ARTIFACT SECURITY

VPN Performance Testing

ARTIFACT SECURITY

Introduction

This test aims to evaluate the impact of VPN services on a system's performance. We aim to take a real-world scenario based approach that reflects a real user's expectations when using such services. This methodology was constructed with the AMTSO VPN Testing - performance assessment guidelines.

Environment

Each executed test the full details of the tested devices and operating systems are disclosed alongside their specifications. Tested devices have enough overhead on their minimum specification for monitoring tools to not have a significant impact on the test results.

Platforms and devices considered in scope:

- Windows
- Mac OS
- Linux
- iOS
- Android

Baseline data for latency and speed is taken at the same time as the test is executed on a Reference Device.

Test Scope

Specific test scope is provided alongside each test plan to indicate the specific "Highways" and scenarios replicated. The default protocol used by each VPN application is used. Upon request specific protocol can be used. These are disclosed in any public report.

Main VPN Features

Time to connect is defined as the average time from multiple tests, measured from the initiation of the attempt to connect to a successfully-established connection.

This is measured from the start event defined as the **first DNS query** for the VPNs server to the **first encrypted application data** seen in the packet capture.

Speed/Latency users

Traffic speed and latency once connected to a VPN server is paramount for a user's browsing experience. To reflect real world conditions, Wireshark and Ookla SpeedTest are used to collect logs during a normal user experience. When using Wireshark a capture is started before each scenario and ended approximately 30 seconds after scenario conclusion.

Metric	**Wireshark Measurement**	**Ookla Test**
Throughput(speed)	I/O Graphs built in	download.bandwidth & upload.bandwidth
Packet loss	tcp.analysis.retransmission filter	tcp.analysis.retransmission
Latency	tcp.analysis.intial_rtt	ping.latency

Leak & Resilience Testing

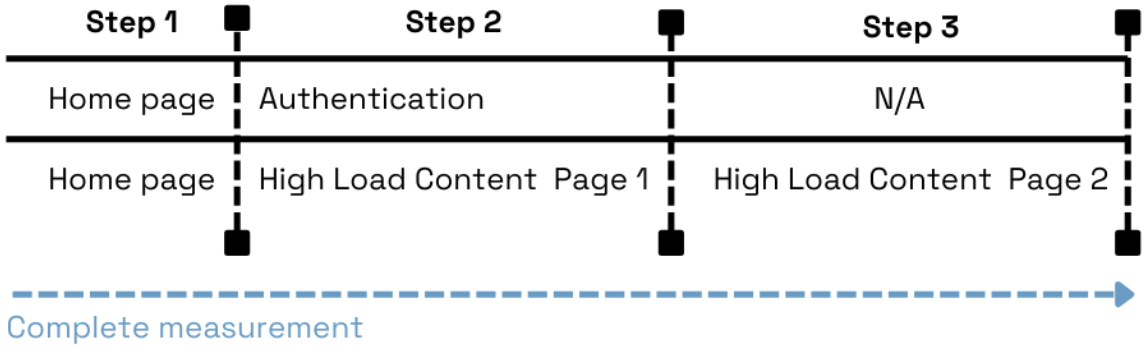
Tests in this section are designed to evaluate the reliability of the VPN tunnel and prevent leaking data.

Scenario	**Description**	**Rating**
IP leak Test	Public IP address verification	Pass/Fail
DNS Leak Test	VPN specific DNS request	Pass/Fail
Network Handover	Mobile - WiFi - Cellular	Pass/Fail
Kill Switch Integrity	Traffic immediately interrupted until tunnel is re-established	Pass/Fail
WebRTC Leak	WebRTC must be be blocked or forced through the VPN Tunnel	Pass/Fail
Split Tunneling	Integrity of traffic when split tunneling is used	Pass/Fail
DHCP Option 121	Rogue DHCP instructions	Pass/Fail

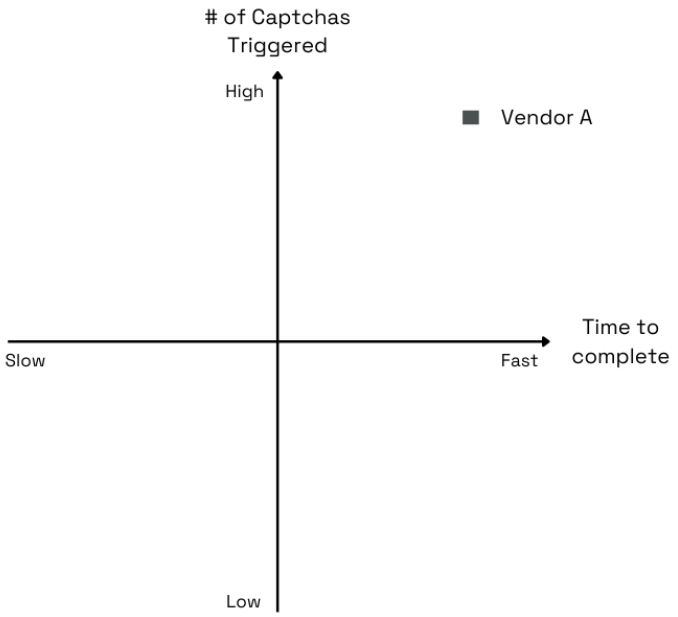
Website Accessibility

Captcha challenges can be troublesome for users of VPN applications. In order to measure the impact using such applications against a multitude of websites. The top 100 list from SimilarWeb is used for the full corpus of websites considered in scope for the month that the test is executed. For each test, navigation to the home page of each website is executed.

