FORSCHUNGSZENTRUM JÜLICH GmbH
Zentralinstitut für Angewandte Mathematik
D-52425 Jülich, Tel. (02461) 61-6402

Interner Bericht

Status und Weiterentwicklung sicherer Dial-In Zugänge zum JuNet

Leon Radermacher

FZJ-ZAM-IB-2000-11

August 2000

(letzte Änderung: 23.08.2000)

Inhaltsverzeichnis

Kapitel 1

Status der PPP-Wählzugänge

1.1 Einleitung

Durch den zunehmenden Einsatz schnellerer Wählverbindungen zum firmeneigenen LAN (xDSL, Cable Modems) und der Tendenz zu sog. Flat Rates der Internet Provider wächst die Wahrscheinlichkeit, dass PPP-Verbindungen dauernd (evtl. auch unbeaufsichtigt) mit dem LAN (Internet) aufrecht erhalten werden. Über PPP sind diese Rechner am weltweiten Internet sichtbar und können relativ leicht ausspioniert werden. Gerade über ISDN/Modem Wählverbindungen können Angriffe potentieller Hacker immer dann leicht vertuscht werden, wenn bestimmte Grundregeln für die Konfiguration der Access Server nicht beachtet werden. Sind dann erst einmal Informationen über das Einwahlnetzwerk bekannt, ist der Weg ins weitere LAN nicht mehr weit, weil die Benutzer oftmals dazu neigen, für das LAN und den externen Zugang identische Passwörter zu benutzen. Aus den genannten Gründen ist es zunehmend erforderlich, die Netzstruktur für die Access-Server zu überdenken und zukünftig alle PPP-Wählverbindungen für den Zugangsbereich zum JuNet in geeigneter Weise zu verschlüsseln. Hier bieten sich Secure Shell (ssh) und sog. Virtual Private Networks (VPNs) in Verbindung mit geeigneten Protokollen und Verfahren zur Verschlüsselung an.

Secure Shell kann für alle Anwendungen durch geeignete Umlenkung der TCP-Ports quasi sofort eingesetzt werden und ermöglicht so den sofortigen Umstieg auf verschlüsselte Verbindungen. Seit einiger Zeit bieten aber auch verschlüsselte VPNs für WAN-Verbindungen im Zugangsbereich (ISDN/Modem) neue, wesentliche Vorzüge. Neben der sehr kostengünstigen Einwahl bei einem lokalen, aber übergegional (evtl. weltweit) operierenden Network Service Provider (NSP) stellt diese Methode bei geeigneter Implementierung einen sicheren Tunnel zum gewünschten Ziel zur Verfügung. Der Benutzer verlagert sozusagen seinen virtuellen Einwählpunkt bis zum/ins Ziel-LAN. Bei geeigneter Auslegung des VPN's liegt dann - falls erwünscht - der Gedanke sehr nahe, die bisher firmeneigenen ISDN/Modem Pools auszulagern (outsourcing). Dies führt zu einer Einsparung von Gerätekosten, darüber hinaus können zusätzliche Dienste (Wartung, Administration, Konfiguration) an geeignete Provider oder Unternehmen ausgelagert werden. Vor diesem Schritt müssen allerdings unbedingt die Sicherheits-relevante System- und Benutzerkonfiguration und nicht zuletzt die Benutzerberatung bedacht werden. Diese wichtigen Dienste sollten - wenn eben möglich - im eigenen Unternehmen verbleiben.

Die Realisierung von VPN's erfolgt über entsprechende Router, die einen sicheren Datentransfer vom Endbenutzer bis ins Zielsystem gewährleisten müssen. Jeglicher Datenverkehr im VPN muss (auch zwischen den Routern) verschlüsselt werden. Die Verschlüsselung muss für den Benutzer transparent sein. Sie erfolgt auf relativ niedriger Ebene (ISO/OSI Schicht 2 oder 3). Die Authentifizierung kann durch public key Verfahren (relativ) sicher gestaltet werden.

Nachfolgend werden konkrete Möglichkeiten aufgezeigt, wie ein sicherer, externer Zugang zum JuNet vom lokalen Einwählpunkt des Benutzers ermöglicht werden kann. Eine Mindestanforderung dazu ist die sichere Authentisierung des Benutzers.

1.2 Formen der Authentisierung

1.2.1 Passwortübertragung im Klartext

Bei der einfachsten Form der Authentisierung nach einzelnen Benutzernamen und zugehörigen Passwörtern (password) besteht die Gefahr, dass die Passwörter im Klartest übertragen werden und durch Mithören auf den Übertragungsleitungen ausspioniert werden können. Dies kann sowohl im Telefonnetz, aber auch im LAN passieren. Letzteres ist deswegen ein Problem, weil viele Benutzer für beide Zugänge das gleiche Passwort benutzen. Dies ist so im Forschungszentrum (FZJ) nicht möglich, da eine zentrale Passwortvergabe eingesetzt wird. Eine weitere Gefahr besteht in diesem Zusammenhang darin, dass das Passwort auf dem entfernten PC oft abgespeichert wird (Bequemlichkeit) und damit jeder potentielle Benutzer vor Ort den Zugang erhält.

1.2.2 Automatischer Rückruf

Beim automatischen Rückruf liegt die Sicherheitsphilosophie darin begründet, dass der endgültige Netzzugang nur zu einem auf dem ISDN/Modem Server hinterlegten Netzanschluss des Benutzers durchgeführt wird. Die Authentisierung nach Benutzername und zugehörigem Passwort erfolgt zwar auch hier im Klartext (beim hingehenden Ruf des Benutzers), nach Trennung dieser Verbindung wird die endgültige Verbindung aber nur zu dem auf dem Server hinterlegten Anschluss realisiert. Durch diese Maßnahme ist sicher gestellt, dass durch einfaches Abhören der Übertragungsleitungen noch kein unberechtigter Zugriff erfolgen kann. Diese Form des Zugangs wird im FZJ von ca. 40 Prozent der Benutzer (Stand: Mitte 2000) eingesetzt.

1.2.3 ISDN Rufnummernübermittlung

ISDN-Verbindungen ermöglichen es, die Rufnummer des Partners auszuwerten. Die Rufnummernübermittlung wird an Stelle von Benutzername/Passwort eingesetzt. Nur bei Übereinstimmung der beim hingehenden Ruf übermittelten Rufnummer mit der auf dem Server hinterlegten Nummer (Überprüfung via D-Kanal) wird eine Datenverbindung aufgebaut. Hier kann dann sowohl eine Verbindung mit als auch ohne Rückruf realisiert werden. Diese Form des Zugangs wird auf dem nicht mehr offiziell unterstützten 'Conware-Server' im FZJ eingesetzt.

1.2.4 Authentisierung innerhalb PPP (PAP, CHAP)

Die wohl am meisten verwendete Methode des Zugangs zum LAN ist die Authentisierung innerhalb des PPP-Protokolls. Dieses Protokoll definiert bereits zwei verschiedene Authentisierungsverfahren als Teil des sog. Link Control Protocol (LCP): Password Authentication Protocol (PAP) und Challenge Handshake Authentication Protocol (CHAP).

