

SEMINAR „SICHERHEIT IN VERTEILTEN SYSTEMEN“
WS 2002/03 - DR. H.-J. MÜCK

Virtual Private Networks

Marcus Heinzl
Nils Michaelsen
Alexander Scheibe

Fachbereich Informatik
Universität Hamburg
Januar 2003

1	EINLEITUNG.....	2
1.1	BETRIEBSWIRTSCHAFTLICHER HINTERGRUND	2
1.2	BEGRIFFSABGRENZUNG „VPN“	2
1.3	ANFORDERUNGEN AN EIN VPN	3
1.3.1	<i>Anforderungen an die Netzwerksicherheit.....</i>	3
1.3.2	<i>logistische Anforderungen.....</i>	3
1.3.3	<i>Anforderungen bzgl. der Abwicklung betriebswirtschaftlicher Prozesse.....</i>	3
2	VPN-SICHERHEITSKONZEPT	4
3	NETZWERKARCHITEKTUR.....	6
3.1	AUFBAU EINES VPN.....	6
3.2	VPN UND FIREWALL.....	6
3.3	VPN-TYPEN	9
3.3.1	<i>Aufteilung des OSI-Modells in drei VPN-Ebenen</i>	9
3.3.2	<i>Einsatzgebiet der VPN-Typen.....</i>	10
4	IMPLEMENTATION EINES GESICHERTEN ÜBERTRAGUNGSKANALS.....	11
4.1	TUNNELING	11
4.1.1	<i>Prinzip</i>	11
4.1.2	<i>General Routing Encapsulation Tunnel</i>	11
4.2	LAYER-2-TECHNIKEN	12
4.2.1	<i>L2F</i>	12
4.2.2	<i>PPTP.....</i>	13
4.2.3	<i>L2TP</i>	14
4.2.4	<i>L2Sec</i>	15
4.2.5	<i>Layer-2 Nachbetrachtung.....</i>	16
4.3	LAYER-3-TECHNIKEN (IPSEC).....	17
4.3.1	<i>Einführung.....</i>	17
4.3.2	<i>Security Associations.....</i>	17
4.3.3	<i>Security Association Database.....</i>	18
4.3.4	<i>Security Policy Database.....</i>	19
4.3.5	<i>Kommunikationsmodi.....</i>	19
4.3.6	<i>Authentication Header.....</i>	20
4.3.7	<i>Encapsulating Security Payload.....</i>	22
4.3.8	<i>Verschachtelungen von IPSec Protokollen.....</i>	23
4.3.9	<i>SA Negotiation (IKE).....</i>	24
4.3.10	<i>Schwächen von IPSec.....</i>	29
4.4	LAYER-4 TECHNIKEN - SSL / TLS	31
4.4.1	<i>Einführung.....</i>	31
4.4.2	<i>Architektur</i>	31
4.4.3	<i>Verbindungsaufbau.....</i>	31
4.4.4	<i>Änderungen in TLS gegenüber SSL.....</i>	33
4.4.5	<i>Vorgehensweise von SSL/TLS.....</i>	33
4.4.6	<i>Sicherheit von SSL.....</i>	33
5	TYPISCHE VPN-SZENARIEN	34
5.1	INTRANET-VPN.....	34
5.2	EXTRANET-VPN	35
5.3	REMOTE-ACCESS-VPN	37
6	SCHLUSSBETRACHTUNG.....	38
7	QUELLENVERZEICHNIS.....	40

1 Einleitung

1.1 Betriebswirtschaftlicher Hintergrund

Im modernen Wirtschaftsleben ist der gezielte Einsatz von Informations- und Kommunikationstechnologien eine zentrale Notwendigkeit für Unternehmen, um auf heutigen Märkten konkurrenzfähig zu bleiben. Insbesondere in Bezug auf die immer kürzer werdenden Entwicklungs- und Lebenszyklen von neuen Produkten (Stichwort „Time To Market“). Unternehmen sind darauf angewiesen, IT-Technologien einzusetzen, um schnell, flexibel und kostengünstig agieren zu können. Im Rahmen zunehmender Globalisierung und damit weltweiter Verteilung von Standorten eines Unternehmens, sind Technologien notwendig, die die einzelnen Filialen eines Unternehmens bzgl. der Arbeitsprozesse integrieren und somit schnelles und effizientes Arbeiten ermöglichen. Es ist also notwendig, die IT-Infrastrukturen der einzelnen Filialen miteinander zu verbinden. VPN (virtuelle private Netzwerke) sind Systeme, die dies, den individuellen Ansprüchen eines Unternehmens entsprechend, ermöglichen und dabei auf die bereits vorhandene Infrastruktur öffentlicher Netze (Internet) zurückgreifen.

1.2 Begriffsabgrenzung „VPN“

Das Kürzel VPN steht für „virtuelles privates Netzwerk“. Unter einem VPN ist die Verbindung von Netzwerken oder Rechnern verschiedener Standorte von Unternehmen / Institutionen, mittels öffentlicher Kommunikationsnetze, zu einem in sich geschlossenen Gesamtnetz zu verstehen (siehe Abbildung 1), so dass letztendlich an verschiedenen Standorten Dienste (z.B. E-Mail, Datenzugriff, etc.) gemeinsam genutzt werden können.

Die Verbindung der einzelnen Standorte findet über eine öffentliche oder gemeinsam genutzte Kommunikationsplattform, meistens das Internet, statt. Deswegen spricht man von einem **virtuellen** Netzwerk, weil durch Nutzung der Paketdienste des Internets keine physikalische Verbindung, sondern nur eine logische Verbindung zwischen den zu verbindenden Standorten eingerichtet wird. Der Weg und die Bandbreite, mit denen ein Datenpaket von einem Netzwerk A zu einem Netzwerk B übertragen wird, werden jeweils dynamisch zugewiesen.

Man spricht von virtuellen **privaten** Netzwerken, weil Unternehmen natürlich den Anspruch an das sich ergebende Gesamtnetzwerk haben, dass es nicht von allen Nutzern des Internets zugänglich ist und nicht kompromittiert werden kann. Nur einer exklusiven geschlossenen Benutzergruppe, nämlich den Mitarbeitern oder Geschäftspartnern des Unternehmens, soll es erlaubt sein, die virtuelle Verbindung zu nutzen. Dementsprechend müssen Vorkehrungsmaßnahmen getroffen werden, um eine eingekapselte, verschlüsselte und authentifizierte Verbindungen zu ermöglichen.

Auf verschiedenen Schichten des ISO OSI-Modells können dabei entsprechend den individuellen Anforderungen eines Unternehmens, verschiedene Übertragungsmechanismen mit verschiedenen Verschlüsselungs- und Authentifizierungsverfahren zum Einsatz kommen. Wie dies technisch in die Implementation von VPN einfließt, wird im Kapitel 4 – „Implementation eines gesicherten Übertragungskanals“ beschrieben.

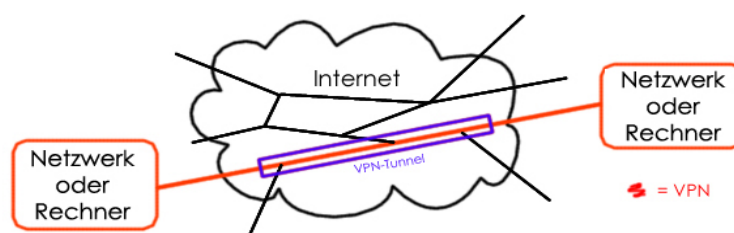


Abbildung 1: Schematische Darstellung eines VPN

1.3 Anforderungen an ein VPN

Das Einrichten eines virtuellen privaten Netzwerkes als betriebswirtschaftlicher Faktor der Informations- und Kommunikationsabwicklung zieht eine Reihe von Anforderungen, bzw. Kernproblemen nach sich, die ein solches System erfüllen muss. Im Vordergrund für diese Ausarbeitung stehen dabei die Anforderungen an die Netzwerksicherheit, um feindlich gesinnten Attacken¹ auf das Netzwerk entgegenzuwirken.

1.3.1 Anforderungen an die Netzwerksicherheit

- *Verschlüsselung der Daten:* Die Daten, die zwischen den Filialen eines Unternehmens ausgetauscht werden, müssen vertraulich bleiben, um Betriebsspionage zu verhindern.
- *Identifizierung und Authentifizierung:* Nutzer eines solchen Systems (Mitarbeiter, Geschäftspartner, Kunden) müssen sich entsprechend authentifizieren, mit dem System arbeiten zu dürfen.
- *Zugriffsberechtigung:* Es muss ein System von Berechtigungen geben, damit die Aktionen und Zugriffe von Benutzern im Rahmen der für sie vorgesehenen Aktivitäten bleiben.
- *Datenintegrität:* Es muss Vorkehrungsmaßnahmen gegen Datenverlust- und ungewollte Manipulation geben.
- *Angriffssicherheit:* Das Netz muss so gut es geht vor feindlichen Angriffen geschützt werden

1.3.2 logistische Anforderungen

- *Leistungsfähigkeit und Skalierbarkeit:* Das System muss steigendem Leistungsbedarf entsprechend skalierbar sein.
- *Weiterentwicklungsmöglichkeiten:* Neue Entwicklungen in der Kommunikationstechnologie, sowie Erweiterungen bzgl. betriebswirtschaftlicher Prozesse müssen integrierbar sein.
- *Administrierbarkeit des VPN:* Der Administrationsaufwand darf den Rahmen des Nutzens des Systems nicht übersteigen.
- *Integration des Netzwerks mit der Benutzerumgebung:* Das System muss sich in vorhandene Benutzungsschnittstellen integrieren lassen.
- ...

1.3.3 Anforderungen bzgl. der Abwicklung betriebswirtschaftlicher Prozesse

- *Globalisierung:* Integration von Geschäftsprozessen weltweit verteilter Filialen eines Unternehmens
- *virtuelle Arbeitsgruppen:* Unterstützung von Projektteams, die sich aus Mitarbeitern verteilter Standorte zusammensetzen
- *Mobile Arbeiter:* Einbindung reisender Mitarbeiter in die Geschäftsprozesse
- *Temporäre Geschäftsverbindungen:* Einbindung von zeitlich befristeten Geschäftspartnern
- *Kundenkommunikation:* Integration von Kunden in das eigene System, um Märkte mit sehr spezifischen und sich schnell ändernden Kundenwünschen bedienen zu können. (z.B. in der Zulieferindustrie der Automobilbranche)
- ...

¹ Bsp. für Attacken: siehe Vortrag „Überblick über Sicherheitsprobleme“ vom 07.11.2002

2 VPN-Sicherheitskonzept

Der zentrale Aspekt eines VPN ist mittels kryptographischer Verfahren eine hinsichtlich Integrität, Vertraulichkeit und Authentizität gesicherte Verbindung über ein öffentliches Netz herzustellen. Aus dem Einsatz von VPN resultiert aber eine komplexe Infrastruktur von Kommunikationseinrichtungen. Die verschlüsselte Verbindung eines VPN-Übertragungskanals allein reicht nicht aus, um eine VPN-Verbindung vor Angriffen zu schützen.

Wie geht man also vor bei der Erstellung eines Sicherheitskonzeptes und welche Vorrichtungen müssen im Rahmen von VPN letztendlich abgesichert werden?

Grundsätzlich gibt es zwei mögliche Ansätze für Unternehmen, ein Sicherheitskonzept für ein VPN-System zu erstellen:

1. Das Unternehmen traut einem Service-Provider, über den es an das Internet angebunden ist, zu, eine ausreichend gesicherte Verbindung zu etablieren.
2. Das Unternehmen muss sich selbst um eine ausreichend gesicherte Verbindung kümmern, gerade dann, wenn die Verbindung zwischen den Filialen und der Zentrale des Unternehmens über mehrere Netzanbieter stattfindet (z.B. internationale VPN).

Das Sicherheitskonzept für ein VPN ist eine Ergänzung zu einem generellen Sicherheitskonzept für Netzwerke. Dementsprechend wird es einem bereits vorhandenen Sicherheitskonzept eines Unternehmens in Bezug auf den zu erreichenden Sicherheitsgrad angepasst, wobei spezifische Besonderheiten der Absicherung eines Netzwerkverkehrs über öffentliche Netze zusätzlich zu beachten sind.

Im Allgemeinen sind folgende Absicherungsmaßnahmen für VPN unabhängig von den Ansprüchen von Unternehmen an individuelle Szenarien von zentraler Bedeutung:

- Schutzmaßnahmen für Quell- und Zielports des VPN-Übertragungskanals:
Eine verschlüsselte VPN-Verbindung allein reicht nicht aus, um sich vor einem Kompromittieren der VPN-Verbindung zu schützen. Die Quell- und Zielports der VPN-Verbindung könnten z.B. mit Denial-Of-Service Attacken lahmgelegt werden. Bei falscher Anordnung der Quell- und Zielports der VPN-Verbindung könnten z.B. E-Mail-Viren die Firewall passieren, weil der Virus aufgrund der Absicherungen des VPN-Übertragungskanals verschlüsselt übertragen wird.
- Welche Sicherheitsprotokolle werden auf welcher Ebene des OSI-Modells eingesetzt?:
Je nach individuellen Ansprüchen von Unternehmen und entsprechenden VPN-Szenarien ist festzustellen, ob eine gesicherte Verbindung auf den untersten Ebenen des OSI-Modells (Layer 2 – Sicherungsschicht) sinnvoll ist oder aber eine Sicherung der Verbindung zu höheren Schichten (Layer 3 – Vermittlungsschicht, Layer 4 – Transportschicht) oder gar bis zu den höchsten Schichten den Anwendungsschichten notwendig ist oder Sinn macht.
- Auswahl der kryptographischen Verfahren und Verschlüsselungssysteme:
Im Rahmen der eingesetzten Protokolle und des angestrebten VPN-Szenarios sind die Sicherheitsanforderungen an Authentifizierungs- und Verschlüsselungssystemen festzulegen.

Bzgl. der Sicherheitspolitik konkreter zu werden, macht an dieser Stelle wenig Sinn, da die Ansprüche von Unternehmen je nach Szenario hochgradig individuell sind. Interessant ist jedoch, welche operativen Absicherungsmaßnahmen im Rahmen eines Sicherheitskonzeptes zur Umsetzung eines VPN-Szenarios zur Verfügung stehen. Dies wird im folgenden Abschnitt auszugsweise wiedergegeben.

Die OSI-Ebenen und mögliche Absicherungsmechanismen

Bei der Implementation eines VPN, bzw. der Erstellung eines Sicherheitskonzeptes für VPN, bieten sich auf den verschiedenen Ebenen des ISO OSI-Schichtenmodells eine Vielzahl von Möglichkeiten, um Schutzvorkehrungen zu treffen.

	Schichtbeschreibung	Schutzmaßnahmen
OSI-Level	5-7 ↕ ↔ ↕	Anwendungsebenen SSH, Kerberos, Virusscans, Content Screening, IPSEC (IKE), ...

	Transport- und Netzwerkebene	
	3-4 ↕ ↔ ↕	TCP / UDP IP SSL, Socks V5, TLS IPSEC (AH, ESP), Paket Filtering, NAT
	1-2 ↕ ↔ ↕	Link- / physikalische Ebene (Bitübertragungs- und Sicherungsschicht) Tunneling Protokolle (L2TP, PPTP, L2F), CHAP, PAP, ...

3 Netzwerkarchitektur

3.1 Aufbau eines VPN

Es gibt zwei Möglichkeiten ein VPN aufzubauen:

Compulsory Mode: Bei einem ISP (Internet Service Provider) oder NSP (Network Service Provider) wird eine vom Anbieter administrierte VPN-Lösung zur permanenten Verbindung von Standorten angemietet, die auf dessen Infrastruktur zugreift. Diese Lösung hat den Nachteil, dass oftmals NSP-Netze, bzw. vom ISP zur Verfügung gestellte Dienstleistungen national beschränkt sind.

