HANSER

# VPN - Virtual Private Networks

Wolfgang Böhmer

Kommunikationssicherheit in VPN- und IP-Netzen, über GPRS und WLAN

ISBN 3-446-22930-2

Leseprobe

# 6 Varianz der VPN-Typen

In Abschn. 6.1 werden drei wesentliche Einsatzmöglichkeiten von VPN-Technologien für unterschiedliche Geschäftsvorfälle beschrieben. Abschn. 6.2 behandelt die Randbedingungen für den Einsatz eines VPN und stellt den Bezug zu der in Abschn. 3.2.6 diskutierten Sicherheitsphilosophie her.

Die elektronischen Unternehmensgrenzen (Perimetergrenzen) lösen sich zusehens auf. Dieser Prozess wird – je nach Geschäftsanforderung – unterstützt durch ein vom Unternehmen selbst realisiertes VPN, durch das VPN eines Netzanbieters (NSP)[1] oder eines reinen Internetanbieters (ISP)[2].

Infonetics Research schreibt in ihrem 1997 erschienenen VPN-Report, dass mit einem VPN eine Kosteneinsparung von 20% bis 47% gegenüber herkömmlichen Weitverkehrsverbindungen erreicht werden kann. Noch größer sind die Kosteneinsparungen (60% - 80%) bei einem Remote-Access-VPN. Damit verspricht die VPN-Technologie den Unternehmen eine Verminderung des zunehmenden Kostendruckes, der auf der IT lastet und hält für jeden Geschäftsvorfall eine adäquate Lösung parat. Abb. 6.1 zeigt die drei wesentlichen Anwendungsfälle heutiger VPN-Lösungen:

**Intranet-VPN:** Dieser VPN-Typ verbindet Außenstellen und entfernt gelegene Büros über eine geteilte, meist öffentliche Infrastruktur mit einer Zentrale. Über diese Infrastruktur werden dezidierte Verbindungen eingerichtet. In den entfernt angebundenen Außenstellen und Büros sind die gleichen Geschäftsprozesse möglich wie im privaten Netzwerk des Unternehmens. Eine Kommunikation findet unter sicheren Randbedingungen statt. Gesonderte Einwahlmechanismen können bei geeigneter Architektur wegfallen.

**Extranet-VPN:** Es ermöglicht eine Anbindung von Zulieferern, Partnern und eventuell eigenen Kunden sowie anderen am Intranetzugang der Firma interessierten Gruppen. Eine Verbindung erfolgt über eine geteilte öffentliche Infrastruktur. Relevante Geschäftsprozesse sind wie im privaten Netzwerk der Firma möglich, allerdings innerhalb vorgegebener Sicherheitsrichtlinien und QoS-Anforderungen. Eine spezielle Einwahl ist auf jeden Fall erforderlich.

**Remote-Access-VPN:** Entfernte technische Außendienstmitarbeiter, Vertriebsmitarbeiter, Heimarbeiter und eventuell kleine Büros wählen sich über öffentliche Wählleitungen, z.B. ISDN oder PSTN, ins Firmennetz ein. Es wird

---

[1] Ein Network Service Provider (NSP) bietet seinen Kunden eine dezidierte IP-Bandbreite auf seinem privaten Backbone an, vielfach auf Grundlage eines Asynchronous Transfer Modus (ATM) oder auf Basis der Frame-Relay-Technik an. Häufig wird darüber hinaus den Kunden auch ein Internetzugang bereit gestellt.

[2] Ein Internet Service Provider (ISP) bietet seinen Kunden ausschließlich einen Internet-Zugang an.

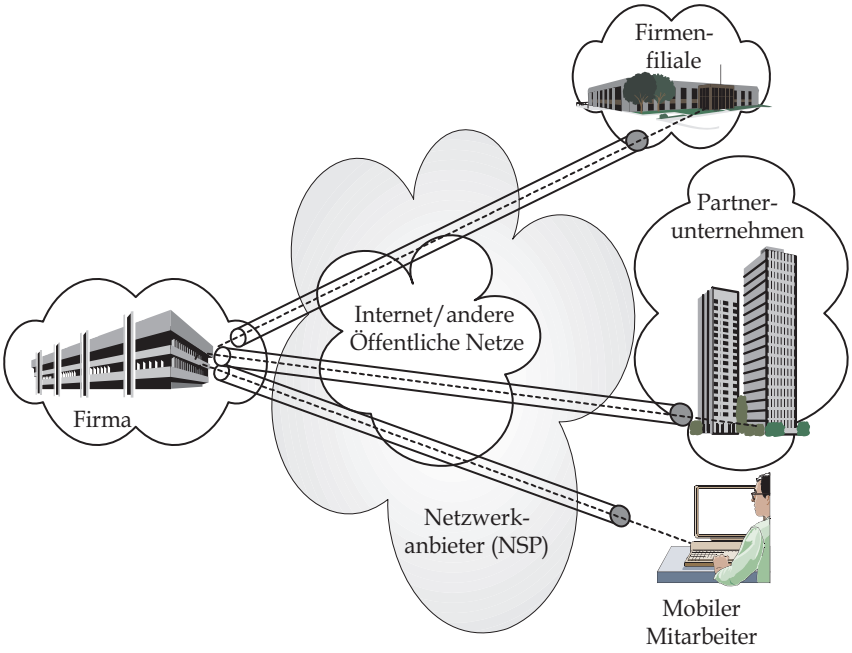


*Abb. 6.1: VPN-Anwendungsspektrum*

ihnen ein Rechteprofil für den Zugriff auf Netzwerkressourcen und Applikationen eingeräumt. Die Mitarbeiter können dieselben Geschäftsprozesse ausführen, als ob sie ihren Computer im Firmennetzwerk bedienten. Eine spezielle Einwahl ist auf jeden Fall erforderlich.

Natürlich können diese drei VPN-Typen gleichzeitig und vermischt eingerichtet werden. Es gibt die Möglichkeit, den jeweiligen VPN-Typ durch einen Netzanbieter (NSP) realisieren zu lassen oder nur den reinen Internetanschluss von einem (ISP) zu beziehen, um in Eigenregie ein eigenes VPN aufzubauen, zu betreiben und zu warten.

Dabei ist bei den drei VPN-Typen offen, welche Art von VPN-Technologie eingesetzt wird. Es kann ein Secure VPN, ein Trusted VPN (Extranet) oder aus einer Hybrid VPN-Technologie bestehen.

## 6.1 VPN-Einsatzmöglichkeiten

Obgleich die VPN-Technologien nahezu standardisiert sind, unterstützen nicht alle Produkte am Markt alle VPN-Typen. Solange nur eine Technologie zum Einsatz kommt, ist dies nicht kritisch. Dennoch sind für eine geeignete VPN-Lösung folgende Gesichtspunkte zu beachten. Die VPN-Lösung sollte:

- auf die Geschäftsprozesse abgestimmt sein,
- eine hinreichende Kommunikationssicherheit bieten,
- ausreichende Performance liefern und
- interoperabel zu den bestehenden Systemen sein.

Den größten Mehrwert kann ein Unternehmen erreichen, wenn sich eine vorhandene Lösung bei Veränderungen – z.B. Geschäftsprozessen – flexibel erweitern bzw. neuen Technologien anpassen lässt. Immer mehr Produkte ermöglichen diese Flexibilität.

Nahezu alle IPSec-basierten VPN beruhen derzeit auf eine IPv4-Umgebung, die in absehbarer Zeit nicht mehr das dominante Protokoll im Internet sein wird; Version IPv6 gewinnt zunehmend an Bedeutung. Somit ist es heute schon wichtig, dass die ausgewählten Lösungen kompatibel bzw. an die künftige IPv6-Version anpassungsfähig sind. Allerdings spielt, um eine gelungene VPN-Implementierung zu erreichen, neben der Technik auch die Erfahrung des beratenden Unternehmens eine große Rolle.

Häufig wird die Kommunikationssicherheit (Kapitel 3) als ein gravierendes Problem beim Einsatz eines VPN hervorgehoben. Es gibt heute ausgereifte kryptographische Absicherungsmöglichkeiten (Kap. 4), die stets aktuell gehalten werden und die auf künftige Gegebenheiten erweitert werden (Abschn. 4.2.5). Bei einer sorgfältigen Planung und einer gut abgestimmten Sicherheitspolitik sowie ausreichenden Sicherheitsmaßnahmen spielt die Kommunikationssicherheit eher eine untergeordnete Rolle. Im Prinzip sollten zwei unterschiedliche Vertrauensmodelle bei einer VPN-Planung berücksichtigt werden. In dem einen Modell vertraut das Unternehmen a priori *nicht* dem Netzanbieter – vor allem dann, wenn das VPN über Netze mehrerer Anbieter geführt werden soll, was im Rahmen der Globalisierung keine Seltenheit mehr ist. So gilt z.B. das *Layer-2-Tunneling-Protokoll* allein schon lange nicht mehr als sicher. Deshalb hat die IETF empfohlen, den Tunnelverkehr mittels IPSec zu verschlüsseln. Somit muss eine Firma, die auf das Layer-2-Tunneling-Protokoll setzt, entsprechende eigene Maßnahmen ergreifen. In Abschn. 7.2.3 wird näher auf das Layer-2-Tunneling-Protokoll (L2TP) eingegangen.