PAP
Die Authentisierung nach PAP entspricht einer einfachen Übermittlung von Benutzername und

Passwort. Das Passwort wird auch hier im Klartext übertragen. Der Rechner des Benutzers sendet LCP-Pakete mit dieser Kombination, bis eine Empfangsbestätigung kommt. Anderenfalls wird die Verbindung von der Gegenseite abgebrochen. Dieses Verfahren ist das zur Zeit im FZJ am meisten verwendete Authentisierungsverfahren.

CHAP
Bei diesem Verfahren wird das Passwort nicht im Klartext übertragen, sondern mit nicht umkehrbaren Hash Funktionen verschlüsselt. Diese Funktionen werden auf eine Kombination einer Zufallsfolge (challenge) und des Passwortes angewendet. Die Antwort des Servers wird vom Rechner des Benutzers nach Generierung dieser Kombination an den Authentisierungsserver zurückgesendet (response), der nach Anwendung der gleichen mathematischen Operation die Ergebnisse vergleicht. Da das PPP-Protokoll verschiedene Rahmentypen definiert, können solche Authentisierungspakete (LCP) auch während einer laufenden Verbindung periodisch ausgetauscht werden, ohne den Datentransfer zu beeinträchtigen. So ist diese Form der Authentisierung nicht nur auf die Verbindungsaufbauphase beschränkt. Der meist verwendete Hash-Funktion ist der MD5 Algorithmus, das aktuelle Verfahren kann aber auch über PPP ausgehandelt werden. CHAP funktioniert auch auf den Servern des FZJ und sollte deswegen zukünftig mehr eingesetzt werden.

1.3 Neue Gefahren von PPP bei Dial-In

Wie bereits erwähnt, stellen ISDN/Modem Wählverbindungen zum Firmen-LAN (hier JuNet) im Zusammenhang mit dem PPP-Protokoll durch die schnelle Weiterentwicklung der Netzwerktechnik im Zugangsbereich und der immer günstigeren Gebührenpolitik der Service Provider eine zunehmende Gefahr für die Sicherheit des LAN dar. Neue Techniken (V.92, xDSL, Cable Modems) und damit einhergehend immer günstigere Flatrates der Service Provider erhöhen die Tendenz zum 24 Stunden Betrieb solcher Netzzugänge. Die heute üblichen schnellen Prozessoren und riesigen Festplatten lassen es zu, dass häusliche PCs wie Server ständig am Netz angeschlossen sind (heute bereits in den USA). Meist wird das sehr mächtige und flexibel einsetzbare PPP-Protokoll verwendet, das die angeschlossenen Rechner prinzipiell zu vollwertigen Teilnehmern am weltweiten Internet macht (Scans, Angriffe). Zudem ist oft die lokale Umgebung dieser Rechner nicht ausreichend gegen eventuelle Angriffe unbefugter Benutzer geschützt (oft unbewacht). Wenn erst einmal Attacken auf das lokale System vorbereitet sind, können mit Hilfe von Informationen aus dem Bereich des Access-Servers evtl. auch Teilbereiche des gesamten LAN ausspioniert werden. Windows-Systeme sind hier grundsätzlich weniger gefährdet als Systeme unter Unix oder Linux (daemons), trotzdem ist unter den genannten neuen Gefahren erhöhte Wachsamkeit gefordert.
PPP wird primär für Netzzugänge über serielle Verbindungen eingesetzt. Das allgemein akzeptierte Verfahren besteht nun darin, Netzwerkprotokolle (z.B. IP) in PPP einzupacken, um mit dieser Information nach Auspacken beim Benutzer das Netzwerkinterface über die serielle Verbindung quasi zu verlängern. Die Protokollstruktur zeigt Abb 1.1 (Encapsulation im WAN-Netz: ISDN, Modem, leased line).

Das PPP-Protokoll handelt Verbindungsaufbau, -abbau, Authentisierung und Kompression aus, zusätzlich wird die Zuverlässigkeit der Link-Verbindung überwacht. Ausserdem enthält jeder PPP-Header eine Beschreibung des eingerahmten Protokolls. Üblicherweise wird IP über PPP via Point-to-Point Verbindungen eingesetzt. In den meisten Fällen wird dem Benutzer bei jedem neuen Login eine neue IP-Adresse (dynamic IP) aus einem Pool des Servers zugeteilt. Obwohl diese Systeme immer nur für die Zeit, in der sie sich eingewählt haben, am weltweiten Internet sichtbar sind, schützt dies trotzdem nicht vor Attacken, da der gesamte Adressbereich gescannt wird. Bei erfolgreichem Angriff kann z.B. Software (Virus, Backdoor) auf diesem Rechner installiert werden. Die Kombination von Backdoor/Password-Sniffer ist besonders gefährlich, weil sie auch jeden Firewall

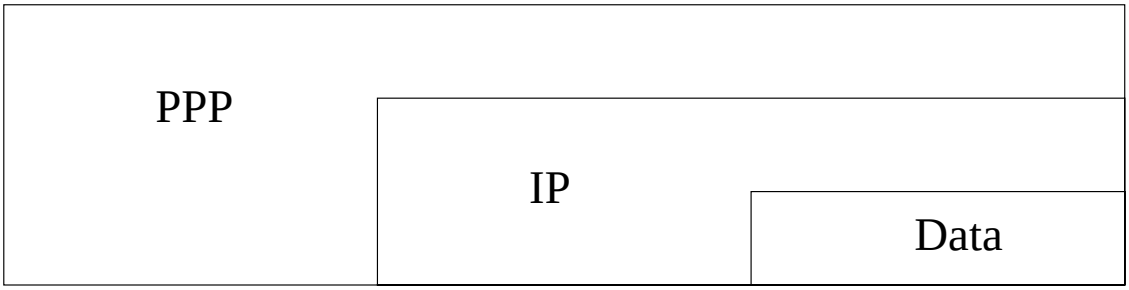

Abbildung 1.1: Encapsulation im WAN-Netz (ISDN, Modem, leased line)

umgehen kann. In diesem Falle ist die dynamische Adressvergabe sogar sicherer als die üblicherweise statischen Adressen bei xDSL und Cable Modems (24 h Betrieb). Oft wird dies umgekehrt gesehen, da unzulässige Aktivitäten des Benutzers im eigenen Netz bei statischer Adressvergabe besser identifiziert werden können.

Die geschilderten Gefahren machen es zunehmend erforderlich, neben einfachen Sicherungsmaßnahmen auf Benutzer- und Serverseite die komplette PPP-Sitzung zu verschlüsseln. Hier bieten sich zunächst das Protokoll ssh (secure shell), aber auch VPNs für Dial-In Zugänge in unterschiedlichen Ausführungsformen (Protokollen) an.