Voluntary Mode: Auch hier wird auf die Infrastruktur eines ISP oder NSP zurückgegriffen, jedoch ist das Unternehmen selbst dafür zuständig, eine Verbindung, die den Ansprüchen an die Netzwerksicherheit eines VPN genügt, aufzubauen.

Wenn ein LAN als eine Seite der Verbindung über öffentliche Kommunikationsplattformen in eine VPN-Lösung integriert werden soll, dann ist ein VPN-Gateway nötig. Das VPN-Gateway ist dafür zuständig, eine gesicherte Verbindung zwischen zwei Kommunikationspartnern herzustellen, also Daten zu verschlüsseln und zu kapseln, so wie Authentifizierungsmaßnahmen vorzunehmen.

Es ist aber auch möglich, einen einzelnen Rechner (z.B. Notebook eines mobilen Arbeiters) als eine Seite der Verbindung über öffentliche Kommunikationsplattformen einzusetzen. Auf diesem ist ein spezielles Client-Programm nötig, über das die gesicherte Verbindung mit dem VPN-Gateway des LANs einer Firmenzentrale hergestellt wird.

Interessant ist das Zusammenspiel von VPN-Gateways und Firewalls, da die am Gateway ankommenden Daten verschlüsselt sind. Mögliche Konfigurationen und deren Vor- und Nachteile werden im folgenden erörtert.

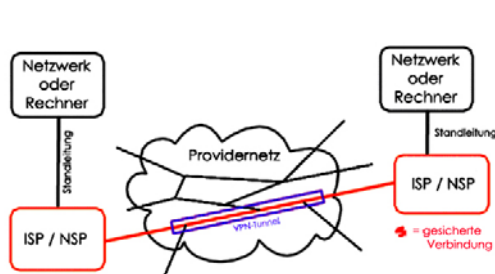


Abbildung 2: Compulsory Mode

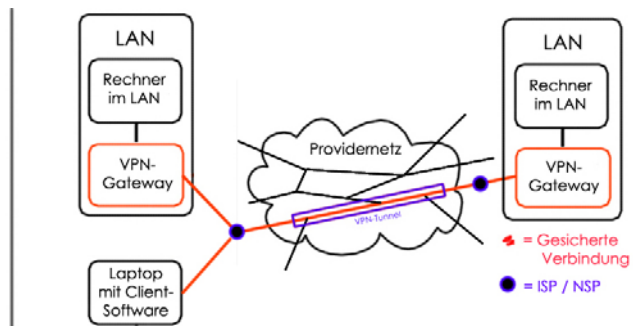


Abbildung 3: Voluntary Mode

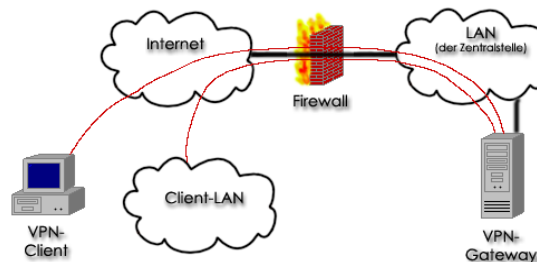
3.2 VPN und Firewall

Philosophie eines Firewallsystems

In Unternehmen bestehende Sicherheitskonzepte geben zumeist vor, dass die Verbindung zum Internet über eine Firewall stattfinden soll und dies die einzige Verbindung zum Internet sein darf. Dementsprechend müsste das VPN-Gateway hinter der Firewall platziert werden. Dies hat aber einige entscheidende Nachteile. In erster Linie ergeben sich Probleme daraus, dass die Übertragung bis zum VPN-Gateway verschlüsselt ist und der Inhalt einzelner Datenpakete somit für die Firewall nicht sichtbar ist. Im folgenden werden die Vor- und Nachteile möglicher Konfigurationen von VPN und Firewalls für eine Zentralstelle eines Unternehmens erörtert (für Filialen bzw. Client-Seiten lassen sich ähnliche Sicherheitsvorkehrungen treffen):

Das VPN-Gateway befindet sich hinter der Firewall

Bei dieser Konstellation passieren die an die VPN gerichteten Pakete die Firewall und werden erst auf dem VPN-Gateway entschlüsselt.



Vorteile:

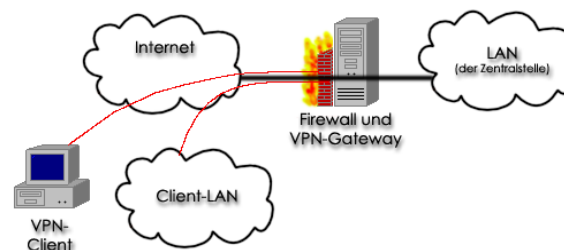
- Die Firewall ist wirklich die einzige Verbindung ins Internet

Nachteile:

- Eingehende für das VPN verschlüsselte Pakete können von der Firewall nicht vernünftig analysiert werden
- Die letztendlichen Zielrechner und Ports der Pakete können nur vom VPN-Gateway und nicht von der Firewall erkannt werden

Das VPN-Gateway und die Firewall sind auf einem Rechner

Das VPN-Gateway wird in Form einer IPSec-Lösung (siehe Kapitel 4) direkt in die Firewall integriert und befindet sich dementsprechend auf dem gleichen Rechner wie die Firewall.



Vorteile:

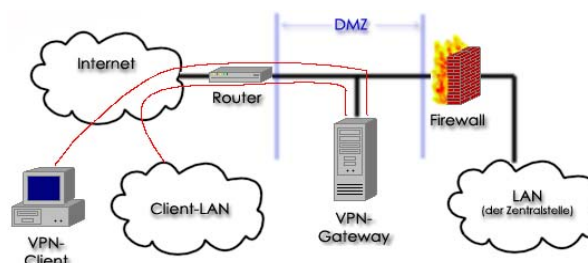
- Die Nachteile einer Konstellation, bei der das VPN-Gateway sich hinter der Firewall befindet, werden neutralisiert.
- Der Administrationsaufwand beschränkt sich auf die Firewall

Nachteile:

- Durch die Integration eines VPN-Gateways in die Firewall werden neue Ports auf der Firewall geöffnet, was neue Angriffsmöglichkeiten für Denial-Of-Service-Attacken bietet.

Das VPN-Gateway befindet sich in der DMZ

Das VPN-Gateway befindet sich in einer demilitarisierten Zone, durch die LAN und Internet voneinander getrennt werden. Die meisten am Router offenen Ports werden in der demilitarisierten Zone bedient und sind nicht für das LAN geöffnet.



Vorteile:

- Es können von außen keine IP-Pakete ins LAN geschleust werden, die nur scheinbar aus dem VPN-Netz kommen
- Die vom VPN-Gateway entschlüsselten Pakete müssen noch die Firewall zum LAN passieren.

- Der Zugriff von außen über das VPN kann auf bestimmte Rechner und Ressourcen beschränkt und E-Mails können auf Viren untersucht werden.

3.3 VPN-Typen

3.3.1 Aufteilung des OSI-Modells in drei VPN-Ebenen

Generell lassen sich die 7 Schichten des OSI-Referenzmodells auf drei Ebenen die für VPN-Technologien wichtig sind, um praxisrelevante Szenarien zu implementieren, unterteilen:

1. VPN-Übertragungskanäle auf der Anwendungsebene
2. VPN-Übertragungskanäle auf der Transport- / Netzwerkebene
3. VPN-Übertragungskanäle auf der physikalischen- / Linkebene

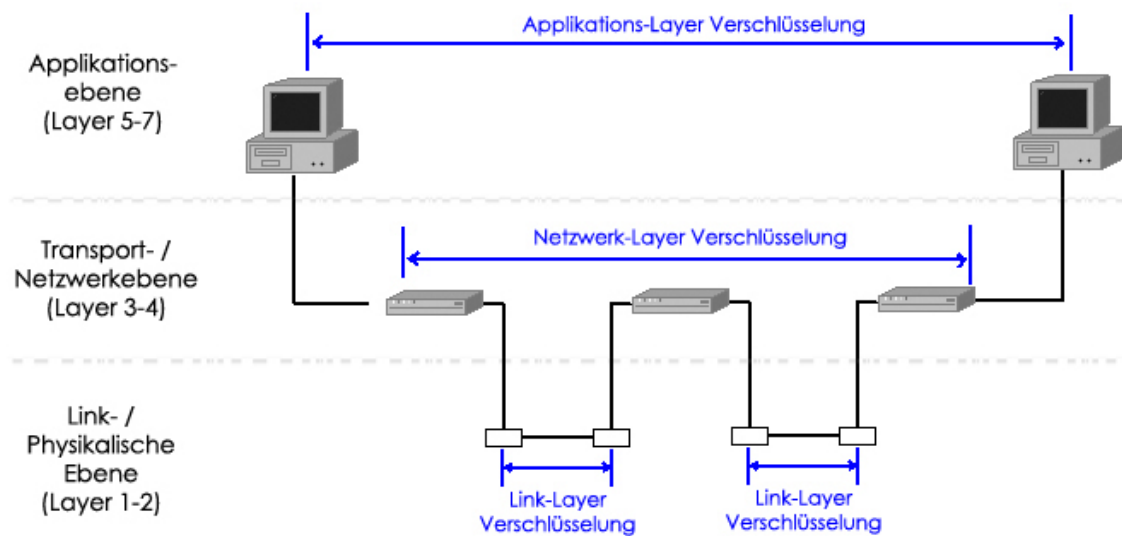


Abbildung 4 : VPN-Typen auf den Schichten des OSI-Modells

3.3.2 Einsatzgebiet der VPN-Typen

VPN auf der Applikationsebene – Layer 5 – 7

VPNs auf der Applikationsebene werden zur Verbindung von zwei Rechnern eingesetzt, auf denen jeweils Softwareprogramme installiert, die eine Vorrichtung zum Aufbau eines gesicherten Übertragungskanals integriert haben.

Der Einsatz von VPN-Übertragungskanälen auf der Anwendungsebene setzt eine gewisse Vertraulichkeitsbasis der kommunizierenden Partner voraus, da die verschlüsselte Verbindung von einem End-Gerät eines Netzes zu einem anderen End-Gerät eines Netzes stattfindet. Das bedeutet letztendlich, dass der gesicherte Übertragungskanal Sicherheitsvorkehrungen in Form einer Firewall überbrückt und die Firewall somit nicht in der Lage ist, die Inhalte der Datenpakete zu überprüfen.

VPN auf der Transportebene – Layer 4 (SSL)

VPN auf der Transportebene sind wie VPN auf der Applikationsebene meistens in Anwendungen integriert und dienen somit dem Aufbau einer verschlüsselten Verbindung zwischen zwei Anwendungen. Weil sie in die Anwendung integriert sind, erlauben sie eine hohe individuelle Sicherung zwischen den Kommunikationspartnern, weil theoretisch alle denkbaren Verschlüsselungs- und Authentifizierungsverfahren integrierbar sind.

Ein Beispiel für den Einsatz von Layer4-VPN sind Internet-Browser, die SSL integriert haben, um sichere Transaktionen durchführen zu können. Der Tunnel zwischen z.B. zwei E-Commercepartnern wird dabei automatisch geöffnet.

VPN auf der Vermittlungsebene – Layer 3

Der generelle Vorteil von VPN, die den sicheren Kommunikationskanal ab Layer 3 aufbauen, ist, dass neben TCP/IP, also ein Protokoll des Layers 4, auch andere Protokolle des Layers 4 (Protokolle für RPC und UDP) eingesetzt werden können.

VPN auf der Link- / physikalischen Ebene – Layer 1 – 2

Protokolle auf der Link- physikalischen Ebene sind unabhängig von einem spezifischen Netztyp, wie z.B. IP-Netze, einsetzbar. Es sind also unter zu Hilfenahme bestimmter Transportmechanismen (Tunneling, wird zu einem späteren Zeitpunkt in dieser Ausarbeitung erklärt) VPN-Verbindungen über eine Kombination verschiedener Netzinfrastrukturen denkbar. (ATM, Frame-Relay, IP-Netze, ...)

Ein weiterer Vorteil niedriger Schichten ist, dass diese besser zu warten sind, da sich der technische Aufwand zum größten Teil auf Hardware mit speziellen Vorrichtungen für einen gesicherten Übertragungskanal beschränkt. Dementsprechend lassen sich Quality-of-Service-Garantien (z.B. Skalierung der Bandbreite, etc.) auf diesen Schichten gut umsetzen.

4 Implementation eines gesicherten Übertragungskanals

4.1 Tunneling

4.1.1 Prinzip

Mit dem Verfahren des Tunnelings können beliebige Datenpakete, die zu beliebigen Protokollen gehören können, über ein Transitnetz verschickt werden, indem die Datenpakete als Nutzlast (Payload) eines für das Transitnetz zuständigen Protokolls verschickt werden. Z.B. ist es somit möglich, IP-Pakete über ein nicht IP-fähiges ATM-Netz als Nutzlast des für das ATM-Netz zuständigen Protokolls zu verschicken (IP-over-ATM). Ein anderes Beispiel wäre das Versenden von IPv6-Paketen über ein Teilnetz, das nur für IPv4-Pakete ausgelegt ist.

Das Verschicken eines Protokoll-Pakets als Nutzlast eines anderen Protokolls wird auch als Encapsulation bezeichnet. Beim Encapsulation-Vorgang wird ein zusätzlicher Protokollheader, der sogenannte Tunnel-Header, der dem Originalpaket vorangestellt ist, erzeugt. Im Tunnel-Header befinden sich Quell- und Zielports für eine Weiterleitung des als Payload verschickten Datenpaketes. Der Anfangspunkt eines Tunnels wird dort definiert, wo der zusätzliche Header angefügt wird, und analog dazu befindet sich der Endpunkt eines Tunnels dort, wo der zusätzliche Header wieder entfernt wird. Im Hinblick auf die drei eingeführten VPN-Typen ist offensichtlich, welche Ausmaße ein jeweils entsprechender VPN-Tunnel annimmt. Bei VPN auf der Anwendungsebene z.B. erstreckt sich der VPN-Tunnel auf dem ganzen Weg zwischen zwei End-Geräten. (Siehe Abbildung 4)

Der Trick des Tunnelings bzgl. VPN-Technologien ist, dass Daten, die als Payload eines Transportprotokolls verschickt werden, für den Tunnel-Transport verschlüsselt werden können. Mal abgesehen davon, dass einem Angreifer dadurch zum einen die Inhalte der Datenpakete so nicht zugänglich sind, kommt hinzu, dass der Angreifer zusätzlich nicht feststellen kann, welches letztendlich das Ziel ist, das das als Payload verschickte Datenpaket hat, da Informationen über Zielports und IP-Adressen des als Payload verschickten Protokolls ebenfalls verschlüsselt werden und erst wieder vom VPN-Gateway entschlüsselt werden.

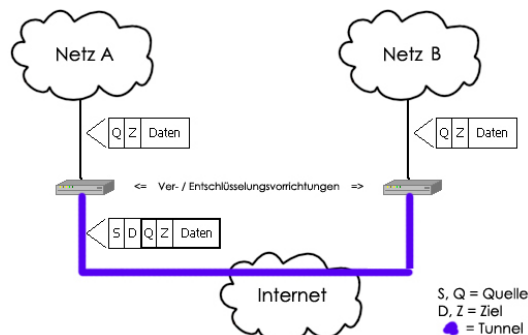


Abbildung 5: VPN Tunnel

4.1.2 General Routing Encapsulation Tunnel

Der GRE-Tunnel ist eine Standardisierung für ein Tunnelverfahren (1994). Es handelt sich dabei nicht um ein konkretes Protokoll, sondern eher um eine generelles Verfahren für Tunneling.

