IPSEC

Gruppenarbeit im Fach Kryptografie

HTA Horw

Rainer Meier
Käserei
6288 Schongau
skybeam@skybeam.ch

Benjamin Schwitter
Titlisstrasse 11
6020 Emmenbrücke
crank@crankshome.ch

 2005-02-28

1. Inhaltsverzeichnis

2. Glossar

Tabelle 1 Glossar

Begriff	Erklärung
HMAC	Hash Message Authentication Codes
SA	Security Association
SAD	Security Association Database
AH	Authentication Header
ESP	Encapsulated Security Payload
SPI	Security Parameter Index
TCP	Transport Control Protocol
IP	Internet Protocol
NAT	Network Address Translation

3. Allgemeine Funktionsweise

IPSec ist wurde 1998 entwickelt um Vertraulichkeit, Integrität und Authentizität auf IP Ebene zu garantieren. IPSec war ursprünglich erst für IPv6 geplant, wurde dann aber doch für IPv4 standardisiert. Die Architektur wird im RFC2401 beschrieben.

IPSec verhält sich transparent gegenüber der oberen Netzwerkschichten. Somit müssen bestehende Anwendungen nicht angepasst werden um IPSec nutzen zu können.

Die wichtigsten Elemente von IPSec sind der Authentication Header (AH), das ESP-Protokoll (Encapsulating Security Payload) und die Schlüsselverwaltung.

IPSec kann entweder nur die Nutzdaten schützen (Transport-Modus) oder das gesamte IP Packet (Tunnel-Modus).

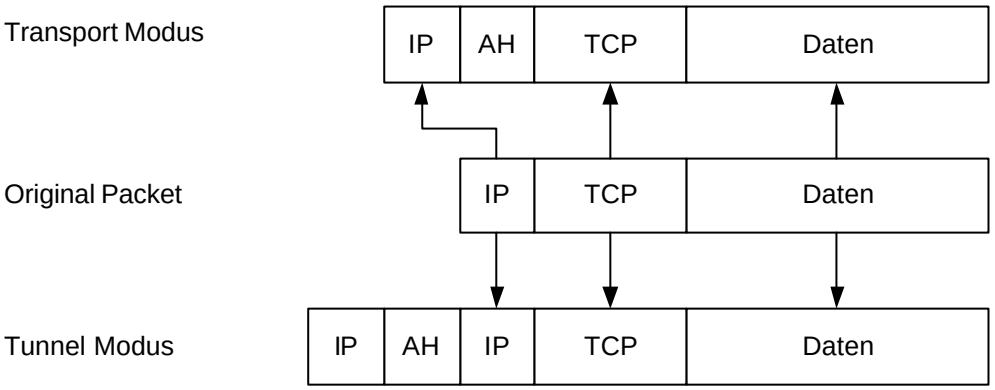

Abbildung 1 IPSec Betriebsmodus

Um die Integrität der IP Datagramme sicherzustellen werden HMAC Algorithmen wie MD5 oder SHA verwendet. Dazu wird aus den Datagrammen und einem geheimen Schlüssel ein HMAC erzeugt und im IPSec Header mitgeschickt. Der Empfänger kann dann mit dem selben Algorithmus prüfen, ob die Meldung verändert wurde.

Die IP Datagramme werden vor der Übertragung mit symmetrischen Verschlüsselungsverfahren verschlüsselt. Gemäss dem Standard müssen NULL und DES implementiert sein. Allerdings werden häufig stärkere Verschlüsselungsverfahren wie 3DES, AES oder Blowfish verwendet.

Für Jede Verbindung müssen Verbindungsparameter wie Quell- und Zieladresse, verwendetes Protokoll, verwendete Algorithmen sowie Schlüssel gespeichert werden. Dies geschieht in der sogenannten Security Association Database (SAD). Jeder Eintrag bekommt eine eindeutige Nummer, den Security Parameter Index (SPI)

4. IPSec Protokolle

Die IPSec Protokollfamilie basiert auf zwei Protokollen, dem Authentication Header (AH) Protokoll und dem Encapsulated Security Payload (ESP) Protokoll.

