VPN Sicherheit

Marina Sturm
(sturmm@in.tum.de)

Hauptseminar: **Sicherheit in Kommunikationsnetzen**
Technische Universität München

WS 2002 (Version 13.12.2002)

Zusammenfassung

Dieses Papier behandelt den Aufbau und die Sicherheitsaspekte so genannter VPNs (Virtual Private Networks). Dies sind private Netzwerke, z.B. Unternehmensnetzwerke, innerhalb eines öffentlichen Netzwerks, wie z.B. dem Internet.
Nach einer kurzen Einführung, in der auch die Vorläufer dieser Netzwerke kurz vorgestellt werden, wird auf die verschiedenen Anforderungen an VPNs eingegangen. Anschließend werden die verschiedenen VPN-Typen behandelt, die jeweils wieder auf einer Basis von unterschiedlichen Technologien aufgebaut sein können. Der zentrale Punkt dieser Ausarbeitung wird sich dann mit der Frage der Sicherheit in VPNs beschäftigen. Durch den Übergang zu konvergenten Netzen hat das Thema Quality of Service (QoS) auch für VPNs große Bedeutung erlangt. Eine Schlüsseltechnologie in diesem Zusammenhang, MPLS, wird im vorletzten Kapitel behandelt. Zum Abschluss wird noch auf VLANs eingegangen. Dabei handelt es sich um eine Technologie zur Bildung von Intranet-VPNs, also VPNs innerhalb eines „privaten“ Netzes.

INHALTSVERZEICHNIS

1 Einführung

Anfänglich benutzten Unternehmen das Internet, um für ihre Firma, ihre Produkte und Services zu werben, indem sie auf WWW-Servern ihre Unternehmens-Seiten ins Netz stellten. Doch im Laufe der letzten Jahre legten die Unternehmen ihren Focus immer mehr auf E-Business.
Dies macht zunehmend erforderlich, dass Geschäftspartner und Zulieferer Zugang zu Daten im Firmen-Intranet erhalten, entweder für eine kurzfristige Zusammenarbeit während eines gemeinsamen Joint-Venture-Projekts oder für eine langfristige strategische Zusammenarbeit.
Des Weiteren verteilen sich global tätige Unternehmen heutzutage auf eine Vielzahl von Unternehmensstandorten, die untereinander kommunizieren.
Auch Mitarbeiter müssen, wenn sie vor Ort bei einem Kunden sind, von unterwegs oder von zu Hause aus als Telearbeiter (*Home Office*) Zugang zu den Informations-Ressourcen ihrer Unternehmens-Intranets haben.
Die Unternehmen suchen hierbei die beste, d.h. kosten-effektivste und sicherste, Lösung, um Remote User, Zweigstellen und Geschäftspartner in ein erweitertes *Corporate Network* einzubinden.
Die herkömmlichen Techniken, mit denen dies bisher realisiert wurde, werden im folgenden Kapitel etwas näher vorgestellt.
Sie bieten jedoch keine perfekte Lösung für die oben angesprochenen Problematiken.
Daher wird zunehmend von diesen „Lösungen“ Abstand genommen und stattdessen ein vollkommen neuer Ansatz verwendet, die so genannten VPNs.

1.1 VPN-Vorläufer

Die früheren Lösungen für die Netzwerkkommunikation zwischen dem Unternehmen und seinen Zweigstellen und Geschäftspartnern etc. wie exklusive Mietleitungen (Leased Lines), Ferngespräche (ISDN,…) oder VPN-Vorläufer, wie z.B. exklusive ATM-VCs, Frame Relay-PVCs, X.25-Verbindungen durch Providernetze bieten nicht die nötige Flexibilität, um schnell neue Verbindungen zu Geschäftspartnern oder für Projektteams im Außeneinsatz einzurichten und sind ebenfalls nicht die preiswertesten Varianten.

1.2 Vorteile von VPNs

Die wachsende Zahl an Telearbeitern und Vertriebs- und anderen Angestellten im Außeneinsatz, die sich über Analog-Modems oder ISDN direkt in das Unternehmensnetz einwählen, frisst immer mehr Ressourcen in Form von finanziellen Mitteln für Modems, ISDN-Karten, Remote-Access-Server und Telefongebühren. Auch Standleitungen zu Zweigstellen und Geschäftskunden stellen einen großen Posten im Kommunikationsbudget eines Unternehmens dar.
Während man mit der oben erwähnten partiellen Nutzung von Providernetzen über ATM, Frame Relay, etc. gegenüber Leased Lines zwar einspart, sind diese Kommunikationskanäle aber immer noch erheblich teurer als eine Nutzung des Internets.

Die so genannten Virtual Private Networks (VPNs), die das Internet nutzen, lösen viele der oben angesprochenen Probleme. Sie erlauben es, Zweigstellen, Geschäftspartner als auch Remote Access Mitarbeiter kostengünstig an das zentrale Unternehmensnetz anzubinden.
Hierbei bieten lokale Internet Service Provider (ISP) für Außendienst-Mitarbeiter einen kostengünstigen Zugang zum Internet - und damit zu deren Firma. Die Kosten für Ferngespräche und das vor-

her notwendige Equipment, wie z.B. große Einwahl-Modem-Arrays und ISDN-Zugangspunkte im Unternehmen, entfallen somit.
Im Fall der Anbindung von verschiedenen Unternehmensstandorten, Geschäftspartnern und Zulieferern nutzt ein VPN anstatt der bisher eingesetzten Mietleitungen oder Frame Relay-PVCs, die offene verteilte Infrastruktur des Internets, um Daten zwischen Unternehmensstandorten zu übertragen. Insgesamt werden also die vielen verschiedenen herkömmlichen Zugangswege durch einen einzigen breitbandigen Internet-Zugang ersetzt, über den zur gleichen Zeit der Verkehr der Remote User, der LAN-to-LAN-Verkehr und der Internet-Verkehr fließen.

Ein VPN Forschungsbericht von Infonetics Research aus dem Jahre 1997 spricht von Einsparungen von 20% bis 47 % an WAN-Kosten durch den Einsatz von VPNs anstatt von Mietleitungen. Für Remote Access VPNs, sollen sich die Einsparungen sogar auf 60% bis 80% der normalen Remote Access Wählverbindungs-Kosten belaufen [Murhammer et. al. 99].
Der Spitzname „Very Profitable Network“ [Lipp2001] kommt also nicht von ungefähr.

Darüber hinaus bieten Internet-VPNs eine große Flexibilität. Man kann beispielsweise sehr schnell neue Benutzer und Standorte in sein Netzwerk einbinden. Ein neuer Remote-Access-Nutzer muss sich dafür nur beim ISP und im eigenen Unternehmens-Netzwerk anmelden und sofort ist das VPN für ihn zugänglich. Es sind jetzt keine neuen Geräte oder etwa gar Zugangsleitungen mehr nötig. Die virtuellen Verbindungen können bei Bedarf aktiviert werden, unterstützen damit also die Flexibilität und Kosteneffizienz des VPNs. Gemietete Leitungen hingegen verursachen auch dann Kosten, wenn die Kapazitäten ungenutzt bleiben [Ling2002].
Weiterhin sind VPNs in der Regel beliebig erweiterbar und relativ problemlos in vorhandene Netzwerkstrukturen integrierbar.

Aber IP-VPNs haben auch ihre Nachteile. Beim Datenaustausch über das Internet ist es unausweichlich, dass die Daten verschiedene unbekannte Teilnetze passieren. Diese Art der Datenübertragung ist aber für sensitive, firmeninterne Daten ohne jegliche Art von Sicherheitsvorkehrungen nicht tragbar. Das verwendete VPN-Protokoll innerhalb des IP-Netzwerkes muss also folgende Voraussetzungen erfüllen: *Vertraulichkeit, Integrität und Authentizität.*
Ein weiterer Nachteil bei der Nutzung des Internets zur Datenübertragung gegenüber den herkömmlichen Technologien wie Standleitungen, ATM und Frame Relay, ist der Verlust der garantierbaren Bandbreiten und Verzögerungszeiten (Dienstqualität).
Eine VPN Technologie, MPLS (*Multi Protocol Label Switching*), die diesem Problem begegnet, wird im Kapitel 7 vorgestellt.

1.3 VPN - Allgemeine Definition

Nach [Lipp2001] ist ein Virtual Private Network (VPN) ein Netzwerk, das ein öffentliches Netzwerk benutzt, um private Daten zu transportieren, d.h. ein privates Netzwerk innerhalb eines öffentlichen Netzes, wie dem globalen Internet.
Erreicht wird dies durch sichere private Verbindungen, vorwiegend durch private Tunnel, über die Remote User, Zweigstellen und Geschäftspartner in das erweiterte Corporate Network eingebunden werden.

Es ist **VIRTUAL**:
Die Verbindungen werden dynamisch je nach Bedarf aufgebaut. Es besteht also keine permanente private physikalische Verbindung. Die physikalische Infrastruktur des Netzwerks ist dabei transparent für jede VPN Verbindung.

Oft wird dieser Begriff auch mit der Bedeutung gebraucht, dass das physikalische Netzwerk nicht dem VPN Benutzer gehört, sondern ein öffentliches Netzwerk ist, das mit vielen anderen Usern geteilt wird.

Es ist **PRIVATE**:
Um die Privatheit des Verkehrs innerhalb des öffentlichen Netzes (logische „private“ Verbindung) zu gewährleisten, sind diverse Sicherheitsanforderungen (Authentifizierung, Verschlüsselung, Tunneling) nötig.

Es ist ein **NETWORK**:
Obwohl nicht physisch existent, muss ein VPN als Erweiterung eines Unternehmensnetzwerks angesehen und behandelt werden.

Um sicherzugehen, dass die Daten vollständig und unverändert beim Empfänger ankommen und die Vertraulichkeit gewahrt bleibt, werden die Pakete meist getunnelt, müssen dann authentifiziert werden und zusätzlich eventuell noch verschlüsselt. Auf diese Mechanismen werden wir später noch genauer eingehen.
Kurz gesagt stellen VPNs also nichts anderes dar als die verschlüsselte und authentifizierte Kommunikation über öffentliche Netzwerke.

[Lipp2001] erklärt das **Gegenstück zum VPN**, also ein **echtes privates Netzwerk** folgendermaßen:
Dies ist ein Netzwerk, das exklusiv von einem Unternehmen oder Organisation betrieben wird, wobei alle Übertragungseinrichtungen und –medien diesem Unternehmen gehören oder ihm zur exklusiven Nutzung überlassen werden.
Beispiele wären z.B. Mietleitungen oder Standardfestverbindungen, die der Organisation zur ausschließlichen Nutzung vermietet werden.
Ein öffentliches Netzwerk hingegen ist eine Kommunikationsinfrastruktur, die von einem Dienstleistungsunternehmen betrieben wird, das die Benutzung des Netzes jedermann gegen entsprechendes Verbindungsentgelt gewährt.

Ein VPN versucht, private und öffentliche Trägernetzwerke zu kombinieren, indem ein öffentliches Netzwerk als Trägernetzwerk für die private Kommunikation benutzt wird.

2 Anforderungen an VPNs

Die Einsatzgebiete für VPNs sind sehr vielfältig. Welche Technologien (Verschlüsselung, Tunneling-Protokolle, etc.) hierfür verwendet werden, hängt ganz allein von den gestellten Anforderungen ab.
Im Folgenden werden die wichtigsten Anforderungen näher beleuchtet:

Sicherheit

Der Begriff Sicherheit ist ein ganz zentraler Punkt beim Einsatz eines VPNs, da hier ein öffentliches Netzwerk für den Transport privater Daten verwendet wird.
In der heterogenen Umgebung eines VPNs (ISP, Intranet, Internet…) gibt es viele Möglichkeiten, Datenströme abzuhören, zu verändern, oder eine Adressänderung an Datenpaketen vorzunehmen. Daher müssen in VPNs gewisse Mechanismen zum Einsatz kommen, die die Sicherheit der Daten beim Transport zwischen Sender und Empfänger gewährleisten. Diese Mechanismen werden in Kapitel 5 genauer behandelt.

Transparenz

Es ist erstrebenswert, dass eine VPN-Lösung möglichst keine Anforderungen bezüglich der Interaktion des Benutzers oder der verwendeten Applikationen stellt. Diese Anforderung wird von verschiedenen VPN-Lösungen verschieden gut erfüllt.

Verfügbarkeit

Es ist wünschenswert, dass die Verfügbarkeit eines VPNs mindestens genauso gut wie bei herkömmlichen WAN-Infrastrukturen (Standardfestverbindungen, Frame Relay, ISDN,…) ist, die durch das VPN ersetzt werden.

Performance und Skalierbarkeit

Für die Garantie der Sicherheit von Daten in VPNs sind, abhängig von der eingesetzten Technologie, aufwendige Verschlüsselungsverfahren notwendig. Die Verschlüsselung für breitbandige Strecken in Echtzeit durchzuführen, kann zu einem Problem werden. Zudem stellt die Verwaltung vieler gleichzeitiger VPN-Verbindungen zu verschiedenen Zweigstellen, Geschäftspartnern und Außendienstmitarbeitern hohe Anforderungen an die VPN-Hardware.
Die Wahl der eingesetzten VPN-Lösung ist von entscheidender Bedeutung im Hinblick auf die Gewährleistung einer langfristigen Skalierbarkeit bezüglich der Benutzerzahlen und Bandbreiten.

Quality-of-Service (QoS)

Mit herkömmlichen WAN-Lösungen (ISDN, Frame Relay, ATM) kann man die meisten Verbindungen mit garantierten, festen Bandbreiten und Verzögerungszeiten betreiben. Bei der Nutzung eines VPNs hat man das Problem, diesen garantierten Service Level einer privaten WAN-Verbindung auch auf einer virtuellen Verbindung über das Internet zu erhalten. Früher war es kein Problem, dass IP als verbindungsloses asynchrones Protokoll keine bestimmte Zeitdauer für die Paketübertragung oder überhaupt die Paketzustellung garantiert, doch mit neuen Realtime-

Applikationen wie VoIP oder Multimedia-Streaming sind gewissse QoS-Anforderungen verbunden. Falls also solche Applikationen über das VPN laufen sollen, ist dies schon bei der Auswahl der verwendeten VPN-Technologie zu berücksichtigen, um später die geforderten QoS-Level bereitstellen zu können.

Migrationsfähigkeit

Bei der Entscheidung für eine VPN-Technologie ist zu berücksichtigen, ob diese auf einem offenen Standard basiert und man dadurch freie Hand bei der Herstellerauswahl der Komponenten hat oder man sich durch Wahl einer proprietären Technologie komplett vom Produkt-Portfolio eines einzelnen Herstellers abhängig macht. Wichtig ist auch, darauf zu achten, inwieweit die verwendete Lösung aus modularen Komponenten aufgebaut und damit später um neue Features erweiterbar ist.

Interoperabilität (versch. VPN-Systeme)

Je nach eingesetzter VPN-Technologie können mehrere Parteien (Provider, Endkunde,…) am Aufbau des VPN-Systems beteiligt sein, die unter Umständen Equipment verschiedener Hersteller einsetzen. Auch bei Extranets können bei den verschiedenen Geschäftspartnern VPN-Produkte unterschiedlicher Ausrüster im Einsatz sein. Damit das VPN dennoch funktioniert, müssen die verschiedenen Produkte natürlich untereinander kompatibel sein, was praktisch nur mit Produkten, die den IETF-Standards entsprechen, zu gewährleisten ist.