Ein GRE-Paket beschreibt drei Abschnitte:

- *GRE-Header (Protokollkopf)*: Enthält Informationen über eingesetzte Tunnel- und Verschlüsselungsalgorithmen
- *Delivery Header (Netzwerk-Protokollkopf)*: Speichert das Ziel außerhalb des Tunnels
- *Payload (Nutzlast)*: Ein beliebiges Paket aus höheren Protokollschichten

4.2 Layer-2-Techniken

Die Layer-2-VPN-Techniken sind auf der 2-ten Ebene des OSI-Referenzmodells angesiedelt. Aufgrund dieser Einordnung besitzen sie drei Vorteile gegenüber den Layer-3-Techniken (siehe 4.3).

1. Sie sind multiprotokollfähig, d.h. sie können außer IP auch z.B. IPX, SNA und NetBios übertragen.
2. Ebenso von Vorteil ist die im allgemeinen leichtere Wartbarkeit von tieferen Schichten gegenüber höheren.
3. Sie ermöglichen eine problemlose Network Address Translation (NAT), die zwischen VPN-Client und VPN-Gateway von IP-Routern vorgenommen wird. Bei den Layer-3-Techniken würde dies zu Fehlern führen, da Daten dieser Techniken Daten von IP-Paketen sind, und eine NAT im Allgemeinen den Hashwert von IP-Paketen verändert.

In der Regel wird ein Point-to-Point-Protokoll (PPP) im Tunnel eingesetzt, so dass mithilfe einiger PPP-Authentifizierungsprotokolle z.B. PAP und CHAP, Sicherheitseigenschaften in die Layer-2-VPN-Techniken mit einfließen.

Alle im folgenden behandelten Techniken liegen als Vorschläge bzw. RFCs bei der IETF vor.

4.2.1 L2F

Layer-2-Forwarding (L2F) wurde gemeinsam von Cisco, Northern Telecom und Shiva entwickelt. Die Bedeutung von L2F als Layer-2-Technik ist mittlerweile zugunsten von PPTP (siehe 4.2.2) und L2TP (siehe 4.2.3) zurückgegangen. Layer-2-Forwarding wird von der IETF unter RFC-2341 beschrieben.

Wie alle anderen im folgenden behandelten Layer-2 Verfahren ermöglicht auch L2F den Aufbau eines VPN über ein öffentliches Netz, indem ein Tunnel zwischen einem Client und einem VPN-Server eingerichtet wird. Für eine L2F-VPN-Verbindung in einem Unternehmen ist dabei eine Wählverbindung über einen Internet Service Provider (ISP) notwendig. L2F kann außer für das Internet-Protokoll auch für andere Medien z.B. ATM, Frame-Relay, HDLC oder FDDI verwendet werden.

In einen L2F-Tunnel ist es möglich, multiple logische Kanäle zu schalten, so dass mehrere Verbindungen gleichzeitig möglich sind. Dieses hat den Vorteil, dass z.B. das LAN einer Filiale nur über eine Wählverbindung an das LAN des Firmenhauptsitzes angeschlossen werden muss.

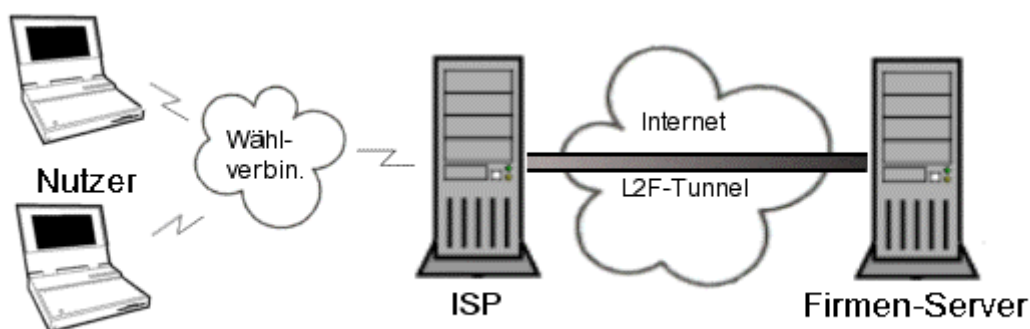


Abbildung 6: Skizzierung eines L2F-Tunnels vom POP (ISP) zum VPN-Gateways eines Unternehmens

Abbildung 6 stellt einen L2F-Tunnel zwischen mehreren Clients und einem Server im Unternehmens-LAN dar. Der eigentliche L2F-Tunnel existiert allerdings nur zwischen ISP und dem VPN-Gateway des Unternehmens. Zur Authentifizierung der Clients wird das Point-to-Point-Protokoll (PPP) verwendet, des weiteren können TACACS+ und RADIUS eingesetzt

werden. Die Authentifizierung erfolgt dabei sowohl beim VPN-Gateway als auch bei der Einwahl zum ISP.

L2F vollzieht sich auf einer unteren Protokollebene, so können außer IP auch z.B. IPX und NetBUI transportiert werden.

Bei einem Layer-2-Frame, das beim POP vom Fernarbeitsplatz eintrifft, wird das Transparency Byte entfernt, anschließend in den Tunnel geschickt und über das Internet oder den Backbone des ISP bis zum Network Access Server (NAS) des Unternehmens geleitet. Am VPN-Gateway wird nach Prüfung das Layer-2-Frame entgegengenommen, die Tunnelhülle entfernt und weiterverarbeitet.

4.2.2 PPTP

Das Point-to-Point-Tunneling-Protokoll (PPTP) wurde zusammen von Microsoft, 3COM, ECI Telematics, Ascend Communications und USRobotics entwickelt. PPTP ist als eine Erweiterung von PPP zusehen, und ist, schon aufgrund seiner Implementation in Microsoft Betriebssystemen Windows NT, Windows 95 und Windows 98, weit verbreitet und relativ etabliert. PPTP ist als RFC-2637 beschrieben, wurde jedoch nicht zum Standard ernannt.

PPTP ermöglicht Anwendern einen sicheren Fernzugriff, über das Internet oder andere Netzwerke sicher auf ein Firmennetzwerk, indem der Anwender sich bei einem ISP einwählt oder eine direkte Verbindung zum Internet herstellt. Ziel von PPTP ist es, diesen Remotezugriff einfacher zu gestalten. Dieses wurde erreicht, indem das PPP mit einem GRE-Header gekapselt und mit einem zusätzlichen IP-Header versehen wird. Dadurch wird erreicht, dass auch IP-, IPX- oder NetBEUI-Verkehr in IP-Paketen übertragen werden kann.

Durch das Wirken von Microsoft besteht eine enge Anbindung an Windows NT durch die Authentifizierungsverfahren PAP und CHAP, sowie Microsofts verbesserte Version MS-CHAP.

Um die Vertraulichkeit der PPP-Verbindung abzusichern, hat Microsoft eine Verschlüsselung entwickelt, die Microsoft Point-to-Point Encryption (MPPE). Sie arbeitet dabei mit MS-CHAP zusammen und stützt sich dabei auf den MD4 Hash-Algorithmus² (40-Bit-Schlüssel). MPPE wird für einen sicheren Schlüsselaustausch während einer PPP-Session eingesetzt.

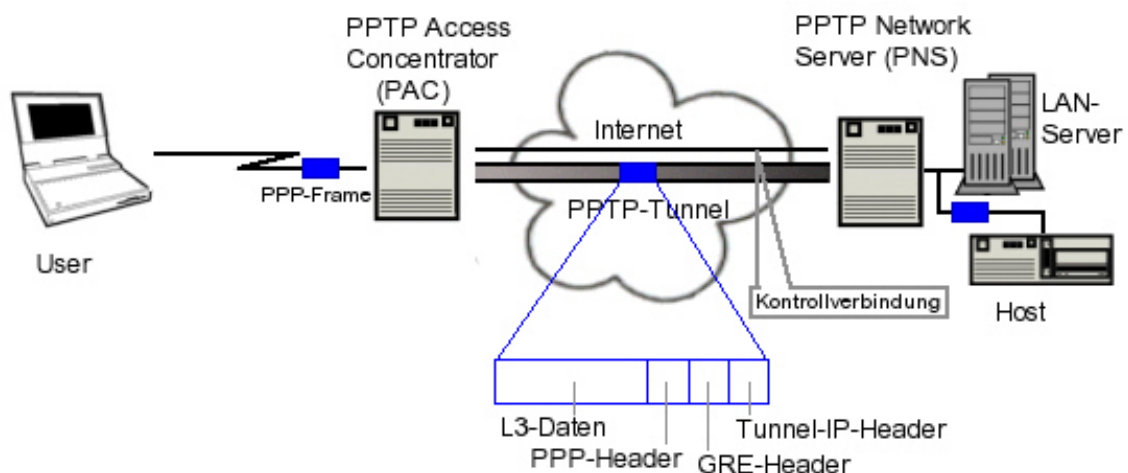


Abbildung 7: Skizzierung eines PPTP-Tunnels.

In Abbildung 7 ist das Prinzip eines PPTP-Tunnels dargestellt. Erkennbar ist eine zum eigentlichen Tunnel verlaufende Kontrollverbindung. Beim PPTP-Verfahren findet eine Trennung

² Es sind auch Schlüssel bis zu 128Bit möglich, jedoch waren diese ursprünglich nicht außerhalb der USA erlaubt, und sind in den meisten Systemen noch nicht eingeführt.

von Daten- und Kontrollfluss statt. Die Kontrollverbindung dient zur Übertragung von Kontrollinformationen, während die Datenpakete über den eigentlichen Tunnel laufen, dieses wird als out-band-Verfahren bezeichnet. Dabei wird die Kontrollverbindung zwischen dem PPTP-Access-Concentrator (PAC) und PPTP-Network-Server (PNS) vor der eigentlichen PPP-Verbindung aufgebaut.

Dem den Tunnel passierenden PPP-Frame werden zwei Header vorangestellt, zunächst der GRE-Header, der neben der Datenfluss- und Kollisionskontrolle hauptsächlich für die Kapselung der PPP-Pakete zuständig ist. Und als zweites der Tunnel-IP-Header, dem nur die Adressen von PAC und PNS bekannt sind. Durch den GRE-Header kann eine Datenflusskontrolle nach dem Sliding-Window-Prinzip durchgeführt werden.

PPTP-Verbindungen werden im Normalfall auf Aufforderung von einem Endgerät initiiert, wobei nur eine Verbindung mit einem Kanal zwischen PAC und PNS aufgebaut wird. Dieser nutzerinitiierte dynamische Dial-In Tunnel wird auch als voluntary Tunnel bezeichnet. Da diese Art des Zugriffs dem Benutzer erlaubt, neben der Adresse des PACs auch andere Adressen anzuwählen, und so unter Umständen die Integrität des Tunnels gefährdet werden kann, gibt es die Möglichkeit, eine Verbindung auf Anfrage zu initiieren.

Dieser sogenannte compulsory Tunnel, d.h. verpflichteter Tunnel, besitzt einen vordefinierten Weg, der nicht verlassen werden kann. Er wird vom NAS aus zum PAC aufgebaut, und hat den Vorteil, mit einer Kontrollverbindung mehrere Verbindungen pro Tunnel zu ermöglichen. Von einem Client, der über einen compulsory Tunnel verbunden ist, können keine Adressen die ihm nicht explizit erlaubt wurden, angewählt werden.

Ein Nachteil des statischen (compulsory) Tunnels ist, dass er ein entsprechendes Equipment, voraussetzt, und den Wartungs- und Betriebsaufwand erhöht. Ebenso wird die Kontrollverbindung des Out-Band-Verfahrens, die bei statischen Verbindungen eine höhere Gefährdung bezüglich eines gezielten Angriffs darstellt, als Nachteil angesehen.

4.2.3 L2TP

Das Layer-2 Tunneling Protocol (L2TP) ist das momentan beherrschende Protokoll des Layer-2. Es wurde grundlegend von Cisco mit entwickelt und ist als Industriestandard unter RFC-2661 von der IETF verabschiedet worden. Die Verbreitung von L2TP hat aufgrund seiner Implementationen in Windows 2000 und XP stark zugenommen.

L2TP kann als Mischform aus den Techniken L2F und PPTP betrachtet werden, so wird die Leistungsfähigkeit von L2F mit den Vorteilen von PPTP verknüpft. So sind je nach Implementierung außer über IP-Netzwerke z.B. auch Verbindungen über ATM, Frame Relay oder X.25 möglich (Windows Implementationen unterstützen nur IP).

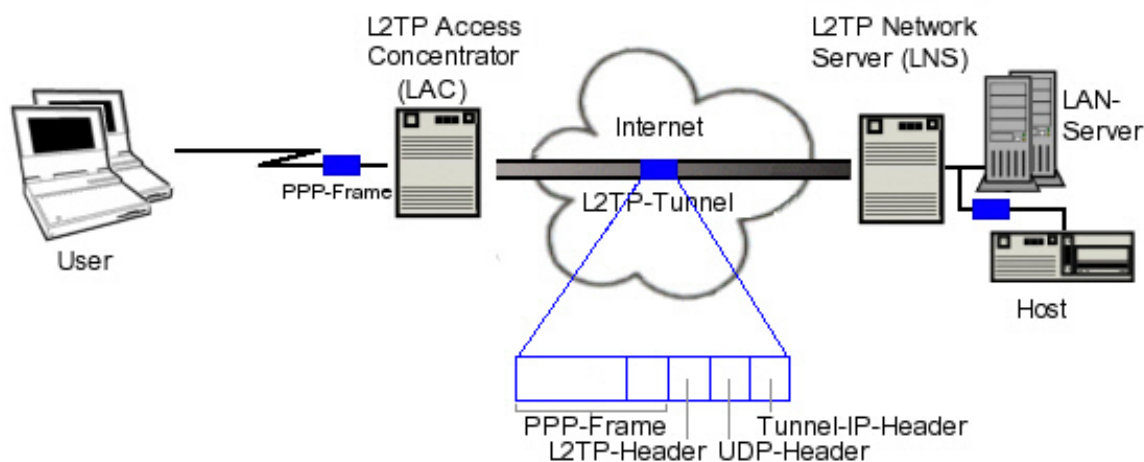


Abbildung 8: Skizzierung eines L2TP-Tunnels

Wie bei PPTP muss vor dem Aufbau einer PPP-Verbindung zwischen L2TP-Access-Concentrator (LAC) und L2TP-Network-Server (LNS) (siehe Abbildung 8) eine Kontrollverbindung aufgebaut werden, nur dass diese sich bei einem L2TP-Tunnel wie eine In-band Lösung verhält. Ein L2TP-Tunnel kann entweder via Dail-In als voluntary Tunnel, oder auf Anforderung als Dail-Out bzw. compulsory Tunnel initialisiert werden. Zwischen LAC und LNS können mehrere Tunnel, mit jeweils einer Kontrollverbindung aufgebaut werden, über die wiederum mehrere logische PPP-Verbindungen betrieben werden können. Über jede solcher PPP-Verbindungen kann unabhängig von anderen Verbindungen kommuniziert, und ein anderes von PPP unterstütztes Protokoll, z.B. IP, IPx, NetBEUI, AppleTalk und SNA verwendet werden. Zur Authentifizierung können dabei die von PPP unterstützten Verfahren eingesetzt werden, z.B. PAP, CHAP oder EAP.

Diese Authentifizierung können allerdings nur beim Aufbau einer Kontrollverbindung durchgeführt werden, wodurch zuerkennen ist, dass beim L2TP keine Mechanismen vorgesehen sind, die Vertraulichkeit während der Datenübertragung zu gewährleisten. Um eine Vertraulichkeit zu gewährleisten, sollte ergänzend das IPSec-Protokoll (siehe 4.3) eingesetzt werden. Durch den Einsatz von IPSec kann für den L2TP-Tunnel eine sichere End-to-End-Verbindung erreicht werden, da IPSec eine Authentifizierung einzelner Pakete ermöglicht.

