

Privacy e sistemi virtuali

Il vantaggio che le reti VPN SSL offrono alle aziende è la capacità di utilizzare browser Web SSL come normali client software sempre disponibili.

Da quando l'accesso a Internet è diventato una realtà diffusa, le aziende se ne servono per collegare alle risorse interne dipendenti, partner e, se necessario, clienti. A tale scopo sono state sviluppate numerose tecnologie. VPN SSL è una delle più recenti, ma si sta diffondendo rapidamente grazie alla capacità di superare alcuni limiti che altre soluzioni non hanno, come ad esempio IPSec.

Fatta questa premessa, occorre precisare che le reti VPN SSL cambiano da prodotto a prodotto: non ne esistono due perfettamente uguali, anche se le funzioni possono essere simili. Questo significa che le aziende devono valutare attentamente le soluzioni disponibili, prima di decidere quale acquistare. Raramente il modo più semplice per affrontare questo tipo di problema è la consultazione di schede tecniche e materiale simile, visto che le soluzioni per l'accesso remoto di singoli produttori possono presentare enormi differenze di utilizzo.

Piuttosto, un metodo più efficace consiste nell'analizzare il problema dal punto di vista personale, esaminando i componenti essenziali di una soluzione per l'accesso remoto di livello enterprise. Stratecast Partners, divisione di Frost & Sullivan, definisce tali componenti nel modo seguente: Connettività, Sicurezza e Prestazioni/Amministrazione.

Connettività

La bellezza di Internet è la possibilità di accedere alle informazioni da qualsiasi posizione. Questa caratteristica ha favorito la diffusione dell'accesso remoto come modo di lavorare, creando tendenze sociali come la mobilità e il telelavoro e rendendo possibile persino il consolidamento, dal momento che viene meno la necessità di supportare gran parte delle infrastrutture nelle filiali. Il vantaggio offerto dalle reti VPN SSL alle aziende è la capacità di utilizzare browser Web SSL come normali client software sempre disponibili. Il risultato è che l'amministrazione del client software viene praticamente eliminata. A questo proposito, entrano in gioco i sistemi operativi supportati dal dispositivo di accesso; ad esempio, le soluzioni basate esclusivamente su Windows sono più comuni. La soluzione FirePass di F5 offre un ampio supporto per sistemi operativi Windows e non Windows, oltre a supportare l'accesso a portali, applicazioni e reti come standard nei prodotti 4000 / 4100.

Sicurezza

Va da sé che la sicurezza è un aspetto assolutamente fondamentale in questa area, per i motivi citati prima. Per evitare di esporre le informazioni riservate e l'integrità della rete a minacce gravi, occorre creare e applicare criteri di protezione. In caso contrario, possono verificarsi perdite di dati, interruzioni del servizio, problemi normativi e legali, per arrivare a un possibile danno di immagine qualora la violazione della protezione diventi di dominio pubblico. In questo senso, dunque, è necessario adottare un approccio alla protezione di tipo end-to-end. È opportuno che le aziende prendano in considerazione l'adozione di soluzioni VPN dotate di funzionalità quali protezione della rete aziendale, controllo dell'accesso alle applicazioni e protezione delle applicazioni da operazioni (intenzionali o meno) non autorizzate, come la modifica dei cookie o il cross-site scripting.

Prestazioni/Amministrazione

Tenuto conto delle complessità associate alla protezione dell'accesso remoto, prestazioni e gestibilità sono aspetti fondamentali. Ciò che si può ottenere per il primo può deludere nel secondo, generando un'esperienza utente limitata e problemi di amministrazione. Il numero e l'intensità di elaborazione delle funzioni del gateway nelle reti VPN SSL sono considerevoli e destinati ad aumentare. Ma il principale fattore di valutazione delle prestazioni per l'utente finale resta la qualità dell'esperienza, e con il passare del tempo questo scenario è destinato ad espandersi per abbracciare sistemi operativi e browser sempre più numerosi e diversi.

Da Sapere

È fondamentale che le soluzioni per l'accesso remoto di fascia enterprise possano integrare facilmente caratteristiche di connettività da qualsiasi posizione, in qualunque momento, conciliando gli aspetti di protezione di reti e applicazioni, prestazioni dal punto di vista di amministratori e utenti e attributi del gateway aziendale.