T42

Tunnel For Two

Secure SSL InterApplication Relay

Clizio Merli - 4u Srl

4u S.r.l.

Il package open source T42 (letteralmente “tea for two”, dove T ha però in realtà il significato di “tunnel”), un relay inter-applicativo sicuro basato sul protocollo SSL. Il package opera sia in ambiente Unix che in ambiente Microsoft Win32 come processo multithread, con il supporto del package di crittografia open source OpenSSL.

Il package è costituito da un daemon (T42) e da un configuratore, (T42conf, scritto in Visual Basic 6 e che opera solo in ambiente Win32).

Il package T42 viene rilasciato sia in formato sorgente che in formato eseguibile.

Architettura del daemon “T42”

Il daemon T42 è un processo multithread che opera come **proxy-handler** in base a due schemi:

CLIENT effettua il trasporto sicuro di una connessione richiesta da un applicativo client locale verso un server remoto con il supporto di un daemon T42 remoto

SERVER cattura una connessione sicura di un daemon T42 remoto che opera in modalità CLIENT e la rilancia verso un server applicativo locale

Essendo multithread il daemon T42 è in grado di gestire più connessioni sicure contemporaneamente, indifferentemente in modalità CLIENT che SERVER.

Proxy T42

Il daemon T42 gestisce solo servizi a connessione singola con server riconfigurabili sia in termini di indirizzo IP che di porta, in quanto opera in base al principio:

remap remote address and port on local address and port

In tal modo i processi applicativi perdono la consapevolezza della località fisica dei processi partner, operando sempre con partner locali, e demandando la responsabilità della effettiva localizzazione dei processi partner all’amministratore T42.

La sicurezza del trasporto viene garantita dall’adozione del protocollo SSL (Secure Socket Layer) con il supporto di certificati X.509 dedicati client e server per ogni singolo tipo di connessione.

La figura seguente illustra lo schema operativo di una connessione applicativa T42.

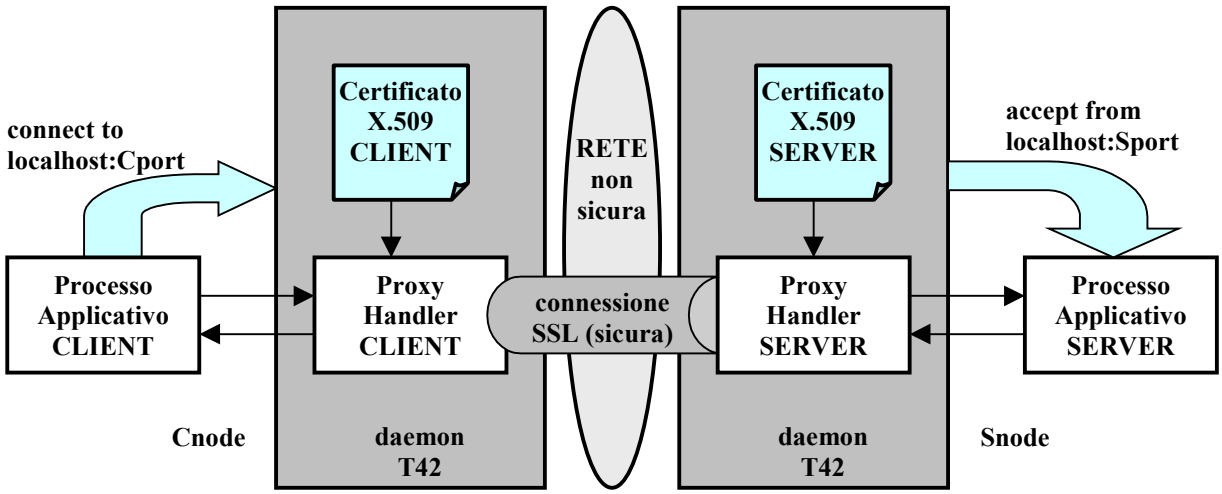


Figura 1 – Connessione applicativa sicura T42

In condizioni non sicure (senza l'utilizzo del daemon T42) i processi applicativi operano in base ad uno schema in cui il processo CLIENT deve conoscere l'indirizzo IP (o il nome DNS) del nodo di rete su cui risiede il processo SERVER, e quest'ultimo quando accetta la connessione è in grado di conoscere l'indirizzo IP (e il nome DNS) del nodo di rete da cui proviene la connessione.