Integration in existierende Netze

Bei der Auswahl einer VPN-Technologie ist zu berücksichtigen, inwiefern diese problemlos in die schon bestehende Netzwerk-Infrastruktur (LANs, WANs, Remote-Dienste,…) integriert werden kann. Ebenso muss das VPN möglichst nahtlos in die vorhandene Sicherheitsstrategie (*Security Policy*) einer Organisation integrierbar sein. Eine solche definiert Konzepte, welche Daten wie vor welchen Angriffen zu schützen sind. Aus diesen Anforderungen werden dann konkrete Sicherheitsmaßnahmen wie z.B. Authentifizierungs- und Verschlüsselungsverfahren abgeleitet.

Koexistenz zu traditionellen WAN-Strukturen

Üblicherweise findet eine Ablösung von traditionellen WAN-Netzen (Frame Relay, ATM) durch VPNs nicht von einem Tag auf den anderen statt, sondern es werden während einer Migrationsphase beide Lösungen gleichzeitig betrieben. Auch im Fall von Remote Access werden oftmals traditionelle Remote Access- und VPN Remote Access-Lösungen parallel betrieben, wobei die traditionellen Lösungen als Backup-Lösung dienen.

Managebarkeit

Für den Administrator eines VPNs ist es von entscheidender Bedeutung, ob für das zu verwendende Produkt mächtige Management-Tools verfügbar sind, die eine einfache Verwaltung aller Bestandteile einer VPN-Lösung unter einer Oberfläche ermöglichen und darüber hinaus für die Remote-Administration ausgelegt sind. Des Weiteren ist es wichtig, dass der Administrationsaufwand auch bei wachsender Anzahl an Benutzern und Sites, die in das VPN eingebunden werden müssen, vertretbar bleibt.

3 VPN-Topologien

Abhängig vom Einsatzgebiet unterscheidet man zwischen den folgenden VPN-Topologien:

3.1 Remote-Access-VPN (Host-to-Network)

Als Remote User bezeichnet man Telearbeiter, die zuhause für das Unternehmen arbeiten, oder Außendienst-Mitarbeiter, die unterwegs vor Ort bei Kunden arbeiten [Murhammer et. al. 99]. Diesen Mitarbeitern muss von ihren lokalen Systemen Zugriff auf das Unternehmensnetz ermöglicht werden.
Früher geschah dies durch direkte Ferngesprächs-Telefonverbindungen zu einem Remote Access Concentrator (RAC) im Unternehmensnetz. Ein RAC ist ein System, das an öffentliche Telefonnetze angeschlossen wird und analoge und digitale Einwahl aus diesen Netzen in das Unternehmens-Intranet ermöglicht.
Diese Lösung hat diverse Nachteile:

- Es fallen hohe Kosten für die Ferngesprächsgebühren an, insbesondere wenn es sich bei Mitarbeitern im Auslandseinsatz um internationale Ferngespräche handelt.
- Ein RAC muss verschiedene analoge und digitale Protokolle terminieren können und ist damit technisch relativ komplex.
- Ein RAC muss skalierbar sein, da die Anzahl der benötigten Einwahl-Ports und die Bandbreiteanforderungen in der Regel stetig wachsen. Nichtsdestotrotz ist die Auslastung oft niedrig, da nicht immer alle Ports belegt sind und damit die Kosten pro Nutzer hoch. Andererseits muss man genügend Ports vorsehen, damit nicht im Fall hoher Last alle Ports belegt sind.

All diese Faktoren machen herkömmliche Remote Access-Lösungen zu einer teuren Angelegenheit.

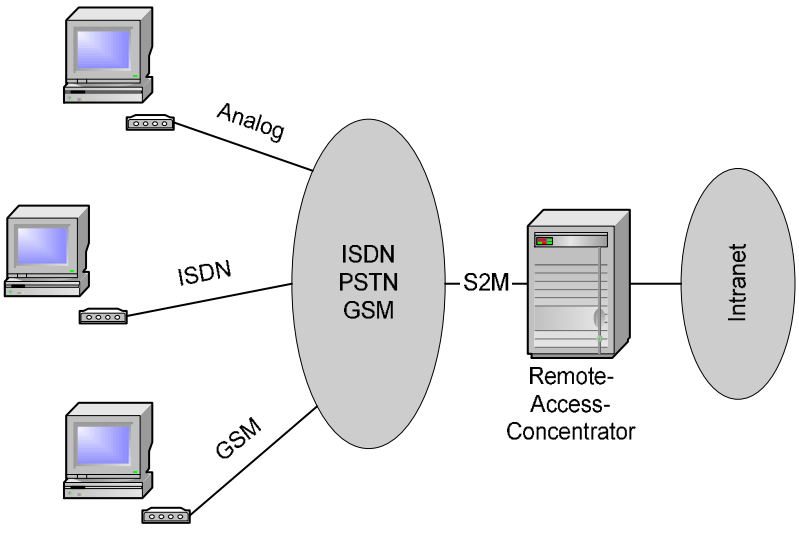


Abbildung 3-1: Remote-Access (herkömmlich)

Ein Remote-Access-VPN [Murhammer et. al. 99] löst diese Probleme:
Hierbei erfolgt die Einwahl eines Remote-Mitarbeiters über eine PPP-Wählverbindung zum lokalen ISP und von dort weiter über das Internet zum Unternehmensnetzwerk. Der Endkunde braucht kein Equipment mehr zur Terminierung der Wählverbindungen bereitzuhalten, dies erledigen die ISPs vor Ort. Damit der Transit der Daten über das Internet sicher abläuft, werden sie in einem Tunnel

(siehe Kapitel 5) transportiert und nur dieser muss im so genannten VPN-Konzentrator beim Endkunden terminiert werden.

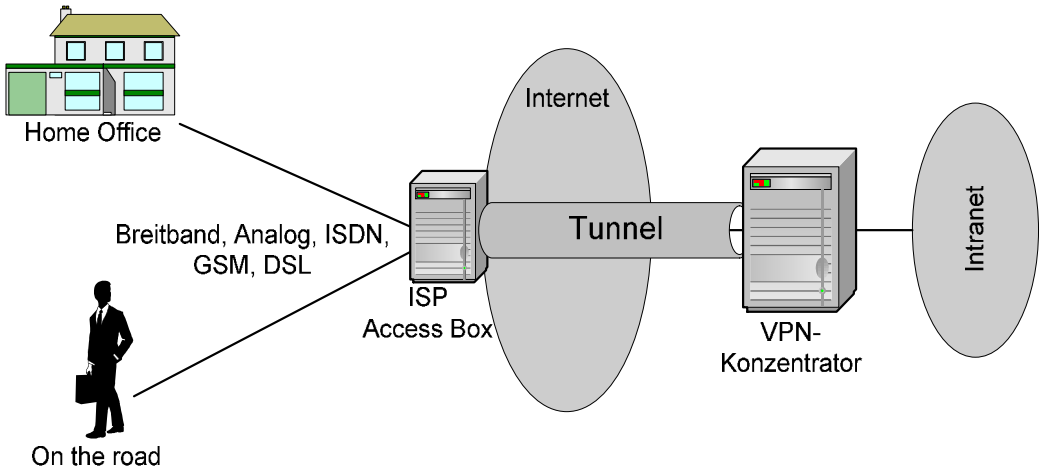


Abbildung 3-2: Remote-Access-VPN

Für den Ursprung des Tunnels auf Remote Client-Seite gibt es zwei Alternativen:

- Es wird ein Software-Client direkt auf dem Remote-Rechner installiert, um den Tunnel zum VPN-Konzentrator aufzubauen (sehr verbreitet).
- In seltenen Fällen wird der Tunnel erst im RAC des ISP initiiert, was eine spezielle Client-Software unnötig macht (Abb. 3-2).

Für den Aufbau der Tunnel können verschiedene Tunneling-Protokolle zum Einsatz kommen, auf die in Kapitel 5 näher eingegangen wird.
Wie oben schon erwähnt, weist die VPN-Lösung erhebliche Vorteile gegenüber dem klassischen Remote Access auf:

- Die Hardware zum Terminieren der Verbindungen im Unternehmen ist kostengünstig und einfach, da sie keine Vielzahl von Technologien, wie Telefonsignalisierung, Modemprotokolle, Analogverarbeitung, etc. implementieren muss, der RAC steht vor Ort beim ISP.
- Die Verbindungsgebühren werden minimiert (Kostenvorteil von 70-80 % laut [Lipp2001]), da nur die Einwahlgebühr zum lokalen ISP entrichtet werden muss.

3.2 Host-to-Host-VPN

Bei dieser Topologie besteht eine direkte VPN-Verbindung zwischen zwei einzelnen Hosts über das Internet. Dies läuft ohne Zutun des ISPs und ohne den Einsatz von VPN-Gateways und Tunneling ab. Die Hosts haben in diesem Fall eine spezielle VPN-Software installiert, welche die Daten ab der Schicht 4 bzw.5 verschlüsselt.

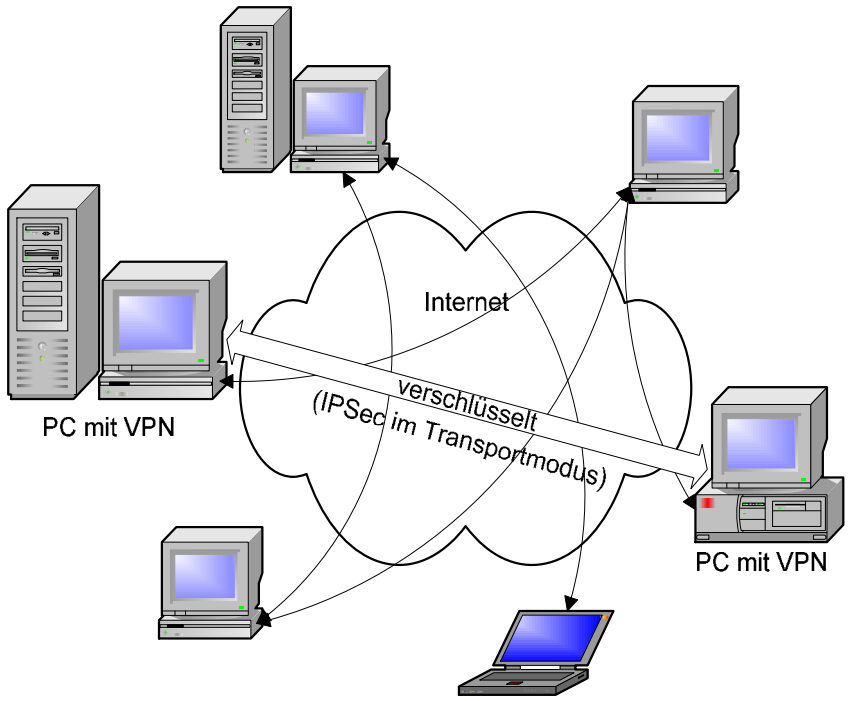


Abbildung 3-3: Host-to-Host-VPN

3.3 Branch-Office-VPN (Network-to-Network)

Bisher wurde die Verbindung verschiedener Standorte eines Unternehmens durch herkömmliche WAN-Verbindungen (Leased Lines, Frame Relay oder ATM) erledigt.

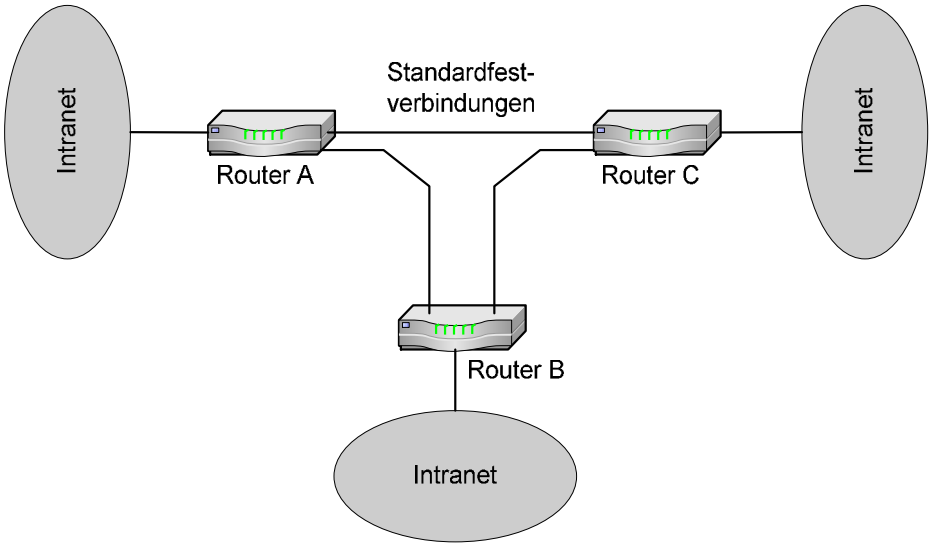


Abbildung 3-4: Branch-Office (herkömmlich)

Der Nachteil bei diesen Lösungen sind die damit verbundenen hohen Kosten, ganz besonders bei weit entfernten Standorten. Das Problem verschlimmert sich noch durch die zunehmenden Globalisierungs-Tendenzen, internationale Fusionen und Kooperationen von Großunternehmen.
Als Ausweg aus dem Kostendilemma bieten sich so genannte Branch Office-VPNs (Site-to-Site-VPNs) an.

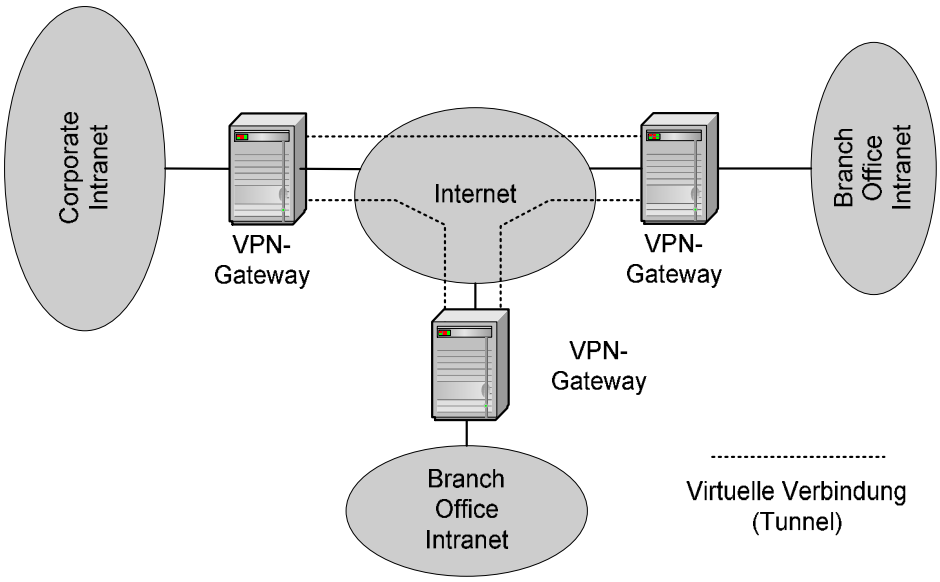


Abbildung 3-5: Branch-Office-VPN

Bei dieser VPN-Lösung werden die Unternehmensnetze über VPN-Gateways und den ISP über das Internet verbunden. Die kostenintensiven, direkten Verbindungen zwischen den Netzen werden durch 2 sehr kurze Verbindungen zwischen den Standorten und den Zugangsknoten eines ISPs ersetzt, die verbleibende Strecke zwischen den POPs der ISPs läuft über das Internet. Damit die Kommunikation über das Internet sicher abläuft, wird zwischen den VPN-Gateways ein sicherer Tunnel aufgebaut, durch den die Daten transportiert werden. Das Einsparpotential ist hier etwas niedriger (bis zu 50 %) [Murhammer et. al. 99] als bei Remote-Access-VPNs.

