# Virtual Private Network

**IT-Technik Netzwerkgrundlagen**

Sebastian Meisel

8. Februar 2023

## 1 Virtual Privat Network (VPN)

Unter einem **VPN** versteht man eine Reihe von Protokollen, die eine verschlüsselte Verbindung zwischen **einzelnen Geräten** oder ganzen **LANs** über das **Internet** oder ein anderes WAN ermöglichen. Die verschlüsselte Verbindung wird **Tunnel** genannt und wirkt aus Sicht der beteiligten Geräte wie ein direkte Verbindung. Man kann sich einen **VPN-Tunnel** als virtuelles Kabel vorstellen.
Teilweise werden auch andere Formen von verschlüsseltem Fernzugriff unter dem Begriff **VPN** vermarktet.
Außerdem gibt es Lösungen, die die **VPN** zweckentfremden, um einen Tunnel zu einem entfernten Zugangspunkt (z. B.) in einem anderen Land herzustellen.

## 2 Protokolle

Das verbreiteste und erprobteste Protokoll zum Aufbau von **VPNs** ist das Protokoll **Internet Protocol Security**. Es arbeitet direkt auf dem *Networklayer (OSI Layer 3)*.
Seit 2015 bietet das **Wireguard**-Protocol eine Alternativer, die **einfacher** einzurichten und deutlich **schneller** als IPsec. Letzteres gilt vor seit dieses Protokoll im Linuxkernel integriet ist.
Die dritte relevante Alternative ist OpenVPN, dass ein **VPN** auf Grundlage von **SSL** aufbaut.

### 2.1 IPsec

IPsec nutzt verschiedene Komponenten, um …

- die Integrität (keine Manipulation),
- die Vertraulichkeit (kein Mitlesen),
- die Authentizität (Verifizierung des Absenders) …

der Daten zu garantieren:

- Zugangskontrolle.

- Benutzerauthentifizierung.
- Schlüsselverwaltung.
- Schlüsselauthentifizierung.

Bei Nutzung eines **NATs** werden in der Regel Technik zum **NAT-Traversal** angewendet.

### 2.1.1 IPsec-Header

- **Authentification Header (AH)**:
  - bestätigt (nur) die Integrität der Daten durch Hashing.
  - wird in der Regel nicht allein verwendet.
- **Encapsulation Security Payload (ESP)**:
  - Verschlüsselt die Daten.
  - Wird ergänzt durch den **ESP-Trailer** und **ESP-Authenticator** am Ende des Datenpakets
  - Wird allein oder gemeinsam mit dem **AH** verwendet.

### 2.1.2 IPsec-Verbindungsaufbau

1. Aushandeln der Vertrauensstellung per **Internet Key Exange**

Dazu generiert das eine Ende von zwei VPN-Endpunkten eine Anfrage an das Zielsystem. Das Zielsystem antwortet und leitet den Schlüsselaustausch **IKE** ein. Beide Endpunkte handeln dabei Verschlüsselungs- und Authentisierungsverfahren aus. Über einen Schlüssel oder ein Zertifikat, das beide System kennen, wird eine Vertrauensstellung zueinander hergestellt. Für beide Seiten wird dann der digitale Master-Schlüssel erzeugt

1. Festlegen der Verschlüsselungs- und Authentisierungsverfahren.
2. Erzeugen und Austausch des **Masterschlüssels**.
3. Austausch der mit dem **Masterschlüssel** (symetrisch) verschlüsselten Daten.

### 2.1.3 IPsec-Modi

- **Transportmodus**: Lediglich die Daten werden verschlüsselt. Die Header (Start-/ Zieladresse/ ~port) bleiben unverschlüsselt
- **Tunnelmodus**: Auch die Headerdaten werden verschlüsselt.

### 2.2 Wireguard

Wireguard bietet gegenüber IPsec einige **Vorteile** (wird aber von deutlich weniger Netzwerkgeräten unterstützt):

- Weniger Overhead.
- Weniger Komplexität.
- Modernere Verschlüsselungsverfahren:
  - schneller.
  - (theoretisch) sicherer.