In condizioni sicure (con l'adozione del daemon T42) i processi applicativi non hanno conoscenza della localizzazione in rete del processo partner, in quanto operano solo in un contesto locale: la conoscenza e il controllo della effettiva localizzazione dei processi applicativi è demandata ai daemon T42.

Il daemon T42 gestisce ogni connessione utilizzando certificati X.509 che possono essere differenti per ogni servizio e porta remota. Ogni certificato, locale o remoto, può essere rilasciato da Certification Authority differenti.

Su un singolo nodo di rete possono operare anche più daemon T42. L'unico vincolo è che ogni daemon T42 operi su un complesso di risorse di comunicazione (**host:port**) unico sul nodo, in quanto ogni risorsa host:port può essere allocata (tramite la primitiva 'bind') da un solo processo.

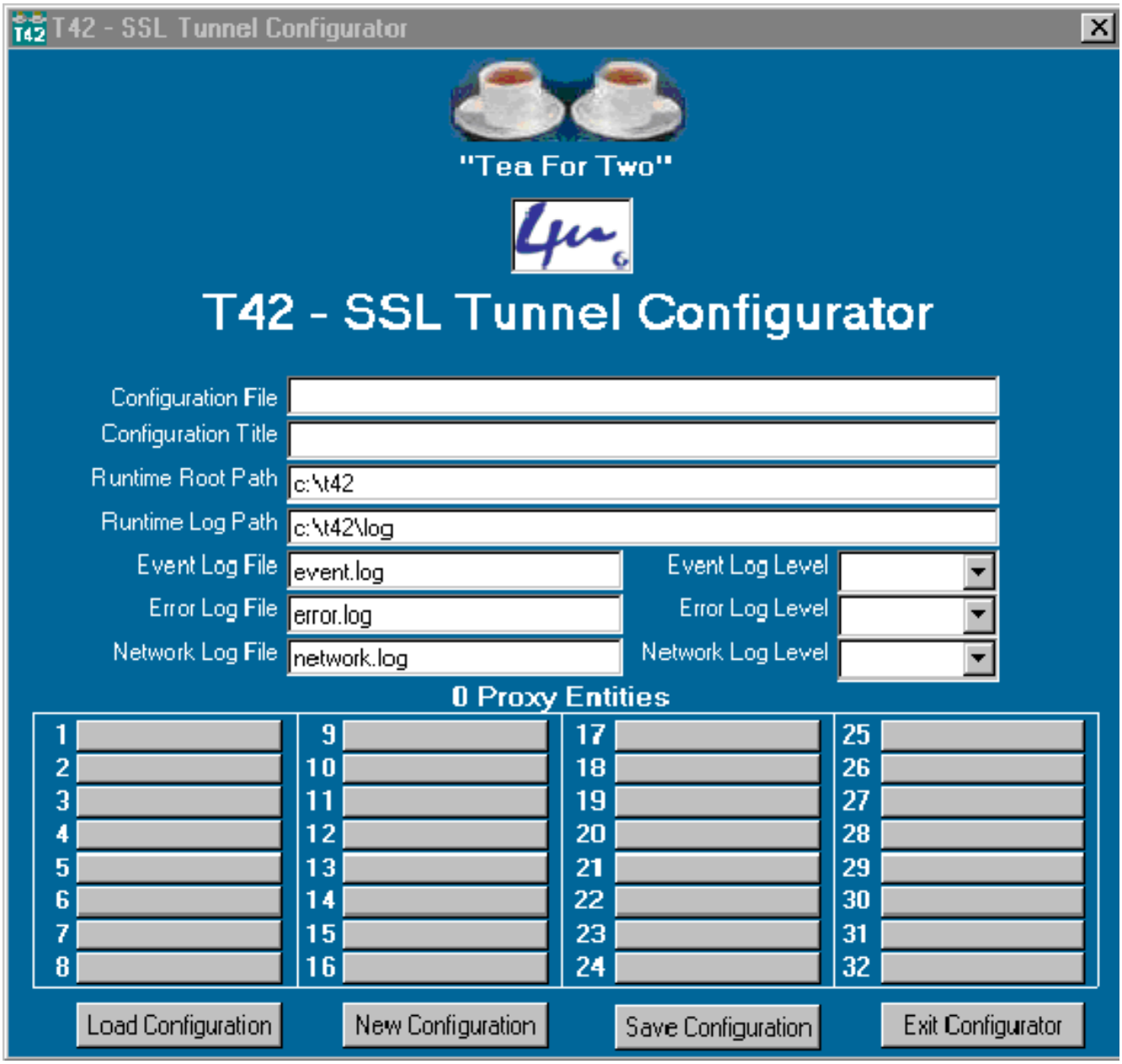
Le connessioni dei processi di tipo CLIENT possono provenire anche da altri nodi di rete, e quindi non essere necessariamente effettuati sull'indirizzo IP corrispondente a 'localhost' (127.0.0.1).

