VPN Comparative Test

A test commissioned by AnchorFree and performed by AV-TEST GmbH
Date of the report: June 15th, 2018

Executive Summary

In April 2018, AV-TEST performed a test of Virtual Private Networks (VPN) solutions. VPNs have been reviewed in its different fields of potential uses such as providing privacy, anonymity or virtual different geographical location.

The presented evaluation assesses AnchorFree's Hotspot Shield Elite, Avast SecureLine, Avira Phantom VPN Pro, Cisco VPN, ExpressVPN, F-Secure FREEDOME VPN, KeepSolid's VPN Unlimited, London Trust Media's Private Internet Access, NordVPN, Pulse VPN, Symantec's Norton WiFi Privacy and Tunnel Bear.

We evaluated VPN on the following four criteria.

Usability: evaluating the ease of use, taking into account novice users. We evaluate how much effort it takes not just to install the application but also to change settings and how much of that effort is omitted by scheduled default settings. The range of clicks required until a product is setup varies, it may take 11 clicks for VPN Unlimited or only two clicks as with F-Secure FREEDOME VPN. The top scores in this tested category are shared between Avast SecureLine VPN, F-Secure FREEDOME VPN and Hotspot Shield Elite.

Privacy and Security: testing how well the Internet Protocol Address (IP) and by extension the identity of the user is protected and hidden from outside parties like internet service providers (ISP) and webservers. This protects the anonymity of the user when accessing content online. Some products like Hotspot Shield Elite have all security and extras included by default others like Pulse Connect Secure or Avast SecureLine VPN don't include certain features which may be considered important to keep privacy intact. The top scores are shared between F-Secure FREEDOME VPN, Private Internet Access, ExpressVPN and Hotspot Shield Elite.

Performance: measuring the amount of time for different VPN utilization compared to an unprotected connection depends on geographical location, the location of the VPN servers as well as the tasks performed by the user while the connection is active. We perform this test through all 7 weekdays at multiple times through each day to balance load times in different regions and for the different use cases. Hotspot Shield Elite is the clear winner when it comes to performance. No other product reaches similar speed when downloading, uploading or when file sharing data. Almost every performance test was led by Hotspot Shield Elite, which on average more than doubled the download speed as the competition. Private Internet Access came second followed by NordVPN, achieving similar scoring.

Functionality: reviewing the amount and quality of features available to choose and customize options. Different users have different requirements. These requirements vary with different proficiency levels. Also, users vary in their expectations for a VPN. Some users will expect a vast net

of servers all around the globe others expect a higher standard in privacy implementations such as no logging of any data. This category is led by NordVPN and close behind Private Internet Access and then ExpressVPN. These applications provide all basic and numerous more advanced features for further configuration.

Overview

VPN provides anonymity through hiding the used IP from visited webpages and used applications. User data is encrypted keeping data anonymous from third parties like the ISP. VPNs allow evading of geographical blocked webpages as well as allowing access to locally censored content. Some VPNs provide additional security and privacy services such as ads-, tracker- and malware blocker, useful not just on personal home PCs but also on mobile devices to save network data. For company and cooperation's it offers the possibility to access local network from anywhere in the world.

There are many use cases for VPNs but only if they work as advertised. Advertisers, webpage providers, governments and others are attempting to track user and their activity online through varies means. Privacy protection needs to be airtight. The users' identity maybe unmasked deliberately by visited web content or accidentally through an unsecured VPN. There are numerous ways such "leaks" may happen and a good VPN will be able to cope with them all. In the context of privacy, it must also be mentioned that the logging policies should be clearly stated and adhered. Such as no personal data or identifying meta-data is logged and in what intervals the logged data is removed from the VPN server. The VPN should also support and use by default most up-to-date and most secure protocols to ensure that data is kept encrypted and transmitted securely.

The user will expect the same experience accessing the internet using a VPN as without it. Fast performance is a necessity which may not always be a given. Of course, in most cases, the performance will suffer using a VPN because of encryption and tunnelling of the data through not the direct route but through the VPN servers. Performance is heavily dependent on the server location because it will make a difference in performance if the connection needs to be routed halfway across the planet or only to a neighbouring country. The more servers are available the more evenly the network traffic will be distributed and therefore a more reliable connection can be expected. More server locations also provide the added advantages of more access to content worldwide which may be geo-blocked.

Different users have different requirements for their chosen solutions some require torrents to work others will put more emphasis on a wide degree of supported systems which can run the VPN like media sticks or routers.

Platforms

Windows

The tests were performed on physical machines and Virtual Machines hosted on Microsoft Azure cloud computing service. All tests for a defined operating system were carried out on devices with identical hardware configurations as described below.

All tests for the Windows operating system were performed on identical PCs equipped with the hardware specified in the appendix. All patches available in April 2018 were previously installed. Windows defender has been deactivated to avoid false positive detections during testing.

There are a few generic principles that were followed:

(1) **Product cloud/Internet connection**. The Internet was available to all tested products.
(2) **Product configuration**. All products were run with their default, out-of-the-box configuration. Including default protocol used
(3) **Clean device for the start of the test**. The test devices were restored to a clean state before testing the malware samples.

Testing Approach

Usability Test

The usability scoring attempts to measure the ease and comfort level when installing and setting up the application on the Windows system. These applications are for private and cooperate users and therefore should address different levels of computer proficiencies. Allowing the user to setup a default connection plan with few clicks out of the box, like auto reconnect upon system start. The number of steps to achieve the desired goal is counted and compared. The available languages are evaluated to determine if non-native English speakers will have alternative choices.

Privacy and Security

We have identified six ways of possible data and information leaks which have to be addressed by the VPN products.

- DNS leaks, tested through *https://www.dnsleaktest.com/*
- IP leak through missing or non-functioning kill switch tested by deactivating and reactivating the network card as well as disconnecting the network connection for 1, 10 and 60 seconds and determining the IP directly after reconnection.
- WebRTC, tested through *https://browserleaks.com/webrtc* verified through *https://www.doileak.com/*
- Windows login leak, tested through *https://msleak.perfect-privacy.com/*
- Torrent IP leak, tested through https://ipleak.net/
- HTTP request leak, tested through *https://www.doileak.com/*

Malware detection has been tested by opening 49 malicious URLs on a physical machine with the active VPN connection. The URLs are verified to be malicious by our in-house analysis systems.

To ensure the VPNs are compatible with all major anti-malware security products, all files copied to the system are scanned by the in-house multi-scanner system VTEST to check for possible false detections.

Performance Test

For the performance test, we measure the time taken for different use cases. The testing was performed up to six times a day distributed through the day from Saturday until Friday. The geographical locations were chosen to be one US location at the east coast and one European location in the UK, both provided through Azure VM. At each geographical location, every product is hosted twice, ones for each VPN location chosen to be tested. The VPN locations to be tested were US west coast and UK London where possible. Not all products allow such specifics but instead allow the overall country. The max and min value of each testing period are omitted from the test results before calculating the averages.

- Downloading, uploading and latency is tested through the testing environment CloudHarmony which is owned and operated by Gartner Group (*https://cloudharmony.com/*). Every connection has three tests performed with different but similar locations. The same connection are then tested while encrypted (through https). This provides six results for every product at each geo location for both different VPN connections. Further details on the connected server in the appendix.
- Video performance is measured through StreamTest.net (*http://www.streamtest.net/*)
- For Torrent, a 650 MB large file is downloaded, which has been in circulation for years, for which a small variation of Leechers and Seeder can be assumed and therefore will be neglected.

Functionality Test

In order to be considered as a complete VPN solution, the features provided by the solution should be comprehensive. We determine the features considered vital for a VPN application and those additional features which complete this kind of application. We validate the existence of such features in the application and through information provided online by the vendors. This also provides potential customers with an insight into what they buy and a guideline to use along with their own expectations from the application.

Test Results

Usability

Products	Setup steps	Con-nection steps	Tutorial during setup steps	Online Account manage-ment	Number of supported languages (provider information)	Establish connection after reboot	Use previously established connection
Avast SecureLine VPN	7	2	4	+	24	-	n/a
Avira Phantom VPN Pro	9	2	5	+	13	-	n/a
Cisco AnyConnect Secure Mobility Client	13	3	-	nip	1	-	n/a
ExpressVPN	4	2	-	+	2	+	+
F-Secure FREEDOME VPN	2	2	-	-	20	+	+
Hotspot Shield Elite	2	2	-	+	10	+	+
NordVPN	2	2	-	+	1	+	+
Norton WiFi Privacy	5	2	-	+	18	+	+
Private Internet Access	5	2	-	+	18	+	+
Pulse Connect Secure	13	2	-	nip	1	-	n/a
TunnelBear	6	2	3	+	1	+	+
VPN Unlimited	11	2	-	+	7	+	+

nip - No information provided, n/a - not applicable, only reviewed when connection established after reboot by default

The setup process should be easy and quick. Some products like F-Secures FREEDOME, Hotspot Shield Elite and NordVPN take only two steps to install after download. Other products require significant more steps like Avira Phantom VPN pro which requires nine steps or VPN Unlimited which requires the user to interact 11 times during installation which is almost as much as Cisco AnyConnect and Pulse Internet Access, each of them requiring 13 steps. Both these products are sole corporate solutions and left out of this assessment.

