1 Motivation für VPN[1]

In den 90er und danach wurden zur Standortverbindung sogenannte **Standleitungen** verwendet. Für die gelegentliche Verbindung (z.B. von einem Außendienstmitarbeiter) in das zentrale Firmennetz wurden **Wählverbindungen** verwendet.

Beide Verbindungsarten waren verhältnismäßig teuer (hohe Monatskosten bei Standleitungen bzw. hohe Minutenpreise bei Wählverbindungen). Auch waren die Übertragungsraten stark begrenzt. Vorteilhaft war hingegen die exklusive Nutzung der Verbindungen. So konnte bei einer Wählverbindung kein anderer auf die Leitung zugreifen und die ausgetauschten Daten waren damit sicher.

Mit dem Aufkommen von schnellen Datenanschlüssen (DSL) und dem rasanten Ausbau des paketbasierten Internets (IP) mit seinen hohen Übertragungsraten kam der Wunsch auf, diese als kostengünstige Alternative für leitungsbasierte Dienste zu nutzen.

Wichtig dabei waren die drei Kriterien einer dedizierten Leitung auf das IP-Netz zu übertragen:

- **Vertraulichkeit**
  Verschleierung der Kommunikationspartner
  - die Daten sind vor der Einsicht durch Unbefugte geschützt
  - nur die Person, an die eine Nachricht adressiert ist, ist in der Lage, diese zu entschlüsseln und die Daten zu lesen
  → ***Verschlüsselung***
- **Integrität**
  „Integrität" = Makellosigkeit, Unbescholtenheit, Unbestechlichkeit
  - Die Daten dürfen auf dem Weg vom Absender zum Empfänger nicht verändert werden können
  → ***Hashfunktion***
- **Authentizität**
  „Authentifizieren" = beglaubigen, die Echtheit bezeugen
  - ermöglicht den Nachweis über die Herkunft der Daten anhand der Bestimmung der Identität des Senders
  - garantiert die Authentizität der Person, die die Daten unterschrieben hat
  → ***digitale Signatur***

1.1 Kryptografie

Das nächste Diagramm veranschaulicht, über welche Verfahren die Kriterien eines VPNs erfüllt werden können. Dabei wird davon ausgegangen, dass die für die Verfahren notwendigen Schlüssel gesichert übertragen wurden (z.B. per Post). Wird ein automatischer Schlüsselaustausch genutzt, so ist für den Schlüsselaustausch zusätzlich noch eine Signatur notwendig.

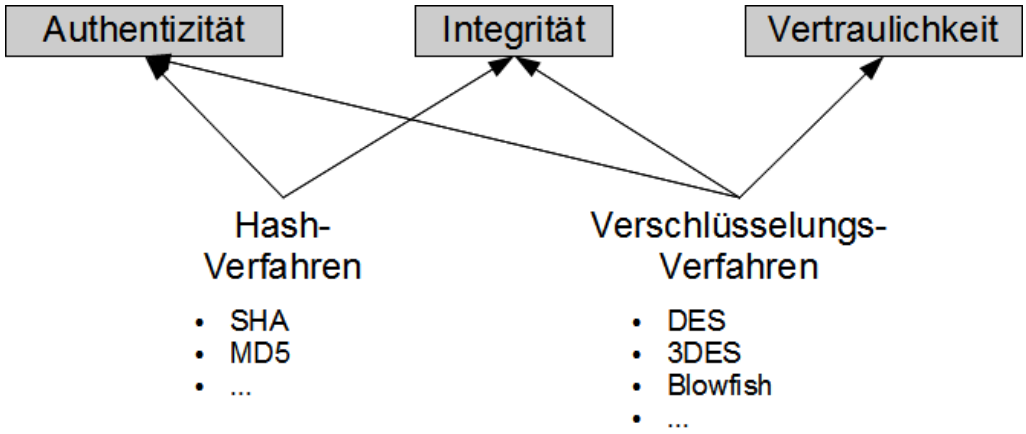

Abbildung 1: Zusammenhang zwischen Tunnel-Kriterien und Kryptografie-Verfahren

1 VPN: Virtual Private Network

Hash-Verfahren sind im wesentlichen über geheime Schlüssel personalisierte Prüfsummenverfahren (vgl. CRC bei Ethernet-FCS). Durch die Nutzung der geheimen Schlüssel und eines nicht reversiblen Algorithmus, ist sichergestellt, dass aus einer beliebigen Zeichenkette nur mit dem korrekten Schlüssel eine gültigen Prüfsumme errechnet werden kann. Damit kann der Empfänger nicht nur die Korrektheit überprüfen, sondern auch die Integrität und Authentizität des Absenders.

