Virtuelle private Netze — weltweite LANs

Tobias Zimmer

Zusammenfassung

Virtuelle private Netze stellen eine neue Entwicklung auf dem Netzwerkmarkt dar. Obwohl die grundlegenden Techniken, auf denen sie beruhen, seit längerem bekannt sind und in verschiedenen Bereichen verwendet werden, sind sie eine Neuheit. Die vorliegende Arbeit beinhaltet eine Einführung in die Technik virtueller privater Netze, ihre Funktion und ihre praktischen Anwendung. Es werden Beispiele für den Einsatz dieser Netze angeführt und die zugrunde liegenden Protokolle und Standards erläutert, um einen Einblick in die vielfältigen Einsatzmöglichkeiten dieser neuen Technik zu gewähren und ihre Vorteile gegenüber klassischen Lösungen herauszustellen. Weiterhin werden auch die Probleme behandelt, zu denen es beim Einsatz virtueller privater Netzwerke kommen kann und wie diese in Zukunft gelöst werden könnten.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einführung

1.1 Was sind virtuelle private Netzwerke?

Ein virtuelles privates Netzwerk (Virtual Private Network, VPN) bietet die gleiche Funktionalität wie jedes andere private Netzwerk. Das heißt, die Daten, die zwischen den Stationen des Netzes ausgetauscht werden, sind sicher vor Angriffen von außen. Der Unterschied zu einem privaten lokalen Netz (Local Area Network, LAN) oder privaten Weitverkehrsnetz (Wide Area Network, WAN) besteht darin, daß das VPN die LAN-Struktur auf einem öffentlichen WAN, wie dem Internet, nachbildet. Hierzu werden virtuelle Verbindungen (Tunnel) verwendet (siehe Abschnitt 2.1).

1.2 Anwendungsgebiete für VPNs

Die Einsatzmöglichkeiten von VPNs entsprechen denen anderer privater Netzwerke, wobei einige Anwendungen erheblich vereinfacht werden und sogar neue hinzukommen, die mit klassischen Netzstrukturen nicht oder nur unter großem Aufwand zu realisieren sind, wie die

- Verbindung von LANs an verschiedenen Standorten eines Unternehmens;
- Anbindung von Außendienstmitarbeitern an interne Firmennetze;
- Erweiterung von Firmennetzen auf Zulieferer und Geschäftspartner (E-Commerce);
- sichere Datenübertragung für Online–Banking Kunden zum Bankrechner.

Mit der Konfiguration der VPNs für die hier angeführten Anwendungen und Beispielen für deren Einsatz beschäftigt sich Abschnitt 3.

1.3 Vorteile des Einsatzes von VPNs

Aus der Sicht des Anwenders liegen die Hauptvorteile des Einsatzes von VPNs in den, im Vergleich zu Direktverbindungen, geringen Unterhaltskosten und in der erheblich vereinfachten Administration des Gesamtnetzwerks. Hinzu kommt, daß das VPN mit geringem Aufwand beliebig erweiterbar ist und vorhandene LAN–Strukturen beim Aufbau übernommen werden können.

Das VPN ersetzt zum Beispiel teure angemietete Leitungen zwischen verschiedenen Standorten durch virtuelle Verbindungen, die bei Bedarf aktiviert werden können. So entstehen keine Kosten für ungenutzte Kapazitäten. Für die Anbindung von Außendienstmitarbeitern wird keine eigene Modem–Bank mit Remote Access Server für Einwahlverbindungen benötigt, da sich diese Mitarbeiter über einen beliebigen Einwahlknoten (Point of Presence, POP) ihres Internet-Dienstanbieters (Internet Service Providers, ISP) mit dem firmeneigenen Netz verbinden können. Für die Internet– und VPN–Anbindung können dieselben Hardware–Komponenten verwendet werden, wodurch der Administrationsaufwand und die Anschaffungskosten minimiert werden.

Zusammenfassend ergeben sich folgende Vorteile:

- geringere Unterhaltskosten als angemietete Leitungen;
- einfachere Administration;
- beliebige Erweiterbarkeit unter Erhaltung vorhandener Teilnetzstrukturen;
- eigene Modem–Bänke werden unnötig;
- vorhandene Internet–Hardware kann verwendet werden, um ein VPN aufzubauen.

Es wird geschätzt, daß der Einsatz von VPNs, gegenüber klassischen Lösungen, eine Kostenersparnis von 20–60% [Full98, Asce97] zur Folge hat.

1.4 Anforderungen

Der Einsatz von VPNs im professionellen Umfeld bedingt einige wichtige Anforderungen an die Dienstmerkmale dieser Netze. Im folgenden werden diese kurz zusammengefaßt.

Datensicherheit: Der Schutz der Daten auf ihrem Weg durch das Internet ist eine der Hauptaufgaben einer VPN–Implementierung. Dieser Schutz wird durch Techniken wie das Tunneln (Tunneling), Kapselung und Verschlüsselung realisiert.

Verfügbarkeit und Dienstgüte (Quality of Service, QoS): Die virtuellen Verbindungen eines VPN müssen bei Bedarf jederzeit zur Verfügung stehen. Anwendungen wie Netztelefonie und Videokonferenz stellen Qualitätsanforderungen an die Datenverbindungen in Bezug auf ihre Bandbreite und die Übertragungsgeschwindigkeit.

Kompatibilität: Ein VPN sollte mit den vorhandenen Anwendungsprogrammen des Benutzers kompatibel sein, um Neuanschaffungen und das Erlernen neuer Programme zu vermeiden. Das heißt, die Implementierung sollte für den Kunden möglichst transparent geschehen.

Adressierung: Die Adressierung innerhalb eines VPN sollte unabhängig von Internet–Adressen sein, da sonst eine komplette Neukonfiguration aller angeschlossenen Teilnetze in den meisten Fällen unumgänglich wäre.

