# Virtuelle Private Netze für das Internet

Dipl. Inf. Manuel Günter
Institut für Informatik und angewandte Mathematik (IAM) der Universität Bern
Mguenter@iam.unibe.ch

Neue Internet Technologien erlauben es Firmen, das Internet als Erweiterung ihres privaten Netzes zu Nutzen. Sogenannte virtuelle private Netze (VPN) sind ein weiterer Schritt in der Entwicklung des Internets zur sicheren und kostengünstigen Universal-Kommunikationsplattform.

Das ungebrochene Wachstum des Internets zieht einschneidende Änderung in der Kommunikations-Infrastruktur von Firmen nach sich. Neben der obligatorischen World Wide Web Präsenz, elektronischer Post und anderen Internet Anwendungen wird auch die Internet Protokoll Suite als Ganzes eingesetzt, um Firmen-interne Netze zu implementieren. Diese geschlossenen „Mini-Internets" werden auch Intranets genannt, und profitieren von der Stabilität und Skalierbarkeit des Internet Protokolls sowie von den vielfältigen Internet Anwendungen. Traditionelle Intranets sind nicht über öffentliche Trägernetze verbunden. Sie laufen auf Firmen-eigener Infrastruktur oder über gemietete Standleitungen. Die Abkapselung von Intranets von öffentlichen Netzen (allenfalls durch eine Firewall[1]) trägt einem grossen Nachteil der Internet Protokoll Suite Rechnung: dem Mangel an Sicherheit. Die meisten der geläufigen Internet Protokolle sind nämlich äusserst einfach abzuhören und böswillig zu manipulieren. Der Einsatz von Standleitungen (X.25, Frame-Relay, ATM) birgt allerdings auch Nachteile. So ist es zum Beispiel ein langwieriger und administrativ aufwendiger Prozess eine neue Standleitung aufzusetzen. Ausserdem wird die Leitung während gewissen Zeiten einen Engpass bilden und während anderen kaum benutzt sein. Das grösste Problem jedoch ist der Preis. Üblicherweise sind Standleitungen teuer, wobei der Preis zudem abhängig von der Länge der Verbindung ist. Ausserdem erzeugen Standleitungen Kosten, ob sie nun ausgelastet sind, oder nicht. Schliesslich gewähren sie keine optimale Sicherheit; der Provider/Carrier kann immer mithören.
In den letzten zwei Jahren wurde eine Alternative zu den Standleitungs-basierten Firmennetzen populär: Virtuelle Private Netze (VPN) [1]. Ein Internet-VPN präsentiert sich dem Benutzer wie ein Intranet. Jedoch wird Verkehr für Intranet Sites, welche nicht am lokalen Netz hängen, über das Internet übertragen. Ein spezieller Mechanismus garantiert, dass VPN Verkehr in sicherer und transparenter Weise das Internet bereist. Der vorliegende Artikel erläutert die Grundprinzipien von VPNs sowie die Anwendungsgebiete. Spezielles Gewicht wird auf die Sicherheits-Architektur des Internet Protokolls (IPSec) gelegt. Dieses neue Internet Protokoll standardisiert den Einsatz von Kryptographie und sogenannten *Tunneln* beim Errichten von virtuellen privaten Netzen auf Internet-Basis.