4.1. Authentication Header (AH)

Das AH-Protokoll garantiert die Integrität des IP-Datagrammes. Dazu muss ein HMAC errechnet werden, der aus dem geheimen Schüssel sowie den Nutzdaten und einigen (statischen) Teilen des IP-Headers generiert wird. Der AH ist 24 Bytes lang und besteht aus folgenden Teilen

- Byte 1 (Next Header): Spezifiziert das Protokoll des nächsten Headers (4: Tunnel Modus, 6: Transport Modus)
- Byte 2 (Payload Length): Länge der Nutzdaten
- Byte 3, 4: Reserviert für zukünftige Belegung
- Byte 5-8 (Security Parameter (SPI): Identifiziert den Security Parameter Index (SPI) aus der Security Association Datenbank (SAD).
- Byte 9-12: Sequenznummer (Wird für das Sliding-Window Verfahren verwendet)
- Byte 12-24: HMAC – Hash-Wert der Nachricht

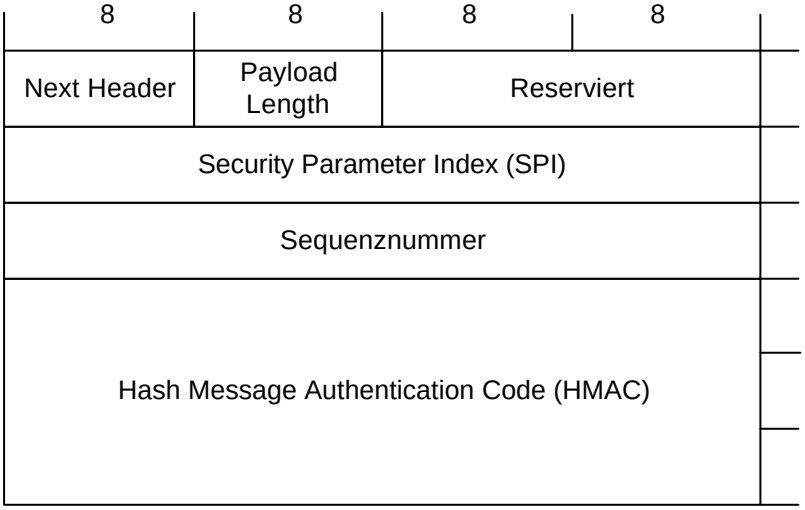

Abbildung 2 Authentication Header (AH)

Da der Authentication Header auch den IP-Header vor Veränderungen schützt funktioniert dies nicht mit NAT, da dabei die IP-Adressen im Header verändert werden.

4.2. Encapsulated Security Payload (ESP)

Der ESP-Header kann sowohl die Integrität des Packetes über HMAC garantieren als auch die Geheimhaltung der Daten mittels Verschlüsselung sicherstellen.

Der ESP-Header besteht aus folgende Teilen:

- Byte 1-4 (Security Parameter (SPI): Identifiziert den Security Parameter Index (SPI) aus der Security Association Datenbank (SAD).
- Byte 5-8: Sequenznummer (Wird für das Sliding-Window Verfahren verwendet)
- Byte 9-12: Inizielisierungs-Vektor (IV): Wird bei der Verschlüsselung verwendet

Danach folgen die Nutzdaten. Da ESP Blockverschlüsselungverfahren verwendet müssen die Daten dabei auf ein Mehrfaches der Blocklänge erweitert werden (Padding). Die Länge der angehängten Daten wird dann im Feld „Padding Länge“ gespeichert. Danach folgt noch ein 2 Byte langes „Next Header“ Feld um den nächsten Header zu spezifizieren. Am Schluss wird noch die 12 Byte lange HMAC Hash angehängt.