Die Absicherung mit dem IPSec-Protokoll kann dabei, über verschiedene Abschnitte der Verbindung zwischen Client und Host im Unternehmensnetzwerk erfolgen. Zum einen kann eine Absicherung des eigentlichen Tunnels zwischen LAC und LNS als Dienstleistung des ISPs erfolgen. Des weiteren ist es möglich und ausreichend um eine vollständige End-to-End Absicherung zu erreichen, die IPSec-Absicherung vom Client bis zum LNS durchzuführen. Und als drittes kann die Absicherung auch vom Client bis zum Server im Intranets reichen.

4.2.4 L2Sec

Als Sicherheitsstandard für IP-Netzwerkverbindungen ist IPSec unübertroffen. Für Remote Access beziehungsweise Bridging ist dieses Protokoll schlecht oder gar nicht geeignet. Der Standardisierungsvorschlag Layer-2 Security (L2Sec) will diese Lücke schließen.

L2Sec kann als Kombination aus L2TP und SSL/TLS-Authentifizierung aufgefasst, und auf den Standardisierungsvorschlag „RFC 2716“, als „PPP EAP TLS Authentication Protocol“ bezeichnet, zurückgeführt werden.

Im Gegensatz zu IPSec, setzt L2Sec während des Verbindungsaufbaus keine gültige Adresse, was bei IPSec als Unzulänglichkeit gesehen wird. Da aber gerade beim Aufbau einer sicheren Datenkommunikation eine angemessene Authentifikation erforderlich ist, wurden im L2Sec-Protokoll die erweiterte PPP-Authentifizierung EAP und die Verschlüsselungseigenschaften von TLS (SSL) (siehe 4.4) verschmolzen.

EAP

Das Extensible Authentication-Protokoll (EAP) stellt einen Standardmechanismus zur Unterstützung zusätzlicher Authentifizierungsmethoden innerhalb des PPPs dar. Durch die Verwendung des EAPs kann eine Unterstützung für verschiedene Authentifizierungsmethoden hinzugefügt werden, beispielsweise Tokenkarten, einmalige Kennwörter, Authentifizierung durch öffentliche Schlüssel mit Hilfe von Smartcards, Zertifikaten u.v.a. Das EAP gewährleistet mehr Sicherheit gegen Hacker- und Wörterbuchangriffe sowie gegen das Erraten von Kennwörtern als andere Authentifizierungsmethoden (beispielsweise CHAP).

Ergebnis der Verwendung von EAP und TSL

Durch SSL/TLS und EAP und der Möglichkeit, andere Protokolle als IP, z.B. IPx, SNA, Net-Bios und HDLC nutzen zu können, so wie problemloses Bridging zu ermöglichen, besitzt L2Sec gegenüber IPSec Vorteile, so dass Implementierungen dieser Technologie bei Standardisierung durch die IETF eine große Verbreitung vorhergesagt wird. Allerdings besitzt L2Sec auch einige Nachteile gegenüber IPSec, so können einzelne Prozesse und Ports nicht abgesichert werden, und der Protokoll-Overhead gegenüber IPSec ist noch wesentlich größer.

4.2.5 Layer-2 Nachbetrachtung

Die verbreiteten Layer-2-Verfahren L2F, PPTP und L2TP haben den Nachteil, dass lediglich die Datenintegrität und Nutzer-Authentisierung definiert sind, nicht jedoch der Schutz der Daten gegen Ausspähen, Maskieren oder andere Manipulationen. Um auch leistungsfähige Verschlüsselungsverfahren in die Übertragung zu integrieren, wurde im Rahmen des Internet-Protokolls IPv6 der IPSec-Standard entwickelt. IPSec soll nach allgemeiner Auffassung den künftigen Standard für VPN-Tunneling darstellen, jedoch bleibt abzuwarten, inwieweit sich L2Sec entwickelt.

4.3 Layer-3-Techniken (IPSec)

4.3.1 Einführung

IPSec ist eine Menge von Maßnahmen zur Sicherung eines Kommunikationskanals auf Schicht 3 des OSI Referenzmodells.

Durch die Öffnung des Internets für private Personen und kommerzielle Organisationen wurde eine Reihe von Sicherheitsmaßnahmen nötig. Die Entwicklung solcher Maßnahmen wurde 1992 durch eine IETF Working Group begonnen. Sie sind in der Ende 1995 festgelegten Weiterentwicklung des Internet Protokolls, IPv6, bereits enthalten.

Da sich IPv6 jedoch bis heute noch nicht etabliert hat, die Sicherheitseigenschaften aber bereits heute benötigt werden, wurden sie in der IPSec genannten Sammlung von Protokollen zusammengefasst, die optional in Verbindung mit dem IPv4 Protokoll verwendet werden.

IPSec soll nach [Davis] folgende Eigenschaften bieten können:

- Data origin authentication
- Connectionless integrity
- Anti-Replay
- Data confidentiality (optional)
- Limited traffic flow confidentiality (optional)

Ein weiteres Ziel von IPSec ist die Offenheit zwischen verschiedenen Implementationen. Dazu soll es auch möglich sein, verschiedene Protokolle, Kommunikationsmodi, Verschlüsselungsalgorithmen und Hashverfahren zu benutzen. Um dies zu gewährleisten, bietet IPSec eigene Verfahren zur Einigung über die Details einer Verbindung.

Zunächst werden die IPSec Sicherheitsarchitektur besprochen, zu der Security Associations, Security Association Database und Security Policy Database gehören. Danach werden Transportmodus und die als IPSec Protokolle bezeichneten IP Header Erweiterungen besprochen. Details zu Verschlüsselungs- und Hash-Verfahren wurden in [Vortrag4] besprochen oder finden sich in [Böhmer] oder [Davis]

4.3.2 Security Associations

In IPSec können viele Parameter wie z. B. die Verschlüsselung oder der Kommunikationsmodus individuell eingestellt werden. Daher ist für jede Verbindung eine Einigung zu erzielen, die besagt, wie die Daten übertragen werden. Diese Einigung zwischen den Endpunkten wird Security Association, kurz SA, genannt. Eine SA wird in den Endpunkten der Verbindung gespeichert.

Eine SA ist ein Tripel bestehend aus SPI, Ziel-Adresse und Protokoll. Die SPI ist ein eindeutiger 32bit Wert zur Identifikation der jeweiligen Verbindung. Die Ziel-Adresse kann nicht nur als eine einzelne Adresse, sondern auch als ein Adressbereich angegeben werden. Als Protokoll können bisher AH³ und ESP⁴ verwendet werden. Auf Grund der Offenheit von IPSec gegenüber Neuerungen, können hier auch potentiell neue Protokolle verwendet werden.

³ AH = Authentikation Header, siehe Abschnitt 4.3.6

⁴ ESP = Encapsulating Security Payload, siehe Abschnitt 4.3.7

In einer SA kann genau ein IPSec-Protokoll (AH oder ESP) angegeben werden. Beide Protokolle können aber auch verschachtelt verwendet werden. Ist dies durch eine Security Policy gefordert, so kann dies durch Verwendung zweier SAs erreicht werden.

SAs sind simplex bzw. unidirektional. So muss für jede Richtung (inbound/outbound) eine passende SA vorhanden sein. Gespeichert werden die SAs in einer Security Association Database.

4.3.3 Security Association Database

Die Verwaltung der ausgehandelten SAs geschieht durch die Speicherung in der Security Association Database. Dabei werden nur SAs für aktive Verbindungen gespeichert. Zusätzlich werden zu jeder Security Association noch weitere Parameter einer Verbindung gespeichert. Diese sind nach [RFC2401]:

- Sequence Number, ein 32-bit Zähler
- Sequence Number overflow, bestimmt bei ausgehenden Verbindungen, ob ein Overflow ein Ereignis erzeugen soll
- Anti-Replay Windows, bestimmt für eingehende Verbindungen, ob es sich um eine Wiederholung (Replay handelt)
- Kryptographische Informationen für die AH Authentikation (Algorithmus, Schlüssel, etc.)
- Kryptographische Informationen für die ESP Authentikation
- Kryptographische Informationen über Algorithmus zur Verschlüsselung
- *SA Lifetime*
- *IPSec protocol mode*, Auswahl des Kommunikationsmodus für AH bzw. ESP; kann auch wildcard sein.
- PMTU, Maximale MTU eines IP Datagrams

```
Inbound esp sas:  
Spi: 0x71BB425D(1908097629)  
Transform: esp-des esp-md5-hmac  
In use settings={Tunnel, }  
Slot: 0, conn id: 2000, flow_id: 1, crypto mal: mode  
Sa timing: remaining key lifetime (K/sec): (4608000/3500)  
IV sitze: 8 bytes  
Replay detection support: Y
```

Abbildung 9: Auszug der SAD eines Cisco Routes für eine inbound ESP (nach [Northcutt et. Al.], Seite 198)

Zu bemerken ist in dem in Abbildung 9 gezeigten Eintrag einer SAD, dass hier keine Destination IP-Adresse enthalten ist. Somit gilt dieser Eintrag für alle eingehenden Verbindungen.

Bei der Abarbeitung von SAD gilt, dass die Einträge sequentiell abgearbeitet werden. Jeder passende Eintrag wird für die weitere Verarbeitung eines Paketes benutzt. Die SAs können aber nicht beliebig sein, sondern unterliegen bei der Verarbeitung den Einschränkungen der Security Policy Database, kurz SPD.

4.3.4 Security Policy Database

Eine Security Association kann nicht beliebig ausgehandelt werden. Sie müssen den Sicherheitsanforderungen der jeweiligen Site entsprechen, die an der VPN beteiligt ist. Diese Anforderungen in der Security Policy Database, kurz SPD, gespeichert. Da die SAs unidirektional sind, werden auch die Security Policies für ein- und ausgehenden Verkehr festgelegt.

Dabei können folgende Merkmale in der SPD enthalten sein :

- Destination IP
- Source IP
- Transport Layer Protocol
- Systemname: FQDN oder X.500 DN
- User ID: Fully Qualified DNS User Name oder X.500 DN

Die Security Policy Database liegt einer Security Association sowohl bei eingehenden als auch bei ausgehenden Verbindungen zugrunde. Vor dem Eintrag einer SA in die SAD werden die Einträge der Security Policy Database, Selektoren genannt, sequentiell abgearbeitet. Danach wird entschieden, wie mit einem Paket verfahren wird. Dabei kann es verworfen werden, ohne dass dieses zur IPSec-Verarbeitung angenommen oder weitergereicht wird⁵. Im letzteren Fall muss die SPD auch einen Verweis auf eine in der SAD gespeicherte SA enthalten, welche die IPSec-Details verbindlich festlegt.

Nun sollen die Details der in der Security Association Database gespeicherten Eigenschaften betrachtet werden.

4.3.5 Kommunikationsmodi

IPSec bietet bei Verbindungen zwei verschiedene Kommunikationsmodi, den Transport und den Tunnel Modus.

Der Transport Modus sichert lediglich die Nutzlast eines IP Paketes. Daher fehlt ihm die Möglichkeit, die Struktur eines Netzes zu verbergen, was vor allem bei einer Kommunikationsverbindung zwischen zwei Netzen über das Internet sinnvoll ist. Daher eignet sich der Transportmodus meist nur für die Host-zu-Host Kommunikation.

Für die Gateway-to-Gateway Kommunikation eignet sich der Tunnelmodus, wobei nach [Northcutt] unter einem Tunnel der Prozess der Kapselung eines Paketes in einem anderen verstanden wird. Dabei werden neben der Nutzlast auch die Adressinformationen mit einbezogen. Im Kontext von IPsec werden IP über IP-Tunnel gebildet. Obwohl IPSec auf Schicht 3 des ISO/OSI Modells arbeitet, kann so trotzdem die Schicht 3 gesichert werden.

Zu der Kommunikation mit Gateways steht in [RFC2401]: “Whenever either end of a security association is a security gateway, the SA MUST be tunnel mode.” Ein Gateway braucht daher nur den Tunnelmodus anzubieten, während ein Host den Transportmodus anbieten muss!

⁵ Somit kann ein IPSec Gateway auch zur Implementation einer Firewall verwendet werden (vgl. [Northcutt et. al.], S. 216 ff.)

4.3.6 Authentication Header

Bei der Übertragung von IP-Packeten entsteht das Problem der Verfälschung auf dem Übertragungsweg. Um die Verfälschung zu erkennen, enthält das Internet Protocol eine Checksumme, die aber wegen der Veränderung des TTL-Feldes bei jedem Hop neu berechnet wird. Zudem sind die Algorithmen öffentlich bekannt. Somit ist die Checksumme nur ein wirksames Mittel zur Erkennung von Veränderung durch Übertragungsfehler, jedoch nicht gegen absichtliche Manipulation. Ein weiteres Problem stellt Spoofing dar.

Abhilfen für diese Probleme entstehen durch einen bei der Übertragung unveränderten Integritätswert und der Authentikation des IP-Headers, wodurch die Identität des Absenders sichergestellt wird. Die wird in IPSec von dem in RFC 2402 spezifizierten Authentikation Header, kurz AH, gewährleistet. Er bietet Wahrung der Sicherheitsmerkmale Integrität und Authentizität und ist wie folgt aufgebaut:

Next header	Payload Len	RESERVED
Security Parameter Index(SPI)		
Sequence Number Field		
Authentication Data (variable)		

Abbildung 10: Authentication Header nach [RFC2402]

Durch Next header wird gewährleistet, dass der Authentication Header in Verbindung mit anderen IPSec-Protokoll verwendet werden kann. AH kann alleine, in Verbindung mit ESP und verschachtelt (nested fashion) benutzt werden.

Die SPI entstammt der Security Association. Durch die Sequenznummer wird eine Vorkehrung gegen Replay Attacken (Anti-Replay) getroffen.

Authentikation Data sichert die Authentizität der Quelle (Data origin Authentication) und auch die Integrität des Paketes (connectionless⁶ integrity). Dies wird durch die Generierung eines Integrity Check Value, kurz ICV, geleistet. Er kann entweder durch eine Digitale Signatur oder einen Message Authentication Code , kurz MAC, errechnet werden.

Bei der Digitalen Signatur wird eine Signatur mittels eines privaten Schlüssels erstellt, wodurch die Authentizität des Senders gewährleistet wird. Gleichzeitig wird hierbei auch die Integrität sichergestellt, denn passen Nachricht und entschlüsselte Signatur nicht zu einander, ist entweder die Unterschrift falsch, oder es kam bei der Übertragung zu einer Verfälschung der Nachricht, also zu einer Integritätsverletzung. Würde die Signatur durch Verschlüsselung der gesamten Nachricht erzeugt werden, wäre die Signatur zu groß. Daher wird nur ein Message Digest verschlüsselt und als Signatur versendet. Ein Message Digest ist ein Hashwert, der weder vorhergesagt noch invertiert werden kann.

Ein MAC ist eine eindeutige Prüfsumme, die der Sicherstellung von Integrität und Authentizität dient. Ziel ist es, die Prüfsumme nicht ohne Kenntnis eines Passwortes oder eines Schlüssels erstellen zu können. Eine Möglichkeit zur Errechnung des MAC ist die Erstellung eines Message Digest, der mit einem Schlüssel verknüpft wird. Hierzu kann der Schlüssel an die Eingabe angehängt werden und danach der Message Digest produziert werden. In diesem Fall

⁶ Man beachte, dass das Internet Protokoll verbindungslos ist.

wird der MAC als HMAC bezeichnet. Eine weitere Möglichkeit ist die Verwendung des letzten Blocks eines Block-orientierten symmetrischen Verschlüsselungsalgorithmus statt des Message Digest. Wird als Algorithmus DES-CBC verwendet, so heißt der Algorithmus CBC-MAC.

