Dr. Suppan International Institute

Der Netzwerk Insider

April 2001

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

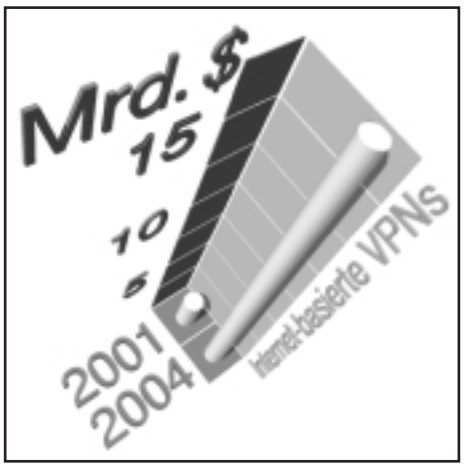
Schwerpunktthema

Virtual Private LANs: Kombination von Kostenoptimierung und Sicherheit

Dipl.-Inform. Petra Borowka

Nachdem Infonetics Research ein VPN Software Wachstum von 121 Prozent mit einem Gesamtvolumen von 269 Millionen US-Dollar berichtet und mehr als eine Millionen verkaufter VPN Router angibt, nachdem eine IDC-Studie ein Wachstum des VPN-Marktvolumens bei Internet-basierten VPN-Lösungen von heute 2 Milliarden US-Dollar auf 17,6 Milliarden US-Dollar im Jahr 2004 in Aussicht stellt – streichen wir von dieser Zahl wegen Optimismus 20 Prozent, bleiben immer noch 14 Milliarden übrig – und das weit mehr ist als der jährliche Routermarkt, stellt sich die Frage:

Wofür sind Anwender diese 14 Milliarden bereit auszugeben?



Optimistische Wachstumsprognose für Internet-basierte VPN-Lösungen

Zunehmender Kostendruck im Verbund mit steigenden Anforderungen an Sicherheit und Dienstgüte für Standort-Verbundnetzwerke bestimmen den Markt für Virtual Private Networks.

Was bedeutet der Einsatz von VPN-Technik für ein Unternehmen und: wie lässt sich mit VPNs DIE günstigste Kombination von Kosteneinsparung und Sicherheit erreichen?

Der nachfolgende Beitrag beleuchtet Konzepte, Techniken, Einsatzszenarios, Implementierungs-Aspekte und Kostenpotential beim Einsatz von VPNs.

weiter Seite 7

Zum Geleit

Bedarf an Netzwerk-Spezialisten wächst weiter

Nach den zur CeBIT vorgelegten Ergebnissen einer Untersuchung des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. Bitkom sind zur Zeit 400.000 offene IT-Stellen nicht zu besetzen. Im Jahr 2003 werden es voraussichtlich 723.000 sein. Von einer Entwarnung oder Verbesserung der Situation kann zur Zeit noch keine Rede sein. Wir können diese Erfahrungen für den Netzwerk-Bereich nur bestätigen. Tatsächlich wird es hier in einigen Regionen immer schwieriger, geeignetes Personal zu finden. Dies betrifft nicht nur die Top-Experten sondern auch und vor allem das Netzwerk-Betriebspersonal.

Beklagt Bitkom noch das damit entgangene Wirtschaftswachstum von 2,3 bis 3 Prozent, so ist der Mangel an Netzwerk-Betriebspersonal für die Unternehmen mehr als kritisch zu sehen.

Weit über alle Prognosen hinaus haben sich Netzwerk-Technologien in den letzten 12 Monaten entwickelt. Damit meine ich nicht den Umsatz sondern die konsequente Einführung der neuen Netzwerk-Technologien: Gigabit, VPN, Wireless, Voice over IP, dsl und wie die neuen Technologien alle heißen, bieten dem Anwender ein riesiges Optimierungs-Potenzial. Dementsprechend intensiv werden sie genutzt.

Gleichzeitig werden Netzwerke noch stärker als bisher zum Kern aller zukünftigen DV-Lösungen.

Technologien wie Network Attached Storage oder Storage Area Networks sind Beispiele für äußerst dynamische und kritische Entwicklungen, in deren Mittelpunkt das Netzwerk steht.

Mehr denn je gilt und wird in den nächsten Jahren gelten:

Steht das Netzwerk – so steht das Unternehmen.

weiter Seite 2

Bedarf an Netzwerk-Spezialisten wächst weiter

Fortsetzung von Seite 1

Das Netzwerk ist zur kritischsten Unternehmenstechnologie geworden.

Dem steht die immer schon gegebene Komplexität von Netzwerken gegenüber. Diese nimmt mit den neuen Netzwerk-Technologien weiter zu. Hinzu kommt, dass ab einem Verfügbarkeitsbedarf von 99 % für das Netzwerk der Mensch in seiner Handlungsfähigkeit zu langsam ist. Automatische Fehlerbearbeitungs- und Redundanzverfahren werden dementsprechend in den nächsten Jahren weiter massiv an Bedeutung gewinnen.

Die sich verschlechternde wirtschaftliche Situation der großen Anbieter ist dabei ein ernst zu nehmender Risikofaktor. Auch wenn bei den meisten Anbietern das Problem in geringen Wachstumsraten und nicht in sinkenden Umsätzen liegt, so ist doch Personalabbau die im Moment wohl vorherrschende Reaktion.

Zum einen wird dies am Fachkräftemangel in Deutschland nichts ändern, zum anderen ist zu befürchten, dass die Service-Qualität stark nachlassen wird und dementsprechend bei den Kunden weitere Lasten entstehen. Bei einzelnen Anbietern ist dies bereits stark zu bemerken.

In dieser Situation ist die Verfügbarkeit ausreichend geschulter Netzwerk-Spezialisten der Faktor, der über Risiko oder Erfolg des Netzwerk-Betriebs in den Unternehmen entscheidet. Umgekehrt entstehen für die Mitarbeiter erhebliche Chancen der beruflichen Entwicklung. Nur wenige Branchen haben derzeit ähnliches zu bieten.

Erfreulicherweise hat sich der ComConsult Certified Network Engineer in der Branche als die ideale Ausbildung und Qualifizierung durchgesetzt. Zum einen wird das notwendige Wissen für Planung und Betrieb von Netzwerken systematisch und erfolgreich vermittelt, zum anderen setzt die Prüfung mit ihrem formellen Nachweis einer vorhandenen Qualifikation Maßstäbe.

Über 1000 Personen haben im Jahr 2000 an den CCNE-Kursen teilgenommen. Und die Zahl steigt weiter.

Dabei sind die Teilnehmer hoch zufrieden und geben ihrer Ausbildung die besten Noten:

"Die Seminare haben mir sehr gut gefallen. Ich habe viele hilfreiche Informationen, viele fachliche Informationen und vor allem auch Informationen, die zukunftsausgerichtet sind." (Jürgen Herder)

"Ich habe vom Marktvergleich her festgestellt, dass diese Ausbildung im Preis-Leistungsverhältnis das Beste ist was geboten wird." (Joachim Treiber)

"Die Ausbildung wird in jedem Fall aktuellen Trends der Netzwerk-Technologie gerecht." (Michael Ederer)

"Alle Seminare bauen aufeinander auf und ergänzen sich sehr gut." (Björn Stauber)

"Gut hat mir gefallen, dass der Stoff schnell durchgezogen wurde. Mir wurde sehr viel Wissen vermittelt, das für meine Arbeit enorm wichtig ist."
(Christian Braunschuh)

"Ich glaube, das kann ich in der Praxis und im täglichen Gebrauch gut anwenden." (Herbert Segmüller)

Natürlich ruhen wir uns auf dem Erreichten nicht aus. In den letzten Wochen haben wir massiv investiert, um das zu vermittelnde Wissen noch wirksamer darstellen zu können. So wurde das einzusetzende Equipment deutlich ausgebaut (neues Kabelmessgerät, neue Layer-3-Switch-Systeme, neues Reporting und Analyse-System). Parallel wird der gesamte Lehrstoff permanent überarbeitet und dem aktuellen Stand der Technik angepasst.

Auch nach Abschluss der Prüfung lassen wir Sie nicht alleine. So wurde die Sommer- und Winterschule aufgebaut, die sich primär an den erfahrenen Netzwerker /in wendet. Innerhalb einer 5-tägigen Intensiv-Schulung stellen wir die neuesten Technologien und Produkte und die heißesten Trends vor.

Wir werden mit unseren Möglichkeiten nicht das generelle Fachkräfte-Problem der Branche lösen können. Aber wir können hoffentlich dazu beitragen, die Vorteile einer systematischen Ausbildung klar heraus zu stellen.

Für die betroffenen Mitarbeiter und Mitarbeiterinnen kann nur gelten: nutzen Sie die Möglichkeiten, die Ihnen unsere Branche bietet. Selten waren die Perspektiven für den beruflichen Erfolg so gut wie jetzt.

Ihr Dr. Jürgen Suppan

Impressum

Verlag:
Dr. Suppan
International Institute b.v.
Ahornenlaan 12
4493 DG Kamperland
Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

Herausgeber
und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan

Gestaltung:
Zweipfennig

Erscheinungsweise:
Monatlich,
12 Ausgaben im Jahr

Bezug:
Kostenlos
als PDF-Datei
über den eMail-
VIP-Service
der ComConsult Akademie

Für unverlangt
eingesandte Manuskripte
wird keine Haftung übernommen

Sicherheit

Protokolle, die nie unter Sicherheitsaspekten entwickelt wurden, bilden eine ständige Gefahr

von Dipl.-Inform. Detlef Weidenhammer

Die weltweite Internetstruktur baut auf einer erschreckend schwachen Grundlage auf: Kaum ein Tag vergeht, ohne dass neue Nachrichten über gravierende Sicherheitsprobleme oder erfolgreich verübte Angriffe auf Unternehmensnetze bekannt werden. Protokolle, die nie unter Sicherheitsaspekten entwickelt wurden, bilden eine ständige Gefahr für jeden Beteiligten. Aber auch neueste Entwicklungen, die zur Grundlage des weltweiten E-Commerce gehören unterminieren durch unsaubere Programmierung und zögerliche Umsetzung von Sicherheits-Standards zu Recht das Vertrauen der Benutzer in heutige Lösungen.

Dipl.-Inform. Detlef Weidenhammer ist als Geschäftsführer der GAI NetConsult GmbH vorwiegend auf den Gebieten Internet/Intranet-Anwendungen und Netzwerk-Sicherheit tätig. Basierend auf langjähriger praktischer Tätigkeit bringt er seine Erfahrungen als Fachberater und auch als Referent bei Seminaren und Kongressen ein, er ist auch der Moderator des Netzwerk Sicherheits-Forums 2001.

Nachstehend wird eine kurze, nicht repräsentative Auswahl einiger aktueller "Vorfälle" wiedergegeben, die ein bezeichnendes Licht auf die derzeitige Situation im Sicherheitsbereich werfen.

Vorhersagbare TCP-Sequenznummern

Beim TCP-Verbindungsaufbau (3-way handshake) wählt der Sender zur Numerierung des Startpaketes eine ISN (Initial Sequence Number). Die ISN muss möglichst zufällig gewählt werden, damit ein Angreifer keine Möglichkeit hat, sie zu erraten und dieses Wissen für Angriffe auszunutzen. Hinweise hierzu gibt der RFC 1948 (Defending Against Sequence Number Attacks), der aber offensichtlich nicht von allen Herstellern beachtet wird, worauf eine Veröffentlichung der Firma Guardent hinweist.

Mit dem Wissen um die Generierung der ISN kann ein Angreifer fremde Verbindungen sehr einfach abbrechen (DoS-Attacke) oder seine eigenen Pakete in den Datenstrom einschleusen (session hijacking).

Letzteres würde selbst eine zuvor erfolgte starke Authentisierung nutzlos machen.

Betroffen ist u.a. Solaris 2.6/SPARC.

Neue Probleme mit dem SNMP Community-String

SNMP (Simple Network Management Protocol) ist die Grundlage praktisch jeder Netzmanagement-Lösung und besitzt in der heute zumeist verwendeten Version 1 große Sicherheitsschwächen bereits im Grunddesign. Dass aber auch immer mit fehlerhaften Implementierungen zu rechnen ist, zeigt der folgende Hinweis:

In verschiedenen Cisco-IOS Releases existieren mehrere unabhängige Fehler, die dazu führen, dass unerwartet SNMP Community-Strings erzeugt werden und damit unautorisierte Zugriffe auf Netzkomponenten möglich sind.

1. Bei Zugriff mit einem Server-Request, der durch einen Community-String autorisiert ist, wird zusätzlich ein read-only Community-String erzeugt und ermöglicht damit eine weitere Zugriffsmöglichkeit. Selbst nach dem Löschen dieses Strings wird er bei Reboot der Komponente neu geladen.

2. Wird eine view-based Access Control MIB (VACM) mittels read-only Community-String ausgelesen, dann wird zusätzlich ein Community-String zurückgeliefert, der auch Schreibzugriff ermöglicht.

3. Bei der Implementierung neuer Standards zur Administration von Kabelmodems wurde ein undokumentierter Community-String eingeführt, der zu unautorisiertem Schreibzugriff führt.

Das Ausnutzen dieser Schwachstellen ist besonders im internen Netz zu beachten, da SNMP-Zugriffe von externer Seite generell geblockt werden sollten.

Die nächsten beiden Vorfälle sind brandaktuell und zeigen in erschreckender Weise auf, wie unsicher auch neueste Entwicklungen sein können.

VeriSign stellt nicht authentische Zertifikate der "Microsoft Corporation" aus

Ende Januar 2001 stellte VeriSign zwei Zertifikate auf die Microsoft Corp. für eine Person aus, die vorgab ein Microsoft-Mitarbeiter zu sein. VeriSign versäumte äußerst fahrlässig die korrekte Identifizierung dieser Person, von der erst jetzt festgestellt wurde, dass sie gar nicht für Microsoft arbeitet. Ihre wahre Identität konnte bisher nicht ermittelt werden.

Jedes ausführbare Programm oder Office Macro, das mit einem dieser Zertifikate signiert ist, scheint damit von Microsoft

authentisiert zu sein. Benutzer, die diesem Zertifikat trauen, könnten damit in gutem Glauben manipulierte Programme ausführen, die äußerst schädliche Nebenwirkungen enthalten.

Betroffen sind Benutzer des Internet Explorers, die das Ausführen von ActiveX aktiviert haben. Benutzer des Netscape Communicators sind nicht betroffen. Erschwerend kommt hinzu, dass selbst das Setzen dieser Zertifikate auf die für solche Fälle vorgesehene Revocation List erfolglos bleibt, da der Internet Explorer derzeit den Widerruf von Zertifikaten nicht automatisch prüft.

Dieser Vorfall hat große Bedeutung über das konkrete Schadenspotential hinaus, da er sowohl Betreibern von Certificate Authorities als auch Software-Herstellern ein äußerst schlechtes Zeugnis über die Güte ihrer Lösungen ausstellt. Wie vertrauenswürdig sind eigentlich VeriSign-Zertifikate noch; zur Erinnerung: ein Großteil aller Webserver verwendet diese zur Authentisierung bei SSL-Kommunikation.

Eine sichere Basis für globalen E-Commerce muss wohl deutlich anders aussehen.

Angriffsmöglichkeiten auf den geheimen Schlüssel bei PGP

Tschechische Kryptologen haben kürzlich Schwachstellen in der Schlüsselhandhabung des weltweit genutzten OpenPGP entdeckt, die es einem Angreifer ermöglichen den verwendeten geheimen Schlüssel zu ermitteln. OpenPGP wird in vielen Implementierungen genutzt, von denen wohl die bekanntesten PGP (NAI) und GNU Privacy Guard sein dürften. Die Sicherung des geheimen Schlüssels ist stets die sensibelste Stelle bei allen kryptographischen Verfahren, weshalb dieser Aufdeckung eine große Bedeutung zukommt.

Grund für die gefundene Schwachstelle ist eine unsaubere Implementierung kryptographischer Techniken zum Schutz des Private Keys, die dazu führt, dass durch eine gezielte Veränderung des Key Files die Signaturerstellung unbemerkt manipuliert werden kann. Aus der aufgefangenen fehlerhaften Signatur kann dann in Sekundenschnelle der geheime Schlüssel rekonstruiert werden und somit jede Nachricht im Namen des Benutzers signiert werden.

Die Attacke wurde erfolgreich mit PGP V 7.0.3 vorgeführt, wobei hier DSA-Algorithmen angreifbar sind, nicht jedoch RSA-Algorithmen, die durch eine zusätzliche eigene Prüfung gegen Manipulationen geschützt sind. Wesentliche Hürde für jeden Angreifer ist aber der notwendige Schreibzugriff auf das Keyfile, ein weiterer Grund für die immer wieder geforderte sichere externe Ablage auf zuverlässigen Medien.

Besuchen Sie das Netzwerk Sicherheits-Forum 2001. Zu diesen und vielen anderen Themen werden Ihnen aktuellste Informationen und Sicherheitsempfehlungen gegeben. In mehreren parallel angebotenen Workshops werden darüber hinaus Betriebsthemen vertieft, aber auch Produktvergleiche nach festgelegtem Präsentationsmuster zusammen mit unterschiedlichen Herstellern durchgeführt.

Dieses Security-Event bietet Ihnen wie in jedem Jahr eine vollendete Mischung aus Erfahrungsberichten, Fachvorträgen und Produktempfehlungen.

Interessenten sollten sich jetzt durch eine rasche Anmeldung noch einen der letzten Plätze auf diesem Kongress sichern.

Neues Seminar

DNS-/IP-Design für Windows 2000 Active Directory

Vom 28. bis 30. Mai 2001 veranstaltet die ComConsult Akademie im Holiday Inn Bonn zum ersten Mal ihr neues Seminar "DNS-Design für Windows 2000 Active Directory" für Planer, Betreiber und Anwender von Unternehmensnetzen.

Viele Unternehmen streben die Einführung von Windows 2000 an. Oft ist es jedoch der Fall, dass DNS-Strukturen innerhalb dieser Unternehmungen historisch, den Bedürfnissen angeglichen, gewachsen sind und somit nicht den Erfordernissen einer Directory-Struktur entsprechen.

Das Seminar "DNS-/IP-Design für Windows 2000 Active Directory behandelt in konzentrierter Form die Implementierungsgrundlagen aus dem IP-Bereich für Windows 2000 bzw. für das Active Directory. Dabei spielt DNS die Hauptrolle, wobei auch insbesondere die dynamische Verbindung zum DHCP betrachtet wird.

