WIKIPEDIA

Virtual private network

A **virtual private network** (**VPN**) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.[1] The benefits of a VPN include increases in functionality, security, and management of the private network. It provides access to resources inaccessible on the public network and is typically used for telecommuting workers. Encryption is common, although not an inherent part of a VPN connection.[2]

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols over existing networks. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.[3]

Contents

Types

Virtual private networks may be classified by several categories:

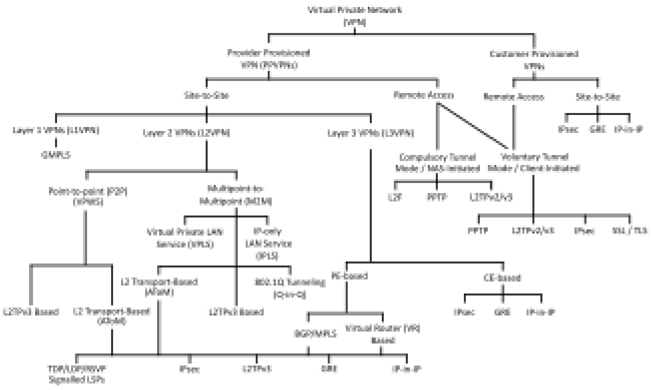
Remote access

A *host-to-network* configuration is analogous to connecting a computer to a local area network. This type provides access to an enterprise network, such as an intranet. This may be employed for telecommuting workers who need access to private resources, or to enable a mobile worker to access important tools without exposing them to the public

Internet.

Site-to-site

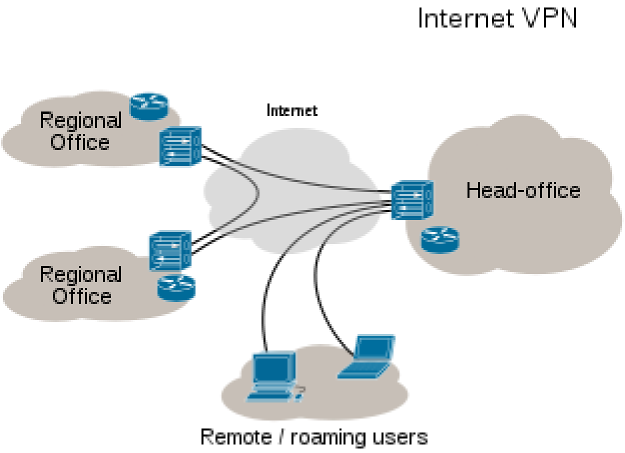
A *site-to-site* configuration connects two networks. This configuration expands a network across geographically disparate offices, or a group of offices to a data center installation. The interconnecting link may run over a dissimilar intermediate network, such as two IPv6 networks connected over an IPv4 network.[4]


Virtual Private Network (VPN)
Provider Provisioned VPN (PPVPNs)
Customer Provisioned VPNs
Site-to-Site
Remote Access
Remote Access
Site-to-Site
IPsec
GRE
IP-in-IP
Layer 1 VPNs (L1VPN)
Layer 2 VPNs (L2VPN)
Layer 3 VPNs (L3VPN)
GMPLS
Compulsory Tunnel Mode / NAS-Initiated
Voluntary Tunnel Mode / Client-Initiated
L2F
PPTP
L2TPv2/v3
Point-to-point (P2P) (VPWS)
Multipoint-to-Multipoint (M2M)
PPTP
L2TPv2/v3
IPsec
SSL / TLS
Virtual Private LAN Service (VPLS)
IP-only LAN Service (IPLS)
L2 Transport-Based (AToM)
802.1Q Tunneling (Q-in-Q)
PE-based
CE-based
L2TPv3 Based
L2 Transport-Based (AToM)
L2TPv3 Based
IPsec
GRE
IP-in-IP
BGP/MPLS
Virtual Router (VR) Based
TDP/LDP/RSVP Signalled LSPs
IPsec
L2TPv3
GRE
IP-in-IP

VPN classification tree based on the topology first, then on the technology used.

Extranet-based site-to-site

In the context of site-to-site configurations, the terms **intranet** and **extranet** are used to describe two different use cases.[5] An *intranet* site-to-site VPN describes a configuration where the sites connected by the VPN belong to the same organization, whereas an *extranet* site-to-site VPN joins sites belonging to multiple organizations.