Kapitel 2

Einfache Sicherungsmaßnahmen auf Benutzer- und Serverseite

Den Benutzern wird dringend empfohlen, einen persönlichen Firewall zu installieren und in geeigneter Weise zu konfigurieren. Hier bieten sich z.B. TCPWrapper und AtGuard an. Die Auswertung der Logs zeigt oftmals überraschend viele Verbindungen, die der Benutzer normalerweise nicht erwarten würde (eye opener).

Modems sind willkommene Ziele für Hacker, da einzelne Rufnummern, die für Dial-In konfiguriert sind, erkannt werden können. Deshalb sollte auch nur eine einzige Rufnummer für den Zugang existieren. Dial-Out (nicht Rückruf) sollte sowieso nicht möglich sein, da so illegale Zugriffe deutlich erleichtert werden. Während die Modemzugänge also sinnvollerweise nur unidirektional konfiguriert werden sollten, verhalten sich übernommene PPP-Verbindungen über die TCP/IP Protokolle bidirektional. Vor allem sollten Konfigurationen, die Dial-Out mit Output Devices beinhalten, unbedingt vermieden werden, da sonst TCP/IP Verbindungen direkt aus dem LAN auf die ISDN/Modem Ports möglich werden. Als Beispiele seien hier telnet oder ping Verbindungen aus dem LAN heraus auf diese Ports genannt, über die illegale Verbindungen beliebig in die Irre geführt oder auch gleich abgehängt werden können (ping -p [+++ atH0]).

Die Einwählpunkte sollten grundsätzlich defensiv konfiguriert sein, d.h. alle Konfigurationselemente müssen so gesetzt sein, dass die volle Bandbreite fehlerhaften Benutzerverhaltens zu keiner Sicherheitslücke beim Server führt. Hier handelt es sich meist um Hunderte von Einzelparametern, die daraufhin optimiert werden müssen. Auch sollten wichtige Traps für einen Alarm Server aktiviert werden, damit Fehlereignisse besser identifiziert werden können. Hier helfen natürlich auch die Aufzeichnungen im Log- (und ggf. Accounting) Server weiter. Weiterhin müssen bei offenen Wählverbindungen die zugehörigen Netzverbindungen getrennt werden, da diese sonst ohne Authentisierung übernommen werden könnten. Das Modem muss nach der Unterbrechung wieder mit einem definierten Profil initiiert werden. Umgekehrt müssen bei hängenden Netzverbindungen die zugehörigen ISDN/Modem Ports zurückgesetzt werden. Das Modem muss dies erkennen und neu initiiert werden. Der Server sollte auch bei Nichtaktivität des Benutzers nach einer festen Vorgabezeit die Verbindung trennen (inactivity timeout). Der Administrator des Access Servers sollte nicht darauf vertrauen, dass ein entsprechendes Timeout beim Benutzer konfiguriert ist.

Kapitel 3

Secure Shell (ssh) und Virtual Private Networks (VPN)

3.1 Secure Shell (ssh)

Nach Einrichtung dieser Sicherungsmaßnahmen auf Benutzer- und Serverseite ist der nächste logische Schritt, eine möglichst einfache Stufe einer verschlüsselten Datenverbindung anzustreben. Hier bietet sich ssh an, weil dieses Protokoll auf einfache Art die gewünschten Anwendungen durch Umlenkung ihrer TCP Ports (via ssh) verschlüsseln kann. Ssh verschlüsselt die Anwendung des Benutzers bis ins eigentliche Zielsystem, die wichtige Zusatzinformation des Netzwerklayer bleibt hier aber ungeschützt. Der Zugang über ssh ist in den USA bereits sehr weit verbreitet. Für das FZJ gilt, dass ssh als nächste logische Fortführung auf dem Wege zu einer sicheren Datenkommunikation verpflichtend gemacht werden sollte, zumal dies für jeden Benutzer relativ einfach zu realisieren wäre. Für die weitere Zukunft könnten VPNs in ihren verschiedenen Ausführungsformen (Protokollen) eingesetzt werden, z.B. das unter Sicherheitsaspekten einheitliche und sehr weitreichend ausgelegte Protokoll IPSec (IP Security Standard).

3.2 Vitual Private Networks (VPN)

3.2.1 Was ist VPN und wofür wird VPN benötigt?

Virtuelle Private Netzwerke schaffen den Benutzern flexible Möglichkeiten, den zunehmenden Bedarf für externe Zugriffe auf das eigene Unternehmensnetz kostengünstig und sicher zu gewährleisten. In dieses Konzept können natürlich nicht nur der Zugang einzelner Benutzer, sondern auch bisherige LAN zu LAN Verbindungen, z.B. für die Anbindung von Firmenniederlassungen, einbezogen werden. Vor allem können auf diese Weise sichere Subnetze über ansonsten unsichere Netze miteinander verbunden werden. Die meist dedizierten Standleitungen zwischen den LANs können so durch deutlich preiswertere VPN-basierte, verschlüsselte Virtual Leased Lines (VLL) ersetzt werden, die einerseits der beschriebenen LAN-Kopplung, dann aber auch für den Internet-Zugang der Außenstelle genutzt werden können. Hier können bei geeigneter technischer Ausstattung (z.B. Tunnel Switch) weitere Tunnel eröffnet oder der Benutzer einem virtuellen LAN (VLAN) zugeordnet werden. Der virtuelle Einwählpunkt des Benutzers wird hier mit Hilfe der Tunneltechnologie quasi ins Ziel-LAN verlagert.

Virtuelle Private Netzwerke stellen Verbindungen zur Verfügung, die sich für den Benutzer wie eine eigene Standleitung oder ein privater Tunnel darstellen, obwohl der Transportmechanismus

über eine bereits vorhandene, gemeinsame (öffentliche) Netzinfrastruktur betrieben wird. Für den Benutzer ändert sich im äusseren Ablauf nichts, er betreibt wie bisher eine normale Point-to-Point Verbindung (PPP), allerdings über einen für ihn exklusiv bereit gestellten (fiktiven) Tunnel (symbolisch: über LAN-Wolke exklusiv betriebene feste Kabelverbindung). Wenn zusätzlich ausreichende Verschlüsselungsalgorithmen eingesetzt werden, sind Integrität und Authentizität der Benutzerdaten gewährleistet.

Im Grunde ist die Technik des VPN sehr einfach: ein entfernter Einzelbenutzer (remote access client) schickt nach wie vor einen Datenstrom von PPP-Paketen an einen Zielserver (remote access server), bei LAN zu LAN Kopplung schickt ein Router des einen LAN seine Pakete zu einem Router des anderen LAN. Neu ist eigentlich nur, dass der Datenverkehr - nach einmaliger Installation und Konfiguration geeigneter VPN Hard- und/oder Software - durch einen Tunnel über ein gemeinsames Netzwerk geführt wird.

