	Netzwerktechnik	Technologie
	VPN-Verbindungen	Datum:

Es sei folgende Situation gegeben: Ein Rechnerarbeitsplatz eines Firmennetzwerkes soll ausgelagert werden, beispielsweise als Heimarbeitsplatz. Man kann natürlich den PC mit einer langen Leitung versehen und den Arbeitsplatz an einen anderen Ort verlegen. Dies scheitert sicherlich an den Kosten für das Verlegen der Leitungen.

Eine andere Lösung wäre, den ausgelagerten Rechner über eine angemietete Leitung von einem Netzanbieter wie der Deutschen Telekom anzuschließen. Dies scheitert meistens an den Kosten und der Bandbreite der Mietleitung.

Das Netzwerk, welches fast überall zur Verfügung steht, ist das Internet. Es ist also naheliegend, dass das Internet für das Anbinden eines entfernten Rechners benutzt wird.

Der Rechner soll allerdings ins Firmennetzwerk eingebunden sein, so als wäre er direkt am Firmenstandort. Hierzu benötigt der PC eine IP-Adresse aus dem Firmennetzwerk (LAN) und der Benutzer ein Anmeldekonto im Firmennetzwerk.

Folgende Schwierigkeiten fallen dabei auf:

Datenpakete mit privaten LAN-Adressen werden nicht im Internet geroutet. Datenpakete, die eigentlich nur firmenintern sichtbar sein sollten, sind im unsicheren Internet unterwegs. Dies ist ein großes Sicherheitsproblem.

Die Lösung heißt VPN-Virtual Private Network oder IP-Tunnel. Man baut sich ein großes virtuelles Netzwerk auf und nutzt dabei ein unsicheres Netzwerk als Basis. Oder anders ausgedrückt, die internen Firmendaten werden durch ein unsicheres Netzwerk getunnelt.


Mit einem VPN wird ein unsicheres Netzwerk durchtunnelt – Daten werden durch einen gesicherten (verschlüsselten) Tunnel transportiert.

Der ausgelagerte Rechner erstellt ganz normale IP-Datenpakete, so als ob er sich im LAN befinden würde. Normalerweise würden nun die Datenpakete von Layer 3 auf Layer 2 weitergegeben, um dort in einen Frame eingepackt zu werden. Hier nun gibt es die entscheidende Veränderung gegenüber einem normalen Datenverkehr:

Das erzeugte Layer-3-Datenpaket wird in ein weiteres Layer-3- Paket eingepackt. Da der Rechner ans Internet angeschlossen ist, kann er nur Datenpakete mit seiner öffentlichen IP-Adresse verschicken, die er von seinem Internetprovider erhalten hat. Er packt also Pakete, die seine öffentliche Quell-IP-Adresse als Absender enthalten und die einen speziellen Rechner / Router in seinem Firmen-LAN adressieren.

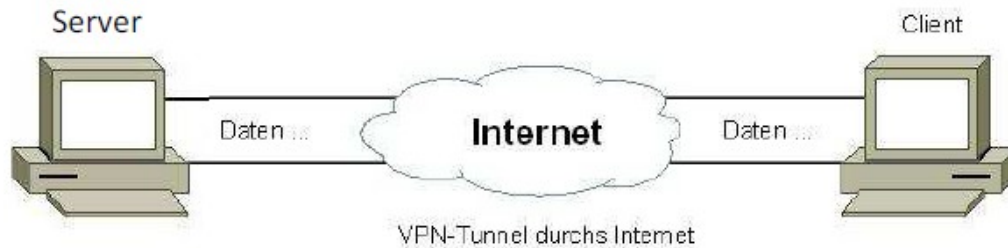
Diese Datenpakete werden ganz normal im Internet transportiert. Als Inhalt eines solchen öffentlichen Paketes wird das LAN-interne IP-Paket transportiert. Der Rechner/ Router im LAN, der diese Pakete empfängt, packt sie aus und erhält ein IP-Paket, welches er ganz normal ins Firmennetz weiterleiten kann.

Wenn man auf diese Weise einen einzigen Rechner an ein Firmennetzwerk anschließen kann, dann kann man ebenso auch ganze Netzwerke an andere Netzwerke anschließen. Ebenso kann man einzelne PCs mit einander verbinden.

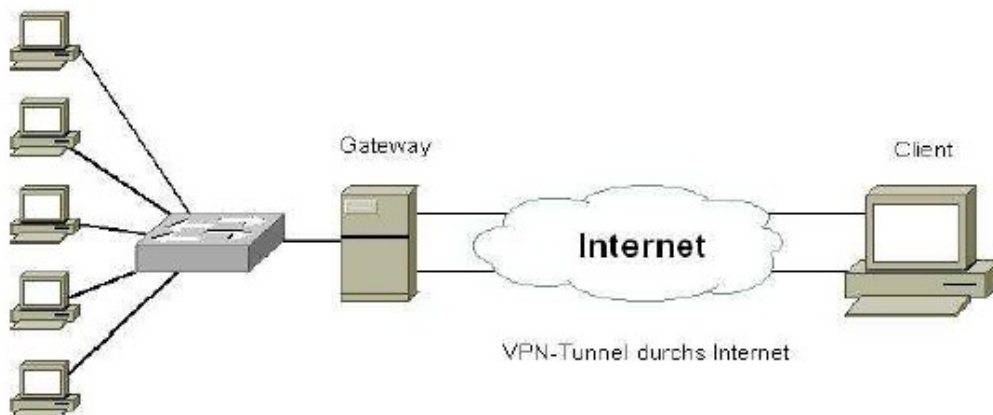
	Netzwerktechnik	Fach: ITS
	VPN-Verbindungen	

Es sind drei Arten von VPNs möglich: End-to-Site-VPN

- **End-to-End-VPN**
Dieser Verbindungstyp kann dazu benutzt werden, um z.B. von zu Hause eine verschlüsselte Remotedesktop-Verbindung zu einem anderen Rechner (Server) aufzubauen. Hierbei ist nur ein bestimmter Rechner im fremden Netz erreichbar.



- **End-to-Site-VPN**
Typische Anwendung für diese Verbindung ist der externe Mitarbeiter, der von zu Hause aus auf das interne Netzwerk der Firma zugreifen will.



- **Site-to-Site-VPN**
Hierbei werden zwei Netzwerke durch einen Tunnel miteinander verbunden. Die Rechner der einen Seite können auf die Rechner der anderen Seite zugreifen.

