VIRTUAL PRIVATE NETWORKS

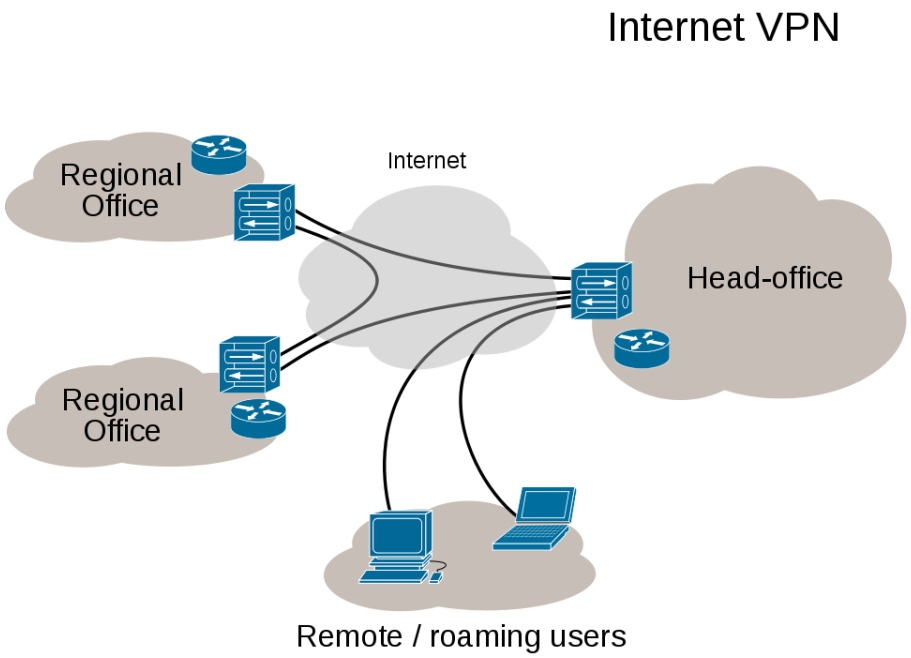
An elaboration by Christian Janeczek

Table of Contents

Definition

What exactly is a Virtual Private Network?

Virtual Private Networking itself allows you to connect to a remote offices' or organizations' internal LAN through a public telecommunication infrastructure such as the Internet. It provides secure access for remote offices or individual users to their organization's network, so to say. Not only does it provide access, it also ensures privacy through security procedures and Tunneling protocols such as the *Layer Two Tunneling Protocol (L2TP)*. Data is encrypted at the sending end and decrypted at the receiving end.



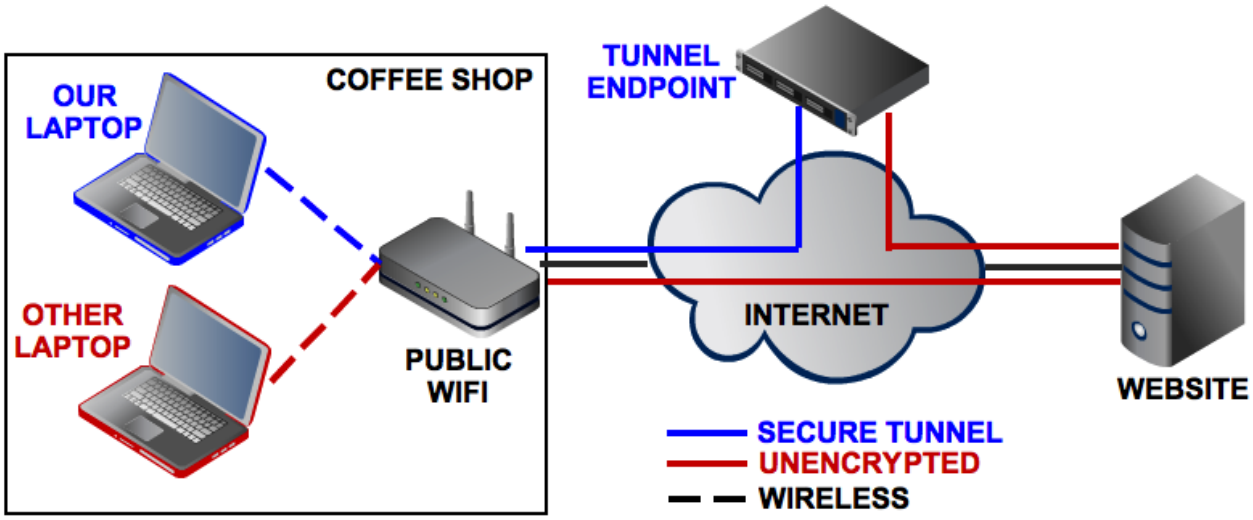
Why should you use a VPN?