Standards: Die Implementierungen von VPNs sind zur Zeit noch sehr herstellerspezifisch. Standards existieren nur für einzelne Komponenten, aber noch nicht für vollständige VPN–Implementierungen, was für den Anwender, zum Beispiel bei einem Wechsel seines ISPs, zu Problemen führen kann.

Wie diese Anforderungen bei der Implementierung von VPNs umgesetzt werden, zeigt Abschnitt 2.

2 Technische Grundlagen von VPNs

Dieser Abschnitt behandelt die Techniken, Protokolle und Standards, die der Implementierung von VPNs zugrunde liegen und zeigt, wie mit diesen den Anforderungen aus Abschnitt 1.4 Rechnung getragen wird.

2.1 Tunneling

Das Tunneling oder Kapselung ist eine Technik, die es erlaubt, beliebige Datenpakete aus einem LAN über ein anderes Netzwerk zu verschicken. Dabei spielt die Adressierung und das im LAN verwendete Übertragungsprotokoll keine Rolle. Das heißt, durch das Tunneling ist es möglich, zwei oder mehrere LANs transparent über ein WAN zu koppeln (siehe Abbildung 1).

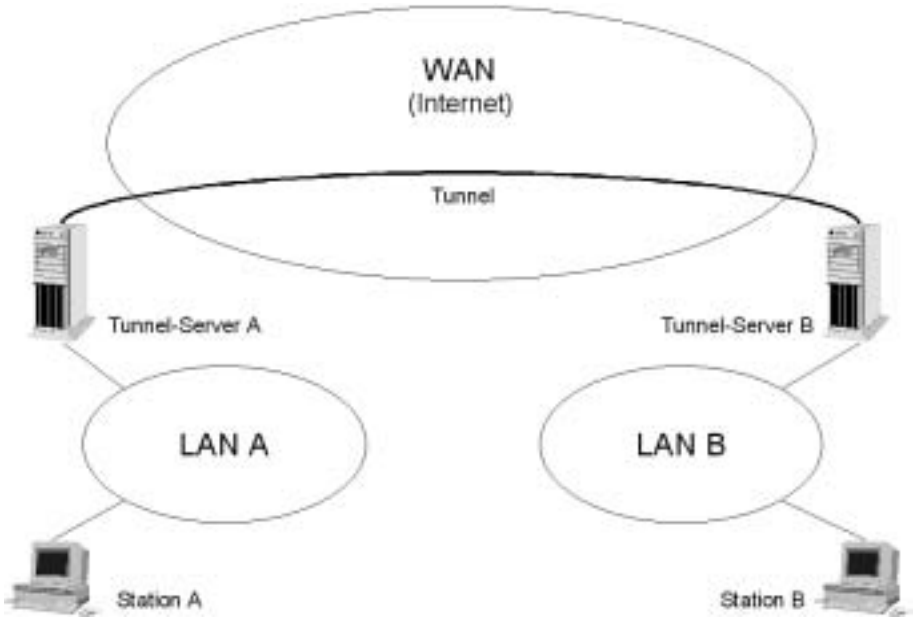

Abbildung 1: Koppelung von zwei LANs durch einen Tunnel

Tranzparenz bedeutet hierbei, daß die kommunizierenden Stationen in den verbundenen LANs nicht mit der Verwaltung und dem Aufbau des Tunnels betraut sind. Diese Aufgabe wird in jedem LAN von einem extra Tunnel-Server übernommen. Die Stationen in den LANs arbeiten so, als ob sie alle an einem einzigen LAN angeschlossen wären.

IP-Tunneling über das Internet beruht darauf, daß dem zu transportierenden Paket ein neuer IP–Kopf vorangestellt wird (IP in IP, RFC 2004 [Inte99]). Dieser Kopf wird in einem Server des LANs oder des ISPs erzeugt, der den Ausgangspunkt des Tunnels bildet. Der Kopf enthält als Quelladresse die Adresse dieses Rechners und als Zieladresse einen Server, der den Endpunkt des Tunnels bildet und das transportierte Paket wieder entpackt, also den Tunnel–Kopf entfernt. Dieses Paket wird dann wie gewohnt im Ziel–LAN seinem Empfänger zugestellt.

Der Tunnel verhält sich also wie eine bidirektionale Direktverbindung zwischen den beiden Tunnel–Servern.

Das Tunneling–Verfahren ist in Schicht 3 des ISO/OSI–Basisreferenzmodells angesiedelt. Dadurch stellt es selber keine Zugriffskontrollmechanismen zur Verfügung. Es bildet aber die Grundlage für einige Schicht–2–Protokolle, die diese Mechanismen implementieren (siehe Abschnitt 2.2).

Ein erster Standard für das Tunneling ist Generic Routing Encapsulation (GRE), RFC 1701 und RFC 1702 [Inte99]. Dabei handelt es sich um eine Richtlinie, wie die Tunnel–Pakete aufgebaut sein sollen.