Durch den ICV werden die Daten der höheren OSI-Schichten, den AH Header selbst und über die Teile des IP-Headers, die sich bei der Übertragung nicht ändern⁷, authentifiziert. Zudem muss ein Auffüllen des Feldes auf ein ganzes Vielfaches von 32bit (IPv4) bzw. 64 Bit (IPv6) von der IPsec Implementation unterstützt werden.

Durch den ICV ergibt sich bei Anwendung des AH im Transportmodus ein Problem. Der ICV wird über alle unveränderlichen Teile des IP-Headers gebildet, wobei auch die Quelladresse - als unveränderlich angenommen wird. Falls Network Address Translation eingesetzt wird, stimmt die ICV beim Empfänger nicht mehr und jedes Packet wird verworfen. Wie oben bereits besprochen, fordert die Verdeckung der Netzstruktur die Verwendung des Tunnelmodus. Im Tunnelmodus wird eine Kopie des originalen IP-Headers erzeugt, die für den Vergleich mit dem ICV beim Empfänger verwendet wird. NAT wird dabei auf den neuen IP-Header angewendet, der nicht zur Berechnung des ICV verwendet wird. Die folgenden Abbildungen veranschaulichen die Veränderung eines IPv4-Paketes durch AH in den beiden Kommunikationsmodi.

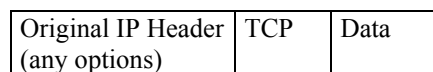


Abbildung 11: IPv4 Header vor der Anwendung des AH

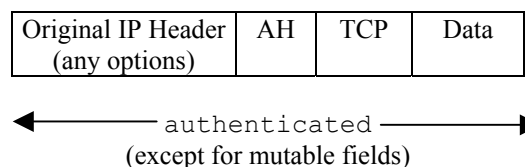


Abbildung 12: IPv4 Header nach der Anwendung des AH im Transport Modus

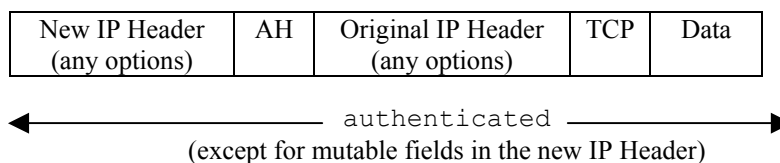


Abbildung 13: IPv4 Header nach der Anwendung des AH im Tunnel Modus

Fragmentation stellt für den ICV kein Problem dar, da er über das ganze Packet gebildet wird. Da es Umständen fragmentiert übertragen werden kann, wartet die IPsec-Anwendung auf der Empfängerseite auf alle Fragmente, bevor die ICV neu berechnet wird.

Der Authentikation Header verwendet jedoch keine Verschlüsselung, wodurch keine Wahrung der Vertraulichkeit der übertragenen Daten gewährleistet ist. Somit ist mit dem AH kei-

⁷ Diese Felder werden als immutable fields bezeichnet. Die mutable fields ToS, TTL, Fragmentoffset, Flags, Header checksums und Options werden mit 0 belegt.

ne VPN im hier definierten Sinne möglich. Um dennoch ein privates Netz erzeugen zu können, bietet sich das im folgenden Abschnitt besprochene ESP an.

4.3.7 Encapsulating Security Payload

Eine weiteres IPSec Protokoll ist das Encapsulating Security Payload Protokoll, kurz ESP. Durch Verschlüsselung bietet es die Wahrung der Vertraulichkeit, wobei zusätzlich Integrität und Authentizität gewahrt werden können. Somit kann mittels ESP eine VPN im hier definierten Sinne erzeugt werden. Zur Verschlüsselung können aus Performancegründen nur symmetrische Verschlüsselungsalgorithmen wie DES, 3DES oder AES verwendet werden. Der ESP Header ist in [RFC2406] spezifiziert und wird in folgender Abbildung dargestellt:

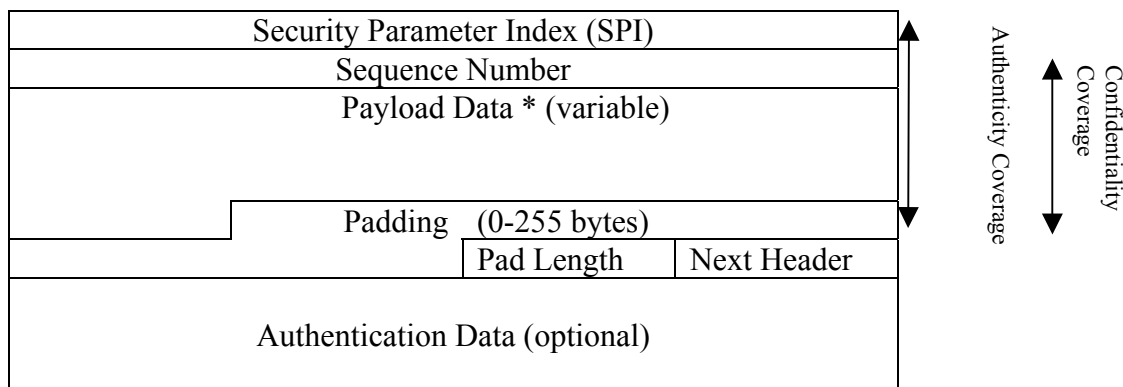


Abbildung 14: ESP Header nach [RFC2406]

SPI und Sequence number und Next Header sind äquivalent zum Authentication Header. Der Unterschied bei ESP ist die Nutzlast, die zwischen den Feldern steht. Somit werden die Felder ab Padding zum ESP Trailer, wobei das Feld Authentication Data nicht dazugehört, weil es eine Checksumme enthält, die nur bis zum ESP Trailer berechnet wird.

Die Wahrung der Sicherheitsmerkmale Integrität und Authentizität ist in ESP optional, jedoch nicht Pflicht. Die Wahrung wird durch das Feld Authentication Data geleistet. Hierbei wird ein ICV berechnet. Im Transport-Modus wird er bei ESP lediglich über die IP-Nutzlast gebildet. Somit bietet ESP im Transportmodus eine schwächere Authentikation als AH. Im Tunnelmodus ist die Authentikation bei ESP durch die Kopie des originalen IP Header äquivalent zu der in AH. Dabei bietet ESP wie der Authentication Header Data origin authentication, Connectionless integrity und Anti-Replay Merkmale.

Zusätzlich gewährleistet es in jedem Fall durch Verschlüsselung der Nutzlast die Vertraulichkeit der Daten (Data confidentiality) sowie eingeschränkt die Vertraulichkeit des Verkehrsflusses (limited traffic flow confidentiality).

Ebenso wie beim Authentication Header, arbeitet der Transportmodus von ESP nicht mit NAT zusammen. Dies hängt hierbei aber nicht mit dem ICV zusammen, da dieser bei ESP nicht den IP-Header einbezieht. Grund ist bei ESP die Verschlüsselung. So wird die TCP Checksumme nicht nur über den TCP Header gebildet, sondern auch über Quell- und Zielad-

resse⁸. Daher muss bei Anwendung von NAT auch die TCP Checksum neu berechnet werden, die bei ESP aber verschlüsselt ist.

Im Tunnelmodus entsteht durch die Kopie des IP Headers dieses Problem im Allgemeinen nicht, jedoch ergibt sich bei 1-to-n NAT das Problem, wenn Quellports verändert werden. Sie liegen im verschlüsselten Teil des ESP-Paketes und lassen sich somit nicht ändern.

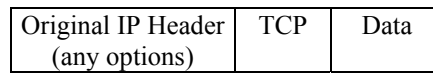


Abbildung 15: IPv4 Header vor der Anwendung des ESP

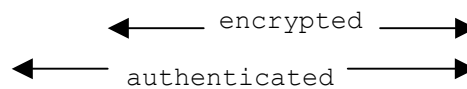
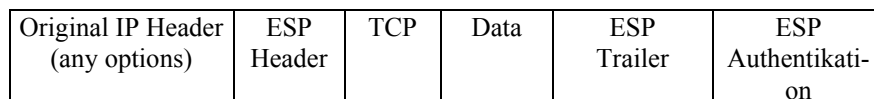


Abbildung 16: IPv4 Header vor der Anwendung des ESP im Transport Modus

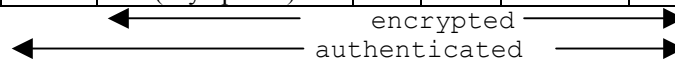
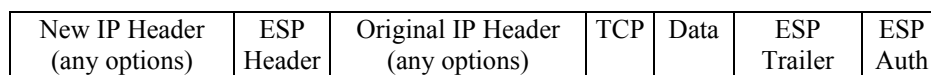


Abbildung 17: IPv4 Header vor der Anwendung des ESP im Tunnel Modus

4.3.8 Verschachtelungen von IPSec Protokollen

Durch den Next Header können ESP und AH auch verschachtelt werden. Eine solche Kombination wird auch als „nested fashion“ bezeichnet. Dabei können auch unsinnige Kombinationen entstehen.

Als sinnvoll und Pflicht für die Implementierung im Transportmodus wird in [RFC2401] die Kombination von ESP innen und AH außen, damit die stärkere Authentikation des AH zum tragen kommt. Sie ist als Pflicht für eine Implementation vorgeschrieben. Allerdings widerspricht dies dem Horton-Prinzip (vgl. [counterpane]), wonach die Semantik der Nachricht und nicht die Syntax zur Authentikation herangezogen werden soll. Weitere Kombinationen können optional unterstützt werden, jedoch sind diese vor allem Tunnelmodus nicht sinnvoll, da die von AH angebotenen Leistungen eine Teilmenge der ESP Leistungen sind.

Bei Kombination beider Protokolle werden genauer betrachtet nicht die Protokolle, sondern die Security Associations geschachtelt. Da eine SA jeweils nur für ein Protokoll existieren kann, müssen hierfür zwei geschachtelte SAs geschaffen werden.

⁸ Dieser Umstand wird z. B. in [RFC793] im Rahmen des Pseudoheaders besprochen.

Die Verschachtelung von Security Associations kommt nicht immer auf der gesamten Verbindung vor, sondern meist nur auf Teilstücken. In der Realität macht eine Verbindung von AH und ESP dann Sinn, wenn ein sicherer Kommunikationskanal von einem ausserhalb des Intranets stehenden Rechner zu einem Rechner im Intranet aufgebaut werden soll. Hierbei kann am Kopplungspunkt zwischen Intra- und Internet der AH-Kanal enden. Kann sich ein Rechner hier nicht authentifizieren, so bleibt das Intranet von zusätzlicher Last durch nicht zugelassene Pakete verschont.

Wichtiger ist aber die Betrachtung, wie die Parameter einer Verbindung in den Geräten eingestellt werden können.

4.3.9 SA Negotiation (IKE)

In einer etablierten IPsec Verbindung sind Verschlüsselungsverfahren, Authentifizierungsmethode sowie die zugehörigen Schlüssel als Parameter für beide Richtungen eingestellt. Beide Partner müssen dabei über dieselben Parameter verfügen. Das bedeutet, dass in jedem IPsec-Gerät vier Schlüssel hinterlegt werden müssen.

Bei der manuellen Einstellung aller Schlüssel wäre ein hoher administrativer Aufwand nötig. So müssten alle Geräte von einem Administrator zugänglich sein. Zudem müssen die Schlüssel als Vorkehrung gegen eine Enthüllung regelmäßig ausgetauscht werden, was schnell vergessen wird.

Eine Alternative ist die automatische Aushandlung von Schlüsseln. Ein solcher Key-Exchange ist durch viele Protokolle möglich, wobei der Urvater aller Protokolle der Diffie-Hellman Key Exchange ist.

Bei einem solchen Schlüsselaustausch zum Aufbau einer IPsec Verbindung sind mehrere Dinge zu beachten. Würden die Schlüssel im Klartext übertragen werden, könnten Dritte die Schlüssel sniffen und so eine Verbindung aufbauen. Zudem muss die Authentizität beider Kommunikationspartner sichergestellt sein. Somit wird der aus dem Diffie-Hellman-Protokoll bekannten⁹ Gefahr eines Man-in-the-Middle Angriffs, bei der ein Angreifer zwischen beiden Kommunikationspartnern vermittelt, vorgebeugt. Zudem soll durch den Schlüsselaustausch auch gewährleistet werden, dass die Schlüssel nicht manuell ausgetauscht werden müssen. Deshalb werden für jede IPsec-Verbindung auf Grund zufälliger Informationen neue Schlüssel erzeugt.

Daher muss vom Key-Exchange Protokoll zunächst ein sicherer Kanal erzeugt werden, der Authentizität und Vertraulichkeit der über ihn übertragenen Daten wahrt. Über ihn werden dann Informationen zur Generierung neuer Schlüssel übertragen.

IPsec bietet dafür mit dem Internet Key Exchange, kurz IKE, ein eigenes Protokoll an, welches die oben genannten Anforderungen erfüllt.

Internet Key Exchange

⁹ Vgl. [Davis], Abschnitt 3.4

Das Internet Key Exchange ist als hybrides Anwendungsschichtprotokoll in RFC2409 definiert. Ziel des IKE ist die automatische gesicherte Aushandlung einer Security Association für eine IPSec Verbindung, die Verschlüsselungsalgorithmus und Authentikationsmethode enthält. Es basiert auf ISAKMP, Oakley Key Determination Protocol und SKEME.

ISAKMP ist in RFC2408 spezifiziert und steht für Internet Security Association and Key Management Protocol. ISAKMP definiert keinen Schlüsselaustausch. Das Protokoll bietet ein Rahmenwerk für Authentikation und Schlüsselaustausch, das von anderen Schlüsselaustauschprotokollen genutzt werden kann.

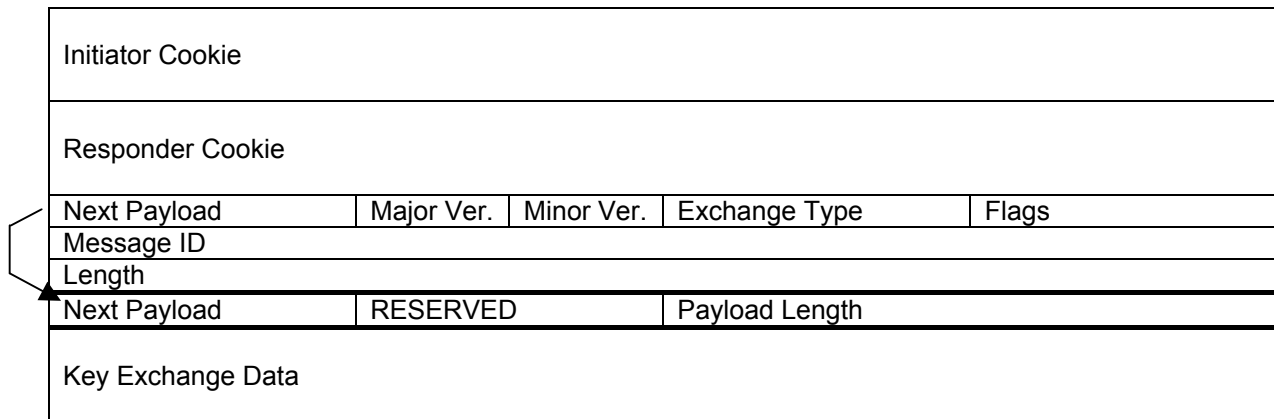
Die hier besprochenen Details basieren auf ISAKMP. So ist der IKE über Port 500/UDP nutzbar, was bereits in ISAKMP definiert ist. Zur Zeit ist IKE die einzige Implementation von ISAKMP. In IKE wird die Aushandlung in Anlehnung an ISAKMP in zwei Phasen unterteilt. Die erste Phase dient dem Aufbau eines sicheren Kommunikationskanals, über den in der zweiten Phase die Details der IPSec Verbindung ausgehandelt werden.

