Virtuelle Private Netze – Ein Überblick

Die Bezeichnung „Virtuelle Private Netze (VPN)“ ist ein Begriff, der für sehr unterschiedliche Techniken genutzt wird und somit häufig zur Verwirrung führt. Leider gibt es bis heute keine allgemein anerkannte Definition. Zudem gibt es eine unüberschaubare Vielfalt an verschiedenen Lösungskategorien, Technologien und Implementierungen, die wiederum in jedem Einzelfall auf die speziellen Bedürfnisse des jeweiligen Einsatzszenarios angepasst werden müssen. Es ist daher schwierig, einen umfassenden und systematischen Überblick zu gewinnen.

Zweifellos ist VPN ein wichtiges Thema. Kaum ein größeres Unternehmen kann es sich auf Dauer leisten, ohne ein eigenes VPN auszukommen. Aber, was genau verbirgt sich dahinter, welche Technologien gibt es und was sind die Unterschiede sowie Auswahlkriterien? Diese Fragen werden im vorliegenden Beitrag behandelt. Ausgehend von einer allgemeinen Begriffsdefinition werden zunächst die Klassen und Einsatzgebiete von VPNs eingeführt. Anschließend werden die wichtigsten Technologien mit deren Vor- und Nachteile analysiert und gegenüber gestellt sowie grundlegende Konzepte näher erläutert.

1. Einführung

Virtuelle Private Netze (VPN) werden eingesetzt, um entweder geographisch verteilte Standorte eines Unternehmens bzw. einer Organisation mit einander zu verbinden oder den Mitarbeitern eines Unternehmens eine kontrollierte Einwahl ins interne Unternehmensnetz zu ermöglichen. Im ersten Anwendungsfall spricht man von „Branch Office VPN“. Einwahllösungen werden dagegen mit „Dial In VPN“ bezeichnet. Ein Spezialfall sind so genannte Extranet-VPNs, die im Gegensatz zu Branch-Office VPNs dezu genutzt werden, Standorte unterschiedlicher Organisationen miteinander zu vernetzen (**Bild 1**).

Solche Netze sind "privat", da sie nur von dem jeweiligen Unternehmen oder der jeweiligen Organisation selber genutzt werden können bzw. sollen. Sie bieten somit einen Schutz vor unbefugten Zugriff, wodurch ein Mitlesen, Manipulieren, Einschleusen von fremden Daten oder Attacken verhindert werden soll. VPNs sind daher durch eine Sicherheitsregelwerk (Policy) definiert, das genau festlegt, wer in welcher Form und unter welchen Bedingungen Zugang zu den Ressourcen im jeweiligen Unternehmensnetz haben soll.

Der praktische Nutzen eines VPN liegt darin, dass die genannten Sicherheitsanforderungen bereits auf unterer Netzebene umgesetzt werden und sich die Anwendungen bzw. die einzelnen Nutzer um derartige Sicherheitsfragen nicht sorgen müssen. Ein praktisches Beispiel ist der Versand vertraulicher Informationen per Email zwischen zwei Unternehmensstandorten. Sofern die Verbindung zwischen diesen Standorten über ein VPN realisiert ist, muss der jeweilige Anwender keine besonderen Verfahrensweisen beachten. Er verschickt die Email, als befände sich der Empfänger im gleichen lokalen Netz. Sind die beiden Standorte jedoch ohne VPN nur über das öffentliche Internet mit einander verbunden, so müssen die Information vor dem Versand durch eine aktive Handlung des Benutzers z.B. mit PGP (Pretty Good Privacy) verschlüsselt und signiert werden, um den nötigen Schutz zu gewährleisten.

Ursprünglich wurden standortübergreifende Unternehmensnetze (CN: corporate networks) mit Hilfe von Mietleitungen realisiert. Dies hatte zur Folge, dass teure Übertragungskapazitäten exklusiv für das jeweilige CN vorgehalten wurden, ohne dass sie auch zu jeder Zeit maximal ausgelastet werden konnten. Daher kamen in der Folge vermittelte Datennetze zunächst auf der Basis von X.25, später dann basierend auf Frame Relay oder ATM, zum

Einsatz, bei denen anstelle von physikalischen Mietleitungen zwischen den einzelnen Standorten virtuelle Kanäle auf der Datenvermittlungsplattform eines Dienstleisters (VPN Service Provider) konfiguriert werden. Derartige vermittelte Unternehmensnetze sind somit "virtuell", da Einrichtungen und Übertragungskapazitäten, die zum Aufbau und zum Betrieb dieser Netze notwendig sind, für mehrere VPNs gleichzeitig genutzt werden, ohne die Trennung bzw. ihre grundlegende Sicherheit dieser Netze aufzuheben. Mit der Verbreitung der Internet-Technologie kamen in der Folge zunehmend IP basierte VPNs (IP-VPNs) zum Einsatz, bei denen anstelle virtueller Verbindungen auf Schicht 2 des OSI Modells so genannte Tunnel-Verbindungen eingerichtet werden. Häufig werden hierfür die Tunnel-Protokolle GRE[1] oder IPSec (Schicht 3) bzw. L2TP oder PPTP (Schicht 2) eingesetzt. PPTP sowie L2TP werden in der Regel für Dial In VPNs genutzt (siehe unten). Als Transportplattform wird das weltweite Internet oder eine spezielle IP-Plattform eines VPN-Providers genutzt. Darüber hinaus haben sich z.B. mit SSL (Secure Sockets Layer) auf Schicht 4 des OSI-Modells im Internet noch weitere Technologien etabliert, mit denen sich ein gesicherter Datenaustausch realisieren lässt. Diese Lösungen können jedoch nur für bestimmte Anwendungen (z.B. Browsing) genutzt werden. **Bild 2** zeigt eine Übersicht verschiedener VPN-Technologien und deren Einordnung im OSI-Modell.