Im Alternativmodell traut das Unternehmen dem Netzanbieter (NSP) zu, ein fremdgewartetes, sicheres VPN zu unterhalten. Dies ist vergleichbar mit der Bereitstellung von öffentlichen Frame-Relay- oder auch ATM-Diensten eines Netzanbieters, wenn man von der zukünftigen MPLS-Technologie und den optischen Netzen absieht. In diesem Modell vertraut das Unternehmen darauf, dass keine IP-Pakete fehlgeleitet, verändert, belauscht oder analysiert werden. Ebenso wird den Firewallaktivitäten – z.B. funktionierende Filterlisten oder Firewall-Monitoring – des Netzanbieters vertraut.

Ausgehend von den sieben Schichten des OSI-Referenzmodells (Abb. 2.2) können verschiedene Sicherungsmaßnahmen auf den verschiedenen Ebenen zur Absicherung unterschiedlicher VPN-Typen installiert werden – je nachdem welches

Ziel und welches Vertrauensmodell verfolgt wird. Generell lassen sich aus einem VPN-Blickwinkel die sieben Schichten auf drei VPN-Ebenen reduzieren (Abb. 6.2):

- VPN auf der Applikationsebene in den Schichten (5 - 7),
  - Ein VPN auf Layer-5 kann eine sichere Kommunikation auf der Session-Ebene über einen Proxy-Dienst aufbauen, indem TCP verwendet wird. Diese Architektur ist gut geeignet, um mit Partnernetzen zu kommunizieren. Der VPN-Client arbeitet auf der Transportschicht problemlos mit den Computern des Partnernetzes zusammen. Ebenso überwindet auf dieser Ebene der VPN-Client auf einfache Weise die Firewall des Partner-Extranetzes, was bei einem VPN auf Layer-3 schwieriger ist. VPN auf Layer-5 sind jedoch nicht in der Lage, RPC-basierte Dienste abzufangen, so dass ein mobiler Nutzer keine File- und Druckerdienste ausführen kann, wie es für einen entfernten LAN-Zugriff üblich ist. Allerdings können alle auf TCP-aufbauenden Anwendungsprotokolle wie HTTP, FTP oder Telnet eingesetzt werden, ohne dass in bestehenden Anwendungen Änderungen auf den Partnercomputern vorgenommen werden müssen.
- VPN auf der Transport-/Netzwerkebene in den Schichten (3 - 4),
  - Ein Layer-4-VPN dient der sicheren Kommunikation auf der Transportschicht. Diese Art VPN ist gut geeignet für die sichere Kommunikation von zwei oder mehreren Netzwerken, die eine sichere Verbindung für E-Commerce-Anwendungen benötigen.
  - Ein Layer-3-VPN bietet die Möglichkeit, neben TCP/IP, auch Protokolle wie RPC und UDP einzusetzen. Derartige VPN-Lösungen werden vornehmlich für ein Remote-Access-VPN eingesetzt und bieten dem Nutzer ein breites Anwendungsspektrum. Allerdings ist das Supportaufkommen nicht zu unterschätzen.
- VPN auf der Sicherungs-/Bitübertragungsebene in den Schichten (1 - 2)
  - VPN auf den unteren Schichten besitzen gegenüber VPN der höheren Schichten den Vorteil, dass wesentlich einfacher Quality of Service-Garantien (QoS) verbindlich erteilt werden können. Vorteile liegen in der Skalierbarkeit und im VPN-Management.

In diesem Kontext wird auf die VPN-Technologie sowohl auf der Applikationsebene als auch auf der Transport/Netzwerk- und der Sicherungs-/Bitübertragungsebene eingegangen. Die technischen Voraussetzungen werden in den nächsten Kapiteln behandelt.

In den drei Ebenen (Applikationsschicht, Transport-/Netzwerkschicht und Link- bzw. Physikalische-Ebene) lassen sich die wesentlichen Protokolle und Sicherungsmechanismen einordnen, mit denen sich die vollständige Absicherung eines VPN und damit auch des sonstigen Datenverkehrs erreichen lässt. Da

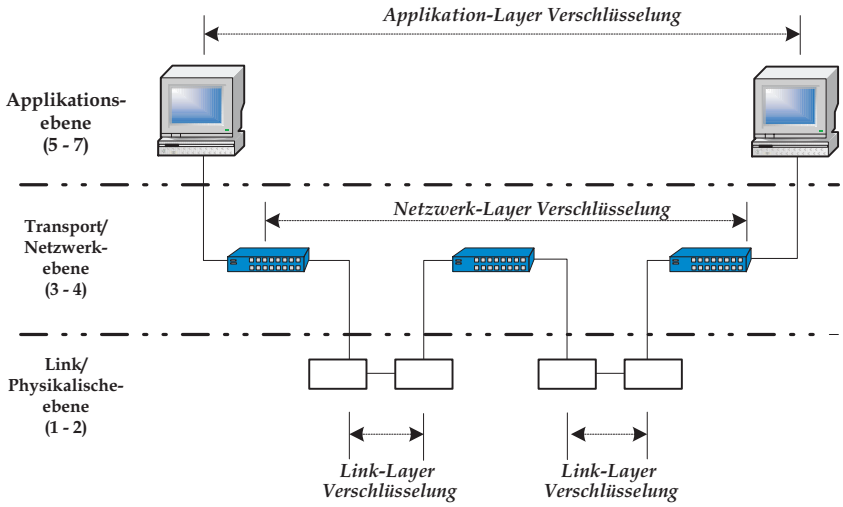


*Abb. 6.2: Einordnung der VPN ins Schichtenmodell*

die VPN-Technologie in direktem Zusammenhang mit der vertraulichen Datenübertragung steht, haben sich im Laufe der Zeit in den drei Ebenen unterschiedliche Absicherungsmechanismen mit unterschiedlichen Zielsetzungen herauskristallisiert. Abb. 6.3 zeigt die Protokolle und Verfahren zur Absicherung der unterschiedlichen VPN-Lösungen auf den Schichten (1 - 7). Hervorzuheben ist die Absicherung auf der Netzwerkebene oder speziell die IP-Absicherung. Eine effektive Absicherung wird in Abschn. 7.4 mit der Diskussion über IPSec vorgestellt.

Einige der modernen kryptographischen Sicherungsmechanismen lassen sich in der Anwendungsebene finden, z.B. in Secure MIME (S/MIME) oder Pretty Good Privacy (PGP). Die gängigen für ein VPN geeigneten Sicherheitstechnologien sind:

- IP Paket Filtertechniken
- Network Address Translation (NAT)
- IP Security Architecture (IPSec)
- SOCKS
- Secure Socket Layer (SSL)
- Application Proxyies
- Firewall-Systeme
- Kerberos, RADIUS, DIAMETER, TACACS+ und andere Authentifizierungssysteme

- Antivirus, Content-Überprüfung und Intrusion Detection Systeme (IDS)

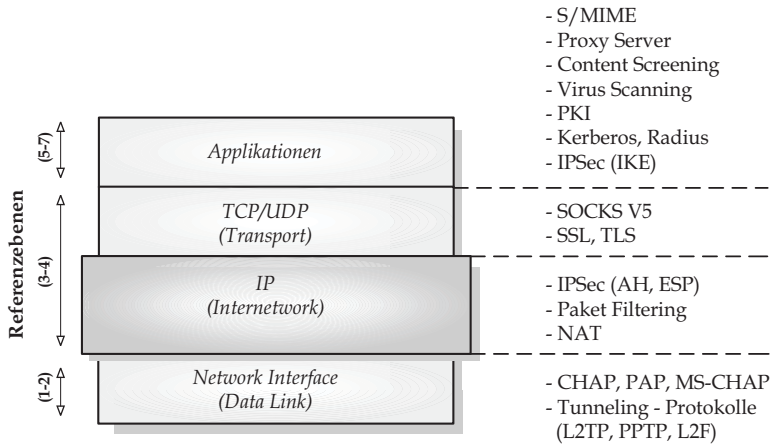


*Abb. 6.3: Typische Absicherungsmechanismen für VPN-Lösungen auf unterschiedlichen Schichten*

Abb. 6.3 zeigt die Technologien bezogen auf die Internet-Schichtenansicht. Die mittlere Schicht (Transport-/Netzwerkschicht) ist hervorgehoben, weil sie eine bedeutende Rolle in der VPN-Technologie spielt. Aufgrund der zahlreichen Möglichkeiten ist es interessant zu wissen, wie sich die einzelnen Technologien ergänzen, überlappen oder ob sie für bestimmte Absicherungen einfach nicht geeignet sind.