3.4 Extranet-VPN (Network-to-Network)

Ein Extranet-VPN ist von seiner Struktur her ähnlich wie ein Branch-Office-VPN aufgebaut. Der Unterschied liegt in der Natur der Teilnehmer: mit einem Extranet-VPN gewährt eine Firma ausgewählten Geschäftspartnern und Zulieferern Zugriff auf Teile (Zugriffsbeschränkung über Firewall) ihres internen Firmennetzes für den Austausch von vertraulichen Daten mit diesen.

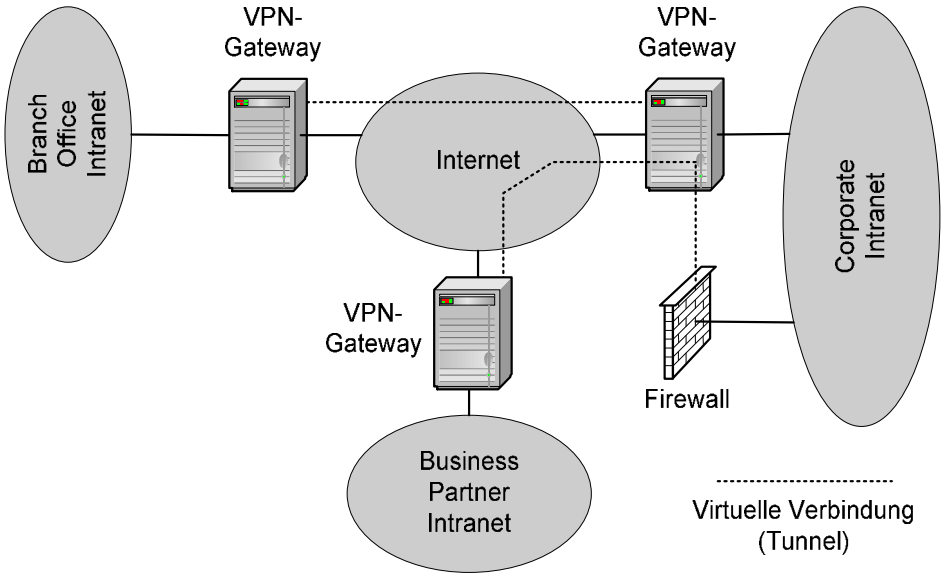


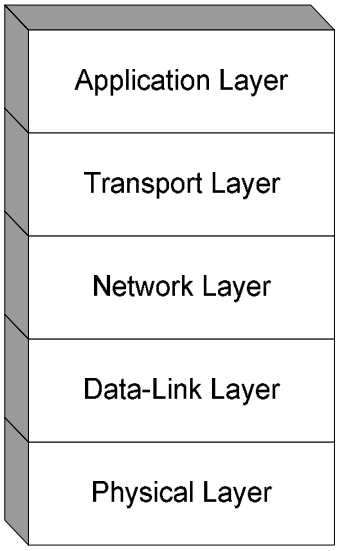
Abbildung 3-6: Extranet-VPN

3.5 Intranet-VPN

VPNs sind auch hervorragend innerhalb eines geschlossenen Unternehmensnetzwerkes einsetzbar, um auch dort vertrauliche Kommunikation innerhalb des „öffentlichen“ Intranets zu ermöglichen. Dies wird z.B. durch die Etablierung von unternehmensinternen IPSec-Verbindungen (siehe Kapitel 5) erreicht. Ein solches Vorgehen ist verständlich, wenn man bedenkt, dass ein erheblicher Teil des Gesamtschadens, der jährlich durch Betriebsspionage entsteht, von Mitarbeitern aus dem eigenen Haus verursacht [Schob99] wird.
Eine andere Art von Intranet-VPNs sind die so genannten VLANs (siehe Kapitel 8), die meist verwendet werden, um Gruppen oder Organisationseinheiten unternehmensintern voneinander zu trennen und ihnen eine „eigene“ Infrastruktur zur Verfügung zu stellen.

4 VPN-Technologien

Bevor man sich für eine VPN-Lösung entscheidet, muss man sich erst einmal darüber klar werden, welche Funktionen ein VPN übernehmen soll. So macht es wenig Sinn, vollwertige VPN-Gateways zu installieren, wenn nur die firmeninterne E-Mail zwischen zwei Filialen geschützt werden soll.
Die verschiedenen verfügbaren VPN-Technologien sind auf verschiedenen Schichten des OSI-Modells [Tanen96] angesiedelt. In welcher Schicht ein Protokoll ansetzt, ist dabei entscheidend für dessen Einsatzbereich.
Im ersten Fall ist die Applikation, wie z.B. ein Web Browser, ein Telnet Client oder ein E-mail-Programm selbst dafür zuständig, die Daten verschlüsselt zu übertragen - der Kommunikationspartner muss dann auch eine Anwendung mit entsprechenden Fähigkeiten einsetzen. Der bekannteste Fall für diesen Ansatz dürfte E-Mail sein. Die Kryptoprotokolle, die hier zum Einsatz kommen, sind PEM (*Privacy Enhanced Mail*), PGP (*Pretty Good Privacy*) und S/MIME (*Secure Multipurpose Mail Extensions*). S/MIME wird unter anderem von den Mail-Clients von Netscape Communicator und Microsoft Internet Explorer benutzt.
Telnet-Clients - ebenfalls auf Anwendungsebene - verwenden SSH (*Secure Shell*) als Kryptoprotokoll [Schmeh98].



ISO-OSI-Schichtenmodell

- PEM, PGP, S/MIME, S-HTTP, SSH, VLANs (applikationsbasiert)
- SSL
- IPSec, VLANs (Protokoll- oder IP-Adress-basiert)
- MPLS
- L2TP, L2F, PPTP, VLANs (MAC-basiert), WEP (WLAN)
- VLANs (portbasiert)

Die Web-Browser sind ein weiteres Beispiel für anwendungsbasierte Verschlüsselung: SSL (*Secure Sockets Layer*) diente ursprünglich nur zur gesicherten Übertragung von HTTP-Daten, inzwischen lassen sich damit aber auch andere Anwendungsprotokolle behandeln.
Es ist ein Kryptoprotokoll für die Applikationsschicht, das eine Schicht zwischen Anwendungs- und Transportschicht einfügt, und arbeitet ausschließlich mit TCP zusammen.
Der Nachteil einer Verschlüsselung auf der Applikationsschicht ist die Notwendigkeit, jede verwendete Software einzeln zu konfigurieren. Allerdings sind nicht die geringsten Änderungen an Netzwerkgeräten erforderlich.
Eine andere Technologie, die mit unter zu dieser Ebene gezählt wird, sind die applikationsbasierten VLANs. Auf die Technologie der VLANs wird im Kapitel 7 noch genauer eingegangen.
Eine weitere Möglichkeit, VPNs zu realisieren, ist der Eingriff direkt auf IP-Ebene. Hier hat sich inzwischen ein Standard-Krypto- und Tunnelingprotokoll durchgesetzt: IPSec (*IP Security Protocol*) ist nahezu vollständig von der Internet Engineering Task Force (IETF) in RFCs festgelegt. Ein

Vorteil dieses Protokolls ist die Möglichkeit, im Gegensatz zu SSL, bei dem nur Ende-zu-Ende Absicherung möglich ist, nur Teilstrecken zwischen Endsystemen abzusichern.
Auf dieser Ebene kommt zusätzlich noch ein weiterer VLAN-Typ zum Einsatz, und zwar die Protokoll- und IP-Adress-basierten VLANs.
Zwischen Schicht 3 und 2 ordnet man MPLS ein. MPLS ermöglicht den Aufbau sicherer Tunnel durch ein Netz, indem virtuelle Pfade, sog. *Label Switched Paths*, geschaltet werden.
Mit Windows NT 4.0 hat die nächste Möglichkeit für ein VPN - das Layer-2-Tunneling - eine gewisse Popularität erlangt: der Eingriff direkt auf der Verbindungsebene (Data Link Layer). Microsoft`s Technik nennt sich PPTP (*Point-to-Point Tunneling Protocol*). Aber mit dieser Entwicklung blieb Microsoft nicht alleine auf dem Markt, denn Cisco entwickelte - gleichzeitig zu Microsoft - sein eigenes Layer-2 Tunneling-Protokoll L2F (*Layer 2 Forwarding*). Nachdem diese beiden Protokolle aber zueinander völlig inkompatibel waren, entschieden sich Microsoft und Cisco schließlich, zusammen mit einigen anderen Firmen, in einer PPP Working Group das neue Layer-2 Tunneling-Protokoll L2TP (*Layer 2 Tunneling Protocol*), das auf den beiden vorherigen aufbaut, zu entwickeln.
Auch auf dieser und der darunterliegenden Schicht 1 kommen zusätzlich verschiedene VLAN-Typen zum Einsatz. Man unterscheidet hier die MAC-basierten und portbasierten VLANs.

Eine umfassende Sicherheits-Lösung für ein VPN ist in manchen Fällen nur durch eine Kombination der eben erläuterten Optionen bzw. Technologien zu erreichen.
Daher ist vor Implementierungsbeginn eine Festlegung einer VPN-Sicherheits-Politik notwendig, in der festgelegt wird, welche Anforderungen das geplante VPN zu erfüllen hat. Sie beschreibt beispielsweise den Verkehr, der geschützt werden soll (Quelle, Ziel, Protokolle und Ports), vor wem dieser geschützt werden soll und die Sicherheitsanforderungen für den Schutz an sich (Authentifizierung, Verschlüsselung, Schlüssellängen, etc.) [Murhammer et. al. 99].

Auf einige der eben erwähnten Technologien, vorwiegend die Tunneling-Protokolle auf Schicht 2 und 3, wollen wir nun im nächsten Punkt etwas genauer eingehen.

5 Sicherheit in VPNs

In diesem Kapitel werden die VPN-Mechanismen, die die Sicherung der privaten Daten beim Transport durch das Internet gewährleisten, genauer beleuchtet.
Man unterscheidet hierbei die folgenden Funktionen:

- ✧ Schlüsselmanagement
- ✧ Datenvertraulichkeit
- ✧ Paket-Authentifizierung
- ✧ Datenintegrität
- ✧ Benutzer-Authentifizierung
- ✧ Benutzer-Authorisierung
- ✧ Schutz vor Sabotage
- ✧ Schutz vor unerlaubten Eindringlingen

Diese Begriffe werden im Folgenden genauer erläutert:

Schlüsselmanagement
Seine Aufgabe besteht in der Erzeugung, der Prüfung und der rechtzeitigen Erneuerung aller benötigten symmetrischen Schlüssel zur Verschlüsselung, Integritätsprüfung und Authentifizierung und deren sichere und automatische Verteilung.
Sichere Schlüssel, vor allem solche zur Datenverschlüsselung, haben eine relative kurze Lebensdauer (eine Session, wenige Stunden) und müssen daher oft erzeugt und verteilt werden. Folglich scheiden manuelle Verfahren und Out-of-Band-Verfahren zu deren Erzeugung und Verteilung aus, anstatt dessen kommt ein Schlüsselmanagement zum Einsatz.
Heutige Verfahren zur Schlüsselvergabe basieren meist auf so genannten asymmetrischen Verfahren. Zum Ver- und Entschlüsseln werden jeweils unterschiedliche Schlüssel verwendet, von denen einer, der öffentliche Schlüssel (Public Key) allgemein bekannt sein darf, daher auch Public Key Verfahren genannt.

Datenvertraulichkeit
Es muss verhindert werden, dass jemand die Daten auf ihrem Weg durch das Internet unauthorisiert im Klartext lesen oder kopieren kann. Vielfach wird auch gefordert, dass das interne Netzwerk mit seinen Verkehrsbeziehungen (Quell- und Zieladresse, Protokoll- und Portnummern) ebenfalls nicht ausgespäht werden kann. Erreicht wird diese Vertraulichkeit durch *Verschlüsselung* der Paketdaten und, falls die Verkehrsbeziehungen ebenfalls zu schützen sind, durch zusätzliches *Tunneling*.
Als Verschlüsselungsverfahren sollten hierbei unbedingt standardisierte, wohl bekannte, wie z.B. DES (*Data Encryption Standard*) oder Triple-DES, zum Einsatz kommen. Meist gibt die eingesetzte VPN-Technologie, aus Gründen der Interoperabilität, die Verfahren auch schon vor. In der Praxis werden, wegen ihrer hohen Geschwindigkeit, ausschließlich symmetrische Verschlüsselungsverfahren eingesetzt.

Paket-Authentifizierung
Es muss garantiert werden, dass ankommende Pakete tatsächlich vom authentischen Sender kommen und nicht von Dritten mit gefälschter Absenderadresse geschickt wurden. Dazu muss jedes eintreffende Paket authentifiziert werden.
Normale Prüfsummenverfahren reichen hier zur Überprüfung nicht aus, da ein Angreifer nach einer Datenänderung auch die Prüfsumme neu berechnen kann. Daher kommen spezielle Verfahren auf Basis von symmetrischen Verschlüsselungsverfahren zur Prüfsummenberechnung zum Einsatz, so genannte Keyed Hash-Algorithmen (HMAC, MD5, SHA) [Schob99], mit denen eine Prüfsumme

des Pakets berechnet wird und mit symmetrischer Verschlüsselung verschlüsselt wird. Der Schlüssel ist dabei nur dem Sender und Empfänger bekannt. Ein Angreifer kann also die Prüfsumme nach einer Datenänderung nicht korrekt berechnen.
Aus Gründen der Geschwindigkeit wird dies meist mit Verfahren zur Prüfung der Datenintegrität kombiniert.

Datenintegrität
Weiterhin muss sichergestellt sein, dass die Daten auf ihrem Transportweg durch das Internet von niemandem verändert werden.
Wie oben schon erwähnt, werden oftmals die Überprüfung der Datenintegrität und die Paket-Authentifizierung mit ein und demselben Verfahren, nämlich verschlüsselten„Einweg-Hash-Funktionen“, erreicht [Schob99].

Benutzerauthentifizierung
Diese stellt sicher, dass der Absender der Daten auch wirklich derjenige ist, der er zu sein vorgibt. Zu Beginn der Kommunikation findet eine Authentifizierung der Kommunikationspartner zur Feststellung von deren Identität statt. Die eingesetzten Verfahren reichen dabei von einfachen Passwortverfahren bis hin zur Verwendung von digitalen Zertifikaten zur Validierung der Public Keys. Ganz besonders wichtig ist diese Authentifizierung bei Remote-Access-VPNs.

Schutz vor Sabotage
Das VPN-Gateway muss sicher vor Angriffen sein, die zu Funktionalitäts-Beeinträchtigung führen können. Derartige Angriffe können z.B. DoS (Denial of Service)-Attacken sein. Erreicht werden kann dies durch den Einsatz einer geeigneten Firewall.

Schutz vor unerlaubtem Eindringen
Weiterhin müssen Zugriffe auf das Unternehmensnetzwerk von Unbefugten über seine öffentlichen Schnittstellen verhindert und damit einem Angreifer der direkte Weg zu Informationen, die er ausspionieren oder manipulieren will, versperrt werden. Dies wird über Authentifizierungssysteme und Firewalls erreicht.

