VPNs

Tom Gehring
gehring@foo.fh-furtwangen.de

Torben Nehmer
torben@nehmer.net

18. Januar 2002

Inhaltsverzeichnis

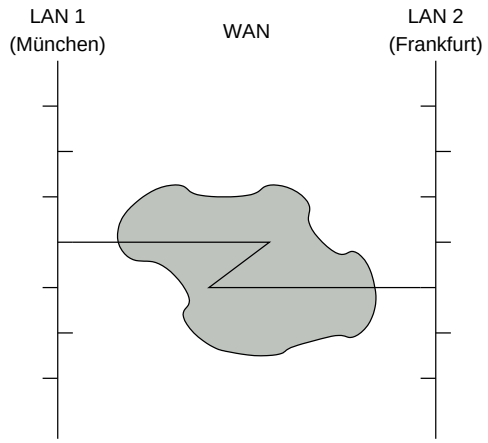

Abbildung 1: Überblick über die Grundproblematik

1 Einführung

In der heutigen Zeit sind Computernetzwerke allgegenwärtig. Auch Firmen nutzen schon seit längerer Zeit die Möglichkeiten der Datenhighways. Eine in dieser Welt allgegenwärtige Problematik ist die Verbindung zweier räumlich getrennter, lokaler Netze untereinander (Abbildung 1). Traditioneller Weg war hier bislang, eine dedizierte Standverbindung zwischen den beiden Standorden zu mieten.

Mit dem Siegeszug des Internets kam erstmals die Idee auf, Standverbindungen dieser Art über die bereits vorhandenen Infrastruktren dieser weltumspannenden Datenautobahn zu verwenden. Die Idee virtueller Netzwerke war damit geboren, und mit ihr eine ganze Reihe von neuen Problemen.

Wichtigster Faktor ist hier die Tatsache, dass diese öffentlich zugänglichen Infrastrukturen keinesfalls als vertrauenswürdig eingeschätzt werden können. Eine direkte Übertragung der Daten durch dieses Netz fällt somit aus.

Diese Ausarbeitung beschäftigt sich mit den Konsequenzen dieser Überlegung, den grundsätzlichen Lösungsansätzen und den Problemen, die sie mit sich bringen.

1.1 Ziele / Motivation

Mit der Entscheidung, Standleitungen durch vorhandene, öffentliche Netze zu ersetzten, sind einige Grundgedanken verbunden:

Flexibilität Netzwerke können über das jedermann zugängliche Internet erheblich flexibler und einfacher etabliert werden. Keine Leitungen zwischen zwei Gebäuden müssen gelegt werden, es ist kaum zusätzliche Infrastruktur seitens des Nutzers nötig. Die meissten Firmen besitzen ohnehin eine Internetanbindung die so effizienter ausgenutzt werden kann.

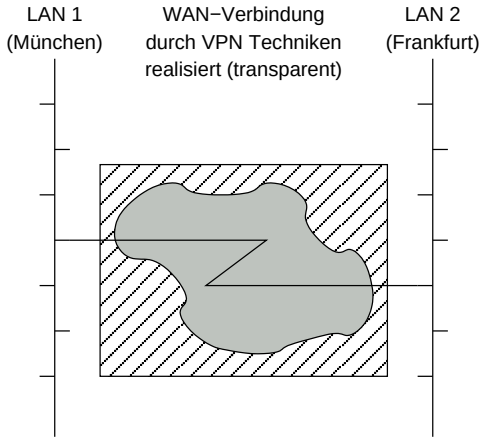

Abbildung 2: Grundidee eines virtuellen, privaten Netzwerkes

Auch mobile Mitarbeiter profitieren von diesem Grundkonzept. Anstatt dass sie sich mit einer direkten Telefonverbindung, die beispielsweise im internationalen Rahmen sehr teuer wird, nutzen sie den nächsten möglichen Zugangspunkt ins Internet und können so theoretisch von überall her ohne zusätzlichen Aufwand die Firmenresourcen nutzen.

Kosten Netzverbindungen über eine bereits vorhandene Infrastruktur sind wesentlich kostengünstiger. Es müssen keine dedizierten Leitungen angemietet werden, die meist eh kaum von einem einzelnen Betreiber ausgelastet werden können. Anbindungen an öffentliche Netze werde im Gegenzug meist nach dem erzeugten Transfervolumen abgerechnet, so dass die entstehenden Kosten sehr viel näher an dem tatsächlich benötigten liegen.

Auch für die Anbindung mobile Mitarbeiter ist eine deutliche Kostenreduktion sichtbar. Es wird keine komplexe Einwahlinfrastruktur notwendig und Telefongebühren für Ferngespräche entfallen.

Bedrohungen im Netz Haupthindernis bei der Nutzung von öffentlichen Netzen ist die fehlende Vertrauenswürdigkeit. Die Kostenersparnis wird ein wenig durch den erhöhten Aufwand der notwendigen Sicherung solcher öffentlicher Verbindungen relativiert.

Mechanismen zur möglichst transparenten Nutzung solcher Netze werden notwendig. Je transparenter diese Verbindungen werden, desto höher ist meist der Einrichtungsaufwand, so dass hier je nach Anwendungsfall der richtige Kompromiss aus Transparenz und Komplexität des Systems gewählt werden muss.

Zieht man dies mit in Betracht, lässt sich das in Abbildung 2 Grundkonzept für ein gesicherte Verbindung dieser Art aufbauen. Die Festverbindung wird nicht mehr als physikalische Leitung zwischen beiden Standorten realisiert, sondern als logische Verbindung über das vorhandene Netzwerk, die entsprechend ge-

sichert und somit transparent ist. Man nennt dies ein "Virtuelles, privates Netzwerk" (VPN).

1.2 Definition

Im IP-Marktsegment sind in den letzten Jahren die Sicherheits-Technologien und Sicherheits-Aspekte immer wichtiger geworden. Dies liegt daran, dass das Internet von der Wirtschaft und der Gesellschaft als "das" globale Netz entdeckt wurde. Dieses "globale Netz" wird heute mehr und mehr für geschäftskritische Anwendungen mit oft sehr hohen Anforderungen an die Sicherheit eingesetzt. Unter diesem Sicherheitsaspekt ist VPN ein Wort dem man immer wieder begegnet. Doch was genau ist ein VPN. Bevor wir weiter auf VPN´s eingehen, sollte klar definiert sein was unter einem VPN den zu verstehen ist.

"Virtual" beudeutet, dass es sich aus der Anwendersicht scheinbar nur um ein Netzwerk handelt, auch wenn sich viele reale Teilnetze hinter einem VPN verbergen.

"Private" bedeutet, dass die Kommunikation vertrauenswürdig, also nicht öffentlich ist. Das heißt das Risiko das die Daten gelesen oder gefälscht werden wird minimiert.

"Network" bedeutet, dass eine Gruppe von definierten Rechnern miteinander verbunden sind, und mit Hilfe eines Protokolls miteinander kommunizieren.

Eine mögliche Definition von Virtual Private Network wäre also:

Ein Netzwerk, das eine Kombination von Tunneling, Verschlüsselung, Authentisierung, Zugriffskontrolle und Services benutzt, um Daten über das öffentliche Internet zu verschicken, und diese Daten somit so schützt, als wär man in einem privaten lokalen Netz, sprich die Daten vor Aussehstehenden geheim hält und unverfälschbar macht.

