

VPN

“Distanze? Le aziende si collegano in rete con le loro filiali, aprono uffici decentrati, promuovono il telelavoro oppure collegano i collaboratori remoti e i fornitori di servizi esterni alla loro rete locale. Poter disporre dei dati interni, indipendentemente dall’ora e dal luogo, è divenuta una cosa di tutti i giorni e un vantaggio concorrenziale decisivo: diminuisce i costi, aumenta la produttività ed offre la possibilità di servirsi delle risorse interne in qualsiasi momento, da qualsiasi luogo del pianeta e con qualsiasi computer, il tutto in modo sicuro. In questo mondo del lavoro virtuale le distanze non esistono più”.

Se anche voi volete avere un accesso veloce alle applicazioni interne, un accesso esclusivo per voi, la vostra azienda e i vostri collaboratori, e volete proteggere i dati confidenziali da qualsiasi accesso non autorizzato, allora una VPN è la soluzione migliore e Argonet il partner giusto.

ARGO.NET

“Vorrei che anche i nostri collaboratori potessero accedere sempre e ovunque alla nostra rete per consultare i file di cui hanno bisogno. E che potessero farlo in modo semplice e sicuro”.



VPN

_ Che cos'è una VPN?

Una VPN ("Virtual Private Network") collega due reti, un computer e una rete o due computer utilizzando la rete pubblica Internet. Affinché la trasmissione di dati sia al riparo da qualsiasi intrusione esterna, un cosiddetto protocollo di tunneling provvede alla cifratura e alla decrittazione sicure dei dati scambiati. Grazie a questo tunnel, che rimane chiuso per gli altri, all'utente autorizzato sembra di utilizzare la rete pubblica come se fosse quella aziendale.

_ Da punto a punto: VPN IPSec

Le soluzioni VPN oggi più diffuse sono quelle basate su IPSec ("Internet Protocol Security"). Inizialmente le VPN IPSec servivano a mettere in comunicazione diversi luoghi, come ad esempio una sede centrale e le sue filiali. Affinché gli utenti che si trovano all'esterno di un firewall aziendale possano accedere alle risorse interne, un IPSec crea il "tunneling" appena descritto, ossia un collegamento protetto. Esso richiede l'impiego, alle due estremità del tunnel, di software e apparecchiature hardware compatibili. Nel caso di un IPSec, è l'azienda a stabilire quale tecnologia debba essere adottata ad entrambe le estremità del tunnel.

Se un utente si trova fuori dalla rete aziendale e vuole accedere attraverso una VPN IPSec ai dati dell'azienda, sul computer da cui egli tenta l'accesso - un portatile o il desktop del suo home office (remote access) - deve essere installata una versione aggiornata di un software client VPN. Questi client devono essere configurati in funzione dell'ambiente in cui si opera e della rete che si utilizza. L'installazione di tale software consente l'impiego di questo tipo di collegamento anche durante gli spostamenti. Tuttavia, sempre nel caso di una rete IPSec, se il computer di un utente non dispone di un client preinstallato - è il caso ad esempio del computer di casa o dei computer di un Internet café - l'utente non ha nessuna possibilità di accedere ai dati aziendali.

La VPN IPsec è perciò particolarmente adatta per una comunicazione punto a punto con postazioni e utenti fissi effettuata attraverso terminali gestiti a livello dell'IT aziendale. Gli home office o il collegamento in rete delle filiali sono tipici esempi dell'impiego di questa tecnologia.

