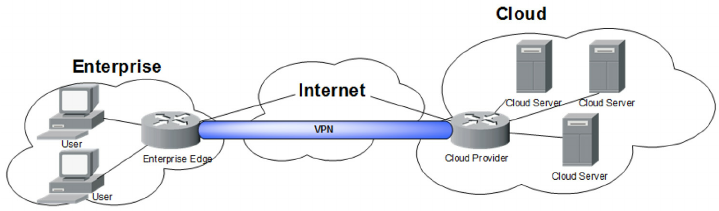
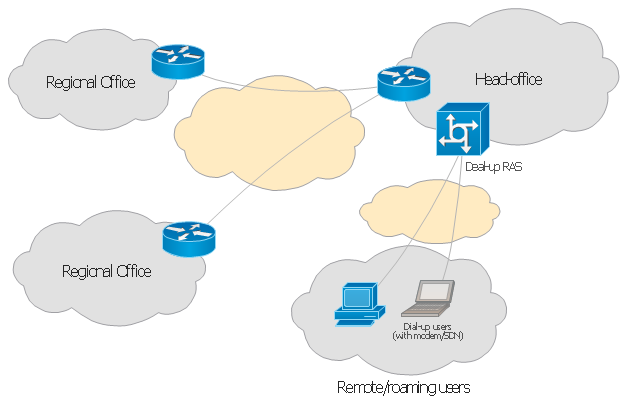
# VPN - Virtual Private Network

VPN ist ein **logisches privates Netzwerk** auf einer **öffentlich zugänglichen Infrastruktur**. Nur die Kommunikationspartner, die zu diesem privaten Netzwerk gehören, können miteinander kommunizieren und Informationen und Daten austauschen.

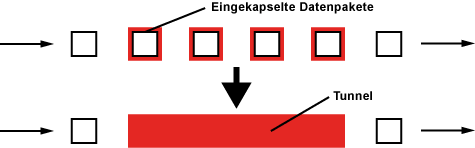
**VPN Netzwerkinfrastruktur**





**VPN Tunneling**

Um eine **gesicherte Datenübertragung** über das unsichere Internet zu gewährleisten, wird mit einem **Tunneling-Protokoll (VPN Protokoll)** eine verschlüsselte Verbindung, der VPN-Tunnel, aufgebaut. Der Tunnel ist eine logische Verbindung **zwischen beliebigen Endpunkten**. Meist sind das VPN-Clients, VPN-Server und VPN-Gateways. Man nennt diese virtuellen Verbindungen Tunnel, weil der eigentliche Inhalt der Datenpakete für andere nicht sichtbar ist.



Tunneling ist die Basis eines jeden VPNs. Tunneling erlaubt es, **Pakete eines Netzwerkprotokolls in die Pakete eines anderen Netzwerkprotokolls einzukapseln**.

Das technische Prinzip einer VPN-Verbindung ist in der Regel immer gleich. Egal welches Protokoll. Am Startpunkt des Tunnels werden die Pakete eingekapselt. Am Endpunkt werden die Pakete wieder entkapselt. Dabei wird jedes Datenpaket verschlüsselt. Der Inhalt des ursprünglichen Pakets können andere nicht sehen.

## Anforderungen an VPN

**Authentizität**: Identifizierung von Nutzern / Endpunkten, Überprüfung der Daten (ob sie vom Endpunkt kommen) --> mit Zertifikaten

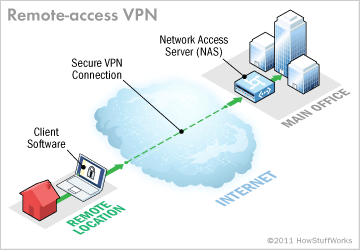
**Vertraulichkeit**: Daten werden verschlüsselt, Daten nicht von anderen einsehbar --> Verschlüsselungsverfahren

**Integrität**: Daten nicht von anderen änderbar (oder wenn die Daten verändert wurden, muss es erkennbar sein) --> (Checksum), Hashalgorithmus

## VPN Typen

Je nach Netzwerkaufbau werden verschiedene VPN Typen unterschieden.