Für den Benutzer sollte ein VPN also eine Art BlackBox sein. Er soll seine Daten verschicken können als sei er im einem LAN. Von dem Tunnel und der Verschlüßelung um die Integrität der Daten die in Wirklichkeit über das öffentliche Netz laufen zu gewährleisten sollte er möglichst nichts mitbekommen. Der Benutzer selbst sollte höchstens mit Aufgaben die zur Authentisierung und Authentifikation gehören konfrontiert werden.

2 Konzepte

Es bestehen zwei grundlegende Ansätze, VPNs zu realisieren: Einerseits besteht die Möglichkeit, die Verbindung auf Netzwerkebene zu realisieren, so dass die Anwendung regulär arbeiten können. Andererseits könne einzelne Anwendunge direkt mit Hilfe von Sicherungsschichten abgesichert werden:

2.1 VPN auf Netzwerkebene

Dies sind die klassischen VPN Verbindungen. Die vorhandenen Netzwerke werden über zwei Router, die durch einen "Tunnel" verbunden sind, unter-

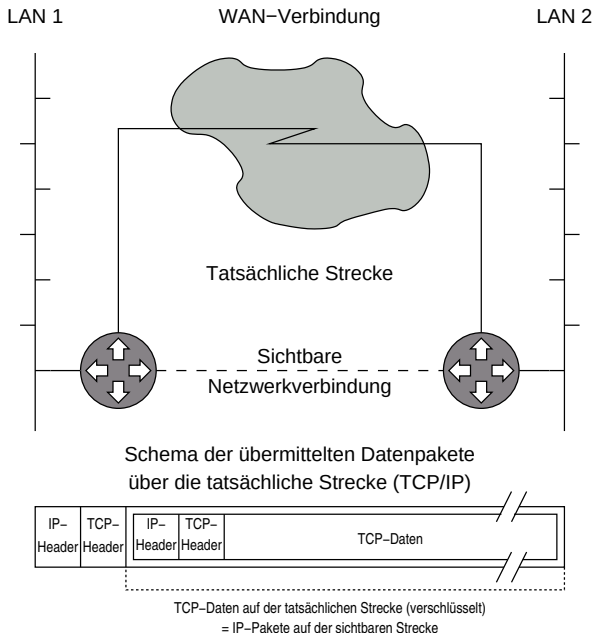

Abbildung 3: Virtuelle Verbindungen auf Netzwerkebene

einander angebunden. Abbildung 3 zeigt eine Skizze dieses Modells.

Die beiden Router bieten den lokalen Netzwerken jeweils eine direkte Verbindung zum Gegenüber. Die Datenübertragung wird durch eine separate Datenverbindung zwischen den beiden Routern erledigt. Übertragen wird dabei direkt der Verkehr der normalerweise über die physikalische Leitung gehen würde.

Im konkreten Beispiel würde der Datenverkehr der zu sichernden TCP/IP-Verbindungen als Daten in die bestehende TCP/IP-Verbindung durch das ungesicherte Netzwerk übertragen. Die übertragenen Daten werden durch eine Verschlüsslung gesichert. Damit erscheint für eine Anwendung in einem der beiden LANs die Netzverbindung durch ein öffentliches Netz wie eine reguläre, dedizierte Standverbindung.

VPN Verbindungen dieser Art sind für jede Anwendung innerhalb der beiden LANs völlig transparent. Die Verbindung durch das öffentliche Netz ist für keine der beiden Seiten sichtbar, für diese laufen die Daten lediglich über die beiden Router.

Der Aufbau dieses Tunnels ist der kritische Punkt in diesem Modell. Die Authentizität der Gegenstelle muss sichergestellt werden. Kann dies nicht garantiert werden, ist das gesamte VPN durch Man-in-the-Middle-Angriffe verwundbar. Moderne VPNs führen die Authentifizierung meist durch Public-Key-Authentifizierung durch.

2.1.1 Vorteile

Hauptvorteil dieser Art der VPNs ist die völlige Transparenz für alle Anwendungen. Es entsteht ein echtes, virtuelles Netzwerk, dass nach aussen hin sehr gut abgesichert ist.

2.1.2 Nachteile

Die völlige Transparenz wird durch einen relativ hohen Einrichtungsaufwand erkauft. Die Router benötigen entsprechende Softwareerweiterungen, die konfiguriert werden müssen.

Realisiert man die Verbindung beispielsweise mit Linux-Routern, müssen Verbindungen dieser Art vom Kernel unterstützt werden. Zudem wird zusätzliche Software benötigt, die die entsprechenden Dienste zur Verfügung stellt.

Werden dagegen echte Routern benutzt, wird meist ein Softwareupdate benötigt. Die Einrichtung ist dann aber meist recht trivial.

Die Problematik der Unterstützung seitens des Betriebssystems kommt besonders dann zum tragen, wenn mobile Mitarbeiter (z.B. mit Notebook) an das lokale Netz angebunden werden sollen.

2.1.3 Beispiele

Es existieren zwei verbreitete Varianten für VPNs auf Netzwerkebene: das Point-To-Point-Tunneling Protocol und IPsec. Ersteres benutzt eine PPP Verbindung um die zu übertragenden Daten zu übermitteln, während IPsec speziell für die Aufgabe TCP/IP-Verbindungen über andere TCP/IP-Netze zu übermitteln entwickelt wurde.

2.2 VPN auf Anwendungsebene

VPNs auf Anwendungsebene sind im eigentlichen Sinne keine virtuellen Netzwerke. Da sie jedoch zur Lösung des Sicherheitsproblemes aktuell verwendet werden, sollen sie hier ebenfalls betrachtet werden.

Wo der Einrichtungsaufwand echter VPN-Verbindungen nicht lohnenswert ist, oder teilweise gar nicht realisiert werden kann (z.B. Web-basiertes Onlinebanking), werden Mechanismen benötigt, die einzelne Anwendungen gezielt absichern.

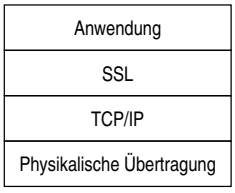

Abbildung 4: TCP/IP Stack mit SSL

Dies wird durch die Einführung einer Sicherungsschicht in den vorhandenen Netzwerk-Stack realisiert. Klassisches Beispiel hierfür sind durch Secure-Sockets-Layer (SSL) geschütze Verbindungen in einem TCP/IP-Netzwerk. Abbildung 4 zeigt einen um SSL erweiterten TCP/IP-Stack: Anstatt die zun übertragenden Daten direkt an den TCP/IP-Stack des Betriebssystems zu übergeben, werden sie an den SSL übergeben, dort verschlüsselt und übertragen.

Anwendungen, die diese Technik nicht direkt unterstüzten, können über SSL Wrapper Systeme gesichert werden. Dabei wird auf dem lokalen System ein "Mini-Server" installiert, der lediglich die Aufgabe hat, die Verbindung anzunehmen, und verschlüsselt an die gegenstelle durchzuschleifen.

2.2.1 Vorteile

Die Absicherung einzelner Anwendungen ist sehr einfach möglich. Vor allem muss im Client-Bereich seitens des Anwenders in der Regel kein Eingriff mehr vorgenommen werden. Vor allem SSL wird heute von den meissten, wichtigen Programmen unterstützt.

