



TeleWorks "Secure & Easy"

Il telelavoro sicuro, affidabile e facile da implementare

Il Telelavoro nasce con lo sviluppo delle tecnologie telematiche.

Con il telelavoro sono stati superati i tradizionali confini fisici e logistici dell'ufficio. Grazie allo sviluppo della telematica aziende, lavoratori e attività possono seguire modalità, tempistiche e logiche molto più flessibili senza più vincoli fisici: è sufficiente avere l'ausilio di strumenti telematici.

È possibile lavorare da casa, in luoghi diversi dal proprio abituale ufficio o fisicamente distanti dalle sedi aziendali.

La modalità del telelavoro è destinata a crescere sempre di più proprio per le prerogative di flessibilità, risparmio e comodità che ha apportato alle dinamiche lavorative, ma è necessario avere la garanzia che lo scambio di informazioni tra il telelavoratore e l'azienda siano effettuate con la massima sicurezza e riservatezza.

Premessa

La necessità di comunicare in modo semplice, veloce e riservato, ha portato alla realizzazione di nuovi scenari di sicurezza, soprattutto per i collegamenti fra ambienti con sistemi operativi e dispositivi di accesso differenti fra loro.

Anche il concetto di "luogo di lavoro" ha acquisito un significato più allargato rispetto ad "ufficio" o "azienda", poiché sempre più spesso le persone hanno esigenze di connettività da luoghi diversi (casa, alberghi, Internet Point, etc.) ed in molti casi le aziende devono espandere il proprio sistema informatico verso strutture esterne, per poter interagire in modo più efficace con fornitori e società partner.

Ogni posto può diventare oggi luogo di lavoro se si dispone di Internet e della giusta tecnologia. Ma è anche vero che la trasmissione dei dati aziendali tramite Internet comporta ovviamente numerosi problemi legati alla sicurezza.

Obiettivi

NEST2 propone due soluzioni per mettere in comunicazione sedi della stessa azienda (partner e/o fornitori) e rendere possibile l'accesso sicuro alle risorse aziendali da parte di personale fuori sede.

Accesso con SSL-VPN. E' una soluzione adatta principalmente per comunicazioni tra il personale remoto e la sede aziendale (Client-to-LAN).

Scegliendo la soluzione **SSL-VPN** l'utente potrà accedere in modo sicuro alle risorse aziendali da qualsiasi luogo **semplicemente utilizzando un comune browser senza installazioni di software aggiuntivi e complicate configurazioni.**

Questa soluzione consente comunicazioni in modalità protetta **tra due dispositivi**, in genere un web server e un PC client, provvedendo all'autenticazione e all'autorizzazione degli utenti che accedono ai dati aziendali.

Dopo essersi autenticato, utilizzando le proprie credenziali di dominio, l'utente potrà accedere ad applicazioni Intranet, a documenti dei file server o prendere in gestione server e workstation via desktop remoto.

Tutto il traffico viaggerà in un tunnel cifrato SSL (Secure Sockets Layer), garantendo quindi la massima protezione per i propri dati.

Vantaggi

- **SSL-VPN** consente di instaurare un collegamento sicuro senza avere ulteriori software di comunicazione, ma semplicemente attraverso il proprio browser in https (Hypertext Transfer Protocol over Secure Socket Layer), il quale viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire le intercettazioni dei contenuti. Il login avviene sempre tramite la propria utenza aziendale e "proietta" la postazione all'interno dell'azienda, permettendogli di lavorare in piena libertà e sicurezza da qualunque luogo.

SSL-VPN significa sicurezza, affidabilità e manutenzione a bassi costi di gestione.



Accesso con VPN IPSec. E' una soluzione adatta principalmente per comunicazioni tra sedi aziendali (LAN-to-LAN), ma può essere usata anche per comunicazioni Client-to-LAN.

Il servizio di VPN IPSec consente di mettere in comunicazione sicura tramite rete pubblica sedi della stessa azienda o partner e fornitori, garantendo integrità e confidenzialità dei dati in transito, tramite protocolli che forniscono la cifratura del flusso di dati.

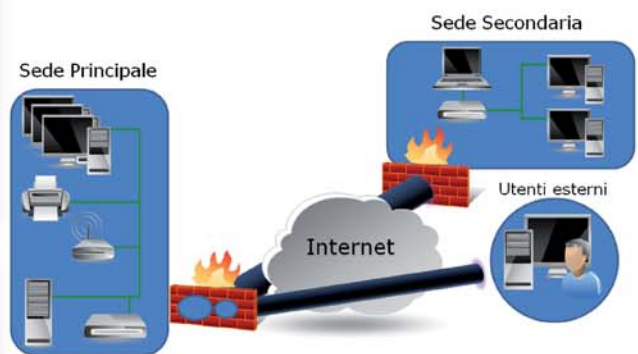
L'IPSec (abbreviazione di IP Security) è uno standard per ottenere **connessioni sicure tra reti IP**, tipicamente attraverso Internet.

Lo standard IPSec normalmente viene implementato installando un apparato di sicurezza presso ciascuna sede, che si occupa di effettuare la crittografia in modo completamente trasparente per l'utente.

La tecnologia IPSec è certamente sicura, ma prevede una certa dimestichezza da parte dell'utente per poter accedere ai dati aziendali.

- **VPN-IPSec** consente di instaurare un collegamento sicuro tramite appositi apparati installati a protezione dell'accesso Internet (p.e. Firewall o VPN Concentrator) o tramite un software-client di norma gratuito (nel caso di utenza mobile), garantendo l'accesso sicuro alla propria rete aziendale e ad altre reti, a seconda della configurazione di collegamento assegnata.

Come per l'SSL-VPN, in caso di personale mobile il login avviene sempre tramite la propria utenza aziendale.



Applicazioni

La flessibilità di queste soluzioni si presta ad adattarsi sia ad aziende multi sede e/o con personale viaggiante, come ad esempio banche, enti pubblici o grandi magazzini, sia ad attività prettamente legate alla manutenzione remota di apparati.