Die Pakete, die in diesem gesicherten, quasi privaten Tunnel verschickt werden, beinhalten für sich wiederum eine (oft in PPP) eingepackte Verbindungsinformation, die erst am Tunnelende wieder ausgepackt wird. So kann sehr unterschiedlicher Netzverkehr, z.B. Protokolle höherer Layer, wie IPX, DECnet, NetBEUI oder sogar innere IP-Pakete, von unterschiedlichen Quellen durch verschiedene Tunnel über dieselbe Netzinfrastruktur transportiert werden (Multiprotokoll VPN's). Wesentliche Komponenten eines Tunnels sind:

- ein Tunnel Initiator (TI),
- ein allgemein zugängliches Netzwerk (Router),
- ein Tunnel Switch (optional),
- ein (oder mehrere) Tunnel Terminator(en) (TT),
- ein Verschlüsselungsalgorithmus.

Ein TI kann auf verschiedene Arten realisiert werden: auf dem Endgerät des Benutzers durch eine geeignete VPN-ertüchtigte Dial-up Client Software, einschl. gewünschter Sicherheitsmerkmale (Windows98, NT), im Büro durch einen VPN-fähigen Router, oder beim NSP Point Of Presence (POP) durch einen entsprechenden Konzentrator. Die VPN-Initiierung kann also sowohl direkt beim Einzelbenutzer/Aussenbüro (NSP ist dann Router) oder auch beim NSP (NSP ist dann VPN-Gateway) erfolgen.

Ein TT ist meist ein VPN Gateway (optional Tunnel Switch), der oft von einem RADIUS-Server (RADIUS = Remote Authentication Dial In User Service) für die Benutzerkennung/Security unterstützt wird. Moderne und leistungsfähige Tunneling Devices sind zudem noch mit einer aufwändigen Hardware-basierten Verschlüsselung (encryption) ausgestattet. Hier wird die sonst Prozessorintensive Verschlüsselung von einem Spezialchip übernommen (z.B. 3Com Pathbuilder S5xx: 100 Mbps, 3DES Verschlüsselung). Nur diese Ausstattung garantiert, dass on-line ein schneller und damit ausreichend sicherer Tunnel über die gemeinsame Netzinfrastruktur gewährleistet werden kann.

Als Quintessenz kann festgehalten werden, dass die VPN-Tunneltechnologie bei richtiger Auslegung eine sichere und performante Lösung sowohl für Einzelbenutzer als auch LAN zu LAN Verbindungen gewährleistet und bei entsprechender Vereinbarung mit dem NSP eine deutliche Gebührenersparnis für Benutzer (Mitarbeiter) und Firma bietet. Ein weiterer wichtiger Aspekt der VPN-Technologie liegt in der möglichen Auslagerung der bisherigen ISDN/Modem Pools (outsourcing). Es könnten zudem noch die Konfiguration und Benutzerbetreuung nach aussen vergeben werden. Dabei sollte aber unbedingt beachtet werden, dass das Security-Management (Benutzerprofil) auch weiterhin in der eigenen Firma verbleibt und hier überwacht wird. Dies kann besonders

effektiv im Zusammenwirken mit einem Tunnel Switch realisiert werden, der bei Bedarf die Benutzer nach bestimmten Kriterien über weitere Tunnel unterschiedlichen Zielsegmenten (ggf. auch Extranet) oder auch bestimmten VLAN's zuordnen kann. Die Firewall Funktionalität des Tunnel Switch kann besonders einfach realisiert werden, indem z.B. nur noch die Tunneling Protokolle durchgelassen werden. Der (innere) Firewall kann so erheblich entlastet und damit einfacher und effizienter ausgelegt werden. Durch den Einsatz eines VPN kann bei Bedarf sogar ein sicheres, Web-basiertes Netzwerk-Management betrieben werden.

3.2.2 Realisierung von VPN's

VPN-Techniken mit Verschlüsselung sind auf dem besten Wege, sich zu einem Standardverfahren für die sichere Kommunikation über IP-Netze oder das Internet zu entwickeln. Dabei vereinigt die VPN-Netztechnik für den Zugangsbereich einen guten Kompromiss zwischen Sicherheit und Netzdurchsatz (Performance) und bietet zudem meist den (globalen) Zugang zum lokalen Tarif. Neben den Verfahren für die Zugangskontrolle, des Netzwerk-Management und der Performance (Interoperabilität unterschiedlicher Hersteller) spielen die Aspekte der Verschlüsselung (Generierung, Verwaltung, Zertifizierung) eine besondere Rolle.

Das allgemein akzeptierte Verfahren zum Aufbau von VPN-Tunnel besteht nun darin, Netzwerk-Protokolle (z.B. IP) wie beim WAN (Abb 1.1) in PPP einzupacken und dieses Gesamtpaket dann als neue Daten mit einer weiteren IP-Adresse über einen Tunnel zu transportieren (Abb 3.1: Encapsulation im IP-Netz). Zum Transfer dieser Pakete über das gemeinsam genutzte IP-Netzwerk werden nur die IP-Adressen der beteiligten Security-Gateways (Source / Destination) verwendet. Erst nach dem Entrahmen dieser Pakete im Zielsystem werden die eigentlichen, bisher verborgenen IP-Adressen verfügbar.

Dieses Verfahren wird Layer 2 Tunneling genannt, da nach dem Vorgang des Einrahmens die jetzt neu definierten Daten über ein Layer 2 Protokoll als Passenger abgewickelt werden. Anders ausgedrückt stehen beide Protokolle PPTP/L2TP beim Layer 2 Tunneling für eine Technologie, bei der ihre Tunneling Header das Layer 2 Protokoll PPP einrahmen, die dann wiederum zum Transport über das Netzwerk von einem IP-Header eingerahmt werden (Abb 3.1). Innerhalb vom PPP können die verschiedensten Protokolle eingerahmt werden, z.B. höhere Protokolle wie z.B. IPX, DECnet, NetBEUI oder auch ein inneres IP-Paket. Als Ergebnis kann also festgehalten werden, dass Layer 2 Tunneling also Multi-Protocol-VPN's unterstützt. Lösungen, die nur die ursprünglichen Nutzdaten verschlüsseln, sind nicht sicher genug, weil viele Informationen auf der Netzwerkschicht (network layer) transportiert werden.

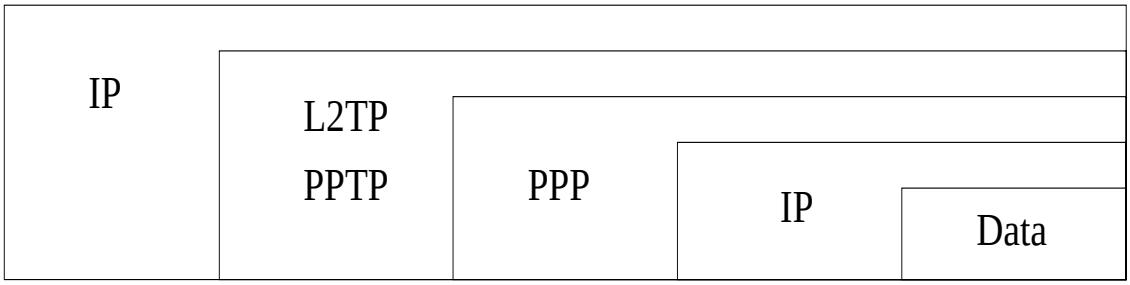

Abbildung 3.1: Encapsulation im IP-Netz (Layer 2 Tunneling)

Alternativ können die Netzwerkprotokolle auch direkt in ein Tunnelprotokoll eingekapselt werden (z.B. VTP: Virtual Tunneling Protocol von 3Com). Dieses Verfahren wird Layer 3 Tunneling genannt, da der im o.g. Sinne definierte Passenger ein Layer 3 Protokoll ist (Abb 3.2).