2.2.2 Nachteile

Verschlüsselungsschichten müssen von der Anwendung direkt unterstützt werden, wenn eine einfache Nutzung seitens des Anwenders möglich sein soll. Dies bedeutet im Client-Bereich in der Regel das Aus von Wrapper Software, deren Einrichtung nicht immer ganz trivial ist.

2.2.3 Beispiele

SSL werden heute von den meißten wichtigen Anwendungen im Internet-Sektor unterstützt. Insbesondere die Dienste der Protkolle HTTP, POP3, IMAP4 und SMTP sind heute sehr oft in SSL-gesicherten Varianten verfügbar.

Neben SSL haben einige Programmierer für ihre Anwendungen eigene Sicherungsschichten eingeführt. Aus diesem Gedanken heraus ist beispielsweise auch der Telnet-Ersatz Secure Shell (SSH) entstanden. Er bietet neben einem gesicherten Remote-Shell Zugriff auch Mechanismen zum Tunneling von TCP/IP Verbindungen.

3 Protokolle

VPNs arbeiten mit einem Verfahren das "Tunneling" gennant wird. Dazu werden die Daten die ausgetauscht werden sollen, auf einer niedrigeren Netzwerkschicht durch ein Tunnel gesendet. Zur Zeit gibt es vier bekannte Tunneling-Protokolle. Weiterhin gibt es zwei Protokolle zum Schutz einzelner Anwendungen, die in dieser Ausarbeitung der Vollständigkeit halber erwähnt werden:

Name	Entwickelt von	Schicht
Point-to-Point Tunneling Protocol PPTP	Microsoft	2
Layer 2 Tunneling Protocol L2TP ´	offener Standard	2
Layer 2 Forwarding L2F	Cisco Systems	2
IP Security	offener Standard	3
Secure Sockets Layer, Secure Shell SSL, SSH	offener Standard	5

Die Spalte Schicht gibt an auf welcher Ebene des ISO-OSI Referenz-Models die Protokolle arbeiten. Je nachdem auf welcher Schicht die Protokolle arbeiten spricht man von Schicht-2-Tunneling oder Schicht-3-Tunneling. In den nächsten Kapitel werden nun zunächst die Layer-2-Tunneling Protokolle, anschließend IP-Secutiy als Layer-3-Tunneling Protokoll vorgestellt und am Ende werden die beiden Layer-5 Protokolle kurz angerissen.

3.1 PPTP, Point-to-Point-Tunneling Protocol

Entwickelt wurde PPTP von Microsoft, und wurde 1996 vom IETF als Standardprotokoll für das Internet Tunneling vorgeschlagen. PPTP ist eine Weiterentwicklung des Point-to-Point-Protocol und kapselt PPP Pakete und IP-Pakete.

3.1.1 Überblick

Da PPTP zum Tunneln der Daten das Point-to-Point-Protocol verwendet, ist es als Schicht-2-Tunneling Protocol anzusiedeln. PPTP stellt grundsätzlich einen verteilten Einwahlrechner dar, der aus 2 Teilen besteht. Der erste Teil PAC, PPTP Access Conncentrator stellt den physikalischen Endpunkt einer PPP Verbindung dar.Der zweite Teil PNS, PPTP Network Server stellt Funktion zur Autorisation des Benutzer bereit. Zwischen PAC und PNS wird der verschlüsselte Tunnel aufgebaut, über den die beim PAC ankommenden PPP-Verbindung virtuell bin zum PNS verlängert wird (vgl. Abbildung 5). In der Praxis wird diese Funktion schon oft auf dem VPN-Client implementiert. Dazu wird auf dem Client eine virtuelle Netzwerkschnittstelle eingerichtet.

Alle Daten die an diese Schnittstelle gesendet werden, werden in PPP-Rahmen gepackt, und durch die physikalische Schnittstelle zum PNS weitergeleitet. Dieser entpackt die Daten dann wieder in umgekehrter Reihenfolge und sendet sie zum endgültigen Ziel weiter. Der Tunnel zwischen PAC und PNS besteht aus 2 unidirektionalen Netzwerkverbindungen, und einer dritten bidirektionalen Verbindung, die den Auf- und Abbau der Verbindungen steuert. Dem sogenannten Steuerungskanal. Da die Pakete in PPP-Rahmen eingepackt werden, wird noch ein zusätzlicher Header vorangestellt. Der zusätzliche Header ist eine Variante des sog. GRE-Headers (GRE= Generic Routing Encapsulation) mit IP-Protokollnummer 47. Nun können die PPP-Rahmen mit GRE Header in ein IP -Paket eingebettet werden. Dieses IP-Paket kann dann über die

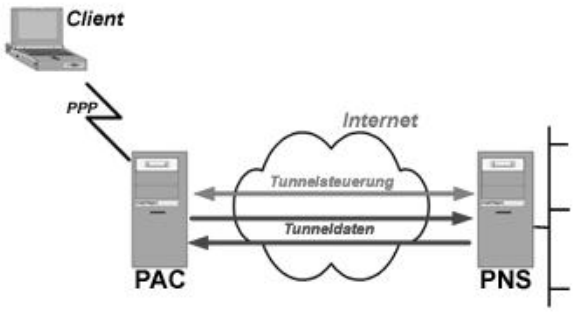

Abbildung 5: Schema einer PPTP-Verbindung

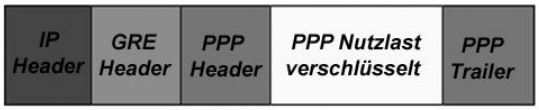

Abbildung 6: PPTP Paket

physikalische Netzwerkschnittstelle zum PNS gesendet werden. (Siehe auch Abbildung 6.

Hier gilt es zu erwähnen das PPTP selbst keine Verschlüsselung, Authenzität und keine Autorisierung vorsieht. Diese Aufgaben werden PPP überlassen. Dies bedeuted, das sowohl der Kanal zur Tunnelsteuerung als auch sämtliche Header in PPTP unverschlüsselt sind.

3.1.2 Authentifizierungsverfahren

Da PPTP eine Entwicklung von Microsoft ist, kommen bei PPP die eigenen Protokolle für die Verschlüsselung und die Authentifizierung zum Einsatz. Das beim PPTP eingesetzte Authentifizierungsverfahren MS-Chap ist eine abgewandelte Form des Challange Handshake Authentification Protocols (Chap), und existiert in zwei Versionen. Die ursprüngliche Version MS-Chapv1, welche massive Sicherheitslücken hat, und somit nicht mehr benutzt werden sollte, und die aktuelle Version MS-Chapv2. Bei MS-Chapv2 besteht ein Authentifizierungsvorgang aus zwei Abschnitten. Zuerst erfolgt die Authentifizierung des Benutzers und anschließend nocheinmal die Authentifizierung des PNS um sogenannte Man-in-the-middle Angriffe zu verhindern.

