VPN - Virtual Private Network

1. Einführung

Als Privates Netzwerk bezeichnet man ein geschlossenes Netzwerk, d.h. ein Netzwerk, auf das nur bestimmte (erwünschte) Clients Zugriff haben. VPN bildet ein Netzwerk, das über andere Netze gelegt wird und über diese Pakete tunneln, dabei aber geschlossen bleiben.

Es wird meist eine verschlüsselte Verbindung aufgebaut, über die der Datenaustausch stattfindet. Auf den Knoten des VPN erstellt die VPN-Software dazu eine virtuelle Netzwerkkarte, deren Pakete nicht wie bei einer „echten“ Netzwerkkarte direkt in das LAN gesendet werden. Stattdessen werden die Pakete der virtuellen Netzwerkkarte an die VPN-Software übergeben, die diese verschlüsselt und dann als neue Pakete an die VPN-Gegenstelle sendet.

Dabei spielt die Art der Anbindung der VPN-Knoten keine Rolle. Diese können direkt per Ethernet oder sogar per Satellitenverbindung angebunden werden. So kann ein VPN als logisches Netz weit verstreuten Knoten zur Verfügung stehen.

Anwendungsbeispiele

VPN werden unter anderem für folgende Anwendungsszenarien verwendet:

- Anbindung von Außendienstmitarbeitern
- Verbindung mehrerer Unternehmensstandorte
  - ggf. auch verschlüsselte Verbindungen innerhalb eines Standortes
- Spielen von LAN-Games über das Internet
- Ausbruch aus verriegelten Netzwerken (z.B. unzensierter Internetzugriff aus China)
- Absicherung von W-LAN-Verbindungen

Dabei treten je nach Anwendung verschiedene Arten der Verbindung auf. Beim Absichern eines W-LAN verbinden sich mehrere Nutzer (Clients) in ein LAN, hierbei handelt es sich um eine End-to-Site oder Client-to-LAN Verbindung. Die Verbindung mehrerer Netze bezeichnet man hingegen als Site-to-Site oder LAN-to-LAN Verbindung.

2. Netztopologien

Es gibt verschiedene Möglichkeiten eine virtuelle Netzwerkverbindung aufzubauen. Dabei kommt es auf den Einsatzzweck des VPN an, welche Methode sich am besten eignet.

Point-to-Point

Über eine sogenannte TUN-Schnittstelle besteht eine direkte Verbindung zweier „Points“, also zweier Netzwerkknoten. Diese Verbindung kann entweder zur direkten Kommunikation zwischen den (beiden) Knoten oder per Routing auch zur Anbindung von Netzwerken genutzt werden. Mehr dazu im Bereich Routing.

Es können sich auch mehrere Clients zu einem Server verbinden. Hierbei hat jeder Client eine Point-to-Point-Verbindung mit dem Server. Allgemein spricht man dann jedoch von einer Point-to-Multipoint-Verbindung. In diesem Fall entsteht eine Stern-Topologie, deren

Zentrum der Server bildet

Ethernet

Über eine sogenannte TAP-Schnittstelle binden sich die Client direkt in ein Netzwerk ein. Hierbei arbeitet der VPN-Server sozusagen als Switch, über das die Clients ans Netzwerk angebunden sind. Es entsteht eine Baum-Topologie mit dem VPN-Server als Verteiler.

Auch TAP-Schnittstellen können für Routing verwendet werden, allerdings werden für reines Routing Point-to-Point-Verbindungen bevorzugt.

3. Netzwerkanbindung

Routing

Beim Verbinden mehrerer IP-Netze über ein VPN setzt man Routing ein. Dabei werden wie beim Routing ins Internet Pakete zwischen den Netzen geroutet. Hier arbeiten die VPN-Knoten also auf der IP-Ebene, also auf der OSI-Schicht 3 und routen die Pakete zu ihrer Ziel-Adresse.

Per Routing kann man z.B. ein VPN einrichten, über das Rechner der beiden privaten Netzwerke 192.168.1.0/24 und 192.168.178.0/24 sich gegenseitig über ihre IP-Adressen erreichen können. Wird hierbei eine Point-to-Point-Verbindung eingesetzt, hat diese ein eigenes Netz, z.B. 192.168.200.0/24. Eine TAP-Schnittstelle kann ebenso für Routing verwendet werden, ist jedoch für reine Routing-Netze weniger geeignet.