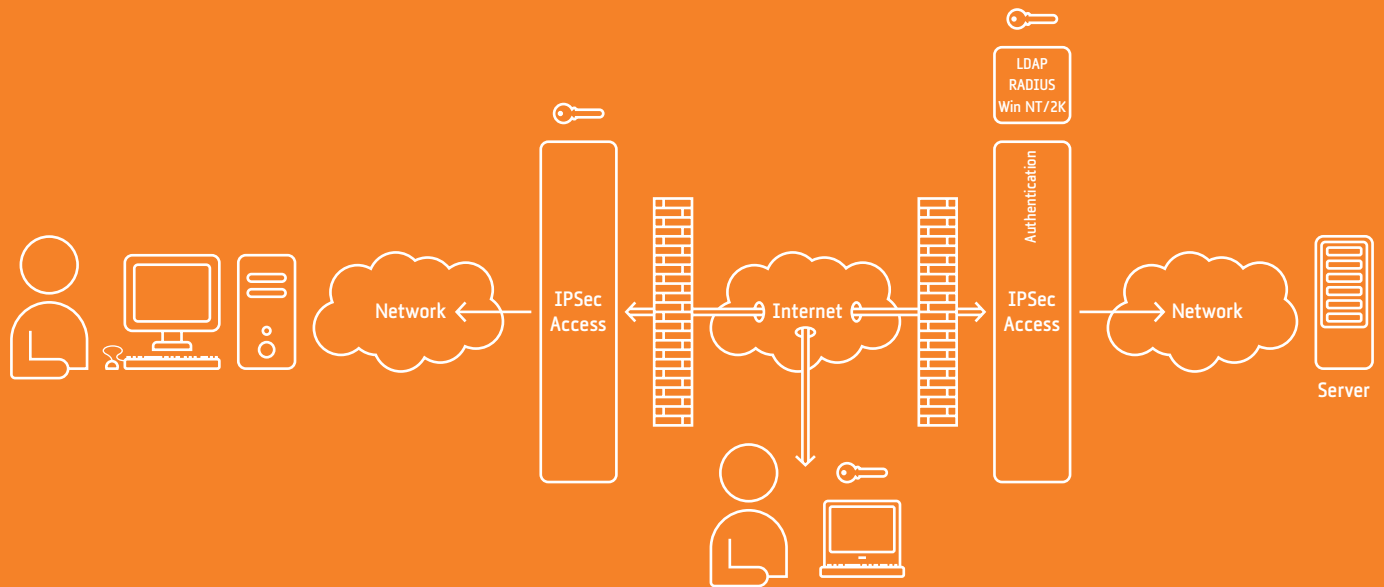
_ Mobilità: VPN SSL

Le soluzioni VPN basate sul protocollo SSL ("Secure Sockets Layer") si sono imposte soprattutto per rispondere alle esigenze degli utenti mobili. In questo caso, perciò, il tunnel, ossia il canale che garantisce la sicurezza di una trasmissione dati su Internet, viene creato grazie a un altro protocollo. Il successo dell'SSL è dovuto al fatto che esso è supportato dai più comuni browser Web (Microsoft Internet Explorer, Netscape e Mozilla). Tutto ciò garantisce l'accesso remoto alla rete interna senza che vi sia bisogno di uno speciale software client. Gli utenti possono accedere da qualsiasi periferica con accesso Internet (il computer della business lounge in aeroporto, un portatile, un palmare o una qualsiasi altra periferica wireless) alle loro applicazioni e ai loro dati. Prima di ammettere un utente, la VPN SSL analizza il computer da cui si tenta l'accesso. La rete privata virtuale basata su SSL, infatti, è in grado di riconoscere se si sta utilizzando un computer dell'azienda (in cui, ad esempio, l'antivirus è aggiornato) o un computer di un Internet Café. L'accesso, quindi, può essere concesso, limitato o negato in base al risultato di questa analisi.

