I.I.R.-Konferenz

Virtual Private Networks (VPNs)

Relexa Hotel, Frankfurt am Main

19.-20. Januar 1999

Beitrag:

Sicherheitsmechanismen bei der Kommunikation über VPNs

AUTOR:

Dipl.-Ing. Kai-Oliver Detken
studierte Nachrichtentechnik an der
Hochschule Bremen und Informationstechnik
an der Universität Bremen. Nach dem Studium wechselte
er zum BIBA-Institut an der Universität Bremen, um im
EU- Bereich an Technologieprojekten zu arbeiten.
Heute ist er als Berater bei der OptiNet GmbH
tätig und für den Bereich ATM/Internet als Leiter des
Competence Center Future Knowledge (CC-FK)
verantwortlich.

Dipl.-Ing. Kai-Oliver Detken
OptiNet GmbH
Goebelstraße 46
D-28865 Lilienthal
Tel.: ++49-4298-9365-0
Fax: ++49-4298-9365-22
URL: http://www.optinet.de
E-Mail: detken@optinet.de
Private URL: http://kai.nord.de

Inhaltsverzeichnis

1 Einleitung

Das Internet erfreut sich einer enormen Beliebtheit und damit hohen Wachstumsraten. Die Teilnehmerzahlen steigen exponential an und lassen neben Problemen bei der Adreßvergabe, Routing, Echtzeitfähigkeit auch Sicherheitslücken erkennen. Durch die wachsende Verbreitung des Internets und dem zunehmenden Einsatz von Internet-Protokollen (IP) wird dabei der Schutz vor unbefugten Zugriffen auf das Unternehmensnetzwerk immer wichtiger. Zusätzlich werden immer mehr geldliche Transaktionen über das Internet durchgeführt sowie Geschäfte abgewickelt, die eine hohe Vertraulichkeit beinhalten müssen.

Allerdings ergeben sich durch die Anbindung an Netzwerke für ein Unternehmen und dessen Mitarbeiter eine Vielzahl zusätzlicher Kommunikationsmöglichkeiten und nutzbarer Dienstleistungen. Dabei sind alle Unternehmen, die direkt an ein WAN wie das Internet angeschlossen sind, durch diese Verbindung Angriffen auf das eigene Intranet ausgesetzt. Den Systemverwaltern der firmeninternen, lokalen Netzwerke (LAN) obliegt es, betriebsspezifische, programmtechnische und persönliche Daten vor dem externen Zugriff durch Unbefugte zu schützen. Im gleichen Maße müssen Daten der verschiedenen Dienstleistungen im Netzwerk aus dem Unternehmen das lokale Netzwerk aber auch verlassen dürfen. Zusätzlich sollen sie auch nur diejenigen Adressaten erreichen, für die die Daten letztendlich bestimmt sind.

Die Nutzung der implementierten Sicherungsmechanismen der am Markt gängigen Betriebssysteme reicht selbst bei optimaler Konfiguration heutzutage bei weitem nicht aus. Optionale Hard- und Software Mechanismen zur Erweiterung des Systemschutzes des lokalen Netzwerks sind ebenfalls unzureichend. Der empfindlichste Schwachpunkt ist der Knotenpunkt der Anbindung des lokalen Netzes an das WAN und der damit jederzeit mögliche, externe Zugriff auf jeden einzelnen Computer in dem lokalen Netzwerk. Der beste Schutz wäre demnach die Trennung der beiden Netze. Eine komplette physikalische Trennung scheidet aus, denn sie würde den notwendigen Datentransport verhindern. Ein globales Sicherheitskonzept muß also definiert werden, das die Kommunikationsstruktur berücksichtigt und Sicherheitslücken und Defizite kenntlich macht.

Weiterhin sind direkte Verbindungen über Virtual Private Networks (VPNs) in verteilter Umgebung von Interesse. Hier können Unternehmen über Tunnelmechanismen ein Intranet über die Unternehmensgrenze hinaus aufbauen. Dafür sind Verschlüsselungsverfahren notwendig, damit andere Teilnehmer nicht auf die sensitiven Daten des Unternehmens zugreifen können. Diese sind allerdings meist proprietär aufgebaut, so daß keine unterschiedlichen Produkte verwendet werden können.

2 Sicherheitsanforderungen an heutige Netze

Um ein Intranet eines Unternehmens nach außen hin abzusichern, sollte ein Sicherheitskonzept erstellt werden, um die Grenzen akzeptablen Verhaltens und die Redaktion auf Übertretung genau definieren zu können. Die Anforderungen an die Sicherheit unterscheiden sich dabei von den Auftraggebern, da unterschiedliche Organisationen verschiedene Sicherheitsanforderungen besitzen. Ein Sicherheitskonzept wird dabei aber jedem Firmentyp, ob Universität oder militärischen Einrichtungen, gerecht. Die Frage, ob eine Firewall im Unternehmen zur Absicherung der Internet-Anbindung notwendig ist, stellt sich aufgrund der Gefahren nicht mehr.

Eine Verbindung zum Internet wird über das öffentliche Netz zum nächsten Point-of-Presence (POP) eines Internet Service Providers (ISP) realisiert. Über geeignete Protokolle

wird dann über Wählverbindungen mittels analoger Modems, ISDN, X.25-Verbindungen oder unterschiedliche Standleitungen (DDV oder Festverbindungen) der Zugang zum Internet eröffnet. Die POPs sind wiederum untereinander und den internationalen Netzen verbunden, so daß eine transparente Kommunikation mit anderen Teilnehmern ermöglicht wird. Die ISP stellen eine eigene Infrastruktur untereinander bereit, die mit Peering Points ausgestattet sind. In einem Peering schalten Provider eigene Router in einem LAN zusammen und tauschen dort die Verfügbarkeit ihrer Netze aus. An einem Peering Point wechseln die Daten von einem Provider-Netz in das eines anderen Providers.

Computersysteme können im allgemein nicht hundertprozentig gegen Angriffe von außen geschützt werden. Es ist jedoch möglich, einzelne Gefahrenquellen deutlich zu minimieren. Das größte Gefahrenpotential geht dabei immer von den Benutzern des Computersystems aus, insbesondere von den Systemverwaltern bei starker Unachtsamkeit. Kein automatisiertes System ist in der Lage, einen versierten Systemverwalter bei der Überwachung eines Computers zu ersetzen bzw. ihn daran zu hindern, seine Machtfülle zu mißbrauchen. Ebenso bestehen oft Gefahren durch rechtmäßige Benutzer, die entweder aus Unachtsamkeit oder aus kriminellen Antrieben die Sicherheit des Systems gefährden, beispielsweise durch unbedachte Wahl von Kennworten oder Datentransfer mittels Disketten nach innen und außen. Die wichtigsten Punkte hierbei sind sogenannte programmierte Bedrohung (Programmed Threats) und die Bedrohung durch nicht autorisierte Eindringlinge. Je nach Herkunft und Absicht können diese mit mehr oder weniger Aufwand vom System ferngehalten werden.

Bei den programmierten Gefahren kann man folgende Typen unterscheiden:

- Viren (Viruses) befallen „normale“ Programme und verbreiten sich über diese weiter, indem sie meist den ausführbaren Code des Wirtsprogrammes modifizieren. Wird das infizierte Programm ausgeführt, versucht das Virus, weitere Programme zu infizieren.
- Würmer (Worms) breiten sich in einem Netz selbständig von Knoten zu Knoten aus, ohne jedoch andere Programme zu infizieren und richten im allgemeinen keinen Schaden, außer einem erhöhten Verbrauch der Ressourcen an.
- Trojanische Pferde (Trojan Horses) sind Programme, die von Benutzern ausgeführt werden und dabei an Stelle der gewünschten Aktion andere, unbeabsichtigte Seiteneffekte hervorrufen.
- Logische Bomben (Logic Bombs) werden meist in anderen ausführbaren Programmen versteckt und werden durch bestimmte Bedingungen ausgelöst, beispielsweise an einem bestimmten Tag oder wenn ein Mitarbeiter nicht mehr auf der Gehaltsliste steht. Meistens zerstören sie dann Daten oder setzen Viren frei.
- Hintertüren (Backdoors) sind Programmteile, mit deren Hilfe ein Zugriff auf das System unter Umgehung der Authentisierungsverfahren oder mit erhöhten Privilegien ermöglicht wird.

Neben den programmierten Gefahren gibt es vor allem Probleme, die durch die direkte Beteiligung von Personen entstehen. In solchen Fällen sollte man die Einschätzung der Vorfälle nach der Motivation eines sogenannten Crackers (nicht Hacker) vornehmen. An dieser Stelle wird deutlich zwischen Crackern und Hackern unterschieden. Hacker versuchen in ein System einzudringen, da sie sich für die Umgehung der Sicherheitsmechanismen interessieren. Sie zerstören dabei keine Daten und setzen keine Viren frei. So wie sie die Hintertür eines Intranets betreten haben, so verlassen sie das Netz auch wieder. Crak-

ker hegen hingegen von Anfang an kriminelle Absichten. Sie versuchen in ein Netzwerk einzudringen, um sich persönliche Vorteile zu beschaffen und eventuell Daten zu zerstören.

Die Unterschiede in den Motiven bestimmen im allgemeinen auch das Gefährdungspotential, das von solchen Vorfällen ausgeht. Beispielsweise wird der Hacker meistens keinen Datenverlust auslösen, es sei denn durch unbedarfte Vorgehensweise im fremden Netzwerk. Allerdings löst der Hacker bei Entdeckung durch den Netzwerkadministrator eine zeitraubende Untersuchung aus, um die Sicherheitslücken rechtzeitig stopfen zu können. Dies ist im Grunde ein relativ gewünschter Vorgang, da so die Lücken einer Firewall erkennt und beseitigt werden können. Mehr Probleme entstehen durch ambitionierte Crakker, die sich vorgenommen haben einen wirklichen Schaden im Netzwerk anzurichten und dieses Ziel auch mit einer gewissen Hartnäckigkeit verfolgen. Dabei hat der Bereich der Industriespionage bzw. der kriminellen Angriffsbemühungen statistisch deutlich zugenommen. Beispielsweise verzeichnen die Top-Level-Domäne COM (Commercial) laut Firewall-Systemen in den USA einen deutlichen Anstieg von Attacken.