Der Vergleich in Tabelle 6.1 berücksichtigt wiederum die speziellen Anforderungen eines VPN und ermöglicht den Entwurf einer ersten Sicherheitsarchitektur. Das gewünschte Sicherheitsniveau lässt sich einfach nivellieren. Details werden im Kapitel 10 behandelt. In der ersten Spalte von Tab. 6.1 sind die wesentlichen Lösungen, Protokolle und Mechanismen aufgelistet, in der ersten Zeile die typischen Sicherungsmöglichkeiten. Wie der Matrix zu entnehmen ist, bietet eine IP-Filterung nur die Möglichkeit einer Zugriffskontrolle und einer UDP-Unterstützung. Im Gegensatz dazu bietet IPSec die weitreichendsten Möglichkeiten, jedoch keine Session-Überwachung. Es wird deutlich, dass eine Kombination der unterschiedlichen Möglichkeiten ratsam ist. Um das gewünschte Sicherheitsniveau zu erreichen, sollte eine entsprechende Sicherheitsstrategie vorhanden sein. An dieser Stelle sei darauf hingewiesen, dass es nicht sinnvoll ist, ein Sicherheitsniveau anzustreben, wenn vorher nicht festgelegt wurde, was vor wem zu schützen ist (Kap. 3).

### 6.1.1 Intranet-VPN (Site-to-Site)

Kennzeichnend für ein Intranet-VPN ist, dass es verschiedene Standorte derselben Firma verbindet. Dies ist eines der einfachsten und häufigsten VPN-Szen-

*Tabelle 6.1: Vergleich charakteristischer Sicherheitstechnologien für VPN-Lösungen*

| Lösung | Zugriffskontrolle | Verschlüsselung | Authentifizierung | Integritätsprüfung | Schlüsselaustausch | Verbergen der internen Adresse | Schutz gegen Wiedereinspielen | Session-Kontrolle | UDP-Unterstützung |
|---|---|---|---|---|---|---|---|---|---|
| **IP-Filter** | Ja | Nein | Nein | Nein | Nein | Nein | Nein | Nein | Ja |
| **NAT** | Ja | Nein | Nein | Nein | Nein | Ja | Nein | Ja (Verbindung) | Ja |
| **L2TP** | Ja (Verbindung) | Ja (PPP-Link) | Ja (call) | Nein | Nein | Ja | Nein | Ja (call) | Ja |
| **IPSec** | Ja | Ja (Paket) | Ja (Packet) | Ja (Paket) | Ja | Ja | Ja | Nein | Ja |
| **SOCKS** | Ja | Optional | Ja (client / user) | Nein | Nein | Ja | Nein | Ja (Verbindung) | Ja |
| **SSL** | Ja | Ja (Daten) | Ja (system user) | Ja | Ja | Nein | Ja | Ja | Nein |
| **Appl.-Proxy** | Ja | normal nicht | Ja (user) | Ja | normal nicht | Ja | normal nicht | Ja (Verbindung, Daten) | normal nicht |
| **AAA-Server** | Ja (Verbindung) | einige | Ja (user) | Nein | normal nicht | Nein | Nein | Nein | Ja |

arien, die heutzutage anzutreffen sind. Abb. 6.1 zeigt das typische Beispiel der Anbindung einer Filiale (oberer Teil der Abbildung) an die Firmenzentrale (unten im Bild).

Am Aufbau eines Site-to-Site-VPN sind zwei VPN-Gateways / Firewall-Systeme beteiligt. Die Verschlüsselung der Daten erfolgt nur auf dem Weg zwischen den beiden VPN-Gateways; der Weg durch das lokale Netz vom Gateway zum Endgerät bleibt unverschlüsselt. Das VPN ist somit für Endgeräte transparent und sie benötigen keine zusätzliche VPN-Client-Software. Abb. 6.4 zeigt eine typische Konfiguration. Hier zielt eine VPN-Absicherung darauf, dass unbefugte Dritte nicht in das Intranet eindringen können, und dass die Daten, die über das Internet oder über das IP-Netz eines Providers (ISP) geführt werden, auf dem Übertragungswege für unbefugte Dritte unbrauchbar sind.

Eine Möglichkeit, ein *Site-to-Site*-VPN zwischen einer Zentrale und einer Niederlassung einzurichten, besteht darin, lediglich einen Internetanschluss bei einem ISP zu mieten und auf beiden Seiten Firewall-Systeme bzw. Router mit integrierter Firewall-Technologie oder spezielle IPSec-Gateways an der Schnittstelle zum Internetanschluss einzurichten. Dieses Szenario benötigt keine zusätzliche IPSec-Technologie, wenn die Firewall bzw. der spezielle Router die für IPSec notwen-

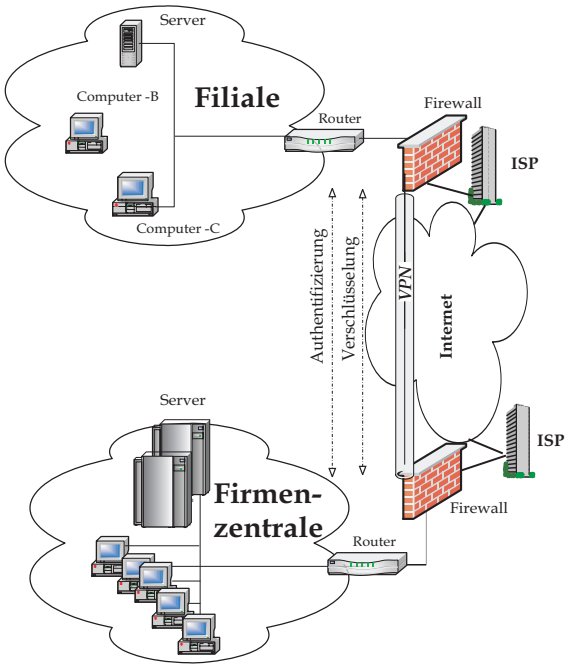


*Abb. 6.4: Beispiel eines typischen Intranet-VPN*

digen Schritte durchführt. Kapitel 7 geht detailliert auf diese Techniken ein. Mit dieser Lösung können vertrauliche Informationen – ohne Zugriff oder Kenntnisnahme von unbefugten Dritten – verschickt werden. Die Firewall hält dabei wirksam Angriffe ab.

### 6.1.2 Extranet-VPN (End-to-End)

In einem Extranet werden virtuelle Verbindungen zwischen den Sites mehrerer Firmen, die unterschiedliche Interessen haben können, verknüpft. Ein sehr eindrucksvolles Beispiel ist in Abbildung 1.4 illustriert. Es zeigt das Branchennetz der Automobilindustrie, das mit dem ENX-Projekt ein europaweites Extranet eingerichtet hat. Dabei haben die beteiligten Organisationen (Hersteller / Zulieferer) unterschiedlich beschränkte Zugriffe auf das Extranet. Es lassen sich weitere Vorteile für ein Extranet-VPN aufzählen:

- Eine weitgefächerte Erreichbarkeit des Unternehmens
- Eine größere zeitliche Effizienz der Geschäftsprozesse
- Ein besserer Kundenservice

- Eine bessere Zusammenarbeit innerhalb des Unternehmens
- Eine Verbesserung der Zusammenarbeit innerhalb der Wertschöpfungskette im Bereich der Zulieferer *(Supply Chain)*
- Eine frühere Investitionsrückgewinnung *(Return of Investment)*

Ein Extranet kann über das Backbone eines einzigen Netzbetreibers geschaltet sein. Es können jedoch auch mehrere Netzbetreiber und sogar autonome Systeme hinzugezogen werden, wenn dies für die Zusammenschaltung erforderlich ist. Somit existiert ein gravierender Unterschied zum Intranet-VPN, in dem Zugangskontrollmechanismen den beschränkten Zugriff der unterschiedlichen Organisationen regeln. Diese Zugangskontrolle wird häufig mit Firewall-Systemen, mit Zugriffslisten *(Access Lists)* in den jeweiligen Routern oder mit richtlinienbasierte Kontrollen *(Policy-based Access Controls)* realisiert. Diese Kontrollen können mit speziellem Equipment firmenseitig oder auf der Netzbetreiber-Seite durchgeführt werden. Abb. 6.5 zeigt ein typisches Extranet-VPN zwischen einem Hersteller und einem Zulieferer.

