Vortragsbegleitendes Material zum Thema *Virtual Private Networks* von *Markus Dahms* und *Jan Tobias Mühlberg*, 15. April 2002.

# VPN: Virtual Private Networks
## - eine Einführung -

### 1. Motivation

VPN ermöglicht es Angehörigen einer Organisation von beliebigen Endgeräten im Internet auf das *private* Netzwerk der Organisation zuzugreifen. Der Zugriff auf das private Netz kann dabei nach strengen Sicherheitsanforderungen erfolgen. So können z.B. Authentifizierung und Verschlüsselung Datenintegrität und -sicherheit gewährleisten. Das Endgerät befindet sich bei der Nutzung von VPN *virtuell* im privaten Netz der Organisation.

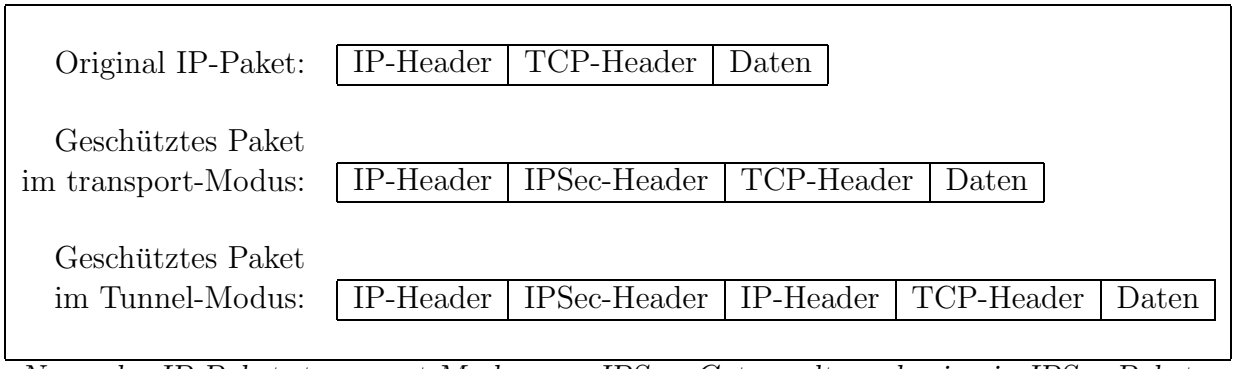
### 2. Technische Konzeption

Um dies zu realisieren werden *Tunnel*, also Möglichkeiten zur ungehinderten aber geschützten Durchquerung eines Hindernisses, hier des furchtbar unsicheren Internets, genutzt. Einen Tunnel zwischen zwei privaten Netzen, der ein unsicheres Netzwerk als Medium nutzt, kann man sich jedoch nicht als zusätzliche physikalische Verbindung vorstellen. Vielmehr werden zwischen zwei VPN-Gateways IP-Pakete ausgetauscht, deren Nutzlast wiederum aus IP-Paketen besteht, nämlich denen, die fuer das private Netzwerk bestimmt sind. Ein IP-Tunnel wird also durch Einkapselung (eng. *encapsulation*) der Pakete des privaten Netzes in die des öffentlichen realisiert. Die eingekapselten Packete können dabei nach Belieben verschlüsselt bzw. mit Mechanismen zur Echtheitsprüfung ausgestattet sein.
Erhält nun ein VPN-Gateway ein solches Paket von einem entfernten Bereich des privaten Netzes, packt es das, für das hinter ihm liegende, lokale private Netz bestimmte Paket aus und gibt es weiter. Analog wird verfahren, wenn ein Paket an einen entfernten privaten Netzbereich gesendet werden soll.
Der übliche Mechanismus zur Realisierung von Tunneln mit oder ohne Verschlüsselung und Authentifizierung heißt *IPSec* (für IP Security). Das Dokument zur Archikektur von IPSec (*RFC 2401*) definiert eine Basisarchitektur,

auf die alle Implementationen aufbauen. Es definiert, welche Sicherheitsdienste bereitgestellt werden, beschreibt, wie und wo sie benutzt werden können, wie Pakete erzeugt und weiterverarbeitet werden und erläutert die Wechselwirkungen bei der Verarbeitung nach IPSec mit einer bestimmten Anwendungsstrategie.

## 3. IPSec

IPSec lässt sich im Wesentlichen in die zwei Protokolle ESP (*Encapsulating Security Payload*) und AH (*Authentication Header*) unterteilen. Beide können dazu benutzt werden, sowohl eine komplette IP-Übertragung als auch nur die übergeordneten Protokolle zu schützen. Dazu werden zwei verschiedene Modi, der *transport-Modus* und der *Tunnel-Modus* unterstützt. Der transport-Modus wird benutzt, um übergeordnete Protokollschichten zu schützen, der Tunnel-Modus ist für komplette IP-Datagramme zuständig.