Neben dem tatsächlichen Schaden wie Datenverlust, Datendiebstahl usw. entsteht bei allen Vorfällen mit Personen aus dem Hackerumfeld immer das Problem, die Integrität des Systems nach einer Attacke wieder sicherzustellen. Es kann notwendig sein, den kompletten Datenbestand des Unternehmens vom Band restaurieren zu müssen, um dies zu erreichen.

Tatsache ist auch, daß sich erfahrene Hacker mit immer raffinierteren Methoden Zugang zu Systemen verschaffen. Vor solchen Attacken kann man sich nur mit extrem gut gesicherten Zugangskontrollsystemen schützen. Für die weniger erfahrenen Cracker stehen dagegen mehrere automatisierte Werkzeugkästen zum Einbruch in ein Rechnersystem zur Verfügung. Teils wurden diese Tools als Hilfsmittel für Sicherheitsanalysen, teils auch gezielt für den Einsatz bei Einbruchsversuchen entwickelt. Diese Tools sind zwar nicht so gefährlich wie ein erfahrener Cracker, sind aber vollkommen ausreichend, um in ein schlecht geschütztes bzw. ungeschütztes System einzubrechen.

Um dem Intranet einen umfassenden Schutz bieten zu können, sollte ein globales Sicherheitskonzept erarbeitet werden, welches sich aus den folgenden Fragestellungen heraus ergibt:

- Vorhandene Infrastruktur
- Betriebssicherheit
- Remote Access Points
- Analyse des Sicherheitsgrads des Intranets im Unternehmen
- Analyse der Sicherheitslücken
- Anforderungen an das Netzwerk
- Firewall-Konzeption für Zugangskontrolle
- Verschlüsselungssysteme und Authentifikation
- Eingesetzte Virenscanner

Erst anschließend kann die Analyse erfolgen und Firewalls für den Schutz von außen implementiert werden. Zusätzlich sollte für diese Aufgabe ein Unternehmen hinzugezogen werden, da man sonst durch die eigene subjektive Sichtweise falsche Entscheidungen treffen wird.

3 Sicherheitslösung Firewall

Aufgrund der Angriffe, die von außen auf ein lokales Netzwerk einwirken können, stellt sich für ein Unternehmen nicht mehr die Frage, ob eine Firewall zur Erhöhung der Sicherheit eingesetzt werden soll. Vielmehr ist entscheidend, welche Firewall aus dem auf dem Markt verfügbaren Angebot für das eigene Unternehmen in Frage kommen könnte. Eine Entscheidungsgrundlage bietet dazu die Analyse der individuellen Kommunikationsprozesse von und zum Internet, die es abzusichern gilt. Die Firewall übernimmt dabei die Aufgabe einer Gateway, die ein Werkzeug für die Abbildung des Sicherheitskonzepts darstellt. Die Kommunikationsabläufe zwischen den Übergangspunkten werden an zentraler Stelle von der Firewall kontrolliert. Dabei ist die Richtung der Zugriffsversuche entscheidend. Es lassen sich drei Hauptaufgabenbereiche für die Überwachung des Intranets definieren:

- Absicherung von Outbound-Zugriffen (Benutzerzugriff auf das Internet aus dem Intranet)
- Absicherung von Inbound-Zugriffen aus dem Internet auf öffentliche Angebote beziehungsweise Dienste (z.B. eigene Webseite) durch anonyme Benutzer
- Absicherung von Inbound-Zugriffen auf Dienste für einen geschlossenen, definierten Teilnehmerkreis (z.B. Heimarbeiter, Außendienst, Geschäftspartner)

Nicht alle Systemlösungen bieten alle drei Bereiche an, da dies auch eine höhere Komplexität der Realisierung nach sich ziehen würde. Beispielsweise sind die Verzögerungen, die durch eine Firewall entstehen, für Echtzeitanwendungen kritisch. Je komplexer die Firewall für höchstmögliche Sicherheit konfiguriert wurde, um so größer ist dabei die Verzögerung. Integriert man wiederum weniger Sicherheitsmechanismen, ist das Intranet auch von außen anfälliger. Das heißt, man muß aufgrund der eingesetzten Applikationen einen Kompromiß zwischen dem Sicherheitsgrad und der Schnelligkeit der Firewall machen.

Abbildung 1 zeigt die Kontrollbereiche einer Firewall. Dabei gehört der unkontrollierte Bereich zur sogenannten De-Militarisierten Zone (DMZ), die den Router, die Verbindung zum Internet, und eventuell ein ungeschütztes System, für Cracker oder Hacker, enthält. Anschließend ist das Firewall-System zu erkennen, welches als Paketfilter, Transportschicht oder Anwendungsschicht Firewall einsetzbar ist. Das dahinter liegende Intranet wird durch die Firewall von Zugriffen geschützt. Ein noch besseren Schutz kann das dedizierte Segment für sich verbuchen, da diese Rechner über eine extra Adapterkarte in einem speziellem Subnetz abgesichert ist.

Da jeder Computer eines lokalen Netzwerkes, das an ein WAN angeschlossen ist, sich so verhält als ob er selber direkt an das WAN angeschlossen wäre, bedeutet das, daß die Anzahl möglicher Sicherheitslücken im System mit der Zahl der installierten Computer wächst. Die Firewall verfügt nun über die notwendigen Sicherheitsmechanismen, um unerlaubte Zugriffe zu verhindern und erwünschte Datentransporte zu gestatten. Sollte eine bestimmte Aktion aufgrund der Sicherheitsanforderungen des Unternehmens nicht erlaubt sein, muß der Firewall gewährleisten, daß alle Versuche, die Aktion auszuführen, fehlschlagen. Außerdem können die verdächtigen Aktionen protokolliert werden, um dem Systemverwalter ein Eingreifen zu ermöglichen. Dadurch, daß alle Informationen des Unternehmens über den Firewall-Rechner laufen, können zudem durch Protokolle unter Beibehaltung von Datenschutzaspekten Kennzahlen erstellt und Statistiken erfaßt werden.

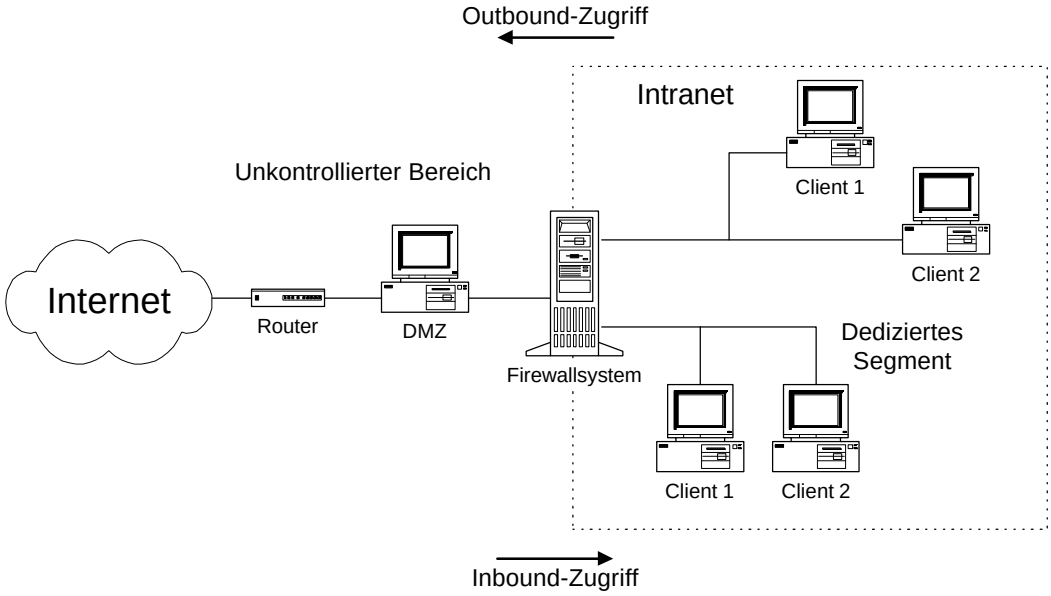

Abbildung 1: Einsatz eines Firewall-Systems

Die grundsätzlichen Möglichkeiten eines Firewall-Systems hängen sehr stark von den integrierten Kontrollkomponenten ab. Firewalls, die ihre Kontrolle allein auf einfache Paketfilter stützen, sind in ihrem Funktionsumfang sehr eingeschränkt und schwer zu warten. Allerdings haben viele Router bereits Paketfilter integriert, so daß diese Lösung sehr preiswert und schnell ist. Eine verbesserte Möglichkeit stellen die dynamischen Paketfilter dar, die durch ihre Flexibilität ein großes Spektrum von Kommunikationsvorgängen abdecken. Ein weiterer Typ von Firewalls sind die der Transportschicht. Diese werden für abgehende Verbindungen bevorzugt und arbeiten auf der Verbindungsschicht. Somit können TCP- oder UDP-Verbindungen kontrolliert weitergereicht werden. Eine externe Verbindung geht dabei auf einen TCP- bzw. UDP-Port des Gateway. Anschließend wird das Ziel im Intranet benachrichtigt. Während einer bestehenden Verbindung müssen die Daten von das Gateway von einer Schnittstelle zur nächsten umgesetzt werden. Die komplexeste Variante von Firewall-Systemen ist die Umsetzung auf der Anwendungsschicht. Statt den gesamten Datenfluß zu kontrollieren, wird für jede gewünschte Anwendung ein spezieller Code verwendet. Dies stellt einen hohen technischen Aufwand dar, der zugleich die sicherste Methode darstellt. Im folgenden werden die verschiedenen Ansätze beschrieben.