Verschlüsselungsverfahren arbeiten ebenfalls mit geheimen Schlüsseln. Allerdings generieren sie keine Prüfsumme, sondern sie „verwürfeln" die zu schützende Zeichenkette derart, dass diese verschlüsselten Daten ebenfalls nur mit dem richtigen Schlüssel zurück in Klartext verwandelt werden können.

2 Überblick der Begrifflichkeiten eines VPNs

2.1 Tunnel

Unter einem Tunnel versteht man den Kanal, über den die Kommunikationspartner ihre Informationen austauschen. Er stellt im Kontext eines VPNs den Ersatz für die dedizierte Leitung (s.o.) dar. Demnach sollte ein solcher Tunnel die oben aufgeführten Kriterien besitzen. Tunneln bedeutet dabei grundsätzlich, Datenpakete so zu kapseln, dass sie nur am Anfangs- und Endpunkt eines öffentlichen Netzes, das zu durchlaufen ist „verstanden" werden (→ Tunnelein- und Tunnelausgang).

2.2 Site, End und Sicherheit

Als ***Site*** wird z.B. ein Firmennetz oder Intranet verstanden. Im Gegensatz dazu wird ein einzelner Rechner als ***End*** bezeichnet. Daraus ergeben sich die folgenden Verbindungsvarianten:

- Sichere End-to-End Verbindung (ohne Tunnel)
- Site-to-Site
- End-to Site
- End-to-End

Der Endpunkt einer Site wird auch **VPN-Gateway** bezeichnet. Die folgenden Diagramme sollen die obigen Verbindungsarten verdeutlichen.

2.3 Encapsulation

Um einen VPN-Kanal zu bilden, werden zusätzliche Informationen benötigt, die für die Kommunikation zwischen den VPN-Endpunkten notwendig sind. Diese Endpunkte stellen somit die Tunnelendpunkte dar, über die die eigentlichen Nutzdaten transparent (ohne Veränderungen) transportiert werden. Da diese VPN-Kommunikationsinformationen die äußere Hülle der Kommunikation darstellen, umhüllen sie die (encapsulate) eigentlichen Nutzdaten. Man nennt diese Informationen daher Encapsulation. Diese gekapselten Informationen müssen ihrerseits vom Tunneleingang über das öffentliche Netz zum Tunnelausgang transportiert werden. Hierzu wird im Internet das IP-Protokoll selbst genutzt.

Zum Tunneln sind demnach **drei Protokolltypen** erforderlich:

- gekapseltes Protokoll (enthält die Nutzdaten) z.B. HTTP
- kapselndes Protokoll (für Auf-/Abbau und Nutzung des Tunnels) z.B. IPsec
- Träger-Protokoll (zur Übertragung der Pakete des kapselnden Protokolls) z.B IP

