

VPN-Technologien

**Alternativen und Bausteine einer erfolgreichen
Lösung**

von

Dipl.-Inform. Andreas Meder

3.5 IPSec

Bekanntermaßen bergen die TCP/IP-Protokolle wie auch die auf dieser Protokollwelt aufsetzenden Standarddienste eine Reihe von teilweise gravierenden Sicherheitslücken. Auf der Dienst- d.h. der Applikationsebene lassen sich diese Lücken größtenteils durch entsprechende Schutzmechanismen der jeweiligen Applikation schließen. Als Beispiel seien hier die in der TCP/IP-Welt üblichen Kennwortübertragungen im Klartext genannt, die sich leicht durch entsprechende Änderung der Client- und Serversoftware absichern lassen.

Problematischer sind die Lücken auf der Ebene der Paketübermittlung. Hier sind vor allem zwei Schwachpunkte zu nennen, die das wesentliche Gefahrenpotential heraufbeschwören:

- Die Möglichkeit für Unbefugte, Paketinhalte zu lesen.
- Die Möglichkeit, IP-Pakete nach Belieben zu manipulieren, und zwar sowohl was den Inhalt als auch was die Ziel- bzw. Absenderadresse betrifft.

Eine Reihe der aus diesen Schwachstellen resultierenden Gefahren lassen sich ebenfalls durch Mechanismen auf der Anwendungsebene, etwa durch Einsatz von Verschlüsselungsverfahren zum Schutz von E-Mails, abwehren, allerdings ist diese Vorgehensweise naturgemäß aufwändig und ineffizient. Jede Anwendung, die vertrauliche oder sonst in irgendeiner Form schützenswerte Daten versendet, muss durch entsprechende Mechanismen abgesichert werden. Außerdem schützen alle Maßnahmen auf der Anwendungsebene nicht davor, dass Angreifer sich mittels gefälschter IP-Adressen eine falsche Identität zulegen und auf diese Weise unberechtigt Pakete versenden können. Selbst wenn diese Pakete mangels korrekter Verschlüsselung in der Regel auf der Anwendungsebene keinen Schaden anrichten, sind doch immer noch Denial-of-Service-Angriffe möglich.

Sogar der Einsatz von Verschlüsselung innerhalb der genutzten Applikation schützt nicht in jedem Fall vor illegalen Manipulationen, wie die Möglichkeit, sich als Angreifer in eine SSL-Verbindung einzuschleusen und auf diese Weise die scheinbar geschützten Daten mitzulesen und gegebenenfalls sogar Manipulationen vorzunehmen, beweist.

Die Schwächen von IP sind seit langem evident und finden in Form entsprechender Schutzmechanismen in der Nachfolgerversion IPv6 Berücksichtigung. Die dort standardmäßig implementierten Mechanismen zur Sicherung von Vertraulichkeit und Integrität wurden von der IETF in dem Bestreben, einen Ende-zu-Ende-Mechanismus zur Gewährleistung von Datensicherheit bei der Kommunikation in IPv4-Netzen zur Verfügung zu stellen, für die aktuelle Protokollversion angepasst und unter der Bezeichnung Internet Protocol Security (IPSec) als Ergänzung zu den etablierten Protokollmechanismen standardisiert. Die diesbezüglichen Mechanismen sind immer noch in der

Weiterentwicklung, um sich an immer wieder auftretende Detailprobleme anzupassen, haben aber mittlerweile einen hohen Qualitätsstand erreicht.

Die zur Verfügung gestellten Mechanismen erweitern das vorhandene Internet Protocol um Schutzmaßnahmen gegen Abhören und Verändern von Paketinhalten und ermöglichen so die sichere Übertragung vertraulicher Informationen über ungeschützte Netze auch ohne zusätzliche Maßnahmen auf den oberen OSI-Protokollschichten. IPSec arbeitet auf OSI-Layer 3 und unterstützt ausschließlich IP-Traffic – zur Nutzung für andere Protokolle müssen diese auf geeignete Weise in IP-Pakete verkapselt werden. Für alle IP-basierten Anwendungen ist IPSec ebenso transparent wie für IP-Router – mit Ausnahme natürlich der notwendigen IPSec-Gateways.