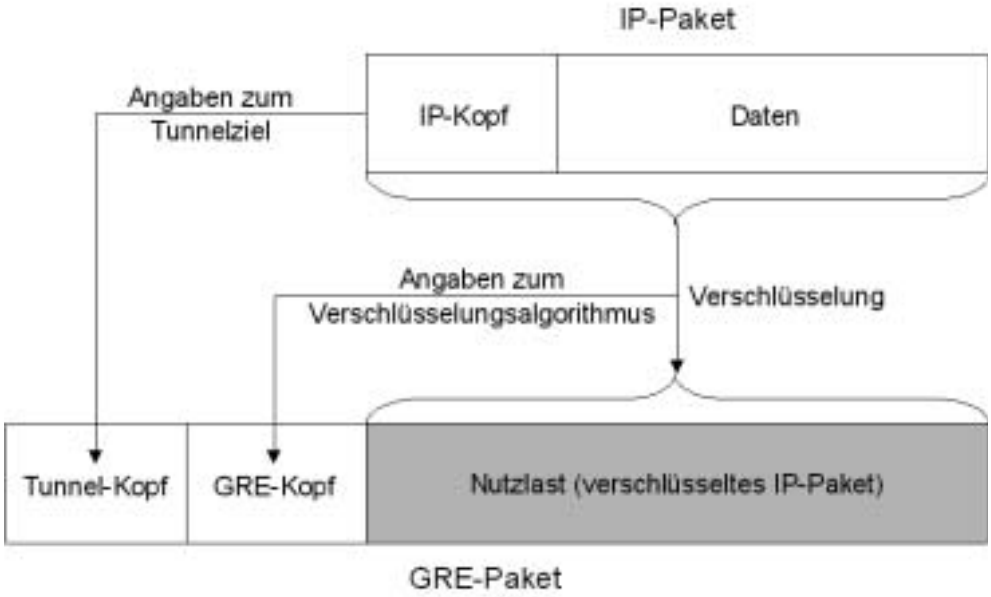

Abbildung 2: Aufbau eines GRE–Paketes zum Transport von IP–Paketen

In einem GRE-Paket werden drei Abschnitte unterschieden: ein Tunnel–Kopf, der das Tunnelziel enthält, ein GRE–Kopf, der Informationen über das verwendete Tunnel–Protokoll und Verschlüsselungsalgorithmen enthält, und die Nutzlast (Payload), also das zu transportierende LAN–Paket. Abbildung 2 zeigt den Aufbau eines solchen GRE–Paketes. Als Beispiel ist hier die Kapselung eines IP–Paketes gewählt. Mit GRE–Paketen lassen sich aber auch beliebige andere Netzwerkprotokolle tunneln.

2.2 PPTP, L2F und L2TP

Die Protokolle, die in diesem Abschnitt vorgestellt werden, arbeiten auf Schicht 2 des ISO/OSI–Basisreferenzmodells. Somit sind sie in der Lage Zugriffskontrollmechanismen bereit zu stellen, die eine Sicherung des Datenverkehrs in einem VPN ermöglichen.

Das Point–to–Point Tunneling Protocol (PPTP) [Micr98] das von Microsoft und anderen führenden Unternehmen der Netzwerkbranche entwickelt wurde, wurde 1996 der Internet Engineering Task Force (IETF) als Standardprotokoll für das Internet–Tunneling vorgeschlagen [Full98]. PPTP ist eine Erweiterung des Point–to–Point Protocol (PPP). PPTP kapselt PPP–Pakete in IP-Paketen, so können Protokolle wie IP, IPX und NetBEUI über das Internet getunnelt werden. Für die Zugangskontrolle werden das Password Authentification Protocol (PAP) und das Challenge Handshake Protocol (CHAP) verwendet. Als Verschlüsselungsalgorithmen dienen die Rivest´s Cipher 4 (RC4) und der Data Encryption Standard (DES) mit Schlüsseln zwischen 40 und 128 Bit Länge [Jach97].

PPTP ermöglicht also den Aufbau eines sicheren Tunnels, in dem die Daten verschlüsselt transportiert werden. Da PPTP mit PAP und CHAP auch einen gesicherten Verbindungsaufbau und Authentifizierung unterstützt, kann es sowohl auf der Seite eines ISP, zur Verbindung von LANs, als auch auf Anwenderseite zur Anbindung von mobilen Rechnern, verwendet werden. Dabei kann der Anwender eine PPP–Verbindung zu seinem ISP aufbauen, die noch nicht gesichert ist. Dann wird entweder der Tunnel vom ISP aufgebaut, wenn dieser PPTP unterstützt, oder der Anwender kann, wenn PPTP auf seinem eigenen

Rechner installiert ist, den Tunnel selbst aufbauen. Nach erfolgreicher Initialisierung des Tunnels nimmt PPTP die Quellpakete entgegen, verschlüsselt sie und gibt sie dann gemäß der GRE (siehe Abschnitt 2.1) weiter.

Ein PPTP–Paket setzt sich aus vier Schichten zusammen. Die oberste Schicht bildet ein Zustellungs–Kopf, der aus dem Netzwerkprotokoll des WAN besteht, über das das VPN aufgebaut wird. Darauf folgt als zweite Schicht ein IP–Kopf, der grundlegende Informationen über das IP–Datagramm enthält, wie die Paketlänge und die Absender– und Empfängeradresse. Die dritte Schicht enthält einen GREv2–Kopf. GREv2 stellt eine für PPTP entwickelte Erweiterung des GRE–Kopfes dar. Er enthält Informationen über die Art der Pakete, die gekapselt wurden und PPTP spezifische Daten über die Verbindung zwischen dem Client und dem Server. Die letze Schicht, das Nutzlast–Datagramm, enthält die eigentlichen Datenpakete. Im Fall von PPP sind das die PPP–Pakete, die zwischen Client und Server ausgetauscht werden. In diesen PPP–Paketen befinden sich dann die zu transportierenden IP–, IPX– oder NetBEUI–Pakete. [ScWE98] Zur Veranschaulichung zeigt Abbildung 3 die aktiven Protokollschichten während einer PPTP–Verbindung.