Der HMAC Hash wird nur aus den Nutzdaten berechnet und beinhaltet keine Header-Daten. Dies erlaubt theoretisch NAT in Verbindung mit ESP.

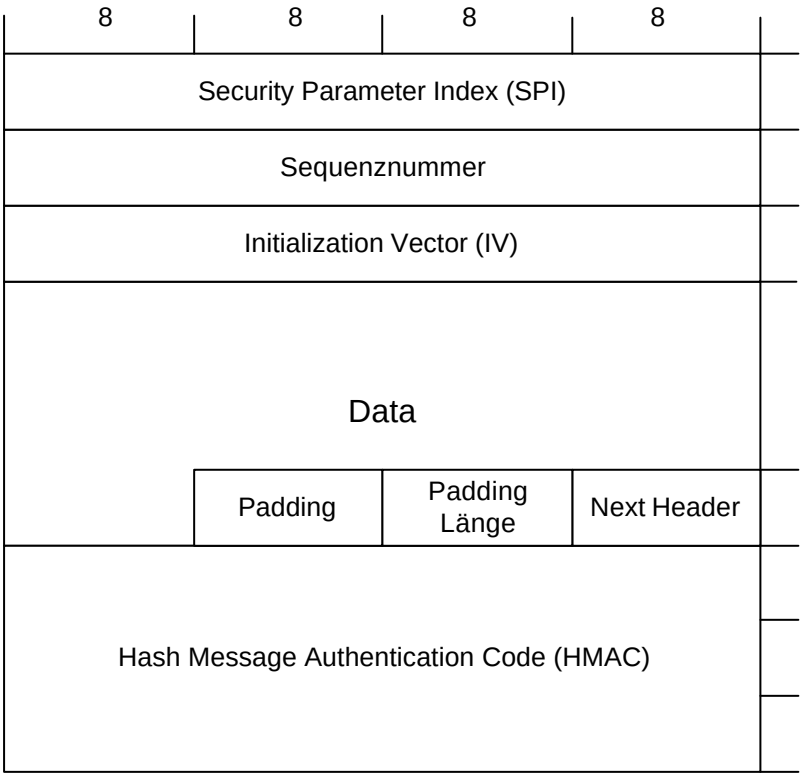

Abbildung 3 Encapsulated Security Payload (ESP)

5. Internet Key Exchange (IKE)

Internet Key Exchange ist ein einfaches Verfahren zum Aufbau sicherer, authentisierter Verbindungen. Es vermeidet die Komplexität von anderen Verfahren, welche auf Entwickler eher abschreckend erscheint.

IKE unterscheidet Modes, in denen Schlüssel ausgetauscht werden, welches in einer oder zwei Phasen geschieht. In der ersten Phase wird eine sichere, authentisierte Verbindung aufgebaut, in der zweiten Phase werden die in den verschiedenen Protokollen benötigten Schlüssel ausgetauscht, wobei in der Regel einzelne Schlüssel (Verschlüsselung, Hashen) von einem Masterschlüssel abgeleitet werden.

5.1. IKE Phase 1

In der ersten Phase wird eine sichere Verbindung zwischen zwei Teilnehmern aufgebaut; diese wird im RFC 2409 als ISAKMP Security Association (SA) bezeichnet. In dieser ersten Phase werden zwei Modi unterschieden.

Im Hauptmodus (main mode) werden drei Nachrichtenpaare mit jeweils einer Anfrage und einer Antwort ausgetauscht. Mit den ersten beiden Nachrichten werden die Verfahren ausgehandelt, die nächsten beiden tauschen die öffentlichen Werte für das Diffie-Hellman-Verfahren aus sowie weitere Daten für den Schlüsselaustausch. Die letzten beiden Nachrichten authentisieren die Diffie-Hellman-Daten; diese Daten sind verschlüsselt und verbergen die Identität der jeweiligen Teilnehmer.