IPSec ist in den RFCs 2401, 2402 und 2406 beschrieben, außerdem existiert eine Reihe von weiteren RFCs, die sich mit Detailergänzungen und -präzisierungen befassen.

3.5.1 Funktionsweise im Überblick

IPSec hat die Aufgabe, die Vertraulichkeit von Datenpaketen und deren Integrität oder beides gleichzeitig zu gewährleisten. Als Methoden kommen hier naturgemäß kryptografische Techniken zum Einsatz. Damit beide Kommunikationspartner diese Techniken koordiniert anwenden, müssen in den Datenpaketen Informationen über die eingesetzten Techniken vorhanden sein. Dazu definiert IPSec zwei optionale zusätzliche Paket-Header:

- Authentication-Header (AH): Dieser dient der Koordination und Durchführung der Integritätsprüfung
- Encapsulating Security Payload (ESP): Dieser Header dient der Koordination und Durchführung der Datenverschlüsselung

Je nach Anforderungen an die Sicherheit kann ein IPSec-Paket einen oder beide Header enthalten.

Voraussetzung für eine IPSec-basierte geschützte Kommunikation zwischen zwei Kommunikationspartnern ist die Festlegung so genannter Sicherheitsassoziationen (**Security Associations, SA**). Aufgabe dieser SAs ist die Festlegung von Parametern im Zusammenhang mit den IPSec-Schutzmechanismen, die auf den Datenverkehr der betreffenden Kommunikationsbeziehung angewandt werden.

Jede SA wird dabei durch folgende Attribute eindeutig beschrieben:

- den Security Parameter Index (siehe unten),
- die IP-Adresse des Kommunikationspartners,
- das jeweils anzuwendende Sicherheitsprotokoll (AH oder ESP).

SAs beschreiben eine „Simplex“-Beziehung zwischen den beiden Kommunikationspartnern, so dass für übliche bidirektionale Kommunikationsbeziehungen zwei SAs definiert sein müssen: eine SA für den eingehenden und eine für den ausgehenden Datenverkehr.

Innerhalb einer SA kann nur ein Sicherheitsprotokoll spezifiziert sein, d.h. es kann entweder AH oder ESP, aber nicht beides zusammen angewandt werden. Sind beide Funktionalitäten erforderlich bzw. erwünscht, so müssen hierzu zwei unabhängige SAs definiert werden. Diese SAs können dann gebündelt werden, so dass beide Sicherheitsprotokolle zur Anwendung kommen.

Die wesentlichen Inhalte jeder SA lassen sich wie folgt zusammenfassen:

- der Algorithmus, d.h. die Methode der Chiffrierung bzw. der Integritätsprüfung, jeweils soweit erforderlich,
- der zu verwendende Schlüssel,
- die Gültigkeitsdauer der SA,
- der Protokollmodus (siehe Kapitel 3.5.4).

Die SAs sind in lokalen Datenbanken auf den jeweiligen IPSec-Systemen abgelegt. Um beiden Kommunikationspartnern eine eindeutige Zuordnung von Datenpaketen zu SAs und umgekehrt zu ermöglichen, korrespondieren diese lokalen SAs mit Informationen in den IPSec-Headern, den so genannten Security Parameter Indices (SPI). Dieser numerische Wert im Header wird vom Sender anhand der anzuwendenden SA ermittelt und im Paket eingetragen; umgekehrt ermöglicht der SPI es dem Empfänger, die entsprechende SA aus seiner lokalen Datenbank zu ermitteln und das IPSec-Paket korrekt zu verarbeiten, da er mit Hilfe der SAs die benutzten kryptografischen Verfahren, die verwendeten Schlüssel und die mit dem Datenpaket assoziierten Rechner-systeme aus dem SPI ermitteln kann.

Der numerische Wert des SPI muss für jeden Empfänger eindeutig sein; er wird daher sinnvollerweise während der Aushandlung der SA-Parameter zwischen Sender und Empfänger (siehe Kapitel 3.5.5) vom jeweiligen Empfänger festgelegt. Aus Sicht des Senders stellt dann wiederum ein Paar aus Empfängeradresse und zugehörigem SPI eine eindeutige Zuordnung zu einer SA sicher.