Die Teilnehmer lernen in diesem Seminar die Grundlagen zu DNS als Auffrischung in komprimierter Form; welche aktuellen DNS-Serverimplementierungen auf dem Markt sind, insbesondere aus dem Hause Microsoft, aber auch die anderer Hersteller; welche DNS-Funktionen vom AD benötigt werden und wie Sie ein AD-DNS-Projekt strukturieren und durchführen.

Die Referenten der ComConsult Beratung und Planung verfügen über entsprechende praktische Erfahrung aus einer Vielzahl von Projekten und kennen auch gerade bei diesem Thema den Konflikt zwischen Netz- und Serveradministration.

Die Referenten diese Seminars haben einen betont praxisorientierten Background und können aufgrund ihrer Projekterfahrung wertvolle Tipps und Erfahrungswerte vermitteln.

Markus Holländer (oben) ist Kompetenz Center Leiter Backoffice bei der ComConsult Beratung und Planung GmbH und besitzt langjährige Projekterfahrung im Design und im Betrieb von Windows NT und Windows 2000, sowie weiterer Backoffice Produkte. In den letzten Jahren hat Herr Holländer zahlreiche Projekte privater und öffentlicher Auftraggeber in diesem Umfeld erfolgreich geleitet.

Dipl.-Ing. Lars Kuhl (unten) ist bei der ComConsult Beratung und Planung GmbH im Backoffice Kompetenz Center

als Berater für die Konzipierung und Umsetzung von Migrationsprojekten auf Windows NT 4 und Windows 2000 beschäftigt. Seine Kenntnisse hat er in der Projektarbeit und der Migration von Netzwerken bei Kunden erworben.

"plan – build – run" Windows 2000 Active Directory Seminarreihe

Der Windows 2000 Server beinhaltet eine Reihe von sehr leistungsstarken Möglichkeiten, den Betrieb von Servern und TCP/IP-Netzen zu vereinfachen und zu signifikanten Kosteneinsparungen zu kommen. Eine Reihe von sehr erfolgreichen Projekten hat bestätigt, dass hier ein erhebliches Potenzial gegenüber den bisherigen Lösungen besteht.

Das eigentlich neue und somit auch der Grund für die vielen Vorteile, die Windows 2000 betriebstechnisch bietet, ist die Kombination einer Reihe von Verwaltungsdiensten mit einem zentralen Directory Service mit einer gleichzeitigen Integration in eine TCP/IP-Kommunikationswelt. Um die gegebenen Vorteile nutzen zu können, sind detallierte Kenntnisse einerseits der Technik des Windows 2000 Directory Services und andererseits seiner methodischen Nutzung erforderlich. Zur Vermittlung dieser Kenntnisse haben wir eine komplette Seminarreihe konzipiert, die mit aufeinander aufbauenden Seminaren aus der Planung und Konzeptionierung bis zum Betrieb von Windows 2000 Active Directory führen.

Im einzelnen besteht die Windows 2000 Active Directory Seminarreihe aus den Seminaren:

1. DNS-/IP-Design für Windows 2000 Active Directory
2. Design Windows 2000 Active Directory
3. Migration zu Windows 2000 Active Directory
4. Betrieb von Windows 2000 Active Directory

Die Seminare sind grundsätzlich unabhängig voneinander, jedoch ist es von Vorteil, wenn bei der Teilnahme an mehreren Seminaren die Reihenfolge eingehalten wird.

Windows 2000 Active Directory

DNS-/IP-Design für Windows 2000 Active Directory

Inhaltlicher Aufbau

Erster Tag

1. Grundlagen des Domain Name System (DNS)
   - Warum DNS?
   - Domain-Name-Space, Domain-Name, Internet-Domain-Name-Space
   - Zonen
   - DNS-Server-Varianten
   - Delegierungen
   - Clientkommunikation
   - DNS-Datenbank, DNS-Dateien
   - DNS intern und extern
   - Dynamisches DNS
   - Service-Records
   - Verbindungen zu DHCP und WINS
2. DNS-Server Implementierungen
   - Windows NT 4.0 Server
   - Alternative(n) auf dem Markt
   - Windows 2000 Server
   - Neuerungen

Zweiter Tag

- Active Directory Integration
  - Multiple-Master-Replikation
  - Delegierungen
  - Primäre DNS-Server
  - Sicherheit
  - SRV-Einträge
  - Verbindungen zu DHCP und WINS
3. AD-Anforderungen an DNS
   - AD-Domäne gleich DNS-Domäne
   - DNS-Domäne ungleich AD-Domäne
   - SRV-Einträge

Dritter Tag

4. DNS-Vorbereitung auf die Einführung vom AD
   - Ist-Analyse
   - Definition der AD-optimierten Zielvorstellungen
   - Migration
5. Fallbeispiel: DNS-Migration zur Einführung von Windows 2000

Der Veranstalter behält sich Änderungen im Programm vor.

ComConsult Akademie – Telefax: 02408/955-399

Fax-Antwort

Windows 2000 Active Directory

☐ Ich melde mich an zum Seminar
DNS-/IP-Design für Windows 2000 Active Directory
☐ 28. - 30.05.01 ☐ 24. - 26.09.01
zum Preis von EUR 1.590,-- zzgl. MwSt.

☐ Ich buche die Seminarreihe
plan - build - run Windows 2000 Active Directory
zum Paket-Preis von EUR 4.990,--
zzgl. MwSt. (statt regulär EUR 5.760,--)
1. ☐ 28. - 30.05.01 ☐ 24. - 26.09.01
2. ☐ 18. - 20.06.01 ☐ 05. - 07.11.01
3. ☐ 27. - 28.09.01 ☐ 26. - 27.11.01
4. ☐ 01. - 02.10.01 ☐ 06. - 07.12.01

☐ Bitte buchen Sie für mich ein Zimmer im Holiday Inn Bonn

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**

☐ Senden Sie mir bitte unverbindlich detailliertes Informationsmaterial über die vier Seminare der **plan - build - run Windows 2000 Active Directory** -Seminarreihe:
1. DNS-/IP-Design für Windows 2000 Active Directory
2. Design Windows 2000 Active Directory
3. Migration zu Windows 2000 Active Directory
4. Betrieb von Windows 2000 Active Directory zu

Name	Vorname
Firma, Abteilung	Position, Funktion
Abteilung	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

Virtual Private LANs: Kombination von Kostenoptimierung und Sicherheit

Fortsetzung von Seite 1

1.
Wofür braucht man VPNs?

Der Hintersinn beim VPN-Einsatz ist folgender: Wenn sich eine Kommunikations-Verbindung zu günstigeren Konditionen als bei Festverbindungen realisieren lässt, so ist dies erstrebenswert.

Hiefür sind verschiedenste Anwendungen denkbar, z.B. E-Mail, Dateitransfer / Download, Transaktionen, bis hin zu EDI zwischen kommerziellen Unternehmen und Behörden, Call Center, E-Business, B2B, B2C und weiteren modernen Szenarien wie online Banking oder Börsentransaktionen. Dabei taucht folgendes Problem auf: "Normaler" Datenverkehr überträgt sensible Parameter wie Webseite (URL), Benutzername, Account-Nummer, Server-Adresse, persönliche Informationen u.v.a.m. sichtbar über das Netzwerk. Was geradezu eine Einladung für alle Hacker darstellt.

Die obige Anforderung ist daher folgend zu modifizieren: Wenn sich eine Kommunikations-Verbindung zu günstigeren Konditionen als bei Festverbindungen UND ohne Sicherheits- und Integritäts-Einbußen realisieren lässt, so kann das beiden Seiten, nämlich Endanwender und Netzprovider nur nutzen.

Zielsetzung beim VPN-Einsatz ist daher die Kosteneinsparung, die sich im WAN-Bereich durch Nutzung eines Shared Netzwerks, im Regelfall eines paketvermittelten / Cell-Multiplex Netzes erreichen lässt. Da hier jedoch allgemein verbreitetes und berechtigtes Misstrauen herrscht, müssen entsprechende Sicherheitsvorkehrungen in Hardware oder Software als Schutzmaßnahmen implementiert werden. Diese bewirken dazu, dass jede physikalische Verbindung über das shared Netz logisch d.h. virtuell wie eine dedizierte Verbindung eines privaten Netzwerks von den anderen Verbindungen separiert wird. Diese Technik heißt VPN, Virtual Private Network. Sie ist natürlich insbesondere bei Internet-Nutzung erforderlich und daher Voraussetzung für jede Art von E-Commerce.

Vorgänger der heutigen VPN-Dienste waren private Intranets über Frame Relay (FR) und ATM Providernetze, die teilweise mit intern/externer Routerverbindung, teilweise mit VPN-Komponenten an allen Standorten vom Endanwender betrieben wurden (siehe Bild 1 und 2).

Zur Autorin

Dipl.-Inform. Petra Borowka leitet das Planungsbüro UBN; langjährige Projekterfahrung mit herstellerunabhängiger standardbasierter Netzwerk-Planung in Beratungsprojekten für verschiedenste Industrie- und Dienstleistungsunternehmen; Schulungen, Veröffentlichungen

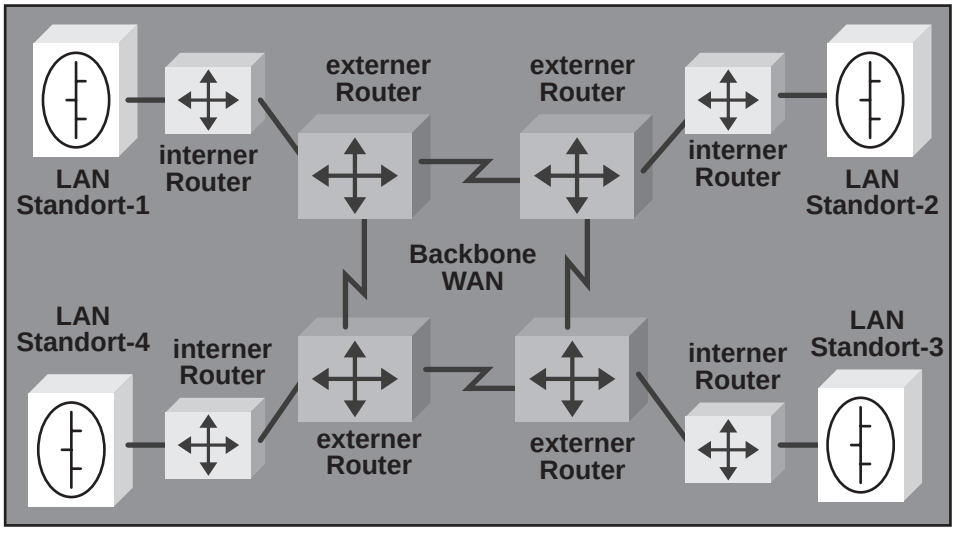
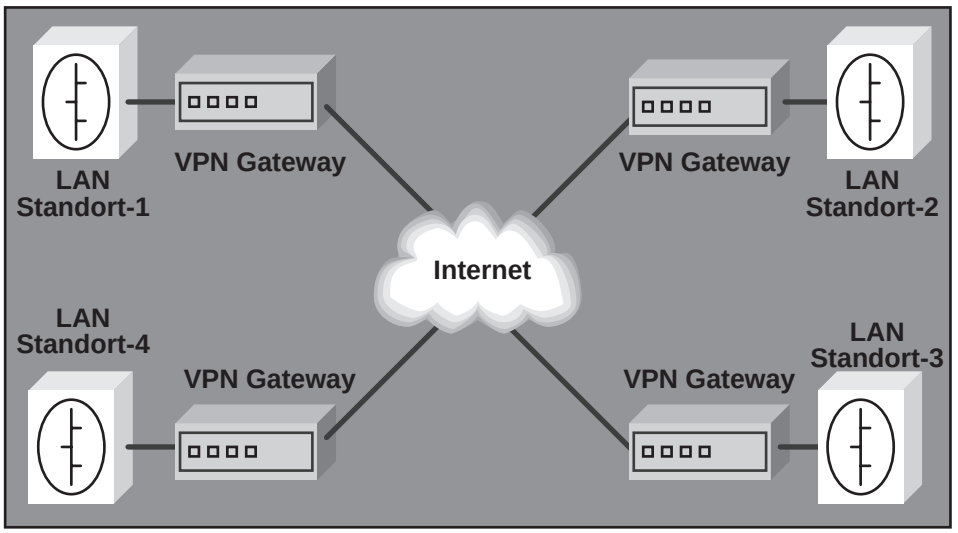


Bild 1 Enterprise Netzwerk
über intern/externe Router und non-Internet Provider

Bild 2 Erste VPN-Konzepte über VPN-Komponente, externe Router und non-Internet Providern



Virtual Private LANs: Kombination von Kostenoptimierung und Sicherheit

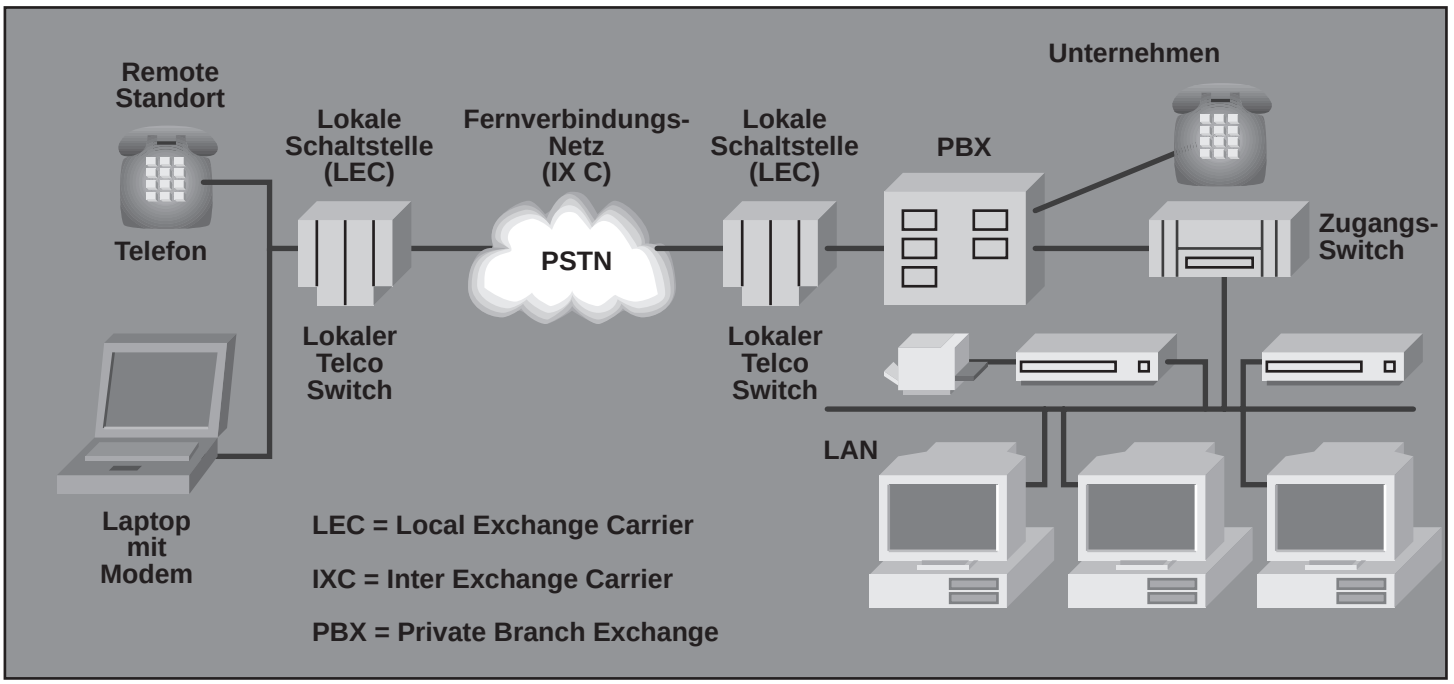


Bild 3 DoV - Datenübertragung über das PSTN-Netz

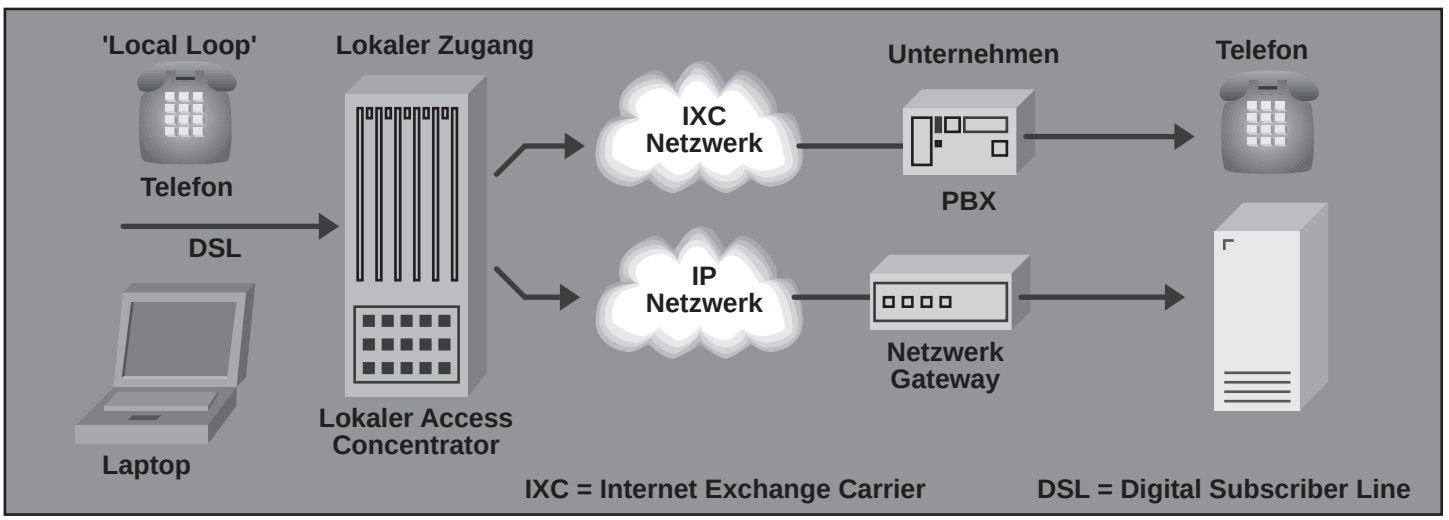
Nachteile dieser Lösungen waren:

- Begrenzung der Kapazität eines Verbindungskanals auf 64 kbit/s
- Einsatz von Modemtechnik mit Begrenzung auf 56 kbit/s am remote Einwahlpunkt
- hohe Customizing, ggf. Entwicklungskosten, da jede Lösung anwenderspezifisch war
- Mangel an qualifiziertem Personal
- vergleichsweise lange Design und Implementierungs-Zyklen, hoher Aufwand für Integration neuer Standorte
- vergleichsweise hohe Einstiegs-Kosten

Ebenso beliebt zur Optimierung von (Fest)-Verbindungskosten sind unter dem Sammelbegriff DoV remote Einwahl-Lösungen per RAS oder NAS über Wählleitungen des PSTN Netzes wie in Bild 3 gezeigt. Es erfolgt eine entfernungs- und zeitabhängige Tarifierung.