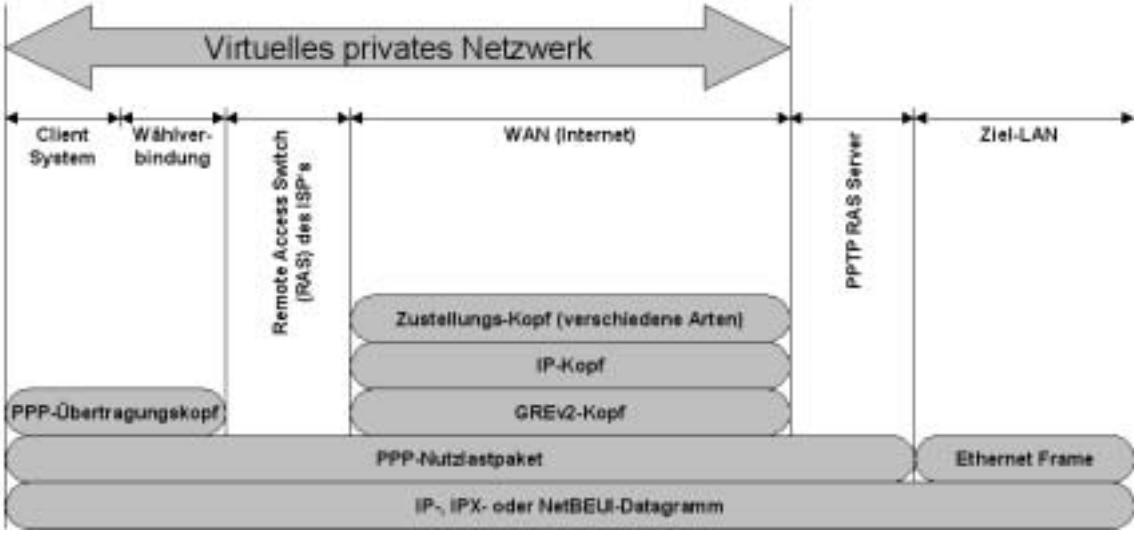

Abbildung 3: Aktive Protokollschichten während einer PPTP–Verbindung

Das Layer 2 Forwarding (L2F) von der Firma Cisco Systems stellt ein ähnliches Protokoll dar, das mit PPTP die Grundlage für das Layer 2 Transport Protocol (L2TP) eine Weiterentwicklung beider Systeme bildet [Aven98]. L2F unterstützt verschiedene Protokolle und mehrere unabhängige, parallele Tunnel. Die Benutzeridentifizierung ist allerdings etwas schwächer als bei PPTP und eine extra Verschlüsselung der Daten ist nicht vorgesehen [Cisc96].

L2TP [Cisc98b] unterscheidet sich nur in wenigen Punkten von PPTP. Zum einen ist hier zu nennen, daß L2TP, wie das L2F, mehrere Tunnel unterstützt, zum anderen liegt die Kontrolle über den Endpunkt eines Tunnels nicht wie bei PPTP beim Anwender, sondern wird vom ISP vorgegeben. Eine ausführliche Erläuterung der Unterschiede zwischen PPTP und L2TP findet sich in [FeHu98].

2.3 IPSec

IP Security (IPSec) ist eine neuere Technik, die PPTP langfristig als VPN-Standard ablösen soll, da sie ein höheres Maß an Sicherheit als PPTP garantieren kann. IPSec arbeitet auf IPv4 und soll fester Bestandteil von IPv6 werden. Bei IPSec handelt es sich um ein Paket von Protokollen (RFC 1825 – 1829) [Cisc98a, Inte99], die für Authentifizierung, Datenintegrität, Zugriffskontrolle und Vertraulichkeitsbelange innerhalb des VPN zuständig sind. IPSec besitzt zwei verschiedene Betriebsmodi: den Transportmodus und den Tunnelmodus.

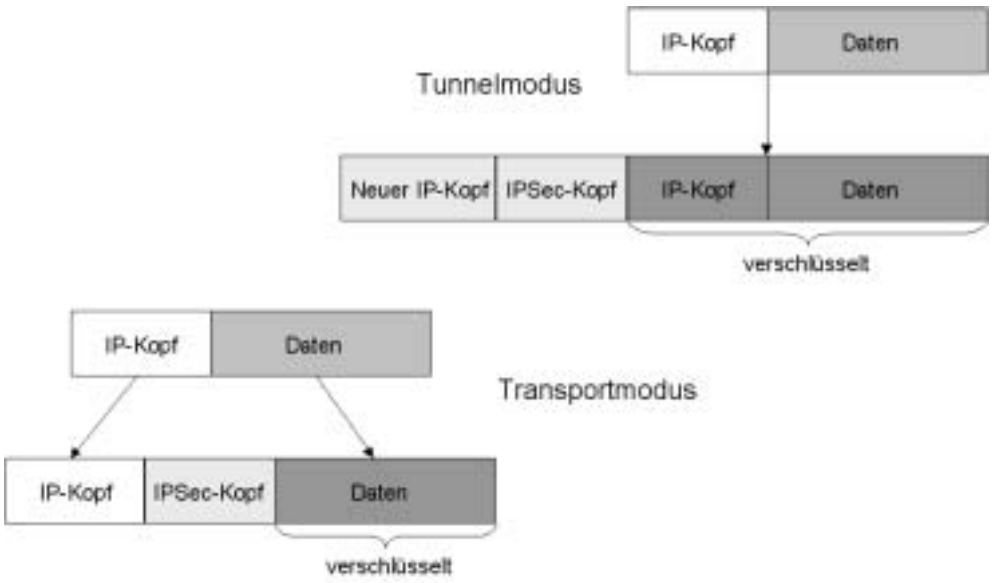

Abbildung 4: Aufbau von IPSec–Paketen in den verschiedenen Betriebsmodi

Transportmodus: Im Transportmodus verschlüsselt IPSec nur den Datenteil des zu transportierenden IP–Paketes. Der Original–IP–Kopf bleibt dabei erhalten und es wird ein zusätzlicher IPSec–Kopf hinzugefügt (siehe Abbildung 4). Der Vorteil dieser Betriebsart ist, daß jedem Paket nur wenige Bytes hinzugefügt werden. Dem gegenüber steht, daß jede Station im VNP IPSec beherrschen muß, was eine Neukonfiguration von bestehenden Netzen nötig macht. Außerdem ist es für Angreifer möglich, den Datenverkehr im VNP zu analysieren, da die IP–Köpfe nicht modifiziert werden. Die Daten selbst sind aber verschlüsselt, so daß man nur feststellen kann, welche Stationen wieviele Daten austauschen, aber nicht welche Daten.