Der Ablauf stellt sich im Einzelnen wie folgt dar:

1. Der Sender ermittelt die zum Empfänger gehörende (eventuell gebündelte) SA.
2. Der Sender wendet das in der SA spezifizierte kryptografische Verfahren auf der Basis des dort vorgegebenen Schlüssels an und erzeugt den IPSec-Header.
3. Der Sender trägt den SPI der benutzten SA in den IPSec-Header ein.

4. Liegt eine Bündelung von SAs vor, wiederholt der Sender die Schritte 2 und 3 für alle weiteren gebündelten SAs.
5. Der Empfänger liest den SPI aus und ermittelt die zugehörige SA.
6. Der Empfänger wendet das in der SA spezifizierte kryptografische Verfahren auf der Basis des dort vorgegebenen Schlüssels an und stellt das ursprüngliche Paket (ohne IPSec-Header) wieder her.
7. Der Empfänger wiederholt die Schritte 5 und 6 gegebenenfalls für weitere IPSec-Header.

Dieser Ablauf wird für jedes Datenpaket durchgeführt. Pakete ohne SPI oder in irgendeiner Weise ungültige Pakete werden (je nach Security Policy) vom Empfänger meist kommentarlos ignoriert.

3.5.2 Integritätsprüfung – Authentication-Header

Der Authentication-Header stellt einen zusätzlichen Header im IP-Paket dar, der hinter dem (äußeren) IP-Header eingefügt wird (siehe Abbildung 3.8). Er enthält im Wesentlichen eine kryptografische Prüfsumme des Inhaltes des IP-Pakets. Von dieser Prüfsumme werden sowohl der IP-Header und die IP-Daten als auch die fixen Felder des AH, also letztlich das gesamte IP-Paket mit Ausnahme der eigentlichen Prüfsumme innerhalb des AH selbst erfasst. Eine Änderung des Datenteils des Pakets erfolgt in keinem Fall, die Sicherheitsfunktionalität des AH ist auf den Header selbst beschränkt. Durch die kryptografischen Eigenschaften der AH-Prüfsumme wird, die Verwendung eines hinreichend starken Hashverfahrens zur Prüfsummenbildung vorausgesetzt, die Integrität des so geschützten IP-Pakets während der Übertragung gewährleistet. Eine Änderung des Pakets in irgendeiner Form zieht notwendigerweise eine Anpassung der Prüfsumme nach sich. Diese Anpassung kann aber nur von jemandem vorgenommen werden, der die dazu erforderlichen Schlüsselinformationen besitzt, ein außen stehender Angreifer ist dazu nicht in der Lage.

Für VPN-Realisierungen ist der AH von eher untergeordnetem Interesse, da es hier praktisch immer auch um den Schutz der Vertraulichkeit geht, die sich nur durch ESP sicherstellen lässt. Setzt man jedoch ESP ein, so wird in der Praxis auch die durch ESP ebenfalls mögliche Integritätsprüfung genutzt, so dass der AH im Grunde seiner Daseinsberechtigung beraubt ist. Zwar ist es richtig, dass die ESP-Authentication Manipulationen gleich welcher Art am (äußeren) IP-Header nicht entdecken kann, da die Prüfsumme letzteren nicht erfasst; dennoch besteht ein wirksamer Schutz gegen derartige Angriffe (z.B. Adress-Spoofing), da ein Kommunikationspartner mit gespoofter Identität zwangsläufig an der Ver- bzw. Entschlüsselungsfunktion von ESP scheitert.

AH-Format

Im AH werden zunächst im ersten Speicherhalbwort (2 Bytes) Art und Position des nächsten Protokollheaders spezifiziert. Dann folgt – nach einem reser-

vierten Bereich in Größe von 2 Bytes, der derzeit stets auf den Wert „0“ zu setzen ist, – der SPI (4 Bytes), der dem Empfänger Information über die SA dieses IP-Pakets liefert. Eine eingefügte Sequenznummer (4 Bytes) bietet Schutz vor Replay-Angriffen, d.h. vor dem Versuch, abgefangene gültige IPSec-Pakete unbemerkt erneut zu senden.