Neuere Lösungen nutzen nach dem Motto "Data Dial statt Dial Tone" anstelle von PSTN-Wählleitungen das Internet mit diversen Mediazugängen wie DSL, Kabelmodem, Frame Relay oder ATM, was als DoD (Data over Data) bezeichnet wird (siehe Bild 4). Die Tarifierung ist in erster Linie volumenabhängig (auch AOL hat seine Flatrate wieder abgeschafft...), in zweiter und wichtiger Linie leistungs- und verfügbarkeits-abhängig (SLA-Vereinbarungen erforderlich).

Bild 4 DoD – Internet statt PSTN



Als Vorteile bei DoD werden insbesondere gesehen

- niedrigere Tarifkosten als Festverbindung, Wählverbindung oder Frame Relay
- Tarife haben wegen Volumengebühr statt Zeitgebühr gute Peak-Eignung
- Nutzung der Flexibilität und Skalierbarkeit öffentlicher Netze
- weltweiter, flächendeckender Zugang mit relativ hoher Kapazität möglich, insbesondere höher als 56 kbit/s
- Nutzung der vollen Zugangskapazität durch eine einzelne Session möglich, keine Begrenzung auf 64 kbit/s
- Outsourcing der VPN-Technik inkl. aller lästigen Details an den Provider
- Integration mobiler Benutzer
- nur ein VPN-Zugang am zentralen Standort anstelle eines RAS mit Unterstützung aller genutzten verschiedenen Einwahl-Schnittstellen (Definition von FR CIR's, Modem Banken, ...)
- vergleichsweise niedrige Einstiegs-Kosten
- Fokussierung und Optimierung für IP Betrieb anstelle von Multiprotokoll-Betrieb (IPX, NetBEUI, SNA, AppleTalk, ...)

2. Was ist ein VPN?

Das Schöne an VPN's ist: Es gibt so viele verschiedene Definitionen, dass jeder Hersteller eine gute Chance hat, sein Produkt so zu vermarkten, als ob es genau das erfüllt, was ein gutes VPN ausmacht. Leider hilft das dem Anwender nicht sonderlich viel weiter. Eine weitgehend allgemeingültige aber etwas formale Definition von VPNs lautet:

Ein VPN ist ein Overlay Netz d.h. eine logische Kommunikations-Struktur unabhängig von der unterliegenden physikalischen Struktur, bei der der Zugang solcher Art kontrolliert ist, dass Kommunikations-Verbindungen nur innerhalb einer definierten Interessengruppe und somit exklusiv möglich sind; dies wird durch eine Art Partitionierung der gemeinsamen darunterliegenden Kommunikations-Infrastruktur erreicht, wobei die Kommunikations-Infrastruktur grundsätzlich nicht-exklusive Netzdienste zur Verfügung stellt.

Die verständlichere aber ungenauere Erklärung von VPNs heißt: Ein privates Netz wird über ein öffentliches Netz betrieben, jedoch so, dass die "Privatheit" d.h. die Zugangssicherheit und Integrität erhalten bleiben. Ein einzelnes VPN kann zwei bis mehrere Tausend Endsysteme beinhalten, Standorte eines oder mehrerer Unternehmen umfassen, das Internet benutzen, mehrere ISP-Netze durchlaufen oder auch nicht, einzelne Applikationen verbinden oder eine beliebige Kombination der genannten Einsatzbereiche bedienen. Der Anwender-Zugang zu einem VPN besteht nicht aus dauerhaften sondern dynamischen Verbindungen, die für den Datentransfer aufgebaut und danach wieder abgebaut werden. Die erforderliche Abschottung verschiedener Anwender-VPNs gegeneinander erfolgt durch Tunnel-Techniken (Enkapsulierung) d.h. definierte Verbindungen zwischen einem Start- und Endpunkt und durch Sicherheits-Maßnahmen: Mindestens Daten und Kennungen / Passwörter werden verschlüsselt und somit nicht mehr sichtbar übertragen.

Sicherheit bedeutet die Abdeckung der Aspekte

- Zugangskontrolle (Access Control)
- Vertraulichkeit (Privacy)
- Authentisierung (Authentication)
- Integrität (Integrity)

Der Grad an "Privatheit" und Flexibilität in einem VPN hängt stark vom Konzept und der Technologie ab, mit der das VPN realisiert wurde: Routen-Filterung bietet den niedrigsten Schutz, Tunneltechnik den höherwertigen Schutz und zusätzliche Authentisierung, Autorisierung, Paketfilterung à la Firewall bis hin zur Teil- oder Vollverschlüsselung den höchsten Schutz.

Im Gegensatz zu einigen Herstelleraussagen und VPN-Dienstleistern gehört Quality of Service (QoS) allgemein nicht zum Leistungsumfang eines VPN!

3. VPN-Typen und Konzepte

Frühe VPN-Lösungen mit noch recht einfachen Konzepten waren eher auf große Unternehmen zugeschnitten, die mit eigenem Personal an der Konfigurierung möglichst selbst beteiligt sein wollten und nicht nur das Internet sondern auch wegen der besseren Performance paketvermittelte Providernetze beliebiger Art wie Frame Relay oder PSTN nutzten.

Mit zunehmender Internet-Nutzung auch und gerade durch SMB Unternehmen (Small & Medium Business), günstigen Internet-Tarifen und wenigstens näherungsweise besserer Internet-Performance hat sich der Focus etwas verschoben.

Eine mögliche Unterscheidung von VPN-Typen kann anhand der genutzten Dienste in Kombination mit den eingesetzten Produkten erfolgen:

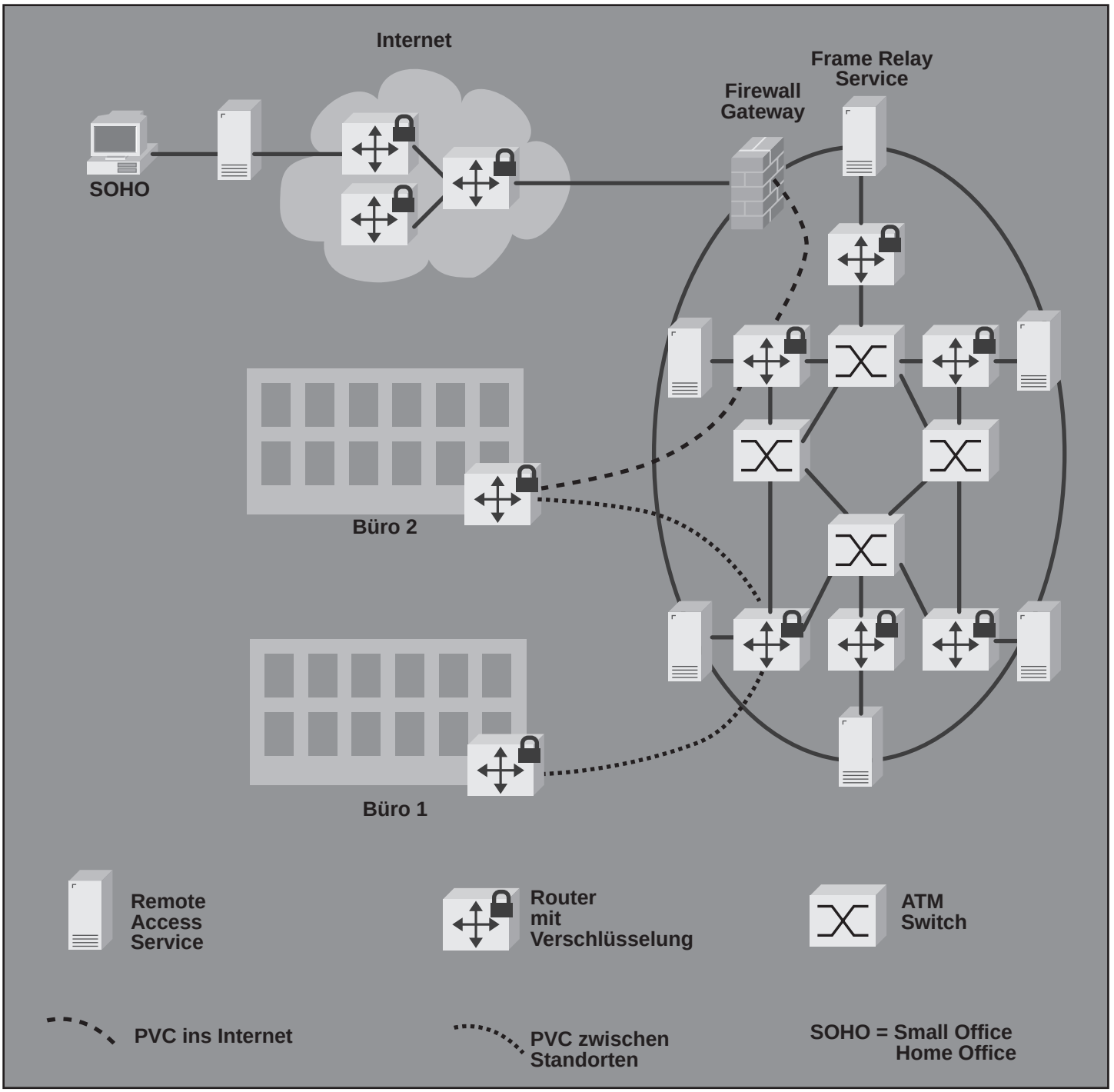
- non-Internet VPN
  (Frame Relay, ATM, ... Providernetz)
- privates VPN
  (CPE-basiertes VPN)
- VPN als Dienst auf Basis Internet-Zugang
  (IP VPN, Internet VPN),
  "Point & Click" VPN-Dienst

Während die ersten beiden Alternativen traditionelle, "legacy" VPN Produkte nutzen, tut sich mit Internet VPN's ein neuer Produkt-Markt auf, wie später beschrieben wird.

Non-Internet VPN's

Vielfach sind dies Frame Relay Netze mit verdecktem Frame Relay Dienst und einer VPN-Struktur als Overlay Netz betrieben wird (siehe Bild 5). Die Technik ist bekannt und etabliert, Betreiber wissen inzwischen wie ihr Equipment funktioniert, der operationale Betrieb hat einige Optimierungszyklen hinter sich und Benutzer vertrauen Frame Relay Dienstanbietern hinsichtlich Durchsatzgarantie erheblich mehr als den ISP's. Vielfach wird jedoch keine Integration von Mobilen Benutzern und Heimarbeitsplätzen angeboten, kein Webzugang realisiert und die Skalierbarkeit hinsichtlich POP's und Zugangskapazität ist begrenzt. Obwohl Frame Relay sicher den leichtesten und schnellsten Weg in die VPN-Technik darstellt, prognostiziert z.B. die Yankee Group nur wenig Wachstum für diesen Markt bis 2005.

Bild 5 VPN auf Basis Frame-Relay



Private VPNs

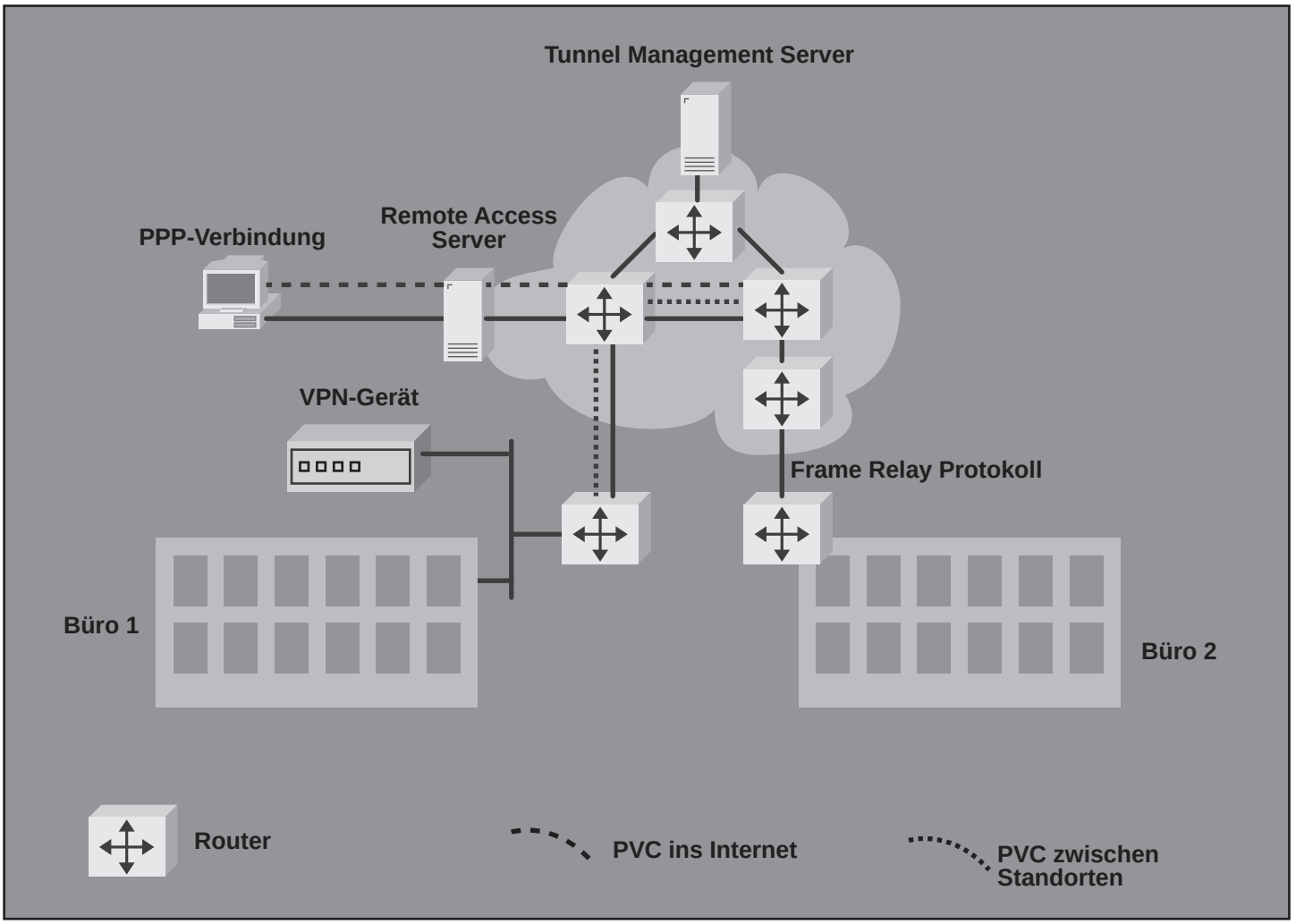
Bei privaten VPN's ist an der Schnittstelle zwischen privatem Standortnetz und Providernetz eine VPN-Komponente installiert, die zum privaten Netz gehört und auch vom privaten Netzpersonal konfiguriert, betrieben, gewartet wird. Eine Übersicht zeigt Bild 6. Nachteilig sind hier bei einem größeren Unternehmen mit mehreren Standorten die hohen Einstiegskosten in Form von Equipment-Investitionen. Dafür ist die VPN-Funktionalität oft besser anpassbar und für komplexere Netze einsetzbar. Vorteilhaft ist die Möglichkeit, bedarfsgerecht einzelne Standorte aufzurüsten. Teilweise wird dieser Ansatz mit Outsourcing kombiniert: Nach der Anfangsinvestition wird das VPN-Equipment von einem Provider betrieben und gewartet.

Eingesetzte VPN Komponenten reichen von low-level bis high-end, z.B.

- nichtdedizierte Server mit VPN-Gateway Software
- Firewalls mit VPN-Erweiterungssoftware
- normale Router mit VPN-Erweiterungssoftware
- spezielle Router mit hardware-implementierten VPN-Funktionen, meistens Verschlüsselung und Tunneling Protokoll-Unterstützung
- standalone VPN Gateways, die mit externen Routern kombiniert werden

Vielfach fehlen in VPN-Umgebungen noch Killer-Applikationen wie E-Commerce und Extranet; solange sich die Nutzung auf E-Mail und Browsertechnik beschränkt, ist das Sicherheitsbedürfnis ggf. noch moderat und Browser-Sicherheit mit SSL wird als ausreichend erachtet. Einige Anwender warten ab, welcher Tunnel-Standard sich endgültig im Markt durchsetzen wird, bevor sie sich für eine VPN-Lösung entscheiden; meine Einschätzung an dieser Stelle ist: die aktuellen RFC's für L2TP und IPsec ebenso wie der Microsoft "Standard" PPTP werden sich länger parallel halten als eine Entscheidung sinnvoll aufschiebbar ist. Einsatz und Management von Verschlüsselungstechnik ist ebenfalls eine Hemmschwelle bei VPN-Einsatz. Nicht zuletzt hält die oft beklagte mangelnde Durchsatzleistung des Internet Anwender vom Schritt zu Internet-basierten VPN's ab und bedingt eine Entscheidung für die Nutzung eines anderen Providers oder eines eigenen Backbones. Hinsichtlich extremer Skalierbarkeit für viele Standorte mit vielen Benutzern liegen allerdings wenig Betriebserfahrungen vor.