There are at least four great reasons for using a Virtual Private Network and I am going to introduce and give you essential information about each of one them.

First, you can use it to connect securely to a remote network via the Internet. Most companies maintain VPNs so that employees can access files, applications, printers or just valuable data – the organization's important resources. You can also set up your own VPN to safely access your secure home network while you're on the road. So the ***Availability*** plays a very important role concerning the use of Virtual Private Networking and is one of its most advantageous features.

Second, and probably the most important aspect of a VPN is ***Security.*** Virtual Private Networks are particularly useful for connecting multiple networks together securely. For this reason, most

businesses rely on a VPN to share servers and other networked resources among multiple offices or stores across the globe. This little trick also allows connecting multiple home networks or other networks for personal use. The security is established via various Tunneling Protocols which I will come to later on in this very elaboration.



This diagram illustrates the difference between using an unencrypted connection and using a VPN-secured Internet connection at your average coffee shop.

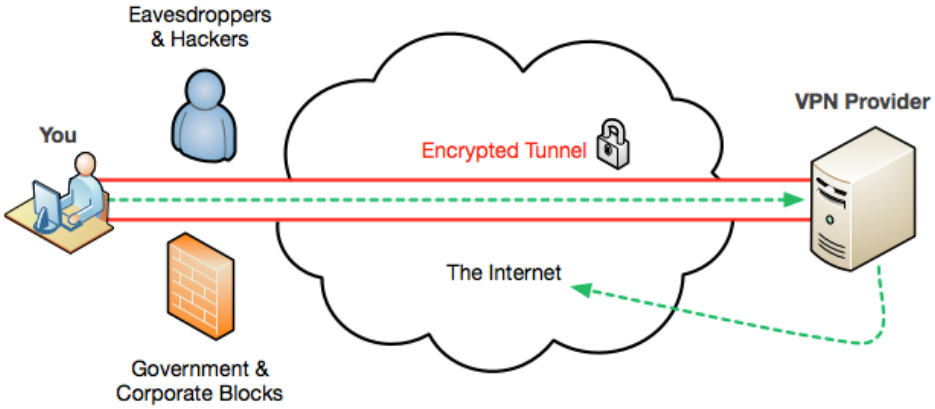
Third, connecting to an encrypted VPN while you are on a public or untrusted network, for example a Wi-Fi hotspot that are often found in hotels, coffee shops as well as bars, is a smart, simple security practice that can deal with any online ***Privacy*** issues someone might have. Virtual Private Networks not only encrypt your Internet traffic they also protect you from potential hackers or people who may be trying to snoop on your browsing via Wi-Fi to capture your passwords.

As long as your VPN is trustworthy and keeps no logs, VPN is a very secure and anonymous means of surfing the internet.

As mentioned before, it is also good for securing connections at public Wi-Fi hotspots and for evading firewalls used to censor the internet.

Fourth and finally: ***Authorization*****.** One of the best reasons to use a VPN is to circumvent regional restrictions. The so called “Geo-blocking”, the practice of preventing users from viewing websites and downloading applications and media based on location can be bypassed. Journalists and political dissidents use VPNs to get around state-sponsored censorship all the time, but you can also use a VPN for recreational purposes, such as connecting to a British VPN to watch the BBC iPlayer outside the UK. If you connect with a British VPN server, you take the identity of a British citizen and are allowed access to all features which are restricted to foreign countries.

I have only mentioned advantages of Virtual Private Networking so far, but disadvantages do exist. For example, if you have a Cisco VPN software installed on your client you are most likely to connect to a Cisco VPN server. If you decide to connect to other vendor-specific VPN servers, e.g. Microsoft or OpenVPN you might have a few complications. It's like two shoes that can only be worn as a pair.