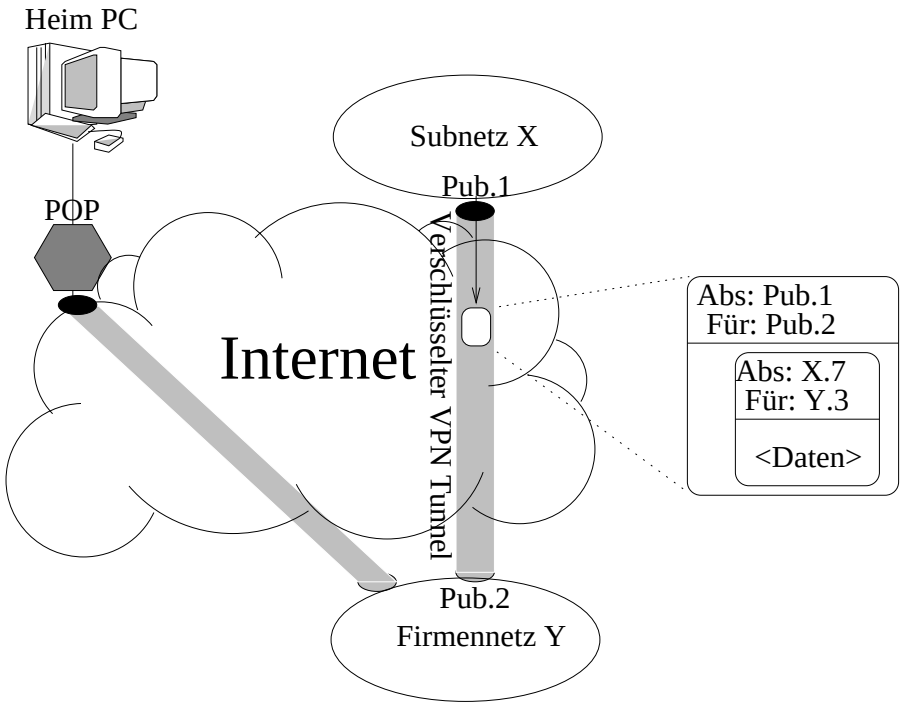
## *Tunneln und Kryptographie – VPN Grundbausteine*

### VPN Tunnel

Ein Tunnel, auch Paket-Einkapselung genannt, ist eine Art Überbrückungsverbindung über mehrere fremde Stationen hinweg. Jede Internet Applikation verschickt ihren Verkehr in Internet Paketen gemäss dem IP Protokoll. Diese Pakete beinhalten die Adressen der Sender und Empfänger Rechner. Dazwischen liegende Rechner geben die Pakete in Richtung Zieladresse weiter. Intranets verwenden nun typischerweise private Adressen, d.h. Adressen, die den Internet Routern nicht bekannt sind, und somit auch nicht weitergereicht werden können. Dieses Problem wir nun mit Tunneln gelöst (siehe Abbildung 1). Am Tunneleingang wir das Intranet Paket für eine nicht-lokale, private Adresse (Y.3) in ein Paket mit der öffentlichen Adresse des entfernten Tunnelendpunkts (Pub.2) verpackt. Dieses wird sodann über das Internet bis zum Tunnelendpunkt weitergereicht, wo das Originalpaket wieder entnommen und im lokalen Netz weiter versandt wird. Dieses vereinfacht dargestellte Prinzip wird schon seit langem angewandt, wenn Pakete über Netze mit anderen Protokollen verschickt werden müssen (z.B. IPX über IP). Für VPNs schafft das tunneln Transparenz, denn der Transit durch das Internets bleibt den Anwendungen verborgen. Für VPNs gibt es nun zwei grundsätzlich verschiedene Arten von Tunnels.
Um dies darzustellen, müssen wir uns näher mit der Internet Protokoll-Suite auseinandersetzen. Diese ist in fünf Schichten aufgeteil. Eine physikalische Schicht (z.B. Glasfaser Kabel) überträgt die Datensignale, welche von einer Sicherungsschicht in eine Null-Eins Folge übersetzt werden. Die Vermittlungsschicht (auch Internet Schicht genannt, durch das IP Protokoll implementiert) ist nun zuständig für die Vermittlung von Datenpaketen durch das Netzwerk. Die korrekte und geordnete Ankunft der Pakete wird durch die Transportschicht gewährleistet (TCP Protokoll). Schliesslich definieren eine Vielzahl von Anwendungsprotokollen Form und Gehalt von Nutzdaten. Das Internet benutzt viele unterschiedliche physikalische Schichten und Sicherungsschichten um die IP Pakete zu übertragen. Es kann nun bereits auf diesen unteren Schichten getunnelt werden. Beispielsweise ist es möglich, die Tunnel-Endpunkte mit permanenten virtuellen ATM Kanälen zu verbinden und private IP Pakete über diese zu verschicken. Derartig konstruierte Netzwerke werden auch *Sicherungsschicht (Link Layer)*

[1] Firewall: Paket filternder Rechner am Zugang zu einem fremden Netz.