Um diese Sicherheitsanforderungen zu erfüllen, kommen die folgenden 3 Kern-Mechanismen in einem VPN zum Einsatz:

- Verschlüsselung (*Encryption*)
- Authentifizierung (*Authentication*)
- Tunneln (*Tunneling*)

Auf diese Mechanismen, besonders aber auf das Tunneling, wird auf den folgenden Seiten genauer eingegangen.

5.1 Verschlüsselung

In der Praxis werden für die Verschlüsselung, wegen ihrer hohen Geschwindigkeit, ausschließlich symmetrische Verschlüsselungsverfahren mit verschiedenen Schlüssellängen eingesetzt. IPSec setzt für die Verschlüsselung seine sog. ESP ein, wobei die verschiedensten Verschlüsselungsverfahren zum Einsatz kommen können: DES (56 Bit), 3DES (168 Bit) , IDEA, AES, CAST, Blowfish.

SSL, S-HTTP sowie die E-Mail-Verschlüsselungsverfahren unterstützen ebenfalls die obigen Verfahren bzw. eine Untermenge davon.
Auf Layer 2 definiert PPTP noch sein eigenes Verschlüsselungsverfahren MPPE. WEP setzt wahlweise 40- oder 105 Bit-Schlüssel ein. L2TP definiert selbst keine Verschlüsselungsverfahren kann jedoch im Verbund mit IPSec eingesetzt werden. Gleiches gilt für MPLS, das jedoch durch sein Konzept von sich aus schon eine gewisse Sicherheit bietet (siehe Kapitel 8).
Es bleibt zu erwähnen, dass die Sicherheit der Verschlüsselung stark von der Schlüssellänge abhängt, die maßgeblich die Zeit für eine Brute Force-Attacke bestimmt. Vor dem Hintergrund stetig steigender Rechnerleistung sind 40 bzw. 56-Bit-Schlüssel, wie sie für MPPE, WEP oder DES zum Einsatz kommen, kaum noch als sicher zu bezeichnen.

5.2 Authentifizierung

Bei der Authentifizierung ist zwischen der Paketauthentifizierung und der User-Authentifizierung zu unterscheiden:
Für die Paket-Authentifizierung kommen bei IPSec (AH bzw. ESP), SSL, S-HTTP und den Mail-Verschlüsselungsverfahren Einweg-Hash-Funktionen (MD5, SHA-1,...) zum Einsatz, deren Prüfsummen mit symmetrischen Verfahren verschlüsselt werden.
Für die Schlüsselverteilung der für die obigen symmetrischen Verschlüsselungs- und Authentifizierungs-Verfahren benötigten Schlüssel definiert IPSec das IKE-Protokoll, das für die User-Authentifizierung Verfahren wie X.509-Zertifikate, RADIUS, TACACS, RSA-SecurID einsetzen kann. SSL, S-HTTP und die Mail-Verschlüsselungsverfahren setzen zur User-Authentifizierung ebenfalls auf X.509-Zertifikate [Schmidt98].
Die Layer 2-Protokolle L2TP und L2F verwenden für die User-Authentifizierung hingegen Passwort-Verfahren wie PAP (unsicher) und CHAP, wie sie durch PPP zur Verfügung stehen. Microsoft definiert für sein PPTP noch das so genannte MS-CHAP-Verfahren.

5.3 Tunneling-Technologien

Tunneling ist die Basis moderner VPNs.
Der Name Tunneling ist in gewisser Weise irreführend, da er das Vorhandensein eines physikalischen Tunnels, durch den aller Verkehr läuft, impliziert [Salam99]. Dies ist im Internet nicht der Fall, im Gegenteil, Tunneling ist ein Weg für Pakete, das Internet oder einen IP-Backbone sicher zu durchqueren.
Die Pakete eines Netzwerkprotokolls werden hierfür in Pakete eines anderen oder des gleichen Netzwerkprotokolls gekapselt und über dieses Netzwerk (*Pseudo Backbone*) übertragen. So wird es möglich, z.B. IPX-Pakete durch ein IP-Netzwerk zu transportieren. Eine andere Möglichkeit, die sich durch das Tunneling ergibt, ist das Verstecken von privaten, nicht registrierten Netzwerk- und Hostadressen durch IP-in-IP-Tunneling. So können private Netze über das Internet verbunden werden, indem IP-Pakete mit privaten Adressen in Pakete mit offiziell registrierten IP-Adressen gekapselt werden.
Für das Tunneln von Paketen stehen eine Reihe von Tunneling-Protokollen zur Verfügung, aber im Bereich VPNs kommen im Moment vorwiegend die folgenden 3 zum Einsatz: L2TP (*Layer 2 Tunneling Protocol*), IPSec (*IP Security Protocol*) im Tunnel Modus und PPTP (*Point-to-Point Tunneling Protocol*). Die verwendete VPN-Topologie hat dabei großen Einfluss auf die Protokoll-Wahl.

5.3.1 Tunneling-Modelle

In Abhängigkeit der Endpunkte des erzeugten Tunnels kann man 3 verschiedene Modelle unterscheiden (hier anhand des Beispiels Remote Access):

1. Intra-Provider-Modell
2. Provider-Enterprise-Modell
3. Ende-zu-Ende-Modell

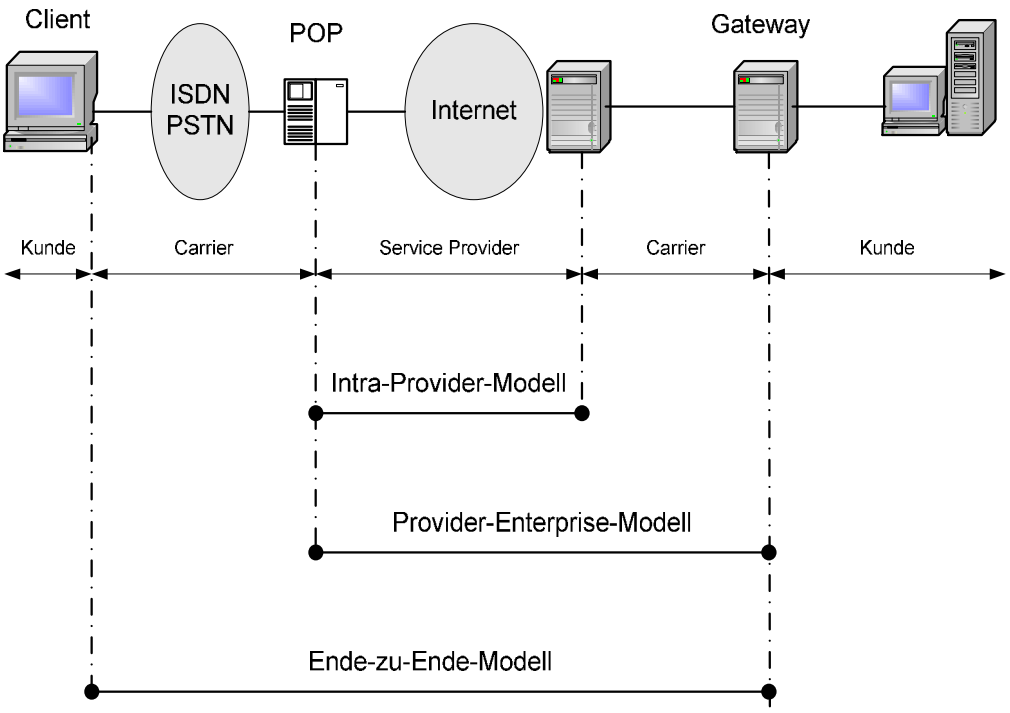


Abbildung 5-1: Tunneling-Modelle

Intra-Provider-Modell
Bei diesem Modell beginnt und endet der Tunnel beim Service Provider, der Kunde ist nicht in das Tunneling involviert. Die notwendigen Gateways werden also von den Providern betrieben. Man braucht folglich keine spezielle Hard- und Software beim Kunden zu installieren. Das Einsatzgebiet sind Remote-Access-VPNs. Es ist jedoch auch ein Einsatz in Branch-Office-VPNs denkbar.

Provider-Enterprise-Modell
Hier sind sowohl die Service Provider als auch Endkunden in das Tunneling involviert. Die Tunnel beginnen im POP (Point of Presence) des Providers und enden im Gateway des Kunden. Der Nachteil dieses Ansatzes ist, dass der Kunde hier für die spezielle Hard- und Software des VPN-Gateways zuständig ist.
Hier sind wiederum Remote-Access-VPNs das primäre Einsatzgebiet. Aber das Modell kann auch in Branch-Office-VPNs seine Verwendung finden.
Typische Tunneling-Protokolle, die in diesem Modell zum Einsatz kommen, sind L2TP und L2F, in seltenen Fällen PPTP.

Ende-zu-Ende-Modell
Bei diesem Ansatz benötigen Clients eine entsprechende VPN Software. Der Tunnel wird hier ausschließlich vom Kunden aufgebaut, Carrier und/oder Provider sind nicht in das Tunneling involviert. Der Remote-Access-Client wählt sich in POPs der Service Provider ein und eine spezielle

VPN-Clientsoftware im Endgerät des Kunden baut dann den Tunnel zum gewünschten VPN-Gateway im Kundennetzwerk auf.
Typische Protokolle, die hier verwendet werden, sind IPSec im Tunnel Modus und PPTP, in seltenen Fällen L2TP mit spezieller Clientsoftware. Theoretisch sind aber fast alle Tunneling-Protokolle in einem Ende-zu-Ende-Modell einsetzbar.

5.3.2 Tunneling Protokolle

Die Tunneling-Protokolle, die im Zusammenhang mit VPNs eingesetzt werden, lassen sich in 2 verschiedene Klassen einteilen: Layer-2- und Layer-3-Tunneling-Protokolle. Die Unterscheidung basiert auf der Schicht des OSI-Modells, deren Pakete eingekapselt werden.
Layer-2-Protokolle kapseln Pakete der Sicherungsschicht (Layer 2) in andere Pakete, meist solche der Schicht 3, wohingegen Layer-3-Protokolle Pakete der Netzwerkschicht (Layer 3) in andere Pakete der Netzwerkschicht kapseln.

5.3.2.1 Übersicht

5.3.2.1.1 Layer-2-Tunneling-Protokolle

Der größte Vorteil dieser Art von Tunneling-Protokollen ist, dass eine Vielzahl von Netzwerkprotokollen getunnelt werden kann, ohne dass sich das Tunneling selbst darum kümmern muss, da dies bereits auf der PPP-Ebene erfolgt ist.
Für das Tunneling auf Layer 2 wurden die drei folgenden Protokolle entwickelt:
L2TP (*Layer 2 Tunneling Protocol*), PPTP (*Point-to-Point Tunneling Protocol*) und L2F (*Layer 2 Forwarding*).

Im folgenden Beispiel werden PPP-Frames in IP-Pakete gekapselt. In den PPP-Frames können wiederum Pakete verschiedener anderer Netzwerkprotokolle, wie IP, IPX, VINES-IP, etc. enthalten sein. In Abb. 5-2 tunnelt L2TP ein IP- bzw. IPX-Paket.
Beim Tunneling entsteht ein gewisser Overhead, denn außer dem L2TP-Header werden zusätzliche UDP-, IP- und PPP-Header erzeugt. Dieser fällt bei großer Nutzdatenlänge allerdings kaum ins Gewicht.

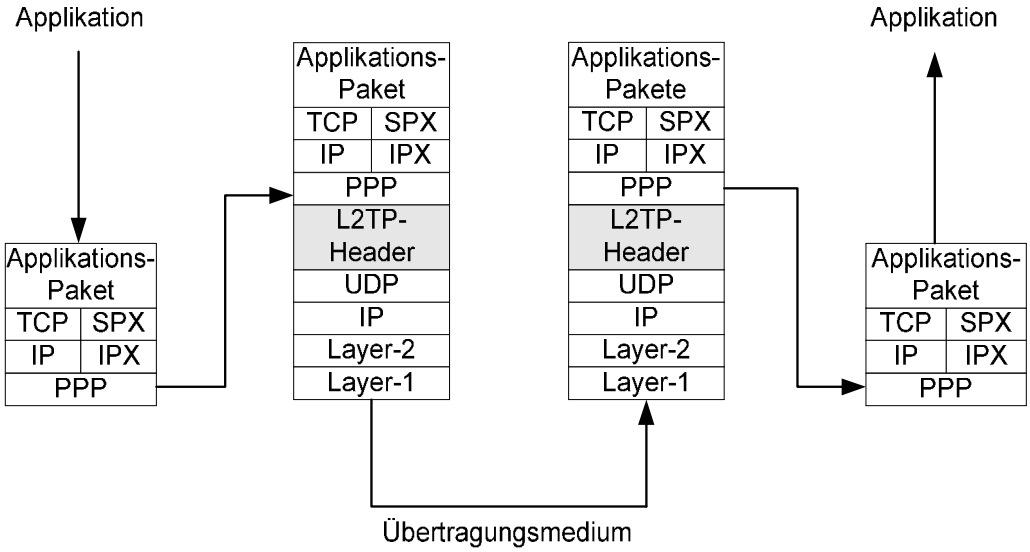


Abbildung 5-2: Layer-2-Tunneling

5.3.2.1.2 Layer-3-Tunneling-Protokolle

Das Layer-3-Tunneling arbeitet eine Schicht höher als die Layer-2-Protokolle. Hier werden, wie oben schon erwähnt, Pakete der Netzwerkschicht in andere Pakete dieser Schicht eingekapselt, wie in Abbildung 5-3 zu sehen ist. Der Paket-Overhead ist hier geringer als bei Layer-2-Tunneling.

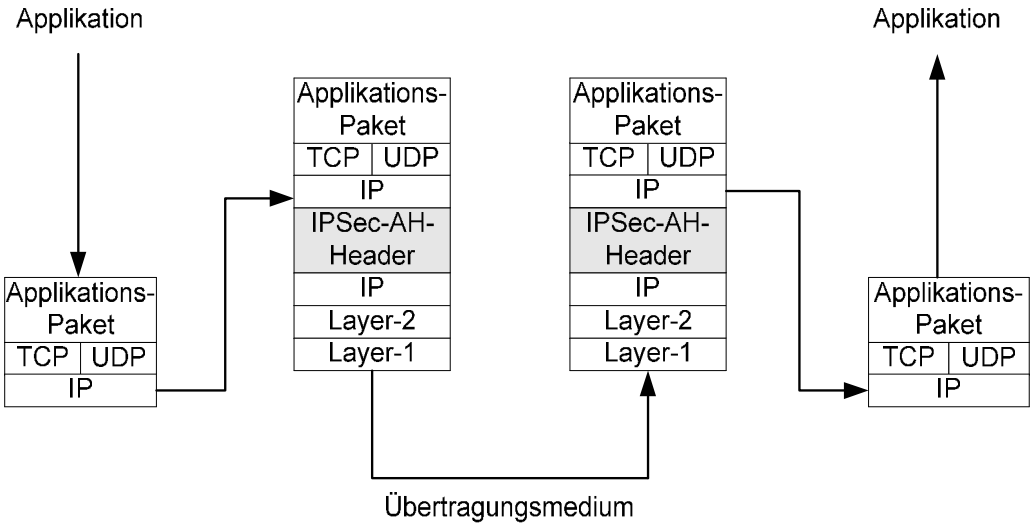


Abbildung 5-3: Layer-3-Tunneling

5.3.2.2 Standardisierte Tunneling-Protokolle

Die für IP-VPNs interessanten und zukunftssicheren Protokolle sind das IP Security Protocol (IPSec) und das Layer 2 Tunneling Protocol (L2TP). Beide sind in RFCs standardisiert.
GRE (*Generic Routing Encapsulation*) spielt als allein stehendes Tunneling-Protokoll keine große Rolle, dient aber als Grundlage für andere nicht standardisierte Protokolle, wie z.B. PPTP. Daher wird hier auch nicht näher auf GRE eingegangen.