3.1 Paketfilter (Screening Firewalls)

Paketfilter Firewalls stellen die einfachste Lösung dar, um Sicherheitskonzepte in Unternehmen zu verwirklichen. Sie entscheiden anhand der Datenherkunft, des Zieles und den Portnummern, ob sie einzelne Datenpakete passieren lassen oder nicht. Das wird durch die Netzwerkprotokolle TCP und UDP ermöglicht, die Sequenz- und Portnummern zur Simulation eines Datenstromes zwischen zwei Computern verwenden. Dabei kennzeichnen Portnummern einzelne Dienste auf einem Computer. Für die speziellen Dienstleistungen im Internet sind Portnummern reserviert, anhand derer sie identifiziert werden können. Moderne Router sind in der Lage, den Zustand der Verbindung zu bestimmen, den Datenstrom zu analysieren und die Datenpakete über diese Verbindung an den Zielort weiterzuleiten. Ein Router kann man daher als ein System betrachten, das Daten zwischen zwei Netzen transferiert, die das selbe Protokoll verwenden. Die Netze können sich dabei aber durch ihre physikalischen Eigenschaften voneinander unterscheiden und eine andere Technologie einsetzen (z.B. Ethernet und ATM).

Die Eigenschaften von Packet Level Firewalls lassen sich folgendermaßen zusammenfassen:

- Datenströme werden direkt weitergeleitet
- Schnelle Überprüfung und Benutzertransparent
- Es kann nur auf vordefinierte Dienste und Rechner zugegriffen werden
- Die Konfiguration erfordert detailliertes Wissen über das Protokoll TCP/IP
- Einrichtung und Wartung ist sehr komplex, insbesondere wenn viele Rechner im eigenen Netz geschützt werden sollen
- Client benötigen keine besonderen Applikationen, da entweder Datentransfer gestattet wird oder die Firewall die Datenpakete unterdrückt
- Preiswerte Realisierung, da ein Router eingesetzt werden kann, der meistens sowieso verwendet werden muß

Die Paketfilter Firewalls sind also Unabhängig von der Applikation, wodurch und arbeiten daher mit geringer Verminderung des Durchsatzes. Die dadurch erreichten guten Performancewerte werden allerdings durch den Nachteil der geringeren Sicherheitsmechanismen erkauft. Durch sogenanntes Spoofing, d.h. Vortäuschen von gültigen Adressen und Sitzungen, gelangen Hacker relativ problemlos ins Netz. Deshalb werden heute Paketfilter eher als Ergänzung eingesetzt, zum Beispiel für kleine Netze mit geringen Sicherheitsanforderungen.

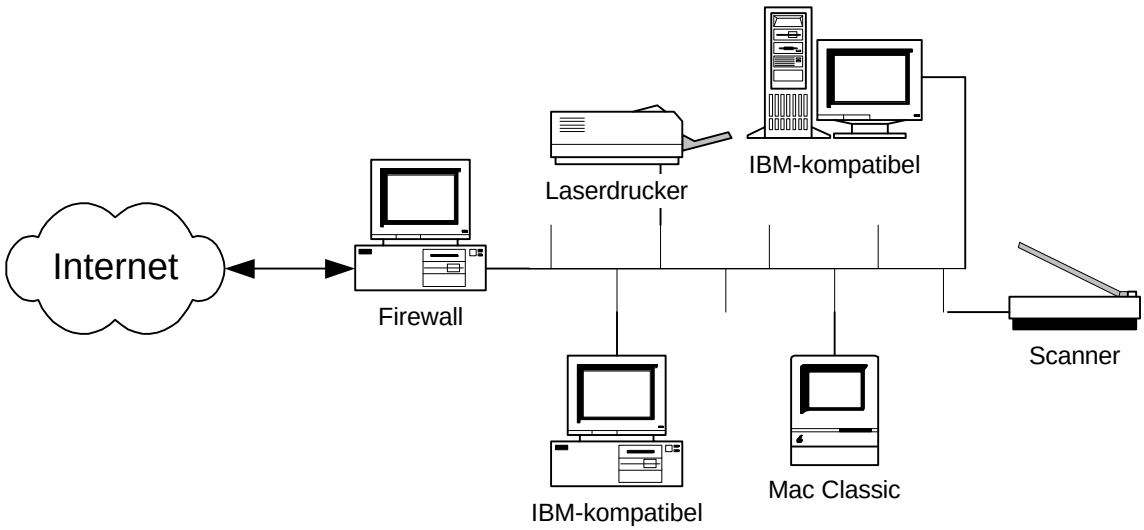

Abbildung 2: Paketfilter Firewall

3.2 Transportschicht (Circuit Firewall)

Eine etwas andere Art ist die Filterung der Transportschicht über eine Circuit Firewall. Sie wird als Relaisstation eingesetzt und vermittelt TCP-Verbindungen. Externe Verbindungen gehen auf einen Port der Firewall ein, während im zweiten Schritt das endgültige interne Zielsystem angesprochen wird. Die Firewall fungiert somit als Gateway zwischen dem externen WAN und internen LAN.

Die Firewall nimmt die Datenpakete entgegen und entscheidet anhand eines Regelwerkes, ob und wohin die Daten weitergeleitet werden. Diese Regelwerke lassen sich leichter defi-

nieren, als die komplexen Tabellen der Paketfilter. Zusätzlich ist es wesentlich einfacher, den Zugriff zu protokollieren. Verbindungen können zwar automatisch erstellt werden, wobei aber die Zugangskontrolle sicherstellt, daß dies nur von einem definierten externen Rechner vorgenommen werden darf. Eine andere Möglichkeiten ist es, dem Vermittlungsdienst das gewünschte Ziel mitzuteilen. Ein Protokoll zwischen Client und Gateway wird dafür benötigt. Durch das Protokoll kann der Client Ziel und Dienst anfordern und ist auch in der Lage Fehlermeldungen zu empfangen. Meistens wird dabei ein Stellvertreter bzw. Proxy eingesetzt, um die Sicherheit zu erhöhen. Der Proxy benötigt für das Ziel den Host-Namen oder die IP-Adresse. Anschließend wird erst über das Protokoll zwischen Client und Gateway der Aufbau der Verbindung vorgenommen und der eigentliche Datenverkehr beginnt. Zur Realisierung dieser Dienste muß das Client-Programm oder die Bibliothek dieses Programms geändert werden.

Die abgehenden Proxy-Dienste können den größten Teil des Internetzugriffs abdecken, den die Benutzer im Intranet des Unternehmens benötigen. Bestimmte Protokolle wie FTP und X11 verwenden aber ebenfalls eingehende Verbindungen zum Datenaustausch. Diese Verbindungen sind unkontrolliert und können nicht gestattet werden, weshalb die Benutzer diese Dienste nicht nutzen dürfen. Dies impliziert auch gleichzeitig ein gewisses Sicherheitsrisiko, da Benutzer im Intranet sich in ihrem Gestaltungsraum beschnitten fühlen könnten. Um die Einschränkung bestimmter erlaubter Ports zu umgehen, können Personen innerhalb des Unternehmens ungesicherte Telnet-Verbindungen oder andere Dienste nach außen anbieten, um wieder alle Internetdienste nutzen zu können. Dieser Mißbrauch führt zu einer Unterwanderung des Sicherheitskonzeptes und kann auch durch Protokollierung schlecht kompensiert werden.

Kontrollmechanismen sind nötig, um die eigenen Mitarbeiter und Angriffe von außen zu kontrollieren. Maximale Nutzungsdauer der Ports, Access Liste der befugten externen Benutzer und Authentifikation sind einzuführen und in einem Sicherheitskonzept zu verankern, um die Sicherheit zu erhöhen. Im Datendurchsatz sind Transportschicht Firewalls langsamer als Paketfilter, allerdings deutlich schneller als Anwendungsschicht Firewalls. Aus diesem Grund werden Transportschicht Firewalls häufig für ausgehenden Datenverkehr verwand, bei dem eine weitere Sicherheitsüberprüfung nicht mehr erforderlich ist. Diese Form von Firewallsystemen ist heute oft bereits als Softwareoption auf einer Reihe von Routern erhältlich.

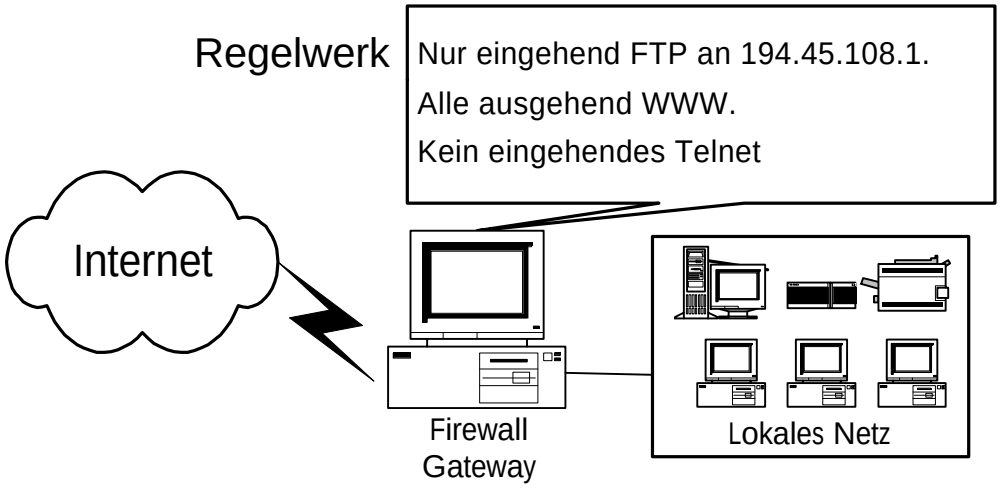

Abbildung 3: Transportschicht Firewall über Regelwerk

Ein anderes Problem ist die nötige Modifizierung an den Clients, die vorgenommen werden muß. Selbst kleine Änderungen an der Software ziehen mannigfaltige Arbeiten mit sich. Es müssen unterschiedliche Systeme und Plattformen verwaltet und gepflegt werden, die man alle für verschiedene Benutzergruppen aufbereiten muß. Die Nutzung der Transportschicht hat aber einen anderen großen Vorteil gegenüber der reinen Paketschicht Firewall, da sich UDP-Verkehr effizienter abwickeln läßt bzw. UDP-Anwendungen besser unterstützt werden. Dabei stellen nur Dienste ein Problem dar, die bestimmte lokale Portnummern benötigen. Wenn man aber eine virtuelle Verbindung zu einem Proxy herstellt, kann eine Filterung erfolgen, die den restlichen Anwendungsfall abdeckt.

