Gara europea per il servizio di assistenza e manutenzione hardware e software "on-site" di apparati di rete e di sicurezza (n. 18_006)

ALLEGATO VPN

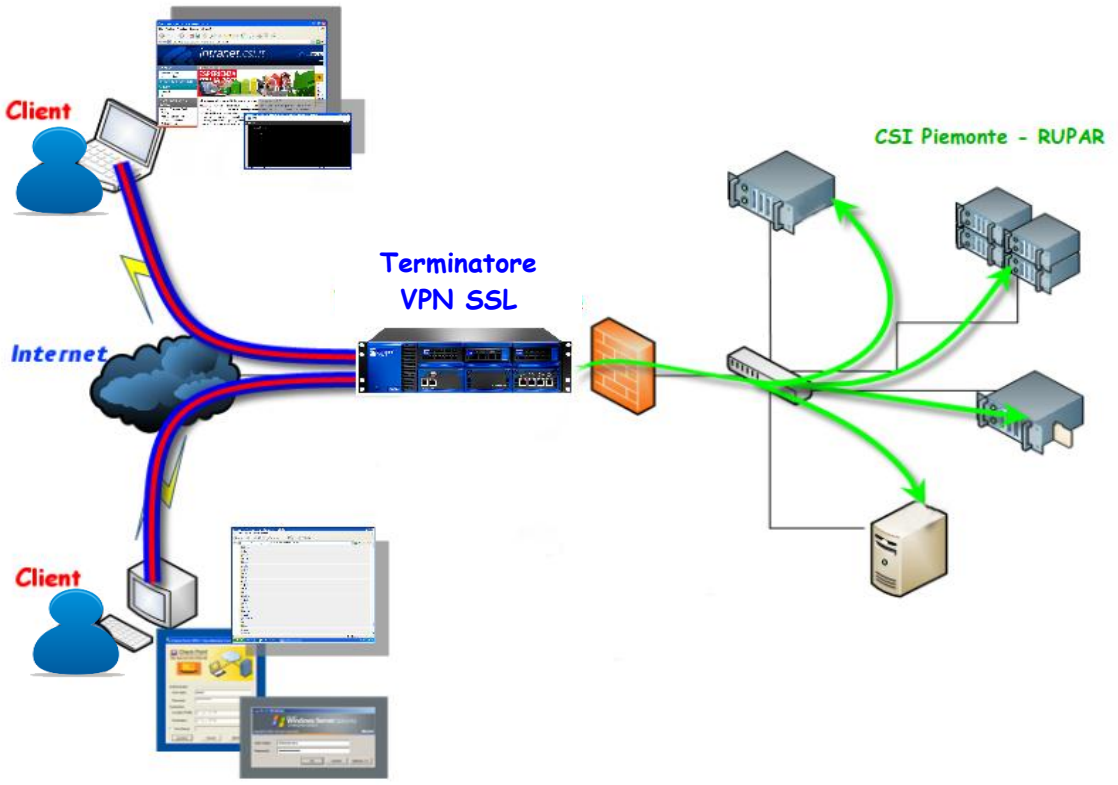
"SERVIZIO DI ACCESSO ALLA RETE CSI-RUPAR TRAMITE VPN SSL"

Premessa

Il presente documento descrive le principali caratteristiche del servizio di accesso alla rete CSI.

Descrizione del Servizio

Il servizio proposto è quello di configurazione e connessione tramite VPN SSL, che consente di realizzare un collegamento punto-punto tra la postazione cliente VPN SSL e la rete CSI senza necessità di un link fisico ma sfruttando la connessione Internet dell'azienda.
La realizzazione di canali logici sicuri tra la postazione dell'utente che accede in VPN SSL (Client) e la rete privata su cui si trovano i servizi, avviene attraverso l'impiego di un protocollo sicuro (SSL) gestito da una componente attiva presso CSI Piemonte e denominato "Terminatore VPN SSL".



Per una descrizione tecnica di maggior dettaglio sulle funzionalità del servizio si rimanda all'appendice tecnica allegata.

Il servizio di accesso tramite VPN SSL è disponibile in modalità gestita e presidiata dal Lunedi al Venerdì dalle ore 9 alle ore 17. Al di fuori di questi orari il servizio è sempre disponibile ma in

modalità non presidiata e pertanto ogni eventuale problematica sul servizio e segnalata fuori dall'orario di servizio presidiato verrà recepita ed espletata a partire dal giorno lavorativo successivo.