5.3.2.2.1 IP Security Protocol (IPSec)

Das IPSec-Protokoll ist als eine Erweiterung des Netzwerksprotokolls IP zu verstehen, um IP-Pakete vor dem Abhören oder einer Manipulation zu schützen, also um die Datenvertraulichkeit und Datenintegrität zu wahren.
Ein Vorteil dieses Protokolls gegenüber den VPN-Protokollen auf höheren Schichten ist die Fähigkeit zur Verschlüsselung aller möglichen Übertragungs- und Anwendungsprotokolle.
IPSec wurde im Rahmen der neuen IP Version 6 (IPv6) entwickelt [RFC2401] und später auch an IPv4 angepasst. Seit Windows 2000 ist es ein fester Bestandteil von Windows [Lipp2001].
Es ist primär ein Sicherheitsprotokoll auf IP-Ebene, mit der Option, *ausschließlich* IP-Pakete zu verschlüsseln und/oder zu authentifizieren.
Es wird hauptsächlich im Ende-zu-Ende-Modell verwendet, um die gewünschte Sicherheitsfunktionalität auf der ganzen Übertragungsstrecke zwischen Client und VPN-Gateway sicherzustellen.
IPsec kann in 2 verschiedenen Modi betrieben werden [RFC2401, Schmidt98]:

IPSec im *Tunnel* Modus
In diesem Modus wird das komplette IP-Paket gekapselt und ein neuer IP-Header außen hinzugefügt. Bei Verschlüsselung werden die wahre Quell- und Zieladresse verborgen.

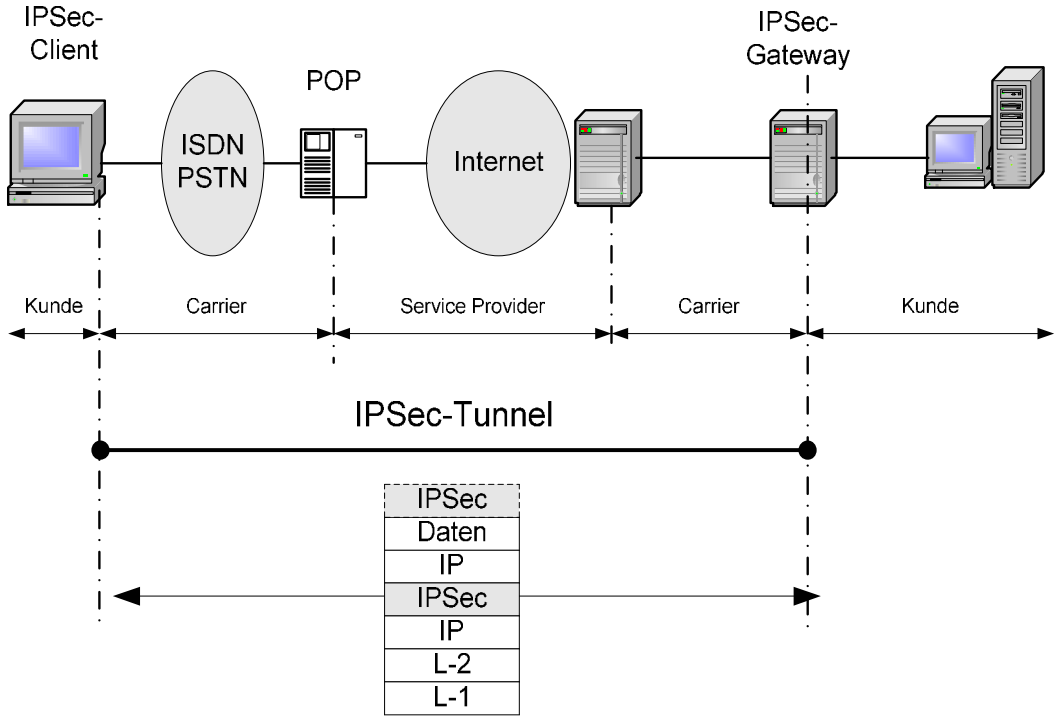


Abbildung 5-4: IPSec (im Tunnel Modus)

Der Tunnel-Modus wird meist als Basis für das *Ende-zu-Ende-Modell* verwendet, d.h. das Tunneling liegt komplett beim Kunden.
Im obigen Beispiel, einem Remote-Access-VPN, beginnt und endet der IPSec-Tunnel auf dem System des Kunden, Carrier und Provider sind nicht am Tunneling beteiligt.

IPSec im *Transport* Modus
In diesem Modus erfolgt keine Kapselung der Datenpakete, folglich wird auch kein neuer IP-Header hinzugefügt, d.h. es findet, wie der Name schon erahnen lässt, kein Tunneling statt.
Bei Verschlüsselung werden hier lediglich die Daten der Transportschicht (Layer4), z.B. UDP oder TCP, und der Anwendungsschicht (Layer 5) geschützt.
Das Einsatzgebiet von IPSec in diesem Modus sind Host-to-Host-VPNs, da hier ein Tunneling der Pakete keinen Sinn macht.

Für die Mechanismen der Authentifizierung kommt der sog. AH (*Authentication*)-Header zum Einsatz. Verschlüsselung wird durch Einsatz von ESP (*Encapsulation Security Payload*) gewährleistet [Schmidt98].

5.3.2.2.2 Layer 2 Tunneling Protocol (L2TP)

Dieses Layer-2 Tunneling-Protokoll stellt eine Verbesserung und Weiterentwicklung zweier älterer, nicht standardisierter Verfahren, und zwar PPTP (Point-to-Point Tunneling Protocol) und L2F (Layer 2 Forwarding), dar, die weniger eingesetzt werden. L2TP besitzt folglich viele Eigenschaften der beiden Vorgängerprotokolle. Es ist, im Gegensatz zu den beiden anderen Protokollen, ein standardisiertes Protokoll [RFC 2661].

Auf die beiden Vorgänger-Protokolle wird weiter unten noch ein wenig genauer eingegangen. Zunächst aber erst einmal zum L2TP-Protokoll. Es ist ein reines Tunneling-Protokoll auf PPP-Ebene, das außer IP verschiedene andere Netzwerkprotokolle tunneln kann [RFC2661]. Diese Eigenschaft stellt einen erheblichen Vorteil gegenüber IPSec dar, das lediglich in der Lage ist, IP-Pakete zu tunneln.
L2TP verfügt andererseits aber über keinerlei Sicherheitsmechanismen wie Datenverschlüsselung oder Authentifizierung, da es, wie schon gesagt, ein reines Tunneling-Protokoll ist. Es greift hier auf das PPP-Verschlüsselungsprotokoll MPPE (*Microsoft Point-to-Point Encryption*) oder IPSec zurück.
Das vorrangige Einsatzgebiet dieses Protokolls ist ein Remote-Access-VPN, da es sich, im Gegensatz zu PPTP, nur für Wählverbindungen [Kuri99] eignet. Der grobe Ablauf des Tunneling mit L2TP sieht folgendermaßen aus: Der Remote Client wählt sich beim nächstgelegenen POP eines Service Providers ein. Abhängig vom jeweiligen L2TP-Tunneling-Modell, die weiter unten noch genauer besprochen werden, kreiert der Client oder auch der Einwahlserver beim ISP, mittels eines L2TP-Tunnels, eine „virtuelle Modem-Verbindung“ [Phifer2000] vom Dial-Up-Client zu einem Unternehmens-LAN Access Server, verlängert also die normale PPP-Verbindung zwischen dem Client und dem POP des Internet Service Providers, wie sie bei einem herkömmlichen Remote Access aufgebaut wird, über einen Tunnel hinweg bis zum Unternehmensnetzwerk (Remote LAN Access). Dort wird die PPP-Verbindung dann terminiert. L2TP ermöglicht somit PPP die Datenkommunikation über andere als Punkt-zu-Punkt-Verbindungen.
Primär ist L2TP für den Einsatz im Provider-Enterprise-Modell gedacht, d.h. der Tunnel beginnt erst beim ISP und nicht schon beim Remote Client und endet im VPN Gateway des Kunden.
Grundsätzlich gibt es aber zwei verschiedene Tunneling-Modelle. Bevor wir aber auf diese zu sprechen kommen, werden im Folgenden erst einmal die wichtigsten Komponenten im Zusammenhang mit L2TP-Tunneling erklärt.

5.3.2.2.2.1 Komponenten

Die Nachteile eines Standard-Remote-Access sind, wie schon ganz am Anfang erwähnt, nicht unerheblich. Daher wäre es aus Sicht des Kunden schön, die Technologie für die Einwahl nicht selbst betreiben zu müssen, die Kontrolle über die Terminierung der Wählverbindung aber trotzdem zu behalten, vor allem, um die Benutzer-Authentifizierung selbst durchführen zu können. Der RAC des herkömmlichen Remote Access ist daher hier in zwei (getrennte) Funktionseinheiten aufgeteilt:
Der **LAC** (*L2TP Access Concentrator*) wird vom Carrier oder ISP betrieben und stellt den POP dar. Er terminiert die Wählverbindungen des Remote Users und den medienabhängigen Teil von PPP (Prüfsummencheck, etc.). Hier wird normalerweise, d.h. wenn nicht schon direkt der Client einen L2TP-Tunnel aufgebaut hat, entschieden, ob eine eingehende Verbindung als normale PPP-Verbindung lokal terminiert wird oder ob ein Tunnel zu einem LNS aufgebaut werden muss. Der LAC stellt also normalerweise den Tunnelanfangspunkt dar.
Der **LNS** (*L2TP Network Server*), der L2TP-Tunnel-Endpunkt, befindet sich auf der Endkunden-Seite. Er terminiert die höheren Schichten der PPP-Sessions. Der Client ist also logisch mit dem Endkunden-eigenen Network Server verbunden. Der LNS ist entweder auf einem Router oder einem speziellen VPN-Gateway angesiedelt.
Die Verbindung zwischen den beiden Funktionseinheiten erfolgt über einen L2TP-Tunnel, der PPP transparent über den Backbone des Providers tunnelt. Es sind auch mehrere Tunnel zwischen denselben Endpunkten möglich (*Multilink*). Innerhalb eines Tunnels können zusätzlich mehrere PPP-Sessions laufen (*Multiple Calls per Tunnel*) [Murhammer et. al. 99].

Das Unternehmen behält also die Kontrolle über die traditionellen RAS-Funktionen (Benutzer-Authentifizierung, etc.), während die Terminierung der Wählverbindung und Transportfunktionen

an einen Service Provider ausgelagert wird. Die Benutzer-Authentifizierung geschieht dabei, aufgrund der Verwandtschaft zu PPP, anhand der PPP-Authentifizierungsprotokolle (PAP, CHAP,…).

5.3.2.2.2.2 L2TP-Tunneling-Modelle

Wie schon gesagt, kann der L2TP-Tunnel entweder vom Remote Host selbst oder vom ISP Access Concentrator (LAC) initiiert werden. Vorwiegend wird L2TP aber im Provider-Enterprise-Modell eingesetzt, d.h. der Tunnel wird vom LAC des ISP initiiert. Man spricht dann auch vom *Compulsary Tunneling*.

5.3.2.2.2.2.1 Compulsary Tunneling

Dieser Tunneling-Mechanismus wurde vom Vorgänger-Protokoll L2F vererbt. Der L2TP-Tunnel beginnt hier im LAC des Service Providers und wird von diesem aufgebaut. Er endet im LNS (Gateway) beim Kunden (Unternehmens-Netzwerk).
Dieses Modell setzt die Kooperation des ISP voraus, der L2TP unterstützen muss.

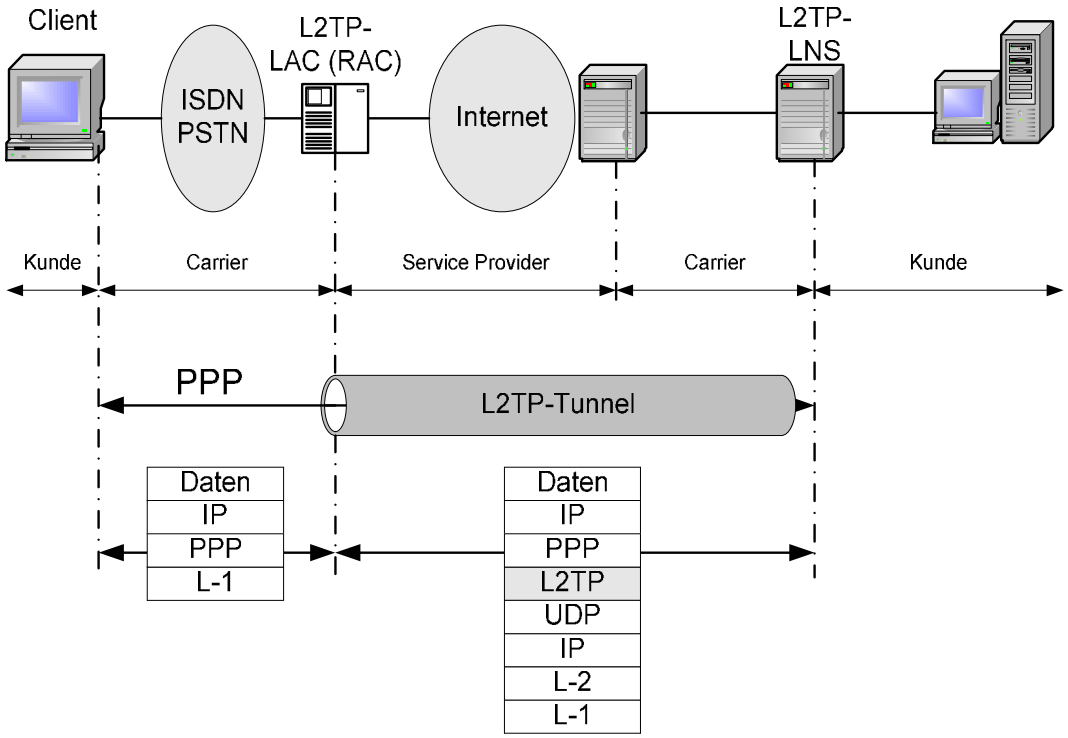


Abbildung 5-5: Compulsary Tunneling mit L2TP

Die Bezeichnung *Compulsory Tunneling* wird aus dem Zwang des Client abgeleitet, seine Daten über einen Tunnel schicken zu müssen, der vom Provider aufgebaut wird. Der Client kann hier also nicht selbst entscheiden, ob ein Tunnel zum Unternehmensnetzwerk aufgebaut wird oder nicht, dies wird allein vom LAC gesteuert. Das Tunneling ist somit transparent für den Client.
Der Service Provider kann so einem Kunden garantieren, dass dessen Clients jedes Mal, wenn sie sich anmelden, auf jeden Fall zu einem entsprechend eingerichteten LNS getunnelt werden und keinen direkten Zugriff auf das Provider-Netzwerk oder das Internet haben. Der Kunde behält hier also eine gewisse Kontrolle über seine Remote Clients.
Weiterhin wird dem IT-Manager im Unternehmens-Netzwerk die Arbeit erheblich erleichtert, da keine zusätzliche Konfiguration der Remote Clients mehr nötig ist.