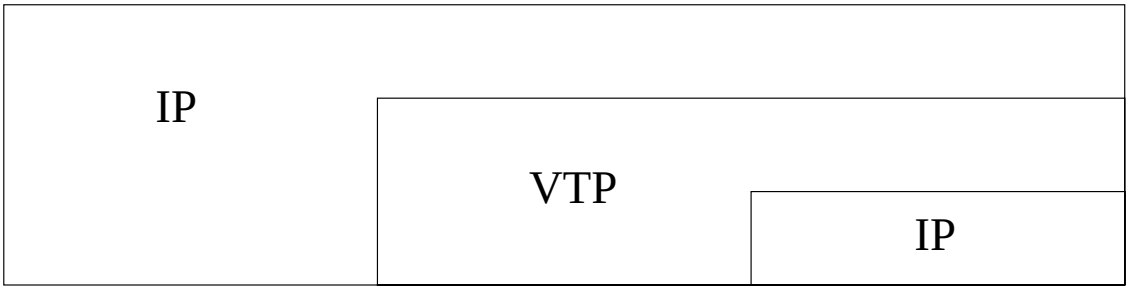

Abbildung 3.2: Virtual Tunneling Protocol (Layer 3 Tunneling)

Layer 2 Tunneling ist besser skalierbar als Layer 3 Tunneling, da dieses Verfahren unabhängig von Applikationen und Netzwerktypen arbeitet. Zudem ist es für jede Art von Informationen (Sprache, Daten, Bewegtbilder), die über Router transportiert werden, einsetzbar.

Gegenwärtig ist das Point-to-Point Tunneling Protocol (PPTP) von Microsoft/3Com wohl das am meisten eingesetzte Protokoll für VPN-Netzwerke (integriert in Win98/NT), wird aber zunehmend von dem Layer 2 Tunneling Protocol (L2TP) abgelöst. Letzteres vereint die besten Eigenschaften von PPTP und dem sog. Layer 2 Forwarding Protocol (L2F), entwickelt von Cisco. PPTP und L2TP bieten mehrere Vorteile gegenüber dem Layer 3 Tunneling:
(1) sie ermöglichen (trotz evtl. outsourcing) das eigene Security Management, wie Benutzer-Validierung, Zugangsberechtigung und Netzwerk-Adressierung. Dies wird durch den Empfang getunnelter PPP-Pakete ermöglicht.
(2) sie ermöglichen Tunnel Switching. So kann der Tunnel beendet (TT) und mit Hilfe der ausgepackten Benutzerinformation ein neuer Tunnel zu einem oder weiteren TT's initiiert werden. Tunnel Switching erweitert also die PPP-Verbindung zu einem weiteren TT.
(3) sie ermöglichen feiner abgestufte Zugangsversionen am Firewall oder den internen Servern. Durch die verfügbare Benutzerinformation können unterschiedliche Datenquellen berücksichtigt werden. Dies ist bei Layer 3 Tunneling prinzipiell nicht möglich, da die vom NSP eingehenden Pakete nicht unterschieden werden können.

Sichere VPN's erfordern natürlich Security-Protokolle für die Pakete, die in den Tunneln transportiert werden. Diese Protokolle ermöglichen den Hosts, eine Verschlüsselung und digitale Signaturtechniken auszuhandeln, um Datenherkunft (authentication) und Vertrauenswürdigkeit (encryption) zu gewährleisten.
Im Windows DFÜ-Netzwerk (Microsoft) ist zur Datenverschlüsselung das Protokoll Microsoft Point-to-Point Encryption (MPPE) integriert. Eine 40 (unzureichend) und 128 Bit Version sind für Win98/NT im PPTP integriert. MPPE verschlüsselt die PPP-Pakete beim Client, bevor sie in den PPTP-Tunnel eintreten. Sobald der Client mit dem Tunnel Terminator TT die PPP-Aushandlung abgeschlossen hat, wird die Sitzung mit den verschlüsselten Daten initiiert. Zur Authentifizierung der Benutzer wird hier ein verbessertes Challenge Handshake Protocol (CHAP) eingesetzt. Übrigens können Interim Tunnel Switches die PPP-Pakete nicht entschlüsseln.
In der Praxis verwenden viele VPN-Benutzer für die Verschlüsselung der Nutzdaten symmetrische Algorithmen wie DES/3DES, zum Austausch der Schlüssel selbst werden asymmetrische Public-Key Verfahren, wie z.B. RSA, eingesetzt. Da die gängigen Schlüsselalgorithmen allgemein bekannt sind, hängt die Wirksamkeit der Verschlüsselung von einer Kombination der folgenden Faktoren ab:
(1) **Schlüssellänge:** sollte deutlich größer als 56 Bit sein. Je länger ein Schlüssel ist, desto schwerer ist er zu knacken.
(2) **Austausch und Verwaltung von Schlüsseln:** Internet Key Exchange (IKE) setzt sich als Verfahren durch, weil unterschiedliche Schlüssel verwaltet werden können.
(3) **Schlüsselwechsel**: sollte regelmäßig und dann automatisch (auch während einer Sitzung) durchgeführt werden.

(4) **Schlüsselgenerierung**: wird am besten über Hardware-generierte Codes realisiert. Software-gestützte Techniken nutzen bekannte Algorithmen.
Ein weiteres wichtiges Auswahlkriterium ist die sog. Zertifizierung (Zugangskontrolle). Als Zertifizierungsinstanz im Rahmen einer Public Key Infrastructure (PKI) kommen entweder die eigene (meist größere) Firma, der Hersteller des VPN-Equipments (bei outsourcing) oder ein NSP, der VPNs vermarktet, in Frage. Im Rahmen einer solchen PKI müssen die Mitglieder des VPN registriert und möglichst automatisch und sicher identifiziert werden, d.h. die Daten werden verschlüsselt übertragen (evtl. digitale Signaturen). Dies alleine reicht aber noch nicht: es ist zusätzlich eine wirksame Zugangskontrolle nötig (Stichwort: Firewall). In diesem Zusammenhang ist u.a. das Betriebssystem einer VPN-Firewall wichtig. Hier ist ein Hardware-basiertes System (meist proprietär) manchmal besser geeignet als Betriebssysteme wie Unix oder NT (bekannte Sicherheitslöcher). Ausserdem kann die Art und Weise, wie das System ein- und ausgehende Daten (auch die verpackten Nutzdaten) analysiert, den Zugang zu bestimmten Bereichen des Netzes beeinflussen.