3.3 Anwendungsschicht (Application Firewall)

Die Anwendungsschicht Firewall trennt den Datentransfer zwischen dem internen und externen Netz physikalisch und logisch komplett ab. Dies ermöglicht ein wesentlich höheres Sicherheitsniveau. Firewall auf der Anwendungsschicht arbeitet mit je einem Proxy-Server pro Dienst (Telnet, FTP, HTTP). Jede Verbindung zwischen einem Server im internen Netz und einem externen Client wird durch die Firewall in zwei Verbindungen aufgeteilt: Die Firewall stellt nach außen den Server dar und nach innen den Client - oder umgekehrt bei einer Verbindung interner Client mit externem Server. Durch die totale Prozeßkontrolle wird für die unterstützten Dienste ein sehr hoher Sicherheitsgrad erreicht. Diese doppelte Verarbeitung geht jedoch zu Lasten der Performance, so daß diese Lösung wesentlich langsamer arbeitet als Paket- oder Transportschicht Firewalls.

Die Anwendungsschicht Firewall besitzt zwei Netzwerkanschlüsse, da in der Vergangenheit Firewalls mit einem einzelnen Adapter zu leicht angreifbar waren. Dabei existiert ein unsicherer bzw. ungeschützter Bereich und eine Schutzzone, die das eigene Intranet darstellt. In diesem Fall müssen sog. Proxy fähige Programme eingesetzt werden. Bei dieser Art der Firewall können nur Daten mit Diensten transportiert werden, für die auf der Firewall ein Programm vorhanden ist. Dabei können die transportierten Daten kontrolliert werden.

Die meisten kommerziellen Firewalls sind eine Mischung aus Transport- und Applikationsschicht Firewalls. Die ausgehenden Dienste werden häufig über Transportschicht Firewalls geleitet, während die hereinkommenden Daten durch Anwendungsschicht Firewalls gefiltert werden. Ein häufig anzutreffende Kombination ist die Installation eines Paketfilters auf dem Router für die hereinkommenden Daten, der nur einen Zugriff auf die Rechner zwischen den beiden Routern und der Firewall ermöglicht. Es wird jedoch nicht der Zugriff auf den Router am internen sicheren Netz gestattet. Weiterhin wird der interne Router so konfiguriert, daß er nur einen Datenverkehr mit der Firewall zuläßt. Diese Konfiguration ist sehr effizient sowie wirksam und wird als Zwinge bezeichnet.

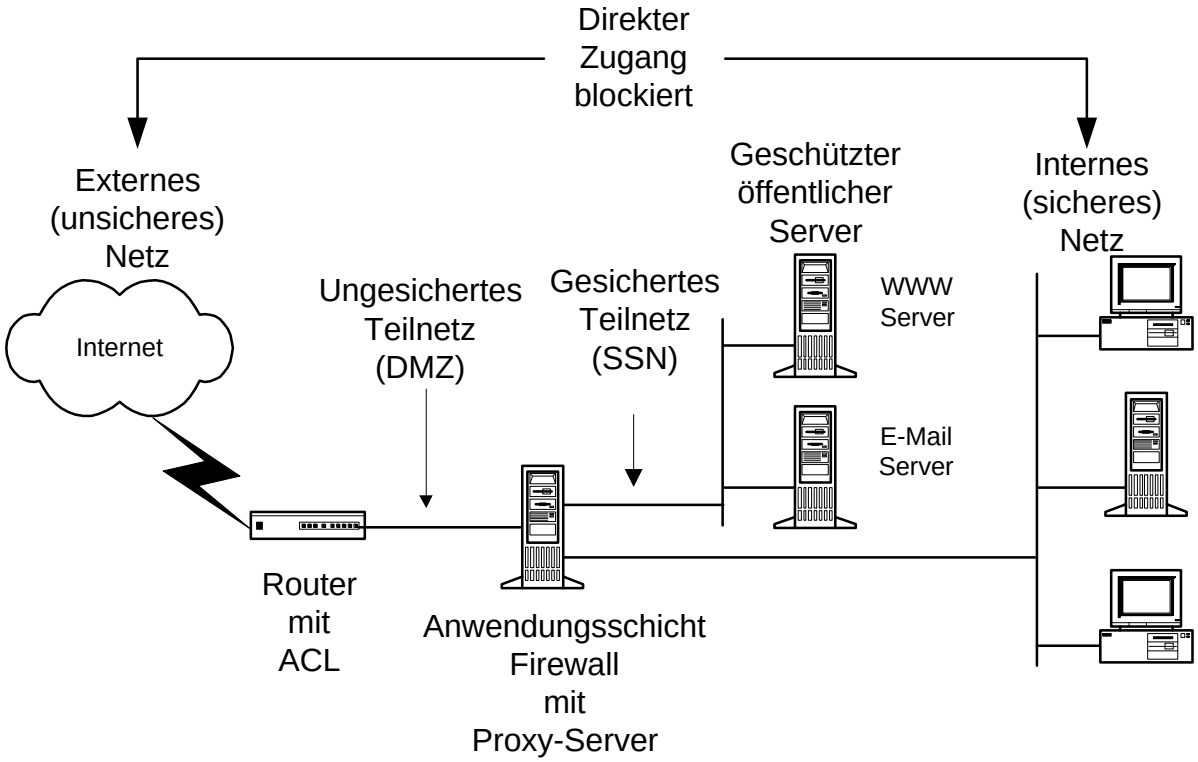

Abbildung 4: Anwendungsschicht Firewall

Der Bereich zwischen dem Router im Eingangsbereich und der Firewall wird häufig als DMZ bezeichnet. In diesem Bereich werden die externen Dienste verfügbar gemacht, auf die von außen zugegriffen wird. Wenn von außerhalb einer der Rechner im Bereich DMZ übernommen wird, so ist von dort kein Zugriff auf die Rechner des internen Netzes möglich. Es besteht jedoch die Gefahr, das die Firewall Flooding-Angriffen nicht standhält. Dabei wird die Firewall zum Beispiel mit Protokollbefehlen überschwemmt und zum Zusammenbruch gebracht. Darüber hinaus kann es Probleme bei der Unterstützung neuer Applikationen im Internet geben. Eine hundertprozentige Sicherheit gibt es also auch hier nicht. Trotzdem ist dieses Firewall-System die sicherste Methode seine Daten und Informationen des eigenen Intranets vor Angriffen zu schützen. Das interne Netz wird nach der Absicherung durch die Firewall als Secure Server Network (SSN) bezeichnet.

Die Arbeitsweise dieser Firewall unterscheidet sich von denen der anderen Firewalls. Für die Teilnehmer, die über eine Anwendungsschicht Firewall kommunizieren möchten, ist zuerst eine Identifizierung und Authentifikation notwendig. Zusätzlich werden unterschiedliche Verfahren für die Authentifikation unterstützt. Deshalb wird zuerst eine Verbindung zum Anwendungsschicht Firewall aufgebaut und nicht zum Zielrechner im Intranet. Eine direkte Kommunikation findet demnach zur Gateway statt und nicht zwischen den jeweiligen Endsystemen. Nachdem sichergestellt wurde, daß eine Kommunikation zwischen bekannten Endsystemen vorliegt, wird der Datenverkehr von der Gateway transparent weitergeleitet. Die Teilnehmer merken nichts von dem dazwischen geschalteten System.

Grundsätzlich empfängt die Anwendungsschicht Firewall Datenpakete an den jeweiligen Ports. Pro Port werden bestimmte Dienste freigegeben. Dies geschieht über entsprechende Software auf der Firewall, die die Datenpakete empfängt und an die sichere Netzwerkseite weiterleitet und umgekehrt. Diese Software kann man auch als Proxy bezeichnen und wurde bereits beschrieben. Der Unterschied liegt darin, daß jeder Proxy auf einer Firewall Gateway einem bestimmten Dienst zugeordnet werden kann. Somit ist er in der Lage zu-

sätzliche Sicherheitsdienste den Anwendungen zu vergeben. Dadurch ergeben sich mannigfaltige Möglichkeiten für Absicherung und Protokollierung. Zu beachten ist, daß auf der Anwendungsschicht Firewall nur die minimal notwendige Software installiert ist, damit Angreifer von außen so wenig Chancen wie möglich haben auf die Proxies einzuwirken, um sie für andere Dienste nutzbar zu machen. Auch sollte das Sicherheitsmanagement nicht auf dem selben Rechner laufen, wie die Firewall. Routing-Funktionen sind auszuschließen, da ansonsten die Proxies umgangen werden können.

Aufgrund der Verbindung zum ungesicherten als auch gesicherten Bereich, muß die Anwendungsschicht Firewall natürlich Network Address Translation (NAT) kennen und anbieten. Bei der Realisierung besitzt die Firewall eine IP-Adresse im ungesicherten Netz, die als öffentliche Adresse im Internet bekannt ist, und eine IP-Adresse im geschützten Intranet. Bei der Kommunikation mit den beiden Bereichen werden auf jeder Seite nur jeweils eine IP-Adresse sichtbar, so daß keine direkte Verbindung durch die Firewall möglich ist.

