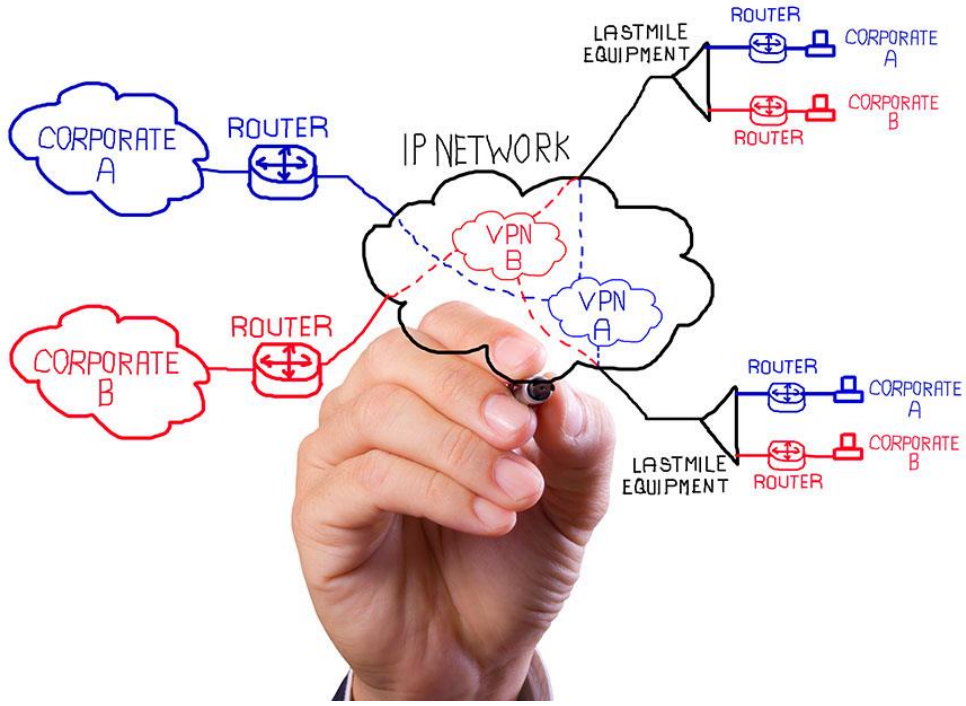
VPN – sichere Datenübertragung über öffentliche Netze

Die zunehmende Vernetzung der Welt bietet weitreichende Möglichkeiten, Geschäftsprozesse effizienter zu gestalten, bringt jedoch auch Gefahren. Immer mehr Unternehmen nutzen das **Internet als Transportmedium**, um Home-Office und mobile Arbeitsplätze zu ermöglichen, Standorte zu vernetzen oder Kunden- und Partner an die eigene IT-Infrastruktur anzubinden. Dabei kommen verschiedene Kommunikationstechnologien zum Einsatz, die es ermöglichen, die **Übertragung sensibler Daten** vor dem Zugriff Unbefugter zu schützen. Eine gängige Lösung ist das VPN.

Was ist ein VPN?

Bei einem Virtual Privat Network (VPN) handelt es sich um ein **virtuelles Kommunikationsnetz**, das auf der Basis eines physischen Netzwerks betrieben wird, logisch von diesem jedoch getrennt ist. Ein typisches Transportmedium für VPNs ist das Internet. Um die Vertraulichkeit von Daten bei der Übertragung über eine öffentliche Leitung sicherzustellen, wird der Transportkanal bei einem Virtual Private Network durch **Verschlüsselungs- und Authentifizierungsverfahren** abgesichert. Man spricht in diesem Zusammenhang von Tunneling, da Daten, die über ein VPN übertragen werden, für andere Teilnehmer des zugrunde liegenden öffentlichen Netzwerks nicht sichtbar sind. Ein VPN ermöglicht somit einen sicheren Transport sensibler Daten über eine nicht-vertrauenswürdige Verbindung und stellt somit eine kostengünstige Alternative zu privaten Leitungen dar.



Einsatzszenarien des Virtual Private Network

Soll ein VPN eingerichtet werden, stehen drei Anwendungsgebiete im Vordergrund: die Vernetzung von zwei oder mehr Unternehmensstandpunkten über ein öffentliches Netzwerk (**Site-to-Site-VPN**), der Zugriff auf das Unternehmensnetz von Zuhause oder unterwegs (**End-to-Site-VPN**) und der Fernzugriff von einem Rechner auf einen anderen (**End-to-End-VPN**).