3.3 IPSec: IP Security Architektur

Das von der IETF standardisierte Internet Protocol Security (IPSec) ist im Request for Comments (RFC) 2401 näher beschrieben siehe Anhang). Es umfasst die VPN Benutzer-Authentifizierung, die Verschlüsselung / Entschlüsselung der Tunnelinformation (encrypting / decrypting) und Austausch / Management der Schlüssel (Unterstützung von IPSec Key Management Protocol). Vor allem aber muss auch die Interoperabilität der VPN-Lösungen verschiedener Hersteller gewährleistet sein. Dies ist beim Einsatz von IPSec weitgehend erfüllt. Nur wenn alle oben genannten Gesichtspunkte optimal ineinander greifen und funktionieren, kann ein guter Gesamtdurchsatz (performance) erreicht werden. Hier spielt u.a. auch die bereits erwähnte Hardware-basierte Verschlüsselung eine besondere Rolle. IPSec unterscheidet zwei Modi: den Transport- und den Tunnelmodus.

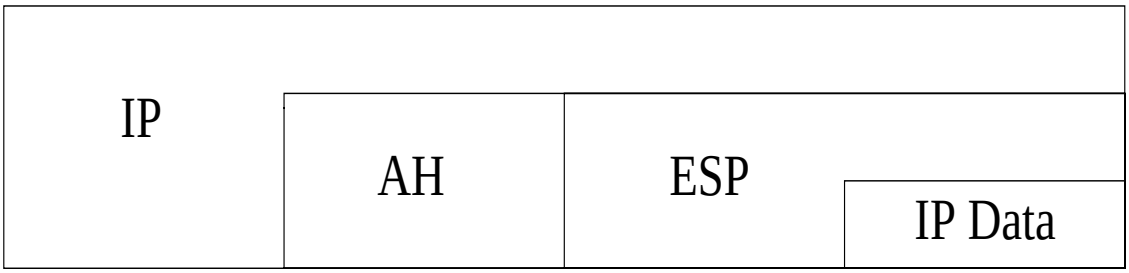

Abbildung 3.3: IPSec Transportmodus

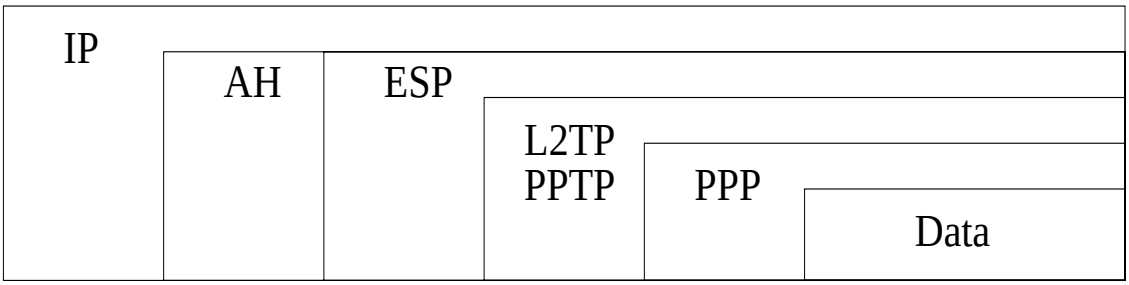

Abbildung 3.4: L2TP/PPTP mit IPSec im Transportmodus

Der **IPSec Tranportmodus** stellt die Standardmethode dar, sichere VPN-Tunnel bei einer Ende-zu-Ende Übertragung (ab Layer 4) zu betreiben, z.B. durch den Einsatz eines Rechners mit einem Verschlüsselungsprogramm, das direkt über ein IP-Netz mit einem Zielhost kommuniziert. In diesem

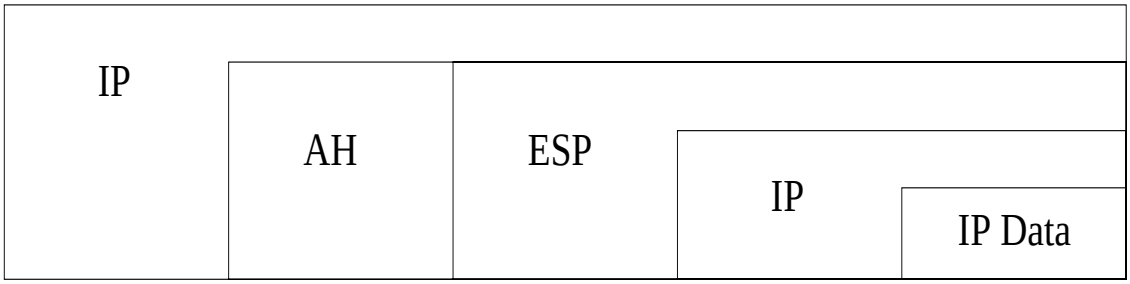

Abbildung 3.5: IPSec Tunnelmodus

Modus wird IPSec eingesetzt, um die IP-Frames zwischen den beiden beteiligten Rechnern sicher zu transferieren. Einer dieser Rechner kann hier ein Layer 3 Tunnel Switch oder TT sein. IPSec realisiert die Authentifizierung und Verschlüsselung (meist) für das äussere IP-Paket. Dazu werden die IPSec-internen Protokolle Authentication Header (AH) und Encapsulated Security Paylod (ESP) eingesetzt (Abb 3.3). Details zur Funktion und Einbettung dieser beiden Protokolle in IPSec können dem Anhang IPSec (RFC 2401) entnommen werden. Da AH und ESP bereits die Security auf höherer Ebene bieten, kann man hier (nicht muss) auf die PPP-level Security, z.B. mit MPPE, verzichten (MPPE: integriert z.B. in PPTP). Damit verzichtet man natürlich auf die Multi-Protokoll Unterstützung, die das Einrahmen anderer Netzwerkprotokolle unter PPP bietet. Man kann diese PPP-Eigenschaften aber bei Bedarf wieder integrieren, wie aus Abb 3.4 ersichtlich ist und kann so einen graduellen Übergang auf die Unterstützung eines reinen IP-Netzes vorbereiten.

