Quando un client remoto richiede l'instaurazione di un tunnel con la LAN aziendale, il concentratore VPN deve innanzitutto verificare l'identità. Il numero di utenze atteso ed una logica separazione funzionale porta all'impiego di un sistema di autenticazione centralizzato, basato sul protocollo standard RADIUS.

Il concentratore VPN anziché autenticare gli utenti grazie ad un database locale, è configurato per appoggiarsi ad un servizio RADIUS esterno.

Il servizio RADIUS puntato dal concentratore è in grado di terminare tutti i diversi protocolli di autenticazione che si rendono necessari per l'erogazione del servizio VPN (PAP, CHAP, MS-CHAP, EAP), reperendo eventualmente all'esterno le informazioni necessarie (database, LDAP, altri server Radius….).

L'unica eccezione a questa regola riguarda la verifica dei certificati utenti al momento dell'instaurazione di tunnel IPSec, la quale deve necessariamente avvenire a bordo dell'apparato che termina fisicamente il tunnel.

In caso di autenticazione avvenuta con successo da parte di un utente remoto, il servizio RADIUS fornisce, nel pacchetto contenente la risposta affermativa, anche un *ID* del gruppo di appartenenza dell'utente. Il concentratore VPN utilizza questa informazione per controllare l'assegnazione dei parametri di rete.
In particolare ad ogni gruppo può essere associato un pool di indirizzi IP distinto, un diverso server DNS, etc…..