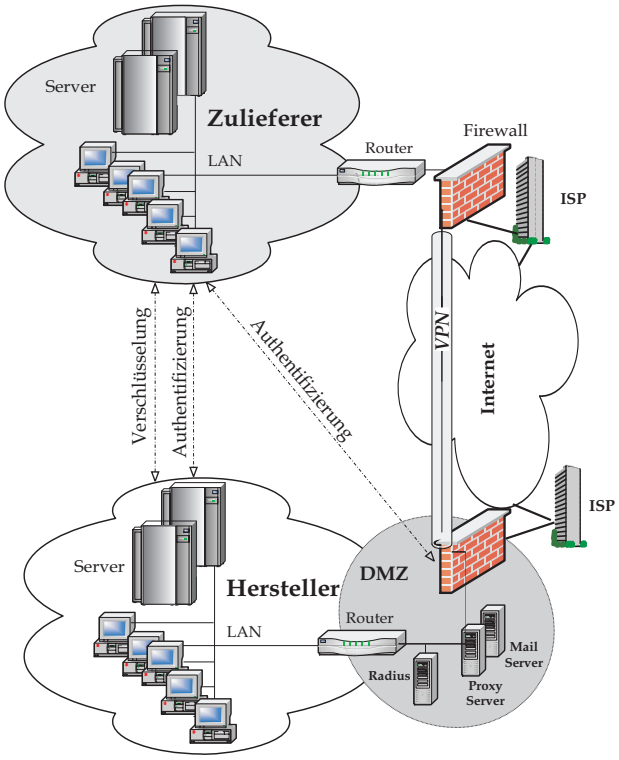


*Abb. 6.5: Beispiel eines Extranet-VPN*

In einem End-to-End-VPN erfolgt die Verschlüsselung häufig direkt zwischen zwei Endgeräten über den gesamten Kommunikationsweg hinweg. Beide Seiten sind mit einer VPN-Client-Software ausgestattet und müssen die öffentlichen Schlüssel aller Kommunikationspartner kennen. Bei der Kommunikation über das Internet benötigt jeder VPN-Client eine offizielle feste IP-Adresse. Ein VPN dieser Kategorie kann z.B. zwischen dem Arbeitsplatzrechner einer Zulieferfirma und der Produktionsfirma, die mit dem Zulieferer zusammenarbeitet, geschaltet sein. Dabei kann eine Kommunikationsverbindung direkt zum Intranet-Server des Herstellers eingerichtet werden. Häufig entsteht eine Ende-zu-Ende-Verbindung.

Die Authentifizierung des Arbeitsplatzrechners bei einem Verbindungsaufbau wird zuerst an der Firewall bzw. an dem Router des Herstellers und anschließend am Server im Intranet des Herstellers durchgeführt. Eine Berechtigungsvalidierung findet für einen Verbindungsaufbau seitens des Zulieferers an zwei Punkten statt. Wie der hierzu notwendige Tunnel eingerichtet wird, hängt stark von den QoS-Anforderungen der Beteiligten ab. Im einfachsten Fall kann z.B. ein IPSec-VPN über das Internet geschaltet werden. Die Datenpakete, die ausgetauscht werden, werden für unbefugte Dritte unbrauchbar übertragen.

### 6.1.3 Remote-Access-VPN (End-to-Site)

Ein End-to-Site-VPN ist eine Mischung aus den ersten beiden Varianten. Sie dient dem Aufbau von Remote-Access-VPN, wenn ein externer Client eine verschlüsselte Verbindung zum Firmennetz benötigt. Die Verschlüsselung erfolgt vom Client zum VPN-Gateway, wobei derzeit noch alle Clients mit einer VPN-Client-Software ausgestattet werden müssen[3], da das IP selbst erst ab der Version IPv6 eine Verschlüsselungsmöglichkeit besitzt. Die klassische Anwendung eines Remote-Access-VPN ist die Anbindung von Außendienstmitarbeitern. Z.B. bei Versicherungsunternehmen ergreifen die Versicherungsvertreter die Initiative, um mit dem Firmennetz eine Verbindung herzustellen. Abb. 6.1 zeigt im oberen rechten Teil den Verbindungsaufbau eines VPN mit einem mobilen Endgerät (Laptop) mittels DFÜ über den Internetzugang eines Providers (ISP) ins LAN seines Unternehmens. Meistens wird DHCP eingesetzt, so dass eine reguläre Firewall die IP-Adresse nicht zuordnen kann. Eine andere Möglichkeit ist die Einwahl[4] in das IP-Netz eines Providers; an der Firmen-Firewall muss dann eine zweite Authentifizierung durchgeführt werden.

Die Kontaktaufnahme mit einem Firmennetzwerk von einem außerhalb gelegenen Standort ist so neu nicht. Seit geraumer Zeit können sich Firmenmitarbeiter

---

[3] In jüngster Zeit wird dieser Zugriff häufig mit einem TLS / SSL-VPN geregelt. Dann ist keine Client-Software notwendig.

[4] Dies geschieht oftmals über eine separate 800-Telefonnummer. Die Einwahl ist dann durch ein allgemeines Passwort für die ganze Firma geschützt.

via Modem ins Firmennetz einwählen – allerdings mit einer inzwischen überholten Übertragungsleistung. Diese Möglichkeit fordert den Unternehmen die Installation von Modempools, entsprechende Räumlichkeiten und geschultes Personal ab. Mit einem Remote-Access-VPN fallen diese häufig aufwändigen Rand-

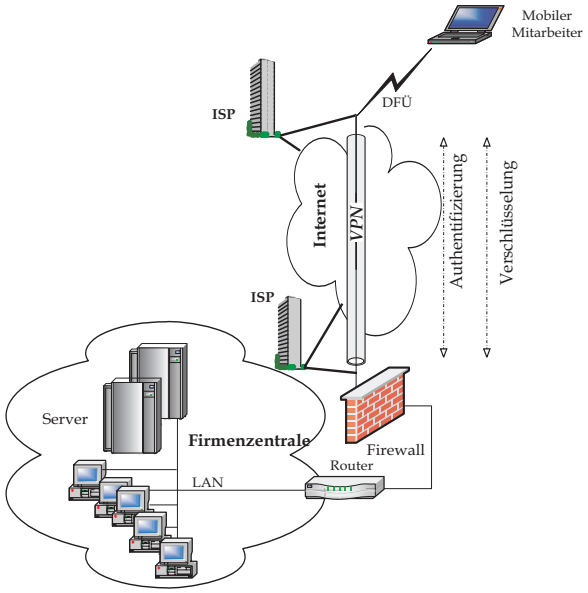


*Abb. 6.6: Schematische Darstellung eines Remote-Access-VPN*

bedingungen weg und ermöglichen eine Kostenreduktion bei gleichzeitigem Übertragungs- und Informationsgewinn für die Außendienstarbeiter des Unternehmens. Im Gegensatz zu einer Modemverbindung wird bei einem Remote-Access-VPN die Kommunikationsverbindung zu einem Internet Service Provider aufgebaut. Heutige Betriebssysteme wie Windows 2000 oder Linux sind hierfür ausreichend vorbereitet. Auch mit preiswerten ISDN-Routern, wie z.B. von DrayTek, Netgear, AVM etc. kann eine Verbindung aufgebaut werden. Verwendete Protokolle sind L2TP, L2F, PPTP oder IPSec. Diese werden im Kapitel 7 ausführlich behandelt.

Ein Tunnelaufbau mittels Authentifizierung und Datenverschlüsselung wird in einem zweiten Schritt zwischen der Firewall des Unternehmens und dem einwählenden Computer, z.B. einem Laptop, aufgebaut (Abb. 6.6). Im Prinzip gibt es für solch ein Szenario zwei Möglichkeiten, um ein Remote-Access-VPN aufzubauen:

**Client-initiiert:** Über die Einwahlsoftware auf dem Laptop des Außendienstmitarbeiters wird eine sichere IP-Verbindung zum Internet Service Provider aufgebaut und zum Unternehmensnetz weitergeleitet.

**Server-initiiert:** Vom Client-Rechner (Laptop) wird eine nichtsichere Verbindung zum ISP aufgebaut und erst der Network Access Server (NAS) stellt anschließend eine sichere Verbindung über das öffentliche Netz zwischen Client-Rechner und NAS her.