Bild 6 VPN mit privatem Equipment



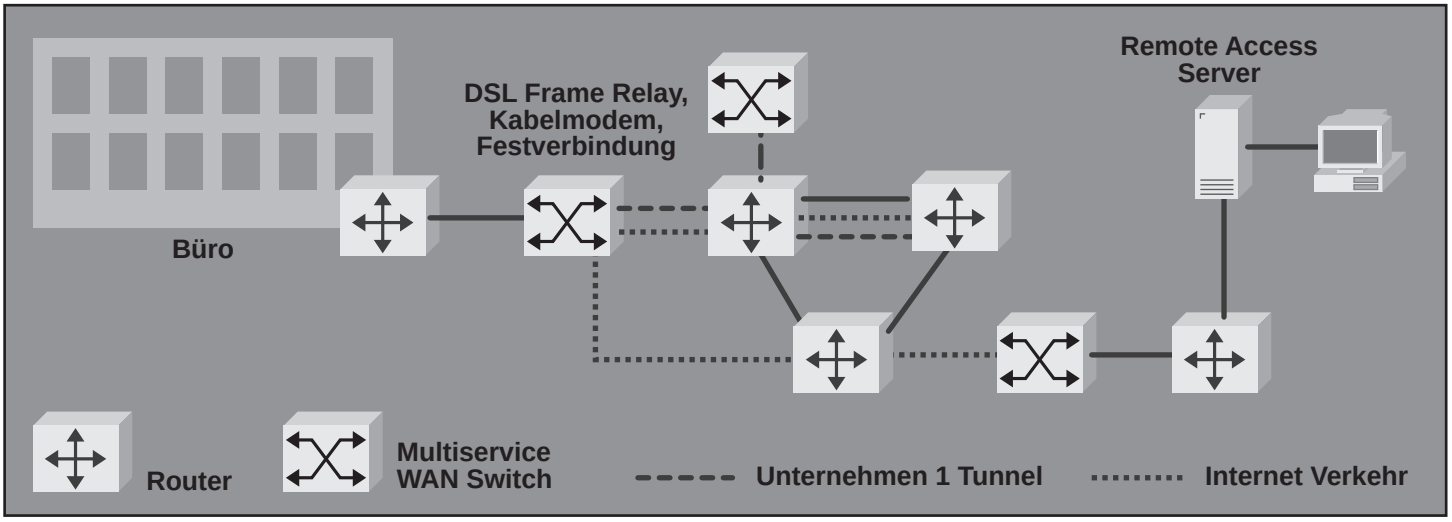


Bild 7 VPN mit Internet-basiertem Zugang und VPN-Komponenten beim Provider

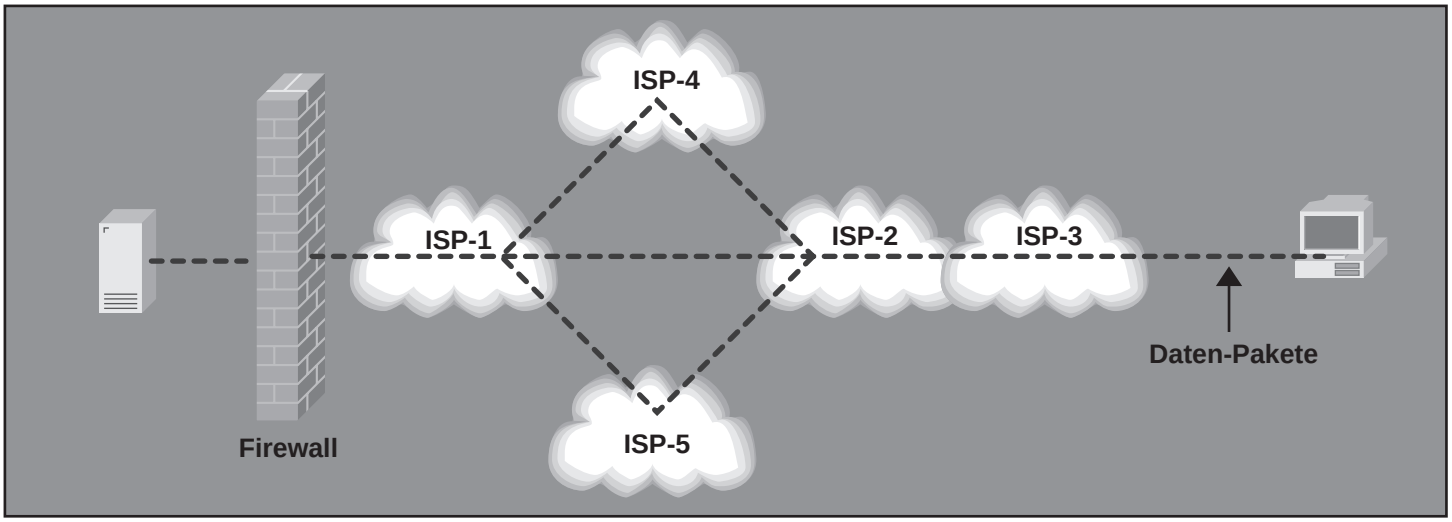
IP VPNs auf Basis Internet-Zugang

Für die sogenannten IP VPNs oder Internet VPNs wird im Vergleich mit den zuvor genannten Alternativen das höchste Wachstum auf 5 Mrd. USD in 2005 erwartet, stellt doch die günstige Internet Tarifstruktur eine besondere Attraktion für sparwillige Netzbetreiber dar. Bei Internet-basierten IP VPNs betreibt der Anwender keine eigenen VPN-Komponenten mehr sondern nutzt einen vom ISP angebotenen VPN-Dienst, bei dem der Provider eigene VPN-Komponenten am Zugangspunkt in sein Netzwerk betreibt, wie Bild 7 darstellt.

Weitverteilte Standorte des Anwenders können dabei über mehrere kaskadierte Providernetze hinweg verbunden werden (siehe Bild 8). Der Internet VPN Ansatz führt dazu, dass an allen Anwender-Standorten dieselbe VPN-Funktionalität zur Verfügung steht anstelle der historisch gewachsenen privaten Komponenten von mindestens drei Herstellern und vier Software-Leveln (Meine Prognose: Nach 5 Jahren Betrieb eines Internet VPN-Dienstes ist dies bei VPN-Providern genauso ...!). Aktuell sind jedoch gerade ISP's, die VPN-Lösungen anbieten, eher auf einem modernen Technikstand; z.B. kombinieren sie BGP Routing und MPLS (siehe Bild 9). Auch wenn letzteres noch nicht vollständig standardisiert ist, ist schon eine breite Akzeptanz bei Providern und Anwendern erkennbar. Alternativ kommt Tunneling mit PPTP, L2TP oder zunehmend IPsec zum Einsatz.

Demgegenüber ist anzumerken, dass Anwender nicht nur skeptisch gegenüber den oft proprietären Lösungen und der damit verbundenen Abhängigkeit von einem einzelnen Provider sind, sondern gegenüber der Leistung, Dienstgüte und Einhaltung von SLA's im Internet allgemein, selbst wenn von Internet VPN Providern mit Quality of Service durch Differentiated Service, Caching und Anti-Virus Schutz per Firewall geworben wird. Hinsichtlich extremer Skalierbarkeit liegen ebenfalls noch keine Betriebserfahrungen vor.

Bild 8 VPN mit ISP-übergreifenden Verbindungen



Virtual Private LANs: Kombination von Kostenoptimierung und Sicherheit

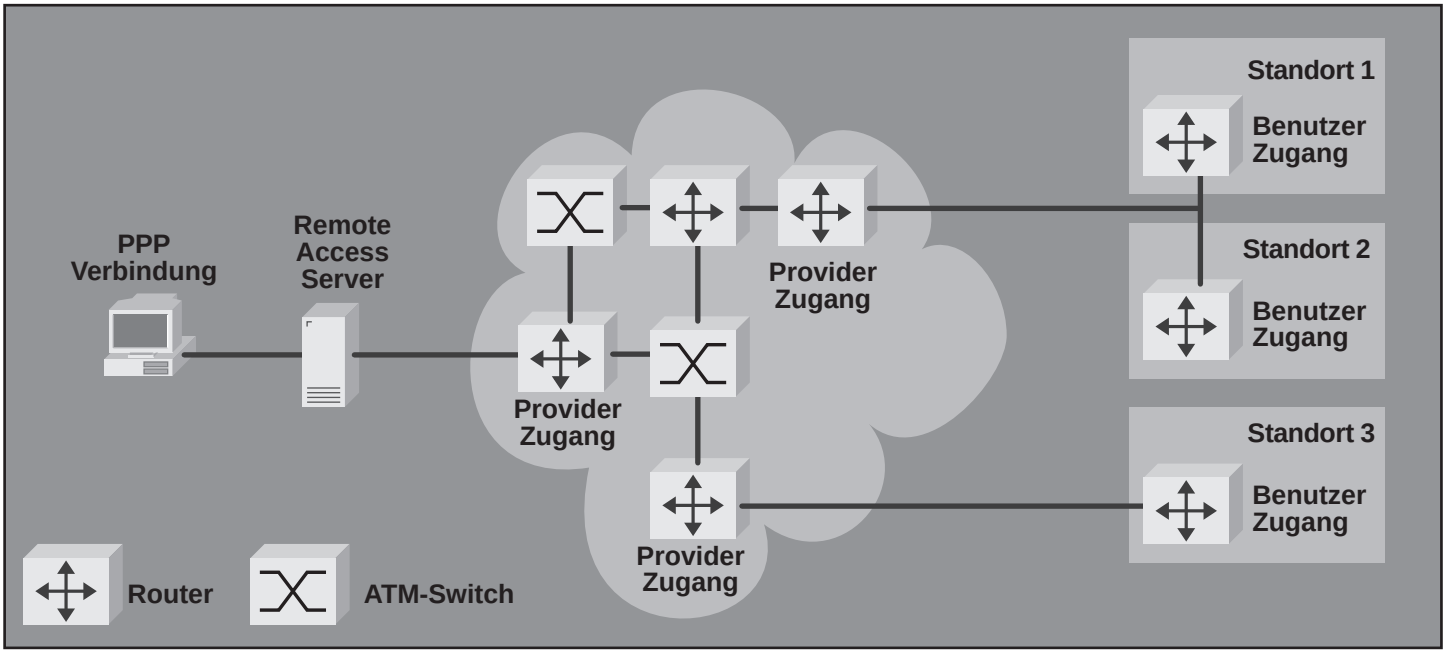


Bild 9 VPN mit Internet-basiertem Zugang und MPLS / BGP Routing

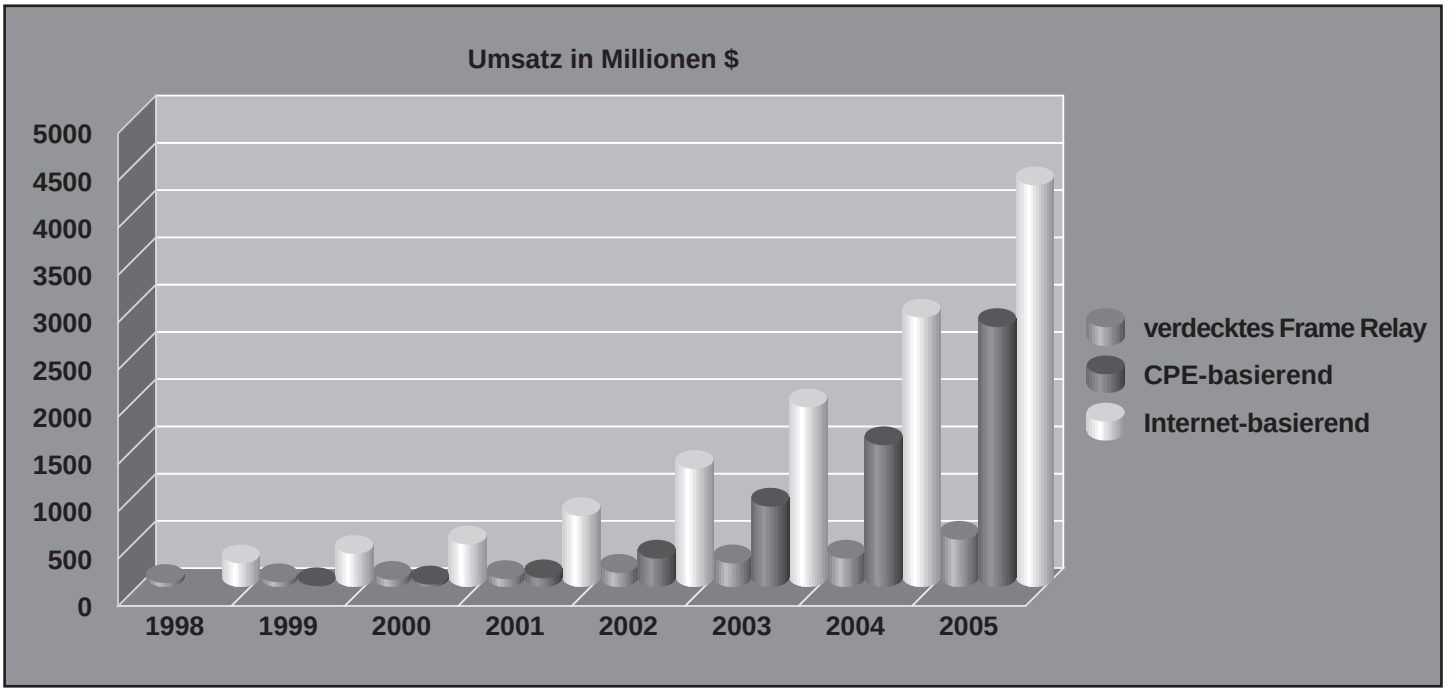
Fazit

Kurz- bis mittelfristig stellen VPN's mit privaten Komponenten einen interessanten Markt dar, mittel- bis langfristig (10 Jahre) geht der Trend zu Internet-basierten VPN's, da diese mehr Dienste, bessere Kontrolle durch die Provider und höhere Flexibilität erwarten lassen.

In der Praxis sind wie immer nicht nur die reinen VPN-Typen zu finden sondern kostenoptimiert und angepasst für spezielle Netze und Betriebssituationen verschiedenste Mischlösungen wie Migrations-Dienste von Frame Relay nach Internet VPN oder Kombinationen aus privatem und Internet VPN, um nur zwei Beispiele zu nennen.

Eine Wachstums-Prognose für die verschiedenen VPN-Dienste zeigt Tabelle 1.

Tabelle 1 Markt für VPN-Dienste



4. VPN-Technik: Verfahren und Komponenten

Um die notwendige Sicherheit und Vertraulichkeit sicherzustellen, werden für VPN's verschiedene Techniken kombiniert, auf die nachfolgend näher eingegangen wird:

- Tunneling (Enkapsulierung)
- Authentisierung
- Verschlüsselung

Tunneling Verfahren

Jeder Tunnel besteht an beiden Endpunkten aus Hardware oder Software, die die Initialisierung, Authentisierung und Terminierung handhabt. Sowohl Nutzer- als auch Daten-Authentisierung sind möglich. Aktuell werden verschiedene Tunneling Verfahren gehandelt unter anderem Cisco und Microsoft gegen den Rest der Welt: Als Zusammenführung des RFC 2341 für Cisco's L2F und des nie über IETF Draft Zustand hinausgekommenen PPTP (Microsoft) entstand L2TP. Die aktuell am meisten unterstützten Verfahren sind L2TP und PPTP. Beide nutzen PPP als Link Protokoll. Beide wiederum konkurrieren mit Tunneling nach IPsec, welches sich als neue Sicherheits-Architektur etabliert. Je nach Einsatzgrund wie z.B. entweder Ersatz von RAS Systemen oder Sicherheit mit Verschlüsselung wird die Entscheidung für unterschiedliche Tunnelprotokolle fallen.

Soll Tunneling mit Verschlüsselung kombiniert werden, entsteht das Problem, dass bei einer Verschlüsselung des IP Headers an jedem Router eine Decodierung erfolgen müsste, um die Routing Informationen erkennen zu können. Als Abhilfe kann das Original-Paket komplett verschlüsselt und der (zweite) IP-Header der Enkapsulierung unverschlüsselt übertragen werden. Somit sind die originalen Sender-/Empfängeradressen sowie höhere Protokollheader für Hacker nicht mehr erkennbar, der Start- und Endpunkt des Tunnels jedoch schon.

Tunnel-Endpunkte können Einzelstationen (VPN Client) oder LAN's mit sogenannten VPN Gateways / Security Gateways (Router, Firewall, standalone VPN-Gerät) sein, die komplette Netze (meistens LANs) an den VPN-Verbund anschalten. Mögliche Kombinationen sind

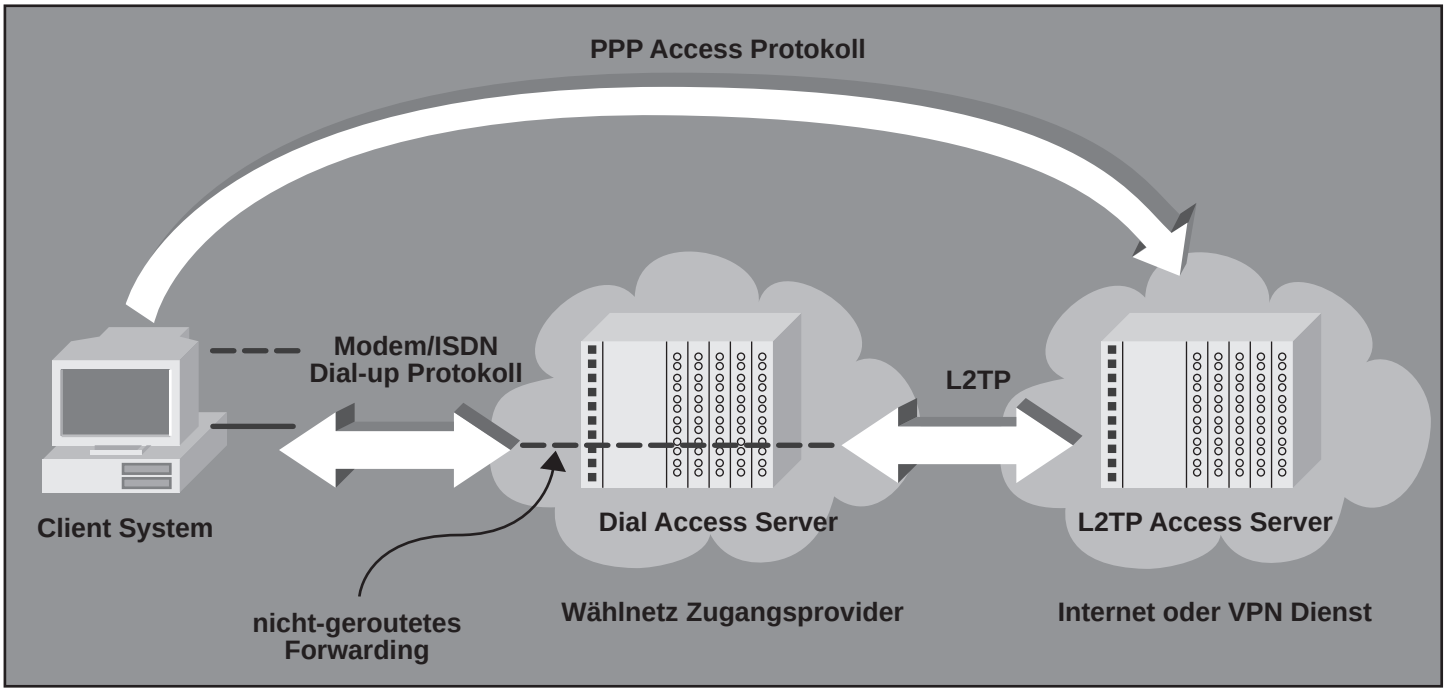
- LAN-to-LAN
- Client-to-LAN

LAN-to-LAN Tunnel sind mit je einem VPN Gateway an jedem Tunnel-Endpunkt als Sicherheits-Interface zwischen LAN und Tunnel bestückt und können von beiden Seiten initiiert werden. Client-to-LAN Tunnel erfordern eine VPN Software auf dem Clientsystem (z.B. PPTP) und werden stets vom Client initiiert. Während PPTP, L2F und L2TP eher auf Client-to-LAN abzielen, ist IPsec für LAN-to-LAN VPNs besser geeignet.