3.1.3 Verschlüsselungsverfahren

Das bei PPTP eingesetzte Verschlüsselungsverfahren ist das Microsoft Point-to-Point Encryption MPPE. MPPE verwendet den RC4 Algorithmus mit einer Schlüssellänge von 40 oder 128 Bit. Da 40 Bit lange RC4 Schlüssel durch eine Brute-Force-Attacke in vertretbarer Zeit geknackt werden können, sind besonders längere Verbindungen deshalb gefährdet. Seit Anfang 2000 kann eine stärkere Verschlüsselung wegen der gelockerten Exportbeschränkungen auch durch ein Update bei bestehenden PPTP Installationen nachgerüstet werden.

3.2 L2F,Layer 2 Forwarding Protocol

3.2.1 Übersicht

L2F, Layer 2 Forwarding Protocol ist eine Entwicklung welche im RFC 2341 beschrieben ist, und die Herstellung einer virtuellen Verbindung zwischen zwei mit einem IP-Netzwerk verbundenen Stationen ermöglicht. Beim L2F-Protokoll werden die Datenpakete mit einer Mulitplex-ID (MID) gekennzeichnet. Die Kennzeichnung der Datenpakete mit der MID erlaubt den gleichzeitigen Betrieb mehrerer Tunnel. Neben dem Point-to-Point Protokoll (PPP) kann L2F auch SLIP also das Serlial Line Internet Protocol tunneln.

3.2.2 L2F Paketstruktur

Die Paket-Struktur eines L2F Pakets besteht aus drei Teilen. Dem L2F-Header, dem Payload Paket (z.B. PPP-Nutzlast) und einer optionalen L2F Prüfsumme. Der Header des L2F-Pakets enthält zwei ID-Parameter. Multiplex-ID (MID), und Client-ID (CLID). Mit Hilfe dieser zwei ID-Paramentern können gleichzeitig verschiedene Verbindungsziele und damit auch mehrere Tunnel, sowie innerhalb dieser Tunnel jeweils mehrere logische Verbindungen verarbeitet werden. L2F definiert für jeden Tunnel eine individuelle Pinkt-zu-Punkt Verbindung, kann jedoch als Protokoll auch Punkt-zu-Multipunkt Verbindungen herstellen.

3.2.3 Beispiel

Ein Remote-User kann über L2F eine virtuelle Wählverbindung über das Internet aufbauen, und sich so in das entfernte Firmennetzwerk einloggen. Ein solches Szenario würde mit dem L2F folgenderaßen aussehen.

Ein Remote-User wählt sich über ISDN oder eine analoge Telefonleitung mit seinem Rechner beim ISP ein, und authentifiziert sich hierbei wie gewohnt bei seinem ISP für den Internetzugang. Anhand des Usernamen und den Einträgen in einer Datenbank auf dem Network Access Servers (NAS), erkennt dieser das Ziel und baut eine Verbindung zum Home-Gateway (vgl. Abbildung 7) des Firmennetzwerk auf. Bei diesem Verbindungsaufbau authentifizieren sich Network Access Server (NAS) und Home-Gateway über ein Challange Handshake Verfahren jeweils beim Kommunikationspartner. Aus sich des

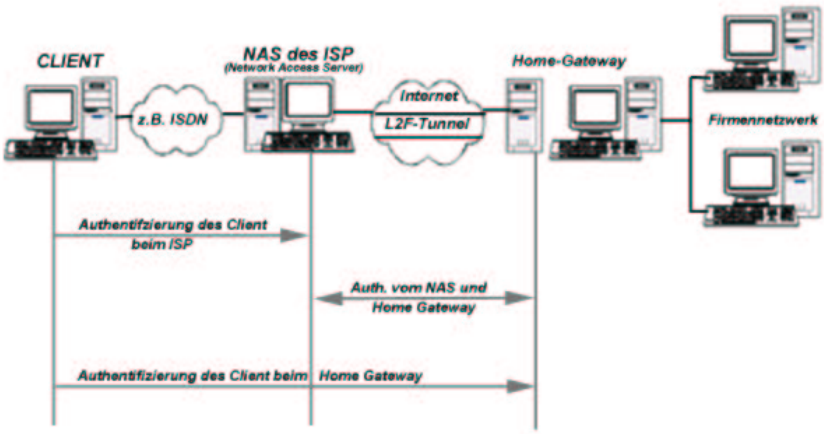

Abbildung 7: Schema einer L2F-Verbindung

Remote-Users besteht bisher jedoch immernoch nur eine Verbindung zwischen seinem Computer und dem NAS des ISP. Er muss sich nun direkt beim Home-Gateway anmelden. Eine hier oft verwendete Möglichkeit hierzu ist das Challange Handshake Authentification Protocol (CHAP).

3.2.4 Authentifizierung / Verschlüsselung

Beim L2F Protokoll authentifizieren sich zwar alle an der Kommunikation beteiligten Parteien untereinander, eine Verschlüsselung der eigentlich zu tunnelnden Nutzdaten ist jedoch nicht vorgesehen. In der Praxis soll sich L2F genau deshalb weniger durchgesetzt haben, und teilweise wurde auch schon davon gesprochen das das RFC zu L2F als veraltet anzusehen ist.

3.3 L2TP, Layer 2 Tunneling Protocol

Das Layer 2 Tunneling Protokoll ist eine Weiterentwicklung von Microsofts Point-to-Point -Tunneling Protokolls (PPTP) und Cisco's Layer 2 Forwarding Protkolls. Ziel beim Design des Protokolls war es, die Vorteile von PPTP und L2F in einem neuen Protokoll zu vereinen. Das Protokoll kapselt dabei ebenfalls PPP-Rahmen zur Übertragung über IP, X.25, Frame Relay oder ATM. L2TP ist ein "proposed" Protokollstandard nach IETF RFC 2661, und bietet Unterstützung für Multiprotokoll-Umgebungen. L2Tp kann also alle gerouteten Protokolle wie Ip, IPX und AppleTalk transportieren.

L2TP komprimiert den Paketheader nicht wie PPTP mit 6 Bytes sondern nur mit 4 Bytes, produziert also weniger Overhead, und wie bei L2F werden ebenfalls mehrere Tunnels unterstützt. Die Kontrolle des Endpunktes eines Tunnels wird jedoch nicht wie bei PPTP auf der Client Seite sondern vom ISP vorgegeben. Außerdem kann mit L2TP auch Quality of Service (QoS) gebo-

ten werden, ermöglicht es also dem ISP die QoS-Garantie anzubieten, die viele Kunden für unternehmenskritische und latenzempfindliche Anwendungen benötigen. L2TP ist ein Tunneling-Protokoll, das Tunnel- und Benutzerauthentifizierung unterstützt, und auch die beim L2F nicht vorgesehene Verschlüsselung der sensiblen Daten ermöglicht. Beim Design von L2TP wurde auch die Adresszuordnung- und Management einbezogen, und so unterstützt L2TP ferner die dynamische Adresszuweisung durch den DHCP-Server.

3.3.1 LAC und LNS, Komponenten in einer L2TP Architektur

LAC, L2TP Access Concentrator ist vergleichbar mit dem Network Access Server beim L2F. Am LAC werden die ankommenden Daten über das L2TP getunnelt und können so an einen oder mehrere LNS´s weitergeleitet werden.Der LNS, L2TP Network Server übernimmt die Serverseite des L2TP Protokoll. Der LNS ist somit Initiator von ausgehenden Anrufen, und der Empfänger von eingehenden Anrufen. Der LNS ist somit das Pendant zum Home-Gateway beim L2F Protokoll.