4 Virtual Private Network (VPN)

Das Internet wird heute von Firmen für mannigfaltige Anwendungen und Dienste eingesetzt und dient längst nicht mehr dazu reine Marketingaspekte auszunutzen. Vielmehr kommunizieren Unternehmen, die verteilte Standorte besitzen, sehr gezielt mittels dieses Mediums. Zusätzlich ist es auch für Unternehmen von Vorteil ihre Außendienstmitarbeiter effektiv in das eigene Firmennetz einzubeziehen. Immer mehr Heimarbeitsplätze entstehen weltweit, die es ermöglichen flexibel, schnell und ortsunabhängig auf die zentralen Datenbanken zuzugreifen. Da die Daten, die Unternehmen über das Internet versenden, selten für die Öffentlichkeit bestimmt sind, müssen sensible Informationen vor dem Zugriff Unbefugter geschützt werden. Beispiele sensitiver Informationen sind Militärdaten, Kreditinformationen, Patientenakten oder Personaldaten. Neben der Sicherheit sind auch die Kosten für eine Unternehmen entscheidend. Das heißt, die Wirtschaftlichkeit der Systeme und die Verbindungskosten während des Betriebs müssen gegeben sein. Das Internet erfüllt diese Wirtschaftlichkeit, da es weltweit existiert und flächendeckende Zugänge zum Ortstarif zur Verfügung stellt. Da aber die Sicherheit im Internet durch aktive und passive Angriffe gefährdet wird, müssen Verschlüsselungsmechanismen eingesetzt werden, die den Datenstrom sicher durch das Netz schleusen. Man spricht in diesem Zusammenhang von der Bildung von Virtual Private Networks (VPNs).

Eine Absicherung von sensitiven Daten ist aber nicht ohne weiteres möglich, da die IP-Pakete von zahllosen Systemen transportiert werden, kann man Daten ohne große Probleme mitlesen. Tunnelmechanismen bietet hierbei den Vorteil eines exklusiven Zugangs unter Vermeidung der Nachteile bei einer üblichen Internet-Anbindung. Heutzutage wird der Internet Access meistens über das Point-to-Point-Protocol (PPP) nach RFC-1661 realisiert, um eine Punkt-zu-Punkt-Verbindung von dem Endgerät zum Point-of-Presence (POP) herzustellen. PPP beinhaltet eine Standardmethode zum Transport von Multiprotokoll Datagrammen und besteht aus den folgenden drei Komponenten:

- Einkapselung von Multiprotokoll Datagrammen
- Link Control Protocol (LCP) zum Etablieren, Konfiguration und Testen einer Data Link Verbindung
- Protokollfamilie des Network Control Protocols (NCP) zum Etablieren und Konfiguration von verschiedenen Netzwerkschicht Protokollen

PPP wurde zum Verbindungsaufbau und zur Authentifikation entwickelt. Zusätzlich findet eine Überwachung der physikalischen Verbindung über Protokolle höherer Schichten (z.B. IP), Vergabe von IPX- bzw. IP-Adressen und das Übertragen von IP/IP-Paketen statt. Die Weiterentwicklung Multilink PPP (ML-PPP) ist fertig standardisiert, findet sich aber noch in kaum einem Produkt wieder. Im Grunde ist PPP aber eine überflüssige Entwicklung, da man ebensogut das bereits vorhandene Protokoll High Level Data Link Control (HDLC) hätte einsetzen könnte. Eine bessere Alternative ist deshalb das Multilink HDLC für redundante Strecken, da man nicht auf Protokolle höherer Schichten angewiesen ist wie bei PPP, was bei Fehlern zu größeren Time-Outs führt. HDLC sorgt hingegen dafür, daß die Leitung fehlerfrei bleibt und erst gar keine Fehler von höheren Protokollen entdeckt werden können. Dadurch ist das Re-Routing wesentlich schneller. Weiterhin ist PPP durch die BER von $>10^{-5}$ anfälliger als HDLC, da durch das HDLC Protokoll die Fehlerrate einer Leitung auf nahezu Null (10^{-26}) reduziert werden kann. PPP ist aber heute der Quasistandard für ISDN-Verbindungen unter Windows95/98/NT geworden und findet deshalb am meisten Anwendung. PPP läßt sich unterteilen in das Password Authentication Protocol (PAP) und Challenge Handshake Authentication Protocol (CHAP), die zur Authentifikation und Überprüfung der Identität eingesetzt werden.

Das Zugangssystem ist über ein LAN oder WAN mit dem dahinter liegenden Netz verbunden und leitet die Pakete über PPP zum jeweiligen Zielrechner weiter. Bei der Tunnellösung packt das Zielsystem die vom Teilnehmer empfangenen PPP-Pakete in ein definiertes Tunnelprotokoll ein und transportiert es über das Internet zum Zielsystem. Durch das Tunnelverfahren verhält sich das System so, als ob der Teilnehmer sich direkt eingewählt hat. Zusätzlich wird der externe Teilnehmer autorisiert, es wird eine IP-Adresse zugewiesen und die IP/IPX-Pakete entpackt, um sie zum Zielrechner weiterzuleiten. Endgeräte für das Tunnelprotokoll kann ein Access Router sein oder ein Server, der in der Lage ist Tunnelmechanismen zu implementieren. Durch die logische Zugehörigkeit des eingeloggten Teilnehmers entsteht ein VPN.

4.1 Tunnelmechanismus

Um den Tunnelmechanismus zu etablieren, muß man den Anfangs- sowie Endpunkt einer Strecke definieren. Auf der Gegenseite müssen diese Daten ebenfalls eingegeben werden, allerdings mit Umkehrung der IP-Adressen. Der äußere IP-Header identifiziert dabei die Endpunkte einer Tunnelstrecke, also Quell- und Zielpunkt eines Tunnels. Der innere IP-Header hingegen erkennt den ursprünglichen Sender und Empfänger des gesendeten Datagramms bzw. IP-Pakets. Die gewählte Dienstart bleibt dabei auf der Tunnelstrecke erhalten und wird vom inneren IP-Header kopiert. Dadurch kann zwischen identischen Schichten der Type-of-Service (TOS) weiterhin garantiert werden. Das Identifikationsfeld bekommt für jeden äußeren Header eine neue Nummer zugewiesen. Das eingekapselte Datagramm kann dabei bereits fragmentiert sein. Wenn das der Fall ist, kommt eine weitere Fragmentierstufe durch den Tunnelmechanismus hinzu. Diese Tunnelfragmente werden am Tunnelende wieder zusammengesetzt, bevor sie den endgültigen Bestimmungsort erreichen. Falls keine Fragmente vorhanden sind, wird der Feldinhalt „don't Fragment" von dem inneren IP-Header kopiert. Das Feld Time-to-Live (TTL) wird auch hier um eine Stelle vermindert, um den Datenstrom zwischen zwei Endpunkten auch für unerwartet lange Tunnel aufrechterhalten zu können. Der TTL-Wert wird dabei ausschließlich durch die Einkapselung vermindert und nicht erneut durch die Entkapselung des IP-Headers.

Das Feld Optionen wird als einziges Feld nicht in den inneren IP-Header kopiert. Werte wie Timestamp, Loose Source Route, Strict Source Route und Record Route werden absichtlich im Tunnel versteckt, da der Tunnelmechanismus oft die Unzulänglichkeiten dieser Optionen überwinden soll. Weiterhin ist es möglich, daß ein Router im Bereich der getunnelten Strecke Fehler während der Verarbeitung eines Datagramms verursacht. Dies kann durch eine ICMP Fehlerrückmeldung des Routers an den Tunnelanfang geschehen. Weiterhin können Probleme auftreten, weil ICMP-Meldungen 8 Byte des Datagramms über den IP-Header erfordern. Diese 8 Byte ermöglichen es nicht mehr, daß zusätzliche Informationen über den Ursprungsort im IP-Header enthalten sein können. Deshalb ist es für einen Router, der die Einkapselung vornimmt, nicht mehr möglich, eine ICMP-Nachricht vom Tunnelinneren zum ursprünglichen Host zurückzusenden. Trotzdem ist in den meisten Fällen eine Rücksendung von ICMP-Nachrichten durch das sorgfältige Einhalten des Soft-State möglich. Die folgenden Soft-State-Informationen sollten im Router mindestens implementiert sein:

- Erreichbarkeit des Tunnelendes
- Überlastung des Tunnels
- Maximum Transmission Unit (MTU) des Tunnels

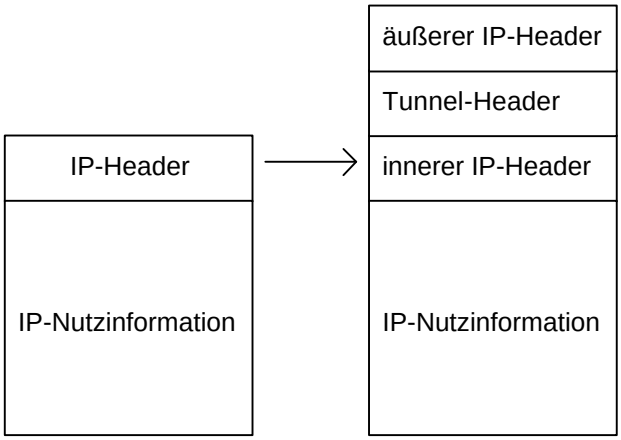

Abb. 4.1: Tunnelprotokoll

Der Router nutzt die ICMP-Nachrichten zum Aktualisieren der Soft-State Informationen. Falls anschließend Datagramme durch den Tunnel befördert werden sollen, wird diese Information zuerst überprüft. Wenn Datagramme den Tunnelstatus verletzen (z.B. bei größerer MTU als vorhandener Tunnel-MTU bei keinerlei Fragmentierung), sendet der Router eine entsprechende ICMP-Fehlermeldung zum Sender zurück und leitet dieses ebenfalls an das Datagramm im Tunnel weiter. Durch diese Fehlermeldung kann das Datagramm sich ändernde Tunnelbedingungen berücksichtigen. Bei Benutzung dieser Technik sollte beachtet werden, daß die ICMP-Fehlermeldung beim Router nicht unbedingt hundertprozentig mit der Fehlermeldung im Tunnel übereinstimmen muß. Die Fehlermeldung im Tunnel spiegelt aber auf jeden Fall den aktuellen Status des Netzwerks wider.