Prerequisiti

Per l'accesso al servizio sono richiesti alcuni requisiti tecnici e di configurazione del Client che sono descritti nel dettaglio nell'appendice Tecnica Allegata.

In generale sono richiesti:

- *HW (minimi)*: 1 processore 1 GHz, 1 GB RAM (256 liberi per il sw di connessione), NIC 10/100 Mbps
- *S.O.*: Windows XP SP3, Windows Vista SP2, Windows 7

  MacOs 1.04 o superiore

  Linux (Red Hat Enterprise, OpenSuse, Ubuntu)
- *Browser*: Microsoft IE 7.0 o superiore

  Firefox 3.6 o superiore

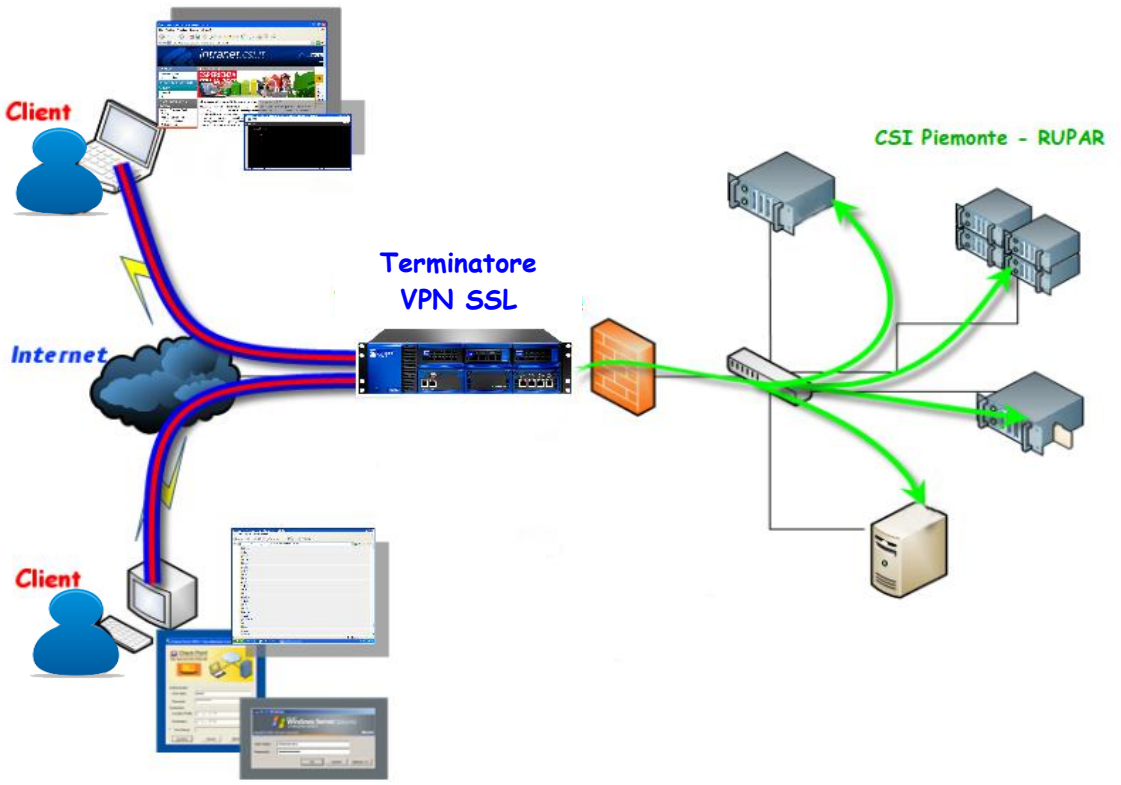
  Safari 3.0 o superiore
- *Configurazione*: L'accesso alla componente che effettua l'autenticazione e che stabilisce il canale sicuro avviene su protocollo https su porta 443/tcp, dopodichè l'accesso verso i servizi abilitati avviene con protocolli/porte utilizzati dai servizi medesimi. È quindi in generale necessario che sul client non vi siano configurazioni (es. di Personal Firewall o di AntiMalware) che blocchino la prima connessione su https - 443/tcp né i protocolli necessari per l'accesso ai servizi specifici.

La componente che permette di accedere al servizio di autenticazione e che attiva il canale sicuro di comunicazione viene installata automaticamente (al netto di configurazioni bloccanti sui client) alla prima installazione.

