

VPN

Virtual private network

Una Virtual Private Network o VPN è una rete privata instaurata da un soggetto utilizzando un mezzo di trasmissione pubblico e condiviso come può essere per esempio internet. Il messaggio e il traffico della VPN transitano sulla rete pubblica utilizzando gli standard di trasmissione della rete e quindi potenzialmente possono essere insicuri dato che sono trasmessi in "chiaro" utilizzando protocolli comuni e quindi conosciuti anche da soggetti esterni alla VPN.

Per rendere le reti VPN sicure si sono adottati dei protocolli che provvedono a cifrare il traffico transitante sulla VPN rendendo la rete più sicura.

Oltre alla cifratura una VPN sicura deve prevedere dei meccanismi nei suoi protocolli che impediscano violazioni della sicurezza come ad esempio il furto dell'identità digitale o l'alterazione dei messaggi.

Il termine VPN è un termine generico e non un marchio di qualità e quindi se un prodotto è marchiato VPN non vuol dire che sia un prodotto di alta qualità o di elevata sicurezza ma solamente che il produttore ha deciso di apporre quelle tre lettere sulla confezione del suo prodotto.

Usualmente si ritiene che una VPN adeguatamente progettata abbia un grado di sicurezza comparabile con quello di una rete dedicata.

I protocolli che implementano una VPN sicura più conosciuti sono:

- IPsec (IP security), parte obbligatoria dell'IPv6;
- SSL utilizzato per instradare specifici protocolli, utilizzato dall'OpenVPN;
- PPTP (point-to-point tunneling protocol), sviluppato da Microsoft.

Alcune reti VPN sicure non usano algoritmi di cifratura ma partono dal presupposto che un singolo soggetto fidato gestisca l'intera rete condivisa e che quindi l'impossibilità di accedere al traffico globale della rete renda i singoli canali sicuri dato che il gestore della rete fornisce ad ogni soggetto solamente la sua VPN.