4.2 Verschlüsselung

Um VPNs nach außen abzusichern, sind verschiedene Verschlüsselungen bereits in den Routern vorhanden, die für das Tunnelprotokoll eingesetzt werden können. Das Point-to-Point Tunneling Protocol (PPTP) von Microsoft, Ascend, 3Com und U.S. Robotics ist eines davon und setzt einen Client voraus, der PPP-Pakete beherrscht. Diese Pakete werden in eine modifizierter Form des Generic Routing Encapsulation Protokolls der Version 2 (GRE V2) eingepackt und über das Netz zum Network Access Server (NAS) des ISP transportiert.

Bei NAS findet keine Authentifikation statt, wodurch eine statische Zuordnung erfolgen muß. Der Teilnehmer ist dadurch nicht in der Lage den Endpunkt der Tunnel zu beeinflussen. Zusätzlich lassen sich für den Betreiber des Zugangssystems keine Accounting-Daten erfassen. Auch auf die übertragene Menge von Datenpaketen sowie auf die Verbindungsdauer muß verzichtet werden.

Ein Nachteil dieses Verfahrens ist der notwendige Einsatz von Windows NT als Home Gateway. Zusätzlich muß eine feste IP-Adresse vergeben werden, da diese für eine statische Vergabe der Route ausschlaggebend ist. Viele Unternehmen besitzen aber private IP-Adressen nach der Spezifikation RFC-1918, wodurch Probleme bei der Zuordnung entstehen. Vorteile von PPTP sind die Möglichkeit der Übertragung von IP- und IPX/SPX-Paketen (Multiprotocol Tunneling) sowie der Dial-Out. Dial-Out ermöglicht die Anwahl einer Rufnummer von der Zentrale aus, um eine direkte Verbindung mit dem einzubindenden Arbeitsplatz herzustellen.

Die zweite Möglichkeit ist das Layer 2 Forwarding (L2F) Protokoll von Cisco nach RFC-2341. Als Home Gateway kann ein Router eingesetzt werden, während als NAS Access Server zum Einsatz kommen. Die Client-Software ist wie beim PPTP beliebig. Allerdings unterstützt L2F auch das Serial Line Protocol (SLIP). Auch ist die Zuordnung von NAS und Home Gateway, im Gegensatz zu PPTP, dynamisch, wodurch Multi-Providing ermöglicht wird. Die Ermittlung des Teilnehmers und des Paßwortes ist ebenfalls gegeben und wird im Zugangssystem ermittelt. Dadurch kann das Zugangssystem den Zielort des Tunnels durch den Namen oder die Wahlziffer bestimmen. Durch das Multi-Providing kann man direkt auf das Internet oder das VPN zugreifen. Weiterhin kann L2F über eine Vielzahl von paketorientierten (u.a. ATM und Frame Relay) Netzen transportiert werden, wodurch dieses Verfahren unabhängig von der verwendeten Technologie ist. Da als Home Gateway meistens ein Router eingesetzt wird, kann auch eine Adreßumsetzung über NAT erfolgen. Ein Dial-Out wird somit von L2F nicht unterstützt.

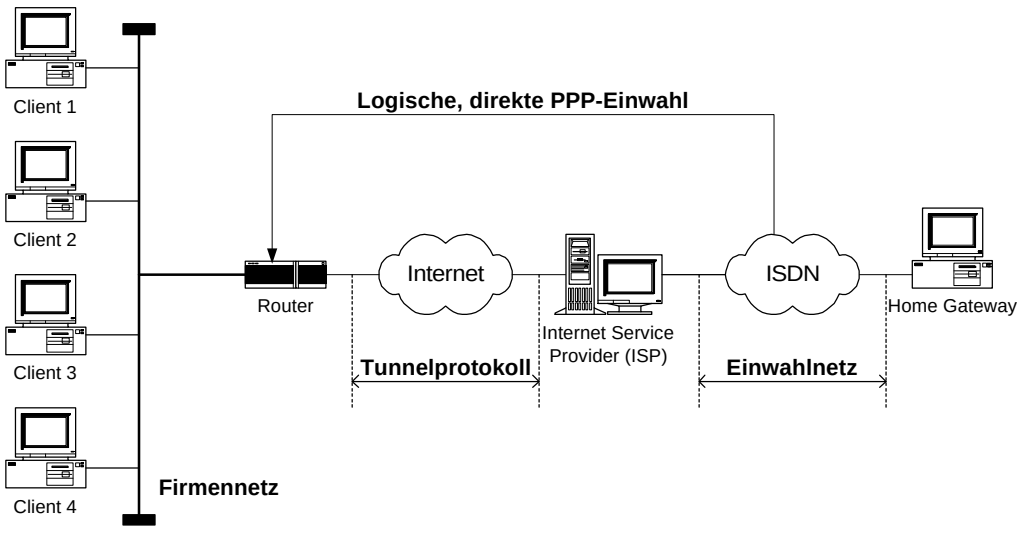

Abb. 4.2: Tunneling und Direktverbindung zum Firmennetz

Durch die bestehenden Vor- und Nachteile beider Verfahren, ist ein drittes Protokoll spezifiziert worden. Das Layer 2 Tunneling Protocol (L2TP) ist ein hybrides Verfahren aus den beiden zuerst genannten. Es ist jedoch stärker mit dem L2F Protokoll verwandt und erweitert dieses um den fehlenden Dial-Out. Das heißt, wenn keine physikalische Verbindung vorhanden ist, wird ein ausgehender Call vom Zugangssystem zur Gegenstelle aufgebaut. Die Abwärtskompatibilität zu L2F ist ebenfalls gesichert.

5 Kryptographie

Um eine zusätzliche Sicherheit bei der Kommunikation über öffentliche Netze zu erreichen, werden kryptographische Verfahren eingesetzt. Dies ist im Grunde nicht neu, da die Kryptographie bereits vor Jahrhunderten zur Verschlüsselung von Daten eingesetzt wurde. Die Verschlüsselung ermöglicht die Umwandlung eines Klartextes in einen nicht mehr allgemein lesbaren Chiffretext. Dieser muß für eine Entzifferung der eigentlichen Nachricht entschlüsselt werden. Die Dechiffrierung erfolgt mit Hilfe eines Schlüssels. Diejenigen, die solche Verfahren anwenden, heißen Kryptographen. Die Analyse verschlüsselter Nachrichten mit dem Ziel, den ursprünglichen Inhalt zu rekonstruieren, nennt sich Kryptoanalyse. Die Wissenschaft, welche die Kryptographie und Kryptoanalyse zum Inhalt hat, ist die Kryptologie – ein Teilbereich der theoretischen Mathematik.

Prinzipiell gibt es zwei Kryptoverfahren, die auf einem Schlüssel basieren: symmetrische und asymmetrische Verfahren. Symmetrische Verfahren erlauben es, den Schlüssel zur Dechiffrierung vom Schlüssel zur Chiffrierung abzuleiten. Symmetrische Verfahren verwenden dabei einen einzigen Schlüssel. Das beinhaltet, daß sich alle Kommunikationspartner vor dem Beginn einer Sitzung –auf einen gemeinsamen Schlüssel einigen müssen. Dieser gilt dann während der gesamten Session. Die Sicherheit der Kommunikation beruht dabei auf dem symmetrischen Schlüssel. Wenn dieser Schlüssel während der Kommunikation rekonstruiert wird, liegt die Sitzung offen. Der Vorteil der symmetrischen Variante liegt in der Schnelligkeit sowie Effizienz bei der Umsetzung. Symmetrische Algorithmen lassen sich auch wieder in zwei Kategorien einsortieren:

- Stream Cipher: Einzelne Bits oder Bytes des Klartextes werden bearbeitet und chiffriert/ dechiffriert.
- Block Cipher: Bitblöcke des Klartextes werden bearbeitet und chiffriert/dechiffriert.

Asymmetrische Verfahren, die auch Public Key Verfahren genannt werden, verwenden dagegen unterschiedliche Schlüssel zur Chiffrierung bzw. Dechiffrierung. Sie sind so aufgebaut, daß sie nicht innerhalb eines sinnvollen Zeitraums voneinander abgeleitet werden können. Das neue daran ist, daß man den Schlüssel für die Verschlüsselung veröffentlicht, wodurch jeder die Möglichkeit besitzt, eine Nachricht zu verschlüsseln. Allerdings ist nur der Empfänger in der Lage, die Nachricht auch wieder zu decodieren. Man benötigt dafür zwei Schlüssel. Einen öffentlichen Schlüssel, der allgemein bekannt ist, und einen privaten Schlüssel, der zur Entschlüsselung hinzu genommen werden muß. Public Key Verfahren sind allerdings sehr langsam und benötigen auch sehr lange Schlüssel. Außerdem sind sie gegenüber kryptoanalytischen Angriffen anfällig. Aus diesem Grund setzt man diese Verfahren nicht zur Verschlüsselung von Nutzdaten ein, sondern zum Austausch von Schlüsseln für symmetrische Verfahren und die digitale Unterschrift. Diese Unterschrift stellt dabei sicher, daß die Nachricht auch unverändert von dem Absender kommt, der in der Meldung angegeben wird. Der Absender verschlüsselt dabei seine Nachricht mit seinem eigenen nur ihm bekannten privaten Schlüssel. Der Empfänger kann diese Nachricht nur mit dem öffentlichen Schlüssel wieder entschlüsseln und stellt gleichzeitig sicher, daß diese Nachricht nur von dem Absender kommen konnte.

Die Sicherheit symmetrischer und asymmetrischer Verfahren kann man durch den Aufwand definieren, der notwendig ist, um einen Schlüssel zu finden und mit ihm das verschlüsselte Dokument zu entschlüsseln. Dieser Aufwand hängt von der Komplexität des Verschlüsselungsalgorithmus und der Größe des Schlüsselraums ab, der die Menge aller mathematisch möglichen Schlüssel für einen bestimmten Algorithmus umfaßt. Dabei war es immer schon ein Ziel der Wissenschaftler, einen Algorithmus zu entwickeln, der nur mit Algorith-

men exponentieller Komplexität entschlüsselt werden kann. Solche Algorithmen sind zum heutigen Zeitpunkt allerdings nicht verfügbar. Solche Algorithmen wären auch praktisch nicht zu dechiffrieren, da sich die Laufzeit der Entschlüsselung bei Verdoppelung der Eingabemenge quadriert.