Some products offer additional tutorials after installation which add additional steps but all of them allow easy skipping the whole process. Those products are Avast SecureLine VPN, Avira Phantom VPN Pro and TunnelBear.

Manually connecting to the VPN serves is very quick with all these products, requiring two steps for all but Cisco AnyConnect which requires three clicks.

F-Secure FREEDOME is the only home user product tested which does not provide some sort of online management console and can only be managed through the application.

The languages supported by the individual products vary greatly. At the highest tier, there are Avast SecureLine VPN which supports up to 24 different languages followed by F-Secure FREEDOME VPN 20 languages and Norton WiFi Privacy and Private Internet Access which each support 18 languages. On the other hand, ExpressVPN only supports English and French and Cisco AnyConnect, NordVPN, Pulse Connect Secure and TunnelBear only support English as far as we could determine.

The user might want to opt-in to automatically connect the system when booting and connect to the previously used server. This option is provided by all but four products. Those not supporting this feature are Avast SecureLine VPN, Avira Phantom VPN Pro, Cisco AnyConnect Secure Mobility Client and Pulse Connect Secure.

Usability Conclusion

Setup is pretty easy for all consumer products and since it's usually done only once on a system having some more clicks may not be a great inconvenience. Having a tutorial can be useful but as all products are pretty straightforward for the basic function this is also not considered very important. What should be considered when choosing a product is if the users' language is supported as not everyone is fluent in English. Also, auto connecting to the VPN seems crucial at least on desktop systems. Taking these points into consideration puts Avast SecureLine VPN, F-Secure FREEDOME VPN and Hotspot Shield Elite in shared first place. Closely followed by Norton WiFi Privacy and Private Internet Access.

Privacy and Security

Leak test results

Products	DNS leak	WebRTC local IP leak	Windows Login leak	P2P & Torrent Protection	HTTP request leak
Avast SecureLine VPN	+	+	-	+	+
Avira Phantom VPN Pro	+	+	-	+	+
Cisco AnyConnect Secure Mobility Client	+	+	-	+	+
ExpressVPN	+	+	+	+	+
F-Secure FREEDOME VPN	+	+	+	+*	+
Hotspot Shield Elite	+	+	+	+	+
NordVPN	+	-	+	+	+
Norton WiFi Privacy	+	+	-	n/a	+
Private Internet Access	+	+	+	+	+
Pulse Connect Secure	+	+	-	+	+
TunnelBear	+	+	-	+*	+
VPN Unlimited	+	+	-	+	+

* - Require selection of dedicated P2P servers. n/a - not applicable, torrent not available for Norton WiFi Privacy

DNS leak, Torrent IP leak and HTTP request Leak

When the users' main focus is privacy there are no compromises on leak prevention of identifying data. Some of the most common possible leaks are the DNS leak, Torrent IP leak and HTTP request leak for which all products provided protection. No case was observed in which the information was leaked.

WebRTC Leak

The Chrome and Firefox browser are both vulnerable to the WebRTC leak. This can be fixed by manually changing the browser settings. Some VPNs provide a browser independent fix. In our test, almost all VPNs offer some protection from the local network IP being disclosed.
NordVPN was the only product which allowed the real local network IP of the user to be published from some of their VPN servers.

Windows Credential Leak

An old yet never patched leak is the Windows Credential Leak. Using the Internet Explorer or Edge browser unprotected on most windows systems, the username and encrypted password will leak. Depending on its strength the account password can be cracked in seconds. This may not just leak a reusable password used but furthermore, the same windows credentials can be associated with other windows services of the user. Only half of the tested products offer protection for this issue those are ExpressVPN, F-Secure FREEDOME VPN, Hotspot Shield Elite, NordVPN, Private Internet Access and TunnelBear.

Kill switch

Products	Kill switch available	Disable-enable network card	Unmasked IP visible in s	Unplugged network cable 1s/10s/60s	Unmasked IP visible in s for unplugged 1s/10s/60s
Avast SecureLine VPN	-	-	15	+ / + / -	0 / 0 / 30
Avira Phantom VPN Pro	+*	+	-	+ / + / -	0 / 0 / -**
Cisco AnyConnect Secure Mobility Client	+	+	-	+ / + / -	0 / 0 / 1
ExpressVPN	+	+	-	+ / + / +	0 / 0 / 0
F-Secure FREEDOME VPN	-	-	2	+ / + / +	0 / 0 / 0
Hotspot Shield Elite	+*	+	-	+ / + / +	0 / 0 / 0
NordVPN	+*	+	-	+ / + / +	0 / 0 / 0
Norton WiFi Privacy	-	-	19	- / - / -	8 / 8 / 8
Private Internet Access	+*	+	-	+ / + / +	0 / 0 / 0
Pulse Connect Secure	-	x	-	- / - / -	8/8/12
TunnelBear	+*	+	-	+ / - / +	0 / 7 / 0
VPN Unlimited	-	-	15	+ / + / -	0 / 0 / 15

* - Feature not enabled by default, ** - No automatic reconnection, x - Network card switch off not working

Kill switch protects the user against sudden drops and re-establishing the connection with an unprotected IP. Two ways were used to emulate a sudden connection drop, first one is to disable and re-enable the network card and the second one is pulling the network plug and inserting it again after a time. Different results were observed when physically pulling the plug.
Seven products offered a kill switch feature. ExpressVPN was the only product to have the feature enabled by default. Hotspot Shield Elite, NordVPN and Private Internet Access require the feature to be activated by the user. These three products and ExpressVPN are the only products in our test with no IP leak observed.
Avira Phantom VPN Pro and Cisco AnyConnect Secure Mobility Client also require the user to manually switch-on the kill switch, but they still leaked the real IP when reconnecting after 60 seconds. Cisco AnyConnect Secure Mobility Client leaked the IP for only one second. Avira Phantom VPN Pro never managed to re-establish the VPN connection and the user was unprotected until manually re-establishing the VPN connection.
TunnelBear also required the manual activation of the kill switch feature. TunnelBear had problems hiding the real IP after a disconnection time of 10 seconds and took on average seven seconds to hide the users IP again.

Malicious URL Protection

Products	Phishing Websites (25 samples)	Malware Websites (24 samples)	Phishing Websites detection rate	Malware Websites detection rate
F-Secure FREEDOME VPN	18	13	72.00%	54.17%
Hotspot Shield Elite	13	2	52.00%	8.33%
NordVPN	0	0	0.00%	0.00%
Private Internet Access	9	0	36.00%	0.00%

Four products claim to offer protection from malicious websites. Some more products offer it when using browser extensions, but those were not considered, as this would not be a complete system protection and in this case, any other security add-ons can be used.
Testing 25 phishing websites and 24 malware dropping websites we found F-Secure FREEDOME VPN, Hotspot Shield Elite and Private Internet Access provided some protection. F-Secure FREEDOME VPN blocked almost two third of the phishing pages and more than half the malware dropping pages. Hotspot Shield Elite manages more than 50% on the phishing pages and just about 10% of the malware pages. Private Internet Access didn't manage to detect any of the phishing sites and only detected about a third of the malware websites.
The sample set size for this test was relatively small, so these numbers cannot be taken for granted and are likely not reflecting the real detection rate of these products. Yet having zero findings from NordVPN seems a bit disappointing.

Security compatibility

All the files installed under windows by the VPN were scanned with all major antimalware products. No issues were found which shows they can be used together on the same systems.

Privacy and Security Conclusion

The ranking for the first spots in the list is very close for this test. By features and provided security it boils down to following four products ExpressVPN, F-Secure FREEDOME VPN, Hotspot Shield Elite and Private Internet Access.

Hotspot Shield Elite passed all security checks. No leaks were detected, all necessary security features are present as well as being one of only three products providing additional security features in form of malicious website blocks. No slip-up in this category ensured the top spot for the product.

ExpressVPN leaves nothing to be desired when it comes to the leak test. By default, it protects against IP leaking when there are network issues which results in sudden connection drops and it did so very well in our test by being one of only four products doing so. The only thing amiss to complete the provided security would be malicious website detection as provided by the other three top products.

Private Internet Access is one of the best VPNs when it comes to leak prevention. It provides full protection for the user's privacy as well as security. It also provides a basic website security feature. In our test, there was no phishing website block observed and only about a third of malware pages were detected.

F-Secure FREEDOME proves very good overall security. It was one of only three products to really provide some protection against any harmful webpages and found the majority of them. It also protects against most leaks. Unfortunately, there is no kill switch feature and the real IP is not protected when the connection re-established.

Performance

Due to the nature of the technology, performance while using VPNs will always be lower than through an unsecured network. The reduction can vary greatly as seen in the following graphs.

