Evaluation of an Additional Security Feature for VPN's

A test commissioned by NordSec and performed by the AV-TEST institute.

Date of the test report: November 14, 2024 (version 1.00)

Executive Summary

In September/October 2024, AV-TEST performed a comparison test of ExpressVPN, IPVanish VPN, Mullvad VPN, NordVPN and Proton VPN. The test focused on their additional capabilities of blocking malicious URLs and phishing websites as well as false positive avoidance.

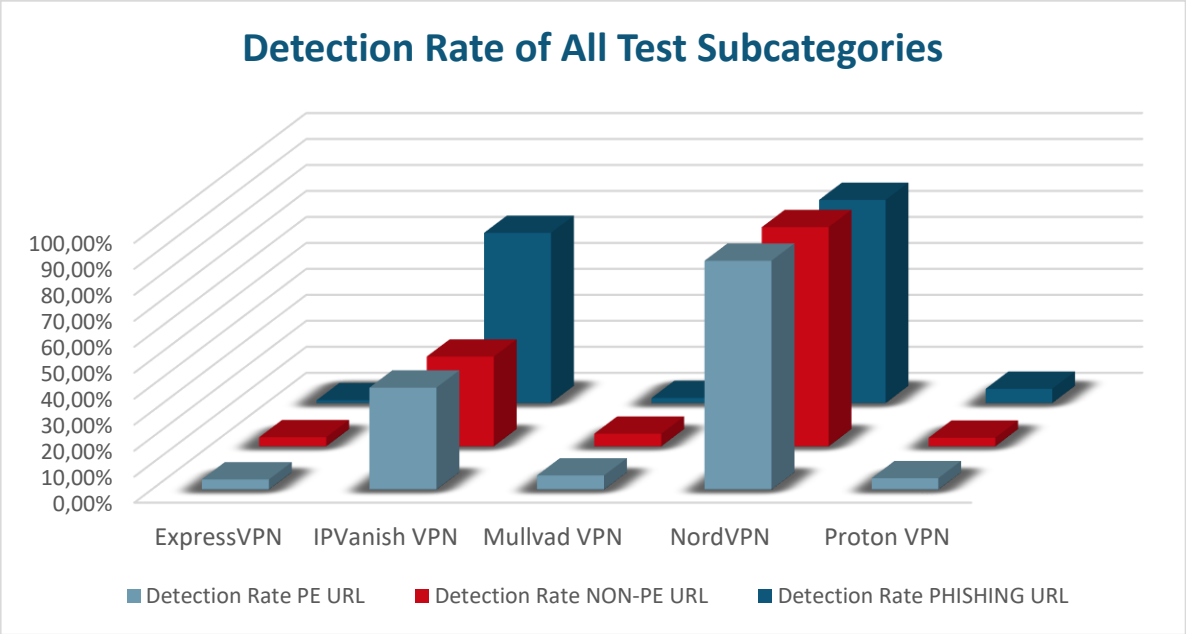

Figure 1 Detection Rate of All Test Subcategories

To maintain an unbiased review, NordSec did not provide any samples (including malicious or clean files, URLs, or related metadata) and had no influence or prior knowledge of the samples selected for testing. All tested links and malicious samples were verified by AV-TEST as recent and active at the time of testing.

The test focused on the detection rate of links pointing directly to portable executable (PEs) malware (e.g., EXE files), links pointing to other types of malicious files (e.g., html, JavaScript) and phishing URLs. A total of 3,209 malicious samples were tested.
In addition, AV-TEST evaluated false positive rates by downloading popular applications from both HTTP and HTTPS websites and conducted an additional false positive test on popular, verified clean websites.

A total of 2,298 test cases were used to determine if the product causes any disruption during normal use.

Detailed information on the test setup and test scenarios can be found in the following sections of this report.

Test Overview

Every second, AV-TEST discovers three to four new malware variants. This sums up to around 9 million new malware every month, or more than 1.35 billion malware objects in total which are included in AV-TEST's database.

While most malware targets the Windows platform, safeguarding all operating systems is essential. Attaining protection against the growing number of threats is essential for all consumers. Phishing is a good example of an attack method that affects all operating systems. A thread actor exploits user deception by creating a false perception of legitimacy, thereby enabling the attacker to steal confidential data.

NordSec commissioned AV-TEST to evaluate additional security layers for VPNs. This evaluation did not focus on the core functionality of VPN products, but rather on additional security features that are built on top of these products, such as protection. Some of the products tested emphasize user privacy by prioritizing the blocking of adware and trackers. While these features are not a substitute for traditional antivirus solutions, they can provide additional protection when accessing the Internet.

Overview of NordVPN Threat Protection Pro

NordVPN's Threat Protection Pro™ is a cybersecurity feature that's integrated directly into the NordVPN app, making your browsing safer and smoother while protecting you from phishing and other cyber threats.

It comes with tools such as a malware scanner and blocker, search results safety indicator, and even an ad and tracker blocker. With these benefits, Threat Protection Pro™ can block unwanted ads and URL trackers, scan the web for malicious websites and search results, and instantly cut off access to harmful content (including downloads).