**End-to-Site-VPN / Remote-Access-VPN**



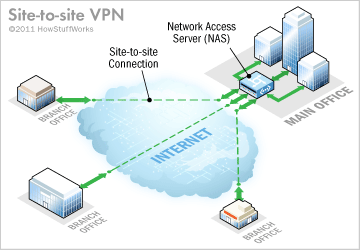


End-to-Site-VPN beschreibt ein VPN-Szenario, bei dem **Heimarbeitsplätze oder mobile Benutzer (Außendienst) in ein Unternehmensnetzwerk** eingebunden werden. Der externe Mitarbeiter soll so arbeiten, wie wenn er sich im Netzwerk des Unternehmens befindet. Man bezeichnet dieses VPN-Szenario auch als Remote Access.

Die VPN-Technik stellt eine logische Verbindung, den VPN-Tunnel, zum entfernten lokalen Netzwerk über ein öffentliches Netzwerk her. Hierbei muss eine **VPN-Client Software** auf dem Computer des externen Mitarbeiters installieren sein.

Im Vordergrund steht ein **möglichst geringer, technischer und finanzieller Aufwand** für einen sicheren Zugriff auf das entfernte Netzwerk.

**Site-to-Site-VPN / LAN-to-LAN-VPN / Branch-Office-VPN**





Site-to-Site-VPN und LAN-to-LAN-VPN, oder auch **Branch-Office-VPN** genannt, sind VPN-Szenarien, um **mehrere lokale Netzwerke von Außenstellen oder Niederlassungen (Filialen)** zu einem virtuellen Netzwerk über ein öffentliches Netz zusammenzuschalten.

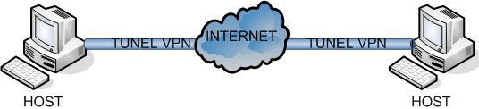
Netzwerke, die sich an verschiedenen Orten befinden lassen sich über eine angemietete Standleitung direkt verbinden. Diese Standleitung entspricht in der Regel einer physikalischen Festverbindung zwischen den beiden Standorten. Bei Festverbindungen, Frame Relay und ATM kommen je nach Anzahl, Entfernung, Bandbreite und Datenmenge sehr schnell hohe Kosten zusammen.

Da jedes Netzwerk in der Regel auch eine Verbindung zum Internet hat, bietet es sich an, diese Internet-Verbindung zur Zusammenschaltung von zwei oder mehr Netzwerken mit VPN-Technik (LAN-to-LAN-Kopplung) zu nutzen. Bei VPNs über das Internet entstehen einmalige Kosten für die Einrichtung und laufende Kosten nur die, die für den Internet Service Provider zu bezahlen sind.

Virtuelle private Netze (VPN) werden immer öfter über das Internet aufgebaut. Das Internet wird so zur Konkurrenz zu den klassischen WAN-Diensten der Netzbetreiber. VPNs lassen sich über das Internet billiger und flexibler betreiben.

Eine Variante von Site-to-Site-VPN ist das Extranet-VPN. Während ein Branch-Office-VPN nur mehrere lokale Netzwerke einer Firma verbindet, ist ein Extranet-VPN ein virtuelles Netzwerk, das die Netzwerke unterschiedlicher Firmen miteinander verbindet. In der Regel geht es darum bestimmte Dienste fremder Unternehmen ins eigene Netzwerk zu integrieren oder Dienste für fremde Unternehmen anzubieten. Zum Beispiel für Geschäftspartner, Lieferanten und Support-leistende Unternehmen. Dabei gewährt man dem externen Unternehmen Zugriff auf Teilbereiche des eigenen Netzwerks. Die Zugriffsbeschränkung erfolgt mittels einer Firewall zwischen dem lokalen Netzwerk und dem Dienstenetzwerk. Extranet-VPNs ermöglichen eine sichere Kommunikation bzw. einen sicheren Datenaustausch zwischen den beteiligten Unternehmen.