Während die verschiedenen Standorte eines Unternehmens bzw. einer Organisation mit Hilfe von Branch Office VPNs miteinander verbunden werden, können mit Hilfe von Dial In VPNs für die einzelnen Mitarbeiter eines Unternehmens gesicherte Einwahlmöglichkeiten über verschiedene Zugangswege (z.B. Modem, ISDN, DSL, GPRS, WLAN, UMTS) realisiert werden. Auch hier wird eine gemeinsame

[1] GRE: Generic Route Encapsulation – Ein von Cisco entwickeltes, weit verbreitetes Tunnel-Verfahren.

Einwahlplattform eines Providers (z.B. die eines Internet Service Providers) anstelle einer eigenen Ende zu Ende Einwahllösung über das Telefonnetz genutzt, um Kosten zu sparen.
Die Einwahl wird ebenfalls unter Beachtung eines Sicherheitsregelwerks (Policy) überwacht, das festlegt, wie sich die Nutzer authentisieren müssen und welche Maßnahmen zum Schutz der Authentizität und der Vertraulichkeit der übertragenen Daten zu beachten sind. Häufig kommen hierzu die Übertragungsprotokolle PPP, PPTP, L2TP oder IPSec zum Einsatz. Der Zugang zum Unternehmensnetz wird in der Regel durch die Abfrage von Benutzername und Passwort von einem RADIUS System oder einem VPN-Gateway kontrolliert. Zunehmend kommen jedoch auch „starke“ Authentisierungsverfahren wie z.B. Einmalpasswort oder Zertifikate zum Einsatz.

Allgemein lässt sich somit festhalten, dass VPNs durch zwei wesentliche Merkmale gekennzeichnet sind:

1. VPNs sind durch eine Regelwerk (Policy) definiert, das genau festlegt, wer in welcher Form Zugang und unter welchen Bedingungen zu dem jeweiligen Unternehmensnetz haben soll.
2. VPNs werden auf einer öffentlichen Datenvermittlungsplattform realisiert und teilen sich gemeinsame Einrichtungen und Übertragungswege eines Providers untereinander.

2. VPN-Klassen

Aufgrund der kaum zu überblickenden Vielzahl an unterschiedlichen VPN-Lösungen ist es hilfreich zunächst verschiedene Klassifizierungen vorzunehmen, die helfen, einen ersten Überblick zu gewinnen, ohne zu sehr ins Detail zu gehen.

Neben der grundlegenden Einteilung nach Branch-Office-VPN und Dial-In-VPN (Bild 1) lassen sich weitere Einteilungen treffen:

- „Layer-2-VPN“ versus „Layer-3-VPN“ (gemäß OSI-Modell)
- „Secure VPN“ versus „Trusted VPNS“
- „CPE[2] basierte VPN“ versus „Netzwerk basierte VPN“
- „Best effort VPN“ versus QoS[3]-VPNs
- Overlay-Modell versus Peer Modell

Die Unterscheidung in „Layer-2-VPNs (L2VPN)“ bzw. „Layer-3-VPNs (L3VPN)“ hängt davon ab, in welcher Schicht des OSI-Referenzmodell das VPN realisiert wird. Eine Einteilung wichtiger VPN-Technologien ist bereits weiter oben vorgenommen (siehe **Bild 2**). L2VPNs auf der Basis von Frame Relay oder ATM sind noch immer am weitesten verbreitet. Da jedoch viele Diensteanbieter neben den klassischen Frame Relay bzw. ATM-Plattformen inzwischen auch IP-basierte Plattformen betreiben, gibt es Bestrebungen, L2VPN Dienste zukünftig auf einer gemeinsamen Layer-3-Plattform zu realisieren. Bei den L3VPNs unterscheidet man im wesentlichen drei Basistechnologien, die weiter unten näher eingeführt werden:

- Tunneling (z.B. IPSec, GRE)
- Virtuelle Router
- MPLS

Die Klassifizierung nach „Secure VPN“ versus „Trusted VPN“ ist eine Einteilung, die vom VPN-Consortium eingeführt wurde (http://www.vpnc.org/). Demnach bezeichnet ein „Secure VPN“ eine VPN-Lösung, die zwischen den jeweiligen

[2] CPE steht für Customer Premise Equipment und bezeichnet in der Regel einen Router oder ein VPN-Gateway, der sich in einem Standort des Kunden am Übergang zwischen dem internen Netz des Kunden und dem Weitverkehrsnetz des Providers befindet.
[3] QoS steht für Quality of Service und bezeichnet die Eigenschaft bestimmter Übertragungsverfahren wie zum ATM, zwischen zwei Endstellen Verbindungen mit einer fest definierten bzw. garantierten Übertragungsqualität (z.B. Mindestbandbreite, maximale Übertragungsverzögerung) bereitzustellen.

Endstellen eine starke Verschlüsselung eingesetzt wird, die es einem Angreifer, der an irgendeiner Stelle des Übertragungsweges den Datenverkehr aufzeichnet, praktisch unmöglich macht, die Daten zu entschlüsseln und im Klartext zu lesen. Die Sicherheit von „secure VPN“ stützt sich demnach einzig auf die eingesetzte Ende-zu-Ende Verschlüsselung, die von den Endstellen vorgenommen wird, und ist im Gegensatz zu der Klasse der „trusted VPNs“ unabhängig von der Vertrauenswürdigkeit der genutzten Übertragungsplattform. Beispiele für „secure VPNs“ sind VPN-Lösungen auf der Basis von IPSec über das Internet. Demgegenüber hängt bei der Klasse der „Trusted VPNs“ die Sicherheit von der Vertrauenswürdigkeit der Übertragungsplattform des jeweiligen Service Providers ab. Der Kunde verlässt sich hierbei darauf, dass niemand anderes als der Service Provider selbst die Übertragungspfade konfigurieren oder ändern kann und dass niemand anderes auf dem Übertragungsweg Zugang zu den übertragenen Daten hat und Daten verändern, löschen oder manipulieren kann. Beispiele für „trusted VPNs“ sind VPN-Lösungen auf der Basis von ATM, Frame Relay oder MPLS der Deutschen Telekom (siehe Produktfamilie IntraSelect weiter unten).