Pre-requisito vincolante, al fine dell'attivazione della VPN è che l'azienda richiedente abbia compilato in ogni sua parte – in coerenza con le attività affidate - e restituito al CSI-Piemonte il modulo denominato "Tabella misure sicurezza adottate", contenente la tabella di autovalutazione sulle misure di sicurezza fisica, logica e organizzativa adottate, debitamente sottoscritto dal Legale rappresentante della Società, e successivamente validato dagli uffici preposti del CSI. È ugualmente valida, in alternativa, la presentazione da parte della Società di analoga documentazione di sicurezza, debitamente sottoscritta, che dovrà comunque essere validata dagli uffici preposti del CSI-Piemonte.

APPENDICE TECNICA

l servizio **VPN SSL** vuole consentire l'accesso sicuro ai servizi della rete privata del CSI Piemonte o della RUPAR senza la necessità di avere un collegamento fisico, bensì utilizzando come infrastruttura di trasporto la rete pubblica Internet.
La realizzazione di canali logici sicuri tra la postazione dell'utente che accede in VPN SSL **(Client)** e la rete privata su cui si trovano i servizi, avviene attraverso l'impiego del protocollo **SSL**, i canali sono instaurati tra i Client e il **Terminatore VPN SSL**.



L'utilizzatore finale del servizio potrà accedere alla rete privata del CSI Piemonte e della RUPAR.

Per motivi di sicurezza sono stati impostati due modalità di Time out:

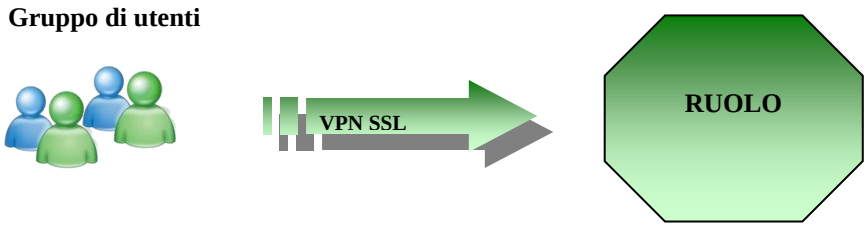
• **Time out per inattività**: se la risorsa non è utilizzata per un certo intervallo di tempo la connessione VPN SSL terminerà.

• **Time out per limite di utilizzo del servizio:** la disconnessione avviene quando l'intervallo di tempo prestabilito di utilizzo complessivo del servizio è terminato.

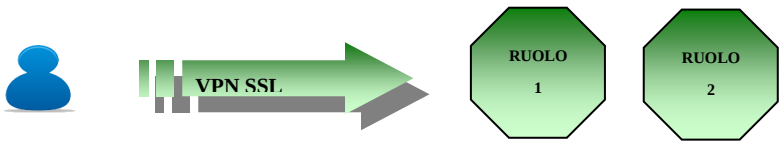
L'accesso alla rete privata è però regolato dalle policy di sicurezza.

Ad ogni utente, identificato tramite credenziali (es. username e password, token, etc…) verrà associato un **Ruolo**, costituito da un gruppo di policy, che rappresenta la **Profilazione dell'utenza.**

Gli utenti saranno inclusi in **Gruppi di Utenze** e di norma tutte le utenze di uno stesso gruppo avranno accesso allo stesso **Ruolo**.



In condizioni particolari un utente potrà accedere a più Ruoli.