Tunnelmodus: Im Tunnelmodus wird das komplette IP–Paket verschlüsselt und mit einem neuen IP–Kopf und IPSec–Kopf versehen. Dadurch ist das IPSec–Paket größer als im Transportmodus. Der Vorteil besteht hier darin, daß in den LANs, die zu einem VPN verbunden werden sollen, je ein Gateway so konfiguriert werden kann, daß es IP–Pakete annimmt, sie in IPSec–Pakete umwandelt und dann über das Internet dem Gateway im Zielnetzwerk zusendet, das das ursprüngliche Paket wiederherstellt und weiterleitet. Dadurch wird eine Neukonfiguration der LANs umgangen, da nur in den Gateways IPSec implementiert sein muß. Außerdem können Angreifer so nur den Anfangs– und Endpunkt des IPSec–Tunnels feststellen.

Wie Abbildung 4 zeigt, wird der IPSec–Kopf hinter dem IP–Kopf eingefügt. Er kann zwei Komponenten enthalten, die einzeln, unabhängig voneinander oder zusammen eingesetzt

werden können: den Authentifizierungskopf (Authentification Header, AH) und den Encapsulating Security Payload (ESP). Der AH sichert die Integrität und Authentizität der Daten und der statischen Felder des IP–Kopfes. Er bietet jedoch keinen Schutz der Vertraulichkeit. Der AH benutzt eine kryptographische Hashfunktion (keyed–hash function) und keine digitale Signatur, da diese Technik zu langsam ist und den Datendurchsatz im VPN stark reduzieren würde. Der ESP schützt die Vertraulichkeit, die Integrität und Authentizität von Datagrammen. Er schließt aber die statischen Felder des IP–Kopfes bei einer Integritätsprüfung nicht ein.

IPSec verwendet das Diffie–Hellman Schlüsselaustauschverfahren zur Identitätsprüfung. Die benutzten kryptographischen Hashfunktionen sind unter anderem HMAC, MD5 und SHA. Als Verschlüsselungsalgorithmen dienen zum Beispiel DES und IDEA, Blofish und RC4. Weiterführende Informationen und genaue Beschreibungen dieser Verfahren finden sich in [Jach97].

2.4 SOCKS v5

SOCKS v5 ist eigentlich das von der IETF eingeführte Standardprotokoll zum sicheren Passieren einer Firewall. In Kombination mit der Secure Socket Layer (SSL) bildet es die Grundlage für den Aufbau hochsicherer VPNs, die mit jeder Firewall kompatibel sind [Aven98].

SOCKS v5 arbeitet auf Schicht 5 des ISO/OSI–Basisreferenzmodells. Aus diesem Grund bietet es weit bessere Zugriffskontrollmöglichkeiten als Protokolle, die auf tieferen Schichten arbeiten, da es mehr Informationen über die laufenden Anwendungen zur Verfügung hat (siehe Abbildung 5).

Abbildung 5: Einordnung der VPN–Protokolle im ISO/OSI–Basisreferenzmodell

SOCKS v5 identifiziert einzelne Benutzer und leitet den gesamten Datenverkehr über eine Firewall. So ist es möglich, die Zugriffsrechte innerhalb des VPN für jeden Benutzer individuell zu konfigurieren, ohne neue Anwendungen extra anpassen zu müssen.

Durch ihre Ansiedlung in Schicht 5 des ISO/OSI–Basisreferenzmodells sind SOCKS v5 und SSL die einzigen Protokolle, die mit VPN–Protokollen niedrigerer Schichten zusammenarbeiten können.

Nachteile des Einsatzes von SOCKS v5 sind die geringere Geschwindigkeit, da alle Daten eine Firewall passieren müssen, und die Notwendigkeit entsprechender Programme auf jedem Rechner im VPN, die einen Verbindungsaufbau durch die Firewall ermöglichen.

2.5 RADIUS (Remote Authentication Dial–In User Service)

RADIUS (RFC 2058, RFC 2059) [Cisc97, Inte99] ist kein VPN–Protokoll im eigentlichen Sinne, sondern ein zusätzlicher Dienst, der die Verwaltung und Sicherung von Wählzugängen zu einem VPN erleichtert und verbessert [Davi98]. Den Aufbau eines VPN mit RADIUS–Servern zeigt Abbildung 6. RADIUS arbeitet mit einer Client–/Server–Architektur, wobei RADIUS den Server darstellt und der ISP–Server oder der Firmen–Server den Client.