3.4 IPsec

Desingziel von IPsec war es, plattformunabhängige, hochwertige, kryptographisch basierte Sicherheit für IPv4 und IPv6 zu bieten. Als vollwertiges VPN-Konzept beinhaltet es Mechanismen zur Zugriffskontrolle, Authentifizierung, Schutz gegenüber den meisten gewöhnlichen Angriffen auf Netzwerkebene und zum Datenschutz.

Abhängig vom gewünschten Sicherheitsgrad kommen verschiedene Sicherheitsprotokolle, kryptographische Verfahren und Schlüsseltauschverfahren zum Einsatz.

Auf Grund der Komplexität von IPsec und der damit verbundenen, weiteren Standards, soll hier nur ein Überblick über das Gesamtsystem gegeben werden. Der hier gegebene Überblick entstammt hauptsächlich auf der Basis der RFC 2401 “Security Architecture for the Internet Protocol”.

3.4.1 Überblick

IPsec arbeitet auf IP-Ebene und ab dieser Ebene Sicherheit bieten. Daher arbeitet IPsec immer in einer Gateway-Umgebung. Dies kann entweder ein (lokales) Gateway für einen einzelnen Host oder ein (öffentliches) Gateway für ein Netzwerk sein.

Somit existieren drei mögliche Konstellationen für IPsec-geschütze Netzwerkstrecken (vgl. Abbildung 8): Verbindungen zwischen zwei Hosts, Verbindungen zwischen zwei Gateways und Verbindungen zwischen einem Host und einer Gateway [1].

IPsec verwendet zwei Protokolle zur Realisierung der Anforderungen:

[1] Gatewas und Hosts in diesem Sinne sind Systeme, die IPsec-Dienste anbieten.

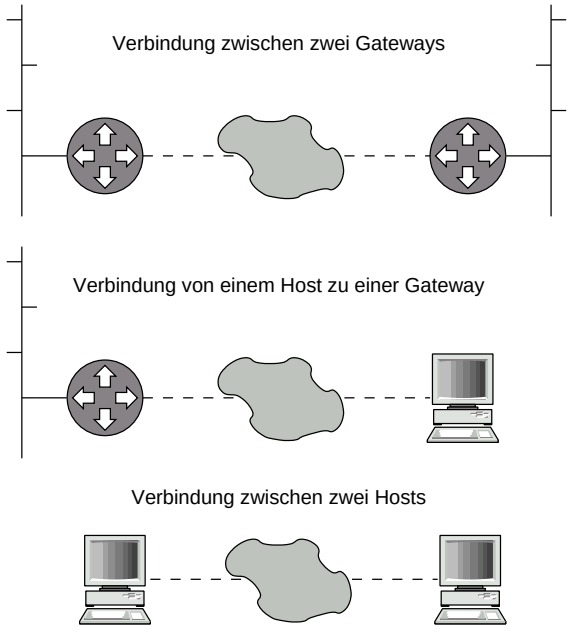

Abbildung 8: Mögliche Verbindungsarten mit IPsec

Authentication Header (AH) Über AH wird Verbindungsunabhängig Datenintegrität, Authentifizierung des Senders und (optional) einen Schutz gegen Replay-Attacken, also gegen das Aufzeichnen und wiederabsenden von IPsec Kommunikation.

Encapsulating Security Payload (ESP) Hauptaufgabe des Protkolles ESP ist es, die übertragenen Daten selbst und ihren Fluss im allgemeinen kryptographisch abzusichern. Optional können über ESP auch die Dienste des AH zur Verfügung gestellt werden.

Mechanismen zur Zugriffskontrolle können sowohl über den AH als auch über ESP realisiert werden. Es müssen nicht zwingend beide Protokolle verwendet werden. Dies ist in der Regel abhängig von den Anforderungen an die Sicherheit der Übertragung.

Alle von IPsec angeboteten Sicherungsmechanismen benutzten kryptographsiche Schlüssel. Das Management dieser Schlüssel ist nicht Bestandteil der IPsec Kernfunktionen. Stattdessen werden sie entweder Manuell oder über einen Public-Key Verfahren (z.B. IKE) ausgetauscht.

3.4.2 Betriebsmodi

IPsec kennt zwei Betriebsmodi: Den Transport Mode und den Tunnel Mode:

Transport Mode: Im Transport Mode setzt IPsec über dem Network Layer an. Dies ist nur dann möglich, wenn es sich um eine Host-zu-Host Verbin-

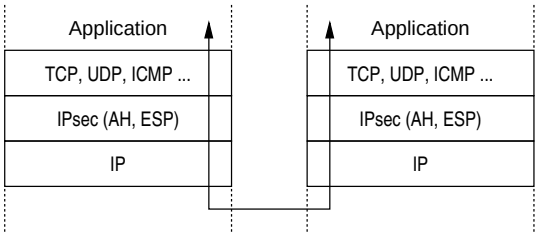

Abbildung 9: IPsec im Transport Mode

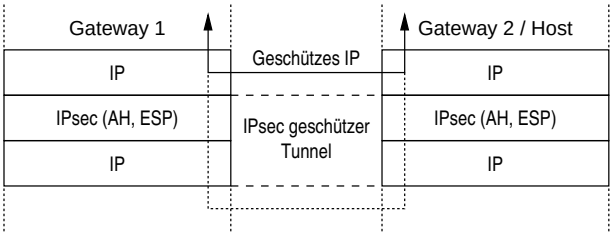

Abbildung 10: IPsec im Tunnel Mode

dung handelt. Nachteil dieser Methode ist es, dass die IP-Schicht nur minimalst geschützt werden kann. (vgl. Abbildung 9)

Tunnel Mode: Sobald eine der beiden Seiten eine Gateway ist, muss die Verbindung im Tunnel Mode arbeiten. Zwei Hosts können wahlweise ebenfalls einen Tunnel untereinander aufbauen. Für die getunnelten Verbindungen ist der Weg zwischen den beiden Gateways unsichtbar. Die getunnelte Verbindung geniesst den vollen Schutz des IPsec Systems.

3.4.3 Schlüsselverwaltung

Grundsätzlich können IPsec Schlüssel wahlweise manuell oder automatisch verwaltet werden. Obwohl die beiden IPsec Protokolle AH und ESP grösstenteils von den Verwaltungsarten unabhängig sind, erfordern einige fortgeschrittene Sicherheitsmechanismen eine automatische Verwaltung. Im Allgemeinen gilt noch, dass die Feinheit der Zugriffskontrolle in direktem Zusammenhang mit den möglichen Einstellungen der Schlüsselverwaltung steht.

Manuelle Techniken: In einfachen Umgebungen kann das IPsec System vollständig manuell konfiguriert werden. Ein Administrator macht dabei auf jedem beteiligten System die notwendigen Einstellungen. Gerade wenn einige wenige Standorte miteinander durch feste IPsec Tunnel verbunden werden sollen, reicht diese Methode bei weitem aus.

Automatische Techniken: Grossflächiger Einsatz von IPsec erfordert ein skalierbares Management-Protokoll. IPsec sieht als Standardprotkoll für die Schlüsselverwaltung IKE vor. Ein IKE konformer Dienst ist für die Erstellung und Verteilung von IPsec Authentifizierungs- und Verschlüsselungs-Schlüssel zuständig.

