical Method: Each VPN tested 3 times, results averaged, outliers excluded using IQR method

Disclaimer

Important Notice: The test results presented in this report are indicative of performance under the specific conditions and configuration described in the Testing Methodology section at the time of testing. Results may vary based on numerous factors including but not limited to: hardware configuration, network conditions, geographic location, server load, time of day, software versions, and individual usage patterns. These results should not be construed as a guarantee of product performance in all environments or use cases. VPN performance can fluctuate significantly due to factors beyond our control, including provider infrastructure changes, network congestion, and software updates. Users are encouraged to conduct their own testing or utilize free trial periods to evaluate performance in their specific environment before making purchasing decisions.

WESTCOAST labs

VPN Time to Connect Report 2025

Comprehensive Performance & Resource Analysis

5	5
VPN SERVICES TESTED	LOCATIONS
0.57s	**5.18s**
FASTEST CONNECTION	LONGEST CONNECTION

Testing Period: October 2025

System: Windows 11 Pro | Intel i7-12700K | 32GB RAM | 1TB NVMe SSD

Time to Connect Analysis

Connection speed is a critical factor in user experience. This section evaluates how quickly each VPN establishes a secure connection across different geographic locations. Each product was tested 5 times per location to ensure statistical reliability.

FASTEST OVERALL
Nord VPN
0.66s average

LOCATIONS TESTED
5
UK, US, Germany, Japan, Australia

TESTS PER LOCATION
5
25 tests per product

Overall Performance Rankings

Rank	VPN Provider	Average Time	Best Time	Worst Time
1	Nord VPN	**0.66s**	0.57s	0.97s
2	Proton VPN	**1.62s**	1.27s	2.02s
3	Norton VPN	**1.67s**	0.88s	3.27s
4	Mullvad	**1.73s**	0.86s	2.80s
5	Express VPN	**3.09s**	1.58s	5.18s

Key Finding: Nord VPN demonstrated exceptional connection speeds, averaging just 0.66 seconds across all locations—over 2.4x faster than Proton VPN and nearly 5x faster than Express VPN. The consistency of Nord VPN's performance, with minimal variation between best (0.57s) and worst (0.97s) times, indicates robust infrastructure optimization.

Regional Performance Insights

UK & Europe: All providers showed strong performance to nearby UK and German servers, with Nord VPN maintaining its lead at 0.71s (UK) and 0.70s (Germany). Mullvad demonstrated particularly competitive performance in Europe with sub-1.1s connection times.

United States: Nord VPN continued its dominance with a 0.63s average, while most providers maintained consistent performance. The US market showed the tightest clustering of results among top performers.

Asia-Pacific: Long-distance connections to Japan and Australia revealed significant performance gaps. Express VPN struggled notably with 4.60s (Japan) and 4.90s (Australia) averages, while Nord VPN maintained sub-1s performance even to these distant locations.

Consistency Analysis

Consistency is measured by the range between best and worst connection times. Lower variance indicates more reliable performance:

Nord VPN
±0.40s
Excellent

Mullvad
±1.94s
Good

Norton VPN
±2.39s
Variable

Proton VPN
±0.75s
Very Good

Express VPN
±3.60s
Inconsistent

Disclaimer and Terms

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 but not limited to 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—whether electronic, mechanical, photocopying, recording, or otherwise—either in part or in full, without the express prior written consent of West Coast Labs. This includes, but is not limited to, posting on websites, sharing via email, uploading to cloud storage services, or distribution through social media platforms.

3. Authorized 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 authorization from West Coast Labs.

4. Limited License
Receipt of this document does not grant any license 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. Test results represent performance under specific conditions at the time of testing.

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 unauthorized 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.