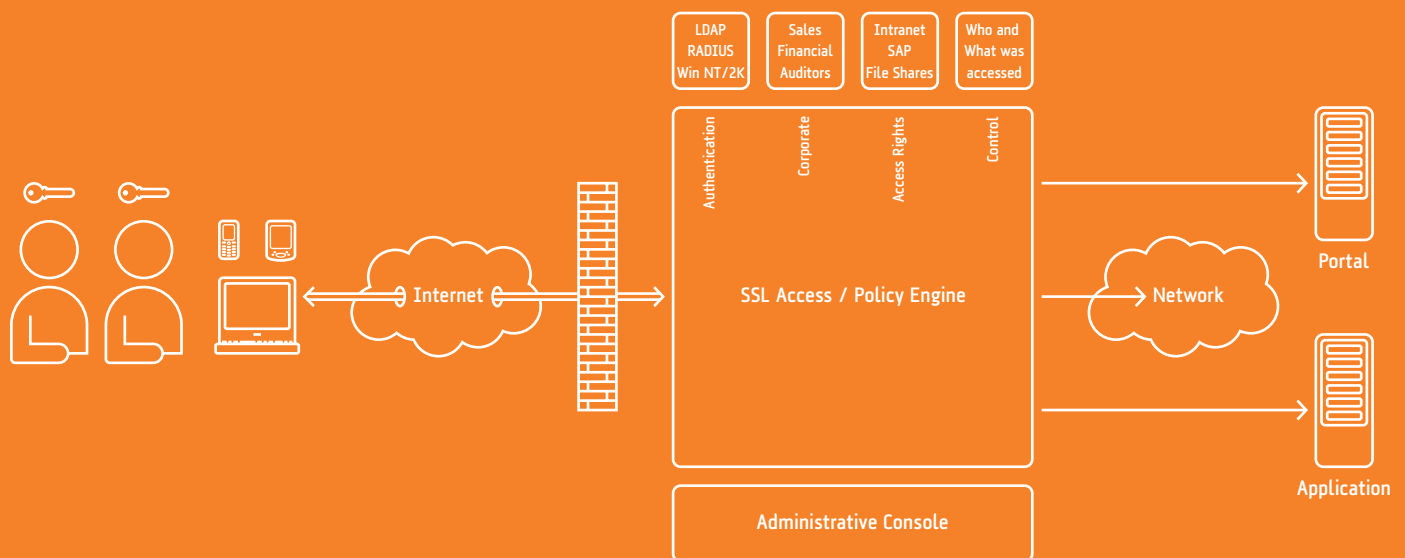
L'accesso clientless semplifica tutto, giacché non è necessario preinstallare nei computer esterni alcun programma da aggiornare o da gestire personalmente. L'utente, inoltre, accede ai dati attraverso una normale interfaccia, ossia il familiare internet browser.

Gli utenti ottengono così senza problemi un accesso sicuro, controllato e realizzato su misura per le loro esigenze e le loro autorizzazioni. Essi quindi possono accedere alle applicazioni e alle risorse più importanti come i programmi e-mail, gli strumenti CRM, il software per il business management, le risorse intranet, le applicazioni specifiche dei clienti o ancora il file server dell'azienda. In tal modo le applicazioni scalari, come ad esempio quelle per il personale mobile di un servizio tecnico, sono facilmente e velocemente realizzabili. Se l'identificazione standard dell'utente tramite ID e password risultasse insufficiente, i cosiddetti meccanismi di "strong authentication" (certificati, smart-card o token card) offrono una sicurezza supplementare.

VPN IPSec



VPN SSL



La soluzione giusta?

Sono le esigenze specifiche del cliente a determinare se un VPN SSL è la soluzione giusta. Se un'azienda desidera migliorare la comunicazione tra postazioni fisse di una rete interna, la scelta giusta è IPSec. Se invece nella comunicazione aziendale devono essere inclusi anche i collaboratori mobili, i partner commerciali esterni, i fornitori e i clienti, l'IPSec si rivela inadeguato. Per un accesso sicuro, personalizzato e clientless ai dati confidenziali da qualsiasi luogo, in qualsiasi momento e da qualsiasi computer con accesso a Internet, la soluzione ideale ed economicamente più vantaggiosa è rappresentata dagli VPN SSL. La VPN SSL, inoltre, consente la gestione di un certo accesso a seconda delle esigenze dell'utente e delle autorizzazioni concesse a quest'ultimo dall'azienda. Queste autorizzazioni granulari possono essere gestite in modo semplice e centralizzato, e riguardano applicazioni specifiche, URL o semplici file. Tali autorizzazioni possono essere modificate, revocate o riassegnate dall'azienda stessa in modo centralizzato e con un paio di click. Per un grado di sicurezza ancora più alto.

A livello pratico le due soluzioni risultano, in molti casi, complementari. Accanto alle specifiche esigenze dell'azienda, infatti, bisogna tener conto di possibilità di accesso differenziate in funzione dei diversi gruppi di utenti e delle diverse richieste. In tal modo, ad esempio, le filiali di una banca possono essere collegate alla rete aziendale tramite una VPN IPSec, mentre gli utenti mobili come il management, i consulenti e i partner esterni possono ottenere un'autorizzazione ad accedere a tale rete attraverso un VPN SSL, autorizzazione realizzata in base alle esigenze di ognuno di loro. Situazioni analoghe si presentano nel caso delle amministrazioni pubbliche, delle assicurazioni, delle aziende del settore finanziario, degli ospedali e delle imprese industriali medie o grandi.