Bei der Differenzierung nach „CPE beasierte VPN“ versus „Netzwerk basierte VPN“ geht es um die Frage, in welcher Komponente die VPN-Policy hinterlegt und umgesetzt wird **(Bild 3)**. Die Fachwelt spricht in diesem Zusammenhang vom Service Creation Point. Grundsätzlich gibt es hier genau zwei Möglichkeiten. Entweder ist die Konfiguration der VPN-Zugehörigkeit in der CPE, z.B. einem Anschluss-Router in den Räumen des Kunden zu finden, oder sie wird am Provider Edge, dem jeweiligen Zugangs-Router zur VPN-Plattform des Providers, vorgenommen. Im ersten Fall spricht man von CPE basierte VPN, in zweiten Fall wird die Lösung Netzwerk basiertes VPN genannt. CPE-basierte VPNs können ohne

spezielle Mitwirkung des Service Providers vom Kunden selbst realisiert werden. Hierzu sind jedoch Spezialkenntnisse erforderlich. Bei Netzwerk basierten VPNs hingegen muss die CPE nur gewöhnliche IP Routing-Funktionen unterstützen.

Die Klassifizierung nach „Best-effort VPN“ versus „QoS VPN“ betrifft die Übertragungsqualität zwischen den einzelnen Standorten eines VPN. Unterschiedliche Anwendungen haben unterschiedliche Anforderungen an ein Übertragungsnetz. So stellt z.B. ein File Transfer hohe Anforderungen in Bezug auf Bandbreite und Netzstabilität. Die Übertragungsverzögerung ist eher unkritisch. Echtzeitanwendungen wie Video-Conferencing oder Voice over IP (VoIP) erfordern demgegenüber ein geringes und stabiles Delay. Um diesen unterschiedlichen Anforderungen Rechnung zu tragen, kommen bei der Realisierung von VPNs Übertragungstechniken wie z.B. ATM, Frame Relay oder MPLS eingesetzt, die die geforderten Qualitäten z.B. Mindestbandbreite, konstantes Delay[4] oder Jitter[5] zwischen zwei Standort Ende zu Ende einhalten können. Zudem müssen die jeweiligen Endstellen bzw. Abschluss-Router so konfiguriert werden, dass diese unterschiedlichen Übertragungsklassen abhängig von der jeweils genutzten Anwendung bereitgestellt werden und somit jede Anwendung die Behandlung erfährt, die sie für eine einwandfreie Funktionsweise benötigt. Ein Beispiel für ein QoS-VPN ist wiederum die Produktfamiele IntraSelect der Deutsche Telekom.
Von einem Best-Effort VPN ist hingegen dann die Rede, wenn sich aufgrund der gewählten Übertragungstechnik oder der genutzten Datenplattform wie z.B. dem Internet keine Ende zu Ende Qualitätszusagen geben lassen und die

[4] Delay: Verzögerungs- oder Wartezeit. Zeitspanne, um die ein Ereignis verzerrt oder verzögert wird. Beispielsweise die Zeit, die vergeht, bis eine abgesandte Information vom Zielsystem empfangen wird.
[5] Jitter: Weitgehend zufallsbestimmte Schwankungen der Flanken eines realen Datensignals um die Sollzeit des Nulldurchganges.

Übertragungsressourcen nicht fest für eine Verbindung reserviert werden können.

Von grundlegender Bedeutung ist die Unterscheidung nach Overlay- versus Peer-Modell, welche im nachfolgenden Abschnitt daher ausführlich behandelt wird.

3. „Overlay-Modell“ versus „Peer-Modell“

Die meisten VPNs sind noch immer nach dem so genannten „Overlay“ Modell (siehe **Bild 4 und 5**) realisiert. Dieses Modell bezeichnet eine Realisierungsvariante, bei der die einzelnen Anschluss-Router in den verschiedenen Standorten eines Unternehmens mit Punkt-zu-Punkt-Verbindungen miteinander vernetzt werden. Hierzu können entweder Mietleitungen oder virtuelle Verbindungen auf der Basis von ATM bzw. Frame Relay als Übertragungstechnologie genutzt werden. Virtuelle Verbindungen werden auf Schicht 2 (Layer 2) des OSI Modells realisiert. Sie werden eingesetzt, um IP-Verkehr zwischen den Anschluss-Routern der einzelnen Standorte zu übertragen.
Das Overlay-Modell erfordert Spezialkenntnisse für die Konzeption und den Betrieb von Router-Netzen sowie die Konfiguration von virtuellen Kanälen auf Basis von ATM- oder Frame Relay. Diese Kenntnisse sind jedoch in vielen Unternehmen nicht vorhanden. Daher bieten fast alle Service Provider so genannte „managed services“, bei denen die einzelnen Anschluss-Router des VPN zentral vom jeweiligen Service Provider konfiguriert und überwacht werden. Der Kunde wird hierdurch von allen Spezialaufgaben rund um das VPN befreit.
Ein Nachteil des Overlay-Moldells ist die schlechte Skalierbarkeit. Hierunter versteht man, dass der Aufwand für die Anschaltung zusätzlicher Standorte überproportional mit der Anzahl bereits angeschalteter Standorte zunimmt. Dies gilt insbesondere für VPNs mit einem hohen

Vermaschungsgrad[6]. Bei vollvermaschten Netzen gibt es beispielsweise insgesamt n*(n-1)/2 Verbindungen. Die Zahl der direkten Verbindungen steigt demnach quadratisch mit der Anzahl n der Standorte. Bei Hinzunahme eines weiteren Standorts muss in diesem Beispiel die Konfiguration aller anderen Anschluss-Router angepasst werden, zu denen eine direkte Verbindung bestehen soll. Nicht nur der Aufwand für die Konfiguration und somit die Fehleranfälligkeit solcher Netze steigt überproportional, sondern auch die betrieblichen Kosten sowie die durchschnittliche Entstörzeit im Fehlerfalle. Sehr große Netze sind somit nur schwer beherrschbar.