Den Rest des Pakets bildet die eigentliche kryptografische Prüfsumme, deren Länge vom jeweils verwendeten Verfahren abhängt. In der Prüfsumme ist gegebenenfalls ein Padding (beliebigen Inhalts) zur Ausrichtung des AH auf eine Wortgrenze innerhalb des IP-Pakets enthalten.

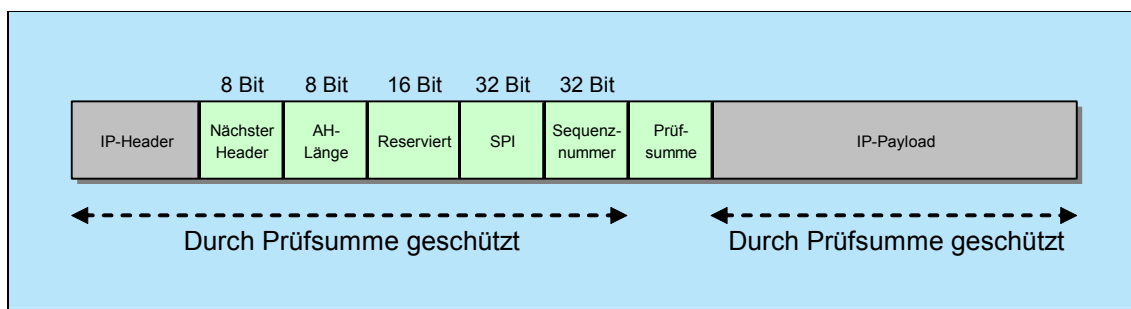


Abbildung 3.8: Format und Position des Authentication-Headers

Ablauf

1. Der Sender ermittelt die SA für die Kommunikationsbeziehung sowie den SPI.
2. Der Sender baut einen AH gemäß der Festlegungen in der SA in das IP-Paket ein. Dabei wird die Sequenznummer inkrementiert (neue Kommunikationsbeziehungen werden mit 0 initialisiert, d.h. der Startwert im ersten Paket ist 1).
3. Der Sender setzt zur Berechnung der Prüfsumme alle veränderbaren oder noch unbekanntenen Werte im Paket auf den Wert „0“. Hierunter fällt insbesondere das Prüfsummenfeld, aber auch fast jedes variable Feld im IP-Header (TTL, CRC, Flags, Fragment Offset). Dann berechnet er die Prüfsumme und setzt den Wert in den AH ein.
4. Der Empfänger ermittelt anhand der SPI die zugehörige SA.
5. Der Empfänger verifiziert die Sequenznummer. Pakete mit ungültiger Sequenznummer werden kommentarlos verworfen.
6. Der Empfänger setzt zur Berechnung der Prüfsumme alle veränderbaren oder aus Sicht des Sender unbekanntenen Werte im Paket auf den Wert „0“, analog zum Sender und berechnet die Prüfsumme mit der Methode und dem Schlüssel aus der ermittelten SA.
7. Der Empfänger vergleicht die ermittelte Prüfsumme mit der im AH des Pakets mitgelieferten.

8. Der Empfänger entfernt den AH und verarbeitet das IP-Paket, falls die Prüfsummen übereinstimmen; stimmen die Prüfsummen nicht überein, verwirft er das Paket.

AH-Prüfsummenverfahren

In der Formatspezifikation des AH sind weder Art noch Länge der Prüfsumme festgelegt. Die einzige Bedingung, deren Erfüllung bei Bedarf mittels Padding erzwungen wird, ist, dass die prinzipiell variable Länge ein Vielfaches von 32 Bit sein muss.

Die Festlegung von Art und Länge der Prüfsumme erfolgt über die Parameterspezifikation in der SA der jeweiligen Kommunikationsbeziehung. Die SA bzw. der damit korrespondierende SPI definiert auch, welcher geheime Schlüssel gegebenenfalls verwendet wird.

Die in der aktuellen IPSec-Spezifikation vorgesehenen Standardverfahren sind HMAC mit MD5 und HMAC mit SHA-1 (spezifiziert in RFC 2104). **HMAC** steht für **Hashed Message Authentication Code** und beschreibt einen Mechanismus zur Integritätsprüfung mittels kryptografischer Hashfunktionen und geheimem Schlüssel (siehe Kapitel 2.6.3.2).

