Virtuelle Private Netze für das Internet

Autor(en): **Günter, Manuel**

Objekttyp: **Article**

Zeitschrift: **Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses**

Band (Jahr): **91 (2000)**

Heft 7

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-855536

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Virtuelle Private Netze für das Internet

Neue Internettechnologien 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 Änderungen in der Kommunikationsinfrastruktur von Firmen nach sich. Neben der obligatorischen World-Wide-Web-Präsenz, elektronischer Post und anderen Internetanwendungen wird die Internet-Protokoll-Suite als Ganzes auch eingesetzt, um firmeninterne Netze zu implementieren. Diese geschlossenen «Mini-Internets» werden auch Intranets genannt. Sie profitieren von der Stabilität und der Skalierbarkeit des Internetprotokolls sowie von den vielfältigen Internetanwendungen. Traditionelle Intranets sind nicht über öffentliche Trägernetze verbunden. Sie laufen auf firmeneigener 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 Internetprotokolle sind nämlich äusserst einfach abzuhören und böswillig zu manipulieren. Umgekehrt birgt allerdings auch der Einsatz von Standleitungen (X.25, Frame-Relay, ATM) Nachteile. So ist es zum Beispiel ein langwieriger und administrativ aufwendiger Prozess, eine neue Standleitung aufzusetzen. Ausserdem wird die Leitung während gewisser 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 geographischen 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.

Adresse des Autors
Manuel Günter, Dipl. Inf., Institut für Informatik und angewandte Mathematik (IAM) der Universität Bern
Neubrückstrasse 10, 3012 Bern
Mguenter@iam.unibe.ch

In den letzten zwei Jahren wurde eine Alternative zu den standleitungsbasierten 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 VPN sowie die Anwendungsgebiete. Spezielles Gewicht wird auf die Sicherheitsarchitektur des Internetprotokolls IPSec gelegt. Dieses neue Internetprotokoll standardisiert den Einsatz von Kryptographie und sogenanntem Tunneln beim Errichten von virtuellen privaten Netzen auf Internetbasis.

VPN-Grundbausteine

VPN-Tunnel

Ein Tunnel, auch Paket-Einkapselung genannt, ist eine Art Überbrückungsverbindung über mehrere fremde Stationen hinweg. Jede Internetapplikation verschickt ihre Daten in Internetpaketen gemäss dem IP-Protokoll. Diese Pakete beinhalten die Adressen der Sender- und der Empfängerrechner. Dazwischen liegende Rechner geben die Pakete in Richtung Zieladresse weiter. Intranets verwenden nun typischerweise private Adressen, das heisst Adressen, die den Internet-Routern nicht bekannt sind und somit auch nicht weitergereicht werden können. Dieses Problem wird durch Tunneln gelöst (Bild 1). Am Tunneleingang wird das Intranetpaket für eine nichtlokale, private Adresse (Y.3) in ein Paket mit der öffentlichen Adresse (Pub. 2) des entfernten Tunnelendpunkts verpackt.