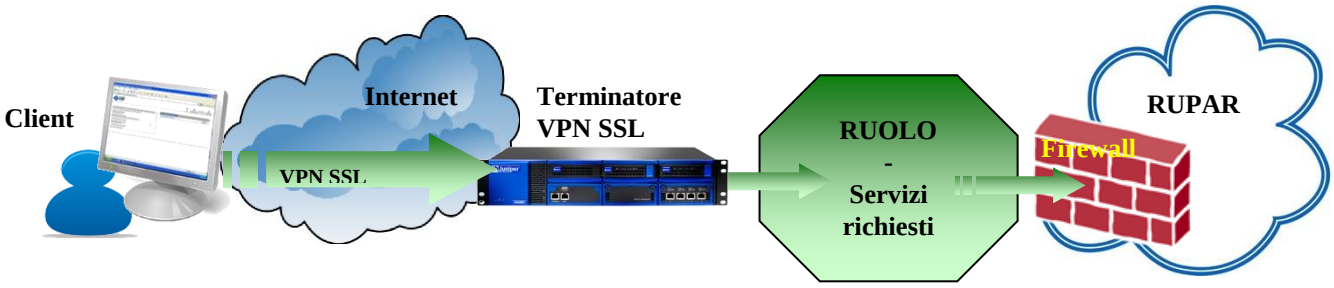
Dettaglio su Tipologia di Policy

A) Policy applicate sul terminatore VPN SSL
Sul terminatore vengono configurate policy di sicurezza sulle rotte che saranno erogate dalla VPN SSL e sulle porte dei servizi:
Esempio:
protocollo: UDP
Server da raggiungere 10.101.0.10
Porta: 53

Questa policy, per esempio permette l'accesso al DNS RUPAR.

B) Policy applicate sui firewall:
Una volta eseguito il controllo della **Profilazione utenza** sul terminatore VPN SSL l'accesso è regolato da policy corrispondentemente definite sui firewall della rete RUPAR

per consentire l'accesso agli IP rilasciati dal collegamento VPN SSL per un particolare **Ruolo.**



Prerequisiti:

Di seguito sono riportati i prerequisiti tecnici previsti per l'accesso da parte degli utilizzatori del servizio, che devono essere in possesso delle credenziali di accesso.

A. Configurazione del client che accede in VPN SSL

Il collegamento avviene utilizzando il protocollo sicuro **HTTPS** sulla **Porta** 443.

In generale è necessario che sulla postazione client non siano attivo software di gestione della sicurezza o impostazioni di sicurezza che possano impedire o bloccare il traffico HTTPS sulla porta 443/tcp (su cui avviene il collegamento verso l'interfaccia di autenticazione del concentratore VPN SSL).

In particolare (vengono citati i casi più frequenti che causano la mancata connessione) è necessario:

- ✓ Configurare i Firewall personali per consentire il traffico interessato sia dalla connessione iniziale sia dalla successiva attività operativa.
- ✓ Disattivare le policy di sicurezza locali del browser non interattive (es.: configurazione di sicurezza restrittiva che non avvisa l'utente in caso di blocco di un pop-up, ecc…)
- ✓ Disattivare o riconfigurare eventuali Toolbar o Barre di gestione della sicurezza del browser (Yahoo, Zonealarm, Google, ecc…)
- ✓ Configurare eventuali Policy di sicurezza di Dominio Windows Server (rivolgersi al proprio amministratore di sistema)
- ✓ Configurazione dei parametri di collegamento a un server Proxy (sul browser) in modo che il collegamento da browser ai servizi utilizzati non debbano transitare dal proxy
- ✓ Utenza Windows con privilegi di installazione locale

Al primo utilizzo sarà installato sul client il componente software necessario a creare il tunnel SSL. La non riuscita dell'installazione potrebbe dipendere da una configurazione della postazione di lavoro non standard, con applicazioni di policy di sicurezza che impediscono la corretta installazione dei componenti software (caso tipico: utenza non abilitata a fare installazioni sul PC).

In caso d'installazione non riuscita consultare il proprio amministratore di sistema per la verifica dell'impostazioni del sistema.

B. Specifiche hardware e software

I requisiti presenti in questo paragrafo sono condizioni indispensabili per la buona riuscita del collegamento e per usufruire dell'assistenza e supporto del CSI Piemonte.

Requisiti hardware:

Requisiti Hardware	Processore 1GHz o superiore
	Memoria RAM 1 GB / 256 MB disponibile per il collegamento o superiore
	Risoluzione del monitor ottimale 1024x768. Supportato fino a 2048x2048
	Scheda video: colore ottimale 16bit. Supportato fino a 32 bit.

