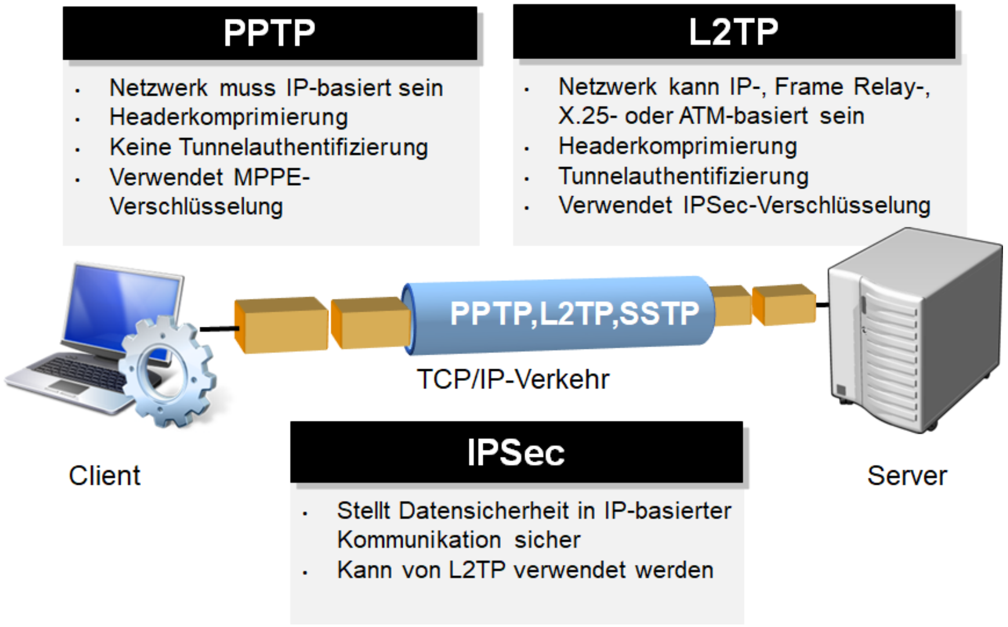
VPN-Protocols



PPTP

- Netzwerk muss IP-basiert sein
- Headerkomprimierung
- Keine Tunnelauthentifizierung
- Verwendet MPPE-Verschlüsselung

L2TP

- Netzwerk kann IP-, Frame Relay-, X.25- oder ATM-basiert sein
- Headerkomprimierung
- Tunnelauthentifizierung
- Verwendet IPSec-Verschlüsselung

IPSec

- Stellt Datensicherheit in IP-basierter Kommunikation sicher
- Kann von L2TP verwendet werden

The conventional **VPN** refers to a virtual private (self-contained) communication network. Virtual in the sense that it is not a physical connection of its own, but an existing communication network that is used as a transport medium. The VPN serves to bind participants of the existing communication network to another network.

You can use **VPNs (Virtual Private Networks)** to establish remote access to servers or other VPN partners regardless of the network connection between them.

VPNs use an additional protocol that allows users to connect to **LANs** via existing Internet connections.

These connections can be secure, although the connection may use public Internet hardware.

VPN protocols include **TCP/IP** in PPP data packets. The server uses the client to perform all security and validation checks and enables data encryption, which makes sending data over unsecured networks such as the Internet secure. Typically, users connect to the VPN by first connecting to an Internet Service Provider (ISP) and then connecting to the VPN ports through that Internet connection.

VPNs are based on the following underlying protocols: (excerpt)

- **PPTP** (Point-to-Point Tunneling Protocol) **was broken!**
- **L2TP** (Layer Two Tunneling Protocol) for establishing the connection.
- **SSTP** (Secure Socket Tunneling Protocol) (Microsoft)
- **IPsec** (Internet Protocol Security-Microsoft)

PPTP

PPTP (**Point-to-Point-Tunneling Protocol**) enables the secure transmission of enclosed data from a PPTP client to a PPTP server via a TCP/IP Internet network such as the Internet. PPTP includes PPP frames for transmission over the Internet network in TCP/IP packets. For this reason, you can use all the features of PPP including TCP/IP and MPPE (Microsoft Point-to-Point Encryption) in a PPTP VPN.

Windows 2000 or later supports PPTP, a protocol that you can use for private LAN-to-LAN networks.

L2TP

L2TP (**Layer Two Tunneling Protocol**)

L2TP is a tunneling solution that combines the advantages of PPTP (Point-to-Point Tunneling Protocol) and L2F (Layer 2 Forwarding). Like PPTP, L2TP uses the authentication and compression mechanisms of PPP. With the help of a tunnel ID in the L2TP header, several tunnels can be used next to each other as well as **NAT (Network Address Translation)** .

L2TP offers the authentication methods CHAP (Challenge Handshake Authentication Protocol) and PAP (Password Authentication Protocol). Encryption is not directly included in L2TP. If necessary, this must be done by protocols. L2TP is therefore often used in combination with IPsec. (RFC 3193 - "Securing L2TP using IPSec")

Due to the lack of confidentiality of the L2TP protocol, it is often implemented together with IPsec. This is called L2TP/IPsec and is standardized in IETF RFC 3193.

IPSec

IPsec is a protocol suite designed to enable secure communication over potentially insecure IP networks such as the Internet.

IPsec works directly on the Internet Layer of the DoD model and is a further development of the IP protocols. The goal is to provide encryption-based security at the network level. IPsec offers this possibility by the connectionless integrity as well as the access control and authentication of the data. In addition, IPsec ensures the confidentiality and authenticity of the packet sequence through encryption.

⚠ **Further Information**

- VoIP Essentials
- Visit the Snom Forum
- Open a support ticket
- Find a local partner

Related articles

- 10.1.20.0
- 8.7.5.35 public release
- 802.1Q
- 802.1X
- <certificates> tag
- <dialplan> tag
- <functionKeys> tag
- <gui-languages>, <web-languages>tag
- <phone-settings> tag
- <ReplacementPlan> tag
- <Setting-Files> tag
- <tbook>,<phone-book> tag
- <uploads> tag
- A100D
- A100M