Die Entscheidung des LAC beim Provider, wohin die Pakete getunnelt werden müssen, d.h *wohin* er den Tunnel aufbauen muss, erkennt er an bestimmten Kennzeichen des eingehenden Calls, wie z.B. der angerufenen Nummer (DNIS) oder einer Benutzer-ID. Er erkennt auch, *ob* es sich um eine Verbindung in das Netzwerk des Providers handelt, oder ob die Verbindung zu einem Endkunden getunnelt werden soll.

5.3.2.2.2.2.2 Voluntary Tunneling

L2TP kann aber auch im Ende-zu-Ende-Modell eingesetzt werden. Dieser Mechanismus ist L2TP vom Vorgänger-Protokoll PPTP vererbt worden. In diesem Modell ist die LAC-Funktionalität vom Remote-Access-Concentrator des Service Providers auf den Client verlagert. Man spricht dann auch von einem so genannten „Virtual LAC“ auf dem Clientrechner, der den L2TP-Tunnel zum LNS aufbaut.

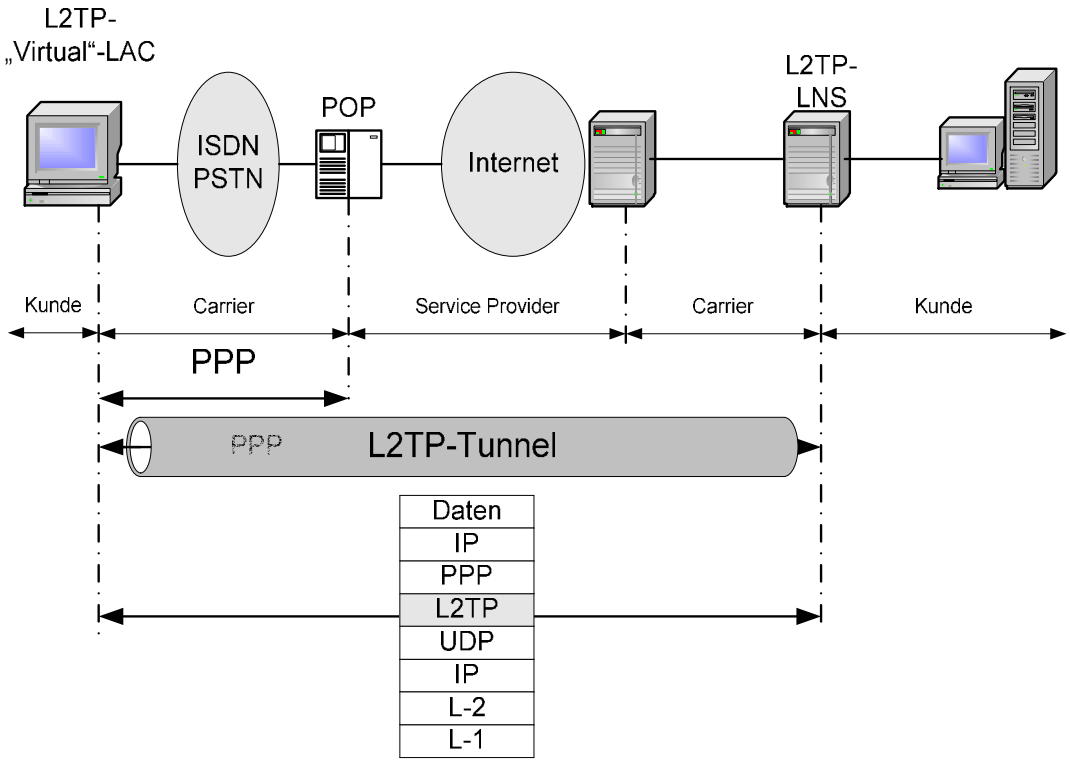


Abbildung 5-6: Voluntary Tunneling mit L2TP

Da der Client hier das Tunneling selbst übernimmt, also über L2TP-Fähigkeiten verfügt, und daher auch entscheiden kann, ob er einen Tunnel aufbaut oder nicht, spricht man hier auch vom so genannten *Voluntary Tunneling*. Die Carrier und Provider sind in diesem Modell nicht mehr ins Tunneling involviert, da der Tunnel bereits beim Client initiiert wird. Der Tunnel ist hier transparent für den Provider. Er überträgt nur die IP-Pakete zwischen Client und LNS und muss folglich auch über keinerlei L2TP-Infrastruktur mehr verfügen. Dafür ist nun L2TP-Support beim Client erforderlich. In der Praxis ist dieses Modell aber sehr selten, da die Kunden in der Regel möchten, dass die Clients zwangsweise zum Netzwerk getunnelt werden, um mehr Kontrolle über deren Zugang zum Intranet und Internet zu haben.
Ein Beispiel dieser Funktionalität ist bei Windows 2000 Professional zu finden. Hier ist als VPN-Protokoll auch L2TP als virtueller LAC implementiert [Lipp2001].

Beide Tunneling-Modelle unterstützen bei L2TP die Vergabe privater IP-Adressen an den Remote Client durch das Unternehmens-Netzwerk.

5.3.2.2.2.3 Sicherheit - IPSec secured L2TP

Wie schon erwähnt, handelt es sich bei L2TP um ein reines Tunneling-Protokoll, d.h. L2TP verfügt über keinerlei bzw. lediglich minimale Sicherheitsmechanismen. Dies macht die Verwendung von Sicherheitsmechanismen anderer Ebenen (Transport- oder Netzwerkebene (IPSec etc.) oder Applikationsebene (SSL, PGP, etc.) erforderlich. Falls L2TP in IP-Umgebungen eingesetzt wird, ist IPSec das empfohlene Verfahren, um die notwendige Sicherheit zu gewährleisten.
IPSec ist zwar ein sehr sicheres Protokoll, unterstützt aber nur das Tunneln von IP-Paketen. L2TP kann alle möglichen Protokolle tunneln, sofern sie in PPP einzukapseln sind, bietet aber keine nennenswerten Sicherheitsfunktionen.

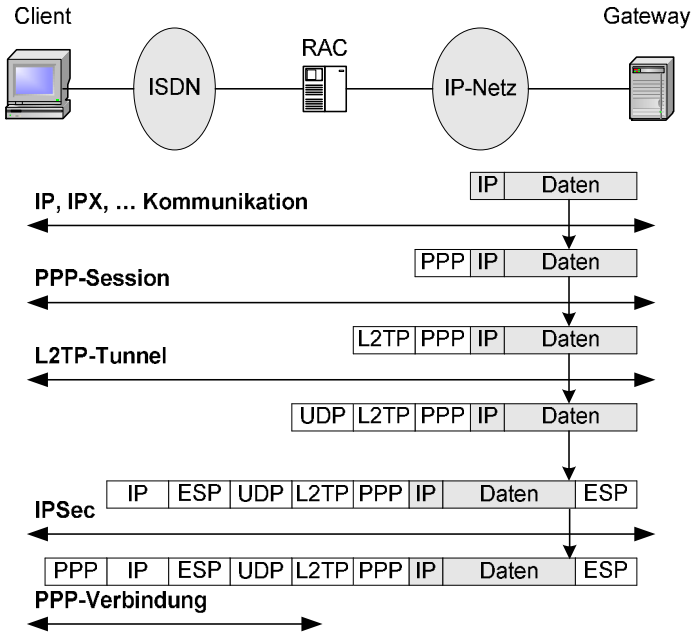


Abbildung 5-7: IPSec secured L2TP

Die Kombination dieser beiden Protokolle, d.h. L2TP auf der einen Seite und IPSec auf der anderen, vereinigt die Vorteile dieser beiden Protokolle und führt somit zu einem sehr flexiblen Tunneling-Protokoll, das sowohl über die Fähigkeit verfügt, unterschiedliche Netzwerkprotokolle zu tunneln, als auch diverse Sicherheitsmechanismen zur Verfügung stellt [RFC3193].
Die Tunnelendpunkte sind hier durch die Quell- und Zieladresse des IPSec-Headers definiert.
IPSec secured L2TP ist in der obigen Zeichnung anhand von Voluntary Tunneling dargestellt, d.h. der Tunnel beginnt beim Client. IPsec schützt hier den Tunnel zwischen Client und Unternehmens-Gateway. Es sind natürlich auch noch andere Möglichkeiten realisierbar, wie z.B. Compulsary Tunneling mit IPSec Schutz bis zu einem IPSec-Host im Unternehmensnetz.

5.3.2.3 Nicht standardisierte Tunneling Protokolle

Neben den standardisierten Tunneling-Protokollen existieren eine ganze Reihe anderer VPN-Tunneling-Protokolle, die jedoch niemals standardisiert wurden.
PPTP (*Point-to-Point Tunneling Protocol*) oder **L2F** (*Layer 2 Forwarding*) sind zwei von diesen.

5.3.2.3.1 Point-to-Point Tunneling Protocol (PPTP)

Dieses Tunneling Protokoll ist definiert im [RFC 2637], jedoch lediglich als „informational“.
Es wurde von einer Reihe Firmen (Microsoft, Ascend Communications, 3Com, ECI Telematics, U.S. Robotics) spezifiziert, die hierfür das so genannte PPTP-Forum gründeten [Lipp2001].
Im Jahre 1996 ist es als Erweiterung des PPP-Protokolls erstmalig in Windows NT 4.0 veröffentlicht worden.
Es wurde so entwickelt, dass sich ein Anwender von jedem Punkt im Internet aus mit einem Remote Access Server verbinden kann, als ob er sich direkt mit einem Modem einwählen würde. Es kann also, genau wie bei L2TP, als eine Fortsetzung einer PPP-Verbindung über das Internet verstanden werden. PPTP unterstützt dabei das Ende-zu-Ende-Modell bzw. das Voluntary Tunneling. Der Unterschied zu L2TP ist aber, dass es nicht nur auf den Einsatz bei Wählverbindungen beschränkt ist. Wegen des Ursprungs, Remote Clients, die sich bei einem Service Provider einwählen, eine sichere Verbindung ins Unternehmens-Netzwerk zu geben, basiert PPTP stark auf PPP [Salam99].
Es verwendet, genau wie L2TP, die Authentifizierungs- (PAP, CHAP) und Verschlüsselungstechnologie (z.B. MPPE) von PPP, die allerdings bei weitem nicht die Stärke von IPSec aufweisen, stellt aber selbst keine Sicherheitsmechanismen bereit.
Aufgrund der direkten Beziehung zu PPP unterstützt PPTP auch verschiedene Netzwerkprotokolle, denn es kapselt die PPP-Pakete in IP-Pakete und somit können Protokolle wie IP, IPX NetBEUI über das Internet getunnelt werden. PPTP benötigt hierfür lediglich eine gültige IP-Verbindung, über die der PPTP-Tunnel aufgebaut wird [RFC2637, Stender97].

Der Aufbau eines PPTP-Tunnels läuft ungefähr so ab: Der Benutzer wählt sich beim Provider ein, dabei wird eine PPP-Session zwischen User und RAC des Providers aufgebaut. Daraufhin initiiert der Benutzer eine PPTP-Session. Er kapselt dazu die PPP-Pakete mit einem modifizierten GRE-Header und fügt außen einen IP- Header mit der IP-Adresse des Tunnelendpunkts (Server auf Unternehmensseite) als Zieladresse an und schließlich ganz außen noch einen Media-Header (Schicht 2), der beschreibt, wie der Tunnel übertragen wird.
Im Gegensatz zu L2TP, ist mit PPTP nur ein Tunnel zwischen den Endpunkten möglich, d.h. kein *Multilink*, und innerhalb dieses Tunnels auch nur eine PPTP Session, also kein *Multicalls per Tunnel*.
In der Vergangenheit war die Ableitung des Schlüssels aus der Benutzer-Authentifizierung eine Zielscheibe einiger erfolgreicher Angriffe. Microsoft reagierte auf diese Angriffe mit einem Update (MS-CHAPv2).
Der Schlüssel des eingesetzten RC4-Protokolls ist, je nach Version von PPTP, 40 oder 128 Bit lang und wird aus einem Hashwert des Benutzer-Passworts erzeugt. Die Sicherheit basiert also lediglich auf dem Benutzer-Passwort, dies ist allerdings für viele Anwender ein zu hohes Sicherheitsrisiko und so wird PPTP zunehmend vom Markt verdrängt.
Microsoft hat PPTP-Unterstützung in alle Windows-Clients und -Server eingebunden [Salam99].

5.3.2.3.2 Layer 2 Forwarding (L2F)

Dieses, ebenfalls nicht-standardisierte, Layer-2-Tunneling Protokoll ist im [RFC 2341] als „informational“ definiert. Es stellt den Konkurrenzvorschlag zu PPTP dar, der von der Firma Cisco etwa zeitgleich entwickelt wurde. Beide Protokolle sind inkompatibel zueinander. Zum Einsatz kommt dieses Protokoll im Provider-Enterprise-Modell bzw. Compulsary Tunneling.
Es ist sehr eng mit L2TP verwandt, folglich können viele L2TP-Network-Server auch als Endpunkt für einen L2F-Tunnel dienen. Zur Client-Authentifizierung verwendet L2F, wie auch PPTP und L2TP, ebenfalls die PPP-Authentifizierungsprotokolle PAP und CHAP. Es bietet, wie L2TP und PPTP, selbst keine Sicherheitsdienste wie Datenverschlüsselung oder starke Authentifizierung und greift daher auf die PPP-Verschlüsselungsprotokolle oder IPSec zurück [Murhammer et. al. 99].

Wie auch die beiden anderen Layer-2-Tunneling Protokolle besitzt L2F die Fähigkeit, verschiedene Netzwerkprotokolle zu tunneln [RFC2341, Stender97].
Es gestattet, im Gegensatz zu PPTP, wieder mehrere, unabhängig voneinander parallel betriebene Tunnel und mehrere Calls pro Tunnel, genau wie L2TP.
Das Tunneling ist hier, im Gegensatz zu PPTP, nicht abhängig von IP [Murhammer et. al. 99], als Basis sind auch andere paketorientierte Systeme wie ATM, Frame Relay und X.25 möglich.

5.3.2.4 Features der Tunneling-Protokolle

Nachdem man, vor der Implementierung des VPNs, eine VPN-Policy mit den geforderten Sicherheits- und anderen Funktionen zusammengestellt hat, scheiden damit, je nach den Anforderungen, von vornherein einige der im Einsatz befindlichen Tunneling-Protokolle aus. So ist es beispielsweise mit IPSec nicht möglich, IPX über ein IP-Netzwerk zu transportieren.
Im Folgenden sehen Sie einen Überblick über die wichtigsten VPN-Tunneling-Protokolle IPSec, L2TP, PPTP und L2F und ihre implementierten Funktionen:

	IPSec	L2TP	PPTP	L2F
Protokolltyp	Layer 3	Layer 2	Layer 2	Layer 2
Standardisiert (RFC)	Ja	Ja	Nein	Nein
Paket-Authentifizierung	Ja	Nein	Nein	Nein
Benutzer-Authentifizierung	Ja	Ja	Ja	Ja
Datenverschlüsselung	Ja	Nein	Ja	Nein
Schlüsselmanagement	Ja	Nein	Nein	Nein
QoS-Signalisierung	Ja	Nein	Nein	Nein
IP-Tunneling	Ja	Ja	Ja	Ja
IPX-Tunneling	Nein	Ja	Ja	Ja
Primäres Modell	Ende-zu-Ende	Provider-Enterprise	Ende-zu-Ende	Provider-Enterprise

Abbildung 5-8: Tunneling-Protokoll Features

Anhand eines vorher angefertigten Anforderungskatalogs lässt sich damit schnell ein geeignetes Protokoll – oder Kombination von Protokollen finden, die für das geplante VPN in Frage kommen.