Beide Varianten habe ihre Vor- und Nachteile, die je nach Anforderung mehr oder weniger ins Gewicht fallen. Bei der zweiten Lösung fällt wesentlich weniger Aufwand für Installation, Wartung und Update-Service an. Beispielsweise kann bei einer umfangreichen Laptop-Basis mit etlichen hundert oder gar tausend Geräten ein erheblicher Aufwand und Kostenblock entstehen, wenn zuvor eine Modemeinwahl möglich war, die nun im Zuge eines Remote-Access-VPN ausgetauscht werden soll. Allein die Installation der Client-Software ist eine logistische und technische Herausforderung, wenn außerdem die künftige Authentifizierung mittels Smart Card erfolgen soll – ganz abgesehen davon, dass zuvor eine Public-Key-Infrastruktur (PKI) im Unternehmen aufgebaut werden muss.

## 6.2 Eckpunkte für den Einsatz eines VPN

Vor der Planung eines VPN muss man sich über einige Randbedingungen im Klaren sein. Der zentrale Anschluss eines VPN in das Firmennetz erfolgt durch ein spezielles VPN-Gateway, eine Firewall oder durch einen Router. An diesem Anschlusspunkt muss eine VPN-Sicherheitspolitik umgesetzt werden, die mit dem vorhandenen IT-Sicherheitskonzept in Einklang stehen muss. Nachfolgend werden zu diesem Anschlusspunkt einige Überlegungen angestellt.

### 6.2.1 VPN-Sicherheitspolitik

Bevor via VPN ein Zugang zum Firmennetz eingerichtet wird, ist es sinnvoll, einige grundsätzliche Überlegungen zum Thema Kommunikationssicherheit anzustellen (siehe auch Kapitel 3). Ausgehend von der Überlegung, dass ein verschlüsselter VPN-Tunnel nicht ohne weiteres kompromittiert werden kann, sind die beiden Endpunkte eine nicht zu unterschätzende Gefahrenzone, wenn keine speziellen Maßnahmen, wie z.B. in Kapitel 5 beschrieben, vorgenommen wurden. Nie kann sich ein Kommunikationspartner vollkommen sicher sein, dass kein unbefugter Dritter eine Verbindung aufbaut. Weiterhin kann es bei der heutigen Virenflut nur zu leicht passieren, dass ein „Wurm“ oder „Trojaner“ seine zerstörerischen Aktivitäten selbst über eine verschlüsselte Verbindung entfaltet – obwohl gerade die Transparenz für die Anwendungen einer der Pluspunkte eines VPN ist.

Von einem Laptop aus können sich Würmer über das VPN ins Firmennetz einschleusen und durch die Windows-Dateifreigaben meist unbemerkt weiterverbreiten. Ähnliches gilt für Trojanische Pferde.

Solche Risiken lassen sich nicht völlig ausschließen, können aber durch ein konkretes Sicherheitskonzept minimiert werden. Grundsätzlich muss das VPN-Gateway gegen Angriffe von außen geschützt werden. Es gelten die gleichen Regeln wie beim Betrieb einer Firewall: Außer den notwendigen Diensten – z.B. der PPTP- bzw. IPSec-Server und SSH für die Fernwartung – muss alles abgeschaltet werden. Die Umsetzung dieser Beschränkungen erfolgt beim Unternehmen, nicht beim auf dem Notebook installierten Client.

Während ein einfaches Netzwerksicherheitskonzept beschreibt, welcher Netzverkehr wohin erlaubt ist und welcher unterbunden werden soll, beschreibt ein VPN-Sicherheitskonzept mehr die Absicherungscharakteristik eines spezifischen Verkehrsprofils. Damit bildet es eine Ergänzung zum regulären Netzwerksicherheitskonzept. Es betrachtet ein spezielles Netzsegment wesentlich detaillierter, wird allerdings durch den Rahmen des Netzwerksicherheitskonzepts eingegrenzt. In einem VPN-Sicherheitskonzept ist beschrieben, durch welche Absicherungsmaßnahmen das Kommunikationsaufkommen, das durch das VPN geleitet wird, zu schützen ist:

- Wie sollen Quell- und Zielports geschützt werden?
- Welche Sicherheitsprotokolle (Tab. 6.1) sollen grundsätzlich auf welcher Ebene (Abb. 6.2) eingesetzt werden?
- Wie sehen die Sicherheitsanforderungen für die Authentifizierung, Verschlüsselung, Schlüsseltransport, Schlüssellänge sowie Lebenszeit der Schlüssel etc. aus?

Dabei können VPN-Sicherheitsrichtlinien für einzelne Geräte, Verbindungen oder zentrale Lösungen installiert werden. Vorzuziehen ist allerdings immer eine zentralisierte Einrichtung, wenn es sich um eine umfangreiche Menge von Sites oder um eine größere Anzahl von Fernzugriffen handelt, die es zu betreuen gilt. Cisco [Halpern et al. 2004] schlägt hierzu beispielsweise die SAFE-Lösung[5] vor, die im Wartungsaufwand gegenüber einer Einzellösung erhebliche Vorteile bietet.

### 6.2.2 VPN und Firewall

Werden die derzeit gängigen VPN-Gateway-Lösungen eingehender betrachtet, so lassen sie sich grob in vier Varianten einstufen. Und auch hier gilt: Die Lösung gibt es nicht, sondern alle Varianten haben ihre Berechtigung und sind in der Praxis vorzufinden. Das Rahmenwerk für die Freiheitsgrade unterschiedlicher Konstellationen ist das Sicherheitskonzept, das von der Sicherheitsarchitektur und von der im Unternehmen vorherrschenden Sicherheitsphilosophie geprägt ist (Abschn. 3.2.6).

[5] Die Fa. Cisco bietet im Rahmen der hauseigenen Blueprint-Serie SAFE eine komplette Beschreibung, konkret für kleine mittelständische, große und sehr große Firmen, zur Einrichtung eines sicheren VPN.

Die einzige Verbindung zum Internet soll ausschließlich über die Firewall erlaubt sein und deshalb soll ein VPN-Gateway hinter der Firewall platziert werden (Abb. 6.7). Allerdings ist diese Konstellation mit einigen Nachteilen verbunden:

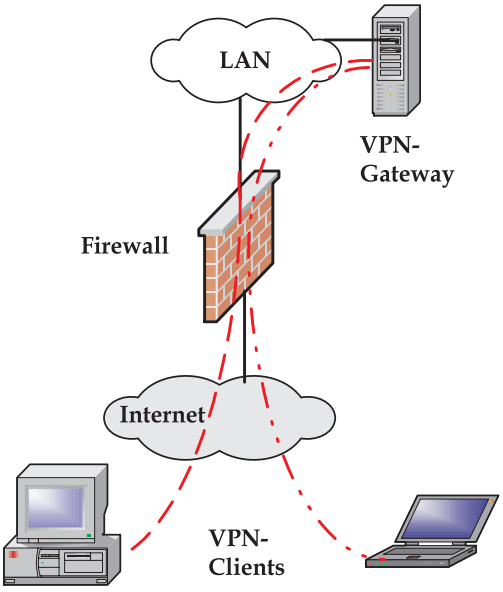


*Abb. 6.7: Das VPN-Gateway ist hinter der Firewall positioniert*

1. Die Firewall kann eingehende verschlüsselte Pakete, die für das VPN-Gateway bestimmt sind, nicht ausreichend analysieren und filtern.
2. Die Firewall kann nicht erkennen, an welche Rechner oder Ports die verschlüsselten Pakete gerichtet sind.
3. Virenfilter und Mail-Gateways haben Schwierigkeiten, mit dieser Konstellation umzugehen.
4. Gewöhnlich treten Probleme mit dem Network Address Translation (NAT) bzw. Masquerading mit einer Firewall auf, wenn z.B. ein IPSec-VPN-Gateway mit einem Authentication Header (AH) betrieben wird. Wird ausschließlich ein AH verwendet, darf aufgrund der vorgenommenen Prüfsumme nachträglich an den IP-Paketen nichts verändert werden. Dies jedoch passiert bei NAT.

Bei IPSec-Installationen (Abschn. 7.4) wird der Hash-orientierte Authentication Header (AH) allerdings seltener eingesetzt. Häufiger ist die Verschlüsselung mit Encapsulation Security Payload (ESP). Und auch hier gibt es Probleme, denn etliche kostengünstige ISDN-Router bzw. DSL-Router mit eingebauter NAT-Funktion können mit ESP oft nicht umgehen. Genaue Ausführungen zu IPSec werden

in Kap. 7 diskutiert. Gleiches gilt für das von PPTP verwendete Generic Routing Encapsulation (GRE).

