

VPN Virtueel Privé Netwerk

VPN

VPN is de afkorting voor virtual private network. Een VPN is, zoals de term al zegt, een virtueel netwerk. Het woord "private" in deze term beschrijft de mogelijkheid om de gegevens die over het virtuele netwerk verstuurd worden te beveiligen. Een VPN verbinding kan opgezet worden tussen 2 (of meer) bedrijfslocaties over bijvoorbeeld een internetverbinding of een leased-line. Bij dit type VPN wordt de term "Site-to-site VPN" gebruikt. Het is ook mogelijk voor individuele gebruikers om een VPN verbinding op te zetten naar een centrale locatie, zoals het hoofdkantoor of het datacenter. Dit noemt men "Client-to-site VPN". De VPN verbinding wordt vaak een VPN tunnel genoemd.

Site-to-site VPN

Bij een Site-to-site VPN verbinding is het noodzakelijk dat op beide locaties apparatuur aanwezig is waar de VPN Tunnel op getermineerd kan worden. In de meeste gevallen is een firewall het apparaat waar de VPN verbinding wordt getermineerd. Dit kan in sommige gevallen ook ander apparatuur zijn. Voor en na deze apparatuur vindt gewoon normaal netwerkverkeer plaats. Zodra er verkeer door de tunnel gaat, wordt dit beveiligd (versleuteld).

Client-to-site VPN

Bij Client-to-site VPN dient de gebruiker (de cliënt) meestal een applicatie te installeren die de over VPN functionaliteit beschikt. Deze applicatie vervangt de apparatuur aan de zijde van de cliënt. Aan de andere zijde van de VPN tunnel dient dan nog steeds apparatuur te staan die een VPN verbinding kan termineren. Het belangrijkste voordeel aan deze verbinding is dat de gebruiker volledig mobiel is. Op elke locatie waar een gebruiker met zijn laptop of pc over internet kan beschikken, is het mogelijk de VPN verbinding beschikbaar te stellen. Naast deze "klassieke" Client-to-Site VPN methode bestaat er ook een Clientless techniek. Hierbij is het niet nodig een applicatie op de pc of laptop van de gebruiker te installeren. De verbinding komt tot stand door het bezoeken van een webpagina en de beveiliging wordt verzorgd door SSL (https) encryptie.

Beveiliging

Een van de meest gebruikte standaarden betreft VPN verbindingen is IPSec. Het voordeel van het gebruik van deze standaard is dat de compatibiliteit tussen verschillende merken vrij goed is. Hierdoor is het niet noodzakelijk om op alle locaties specifiek apparatuur te plaatsen, maar kan er vaak gebruik gemaakt worden van een reeds aanwezige firewall. Deze firewall moet dan uiteraard wel over deze functionaliteit beschikken. De beveiliging van gegevens wordt verzorgd door encryptie en hashing, waardoor de data niet uitleesbaar is of ongemerkt aan te passen is door derden.