6 Quality-of-Service in VPNs: Multi Protocol Label Switching (MPLS)

6.1 Einführung

Neue konvergente Netze, in denen neben Datenübertragung gleichzeitig auch die Übertragung von Sprache und Videostreams stattfindet, stellen neue Anforderungen an die QoS, die das Netz zur Verfügung stellen muss. Die Forderung nach garantierten Bandbreiten und Verzögerungszeiten ist in lokalen Netzen und selbst in WANs mit Frame Relay und ATM, mit denen sich verschiedene Dienstqualitäten definieren lassen, durchaus erfüllbar. Mit konventionellen Internet-VPN-Technologien, wie sie in den letzten Kapiteln präsentiert wurden, sind jedoch definierte Dienstgüten nicht realisierbar.
Multiprotocol Label Switching (MPLS) wurde von der IETF Ende der 90er ursprünglich als eine Technologie zur Verbesserung der Durchsatzgeschwindigkeit von Routern eingeführt [Ryan98, Knabl2001], ist aber inzwischen zu einer Standardtechnologie geworden, die den Backbone großer Carrier-Netze um neue Fähigkeiten erweitert [Schob2002]. Traffic Engineering, also die Möglichkeit für den Netzwerk-Operator festzulegen, welchen Weg die Daten durch das Netz nehmen (sog. Label Switched Path (LSP)), QoS-Unterstützung (Bandbreiten-Zuweisung) und VPN-Support sind Beispiele für den aktuellen Einsatz von MPLS [Ryan98, Britt2000, Bell2001].
MPLS ist mit praktisch allen Layer 2 Technologien (Ethernet, FDDI, PPP, Frame Relay, ATM,…) kompatibel und kann ebenso mit allen Schicht 3-Protokollen zusammenarbeiten [Knabl2001].

6.2 Struktur und Funktion eines MPLS-Netzes

Der Kern von MPLS ist die schnelle Paketweiterleitung anhand von kurzen Labels, die am Rand des MPLS-Netzwerks in einen zusätzlichen MPLS-Header in das Paket eingefügt werden, anstatt wie in einem herkömmlichen IP-Netz an jedem Hop in einem zeitaufwendigen Prozess den ganzen IP-Header auszuwerten (*Hop-by-Hop-Routing*) [Schob2002].
Beim Eintritt eines Pakets in ein MPLS-Netzwerk nimmt der *Ingress Label Edge-Router* (LER) auf der Basis des IP-Headers des ungelabelten Paketes eine Klassifikation vor und trifft eine Routing-Entscheidung [MPLS2000, Ryan98]].
Wie die Daten innerhalb des Netzwerks behandelt werden, das heißt, mit welchen Prioritäten, Übertragungskapazitäten und Übertragungsverzögerungen (QoS) und welchen Paketverlustraten der Transport erfolgt, wird in speziellen Vereinbarungen, den sog. *Forwarding Equivalence Classes* (FECs) festgelegt [Ryan98, Britt2000]. Eine FEC ist nichts anderes als eine Gruppe von Paketen, die bezüglich ihrer Weiterleitung gleich bezüglich der obigen Parameter behandelt wird. Es gibt verschiedene Arten, eine solche Klasse zu definieren, z.B. Zielsubnetz, Zielhost und Zielapplikation (verschiedene Granularität).
Labels werden durch einen Binding-Prozess mit einer FEC und damit einem Verkehrsstrom assoziiert. Auf der Basis der Einordnung eines Pakets in eine FEC und der Bindung dieser FEC an ein Label werden die Pakete mit Labels fester Länge versehen und dann weitergeleitet.
An allen folgenden Knoten innerhalb des MPLS-Netzes, den sog. *Label Switch Routern* (LSRs) wird nur das Label für die Forwarding-Entscheidung genutzt (Switching) und nicht der IP-Header, wodurch sich der Verarbeitungsaufwand in den folgenden Knoten auf dem Weg verringert [Britt2000].

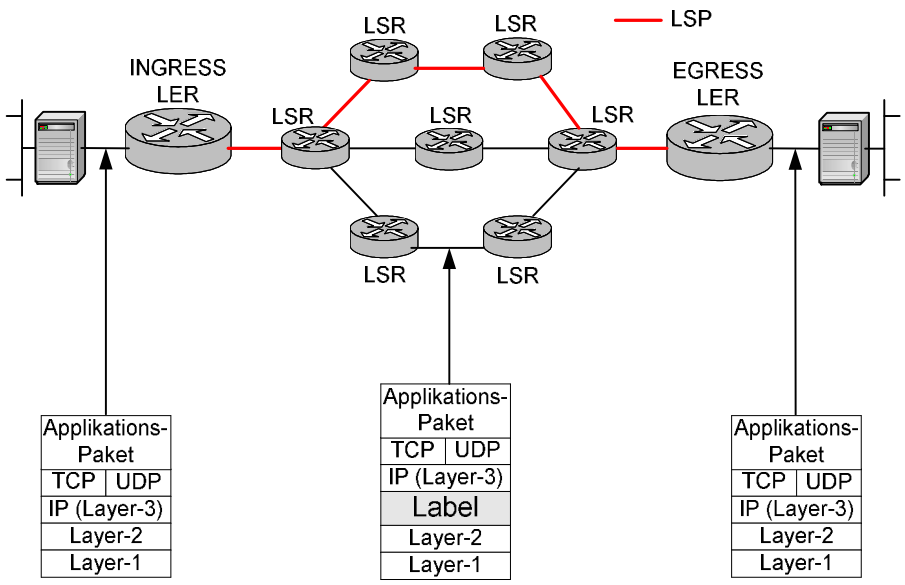


Abbildung 6-1: Struktur eines MPLS-Netzes

Der Wert des Labels ändert sich für gewöhnlich an jedem LSR auf dem Weg durch das Netz. An jedem LSR wird auf der Basis des Eingangsinterfaces und dem Label aus der Forwarding Tabelle [Bell2001] des LSR das Ausgangsinterface und das neue Label bestimmt, mit dem das Paket versehen und weitergeschickt wird.

Da das Mapping zwischen den Labels an jedem LSR konstant ist, wird der Pfad eines Pakets vom Anfangswert des Labels bestimmt. Solch einen Pfad nennt man einen *Label Switched Path* (LSP). Alle Pakete mit demselben Label folgen demselben Label Switched Path (LSP) durch das Netzwerk. Da das erste Label im Ingress Edge LSR vergeben wird, bestimmt dieser damit den gesamten Weg des Paketes durch das Netz [Knabl2001].
Wenn die Pakete das MPLS-Netz wieder verlassen, entfernt der Egress Edge LSR die Labels wieder.
Die Information über die Bindungen zwischen lokal gewählten Labels und den mit ihnen assoziierten Interfaces muss an benachbarte LSRs weitergeleitet werden (*Label Distribution*), damit diese sie für die Bildung ihrer eigenen Forwarding Tabellen nutzen können. Label Binding-Informationen können entweder huckepack auf Routing Protokoll-Paketen, über das spezielle Label Distribution Protocol (LDP) oder über das Resource Reservation Protocol (RSVP) weitergeleitet werden [MPLS2000].

6.3 Vergleich IP - MPLS

	Konventionelles IP-Netzwerk	**MPLS-Netzwerk**
Quality of Service	kein differenzierter QoS-Support	QoS-Support (Intserv und Diffserv) über das Resource Reservation Protocol (RSVP)
Traffic Engineering	Nur im Ansatz möglich: Source Routing	Möglich über die Definition von Label Switched Paths (LSPs) durch das Netz

Analyse des vollen IP-Headers	an jedem Knoten des Netzwerks	nur einmal am Rand des Netzwerks
Routing-Entscheidungen	basiert ausschließlich auf der Adresse	Kann auf jeder Anzahl von Parametern, wie z.B. QoS oder VPN-Zugehörigkeit gefällt werden

6.4 MPLS-VPNs

Wie oben schon erwähnt, ist eines der Features von MPLS die Möglichkeit zum Aufbau von VPNs durch das MPLS-Netz des Service-Providers. Ein zentrales Merkmal von MPLS im Hinblick auf VPNs ist, dass die LSRs auf dem LSP den Inhalt der Paket-Header oder die Paket-Daten für die Weiterleitung nicht untersuchen müssen. Aus diesem Grund lassen sich mit den LSPs VPN-Tunnel durch das MPLS-Netzwerk bilden. Da MPLS mit allen möglichen Schicht-3-Protokollen kompatibel ist, können auch andere Protokolle als IP getunnelt werden.
Wo mehrere LSPs parallel laufen, können sie in einem *Higher-Level LSP* zwischen LSRs im Netz zusammengefasst werden. Gelabelte Pakete, die in den Higher-Level LSP-Tunnel eintreten, werden mit einem weiteren Label versehen und behalten ihre First-Level-Label, um sie unterscheiden zu können, wenn sie den Higher-Level Tunnel wieder verlassen. Den Vorgang, ein Paket mit mehreren Labeln zu versehen, nennt man *Label Stacking* [Bell2001, Knabl2001]. Hiermit erreicht man unter anderem eine Verkleinerung der Forwarding Tabellen in den LSRs, da weniger Tunnel zu verwalten sind, und damit eine bessere Skalierbarkeit.
Wegen des Tunnelns der IP-Pakete ist beim Übergang vom Unternehmensnetz mit privaten IP-Adressen in das MPLS-Internet kein NAT nötig, da die privaten IP-Adressen innerhalb des MPLS-Netzes im Label getunnelt werden. Falls verschiedene Kunden den gleichen privaten Adressraum verwenden, so werden sie durch Virtuelle Router [Ryan98, Knabl2001] über einen Route Distinguisher-Präfix in den Edge LSRs getrennt, die multiple Forwarding Tabellen verwalten können.
Der Kunde erwartet, dass VPN-Daten privat bleiben, inklusive der Topologie und der Adressen seines privaten Netzes. Mit MPLS erreicht man ähnliche Sicherheit [Britt2000] wie mit Layer 2-Virtual Circuits (ATM, Frame Relay):

- Für verschiedene Kunden werden verschiedene Tunnel festgelegt, die durch ihre Label getrennt sind.
- Am Ingress Edge Router des Service Providers (SPs) werden alle Daten-Pakete einer VPN-Verbindung mit einem Label Stack versehen, der für jeden VPN-Zielpunkt verschieden ist. Dies stellt sicher, dass die Daten nur an dieses Ziel ausgeliefert werden, so dass keine Daten das VPN verlassen.
- Jedes andere Paket, das in das SP-Netzwerk gelangt, wird entweder ohne die Nutzung von MPLS geroutet oder wird mit einem anderen Label Stack versehen, so dass ein Angreifer keine Daten in das VPN von außerhalb des SP-Netzwerks einschmuggeln kann.
- SP-Router können den kryptographischen Algorithmus MD5 oder ähnliche Techniken verwenden, um das VPN gegen Einspeisung von falschen Labels oder Verwendung von falschen LSRs beim Label Distribution Protocol (➔Authentifizierung der Endpunkte der LSP-Tunnel) zu schützen.

Deshalb muss das Kunden-Equipment, welches an das VPN angeschlossen ist, kein IPSec oder andere kryptographische Software fahren, was sich für den Kunden in großen Einsparmöglichkeiten, sowohl was die Equipment-Kosten als auch die Management-Komplexität angeht, auszahlt.
Es gibt zwei Situationen, wo ein Kunde zusätzlich noch weitere kryptographische Sicherheitsmechanismen einsetzen muss, selbst wenn er eine MPLS-VPN-Lösung einsetzt. Dies ist ohne Proble-

me möglich, da die komplette Payload inklusive IP-Header des Pakets auf dem Weg durch das MPLS-Netz verschlüsselt werden kann, da vom Netz nur das Label für die Weiterleitung benötigt wird.

- Wenn die Kunden-Daten eine so hohe Vertraulichkeit erfordern, dass sie sogar gegen Ausspionieren von innerhalb des SP-Netzwerks geschützt werden müssen, müssen die VPN-Daten mit IPSec oder anderen kryptographischen Techniken verschlüsselt werden, bevor sie in das SP-Netzwerk eintreten. In diesem Fall liegt die Verantwortung für die Verteilung der kryptographischen Schlüssel beim Kunden.
- Wenn ein VPN über die Netze mehrere Service Provider läuft, können die SPs IPSec-basierte Tunnel aufbauen, um den VPN-Verkehr zwischen ihren Netzen über das öffentliche IP-Internet zu transportieren, wenn eine direkte MPLS-Verbindung zwischen den SPs nicht zur Verfügung steht. In diesem Fall sind die SPs für die Verteilung der Schlüssel verantwortlich.

7 VLANs

7.1 Konzept

In einem rein mit Routern aufgebauten Netzwerk, so wie es sie früher gab, hat man das Problem einer hohen Verzögerungszeit beim Routing-Vorgang in den Routern.
Deswegen hat man in modernen Netzwerken zu einer geswitchten Netzwerktopologie gewechselt, da diese wesentlich kürzere Latenzzeiten bieten. Bei einem rein aus Switches aufgebauten Netz befinden sich jedoch alle Hosts in derselben Broadcast-Domain, wodurch sich der Broadcast-Vekehr auf das gesamte Netz ausbreitet.
Durch die Einführung sogenannter VLANs (*Virtual LANs*) innerhalb eines geswitchten Netzwerks wird dieses in so genannte Broadcast-Domains [UCD98, Welch99a] aufgetrennt. Ein VLAN bildet eine solche Broadcast-Domain, womit sich der Broadcast-Verkehr innerhalb des VLANs nicht außerhalb des VLANs verbreitet. Ein VLAN besteht aus einer Gruppe von Hosts in unterschiedlichen physikalischen LAN-Segmenten, die damit so miteinander kommunizieren können, als ob sie sich im selben physikalischen LAN-Segment befinden.
Bei VLANs werden keine speziellen Sicherheitstechnologien wie Verschlüsselung, Integritätssicherung oder Paketauthentifizierung eingesetzt. Es erfolgt eine Trennung des Transports der Datenpakete auf OSI-Schicht 2, und statt auf Sicherheit wurde hier mehr auf Performance abgezielt.
Da ein VLAN eine Broadcast-Domäne bildet, ist bei der Definition von VLANs zu beachten, dass ein IP-Subnetz als Ganzes Bestandteil eines VLANs sein muss [Welch99a] und nicht auf mehrere VLANs gesplittet werden darf, da sich sonst Hosts innerhalb eines Subnetzes, die zu verschiedenen VLANs gehören, nicht mehr erreichen können. Es ist jedoch durchaus möglich, mehrere Subnetze zu einem VLAN zusammenzufassen.