Um die Zahl der direkten Verbindungen und die betrieblichen Aufwände sowie die Fehleranfälligkeit deutlich zu reduzieren, betreiben manche Service Provider auf ihrer Plattform kundenspezifische Aggregations-Router bzw. virtuelle Router[7] (siehe **Bild 6**). Hiermit wird die Zahl der Verbindungen von n*(n-1)/2 auf n reduziert. Die Komplexität verringert sich dabei im gleichen Maße. Ein weiterer Vorteil dieses Konzeptes ist, dass gerade bei den häufig zu findenden sternförmigen Netzen, bei denen die Außenstellen jeweils nur mit der Zentrale verbunden sind, der Datenverkehr zwischen den Außenstellen nicht unnötigerweise über die Zentrale geführt wird. Dies verringert den Bandbreitenbedarf am zentralen Anschluss und erhöht zudem die Ausfallsicherheit.

Alternativ zur Verwendung von virtuellen Verbindungen auf der Basis von FR oder ATM können auch Tunnel-Verbindungen, z.B. mit IPSec oder GRE genutzt werden. Mit diesen Tunnel-

[6] Der Vermaschungsgrad gibt an, mit wie vielen Gegenstellen die einzelnen Standorte durchschnittlich verbunden sind. Bei sternförmigen Netzen, bei denen die Unternehmenszentrale jeweils nur mit den einzelnen Außenstelle verbunden ist, beträgt der Vermaschungsgrad 1. Bei vollvermaschten Netzen mit n Standorten, wo zwischen allen Standorten jeweils paarweise eine direkte Verbindung besteht, ist der Vermaschungsgrad demgegenüber (n-1).

[7] Ein virtueller Router verhält sich wie ein normaler Router. Der einzige Unterschioe besteht darin, dass er sich Speicher, CPU sowie Übertargungskapazität, also die Hardware-Ressourcen, mit anderen virtuellen Routern teilt.

Verfahren werden wie im Falle von FR oder ATM ebenfalls Punkt-zu-Punkt realisiert. Der Unterschied liegt darin, dass die Verbindungen hierbei auf Schicht 3 des OSI Modells über eine IP-Plattform (z.B. das Internet) realisiert werden. An dem zugrunde liegenden Overlay-Modell und der oben beschriebenen Einschränkung ändert es sich jedoch nichts. Vielmehr ergeben sich hierdurch weitere Besonderheiten: Zum einen erhöhen sich Komplexität und Kosten, wenn z.B. aufwendiges Schlüsselmanagement genutzt wird, und zum anderen bietet diese Übertragungsverfahren keine definierten Übertragungsqualitäten bzw. Quality of Service (QoS). Die Übertragung geschieht nach dem so genannten „Best Effort“-Prinzip. Feste Übertragungsbandbreiten oder konstante Übertragungsverzögerungen (Delay), wie sie beispielsweise für Sprachübertragung (VoIP: Voice over IP) benötigten werden, können hiermit nicht garantiert werden.
Demgegenüber steht der Vorteil, dass sich z.B. mit Hilfe von IPSec sehr leicht weltweite Verbindungen über das Internet realisieren lassen.
Die Nutzung des Internet als Datenplattform wirft jedoch zusätzliche Sicherheitsfragen auf. Die Zahl der Angriffe aus dem Internet nimmt weiterhin zu. Die Unternehmen sind gezwungen, in immer kürzerer Zeit auf neue Bedrohungen (z.B. Würmer oder Viren) zu reagieren und neue Software-Stände (Patches) in ihre Systeme einzuspielen, wodurch entsprechend der Personalaufwand zunimmt. Hinzu kommt, dass zum Schutz des eigenen Netzes immer mehr Spezialsysteme wie Firewalls, Intrusion Detection Systeme oder Virenscanner eingesetzt werden müssen.

Der entscheidende Nachteil des Overlay-Modell ist seine eingeschränkte Skalierbarkeit für große Netze mit einem hohen Vermaschungsgrad. Durch die Nutzung von virtuellen Routern auf der Provider-Plattform konnte dieser Nachteil teilweise kompensiert werden, wenngleich das grundlegende

Modell erhalten bleibt und das Problem der Skalierbarkeit hiermit nicht grundsätzlich gelöst werden konnte. Ein weiterer Schritt ist das Peer-Modell. Die Bezeichnung Peer-Modell bringt zum Ausdruck, dass die IP-Gegenstelle des Kunden-Router (CE: Customer Edge) nicht wie im Falle des Overlay-Modells ein Kunden-Router in einem anderen Unternehmensstandort ist, sondern ein Zugangs-Router (PE: Provider Edge) des Service Providers auf der VPN-Plattform selbst. Mit Hilfe des Peer-Modell kann ein Service Provider eine weit größere Anzahl von verschiedenen VPNs unterschiedlicher Größe und Komplexität mit geringeren Kosten betreiben.

4. VPN-Basistechnologien

Neben der Kenntnis der unterschiedlichen VPN-Klassen und Konzepte gehört ein grundlegendes Verständnis der wichtigsten VPN-Technologie zum Basiswissen über Virtuelle Private Netze.

Dieser Abschnitt bietet jeweils einen kurzen Überblick über wichtige Basistechnologien, die am häufigsten zum Aufbau von VPNs genutzt werden. Dabei werden lediglich die grundlegenden Eigenschaften vermittelt. Weitergehende Aspekte würden den Rahmen dieses Beitrags sprengen und werden bewusst ausgeklammert.