Im agressiven Modus (agressive mode) werden im ersten Paket gleichzeitig die Verfahren ausgehandelt, öffentliche Werte für das Diffie-Hellman-Verfahren gesendet sowie weitere Daten für den Schlüsselaustausch und zur Identifizierung der Teilnehmer. Die Antwortnachricht umfasst die gleichen Daten und identifiziert zusätzlich den Absender. Schließlich werden in einer dritten Nachricht der Initiator authentifiziert und dessen Berechtigungen belegt.

5.2. IKE Phase 2

In der zweiten Phase wird die ISAKMP SA verwendet, um eine Security Association auf der Basis eines sicheren Dienstes auszuhandeln, wie IPsec oder irgendeines anderes Dienstes, der Schlüssel oder weitere Parameter benötigt. Dieses wird als Informational Exchange bezeichnet und sieht vor, dass die Daten verschlüsselt und mit einem geeigneten Hash-Algorithmus vor Verfälschung geschützt werden.

6. Diffie-Hellman Key Exchange

Das Diffie-Hellman Key Exchange Protokoll wurde 1976 von Diffie und Hellman entwickelt. Es erlaubt zwei Benutzern einen geheimen Schlüssel über eine unsichere Verbindung auszumachen, ohne vorher bereits Geheimnisse ausgetauscht zu haben.

Es existieren zwei Parameter p und g. Beide sind öffentlich und können von allen Benutzern in einem System verwendet werden. p ist eine Primzahl und g (auch Generator genannt) ist eine Zufallszahl kleiner p mit folgender Eigenschaft: Für jede Zahl zwischen 1 und p-1 gilt n = gk mod p.

Angenommen Alice und Bob wollen mittels dem Diffie-Hellman Verfahren einen gemeinsamen Schlüssel aushandeln. Sie gehen folgendermassen vor:

Zuerst generiert Alice eine geheime Zufallszahl a. Bob macht das gleiche und erhält eine Zahl b. Darauf berechnen beide ihre Werte zur öffentlichen Übermittlung mittels p und g und den ausgewählten Zahlen. Alice hat den Wert g^a mod p und bob a^b mod p. Diese Zahlen tauschen sie aus. Schliesslich berechnet Alice $g^{ab} = (g^b)^a$ mod p und Bob $g^{ba} = (g^a)^b$ mod p. Da $g^{ab} = g^{ba} = k$, haben die beiden Parteien nun ihren geheimen Schlüssel k.

Die Sicherheit des Verfahrens basiert auf der Verwendung einer sogenannten Einwegfunktion. Hierbei macht man sich die Tatsache zunutze, dass es zwar sehr einfach ist eine Zahl zu potenzieren, dass es jedoch nur mit sehr großem Aufwand möglich ist, den diskreten Logarithmus einer Zahl zu berechnen. In der Praxis werden sehr große Primzahlen verwendet, die Sicherheit kann weiter erhöht werden, wenn g = (p - 1) / 2 ebenfalls eine Primzahl ist (g ist dann eine Sophie-Germain-Primzahl).

Potenzielle Lauscher erfahren zwar p, g, A und B. a und b bleiben hingegen unbekannt.

Das Verfahren gilt als sicher gegen passives Abhören ("Eavesdropping"), da die im Klartext übertragenen Informationen nicht zur Konstruktion des Schlüssels K ausreichen. Wenn der Angreifer jedoch aktiv Datenpakete abfangen und verändert weiterschicken kann, besteht die Möglichkeit der Man-In-The-Middle-Attacke: Der Angreifer M vereinbart mit Partner A den Schlüssel KAM und mit Partner B den Schlüssel KMB, wobei A und B davon ausgehen, der Austausch fände mit dem berechtigten Kommunikationspartner statt. Auch die folgende symmetrisch verschlüsselte Kommunikation wird über den Angreifer M umgeleitet. Daten von A an B werden von A mit KAM verschlüsselt und können von M gelesen werden, bevor sie mit KMB verschlüsselt an B weitergeschickt werden (und umgekehrt). Dabei kann der Nachrichteninhalt sogar unbemerkt verändert werden.