Configuratore Grafico T42CONF

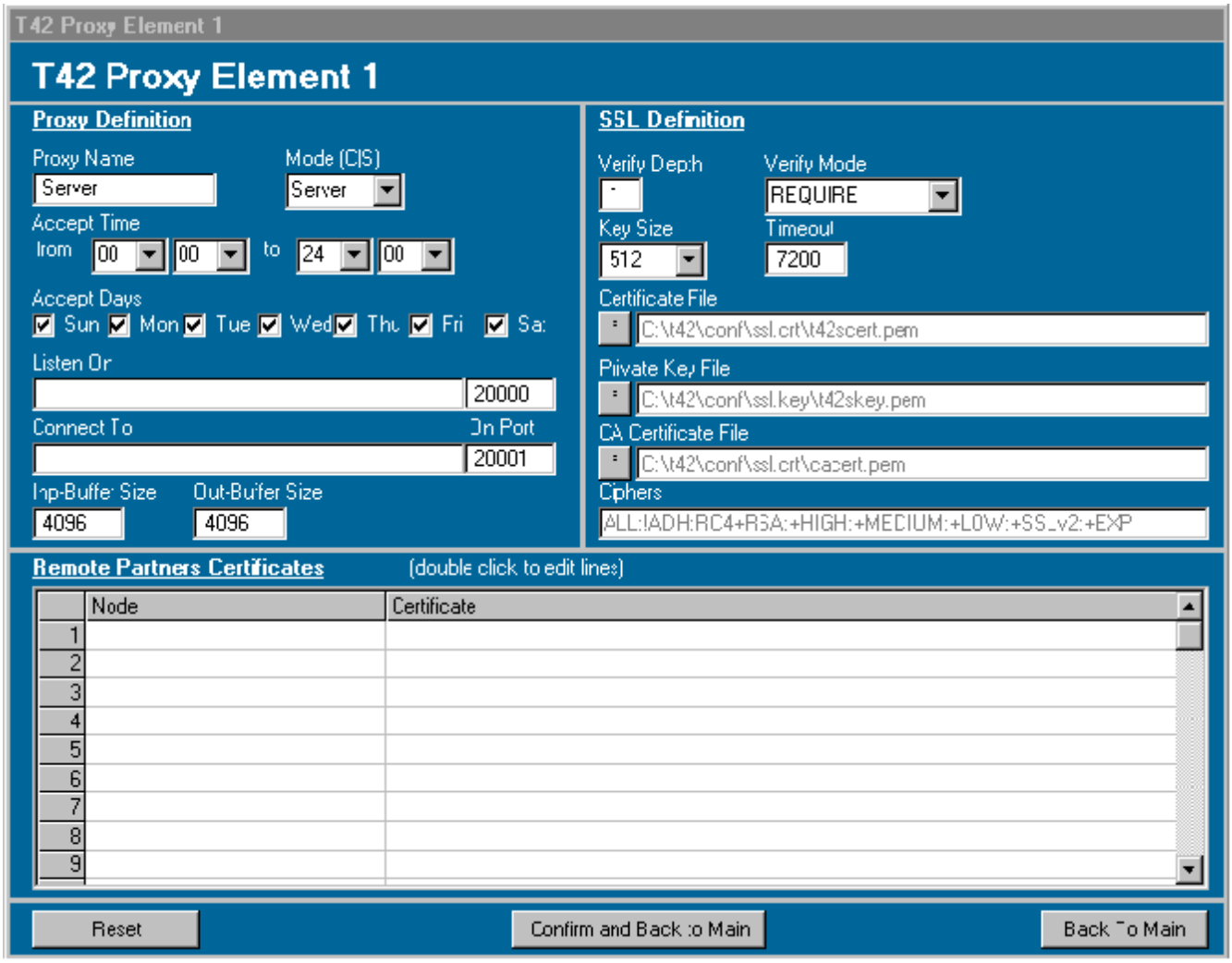
I file di configurazione T42 sono file testo, generati e mantenuti mediante un normale editor testuale. In ambiente Win32 è disponibile un tool grafico, T42conf.exe (applicazione Visual Basic 6.0), che permette di creare e gestite i file di configurazione T42 secondo una procedura aiutata di semplice utilizzo.