L2TP

L2TP (RFC 2661; RFC 3071: L2TP over FR) beinhaltet Verbesserungen der Schwachpunkte von L2F und PPTP. Es setzt den Einsatz von NAS und RAS-Servern voraus, da der Tunnel am Netzübergang endet (Bild 10), und nutzt weder L2F noch PPTP sondern definiert ein eigenes Tunneling. Verschiedenste Medien angefangen von X.25 über Frame Relay, DSL bis ATM werden unterstützt. L2TP Tunnel können entsprechend des Sessionverlaufs dynamisch auf- und abgebaut werden, das PPP Protokoll wird für Dial up zwischen Zugangspunkt und Ausgangspunkt des Backbone-Netzes gefahren. Für Authentisierung werden PPP Verfahren (PAP, CHAP, EAP, ...) oder Authentisierungs-Server wie RADIUS genutzt. Da L2TP ein Layer-2 Verfahren ist, können auch non-IP Protokolle gefahren werden (SNA, IPX, AppleTalk). Diese werden in IP enkapsuliert bzw. getunnelt. L2TP hat keine eigene Verschlüsselung definiert sondern verweist hierfür auf IPsec.

Bild 10 PPP Tunnel mit L2TP



Virtual Private LANs: Kombination von Kostenoptimierung und Sicherheit

PPTP

PPTP ist ein Microsoft-"Standard" und hat entsprechende Verbreitung im Markt, ist aber nie ein offizieller (RFC)-Standard geworden.

PPTP definiert einen Tunnel zwischen Endsystemen bzw. Ende zu Ende zwischen Client und Serversystem und ist z.B. in Windows95/98 und NT Dial Up Networking standardmäßig enthalten. PPP wird nur zwischen Client/Server Endsystem und NAS/RAS Server gefahren und dort auf beiden Seiten terminiert, läuft also nicht im Backbone-Netz (Bild 11).

NAS/RAS Server sind nicht am Tunnel-Aufbau und Aushandeln der Parameter beteiligt, sondern realisieren den Eingangs- und Ausgangspunkt zu einem traditionell gerouteten Netz. Dies entspricht dem klassischen Internet Access PPP-Modell. Zusammen mit PPTP nutzt Microsoft eine eigene Authentisierung (keine Token Verfahren) und Verschlüsselung, z.B. das schwächere RSA oder MPPE anstelle von DES oder 3DES aus IPsec.

Authentisierungs- und Verschlüsselungsverfahren auf Basis PPP sind ebenfalls möglich (PAP, CHAP, EAP,...). Ähnlich wie L2TP kann PPTP auch non-IP-Protokolle handhaben.

LF2

L2F nutzt PPP für Dial up und Authentisierung (PAP, CHAP, EAP), zusätzlich RADIUS oder das Cisco-eigene TACACS+. Im Unterschied zu PPTP können mehrere Verbindungen über denselben Tunnel betrieben werden, hierfür sind entsprechende manuelle Definitionen vorzunehmen. Es gibt zwei hintereinandergeschaltete Authentisierungen für den Benutzer, zuerst beim ISP zu Beginn des Tunnel-Aufbaus, danach am VPN-Gateway (Router) des Unternehmens.

Zu beachten:

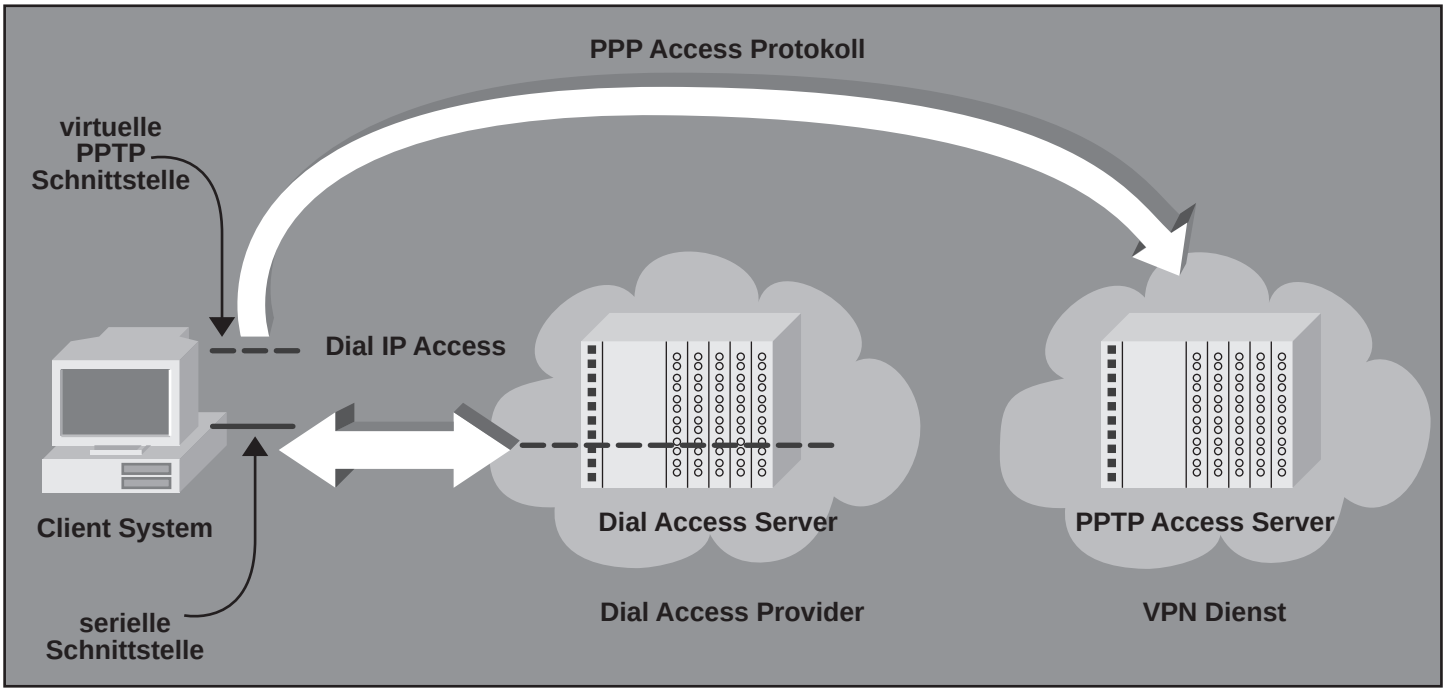
Weder L2TP noch PPTP noch L2F berücksichtigen Verschlüsselung oder Schlüsselmanagement-Systeme!

IPsec

IPsec ist eigentlich eine Sicherheits-Architektur, die verschiedene Protokolle und Verfahren für Verschlüsselung, Authentisierung und Tunneling vorgibt und sich zunehmend im Markt etabliert. Ursprünglich wurde es für IPv6 erfunden, dann aber für IPv4 adaptiert. Jede Session kann entweder verschlüsselt oder lediglich authentisiert werden. Soll nur Authentisierung erfolgen, wird ein Header Authentication Header Protokoll eingefügt (AH), erfolgt Verschlüsselung, wird ein Header nach dem Encapsulation Security Payload Protokoll (ESP) eingefügt. Für Verschlüsselung sind zwei Bearbeitungs-Modi definiert, der Transport Modus und der Tunnel-Modus.

Für LAN Umgebungen ist der sogenannte Transport Modus vorgesehen, der nur die oberen Protokoll-Header authentisiert oder verschlüsselt, was den Rechenaufwand verringert. Für WAN-Umgebungen wird der gegen Angriffe und Spionieren sicherere Tunnel-Modus vorgeschlagen, wobei der Tunnel-Modus unter IPsec nicht mit dem Tunneling-Begriff bei L2TP und PPTP gleichzusetzen ist: IPsec gibt für den Tunnel-Modus nämlich vor, dass das getunnelte Original-IP-Paket komplett verschlüsselt wird, während andere Tunnelverfahren auch Einkapsulierung ohne Verschlüsselung zulassen. Eine Übersicht beider Modi und der resultierenden Verschlüsselung / Authentisierung zeigt Bild 12.

Bild 11 PPP Tunnel mit PPTP



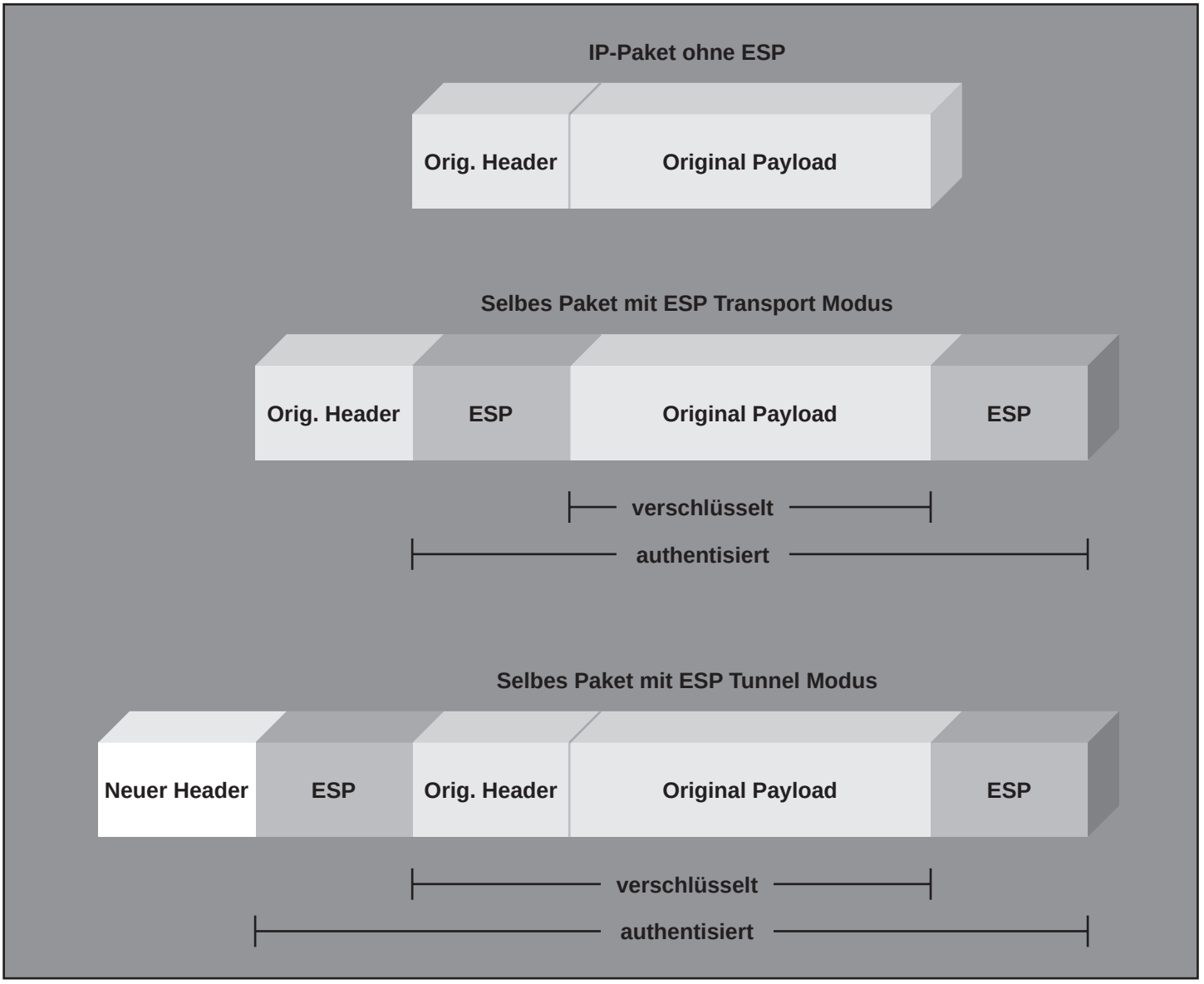


Bild 12 IPsec: Transport Modus und Tunnel Modus mit resultierender Paketstruktur

Die IPsec Spezifikationen stützen sich auf eine Reihe standardisierter Verschlüsselungs-Techniken ab wie

- Diffie-Hellman Schlüsselaustausch
- Public Key für Diffie-Hellman
- DES, 3DES
- Hash-Verfahren wie HMAC, MD5, SHA für Authentisierung von Benutzer-Parametern und auch Dateninhalten via Prüfsumme
- Digitale Zertifikate und Zertifikat-Server

Schlüsselmanagement erfolgt mit IKE (früher ISAKMP; geeignet für viele Standorte) oder manuell (geeignet für wenige Standorte). Ein vertiefter Ausflug in Verschlüsselungstechniken unterbleibt an dieser Stelle, dies ist ein separates Netzwerk-Insider Thema. Grundsätzlich gilt: Die Schlüsselgültigkeit (Krypto-Periode) ist zeitlich zu begrenzen und je höher das Sicherheitsbedürfnis, desto größer sollte die Schlüssellänge sein: Während DES einen 56-Bit Schlüssel erlaubt (für eine Cray eine Sache von 12 Sekunden), entspricht Triple-Des einem 112-Bit Schlüssel und 3DES einem 168-Bit Schlüssel. Bei Nutzung von Internet-Diensten ist letzteres vorzuziehen.

Für Authentisierung sind folgende Varianten mit steigender Komplexität und Sicherheit denkbar:

- Benutzername: unsicher
- Passwort: mindestens verschlüsselt und unter Einsatz von Authentisierungs-Servern wie RADIUS, NT Domäne, NDS
- Secure Token: sicherer, da Passwort zufällig ausgewählt wird
- Digitale Zertifikate: sicherstes Verfahren, entwickelt sich zum de facto Standard

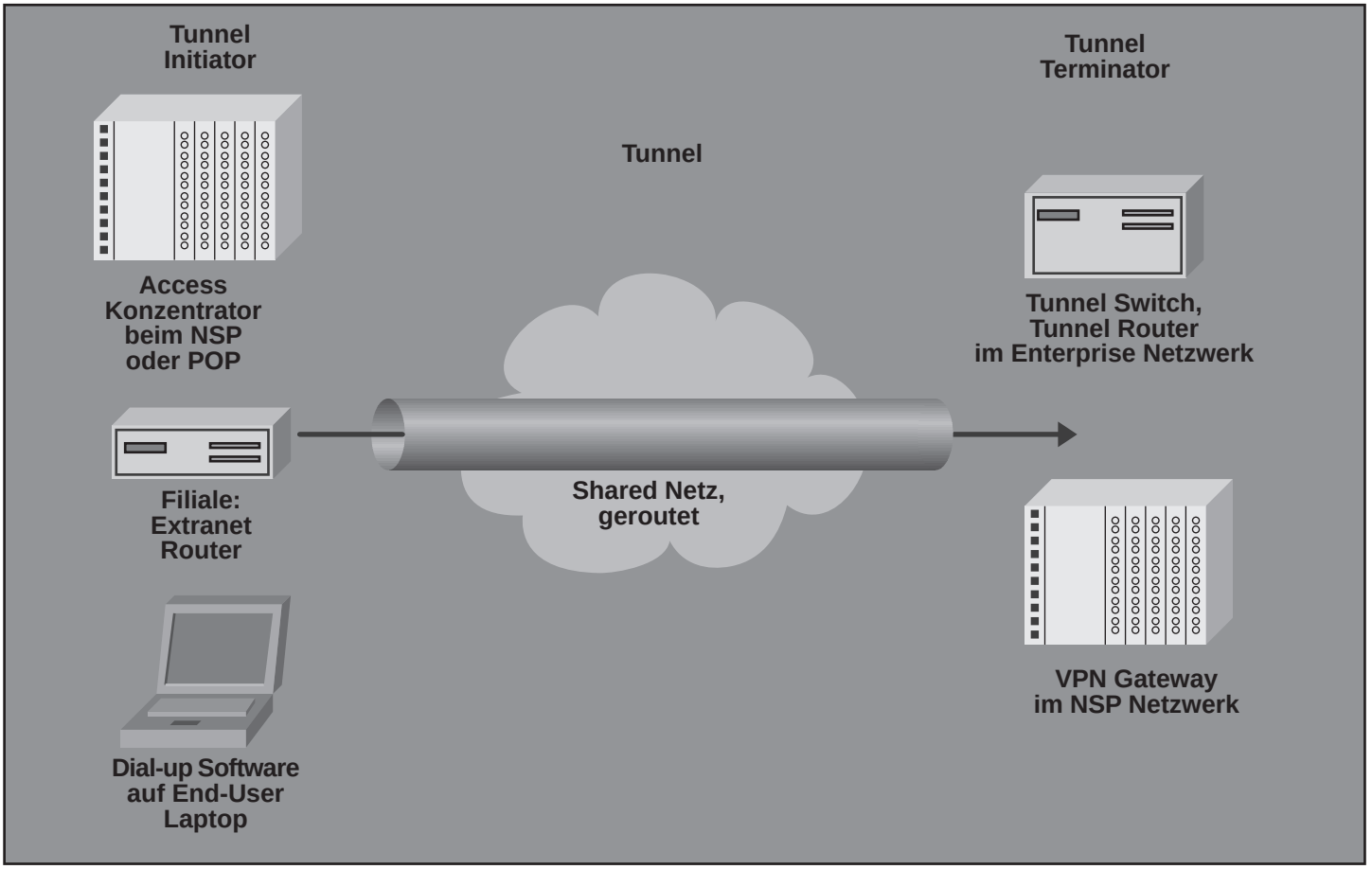


Bild 13 Mögliche VPN-Komponenten

Die Qual der Wahl im Komponentenurwald

Für eine VPN-Lösung in der Praxis spielen verschiedene Komponenten zusammen:

- Provider-Netz oder Internet, dies können wir als vorausgesetzt abhaken
- VPN-Komponente
- Policy Server
- Certificate Authority / Server

VPN-Komponenten können in Firewalls oder Router integriert sein, als separate standalone Hardware betrieben werden oder als Software auf einer Serverplattform implementiert sein (siehe Bild 13).