Frühere Spezifikationen (RFC 1826) sahen MD5 mit geheimem Schlüssel und einem 128-Bit-Hashwert vor. Die Länge des geheimen Schlüssels war in diesem Fall nicht festgelegt, betrug aber in der Regel ebenfalls 128 Bit. Aufgrund der Art und Weise, wie der Schlüssel in die Prüfsummenberechnung einging, spielt seine Länge auch im Grunde keine Rolle: er wird zur Prüfsummenkalkulation vor und hinter die zu schützenden Daten gesetzt und dann die Prüfsumme darüber gebildet.

3.5.3 Verschlüsselung – Encapsulating Security Payload

Analog zur Integritätsprüfung durch den AH wird auch der Vertraulichkeitsschutz mit Hilfe eines zusätzlichen Headers zwischen (äußerem) IP-Header und Payload realisiert. Anders als beim AH ist jedoch naturgemäß eine Veränderung des ursprünglichen Paketinhalts notwendig, so dass sich die Schutzfunktionalität im Falle des ESP-Mechanismus in zwei Bereiche aufteilt:

- Der Schutz der Vertraulichkeit wird durch die Verschlüsselung der Payload erreicht. Der ESP-Header trägt hierzu nur insofern bei, als er diejenigen Informationen bereitstellt, die der Empfänger benötigt, um die Verschlüsselung rückgängig zu machen. Dies geschieht analog zum AH mittels des SPI, aus dem sich durch den Empfänger eindeutig die der Verschlüsselung zugrunde liegende SA ableiten lässt.
- Weitere Schutzfunktionen werden durch den ESP-Header selbst realisiert. Hierunter fallen eine Integritätsprüfung sowie ein Anti-Replay mittels Sequenznummer. Die Integritätsprüfung erstreckt sich hier auf den gesamten ESP-Bereich mit Ausnahme der generierten Prüfsumme selbst, die sich

weder im Header noch in der Payload befindet, sondern am Paketende angehängt wird.

Alle Sicherheitsfunktionen sind optional, allerdings muss mindestens eine Option gewählt werden.

ESP-Format

ESP besteht aus vier Teilen. Zunächst wird der SPI spezifiziert. Die Länge dieses Protokollfeldes beträgt wie im Falle des AH 32 Bit. Danach folgt eine ebenfalls 32 Bit lange Sequenznummer zum Schutz vor dem erneuten Versenden aufgezeichneter Datenpakete. Anschließend folgt die eigentliche Payload, den Abschluss bildet die Prüfsummeninformation (siehe Abbildung 3.9).

Sowohl Payload als auch Prüfsummeninformation sind in ihrer Länge variabel und hängen von der ursprünglichen Länge der zu verschlüsselnden Daten sowie von den spezifizierten kryptografischen Verfahren ab. Im Falle der Payload bestimmt das gewählte Chiffrierverfahren darüber hinaus auch das Format der Payload: so muss z.B. bei Verwendung von DES-CBC (siehe unten) ein Initialisierungsvektor mit übergeben werden, und bei Verwendung eines Blockchiffrieralgorithmus muss gegebenenfalls eine Ausrichtung der Daten auf die Blockgrenzen durch Hinzufügen von Dummy-Daten (Padding) erreicht werden. Dieses Padding bildet zusammen mit weiteren Steuerinformationen den so genannten ESP-Trailer.

