

COME FUNZIONA LA VPN

- il client VPN si collega all'ISP utilizzando una connessione crittografata.
- Mantenendo sempre una connessione crittografata, il client VPN si connette al server VPN
- Il server VPN decodifica i dati dal dispositivo dell'utente e quindi si connette a Internet per accedere al server Web, a questo punto in una comunicazione non crittografata.
- fase di tunnelling: un processo che incapsula il pacchetto di dati all'interno di un altro pacchetto, che viene poi spedito sulla rete. I dati vengono "imbustati" due volte per far sì che essi siano trasmessi solamente ai destinatari finali autorizzati, l'ISP non può visualizzare l'attività dell'utente.



I VANTAGGI DELLA RETE VPN

- Permette la comunicazione in aree diverse da quelle della LAN
- Migliora la sicurezza criptando i dati
- E' economica
- Riduce il tempo di transito e i costi di trasporto per i clienti remoti;
- Semplifica la topologia di rete
- Fornisce la possibilità di reti globali;
- E' compatibile con le reti a banda larga
- Fornisce un più veloce tempo di ritorno dell'investimento rispetto al trasporto tradizionale delle linee WAN (Wide Area Network)
- In alcuni Stati non democratici, l'impiego della VPN rende poi possibile aggirare le censure governative, che spesso portano al blocco di una quantità significativa di domini.



LA RETE VIRTUALE PRIVATA

Scopri cos'è la rete virtuale privata (o VPN) e quali sono i suoi vantaggi



RIFERIMENTI

- <https://www.c3t.it/projects/awareness/articoli&brochure/vpn/>



Una rete virtuale privata (conosciuta anche come VPN, acronimo di Virtual Private Network) è una rete di telecomunicazioni che consente a diversi dispositivi di comunicare anche se questi non fanno parte della stessa LAN (Local Area Network, ad esempio un ufficio, una scuola o una azienda). La rete virtuale privata consente di mantenere gli stessi vantaggi della comunicazione all'interno di una LAN anche a dispositivi che non si trovano all'interno della LAN, che copre un'area abbastanza limitata.

Possiamo quindi vedere la VPN come l'estensione a livello geografico di una **rete locale** privata sicura che mette in comunicazione tra loro siti interni di una stessa organizzazione variamente dislocati su un ampio territorio, sfruttando l'**instradamento** tramite **IP** per il trasporto su scala geografica e realizzando di fatto una rete LAN, detta appunto "virtuale" e "privata", equivalente a un'infrastruttura fisica di rete (ossia con collegamenti fisici) dedicata.

La connessione si svolge attraverso un tunnel "virtuale" (protetto e sicuro) supportato da Internet esattamente come fosse il cavo fisico abituale. In questo modo si possono utilizzare le risorse di rete abituali: cartelle, sistemi informatici gestionali, posta elettronica aziendale e così via.



Conessione VPN ad accesso remoto

Consente agli utenti (ad esempio in smart working) di accedere a un server su una rete privata per il tramite della rete Internet. Questo tipo di connessione può essere vista come un collegamento tra un PC client VPN e il server dell'azienda.

Conessione VPN site-to-site

Si utilizza per connettere in una rete privata, sempre con l'ausilio di una rete pubblica, uffici dislocati in più sedi o di altre organizzazioni, consentendo il routing ed una comunicazione sicura. In questo scenario, ogni sede avrà un router dedicato



SICUREZZA DELLA COMUNICAZIONE

Le VPN utilizzano segnali cifrati e meccanismi di autenticazione per assicurare la sicurezza della comunicazione in un ambiente, quello Internet, che altrimenti sarebbe non sicuro. Il più diffuso protocollo utilizzato a questo scopo al livello IP è l'IPsec. Inoltre, una VPN sicura deve prevedere nei suoi protocolli dei meccanismi che impediscano violazioni della sicurezza, come ad esempio il furto dell'identità digitale o l'alterazione dei messaggi. Nelle VPN c'è in genere un firewall tra il computer del dipendente o di un cliente e il terminale della rete o del **server**. Il dipendente, per esempio, quando stabilisce la connessione con il firewall deve verificare i dati che vuole trasmettere, passando attraverso un servizio di autenticazione interno.