_ VPN su misura

L'accesso alle risorse interne tramite una Virtual Private Network (VPN) basata su IPSec, su SSL o su una combinazione dei due sistemi, offre numerosi vantaggi. Nell'ambito della realizzazione è necessario tenere in considerazione soprattutto tre punti: la sicurezza, la disponibilità e i costi d'investimento. In questo caso, un'analisi dettagliata delle esigenze specifiche di un'azienda è di importanza decisiva. Una consulenza qualificata è estremamente importante se si desidera che il proprio investimento si riveli conveniente.

_ Come lavoriamo

Argonet vi mostra le diverse possibilità e, insieme a voi, realizza soluzioni intelligenti, soluzioni su misura per voi e per le vostre risorse interne. In ambito di software e hardware, ci avvaliamo della collaborazione di importanti aziende del settore (Nokia, Juniper, F5, Cisco, ecc.). Ciononostante conserviamo sempre la nostra indipendenza, per poter tutelare ad ogni decisione un solo interesse: quello dei nostri clienti.

Dall'installazione di reti locali all'integrazione degli utenti mobili, Argonet realizza su misura la soluzione ideale. Sulla base delle vostre specifiche esigenze elaboriamo la configurazione migliore, occupandoci nel contempo dell'integrazione e della gestione della VPN, ossia di tutto quello di cui avete bisogno e che non potete affidare ai collaboratori del vostro reparto IT.

Qualsiasi VPN scegliate, Argonet vi aiuta a costruire una rete privata virtuale che offra il massimo grado di sicurezza e la massima efficienza dei costi. I nostri collaboratori elaborano insieme a voi un progetto che viene quindi realizzato sotto la loro responsabilità. Il nostro capo progetto, inoltre, coordina tutte le fasi dell'installazione. In qualità di azienda certificata ISO - l'unica del settore con sede in Ticino - Argonet integra nell'intera realizzazione del progetto un management della qualità.

Componete il vostro servizio Argonet utilizzando i nostri moduli.

_ Modulo 1 Audit

Team: Account Manager,
Technical Account Manager

- _ Formulazione della richiesta
- _ Analisi delle esigenze
- _ Registrazione delle richieste / Condizioni generali
- _ Bozza di progetto

_ Modulo 2 Pianificazione

Team: Account Manager,
Technical Account Manager

- _ Pianificazione delle scadenze
- _ Presentazione dei costi
- _ Capitolato
- _ Offerta
- _ Piano del progetto (Pianificazione risorse / collaboratori)

_ Modulo 3 Realizzazione

Team: Project Manager, Account
Manager, Technical Account Manager

- _ Specificazione delle funzioni / Progetto dettagliato
- _ System Integration
- _ Installazione
- _ Sviluppo
- _ Implementazione
- _ Test e collaudo

_ Modulo 4 Assistenza

Team: Account Manager, Technical
Account Manager

- _ Assistenza
- _ Servizio 24 ore su 24 Support / Manutenzione
- _ Tempo di reazione: 1 ora

_ Modulo 5 Gestione

Team: Argonet

- _ Outsourcing

Naturalmente il successo della realizzazione del progetto pre-suppone una documentazione dettagliata di tutte le sue fasi. Grazie ad Argotrack, in ogni momento è possibile controllare e seguire on-line lo stato di ciascun progetto.

Parlatene con noi.

Siamo un team di esperti e di professionisti altamente qualificati nel settore delle reti telematiche e della teleinformatica. L'unico con sede in Ticino ad avere ottenuto la certificazione ISO 9001:2000. Partner affidabile di importanti imprese e istituzioni regionali, nazionali e internazionali, lavoriamo per diverse industrie, banche e PMI ticinesi. Sempre al loro fianco e sempre a portata di mano. Per una consulenza, per l'hardware e il software, per l'integrazione di sistemi, come pure per il servizio di assistenza e per la manutenzione. Noi, infatti, possiamo offrirvi tutto ciò di cui avete bisogno. In modo indipendente e sempre su misura per voi.

ARGO.NET