L'infrastruttura VPN può essere utilizzata per permettere l'accesso protetto ad alcuni particolari servizi IDC (internet Data Center) ad una pluralità di piccoli uffici (dealer) dislocati nel territorio.

Le agenzie o uffici si doteranno di un router con supporto IPSec; eventualmente lo stesso router può essere equipaggiato con un'opportuna interfaccia WAN (ISDN, xDSL…) ed impiegato sia per l'accesso ad Internet che per quello VPN verso l'IDC dell'organizzazione

Sono possibili due diverse soluzioni a seconda del grado di conoscenza che i router dell'IDC avranno delle reti degli uffici, descritte di seguito:

- **Soluzione con IPSec in modalità accesso remoto e NAT:**
  Questa soluzione richiede che il router che instaura il tunnel IPSec con l'IDC sia in grado di effettuare il Network Address Translation (NAT) sul tunnel stesso. Il router, all'accensione, attiva una VPN con i concentratori presso l'IDC esattamente come farebbe un normale PC utilizzando il protocollo L2TP / IPSec, ed autenticandosi con un certificato macchina lato IPSec e con un'utenza di una classe predisposta appositamente lato L2TP; al termine dell'autenticazione al router viene assegnato un indirizzo IP dinamico.
  A questo punto le postazioni nella LAN dell'ufficio possono accedere ai servizi grazie al mascheramento operato dal NAT: la rete IDC vedrà unicamente pacchetti originati da, oppure destinati a, l'IP dinamico assegnato al router, indipendentemente dalla postazione che genera effettivamente il traffico.
  Vengono di seguito elencati le limitazioni di questo approccio:

  1. il router deve supportare il NAT su tunnel IPSEc;

  2. la LAN dell'ufficio può avere un indirizzamento qualunque, purchè non ci siano sovrapposizioni con le sottoreti dei servizi a cui la LAN intende accedere;

  3. nel caso il router che instaura il tunnel sia distinto da quello che fornisce connettività ad Internet, occorre tenere conto di tutti i limiti nell'uso di IPSec dietro NAT, ed in più sarà necessario che nelle postazioni di lavoro, accanto al default gateway verso il router Internet, siano inserite delle rotte statiche permanenti che, per le subnet dell'IDC, puntino al router IPSec.

  4. sulla rete IDC e sui servizi applicativi si perde di granularità nella registrazione (logging) degli accessi, giacchè l'intera LAN risulta mascherata dal solo indirizzo IP del router.

- **Soluzione con IPSec in modalità LAN to LAN**
  In questa modalità il router che effettua il collegamento VPN utilizza direttamente il protocollo IPSec in versione nativa, senza cioè lo strato L2TP. La gestione dell'IDC assegna staticamente alla LAN dell'ufficio/agenzia una sottorete IP compatibile con l'indirizzamento del Data Center e predispone il router come se tale sottorete fosse connessa direttamente ai concentratori VPN. In altre parole le sottoreti degli uffici/agenzie sono regolarmente ruotate nel Data Center ed i tunnel IPSec si comportano come normali connessioni WAN punto-punto tra i concentratori e le reti remote.
  Le caratteristiche salienti di questo approccio sono:

  1. l'aggiunta di nuove LAN è un'operazione complessa (scelta di indirizzi, predisposizione routing sulla rete IDC, configurazione delle postazioni di lavoro);

  2. la configurazione delle postazioni di lavoro sulle LAN remote deve essere tenuta sotto controllo;

  3. di contro la rete IDC può disporre dei dati di attività delle singole postazioni, disponendo esse di indirizzi IP riconosciuti.