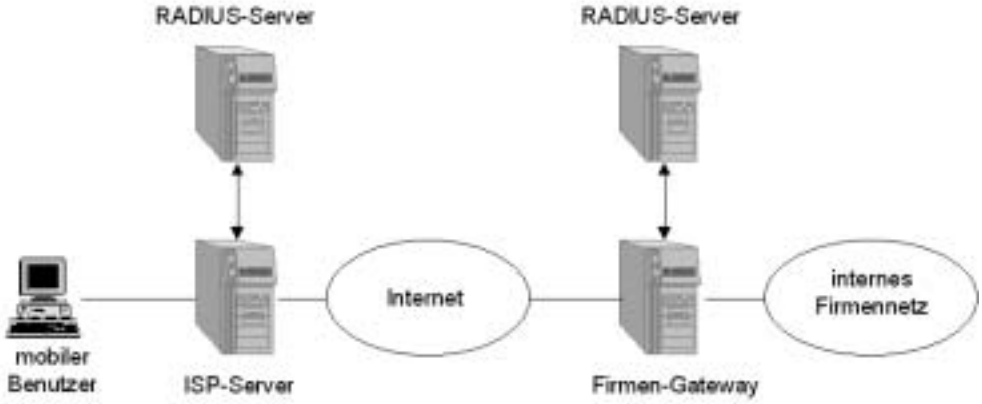

Abbildung 6: Aufbau eines VPN mit RADIUS–Servern

RADIUS stellt Mechanismen zur Benutzeridentifizierung über PAP und CHAP, zur Zugriffskontrolle über eine eigene RADIUS–Datenbank und zur Verwaltung von dynamischen IP–Adressen bereit [Asce97]. Zur Kommunikation zwischen dem RADIUS–Server und dem ISP–Server wird das User Datagram Protocol (UDP) benutzt [Cisc97]. Das Format der RADIUS–Pakete ist in RFC 2058 [Inte99] beschrieben.

RADIUS wird im allgemeinen in Kombination mit anderen VPN–Protokollen wie zum Beispiel L2F eingesetzt. Eine ausführliche Beschreibung der Zusammenarbeit dieser beiden Protokolle findet sich bei [Cisc97].

3 Konfigurationen von VPNs

Dieser Abschnitt befaßt sich mit der Konfiguration und dem Aufbau von VPNs für verschiedene Anwendungsbereiche. Anhand von Beispielen soll gezeigt werden, welche Netzwerkstrukturen sich für welche Einsatzgebiete besonders gut eignen. Ferner werden die Einsatzmöglichkeiten der in Abschnitt 2 beschriebenen Protokolle unter Einbeziehung des Sicherheitsaspektes angeführt.

3.1 End–to–End–VPNs

End–to–End–VPNs stellen eine direkte Verbindung zwischen mehreren Arbeitsrechnern dar. Eingesetzt werden kann diese Art der VPNs zum Beispiel, um Bankkunden über das Internet sicher mit einem Buchungsrechner zu verbinden, oder um mehreren Wissenschaftlern an verschiedenen Standorten die Arbeit an einem gemeinsamen Projekt zu erleichtern (siehe Abbildung 7).

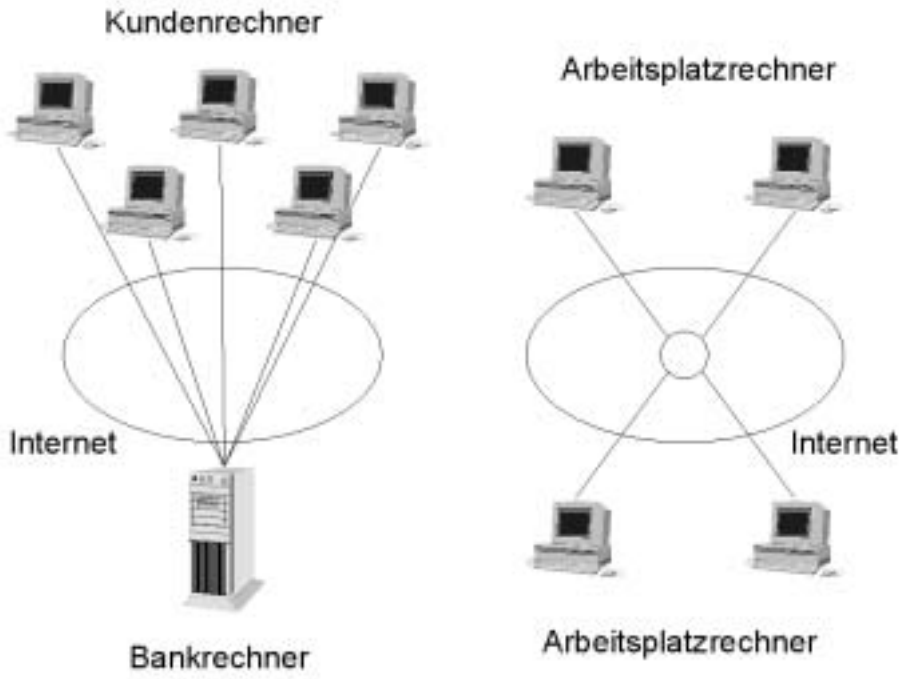

Abbildung 7: Zwei Beispiele für den Aufbau von End–to–End–VPNs

Zu beachten ist hierbei, daß auf jedem der an das VPN angeschlossenen Rechner ein entsprechendes VPN–Protokoll installiert sein muß, da die Arbeitsrechner direkt untereinander und nicht über zwischengeschaltete VPN–Server verbunden werden.

Besonders geeignete Protokolle für den Aufbau von End–to–End–VPNs sind L2F, L2TP und IPSec, wobei IPSec für Anwendungen, die ein Höchstmaß an Sicherheit erfordern, am besten geeignet ist. Bei dieser Konfiguration ergibt sich aber immer das Problem der Verwaltung des Netzwerks. Im Fall der Online–Banking–Anwendung wird die Verwaltung vom Bankrechner übernommen, da keine Notwendigkeit des Datenaustausches einzelner Kunden untereinander besteht. Im Fall der verteilten Projekte dagegen muß jede der angeschlossenen Stationen die Zugriffe von allen anderen Rechnern selbst verwalten, da der Austausch von Daten der einzelnen Projektteilnehmer untereinander möglich sein muß.

3.2 Site–to–Site–VPNs

Site–to–Site–VPNs stellen die klassische VPN–Variante dar. Hierbei werden mehrere LANs an verschiedenen Standorten verbunden. Diese Konfiguration eignet sich zum Beispiel, um Firmennetze zusammenzuschließen (Abbildung 8), Krankenhäuser zum Datenaustausch zu verbinden, oder Forschungsnetze mit mehreren Forschungsgruppen aufzubauen.