VPN connectivity overview, showing intranet site-to-site and remote-work configurations used together

Typically, individuals interact with remote access VPNs, whereas businesses tend to make use of site-to-site connections for business-to-business, cloud computing, and branch office scenarios. Despite this, these technologies are not mutually exclusive and, in a significantly complex business network, may be combined to enable remote access to resources located at any given site, such as an ordering system that resides in a datacenter.

VPN systems also may be classified by:

- the tunneling protocol used to tunnel the traffic
- the tunnel's termination point location, e.g., on the customer edge or network-provider edge
- the type of topology of connections, such as site-to-site or network-to-network
- the levels of security provided
- the OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity
- the number of simultaneous connections

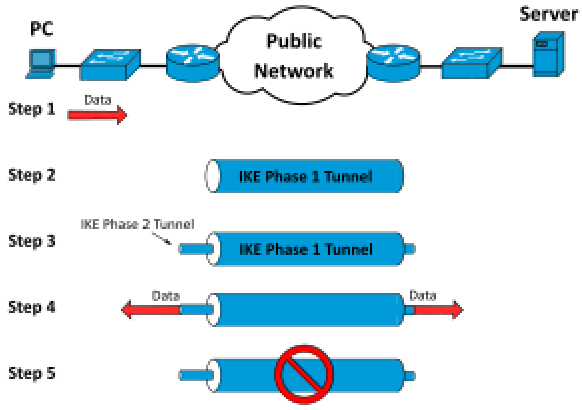
Security mechanisms

VPNs cannot make online connections completely anonymous, but they can usually increase privacy and security. To prevent disclosure of private information, VPNs typically allow only authenticated remote access using tunneling protocols and encryption techniques.

The VPN security model provides:

- confidentiality such that even if the network traffic is sniffed at the packet level (see network sniffer and deep packet inspection), an attacker would see only encrypted data
- sender authentication to prevent unauthorized users from accessing the VPN
- message integrity to detect any instances of tampering with transmitted messages.

Secure VPN protocols include the following:



The life cycle phases of an IPSec Tunnel in a virtual private network.

- Internet Protocol Security (IPsec) was initially developed by the Internet Engineering Task Force (IETF) for IPv6, which was required in all standards-compliant implementations of IPv6 before RFC 6434 (https://datatracker.ietf.org/doc/html/rfc6434) made it only a recommendation.[6] This standards-based security protocol is also widely used with IPv4 and the Layer 2 Tunneling Protocol. Its design meets most security goals: availability, integrity, and confidentiality. IPsec uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic (as it does in the OpenVPN project and SoftEther VPN project[7]) or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.
- Datagram Transport Layer Security (DTLS) – used in Cisco AnyConnect VPN and in OpenConnect VPN[8] to solve the issues SSL/TLS has with tunneling over TCP (tunneling TCP over TCP can lead to big delays and connection aborts[9]).
- Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
- Microsoft Secure Socket Tunneling Protocol (SSTP) tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL/TLS channel (SSTP was introduced in Windows Server 2008 and in Windows Vista Service Pack 1).
- Multi Path Virtual Private Network (MPVPN). Ragula Systems Development Company owns the registered trademark "MPVPN".[10]
- Secure Shell (SSH) VPN – OpenSSH offers VPN tunneling (distinct from port forwarding) to secure remote connections to a network or to inter-network links. OpenSSH server provides a limited number of concurrent tunnels. The VPN feature itself does not support personal authentication.[11][12][13]
- WireGuard is a protocol. In 2020, WireGuard support was added to both the Linux[14] and Android[15] kernels, opening it up to adoption by VPN providers. By default, WireGuard utilizes Curve25519 for key exchange and ChaCha20 for encryption, but also includes the ability to pre-share a symmetric key between the client and server.[16][17]
- IKEv2 is an acronym that stands for Internet Key Exchange volume 2. It was created by Microsoft and Cisco and is used in conjunction with IPSec for encryption and authentication. Its primary use is in mobile devices, whether on 3G or 4G LTE networks, since it is effective at rejoining when a connection is lost.

Authentication

Tunnel endpoints must be authenticated before secure VPN tunnels can be established. User-created remote-access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods. Network-to-network tunnels often use passwords or digital certificates. They permanently store the key to allow the tunnel to establish automatically, without intervention from the administrator.