**End-to-End-VPN / Host-to-Host-VPN / Remote-Desktop-VPN**



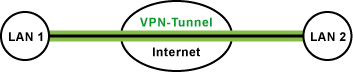


End-to-End-VPN beschreibt ein VPN-Szenario, bei dem ein Client auf einen anderen Client in einem entfernten Netzwerk zugreift. Hierbei deckt der VPN-Tunnel die gesamte Verbindung zwischen zwei Hosts ab. Auf **beiden Seiten muss eine entsprechende VPN-Software** installiert und konfiguriert sein. Das bedeutet, eine direkter Verbindungsaufbau von Host zu Host ist nicht möglich. Stattdessen bauen beide Seiten eine Verbindung zu einem Gateway auf, dass die beiden Verbindungen dann zusammenschaltet.

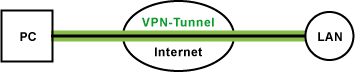
Typische Anwendung eines End-to-End-VPN ist **Remote-Desktop über öffentliche Netze**. Während RDP und VNC sich wegen der fehlenden Verschlüsselung nur für den Einsatz in lokalen Netzwerken eignet, gibt es für Remote-Desktop-VPNs meist nur proprietäre und kommerzielle Lösungen.

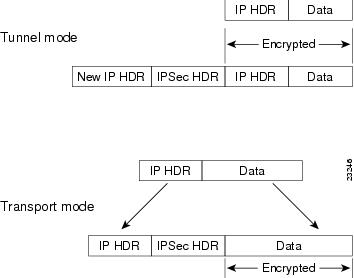
## Tunnelmodus / Transportmodus

**Tunnelmodus**: es wird das **komplette zu übertragende Datenpaket verschlüsselt**, das ursprüngliche Paket wird zur Nutzlast für das neue Paket, kompletter LAN Traffic über VPN, wird für LAN-to-LAN-Kopplungen eingesetzt



**Transportmodus**: **ursprünglichen IP Header werden beibehalten, es wird nur die eigentliche Nutzlast verschlüsselt**, IP Header enthält IP Adressen der tatsächlichen Kommunikationspartner, zur Kommunikation von 2 VPN Endpunkten, einzelne Clients bindet man in der Regel per Transportmodus an





## VPN-Endpunkt

Ein VPN-Endpunkt ist die Stelle an der der VPN-Tunnel endet bzw. beginnt. Der Endpunkt ist der Host, der für die Einhaltung von Authentizität, Vertraulichkeit und Integrität zuständig ist.

Ein **VPN-Endpunkt kann ein Router, Gateway oder auch ein Software-Client** sein.

## VPN-Router / VPN-Gateway / VPN-Server

VPN-Lösungen gibt es als Hardware (VPN-Router), Software (VPN-Server) oder auch als Service (Layer-2-VPN vom Netzbetreiber). Typischerweise setzt man an VPN-Endpunkten einen VPN-Router oder ein VPN-Gateway ein. Es gibt aber auch Server, auf denen VPN-Dienste oder VPN-Software installiert sind. Diese VPN-Server dienen dann als VPN-Endpunkte. Ein eigenständiger VPN-Server ist eher selten nötig. VPN-Gateway-Funktionen finden sich auch in Routern und Firewalls.

VPN-Gateways und -Router können VPN-Verbindungen und normale Verbindungen verarbeiten. Die VPN-Verbindungen erkennen sie am Header der Datenpakete oder an der IP-Protokollnummer.

Eine Sonderform sind VPN-Services von Netzbetreibern, die keine Installation zusätzlicher Hardware notwendig macht.

## VPN und Firewall

In der Regel **sollte eine Firewall gekapselten Datenverkehr verhindern**. Denn der gekapselte Datenverkehr könnte unberechtigte und unsichere Daten enthalten. Deshalb lässt man in der Regel eine Tür im Sicherheitskonzept geöffnet, wenn man ein VPN betreibt.