*VPNs* genannt. Sie bringen jedoch die genau gleichen Nachteile wie Standleitungs-basierte Intranets, daher sind sie vom gegenwärtigen VPN Trend weniger betroffen und werden in diesem Artikel auch nicht näher diskutiert. *Internet VPNs*, wie wir sie in diesem Artikel behandeln, basieren auf IP Tunneln. IP Tunnels verschicken private IP Pakete abgepackt in öffentlichen IP Paketen. Da das IP Protokoll der gemeinsame Nenner von allen ans Internet angeschlossenen Netzen ist, kann eine auf IP basierende VPN Technik (im Gegensatz zu Sicherungsschicht VPNs) problemlos auf dem ganzen Internet angewandt werden.




## Kryptographische Bausteine

Das Tunneln schleust zwar den VPN Verkehr durch das öffentliche Internet, es sorgt aber in keiner Weise für mehr Sicherheit. Gewünscht ist eine vertrauenswürdige und vertrauliche Kommunikation. Kein Internet Benutzer und keine öffentliche Netzwerkkomponente soll in der Lage sein, VPN Datenverkehr auszuspionieren, unbemerkt zu verändern oder zu erzeugen. Das Mittel um diese Sicherheit zu erreichen ist Kryptographie. Es gibt drei verschiedene Typen von kryptographischen Mechanismen*: Symmetrische Verschlüsselung*, *asymmetrische Verschlüsselung* (mit öffentlichem und privatem Schlüssel) sowie sichere *Einwegfunktionen*.

- Symmetrische Verschlüsselungsverfahren setzten voraus, dass die Kommunikationspartner über einen gemeinsamen Geheimschlüssel verfügen. Das Verfahren kodiert Daten in Abhängigkeit des Schlüssels. Gute Verfahren bieten als einzige Angriffsfläche die vollständige Suche durch den Schlüsselraum. Das heisst ein Angreifer muss alle möglichen Schlüssel durchprobieren, um an den Inhalt einer Nachricht zu gelangen. Bei empfohlenen Schlüssellängen von 128 Bits ist dies ein hoffnungsloses Unterfangen (auch wenn eine Million Rechner je eine Milliarde Entschlüsselungsversuche pro Sekunde lancieren, wird die durchschnittliche Suchzeit immer noch über fünf Billiarden Jahre betragen). Symmetrische Verschlüsselung ist in der Regel schnell, insbesondere wenn das Verfahren für Hardware optimiert, oder gar in Hardware implementiert ist. Nachteil der symmetrischen Verfahren ist, dass zuerst ein gemeinsamer, geheimer Schlüssel etabliert werden muss. Beispiele für symmetrische Verfahren sind: DES, IDEA, Blowfish, SEAL uvm.
- Asymmetrische Verschlüsselungsverfahren benutzen ein Schlüsselpaar pro Kommunikationsteilnehmer. Das Paar beinhaltet einen öffentlichen und einen privaten Schlüssel. Der öffentliche Schlüssel eines Teilnehmers ist allen anderen Teilnehmern bekannt. Der private Schlüssel behält jeder Teilnehmer für sich. Das besondere eines Schlüsselpaares ist nun, dass sich eine Verschlüsselung mit dem einen Schlüssel nur mit dem anderen Schlüssel dechiffrieren lässt. Dies erlaubt zwei unterschiedliche Anwendungen: will Alice eine Nachricht an Bob verschlüsselt verschicken, so verwendet sie den öffentlichen Schlüssel von Bob. Damit ist sichergestellt, dass nur Bob die Nachricht entschlüsseln kann, denn nur er hat den zugehörigen privaten Schlüssel. Will hingegen Alice öffentlich sicherstellen, dass sie es war, die eine Nachricht verfasst hat, so kodiert sie diese mit ihrem privaten Schlüssel. Jedermann kann nun mit Alices öffentlichem Schlüssel die kodierte Nachricht entschlüsseln. Aus der Tatsache das die Entschlüsselung klappt, kann man schliessen, dass Alice die Nachricht verfasst haben muss. Heutige asymmetrische Verfahren wie

RSA, und ElGamal beruhen auf gründlich analysierten mathematischen Problemen. Sie bieten eine sehr hohe Sicherheit, allerdings sind sie in der Regel viel langsamer als die symmetrischen Verfahren.