Bei Site–to–Site–VPNs unterscheidet man zwischen Intranet VPNs und Extranet VPNs, die verschiedenen Sicherheitsanforderungen genügen müssen.

3.2.1 Intranet VPNs

Unter Intranet VPNs versteht man Netze, die zur Erweiterung interner LANs dienen. Ein typisches Beispiel ist die in Abbildung 8 gezeigte Anwendung. Hierbei wird davon

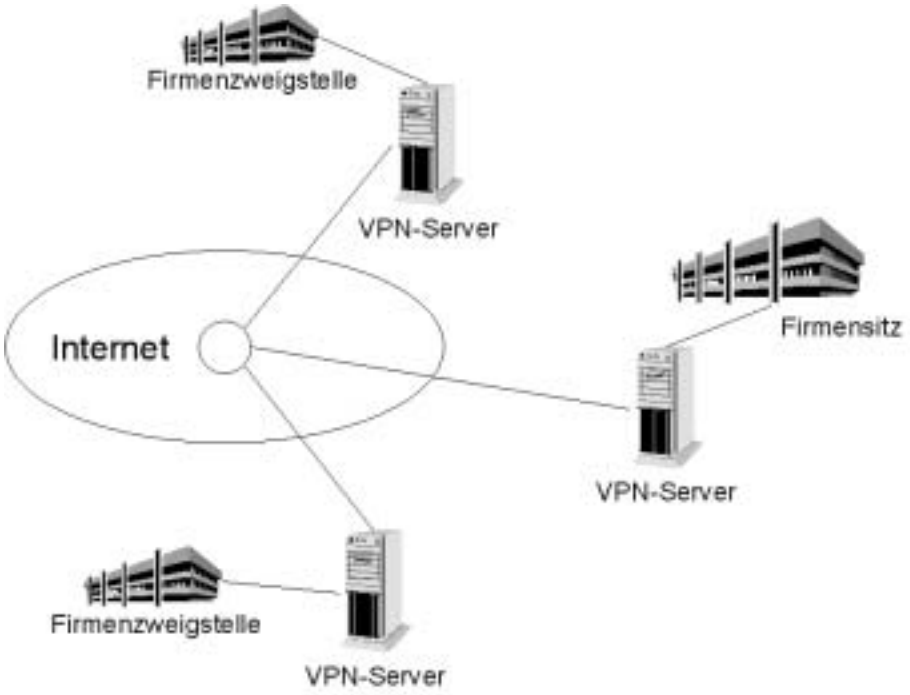

Abbildung 8: Site–to–Site–VPN zur Verbindung verschiedener Firmenstandorte

ausgegangen, daß jede der angeschlossenen Parteien den anderen voll vertraut, und daß alle Ressourcen im Netz allen Parteien zugänglich sein sollen. Daher wird bei diesem VPN–Typ, bei einem Mindestmaß an Sicherheit, großer Wert auf die Geschwindigkeit gelegt. Um die Datensicherheit zu erhöhen, können Zugriffsbeschränkungen auf Benutzerebene eingesetzt werden.

Als Protokoll kann hier zum Beispiel IPSec im Transportmodus eingesetzt werden. Dabei sind die transportierten Daten auf ihrem Weg durch das Internet durch eine Verschlüsselung geschützt und es werden nur wenige zusätzliche Byte für den IPSec–Kopf benötigt.

3.2.2 Extranet VPNs

Bei Extranet VPNs legt man im Vergleich zu Intranet VPNs weit größeren Wert auf die Sicherheit. Extranet VPNs werden zum Beispiel eingesetzt, um das interne Netzwerk einer Firma mit den Netzen von Geschäftspartnen und Zulieferern zu verbinden. Hierbei muß das VPN gewährleisten, daß jeder Teilnehmer nur auf die für ihn bestimmten Ressourcen Zugriff erlangen kann.

Das Datenaufkommen in Extranet VPNs ist im allgemeinen auch geringer als in Intranet VPNs, so daß man zur Realisierung ohne weiteres Lösungen einsetzen kann, die bei geringerer Geschwindigkeit ein Höchstmaß an Sicherheit bieten. Hierzu kann SOCKS v5 und SSL verwendet werden, da diese Kombination in Verbindung mit einer geeigneten Firewall auch Kontrolle über die Zugriffe einzelner Anwendungen erlaubt.

3.3 End–to–Site–VPNs

End–to–Site–VPNs oder Remote–Access VPNs dienen in erster Linie zur Anbindung von Außendienstmitarbeitern an ein internes Firmennetz. Eine solche Konfiguration zeigt Abbildung 9. Der Hauptvorteil eines solchen Netzes besteht darin, daß sich die Mitarbeiter über einen beliebigen POP des ISPs der Firma in das Netz einwählen können. Dadurch können die meist sehr hohen Kosten für Fernverbindungen reduziert werden, und das Unternehmen ist nicht gezwungen, eigene Modem–Bänke zu unterhalten und zu administrieren.

