Virtual Private Network

Einleitung

In erster Linie dient VPN (Virtual Private Network) dazu, Teilnehmer eines privaten Netzwerks (bspw. Heimnetz) an ein anderes privates Netzwerk zu binden (bspw. Firmennetz). Dadurch wird es möglich, sich Zugang zu einem lokalen Netzwerk zu verschaffen, ohne physisch anwesend sein zu müssen. VPN ist ein reines Softwareprodukt, dessen wichtigste Funktion darin besteht, eine verschlüsselte Verbindung über einen sogenannten Tunnel herzustellen. Dies geschieht über die Erstellung einer virtuellen Netzwerkkarte, welche die Datenpakete direkt an die VPN-Software weiterreicht, die diese verschlüsselt und an die VPN-Gegenstelle sendet. Die Anordnung und Anzahl der verwendeten VPN-Knoten spielt dabei keine Rolle, da VPN als eigenständiges logisches Netz arbeitet.

Anwendung

Es folgen einige Anwendungsszenarien, für die VPN unter anderem Verwendung findet:

* Netzwerkzugriff für Außendienstarbeiter (Client-to-LAN)
* Verbindung mehrerer Unternehmensstandorte (LAN-to-LAN)
* Umgehung von Zensur
  + Bspw. bei Standort in China oder Nordkorea
* LAN-Spiele über Internet

Funktionsweise | Aufbau einer VPN-Verbindung

1. Internetverbindung über normalen ISP wird hergestellt
2. VPN-Client sendet Verbindungsanfrage an VPN-Server
3. Authentisierung beim VPN-Server
4. IPsec-Tunnel (sicherer VPN-Datentunnel) wird geöffnet

Die Standardkonfiguration sieht vor, dass eine direkte Internetverbindung vom Client ins Internet nicht mehr möglich ist, sobald der IPsec-Tunnel geöffnet wurde. D.h. der Zugriff auf das Internet erfolgt über die Anbindung des am anderen Ende des Tunnels befindlichen Netzwerks. Ist dies nicht der Fall, besteht ein sogenannter Split-Tunnel und die Sicherheit des Clients/der Daten ist nicht gewährleistet (da der Client über das Internet angesprochen werden kann).

Gleichzeitig bekommt der Client eine private IP-Adresse aus dem Netzwerk (Intranet) zugewiesen. Dies ermöglicht es, das firmenseitige Ende des Tunnels mit einer Firewall zu sichern. Nun ist es dem Client möglich, sich von überall auf der Welt, mit (fast) jedem Verbindungsmedium (bspw. auch Satellit) mit dem Firmennetzwerk zu Verbinden.