Von besonderer Bedeutung sind hierbei die Übertragungstechnologien MPLS (Multi Protocol Label Switching) und IPSec (Internet Protocol Security). Diese Technologien werden zukünftig eine immer wichtigere Rolle im Bereich der Branch-Office VPNs einnehmen, wobei MPLS die etablierten Übertragungstechniken wie Frame Relay oder ATM im Bereich der VPN-Lösungen sukzessive ablösen wird. Bereits heute ist IPSec im Bereich der Internet-VPNs bzw. „secure VPNs“ die am häufigsten genutzte Technologie.

Frame Relay

Frame Relay (ITU-T Q.022) ist ein paket- und verbindungsorientiertes Datenübertragungsverfahren und gilt als Weiterentwicklung von X.25. Durch den Verzicht auf Übertragungssicherungsverfahren auf Schicht 3 des OSI-Modells können deutlich höhere Durchsatzraten bzw. Bandbreiten realisiert werden als mit der Vorgängertechnik.

Genauso wie X.25 arbeitet Frame Relay ebenfalls verbindungsorientiert. D.h. zwischen den einzelnen Anschlüssen werden feste virtuelle Verbindungen eingerichtet, die festlegen, über welchen Weg die einzelnen Datenpakete durch die Plattform zum jeweiligen Ziel gelangen.
Die Nutzdaten (z.B. einzelne IP-Pakete) werden dabei jeweils in einem Rahmen (Frame) verpackt. Ein Frame hat eine variable Länge und besteht aus vorangestellten Informationselementen zur Verbindungssteuerung (Header) sowie aus angehängten Informationselementen (Trailer), die das jeweilige Rahmenende markieren. **Bild 7** zeigt den Rahmen des Frame Relay Protokolls. Jeder einzelnen Frame enthält im Header eine Kanalnummer (DLCI[8]), anhand derer er entlang eines „virtuellen Pfads“ durch die Datenplattform vermittelt wird. Die einzelnen Rahmen einer virtuellen Verbindungen nehmen dabei stets den gleichen Übertragungsweg durch die Datenplattform. Die Verbindung ist insofern wie bei einer Mietleitung durch den Provider fest vorgegeben, wenngleich sie nur aufgrund der Kanalnummer virtuell existiert.
Eine wesentliche Eigenschaft von Frame Relay ist, dass sich mit dieser Technik für jede Verbindung eine garantierte Übertragungsbandbreite (CIR: Commited Information Rate) fest vergeben läßt. Diese Eigenschaft macht Frame Relay zu

[8] DLCI: Data Link Connection Identifier

einer QoS-Technologie, mit deren Hilfe sich QoS-VPNs realisieren lassen.

ATM

ATM (Asynchronous Transfer Mode, ITU-T I.361- ITU-T I.366)[9] ist wie Frame Relay ein paket- und verbindungsorientiertes Übertragungsverfahren. Die einzelnen Pakete werden ATM-Zellen genannt. Im Gegensatz zu Frame Relay haben sie eine feste Größe von nur 53 Byte und bestehen aus einem Header von insgesamt 5 Byte und einem Nutzdatenfeld von 48 Byte (**Bild 8**). Ein Tailer wie bei Frame Relay ist aufgrund der festen Größe nicht notwendig. Genauso wie bei Frame Relay werden die Daten verbindungsorientiert übertragen. Dies bedeutet, dass zwischen zwei Endstellen jeweils eine feste virtuelle Verbindung bzw. eine virtuelle Wählverbindung eingerichtet wird. ATM zeichnet sich gegenüber Frame Relay im wesentlich durch höhere Übertragungsraten sowie weiter differenzierte Übertragungsqualitäten in Bezug auf Bandbreite, Übertragungsverzögerung und Zellverlust aus. Aufgrund der zur Verfügung stehenden Übertragungsqualitäten bzw. Verkehrskategorien ist ATM universell sowohl für isochronen[10] Verkehr (wie z.B. Sprache) als auch bursthaften Verkehr (wie z.B. LAN-Kopplung) einsetzbar. Folgende Verkehrskategorien stehen zur Wahl:

Verkehrskategorie	**Beschreibung**
CBR Constant Bit Rate)	Die Verkehrskategorie CBR wird im allgemeinen zur Übertragung von isochronem, zeitsensitivem Verkehr, wie von Sprache und Video, genutzt. Bei CBR werden die einzelnen Zellen mit höchster Priorität und minimaler

[9] siehe Unterrichtsblätter 10/98 bzw. http://www.atmforum.com

[10] Isochrone Anwendungen: Diese Anwendungsklasse erfordert ein sehr geringes Delay sowie eine sehr geringe Delay-Varianz (Jitter).

	Übertragungsverzögerung übertragen.
nrt-VBR (non-real-time Variable Bit Rate)	Die Verkehrskategorie nrt-VBR ist definiert durch eine Spitzenzellrate (PCR: Peak Cell Rate; MBS: Maximum Burst Size) sowie einer garantierten durchschnittlichen Zellrate (SCR: Sustainable Cell Rate) für nicht-synchronen Verkehr, wie z.B. für Anwendungen mit variablem oder burstartigem Verkehrsverhalten, konzipiert. Sie eignet sich daher für die Übertragung von paketorientierten Daten, d.h. für Anwendungen, für die keine Bitsynchronität erforderlich ist. In der Regel wird der nrt-VBR Service genutzt, um Informationen zwischen LANs über ATM zu transportieren.
UBR (Unspecified Bitrate)	Die Verkehrskategorie UBR ist definiert durch eine Spitzenzellrate (PCR: Peak Cell Rate) in Sende- und Empfangsrichtung und speziell für Anwendungen mit stark burstartigem, nicht-synchronem Verhalten geeignet, bei denen keine oder nur geringe Anforderungen hinsichtlich Zellenverzögerung und Zellverzögerungsschwankungen bestehen. Diese Verkehrskategorie ist auch besonders geeignet für Anwendungen, deren Verkehrsverhalten nicht oder nur sehr ungenau vorhersagbar ist (z.B. Internet-Anwendungen). Für die UBR Verkehrskategorie werden dem Anwender keine Güteparameter garantiert.