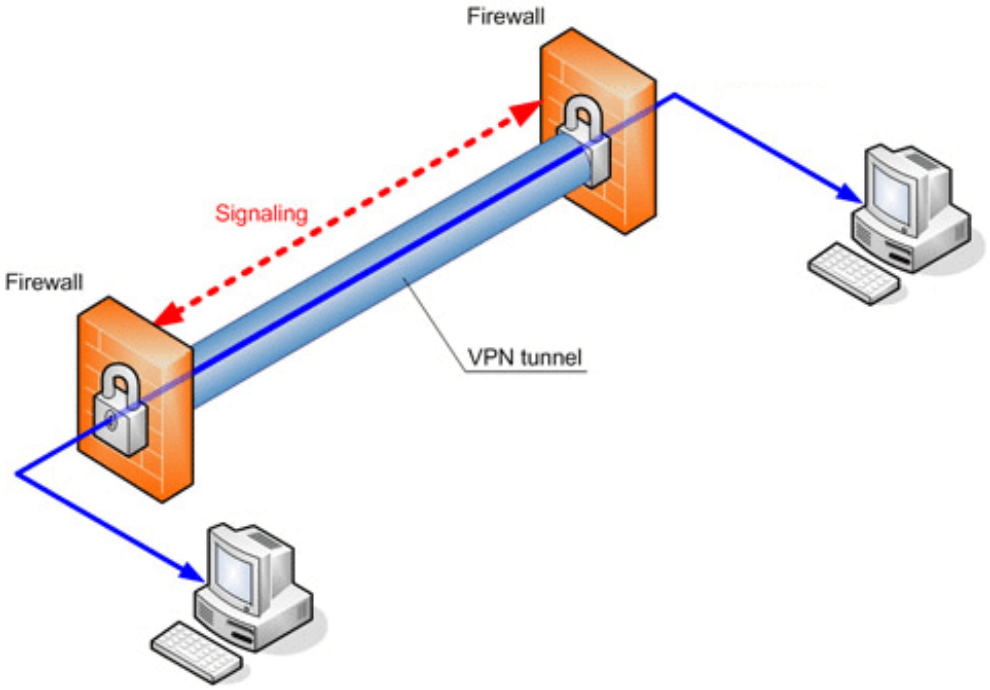
How does a Virtual Private Network work?

To explain the main idea and functionality behind a Virtual Private Network, I would like to begin at the creation of the Internet itself. First, I would like you to understand, why the Internet was invented in particular.

One of the important reasons was the instantaneous communication around the globe during the time of wars. Before the creation of the Internet there were several stations, which were responsible for the maintenance of the communication. But what would happen if a potential nuclear attack destroys one of these stations? The communication-stations and their static structure would fall apart and it wouldn't be possible to send and retrieve important data.

Especially for that reason, the arrangement of plenty routers was initialized. These routers were connected to each other, showing a completely dynamic structure, which could even withstand a nuclear attack, by recreating the route of communication somewhere else. The Internet gained the property of high availability but there was still one problem concerning the major security of the whole communication process.

A hacker could sit at one of these routers and listen as well as sniff at data packages passing by. This certain attack is called a "Man in the Middle" - Attack. For exactly that reason, Virtual Private Networks were invented. With the help of VPNs, the data, which is sent through the Internet is coated in a Tunnel, working with a specific Tunneling Protocol. There are many different Tunneling Protocols, some of which I will address later on in this elaboration.



You can imagine the Tunnel as some kind of wall, existing for the whole purpose of security. If an attacker should think about sniffing your data traffic, he first has to penetrate the tunnel's wall. Part of the Tunneling Protocol is looking for this kind of penetration attempts and if an attack should be detected, the Tunnel recreates a new route with a new set of routers between the client and the server. Even if, in the worst case scenario, the attacker should penetrate the tunnel and gather the data traffic's information, it still is encrypted and not readable with the correct key.

As a little summary:

The VPN's Tunneling Protocol creates a tunnel, which is responsible for your data's safety. An attacker has to penetrate the tunnel's wall to get access to your encrypted data. Part of the Tunneling protocol has something called "Penetration Detection", which is a process of recreating the connection with a completely new set of routers to escape the attacker's grasp.

Tunneling Protocols

There are a lot of different Tunneling Protocols at your disposal but in this elaboration, only the four most important ones are mentioned. Here's a quick rundown, including the strengths and weaknesses of each.

Point-to-Point Tunneling Protocol (PPTP)

The Point-to-Point Tunneling Protocol (PPTP) is the least secure VPN method, but it's a great starting point for your first VPN because almost every operating system supports it, including Windows, Mac OS, and even mobile OSs like Android.

PPTP uses a control channel over TCP and a GRE (Generic Routing Encapsulation) tunnel operating to encapsulate PPP packets. Generic Routing Encapsulation is a Tunneling protocol developed by Cisco System that can encapsulate a variety of network layer protocols inside virtual point-to-point links over an Internet Protocol.

In other words, the information is sent as a native plaintext without any signs of encryption, thus the tunnel and its penetration-detection are the only measurements to prevent attackers from stealing your data.

Advantages: The easiest Tunneling protocol to use

Disadvantages: The most insecure Tunneling protocol

Layer 2 Tunneling Protocol (L2TP)

The Layer 2 Tunneling Protocol is more secure than PPTP and is almost as widely supported, but more complicated to set up. It does not provide any encryption or confidentiality by itself. Moreover it provides privacy by relying on an encryption protocol that is passed within the tunnel.

Advantages: More secure than the Point-to-Point Tunneling Protocol

Disadvantages: More complicated to set up than the PPTP

Internet Protocol Security (IPSec)

The Internet Protocol Security is more secure than PPTP and is almost as widely supported, but more complicated to set up. By authenticating and encrypting each IP packet of a communication session the security of the IPSec protocol suite for Internet Protocol communications is established.