Wesentlich weniger problembehaftet ist die Konstellation, bei der ein VPN-Gateway in Form einer IPSec-Lösung direkt in die Firewall integriert ist (Abb. 6.8). Hierzu existieren mittlerweile etliche Herstellerlösungen. Bei dieser Konstellation konzentriert sich z.B. für den Administrator der Aufwand in Wartung und Pflege allein auf die Firewall. Und somit reduziert sich neben den Anschaffungskosten auch die Anzahl der zu betreuenden Computer. Dennoch rät das Bundesamt für

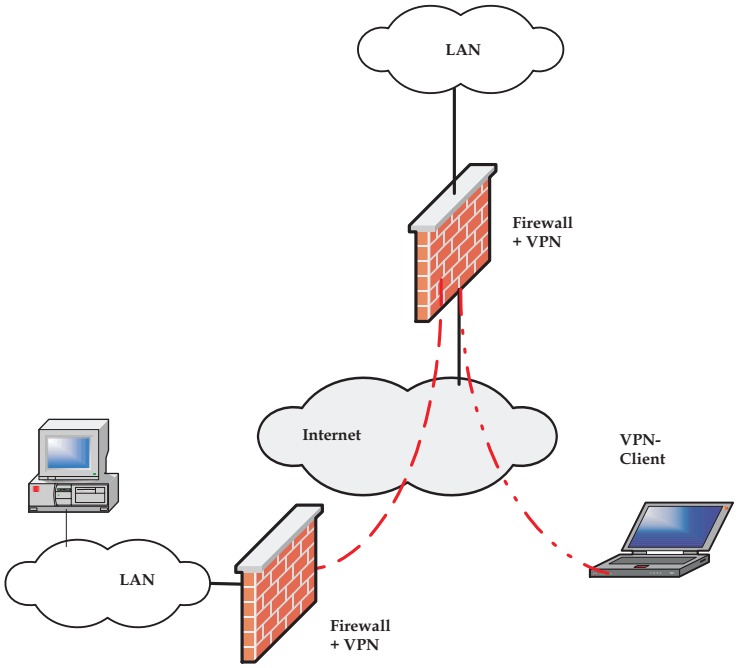


*Abb. 6.8: Das VPN-Gateway und die Firewall befinden sich auf demselben Computer*

Sicherheit in der Informationstechnik (BSI) nachdrücklich von diesen als *All-in-One* bezeichneten Lösungen ab. Begründet wird dies damit, dass jeder zusätzliche Dienst auf einer Firewall die Sicherheit beeinträchtigen kann. Häufig weisen gerade offene VPN-Ports in der Praxis eine gewisse Angriffsschwäche gegenüber den gefürchteten *Denial-of-Service-Attacken* (DOS) auf. Z.B. bei der Checkpoint-Lösung (Firewall-1) sowie bei der Nachfolger Version NG ist eine VPN-Lösung (Modul) direkt in der Firewall implementiert. Ein VPN-Client (Secure Remote-Verschlüsselungsclient) kann eine gesicherte Remote-Kommunikation über das Internet aufnehmen. Weiterhin kann eine LAN-to-LAN-Kopplung über das Internet durch die Absicherung zweier Firewall-Systeme erreicht werden. Eine vergleichbare Konstellation ist auch bei etlichen Routern möglich. Hier werden dann Anpassungen bzw. Konfigurationsänderungen an der Firewall bzw. am Router

notwendig. Folgende Änderungen müssen vorgenommen werden:

- Das IP-Forwarding muss freigeschaltet (erlaubt) werden
- Der UDP-Port 500 für das Schlüsselmanagement (IKE) muss geöffnet werden
- Die Protokollnummern 50 und 51 für (ESP) und (AH) müssen geöffnet werden
- Der UDP-Port 1701 für L2TP und L2F muss geöffnet werden
- Die IP-Protokollnummer 47 (GRE) und der TCP-Port 1723 für PPTP muss geöffnet werden

Sicherheitstechnisch ist es daher sinnvoll, das VPN-Gateway völlig aus dem Einflussbereich des LAN und der Firewall zu entfernen. Ideal ist es das VPN-Gateway in die ohnehin oft schon vorhandene demilitarisierte Zone (DMZ) zu integrieren.

Eine Minimalkonstellation zeigt Abb. 6.9: Hier wird die Firewall mit einer zusätzlichen Netzwerkkarte (Interface) ausgerüstet und an diese das VPN-Gateway angeschlossen. Zusätzlich benötigt die Firewall noch spezielle Regelerweiterungen, mit denen der Netzwerkverkehr über das Interface zum VPN-Gateway geleitet wird. Obwohl diese Konstellation in die richtige Richtung weist,

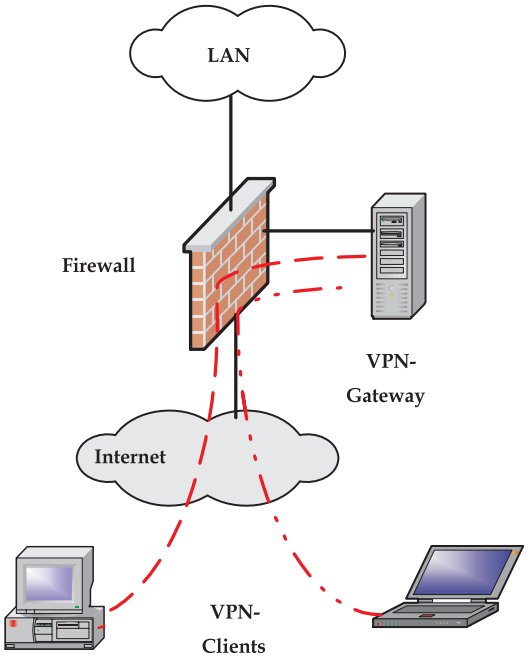


*Abb. 6.9: Das VPN-Gateway ist über eine Netzwerkkarte mit der Firewall verbunden und steht in der DMZ*

gibt es Anlass zur Kritik. Die verschlüsselten IP-Pakete, die zum VPN-Gateway umgeleitet und dort entpackt werden, werden anschließend direkt in das LAN eingespeist. Folglich müssen alle Prüfungen, die sonst auf der Firewall durchgeführt werden, auf dem VPN-Gateway vorgenommen und somit an zwei Orten bzw. auf zwei Rechnern (Firewall, VPN-Gateway) Filterregeln eingerichtet und gepflegt werden. Hierbei können den oftmals überlasteten Administratoren gefährliche Fehlkonfigurationen unterlaufen. Natürlich ist diese Gefahr immer gegeben, doch sollte eine Konstellation bevorzugt werden, die möglichst einfach und stringent zu handhaben ist.

Als derzeit ideal hat sich jene Konstellation herauskristallisiert, bei der ein Router mit Paketfilterregeln, die den ein- und ausgehenden Verkehr überwachen, vorgeschaltet ist. Hinter diesem Router, der nur bestimmte IP-Pakete aus dem Internet an das Gateway weiterleitet, findet gleichzeitig das VPN-Gateway Schutz (Abb. 6.10). Außerdem stellen spezielle Filterregeln sicher, dass niemand von außen IP-

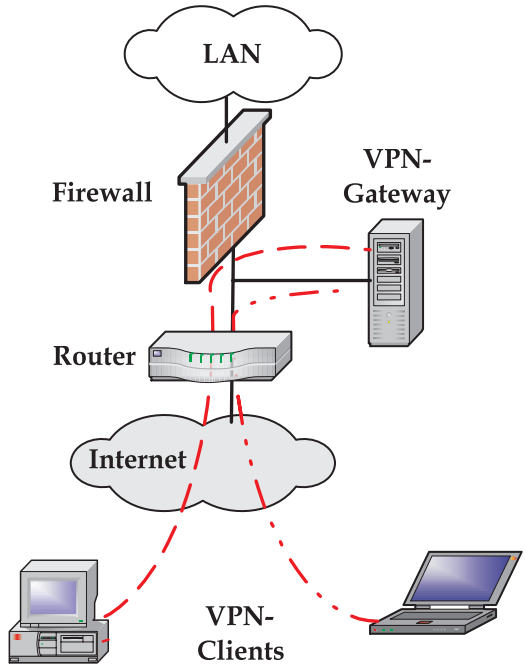


*Abb. 6.10: Das VPN-Gateway befindet sich vor der Firewall in einer DMZ und wird über einen zusätzlichen Router angesprochen*

Pakete einschleusen kann, die nur scheinbar aus den VPN-Netzen kommen. Ein weiterer großer Vorteil dieser Konstellation besteht darin, dass die bereits vom VPN-Gateway entschlüsselten IP-Pakete noch die Firewall passieren müssen, um ins Firmen-LAN zu gelangen. Damit wird sichergestellt, dass die lokalen Sicherheitsregeln nicht unterlaufen werden. Auch kann der Zugriff von außen über das

VPN auf bestimmte Rechner und Ressourcen beschränkt und E-Mails auf Viren untersucht werden.