Phase 1

Aushandlung einer ISAKMP SA für einen sicheren Kanal durch wechselseitiges Versenden von ISAKMP Paketen mit SA Payload

Zum Aufbau des gesicherten Kommunikationskanals wird eine ISAKMP SA aufgebaut. Sie dient nur der Festlegung, wie weiterer Verkehr gesichert wird, und ist daher nicht mit einer IPSec SA zu verwechseln. Zwischen zwei Kommunikationspartnern können mehrere ISAKMP SAs ausgehandelt werden. Jede ausgehandelte ISAKMP SA ist multidirektional.

Bei einer ISAKMP SA handelt es sich um ein in ISAKMP definiertes Paketformat. Ein Paket kann dabei je nach Anforderungen aus 12 verschiedenen Payloads zusammengesetzt werden, die z. B. ISAKMP-Security Associations, Informationen über den Schlüsselaustausch, Authentikations-Informationen, Signaturen oder Zertifikate enthalten können. Die Pakete werden wie eine verkettete Liste aus den Payloads zusammengesetzt, wobei jedes Packet mit einem ISAKMP Header beginnt. Die folgende Abbildung stellt ein Packet bestehend aus ISAKMP Header und Key Exchange Payload dar.



...

Abbildung 18: Packet bestehend aus ISAKMP Header und Key Exchange Payload

Mittels der Cookies soll nach [RFC2408, Abschnitt 1.7] Denial of Service Attacken entgegengewirkt werden. Diesem Argument wird aber Kritik entgegen gestellt. Für nähere Informationen zur Kritik wird auf den Abschnitt „Schwachstellen von IPSec“ verwiesen.

Das Feld “Key Exchange Data” enthält nach [Davis] “the data required to generate a session key.” Dies können Zufallszahlen oder Diffie-Hellmannwerte sein.

IKE fordert eine starke Authentikation der Kommunikationspartner. Eine starke Authentikation lässt sich mittels eines vorab ausgetauschten Schlüssels, mittels public key-Verfahren oder Digitalen Signaturen erreichen. Bei pre-shared keys wird ein HMAC⁹ aus einer Zufallsinformation und dem vorab ausgetauschten Schlüssel erzeugt.

Beim Public Key Verfahren wird die zufällige Information verschlüsselt übertragen, so dass nur der Empfänger die Zufallsinformation richtig hashen und zurücksenden kann. Bei der Verwendung einer Digitalen Signatur wird ein Zufallswert digital signiert und zurückgeschickt. Damit die Signatur auch zur Authentikation verwendet werden kann, wird ein Digitales Zertifikat angefordert.

Zudem soll die Übertragung von Daten auf dem Kommunikationskanal verschlüsselt geschehen. Dazu werden Verschlüsselungsinformationen wie Zufallszahlen (Nonce) oder Diffie-Hellman-Werte übertragen.¹⁰ Am Ende der Phase 1 haben beide Seiten einen symmetrischen Schlüssel, der zur Verschlüsselung der über den Kommunikationskanal versendeten Daten verwendet werden.

IKE kann in der Phase 1 in Main Mode als auch im Aggressive Mode ausgeführt werden. Der Aggressive Mode tauscht im Gegensatz zum Main Mode drei statt sechs Nachrichten aus. Dies geht aber zu Lasten der Authentizität. Main-Mode und Aggressive Mode sollen in den folgenden Beispielen verdeutlicht werden.

¹⁰ Dies sind die gleichen Daten wie die der Key-Exchange Payload; siehe Erläuterung des ISAKMP-Headers auf Seite 26

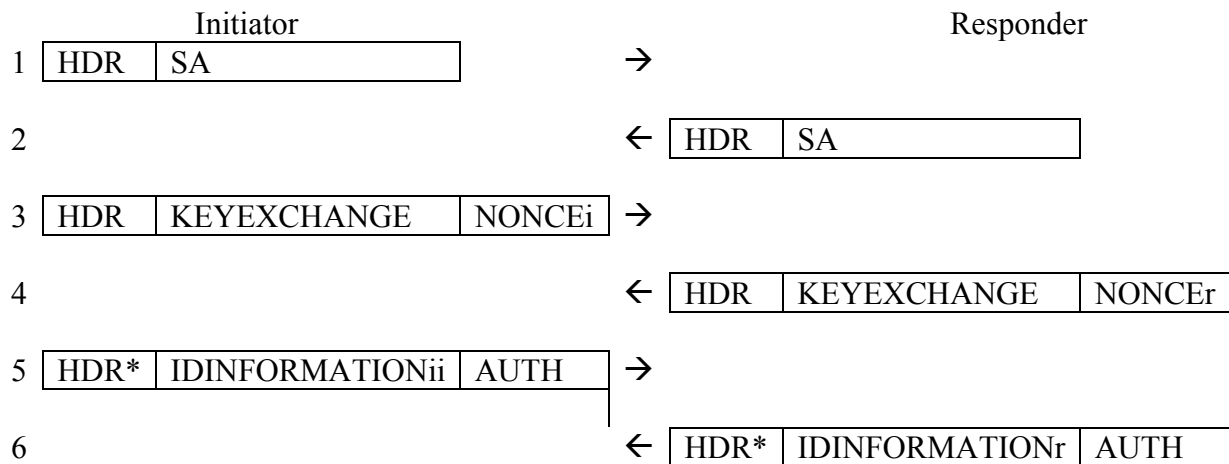


Abbildung 19: IKE Phase 1 im Main Mode mit pre-shared keys nach [Davis], das Symbol * bedeutet Verschlüsselung

Die eben betrachtete Abbildung stellt eine IKE Aushandlung in Phase I nach Main-Mode dar. Hierbei senden sich beide Seiten durch die ersten beiden Nachrichten gegenseitig Informationen über unterstützte Verschlüsselungs- und Authentikationsmethoden. Die Nachrichten bestehen aus ISAKMP-Packeten, deren Header hier mit HDR gekennzeichnet sind. Dabei handelt es sich bei Feld SA um eine SA-Payload, die wiederum ein oder mehrere PROPOSAL-Payloads enthält. Die PROPOSAL-Payloads sind Vorschläge, die wiederum eine TRANSFORM-Payload enthalten. Die TRANSFORM-Payload beinhaltet Informationen über die von einem Kommunikationspartner unterstützten Authentikations- bzw. Verschlüsselungsmethoden.

Mit den nächsten beiden Nachrichten (3 und 4) werden mittels der KEYEXCHANGE-Payload⁸ Informationen zur Generierung der Schlüssel ausgetauscht. Die Nonce ist ein Zufallswert, der zur Sicherstellung der Authentikation als auch zum Schutz gegen Replay Attacken verwendet wird. Zudem kann es als zufälliges Element für die Generierung der Schlüssel gelten. Für die Generierung der Schlüssel wird eine pseudo random function, kurz prf, benutzt. Diese Funktion selbst soll optional auch ausgehandelt werden können, dies ist aber nach [RFC2409] zur Zeit noch nicht möglich.

Vor Sendung der fünften Nachricht verfügen die beiden Kommunikationspartner bereits über einen gemeinsamen Schlüssel. Daher werden sowohl Nachricht 5 und 6 verschlüsselt übertragen, was durch HDR* gekennzeichnet ist. Hierbei wird eine ID-Payload übertragen, welche die IP-Adresse des Kommunikationspartners enthält. Diese Nachricht enthält durch die AUTH-Payload auch einen Authentizitätsnachweis, der durch Bildung eines HMACs¹¹ aus der vorher übertragenen NONCE-Payload sowie des pre-shared keys gebildet wird.

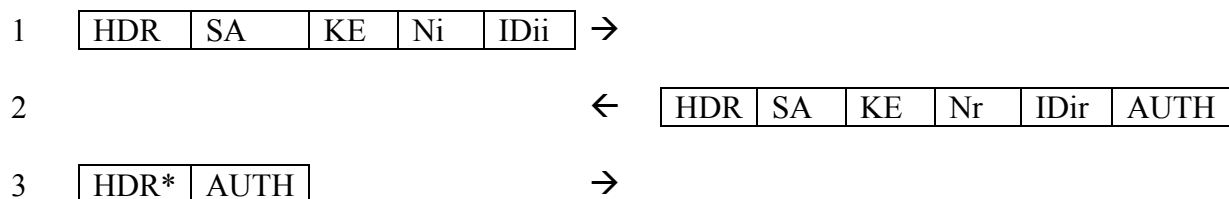


Abbildung 20: IKE Phase 1 im Aggressive Mode mit pre-shared keys nach [Davis]

¹¹ vgl. Seite 21

Im Aggressive Mode werden so viele Payload wie möglich mit einer Nachricht verschickt. Dabei entsteht aber das Problem, dass wegen fehlender Verschlüsselung die IP-Adresse in der ID Payload beider Partner nicht gewährleistet wird.

Nachdem nun ein gesicherter Übertragungskanal besteht, können in der zweiten Phase die Parameter einer IPsec SA ausgehandelt werden.

IKE Phase 2

In der Phase 2 des IKE sollen IPSEC SA sowie die Authentifizierungsmethoden, Hashwertbildung und Verschlüsselungsmethoden ausgehandelt werden.

Diese Phase stellt mit dem Quick Mode nur ein Modus zur Verfügung, von dem es aber zwei Varianten gibt. In einem Base-Quick Mode werden die in Phase 1 ausgehandelten Schlüsselinformationen verwendet, um die Schlüssel für die IPsec Verbindung zu generieren. Dabei wird das Prinzip der Perfect Forwarded Secrecy, kurz PFS, nicht gewahrt. Dieses Prinzip besagt, dass die Kompromittierung eines Schlüssels nicht die Kompromittierung der weiteren Schlüssel begünstigt. Ist PFS gefordert, so werden im PFS-Quick Mode neue Key Exchange Informationen⁸ versandt.

Die Aushandlung der IPsec SA erfolgt durch wechselseitiges Versenden von ISAKMP Paketen über den in Phase 1 aufgebauten sicheren Kommunikationskanal. Dabei sind die Pakete mit den in Phase 1 ausgehandelten Parametern verschlüsselt. Diese ISAKMP Pakete enthalten Hashwerte, mit denen die Authentizität der Kommunikationspartner weiterhin zu wahren ist. Dadurch soll auch gewährleistet werden, dass es sich bei den Kommunikationspartnern immer noch um die an der Phase 1 Beteiligten handelt. Der Hash wird dabei über Schlüsselinformationen und der Nachricht gebildet, weshalb es sich genauer um einen HMAC handelt. Er wird unter Zuhilfenahme der prf berechnet, die zurzeit nur einen HMAC erstellt.

In Abb. 18 ist der Quick Mode dargestellt. Die ersten beiden Nachrichten enthalten nach dem Hash, der zwingend als erste Payload gefordert ist, folgende Payloads :

- Security Association Payloads, wobei hier ein oder mehrere SA-Payloads versendet werden können.
- Nonces für Anti-Replay und Schlüsselinformationen
- bei geforderter PFS sind Key Exchange Informationen (KE) enthalten
- optional ID Informationen, die IP-Adressen der Clients sind

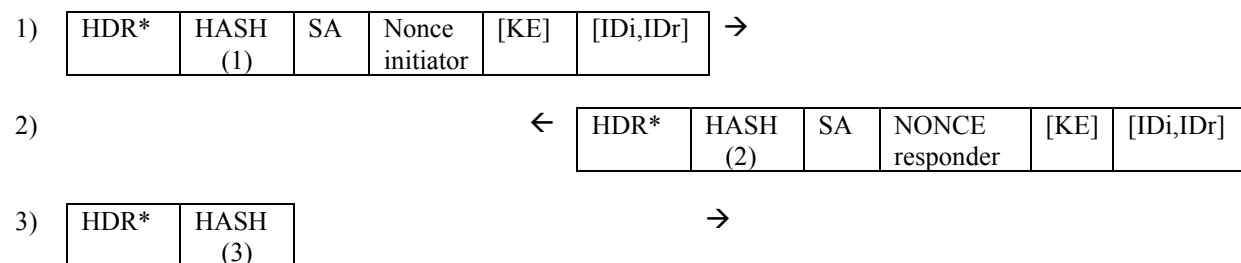


Abbildung 21: IKE Phase 2 nach [RFC2409]

Unterstützung für dynamische Adressierung

In der heutigen Zeit entsteht immer mehr der Bedarf, remote in einem Netzwerk zu arbeiten. Ein Beispiel ist ein Mitarbeiter, der auf einer Reise mit seinem Notebook in einem Firmennetz arbeiten möchte. Bei der Einwahl ins Internet bekommt er meist die IP-Adresse von dem jeweiligen ISP dynamisch zugewiesen.

Durch die dynamische Adresse gibt es bei Verwendung von IPSec folgende zwei Probleme:

- Der Remotepartner enthält eine IP-Adresse, die nicht zum internen Firmennetz gehört
- Die Security Policy Database lässt keine Verbindungen zu dynamisch vergebenen Adressen zu.

Diesen Problemen kann aber mittels IKE durch eine Lösung namens mode-config begegnet werden. Hierbei erhält der Remote-Partner eine virtuelle IP-Adresse am VPN Gateway. Diese virtuelle IP-Adresse gehört zu dem privaten Netzbereich und wird von dem Gateway mit der dynamische IP-Adresse verknüpft.

Die Zuordnung erfolgt durch die ISAKMP Attribute-Payload während der Schlüsselaushandlung, so dass die Authentikation über die in IKE definierten Verfahren erfolgt. Im Tunnelmodus kann hierbei in einer speziellen Variante des Mode-configs auch das DHCP-Protocol zur Adressvergabe verwendet werden.

4.3.10 Schwächen von IPSec

IPSec gilt als sicherer als alle anderen Verfahren zum Aufbau einer sicheren Verbindung. Dennoch gibt es Schwächen, die vor allem auf konzeptioneller Ebene liegen. Der kryptoExperte Bruce Schneier hat zusammen mit Niels Ferguson eine 28 seitige Kritik (siehe [counterpane]) an IPSec erstellt. Hier soll eine Auswahl von Kritikpunkten an IPSec aufgeführt werden.

Komplexität

Die Komplexität des IPSec-Protokolls beruht auf der Behandlung komplizierter Details wie Fragmentation oder der riesigen Auswahl von Optionen. Bekanntlich ist Komplexität der Feind der Sicherheit. So lassen sich komplexe Systeme selten richtig implementieren oder überprüfen. Dies trifft nach [Counterpane] auch auf IPsec zu.

Eine Reduktion der Komplexität kann nach [counterpane] durch die Elimination von AH und des Transportmodus erreicht werden. Der einzige Vorteil des Transport Modus ist die geringere Paketgröße und somit die Ersparnis an Bandbreite. Dieser Vorteil könnte aber durch die Anwendung von Kompressionsmechanismen wie IP-Compression wettgemacht werden. Zudem enthält auch ESP Authentikation. Passt man diese dem Niveau des AHs an und macht nur die Verschlüsselung optional, so hat man mit nur einem Protokoll und Kommunikationsmodus alle Elemente abgedeckt und die Komplexität verringert.

Die Cookies in ISAKMP bewirken nach [counterpane] keinen Schutz gegen Denail Of Service. Sie erhöhen lediglich die Komplexität des Protokolls. Auch Gegenmaßnahmen wie die

Vorkehrungen gegen Anti-Replay Attacken tragen zur Komplexitätserhöhung bei, funktionieren aber nicht richtig.