Advanced Website Accessibility module:
Of the base 100 websites, 25 randomly selected websites are used for common use scenarios such as user authentication and high content-load.



Measurement is done via navigation timing API and taken upon completion of each step. The completion of a step is defined as the time it takes for the target page to be responsive to the user. Triggered captchas are removed from speed calculation but counted towards # of captchas triggered rating. Measurement is shown as such:



Resource Consumption & Feature Validation

All resources used by VPNs processes are measured during test execution. Unique selling points of VPN providers can be validated to give a complete overview of the feature list available to buyers.

Example feature check table

Feature Name	Advertised	Validated
Feature 1	✓	X
Feature 2	✓	✓
Feature 3	✓	✓

Metrics and Rating

All metrics will be taken throughout different scenarios and highways across all devices considered in scope in the test plan. A minimum of 5 attempts per scenario will be executed and a mean average is calculated. The lowest and the highest times will be removed from the calculation. In case of comparative testing, the same number of attempts are executed for all tested solutions.

Each metric is measured during peak live events and off-peak times for each of the chosen highways in the test plan, results are presented as both raw tables and rating applied on the data represented.

Example raw results tale:

	Peak	Off-Peak
UK - France	Time in ms	Time in ms
UK - US East	Time in ms	Time in ms
UK - US West	Time in ms	Time in ms
UK - Asia	Time in ms	Time in ms
UK - UK	Time in ms	Time in ms

*This table is not an exhaustive list and is for illustrative purposes only

Key Metrics:

Metric	Notes	Off-Peak	Peak
Time to Connect	Snapshot measurement, repeated	✓	✓
Throughput	Snapshot & Constant measurement	✓	✓
Packet Loss	Snapshot & Constant measurement	✓	✓
Latency	Snapshot & Constant measurement	✓	✓
Captcha Impact	Snapshot measurement	N/A	N/A

Ratings:

Time to Connect:

Formula: $T_{Time\ to\ Connect} = T_{Encrypted\ Data} - T_{Handshake\ Start}$

Rating	Definition
Negligible	≤2s
Minor	2s < T ≤ 4s
Disruptive	4s < T ≤ 10s
Critical	10s < T

NOTE: National Highways table rating. Each highway chosen can have their own thresholds.

Throughput/Speed Rating:

Formulas: $T_{Peak\ Throughput}$ = Peak Value in I/O Graph/Download/Upload

$T_{Average\ Throughput}$ = Conversations Bits/s A -B for stream

Speed loss % = $\left(\frac{Reference\ Speed - VPN\ Speed}{Reference\ Speed}\right) x\ 100$

Rating	Thresholds
Negligible	0% - 15%
Minor	15% - 30%
Disruptive	30% - 50%
Critical	> 60%

NOTE: National Highways table rating. Each highway chosen can have their own thresholds.

Latency

Formula: $T_{Latency} = \text{Average } (T_{ack} - T_{syn})$

Rating Formula: Latency Increase % = $(\frac{V-R}{R}) \times 100$

Rating	Thresholds
Negligible	0% - 5%
Minor	5% - 15%
Disruptive	15% - 30%
Critical	> 30%

NOTE: National Highways table rating. Each highway chosen can have their own thresholds.

TCP Packet Loss

Formula: Packet Loss % = $(\frac{Retransmission\ Packets}{Total\ Packets})$ x 100

Rating formula: Stability Impact = $V_{loss\%}$ - $R_{loss\%}$

V = VPN loss
R = Reference loss

Rating	**Thresholds**
Negligible	0% - 0.5%
Minor	0.5% - 1%
Disruptive	1% - 3%
Critical	> 3%

NOTE: National Highways table rating. Each highway chosen can have their own thresholds.

Overall grade:

Each key metric is weighted to contribute to the final grade.

Throughput/Speed Impact (T)	35%
Stability Impact (S)	30%
Latency Impact (L)	20%
Time to Connect (TC)	15%

Weights table

$$Grade = (T \times 0.35) + (S \times 0.30) + (L \times 0.20) + (TC \times 0.15)$$

Ratings given during each scenario earn the following points:

Rating	Points
Negligible	100
Minor	80
Disruptive	40
Critical	20

Each highway is given an overall award which is then averaged out to given the final grade based on these thresholds:

Award	Threshold
S	> 90%
A	80% - 90%
B	70% - 80%
C	60% - 70%

Change Log

28/01/2026 - Document Created - Identifier - VPNPerformance2026V1