- Sichere Einwegfunktionen (auch sichere Hashfunktionen genannt) berechnen eine Art Prüfsumme aus einer Nachricht und allenfalls einem Schlüssel. Eine Einwegfunktion gilt als sicher, wenn es nahezu unmöglich ist, aus der Prüfsumme die Nachricht zu rekonstruieren, oder auch nur zwei Nachrichten zu konstruieren, die dieselbe Prüfsumme ergeben.

Aus diesen drei kryptographischen Grundkomponenten lassen sich nun mächtige Protokolle konstruieren. Als kleines Beispiel sei hier die digitale Unterschrift angeführt. Will Alice ein Dokument unterzeichnen, so berechnet sie darüber eine Prüfsumme mittels einer sicheren Einwegfunktion. Diese Prüfsumme verschlüsselt sie nun mit ihrem privaten Schlüssel und fügt das Resultat als digitale Unterschrift dem Dokument an. Da Alices öffentlicher Schlüssel jedermann bekannt ist, kann die Signatur leicht überprüft werden. Es ist jedoch unmöglich, das Dokument zu ändern, ohne dabei die Unterschrift zu entwerten.

## *Anwendungsszenarien von Internet VPNs*

Mit Tunneln und kryptographischen Mechanismen können wir nun verschiedenartige VPNs realisieren. Wir unterscheiden zwei Szenarien: der Anschluss eines ganzen Subnetzes an ein VPN oder der Anschluss einer einzelnen Maschine (siehe Abbildung 1). Werden Subnetze verbunden, so spricht man von einem Netz-zu-Netz oder auch „Branch-office“ VPN. Der typische Anwendungsfall ist die Netzwerk-Anbindung einer kleinen Zweigstelle, welche sich ausserhalb der Reichweite des Firmen-Hauptquartiers befindet. In diesem Szenario wird ein Tunnel zwischen den Subnetzen etabliert, welcher eine transparente Verbindung für alle Rechner des Subnetzes stellt. Dies ist ein weit verbreitetes und einfaches VPN Szenario. Nur die Rechner, die Tunnelendpunkte aufsetzen, müssen VPN spezifische Arbeiten ausführen. Die anderen Rechner benötigen keine zusätzlichen Installationen oder Konfigurationen. Erwähnenswert ist ein anspruchsvoller Netz-zu-Netz Spezialfall: Beim sogenannten „Extranet VPN“ werden Netze von verschiedenen Firmen für projektbezogene Kollaboration verbunden. Hier braucht es zusätzliche, Firewall-ähnliche Mechanismen, welche die Zugriffsrechte der Teilnehmer gegenseitig einschränken. In der Regel will ja eine Firma auch ihrem Partner nicht alle Geheimnisse eröffnen.
Im zweiten VPN Szenario geht es darum, einzelne Aussenmitarbeiter mit dem Heimnetz zu verbinden. In diesem Fall spricht man von einem „Remote Access VPN“. Sie erlauben den Anwendern von zuhause aus oder unterwegs das Firmennetz zu nutzen, ohne Sicherheitsprobleme zu befürchten. Die Anwender wählen sich dazu üblicherweise in einen Internet Service Provider ein. Dabei wird meist das Punkt-zu-Punkt Protokoll (PPP) verwendet. Die PPP Pakete werden nun über einen VPN Tunnel ins Firmennetz gespiesen. Dabei unterscheidet man zwischen „freiwilligem“ und „unfreiwilligem“ Tunneln. Die freiwilligen Tunnel werden durch die Benutzermaschine (Laptop oder Heim-PC) erstellt. Ein Beispiel eines solchen Protokolls ist das Point-to-Point Tunneling Protokoll (PPTP). Unfreiwillige Tunnel werden vom Internet Service Provider basierend auf der anrufenden Telefonnummer automatisch erstellt. Beispiel eines solchen Protokolls ist das Layer Two Tunneling Protokoll (L2TP). Aus Platzgründen kann an dieser Stelle auf PPTP und L2TP nicht näher eingegangen werden. Erwähnenswert ist jedoch, dass beide Protokolle trotz Verschlüsselungsoptionen Sicherheitslücken aufweisen. Für sichere VPNs kombiniert man sie am besten mit einem auf Sicherheit spezialisierten Protokoll wie IPSec.