Schlechte Dokumentation

Die Dokumentation sei nach [counterpane] unübersichtlich und schwer verständlich. Ein besonderes Extrem hierbei ist ISAKMP. Grund hierfür sind häufige Wiederholungen sowie fehlende Zielsetzungen und Begründungen.

So sei auch die Definition der Authentikationsmechanismen schwach. Die Authentikation in ISAKMP basierenden Protokollen soll durch Hash-funktionen geschehen, wobei als Hash-funktionen sowohl HMACs als auch „Native Hashes“ unterstützt werden sollen. Ein Native Hash wäre ein reiner MD5, der aber von jedem erzeugt werden kann, und so für eine Authentikation nicht geeignet ist. So kann die Authentikation geschwächt werden. Daher sollte zur Authentikation die Benutzung eines HMAC vorgeschrieben werden.

Krypthographie

Die Sicherheit von IPSec ist auch Abhängig von der Stärke der kryptographischen Verfahren, mit denen eine Verbindung realisiert wird. So kann eine IPSec-Verbindung durch die Verwendung eines schwachen Verschlüsselungsalgorithmus, eines zu kurzen Schlüssels oder durch Kollision des Hash-Verfahrens geschwächt werden. Über die Schwächen der einzelnen Verschlüsselungsalgorithmen wird auf den Vortrag 4 verwiesen.

Allerdings kann einer Verbindung die Verwendung bestimmter Algorithmen zwingend vorgeschrieben werden, wodurch die Benutzung vermeintlich schwacher Algorithmen unterbunden werden kann.

Fehlerhafte Implementationen

Auch die durch Implementationsfehler entstehenden typischen Gefahren müssen bei IPSec betrachtet werden. So ist ein aus ISAKMP basierender Schlüsselaustausch als ein Dienst implementiert, der über Port 500/UDP ansprechbar ist. In manchen Implementationen des Dienstes hat es bereits Schwächen gegeben, die zu Denial of Service Angriffen geführt haben. Fehler in der Implementation werden in IPSec durch seine Komplexität begünstigt.

4.4 Layer-4 Techniken - SSL / TLS

4.4.1 Einführung

Die Secure Socket Layer Protokolle (SSL) und deren Nachfolger Transport Layer Security (TLS) dürften wohl die meist genutzte VPN-Technologie des Internet darstellen. Als VPN-des-kleinen-Mannes bezeichnet, wird es zumeist zur kryptographischen Absicherung der zwischen Web-Browser und Web-Server bestehenden HTTP-Verbindung eingesetzt.

SSL wurde 1994 von der Netscape Communication Corporation entwickelt, um die Transportschicht abzusichern, die bis dahin Daten nur im Klartext über das Netz schickte. Durch den Einsatz von SSL soll ein Belauschen und Verfälschen von Informationen unterbunden, und außerdem sichergestellt werden, dass nur autorisierte Kommunikationspartner miteinander Daten austauschen. Mit SSL ist eine verbindungsorientierte Ende-zu-Ende Kommunikationssicherheit möglich.

4.4.2 Architektur

Die Protokolle der SSL-Architektur ordnet sich als oberste Protokolle der Transportschicht in das TCP/IP-Schichtenmodell ein, um so die Daten der Anwendungsschicht sicher weiterzureichen.



Abbildung 22: Einordnung von SSL in das TCP/IP-Modell

Die SSL-Architektur besteht aus vier Protokollen, das unterste davon ist das SSL Record Protocol, das die beiden für eine SSL-Verbindung wichtigen Eigenschaften Vertraulichkeit und Integrität zur Verfügung stellt. Darüber angeordnet sind das SSL Handshake Protocol, das SSL Cipher Spec Protocol und das SSL Alert Protocol, die für das Management eines SSL-Austauschs verantwortlich sind.

4.4.3 Verbindungsaufbau

Zum Aufbau einer Verbindung werden mithilfe des SSL-Handshake-Protokolls eine Reihe von Nachrichten zwischen Client und Server ausgetauscht, die sich in vier Phasen aufteilen lassen.

1. Aufbauphase

In dieser Phase sendet der die Verbindung initiiierende Client eine „client_hello“-Nachricht an den Server. Die wesentlichen Bestandteile dieser Nachricht sind zum einen die höchste Versionsnummer die der Client unterstützt, sowie im Parameter Cipher Suite eine Liste von kryptographische Methoden, die dieser unterstützt. Jede der Methoden enthält dabei ein eigenes Schlüssel-Austausch-Verfahren und eine kryp-

tographische Spezifikation. Beim Schlüssel-Austausch-Verfahren handelt es sich um eine Austauschmethode und ein Integritätsverfahren (MAC).

Für den Austausch zulässige Verfahren sind RSA, Ephemeral Diffie-Hellman, Fixed Diffie-Hellman, Anonymous Diffie-Hellman und Frotezza. Dabei sollten die ersten beiden Verfahren bevorzugt dann eingesetzt werden, wenn Vertraulichkeit und Integrität im Vordergrund stehen. (RSA und Ephemeral Diffie-Hellman setzen eine PKI voraus.)

Mit dem einfachsten der SSL-Protokolle, dem Change-Cipher-Spec-Protokoll, wird dem Kommunikationspartner die Art der Verschlüsselung (Byte oder Stream), der MAC-Algorithmus (MD5 oder SHA-1) die Hash-Größe, die Größe der Initialisierungsvektoren, bei Verwendung des CBC-Modus, ein IsExportable-Flag, sowie eine Byte-Sequenz (Key-Material), die zur Erzeugung der Write Keys verwendet werden kann, mitgeteilt.

Die Aufbauphase wird mit der „server_hello“-Message abgeschlossen, die ähnlich der „client_hello“-Nachricht aufgebaut ist.

2. Server-Identifizierung-Phase

Der Server sendet anschließend eine Zertifikatsnachricht, sofern dies das Austauschverfahren verlangt, an den Client. Die Nachricht enthält ein oder mehrere x.509v3-Zertifikate. Eine Zertifikatsnachricht ist z.B. nicht beim Anonymous-Diffie-Hellman-Verfahren erforderlich.

Als nächstes wird eine „server_key_exchange“-Nachricht versandt, die den Public-Key der Servers enthält. Für das Fixed-Diffie-Hellman-Verfahren ist diese Nachricht nicht erforderlich.

Optional kann jetzt eine „certificate_request“-Nachricht geschickt werden, die dem Client auffordert, sein Zertifikat an den Server zu schicken.

Die Phase wird mit der „server_done“-Nachricht abgeschlossen, womit der Server auf eine Antwort vom Client wartet.

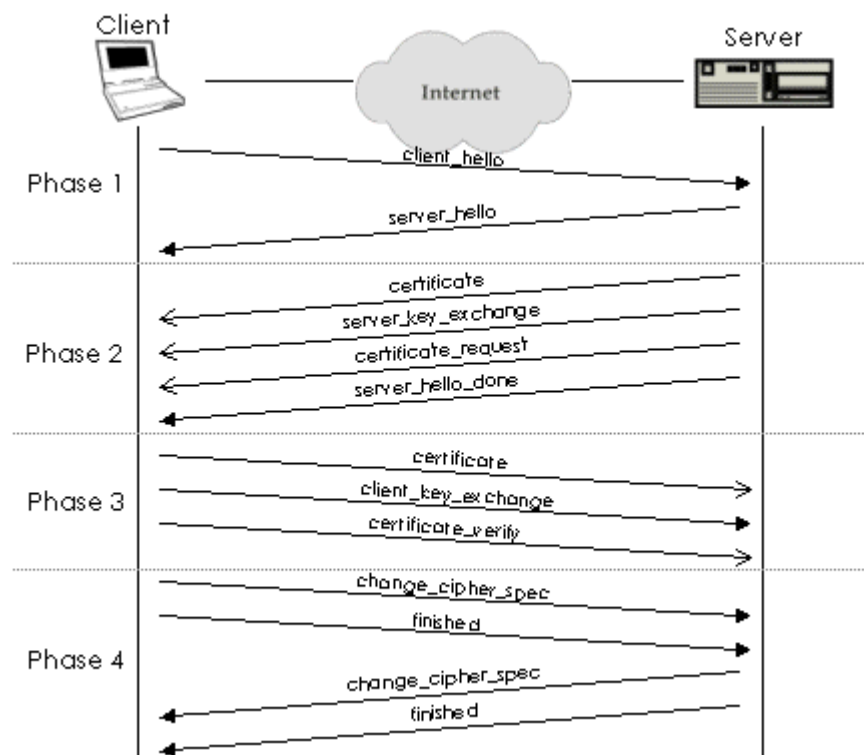


Abbildung 23: Nachrichten Austausch für einen SSL/TLS-Verbindungsaufbau.
 „→“ kennzeichnet je nach Verfahren optionale Nachrichten

3. Client-Identifizierungs-Phase

Mit Erhalt der „server_done“-Nachricht verifiziert der Client die Zertifikate und überprüft die Parameter der „server_hello“-Nachricht. Falls der Server ein Zertifikat angefordert hat, sendet der Client eine Zertifikats-Nachricht zurück, besitzt dieser kein geeignetes, so sendet er eine „no_certificate_alert“-Meldung zurück.

Anschließend sendet der Client eine „client_key_exchange“-Nachricht, die je nach Austauschverfahren, bei RSA z.B. einen 48-Byte großen Zwischenschlüssel, bei Diffie-Hellman z.B. die Diffie-Hellman Parameter, enthält.

Anschließend kann optional eine „certificate_verify“-Nachricht zur genauen Überprüfung des Client Zertifikates zurückgeschickt werden.

4. Abschluss-Phase

Um zur eigentlichen Datenübertragung zu kommen, senden Client und Server mit Hilfe des Change-Cipher-Spec-Protokolls die „change_cipher_spec“-Nachricht an den Server und kopiert kryptographische Spezifikationen in die vereinbarte CipherSpec. Nachdem beide Partner auf den selben Informationsstand sind, senden sie eine „finished“-Nachricht, die die aktuellen Algorithmen, Schlüssel und Geheimnisse enthält.

4.4.4 Änderungen in TLS gegenüber SSL

TSLv1.0 ist als Erweiterung von SSLv3.0 zu sehen und ist auch als SSLv3.1 im Protokoll-Header identifizierbar. TSL ist die erste Version, die RFC-Status (RFC-2246) bei der IETF erreicht hat, während SSLv3.0 nur als Draft eingereicht wurde und seine Gültigkeit bereits 1997 verloren hat.

Die wesentlichen Neuerungen in TLS sind das MAC-Verfahren und die Hash-Wertbildung. TLS benutzt den HMAC-Algorithmus strikt nach RFC-2104, inklusive der Paddingbildung. SSL benutzt zwar auch RFC-2104, jedoch wird das Padding nur an den Schlüssel angehängt und nicht wie bei TLS mit XOR verknüpft. Mit TLS kann dadurch ein vielfaches an zu übertragenden Daten eingespart werden, und außerdem die Kryptoanalyse erschwert werden.

Weiterhin unterscheiden sich SSL und TLS in einigen Punkten des Alert-Codes und in den unterstützten Certificate Types des Client, so bietet TLS hier weder Ephemeral Diffie-Hellman noch Fortezza an.

4.4.5 Vorgehensweise von SSL/TLS

Für Protokolle höherer Schichten ist die Verwendung von SSL/TLS transparent. Jedoch müssen Modifikationen im Quellcode vorgenommen werden, um die SSL/TLS-API anzuwenden, so dass der Anwendungsschicht Funktionen zur sicheren Nutzung der Transportschicht zur Verfügung gestellt werden.

Dabei werden Daten der Anwendungsschicht vom SSL-Record-Protokoll entgegengenommen, fragmentiert, komprimiert, der MAC hinzugefügt, verschlüsselt und letztlich der SSL-Header vorangestellt. Die SSL/TLS-API kann auch zum Schutz anderer Implementationen z.B. Telnet, NNTP oder FTP eingesetzt werden.

4.4.6 Sicherheit von SSL

Ein Eindringen in eine SSL-Verbindung ist aufgrund des Aufbaus relativ einfach, jedoch ist der Rechenaufwand sehr hoch. Je nach verwendeten Verfahren kann der Sicherheitsgrad einer SSL-Verbindung und der benötigte Rechneraufwand in sie einzudringen schwanken.

Allgemein kann gesagt werden, dass SSL Schutz gegen Bruce-Force-, Known-Plaintext-, Replay-, Man-in-the-Middle-, Sniffing-, IP-Spoofing und IP-Hijacking- (ab v3.0) Angriffe bieten kann.

5 Typische VPN-Szenarien

5.1 Intranet-VPN

Zielsetzung

Bei einem Intranet-VPN werden die Zweigstellen eines Unternehmens miteinander verbunden. In der Regel werden Filialen mit einer zentralen Geschäftsstelle eines Unternehmens verbunden. Die Zielsetzung ist es, in den Filialen die gleichen Geschäftsprozesse zu ermöglichen, wie sie in der zentralen Geschäftsstelle möglich sind, und dementsprechend die dafür benötigten Informations- und Kommunikationsgrundlagen zu schaffen.

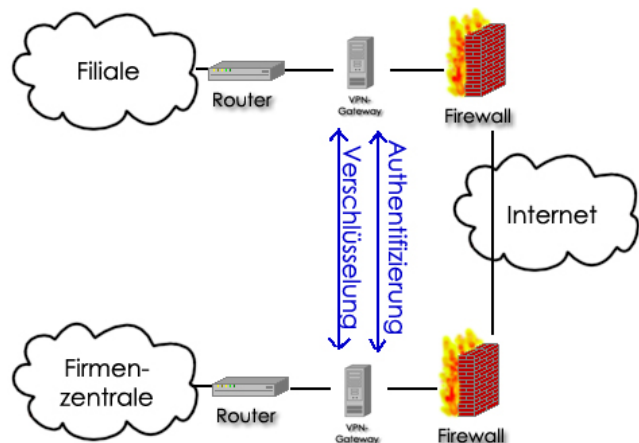
Anforderungen an die Implementation

Um ein Intranet-VPN zu realisieren, werden z.B. über das Internet permanente Verbindungen zwischen den Zweigstellen und der Zentrale eingerichtet. Dafür ist an beiden Enden der Kommunikationsverbindung jeweils ein VPN-Gateway/Firewall-System notwendig, zwischen denen eine gesicherte Verbindung aufgebaut wird. Weitere Sicherheitsvorkehrungen, die über die im Unternehmen üblichen Sicherheitsvorkehrungen für Netzwerke hinausgehen, sind in der Regel nicht nötig, da in den Zweigstellen ja alle Geschäftsprozesse in gleicher Weise zur Verfügung stehen sollen, wie dies in der Zentrale der Fall ist. Die Übertragung vom VPN-Gateway zu einem Client im lokalen Netz ist unverschlüsselt. In erster Linie gilt es dafür zu sorgen, dass der Übertragungsweg über das Internet für unbefugte dritte nicht zugänglich ist. Man spricht deswegen auch von einem Site-To-Site-VPN, weil die gesicherte Verbindung zwischen zwei Sites aufgebaut wird.

Technische Implementationsmöglichkeiten

Möglichkeit 1: Auf den VPN-Gateways wird jeweils eine IPSEC-Lösung mit ESP installiert. ESP enthält dabei die notwendigen Verschlüsselungs- und Authentifizierungsmaßnahmen

Möglichkeit 2: Installation einer IPSEC-Lösung auf Basis von L2TP. Der Vorteil dieser Lösung ist, dass die Nutzerauthentifizierung bereits beim Verbindungsaufbau erfolgt.