Router

Routerlösungen sind teilweise reine add-on Software mit entsprechend limitierter Leistung oder Zusatzkarten, insbesondere für Verschlüsselung verfügbar (Alcatel, Avaya, Cisco, Enterasys, Intel, Lucent, Motorola, Nortel, ...). In jedem Fall ist darauf zu achten, dass nicht durch Aktivierung der VPN-Funktionalität die CPU-Last zu groß wird und zu einem Leistungseinbruch im normalen Routing Durchsatz führt. Der Backup-Bedarf ist durch Router-Redundanz Protokolle wie VRRP und HSRP lösbar.

Firewalls

Firewalls bieten oft Tunneling und Verschlüsselung als Zusatzfunktion an (Checkpoint, Fortress, F-Secure, Lucent, NetScreen, Network Associates, Nokia, SoniWALL, WatchGuard, ...), wobei dies analog zu Routern die Gesamtleistung belastet. Integrierte Firewall/VPN's sollten nur in kleinen Netzen und mit maximal 1 bis 2 Mbit WAN-Zugangskapazität eingesetzt werden. Redundanzlösungen sind begrenzt verfügbar und vor allem nicht standardisiert. Ändert sich der VPN-Bedarf, müssen die Firewalls rekonfiguriert werden, was oft komplexer ist als bei reinen VPN-Komponenten.

Standalone VPN Gateway

Standalone VPN Komponenten sind im Regelfall zwischen internen Router und Provider-Router geschaltet (Altiga, Indus River, Radguard, RedCreek, VPNet, ...).

Der typische Einsatzfall sind LAN-to-LAN Kopplungen mit einer hohen Anzahl parallel unterstützter Tunnel. Diese Geräte bieten reine VPN-Funktionalität, vermeiden somit eine "Überintegration" und sind teilweise erheblich leichter zu konfigurieren als entsprechende Funktionen auf Routern oder Firewalls.

Redundanz macht noch Probleme, mindestens sollte auf doppelte Stromversorgung (PSU) geachtet werden. Einige Produkte arbeiten mit einem Policy Server desselben Herstellers zusammen und ermögichen so die Integration von Authentisierung mit der Programmierung von Sicherheits-Regeln für mehrere VPN-Komponenten gleichzeitig (Redback/ Abatis, Nortel/Shasta, Lucent/ Springtide).

Virtual Private LANs: Kombination von Kostenoptimierung und Sicherheit

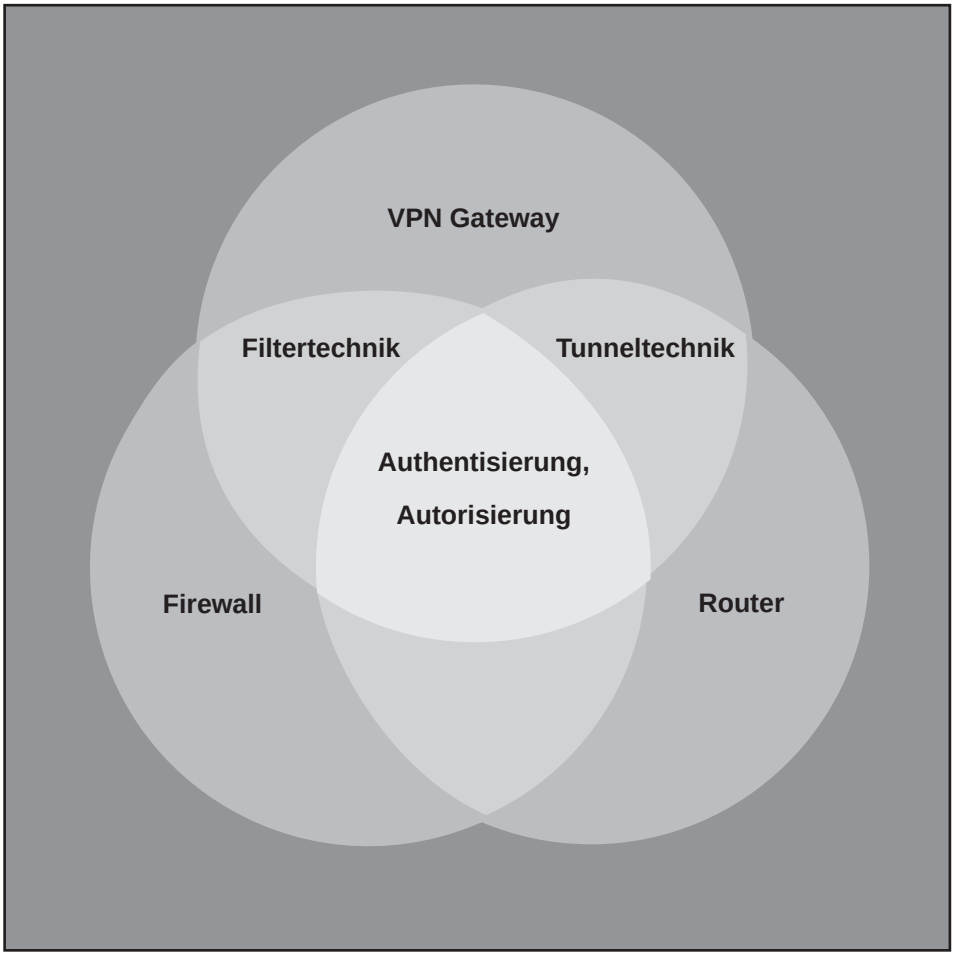


Bild 14 Funktionsbereiche von VPN Gateways, Firewalls und Routern

In der aktuellen Marktentwicklung ist erkennbar, dass die früher stark separierten Produktgruppen Router, Firewall und VPN Gateway funktional in die jeweils anderen Gerätebereiche hineinwachsen, um sich ein Stück von dem begehrten Kuchen mit Namen Umsatzvolumen abzuschneiden (Bild 14).

RVPN Software

Softwarelösungen müssen an beiden Endpunkten eines Tunnels immer konsistent installiert sein, aber wer käme auch auf die Idee, eine Microsoft Software am VPN Server mit einer Intel Software oder gar einem Cisco IOS am Client zusammenzuschalten... Diese Alternative ist klar als low cost low function einzustufen und wenn überhaupt, dann nur für Client-to-LAN VPN's empfehlenswert.

Policy Server

Policy Server verwalten Benutzer-Profile und Access Control Listen. Bei Aufbau einer Session, z.B. mittels RADIUS, wird das hinterlegte Profil mit den übermittelten Parametern abgeglichen, nur bei Übereinstimmung wird die Session zugelassen.

Zertifikat Server

Für unternehmens-interne Kommunikation sind ggf. eigene Server geeignet, für übergreifende Kommunikation mit anderen Unternehmen ist die Nutzung externer Zertifikat Server sicherer und leistungsstärker.

IP Service Switches

Zusammen mit Internet VPN's kommt eine neue Produktgruppe mit dem Namen IP Service Switches und Virtual Private Router in Mode (CoSine, Ennovate Networks, Redback, Shasta/Nortel, SpringT∏tide/Lucent). Diese Geräte sind am Provider-Zugang positioniert und haben eine VPN Routing Intelligenz, mit der sie Tausende separater Benutzer oder Benutzergruppen bedienen können. In diesem Sinn ist die Bezeichnung Virtueller Router angebracht, da der Switch logisch in viele "Minirouter" gesplittet ist, nämlich ein virtueller Router je VPN. Je VPN / Virtuellem Router lassen sich dann verschiedene Tunneling, Verschlüsselungs-Routing und Quality of Service Funktionen aktivieren. Diese Entwicklung verwundert nicht weiter, wir haben sie ja in den LAN's mit VLAN-Technik schon einmal hinter uns gelassen.

Die Unterstützung verschiedenster Medienschnittstellen wie FR, ATM, DSL, Wireless, ISDN, Kabelmodem wird vorausgesetzt. Für Management und Accounting sind im Vergleich zu Standard Routern mehr Monitoring Funktionen verfügbar. Für Nutzergruppen und einzelne Nutzer werden Status-Informationen über Leistungs-Anforderungen und Lastprofile abgelegt. Einige Hersteller fokussieren sich mehr auf Kundenmanagement, andere mehr auf VPN Customizing Funktionen (Shasta, CoSine). Funktionen, die in naher Zukunft verfügbar werden und zur Bewertung von IP Service Switches gewichtet und hinterfragt werden sollten, sind insbesondere

- hoher Durchsatz
- Unterstützung verschiedener Interfaces (FR, DSL, ATM, E1, ..)
- 3DES oder TripleDES Verschlüsselung
- IPsec und Dial Tunnel Terminierung (PP TP, L2TP)
- LDAP für Verzeichnis-Zugriff
- MPLS
- Frame Relay
- NAT
- PKI Unterstützung mittels Partnerschaften
- Denial-of-Service Schutz
- Virenschutz
- Echtzeit und Langzeit SLA Monitoring
- Abrechnungs-Informationen
- Content / URL Filter
- Content Load Balancing
- Content Management
- Integration, Zugang zu Portalen
- leichte Integration neuer Dienste

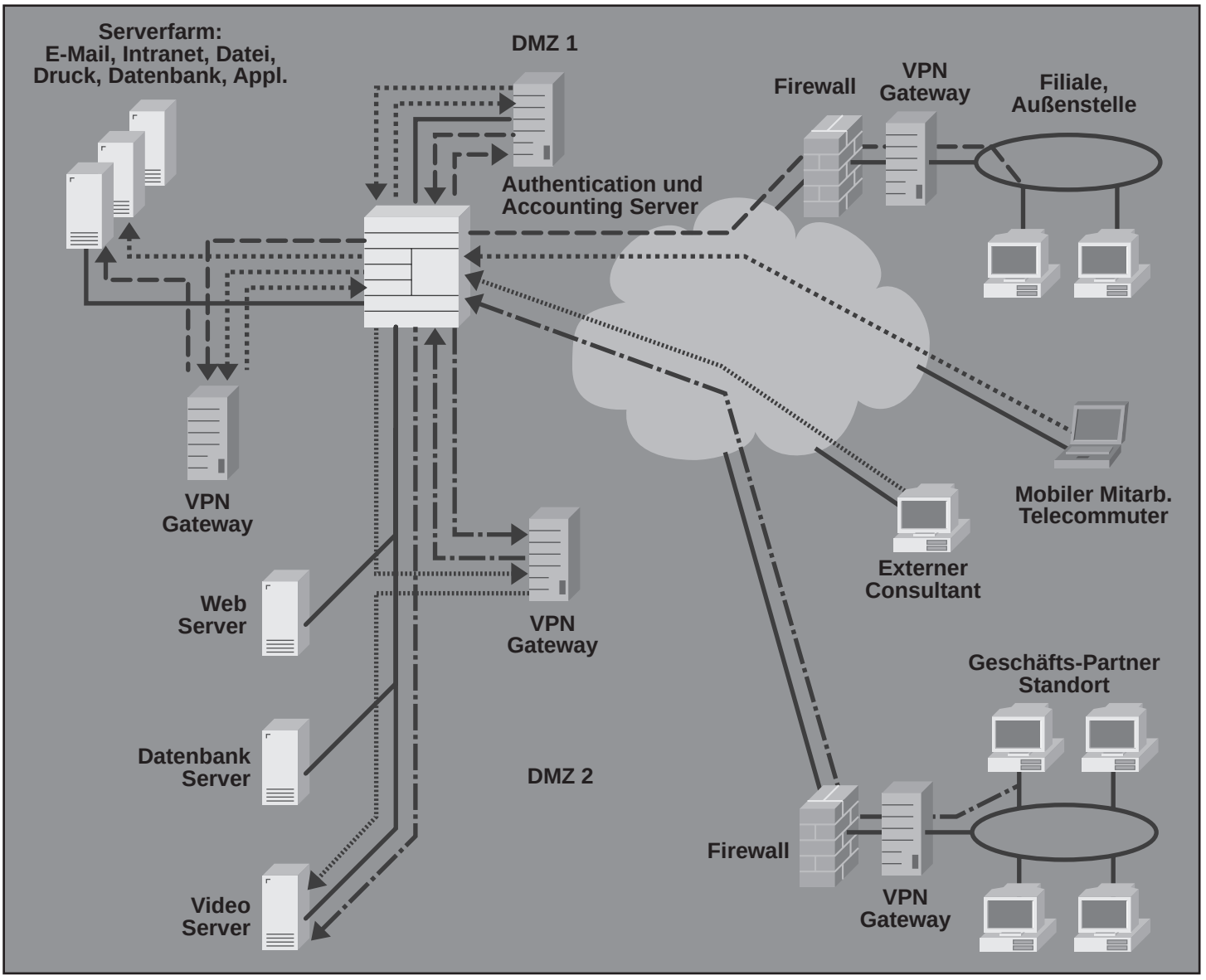
5. VPN Einsatzszenarios und Implementierungen

Einsatzmöglichkeiten gibt es in fast beliebigen Ausprägungen, hier nur einige grundsätzlich unterschiedliche Szenarios aus der älteren und neueren VPN-Entwicklung.

Szenario 1

Anstelle von teuren sternförmig angemieteten Festverbindungen über Fernstrecken vereinbart eine Versicherung mit dem Netzbetreiber einen Frame Relay Dienst. Hierbei nutzt sie die Zugangsleitungen zum jeweils nächsten POP exklusiv, dahinter nutzt sie zusammen mit allen anderen Kunden des Netzbetreibers einen Frame Relay oder ATM Backbone. Für kleine Standorte ist ISDN Einwahl implementiert. Für den Provider sind VPNs im Gegenzug ein wichtiges Mittel, um SLA's mit verschiedenen Kunden getrennt bearbeiten zu können: Einzelne Service-Level-Klassen bis hin zu einzelnen Kunden können über jeweils eigene VPNs bedient werden. In der gezeigten Konfiguration (Bild 15) sind verschiedene Zugangsmöglichkeiten implementiert: Für Mitarbeiter, die remote Zugang benötigen, steht ein VPN Server am Außenstandort und bildet einen sicheren Tunnel mit dem VPN Server im privaten Netzbereich der Zentrale. Mobile Mitarbeiter müssen sich authentisieren, daher stellt der VPN Server eine Anfrage an einen Authentisierungs-Server in der DMZ1. Consultants müssen sich nicht authentisieren, werden aber über einen separaten VPN Server in DMZ2 geschleust, da dies einerseits sicherer ist als der Zugriff auf den VPN Server im privaten Bereich und andererseits sicherer ist als den VPN Server vor dem Firewall zu positionieren...! Mitarbeiter von anderen Unternehmen haben es am schwersten und müssen über den VPN Server in DMZ2, der dann eine Anfrage an den Authentisierungs-Server in DMZ1 stellt. Authentisierungs-Server gehören grundsätzlich in eine DMZ, wo sie gut verwaltet und gegen Attacken sowohl von innen als auch von außen geschützt werden können.

Bild 15 Standort von VPN Servern, Authentisierungs-Servern und Firewalls



Virtual Private LANs: Kombination von Kostenoptimierung und Sicherheit

Szenario 2

Ein Media-Unternehmen HYPE veröffentlicht die neuesten Nachrichten im Gesetzgebungs-Bereich innerhalb von 12 Stunden. Genutzt wird eine kombinierte Lösung mit Nachrichten-Journalisten und Software-Retrieval. 35 Mitarbeiter sind in drei europäischen Ländern positioniert (Italien, Deutschland, Schweden). Da der Neuheitsgehalt der Nachrichten entscheidend für das Image von HYPE ist, wird die bisher genutzte Kombination von E-Mail und FTP nicht mehr als ausreichend betrachtet.

Das Problem

- drei verschiedene Standorte mit verschiedenen Internet-Zugängen (2 Mbit SFV, DSL, Frame Relay)
- Verbindungs-Störungen, unzureichende Verfügbarkeit
- begrenzte IT Ressourcen
- begrenztes IT Budget
- Wachstums-Bedarf / Skalierbarkeit

Die Firma HYPE schließt einen Vertrag mit dem Internet VPN Dienstleister WorldNet für einen LAN-to-LAN VPN-Verbund der drei Standorte. WorldNet stattet die PC's via Download mit entsprechender VPN-Client Software aus und konfiguriert die notwendigen VPN-Parameter auf einem WorldNet-eigenen Server. Die genutzte Überwachungs-Software führt dazu, dass WorldNet HYPE einige Tage später mitteilt, dass es ein Problem mit dem Internet-Zugang in Italien gibt, der eigentlich in keiner Form von WorldNet betreut wurde oder managementmässig integriert war. Kostenmäßig fallen für HYPE monatliche Grundgebühren und Volumengebühren an. Equipment-Investitionen sind mit Ausnahme von der Hochrüstung einiger älterer PC's nicht entstanden.

Szenario 3

Das Vorspiel

Eine bekannte englischsprachige Netzwerkzeitschrift mit gleichnamigem deutschen Ableger hat sich nach 8 Jahren CompuServe Netzbetrieb inklusive Aufkauf durch WorldCom, Merger mit MCI und Integration mit UUNET über die insbesondere tarifliche und funktionale Inflexbilität ihres Frame Relay Providers CompuServe so geärgert, dass ein Wechsel geplant wurde. Statt Frame Relay sollte DSL die neue Netzzugangstechnik werden.