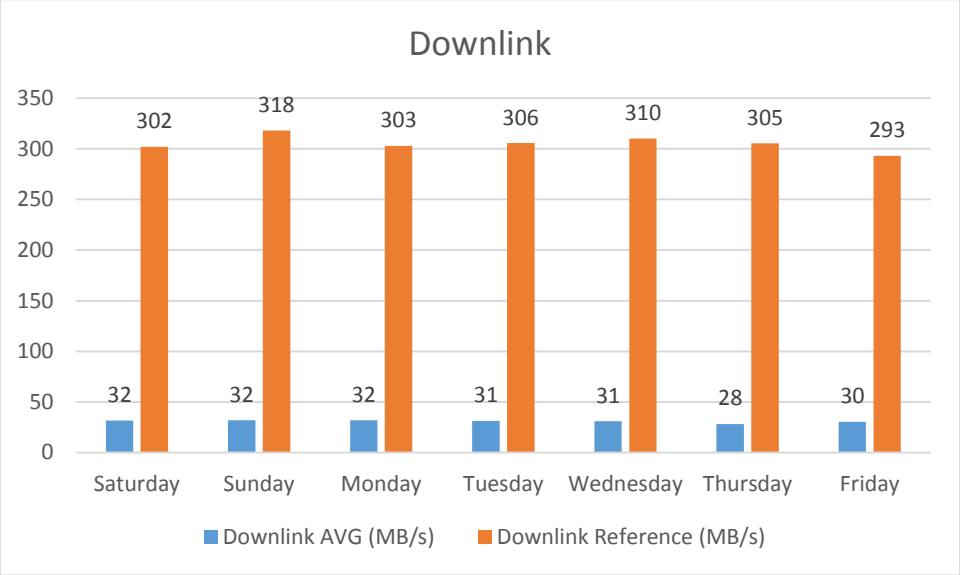

Figure 1: The average download speed in MB/s for VPN compared with a direct connection.

The difference for download speed between secured and unsecured connection ("Reference") is huge, with the download speed being around 10 times as high as the average VPN connected download performance.

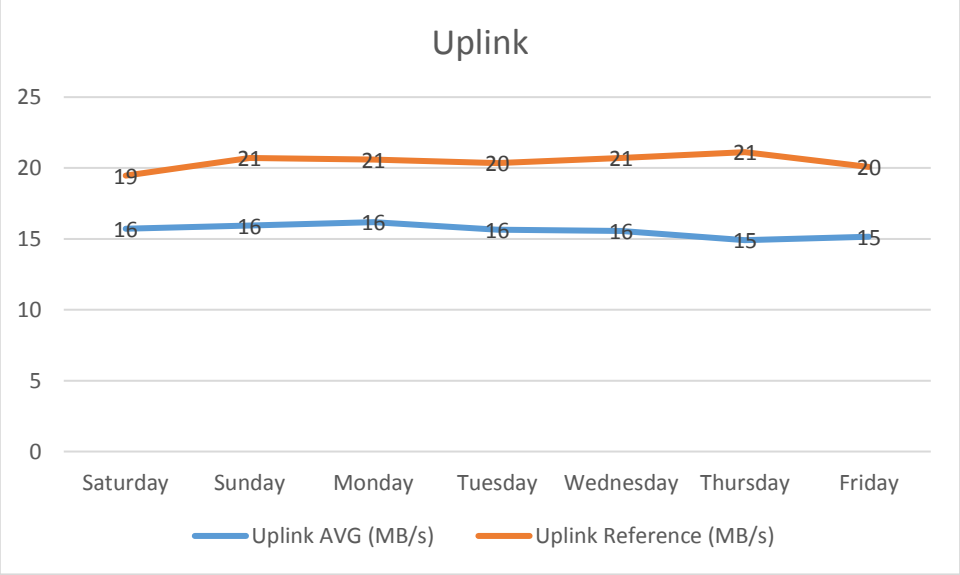

Figure 2: The average uplink speed in MB/s for VPN compared with a direct connection.

As seen in the previous graph, not all performance losses are as significant as observed for the download speed. The upload speed is only decreased by about a quarter and perceived performance reductions can be minimal.

Latency

Latency is the time it takes for a data packet to reach the server. Higher distances between the user device and the server location will result in a higher latency. So a lower latency will result in a speedier perceived connection. Also, a low latency is required to provide consistently fast uploads.

To create equal test cases for all tested products, not the optimal VPN connection suggested by the product was used but instead the VPN servers are manually chosen to be similar for all products. As default location in the US the west coast location was chosen if available and for the EU location always London or the UK.
VPN connections don't just connect from the users EU machine to an EU server through a European placed VPN server but also included more extreme cases such as an EU user connecting to another EU server through a US-based VPN server. This means the connection travels the Atlantic twice.

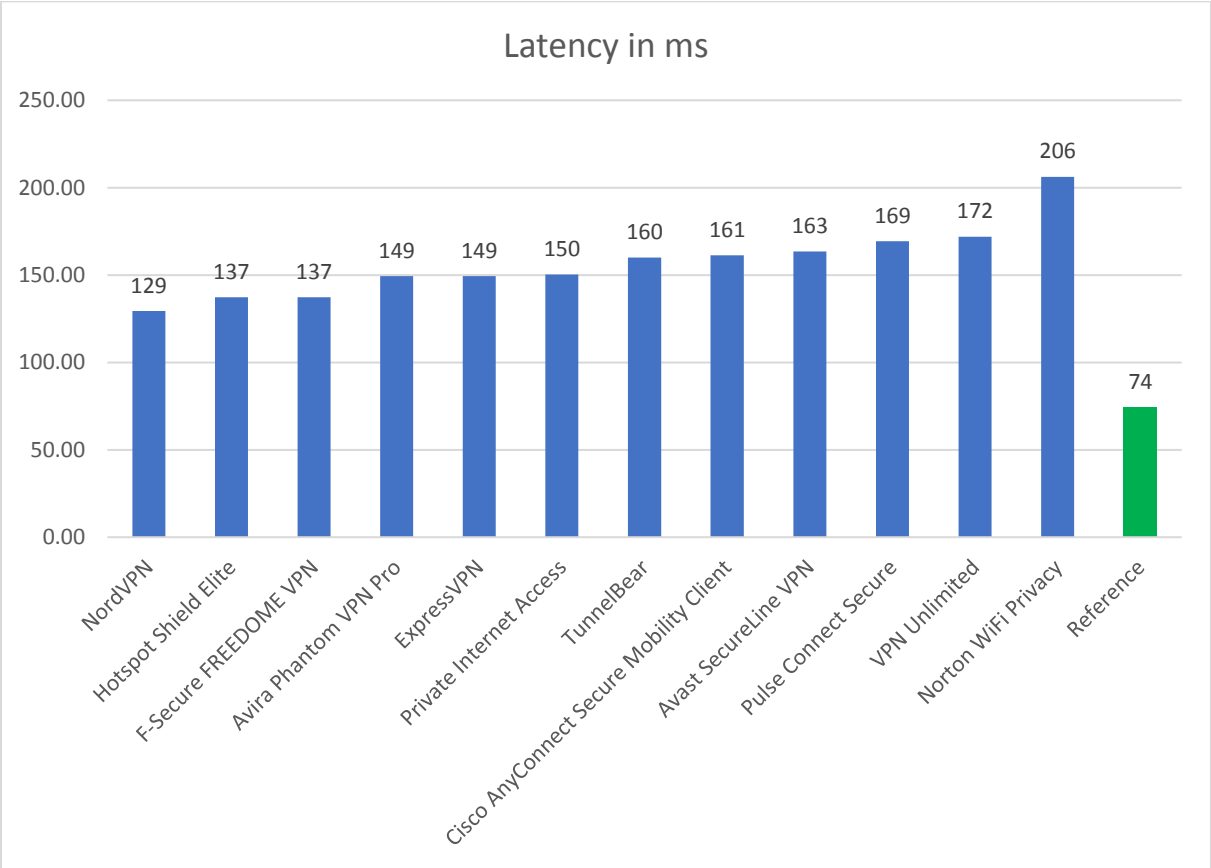

Figure 3: The latency in ms for all week for encrypted and direct network connections.

The graph shows the average latency per week for all product. There has been no great difference seen between SSL encrypted connections and those not encrypted by SSL. As a result, all averages were combined to get the overall results. As seen, the fastest VPN connection takes twice as long to reach the designated server as the reference. NordVPN performs best followed by a close second in Hotspot Shield Elite and F-Secure FREEDOME VPN. It should be noted that Norton WiFi Privacy had by far the slowest result almost three times slower than the reference.

Stream

A good transfer rate is vital for fluent and clear streaming enjoyment. In the performed tests there were no perceived issues when playing the 4k video content. Yet when measuring and looking at the numbers there are significant differences in performances.