*Normales IP-Paket; transport-Modus von IPSec; Getunneltes, also in ein IPSec-Paket eingekapseltes IP-Paket*

Um IPSec-Pakete ordnungsgemäß erzeugen und interpretieren zu können, ist es notwendig, Sicherheitsdienste mit einem Schlüssel und evtl. weiteren zusätzlichen Parametern assoziieren zu können. Hierfür werden alle Parameter, die eine sichere Verbindung zu einem entfernten Rechner bzw. Subnetz charakterisieren in einer *Sicherheitsassoziation* (SA, *security association*) zusammengefasst. Üblicherweise definiert eine SA vor allem welcher IP-Verkehr geschützt wird, sowie wie und mit wem der Schutz durchgeführt wird. Meistens nutzt man für eine Verbindung ein Paar von SAs - eine SA für den Verkehr vom eigenen Gateway zu einem entfernten Bereich des privaten Netzes, eine weitere für die Rückrichtung.

Sicherheitsassoziationen werden, je nach Implementation, in einer kernelinternen Datenbank (SADB, *security association database*) abgelegt und werden über eine eindeutige Nummer (SPI, *security parameter index*) angesprochen. Leistungsstarke Betriebssysteme stellen zum Zugriff auf die SADB eine Schnittstelle namens PF_KEY (siehe RFC 2967) und eine dazugehörige API bereit.
Wenn eine SA manuell erzeugt wird, hat sie keine festgelegte Lebensdauer. Sie existiert so lange, bis sie manuell gelöscht wird. Wenn sie dynamisch erzeugt wird, kann ihr eine Lebensdauer zugeordnet werden. Dies geschieht je nach Konfiguration der für die Schlüsselaushandlung verwendeten Software. Die Lebensdauer kann sich dabei sowohl auf einen tatsächlichen Zeitraum aber auch z.B. auf die Menge des zu verschlüsselnden IP-Verkehrs beziehen. Ist die Lebensdauer einer SA abgelaufen, müssen die Verbindungspartner eine Neue aushandeln.
Dynamische SA-Erzeugung funktioniert mittels ISAKMP (*Internet Security Association and Key Management Protocol*) und IKE (*Internet Key Exchange*) und wird in den RFCs 2408 und 2409 beschrieben. Beide sind eine Erfindung der NSA.

### 3.1. ESP

ESP ist das IPSec-Protokoll, das für Vertraulichkeit, Datenintegrität und die Authentifizierung der Datenquellen von IP-Paketen sorgt. Es schützt außerdem davor, daß ein Angreifer IP-Pakete wiederholt sendet. Dies geschieht, indem ein neuer Header, ein ESP-Header, eingefügt wird. Dieser steht hinter dem IP-Header und vor den Daten, die geschützt werden sollen. Bei diesen Daten kann es sich entweder um ein übergeordnetes Protokoll oder um ein vollständiges, eingekapseltes IP-Paket handeln. Zusätzlich wird ein ESP-Trailer am Ende des Paketes angehangen.
ESP ist ein IP-Protokoll und wird durch den Wert des Protokollfeldes im IP-Header identifiziert. Der direkt darauf folgende Header ist ein ESP-Header. ESP wird im RFC 2406 spezifiziert.
Da ESP sowohl Authentifikation als auch Verschlüsselung zulässt, werden in seinen SAs mehrere Algorithmen parametrisiert. So hat jede ESP-SA zumindest einen *Authentificator* und einen *Cipher*. Es ist jedoch möglich, einen NULL-Cipher bzw. einen NULL-Authentificator zu definieren. Es ist jedoch verboten, beide auf NULL zu setzen, dies würde nicht nur das System unnötig belasten sondern auch keine Sicherheit bieten.
Zur Identifikation der verwendeten SA enthält ein ESP-Header die zugehörige SPI.

### 3.2. AH

AH wird in RFC 2402 spezifiziert. Mit Ausnahme der Vertraulichkeit bietet AH die gleichen Möglichkeiten zum Schutz von IP-Paketen wie ESP.
Vorallem durch das Fehlen der Verschlüsselung und damit verbundene Parameter, ist der AH-Header wesentlich einfacher aufgebaut und kleiner dimensioniert als in ESP. Einen Trailer gibt es nicht.

### 3.3. Algorithmen

Zur Verschlüsselung werden von IPSec viele verschiedene symetrische Verschlüsselungsverfahren wie DES, 3DES oder AES (siehe RFCs 2405, 3217) unterstützt. Allerdings müssen diese im CBC-Modus (*Cipher Block Chaining*) arbeiten. Die verfügbaren Schnittstellen erlauben auch die Implementation und Einbindung weiterer, auch proprietärer Algorithmen.
Änlich verhält es sich mit den Verfahren zur Authentifikation. Hierbei werden Algorithmen zur Erzeugung von MACs (*Message Authentification Codes*), also Verfahren, die verschlüsselte Prüfsummen (engl. *keyed hashing*) erzeugen, verwendet. Üblich sind z.B. MD5 und SHA (siehe RFCs 2202, 2403, 2404).
In IPSec wird häufig eine besondere Form des MAC, der HMAC nach RFC 2104, verwendet. Der HMAC ist kryptographisch stärker als der darunter liegende Hash-Algorithmus und ist universell einsetzbar.