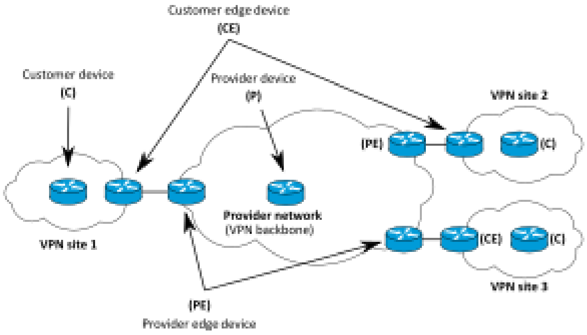
Routing

Tunneling protocols can operate in a point-to-point network topology that would theoretically not be considered a VPN because a VPN by definition is expected to support arbitrary and changing sets of network nodes. But since most router implementations support a software-defined tunnel interface, customer-provisioned VPNs often are simply defined tunnels running conventional routing protocols.

Provider-provisioned VPN building-blocks

Depending on whether a provider-provisioned VPN (PPVPN) operates in layer 2 or layer 3, the building blocks described below may be L2 only, L3 only, or a combination of both. Multi-protocol label switching (MPLS) functionality blurs the L2-L3 identity.[18]

RFC 4026 (https://datatracker.ietf.org/doc/html/rfc4026) generalized the following terms to cover L2 MPLS VPNs and L3 (BGP) VPNs, but they were introduced in RFC 2547 (https://datatracker.ietf.org/doc/html/rfc2547).[19][20]



Site-to-Site VPN terminology.

Customer (C) devices

A device that is within a customer's network and not directly connected to the service provider's network. C devices are not aware of the VPN.

Customer Edge device (CE)

A device at the edge of the customer's network which provides access to the PPVPN. Sometimes it is just a demarcation point between provider and customer responsibility. Other providers allow customers to configure it.

Provider edge device (PE)

A device, or set of devices, at the edge of the provider network which connects to customer networks through CE devices and presents the provider's view of the customer site. PEs are aware of the VPNs that connect through them, and maintain VPN state.

Provider device (P)

A device that operates inside the provider's core network and does not directly interface to any customer endpoint. It might, for example, provide routing for many provider-operated tunnels that belong to different customers' PPVPNs. While the P device is a key part of implementing PPVPNs, it is not itself VPN-aware and does not maintain VPN state. Its principal role is allowing the service provider to scale its PPVPN offerings, for example, by acting as an aggregation point for multiple PEs. P-to-P connections, in such a role, often are high-capacity optical links between major locations of providers.

User-visible PPVPN services

OSI Layer 2 services

Virtual LAN

Virtual LAN (VLAN) is a Layer 2 technique that allows for the coexistence of multiple local area network (LAN) broadcast domains interconnected via trunks using the IEEE 802.1Q trunking protocol. Other trunking protocols have been used but have become obsolete, including Inter-Switch Link (ISL), IEEE 802.10 (originally a security protocol but a subset was introduced for trunking), and ATM LAN Emulation (LANE).

Virtual private LAN service (VPLS)

Developed by Institute of Electrical and Electronics Engineers, Virtual LANs (VLANs) allow multiple tagged LANs to share common trunking. VLANs frequently comprise only customer-owned facilities. Whereas VPLS as described in the above section (OSI Layer 1 services) supports emulation of both point-to-point and point-to-multipoint topologies, the method discussed here extends Layer 2 technologies such as 802.1d and 802.1q LAN trunking to run over transports such as Metro Ethernet.

As used in this context, a VPLS is a Layer 2 PPVPN, emulating the full functionality of a traditional LAN. From a user standpoint, a VPLS makes it possible to interconnect several LAN segments over a packet-switched, or optical, provider core, a core transparent to the user, making the remote LAN segments behave as one single LAN.[21]

In a VPLS, the provider network emulates a learning bridge, which optionally may include VLAN service.

Pseudo wire (PW)

PW is similar to VPLS, but it can provide different L2 protocols at both ends. Typically, its interface is a WAN protocol such as Asynchronous Transfer Mode or Frame Relay. In contrast, when aiming to provide the appearance of a LAN contiguous between two or more locations, the Virtual Private LAN service or IPLS would be appropriate.

Ethernet over IP tunneling

EtherIP (RFC 3378 (https://datatracker.ietf.org/doc/html/rfc3378))[22] is an Ethernet over IP tunneling protocol specification. EtherIP has only packet encapsulation mechanism. It has no confidentiality nor message integrity protection. EtherIP was introduced in the FreeBSD network stack[23] and the SoftEther VPN[24] server program.