3.4.4 Internet Key Exchange (IKE)

IKE ist ein hybrides Protokoll. Es stellt einen sicheren Mechanismus zum Aushandeln von Schlüsseln zur Verfügung. Zusätzlich stellt es authentifizierte Schlüssel zur Verfügung. IKE ist in der RFC 2409 beschrieben.

Mit Hilfe von IKE können nicht nur gewöhnliche VPNs ihre Schlüssel untereinander aushandeln. Es ist zudem möglich, mobile Anwender – deren IP Adresse nicht immer im Vorraus bekannt ist – an sicher an ein Netzwerk anzubinden.

IKE arbeitet zweistufig: Zunächst wird eine gesicherte Verbindung zum IKE-Server aufgebaut. Danach können Schlüssel- und Parameter-Verhandlungen zum Kommunikationsaufbau mit der gewünschten Gegenstelle durchgeführt werden.

3.4.5 Sun's SKIP Firewall Traversal for Mobile IP

Im Bereich des Mobile Computing können Sicherheitsprobleme in grösserem Rahmen entstehen. Ein mobiler Anwender benötigt die Möglichkeit, auch durch eine Firewall hindurch eine sichere Verbindung in das eigene Netzwerk zu bekommen. Die RFC 2356 beschreibt das bei Sun Microsystems entstandene System um die Hauseigene SKIP Firewall für Mobile Arbeiter öffnen zu können.

Da sowohl die eigentliche Anbindung an das Internet als auch die Strecke in das Firmennetzwerk als hochgradig unsicher angesehen werden müssen, wird eine Möglichkeit benötigt, einen geischerten Weg bis zur Firewall auszuhandeln.

Hauptgrund für die Entwicklung von SKIP war die Notwendigkeit nach einem sehr performanten, nicht Session-orientierten Schlüssel-Austausch-Systems. SKIP-gestützte Verbindungen verwenden wie gewohnt AH und/oder ESP zum Datenaustausch.

Wichtiger Vorteil von SKIP ist die völlige Ausrichtung auf Mobile Computing. Die in den IP-Paketen angegebenen Zieladressen können von SKIP nach Wunsch des Benutzers auf der Basis der verwendeten Schlüssel umgeschrieben werden. Anstatt einen Tunnel aufzubauen können die Kommunikationspartner so direkt miteinander Reden, obwohl sie eigentlich in völlig getrennten Netzen stehen: Der SKIP-Router schreibt die IP-Adressen auf der Basis des verwendeten Identifikations-Schlüssels um. Parallel dazu können in einer SKIP-Firewall in Zugriffslisten nicht nur IP-Adressen sondern auch Schlüssel-IDs verwendet werden.

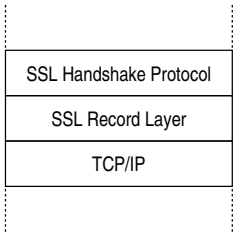

Abbildung 11: Einordnung von SSL

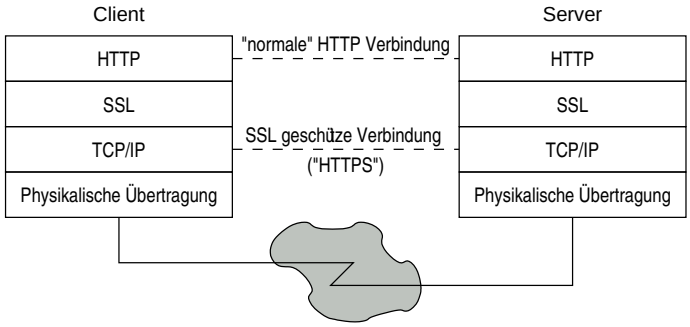

Abbildung 12: SSL-geschütze HTTP-Verbindung

3.4.6 Mobile Computing und Sicherheit

Aus Sicht der Sicherheit für ein Firmennetzwerk gilt es noch zu berücksichtigen, das jedes Mobile Gerät die Peripherie des Firmennetzwerkes erweitert.

Alle mobilen Geräte besitzten in der Regel direkten Zugriff auf das (ungesicherte) Internet, sei es beispielsweise nur, um DHCP Leases erneuern zu können. Da dieser Zustand nicht restriktiert eine enorme Angriffsgefahr für ein Netzwerk bieten würde, ist es unbedingt notwendig, die Mobilen Systeme selbst wieder abzusichern.

3.5 SSL

SSL ist das klasqsische Verschlüsslungssystem im Internet. Entwickelt von Netscape auf Grund der fehlenden Sicherheit im TCP/IP-Stack ist es heute ein de-facto Standard im WWW zur Sicherung bereits existierender Anwendungen. SSL selbst besteht aus zwei Teilen: Dem Handshake und dem Record Layer (siehe unten). Abbildung 11 zeigt die Einordnung von SSL innerhalb des TCP/IP-Schichtenmodells.

Wie in Abbildung 12 ersichtlich, ist eine SSL-Verbindung für die Anwendung in soweit transparent, als dass beide Seiten ihr gewohntes Protokoll sprechen. Die Daten werden nur nicht direkt an den TCP/IP-Stack übergeben sondern an das SSL-System, welches die eigentliche Übertragung durchführt.

Innerhalb einer SSL Sitzung, die eine Anwendung öffnet, können mehrere Verbindungen geöffnet werden, so dass nicht für jeden benötigten Kommunikationskanal eine neue SSL Authentifizierung durchgeführt werden muss.

3.5.1 SSL Record Layer

Der SSL Record Layer ist ist für die eigentliche Datenübertragung des SSL Systems zuständig. Er erhält Daten beliebiger Länge aus den höheren Schichten, verschlüsselt die Daten und überträgt sie über das ungesicherte Netzwerk.

Grosse Blöcke dürfen falls notwendig fragmentiert werden, wobei die Blockstruktur der übergeordneten Schicht nicht unbedingt eingehalten werden muss. Wahlweisse können die Nutzdaten noch komprimiert werden, dies ist aber optional.

Da aus Gründen der Performance nicht die gesamte Übertragung mit einem assymetrischen System verschlüsselt wird, wird bei SSL ähnlich wie bei PGP zur eigentlichen Verschlüsselung der Daten ein symetrisches Verfahren verwendet. Der Schlüssel wird über das Public/Private Key Verfahren für jede Session neu ausgehandelt.

Zur Übertragung von kryptographischen Statusinformationen, beispielsweise der symetrischen Session Schlüssel, wird meist RSA oder Diffie-Hellman verwendet. Als symetrisches Verfahren wird oft DES bzw. 3DES verwendet. Die Integrität der Daten wird mit Hilfe von MD5 oder SHA Hashes gesichert.

3.5.2 SSL Handshake Protocol

Wichtigster Bestandteil von SSL ist der in Abblidung 13 beschriebene Handshake, mit dem die Parameter der Kommunikation ausgehandelt werden. Dieser läuft in zwei Phasen ab:

Zunächst schlägt der Client dem Server über die HELLO-Nachrichten die von ihm unterstützen Verschlüsslungs- und SSL-Protokoll-Versionen vor. Der Server wählt aus diesen eine aus, und übermittelt sie dem Client. Wahlweise kann der Client in diesem Schritt den Server zusätzlich zur Authentifizierung auffordern. In diesem Falle antwortet der Server zusätzlich mit seinem eigenen Zertifikat. In seiner Antwort hat der Server ebenfalls die Möglichkeit, den Client zur Authentifizierung aufzufordern.