Advantages: More secure than the Point-to-Point Tunneling Protocol

Disadvantages: More complicated to set up than the PPTP

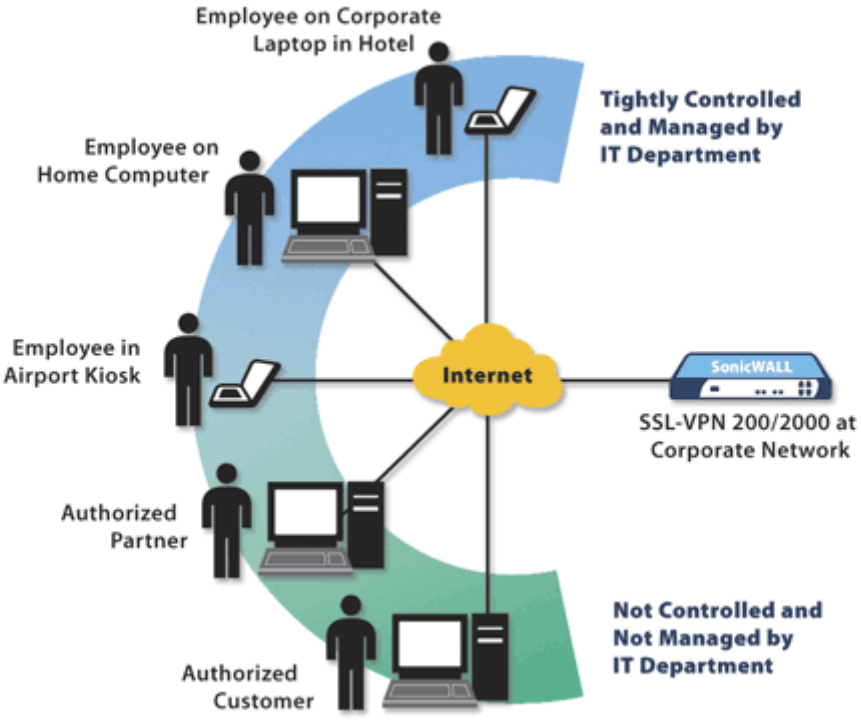
Secure Sockets Layer (SSL)

Secure Sockets Layer VPN systems are the most secure way of Tunneling. For example, if you log on to banking sites and other sensitive domains, SSL is used to provide the highest level of security.

Most SSL VPNs are referred to as “clientless”, since a dedicated VPN client is not needed to connect to one of them. The connection happens via a Web browser and thus is easier and more reliable to use than PPTP, L2TP, or IPSec.

Advantages: The connection happens via a Web browser -> Easier and more reliable than the other Tunneling Protocols

Disadvantages: The most complex Tunneling protocol



An SSL VPN server is designed to be accessed via Web browser and creates encrypted channels so that you can safely access the server from **anywhere.**

Advantages and Disadvantages of VPN

By using a VPN companies are given an easy and safe way to link users together that are distributed across multiple locations. As mentioned earlier, not only are VPNs used to communicate securely over a public network such as the Internet, they are also deployed for virtualized services such as customer service call centers. Other new technologies have emerged during the past few years, but Virtual Private Networking offers more advantages than disadvantages when it comes to secure communications.

In this chapter you will be introduced to some pros and cons associated with deploying this type of communications technology.

VPN Security and Design

Pro – Virtual private networks offer a much higher level of secure communication when compared to other remote methods of communication. The reason for that is the use of advanced technologies that are used to protect the network from unauthorized access, for example various Tunneling Protocols.

Contra – The design and security implementation for a virtual private network can be very complex. You might need a competent professional with a high level of understanding to get the best VPN configuration and someone who is able to solve any security issues that occur when using a VPN.

VPN Cost

Pro – If an organization decides to operate with a virtual private network, the costs significantly lower than other types of configurations. This is mainly due to the absence of variables for different types of communications over the VPN and the opportunity to communicate securely at low cost in other parts of the world.

Contra – Probably one of the most annoying disadvantages of using a virtual private network is ***Reliability***. This means that you and all your employees rely on the VPN service provider that you choose, whether security or update-wise. If the VPN utilizes the Internet it is important to work with a provider that can guarantee minimal downtime because time is money and you want your VPN service to work 24 hours a day. The less complications the better.

VPN Scalability

Pro – Virtual private networks are very flexible in terms of growing with the company and adding new users to the network. This type of infrastructure allows for scalability without having to add new components to accommodate the growth.