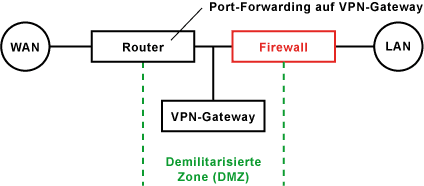
Beim Aufbau eines VPNs ist die Platzierung des VPN-Endpunktes, üblicherweise ein VPN-Router oder VPN-Gateway, eine wichtige Entscheidung. Es steht dabei die Frage im Raum, ob das VPN-Gateway vor oder hinter der Firewall sitzen soll.



Eigentlich soll eine Firewall vor ungewollten Zugriffen aus dem Netz schützen. Wenn nun das **VPN-Gateway hinter der Firewall** sitzt, dann ist die Firewall nicht in der Lage in die verschlüsselten Pakete hineinzusehen. Die verschlüsselten IP-Pakete (z. B. mit IPsec und IKE) werden auf Port 500 an das VPN-Gateway durchgelassen. Ein VPN-Teilnehmer könnte auf diese Weise unkontrolliert das Netzwerk angreifen oder ungewollte Daten ins Netzwerk einschmuggeln.



Eine bessere Lösung ist, das **VPN-Gateway vor die Firewall** zu setzen und alle verschlüsselten Datenpakete zu entschlüsselt und erst danach die Prüfung auf ungewollte Verbindungen zu prüfen.



Die **beste Lösung** ist jedoch, das **VPN-Gateway oder den VPN-Server in eine demilitarisierte Zone (DMZ)**, zwischen Netzzugangsrouter und Firewall, zu setzen. Auf diese Weise kann der entschlüsselte Datenverkehr in einer zweiten Filterstufe durch die Firewall nochmals überprüft werden.

## VPN Protokolle

**PPTP (Point to Point Tunneling Protocol)**

PPTP ist ein Tunnel-Protokoll auf Schicht 2. Es dient dazu, PPP-Verbindungen (Point to Point Protocol) über ein IP-Netz aufzubauen. Über die so hergestellte PPP-Verbindung können dann beispielsweise **IP-Pakete transportiert ("getunnelt")** werden. Die Sicherheitsfunktionen zur Authentisierung, Schlüsselverwaltung und Verschlüsselung werden von PPP bereitgestellt, häufig unter Nutzung des **Microsoft** Point-to-Point Encryption Protocol (MPPE). Im Sprachgebrauch wird jedoch oft nicht zwischen dem eigentlichen PPTP und der Kombination PPTP/PPP/MPPE unterschieden.

In gängigen Implementierungen dieses Tunnel-Verfahrens wurden Sicherheitslücken entdeckt, insbesondere in Zusammenhang mit schwachen Passwörtern. Ohne zusätzliche Sicherheitsmechanismen sollte PPTP daher nicht als VPN-Lösung eingesetzt werden.

**Kaum mehr benutzt, relativ viele Sicherheitslücken.**

**L2TP (Layer 2 Tunneling Protocol)**

Ähnlich wie PPTP dient L2TP in der Version 2 (L2TPv2) dazu, PPP-Verbindungen über paketvermittelte Netze aufzubauen. Im Gegensatz zu PPTP können bei L2TP jedoch neben IP auch andere Techniken als Trägernetz dienen, beispielsweise ATM. Für die Tunnel-Funktionalität nutzt L2TP dabei Mechanismen des von der Firma **Cisco** entworfenen Protokolls **L2F (Layer 2 Forwarding)**.

**L2TP bietet selbst keine Funktionen zur Verschlüsselung der Datenpakete an**. Eine solche Verschlüsselung muss entweder vom Trägernetz oder von den transportierten Protokollen geleistet werden. L2TP wird daher **häufig in Kombination mit IPSec** (siehe unten) eingesetzt.

**IPSec (Internet Protocol Security)**

IPSec ist ein Protokoll auf **Schicht 3**, das **Funktionen zur Verschlüsselung und Integritätssicherung für IP-Kommunikation** bietet. In Kombination mit dem IKE-Verfahren (Internet Key Exchange, früher ISAKMP/Oakley) kann auch ein automatisierter Schlüsselaustausch sowie eine Authentisierung der Tunnel-Endpunkte erfolgen. Auch über das von der Firma Sun Microsystems stammende Verfahren SKIP (Simple Key Management for Internet Protocol) kann ein Schlüsselaustausch für IPSec-Kommunikation erfolgen. Ein manueller Schlüsselaustausch wird durch IPSec ebenfalls unterstützt. Die Authentisierung der Benutzer muss jedoch über andere Verfahren erfolgen.