Um die Nutzdaten an die Größe der ATM-Zellen anzupassen, ist innerhalb des OSI Layers 2 eine zusätzliche Umsetzungsfunktion erforderlich, die als ATM Adaption Layer (AAL) bezeichnet wird. Je nach gewählter Verkehrskategorie bzw. je nach Anwendung stehen hier fünf verschiedene AALs zur Wahl, die an dieser Stelle jedoch nicht im Einzelnen eingeführt werden.

Wichtigster Apaption Layer ist AAL5 (siehe **Bild 9**), der für typischen LAN-Verkehr eingesetzt wird und somit im Bereich der Branch-Office VPN am häufigsten genutzt wird.

MPLS

Im Gegensatz zu ATM und FR ist MPLS eine „Peer-Technologie“, mit deren Hilfe VPNs nach dem bekannten Peer-Modell realisiert werden.
MPLS steht für Multi Protocol Label Switching (RFC 2547) und vereint die Vorteile der schnellen ATM-Vermittlungstechnik mit den Felexibilität von IP-Routing. MPLS bietet die Möglichkeit viele VPNs mit identischen privaten IP-Adressbereichen ohne Adressvermischung transparent über eine MPLS-Plattform zu transportieren. Die Einrichtung eines VPNs wird vollständig im Zugangs-Router zur MPLS-Plattform, den so genanten „Label Edge Router“ (LER), und nicht wie bei ATM- oder Frame Relay basierten VPNs im Kunden-Router (CPE) vorgenommen. Das Innere einer MPLS-Plattform wird von ‚Label Switch Router‘ (LSR) gebildet, die für den VPN-Verkehr völlig transparent sind. Dies bedeutet, dass die einzelnen LSR keine Unterscheidung der einzelnen VPNs treffen und jeglichen Verkehr in gleicher Weise bearbeiten.
Dadurch ist eine gute Skalierbarkeit zur Unterstützung vieler VPNs auf der MPLS-Plattform gewährleistet. Grob gesagt, ist MPLS eine Technik, die die Vorzüge von IP-Routing sowie Layer2-Switching wie beispielsweise bei Frame Relay oder ATM vereint. Routing-Funktionalitäten sind

lediglich in den Zugangsknoten der MPLS-Plattform, den LER, zu finden. Im Inneren wird der Verkehr ähnlich wie bei Frame Relay anhand einer Pfadkennung, dem so genanten Label, vermittelt bzw. „geswitcht“. Das Label ist daher vergleichbar mit der Kanalkennung DLCI im Falle von Frame Relay mit dem einzigen Unterschied, dass dieses Label nicht fest vorkonfiguriert ist, sondern sich dynamisch mit Hilfe der Routing-Funktionalität der LER ergibt. Somit lässt sich die Flexibilität des IP-Routings mit der Übertragungseffizienz des Layer-2-Switchings kombinieren (siehe **Bild 10**).

Getunnelte Übertragungsverfahren (Tunneling):

Tunneling-Verfahren werden eingesetzt, um VPNs über IP-Netze zu realisieren. In diesem Falle spricht man von einem IP-Tunnel. Ein IP-Tunnel wird allgemein dadurch realisiert, dass die Protokolldaten von Layer-2- (z.B. PPP) bzw. Layer-3-Protokollen (z.B. IP) in IP-Pakete eingepackt, an eine feste Zieladresse bzw. den Tunnelendpunkt übertragen und dort entsprechend wieder ausgepackt werden **(siehe Bild 11)**. Mit diesem Verfahren können beispielsweise lokale Netze mit privaten IP-Adressräumen über das öffentliche Internet miteinander vernetzt werden, ohne dass es zu Adresskonflikten kommt. Da die ursprünglichen IP-Pakete mit privaten IP-Adressen aus den lokalen Netzen jeweils in ein neues äußeres IP-Paket mit offiziellen IP-Adressen eingepackt und am Zielpunkt jeweils wieder ausgepackt werden, sind im Internet nur die offiziellen IP-Adressen sichtbar. Ein häufig genutztes Verfahren, das im Bereich der Branch-Office-VPNs Anwendung findet, ist das von CISCO entwickelte und im RFC 2784 spezifizierte Tunnelprotokoll GRE (Generic Route Encapsulation). GRE ist ein sehr einfaches Tunnelverfahren, bei dem die ursprünglichen IP-Paket aus dem internen Unternehmensnetz ein GRE-Header von 8 Byte und eine neuer IP-Header mit einer externen IP-

Adresse vorangestellt wird. Mit Hilfe von GRE werden die innerern IP-Paket lediglich „getunnelt“. Eine Verschlüsselung wird nicht durchgeführt.

Ebenfalls weit verbreitet sind die Layer-2-Tunneling Verfahren PPTP und L2TP, mit deren Hilfe sich Dial-In-VPN realisieren lassen. Im Gegensatz zu dem Layer-3-Tunneling Verfahren IPSec (Internet Protocol Security, RFC 2401) werden die Nutzdaten bei der Übertragung mit PPTP bzw. L2TP ebenfalls unverschlüsselt und ohne Manipulationsschutz übertragen. PPTP ist eine Erweiterung von PPP und wird häufig verwendet, da es fester Bestandteil von Windows ist. L2TP erlaubt gegenüber PPTP zudem den Aufbau sowie den gleichzeitigen Betrieb paralleler Tunnel-Sitzungen (Sessions) zu unterschiedlichen Gegenstellen.