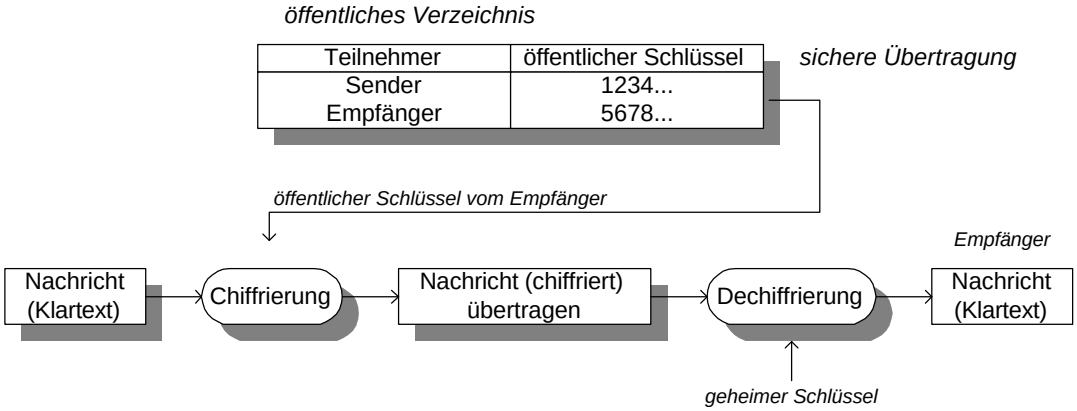

Abb. 5.1: Asymmetrische Verschlüsselung

Bei einem Algorithmus exponentieller Komplexität, z.B. 0 (2n), verdoppelt sich die Laufzeit des Algorithmus, wenn 1 Bit zur Eingabemenge hinzugefügt wird. Bei einem 40-Bit-Schlüssel liegt der Aufwand zur Berechnung des Schlüssels (Durchsuchen des Schlüsselraums) bei 2^{40} Operationen, bei einem 56-Bit-Schlüssel bei 2^{56} und bei einem 112-Bit-Schlüssel bei 2^{112} Operationen. Wenn man nun noch davon ausgeht, daß der Schlüssel bereits nach der Hälfte des Schlüsselraums gefunden wird, kann man gleichzeitig die Kosten und den Zeitbedarf berechnen. So kann beispielsweise ein 40-Bit-Schlüssel mit der entsprechenden Hardware in ca. 0,2 s entschlüsselt werden. Für 56 Bit benötigt man bereits ca. 20 min und für 64 Bit wird erst nach 4 Tagen eine Dechiffrierung ermöglicht. 128-Bit-Schlüssel machen eine Entschlüsselung dann bereits unmöglich, da man 1017 Jahre nach heutigen Schätzungen ansetzen müßte. Zugegeben, bei den Berechnungen geht man von einem millionenschweren Equipment aus. Da die Leistung der CPUs sich aber in bestimmten Zeitabständen verdoppelt, kann man aber davon ausgehen, daß sich die Zeiten für die Entschlüsselung laufend ändern werden. Letztendlich gibt es keine absolute Sicherheit, so daß man immer einen Kompromiß zwischen schneller Verarbeitung und dem erreichbaren Sicherheitsgrad abwägen muß. Zusätzlich ist die Sensitivität der Daten bzw. Nachrichten zu beurteilen, um eine Schlüssellänge zu definieren. Nachrichten, die nur für kurze Zeit Bedeutung haben, muß man anders behandeln, als Regierungs- oder Firmengeheimnisse. Deshalb muß schließlich der Anwender entscheiden, welche Verfahren mit welcher Schlüssellänge seinen Bedürfnissen angemessen sind.

Diese freie Entscheidung will man aber in den USA nicht unterstützen, da praktisch alle Verschlüsselungsverfahren nicht so sicher sein dürfen, daß der Geheimdienst FBI sie nicht dechiffrieren kann. So verwendet der amerikanische Data Encryption Standard (DES) nur einen bis zu 56-Bit langen Schlüssel. Andere Verfahren sind hier bislang nicht zulässig. Verbesserte Ansätze ermöglicht das Verfahren Triple-DES, welches jeden Datenblock dreimal chiffriert, mit zwei oder drei verschiedenen DES-Schlüsseln. Dieses Verfahren hat dabei im Grunde einen Schlüssel der doppelten Länge des Standards DES. Da es sich bei DES und Triple-DES jedoch um unterschiedliche Mechanismen handelt, sind die Schlüssellängen nicht direkt vergleichbar. Triple-DES ist sicherer als 40-Bit-DES, allerdings nicht so sicher wie ein 128-Bit-Algorithmus. Verfahren, die Schlüssellängen von 40 oder 56 Bit benutzen, kann man aus den genannten Gründen als nicht sicher genug bezeichnen. Ob-

wohl die Exportbeschränkungen der USA die Ausfuhr von 128-Bit-Algorithmen erschweren, gibt es auf dem europäischen Markt folgende Verfahren, die einen höheren Schlüssel ermöglichen:

- International Data Encryption Algorithm (IDEA): Chiffrierung mit 128-Bit-Schlüsseln.
- Cast-128: IETF spezifizierte 1997 in der RFC-2144 einen Algorithmus, der 64-Bit-Blöcke mit einem 128-Bit-Schlüssel codiert.

Inzwischen hat man Wege gefunden, solche Verfahren zu exportieren, so daß kein Anwender mehr auf die bislang sicheren 128-Bit-Schlüssel verzichten sollte. Kryptoboxen erhöhen dabei die Sicherheit eines VPNs erheblich. Firewalls werden hierbei mit Verschlüsselungsmechanismen ausgestattet, die zwischen einzelnen Standorten eine virtuelle Verbindung über VPNs aufbauen. Ausschließlich die Firewalls kommunizieren über das Internet miteinander. Zur Absicherung der Kommunikationskanäle, werden die Nutzdaten verschlüsselt. Das kann intern auf dem TCP/IP-Protokollstapel erfolgen oder extern durch Kryptoboxen. Ein Rechner, der keinen Schlüssel besitzt, kann nicht an der Kommunikation teilhaben.

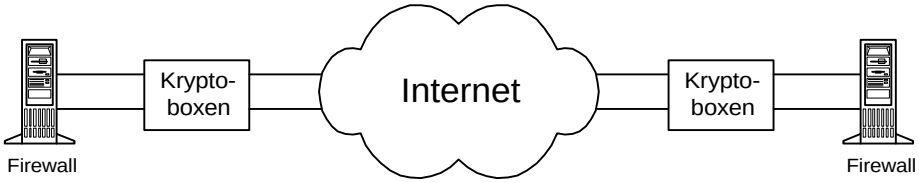

Abbildung 5: Zusätzliche Absicherung von VPNs durch Kryptoboxen

5.1 Neuer Ansatz IPsec

Die Arbeitsgruppe IPsec der IETF hat 1998 einen Entwurf für einen Standard vorgelegt, um eine sichere IP-Architektur zukünftig bereitzustellen. Grundlage dieser Spezifikation bildet ein vor ein paar Jahren erarbeiteter Standard (RFC-1825). Der Vorschlag legt fest, auf welche Weise Authentifikation und Verschlüsselung auf der IP-Schicht einzurichten sind. Firewalls, die sich an diese Spezifikation halten, können untereinander chiffrierte Daten austauschen, auch wenn sie von unterschiedlichen Herstellern stammen und verschiedene Verschlüsselungsverfahren verwenden. Dies war bislang nicht möglich, da es sich immer um proprietäre Lösungen handelte.

Zu der Spezifikation RFC-1825, kommen RFC-1826 und RFC-1827 noch hinzu. Sie bauen alle aufeinander auf. Zusätzlich sind eine Menge Drafts entstanden, die unterschiedliche Themen behandeln. Beispielsweise wurde das Zusammenwirken von Authentification Header (AH), Encapsulated Security Payload (ESP) und Key Management festgelegt. Weiterhin sind spezielle Drafts für die Nutzung konkreter Verschlüsselungs- und Authentifikationsalgorithmen entstanden. Key Management Protokolle sind ebenfalls angegeben.

IPsec unterscheidet sich von den bisherigen Ansätzen. Wie im vorherigen Unterkapitel beschrieben, gibt es bereits Sicherheitsmechanismen auf der Anwendungsschicht, wie SSL oder PGP für E-Mails. Um aber das Intranet effizienter abzusichern, unabhängig von den Anwendungen und deren Verschlüsselungsverfahren, müßte man auf der Netzwerkschicht ansetzten. Da IP bislang keine solchen Mechanismen vorsah, entstanden proprietäre Implementierungen, die sich auch auf VPN-Produkte auswirkten. So ist kein Hersteller eines VPN-Produktes momentan in der Lage mit einem anderen zu kommunizieren. IPsec stellt hingegen eine Sicherheitserweiterung auf der IP-Schicht dar, wodurch es jedes Datenpaket vor Verfälschung (Authentizität und Integrität) schützt und zusätzlich noch verschlüsselt

(Vertraulichkeit). Im Grunde würden Sicherheitsmechanismen auf der Anwendungsschicht dadurch überflüssig, wenn IPsec die Daten auch nach dem Empfang weiter schützen würde. IPsec hat dafür aber keine Möglichkeiten vorgesehen – es schützt die Daten nur zwischen zwei Instanzen. Andere Ansätze, wie z.B. die digitale Signatur, werden weiter benötigt.