## *Die Sicherheits-Architektur für das Internet Protokoll: IPSec*

Die Internet Technologie wurde ursprünglich entwickelt, um verschiedene heterogene Teilnetze untereinander zu verbinden. Daher wurde wenig auf die Sicherheit des Protokolls geachtet, denn es ging in der ersten Linie darum, Kommunikation zuzulassen, und nicht sie zu unterbinden. Die schwerwiegenden Sicherheitsmängel blieben bis zur heutigen Version 4 des Internet Protokolls (IPv4) bestehen. Die IETF wollte mit der Entwicklung des neuen Internet Protokolls IPv6 nicht nur die Adressknappheit beenden, sondern auch rigorose Sicherheitsmechanismen ins Protokoll einbinden. Zwar hat sich IPv6 bis heute nicht durchsetzen können, aber die Sicherheitsarchitektur die eigentlich für IPv6 entwickelt worden war, lässt sich als Protokollerweiterung auch auf die gegenwärtige Version anwenden. Die IETF standardisierte sie 1998 in [2] unter dem Namen “Security Architecture for the Internet Protocol”, oder kurz IPSec.
IPSec ist eigentlich nicht ein einzelnes Protokoll und schon gar kein Verschlüsselungsalgorithmus, sondern eine Protokollfamilie. Im wesentlichen fügt IPSec jedem IP Paket zwischen dem Paketkopf und den Paketdaten in noch näher zu beschreibender Weise Sicherheitsinformationen ein. Diese Informationen gliedern sich in zwei Protokoll-Typen. Zum einen ist da der Authentication Header (AH), welcher die Integrität des Pakets gewährleistet, und zum anderen die Encapsulation Security Payload (ESP), welcher die Verschlüsselung der Nutzdaten beschreibt. Sowohl AH wie auch ESP sind eigenständige Protokolle, die separat voneinander oder kombiniert eingesetzt werden können. Beide kennen einen Tunnel Modus, der sogar mehrfache Verschachtelung von AH und ESP erlaubt. Während im Transport Modus AH oder ESP einfach einem Einschub von zusätzlichen Protokollfelder in den IP Header gleichkommt, wird im Tunnel Modus ein komplett neues IP Paket erzeugt, in dessen Nutzdaten nun die Sicherheitsinformationen, sowie das gesamte (bei ESP verschlüsselte) Original-Paket geschrieben wird. Interessant ist ferner, dass AH und ESP unabhängig von konkreten kryptographischen Algorithmen arbeiten. Zwar setzt AH eine sichere Einwegfunktion voraus, mit deren Hilfe die Integrität

eines Pakets überprüft wird. Welche Funktion dies aber ist, wird nicht näher festgelegt. Ausnahme sind zwei Default Hash-Funktionen (MD5 und SHA), die vorhanden sein müssen um die Interoperabilität zu gewährleisten. Analog verhält sich auch ESP. Während im Minimum DES zur Verschlüsselung vorhanden sein muss, kann IPSec auch die Verwendung von andere Algorithmen aushandeln.
AH und ESP gehen beide vom Vorhandensein eines nur den beiden Endsystemen bekannten Geheimschlüssels aus. Wenn nun ein solcher nicht bereits manuell installiert wurde, so muss er auf sichere Art erzeugt werden. Dieser hochkomplexe Vorgang ist mit dem Internet Key Exchange (IKE) Protokoll in IPSec eingebunden.