7. Kritik an IPSec / Mögliche Angriffe / Schwachstellen

Bruce Schneier und Niels Ferguson haben anhand der existierenden Dokumentationen und RFCs über Ipsec einen Bericht erstellt, in dem es von Kritik und Schwachstellen nur so hagelt.

Die Stärke eines kryptographischen Systems liege in der Einfachheit des Aufbaus und der verwendeten Algorithmen.

Komplexere Systeme seien schlechter überschaubar und damit generell anfälliger für Fehler. Dies zeige sich nicht nur beim eigentlichen Systemaufbau, sondern vor allem auch bei dessen Software-Implementation, so Schneier.

Eine Kette ist nur so stark wie sein schwächstes Glied. Wenn also irgendwo ein kleiner Fehler eingebaut wird, was durch die grosse Komplexität sehr wahrscheinlich ist, ist die ganze Verschlüsselung wertlos.

Der Hauptkritikpunkt von IPSec liegt also bei dessen beinahe unüberschaubaren Konstruktion. Die beiden Krypto-Genies schlagen darum folgende Vereinfachungen vor:

- Der Transport Modus soll eliminiert werden, da er vom Tunnel Modus vollständig ersetzt werden kann.
- Das AH Protokoll soll entfernt werden, weil dessen Funktionalität vom ESP restlos übernommen werden kann.
- Bei ESP soll die Authentifizierung zwingend sein, bloss die Verschlüsselung optional. Verschlüsselung ohne Authentifizierung wäre nur im Transport Modus sinnvoll und dieser soll ja entfernt werden.
- Ausserdem müssen bei ESP alle Daten inklusive des Schlüssels für die Entschlüsselung authentifiziert werden. Ansonsten könnte sich ein „Man-in-the-Middle“ gewisse Informationen abstauben.
- Die Voraussetzung, schwache Schlüssel abzufangen, soll nicht zwingend sein. Auch hier besteht die Gefahr, dass beim Implementieren dieser Logik Sicherheitslöcher entstehen. Laut Schneier ist die Wahrscheinlichkeit viel grösser damit ein Loch zu schaffen als eines zu stopfen. Desweiteren soll man einfach eine Verschlüsselung wählen, die kaum schwache Schlüssel hat.
- Weitere kleinere Anpassungen innerhalb des Algorithmus selbst.

Besonders zu bemerken ist noch die Schlussfolgerung, die Schneier und Ferguson ziehen:
“Wir raten allen ab, IPSec in dessen gegenwärtigen Zustand zu verwenden (...). Wir raten aber noch viel mehr davon ab, andere aktuelle Alternativen zu verwenden und empfehlen IPSec als Alternative zu einem unsicheren Netzwerk. So ist die Realität.“

Das grösste Problem bei der Sicherheit ist nicht IPSec selbst, sondern wie es eingesetzt wird. Wenn nur Verschlüsselung, nicht aber Authentifizierung aktiviert ist, sind „Man-in-the-middle“ Attacken relativ einfach möglich.

Ausserdem ist eine Verbindung nur so sicher wie ihr schwächstes Glied. Wenn also zwar ein sicheres VPN Tunneling eigerichtet ist, auf das interne Netzwerk aber jeder über WLAN Zugriff hat, nützt der ganze Aufwand nichts. Zudem muss auch die Sys-

temsicherheit des VPN-Gateways selbst sehr hoch sein, um die Kompromittierung von Daten zu erschweren.

8. IPSec über NAT

Das Hauptproblem bei IPSec über NAT-Router ist, dass die Endpunkte hinter den NAT-Geräten von aussen nicht lokalisiert werden können. Aus diesem Grunde wurde eine Technik namens IPSec NAT Traversal (auch bekannt als NAT-T) definiert.