Requisiti software:

	Sistemi Operativi	Browser	Arch. CPU
	Windows XP Professional con SP3	Microsoft Internet Explorer, versione 7.0, 8.0 Firefox 3.6	32 bit
	Windows Vista Enterprise con SP2	Microsoft Internet Explorer, versione 7.0, 8.0 Firefox 3.6	32, 64 bit
	Windows 7 Enterprise	Microsoft Internet Explorer, versione 8.0,9.0 Firefox 3.6	32, 64 bit
	Mac OS X 10.6	Safari 4.0	32, 64 bit
	Mac OS X 10.5.x	Safari 3.2 o superiore	32, 64 bit
	Mac OS X 10.4.x	Safari 3.0 o superiore	32 bit
	Linux Red Hat Enterprise	Firefox dalla versione 3.6	32 bit
	Linux Opensuse 11	Firefox dalla versione 3.6	32 bit
	Linux Ubuntu 10	Firefox dalla versione 3.6	32 bit

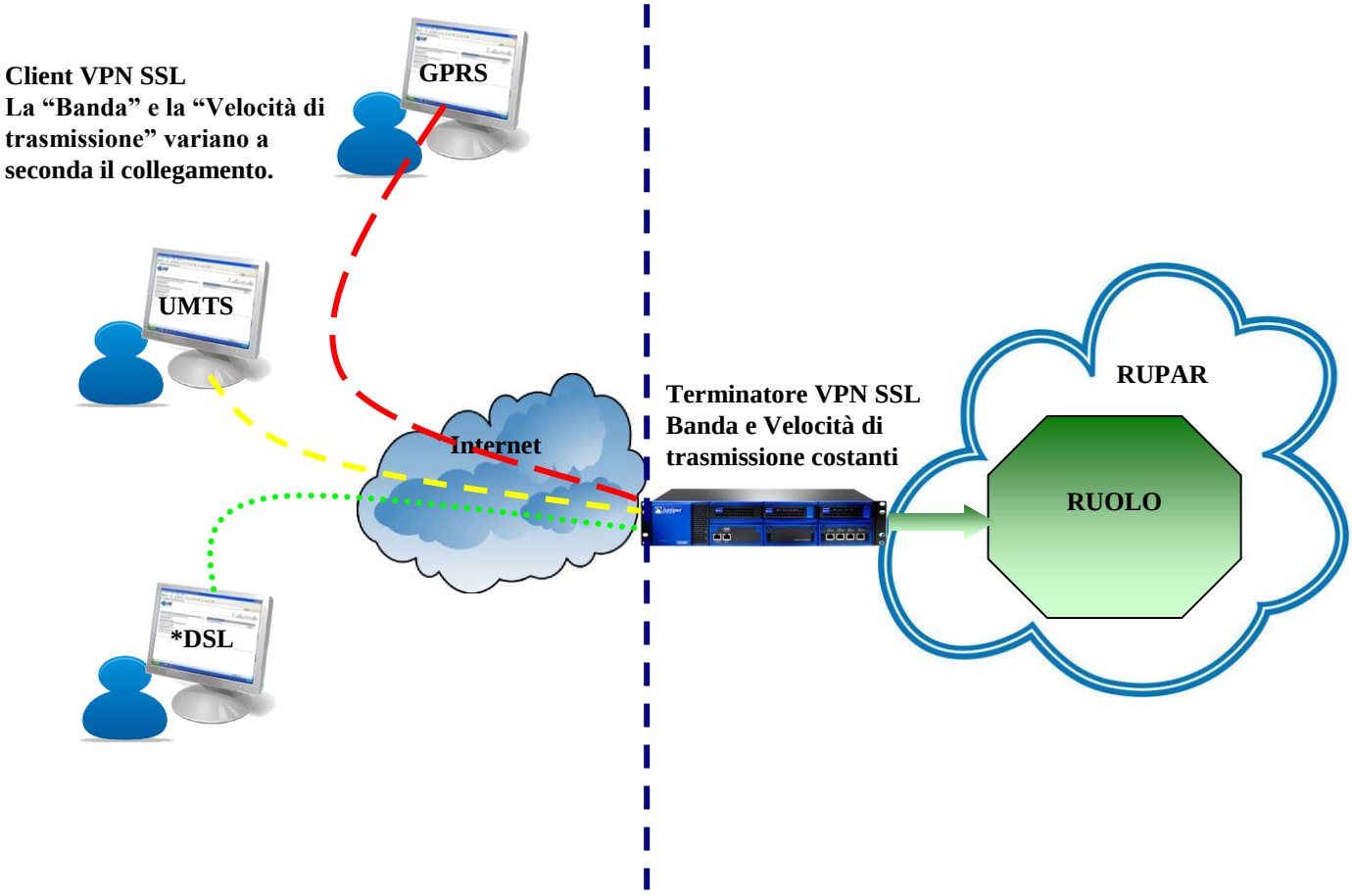
Altri software	**Sun JRE (Java Virtual Machine)**

Alcune funzionalità richiedono l'installazione di Java Virtual Machine (JRE).