Sind die grundlegenden Parameter der Verbindung ausgehandelt, werden die zur Initialisierung der Verschlüsslungsalgorithmen notwendigen Informationen ausgetauscht. In seiner Antwort muss der Client, falls vom Server erwünscht, sein Zertifikat mit übertragen.

Falls Client und Server eine vorausgegangene Sitzung wieder aufnehmen wollen, wird eine verkürzte Version des Handshakes durchgeführt. Dabei werden in den HELLO Nachricht lediglich die Session ID an den Server übermittlet. Akzeptiert der Server, werden direkt die CHANGE-CIPHER Nachrichten übertragen.

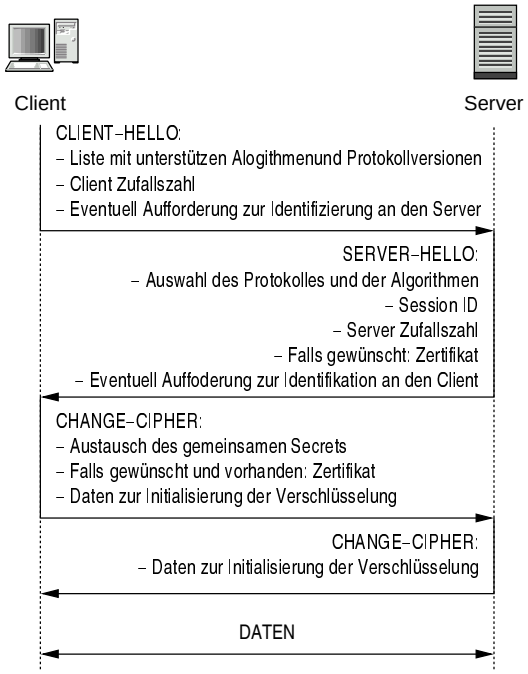

Abbildung 13: Der SSL-Handshake

3.5.3 Authentifizierung

Ein wichtiger Gedanke bei der Entwicklung von SSL war die Möglichkeit, die Identität des Servers verfizieren zu können. Durchgeführt wird dies mit Hilfe von Zertifikaten. Diese Zertifikate basieren auf asymetrischen Schlüsselpaaren. Der öffentliche Schlüssel des Servers wird dabei von einer "Certification Authority" signiert und dadurch als echt gekennzeichnet. Client-Authentifizierung kann nach den gleichen Mechanismen durchgeührt werden, ist aber weit weniger verbreitet.

3.5.4 Sicherheit von SSL

SSL gilt allgemein als recht sicheres Protokoll. Nichtsdestotrotz hat auch SSL einige Schwachstellen:

Abhören von Passwörtern: Die Sicherheit von SSL-Geschützen Passwörtern steht und fällt mit der Grösse des Session-Keys. Viele ältere Web-Browser beispielsweise arbeiten noch mit 40 Bit langen Schlüsseln, die mit Brute-Force Angriffen durchaus knackbar sind. Aktuelle Software arbeitet in der Regel mit 128 Bit langen Schlüsseln, die aktuell als relativ sicher gelten können.

IP Spoofing und IP Hijacking: Auf Grund der Integritätsprüfung über MD5 oder SHA Hashes, in deren Berechnung ja auch das gemeinsame Secret miteinfliesst, sind Spoofing- und Hijacking Angriffe kaum möglich. Gefälschte Pakete werden auf Grund der falschen Prüfsumme sofort erkannt.

Man-in-the-Middle: Da zur Authentifizierung des Gegenparts ein von ein CA unterschriebenes Schlüsselpaar verwendet wird, kann die Gegenseite – vorausgesetzt sie vertraut der betreffenden CA – von einem sehr zuverlässigen Schutz gegenüber Man-in-the-Middle Angriffen ausgehen. Da zur Initiierung der Kommunikation der private Schlüssel der Gegenseite benötigt wird, ist eine Fälschung der Authentifizierung kaum möglich.

3.6 Secure Shell - SSH

Grundsätzlich arbeitet SSH aus kryptographischer Sicht sehr ähnlich wie SSL. Da das SSH-Paket als Ersatz für die Berkley *rtools*[2] gedacht ist, unterscheidet sich aber die Authentifizierung gegenüüber SSL ein wenig:

Zunächst erfordert SSH explizit die authentifizierung des Gegenübers als legitimer Benutzer des lokalen Systems. Dabei sind mehrere Arten der Authentifizierung vorgesehen: Neben einer interaktiven Passwort-Abfrage ist die Authentifizierung über ein Schlüsselpaar möglich. Dies entspricht grunsätzlich der SSL Authentifizierung.

Um Rückwärtskompatibilität mit den rtools zu halten, werden zudem `.rhost`-ähnliche Dateien unterstützt. Wichtigster Unterschied ist hier, dass nicht IP-Adressen sondern Host-Keys (siehe unten) zur Zugriffsbeschränkung eingesetzt werden.

Als Remoteshell Ersatz ist SSH sehr sicher. Auch gelten die aktuellen Implementierungen als recht zuverlässig.

Ein wichtiger Bestandteil der SSH sind die sogenannten Host-Keys. Jedes System besitzt ein eigenes Schlüsselpaar, mit dessen Hilfe es sich selbst authentifizieren kann. Dies wird vor allem zur Verhinderung von Man-in-the-Middle Angriffen verwendet, da ein zwischengeschalteter Angreifer den privaten Teil des Host Keys nicht kennt. Einziger Nachteil ist, dass der Client nur Änderungen des Schlüssels nachvollziehen kann. Erhält der Client von Anfang an gefälschte Daten, kann er den Angriff nur noch an der falschen Key ID nachvollziehen.

Sollen Angriffe wie Man-in-the-Middle, IP-Spoofing oder IP-Hijacking vermiden werden, ist es unbedingt notwendig, jedem Client den korrekten Public Host Key zukommen zu lassen.

Leider bietet SSH momentan kein konkretes Konzept zur automatischen Verteilung von Schlüsseln. Dies ist somit der grösste Schwachpunkt dieses Konzeptes, der einen grossflächigen Einsatz in diesem Rahmen sehr schwierig macht.