IPsec ermöglicht den Datenschutz hauptsächlich durch zwei Paketerweiterungen. Hinzugekommen sind der AH und die Nutzdaten ESP. Der AH beinhaltet eine kryptographische Prüfsumme über die Nutzdaten und Teile des Paket-Headers. Bekannte Hash-Funktionen, wie Message Digest 5 (MD5) und Secure Hash Algorithm (SHA), bilden die Prüfsumme mit einem symmetrischen Schlüssel. MD5 weist allerdings heute einige Schwächen auf, so daß man bereits SHA einsetzen sollte. Durch die Bildung der Prüfsumme entsteht ein Message Authentification Code, der die Nutzdaten vor Verfälschung schützen soll. Zusätzlich werden wichtige Daten des IP-Headers gesichert. Das betrifft beispielsweise die Sende- und Empfangsadresse, wodurch das IP-Spoofing abgewehrt werden kann. Es werden nicht alle Felder des Headers in die Prüfsumme eingeschlossen, da sich ändernde Felder, wie z.B. TTL, die Prüfsumme ungültig machen würden. ESP wird hauptsächlich zum Verschlüsseln der Nutzdaten verwendet. Das wird mit symmetrischen Verschlüsselungsverfahren, wie DES, Triple-DES oder IDEA realisiert. Asymmetrische Verfahren könne aufgrund der Performance nicht eingesetzt werden. So würde die Datenrate von 100 MBit/s auf 1 MBit/s sinken, wenn man Public Key Verfahren einsetzen würde.

Um VPNs mittels IPsec aufbauen zu können, damit ganze Netze über virtuelle Verbindungen getunnelt werden können, wird unterschieden zwischen dem Transport Mode und dem Tunnel Mode. Der Tunnel Mode ermöglicht die sichere Datenübertragung von IP-Paketen in IPsec-Paketen. Für viele Situationen wird die Anwendung von nur einer IPsec-Funktion nicht ausreichend sein, wenn beispielsweise nur Teilstrecken im Tunnelmodus betrieben werden können, falls nicht alle Knotenpunkte IPsec erkennen. Dann müssen Kombinationsformen aus Transport und Tunnel Mode spezifiziert werden, die jede Implementierung unterstützen muß. Ansonsten besteht aber der große Vorteil, daß Datensicherheit den Anwendungen transparent zur Verfügung gestellt wird, wodurch proprietäre VPNs der Vergangenheit angehören werden.

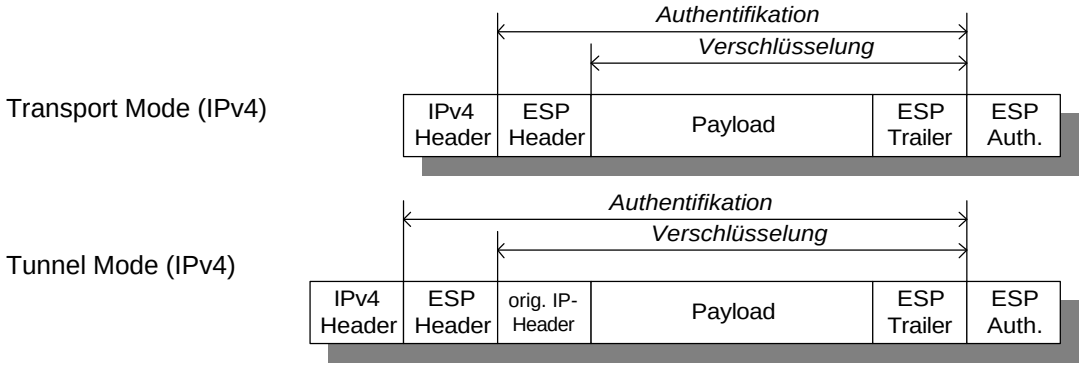

Abb. 5.2: AH und ESP Einkapselung bei IPsec in IPv4

IPsec ist unabhängig von der verwendeten IP-Version. Damit kann man IPsec auch beim zukünftigen IPv6 einsetzen. Hersteller werden momentan aber nur Implementierungen für IPv4 anbieten, da sich die Einführung von IPv6 weiter verzögern wird. IPv6 bietet aber auch eine ganze Anzahl von Sicherheitsmechanismen an, die denen von IPsec sehr ähnlich sind,

so daß es hier zu einem Konsens kommen wird. IPsec kann somit als eine Erweiterung von IPv4, um die fehlenden Sicherheitsmechanismen angesehen werden.

Abschließend kann man feststellen, daß IPsec Sicherheitsfunktionen für fast alle Anwendungsbereiche erschließt. Es mangelt momentan jedoch noch an den Implementierungen. Das liegt an den Fortschritten der RFCs, die größtenteils noch Drafts sind. Dies wird sich in naher Zukunft jedoch ändern. Vor der Einführung von IPv6 kann man so bereits Sicherheitsmechanismen verwenden, die die Vertraulichkeit, Integrität und Authentizität über das Internet nahezu zusichern können.

6 Fazit

Sicherheitsmechanismen sind absolut notwendig, um die Zugriffssicherheit auf das private Intranet garantieren zu können. Zusätzlich wenden Sie aber die Gefahren aus dem Internet nicht effektiv ab, wenn sich die Anwender nicht nach einem definiertem Regelwerk verhalten bzw. regelmäßige Kontrolle der Nachbesserung der Sicherheitslösung erfolgt. Bei der Implementierung eines globalen Sicherheitskonzepts muß deshalb neben der Kommunikationsanalyse auch eine Analyse der passiven und aktiven Infrastruktur erfolgen. Weiterhin spielt hier die Betriebssicherheit eine entscheidende Rolle, da man sich gerade hier vor Datenverlust schützen muß. Auch die verwendeten Applikationen oder die zukünftig geplanten Dienste sind für dieses Konzept entscheidend. Beispielsweise lassen Videokonferenzen die Anforderung an die Performance drastisch steigen. Aber gerade hier wird man immer einen Kompromiß zwischen der Leistung einer Systemlösung und der zur Verfügung stehenden Sicherheit machen müssen, da kein Firewall-System in der Lage ist, die notwendige Echtzeit-Performance bereitzustellen. Letztendlich beinhaltet die Erstellung eines solchen Sicherheitskonzeptes viele Bereiche eines Intranets, die alle angesprochen und eingebracht werden müssen. Erst dann wird man einen hohen Sicherheitsgrad gewährleisten können. Eine Firewall-Lösung stellt dabei nur ein Teilbereich dieser Gesamtlösung dar.

VPNs lassen sich für verteilt sitzende Unternehmen sehr effizient einsetzen. Die Technik ist heute auf einem ausreichenden Stand der Standardisierung, um interessante Lösungen anbieten zu können. Proprietäre Ansätze werden durch IPsec demnächst verdrängt werden, so das durchgängige Systeme sich verwenden lassen. Zur Unterstützung von Echtzeitverkehr ist nur der Einsatz von symmetrischen Schlüsseln bzw. Kryptoboxen möglich, da asymmetrische Verfahren zuviel Verzögerungen hervorrufen würden. Da aber nur wenig sensitive Daten über Audio- und Videoströme versandt werden, ist das kein grundsätzliches Problem. Schwieriger wird Application Sharing abzusichern, da durch diese Anwendung wieder Daten aus dem gesicherten Intranet verwendet werden, die bessere Verschlüsselung benötigen. Hier wird man sicher noch nachbessern müssen.

7 Glossar

AH	Authentification Header
ATM	Asynchroner Transfer Modus
CERT	Computer Emergency Response Team
CHAP	Challenge Handshake Authentication Protocol
COM	Commercial
DDV	Datendirektverbindung
DES	Data Encryption Standard
DMZ	De-Military Zone; entmilitarisierte Zone bei Firewall-Systemen
ESP	Encapsulated Security Payload
FTP	File Transfer Protocol
GREV2	Generic Routing Encapsulation Protokolls der Version 2
HDLC	High Level Data Link Control
HTTP	Hypertext Transport Protocol
ICMP	Internet Control Message Protocol
IDEA	International Data Encryption Algorithm; 128-Bit-Verschlüsselung
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPX	Internetwork Packet Exchange Protocol
ISDN	Integrated Service Digital Network
IPsec	Standard RFC-1825, der IP-Pakete schützt und Sicherheit transparent für Anwendungen gewährleistet
ISP	Internet Service Providers
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCP	Link Control Protocol
MD5	Message Digest 5
MPPP	Multilink PPP
MTU	Maximum Transmission Unit
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocols
PAP	Password Authentication Protocol
PGP	Pretty Good Privacy
POP	Point-of-Presence
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-In User Service
SATAN	Security Administrator Tool for Analyzing Networks
SHA	Secure Hash Algorithm
SLIP	Serial Line Protocol
SSL	Secure Socket Layer
SSN	Secure Server Network
TOS	Type-of-Service; Feld im IPv4-Header
TTL	Time-to-Live; Feld im IPv4-Header
V.24	Definitionen der Schnittstellenleitungen zwischen Datenendeinrichtungen und Datenübertragungseinrichtungen

VPN	Virtual Private Network
WAN	Wide Area Network
X.11	Kommunikationsprotokoll unter Unix, welches Anwendungen über das Netzwerk auf Terminals umleitet
X.25	Paketvermittelndes Netz

8 Literaturverzeichnis

1. Detken, Kai-Oliver: Security Concept - Sicherheitsmechanismen für das Intranet; NetSiKom99; Köln 1999
2. Atkinson, R.: Security Architecture for the Internet Protocol; Network Working Group; Request for Comments: 1825; Category: Standards Track; IETF 1995
3. Atkinson, R: IP Authentication Header; Network Working Group; Request for Comments: 1826; Category: Standards Track; IETF 1995
4. Atkinson, R: IP Encapsulating Security Payload (ESP); Network Working Group; Request for Comments: 1827; Category: Standards Track; IETF 1995
5. Weihrich, Thomas: Wasserdichtes Netz - Internet-Sicherheit, Teil 1. In: Gateway 07/97; Heinz Heise Verlag; Hannover, 1997
6. Valencia, Littlewood, Kolar: Cisco Layer Two Forwarding (Protocol) "L2F"; Network Working Group; Request for Comments: 2341; Category: Historic; IETF 1998
7. Rekhter, Moskowitz, Karrenberg, de Groot, Lear: Address Allocation for Private Internets; Network Working Group; Request for Comments: 1918; Category: Best Current Practice; IETF 1996
8. W. Simpson, Editor: The Point-to-Point Protocol (PPP); Network Working Group; Request for Comments: 1661; STD: 51; Category: Standards Track; IETF 1994