5.2 Extranet-VPN

Zielsetzung

Unternehmen, die ein Extranet aufbauen, haben die Zielsetzung, Zulieferunternehmen, Geschäftspartner und evtl. Kunden in die eigenen Geschäftsprozesse zu integrieren und damit letztlich die Effizienz der Abwicklung betriebswirtschaftlicher Zielsetzungen zu steigern.

Beispiele betriebswirtschaftlicher Zielsetzungen, die sich durch eine Verbesserung der Informations- und Kommunikationsinfrastruktur erreichen lassen, sind unter anderem:

- Eine Optimierung der betriebsinternen Geschäftsprozesse durch Integration von Zulieferern, Kunden und Partnerunternehmen in die eigenen Geschäftsprozesse,
- Eine Optimierung der Wertschöpfungskette eines Produkt-Herstellungsprozesses. (Stichwort: Supply-Chain-Management),
- Eine bessere Erreichbarkeit des Unternehmens (auch unternehmensintern),
- Eine Verbesserung des Kundenservices,
- usw.

Anforderungen an die Implementation

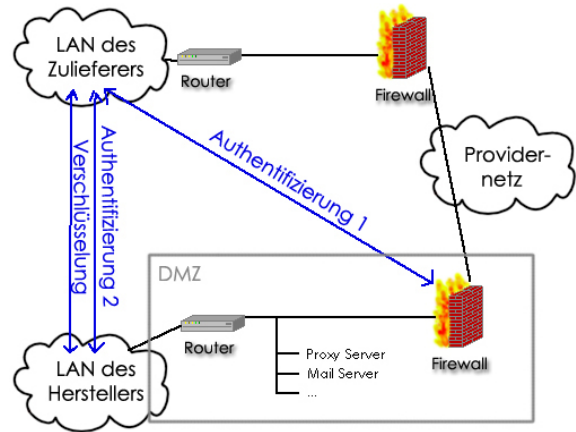
Die betriebswirtschaftlichen Zielsetzungen basieren jeweils auf individuellen Interessen der am Extranet teilnehmenden Unternehmen (oder Unterabteilungen von Unternehmen). Wie bei Intranet-VPN werden permanente gesicherte Verbindungen über ein öffentliches Netz aufgebaut, die sich in diesem Fall aber eine Vielzahl verschiedener Teilnehmer teilen. Daraus folgt ein entscheidender Unterschied, nämlich, dass für die Teilnehmer jeweils nur Zugriffsrechte zur Verfügung stehen sollen, die den spezifischen Anforderungen der Teilnehmer gerecht werden. Aus diesem Grund findet eine erste Authentifizierung an der Firewall/Router statt und eine zweite Authentifizierung an entsprechend zur Kommunikation freigeschalteten Ressourcen (Intranet-Server).

Oftmals ist bei Extranet-VPN sogar der gesamte Übertragungsweg zwischen zwei Endgeräten, die miteinander kommunizieren sollen, verschlüsselt. Dies macht zum Beispiel dann Sinn, wenn nur bestimmte Abteilungen (Arbeitsplatzrechner) der Partnerunternehmen miteinander kommunizieren sollen (z.B. Einkaufsabteilung eines Herstellers mit der Verkaufsabteilung eines Zulieferers). Die jeweiligen Rechner müssen dann mit einer VPN-Client-Software ausgestattet sein. Deswegen spricht man bei Extranet-VPN auch häufig von End-To-End-Verbindungen. Die Sicherheitsvorkehrungen für ein Extranet-VPN können also auch über eine gesicherte Verbindung zwischen zwei VPN-Gateways hinausgehen, wenn zwischen einzelnen Rechnern der lokalen Netze gesicherte Verbindungen hergestellt werden sollen.

Technische Implementationsmöglichkeiten

Möglichkeit 1: Die erste Authentifizierung erfolgt über Firewall-Systeme mit Zugriffslisten (access lists), die in den jeweiligen Routern realisiert werden (jeder Teilnehmer benötigt eine feste IP-Nummer). Die zweite Authentifizierung und gleichzeitig die Verschlüsselung der Übertragung erfolgt über eine IPSEC-Lösung mit ESP-Tunnel.

Möglichkeit 2: Die erste Authentifizierung erfolgt über IPSEC – AH. Die zweite Authentifizierung erfolgt z.B. über Kerberos. Die Verschlüsselung der Verbindung erfolgt über IPSEC – ESP. Vorteil dieser Lösung gegenüber Möglichkeit 1 ist die stärkere Authentifikation. Sie ist beim Authentication Header stärker als bei ESP und durch Kerberos wird eine Nutzerauthentifizierung ermöglicht.



5.3 Remote-Access-VPN

Zielsetzung

Ein Remote-Access-VPN ermöglicht Außendienstmitarbeitern den Zugriff auf das Netz der Firmenzentrale und zwar in der Form, dass sie von jedem beliebigen Ort, von dem sie sich über einen Internet-Service-Provider ins Internet einwählen können, die unternehmensüblichen und durch EDV unterstützten Geschäftsprozesse durchführen können.

Im Prinzip funktionieren Remote-Access-VPN ähnlich wie Wählverbindungen zwischen zwei Rechnern mit Modems, mit dem Unterschied, dass die Verbindung über einen Internet-Service-Provider stattfindet und somit firmenseitig keine Modem-Pools notwendig sind. Ein weiterer großer Vorteil ist das Einsparen von sehr hohen Verbindungskosten bei zum Beispiel internationalen Wählverbindungen.

Anforderungen an die Implementation

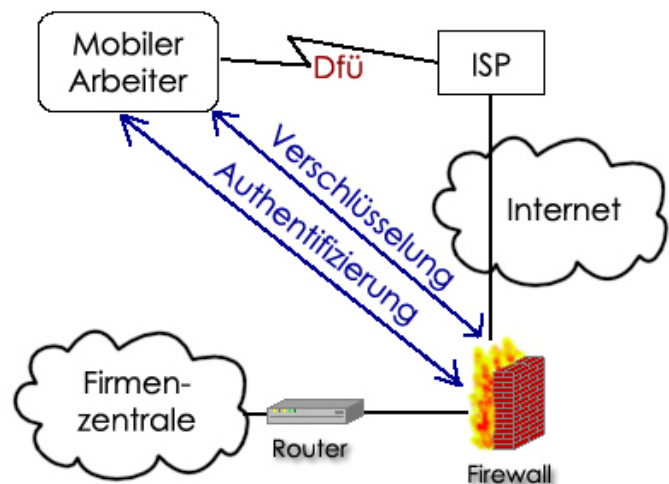
Nach dem DFÜ-Verbindungsaufbau des mobilen Endgeräts mit dem Internet-Service-Provider wird eine gesicherte Verbindung vom mobilen Endgerät ins Firmen-Netz über ein VPN-System aufgebaut. Dazu ist auf dem mobilen Rechner eine VPN-Client-Software installiert, die mit dem VPN-Gateway des Unternehmens in Verbindung tritt. Wie bei Intranet-VPNs findet im LAN des Unternehmens (hinter dem VPN-Gateway) keine gesicherte Kommunikation statt.

Da ein Client mit dem Intranet eines Unternehmens verbunden wird, spricht man auch von einem End-To-Site-VPN.

Technische Implementationsmöglichkeiten

Möglichkeit 1: Zunächst authentifiziert sich der mobile Mitarbeiter über PPP EAP. Anschließend wird eine verschlüsselte Übertragung zwischen Firewall und Laptop über TLS aufgebaut.

Möglichkeit 2: Der Mitarbeiter authentifiziert sich mittels einer digitalen Signatur, um per IKE eine IPSec-Verbindung auszuhandeln. Dabei wird ihm per mode config eine Virtuelle IP-Adresse innerhalb des Netzwerkes zugewiesen.



Für ein Netzwerk, das bis zur OSI-Schicht 3 nur IP verwendet, ist die Möglichkeit 2 besser geeignet, da ab Schicht 3 verschlüsselt. Möglichkeit 1 bietet hierbei nur Verschlüsselung ab Schicht 4.

Allerdings werden in Möglichkeit 2 meist nur Rechner authentifiziert, aber keine Benutzer¹². Ist eine technisch einfachere Benutzerauthentifikation gewünscht, so ist Möglichkeit 1 vorzuziehen.

¹² Eine Benutzerauthentifikation ist bei IKE mittels PKI-Verfahren möglich, aber aufwendiger als EAP.

6 Schlussbetrachtung

Die SSL / TLS-Architektur ermöglicht eine hohe Sicherheit für End-to-End-Verbindungen zweier Anwendungen. Durch die Implementation der SSL-API kann daher eine hohe individuelle Sicherheit für Netzwerkkommunikation erreicht werden, ohne dass auf eine VPN-Technologie der tieferen Ebenen zurückgegriffen werden muss.

Für die Protokolle von Layer 2 und 3 spricht, dass über sie kommuniziert werden kann, ohne dass Anwendungen direkt von ihnen Kenntnis haben müssen.

Bei den Layer 2 Technologien hat sich das aufgrund der Vorteile, multiple Verbindungen bei jeder Betriebsart und ein geschlossenes In-Band-Verfahren zu verwenden, das L2TP-Protokoll gegenüber PPTP durchgesetzt. Da L2TP als solches, jedoch weder Verschlüsselung, Paket-Authentifizierung noch eine PKI verwendet, wird es meist in Verbindung mit IPsec eingesetzt.

IPsec ist nur dann sinnvoll, wenn der ESP-Tunnelmodus verwendet wird. Nur er verwendet Verschlüsselung über ein VPN-Gateway hinweg und sichert die Authentizität der IP-Datagramme und ist somit die einzig sinnvolle Lösung, mittels IPsec eine VPN im hier definierten Sinne herzustellen.

Allerdings ist dann keine Network Address Translation (NAT) möglich. So sind IPsec Lösungen besonders für Site-to-Site VPNs nützlich. In Verbindung mit IKE ist auch eine Remote-Access-VPN sinnvoll, da mittels IKE auch eine dynamische Adressierung berücksichtigt werden kann. Dies ist besonders dann sinnvoll, wenn ein Mitarbeiter mit einem Notebook von außerhalb über Zugriff auf ein oder mehrere Subnetze eines Unternehmens verfügen muss.

Der Authentication Header und Verschlüsselung ermöglicht in Verbindung mit einem ESP Tunnelmodus, bereits vor dem Netzwerk autorisierte Kommunikationspartner zu selektieren. Somit kann mittels IPsec der Verkehr im Netzwerk reduziert werden. Zwar könnte dies zwar auch mittels der Adressfilterung einer Firewall geschehen, die Firewall kann aber keine Remote-partner mit dynamischer Adressierung erkennen.

L2Sec ist von den Möglichkeiten her eine sehr leistungsfähige Technologie. Bei ihr wird es davon abhängen, inwieweit sich Implementationen als leistungsfähig erweisen, so dass eine Standardisierung erfolgen kann und inwieweit sich IPsec entwickelt.

Die folgende Tabelle stellt noch einmal die Layer 2- und Layer 3 Techniken stichpunktartig gegenüber.

Tabelle 1: VPN-Techniken der Layer-2 und der Layer-3 im Vergleich nach [Böhmer]

Eigenschaft	PPTP	L2TP	IPsec	L2Sec
Nutzer-Authentifizierung	Ja	Ja	Nein	Ja
NAT-Support	Ja	Ja	Nein	Ja
Multiprotokollfähigkeit	Ja	Ja	Nein	Ja
Dynamische Zuweisung von Tunnel-IP-Adressen	Ja	Ja	N/A ¹³	Ja
Verschlüsselung	begrenzt	Nein	Ja	Ja
Public-Key-Infrastruktur	Nein	Nein	Ja	Ja
Authentizitätsprüfung von Paketen	Nein	Nein	Ja	Ja
Überprüfung von Multicats	Ja	Ja	Nein	Ja

¹³ Mit IKE und mode-config ist die dynamische Zuweisung von Tunnel-IP-Adressen möglich.

Für eine einfache Einbindung eines Kunden in das eigene Netzwerk ist die Layer4-Technologie sinnvoll. Sie bietet ausreichende Sicherheit hinsichtlich der Vertraulichkeit der übertragenen Verbindung, erfordert aber keine individuelle Konfiguration der Rechner. Eine solche VPN-Variante ist nicht nur bei der Einwahl eines Zulieferers in das Netzwerk des Produzenten, sondern auch im B2C-Bereich des e-commerce sinnvoll. Beispiele hierfür sind Online-Banking oder e-shopping.

7 Quellenverzeichnis

- [Davis] C. R. Davis: „IPSec : Securing VPNs“, Osborne/McGraw-Hill, 1. Auflage, 2001
- [Böhmer] W. Böhmer: „VPN – Virtual Private Networks; Die reale Welt der virtuellen Netze“, Carl Hanser Verlag, 1. Auflage, 2002
- [Northcutt et al.] S. Northcutt, L. Zeltser, S. Winters, K. K. Frederik, R. W. Ritchey: “Inside Network Perimeter Security”, New Riders, 1. Auflage, Juli 2002
- [Vortrag4] M. Mariach, E. Hofmann, I. Tsalman: „Kryptographische Verfahren“, Vortrag im Seminar „Sicherheit in vernetzten Systemen“, WS 2002/03, FB Informatik, Uni Hamburg
- [counterpane] N. Ferguson, B. Schneier: “A Cryptographic Evaluation of IPsec”, 1999, www.counterpane.com/ipsec.pdf
- [RFCxx] Request For Comment, Nummer xx, <http://rfc-editor.org> oder <http://www.ietf.org/rfc.html>
- [Gerbich] S. Gerbich :<http://www.informationweek.de/channels/channel05.htm>
- [Oppliger] R. Oppliger: „IT-Sicherheit: Grundlagen und Umsetzung in der Praxis“. Vieweg Verlag, 1997.

Abbildungsverzeichnis:

Abbildung 1: Schematische Darstellung eines VPN.....	2
Abbildung 2: Compulsary Mode.....	6
Abbildung 3: Voluntary Mode.....	6
Abbildung 4 : VPN-Typen auf den Schichten des OSI-Modells.....	9
Abbildung 5: VPN Tunnel.....	11
Abbildung 6: Skizzierung eines L2F-Tunnels vom POP (ISP) zum VPN-Gateways eines Unternehmens.....	12
Abbildung 7: Skizzierung eines PPTP-Tunnels.....	13
Abbildung 8: Skizzierung eines L2TP-Tunnels.....	14
Abbildung 9: Auszug der SAD eines Cisco Routes für eine inbound ESP (nach [Northcutt et. Al.], Seite 198).....	18
Abbildung 10: Authentication Header nach [RFC2402].....	20
Abbildung 11: IPv4 Header vor der Anwendung des AH.....	21
Abbildung 12: IPv4 Header nach der Anwendung des AH im Transport Modus.....	21
Abbildung 13: IPv4 Header nach der Anwendung des AH im Tunnel Modus.....	21
Abbildung 14: ESP Header nach [RFC2406].....	22
Abbildung 15: IPv4 Header vor der Anwendung des ESP.....	23
Abbildung 16: IPv4 Header vor der Anwendung des ESP im Transport Modus.....	23
Abbildung 17: IPv4 Header vor der Anwendung des ESP im Tunnel Modus.....	23
Abbildung 18: Packet bestehend aus ISAKMP Header und Key Exchange Payload.....	26
Abbildung 19: IKE Phase 1 im Main Mode mit pre-shared keys nach [Davis].....	27
Abbildung 20: IKE Phase 1 im Aggressive Mode mit pre-shared keys nach [Davis].....	27
Abbildung 21: IKE Phase 2 nach [RFC2409].....	28
Abbildung 22: Einordnung von SSL in das TCP/IP-Modell.....	31
Abbildung 23: Nachrichten Austausch für einen SSL/TLS-Verbindungsaufbau.....	32