IP-only LAN-like service (IPLS)

A subset of VPLS, the CE devices must have Layer 3 capabilities; the IPLS presents packets rather than frames. It may support IPv4 or IPv6.

OSI Layer 3 PPVPN architectures

This section discusses the main architectures for PPVPNs, one where the PE disambiguates duplicate addresses in a single routing instance, and the other, virtual router, in which the PE contains a virtual router instance per VPN. The former approach, and its variants, have gained the most attention.

One of the challenges of PPVPNs involves different customers using the same address space, especially the IPv4 private address space.[25] The provider must be able to disambiguate overlapping addresses in the multiple customers' PPVPNs.

BGP/MPLS PPVPN

In the method defined by RFC 2547 (https://datatracker.ietf.org/doc/html/rfc2547), BGP extensions advertise routes in the IPv4 VPN address family, which are of the form of 12-byte strings, beginning with an 8-byte route distinguisher (RD) and ending with a 4-byte IPv4 address. RDs disambiguate otherwise duplicate addresses in the same PE.

PEs understand the topology of each VPN, which are interconnected with MPLS tunnels either directly or via P routers. In MPLS terminology, the P routers are Label Switch Routers without awareness of VPNs.

Virtual router PPVPN

The virtual router architecture,[26][27] as opposed to BGP/MPLS techniques, requires no modification to existing routing protocols such as BGP. By the provisioning of logically independent routing domains, the customer operating a VPN is completely responsible for the address space. In the various MPLS tunnels, the different PPVPNs are disambiguated by their label but do not need routing distinguishers.

Unencrypted tunnels

Some virtual networks use tunneling protocols without encryption for protecting the privacy of data. While VPNs often do provide security, an unencrypted overlay network does not neatly fit within the secure or trusted categorization.[28] For example, a tunnel set up between two hosts with Generic Routing Encapsulation (GRE) is a virtual private network but is neither secure nor trusted.[29][30]

Native plaintext tunneling protocols include Layer 2 Tunneling Protocol (L2TP) when it is set up without IPsec and Point-to-Point Tunneling Protocol (PPTP) or Microsoft Point-to-Point Encryption (MPPE).[31]

Trusted delivery networks

Trusted VPNs do not use cryptographic tunneling; instead they rely on the security of a single provider's network to protect the traffic.[32]

- Multi-Protocol Label Switching (MPLS) often overlays VPNs, often with quality-of-service control over a trusted delivery network.
- L2TP[33] which is a standards-based replacement, and a compromise taking the good features from each, for two proprietary VPN protocols: Cisco's Layer 2 Forwarding (L2F)[34] (obsolete as of 2009) and Microsoft's Point-to-Point Tunneling Protocol (PPTP).[35]

From the security standpoint, VPNs either trust the underlying delivery network or must enforce security with mechanisms in the VPN itself. Unless the trusted delivery network runs among physically secure sites only, both trusted and secure models need an authentication mechanism for users to gain access to the VPN.

VPNs in mobile environments

Mobile virtual private networks are used in settings where an endpoint of the VPN is not fixed to a single IP address, but instead roams across various networks such as data networks from cellular carriers or between multiple Wi-Fi access points without dropping the secure VPN session or losing application sessions.[36] Mobile VPNs are widely used in public safety where they give law-enforcement officers access to applications such as computer-assisted dispatch and criminal databases,[37] and in other organizations with similar requirements such as field service management and healthcare.[38].

Networking limitations

A limitation of traditional VPNs is that they are point-to-point connections and do not tend to support broadcast domains; therefore, communication, software, and networking, which are based on layer 2 and broadcast packets, such as NetBIOS used in Windows networking, may not be fully supported as on a local area network. Variants on VPN such as Virtual Private LAN Service (VPLS) and layer 2 tunneling protocols are designed to overcome this limitation.[39]

See also

- Anonymizer
- Dynamic Multipoint Virtual Private Network
- Ethernet VPN
- Internet privacy
- Mediated VPN
- Opportunistic encryption
- Split tunneling
- Virtual private server
- VPN service