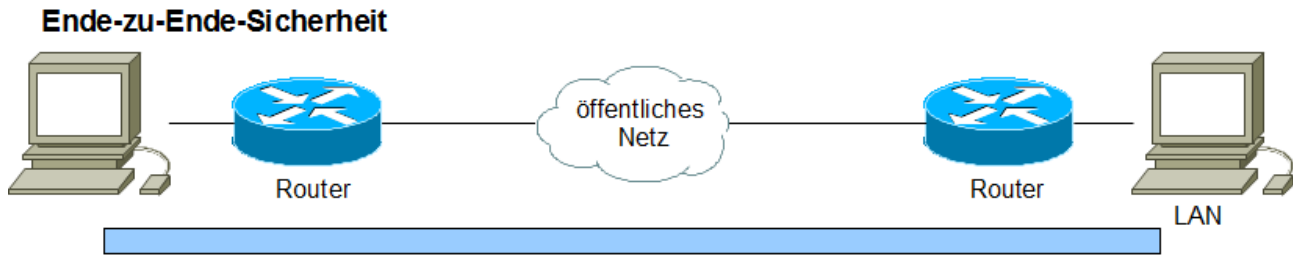

Abbildung 2: Sichere End-to-End-Verbindung

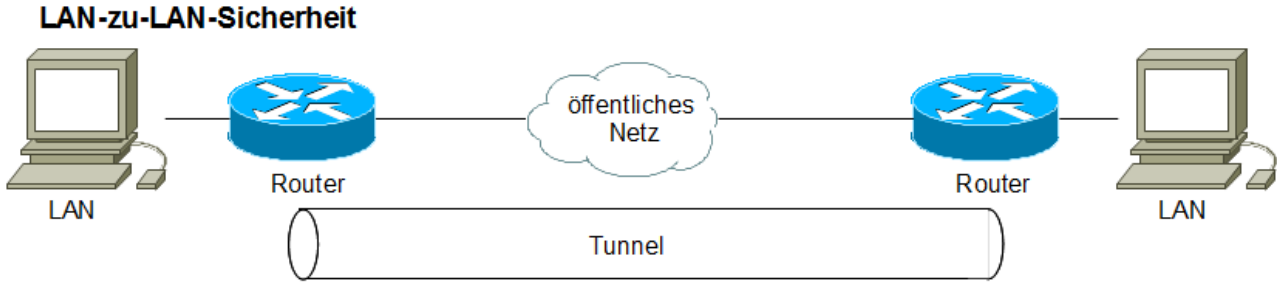

Abbildung 3: Site-to-Site-Verbindung

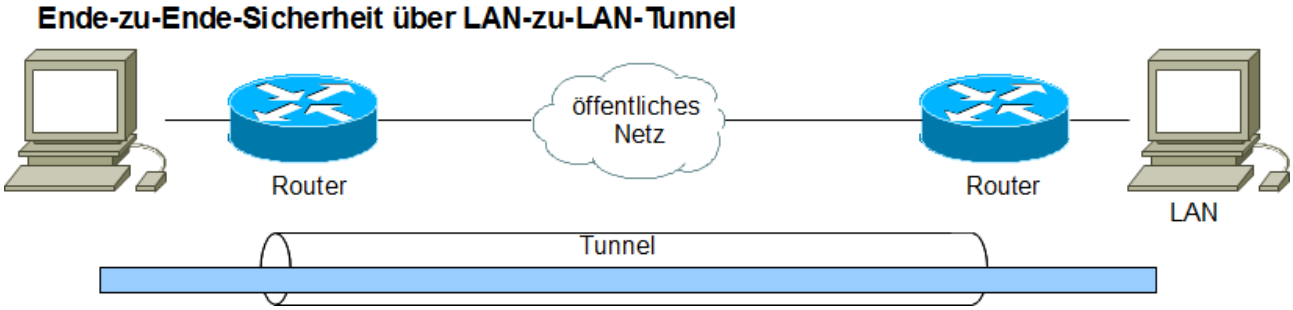

Abbildung 4: End-to-End-Verbindung

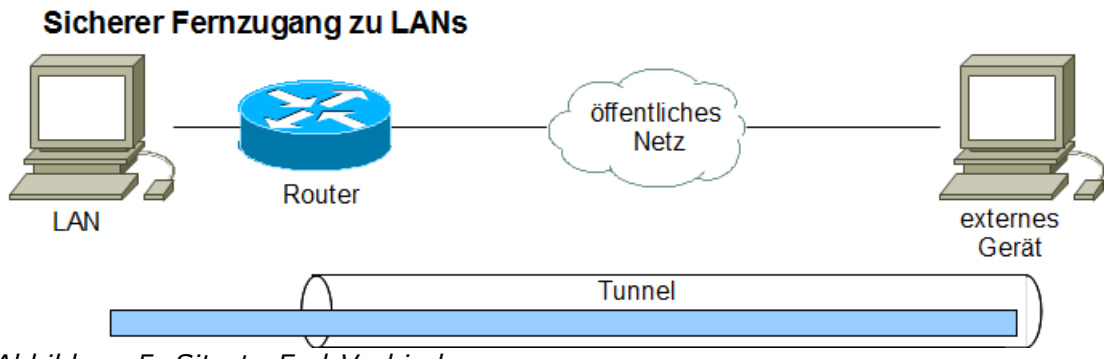

Abbildung 5: Site-to-End-Verbindung

Quellen für dieses Arbeitsblatt: A. Badach, Technik der IP-Netze sowie R. Spenneberg, VPN mit Linux