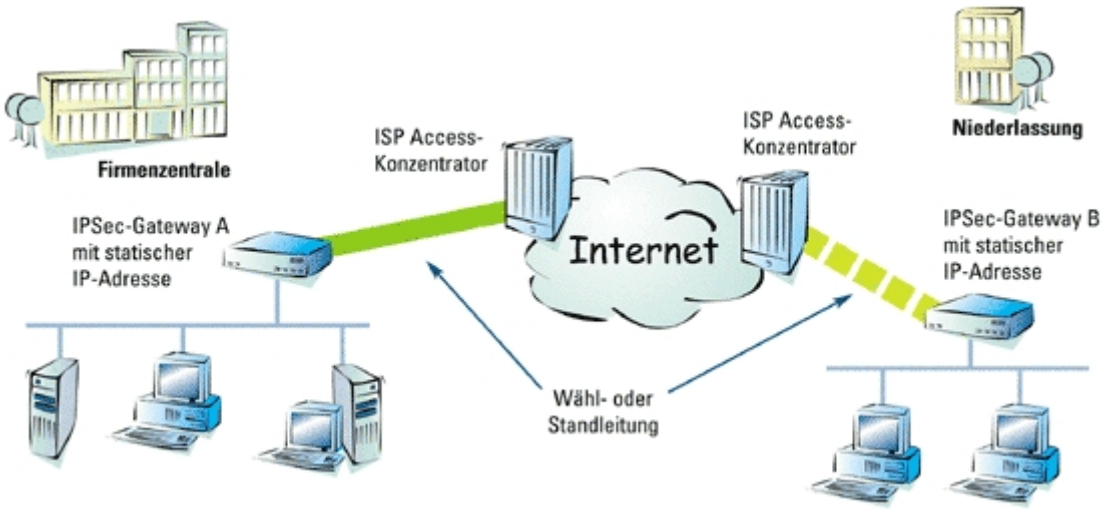
VPN

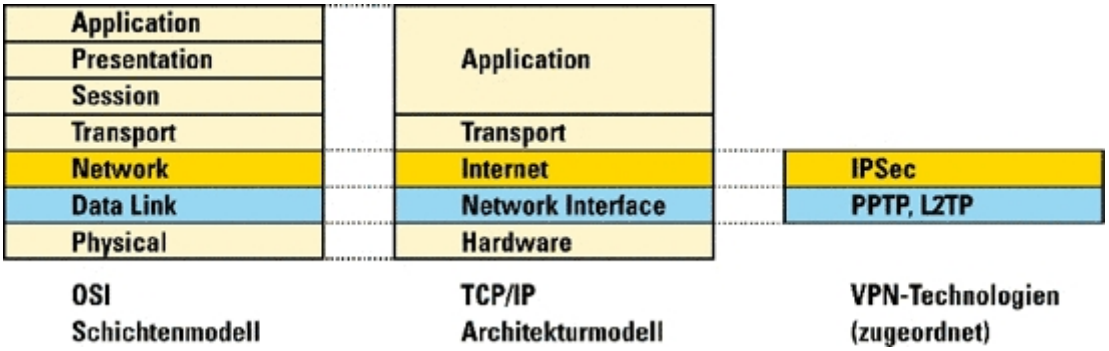
Abkürzung für "Virtual Private Network" • ein VPN ist ein Netzwerk bestehend aus virtuellen Verbindungen (z.B. Internet), über die nicht öffentliche bzw. firmeninterne Daten sicher übertragen werden. Die VPN-Technologie ermöglicht kostengünstige und sichere Anbindungen von Außenstellen bzw. Niederlassungen.



- Prinzipiell wird bei *IP*-basierenden VPNs zwischen zwei unterschiedlichen Ansätzen unterschieden: Seit einigen Jahren schon werden "**IP-VPN-Lösungen**" von den großen NSPs/*ISPs* angeboten. Gerade große, international arbeitende Unternehmen nutzen diese Dienste, um ihre, die Grenzen von Ländern und Kontinenten überschreitenden, firmeninternen Kommunikations-Infrastrukturen aufzubauen. Übergänge in das eigentliche Internet werden an geeigneten Punkten im Netzwerk zentralisiert und kontrolliert. Der firmeninterne Datenverkehr erfolgt nicht über das Internet, sondern über die Leitungen des NSP/ISP.