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

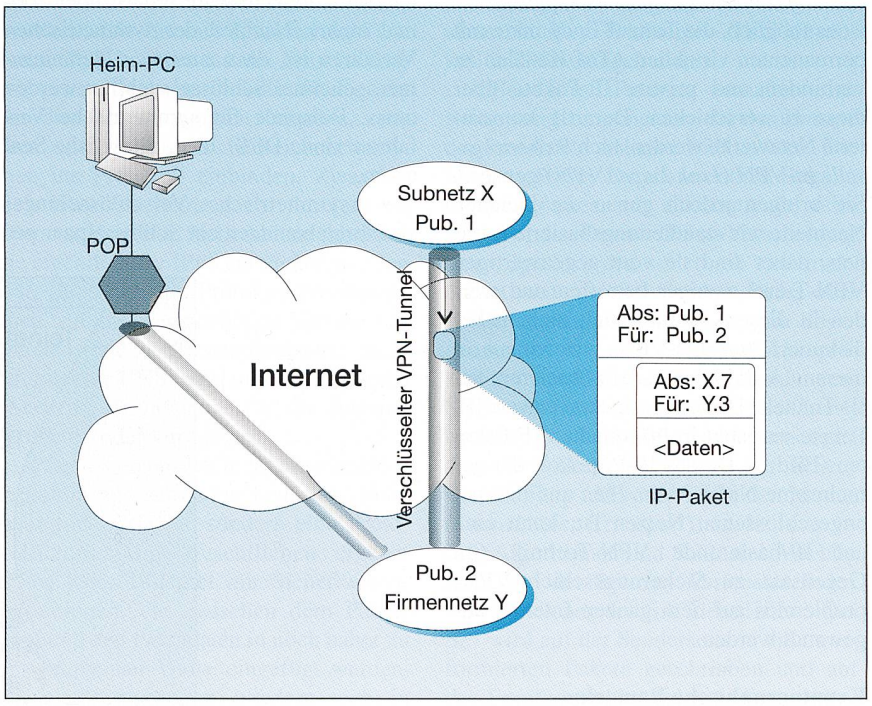

Bild 1 VPN-Szenarien mit Tunnel
Pub. 1 und Pub. 2 sind öffentliche IP-Adressen der Tunnel-Rechner (Gateways). Die Daten und die privaten Adressen (X.7, Y.3) können nur innerhalb der privaten Subnetze entschlüsselt werden.

Dieses wird sodann über das Internet bis zum Tunnelendpunkt weitergereicht, wo das Originalpaket wieder entnommen und im lokalen Netz weiterversandt 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 VPN schafft das Tunneln Transparenz, denn der Transit durch das Internet bleibt den Anwendungen verborgen. Der Datentransport funktioniert daher wie innerhalb eines echten privaten Netzes. Für VPN 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 aufgeteilt (Bild 2). Eine physikalische Schicht (z.B. Glasfaserkabel) 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 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. Bereits auf diesen unteren Schichten kann 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*-VPN *(Link Layer* VPN) genannt. Sie bringen jedoch genau die gleichen Nachteile wie standleitungsbasierte Intranets, daher sind sie vom gegenwärtigen VPN-Trend weniger betroffen und werden in diesem Artikel auch nicht näher diskutiert. *Internet*-VPN, wie wir sie in diesem Artikel behandeln, basieren auf IP-Tunnels. Diese verschicken private IP-Pakete verpackt in öffentlichen IP-Paketen (Bild 1). 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-VPN) 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 Internetbenutzer und keine öffentliche Netzwerkkomponente soll in der Lage sein, VPN-Datenverkehr auszuspionieren, unbemerkt zu verändern oder zu erzeugen. Dieses Ziel kann durch Kryptographie erreicht werden. Es gibt drei verschiedene Typen von kryptographischen Mechanismen: symmetrische Verschlüsselung, asymmetrische Verschlüsselung (mit öffentlichem und privatem Schlüssel) sowie sichere Einwegfunktionen.

- Symmetrische Verschlüsselungsverfahren setzen 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 Bit 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 (Software kann Daten mit bis zu 3 MBit/s verarbeiten, schnelle Hardware schafft über 200-mal mehr). Nachteil der symmetrischen Verfahren ist, dass zuerst ein gemeinsamer, geheimer Schlüssel etabliert werden muss. Beispiele für symmetrische Verfahren sind: DES, Idea, Blowfish, Seal u.v.m.
- 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. Den privaten 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, dass 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 Hash-Funktionen 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

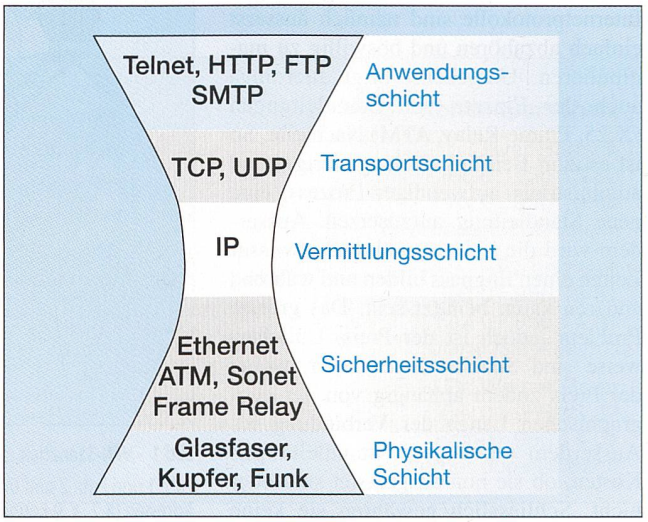

Bild 2 Die fünf Schichten des Internetprotokolls

kleines Beispiel sei hier die digitale Unterschrift angeführt. Dies geschieht mit Hilfe sicherer Einwegfunktionen, mit denen eine charakteristische Prüfsumme eines zu unterzeichnenden Dokuments berechnet werden kann. Will Alice ein Dokument unterschreiben, so berechnet sie zunächst die Prüfsumme, verschlüsselt diese Summe 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-VPN

