VPN (E2E, E2S, S2S)

> VPN bedeutet Virtuelles Privates Netzwerk (aus dem Englischen „Virtual Private Network“). Eine VPN-Verbindung bietet die Möglichkeit, von außen auf ein bestehendes Netzwerk zuzugreifen. Dabei kann es sich um ein Unternehmens- aber auch um ein privates Netzwerk handeln.

Grundsätzlich gibt es drei Arten von VPNs, die in verschiedenen Szenarien zum Einsatz kommen.

End-to-End-VPN

Bei einem End-to-End-VPN werden zwei Clients miteinander verbunden. Dabei befindet sich ein Client innerhalb eines Netzwerks, der andere hingegen außerhalb. Diese Art von VPN ermöglicht beispielsweise den direkten Zugang zu einem Server im Netzwerk.

Um einen solchen VPN-Tunnel herzustellen, ist jedoch auf beiden Clients eine VPN-Software erforderlich. Die Verbindung wird allerdings nicht direkt hergestellt. Stattdessen geht man den Umweg über ein Gateway, mit dem sich beide Clients verbinden. Das Gateway sorgt dann dafür, dass die zwei aufgebauten Verbindungen zusammengeschaltet werden und eine direkte Kommunikation erfolgen kann.

End-to-Site-VPN

Über ein End-to-Site-VPN wird ein einzelner Client außerhalb eines Netzwerkes mit einem Unternehmensnetzwerk verbunden. Auch hier bedient man sich wiederum der öffentlichen Internetverbindung, um sich in das Unternehmensnetzwerk einzuwählen.

Verwendet wird diese Art von VPN beispielsweise für Heimarbeiter oder mobile Außendienstmitarbeiter, die sich von zuhause oder vom Kundentermin aus per Remote Access mit dem Unternehmensnetzwerk verbinden. Sie können es dann so nutzen als würden sie gerade im Betrieb sitzen.

Site-to-Site-VPN

Bei einem Site-to-Site-VPN werden mehrere lokale Netzwerke zusammengeschlossen. Im Gegensatz zur herkömmlichen Standleitung, die eine physikalische Verbindung zwischen den zwei Netzwerken herstellt, wird beim Site-to-Site-VPN eine Internetverbindung herangezogen. Dadurch können die hohen Kosten eingespart werden, die eine Standleitung mit sich bringt. Auf diese Weise können beispielsweise die lokalen Netzwerke eines Unternehmens mit mehreren Filialen oder Betrieben miteinander kommunizieren.

MPLS-VPN

Es handelt sich um ein in sich geschlossenes, privates IP-Netz, das vom Anbieter zur Verfügung gestellt und komplett gemanagt wird. MPLS (Multiprotocol Label Switching) ist eine Kombination von Switching und Routing. Bei MPLS ist der Transportweg von Datenpaketen im Unterschied zur „normalen“ Internet-Übertragung vorgegeben. Es handelt sich somit um eine Lösung, die die verbindungsorientierte Übertragung von Datenpaketen in einem eigentlich verbindungslosen Netz ermöglicht. So werden unnötige Umwege oder falsche Paketreihenfolgen bei der Datenübertragung beispielsweise zwischen Unternehmensstandorten verhindert. Auf diese Weise entstehen vordefinierte Pfade, da Pakete mit dem gleichen Label immer den gleichen Weg nehmen.

Vor- und Nachteile eines MPLS-VPN:

+ Stabile Qualität	– Höhere Kosten
+ Gesicherte Bandbreite	– Weniger Flexibilität
+ Geringer betrieblicher Aufwand	

Vorteile von VPN

- **Kosteneinsparung** durch Verzicht auf eine physikalische Standleitung
- **Hohe Verfügbarkeit** durch gute Netzabdeckung
- Höhere Abhörsicherheit
- Verschlüsselte Datenübertragung
- Bedienerfreundlichkeit

Neben diesen Vorteilen haben VPN außerdem den großen Vorteil, dass sie ohne großen Aufwand eingesetzt werden können. Es bedarf lediglich eines entsprechenden Clients, um sichere Verbindungen herzustellen.

Nachteile von VPN

- Geschwindigkeitseinbußen
- Webseiten-Blockaden
- Dubiose Anbieter

Transport vs Tunnel Mode

Im **Transport Mode** kommunizieren zwei Hosts direkt via Internet miteinander. In diesem Szenario lässt sich IPsec zum einen dazu nutzen, die Authentizität und Integrität der zu gewährleisten. Man kann also nicht nur sicher sein, mit wem man da gerade kommuniziert, sondern sich auch darauf verlassen, dass die Pakete nicht unterwegs verändert wurden. Per optionaler Verschlüsselung kann man zudem verhindern, dass Unbefugte die transportierten Inhalte mitlesen. Da hier zwei Rechner direkt über ein frei zugängliches Netz miteinander Daten austauschen, lassen sich jedoch Ursprung und Ziel des Datenstroms nicht verschleiern.

Der **Tunnel Mode** kommt stets dann zum Einsatz, wenn zumindest einer der beteiligten Rechner nicht direkt angesprochen, sondern als Security Gateway genutzt wird. In diesem Fall bleibt

zumindest einer der Kommunikationspartner - der hinter dem Gateway - anonym. Tauschen gar zwei Netze über ihre Security Gateways Daten aus, dann lässt sich von außen gar nicht mehr bestimmen, welche Rechner hier tatsächlich miteinander sprechen. Auch im Tunnel Mode lassen sich natürlich Authentifizierung, Integritätskontrolle und Verschlüsselung einsetzen.

Revision #7
Created 2022-08-01 07:32:22 UTC by Joshua Lieder
Updated 2022-11-07 13:39:08 UTC by Joshua Lieder