- Eine zweite, neuere Technik, "**Internet VPN**" genannt, nutzt dagegen das Internet als Infrastruktur für die firmeninterne Kommunikation. Gerade für kleine und mittelständische Unternehmen werden bei diesem Ansatz Kommunikationslösungen möglich, die bislang nicht bezahlbar waren. Dies spiegelt sich auch in aktuellen Untersuchungen von Analysten wieder, die die zunehmende Bedeutung von Internet-VPN-Lösungen zeigen. Das "Mehr" an Sicherheit, das uns moderne VPN-Technologie garantiert, erlaubt nun auch die Nutzung sehr günstiger Internet-Zugänge. Gerade durch die Nutzung des Internets als verbindende Netzwerk-Infrastruktur, ergeben sich eine ganze Reihe weiterer Vorteile. Diese wirken sich nicht nur positiv auf die laufenden Kosten aus, sondern erlauben auch sehr flexible Lösungen. Das Internet als "virtuelles Backbone" ermöglicht die Wahl der optimalen lokalen Internet-Anbindung. Ob *xDSL*, ISDN, *GSM* oder analoge *Modems* - mit Internet VPNs gibt es keinerlei Bindung an bestimmte *WAN*-Technologien (und damit auch nicht an Tarife und Bandbreiten), die ein einzelner ISP/NSP an einem bestimmten Ort anbieten kann. Damit entfällt für den Kunden auch die Festlegung auf bestimmte, vom ISP/NSP vorgegebene Hardware / Software-Lösungen: Im Gegensatz zu dedizierten *IP-VPN-Lösungen* können viele *Internet VPN-Lösungen* auch nach einem Wechsel von einem ISP zu einem anderen Anbieter weiter

eingesetzt werden. Durch diese Flexibilität sind Investitionen in Netzwerk-Produkte und Ausbildung in idealer Weise gesichert.



In den letzten Jahren wurde eine ganze Reihe zum Teil standardisierter Verfahren entwickelt, welche die technischen Grundlagen für verschiedene VPN-Lösungen darstellen. Auch wenn diese Protokolle alle das "Tunneling"-Verfahren darstellen, unterscheiden sie sich doch grundsätzlich in der Art und Weise, wie dieses "Tunneling" erreicht wird. So werden zum Beispiel bei *Verschlüsselung* und Authentifizierung verschiedene technologische Ansätze gewählt. Dabei haben sich in den letzten Jahren einige Verfahren bzw. Protokolle als vielversprechende Lösungen abgezeichnet. Unter Zuhilfenahme des *OSI*-Schichtenmodells lassen sich diese Verfahren in zwei Gruppen einteilen, die auf jeweils der OSI-Schicht 2 (Link Layer) bzw. Schicht 3 arbeiten. So sind PPTP (Point-to-Point Tunneling Protocol) und auch L2TP (Layer 2 Tunneling Protocol) typische Vertreter für OSI-Schicht 2 Protokolle:

PPTP ist ein Punkt-zu-Punkt Tunneling Protokoll, das ursprünglich für *RAS (Remote Access Server)* Hardware und Software (insbesondere Windows NT) entwickelt wurde.

- Anstrengungen, auch technische Ansätze anderer Hersteller von *Router* und *RAS*-Komponenten mit PPTP zu kombinieren und damit einen breiteren Standard zu schaffen, führten zur Entwicklung von **L2TP**.

Als Schicht 2 Protokolle (nach dem OSI Modell) sind PPTP oder L2TP auch für Multiprotokoll-Anwendungen einsetzbar.

- **IPSec** wird von vielen Seiten als die umfassendste und zugleich vielversprechendste VPN-Technologie für IP-Netzwerke angesehen. So beinhalten die IPSec betreffenden Standards umfassende Sicherheitsfunktionen, die neben Verschlüsselung auch Verfahren zur Authentifizierung und Verwaltung von "Schlüsseln" dienen. Da IPSec ein *OSI*-Schicht 3 basierendes Protokoll ist, kann IPSec ausschließlich in IP-Netzwerken eingesetzt werden. Dieses Dokument versucht, Internet VPN-Lösungsansätze für kleine und mittelständische Unternehmen aufzuzeigen. Aus diesem Grunde steht auch die genauere Beleuchtung von IPSec-Lösungen im Vordergrund.

- Viele der in den letzten Jahren angebotenen VPN-Lösungen stützten sich auf proprietäre Lösungen einzelner Hersteller. Mit den verschiedenen Arbeiten der *IETF (Internet Engineering Task Force)* zum Thema "IP Security", kurz IPSec genannt, macht die Standardisierung von IP-basierenden VPN-Lösungen große Fortschritte. Ein großer Teil der Entwicklung von IPSec wurde ursprünglich als integraler Bestandteil der nächsten Generation von IP-Protokollen (*IPv6*) in Angriff genommen. Da IPv6 sich aber nicht wie geplant schnell durchsetzen konnte, wurde sichergestellt, dass IPSec-Verfahren und Protokolle auch mit IPv4 nutzbar sind, um so die aktuellen Probleme mit Sicherheit in IP-Netzwerken adressieren zu können. Diese Kompatibilität mit IPv4 Protokollen bedeutet, dass Netzwerkanwendungen transparent die IPSec-Sicherheitsvorteile nutzen können, sofern sie auf einer Implementierung der *TCP/IP* Protokoll Suite aufsetzen, welche IPSec unterstützt.

Auch wenn mit *RFC* 2401 grundsätzliche Aussagen zur Architektur gemacht werden, ist IPSec nicht als einzelner Standard zu verstehen. Vielmehr ist man in der *IETF* bemüht, den einzelnen Sicherheitsaspekten von IP-Netzwerken in dedizierten Dokumenten gerecht zu werden. Wie diese verschiedenen Standardisierungs-Dokumente zusammenhängen, wird in der "IP Security Document Roadmap" in RFC 2411 beschrieben. Die so entstehenden Standards bilden die Basis für kompatible, flexible und auch erschwingliche VPN-Lösungen. Die wichtigsten Elemente der IPSec-Architektur spiegeln sich auch in der IP Security Document Roadmap wider. Zentrale Funktion in der IPSec-Architektur nehmen dabei

- das AH-Protokoll (Authentification Header),
- das ESP-Protokoll (Encapsulating Security Payload) und
- die Schlüssel-Verwaltung (Key Management) ein.

