

VPN (virtual private network)

Virtuálna privátna sieť (VPN) je prostriedok na prepojenie niekoľkých počítačov pomocou verejnej (nedôveryhodnej) siete. Je možné dosiahnuť stav, kedy prepojené počítače budú medzi sebou môcť komunikovať, ako keby boli prepojené v rámci jednej uzavretej privátnej (teda dôveryhodnej) siete.

Pri nadväzovaní spojenia oboch strán je ich totožnosť overovaná pomocou digitálnych certifikátov, dôjde k autentizácii, komunikácia je šifrovaná, a preto môžeme také spojenie považovať za bezpečné.

VPN siete sa väčšinou vytvárajú medzi počítačmi, ktoré sú pripojené k Internetu. Napríklad je možné zaistiť pripojenie firemných notebookov pripojených k Internetu kdekoľvek na svete do firemného intranetu (vnútorná sieť firmy).

K prepojeniu s firemnou sieťou sa najskôr sprevádzkuje VPN server, zaistí sa pripojenie k Internetu, kde sa potom pripájajú VPN klienti z akéhokoľvek miesta prostredníctvom Internetu.

VPN server plní funkciu sieťovej brány, ktorá sprostredkúva pripojenie, zaistuje zabezpečenie a šifrovanie komunikácie.

Všeobecne VPN je sieťové tunelovanie, kde sa prostredníctvom štandardného sieťového spojenia vytvorí virtuálna linka medzi dvoma počítačmi, v rámci ktorej je potom možné nadviazať ďalšie sieťové spojenia.

Sieťové tunelovanie je technika používaná na prenos jedného alebo viacerých sieťových spojení a umožňuje prenášať dáta cez nekompatibilné siete, obchádzať administratívne obmedzenia určitej siete a poskytuje zabezpečenú komunikáciu cez nezabezpečenú sieť.

Často sa používa tunelovanie cez SSH spojenie, čo zaistuje, že prenášané dáta budú zašifrované, aj keď samotný tunelovaný protokol šifrovanie nepodporuje.

Technicky sa tunelovanie prevádza zabalením dátovým prvkom (PDU – Protocol Data Unit) prenášaného protokolu do PDU iného protokolu. Pritom je väčšinou narušené normálne poradie vrstiev, pretože PDU jednej vrstvy referenčného modelu ISO/OSI balí do PDU vyššej alebo rovnakej vrstvy.