Contra – If it happens to be necessary to create additional infrastructure the solutions can become incompatible and cause technical issues if you use a different product vendor than used for the current infrastructure. On the other side of the coin and depending upon the product vendor you use, working with the same vendor cam sometimes increase the cost of deploying additional infrastructure.

VPNs and Mobile Workers

Pro – Virtual private networks offer more flexibility for business partners to communicate over a secure connection. Installing a VPN service on your smartphone and accessing files even more mobile is a really great feature. A VPN will also create more ease of communication with remote workers and enable them to check in at the office without sacrificing security.

Contra – The use of mobile devices to initiate connectivity to the virtual private network can cause security issues especially if the connection is wireless. For this reason, an added solution is sometimes needed to tighten up security when logging on to the VPN with a mobile device.

Conclusion

Despite the pros and cons of a virtual private network they still offer a viable solution for secure communications between distributed users. The most important thing is to have a competent VPN-professional employed to ensure that you get a secure solution for your business that is free of technical issues and other upcoming problems.

Comparison of VPN providers

Millions of people use a VPN service to protect their privacy, but not all VPNs are as anonymous as one might hope. In fact, some VPN services log users' IP-addresses for weeks. To find out how secure VPNs really are TorrentFreak asked the leading providers about their logging policies, and more.

To prevent their IP-addresses from being visible to the rest of the Internet, millions of people have signed up to a VPN service. Using a VPN allows users to use the Internet anonymously and prevent snooping.

Unfortunately, not all VPN services are as anonymous as they claim.

Following a high-profile case of an individual using an 'anonymous' VPN service that turned out to be not so private, TorrentFreak decided to ask a selection of VPN services some tough questions.

By popular demand we now present the third iteration of our VPN services "logging" review. In addition to questions about logging policies we also asked VPN providers about their stance towards file-sharing traffic, and what they believe the most secure VPN is.

---

1. Do you keep ANY logs which would allow you to match an IP-address and a time stamp to a user of your service? If so, exactly what information do you hold and for how long?

2. Under what jurisdictions does your company operate and under what exact circumstances will you share the information you hold with a 3rd party?

3. What tools are used to monitor and mitigate abuse of your service?

4. In the event you receive a DMCA takedown notice or European equivalent, how are these handled?

5. What steps are taken when a valid court order requires your company to identify an active user of your service?

6. Is BitTorrent and other file-sharing traffic allowed on all servers? If not, why?

7. Which payment systems do you use and how are these linked to individual user accounts?

8. What is the most secure VPN connection and encryption algorithm you would recommend to your users?

What follows is the list of responses from the VPN services, in their own words. Providers who didn't answer our questions directly or failed by logging everything were excluded. Please note, however, that several VPN companies listed here do log to some extent. The order of the lists holds no value.

Private Internet Access

1. We absolutely do not log any traffic nor session data of any kind, period. We have worked hard to meticulously fork all daemons that we utilize in order to achieve this functionality. It is definitely not an easy task, and we are very proud of our development team for helping Private Internet Access to achieve this unique ability.

2. We operate out of the US which is one of the few, if only, countries without a mandatory data retention law. We explored several other jurisdictions with the help of our professional legal team, and the US is still ideal for privacy-based VPN services.

We severely scrutinize the validity of any and all legal information requests. That being said, since we do not hold any traffic nor session data, we are unable to provide any information to any third-party. Our commitment and mission to preserve privacy is second to none.

3. We do not monitor any traffic, period. We block IPs/ports as needed to mitigate abuse when we receive a valid abuse notification.

4. We do not host any content and are therefore unable to remove any of said content. Additionally, our mission is to preserve and restore privacy on the Internet and society. As such, since we do not log or monitor anything, we're unable to identify any users of our service.

5. Once again, we do not log any traffic or session data. Additionally, unlike the EU and many other countries, our users are protected by legal definition. For this reason, we're unable to identify any user of our service. Lastly, consumer protection laws exist in the US, unlike many other countries. We must abide by our advertised privacy policy.

6. We do not discriminate against any kind of traffic/protocol on any of our servers, period. We believe in a free, open, and uncensored internet.

7. Bitcoin, Ripple, PayPal, Google Play (Mobile), OKPay, CashU, Amazon and any major Gift Card. We support plenty of anonymous payment methods. For this reason, the highest risk users should definitely use Bitcoin, Ripple or a major gift card with an anonymous e-mail account when subscribing to our privacy service.

8. We're the only provider to date that provides a plethora of encryption cipher options. We recommend, mostly, using AES-128, SHA1 and RSA2048.