IPSec fähige Rechner enthalten eine Reihe von Komponenten, die den Einsatz der Protokolle AH und ESP steuern. Die Security Policy Database enthält Regeln, die bestimmen, ob einkommender oder ausgehender Verkehr IPSec Verarbeitung unterzogen werden soll, ob er unverändert weitergeleitet werden darf, oder ob er verworfen werden muss. Sogenannte Security Associations (SA) repräsentieren 'offene' IPSec Verbindungen. Sie beschreiben genau eine IPSec Transformation, und enthalten die dafür nötigen Angaben. Diese umfassen den IPSec Prokokoll-Typ (AH oder ESP), den Modus (Tunnel oder Transport), sowie verwendete Algorithmen und Schlüssel. Wichtig ist ferner der Security Parameter Index (SPI), welcher die SA identifiziert. Der SPI wird auf der Senderseite in die transformierten Pakete geschrieben und auf der Empfängerseite gelesen. Somit können verschiedene SA auf einem Rechner installiert und sogar miteinander verknüpft werden. Dies erlaubt die verschachtelte Anwendung der IPSec Transformationen.
Im folgenden betrachten wir den Aufbau von AH und ESP, und welche Sicherheiten sie bieten.

## Authentication Header (AH)

Wie bereits erwähnt enthält der Authentication Header einen Security Parameter Index (SPI), sowie eine Paket-Laufnummer. Kern des Authentication Header ist eine Prüfsumme, die mit einer sicheren Einwegfunktion berechnet wird. Die Prüfsumme umfasst das gesamte IP Paket und einen geheimen Schlüssel. Insbesondere wird auch der Paketkopf, welcher unter anderem Sender- und Empfängeradresse enthält in die Berechnung mit einbezogen. Einzige Ausnahme sind die als veränderlich definierten IP Protokollfelder (TOS und TTL). Die Prüfsumme garantiert nun, dass ein Angreifer das Paket nicht verändern (oder gar erzeugen) kann, ohne dass der Empfänger dies nicht an der Prüfsumme bemerken könnte. Der Angreifer kann diese nämlich ohne die Kenntnis des geheimen Schlüssels nicht selber berechnen.
AH überprüft somit die Integrität der Kommunikation paketweise und garantiert damit unter anderem auch, dass der Absender nicht gefälscht werden kann (Authentizität des Pakets).