References

1. "What Is a VPN? - Virtual Private Network" (https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html). *Cisco*. Retrieved 5 September 2021.
2. Mason, Andrew G. (2002). *Cisco Secure Virtual Private Network* (https://archive.org/details/ciscosecurevirtu00andr). Cisco Press. p. 7 (https://archive.org/details/ciscosecurevirtu00andr/page/7). ISBN 9781587050336.
3. "Virtual Private Networking: An Overview" (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb742566(v=technet.10)). TechNet. *Microsoft Docs*. 4 September 2001. Retrieved 7 November 2021.
4. Davies, Joseph (July 2007). "IPv6 Traffic over VPN Connections" (https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc138002(v=msdn.10)). The Cable Guy (https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc135901(v=msdn.10)). *TechNet Magazine*. Retrieved 7 November 2021 – via Microsoft Docs.
5. *RFC 3809 - Generic Requirements for Provider Provisioned Virtual Private Networks* (https://tools.ietf.org/html/rfc3809#section-1.1). sec. 1.1. doi:10.17487/RFC3809 (https://doi.org/10.17487%2FRFC3809). RFC 3809 (https://tools.ietf.org/html/rfc3809).
6. RFC 6434 (https://datatracker.ietf.org/doc/html/rfc6434), "IPv6 Node Requirements", E. Jankiewicz, J. Loughney, T. Narten (December 2011)

7. "1. Ultimate Powerful VPN Connectivity" (http://www.softether.org/1-features/1._Ultimate_Powerful_VPN_Connectivity#SoftEther_VPN's_Solution:_Using_HTTPS_Protocol_to_Establish_VPN_Tunnels). *www.softether.org*. SoftEther VPN Project.
8. "OpenConnect" (http://www.infradead.org/openconnect/index.html). Retrieved 8 April 2013. "OpenConnect is a client for Cisco's AnyConnect SSL VPN [...] OpenConnect is not officially supported by, or associated in any way with, Cisco Systems. It just happens to interoperate with their equipment."
9. "Why TCP Over TCP Is A Bad Idea" (http://sites.inka.de/~W1011/devel/tcp-tcp.html). *sites.inka.de*. Retrieved 24 October 2018.
10. "Trademark Status & Document Retrieval" (http://tarr.uspto.gov/servlet/tarr?regser=serial&entry=78063238&action=Request+Status). *tarr.uspto.gov*.
11. "ssh(1) – OpenBSD manual pages" (https://man.openbsd.org/ssh.1#SSH-BASED_VIRTUAL_PRIVATE_NETWORKS). *man.openbsd.org*.
12. c@cb.vu, Colin Barschel. "Unix Toolbox" (http://cb.vu/unixtoolbox.xhtml#vpn). *cb.vu*.
13. "SSH_VPN – Community Help Wiki" (https://help.ubuntu.com/community/SSH_VPN). *help.ubuntu.com*.
14. Salter, Jim (30 March 2020). "WireGuard VPN makes it to 1.0.0—and into the next Linux kernel" (https://arstechnica.com/gadgets/2020/03/wireguard-vpn-makes-it-to-1-0-0-and-into-the-next-linux-kernel/). *Ars Technica*. Retrieved 30 June 2020.
15. "Diff - 99761f1eac33d14a4b1613ae4b7076f41cb2df94^! - kernel/common - Git at Google" (https://android.googlesource.com/kernel/common/+/99761f1eac33d14a4b1613ae4b7076f41cb2df94%5E!). *android.googlesource.com*. Retrieved 30 June 2020.
16. Younglove, R. (December 2000). "Virtual private networks - how they work" (https://ieeexplore.ieee.org/document/892887). *Computing & Control Engineering Journal*. **11** (6): 260–262. doi:10.1049/cce:20000602 (https://doi.org/10.1049%2Fcce%3A20000602). ISSN 0956-3385 (https://www.worldcat.org/issn/0956-3385).
17. Benjamin Dowling, and Kenneth G. Paterson (12 June 2018). "A cryptographic analysis of the WireGuard protocol". *International Conference on Applied Cryptography and Network Security*. ISBN 978-3-319-93386-3.
18. "Configuring PFC3BXL and PFC3B Mode Multiprotocol Label Switching" (https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/pfc3mpls.pdf) (PDF).
19. E. Rosen & Y. Rekhter (March 1999). "BGP/MPLS VPNs" (http://www.ietf.org/rfc/rfc2547.txt). Internet Engineering Task Force (IETF). RFC 2547 (https://tools.ietf.org/html/rfc2547).
20. Lewis, Mark (2006). *Comparing, designing, and deploying VPNs* (1st print. ed.). Indianapolis, Ind.: Cisco Press. pp. 5–6. ISBN 1587051796.
21. *Ethernet Bridging (OpenVPN)* (http://openvpn.net/index.php/access-server/howto-openvpn-as/214-how-to-setup-layer-2-ethernet-bridging.html)
22. Hollenbeck, Scott; Housley, Russell. "EtherIP: Tunneling Ethernet Frames in IP Datagrams" (http://tools.ietf.org/search/rfc3378).
23. Glyn M Burton: RFC 3378 EtherIP with FreeBSD (https://securethoughts.com/9-rfc-3378-etherip-with-freebsd/), 03 February 2011
24. net-security.org news: Multi-protocol SoftEther VPN becomes open source (http://www.net-security.org/secworld.php?id=16171), January 2014
25. Address Allocation for Private Internets (http://www.ietf.org/rfc/rfc1918.txt), RFC 1918 (https://datatracker.ietf.org/doc/html/rfc1918), Y. Rekhter *et al.*, February 1996
26. RFC 2917 (https://datatracker.ietf.org/doc/html/rfc2917), *A Core MPLS IP VPN Architecture*
27. RFC 2918 (https://datatracker.ietf.org/doc/html/rfc2918), E. Chen (September 2000)