„Anonymous VPN Service From the Leaders | Private Internet Access"

https://www.privateinternetaccess.com/pages/buy-vpn/

TorGuard

1. TorGuard does not store any IP address or time stamps on any VPN and proxy servers, not even for a second. Further, we do not store any logs or time stamps on user authentication servers connected to the VPN. In this way it is not even possible to match an external time stamp to a user that was simultaneously logged in. Because the VPN servers utilize a shared IP configuration, there can be hundreds of users sharing the same IP at any given moment further obfuscating the ability to single out any specific user on the network.

2. TorGuard is a privately owned company with parent ownership based in Nevis and our headquarters currently located in the US. Our legal representation at the moment is comfortable with the current corporate structuring however we wouldn't hesitate to move all operations internationally should the ground shift beneath our feet. We now offer VPN access in 23+ countries worldwide and maintain all customer billing servers well outside US borders.

We would only be forced to communicate with a third-party in the event that our legal team received a court ordered subpoena to do so. This has yet to happen, however if it did we would proceed with complete transparency and further explain the nature of TorGuard's shared VPN configuration. We have no logs to investigate, and thus no information to share.

3. Our network team uses commercial monitoring software with custom scripts to keep an eye on individual server load and service status/uptime so we can identify problems as fast as possible. If abuse reports are received from an upstream provider, we block it by employing various levels of filtering and global firewall rules to large clusters of servers. Instead of back tracing abuse by logging, our team mitigates things in real-time. We have a responsibility to provide fast, abuse-free VPN services for our clients and have perfected these methods over time.

4. In the event of receiving a DMCA notice, the request is immediately processed by our abuse team. Because it is impossible for us to locate which user on the server is actually responsible for the violation, we temporarily block the infringing server and apply global rules depending on the nature

of the content and the server responsible. The system we use for filtering certain content is similar to keyword blocking but with much more accuracy. This ensures the content in question to no longer pass through the server and satisfies requirements from our bandwidth providers.

5. Due to the nature of shared VPN services and how our network is configured, it is not technically possible to effectively identity or single out one active user from a single IP address. If our legal department received a valid subpoena, we would proceed with complete transparency from day one. Our team is prepared to defend our client's right to privacy to the fullest extent of the law.

6. BitTorrent is only allowed on select server locations. TorGuard now offers a variety of protocols like http/socks proxies, OpenVPN, SSH Tunnels, SSTP VPN and Stealth VPN (DPI Bypass), with each connection method serving a very specific purpose for usage. Since BitTorrent is largely bandwidth intensive, we do not encourage torrent usage on all servers. Locations that are optimized for torrent traffic include endpoints in: Canada, Netherlands, Iceland, Sweden, Romania, Russia and select servers in Hong Kong. This is a wide range of locations that works efficiently regardless of the continent you are trying to torrent from.

7. We currently accept payments through all forms of credit or debit card, PayPal, OKPAY, and Bitcoin. During checkout we may ask the user to verify a billing phone and address but this is simply to prevent credit card fraud, spammers, and keep the network running fast and clean. After payment it is possible to change this to something generic that offers more privacy. No VPN or Proxy usage can be linked back to a billing account due to the fact we hold absolutely no levels of logging on any one of our servers, not even timestamps!

8. For best security we advise clients to choose OpenVPN connections only, and if higher encryption is called for use AES256 bit. This option is available on many locations and offers excellent security without degrading performance. For those that are looking to defeat Deep Packet Inspection firewalls (DPI) like what is encountered in countries such as China or Iran, TorGuard offers "Stealth" VPN connections in the Netherlands, UK and Canada. Stealth connections feature OpenVPN obfuscation technology that causes VPN traffic to appear as regular connections, allowing VPN access even behind the most strict corporate Wi-Fi networks or government regulated ISPs.

"Anonymous VPN, Proxy & Torrent Proxy Services | TorGuard"

https://torguard.net/

IPVanish

1. IPVanish has a no-log policy. We keep no traffic logs.

2. IPVanish is headquartered in the US and thus operates under US law.

3. IPVanish has no monitoring in place. To elaborate, IPVanish does not sniff or monitor any user's traffic or activity for any reason.

4. IPVanish keeps no logs of any user's activity and responds accordingly.

5. IPVanish, like every other company, has to follow the law in order to remain in business. Only US law applies.

6. P2P is permitted. IPVanish in fact does not block or throttle any ports, protocols, servers or any type of traffic whatsoever.

7. PayPal and all major credit cards are accepted. Payments and product use are in no way linked. User authentication and billing info are help on completely different and independent platforms.

8. OpenVPN generally provides the strongest encryption algorithm, so that is the recommended encryption protocol. IPVanish also allows a choice between TCP and UDP, and UDP is generally recommended for better speed.

