L'infrastruttura per l'erogazione del servizio VPN prevede il soddisfacimento dei requisiti di alta affidabilità mediante ridondanza degli apparati critici e l'impiego di meccanismi automatici di *failover* allo scopo di limitare al minimo il disservizio in caso di avaria di un componente.

Alta Affidabilità senza bilanciamento del carico:

Se il carico atteso non è tale da giustificare il bilanciamento tra due o più apparati di concentrazione VPN attivi contemporaneamente , è possibile garantire l'alta affidabilità dei VPN concentrator ricorrendo al meccanismo di Hot-Standby.

In questa configurazione si impiegano due macchine uguali configurate allo stesso modo, du cui una preposta all'effettivo smaltimento del traffico e l'altra inattiva, pronta a subentrare alla prima in caso di avaria. La configurazione Hot-Standby dei concentratori è realizzata dal protocollo standard VRRP (Virtual Router Redundancy Protocol), per mezzo del quale due o più macchine gestiscono automaticamente un indirizzo IP condiviso.

In particolare i concentratori condivideranno un indirizzo IP sulla sottorete pubblica su cui sono attestati ed uno su quella privata (entrambi diversi dagli indirizzi assegnati alle interfacce). L'indirizzo VRRP pubblico servirà come punto di accesso al servizio VPN, mentre quello privato servirà per il routing dei pacchetti di ritorno.

In ogni momento un solo concentratore gestisce l'indirizzo VRRP, ossia prende in carico i pacchetti e quindi le connessioni VPN ad esso destinati. In caso di avaria della macchina attiva, l'altra subentrerà nella gestione dell'indirizzo automaticamente.

Alta Affidabilità con bilanciamento del carico:

Per ottenere una scalabilità virtualmente senza limiti è necessario adottare un approccio architetturale che preveda un dispositivo di bilanciamento anteposto a due o più concentratori; questo tipo di dispositivo garantirà contemporaneamente sia la ripartizione equa del carico in modo che tutti i concentratori possano essere utilizzati in uno stato attivo, sia la tolleranza alle avarie con esclusione immediata degli apparati che risultassero fuori uso dalle politiche di bilanciamento.

E' necessario quindi impiegare dispositivi di bilanciamento che supportino esplicitamente i protocolli VPN; è infatti richiesto da parte dei bilanciatori la capacità di analizzare alcuni dettagli dei meccanismi di instaurazione dei flussi appartenenti a tali protocolli (in particolate IPSec) per la corretta associazione dei pacchetti alle sessioni attive.