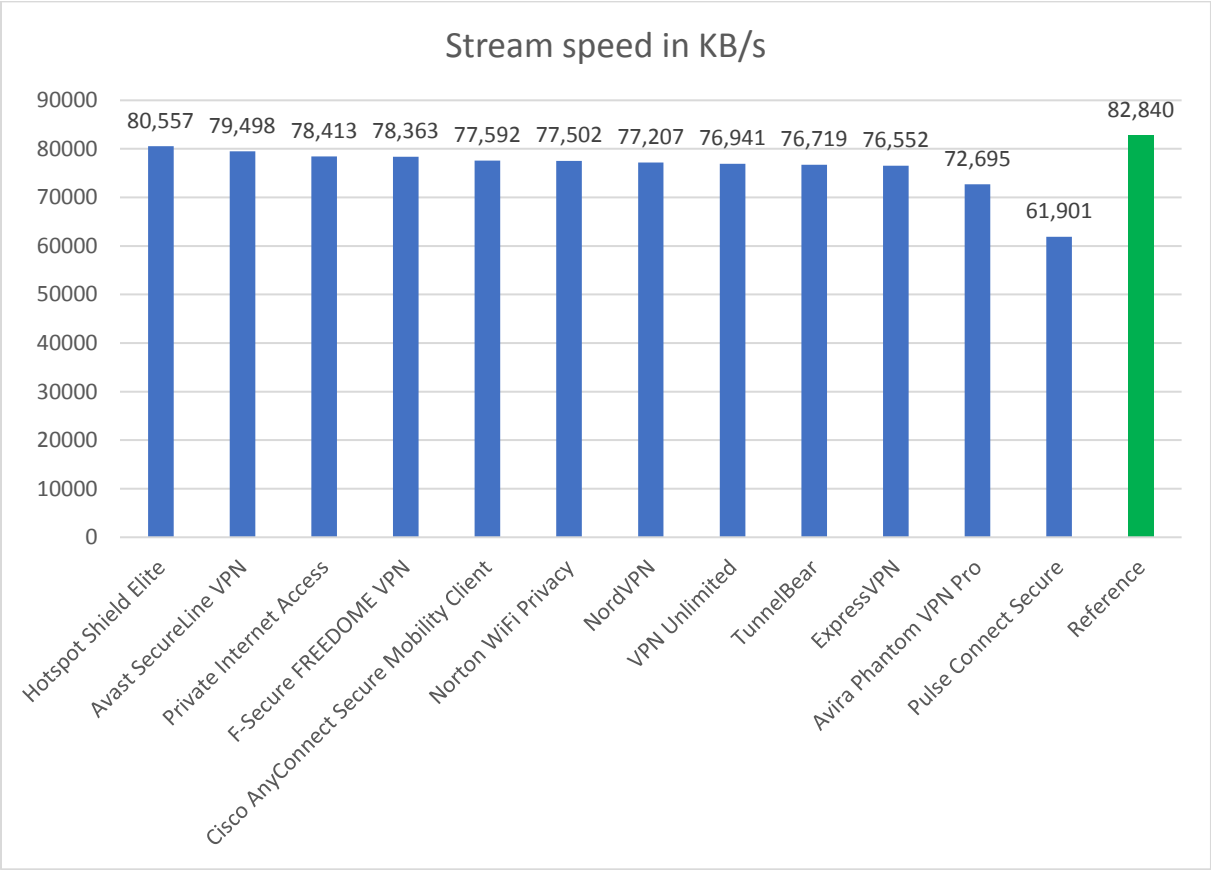

Figure 4: The stream speed in KB/s for all week for encrypted and direct network connections.

Unlike some other performance test results, there are no great differences between the speed measured for the VPN connections and the reference. In fact, the performance difference between the first placed VPN product Hotspot Shield Elite is similar to the difference between the first placed and the fifth-placed Cisco AnyConnect Secure Mobility Client. What stands out are the differences for Avira Phantom VPN Pro to the other products and even more though Pulse Connect Secure with only 75% of the performance reached by the top products.

Torrent

Many users decide to use a VPN to hide their identity when using P2P services. There are several reasons for that. Some ISPs might block or limit the torrent protocol. Others fear they might get notices from intellectual property right holders. Being able to use torrent and have a decent download speed when doing so can be a very different experience.

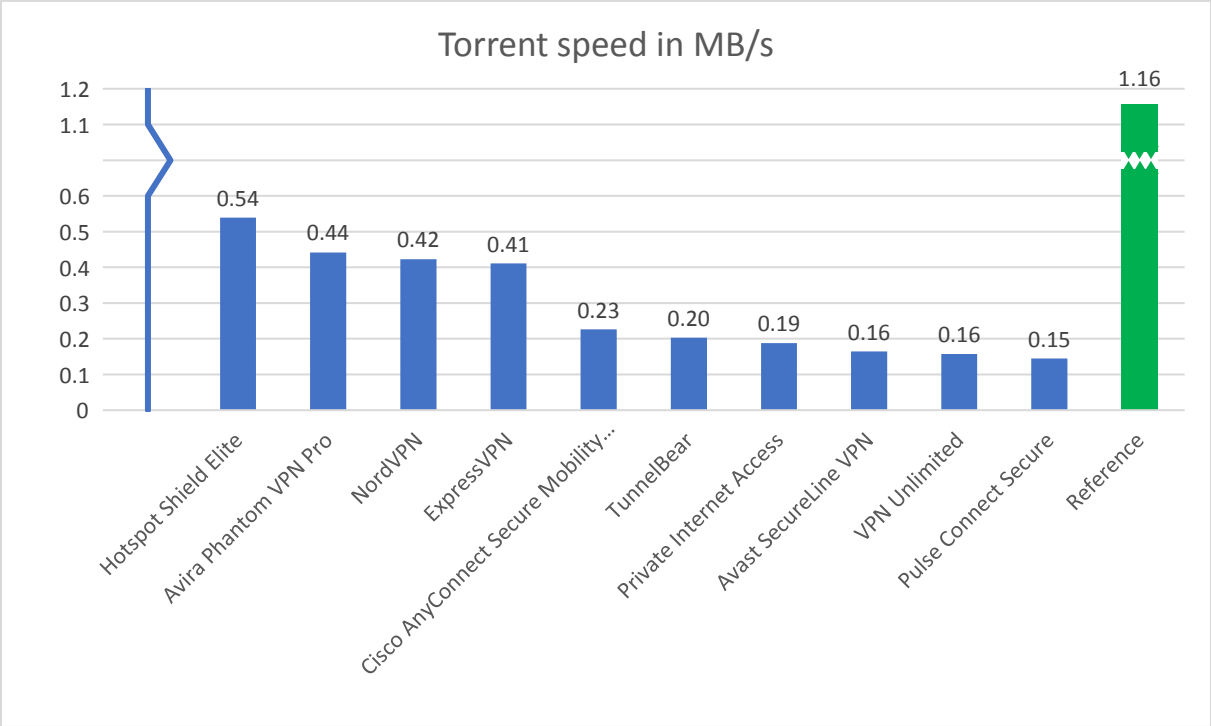

Figure 5: The torrent speed in MB/s for all week for encrypted and direct network connections.

The torrent performance results can be separated into three categories. First being Hotspot Shield Elite as it is 20% faster than the next group of products at about half the speed as the direct yet unsecured reference connection. Avira Phantom VPN Pro, NordVPN and ExpressVPN still provide very acceptable performances with about a third of the direct connection. The remaining products are significantly lower in speed with half the speed of the second group and the direct connection being six times faster.

Downlink

The download speed directly influences the speed content from the internet is transferred to the users' device and is the most sought-after reference when it comes to VPN network performance. It directly influences how fast the user will be able to open webpages, access mobile apps or just generally download content. With increasing bandwidth available for more people around the world it can be expected that this will show the biggest difference between using a VPN connection and using the direct connection. The VPN servers will have to deal with requests from users who are used to very fast downlink speeds.