T42conf.exe opera con un pannello principale, e due pannelli secondari.

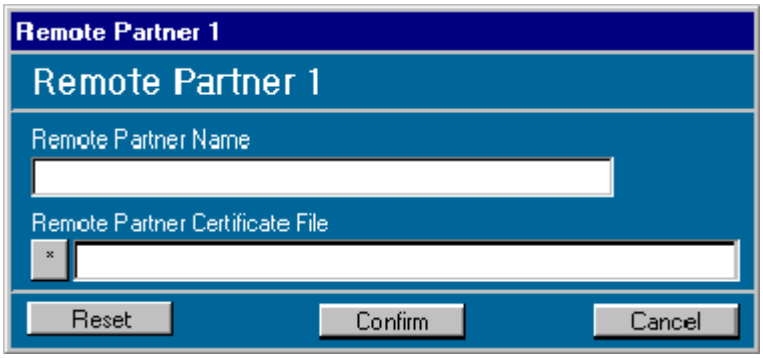
Con il pannello principale si possono effettuare le operazioni di selezione e salvataggio dei file di configurazione, la definizione dei parametri generali di impianto e la selezione dei proxy da configurare.



La configurazione di un proxy e del relativo profilo SSL viene effettuata con l'ausilio di un secondo pannello grafico, organizzato in tre sezioni (proxy, SSL, porte remote).



Per configurare le singole porte remote associate au un proxy si utilizza un terzo pannello grafico che permette di definire il nodo remoto e il relativo certificato.



T42conf.exe genera e tratta file di configurazione in cui ogni proxy ha un proprio profilo, un profilo SSL e un insieme di porte remote dedicati. Il nome del profili SSL e dell'insieme delle porte remote associati viene definito automaticamente in base al nome del profilo proxy impostato dall'operatore:

Nome del profilo proxy	<nome-utente>
Nome del profilo SSL associato	SSL<nome-utente>
Nome delll'insieme remoto associato	REM<nome-utente>