### 6.2.3 VPN und Router

Router können – genauso wie Firewall-Systeme – zum Aufbau eines VPN eingesetzt werden, wenn sie ein entsprechend ausgelegtes Betriebssystem haben. Im Gegensatz zu Site-to-Site-VPN, die Daten auf physikalischer Ebene zwischen zwei Geräten Punkt-zu-Punkt verschlüsseln, ist der Einsatz von IPSec-VPN problematischer.

Zurückzuführen ist das auf die mangelnde Spezifikation des IPSec-Protokolls im Bereich der Remote-Nutzer-Authentifizierung und der Client-Konfiguration. Remote-Nutzer-Authentifizierung und Datenkompression werden derzeit von vielen Herstellern noch proprietär gehandhabt. Damit sind diese wichtigen Funktionen in einem heterogenen Umfeld oftmals nicht nutzbar, weil nicht jedes Gerät diese Eigenschaften auf gleiche Weise umgesetzt hat. Wichtige Funktionen wie automatische Konfiguration sind in einem heterogenen Netz nicht möglich. Der Administrator kann zwar in einigen Fällen detaillierte Rechteprofile bis zum Endanwender weiterleiten, doch gilt dies meist nur, wenn durchweg Komponenten nur eines Herstellers verwendet werden. Folglich muss manuell konfiguriert werden, was sich auf die Skalierbarkeit nachteilig auswirkt. Dies ist bei der Betreuung einer großen Anzahl von Geräten nicht mehr machbar.

### 6.2.4 Quality of Service in VPN

Die Frage nach einer garantierten Dienstgüte, z.B. der Quality of Service (QoS), ist für ein Overlay-Netz, welches mit Tunneltechniken oder allein mit IPSec verkapselten IP-Paketen aufgebaut wird, zunächst negativ zu beantworten, sofern das darunter liegende Netz (z.B. Internet) nach dem Best-Effort-Prinzip arbeitet.

### 6.2.5 Diffserv in VPN

Allerdings ist es, wie in Abschn. 2.3.4 über DiffServ diskutiert, dennoch möglich, ein IPSec-basiertes End-to-End-VPN mit Dienstgüten zu realisieren. Das erweiterte TOS-Feld im IPv4-Protokollkopf und das *Traffic-Class-Octet* im IPv6-Protokollkopf, das gemäß Diffserv als *DS-Field* bezeichnet wird und ein Per-Hop-Behavior (PHB) ermöglicht, lässt in den dafür ausgelegten Netzknoten eine Steuerung nach Dienstgüten und zuvor festgelegten Service Level Agreements (SLA) zu.

Der Einsatz von DiffServ in IPSec-VPN ist im Wesentlichen darauf zurückzuführen, dass IPSec das DS-Feld im Protokollkopf nicht nutzt und auch nicht in kryptographische Berechnungen, z.B. bei einer Hash-Wert-Bildung zur Integritätssicherung, einschließt. Somit hat eine Modifikationen des DS-Felds

zugunsten einer Steuerung nach Dienstgüten auf einen Netzknoten, der Teil eines IPSec-Tunnels ist, keine Auswirkungen. Im Tunnel-Mode des IPSec-Frameworks wird zusätzlich am Tunnelanfang ein IP-Header *(Outer-Header)* gebildet, der den eigentlichen IP-Header des Senders (Host) einkapselt *(Inner-Header)*. Nähere Ausführungen finden sich in Abschn. 7.4 über IPSec. Die Arbeitsweise des DS-Felds in einem IPSec-Tunnel verläuft nach folgendem Schema:

1. Der Netzknoten zu Beginn eines IPSec-Tunnels verpackt gemäß IPSec das IP-Paket des Senders und setzt das DS-Feld im Outer-Header gemäß den vorab eingestellten SLA-Werten der lokalen DS-Domain.
2. Das gesicherte (gekapselte) IP-Paket durchläuft nun das DS-fähige Netzwerk. Passierte Zwischenknoten modifizieren das DS-Feld.
3. Am Tunnelende angelangt, werden die Tunnelpakete im letzten Netzknoten entfernt und somit die originalen (ursprünglichen) Informationen im IP-Header des Senders zur Weiterleitung wiederhergestellt.
4. Falls die letzte DS-Domain des originalen IP-Datagramms sich von der DS-Domain des IPSec-Tunnelanfangs unterscheidet, wird am Tunnelende im letzten Netzknoten das DS-Feld des originalen IP-Paketes den herrschenden SLA-Bedingungen angepasst. Damit übt der letzte Netzknoten die Eigenschaft eines *DS-Ingress-Node* aus.
5. Nach Verlassen des IPSec-Tunnels – falls das IP-Paket weiterhin in einem DS-fähigen Netzwerk zur Zieladresse weitergeleitet werden muss – modifizieren die Zwischenknoten das originale IP-Paket.

### 6.2.6 Beispiel einer komplexen VPN-Architektur

In diesem Abschnitt wird eine VPN-Architektur diskutiert, die *on the wild* existiert, d.h. diese Architektur wird in einer realen Umgebung operativ eingesetzt, gewartet, gepflegt und weiterentwickelt. Die Verwaltung und Betreuung der VPN-Plattform wird von einem Drittanbieter (IT-Dienstleister) durchgeführt. Die VPN-Plattform wird als Remote-Access-Plattform von vier Finanzdienstleistern zur Einwahl (Fernzugriff) in das jeweilige Unternehmensnetz genutzt. Beabsichtigt ist, mit dem VPN eine Ende-zu-Ende Sicherheit (Vertraulichkeit) zu ermöglichen sprich eine verschlüsselte Verbindung zwischen dem VPN-Client eines Nutzers und dem VPN-Gateway zu etablieren. Ebenso soll eine starke Authentifizierung mittels Zertifikaten vorgenommen werden. Das VPN bietet Fernnutzern die Freiheit, sich von jedem Festnetz- bzw. Internetanschluss in das jeweilige Firmennetz einzuwählen.

Die Abb. 6.11 skizziert die Remote-Access-VPN-Plattform aus Sicht der Kommunikationsobjekte. Eine funktionale Betrachtung der Einwahl eines Fernnutzers geschieht wie folgt:

- Ein Fernnutzer wählt sich mit seiner eigens installierten Software (NCP-Client) z.B. über eine Wählverbindung auf den Access-Router der VPN bzw. RAS-Plattform ein (vgl. linke obere Bildhälfte). Es handelt sich bei dem VPN um eine L2Sec-Implementierung der Fa. NCP aus Nürnberg (vgl. Abschn. 7.2.4 und Abb. 7.11).
- Das VPN-Gateway ist in der Beispielarchitektur hinter der Firewall platziert, so dass die verschlüsselten Pakete von der Firewall durchgelassen werden. Damit kann die Firewall lediglich Ports und IP-Adressen filtern und nicht Paketinhalte.
- Am VPN-Gateway wird der VPN-Tunnel terminiert und die Pakete entschlüsselt. Da die Höhe der Last zeitlichen Schwankungen, z.B. je nach Tageszeit und Wochentag, unterworfen ist, ist es erforderlich mehrere VPN-Gateways parallel zu betreiben. Damit wird die Last der einzelnen Gateways aufeinander abgestimmt. In der Abb. 6.11 ist dies durch die hintereinander geschachtelte schematische Darstellung der VPN-Gateways angedeutet. Sind die Pakete des Fernnutzers entschlüsselt, werden diese in die eigentliche DMZ an den RADIUS-Server weitergeleitet.
- Der RADIUS-Server führt im Wesentlichen ein Accounting durch, um auf der mandantenfähigen Plattform, für den Betreiber der Plattform eine verursachergerechte Abrechnung zu erstellen. Nach Erfassung der relevanten Abrechnungsparameter, wird das eingangene Paket weitergeleitet.
- Am LADAP-Server (DirX) findet eine Zertifikatsüberprüfung und eine Rollen- und Berechtigungsprüfung statt. Im Rahmen der Zertifikatsprüfung wird u.a. eine mögliche Revokation des Zertifikats abgeprüft.
- Nach Durchlaufen der Prüfungen werden die Pakete in einem GRE-Tunnel zu den Partnernetzen bzw. zu den Routern am Ausgang der Plattform geschickt. Je nach Zugehörigkeit des Fernnutzers wird eine Tunnlerichtung vorgegeben.
- Zwischen den Routern am Ausgang der Plattform und den Firewall-Systemen (unterer Teil der Abb. 6.11) ist keine Absicherung hinsichtlich der Vertraulichkeit vorgesehen. Die Partnernetze gelten a priori als vertrauenswürdig. Damit ist der Fernnutzer schließlich in sein Firmennetz gelangt und kann seine Geschäftsvorfälle bearbeiten.