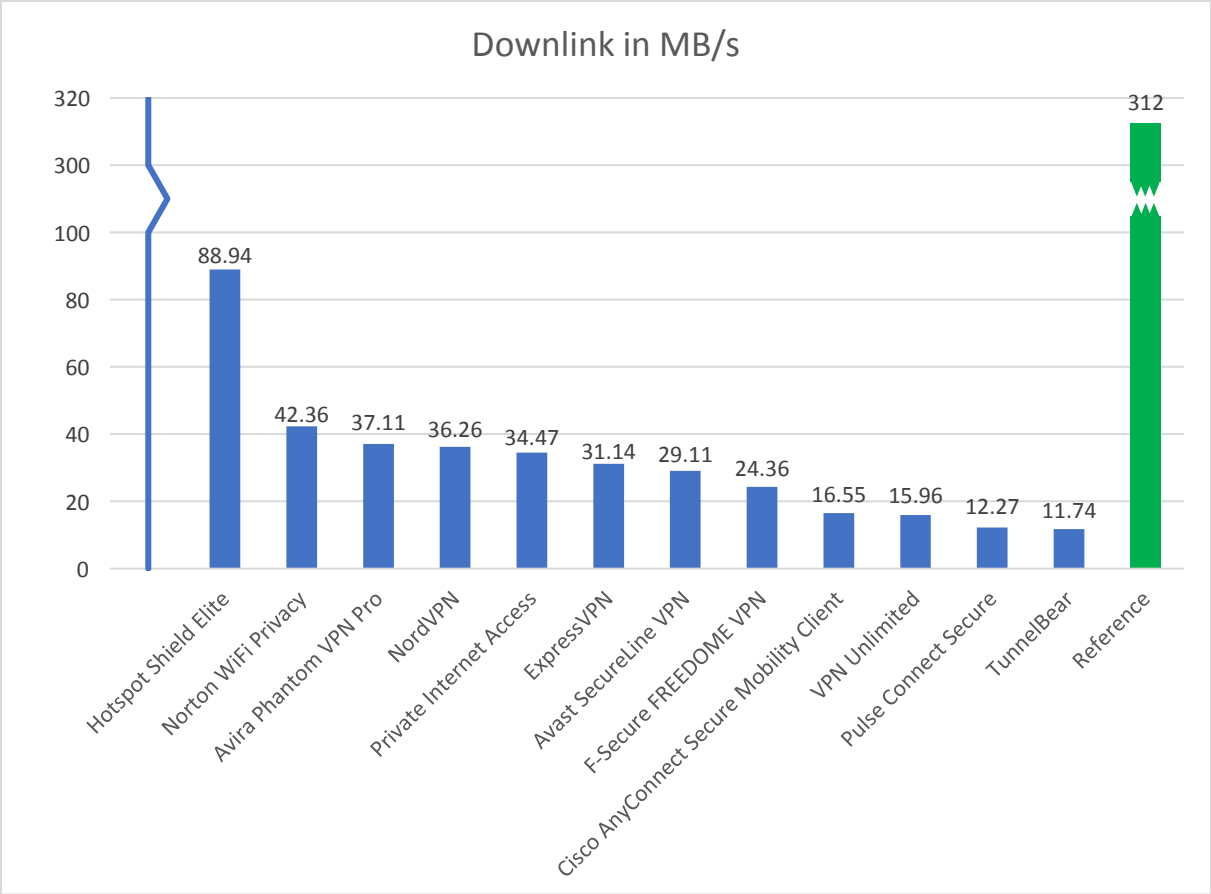

Figure 6: The downlink in MB/s for all week for encrypted and direct network connections.

As seen in Figure 6 there is no VPN getting even close to the average performance achieved through a direct connection. Best ranked among VPNs is Hotspot Shield Elite with the speed of about a third of the direct connection. The runner-up is Norton WiFi Privacy with less than half the speed of the top product. A clear ranking emerges from the table. Even if Norton WiFi Privacy, Avira Phantom VPN Pro, NordVPN and Private Internet Access are not nearly as fast as Hotspot Shield Elite they still outperform the bottom of the table such as Pulse Connect Secure or TunnelBear by about 300%.

Uplink

The upload speed relates to the speed data is sent from the user to the servers placed in the internet. The performance influences how fast the user can use cloud services, upload backups, host servers or in general share information through for example social media.

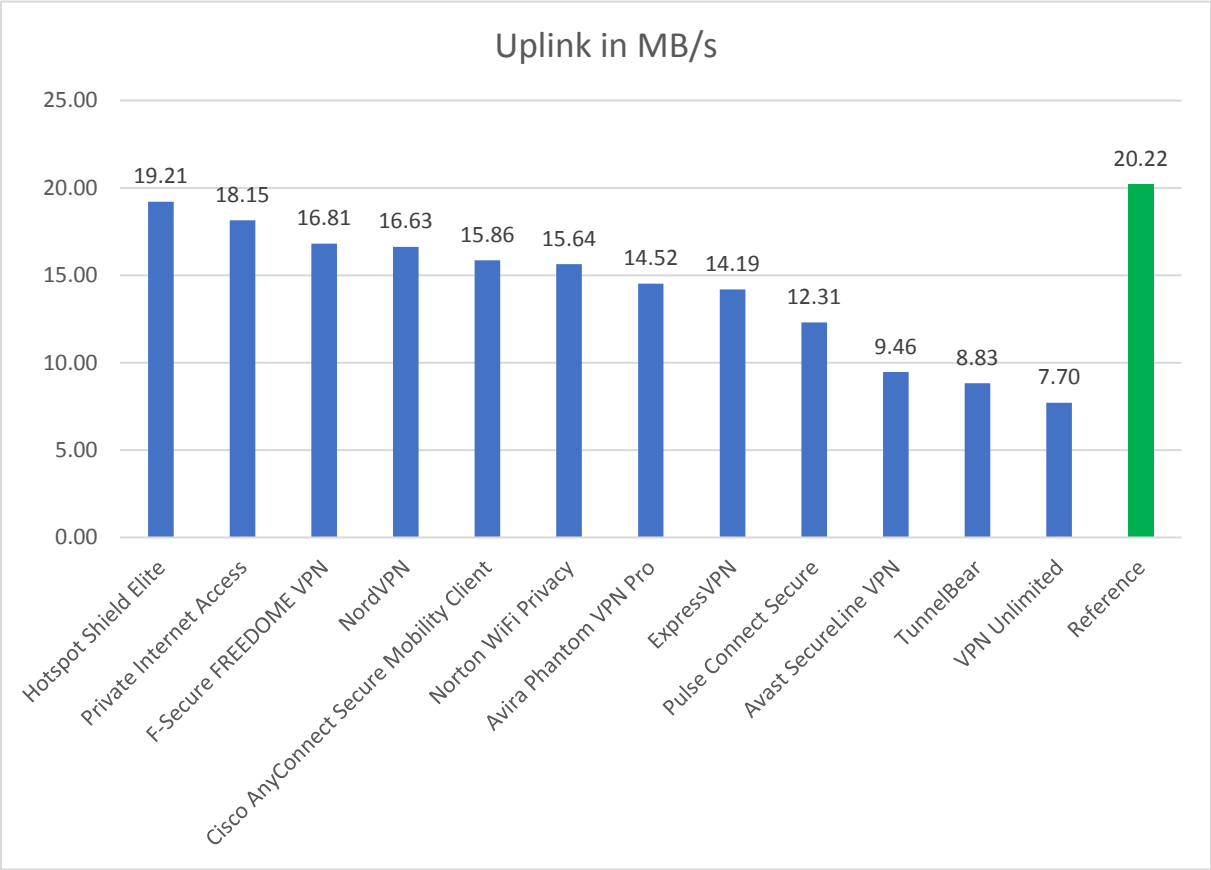

Figure 7: The uplink in MB/s for all week for encrypted and direct network connections.

The differences between the top VPN products and the reference uplink is almost neglectable. In the case of Hotspot Shield Elite, the difference is only around 5%, for Private Internet Access it is 10% and for the third places F-Secure FREEDOME VPN and NordVPN 15%. At the bottom of the ranking, there are VPN Unlimited with a third of the speed achieved by the reference. Only slightly better are TunnelBear and Avast SecureLine VPN still with less than half the speed of the reference.

Summary Performance

The performance speed is a crucial data point reviewed when making the decision on which VPN to choose. The tests didn't use the optimal connection but instead connections where chosen so all VPN servers where situated in similar VPN location. This will result in some variations to results observed in a non-testing environment because some servers might be more suited for the location of the test devices than others.

Most products for the majority of the tests provide similar and consistent results. There are some exceptions some products break-in in one category yet perform average or even above average in another tested category.

Hotspot Shield Elite performed consistently in all tests and came first in all but one category where they came second. They didn't just perform well in the downlink and torrent test but exceptional compared to the other tested products. Also, in the stream and uplink test they came close to performing at reference level.

Runner-up is Private Internet Access followed by a close NordVPN. Private Internet Access disappointed for the torrent speed but was in general slightly better than NordVPN which convinced most with its latency results.

More detailed breakdown of the results for the geographical and VPN-server location can be found in the appendix.

Features

Licensing

The licensing varies greatly. All products except for TunnelBear offer some sort of trial through money back guarantee. The money back period is usually 30 days but it can also be as low as 7 days for Private Internet Access and VPN Unlimited or up to 60 days for Norton WiFi Privacy or Hotspot Shield Elite.

More comfortable is a simple “press-trial-option” which allows a trial period without having to go through the process of providing some form of financial details, such as offered by most products with some limitations on time or bandwidth. Not offering such service are Avast SecureLine VPN, ExpressVPN and Private Internet Access.

Prices and Payment

The price depends on the subscription length number of devices used and if it is a desktop or mobile device.
If only a one month license is required or desired there are reasonable prices options such as Norton WiFi Privacy for one device 4.99$ or Avira Phantom VPN Pro 10$ for an unlimited amount of devices.
For a one year licence, the prices are between 39.95$ for five Private Internet Access devices and 99.95$ for three ExpressVPN devices.
Hotspot Shield Elite and VPN Unlimited offer a lifetime subscription for five devices for 119.99$ and 149.99$ respectively.

All products allow payment by credit card, which is probably one of the most convenient ways but not necessarily the one providing the best privacy. ExpressVPN, VPN Unlimited and to some degree Avira Phantom VPN allow payment through bitcoin. NordVPN, Private Internet Access and TunnelBear also allow payment through bitcoin but also offer a wider variety of payment options for cryptocurrencies. Hotspot Shield doesn’t offer the anonymous cryptocurrency option but does allow payment through 80 different gift cards in the US.