Die Planung

Es begann die Suche nach den Dutzenden von WAN Providern, die hinter diesem Deal her waren. Aber wo waren sie? Schon der Versuch, einen von ihnen ans Telefon zu bekommen, entpuppte sich als Abenteuer. Einen Rückruf zu bekommen, um Preise und Logistik zu diskutieren, schien außerhalb des Machbaren. UUNET bot eine Migration von Frame Relay zu einem managed VPN Dienst an. Falls in Wisconsin ein Zugang von 512k gemietet würde und in Washington auch, so sollte garantiert werden, dass der Durchsatz auf der Verbindungsstrecke (welche auch immer es wäre) auch 512k beträgt und dass die Verbindung keinesfalls über andere Netze als den eigenen Backbone geroutet würde. Nach den mit UUNET bereits gemachten Erfahrungen wurde diesen Zusicherungen nur bedingt Glauben geschenkt.

Qwest zeigte sich relativ interessiert, sobald nach einigen Kontaktaufnahme-Schwierigkeiten eine Person gefunden war, die sich zuständig fühlte. Qwest machte die Aussage, dass der eigene Backbone weniger als 5% ausgelastet ist - während die Presse berichtete, dass Qwest permanent an die Leistungsgrenzen ihres Backbones stößt ... Auch Digital Island, AT&T und GTE wurden gefragt. Die Entscheidung fiel schließlich für VPN Komponenten von Nokia sowie für @Link und Genuity (früher GTE) als DSL Provider außerdem für eine Ankopplung an das Internet der Syracuse Universität.

Die Story

Der DSL-Zugang in Washington wurde innerhalb von 3 Wochen von Bell Atlantik geschaltet. Nokia benötigte mehr als 3 Monate, um die Komponenten auszuliefern. Die zum Testen geplante Zeit verstrich ungenutzt. Danach lief die Deadline für die Implementierung ab. Als Workaround wurden Firewall-Komponenten von Netscreen geleast, die anstelle der Nokia-Komponenten im selben Konzept betrieben werden konnten. Es stellte sich heraus, dass @Link weder in Chicago noch in Madison eine T1 Zugangs-Kapazität realisieren konnte. Die Verfügbarkeit hierfür war bei Tageslicht betrachtet als "möglicherweise in einigen Monaten für Chicago" angekündigt. In Madison: nicht geplant. Eine niedrigere DSL-Zugangsrate wurde für Madison als verfügbar mitgeteilt, was sich jedoch als falsch herausstellte. Um dies herauszufinden, benötigte @Link sechs Wochen. @Link musste eine T1-Verbindung anstelle DSL aktivieren, was dann zum selben Preis angeboten wurde. Dies dauerte weitere sechs Wochen. Sämtliche zugesagten Fertigstellungstermine wurden überschritten. Da im Verlagsnetz ein eigener DNS-Dienst gefahren wird, sollte kein Hosting der Domäne erfolgen. Später wurde eine Anfrage gestellt, von Washington aus reverse DNS zu fahren. Genuity bot reverse Adressierung für Mailserver an, jedoch nicht für irgendetwas anderes, auch nicht DNS Server.

Das Resultat

Verkehr zwischen @Link-angebundenen Standorten ist mit einem Delay von 20 ms sehr schnell. Kommunikation mit Washington dagegen zeigt ein Delay von 140 ms! Die Management Software zeigt gelegentliche unerklärliche Paketverluste, denen jedoch aktuell eine größere Beachtung gewidmet wird. Als negativ stellte sich heraus, dass sich in einem Zeitraum 9 Tagen die Ausfallzeit auf 20 Minuten addierte. Zwar lagen die meisten Totalausfälle außerhalb der Arbeitszeiten, aber trotzdem bleibt ein ungutes Gefühl zurück. Eine Störfall-Analyse wurde bisher nicht vorgenommen. Längere Ausfallzeiten, die die Kommunikation signifikant beeinträchtigten, ereigneten sich jedoch in den ersten Betriebswochen nicht.

Vergleich zu früher

- Die Migration war ein Friss-oder-stirb Szenario.
- Die monatliche Gebühr sank von $ 16.000 auf $ 2.000.
- Der frühere Frame Relay Dienst hatte etwa eine Verfügbarkeit von 24x7.
- Mit Frame Relay gab es gelegentlich Ausfälle, aber keine nichtdeterministischen kurzzeitigen Aussetzer.

Nebenbemerkung

Welches Szenario - 2 oder 3 - erscheint Ihnen realistischer?

Stimmt - mir auch!

6. Das Spiel mit Budgetplanung und Kosten

Grundsätzlich sind hier zwei Varianten zu betrachten: der Aufbau eines VPNs mit selbstbetriebenem Equipment unter Nutzung "ganz normaler" Netzdienste gegenüber der Nutzung eines angebotenen VPN-Dienstes. Im ersten Fall ist die Kontrolle und Anpassung der VPN-Funktionen an die eigenen Bedarfe besser erreichbar, dafür entstehen Kosten für Know How Aufbau, Erstkonfiguration und laufenden Betrieb.

In einem Extremfall betrug der Implementierungs- und Test-Aufwand für ein VPN mit 5.000 Benutzern 60 Arbeitstage, also etwa 25.000 DM bis 30.000 DM. Weiterhin war eine Person fulltime damit beschäftigt, Pflege und Änderungen durchzuführen, das bedeutet weitere 150.000 DM bis 170.000 DM Betriebskosten pro Jahr. Werden auf der anderen Seite diese Kosten durch die Umstellung eines Festverbindungs-Netzes auf Frame Relay / ISDN nicht eingespielt, ist das VPN lediglich ein Arbeitsbeschaffungsprogramm.

Sind die laufenden Betriebskosten aufgrund einfacherer Konfigurationen niedriger, kann die Rechnung anders aussehen:

Die VPN-Einrichtung für 10 weit auseinanderliegende Standorte kostete 85.000 DM. Durch die Nutzung von Zugangsleitungen im Nahbereich anstelle von Fernverbindungen sank die monatliche Gebühr von durchschnittlich 8.500 DM auf 5.500 DM je Standort. Die monatlichen Betriebskosten betrugen 10.000 DM. Dies bedeutete eine monatliche Einsparung von 20.000 DM. Nach 5 Betriebsmonaten hat sich die VPN-Entscheidung amortisiert.

Bei Nutzung eines VPN-Dienstangebots fallen üblicherweise monatliche Zugangskosten und Nutzungsgebühren an. Das kann je nach Konfiguration zwischen 1.000 DM und 20.000 betragen. Wenn schon ein Netzdienst genutzt wird und der VPN-Dienst nur eine Ergänzung darstellt, sollte eine erneute Berechnung des Netzdienstes zurückgewiesen werden, da sie nicht gerechtfertigt ist. Zu berechnen sind in diesem Fall nur noch die Mehrkosten für die Nutzung des VPN Overlays. Bei Vereinbarung eines VPN-Dienstes ist auch die enthaltene Funktionalität zu überprüfen, d.h. wenn keine Authentisierung und Verschlüsselung benötigt wird, sollte auch keine bezahlt werden, wenn Authentisierung und/oder Verschlüsselung benötigt wird, muss dies im Vertrag enthalten sein.

RAS versus Internet VPN

RAS-Lösungen können durch einen VPN-Zugang ins Internet abgelöst werden, bei dem anstelle der vorherigen (Fern)-Wähltarife die lokalen Internet-Einwahlkosten anfallen. Die jeweiligen Kostenfaktoren zeigt Tabelle 2.

Tabelle 2 Kostenfaktoren bei RAS- versus VPN-Lösungen

Remote Access, RAS/NAS	VPN mit Internet-Zugang
RAS Hardware, Software in der/den Zentrale(n)	VPN Server/Gateway in der/den Zentrale(n)
Wählmodems an den Außenstandorten	VPN Client Software an den Außenstandorten
Arbeitszeit/Betriebsaufwand	Grundgebühr für VPN Zugang

Intranet versus Internet VPN

Bei einem Vergleich zwischen Intranet und Internet VPN zwischen mehreren Unternehmensstandorten sind Kostenaspekte zu berücksichtigen wie in Tabelle 3 dargestellt. Die entsprechenden Konzeptansätze sind in Bild 1 und Bild 2 gezeigt.

Tabelle 3 Kostenfaktoren bei Intranet versus Internet VPN

Intranet mit intern/extern Router	VPN mit Internet-Zugang
interner WAN Router	PN Server / Gateway in der/den Zentrale(n)
TK-Dienst (FR, SFV), insbes. für Fernverbindungen	VPN Gateway an den Außenstandorten
Multinationale Koordinierung von TK-Tarifen	Internet Zugang je Standort
ggf. Produktionsverluste aufgrund langer Umrüstzeiten bei Erweiterungsbedarf	Grundgebühr für VPN Zugang, ggf. Volumengebühr

Dial Up versus Internet VPN versus Mischkonzept

In einem Beispiel werden die drei Ansätze und resultierenden Kosten gegenübergestellt. Die Firma Aceme hat 900 Mitarbeiter. 523 Mitarbeiter, also 58% der Belegschaft müssen remote Zugang erhalten. Sie lassen sich in 315 Heimarbeiter, durchschnittlich 95 Benutzer auf Reisen und 113 Außendienst-Mitarbeiter unterteilen. Jeder Benutzertyp zeigt eine spezifische Nutzungszeit und Zugriffsverteilung im Nah- und Fernbereich, wie in Tabelle 4 zu sehen ist.

Tabelle 4 Nutzergruppen und Nutzungsprofile

User Typ	durchschnittliche Stunde / Woche	Anzahl User	Lokal-tarif	Fern-verb.
Heimarbeiter	2	315	5 %	85 %
verreiste Besucher	2	95	2 %	98 %
Außendienst	8	113	82 %	18 %

	Kosten / Monat		
	reines Dial-Up (DoV)	reines VPN	Hybrides DoV / DoD
monatliche Hardware Kosten	1.894	948	1.331
monatliche Pflege	570	284	399
monatliche Kosten Zentrale Telco (T1-Leitungen)	4.831	1.449	3.272
monatliche Fernverbindungskosten	23.308	0	0
monatliche Personalkosten (Help Desk etc.)	36.087	36.087	36.087
monatliche ISP-Kosten	0	34.102	8676
Summe der Zugangskosten bei direkter Einwahl	66.690	72.870	49.765

Tabelle 5 Kosten mit Dial up und VPN

Multiplizieren Sie nun die anteiligen Arbeitszeiten für lokalen und Fernzugriff mit den jeweiligen Benutzerzahlen, so ergeben sich 26% Fernzugriff und 76% Nahzugriff. Als übliche Näherung wird 1 Zugangsport je 10 Benutzer (1:10 Ratio) vorgesehen und eine Sammelnummer für Fernzugriffe eingerichtet, um die Ferntarifkosten zu senken. Als Invest-Amortisierung werden 36 Monate angesetzt und Help Desk Kosten eingeplant. Die Ergebnisse zeigt Tabelle 5.

Ähnliche Kostenvergleiche aus mehreren Projekten ergeben, dass sich zum aktuellen Zeitpunkt Dial up Lösungen und Internet VPN Lösungen nicht ausschließen sondern ergänzen. Eine Kombination von Dial up für Entfernungen im Nahbereich mit Internet VPN im Fernbereich ist vielfach kostenoptimiert betreibbar.

7. Einige Playerim IP / Internet VPN Dienstleistungs-Markt

Wenn Sie die Yankee Group für glaubwürdig halten, gehören UUNET und Genuity zu den Marktführern, beide mit Lösungen die auf VPN-Komponenten beim Kunden setzen. Infonet und Equant sind klassische Frame Relay Player. Überraschend hat sich AT&T zu dem am schnellsten wachsenden VPN Anbieter mit IP VPN Diensten gemausert. Besonders der IP-fähige Frame Relay Dienst (der in Wirklichkeit MPLS-basiert arbeitet) erhielt gute Noten.

MCI WorldCom betreibt einen MPLS-basierten IP VPN Dienst, ähnlich Qwest und Global One. Unter den neueren Providern verdienen SAVVIS und Qwest Beachtung, SAVVIS insbesondere wegen seines Hochkapazitäts-Backbone mit intelligenter Routing-Steuerung (in 2000 mehr als 100 Kunden mit jeweils 5 bis 20 Standorten). SAVVIS setzt z.B. Shasta / Nortel Komponenten in Nordamerika, Europa und Asien ein. Anbieter mit starkem Fokus auf IP VPNs und E-Commerce sind Pilot Network Services und Aventail.

Eine weitere Gruppe spezialisiert sich auf die optimierte Nutzung verschiedener Providernetze. Hierzu gehört z.B. InterNAP, die Verträge mit einer Reihe etablierter Netzprovider haben und mittels intelligentem Routing die Durchleitung unter Umgehung der Standard/Default-Zugangsrouter optimiert. CoreExpress betreibt einen MPLS Backbone mit Terabit Routern und Service Providern als Kunden (!). Jeder Service Provider hat eine spezielle Management-Ausrüstung, um SLA's Ende-zu-Ende sicherzustellen. SmartPipes betreibt eine Front End Lösung, mit der sich Netzzugänge schneller und effizienter abwickeln lassen als bisher bei VPN Diensten und Backlogs reduziert werden.

8. Hinweise für die VPN-Realisierung und den Umgang mit VPN Providern

Abschließend seien einige Anmerkungen für die Vorplanung zusammengefasst.

- Planen Sie die benötigte Anzahl an Einwahl-Ports oder die benötigte Anzahl paralleler Sessions (erste Näherung: 10:1 #Benutzer : #Ports oder #Sessions).

- Bestimmen Sie dann die Bandbreite je Tunnel bzw. je Port als worst case d.h. bei maximaler Parallelität.

- Klassifizieren Sie die Benutzer in Gruppen mit jeweils typischen Last- und Nutzungsprofilen, z.B.
  – Heimarbeiter
  – Außendienst
  – Mitarbeiter mit leitender Funktion, die verreisen
  – Mitarbeiter, die von zu Hause aus noch E-Mails und Paging-Nachrichten bearbeiten
  – Außenstellen mit mehreren Mitarbeitern etc.

- Führen Sie eine Standort-Analyse durch: Wo liegen die Standorte: Großstadt, Stadt, Land, (Wüste, Insel), europäisch, international? Wieviele Standorte sind anzuschließen? Wie verteilen sich die Standorte?

- Führen Sie eine up to date Datenbank mit gleichen Authentisierungs-Profilen für Dial up und VPN.

- Bei VPN und insbesondere Internet-Nutzung ist die Vertraulichkeit wichtiger als bei Dial up, daher ist insbesondere hier Verschlüsselung und der IPsec Tunnel Modus vorzuziehen.

Und hier noch einige Anmerkungen zur Projekt-Umsetzung:

1. Planen Sie reichlich Zeit für Testen / Pilotinstallation ein.

2. Schließen Sie Regress-Zahlungen bis hin zur Rückabwicklung in den Vertrag ein, falls Fertigstellungstermine nicht eingehalten werden.

3. Addieren Sie auf jede Lieferzeit-Zusage des Herstellers 50%, bei kleinen Herstellern 100%.

4. Bedenken Sie, dass es Klauseln gibt, nach denen vereinbarte Fertigstellungstermine hinfällig werden können, wenn "besondere Umstände" geltend gemacht werden können. Am übelsten ist "höhere Gewalt", davor rettet Sie gewissermaßen gar nichts.

5. Speichern Sie irgendwo in Ihrem Langzeitgedächtnis, dass Inter-ISP Verbindungen gelegentlich nicht funktionieren.

6. Lächeln Sie; es könnte schlimmer kommen.

7. Es wird schlimmer kommen.

8. Üben Sie sich in Galgenhumor.

Tipps für den VPN-Einsatz

Welche Produkte sind geeignet und was ist bei der Nutzung von VPN-Technologie oder VPN Diensten zu beachten, um die gewünschte Funktionalität mit Kostenersparnis zu kombinieren? Wichtige Aspekte sind insbesondere:

- Einsatz von Standardverfahren für Tunneling, Verschlüsselung und Authentisierung;
- Optionale Unterstützung von Kompression
- Bei Bedarf integrierte Routingfunktion (MPLS, BGPv4)
- Unterstützung von anderen Client/Server Protokollen außer IP soweit erforderlich, z.B. SNA und IPX
- Unterstützung von LAN- und WAN-Interfaces in der geforderten Konfiguration
- Unterstützung von full duplex für LAN Interfaces (aktuell typische Switchkonfiguration im LAN!)
- Unterstützung der geforderten WAN-Zugangsdienste wie Frame Relay, ATM, Dial Up ISDN, DSL, Wireless
- Ausreichender Durchsatz bei Nutzung einer oder mehrerer 2 Mbit-Verbindungen
- Unterstützung von Redundanz-Konfigurationen, Backup-Lösungen
- Flexible Skalierbarkeit auf mehr Standorte, andere Zugangsverfahren (DSL, ATM, ...) und höhere Zugangs-Kapazität
- Flächenabdeckung für alle gewünschten Standorte und Länder
- Unterstützung eines Basis-QoS z.B. mit TCP/UDP Port-Klassifizierung oder aktivem Setzen des DS Byte und Traffic Shaping; ggf. zusätzlich Unterstützung eines Policy Serverkonzepts
- Nachweis der Sicherheit gegen gängige bekannte Attacken
- Einfache Bedienbarkeit und Unterstützung von remote Management, insbesondere Verschlüsselung und Passwortschutz für remote Management, am besten über einen separaten VPN-Kanal
- Gute Monitoring und Logfunktionen, Möglichkeiten, SLA-Einhaltung durch den Provider zu kontrollieren
- Für Amortisationsrechnungen nicht nur Erstinvestition betrachten, sondern auch die laufenden Betriebskosten bei Einsatz eigenen VPN-Equipments berücksichtigen
- Genau prüfen, welche Funktionalität bei einem angebotenen VPN-Dienst wirklich vorhanden ist (Tunnel, Verschlüsselung, Certifikate, Durchsatz etc.)
- Doppelberechnung des Netz-Zugang beim VPN-Dienstangebot zurückweisen bzw. minimieren
- Detail-Rechnungen anfordern um versteckte Kosten zu erkennen
- Berichtswesen für VPN-Dienst bei Vertragsabschluss definieren und festlegen
- konstantes und deterministisches Leistungsverhalten prüfen
- Einhaltung der zugesagten Verfügbarkeiten prüfen

Fazit

VPNs werden als kostengünstige und sichere Alternative zu teuren Festverbindungs-Netzen und unsicheren Wähldiensten vermarktet. Mit welchen Dienstangeboten, ggf. welchen Dienst-Kombinationen die erreichbaren Kosteneinsparungen optimierbar sind, muss anhand Investkosten und laufender Betriebsaufwände im Vergleich zu den Gebühren herkömmlicher Dienste überprüft werden. Die Produktwahl ist sorgfältig zu untersuchen und auszutesten. Aktuell verfügbare Implementierungen sind sehr unterschiedlich und in Teilen proprietär. Ausgereifte insbesondere flächendeckende Angebote der ISPs und Netzbetreiber fehlen immer noch, ebenso wie erprobte Service Level Konzepte mit vereinbarter Dienstgütegarantie und hoher Skalierbarkeit.