## Encapsulated Security Payload (ESP)

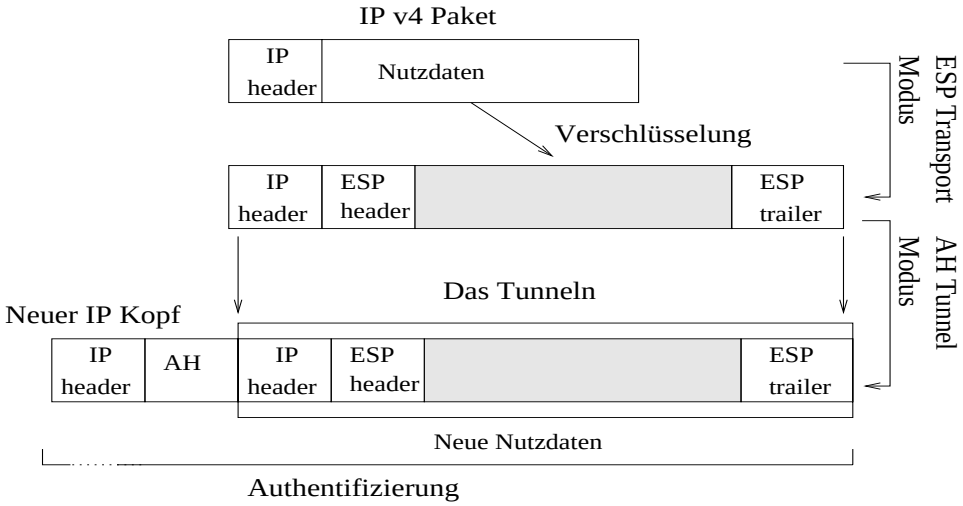
Die Encapsulated Security Payload dient hauptsächlich zur Sicherung der Vertraulichkeit der Kommunikation, und zwar mittels Verschlüsselung der Nutzdaten. ESP fügt ebenfalls einen neuen Header nach dem IP Kopf ein, der wieder den SPI und eine Laufnummer enthält. Ausserdem hängt ESP aber auch noch einen Trailer an die Nutzdaten, welcher ebenfalls verschlüsselt wird. Der Trailer dient dazu, die Nutzdaten aufzufüllen, was die Paketlänge vereinheitlicht. Dies ist für einige Verschlüsselungsarten nötig und kann helfen, den Typ der Nutzdaten zu verschleiern. Dieser könnte nämlich aufgrund der Paketlänge erraten werden, da verschiedene Anwendungsprotokolle charakteristische Paketlängen aufweisen. ESP kann die Integrität der Nutzdaten mit einem optionalen Authentifizierungs-Trailer schützen. Das Prinzip ist hierbei dasselbe wie bei AH, nur dass ESP den IP Paketkopf nicht mit einbezieht. Somit könnte zum Beispiel die Sender Adresse des Pakets unbemerkt verändert werden. ESP bietet zwar mit Verschlüsselung und Authentifikation mehr Funktionalität als AH, kann AH aber nicht komplett ersetzen.

## Internet Key Exchange (IKE)

Wie bereits erwähnt sind AH und ESP unabhängig von konkreten kryptographischen Algorithmen. Natürlich müssen sich aber zwei über IPSec kommunizierende Rechner in der Wahl der Algorithmen einig sein. Ausserdem setzen sowohl AH als auch ESP das Vorhandensein von geheimem, beiden Seiten bekanntem Schlüsselmaterial voraus. Das Internet Key Exchange Protokoll schafft nun genau diese Voraussetzungen. Ausgehend von entweder manuell konfigurierter 'Urschlüssel', oder asymmetrischer Schlüssel, oder auch von X.509 Zertifikaten können zwei Rechner automatisch und auf sichere Weise Schlüsselmaterial sowohl generieren wie auch regelmässig erneuern. Ferner erlaubt IKE die automatische Konfiguration von Security Associations. Das heisst, mit IKE können IPSec Verbindungen und Tunnels automatisch errichtet werden.
IKE ist die mit Abstand komplizierteste Komponente von IPSec. Die Standardisierung von IKE hat sich deswegen auch verzögert, so dass viele der heutigen IPSec Implementationen nur eine Teilfunktionalität von IKE umfassen. Wenn daher IPSec Programme verschiedener Hersteller nicht kompatibel sind, so liegt dies meist an IKE.

## Erstellen von Internet VPNs mit IPSec

IPSec unterstützt mit der Verschachtelung von AH, ESP und jeweils zwei Modi eine Fülle von verschiedenen Anwendungsszenarien. Wir wollen uns hier auf zwei mögliche Lösungen für die VPN Anwendungs-Szenarien beschränken, die bereits vorgestellt wurden. Falls ein Subnetz mit dem VPN verbunden werden soll, so wird auf dem der Internet-Router des Subnetz (in der IPSec Terminologie auch „Security Gateway" genannt) mindestens ein (logisches) IPSec Interface konfiguriert. Dieses tunnelt beispielsweise sämtlichen Verkehr von den lokalen privaten Adressen mit ESP (im Tunnel Modus). Dabei wird oft mit der Aktivierung der optionalen Authentifizierung von ESP der Einsatz von AH vermieden. In diesem Szenario kann die aufwendige Verschlüsselungsarbeit in die spezialisierte Hardware des Security Gateways ausgelagert werden.
Im Falle einer einzelnen Maschine (Laptop oder Heim-PC), die sich ins VPN einwählen können muss, wird oft ein AH Tunnel zum Security Gateway geöffnet. Verschachtelt darin wird dann ESP im Transportmodus verwendet. Dabei wird ESP nicht vom Security Gateway betrieben, sondern vom Sender bis zum Empfänger (Ende-zu-Ende Sicherheit). Diese Verschachtelung von AH und ESP ist in Abbildung 2 dargestellt. Wie bereits früher erwähnt, kann IPSec bei Remote Access VPNs mit anderen Protokollen (L2TP) kombiniert werden, um beispielsweise das fremd-initiierte Tunneln oder Benutzer-basierte Authentifikation zu unterstützen.