Aus Sicht des Wartungspersonals sind die hierzu erforderlichen Komponenten in der rechten Hälfte der Abbildung dargestellt. Denn neben der eigentlichen Bereitstellung der Funktionalität, ist es ebenso zwingend die Perimeterkomponenten auf den neuesten sicherheitstechnischen Stand (Patch) zu halten. Jedoch sind auch reguläre Updates der verschiedenen Hersteller zu berücksichtigen.

Dies Beispiel illustriert, wie ein Zusammenspiel derjenigen Komponenten, die in den vorangegangenen Kapiteln diskutiert wurden, in einer mandantenfähigen Plattform zum Einsatz kommen. Oftmals ist es einfacher, nur einzelne Komponenten isoliert zu betrachten. Doch erst das Zusammenspiel und die Beherrschung

des Zusammenspiels der Komponenten einer komplexen Infrastruktur ist eine nicht zu unterschätzende Aufgabe für den Betrieb einer solchen Plattform.

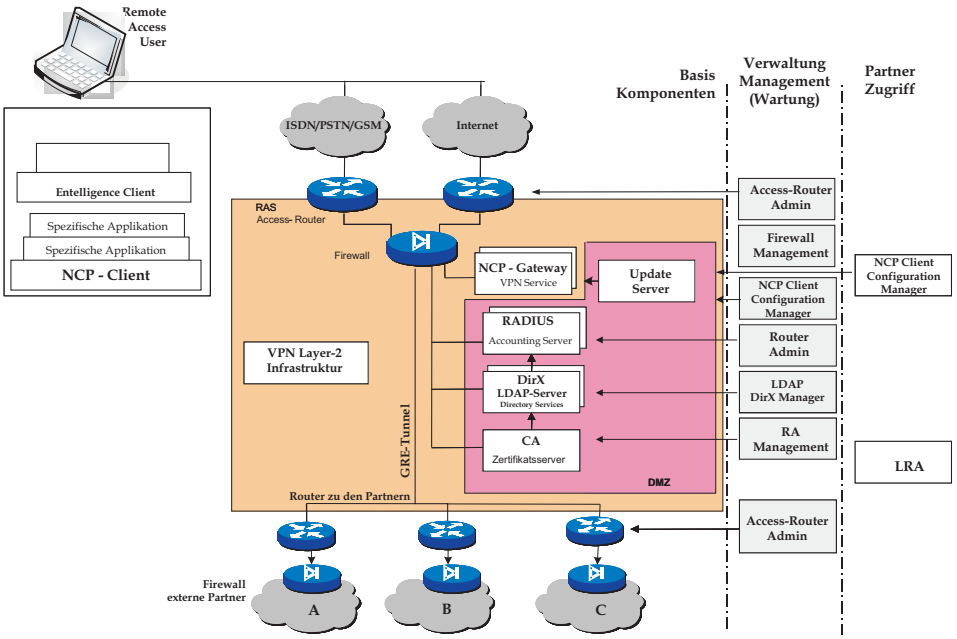


*Abb. 6.11: Mandantenfähige Remote-Access-VPN-Plattform für die Einwahl von ungefähr 6000 Nutzern*

Natürlich stellt die Architektur einige Herausforderungen an den Architekten der Plattform. So muss die Plattform mit zunehmender Anzahl der Nutzer mitwachsen (vgl. Abschn. 9.2). Neben den rein technischen Aspekten sind z.B. nachprüfbare Leistungsparameter, derer die Zuverlässigkeit anhand und Verfügbarkeit der VPN-Plattform gemessen werden kann, für die einzelnen Mandanten wichtig. Der Abschnitt 9.2.3 beschäftigt sich ausgiebig mit diesem Thema.

### 6.2.7 Ausblick

Bezogen auf das OSI-Referenzmodell lassen sich gemäß Abb. 6.2 drei unterschiedliche VPN-Layertypen definieren. Es sind die VPN der Anwendungsebene (Application Layer), der Transport- und Netzwerkebene (Network Layer) sowie der Netzwerkverbindungsebene (Link / Physical Layer).

Neben den oben aufgezeigten Varianten der VPN-Layertypen, gibt es zwei grundsätzliche Ansätze (Secure, Trusted) ein VPN zu implementieren, sowie ergänzend eine Mischform (Hybridform). Im ersten Ansatz (Eigenrealisierung) wird das (Secure, Trusted) VPN vom Unternehmen in Eigenregie betrieben. Im zweiten An-

satz, in der reinen Provider-Lösung oder Hybridform, wird ein VPN durch einen Netzanbieter vollständig bzw. teilweise implementiert.

Tab. 6.2 zeigt, welche VPN-Services zu welcher Architektur und Technologie zuzuordnen sind. Weiterhin wurde eine Abgrenzung der Architektur und Technologie eines Remote-Access-VPN gegenüber einem Intra- und Extranet-VPN vorgenommen. Der Architektur- bzw. Technologie-Einsatz kann in Bezug auf Fremdleistung, Hybrid-Form und Eigenrealisierung betrachtet werden.

Die in Tab. 6.2 aufgezeigten Tunneltechnologien stehen im Kap. 7 im Vordergrund. Die WAN-Technologien (Frame Relay, ATM, MPLS) werden im Kap. 8 behandelt.

*Tabelle 6.2: VPN-Services, Architekturen und Technologien auf Netzwerk- und Protokollebene*

| **Service** | **Architektur** | **Technologien** |
|---|---|---|
| Access-VPN | Vom Endgerät aufgebaut und vom Netzzugang (NAS) initiiert | L2F / L2TP, IPSec,<br>PSTN, xDSL,<br>Mobile-IP, Kabel |
| Intranet und<br>Extranet-VPN | IP-Tunnel<br>Virtual Circuit<br>MPLS | GRE, IPSec<br>Frame Relay, ATM<br>IP oder IP-over-ATM |

Beide Ansätze bzw. Anwendungsszenarien haben ihre Besonderheiten, Vorzüge und Nachteile im Betrieb. Diese und die Entscheidung, welche Lösung (Site-to-Site, End-to-Site, End-to-End) mit einem Netzwerkanbieter bzw. in Eigenregie verwirklicht werden sollte und welche Kriterien dabei zu beachten sind, werden im Kap. 9 behandelt.

## 6.3 Übungen

1. Auf welche drei grundsätzlichen Strukturen lassen sich die unterschiedlichen VPN-Architekturen zurückführen. Wie lautet die Begründung für diese drei Strukturen?
2. Welche drei Architekturen gibt es, um ein VPN-Gateway in Bezug zu einer Firewall zu platzieren?
3. Welche Vor- bzw. Nachteile haben die drei Architekturen hinsichtlich einer zentralen Administration der Perimeterkomponenten?
4. Wie könnten in den jeweils drei Architekturen des Abschn. 6.2.2 starke Authentifizierungen vorgenommen werden *(a)* und welche Protokolle müssten dazu eingesetzt werden *(b)*?
5. Welche Vorteile bietet eine demilitarisierte Zone (DMZ) gegenüber anderen Perimeterarchitekturen, die ein VPN-Gateway beinhalten?

6. Welche Anforderungen (QoS) müssten an ein VPN gestellt werden, wenn es Sprache in verschlüsselter Form übertragen soll *(a)* und wie könnte dies realisiert werden *(b)*?

7. Wie wird in der Beispielarchitektur (Abb. 6.11) die Authentifizierung bei der VPN-Einwahl eines Nutzers durchgeführt?

8. Wozu dient der GRE-Tunnel in der Beispielarchitektur (Abb. 6.11)?

9. Welchen Sinn haben die Firewall-Systeme (Abb. 6.11) im Bereich der Partner-Anbindung?

10. Was könnte die Erklärung sein, warum in der Beispielarchitektur (Abb. 6.11) sowohl RADIUS als auch Software-Zertifikate (X.509 v3) eingesetzt werden?

11. Ist es für einen mobilen Nutzer der Plattform auch möglich, sich über ein Roaming-unterstützendes Verfahren einzuwählen *(a)*? Falls nein, warum nicht *(b)* und wie müsste die Beispielarchitektur nachgebessert werden *(c)*?

12. Was könnte ein technischer Grund dafür sein, das bei dieser VPN-Plattform IPSec nicht eingesetzt wurde bzw. werden konnte?

13. Wie und welche Messgrößen müssten definiert werden, um die Leistungsfähigkeit der Plattform zu dokumentieren?