A – D

A	AH	Authentication Header
	ATM	Asynchronous Transfer Mode
B	B2B	Business to Business
	B2C	Business to Customer
	BGP	Border Gateway Protocol
C	CBQ	Class Based Queueing
	CHAP	Challenge Handshake Authentication Protocol
	CIR	Comitted Information Rate
D	DMZ	Demilitarized Zone
	DoD	Data over Data
	DoV	Data over Voice
	DSL	Digital Subscriber Line

E –W

E	EAP	PPP Extensible Authentication Protocol
	ESP	Encapsulation Security Payload
F	FR	Frame Relay
I	IEEE	Institute for Electrical and Electronic Engineers
	IETF	Internet Engineering Task Force
	IKE	Internet Key Exchange
	IPsec	Internet Protocol Security
	ISA/KMP	Internet Security Association/Key Management Protocol
	ISDN	Integrated Services Digital Network (für USA: I Still Don't Know)
	ISP	Internet Service Provider
L	L2F	Cisco Layer-2 Forwarding Protocol
	L2TP	Layer-2 Tunneling Protocol
M	MD5	Message Digest 5
	MPLS	Multi-Protocol Label Switching
	MPPE	Microsoft Point-to-Point Encryption
N	NAT	Network Address Translator
	NAS	Network Access Server
	NSP	Network Service Provider
P	PAP	Password Authentication Protocol
	PAT	Port Address Translator
	PDN	Public Data Network
	POP	Point of Presence
	POTS	Plain Old Telephony Service
	PPP	Point-to-Point Protocol
	PPTP	Point-to-Point Tunneling Protocol
	PSTN	Public Switched Telephone Network
	PSU	Power Supply Unit
Q	QoS	Quality of Service
R	RADIUS	Remote Dial In User Service
	RAS	Remote Access Server
	RSA	Rivest, Shamir, Adleman (Verfasser des gleichnamigen Schlüsselverfahrens)
S	SFV	Standard-Festverbindung
	SHA	Secure Hash Algorithm
	SHS	Secure Hash Standard
	SLA	Service Level Agreement
	SMB	Small & Medium Business
	SSL	Secure Socket Layer
T	TACACS	Terminal Access Controller Access Control System
U	URL	Universal Resource Locator
V	VPN	Virtual Private Network
W	WFQ	Weighted Fair Queueing

ComConsult Certified Network Engineer

"Wir haben also auch noch Support für unser Projekt."

Stephan Schleibinger (23) wurde von Burda direkt vom Studium der Elektro- und Informationstechnik weg abgeworben und arbeitet jetzt bei der Burda Systems in der Netzwerktechnik. Der Netzwerk Insider sprach mit ihm unmittelbar nach seiner bestandenen Prüfung zum ComConsult Certified Network Engineer.

Insider: Wie kamen Sie zu ComConsult?

Stephan Schleibinger: Ich habe Elektro- und Informationstechnik studiert an der TU München. Ich hatte während des Studiums einen Nebenjob bei Burda und habe da das Netzwerk kennengelernt. Ich hab da dann den ersten Einblick ins Netzwerk bekommen und war total begeistert von meinen Kollegen, weil die so viel wissen. Ich habe dann letzten Jahr gemerkt, dass das für mich alles zu theoretisch ist, dass ich gerne in die Computerbranche wechseln würde. Ich wollte dann unbedingt auch im Netzwerkbereich weitermachen. Und weil die Uni mir kein Studium in dem Bereich anbieten konnte, außer so Randstudienbereiche wie Informatik, wo ich dann doch hätte umsteigen müssen, hab ich gesagt, okay, dann werde ich jetzt fest einsteigen im Netzwerkbereich.

Insider: Und dann haben Sie sich bei Burda beworben?

Stephan Schleibinger: Ich hab gesagt, ich fang hier an, wenn ich in den Netzwerkbereich darf. Und dann hat auch gleich mein Chef gesagt, dass ich mir einen Kurs aussuchen soll, der mir entsprechendes Know-how vermitteln kann. Ich hatte von meinen Kollegen gehört, dass ComConsult da eine sehr umfassende Ausbildung bietet und dass man mit dem Wissen da auch wirklich weiterkommt in dem Bereich, dass es nicht herstellerspezifisch ist, sondern dass alle Hersteller mit einbezogen werden und das man die generellen Netzwerkkentnisse sehr gut erlangt.

Insider: Und, hatten die Kollegen Recht?

Stephan Schleibinger: Ja, das kann ich nur bestätigen. Mittlerweile habe ich die Verantwortung für die Neuverkabelung von drei Häusern von Burda das neue Datennetz da aufzuziehen mit meinen beiden Kollegen, die auch die CCNE-Ausbildung machen und in Kürze die Prüfung ablegen werden. Wir zusammen

ComConsult Certified Network Engineer Stephan Schleibinger

müssen also die Häuser komplett neu verkabeln. Wir machen das schon auf CAT7-Basis auch auf Grund der Absprache mit der ComConsult Akademie was die Standard-Kabel betrifft. Auch mit der Messung der Kabel habe ich immer wieder Rücksprache gehalten mit ComConsult. Ich habe dann dem Referenten, der das Verkabelungs-Seminar* hält, gemailt und gefragt, wie die Norm ist und wie die aktuellen Messdaten sind, auf die man Wert legen sollte. Er hat mir dann Listen zugemailt, nach denen ich mich jetzt auch ziemlich richte. Das hat mir sehr weitergeholfen. Wir haben also auch noch ein Support für unser Projekt, das jetzt läuft.

Insider: Sie haben die Kurse ziemlich schnell durchgezogen.

Stephan Schleibinger: Ja, ich hab das sehr komprimiert gemacht, so schnell wie möglich. Ich habe im April den ersten Kurs gemacht und im Oktober den letzten. Ich hab also ein gutes halbes Jahr gebraucht. Und jetzt bin ich richtig glücklich, dass ich es geschafft hab.

Insider: Dann haben Sie für die Prüfungsvorbereitungen ja nicht viel Zeit gehabt.

Stephan Schleibinger: Dadurch dass ich durch den laufenden Betrieb ständig mit den Netzwerkproblemen konfroniert war, war das von der Vorbereitung her gar nicht so der Riesenaufwand für mich. Ich habe die Fragen einmal komplett durchgearbeitet an Hand der Bücher und der Unterlagen von ComConsult. Ich habe mir dann die meiner Meinung nach besten Antworten notiert, bin das vor der Prüfung nochmal durchgegangen und hab mich dann soweit relativ gut vorbereitet gefühlt, was sich in der Prüfung dann auch bestätigt hat.

Insider: Und warum waren Sie dann so nervös?

Stephan Schleibinger: Ich weiß nicht, ich bin ein Mensch, der generell vor Prüfungen ziemlich nervös ist. Besonders bei der mündlichen Prüfung. Bei der schriftlichen Prüfung konnte ich direkt loslegen. Ich hätte am liebsten zwei Seiten zu jedem Thema geschrieben, aber die Kunst ist dann sich auf die einzelnen Punkte festzulegen.

Insider: Es hat ja alles gut funktioniert. Schönen Dank.

* Der Referent ist Dipl.-Ing. Hartmut Kell, er hat seine Arbeitsschwerpunkte bei der ComConsult Beratung und Planung GmbH auf dem Gebiet der Netzwerk-Konzeptionierung. Im Bereich der Messtechnik der Lokalen Netzwerke hat er sich umfassendes Spezialwissen angeeignet. Sein Seminar "Verkabelungssysteme für Lokale Netze" basiert auf der Erfahrung einer Vielzahl aktueller Verkabelungsprojekte und deren Betrieb. Es führt methodisch vom aktuellen Stand der Technik bis zu den Leistungsmerkmalen zukünftiger Lösungen. Aktuelle Informationen über dieses Seminar finden Sie auf dem Web-Server der ComConsult unter www.comconsult-akademie.de

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Fehlersuche in lokalen Netzen für Einsteiger, 23.04. - 25.04.01 in der AGIT Aachen

Das Praxis-Seminar stellt wesentliche Hilfsmittel für die Netzwerk-Überwachung und Fehlersuche über Vorträge und Übungen vor, typische Problemsituationen werden simuliert und systematisch deren Beseitigung erarbeeitet.
Referenten: 8 Mitarbeiter der ComConsult Beratung und Planung GmbH Preis: EUR 1.790,--

TCP/IP und SNMP, 23. - 27.04.01 im Exelsior Hotel Berlin

Das Intensiv-Seminar vermittelt einen praxis-orientierten Einblick in den Aufbau und den Betrieb von heterogenen Netzen, die den Kommunikationsstandard TCP/IP und den Netzmanagement-Standard SNMP benutzen.
Referenten: Dipl.-Phys. Frank Breitschaft, Dipl.-Inform. Detlef Weidenhammer (GAI NetConsult) Preis: EUR 1.990,--

Moderne Datenkommunikation, 07.05. - 11.05.01 im Exelsior Hotel Berlin

Das Intensiv-Seminar vermittelt Techniken, Verfahren und Systeme der Datenkommunikation für Ein- und Umsteiger. Der Schwerpunkt liegt auf dem erfolgreichen Einsatz der Internet/Intranet-Technologien.
Referent: Dr. Franz-Joachim Kauffels Preis: EUR 1.990,--

Schirmung, Erdung, Potentialausgleich..., 14.05. - 15.05.01 im Holiday Inn Bonn

Das Seminar behandelt die scheinbar unerklärbaren Störerscheinungen in Netzwerken und im Betrieb elektronischer Geräte, die durch Wechselwirkungen mit der Elektroinstallation entstehen.
Referenten: Dipl.-Ing. Karl-Heinz Otto und Hans-Günter Hergesel Preis: EUR 990,--

Projekt-Management, 14. - 16.05.01 im Holiday Inn Bonn

In diesem Seminar lernen Projektleiter ein Projekt effektiv zu organisieren und überzeugend zu führen. Es basiert auf einem kreativen Mix aus Lehrvorträgen, Erfahrungsaustausch und praktischen Übungen.
Referent: Dr. Ralf Hillemacher Preis: EUR 1.590,--

IP-VPNs erfolgreich einsetzen, 14. - 16.05.01 im Holiday Inn Bonn

Das Seminar beschäftigt sich mit dem Home-Office-/Teleworker-Zugang, dem Unternehmens-WAN-Backbone, dem Filialnetzwerk und der Standort-Kopplung, denn VPNs stellen die wichtigste Weiterentwicklung im Bereich der Weitverkehrskommunikation dar.
Referenten: Dipl.-Inform. Andreas Meder, Dr. Behrooz Moayeri, ComConsult Beratung und Planung Preis: EUR 1.590,--

Verkabelungssysteme für Lokale Netze, 21. - 22.05.01 im Holiday Inn Bonn

Das Seminar basiert auf der Erfahrung einer Vielzahl aktueller Verkabelungsprojekte und deren Betrieb. Es führt methodisch vom aktuellen Stand der Technik bis zu den Leistungsmerkmalen zukünftiger Lösungen.
Referent: Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung Preis: EUR 1.290,--

IP-/DNS-Design für Windows 2000 Active Directory, 28. - 30.05.01 im Holiday Inn Bonn

Dieses Seminar behandelt in konzentrierter Form die Implementierungsgrundlagen aus dem IP-Bereich für Windows 2000 bzw. für das Active Directory. Dabei spielt DNS die Hauptrolle, wobei auch insbesondere die dynamische Verbindung zum DHCP betrachtet wird.
Referenten: Markus Holländer, Lars Kuhl, Michael van Laak, Frank Neunzig, ComConsult Beratung und Planung Preis: EUR 1.590,--

Switching-Technologien in LANs, 28. - 30.05.01 im Holiday Inn Bonn

Das Seminar vermittelt Teilnehmern mit vorhandenen Grundlagenkenntnissen den erfolgreichen Umgang mit Switching-Technologien sowie den methodischen Einsatz dieser Technologien.
Referent: Mathias Hein Preis: EUR 1.590,--

Anmeldung

Titel des Seminars _____

Name _____

Vorname _____

Termin _____

Firma, Abteilung _____

Position, Funktion _____

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Straße _____

PLZ, Ort _____

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**

Telefon _____

Fax _____

eMail _____

Unterschrift _____

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebrauchte Netzwerk-Komponenten

Die Spielregeln

Gebrauchte Netzwerk-Komponenten, die im Rahmen eines Redesigns ausgemustert werden, könnten einige Betriebe sehr gut gebrauchen. Hier wollen wir helfen. Wir bauen für unsere Kunden eine Handelsplattform für gebrauchte Netzwerk-Komponenten auf. Die Spielregeln: Sie melden uns, welche Produkte/Komponenten Sie anbieten/suchen mit Ihrer Preisvorstellung. Ihr Angebot wird in anonymer Form auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de und im Netzwerk Insider veröffentlicht. Interessenten melden sich per Mail, mit dem Fax-Formular (unten) oder über den Web-Server bei uns. Wir stellen den Kontakt zwischen Anbieter und Nachfrager her. Wir erhalten vom Verkäufer für diese Leistung 10% Provision auf den erzielten Kaufpreis. Davon stellen wir die Hälfte ausgewählten Schulen als Spende zum Aufbau ihres Internet-Zugangs oder ihres internen Netzwerks zur Verfügung. Der Kaufvertrag entsteht direkt zwischen Käufer und Verkäufer. Wir selber haften in keiner Form für die Qualität oder Nutzbarkeit der Komponenten.

Aktuelle Gebote und Gesuche

finden Sie in dieser Ausgabe vom **Netzwerk Insider** auf der nächsten Seite

Weitere Gebote und Gesuche

finden Sie auf dem Web-Server der ComConsult Akademie unter **www.comconsult-akademie.de**

Fax an 02408/955-399

☐ **Ich biete**

☐ ☐

Produkt/Komponente/Release/Software

Preisvorstellung

Ansprechpartner

Firma

Ort

Straße

Telefon, Fax

eMail

☐ **Ich suche**

☐ ☐

Produkt/Komponente/Release/Software

Preisvorstellung

Ansprechpartner

Firma

Ort

Straße

Telefon, Fax

eMail

☐ **Antwort auf Gesuch**

☐ ☐

Produkt/Komponente/Release/Software

Preisvorstellung

Ansprechpartner

Firma

Ort

Straße

Telefon, Fax

eMail

☐ **Antwort auf Gebot**

☐ ☐

Produkt/Komponente/Release/Software

Preisvorstellung

Ansprechpartner

Firma

Ort

Straße

Telefon, Fax

eMail

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebote

Adapter

Madge,TR-Karten ver. Typen (BM2, MK3, MK4, HSTR) alle PCI, 200, 60% d. Neupreises B1095

Concentrator

Token Ring, Rac 4001 Lan, Optics 12, Slot, 5 , DM 400,- B1014

Hub

LET36, 4 Stck., VS B1015

LE20N, 16 Stck., VS B1019

LE 180 XT, 4 Stck., VS B1020

LE140 XTN, 10 Stck., VS B1021

LE140 XT,12 Stck., VS B1022

NMAII, 1 Stck., VS B1023

LE10 C2, 2 Stck., VS B1024

LE15, 1 Stck., VS B1025

Repeater

Cabletron, Repeater-Module FOMIN, 5 Stck., DM 100,-- B1093

AI 3008SL 10 Base 2 Ethernet 8 Port Allied, 1Stck., DM 350,- B1096

Router

RSP2- Boardfür Cisco 75xx, 8MB on-board Flash, 64MB Memory, 20 MB PCMIA Flash, 1Stck., VS B1097

Sternkoppler

Hirschmann, ASGE mit diversen Interfacekarten wie: UYDE, CYDE, OYDE, BfOC, KTDE, TYDE, 35 Stck., DM 200,-- bis 800,-- B1026

Steuereinheit

IBM Token Ring / SNA IBM 3174, 25 Stck., DM 280,-- B1012

Switch/Brücke

Cisco, Catalyst 5000 Chassis mit 1x WS-X5009 (mit 2x 100 Base TX), 1x WS-5111 (12x 100 Base FX), 1x WS-5213 (12x 100 Base TX), 20MB Memory, V4.5 (7), 1 Stck., EUR 5000,-- B1010

Madge, Smart Token, Ring 12 Port, 5 Stck., DM 650,-- B1011

Cabletron 8 Port Ethernet Module for ATX 3E02-08-ATX, 1 Stck., $ 300,- B1016

Cabletron Enhanced ATX Packet Processing Engine 3X00-ATX, 1 Stck., $ 500,- B1017

Cabletron, 3C05-ATX Chassis, inkl. 1 Power Supply 3CPSM-R-ATX, 1 Stck., $ 300,- B1018

Cabletron 2-Port-Bridges,5 Stck., DM 20,-- B1094

Sonstige

Token Ring Einschübe für Rac 4001 12 port, Lobemodul 4283 Lan Optics, 20Stck., DM 400,-- bis 700,-- B1013

TR LWL Karten BKM 4521 850 Nm 1300 Nm Lan Optics, 10 Stck., DM 400,-- bis 700,-- B1077

Cabletron-Ersatz-Netzteil für MMAC-3, 8 Stck., DM 350,-- B1092

Gesuche

Adapter

IBM, Olicom, Token Ring Adapter PCI, 30 Stck., VS S1026

Concentrator

IBM, 8.230.013, 10 bis 50 Stck., DM 400,- S1030

Hub

3Com, SuperStack II Hub, TR, 24 Port UTP, 1 Stck., VS S1027

Prozessor

Intel, 450 oder 500 MHZ II, 1 Stck., DM 200,-- S 1028

Repeater

Madge, Smart Lam Plus UTP 55-50, 3 bis 6 Stck., DM 800,- - S1029