Routing über eine Point-to-Point-Verbindung lässt sich relativ einfach einrichten und arbeitet effektiv. Dabei hat sie aber den Nachteil, dass Broadcasts zwischen den Netzen nicht möglich sind und somit einige Dienste nicht ohne Weiteres genutzt werden können. Ein Beispiel hierfür sind einfache Windowsnetzwerke ohne WINS-Server, da hier die Rechner ihren Namen per Broadcast verbreiten.

Bridging

Beim Bridging wird die virtuelle TAP-Schnittstelle über das Betriebssystem (Windows: „bridge connections“, Linux: bridge-utils) mit einer echten Netzwerkkarte verbunden. Diese „Bridge“ arbeitet wie ein Switch auf der OSI-Schicht 2 und reicht Pakete mit entsprechendem Zielrechner sowie Broadcasts an die TAP-Schnittstelle und somit an den VPN-Gegenüber weiter.

Dadurch vehalten sich die über die Bridge verbundenen Rechner, als wären sie alle im selben Netzwerk. Dadurch kann man dann auch Dienste nutzen, die Broadcasts verwenden. Dazu zählen z.B. Windows-Arbeitsgruppen ohne WINS-Server oder auch viele Spiele, die oft mit Broadcasts oder auch eigenen Protokollen arbeiten.

Der Nachteil ist, dass die Broadcasts einen Teil der Bandbreite verbrauchen und so ggf. unnötige Netzwerkpakete die VPN-Verbindung verlangsamen. Außerdem muss man beim Verbinden zweier Netzwerke per Bridging darauf achten, das die Broadcasts das System nicht lahmlegen, so sollte es z.B. nur ein DHCP-Server pro Netzwerk geben bzw. jeder muss unterschiedliche Adressbereiche verteilen.

Verwendet man eine TAP-Schnittstelle und verzichtet dabei auf das Erstellen einer Netzwerkbrücke, erhält man ein eigenes Netzwerk, welches die Vorteile des

Broadcastings bietet, dabei aber getrennt von den eigentlichen Netzwerkverbindungen des Servers und der Clients arbeitet.

4. Verschiedene VPN-Techniken

Es gibt viele verschiedene VPN-Techniken, die auf verschiedene Übertragungstechniken und Verschlüsselungen setzen. Bekannte und verbreitete VPN-Techniken sind:

- L2TP
- PPTP
- IPSec
- OpenVPN
- Hamachi

Jede Technik hat ihre Vor- und Nachteile. L2TP alleine bietet keine Verschlüsselung, PPTP fiel in der Vergangenheit öfters durch Sicherheitslücken auf. IPSec dagegen gilt als sehr sicher, ist jedoch in der Konfiguration umständlich.

Hamachi, eine vergleichsweise junge VPN-Software, erfordert dagegen nahezu keine Konfiguration und ermöglicht somit ein schnelles Aufsetzen eines VPN, ist aber vom Prinzip für kleine Spielenetzwerke und ähnliches gedacht. Außerdem sind die Software und das Protokoll Closed Source und proprietär, weshalb ein Prüfen der Sicherheit durch Experten schwer möglich ist.

Dies widerspricht Kerckhoffs' Prinzip. Dies besagt, dass eine Verschlüsselung durch Geheimhaltung des Schlüssels sicher sein muss, der kryptographische Algorithmus jedoch offen liegen muss. Dadurch werden Sicherheitslücken schneller entdeckt. Außerdem ist man durch offene kryptographische Algorithmen flexibler, da man mit diesen nicht abhängig von einem bestimmten Hersteller ist.

5. OpenVPN

OpenVPN wurde von James Yonan entwickelt und als Version 0.90 am 13. Mai 2001 erstmals veröffentlicht. Er setzte damit seine Idee um, sichere Kommunikation über SSL als einfach zu konfigurierende Verschlüsselung mit Netzwerschnittstellen wie bei IPSec im Einsatz zu kombinieren.

Entstanden ist dabei eine einfach zu konfigurierende Software, die durch Sicherheit und Plattformunabhängigkeit glänzt. Außerdem erzwingt es keine komplizierten Firewallkonfigurationen und erlaubt Verbindungen auch über einen Proxy herzustellen.

Ausführliche Dokumentation und volle Quellenangaben: http://www.ingmars-bastelecke.net/de/netzwerk/vpn.html

Quellen:

- Buch: OpenVPN, dpunkt.verlag, 2006
- Viele Wikipedia-Artikel zum Thema auf Deutsch und Englisch (OpenVPN, VPN, PPTP
  und viel mehr)
- Erfahrung aus der OpenVPN-Entwicklung für die Fritz!Box (http://ip-phone-forum.de)
- Erfahrungen aus dem OpenVPN-Forum (http://openvpn-forum.de/)