And that's not all. Threat Protection Pro™ is an advanced antivirus tool that works independently of a VPN connection. It's powered by cyber-threat intelligence and machine learning, providing similar functionality to an antivirus. It also places greater focus on user privacy and safe browsing for Windows and macOS users.

Test Description

All the tests were performed at AV-TEST's laboratory in Magdeburg, Germany. All data used for testing, including all sample URLs and metadata, were exclusively sourced by AV-TEST.

NordSec did not have access to any sample URLs before the testing, nor did they provide such data for the testing. All samples were pre-verified by AV-TEST as known malicious or phishing sites. AV-TEST uses both static and dynamic analysis to confirm that the domains are actively hosting malicious content at the time of testing and that the samples exhibit their malicious behavior.

The Real-World test has three categories, that cover the different types of attacks:

- URLs pointing to malicious PE files (for Windows, EXE files)
- URLs with other malicious destinations (non-PE files, usually html or php web pages, including links to scripts such as JavaScript or VBS)
- Links to phishing sites

A total of 3,209 samples were used in the Real-World test, consisting of 1,050 malicious links to PE files, 1,031 links to other malicious (non-PE) file types, and 1,128 links to phishing sites.

For false positive testing, AV-TEST used the following types of known clean files and websites from http and https sources:

- URLs pointing to clean file downloads (mainly PE for Windows, EXE files)
- URLs with other non-malicious destinations (non-PE files, usually clean html or php websites)

All samples utilized for false-positive testing were carefully curated and validated. In an exhaustive review by AV-TEST, the samples did not show any signs of malicious behavior and were considered clean. A total of 2,298 clean websites and downloads were used for the initial test (1,194 downloads and 1,104 websites)

All VPN products were installed on virtualized Windows systems running Windows 10 Professional (English, 64 bit), with all patches installed.
The VPN connectivity was ensured at any time of the test

All download attempts were triggered using Google Chrome to access the test URLs.
The evaluation process included checking to see if access to the URL was successful or if it was blocked by the product.

All testing was conducted between September 3rd and October 28th, 2024.

Test Results

Looking at the overall detection rate, the best product is NordVPN with 83.42%, followed by IPVanish with 46.96% and then the remaining products. This pattern of NordVPN being the best product and IPVanish being the second best applies to all the three subcategories PE URL, NON-PE URL and Phishing. The best covered category for IPVanish's is Phishing, while for NordVPN it is PE URL.

The detailed results of the detection tests are as follows (higher is better):

	Ref.	Express VPN		IPVanish VPN		Mullvad VPN		NordVPN		Proton VPN	
Total Detection Rate	**3209**	89	2.77%	1507	46.96%	129	4.02%	2677	83.42%	142	4.43%
Detection Rate *											
PE Url	**1050**	41	3.90%	412	39.24%	57	5.43%	925	88.10%	46	4.38%
NON-PE Url	**1031**	36	3.49%	356	34.53%	50	4.85%	870	84.38%	34	3.30%
PHISHING Url	**1128**	12	1.06%	739	65.51%	22	1.95%	882	78.19%	62	5.50%

Chart 1 Total Detection Rate and Detection Rate of All Test Subcategories

For the false positive testing, the detailed results are the following ones (lower is better):

	Ref.	Express VPN		IPVanish VPN		Mullvad VPN		NordVPN		Proton VPN	
Total Detection Rate	**2298**	16	0.70%	35	1.52%	7	0.30%	11	0.48%	17	0.74%
Detection Rate *											
FP-INST	**1194**	11	0.92%	15	1.26%	2	0.17%	4	0.34%	10	0.84%
FP-Websites	**1104**	5	0.45%	20	1.81%	5	0.45%	7	0.63%	7	0.63%

Chart 2 False-Positive Detection Rate and Both Subcategories

As shown in the chart, the false positive rate is relatively low given the number of URLs tested. IPVanish has the highest rate at 1.52%, followed by Proton VPN, Express VPN, Nord VPN and Mullvad VPN has the lowest rate. However, the risk of a false positive remains at a low level for all tested products.

Criteria

To receive the TEST APPROVED Network Threat Protection VPN certificate, it is necessary to prove adequate blocking results for Real-World web threats overall and for all three test subcategories. A low false-positive rate is also required to receive the certificate.

Awarded

By meeting all certification criteria, NordSec NordVPN was awarded the AV-TEST APPROVED Network Threat Protection VPN certificate from all test candidates.

Conclusion

All five VPN products were tested independently by AV-TEST, with no knowledge of the URLs tested, the testing methodology, or the providing samples for the testing. Across all three malicious test categories, NordVPN showed the best performance of all five products tested with an overall detection rate of 83.42%, followed by IPVanish VPN with 46.96%, Proton VPN, Mullvad VPN and Express VPN. Looking at the false positive rates, the test shows that there is only a low risk of disruption to the average user.