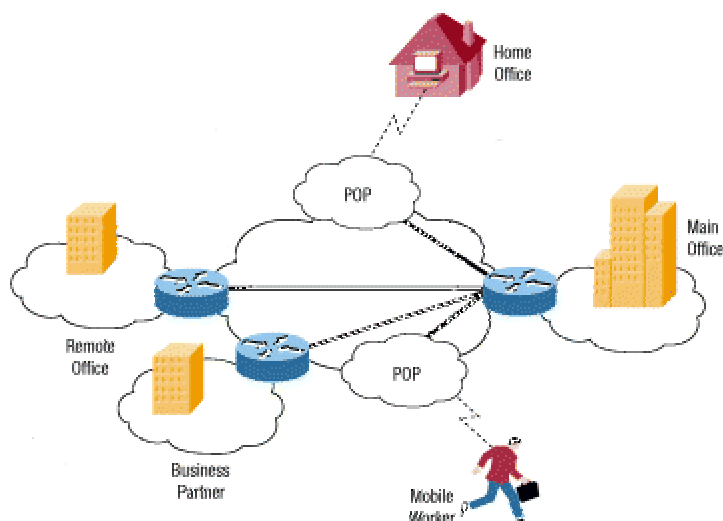


## Wat is een VPN

Privé netwerken zijn traditioneel gebouwd met toepassingsgerichte lijnen, inbel-lijnen of andere verbindingen zoals satelliet of microgolven. Verbindingen worden op afstand gemaakt met sites. De verbindingen zijn privé omdat geen verkeer behalve het verkeer van de organisatie zelf de verbindingen kruisen.



Een virtueel privé netwerk is de creatie van privé verbindingen die publieke netwerken zoals het internet kruisen. Het idee is het creëren van een specifieke privé verbinding op een gedeeld netwerk die gebruikt maakt van coderen en tunneltechnieken. Iedereen kan een privé verbinding maken door de inhoud van het verkeer dat door het netwerk verstuurd wordt te coderen, maar echte veilige VPNs zijn beter gebouwd met de hulp van service-providers die toegewezen wegen met gegarandeerde ondersteuningsniveaus door hun netwerken creëren.

VPNs zijn relatief makkelijk in ATM en FRAME relay netwerken omdat de netwerkprovider virtuele circuits in het netwerk creëert die klanten voorziet van specifieke bandbreedte en controle van het pad dat de data volgt. Verkeer is dan gecodeerd door de afzender en wordt verzonden door het virtuele circuit. In sommige gevallen, besteedt de klant alle VPN gerelateerde zaken uit aan de service-provider. Een fysieke verbinding is gemaakt naar de POP (Point Of Presence) van de provider die alle aspecten van encryptie, point of presence en path control afhandelt.

De open omgeving van het Internet laat iedereen toe een privé-verbinding te maken door pakketten te coderen die over het netwerk gaan. Hoe dan ook, het virtuele netwerkgedeelte van de VPN (het tegenovergestelde van het privé gedeelte) heeft de medewerking van service-providers nodig die gebruik maken van virtuele-circuits en van verkeers engineering technieken die wegen maken voor gereserveerde bandbreedte. Dit is mogelijk met MPLS (Multiprotocol Label Switching), welke netwerkverkeer engineering voor het Internet verleent. Als het verkeer privé gemaakt moet worden, is IPSec een goede keuze.

VPNs in publieke netwerken kunnen de medewerking van een aantal providers nodig hebben. Bijvoorbeeld, als je een VPN die door het land gaat op een virtueel circuit tussen LA en New York heb je misschien de ondersteuning van meerdere providers nodig die je kunnen helpen met het maken van een MPLS weg op het Internet.

Voordat MPLS en IPSec er waren, werden basis-tunnelling en gecodeerde ontwerpen gebruikt om Internet VPNs te maken. L2TP (Layer 2 Tunneling Protocol) is een voorbeeld van een protocol dat IP pakketten in "tunnelling" pakketten die het onderliggende Internet routing samenstelling encapsuleerd. L2TP laat gebruikers de lokale inbel sessies in samenwerkende netwerken op het Internet creëren, om zodoende lange afstand lasten te beperken.