28. Yang, Yanyan (2006). "IPsec/VPN security policy correctness and assurance". *Journal of High Speed Networks*. **15**: 275–289. CiteSeerX 10.1.1.94.8561 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.94.8561).
29. "Overview of Provider Provisioned Virtual Private Networks (PPVPN)" (https://securethoughts.com/overview-provider-provisioned-virtual-private-networks-ppvpn/). Secure Thoughts. Retrieved 29 August 2016.
30. RFC 1702 (https://datatracker.ietf.org/doc/html/rfc1702): Generic Routing Encapsulation over IPv4 networks. October 1994.
31. IETF (1999), RFC 2661 (https://datatracker.ietf.org/doc/html/rfc2661), Layer Two Tunneling Protocol "L2TP"
32. Cisco Systems, Inc. (2004). *Internetworking Technologies Handbook* (https://books.google.com/books?id=3Dn9KlIVM_EC). Networking Technology Series (4 ed.). Cisco Press. p. 233. ISBN 9781587051197. Retrieved 15 February 2013. "[...] VPNs using dedicated circuits, such as Frame Relay [...] are sometimes called *trusted VPN*s, because customers trust that the network facilities operated by the service providers will not be compromised."
33. Layer Two Tunneling Protocol "L2TP" (http://www.ietf.org/rfc/rfc2661.txt), RFC 2661 (https://datatracker.ietf.org/doc/html/rfc2661), W. Townsley *et al.*, August 1999
34. IP Based Virtual Private Networks (http://www.ietf.org/rfc/rfc2341.txt), RFC 2341 (https://datatracker.ietf.org/doc/html/rfc2341), A. Valencia *et al.*, May 1998
35. Point-to-Point Tunneling Protocol (PPTP) (http://www.ietf.org/rfc/rfc2637.txt), RFC 2637 (https://datatracker.ietf.org/doc/html/rfc2637), K. Hamzeh *et al.*, July 1999
36. Phifer, Lisa. "Mobile VPN: Closing the Gap" (http://searchmobilecomputing.techtarget.com/tip/0,289483,sid40_gci1210989_mem1,00.html), *SearchMobileComputing.com*, July 16, 2006.
37. Willett, Andy. "Solving the Computing Challenges of Mobile Officers" (http://www.officer.com/print/Law-Enforcement-Technology/Solving-the-Computing-Challenges-of-Mobile-Officers/1$30992), *www.officer.com*, May, 2006.
38. Cheng, Roger. "Lost Connections" (https://www.wsj.com/articles/SB119717610996418467), *The Wall Street Journal*, December 11, 2007.
39. Sowells, Julia (7 August 2017). "Virtual Private Network (VPN) : What VPN Is And How It Works" (https://hackercombat.com/virtual-private-network/). *Hackercombat*. Retrieved 7 November 2021.

Further reading

- Kelly, Sean (August 2001). "Necessity is the mother of VPN invention" (https://web.archive.org/web/20011217153420/http://www.comnews.com/cgi-bin/arttop.asp?Page=c0801necessity.htm). *Communication News*: 26–28. ISSN 0010-3632 (https://www.worldcat.org/issn/0010-3632). Archived from the original (http://www.comnews.com/cgi-bin/arttop.asp?Page=c0801necessity.htm) on 17 December 2001.