NAT-T fähige Geräte handeln beim Verbindungsaufbau automatisch aus, ob beide NAT-T unterstützen und ob NAT-Geräte im Verbindungsweg liegen. Falls beides zutrifft, dann wird IPSec über NAT-T benutzt. Ansonsten beginnt die normale IPSec Initialisierung.

8.1. Probleme von IPSec in NAT-Umgebungen

In diesem Abschnitt werden die Probleme beschrieben, die in NAT-Umgebungen in Verbindung mit IPSec auftreten.

Da NAT-Router die Source bzw. Destination Adressen im IP Header ersetzen müssen darf dieser (oder die entsprechenden Felder) nicht zur Authentisierung verwendet werden. Somit ist ein Betrieb über NAT nur im Tunnel-Modus möglich und auch nur mit dem ESP-Protokoll, da nur bei der Kombination aus Tunnel & ESP Modus der IP-Header verändert werden kann. Siehe dazu auch folgende Abbildungen des IPSec Headers im AH bzw. ESP Protokoll.

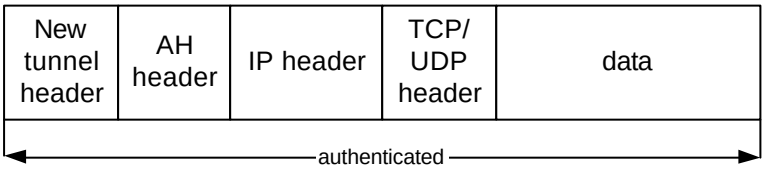

Abbildung 4 AH Packet (Tunnel Modus)

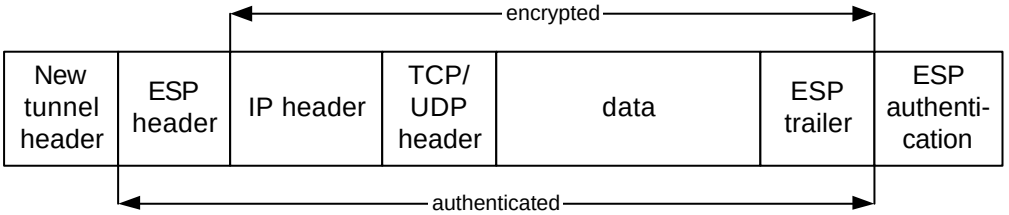

Abbildung 5 ESP Packet (Tunnel Modus)

8.1.1. Checksummen können nicht aktualisiert werden

Die TCP/UDP Header enthalten Checksummen für die IP Adressen und Portnummern. Ein NAT-Router muss diese Checksummen aktualisieren können. Dies ist durch die Verschlüsselung nicht mehr möglich.

8.1.2. Verteilung der Datenströme

Im ESP-Protokoll befindet sich der ESP-Header (Protokollnummer 50) zwischen dem neuen IP-Header und dem verschlüsselten Original TCP/IP Header. Normalerweise verwenden NAT-Router die Port-Nummern um den Datenverkehr an einzelne Hosts zuweisen zu können. Da der TCP-Header aber verschlüsselt ist kann diese Information nicht verwendet werden. Der ESP-Haeder bietet dafür keinen Ersatz. Siehe dazu auch Abbildung 5 ESP Packet (Tunnel Modus).

8.1.3. IKE UDP Port-Mapping

Einige IPSec Implementationen benutzen den UDP Port 500 für die Kommunikation in beide Richtungen. NAT verändert den Absender-Port, was bei einigen Implementierungen zu Problemen führt.

8.1.4. NAT Timeout

Die Einträge in einer NAT-Tabelle werden nicht ewig aufbewahrt sondern besitzen eine Lebensdauer. Spätere IKE-Nachrichten können somit den Empfänger eventuell nicht mehr erreichen.

8.1.5. IKE beinhaltet IP Adressen

Bei der Main und Quick-Mode Aushandlung senden beide Parteien ihre IP-Adresse innerhalb eines IKE-Paketes. Da NAT die Adressen ändert stimmen die Adressen im IP-Header nicht mehr mit denen im IKE-Paket überein. Dies kann zum Verbindungsabbau führen.