Das modulare Design der AH- und ESP-Protokolle erlaubt die Nutzung verschiedener Verschlüsselungs bzw. Authentifizierungs-Techniken. So lassen sich entsprechende neue Algorithmen und Verfahren leicht in die AH- und ESP-Protokolle integrieren.

- AH-Protokolle sorgen dabei für die Authentifizierung der zu übertragenden Daten und Protokollinformationen. Es wird nicht nur sichergestellt, dass die Datenpakete den "korrekten" Absender beinhalten, sondern auch, dass keine Änderungen während der Datenübertragung vorgenommen worden sind. Auch wenn die Integrität der übertragenen Daten gewährleistet ist, kann jedoch ein unbefugtes "Mitlesen" Dritter nicht verhindert werden.
- ESP-Protokolle werden eingesetzt, wenn es darum geht, schützenswerte Informationen in IP-Paketen durch Verschlüsselung zu sichern. Abhängig vom gewählten Verschlüsselungsalgorithmus kann so die Datensicherheit bedeutend erhöht werden.

Um nun eine gesicherte Verbindung zwischen zwei Endpunkten aufbauen zu können, müssen auf beiden Seiten der Kommunikationsverbindung zahlreiche Parameter übereinstimmen bzw. aufeinander abgestimmt sein.

Die Kommunikationspartner müssen sich zum Beispiel auf die Art der gesicherten Übertragung (Authentifizierung und/oder Verschlüsselung), den Verschlüsselungsalgorithmus sowie die passenden Schlüssel einigen. Auch muss festgelegt werden, wie und wie oft die eingesetzten Schlüssel ausgetauscht werden. All diese Parameter einer gesicherten Verbindung werden gemäß der IPSec-Architektur durch eine sogenannte "Security Association" (SA) beschrieben. Jede einzelne gesicherte Verbindung bedingt je eine Security Association für jedes genutzte IPSec-Protokoll an jedem Ende der logischen Verbindung. So ist zum Beispiel für die Verschlüsselung eines Datenpaketes eine SA (in einer Richtung) erforderlich. Für die Authentifizierung wird eine weitere SA benötigt. Auch wenn die IPSec-RFC-Dokumente Standard-Algorithmen für Authentifizierung und Verschlüsselung vorsehen, können andere Verfahren eingesetzt werden. Da für jedes Protokoll einer jeden Verbindung eine SA mit den jeweils protokollspezifischen Parametern notwendig ist, wird ein Verfahren benötigt, das die entstehende Komplexität mindert. Über eine so genannte "Domain of Interpretation" (DOI) werden die Parameter, die für eine protokollspezifische SA erforderlich sind, standardisiert.

Die DOI beinhaltet demnach Informationen über Sicherheitsprotokolle, passende Verschlüsselungsalgorithmen sowie Mechanismen zur Schlüsselverwaltung. Aufgrund der vielen Schlüssel, die für den erfolgreichen Aufbau einer IPSec-Verbindung benötigt werden, muss der Schlüsselverwaltung (Key Management) eine hohe Bedeutung beigemessen werden. Es gibt im Augenblick zwei verschiedene Wege, die Verwaltung und Verteilung von Schlüsseln in einer IPSec-Umgebung zu gewährleisten.

- Neben der manuellen Schlüsselverwaltung kann auch
- das Internet Key Exchange Protocol (IKE) eingesetzt werden.

Grundsätzlich sehen die IPSec-Spezifikationen zwei verschiedene Betriebsarten vor; den Transport- bzw. Tunnel-Modus. Im so genannten Transport-Modus werden in das bestehende IP-Paket entweder AH- oder ESP-Informationsfelder (Header) eingefügt. Des Weiteren werden im Fall von ESP die Nutzdaten gemäß dem gewählten Algorithmus verschlüsselt. Im Tunnel-Modus wird das gesamte IP-Paket mit einbezogen. Es wird einschließlich der ursprünglichen IP-Protokoll-Informationen in ein neues IP-Paket "verpackt". Das "neue" IP-Paket wird dann mit einem entsprechenden AH- oder ESP-Informationsfeld (Header) versehen. Bei der Wahl von ESP wird dann eine Verschlüsselung des gesamten eingeschlossenen IP-Pakets vorgenommen. Dies ist gerade dann von entscheidendem Vorteil, wenn IP-Netze über das Internet miteinander verbunden werden sollen, die nicht mit registrierten gültigen Internet-Adressen arbeiten. Typische Beispiele für solche Netzwerke sind Intranets, die ein "privates" Adressierungsschema benutzen und über Router, die eine entsprechende Adressenumwandlung (*IP-Masquerading*, *NAT*, PAT) vornehmen, an das

Internet angebunden werden.