C. **Collegamento Internet del Client: Concetto di "Best Effort"**

A causa della possibilmente limitata disponibilità di banda disponibile da parte del fruitore, le effettive prestazioni in termini di "**Banda**" e "**Velocità di trasmissione**" sono direttamente vincolate alla connessione Internet utilizzata al momento del collegamento.

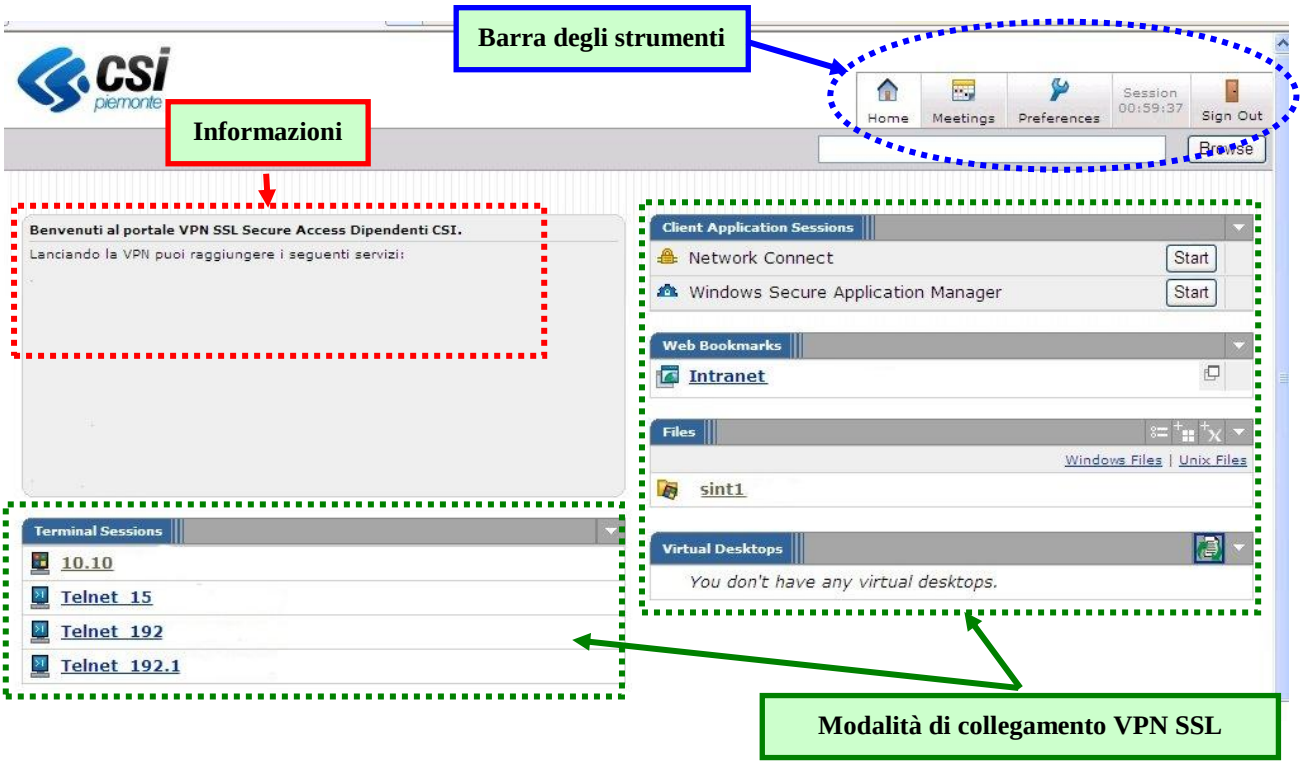
Per questo motivo il servizio VPN SSL è considerato **Best Effort**.



Anche le diverse "personalizzazioni" al sistema operativo delle postazioni che si collegano (client) e le provabili configurazioni di rete, firewall, Proxy, ecc della sede dell'utente determinano la condizione di "Best Effort" del servizio.

Il Portale dell'Utente

Di seguito si riporta un esempio del Portale che si presenta agli utenti che che hanno effettuato l'accesso al servizio e che, in funzione del proprio **Ruolo** ottengono la visibilità dei servizi presso la rete del CSI Piemonte o della RUPAR.



Le modalità di collegamento assegnate ai Ruoli variano a seconda dell'esigenza lavorativa