Aufgrund des unzureichenden Schutz bei PPTP sowie L2TP wurden mit IPSec verschiedene Verfahren entwickelt, um die Unversehrtheit (Integrität), die Vertraulichkeit (Privacy) der Nutzdaten sowie die Echtheit (Authentizität) von Absender und Empfänger zu gewährleisten. Hierzu können wahlweise verschiedene Sicherheitsverfahren wie die Hash-Algorithmen MD-5 oder SHA-1 zur Gewährleistung der Datenintegrität sowie bewährte Verschlüsselungsverfahren wie DES (Data Encryption Standard), 3DES (Triple DES) oder AES. IPSec besteht somit nicht aus einem einzigen Protokoll, sondern stellt vielmehr eine Sammlung unterschiedlicher Protokolle und Verfahren bereit, die in unterschiedlichster Kombination eingesetzt werden können. Trotz dieser Vielfalt haben sich dennoch bestimmte Standardkonfiguration bewährt, die in den meisten Fällen zur Anwendung kommen.
IPSec ist inzwischen neben MPLS die wichtigste VPN-Technologie und hat sich im Bereich der Internet-VPNs zum beherrschenden Standard entwickelt.

5. Schlussbetrachtung

VPN ist in mehrerer Hinsicht ein hochkomplexes Thema, das aufgrund der unüberschaubaren Vielfalt an Technologien, Konzepten und Lösungen sehr leicht zur Verwirrung führt. Es ist daher schwer, einen umfassenden Überblick zu gewinnen. Der vorliegende Beitrag versucht, einen kompakten und dennoch verständlichen Zugang zu diesem Themenfeld zu vermitteln, und bietet somit einen Leitfaden für eine weitere Vertiefung.

Bildtexte

Bild 1:

Bild 2:

Bild 3:

Bild 4:

Der Autor

Dipl.-Ing. Stefanus Römer studierte Allgemeine Elektrotechnik an der RWTH Aachen und ist seit 1994 im Konzern Deutsche Telekom im Produktmanagement tätig. Seit April 2001 arbeitet er als Produktmanager bei T-Mobile, wo er insbesondere für das Produkt Mobile IP VPN und für mobile Intranet-Access-Lösungen zuständig ist.

Verwendete Abkürzungen

3DES	
AES	
ATM	Asynchronous Transfer Mode
CE	Customer Edge
CPE	Customer Premise Equipment
CN	Corporate Network
DES	Data Encryption Standard
DLCI	Data Link Connection Identifier
GRE	Generic Route Encapsulation
L2TP	Layer 2 Tunneling Protocol
L2VPN	Layer 2 VPN
L3VPN	Layer 3 VPN
LER	Label Edge Router
LSR	Label Switch Router
MD-5	
MPLS	Multiprotocol Label Switching
FR	Frame Relay
IP	Internet Protocol
IPSec	IP Security
MBS	Maximum Burst Size
QoS	Quality of Service
PCR	Peak Cell Rate
PE	Provider Edge
PGP	Pretty Good Privacy
PPP	Point to Point Protocol
PPTP	Point to Point Tunnelling Protocol
SCR	Sustainable Cell Rate
SHA-1	
SSL	Secure Sockets Layer
VPN	Virtual Private Network

Bild 1: VPNs in verschiedenen Einsatzszenarien.

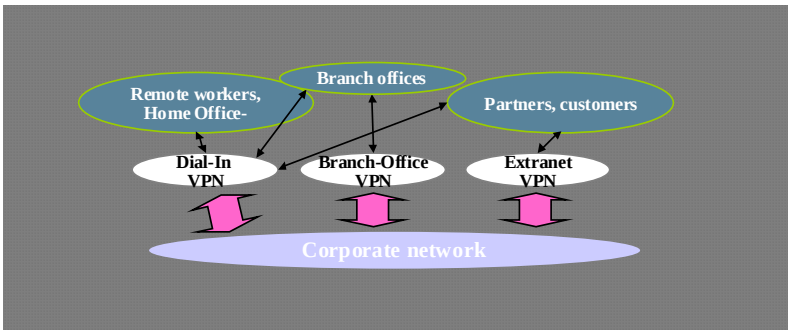


Bild 2: VPN-Technologien im OSI-Modell

VPN Technologien und Protokolle	
OSI Schicht	VPN Protokoll
Transport (Schicht 4)	•Secure Socket Layer (SSL)
Netzwerk (Schicht 3)	•IP Security (IPSec) •Generic Route Encapsulation (GRE) •Multi Protocol Label Switching (MPLS)
Verbindung (Schicht 2)	•Frame Relay (FR) •Asynchronous Transfer Mode (ATM) •Layer 2 Tunnelling Protocol (L2TP) •Point to Point Tunnelling Protocol (PPTP)
Physik (Schicht 1)	•Mietleitungen