Mit Tunneln und kryptographischen Mechanismen können wir nun verschiedenartige VPN realisieren. Wir unterscheiden zwei Szenarien: den Anschluss eines ganzen Subnetzes an ein VPN oder den Anschluss einer einzelnen Maschine (Bild 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 Firmenhauptsitzes befindet. In diesem Szenario wird ein Tunnel zwischen den Subnetzen etabliert, der 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 Firmennetz zu verbinden. In diesem Fall spricht man von «Remote Access VPN». Sie erlauben den Anwendern von zuhause aus oder unterwegs, das Firmennetz ohne Gefahren für die Sicherheit zu nutzen. Die Anwender wählen sich dazu üblicherweise über 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 gespeist. Dabei unterscheidet man zwischen selbstinitiiertem und fremdinitiiertem (auch «unfreiwillig» genanntem) Tunneln. Die selbstinitiierten Tunnel werden durch die Benutzermaschine (Laptop oder Heim-PC) erstellt. Ein Beispiel eines solchen Protokolls ist das Point-to-Point-Tunneling-Protokoll (PPTP). Fremdinitiierte 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 VPN kombiniert man sie am besten mit einem auf Sicherheit spezialisierten Protokoll wie IPSec.

Die IP-Sicherheits-Architektur

Die Internettechnologie wurde ursprünglich entwickelt, um verschiedene heterogene Teilnetze untereinander zu verbinden. Daher wurde wenig auf die Sicherheit des Protokolls geachtet, denn es ging in erster Linie darum, Kommunikation zu etablieren, und nicht darum, sie durch komplizierte Protokolle zu erschweren. Die schwerwiegenden Sicherheitsmängel blieben bis zur heutigen Version 4 des Internetprotokolls (IPv4) bestehen. Die Internet Engineering Task Force (IETF) wollte mit der Entwicklung des neuen Internetprotokolls 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 diese Architektur 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 ergänzt IPSec jedes IP-Paket mit Sicherheitsinformationen, die zwischen dem Paketkopf und den Paketdaten in noch näher zu beschreibender Weise eingefügt werden. Diese Informationen gliedern sich in zwei Protokolltypen: den Authentication Header (AH), der die Integrität des Pakets gewährleistet, und die Encapsulation Security Payload (ESP), die die Verschlüsselung der Nutzdaten beschreibt. Sowohl AH als auch ESP sind eigenständige Protokolle, die separat voneinander oder kombiniert eingesetzt werden können. Beide kennen einen Tunnelmodus, der sogar mehrfache Verschachtelung von AH und ESP erlaubt. Der Transportmodus schiebt zusätzliche Protokollfelder in den IP-Header ein und verschlüsselt (im Falle von ESP) die Nutzdaten. Im Tunnelmodus wird ein komplett neues IP-Paket erzeugt, in dessen Nutzdaten nun die Sicherheitsinformationen sowie das gesamte (bei ESP verschlüsselte) Originalpaket 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 anderen 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 ankommende oder ausgehende Daten IPSec-Verarbeitung unterzogen werden sollen, ob sie unverändert weitergeleitet werden dürfen oder ob sie verworfen werden müssen. Sogenannte Security Associations (SA) repräsentieren «offene» IPSec-Verbindungen. Sie beschreiben genau eine IPSec-Transformation und enthalten die dafür nötigen Angaben. Diese umfassen den IPSec-Prokokolltyp (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 ver-

schachtelte 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-Sequenznummer. 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 Sequenznummer 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 auf Grund 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 Senderadresse des Pakets unbemerkt verändert werden. ESP bietet zwar mit Verschlüsselung und Authentifizierung 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 konfigurierten «Ur-Schlüsseln», asymmetrischen Schlüsseln oder auch von X.509-Zertifikaten können zwei Rechner automatisch und auf sichere Weise Schlüsselmaterial sowohl generieren als auch regelmässig erneuern. Ferner erlaubt IKE die automatische Konfiguration sicherer IPSec-Verbindungen und -Tunnels (Security Associations).