8.2. Die Lösung: NAT-T

Um diese Probleme zu beheben wurden einige Änderungen nötig:

- UDP Encapsulation: Zwischen dem IP-Header und dem ESP-Header wird ein UDP Header mit den selben Portnummern wie beim IKE-Protokoll eingefügt.
- IKE Header: Der IPSec NAT-T IKE Header beinhaltet ein Feld um dem Empfänger mitzuteilen, ob es sich um ein ESP Packet oder ein IKE Packet handelt.
- NAT-Keepalive: Um NAT-Timeout zu verhindern wird von Zeit zu Zeit ein IKE-Paket mit nur einem Byte (0xFF) gesendet.
- Neue „Vendor ID“ im IKE Datenstrom: Beinhaltet einen allgemein bekannten Hash-Wert um dem Partner NAT-T Fähigkeit zu signalisieren.
- NAT-Discovery (NAT-D): Die beteiligten Partner schicken sich gegenseitig Pakete mit ihren IP-Adressen und Port-Nummern. Diese werden mit den Header-Informationen verglichen um herauszufinden, ob NAT-Router zwischen den Geräten stehen.
- Neue Encapsulation-Modes für ESP über UDP im Transport/Tunnel Modus: Im Quick-Mode wird ausgehandelt, ob das ESP-Protokoll über UDP versendet werden soll.
- NAT-OA (Original Address) Austausch (IKE): Die originale Adressen werden im Quck Mode ausgetauscht und für die Specherung der SAs verwendet.

Somit sind alle Probleme von IPSec über NAT mehr oder weniger gut gelösst. Eine Diskussion über Wirksamkeit und Sicherheitsaspekte würde den Rahmen dieser Arbeit bei weitem sprengen. Der interessierte Leser sei hier an das Quellenverzeichnis [9] verwiesen.

8.3. NAT-T unter Windows

Microsoft Windows Server 2003 und Windows XP Service Pack 2 unterstützen NAT-T bereits. Für Windows 2000 und Windows XP Service Pack 1 existiert unter der Knowledge Base ID „818043“ ein Update

Leider hat Microsoft aus Sicherheitsgründen beschlossen NAT-T in der Standardeinstellung auszuschalten. Deshalb ist folgender Registry-Eintrag nötig um die NAT-T Unterstützung wieder einzuschalten:

```
Windows Registry Editor Version 5.00


[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPSec
]
"AssumeUDPEncapsulationContextOnSendRule"=dword:00000002
```

9. Quellen / Links / Literatur

RFC 2401, Security Architecture for the Internet Protocol, http://www.faqs.org/rfcs/rfc2401.html

RFC 2402, IP Authentication Header, http://www.faqs.org/rfcs/rfc2402.html

RFC 2406, IP Encapsulating Security Payload (ESP), http://www.faqs.org/rfcs/rfc2406.html

RFC 2407, Internet IP s. Domain of Interpretation for ISAKMP, http://www.faqs.org/rfcs/rfc2407.html

RFC 2408, ISAKMP, http://www.faqs.org/rfcs/rfc2408.html

RFC 2409, The Internet Key Exchange (IKE), http://www.faqs.org/rfcs/rfc2409.html

RFC 3947, Negotiation of NAT-T in the IKE, http://www.faqs.org/rfcs/rfc3947.html

RFC 3948, UDP Encapsulation of IPSec ESP Packets, http://www.faqs.org/rfcs/rfc3948.html

The IPSec Working Group, http://www.ietf.org/html.charters/ipsec-charter.html

IPSec Howto, http://www.ipsec-howto.org/

Bericht von Bruce Schneier und Niels Ferguson, http://www.schneier.com/paper-ipsec.html

10. Abbildungsverzeichnis

11. Tabellenverzeichnis

12. Index