"The Best VPN Service Provider with Fast, Secure VPN Access"

https://www.ipvanish.com/index-c.php?a_aid=start

VikingVPN

1. No. We run a zero knowledge network and are unable to tie a user to an IP address.

2. United States, they don't have data retention laws, despite their draconian surveillance programs. The only information we share with anyone is billing information to our payment gateway. This can be anonymized by using a pre-paid anonymous card. If asked to share specific data about our users and their habits, we would be unable to do so, because we don't have any logs of that data.

3. That is mostly confidential information. However, we can assure our users that we do not use logging to achieve this goal.

4. In the event of a DMCA notice, we send out the DMCA policy published on our website. We haven't yet received a VALID DMCA notice.

5. We exhaust all legal options to protect our users. Failing that, we would provide all of our logs, which do not actually exist. If required to wiretap a user under a National Security Letter, we have a passively triggered Warrant Canary. We would also likely choose to shut down our service and put it up elsewhere.

6. Yes. Those ports are all open, and we have no data caps.

7. We currently only take credit cards. Our payment provider is far more restrictive than we ever imagined they would be. We're still trying to change payment providers. Fortunately, by using a pre-paid credit card, you can still have totally anonymous service from us.

8. A strong handshake (either RSA-4096+ or a non-standard elliptic curve as the NIST curves are suspect). A strong cipher such as AES-256-CBC or AES-256-GCM encryption (NOT EDE MODE). At least SHA1 for data integrity checks. SHA2 and the newly adopted SHA3 (Skein) hash functions are also fine, but slower and provide no real extra assurances of data integrity, and provide no further security beyond SHA1. The OpenVPN HMAC firewall option to harden the protocol against Man-in-the-Middle and Man-on-the-Side attacks.

"The Fastest, Most Secure Premium VPN Service Provider | Viking VPN"

https://vikingvpn.com/

CyberGhost

1. We do not log, keep logs, protocol surfing behaviors or record content, visited websites or IP addresses of our users! Why? People in non-democratic countries are in real danger, just for expressing their opinions. If we implemented backdoors, deep packet inspections or store information about our users and share those with authorities regardless their origins, we would risk the lives of people. We will not do that! Ever!

2. We are a Romanian company and operate under the laws of Romania inside the European Union (good thing!). We do not hold information, so we cannot share information! The same mechanisms that offer protection to respectable citizens, journalists and other persons against data espionage and more serious deeds make it impossible for us to identify or track users suspected of having committed crimes using the CyberGhost VPN network.

There is only the theoretical possibility to intercept them, based on a court order, to record future surfing on a specific account (for example, to survey the activities of a terrorist cell). However, such operations require that, in addition to the court request, the relevant investigation authorities communicate us a connection IP or log-in data. In practice, this theoretical hypothesis is almost completely void of significance, and we have never used it.

We think that company headquarters like ours in the European Union is a very good solution for users: It offers a high legal standard in private data protection for the user and a possibility to operate absolutely transparent for us. We believe that US Lavabit owner Ladar Levison was right as he said, after he shut down is encrypted e mail service: “I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States.”

3. As we said, we do not log, keep logs, protocol surfing behaviors or record content, visited websites or IP addresses of our users. Theoretically, we could do that. By implementing special logging tools a server can be monitored in general. However, the data flow from and to a certain user needs some more analysis to be done – which CyberGhost VPN explicitly refuses to do. To underline this, the company will always agree to be inspected by network specialists or net activists like EFF at any time on its own costs. We also announced a public Google hangout where we connect to a server of the audits choice and go in public through all settings, so everybody can see that there is no logging enabled or installed. Torrentfreak editors are welcome to ask questions live.

In case we are ordered to monitor a certain user account by a court in favor of preventing or unweave a crime, we will of course agree. No anonymization service stands outside the law. However, these orders are very rare. CyberGhost VPN itself never got asked up to now. The reason is quite simple: To be able to monitor a single account, CyberGhost VPN needs data about the account in question from the court, which is only available, if the respective owner already is under surveillance. The data CyberGhost VPN stores (the amount of traffic and its timestamps) cannot be used to identify a user – which finally means, that the use of an anonymization service by a suspect doesn’t offer any additional evidence as already known.

4. CyberGhost VPN has decided to publish a Transparency Report detailing only the number of the requests to disclose individual users' personal data received since its founding in 2011 up to the present day. The requests have been made by authorities, companies and individuals in relation to suspected offenses carried out through CyberGhost VPN. The company has not and could not in any circumstance provide user data to those who request it, because this would be in breach of CyberGhost VPN's mission to protect its users, and because no user data records exist.

Since CyberGhost VPN does not keep any records, the report does not list additional procedures following the requests. A review of the legality of the requests has not taken place either.

5. First we would do is to review the legality of the court order with our local and international team of lawyers and search for possibilities to lodge an appeal to make sure that we operate on legal ground and that "Lady Justice is blind" and no procedural error happened.