Site-to-Site-VPN

Ein Site-to-Site-VPN kommt zum Einsatz, wenn mehrere lokale Netzwerke über ein öffentliches Transportmedium zu einem virtuellen Kommunikationsnetz verbunden werden sollen. Denkbar ist ein solches Szenario beispielsweise bei der **Vernetzung von Unternehmensstandpunkten**, Außenstellen oder Niederlassungen. Alternativ lässt sich eine Standortvernetzung auch in Form eines **Corporate Network (CN)**

auf Basis einer privaten Festverbindung realisieren. In diesem Fall müsste die entsprechende Infrastruktur jedoch kostenpflichtig angemietet werden. Eine Verbindung via VPN hingegen nutzt das öffentliche Netz, sodass lediglich die Kosten für den Internetanschluss anfallen. Der Aufbau eines Site-to-Site-VPN setzt an jedem Standpunkt einen VPN-Router voraus, der den VPN-Tunnel zwischen den lokalen Netzwerken aufbaut. Andere Bezeichnungen für das Site-to-Site-VPN sind LAN-to-LAN-VPN oder Branch-Office-VPN.

End-to-Site-VPN

Auf ein End-to-Site-VPN greifen Unternehmen zurück, wenn das Firmennetzwerk für **mobile Nutzer im Außendienst** oder **Home-Office** zugänglich gemacht werden soll. Der Tunnel zum lokalen Netzwerk wird durch einen VPN-Client auf dem Endgerät des externen Mitarbeiters hergestellt. Als Transportmedium kommt das Internet zum Einsatz. Dies ermöglicht Mitarbeitern, über einen beliebigen Internetzugang auf das Firmennetz und somit auf Datei- und Mail-Server oder spezielle Branchensoftware zuzugreifen. Ein End-to-Site-VPN wird auch als **Remote-Access-VPN** bezeichnet.

End-to-End-VPN

Erfolgt der **Fernzugriff** nicht auf ein lokales Netzwerk, sondern lediglich von einem Rechner auf einen anderen, spricht man von End-to-End-VPN. Das klassische Einsatzszenario für diese Art der VPN-Verbindung ist **Remote Desktop**. Eine Technik, bei der Anwendungsprogramme auf einem Rechner ausgeführt und auf einem anderen dargestellt und bedient werden. Transportmedium kann das Internet oder ein lokales Firmennetz sein. Im Unternehmenskontext kommt ein Remote-Desktop-VPN zum Einsatz, wenn Mitarbeiter von zu Hause auf den Rechner am Arbeitsplatz zugreifen möchten.

Technische Umsetzung eines Virtual Private Network

Bei der Implementierung verschlüsselter Verbindungen via VPN kommen verschiedene Protokolle zum Einsatz. Gängige Lösungen setzen auf **IPSec**, **L2TP over IPSec** und **SSL**.

VPN mit IPSec

„Internet Protocol Security“ (IPSec) ist eine Protokoll-Suite, die für das Internetprotokoll (IP) in der Version 6 (IPv6) entworfen wurde und eine **gesicherte Kommunikation über nicht-vertrauenswürdige IP-Netze** ermöglicht. Vertraulichkeit, Authentizität und Integrität des Datenverkehrs werden durch Verschlüsselungs- und Authentifizierungsmechanismen sichergestellt. IPSec wurde zusammen mit IPv6 entwickelt und nachträglich auch für IPv4 spezifiziert.

L2TP over IPSec

Ein VPN, das mittels L2TP over IPSec realisiert wird, greift auf das „Layer 2 Tunneling Protocol“ (L2TP) zurück. L2TP allein beinhaltet jedoch keine Verschlüsselung. Das Protokoll wird daher in der Regel mit IPSec kombiniert. Während IPSec nur IP-Pakete tunneln kann, unterstützt L2TP eine Vielzahl paketvermittelnder Protokolle. Die **Kombination L2TP over IPSec verbindet somit die Stärken beider Standards**. Das Ergebnis ist ein flexibles Tunneling-Protokoll mit hoher Sicherheit.

SSL-VPN

SSL wurde ursprünglich für den Einsatz im HTTP-Umfeld entwickelt, jedoch anwendungsunabhängig spezifiziert. Das Verschlüsselungsprotokoll kommt daher auch bei der Absicherung von VPN-Verbindungen zum Einsatz. Eine beliebte Softwarelösung zum Aufbau eines Virtual Private Network über eine SSL-Verbindung ist **OpenVPN**.