Der **Tunnelmodus** stellt eine alternative Methode zum Aufbau von VPN-Tunnel in reinen IP-Netzen dar und befindet sich hier in Koextistenz mit dem L2TP-Protokoll für Multiprotokoll- Netzwerke. Während Einrichtungen mit reinen IP-Netzen wohl schnell zum IPSec Tunnelmodus übergehen werden, wird sich die Mehrzahl nach wie vor für die Multiprotokoll Unterstützung, aber auf der Basis des L2TP-Protokolls, entscheiden. Der IPSec Tunnelmodus wird auch oft Layer 3 Tunneling genannt, weil die Payload hier ein IP-Paket (Layer 3) und kein PPP-Paket (Layer 2) ist. Aus diesem Grunde erlaubt IPSec oftmals (im Gegensatz zu Layer 2 Tunneling) nur Maschinen- (und keine Nutzer-) Authentifizierung. IPSec kann zur Lösung dieses Nachteile mit einem Layer 2 Protokoll kombiniert werden. Die IP-Payload wird beim IPSec Tunnelmodus wiederum von einem anderen IP-Paket eingerahmt, das hier als Tunneling Protokoll fungiert. Weil IP-basierte Tunnel via Router hinweg transportiert werden können, besteht hier kein Bedarf für einen Tunnel Switch. Vergleichbare Eigenschaften können durch einen Router erreicht werden, der die ankommenden Tunnel zu evtl. mehreren secure gateways weiterleitet. Diese stehen vom Namen her in Analogie zu den bereits bekannten TT's. Sie müssen dafür ausgelegt sein, IPSec Pakete zu empfangen und auszuwerten. Weil Tunnel Switches nicht nur VPN-Gateways, sondern auch eine normale Routerfunktion ausüben, können sie natürlich auch IPSec Tunnel zu secure gateways weiterleiten (forwarding). An den Tunnelenden können TT's vieler Hersteller relativ einfach durch Rekonfiguration der Software auf die Funktion als IPSec secure gateway umgestellt werden. Die meisten Geräte unterstützen gleichzeitig PPTP, L2TP und beide IPSec Modi.

Da die IPSec-Kommunikation auf Ebene 3 erfolgt, müssen die (VPN-) Gateways den gesamten ein- und ausgehenden Datenverkehr prüfen, auch die Datenpakete, die ungeschützt über das Netz laufen. Sie müssen also für den erforderlichen Durchsatz ausgelegt sein. Die Bandbreiten des VPN-Gateways (Latenzzeit) und des Netzes müssen also vergleichbar sein, anderenfalls gehen evtl. Pakete verloren. Aus diesen Überlegungen heraus sind Hardware-basierte VPN-Gateways vorzuziehen, da nicht der Zentralprozessor, sondern evtl. mehrere Spezialprozessoren für die Sicherheitsfunktionen bei IPSec und IKE zuständig sind. Dies ist auch nötig, da hier entgegen den üblichen Gateway Routingverfahren nicht nur der Header, sondern das gesamte Paket mit den Daten bearbeitet werden muss. Ausserdem beanspruchen IPSec-Algorithmen erheblich mehr Rechenzeit als übliche

Routingverfahren. Beispielsweise können so die Verarbeitung des IP-Kopffeldes, einschl. Tunneling und Generierung des IPSec-Headers und das Codieren und Decodieren der Daten voneinander getrennt werden. Hardware-basiertes IKE ist für das Netzwerk Management besonders wichtig, da damit die VPN-Sites in separate Subnetze (mehrere 1000) aufgeteilt werden können (VLANs).

Zuammenfassend kann gesagt werden, dass der IPSec-Standard sich in kurzer Zeit zum wichtigsten Protokoll für den sicheren Datentransfer über VPN-Netze entwickelt hat. Bei IP-basiertem Tunnelverkehr unterstützt IPSec die Interoperabilität verschiedener Produkte unterschiedlicher Hersteller zum Auf-/Abbau von Tunneln (TI/TT). Der IETF-Standard besteht aus einem Satz von IP-Level Protokollen zur Aushandlung der Verschlüsselung und digitaler Signaturmethoden zwischen zwei IP-Partnern. IPSec wird für den Einsatz von L2TP empfohlen, für IPv6 ist IPSec verpflichtend. IPSec ist robuster als MPPE, es umfasst authentication, encryption und privacy. Ausserdem kann mit IPSec über den Tunnel Terminator hinaus das endgültig bestimmte Endgerät adressiert werden. Ein weiterer wichtiger Vorteil von IPSec ist, dass die Mechanismen für Authentication und Security lose mit den Key Management Systemen gekoppelt sind, um einfache, spätere Erweiterungen zuzulassen (ohne Änderung der Security Mechanismen).

VPNs sollten so konzipiert werden, dass die firmenseitigen Einwählpunkte in ein evtl. bestehendes oder neu zu planendes Firewallkonzept integriert werden. Diese Gesichtspunkte werden im folgenden Kapitel dargestellt.

Kapitel 4

Einwählpunkte und Firewallkonzepte

4.1 Konzept für Einwählpunkte

Wie bereits oben erwähnt, sollte die NAS-Einwahl in ein bestehendes oder neues Firewall-Konzept integriert werden. Der U.S.Robotics-Server kann in seinem jetzigen Betriebszustand zunächst weiter eingesetzt werden, da er stabil läuft. Ein Outsourcing sollte möglichst vermieden werden, auf jeden Fall muss das Security Management im FZJ verbleiben.

4.2 Firewall mit geschirmtem Zwischennetz

Der Firewall wird üblicherweise in einer sog. demilitarized zone (DMZ) installiert. Er befindet sich also weder LAN extern noch intern, sondern in einem besonderen Zwischennetz. Die U.S.Robotics (NAS Server) und RADIUS Server sollten mit ihrem jetzt schon bestehenden, separaten Zwischennetz in diese DMZ integriert werden. Auf diese Weise bleiben diese Systeme für weiter gehende Konzepte offen. Zum Beispiel können bei einem eventuellen Einsatz eines Tunnel Switch neue Tunnel zu weiteren Zielen im LAN eröffnet werden, alternativ kann die Information auch bestehenden V-LANs zugeordnet werden.

4.3 Bereinigung der Zugangsversionen

Die lange Erfahrung im Kontakt mit den Benutzern hat gezeigt, dass für den Rückruf in den verschiedenen Versionen und Betriebssystemen ein erheblicher Beratungsaufwand erforderlich ist. Deshalb wird vorgeschlagen, den Rückruf durch den sog. freecall (0800) zu ersetzen. Dies soll aber nur für die Rückrufbenutzer möglich sein, die definitiv auf ssh oder VPN (IPSec) umgestellt haben. Hier sollte eventuell auch der 0800 Regiotarif untersucht werden, der diesen gebührenfreien Dienst nur im Umkreis von 50 km anbietet (Aachen, Köln, Düsseldorf sind eingeschlossen). Hier muss zukünftig aber unbedingt ein Kontingent pro Organisationseinheit (OE) eingeführt werden, da dieser kostenintensive Dienst sonst ungerecht und willkürlich verteilt ist. Dies stärkt zudem die Eigenverantwortung der einzelnen OE. Außerdem sollte unbedingt ein Session Timeout (z.B. 1 Stunde) eingeführt werden. Wenn jeder Benutzer dies weiß, sollte es hier keine weiteren Probleme geben. Das schon bestehende expiration date sollte unbedingt beibehalten werden. Der Verzicht auf den Rückruf bietet aber auch eine deutliche Entlastung für die U.S.Robotics Server, da die internen Benutzereintragungen für PPP-Rückrufbenutzer entfallen (Speicherproblem auf den Servern). Damit befinden sich dann alle Benutzer relevanten Eintragungen nur noch auf dem RADIUS Server, Teilkonfigurationen auf den U.S.Robotics Servern entfallen. Bei den Benutzern ohne Rückruf

kann an den Tarif-Share 0180 (Folgeziffern 1 bis 5) gedacht werden (Gleichstellung aller Ortsnetzzugänge). Zum Beispiel zahlt der Benutzer bei der Folgeziffer 1 nur den City Tarif, der Tarifnehmer den Rest zur vollen Gebühr. Alternativ kann eventuell auch ein sog. Call by Call Zugang bei einem anderen Provider in Frage kommen. Letzteres hat aber den Nachteil, dass der Benutzer kein interner JuNet Benutzer mehr ist und ihm damit bestimmte interne Dienste nicht mehr zugänglich sind.