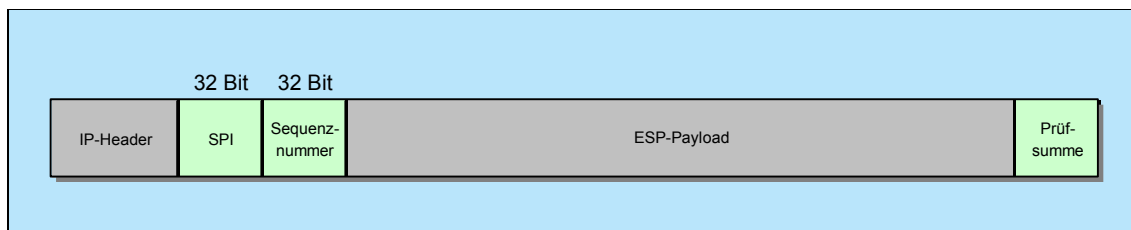


Abbildung 3.9: Format und Position von ESP-Header, -Payload und -Prüfsumme

Ablauf

1. Der Sender ermittelt die SA für die Kommunikationsbeziehung sowie den zugehörigen SPI.
2. Der Sender verkapselt die zu schützenden Daten in das ESP-Payload-Feld, d.h. er erzeugt den ESP-Header und -Trailer, sowie gegebenenfalls notwendige Padding-Bits.
3. Der Sender verschlüsselt die zu schützenden Daten mit der für die SA vorgesehenen Methode und dem zugehörigen Schlüssel und trägt gegebenenfalls benötigte Synchronisierungsdaten am Anfang des Payload-Feldes ein.

4. Der Sender inkrementiert die Sequenznummer der SA (neue Kommunikationsbeziehungen werden mit 0 initialisiert, d.h. der Startwert im ersten Paket ist 1) und trägt den Wert in das entsprechende ESP-Protokollfeld ein.
5. Der Sender berechnet die Prüfsumme über die gesamten ESP-Daten (SPI, Sequenznummer, Payload) mit dem für die SA vorgesehenen Verfahren und fügt den Wert hinter der Payload in das entsprechende Protokollfeld ein.
6. Der Empfänger ermittelt anhand des SPI die zugehörige SA.
7. Der Empfänger verifiziert die Sequenznummer; Pakete mit ungültiger Sequenznummer werden kommentarlos verworfen.
8. Der Empfänger berechnet die Prüfsumme mit der Methode und dem Schlüssel aus der ermittelten SA. Stimmt die berechnete Prüfsumme mit der im Paket übermittelten nicht überein, wird das Paket kommentarlos verworfen.
9. Der Empfänger entschlüsselt den Inhalt der Payload mit der Methode und dem Schlüssel aus der ermittelten SA gegebenenfalls unter Verwendung der im Paket enthaltenen Synchronisierungsdaten und entfernt ein eventuelles Padding.

Standardverfahren

RFC 2406 legt als Standardverfahren für die Verschlüsselung den DES im CBC-Modus fest; somit muss jede RFC-konforme IPsec-Implementierung zumindest diesen Algorithmus unterstützen. Darüber hinaus sind u.a. für 3DES/CBC, AES/CBC sowie AES/CTR Implementierungsvorgaben in RFCs spezifiziert.

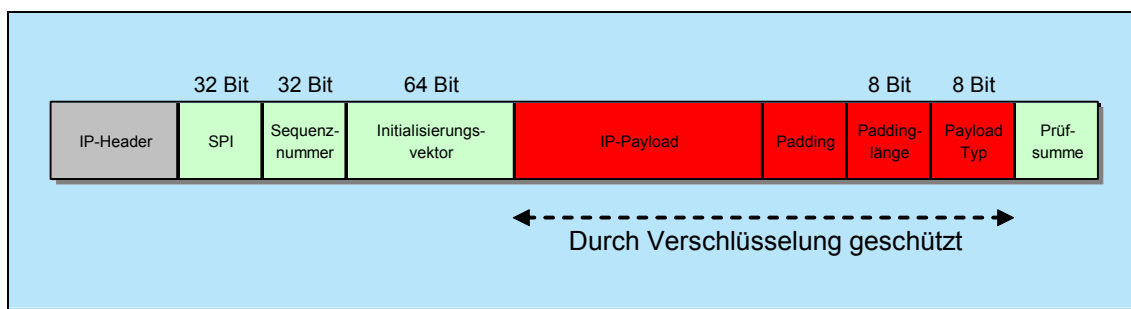


Abbildung 3.10: ESP-Paketformat für CBC-DES

Bei CBC-DES beträgt die Schlüssellänge 64 Bit (effektiv 56 Bit), ebenso die Blockgröße. Es wird ein 64 Bit langer Initialisierungsvektor benötigt. Für das konkrete Format der ESP-Payload bedeutet dies:

- sie beginnt mit einem 64 Bit-Wert für den IV,
- sie enthält gegebenenfalls Padding-Bits, falls der zu verschlüsselnde Teil der Payload kein Vielfaches von 64 Bit sein sollte.

