Il Network Address Translation (NAT) è di solito impiegato su Internet come mezzo per “risparmiare” indirizzi IP pubblici.

In mancanza di una corrispondenza biunivoca tra numero di client e numero di indirizzi pubblici, i dispositivi che applicano il NAT (solitamente router o firewall) tengono traccia delle connessioni instaurate dagli utenti basandosi sui numeri di porta caratteristici dei protocolli di trasporto TCP ed UDP.

Questo meccanismo non può però funzionare per flussi dati trasportati da protocolli di livello 4 che non fanno uso di numeri di porta come GRE (necessario per PPTP), ESP ed AH (L2TP su IPSec), ovvero ogni qualvolta il numero della porta sorgente non può essere modificato.

Queste limitazioni fanno sì che, in generale, gli utenti attestati dietro NAT non possono instaurare Reti Private Virtuali con l’esterno.

Qualora il dispositivo che effettua il NAT supporti esplicitamente i protocolli coinvolti, è possibile instaurare VPN PPTP o L2TP anche dietro NAT, ma con la limitazione di un solo client per dispositivo; quest’ultima limitazione può essere superata del tutto nel caso di tunnel IPSec o L2TP/IPSec grazie ad alcune estensioni del protocollo che devono essere supportate sia dal concentratore VPN che dal client, quali:

- **IPSec over TCP:** i pacchetti IPSec ed IKE vengono dotati di un header compatibile TCP in modo che i dispositivi di NAT possano elaborarli correttamente.

- **IPSec over UDP:** approccio simile ma che prevede l’incapsulamento dei protocolli IPSec ed IKE in pacchetti UDP.

- **NAT-T:** è un’estensione del protocollo IKE che permette ai due *peer* di individuare automaticamente la presenza di NAT, ed in caso affermativo di negoziare una porta UDP per l’incapsulamento di IKE ed IPSec su tale protocollo. In assenza di NAT non viene intrapresa alcuna azione particolare.