More details and prices, licences and payment methods are found in the related appendix table.

No details available for Cisco AnyConnect Secure Mobility Client and Pulse Connect Secure.

Compatibility

All tested products support Windows, Android and iOS. MacOS can be used by all products except by Cisco AnyConnect Secure Mobility Client. Just over half the products claim to support Linux, those are ExpressVPN, NordVPN, Private Internet Access, Pulse Connect Secure, TunnelBear and VPN Unlimited. Also, only about half the products offer an option for manual setup on devices such as routers those are Cisco AnyConnect Secure Mobility Client, ExpressVPN, NordVPN, Private Internet Access, Pulse Connect Secure and VPN Unlimited.
With NordVPN and Private Internet Access there are two more products even offering the option of using socks5 proxies.

Location of servers

The location of the servers is crucial for the working of a VPN. In order to circumvent geo-restrictions and access, local content servers need to be located in those areas. To provide the user with a fast and stable connection enough resources in form of servers need to be allocated.

The countries with VPN servers range from 20 for TunnelBear up to 94 for ExpressVPN distributed over 148 location in those countries. The number of servers claimed to be available are between 400+ for VPN Unlimited and 4267 for NordVPN. Except for Hotspot Shield Elite, all products offered the option to connect with an optimal VPN server.

NordVPN was the only product in the test that supports the possibility of multihop cascading. That is with predefined hops only.
No details available for Cisco AnyConnect Secure Mobility Client and Pulse Connect Secure.

Logging

A no logging policy is important to almost all users just by nature of a VPN user. Almost all tested products claim that no logs are saved. This really means “no personal data”. This statement varies greatly in its meaning. All products supply some more information on what they mean by “no logging”. The logging of data can result from various limitations vendors are constrained by, like complying with national laws, limitations of the number of devices, implementing features such as ad- or malware blocker, placing personalised ads and processing payments.

It is a good idea to look at the details of what data is stored and what isn’t by each user individually for their own preferences. Except for Avast SecureLine VPN and Avira Phantom VPN Pro we found dedicated terms of use for each product. It is not just about what data is stored but also for how long. Avast SecureLine VPN stores data for 30 days, F-Secure FREEDOME VPN for 90 days and Pulse Connect Secure for as long the account is active.

Protocol and encryption

It is very important what sort of tunnelling protocol is used when transmitting the data. The two main aspects are security with privacy and performance. The protocols consider to provide the best security are OpenVPN, IKEv2 combined with IPSec, SSTP and, if ignoring doubts spread by Edward Snowden, L2TP in combination with IPSec. Almost all tested products support a secure protocol which is usually OpenVPN. Also, almost all products provide a 256-bit AES data encryption, which is mostly set to default except for Private Internet Access and Pulse Connect Secure.

Hotspot Shield Elite is the main exception to the default protocols. They use their own in-house developed protocol Catapult Hydra, which they claim provides much better performance which has been confirmed in the performance test of this report. Unlike OpenVPN, the Catapult Hydra protocol it is not open source and therefore has not been independently reviewed by us but assumed secure until proven otherwise. According to Hotspot Shield, Catapult Hydra it is used by a large number of security vendors worldwide who trust it enough to use it to provide wireless security to their mobile device customers.

For this test, only the protocols for windows are reviewed. The other operating system protocols are included in the appendix table when the information is freely provided by the vendors.
No details available for Pulse Connect Secure.

Blocking

Ads and trackers can compromise the users' privacy and threaten the security. This can be resolved by the user in the browser with additional add-ons. But some VPN providers also offer solutions. NordVPN provides CyberSec which can block ads when activated. F-Secure FREEDOME VPN and Norton WiFi Privacy offer the option to block trackers. Private Internet Access MACE can block ads and trackers. Furthermore, when we tested MACE, the anti-ad-blocker features of the webpage did not block the ad-blocker. Hotspot Shield Elite and TunnelBear provide a chrome add-on to block advertisement and trackers.

Additional

Unlimited bandwidth with no throttling is the norm for VPNs Except for Cisco AnyConnect Secure Mobility Client and Norton WiFi Privacy for which no information is available and for Pulse Connect Secure which limits the bandwidth to 50%, 75%, 90% or 100%.

Video streaming was no issue with any of the products. All provided sufficient performance to provide continues uninterrupted streaming experience of HD content. Hotspot Shield Elite, NordVPN and VPN Unlimited also allow the circumvention of several geo-locked streaming content.

Except for Norton WiFi Privacy, it is possible to torrent with all tested products. Although, some of them like F-Secure FREEDOME VPN and TunnelBear require connection with dedicated servers.

The support for IPv6 is still limited to Avira Phantom VPN Pro and F-Secure FREEDOME VPN. NordVPN claims it will be available at some point in 2018.

Summary Features

When deciding on the extent of features and options available in VPN products it boils down to individual preferences and needs. Some products have almost all that can be desired from a VPN and they distinguish themselves from the crowd. NordVPN, Private Internet Access or VPN Unlimited provide features such as multihop cascading, malware- and ad-blocker, a huge number of servers or the possibility to circumvent geo-blocked streaming content. Other solutions such as F-Secure FREEDOME VPN or Hotspot Shield Elite don't provide the same range of features but they do offer malware and phishing protection and are sufficiently equipped to cater all security and privacy needs for the user while also being easy and comfortable to use.

Summary

The test reviewed the four test categories usability, privacy and security, performance and features.

In the usability test, the results were pretty balanced. Setup and usage are usually straightforward. Differences emerge when looking at available languages and a provided tutorial which some users may feel might be overkill for such intuitive programs. Other differences can be found for auto reconnect after the system start, a feature which only has relevance for desktop devices.
In first place with equal scoring are AnchorFree's Hotspot Shield Elite, Avast SecureLine VPN and F-Secure FREEDOME VPN followed by Norton WiFi Privacy, Private Internet Access, NordVPN, TunnelBear, Avira Phantom VPN Pro, ExpressVPN, VPN Unlimited, Cisco AnyConnect Secure Mobility Client and Pulse Connect Secure at last place.

The main reason to use a VPN especially for home use is the privacy, anonymity and security aspect. No tested product failed in spectacular fashion. Some products didn't offer the kill switch function, and even some of those providing it failed the appropriate test.
ExpressVPN, F-Secure FREEDOME VPN, Hotspot Shield Elite and Private Internet Access all provide above average protection. Except for ExpressVPN, all these products provide some form of malware protection. F-Secure FREEDOME VPN was the only one not providing a kill switch feature.
The first four ranked products are almost equal in scoring. Those are Hotspot Shield Elite, F-Secure FREEDOME VPN, Private Internet Access and ExpressVPN followed by NordVPN, Cisco AnyConnect Secure Mobility Client, TunnelBear, Avira Phantom VPN Pro, Avast SecureLine VPN and at shared last place Norton WiFi Privacy, Pulse Connect Secure and VPN Unlimited.

The performance speed is a crucial data point reviewed when making the decision on which VPN to choose. There is no point in having a product with a hundred features but a connection speed too slow to use it effectively. Far outperforming all other products was Hotspot Shield Elite in the categories downlink and torrent speed and doing extremely well for testing in latency and downlink speed, getting a very comfortable first place. NordVPN was the only other product to claim a first place in this category which was in the latency test, putting it with some distance in third place only outperformed by Private Internet Access which also showed very good overall results.
Ranked first is unsurprisingly Hotspot Shield Elite followed by Private Internet Access, NordVPN, F-Secure FREEDOME VPN, Avira Phantom VPN Pro, ExpressVPN, Cisco AnyConnect Secure Mobility Client, Avast SecureLine VPN, Norton WiFi Privacy, TunnelBear, VPN Unlimited and Pulse Connect Secure.

Extensive features apart from what can be considered default requirements are provided by NordVPN, Private Internet Access or VPN Unlimited. For an everyday user who just wants to open, connect and forget, who doesn't require more advanced features F-Secure FREEDOME VPN or Hotspot Shield Elite will suffice.
The ranking is NordVPN at the top closely followed by Private Internet Access and with almost no difference VPN Unlimited followed by ExpressVPN, F-Secure FREEDOME VPN, Hotspot Shield Elite, Avira Phantom VPN Pro, TunnelBear, Avast SecureLine VPN, Norton WiFi Privacy, Cisco AnyConnect Secure Mobility Client, Pulse Connect Secure.

Conclusion

With its seconds to none showing in the performance test, Hotspot Shield Elite make it hard for a user to see past this VPN solution. Also taking the top of the security and usability placing as well as providing for all essential needs of the VPN users. Hotspot Shield Elite provides a comprehensive VPN product which came first in the overall testing.
The objective of the here-presented tests was to assess the products' completeness as a VPN application providing security and performance. Indeed, the Hotspot Shield Elite product delivered convincing results across all tests as well as providing some useful additional features such as malware and phishing website protection. What also makes it stand out is a 45 days money return guarantee as well as the possibility to try it as an unlimited ad-supported free version.