Aus Gründen der Redundanz und Robustheit des Mechanismus wird in jedem ESP-Paket ein eigener IV übermittelt. Dabei handelt es sich bei dem IV des ersten gesendeten Pakets um einen zufälligen Wert, während die IVs der folgenden Pakete sich aus den jeweils letzten 8 Byte des Chiffretextes im vorhergehenden Paket ergeben.

3.5.4 IPSec-Modi

IPSec kann in zwei verschiedenen Modi betrieben werden: dem Transport-Modus sowie dem Tunnel-Modus.

Beim Transport-Modus befindet sich die IPSec-Header-Information zwischen dem IP-Header und dem nächsten Protokollheader des Originalpakets (siehe Abbildung 3.11). In diesem Modus können entweder AH oder ESP oder AH zusammen mit ESP eingesetzt werden. In letzterem Fall sollte sich der AH vor dem ESP befinden, so dass sich die Schutzwirkung des AH auch auf den ESP-Teil des Pakets erstreckt. FC2401 fordert zwingend, dass Host-Implementierungen die entsprechende Reihenfolge der Anwendung der Sicherheitsprotokolle sicherstellen müssen.

Beim Tunnel-Modus wird das gesamte Originalpaket mit einem neuen IP-Header versehen; die IPSec-Header-Information befindet sich in diesem Fall zwischen dem äußeren neuen und dem inneren Original-Header (siehe Abbildung 3.12). In diesem Modus sieht RFC2401 nur die Unterstützung von entweder AH oder ESP vor. Eine Kombination ist nicht vorgesehen. Sie lässt sich aber mit einem kleinen Trick letztlich doch erreichen: Es wird zunächst ein ESP-Tunnel etabliert und in das so erzeugte Paket ein zusätzlicher AH im Transport-Modus eingefügt. Das klappt natürlich nur dann, wenn beide Kommunikationspartner auch den Transport-Modus beherrschen, was (siehe unten) bei Gateways nicht zwingend der Fall ist.

Die Schutzwirkung des Authentication-Headers erstreckt sich stets auf das gesamte Paket, unabhängig vom gewählten Modus. ESP schützt allerdings im Transport-Modus nur die IP-Payload, der IP-Header bleibt ungesichert. Im Tunnel-Modus wird auch der Original-IP-Header in die Verschlüsselung und Integritätsprüfung mit einbezogen.

Die IETF hat in RFC2401 den Transport-Modus nur für Ende-zu-Ende-Kommunikationsbeziehungen als zwingenden Bestandteil von IPSec-Implementierungen definiert; bei Einsatz von z.B. VPN-Gateways zur transparenten Netzwerkkopplung kommt daher in der Praxis fast immer der Tunnel-Modus zum Einsatz. Bei Nutzung eines „fremden“ Trägernetzes, wie es beim VPN-Einsatz praktisch immer der Fall ist, verbietet sich der Transport-Modus sogar, da dieser keine Entkopplung der Adressräume und des Routings zwischen VPN und Trägernetz ermöglicht. Umgekehrt hingegen kann in Ende-

zu-Ende-Kommunikationsbeziehungen bei Bedarf auch der Tunnel-Modus verwendet werden.

