L'accesso al servizio di VPN da parte di utenti remoti attestati su rete Internet/Extranet è garantito da apparati noti come ***"VPN Concentrator"***; essi sono generalmente installati all'interno di un Data Center (Server Farm) preposto all'erogazione di servizi all'esterno (IDC).

I concentratori VPN attivano i tunnel su richiesta degli utenti solo se l'identità di quest'ultimi è stata accertata; la verifica delle credenziali utente (coppia username/password oppure certificati digitali X.509) è demandata ad un servizio RADIUS al quale i concentratori fanno riferimento.

Il servizio RADIUS centralizza la funzionalità di autenticazione reperendo le informazioni necessarie da tutte le sorgenti coinvolte; durante lo scambio delle informazioni di autenticazione il servizio RADIUS fornisce ai concentratori VPN un identificativo del gruppo di appartenenza dell'utente.
Il concentratore può utilizzare questa informazione per configurare opportunamente il client, ad esempio assegnando un indirizzo IP appartenente al pool particolare, oppure un DNS server specifico. Questo approccio garantisce la massima scalabilità dell'architettura.

Le macchine che realizzano il servizio RADIUS sono posizionate in un'area ad alta sicurezza che raggruppa i servizi vitali per l'infrastruttura.

Requisiti di infrastruttura:

Per poter erogare il servizio i concentratori VPN dispongono di indirizzi IP pubblici raggiungibili da Internet, di indirizzi privati appartenenti alla rete interna dell'organizzazione e di indirizzi attraverso i quali può avvenire la configurazione ed il monitoraggio dei concentratori stessi.

A questo scopo gli apparati dispongono di più interfacce Fast Ethernet, di cui:

La prima denominata "public" è collegata ad un segmento layer 2 (switch o Vlan) a cui corrisponde una sottorete IP di almeno sei indirizzi pubblici (maschera /29), così ripartita:

- due indirizzi per le interfacce "public" dei concentratori
- un indirizzo virtuale VRRP gestito dai concentratori
- due indirizzi per le interfacce dei router o firewall che permettono il raggiungimento del resto della rete Internet
- un indirizzo virtuale VRRP, gestito dai suddetti router, da configurare come default gateway dei concentratori.

La seconda interfaccia Fast Ethernet denominata "private" permette il raggiungimento della rete Intranet; essa è pertanto attestata su un segmento layer 2 a cui corrisponde una sottorete IP ad indirizzo privato, dalla quale è possibile raggiungere il resto della intranet. La sottorete in questione comprende almeno 6 indirizzi:

- due indirizzi per le interfacce "private" dei concentratori
- un indirizzo virtuale VRRP gestito dai concentratori
- due indirizzi per le interfacce dei router o firewall che permettono il raggiungimento del resto della Intranet
- un indirizzo virtuale VRRP, gestito dai suddetti router, da configurare come next-hop nei concentratori per le sottoreti che si intende rendere accessibili ai client remoti.

La terza interfaccia Fast Ethernet dei concentratori è attestata direttamente sulla LAN di management, oppure eventualmente su un'altra rete da essa raggiungibile, sulla quale sono riservati due indirizzi IP, uno per ciascun concentratore.

L'amministrazione ed il monitoraggio degli apparati, via HTML, Telnet o SNMP, avviene per mezzo di questi due indirizzi.

Pool address IP utenze e routing:

Il tunnel VPN che collega un client remoto con il concentratore attivo è concettualmente identico ad una connessione PPP dial-up.

Il client che instaura il tunnel riceve un indirizzo IP appartenente al piano di indirizzamento della Intranet della organizzazione aziendale, che gli permette di accedere alle risorse consentite.

L'assegnazione degli indirizzi ai client è effettuato dal concentratore VPN, il quale dispone a questo scopo di uno o più *pool* di indirizzi.

Benché in generale i *pool* di indirizzi possono essere di dimensione qualunque, nell'architettura del servizio VPN essi sono scelti coincidenti con delle sottoreti IP.

Infatti il traffico di ritorno dovuto ai client VPN remoti è composto da pacchetti destinati agli indirizzi di pool, pacchetti che devono necessariamente venire instradati dalla rete verso il concentratore di VPN che li incapsulerà e li invierà ai client su Internet.

Occorre quindi che i router coinvolti nei flussi di ritorno abbiano gli indirizzi dei pool in tabella di routing e che le rotte siano tali da far giungere i pacchetti all'indirizzo VRRP interno dei concentratori.

A questo scopo l'uso di pool di ampiezza compatibile con una subnet IP semplifica il processo di diffusione delle rotte tra i router; questo processo può avvenire manualmente mediante inserimento di route statiche nella configurazione dei router coinvolti, ovvero automaticamente sfruttando un protocollo di routing