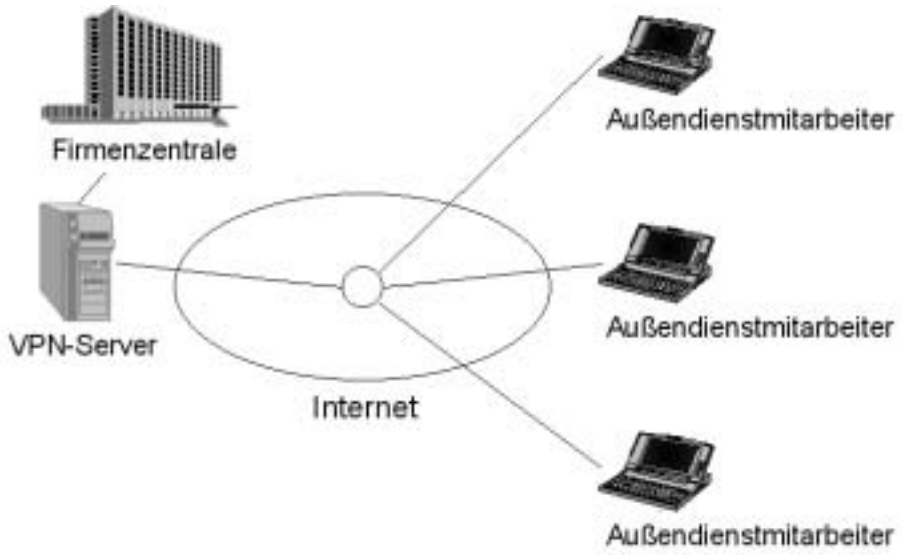

Abbildung 9: End–to–Site–VPN zur Anbindung von mobilen Mitarbeitern an ein Firmennetz

Für den Aufbau von End–to–Site–VPNs eignen sich im besonderen adressunabhängige VPN–Protokolle wie PPTP, da der Großteil der ISPs mit dynamischen IP–Adressen arbeitet. Auf Seiten der Sicherheit wird bei diesem VPN–Typ großer Wert auf die Identifizierung der einzelnen mobilen Mitarbeiter gelegt, um das Firmennetz gegen Angriffe Dritter abzusichern. Hierzu kann ein RADIUS–Server verwendet werden, der dann unabhängig vom benutzten VPN–Protokoll eine zusätzliche Benutzeridentifizierung anhand einer eigenen Datenbank vornehmen kann. Alternativ ist auch hier eine Konfiguration mit SOCKS v5 in Kombination mit einem solchen RADIUS–Server vorstellbar.

4 Ausblick

VPNs versetzen Unternehmen in die Lage, auf einfache und kostengünstige Weise Netzwerke aufzubauen, bestehende Netze zu erweitern und Außendienstmitarbeiter anzubinden und dabei bestehende WANs wie das Internet zu nutzen. VPNs stellen eine billigere Alternative zu klassischen Wählleitungen dar und vereinfachen so die Administration von Netzwerken, da sie die sonst nötigen Modem–Bänke ersetzen können.

Aber trotz all dieser Vorteile können die Sicherheitsfragen, die diese neuen Netze aufwerfen nicht unbeachtet bleiben. Bei einem Datenaustausch über ein öffentliches Netz, wie dem Internet, besteht immer die Gefahr von Angriffen. Es ist also immer nötig, die Daten zu verschlüsseln und die Zugangspunkte zu den VPNs abzusichern.

Hier zeigt sich, wo zur Zeit noch die Schwächen der bestehenden VPN–Implementierungen liegen. Eine Betrachtung der auf dem Markt befindlichen Protokolle erweckt den Eindruck, daß jeder Hersteller seine eigenen Verschlüsselungsalgorithmen, Schlüsselaustausch– und Benutzeridentifizierungsverfahren verwendet. Die Kompatibilität scheint dabei unbeachtet zu bleiben. Und tatsächlich ist diese Inkompatibilität der Systeme das Argument, das heute viele Unternehmen vom Einsatz moderner VPN–Lösungen abhält.

Die aussichtsreichsten Anwärter als VPN–Standards sind PPTP und IPSec. Viele Experten bescheinigen vor allem IPSec beste Zukunftschancen im Hinblick auf die bevorstehende Einführung von IPv6.

Literatur

[Asce97] Ascend Communications INC. Virtual Private Networks Resource Guide. Internet, http://www.ascend.com, 1997.

[Aven98] Aventail Corporation. Making Sense of Virtual Private Networks. Internet, http://www.aventail.com, September 1998.

[Cisc96] Cisco Systems. Solutions for Virtual Private Dialup Networks. Internet, http://www.cisco.com, 1996.

[Cisc97] Cisco Systems. Cisco IOS Technologies: RADIUS Support in Cisco IOS Software. Internet, http://www.cisco.com, 1997.

[Cisc98a] Cisco Systems. IPSEC White Paper. Internet, http://www.cisco.com, 1998.

[Cisc98b] Cisco Systems. Layer Two Tunnel Protocol (L2TP). Internet, http://www.cisco.com, 1998.

[Davi98] I. Davies. An Introduction to Virtual Private Networks. Internet, http://www.cs.uct.ac.za/home/idavies/Security/Security.html, April 1998.

[FeHu98] Paul Ferguson und Geoff Huston. What is a VPN? Internet, http://www.employees.org:80/ ferguson/vpn.pdf, April 1998.

[Full98] Fullerton University. Virtual Private Networks. Internet, http://amir.fullerton.edu/msis410/Projects/Group12/vpnpaper.htm, 1998.

[Inte99] Internet Engineering Task Force. Homepage der Internet Engineering Task Force. Internet, http://www.ietf.org, 1999.

[Jach97] Jörn Jachalsky. Untersuchung kryptografischer Verfahren in der TCP/IP-Protokollarchitektur. Studienarbeit, Universität Hannover Lehrgebiet Rechnernetze und Verteilte Systeme, http://www.rvs.uni-hannover.de/arbeiten/studien/sa-jacha.html, April 1997.

[Micr98] Microsoft INC. PPTP and Implementation of Microsoft Virtual Private Networking. Internet, http://www.microsoft.com/windows/common/nrpptp.htm, 1998.

[ScWE98] Charlie Scott, Paul Wolfe und Mike Erwin. *Virtual Private Networks.* O´Reilly. 1. Auflage, März 1998.