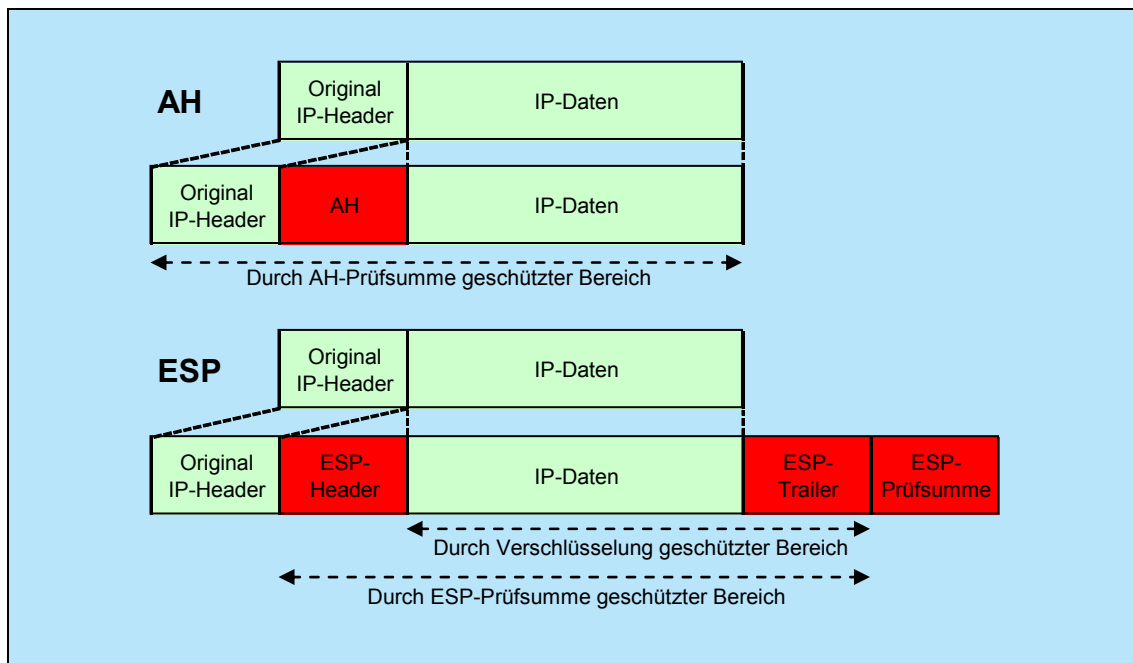


Abbildung 3.11: IPsec Transport-Modus

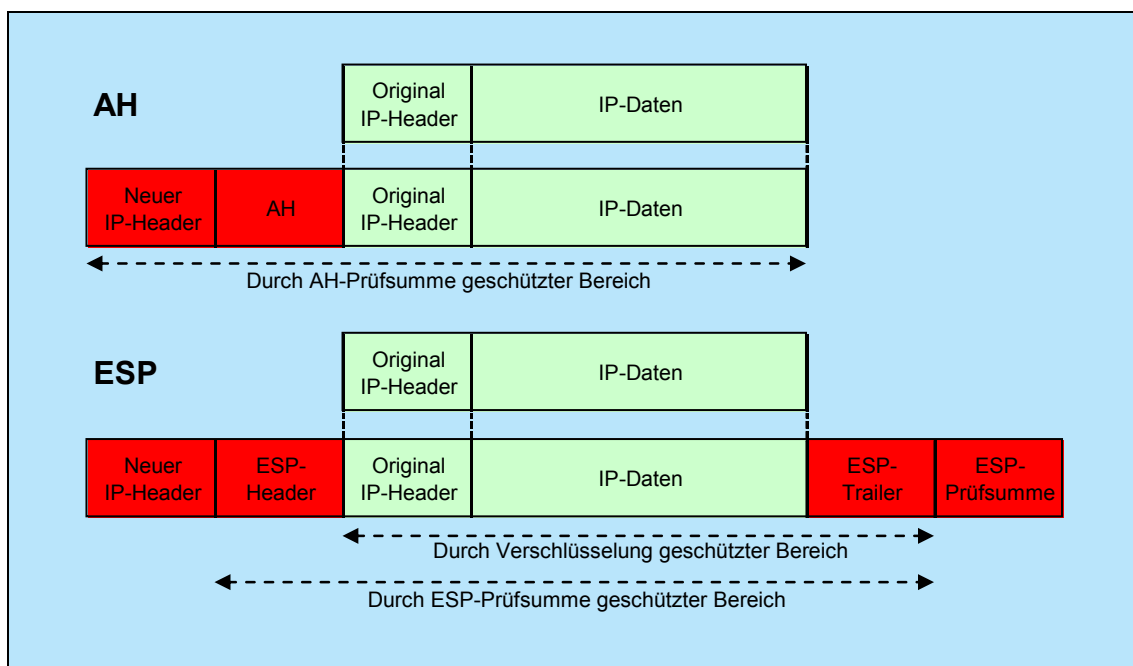


Abbildung 3.12: IPsec Tunnel-Modus