[2] rsh, rlogin, rcp

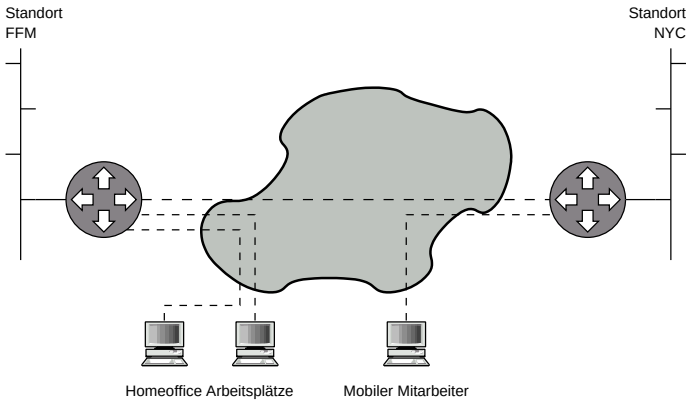

Abbildung 14: Beispielszenario

3.6.1 Einsatzmöglichkeiten im Rahmen von VPNs

Als reiner Remoteshell Ersatz wäre SSH im Rahmen von VPNs von keiner nennenswerten Bedeutung. Zwei spezielle Anwendungen sorgen aber für einige interessante Anwendungsmöglichkeiten: Unterstützung X11-Forwarding und Tunneling:

X11-Forwarding: Über eine bestehende SSH-Verbindung auf ein Zielsystem lassen sich die Ausgaben von X11-basierten Programmen umleiten. Dies erfolgt mit Hilfe eines Proxy-Ansatzes, bei dem das SSH-System alle X11-Anfragen abfängt und über die SSH-Verbindung leitet, anstatt dem X-Server eine direkte Verbindung zum Client zu erlauben. Da diese Verbindung durch die SSH-Verschlüsselung gesichert ist, können so auch X11-Anwendungen über ungesicherte Netze umgeleitet werden.

Tunneling: Allgemein können über SSH-Verbindungen TCP-Verbindungen aller Art getunnelt werden. Hier findet ein reguläre Proxy-Ansatz verwendung.

4 Beispielszenario

Abbildung 14 skizziert ein VPN-Beispielszenario.

Dieses Szenario basiert auf einer typischen Lösung, die zwei LANs miteinander Verbindet. In diesem Falle werden die Standorte Frankfurt am Main und New York City eines fiktiven Unternehmens über ein vorhandenes WAN – das Internet – miteinander verbunden. Eine echte Standverbindung würde zwischen diesen beiden Standorten aus kostengründen nicht in Frage kommen. Der Einrichtungsaufwand für diese VPN-Lösung ist vergleichsweise trivial, da kaum Probleme wie dynamische IP-Adressen oder wechselnde Partner bedacht werden müssen.

Da in den meisten heute genutzten LANs TCP/IP genutzt wird, wird hier eine Lösung über IPsec bevorzugt. PPTP und L2F scheiden auf Grund der geringen Sicherheit ohnehin aus, L2TP wurde auf Grund der geringeren Verbreitung und der vergleichsweise komplexen Einrichtung ebenfalls nicht in Betracht gezogen.

Bereits an dieser Stelle stellt sich die Frage, an welcher Stelle die IPsec Tunnel enden. Da jedes heutige Unternehmen eine Firewall besitzt, bestehen theoretisch drei Möglichkeiten: Vor, in oder hinter dem Firewal-Komplex:

Vor oder hinter des Firewall-Systems scheidet unter Gesichtspunkten der Sicherheit aus. Vor dem System exponiert den IPsec Endpunkt zu stark für potentielle Angreifer. Hinter der Firewall würde eine zu grosse Lücke in das System setzten. Diese Lösung ist nur dann notwendig, wenn die Firewall VPNs als Konzept nicht unterstützen kann.

Sicherheitstechnisch korrekt sollte ein VPN-Endpunkt innerhalb der DMZ des Systems enden. Grundsätzlich werden IPsec-Verbindungen durch das Packet-Filter System am Internet zugelassen, durch den internen Packet-Filter jedoch nicht. IPsec Verbindungen werden so nur von genau definierten Verbindungen zu einem definierten Host zugelassen, der von aussen her sonst keine weiteren Verbindungen erlaubt. Der Datenverkehr in das interne Netz kann zudem am internen Packet-Filter weiter limitiert werden, da er trotz allem nicht als 100 Prozent vertrauenswürdig einzustufen ist.

In einer erweiterten Lösung könnte man sich die Anbindung von Heim- und mobilen Arbeitsplätzen vorstellen. Grundsätzlich sind beide Arten als kritscher zu sehen, als die direkten LAN-LAN Verbindungen. Dies resultiert hauptsächlich aus der fehlenden Kontrolle über diese Arbeitsplätze.

Hier ist die Einrichtung eines Key-Servers in den meisten Fällen zwingend notwendig, da diese Clients in der Regel mit dynamischen IP-Nummern genutzt werden. Die Homeoffice Arbeitsplätze könnten zwar noch mit festen IP-Adressen arbeiten, aber spätestens der mobile Mitarbeiter besitzt diese Möglichkeit nicht mehr. Zudem vereinfacht der Keyserver die Konfiguration von VPNs mit vielen Teilnehmern.

Die Unterstützung von dynamischen Arbeitsplätzen – insbesondere im Zusammenhang mit Arbeitsplätzen hinter NAT-Systemen – wird sich mit der Einführung von IPv6 stark verbessern. Hauptgrund hierfür ist, dass IPsec primär für IPv6 und nicht für IPv4 konzipiert wurde.

Ein letzter wichtiger Punkt bei der Einbdung dieser Arbeitsplätze ist die Tatsache, dass all diese Systeme zusätzlich zur IPsec Verbindung noch eine reguläre Verbindung ins Internet offen haben. Diese bietet neue Angriffspunkte in das geschützte Firmennetz. Daher müssen diese Arbeitsplätze auf jeden Fall mit Hilfe von Packetfiltern so weit geschützt werden, dass ein “Einsteigen” in den IPsec Tunnel über die ungesicherte Internetverbindung nicht möglich ist. In weiterer Konsequenz sollte bei solchen geschützen Arbeitsplätzen der normale Internet-Zugriff ebenfalls über den IPsec-Tunnel durch das Firmen-LAN erfolgen.

5 Fazit

Die Entwicklung der technischen Infrastruktur für VPNs ist bereits sehr weit fortgeschritten und als produktionsfähig zu bezeichnen. Als de-facto Standard hat sich hier mittlerweile IPsec herauskristallisiert. Gegenwärtig werden VPNs vor allem noch zur Verbindung von Standorten eingesetzt. Die Verwendung im Client-Bereich, insbesodere von mobilen Mitarbeitern, wird mit der Einführung von IPv6 stark vereinfacht werden.

6 Links

- RFC 2637: PPTP, Point-to-Point Tunneling Protocol, `http://www.ietf.org/rfc/rfc2637.txt?number=2637`
- RFC 2341: L2F, Layer 2 Forwarding Protocol, `http://www.ietf.org/rfc/rfc2341.txt?number=2341`
- RFC 2661: L2TP, Layer 2 Tunneling Protocol, `http://www.ietf.org/rfc/rfc2661.txt?number=2661`
- RFC 2401: IP Security `http://www.ietf.org/rfc/rfc2401.txt?number=2401`
- Cisco Fact Sheet zu L2TP Layer 2 Tunneling Protocol, `http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/_de_l2tun_ds.htm`
- VPNC, Virtual Private Network Consortium, `http://www.vpnc.org/`
- Mehr Schutz im virtuellen Netz, Artikel von Klaus Eppele, `http://www.improve-mtc.de/Veroffentlichungen/VPN-CW/vpn-cw.html`
- Cisco Dokumentation L2TP Layer 2 Tunneling Protocol, `http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/l2tpt.htm`
- Cisco Webseite zu Virtual Private Network Design, `http://www.cisco.com/warp/public/779/largeent/design/vpn.html`