## 3 VPN-Arten

### 3.1 Site-to-Site

Auch **LAN-to-LAN** oder **Gateway-to-Gateway**: Vertrauensstellung zwischen zwei Routern, die **VPN-Gateways** genannt werden. Zwei **LANs** werden mit einander verbunden. **Tunnelmodus**

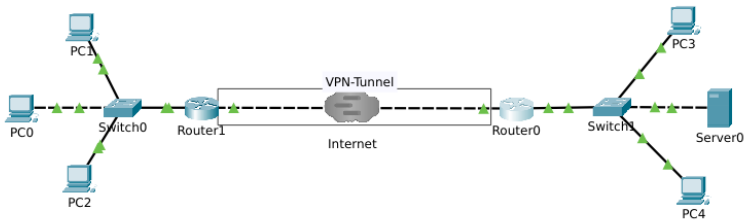


Abbildung 1: Site-to-Site-VPN

### 3.2 End-to-Site

Auch **Host-to-Gateway** oder **Remote-Access**: Vertrauensstellung zwischen einem Host und einem **VPN-Gateways**. Ein Rechner (z. B. im Homeoffice) wird mit einem **LAN** (z. B. Unternehmen) verbunden. In der Regel **Tunnelmodus**.

### 3.3 End-to-End

Auch **Host-to-Host**, **Peer-to-Peer** oder **Remote-Desktop**: Vertrauensstellung zwischen zwei Hosts. Zwei Rechner werden mit einander verbunden. **Transportmodus**.

## 4 Pre-Shared-Keys

IPsec arbeitet zur Vertrauensstellung etweder mit Zertifikaten oder mit Pre-Shared-Keys, wobei Zertifikatesicherere sind. Der Pre-Shared-Key ist ein beiden Seiten bekanntes Geheimnis (Pass-

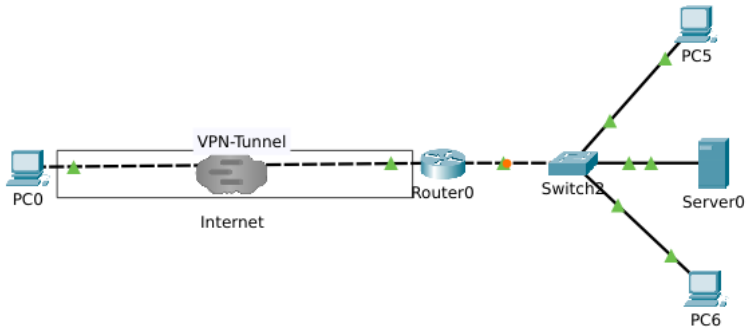


Abbildung 2: End-to-Site-VPN

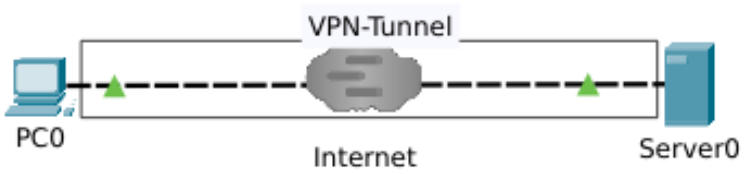


Abbildung 3: End-to-End-VPN

wort). Von diesem wird auf jeder Seite ein Hashwert mit einem zuvor ausgehandelten Hashverfahren gebildet, der dann übertragen und mit dem selbsterstellten Hashwert verglichen wird. Bei Übereinstimmung wird die Ipsec-Verbindung akzeptiert.Allerdings kann man (wenn der PSK nicht lang und komplex genug ist) mit Hilfe von Hashtables einen abgefangenen PSK rekonstruieren.

# 5 Symmetrische vs. Asymmetrische Verschlüsselung

- Symmetrisch
  - beide benutzen den gleichen Schlüssel
  - Problem ist der Schlüsselaustausch
  - Sind schneller
- Asymmetrisch
  - Öffentlicher Schlüssel zum Verschlüsseln von Nachrichten an mich wird geteilt
  - Private Schlüssel zum Entschlüsseln der Nachrichten
  - Problem: Langsameres Verfahren
  - Schlüsselaustausch in unverschlüsselten Netzwerken möglich
- Hybrid
  - Austausch eines symetrischen Schlüssels über eine asymmetrisch verschlüsselter Verbindung