Quando un utente tenta di connettersi alla rete attraverso una connessione VPN oppure in dial-up, la richiesta AAA (Autenticazione Autorizzazione ed Accounting) segue il flusso descritto di seguito secondo quanto indicato dal protocollo RADIUS (RFC 2138 ed RFC 2139).

Il protocollo di trasporto utilizzato dal RADIUS è l'UDP.

1. il VPN Concentrator raccoglie una richiesta di autenticazione e negozia la connessione con il RADIUS server utilizzando il protocollo di accesso scelto dal client (ad esempio EAP-TLS)

2. il VPN Concentrator crea ora un "Access-Request" contenente gli attributi necessari per l'autenticazione, quali ad esempio la username, password, l'ID del client e la Port ID che l'utente sta usando per l'accesso. Quando una password è presente, questa viene nascosta usando un metodo che si basa su RSA Message Digest Algorithm MD5.

3. il VPN Concentrator invia l'Access-Request al RADIUS server su una delle due porte standard: la 1645 oppure la 1812.

4. Il RADIUS server verifica che l'indirizzo IP sorgente contenuto nel pacchetto di Access-Request appartenga ad un valido RADIUS client e che la *shared secret* che i due apparati si scambiano sia quella corretta. Le transazioni tra i client ed i RADIUS server sono autenticate attraverso l'uso di una *shared secret* che non è mai stata spedita attraverso la rete. In aggiunta a ciò tutte le password utente sono spedite criptate tra i client ed i Radius server per eliminare la possibilità che qualcuno su una rete non sicura possa recuperare le password utente.

5. se il RADIUS server identifica una *shared secret* non corretta, la richiesta è scartata senza ulteriori elaborazioni

6. se il VPN Concentrator non riceve risposta dopo un determinato timeout, reitera la richiesta ed infine, in caso negativo, l'utente viene disconnesso

7. se le credenziali sono corrette, il RADIUS server si comporta da proxy e ruota il pacchetto verso il RADIUS server di autenticazione utilizzando le proprie policy interne, discriminando ad esempio in base al "Realm" estratto dall'attributo Radius username e se necessario modificando uno o più attributi contenuti all'interno del pacchetto di Access-Request come ad esempio la stessa username.

8. se nessuna delle policy è verificata il RADIUS server che funge da proxy invia un "Radius Access-Reject" al VPN Concentrator

9. Se una policy viene verificata il RADIUS server che contiene i dati per il controllo dell'utente riceverà ora un "Radius Access-Request"; il server verifica che l'indirizzo IP del sorgente nell'Access-Request appartenga ad un valido Radius Client e che la secret che i due apparati si scambiano sia quella corretta

10. una volta preso in carico il pacchetto il RADIUS server controlla le credenziali dell'utente secondo le proprie policy interne (ad esempio controllo login, password, DNIS chiamato e CLI chiamante con dial-up)

11. una volta superati positivamente tutti i controlli il Server invia un "Accept-Accept" al RADIUS proxy dopo aver modificato ed aggiunto attributi Radius secondo la policy configurata. Ad esempio viene valorizzato l'attributo Radius Class con il Realm di appartenenza della login; viene valorizzato l'attributo "Framed IP Address" se l'IP address è assegnato dal Server oppure l'attributo "Framed Pool" se l'IP address verrà assegnato dal VPN Concentrator.

12. il VPN Concentrator, ricevuto l'accept-accept, costruisce un "Accounting_Request" di start che è inviato al RADIUS server che fa da proxy sulle porte standard 1646 o 1813 e da questo al RADIUS server (se le policy interne al proxy lo prevedono, altrimenti si ferma al Radius proxy) e questo invia un acknowledgment quando questo è ricevuto.

13. se nessun acknowledgment viene ricevuto, il VPN Concentrator rinvia la richiesta per un certo numero di volte, nel caso non riceva nessuna risposta invia la richiesta ad un RADIUS server alternativo.

14. alla conclusione della sessione il VPN Concentrator genera un pacchetto di "Accounting" di stop, inviato sulla porta 1646 o 1813 valorizzando alcuni attributi della sessione,quali: Acct Imput Octets, Acct Output Octect, Acct Session Id, Acct Session Time, Acct Imput Packets, Acct Output Packets, Acct Terminate Cause.