After we have left no stone unturned we would follow the court order. We do not stand outside the legal system – and we don't want to.

If the specification of the court order would not be covered from our own Terms and Conditions (for example, because the court wants – for what reasons ever – find out the activities of a whistle-blower like Edward Snowden) and our conscience would not allow to follow the court order, then we would shut down CyberGhost VPN and try to find a legal way to inform the public.

6. None of the current P2P technologies are illegal per definition, but we have to block P2P protocols on our free servers due to strategic reasons. We think this is traffic that unnecessary slows down the free service and we want to keep the "lines free" for people that need a Free VPN to access and surf the web.

However, we do have Premium servers that allow the use of P2P networks – except those in countries where we are forced by providers to block torrent traffic, e.g. in the USA.

7. In order to enable a separation of the payment data from the data of the VPN user account, the invoicing and payment procedure is performed exclusively by third party resellers. All transactions performed via our internet website and our clients are conducted by our business partner cleverbridge AG who operates in the European Union. Cleverbridge AG supports customer payment in 29 currencies, representing 75 percent of the world's population.

We also added anonymous ways to pay for our service. Bitcoin payments are conducted by our business partner Paybilla, who also operates in the EU. And costumers in Germany, Austria and Switzerland can buy CyberGhost VPN anonym by paying cash in a retail store.

8. We recommend our users to use the Open VPN protocol that is integrated in our native clients for Windows, Mac and Android.

"Surf anonymously – Download and use for free | CyberGhost VPN"

http://www.cyberghostvpn.com/en_us

	Logging?	**Jurisdictions/Information Sharing?**	**Monitoring Tools?**	**DMCA takedown?**	**Court Order Identification**	**File-Sharing Traffic?**	**Payment Methods?**	**Securest Encryption Algorithm**	**Price**
PIA	Not logging any traffic	US, no information, cause no logging	No monitoring	Not able to identify	Users are protected by legal definition	No discrimination against any kind of protocol/traffic	Bitcoin, PayPal, Ripple, CashU, Google Play, etc.	AES-128, SHA1, RSA2048	6.95$
TorGuard	Not logging any traffic	US, no information, cause no logging	Commercial monitoring software, keep an eye on servers' status	Processed by abuse team	Not possible to identify because of the network configuration	Allowed on specific servers	PayPal, OKPAY, Bitcoin, etc.	AES256	A: 5.95$ P: 9.99$

IPVanish	Not logging any traffic	US, US Law	No monitoring	No logs of any user's activity	US law applies	P2P permission	PayPal, major credit cards	OpenVPN	10$
Viking VPN	Zero Knowledge network	US, data retention laws	No logging, but other reasons ?	DMCA policy, website	No loggings do exist	All ports open	Only credit card payment	RSA-4096+ SHA1, SHA2, SHA3	14.95$
Cyber Ghost	Not logging any traffic	Romanian Company, Romanian Laws	No monitoring	Transparency Report	"Lady Justice is blind"	Blocked P2P, strategic reasons	PayPal	OpenVPN Protocol	N: 0$ P: 5.83$

List of References

[1] Virtuelle Private Netzwerke, Aufbau und Sicherheit; Manfred Lipp;

ISBN 978-3-8273-2647-8

[2] How and why to set up a VPN today; Eric Geier;

http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html

[3] Virtual Private Network; Vangie Beal;

http://www.webopedia.com/TERM/V/VPN.html

[4] Geo-Blocking; Wikipedia;

http://en.wikipedia.org/wiki/Geo-Blocking

[5] Virtual Private Network Definition; Margaret Rouse;
http://searchenterprisewan.techtarget.com/definition/virtual-private-network

[5] VPN Tunnel Picture;

http://bestvpn.biz/wp-content/uploads/2013/10/vpn-tunnel.gif

[6] VPN Provider-You Image;

http://blog.rastating.com/content/images/2014/11/vpn-diagram.png

[7] Point-to-Point Tunneling Protocol; Wikipedia;

http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol

[8] Generic Routing Encapsulation; Wikipedia;
http://en.wikipedia.org/wiki/Generic_Routing_Encapsulation

[9] Layer 2 Tunneling Protocol; Wikipedia;

http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol

[10] IPSec; Wikipedia;

http://en.wikipedia.org/wiki/IPsec

[11] SSL-VPN Image;

http://core0.staticworld.net/images/article/2013/03/ssl-vpn-100029646-orig.png

[12] The Pros and Cons of using a Virtual Private Network; Tech Blog;

http://www.thrivenetworks.com/blog/2011/07/28/the-pros-and-cons-of-using-a-virtual-private-network/

[13] Which VPN services take your Anonymity seriously?; Ernesto;

http://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/