Bild 3: CPE-based versus Network-based VPN

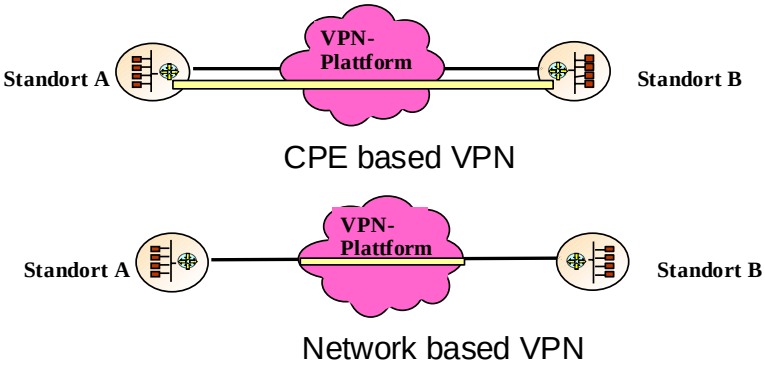


Bild 4: Overlay-Modell: Sternförmiges Netz

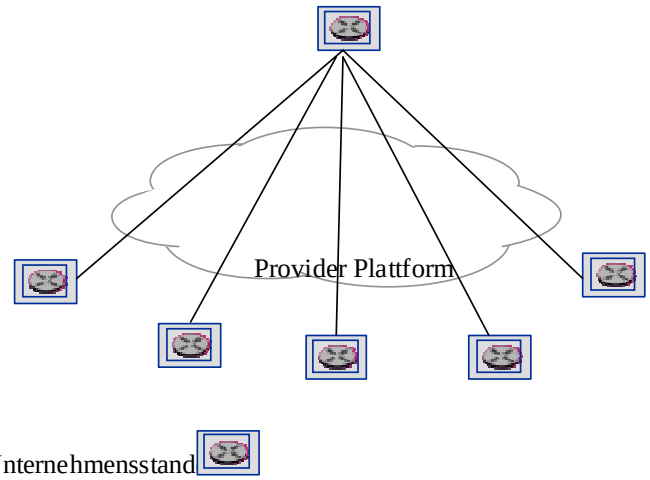


Bild 5: Overlay-Modell: Netz mit hohem Vermaschungsgrad

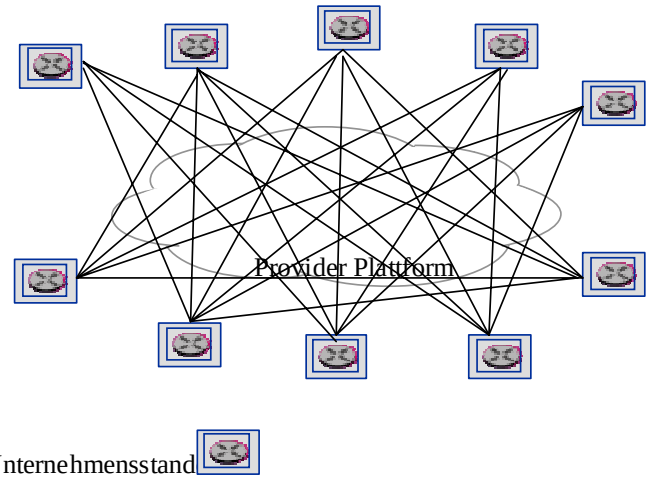


Bild 6: Vollvermaschtes “Any to Any”-Netz mit virtuellen Router

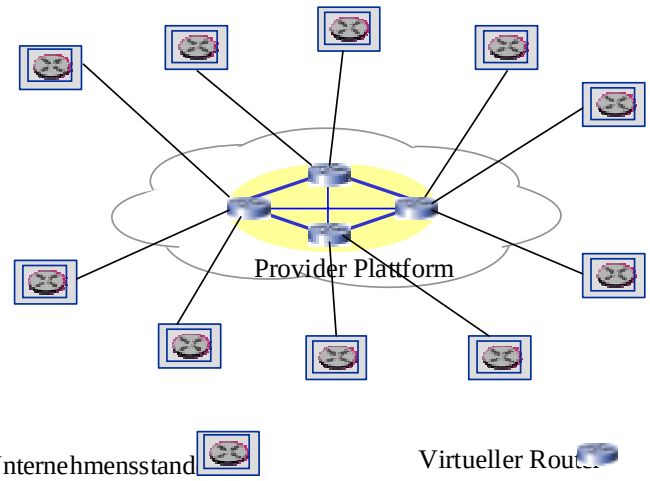


Bild 7: Frame Relay Rahmenformat

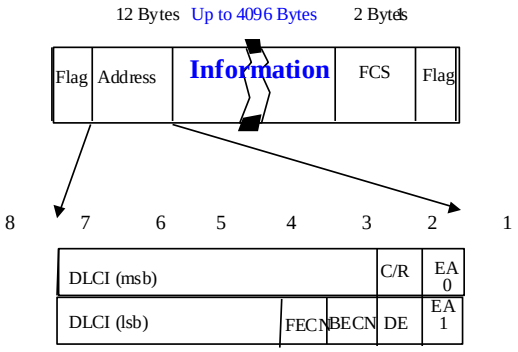


Bild 8: ATM Zellformat

Bild 9: AAL5

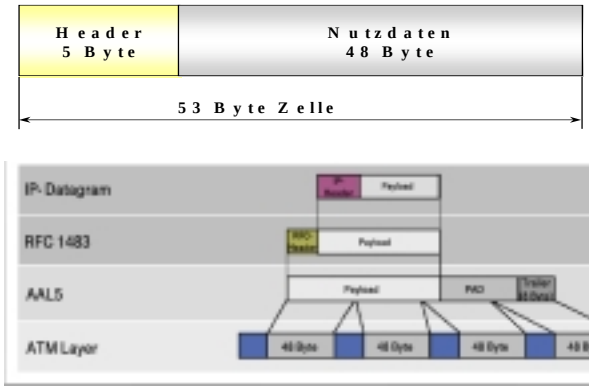


Bild 10: MPLS

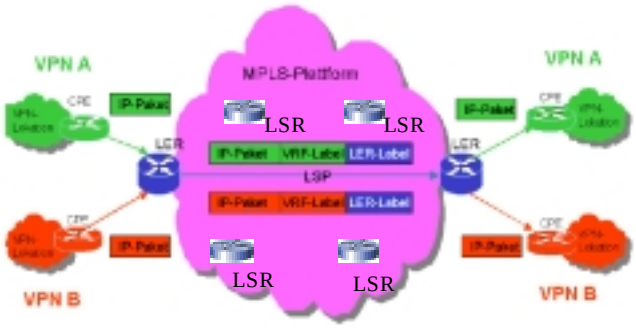
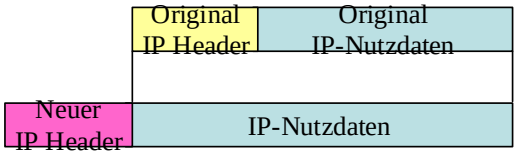


Bild 11: IP-Tunnelverfahren



•Der original IP-Header enthält IP-Adressen aus dem privaten Netz (
•Der neue IP-Header enthält IP-Adressen, die zum IP-Adressbereich
VPN-Plattform des Service Providers gehören.
•Der private Adressbereich ist innerhalb der VPN-Plattform nicht sic