IPSec ist ein **komplexes Protokoll, das mehrere unterschiedliche Optionen und Betriebsmodi** bietet. Weiterhin sind die eingesetzten kryptographischen Verfahren in der Spezifikation nicht abschließend festgelegt, sondern es sind lediglich Mindestanforderungen aufgeführt. Beim Einsatz von IPSec muss daher im Rahmen der Konfiguration sichergestellt werden, dass die für den vorliegenden Anwendungsfall ermittelten Sicherheitsanforderungen erfüllt werden und dass geeignete kryptographische Verfahren verwendet werden.

**TLS/SSL (Transport Layer Security, Secure Sockets Layer)**

TLS/SSL ist ein **weit verbreitetes** Verfahren, um Transportsicherheit beispielsweise für Web-Anwendungen oder E-Mail-Übertragung bereitzustellen. Einerseits können über TLS/SSL unterschiedliche Anwendungsprotokolle, wie z. B. **HTTP, SMTP, POP oder IMAP oder VPN Verbindungen,** transportiert werden. Andererseits ist es mit Hilfe s**pezieller Software-Komponenten auch möglich, IP-Tunnel über TLS/SSL** aufzubauen. Aufgrund seiner Arbeitsweise lässt sich TLS/SSL nicht eindeutig einer bestimmten Protokollschicht zuordnen, häufig wird es jedoch als **Schicht-4-Protokoll** bezeichnet.

TLS/SSL bietet Sicherheitsfunktionen zur Authentisierung und Verschlüsselung sowie zum Schlüsselaustausch und Integritätsschutz. Ähnlich wie bei IPSec sind die hierfür erforderlichen kryptographischen Verfahren in der Spezifikation nicht abschließend festgelegt. Vielmehr handeln die beteiligten Kommunikationspartner die verwendeten Verfahren beim jeweiligen Verbindungsaufbau aus. Es muss daher im Rahmen der Konfiguration sichergestellt werden, dass die ermittelten Sicherheitsanforderungen erfüllt werden und dass geeignete kryptographische Verfahren verwendet werden.

**Typischer Einsatz bei VPN: OpenVPN**

1. **Was ist ein VPN?**

Ein VPN ist ein virtuelles privates Netzwerk. Es lässt nur die zwei Kommunikationspartner das Gespräch lesen.

1. **Was ist Tunneling?**

Protokoll für eine verschlüsselte gesicherte Verbindung zwischen VPN Clients.

1. **Welche Anforderungen an ein VPN gibt es:**
   1. **Authentizität**

Überprüfung ob die Daten richtig angekommen sind und das es der korrekte Benutzer bekommen hat.

* 1. **Vertraulichkeit**

Die Daten müssen verschlüsselt sein

* 1. **Integrität**

Daten können von jemanden anderen nicht verändert werden

1. **End-to-Site VPN**

Außen Arbeiter verbindet sich zum Unternehmensnetzwerk 🡪 remote access. VPN erstellt tunnel über ein öffentliches netz.

1. **Site-to-Site (Branch Office) VPN**

Netzwerke an verschiedenen Orten werden miteinander Verbunden. Oft: Dienste anderer Unternehmen zu integrieren.

1. **End-to-End VPN**

Zwei clients werden über einen VPN tunner miteinadner verbunden: RDP über ein öffentliches Netz

1. **Wie funktioniert der Tunnelmodus?**
2. **Wie funktioniert der Transportmodus?**
3. **VPN und Firewall: Kombinationsmöglichkeiten**
4. **Erkläre die Funktion des PPTP Protokolls.**
5. **Erkläre die Funktion des L2TP Protokolls.**
6. **Erkläre die Funktion des IPSec Protokolls.**
7. **Erkläre die Funktion des TLS / SSL Protokolls.**