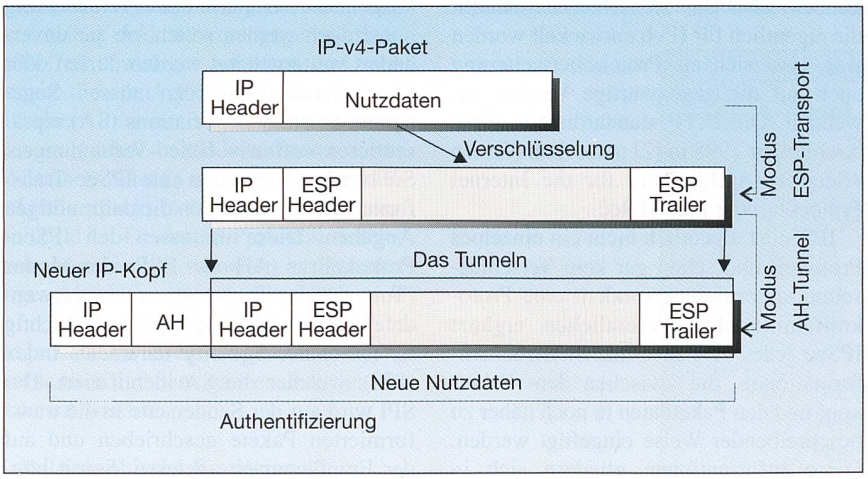

Bild 3 Verschachtelte Anwendung von IPSec

Die Daten des IP-v4-Pakets werden durch das ESP-Protokoll verschlüsselt. Die Authentifizierung der Daten wird anschliessend durch den Authentication Header gewährleistet.

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-VPN mit IPSec

IPSec unterstützt mit der Verschachtelung von AH, ESP und jeweils zweier Modi eine Fülle von verschiedenen Anwendungsszenarien. Wir wollen uns hier auf zwei mögliche Lösungen für die VPN-Anwendungsszenarien beschränken, die bereits vorgestellt wurden. Falls ein Subnetz mit dem VPN verbunden werden soll, so wird auf dem Internet-Router des Subnetzes (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 Tunnelmodus). 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 Gateway 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. Darin verschachtelt 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 Bild 3 dargestellt. Wie bereits früher erwähnt, kann IPSec bei Remote Access VPN mit anderen Protokollen (L2TP) kombiniert werden, um beispielsweise das fremdinitiierte Tunneln oder die benutzerbasierte Authentifizierung zu unterstützen.

Angebot und Ausblick

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-Software-Entwickler haben IPSec basierte VPN-Lösungen im Angebot. Es gibt auch freie Implementationen für Linux [3] und OpenBSD. Internet-Ser-

vice-Provider bemühen sich um den Zukunftsmarkt des VPN-Outsourcing. Für diesen rechnen die Provider besonders im Bereich Remote Access VPN mit traumhaften Wachstumsraten, denn solche VPN 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 netzwerkweite Sicherheits- und Dienstgütebestimmungen durch automatische Konfiguration der Netzwerkkomponenten 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] *M. Günter:* Virtual Private Network Configuration, http://www.iam.unibe.ch/~rvs/cati/

Les réseaux virtuels privés pour Internet

Les nouvelles technologies Internet permettent aux sociétés d'utiliser Internet comme extension de leur réseau privé. Des réseaux virtuels privés (Virtual Private Networks, VPN) sont un nouveau pas dans l'évolution d'Internet comme plateforme de communication universelle sûre et économique.

A l'aide de tunnels de protocole et de la cryptographie, Internet interconnecte fiablement les abonnés au réseau virtuel privé. Lorsque deux sous-réseaux sont interconnectés de cette manière, on parle d'un VPN de réseau à réseau ou encore d'un VPN «Branch-office». Le cas typique d'application est le raccordement au réseau d'une petite succursale située hors de portée du siège de la société. Lorsqu'il s'agit de raccorder au réseau des collaborateurs externes, on parle de «Remote Access VPN». Quant au réseau dit «Extranet VPN», il sert à interconnecter divers réseaux de société en vue d'une collaboration sur un projet donné, les droits d'accès étant limités de part et d'autre. Le protocole IPSec développé par l'Internet Engineering Task Force supporte tous ces scénarios d'application et s'impose peu à peu parmi les fabricants et clients. Le présent article donne un aperçu des éléments de base de l'IPSec et explique la manière dont ils sont utilisés à des solutions VPN.

Der SEV auf dem Internet / L'ASE sur l'Internet:
http://www.sev.ch