Private Internet Access took second place in the security test by providing excellent leak protection, combined with its well working kill switch and the ability to block at least some malicious websites. An overall a very good product, with competitive pricing, support for most common payment methods and support for all possible devices and operating systems. Even though it came second in the performance testing it didn't come close to the first placed product.

NordVPN impressive features list put it in the top list of VPN choices. It achieved the highest scoring for features provided. It was also the only product providing the multihop cascading feature for increased anonymity. NordVPN came close third in the performance test just been beaten by Private Internet Access. More than 4000 servers in 62 countries provide reliability and consistent performance for active connections. The security provided is solid but could be extended by fixing the WebRTC leak and the leaking of the local network IP. NordVPN claims to be able to provide a malware protection and ad-blocking. unfortunately, the malware blocking didn't play out in the conducted testing.

When listing the top tested products F-Secure FREEDOME VPN should not be missing. With no leaks detected and best detection for malware and phishing sites, only one product convinced more in terms of security. Like Hotspot Shield Elite it is a two click install, two clicks activate application which makes it ideal for novice users. It is available in 20 languages, supports ipv6 as one of only two tested VPNs.

Appendix

Hardware Specifications

Windows

Operating system	Windows 10 Pro Version 1709 OS Build 16299.309 with all patches available in April 2018.
Cloud VM-hoster	Microsoft Azure, EAST US Microsoft Azure, West Europe
Hardware	• Intel Xeon CPU E5-2673 v4 @ 2.30GHz • 16 GB RAM • 50GB free Space
Installed applications	• Chrome Browser 66.0.3359.139 (64-bit) • µTorrent torrent client 3.5.3 (build 44396) [32-bit]

Performance Test Server Locations

Below are sets of CloudHarmony test links for selected combinations of client and server locations. Each link is tested with both, http:// and https://.

VPN client: US; VPN server: US

cloudharmony.com/speedtest-downlink-uplink-latency-for-azure:compute-us-west2
cloudharmony.com/speedtest-downlink-uplink-latency-for-aws:ec2-us-west-2
cloudharmony.com/speedtest-downlink-uplink-latency-for-google:compute-us-west1

VPN client: US; VPN server: EU

cloudharmony.com/speedtest-downlink-uplink-latency-for-azure:compute-eu-west
cloudharmony.com/speedtest-downlink-uplink-latency-for-aws:ec2-eu-central-1
cloudharmony.com/speedtest-downlink-uplink-latency-for-google:compute-europe-west3

VPN client: EU; VPN server: EU

cloudharmony.com/speedtest-downlink-uplink-latency-for-azure:compute-eu-west
cloudharmony.com/speedtest-downlink-uplink-latency-for-aws:ec2-eu-central-1
cloudharmony.com/speedtest-downlink-uplink-latency-for-google:compute-europe-west3

VPN client: EU; VPN server: US

cloudharmony.com/speedtest-downlink-uplink-latency-for-azure:compute-us-east
cloudharmony.com/speedtest-downlink-uplink-latency-for-aws:ec2-us-east-1
cloudharmony.com/speedtest-downlink-uplink-latency-for-google:compute-us-east4

Test Results

Performance Test Results

Further in-depth details available upon request at AV-TEST.

Latency

Products	Geo location EU VPN location EU in ms	Geo location EU VPN location US in ms	Geo location US VPN location EU in ms	Geo location US VPN location US in ms	Average in ms
Avast SecureLine VPN	63.75	311.73	146.72	131.51	163.43
Avira Phantom VPN Pro	55.49	271.76	137.25	132.77	149.32
Cisco AnyConnect Secure Mobility Client	56.76	306.47	147.85	134.37	161.36
ExpressVPN	51.30	130.60	279.39	136.03	149.33
F-Secure FREEDOME VPN	47.17	252.12	122.73	127.02	137.26
Hotspot Shield Elite	57.37	250.45	109.06	131.99	137.22
NordVPN	49.56	126.49	145.00	196.51	129.39
Norton WiFi Privacy	81.04	363.10	191.07	189.35	206.14
Private Internet Access	56.57	266.73	130.37	147.57	150.31
Pulse Connect Secure	56.81	318.92	151.86	149.71	169.32
TunnelBear	76.52	254.92	152.33	156.61	160.10
VPN Unlimited	72.23	314.47	148.76	152.27	171.93
Reference	25.68	n/a	122.97	n/a	74.33

n/a - not applicable, no VPN connection establish only direct connection is measured ones

Stream

The stream speed test was performed with a dedicated streaming test site in the Chrome browser. Unfortunately, during the test period, a Chrome browser update was released which changed the working of the test page and the testing automatism had to be changed, which resulted in an overall performance drop after the first two test days.

Products	Geo location EU VPN location EU in KB/s	Geo location EU VPN location US in KB/s	Geo location US VPN location EU in KB/s	Geo location US VPN location US in KB/s	Average in KB/s
Avast SecureLine VPN	82461	74608	79086	81835	79498
Avira Phantom VPN Pro	73610	70330	73643	73196	72695
Cisco AnyConnect Secure Mobility Client	80172	73159	78626	78411	77592
ExpressVPN	74674	75851	80795	74887	76552
F-Secure FREEDOME VPN	77983	76982	77652	80834	78363
Hotspot Shield Elite	81296	81296	81312	78326	80557
NordVPN	74743	82144	77700	74241	77207
Norton WiFi Privacy	75706	73266	81308	79727	77502

Private Internet Access	79098	72465	82844	79243	78413
Pulse Connect Secure	55673	65386	62827	63718	61901
TunnelBear	73986	74688	77149	81054	76719
VPN Unlimited	77626	75939	78231	75971	76941
Reference	82734	n/a	82947	n/a	82840

n/a - not applicable, no VPN connection establish only direct connection is measured ones

Torrent

There were no dedicated torrent servers available for the testing regions for the EU for F-Secure FREEDOME VPN and TunnelBear as well as for the US for F-Secure FREEDOME VPN.
Norton WiFi Privacy is excluded as it does not support the torrent protocol.

Products	Geo location EU VPN location EU in MB/s	Geo location EU VPN location US in MB/s	Geo location US VPN location EU in MB/s	Geo location US VPN location US in MB/s	Average in MB/s
Avast SecureLine VPN	0.21	0.14	0.14	0.17	0.16
Avira Phantom VPN Pro	0.55	0.41	0.36	0.45	0.44
Cisco AnyConnect Secure Mobility Client	0.29	0.19	0.22	0.21	0.23
ExpressVPN	0.56	0.40	0.35	0.33	0.41
F-Secure FREEDOME VPN	-	-	-	-	-
Hotspot Shield Elite	0.47	0.46	0.64	0.59	0.54
NordVPN	0.53	0.37	0.35	0.44	0.42
Private Internet Access	0.18	0.15	0.15	0.27	0.19
Pulse Connect Secure	0.16	0.13	0.15	0.14	0.15
TunnelBear	-	0.19	-	0.22	0.20
VPN Unlimited	0.25	0.11	0.15	0.11	0.16
Reference	1.00	n/a	1.31	n/a	1.16

n/a - not applicable, no VPN connection establish only direct connection is measured ones

Downlink

Products	Geo location EU VPN location EU in MB/s	Geo location EU VPN location US in MB/s	Geo location US VPN location EU in MB/s	Geo location US VPN location US in MB/s	Average in MB/s
Avast SecureLine VPN	61	9	24	22	29
Avira Phantom VPN Pro	66	19	27	36	37
Cisco AnyConnect Secure Mobility Client	37	4	12	12	17
ExpressVPN	50	32	17	25	31
F-Secure FREEDOME VPN	54	13	14	16	24
Hotspot Shield Elite	118	75	90	73	89
NordVPN	68	32	24	22	36

Norton WiFi Privacy	60	21	33	55	42
Private Internet Access	77	12	27	21	34
Pulse Connect Secure	28	4	9	9	12
TunnelBear	29	5	7	6	12
VPN Unlimited	29	6	12	17	16
Reference	357	n/a	268	n/a	312

n/a - not applicable, no VPN connection establish only direct connection is measured ones

Uplink

Products	Geo location EU VPN location EU in MB/s	Geo location EU VPN location US in MB/s	Geo location US VPN location EU in MB/s	Geo location US VPN location US in MB/s	Average in MB/s
Avast SecureLine VPN	17.28	3.17	8.52	8.88	9.46
Avira Phantom VPN Pro	13.93	11.99	15.67	16.51	14.52
Cisco AnyConnect Secure Mobility Client	15.26	12.70	17.83	17.66	15.86
ExpressVPN	15.49	13.54	14.24	13.49	14.19
F-Secure FREEDOME VPN	17.29	16.39	16.20	17.37	16.81
Hotspot Shield Elite	18.29	15.86	21.38	21.29	19.21
NordVPN	16.70	16.86	18.64	14.33	16.63
Norton WiFi Privacy	16.80	10.78	19.29	15.70	15.64
Private Internet Access	18.14	13.09	21.24	20.15	18.15
Pulse Connect Secure	11.88	10.50	13.53	13.35	12.31
TunnelBear	14.52	4.94	7.79	8.07	8.83
VPN Unlimited	12.66	3.21	6.74	8.20	7.70
Reference	17.85	n/a	22.58	n/a	20.22

n/a - not applicable, no VPN connection establish only direct connection is measured ones

Features Test Results

The features described in the following table and described in the report have been taken as provided information from the vendors or trusted third parties. They may not reflect the actual availability or functionality due to a lack of more information.