Kapitel 5

Anhang: IPSec (RFC 2401)

IPSec benutzt 2 Protokolle, um einen sicheren Datentransfer zu erreichen: Authentication Header (AH) und Encapsulating Security Payload (ESP).

AH garantiert die (verbindungslose) Integrität der Datenquelle, also ihre Zuverlässigkeit (origin authentication).
ESP garantiert die Vertrauenswürdigkeit (confidentiality) der Daten (encryption). Es kann auch bei Bedarf zusätzlich die bei AH genannten Eigenschaften aushandeln.

AH und ESP dienen einer Zugangskontrolle, die auf der Verteilung kryptografischer Schlüssel und deren Management beruht. Beide Protokolle können also für sich allein oder in Kombination miteinander eingesetzt werden, um die gewünschten Sicherheitsstufen zu gewährleisten.
Jedes dieser Protokolle unterstützt 2 Modi: Transport- und Tunnelmodus. Im Tranportmodus bringen diese Protokolle in erster Linie Sicherheit für die oberen Protokoll-Layer, im Tunnelmodus wirken die Protokolle auf die getunnelten IP-Pakete.
IPSec erlaubt auch Benutzer-kontrollierte Mischversionen, z.B. zum Aufbau eines einzelnen verschlüsselten Tunnels zwischen 2 Security Gateways oder eines separaten verschlüsselten Tunnels für jede TCP-Verbindung zwischen jedem Paar von Hosts, die über diese Gateways Daten transferieren. IPSec beinhaltet geeignete Management-Funktionen, um Kombinationen von Sicherheitsstrategien aufzusetzen. Weil zur Realisierung dieser Security-Dienste Geheimschlüssel (cryptographic keys) ausgetauscht werden, beruht IPSec auf separaten Mechanismen (z.B. IKE), diese Schlüssel an der geforderten Stelle vorzuhalten (authentication / integrity - encryption).
RFC 2401 definiert sog. Security Associations (SA) zur Implementierung von AH, ESP oder AH+ESP. AH und ESP benutzen diese SA's und auch wichtige Funktionen von IKE. Per Definition ist einer SA eine sog. Simplex-Verbindung (nur eine Richtung) mit den zugehörigen Security Diensten zugeordnet und bezieht sich ausdrücklich entweder auf AH oder ESP (nicht beide). Für eine typische bi-direktionale Verbindung mit geforderten Sicherheitsaspekten müssen also z.B. 2 SA's realisiert werden.

Es gibt 2 Typen von SA's: Transport- und Tunnelmodus.
Eine Transportmodus SA wird zwischen 2 Hosts aufgebaut. Ein sog. Transport Mode Security Protocol Header erscheint sofort hinter dem IP-Header (+ Optionen) und vor jedem Protokoll der höheren Layer (z.B. TCP oder UDP).
Bei ESP wirken die Security-Dienste nur für die höheren Protokoll-Layers, nicht für den IP-Header (oder Erweiterungen), der dem ESP-Header vorausgeht. Bei AH wird der Schutz auf bestimmte Bereiche des IP-Headers ausgedehnt.
Eine Tunnelmodus SA wirkt prinzipiell auf einen IP-Tunnel. Wenn eine oder beide Seiten dieser SA Security Gateways sind, MUSS die SA im Tunnelmodus sein. Zwei HOSTS KÖNNEN aber auch

eine Tunnelmodus SA (transit traffic via security gateway) z.B. dann vereinbaren, wenn Probleme mit der Frakmentierung (oder Reassembly) der IPSec-Pakete oder multiple paths Probleme über mehrere Security Gateways erwartet werden.
Bei einer Tunnelmodus SA gibt es einen äusseren IP Header, der das IPSec-Ziel adressiert und einen inneren IP-Header, der die endgültige Zieladresse für das Paket beinhaltet. Der Security Protokoll-Header AH oder ESP) erscheint direkt nach dem äusseren und vor dem inneren IP-Header. Wenn AH im Tunnelmodus verwendet wird, werden bestimmte Bereiche des äusseren IP-Headers mit geschützt (wie vorher), aber natürlich auch das gesamte getunnelte IP-Paket (d.h. der gesamte innere IP-Header und die höheren Protokoll-Layer). Wird ESP verwendet, wird nur das getunnelte Paket geschützt, nicht Teile des äusseren Headers.

Zusammenfassend für den RFC 2401 gilt:

- Ein Host MUSS den Transport- UND Tunnelmodus unterstützen.
- Ein Security Gateway unterstützt nur den Tunnelmodus. Ausnahme: Security Gateway arbeitet im Transportmodus als Host, wenn Netzwerk Management-Funktionen übertragen werden (z.B. SNMP).
- Der jeweils in Aktion befindliche Security-Service einer SA hängt ab vom ausgewählten SA Modus, vom Security Protokoll, den Endpunkten der SA und von der Auswahl der Dienste innerhalb des Protokolls.
- AH bietet die abgesicherte Herkunft der Daten (origin authentication) und die verbindungslose Integrität der IP-Datagramme. Ausserdem wird ein Dienst gegen Hacker-Angriffe beim Denial of Service angeboten (anti replay partial sequence integrity). AH ist immer dann geeignet, wenn die o.g. Integrität der IP-Datagramme nicht gefordert oder erlaubt ist, z.B. Einschränkungen beim Einsatz der Verschlüsselung durch staatliche Verordnung). AH bietet zudem eine Absicherung von bestimmten Bereichen des IP-Headers (wenn speziell erwünscht). ESP bietet optional die Datenintegrität, der Grad der Absicherung hängt vom Encryption Algorithmus ab. ESP bietet auch optional denselben Authentication Dienst wie bei AH, auch den anti replay Dienst. Wenn nur die höheren Protokoll-Layer geschützt werden sollen, ist ESP die geeignete Wahl, zumal ESP schlanker als AH ist (rahmt ESP ein).
- Abgesicherte Herkunft der Daten (user authentication) und Datenintegrität (confidentiality, encryption) sind optional, aber EINER der beiden Dienste (Protokolle) MUSS ausgewählt werden.