L'ente di certificazione (CA) preposto al rilascio dei certificati digitali per l'autenticazione degli estremi del «tunnel IPSec» (VPN) sarà il CED Interforze del Ministero dell'Interno.

La sicurezza della comunicazione sarà garantita tramite l'adozione della suite di protocolli IPSec (Internet Protocol Security) per livello di rete (layer 3), mentre per il livello applicativo (layer 7) gli standard di sicurezza saranno assicurati mediante l'adozione del protocollo HTTPS (HTTP con protocollo sicuro SSL v3). In particolare per il protocollo HTTPS dovrà essere abilitata la porta 10036.

L'autenticazione al livello applicativo avverrà attraverso UserID e Password, il «concentratore interforze» richiederà il servizio di localizzazione utilizzando l'HTTP POST request e la risposta sarà inviata attraverso l'HTTP response.

In alternativa potrà essere gestita una mutua autenticazione tra Client (CED Interforze) e Server (Operatore di Telefonia) mediante scambio di certificati digitali [12]. L'ente di certificazione (CA) preposto al rilascio dei certificati digitali per la mutua autenticazione (HTTPS) sarà il CED Interforze del Ministero dell'Interno.

Nell'ambito dell'interconnessione tra il CED Interforze e gli Operatori di Telefonia - per il progetto 112 NUE - la **Figura 4** che segue illustra l'architettura generale di rete per l'accesso alla rete Internet da parte del CED Interforze.

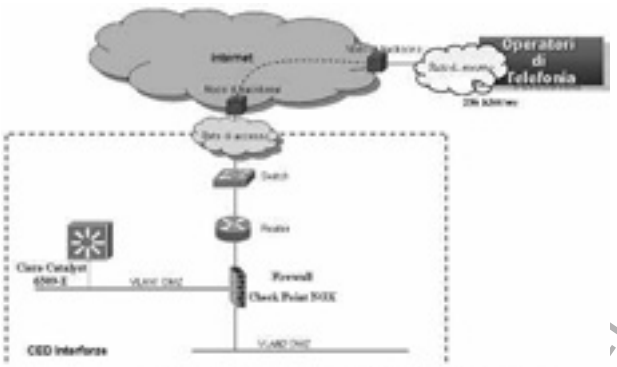

Figura 4 - Architettura di rete per l'accesso alla rete pubblica

Per quanto riguarda la capacità del canale di trasporto delle informazioni, considerando una dimensione massima per i messaggi ELIR o ELIA di circa 2 Kbyte, i dati di traffico in precedenza esposti ed infine l'overhead introdotto dal solo protocollo IPSec (circa il 20 %), si richiede agli Operatori di Telefonia (sulla propria rete di accesso) una banda minima garantita di 256 kbit/sec. In virtù dei requisiti del servizio 112 NUE, l'infrastruttura tecnologica dovrà essere ad *alta affidabilità*.

Di conseguenza, nelle soluzioni architetturali previste a livello di PSAP, CED Interforze e Operatori di Telefonia non dovranno essere presenti single-point-of-failure. Quindi, per l'*alta affidabilità* sarà necessaria la ridondanza nell'hardware previsto per i diversi «layer» dell'infrastruttura tecnologica [13].

Visto il requisito che prevede l'*alta affidabilità* per i diversi «layer» dell'infrastruttura tecnologica, anche il «Network layer» dovrà prevedere la ridondanza degli apparati di rete e dei link fisici per il collegamento alla rete pubblica o all'interno della rete locale. Infatti, una delle cause più comuni dell'interruzione dell'operatività è rappresentata da un guasto nel collegamento verso la dorsale (nodo di backbone) del «provider» di servizi Internet. Quindi, oltre al «collegamento principale» bisognerà prevedere anche un «collegamento di protezione» (**Figura 5**).

[12] HTTPS con mutua autenticazione.

[13] Ad esempio ambienti di «cluster» per Application & Database Server o ambienti di «load balancing» per Web Server (front-end).

***Figura 5** - Architettura di rete ad alta affidabilità per l'accesso alla rete pubblica*

Nel caso della ridondanza del router (in configurazione «Active Standby»), poiché i due apparati di rete avranno «indirizzi» differenti bisognerà prevedere un *meccanismo* (ad esempio: tramite l'adozione di protocolli HSRP, VRRP, ecc) che utilizzerà un unico «indirizzo» e lo assegnerà sempre all'apparato funzionante.

L'adeguamento ai requisiti generali di interconnessione in precedenza descritti si potrà realizzare secondo un piano da stabilire e concordare, ad esempio per fasi, definendo per ogni fase il livello di adeguamento dell'infrastruttura tecnologica fino ad arrivare alla garanzia del servizio 112 NUE, entro il completamento dell'attivazione del servizio su tutto il territorio nazionale.

2.4 *Sincronizzazione dei sistemi informatici*

Il «concentratore interforze» è il sistema informatico ubicato presso il CED Interforze del Ministero dell'Interno che prevede: da un lato l'interfaccia con i Centri Operativi **112** e **113** (PSAP) per la ricezione delle richieste di localizzazione e l'invio delle relative risposte, e dall'altro l'interfaccia con gli Operatori di Telefonia fissa per la richiesta del servizio di localizzazione. Le richieste di localizzazione provenienti dal PSAP (CO 112/113) - alla ricezione di una chiamata di emergenza - e ricevute dal CED Interforze saranno tracciate all'interno del database server del CED Interforze così come, le richieste del servizio di localizzazione inoltrate dal CED Interforze verso l'Operatore di Telefonia. Anche le risposte del servizio di localizzazione provenienti dall'Operatore di Telefonia e ricevute dal CED Interforze saranno tracciate all'interno del database server del CED Interforze così come, le risposte di localizzazione inoltrate al PSAP (CO 112/113) - che iniziò il processo di localizzazione -. Analogamente, anche gli Operatori di Telefonia dovranno prevedere il tracciamento e la registrazione in un apposito audit log, sia delle richieste di localizzazione provenienti dal CED Interforze che delle risposte inoltrate allo stesso CED Interforze [14]. Per quanto riguarda il tracciamento delle richieste e delle risposte di localizzazione, si potranno prevedere le seguenti informazioni di dettaglio:

Trace per la richiesta del servizio di localizzazione- CLI (Identificativo del chiamante);

— TIME.

Trace per la risposta del servizio di localizzazione;

[14] Ogni Operatore di Telefonia dovrà conservare tali dati (richieste/risposte di localizzazione) per un periodo di quattro mesi.