### *Angebot und Ausblicke*

Der Internet VPN Technologie wird eine rasante Marktentwicklung vorausgesagt. Das dominierende Protokoll ist heute IPSec, dank seiner Vielfältigkeit, seinem seriösen Sicherheitsdesign und der frühen und offenen Standardisierung. Viele Router Hersteller, Betriebssystem Anbieter sowie Firewall- und Security Softwareentwickler haben IPSec basierte VPN Lösungen im Angebot. Es gibt auch freie Implementationen für Linux [3] und OpenBSD. Internet Service Provider bemühen sich um den Zukunftsmarkt des VPN Outsourcing. Für diesen rechnen die Provider besonders im Bereich Remote Access VPNs mit traumhaften Wachstumsraten, denn solche VPNs sind für gewöhnliche Firmen schwer zu verwalten. Genau in diesen Bereich fällt auch die aktuelle VPN Forschung an der Universität Bern [4], wo mit benutzerfreundlicher Software Netzwerk-weite Sicherheits- und Dienstgütenbestimmungen durch automatische Konfiguration der Netzwerk Komponenten forciert wird.

### *Informationen im WWW*


§ [1] Tina Bird, „VPN Info on the World Wide Web", http://kubarb.phsx.ukans.edu/~tbird/vpn.html
§ [2] Internet Engineering Task Force, „Security Architecture for the Internet Protocol", Request for Comments (RFC) 2401-2409, http://www.ietf.org/rfc.html
§ [3] Secure Wide Area Network Project, „Linux FreeS/Wan", http://www.xs4all.nl/~freeswan/
§ [4] Manuel Günter, „Virtual Private Network Configuration", http://www.iam.unibe.ch/~rvs/cati/


### *Übersetzungstext*

Neue Internet Technologien erlauben es Firmen, das Internet als Erweiterung ihres
privaten Netzes zu Nutzen. Sogenannte virtuelle private Netze (VPN) sind ein weiterer Schritt in der Entwicklung des Internets zur sicheren und kostengünstigen Universal-Kommunikationsplattform.

Mithilfe von Protokoll-Tunneln und Kryptogaphie verbindet das Internet auf sichere Weise die Teilnehmer des virtuellen privaten Netzes. Werden auf diese Weise zwei Subnetze verbunden, so spricht man von einem Netz-zu-Netz oder auch „Branch-office“ VPN. Der typische Anwendungsfall ist die Netzwerk-Anbindung einer kleinen Zweigstelle, welche sich ausserhalb der Reichweite des Firmen-Hauptquartiers befindet. Geht es darum, Aussenmitarbeiter mit dem Heimnetz zu verbinden, so spricht man von einem „Remote Access VPN“. Beim sogenannte „Extranet VPN“ werden verschiedene Firmennetze für projektbezogene Kollaboration verbunden, wobei aber die Zugriffsrechte gegenseitig eingeschränkt werden. Das von der Internet Engineering Task Force entwickelte IPSec Protokoll unterstützt alle diese Anwendungsszenarien und setzt sich bei den Herstellern und Kunden durch. Der vorliegende Artikel gibt einen Einblick in die Grundbausteine von IPSec, und erläutert, wie diese für VPN Lösungen eingesetzt werden.

## *Bildlegenden*

1. VPN Szenarien mit Tunnel.
2. Verschachtelte Anwendung von IPSec.