Licensing

Products	Trial period in days	Number of devices per license	Money back guarantee
Avast SecureLine VPN	-	5	30
Avira Phantom VPN Pro	free version (max 500MB/month)	unlimited	30
Cisco AnyConnect Secure Mobility Client	nip	nip	nip
ExpressVPN	-	3	30
F-Secure FREEDOME VPN	5	3 / 5 / 7	30

Hotspot Shield Elite	Free (with ads)	5	45
NordVPN	3	6	30
Norton WiFi Privacy	7 (android only)	1 / 5 / 10	60
Private Internet Access	-	5	7
Pulse Connect Secure	nip	nip	nip
TunnelBear	7, free version (max 500MB/month)	5	-
VPN Unlimited	7	5	7

nip - No information provided

Prices and Payment

Prices and payment options may differ on the location of purchase, country the products site is accessed from and currently available offers for the products.

Products	1 Month license	1 Year license	Unlimited license	Payment Methods Paypal / Bank Transfer / Bitcoins / DebitCard / Credit card
Avast SecureLine VPN	Desktop 1 device 5.99$ (5.99€), Android, iOS 5 devices 2.99$ (2.99€)	Desktop 1 device 59.99$ (59.99€), 3 devices 69,99$ (69,99€), 5 devices 79.99$ (79.99€), Android, iOS 5 devices 19.99$ (19.99€)	-	+ / +* / - / - / +
Avira Phantom VPN Pro	Desktop 7.99€ (10.00$) Android, iOS 4.95€	Desktop 59.95€ (78.00$)	-	+ / + / +** / - / +
Cisco AnyConnect Secure Mobility Client	nip	nip	nip	nip
ExpressVPN	12.95$	99.95$	-	+ / + / + / - / +
F-Secure FREEDOME VPN	-	3 devices 49.99$ (49.90€) 5 devices 59.99$ (59.90€) 7 devices 79.99$ (79.90€)	-	+ / + / - / +* / +
Hotspot Shield Elite	5.99$ (15.99€)	71.88$ (83.99€)	119.99$ (139.99€)	+ / - / - / + / +
NordVPN	11.95$ (11.95€)	69.00$ (69.00€)	-	+ / + / + / - / +
Norton WiFi Privacy	1 devices 4.99$ 5 devices 7.99$ 10 devices 9.99$	1 device 39.99$ (49.99€) 5 devices 39.99$ (29.99€) 10 devices 59.99$ (69.99€)	-	+ / +* / - / - / +

Private Internet Access	6,95$	39.95$	-	+ / + / + / + / +
Pulse Connect Secure	nip	nip	nip	nip
TunnelBear	9.99$	59.99$	-	- / - / + / - / +
VPN Unlimited	9.99$	59.99$	149.99$	+ / + / + / + / +

nip - No information provided
* - Varies between US, EU and possibly individual states
** - Only available for one year subscription

Compatibility

Products	Additional supported OS, Win (XP/Vista/7/8) / Mac OS / iOS / Linux / Android	Option for manual setup available (installation through configuration)	Socks5 Proxy included
Avast SecureLine VPN	+ / + / + / - / +	nip	nip
Avira Phantom VPN Pro	+ / + / + / - / +	-	-
Cisco AnyConnect Secure Mobility Client	+ / - / + / + / +	+	-
ExpressVPN	+ / + / + / + / +	+	nip
F-Secure FREEDOME VPN	+ / + / + / - / +	-	nip
Hotspot Shield Elite	+ / + / + / - / +	-	-
NordVPN	+ / + / + / + / +	+	+
Norton WiFi Privacy	+ / + / + / - / +	nip	-
Private Internet Access	+ / + / + / + / +	+	+
Pulse Connect Secure	+ / + / + / + / +	+	-
TunnelBear	+ / + / + / + / +	-	nip
VPN Unlimited	+ / + / + / + / +	+	nip

nip - No information provided

Location of servers

Products	Number of countries with server (number virtual servers (VPS))	Number of server locations (actual server location)	Optimal Location selection provided	Possibility to use Multihop Cascading
Avast SecureLine VPN	33	52	+	-
Avira Phantom VPN Pro	25	36	+	-
Cisco AnyConnect Secure Mobility Client	nip	nip	nip	nip
ExpressVPN	94 (2000+ server)	148	+	-
F-Secure FREEDOME VPN	22	28	+	-
Hotspot Shield Elite	25 (2600 server)	nip	-	-
NordVPN	62 (4267 Server)	nip	+	+
Norton WiFi Privacy	28	nip	+	-
Private Internet Access	28 (3041)	45	+	-
Pulse Connect Secure	nip	nip	nip	nip
TunnelBear	20	nip	+	-
VPN Unlimited	52 (400+)	70	+	-

nip - No information provided

Logging

Products	No personal user data is logged	Time for which logged data is kept	Dedicated Terms of use
Avast SecureLine VPN	+	30 days	-*
Avira Phantom VPN Pro	+	nip	-*
Cisco AnyConnect Secure Mobility Client	+	nip	+
ExpressVPN	+	nip	+
F-Secure FREEDOME VPN	+	90 days	+
Hotspot Shield Elite	+	nip	+
NordVPN	+	nip	+
Norton WiFi Privacy	+	nip	+
Private Internet Access	+	nip	+
Pulse Connect Secure	-	as long the account is active	+
TunnelBear	+	nip	+
VPN Unlimited	+	nip	+

* - No dedicated terms of use. Terms of use for wider product range by the vendor

Protocol and encryption

Products	Available protocols	Used data encryption
Avast SecureLine VPN	OpenVPN on UDP (Windows), IPsec (Mac), PPTP (Android, iOS)	256-bit AES encryption
Avira Phantom VPN Pro	OpenVPN (Windows, Android), L2TP/IPsec (iOS, Mac)	256-bit AES encryption
Cisco AnyConnect Secure Mobility Client	Secure SSL and IPsec/IKEv2	256-bit AES encryption
ExpressVPN	OpenVPN (UDP or TCP), L2TP/IPsec, SSTP, PPTP	256-bit AES encryption
F-Secure FREEDOME VPN	OpenVPN (Windows, Android, Mac), IPsec (iOS)	256-bit AES encryption
Hotspot Shield Elite	Catapult Hydra	256-bit AES encryption
NordVPN	OpenVPN, IKEv2/IPsec, PPTP, L2TP/IPsec	256-bit AES encryption
Norton WiFi Privacy	OpenVPN (probably IKEv2 on iOS)	nip
Private Internet Access	OpenVPN (Windows, MacOS, Linux, iOS, Android rooted) , L2TP/IPSec and PPTP (Android, iOS)	128-bit AES encryption is default, 256-bit encryption available
Pulse Connect Secure	nip	128-bit AES encryption is default, 256-bit encryption available
TunnelBear	OpenVPN, IKEv2 (Windows, MacOS) OpenVPN (Android) IPSec/IKEv2 (iOS)	256-bit AES encryption
VPN Unlimited	OpenVPN (Android, Windows), IKEv2 (macOS, iOS)	128-bit and 256-bit AES encryption

nip - No information provided

Blocking

Products	Ads	Tracker	Malware
Avast SecureLine VPN	-	-	-
Avira Phantom VPN Pro	-	-	-
Cisco AnyConnect Secure Mobility Client	-	-	-
ExpressVPN	-	-	-
F-Secure FREEDOME VPN	-	+	+
Hotspot Shield Elite	+*	+*	+
NordVPN	+	-	+
Norton WiFi Privacy	-	+	-
Private Internet Access	+	+	+
Pulse Connect Secure	-	-	-
TunnelBear	+*	+*	-
VPN Unlimited	-	-	-

* - Available in Chrome browser with add-on

Additional

Products	No Bandwidth limitations	Support Video streaming / Circumvent some geo locks (US)	Support torrents	Support IPv6 addressing
Avast SecureLine VPN	+	+ / -	+*	-
Avira Phantom VPN Pro	+	+ / -	+	+
Cisco AnyConnect Secure Mobility Client	nip	+ / -	+	-
ExpressVPN	+	+ / -	+	-
F-Secure FREEDOME VPN	+	+ / -	+*	+
Hotspot Shield Elite	+	+ / +***	+	-
NordVPN	+	+ / +***	+	-**
Norton WiFi Privacy	nip	+ / -	-	-
Private Internet Access	+	+ / -	+	-
Pulse Connect Secure	-	+ / -	+	-
TunnelBear	+	+ / -	+*	-
VPN Unlimited	+	+ / +***	+	-

* - Through dedicated servers only
** - Announced for 2018
*** - Applies to tested streaming sites and may vary with content providers
nip - No information provided