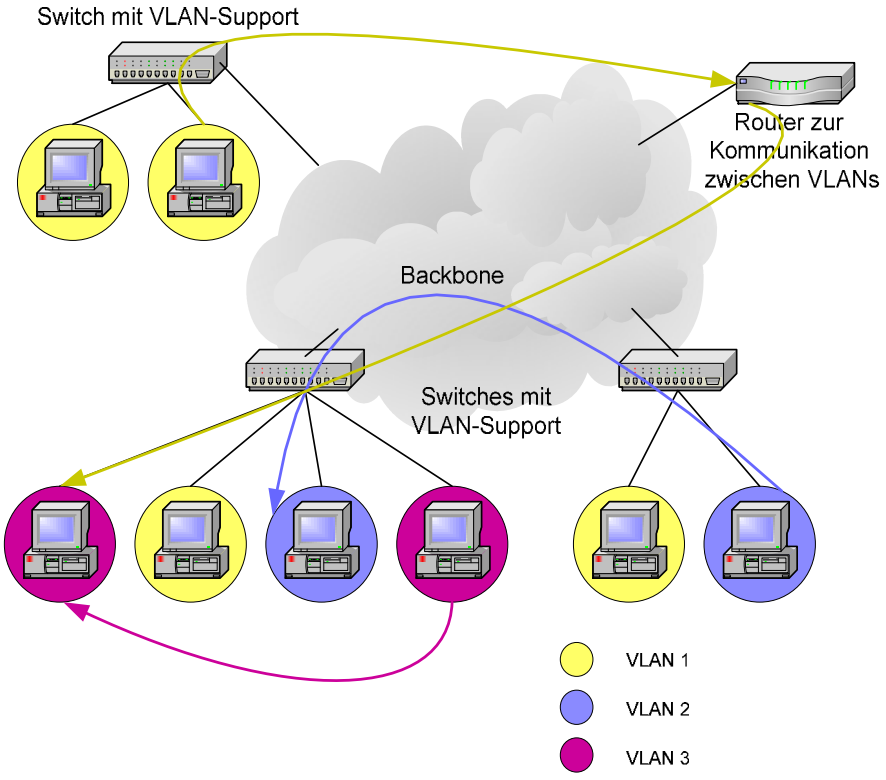


Abbildung 7-1: VLAN - Konzept

Zum Transport von Paketen zwischen verschiedenen VLANs sind weiterhin Router bzw. Layer 3-Switches [Pass96] notwendig. Innerhalb eines VLANs erfolgt der Transport über Switches.
Da sich VLANs im Regelfall über mehrere Switches hinweg erstrecken, müssen Switches über eine Möglichkeit verfügen, die Zugehörigkeit von von anderen Switches eingehendem Netzwerkverkehr zu einem bestimmten VLAN zu erkennen, andernfalls wären VLANs auf einen Switch beschränkt. Generell müssen bei Layer 2-basierten VLANs (also Port- oder MAC-basierten VLANs) (siehe Kapitel 7.2) diese Informationen mit übertragen werden [Welch99b], während diese Information bei IP-basierten VLANs implizit über die IP-Adresse mit übertragen wird. Ein Switch, der ein MAC-Paket an einen anderen Switch weiterleitet, fügt eine Markierung (*Tag*) [Bor99] mit der VLAN-ID in den MAC-Header ein (Frame Tagging, 802.1q). Mit dem VLAN-Tag lassen sich auch QoS-Anforderungen realisieren, da im 802.1q-Tag Priorisierungsbits vorgesehen sind.

7.2 Typen

Es gibt verschiedene Kriterien, nach denen die Zugehörigkeit zu einem VLAN geregelt werden kann [Pass96, Cisco2000]:

7.2.1 Statisches VLAN

Port-Gruppierung
Hier erfolgt eine manuelle Zuordnung bestimmter Switch-Ports zu bestimmten VLANs (auch über Switch-Grenzen hinweg).
Aufgrund dieser Einteilung ergeben sich einige Nachteile:

- ein Port kann nur zu einem einzigen VLAN gehören
- beim Umzug eines Users an einen anderen Port ist eine eventuelle Neukonfiguration der VLAN-Mitgliedschaft notwendig

7.2.2 Dynamisches VLAN

MAC-Layer-Gruppierung
Die Zugehörigkeit zu einem VLAN wird hier anhand der MAC-Adresse geregelt. Die Ports des Switches werden bei Empfang eines entsprechenden MAC-Frames dynamisch einem VLAN zugewiesen.
Vorteil: bei Umzug keine Neukonfiguration nötig
Problem: Notebooks / Dockingstation

Layer 3-basierte Gruppierung
Die Zuordnung erfolgt hier je nach genutztem Layer 3-Protokolltyp oder Layer 3-Adresse (IP-Subnetz).
Vorteile:

- Umzug ohne Neukonfiguration der Netzwerk-Adresse möglich
- keine Notwendigkeit für aufwendige Zuordnung zu VLANS und Frame Tagging (da VLAN-Zugehörigkeit implizit durch den IP-Header gegeben)
- Host kann an mehreren VLANS partizipieren

Probleme:

- inkompatibel mit DHCP [Pass96]
- Performance-Nachteile wegen Auswertung der Layer-3-Informationen

Applikationsbasierte Gruppierung
Hier entspricht jedes VLAN einem Service im Netzwerk. User, die diesen Service benutzen, werden demselben VLAN zugeordnet.

Natürlich ist auch eine Mischung der obigen Gruppierungs-Methoden bei der Definition von VLANs möglich.

7.3 Vorteile

Verbesserte Performance
Die Gruppierung von Hosts, die einer logischen Arbeits- bzw. Nutzergruppe angehören, in logische Netzwerke erhöht die Performance durch Einschränkung des Broadcast-Verkehrs auf Hosts [Pass96, Cisco2000], die den gleichen Workgroups angehören. Darüber hinaus muss weniger Verkehr geroutet werden [Stern98] und die Latenzzeiten durch die Router kommen somit nicht mehr so stark zum Tragen.

Einfacheres Netzwerk-Management
VLANs bieten einen einfachen, flexiblen und billigen Weg, logische Gruppen in einer Umgebung zu ändern [Cisco2000, Pass96]. Sie verbessern die Managebarkeit, indem sie eine zentralisierte Konfiguration von Netzwerk-Devices an physikalisch getrennten Orten über eine ausgefeilte VLAN-Management-Software erlauben.

Unabhängigkeit von der physikalischen Topologie
indem VLANs es ermöglichen, Workgroups an physikalisch getrennten Orten logisch zu einer einzigen Broadcast-Domain zusammenzufassen [Cisco2000]. Darüber hinaus erlauben sie einen einfachen Umzug eines Hosts bzw. die Erweiterung einer Abteilung und eine einfache Bildung virtueller Projektarbeitsgruppen.

Erhöhung der Sicherheit
Bei flacher Netzwerkhierarchie hat ein Angreifer Zugang zu allen Broadcasts, dies ist nach einer Aufteilung in VLANs nicht mehr der Fall [Cisco2000, Stern98]. Außerdem gestattet es die VLAN-Management-Software, Hosts vom Zugang ohne Registrierung bei der Netzwerk-Management-Software auszuschließen.

Transparenz
VLANs sind für Hosts bzw. End-User völlig transparent.

8 Zusammenfassung und Ausblick

Im Laufe der letzten Jahre legten die Unternehmen ihren Focus immer mehr auf E-Business. Dies macht zunehmend erforderlich, dass Geschäftspartner und Zulieferer Zugang zu Daten im Firmen-Intranet erhalten. Des Weiteren verteilen sich global tätige Unternehmen heutzutage auf eine Vielzahl von Unternehmensstandorten, die untereinander kommunizieren.
Auch Mitarbeiter müssen, wenn sie vor Ort bei einem Kunden sind, von unterwegs oder von zu Hause aus Zugang zu den Informations-Ressourcen ihrer Unternehmens-Intranets haben.
Die Unternehmen suchen hierbei die beste, d.h. kosteneffektivste und sicherste, Lösung, um Remote User, Zweigstellen und Geschäftspartner in ein erweitertes *Corporate Network* einzubinden.
Diese Lösung bietet der Einsatz von Virtual Private Networks (VPNs), die zunehmend ihre Verbreitung in der Geschäftswelt finden.
Diese Netzwerke ermöglichen es, private Daten gesichert über ein öffentliches Netzwerk (Internet), zu transportieren. Erreicht wird dies durch Mechanismen wie Verschlüsselung, Authentifizierung und Tunneling.
Die zukünftige Entwicklung im Internet wird vor allem im Bereich der Erhöhung der Bandbreite und der Verfügbarkeit sowie der durchgehenden Implementierung von Bandbreitenmanagement und verschiedenen Dienstqualitäten stattfinden.
Quality-of-Service-Anforderungen sind mit konventionellen Internet-VPN-Technologien, wie sie in den letzten Kapiteln präsentiert wurden, jedoch nicht realisierbar.
Hier kommt Multiprotocol Label Switching (MPLS) ins Spiel. MPLS ermöglicht den Aufbau sicherer Tunnel durch ein Netz, indem virtuelle Pfade, sog. *Label Switched Paths*, geschaltet werden. Diesen Pfaden können vorbestimmte Bandbreiten und Verzögerungszeiten zugewiesen werden und somit wird eine Bereitstellung von Quality-of-Service ermöglicht.
Auch mit VLANs lassen sich QoS-Anforderungen realisieren. Primär sind diese aber zur Gruppierung von Hosts, die einer logischen Arbeits- bzw. Nutzergruppe angehören, in logische Netzwerke innerhalb eines Unternehmens-Netzwerks gedacht.

VPNs sind jedoch keinesfalls die ultimative Lösung für alle Sicherheitsprobleme. So bietet die Einrichtung eines VPNs alleine keinen wirksamen Schutz gegen Datendiebstahl- oder -mißbrauch. VPNs bieten zwar einen recht guten Schutz der Daten auf ihrem Weg durch öffentliche und private Netze, sind aber kein Allheilmittel gegen jede Form des Abhörens.
VPNs helfen beispielsweise nicht gegen die Belauschung der Monitor-Abstrahlung oder etwa der Datenleitungen bis zu einem VPN-Gateway. Auch Schutz gegen Viren ist durch VPNs nicht gegeben. Und der Wirtschaftsspionage , die gar nicht auf der technischen Ebene ansetzt, sondern durch „soziales Hacking“ Passwörter herausbekommt oder gar Mitarbeiter zur Preisgabe von Informationen erpresst, ist mit VPNs ebenfalls kein Riegel vorgeschoben.
Es ist vielmehr eine wirksame Kontrolle des gesamten Netzverkehrs in und aus den an das VPN angeschlossenen lokalen Netzwerken notwendig. Dazu sind die lokalen LANs, die über ein VPN miteinander gekoppelt sind, auf adäquate Weise mittels Firewalls abzusichern, da andernfalls der über das öffentliche Netz verschlüsselt übertragene Verkehr innerhalb der LANs von einem Angreifer, dem es gelingt, in diese einzubrechen, wieder leicht im unverschlüsselten Format abzuhören ist.

Nichtsdestotrotz sieht die Zukunft von virtuellen privaten Netzwerken sehr rosig aus und alle Wirtschafts-Institute prognostizieren für die Zukunft große Wachstumsraten.

9 Abbildungsverzeichnis

10 Literatur

[Bell2001] Bob Bellman: *MPLS: Panacea or Passing Fancy?*; Business Communications Re view, S.38-44, Februar 2001

[Bor99] Petra Borowka: *Internetworking – Wege zum strukturierten Netzwerk*; MITP, 1999, Bonn

[Britt2000] Paul Brittain, Adrian Farrell: *MPLS Virtual Private Networks – A review of the implementation options for MPLS VPNs including the ongoing standardization work in the IETF MPLS Working Group*; Nov 2001, http://www.dataconnection.com/download/mplsvpns.pdf

[Cisco2000] Virtual LAN Communications, Cisco White Paper, Cisco Systems Inc., http://www.cisco.com/warp/public/cc/pd/wr2k/cpbn/tech/vlan_wp.htm

[Knabl 2001] Gisela Knabl: *Sprache und Daten aus einer Hand*; Funkschau 25/2001, S.40-43

[Kuri99] Jürgen Kuri: *Privatissimo - Virtual Private Networks als Abhilfe gegen Lauschangriffe*, c´t 4/99, S.190-194

[Lipp2001] Manfred Lipp: *VPN–Virtuelle Private Netzwerke*; Addison-Wesley, 2001

[MPLS2000] *Multiprotocol Label Switching (MPLS)*; Web Tutorial, http://www.iec.org

[Murhammer et. al. 99] Martin W. Murhammer, Orcan Atakan, Zikrun Badri, Beomjun Cho, Hyun Jeong Lee, Alexander Schmid: *A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management*; IBM Redbook, 1999; http://www.redbooks.ibm.com

[Pass96] David Passmore, John Freeman: *The Virtual LAN Technology Report*; 1996, http://www.3com.com/nsc/200374.html

[Phifer2000] Lisa Phifer: *The Remote Access Conundrum Part 2: Tunneling at Layer Two*; VP Core Competence, Inc., 2000

[RFC2341] A. Valencia, M. Littlewood, T. Kolar: *Cisco Layer Two Forwarding (Protocol) "L2F"*, RFC 2341, IETF Network Working Group, Mai 98

[RFC2401] S. Kent, R. Atkinson: *Security Architecture for the Internet Protocol;* RFC2401, IETF Network Working Group, Nov. 98

[RFC2637] K. Hamzeh, G. Pall, W.Verthein, J. Taarud, W. Little, G. Zorn: *Point-to-Point Tunneling Protocol (PPTP)*; RFC 2637, IETF Network Working Group, July 1999

[RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter: *Layer Two Tunneling Protocol "L2TP"*; RFC 2661, IETF Network Working Group, August 1999

[RFC3193] B. Patel, B. Aboba, W. Dixon, G. Zorn, S. Booth: *Securing L2TP using IPSec*; RFC 3193, IETF Network Working Group, Nov. 2001

[Ryan98] Jerry Ryan: *Multiprotocol Label Switching (MPLS)*; Technology Guide, 1998, http://www.itpapers.com/resources/tech_guides.html

[Salam99] Salvatore Salamone: *PPTP is the Tunnel most travelled*; Internet Week , Juni 99 http://www.internetwk.com/vpn/vpnsupp062199-4.htm

[Schmeh98] Klaus Schmeh:*Krypto-Protokolle für das Internet - Einer passt*; iX 12/98, S. 113-117

[Schmidt98] Michael Schmid: *Unter Ausschluß der Öffentlichkeit - Virtual Private Networks-vertraulicher Datenaustausch über das Internet*; c´t 8/98, S.226-233

[Schob99] Robert Schoblick: *Virtuelle private Netze - die Technik*; Funkschau 24/99 (1999), S.73-75

[Schob2002] Robert Schoblick: *Multiprotocol Label Switching (MPLS)*; Funkschau 8/2002, S.57/58

[Stender97] Arnold Stender: *Tunnel durchs Internet*; Gateway Juli 97 (1997), S.102-105

[Stern98] Andreas Stern: *Switching im lokalen Netzwerk*; Funkschau 4/98, S. 44-47

[Tanen96] Andrew S. Tanenbaum: *Computer Networks;* Prentice-Hall, 1996

[UCD98] University of California, Davis – Network 21 Project: *VLAN Information*; 1998, http://net21.ucdavis.edu/newvlan.htm

[Welch99a] Peter J. Welcher: *Switching - VLAN´s*; Cisco World Article 8/99, http://tele.sunyit.edu/welcher/switchvlan.pdf

[Welch99b] Peter J. Welcher: *Switching – Trunks and Dynamic Trunking Protocol (DTP)*; Cisco World Article 9/99, http://tele.sunyit.edu/welcher/switchvtp.pdf