



Article de Mathieu Grignon  
Directeur des services de sécurité  
ESI Technologies

### **Le protocole SSL, une option intéressante pour les réseaux privés virtuels des entreprises**

Au cours de la dernière décennie, l'utilisation des réseaux privés virtuels (VPN) a connu une très forte progression. Dans un premier temps, la commercialisation d'Internet a facilité leur mise en œuvre puisque l'utilisation des VPN, basés sur un réseau public, devenait beaucoup plus économique. Par la suite, la nécessité d'obtenir plus de mobilité en raison de la croissance du télétravail et des extranets a contribué à accroître la popularité des VPN.

#### Le protocole IPsec

L'IPsec a été développé par l'IETF (Internet Engineering Task Force) pour soutenir l'échange sécuritaire de paquets au niveau de l'IP, pour authentifier et crypter les données transmises. L'IPsec (*IP security*) est associé à la couche de transport du modèle OSI et permet de sécuriser les accès à distance par VPN. Il est indépendant des applications et fournit une sécurité étanche lors des échanges d'information, mais présente un inconvénient majeur. Le client VPN doit obligatoirement installer un IPsec sur chacun des postes de travail, puisque ce dernier reconnaît les PC et non les personnes.

Un élément qui complique le déploiement d'un réseau privé virtuel dans un environnement multiutilisateur, malgré le fait que de nombreuses améliorations techniques aient été apportées au fil des ans. L'installation du VPN basé sur IPsec demeure donc plus complexe, presque un casse-tête pour les grandes organisations.

De plus, cette caractéristique associée aux IPsec confine le réseau aux seuls ordinateurs appartenant au parc de l'organisation, puisque l'on ne peut installer le client que sur les appareils dont on a la maîtrise. Pas question dans ce cas, de se relier à un serveur d'entreprise à partir d'un cybercafé, ni de fournir un accès aux clients et aux partenaires. Or, pour éviter les problèmes et empêcher les actions hostiles à leur égard, certains endroits, dont les hôtels, bloquent les accès IPsec.

#### Le protocole SSL

Devant ces difficultés, de plus en plus d'entreprises choisissent une solution alternative : le protocole SSL. Conçu à l'origine par Netscape à des fins de transmission de documents confidentiels par Internet, le *Secure Socket Layer* (SSL) existe depuis un certain temps déjà. Toutefois, son utilisation pour sécuriser les VPN n'a commencé qu'il y a quelques années. Le développement de petits clients Java et ActiveX a joué un rôle en ce sens, en permettant aux VPN munis de SSL d'offrir les mêmes fonctionnalités que l'IPsec. Pendant longtemps, personne n'avait songé à baser son réseau privé virtuel sur SSL, même si on savait déjà qu'on pouvait en retirer des avantages indéniables.

Le premier avantage du protocole SSL est d'être déjà intégré à tous les navigateurs Web. Ce qui élimine la nécessité d'installer le client VPN sur tous les postes et facilite la mise en oeuvre du réseau. Le deuxième avantage se rapporte à ses fonctionnalités de gestion, car il est permis de se brancher à l'environnement de l'organisation depuis n'importe quel ordinateur, peu importe où il se trouve. Il suffit à l'utilisateur d'entrer le nom du lien Web, son code et son mot de passe. Grâce à la simplicité de cette connexion, faite à partir d'une page Internet, l'utilisateur n'a besoin d'aucune formation particulière.

Troisième avantage, le VPN combiné à SSL offre une fonctionnalité accrue par rapport à son pendant IPsec, puisqu'il agit au niveau applicatif ce qui permet de déployer un véritable portail dans l'ensemble du réseau. L'entreprise peut alors s'en servir pour diffuser diverses informations et enrichir par la même occasion ses communications internes et externes.

Il y a cependant un bémol, IPsec offre une sécurité plus étanche que SSL, puisqu'on sait à l'avance quels ordinateurs se connecteront au réseau et ainsi en contrôler plus facilement l'intégrité. Ainsi, il existe deux options supplémentaires qui s'offrent avec certains produits de VPN jumelés à SSL. Premièrement, le système peut faire une vérification du poste avant de le laisser établir une connexion VPN, il recherchera la présence de « *malware* », l'existence d'un anti-virus à jour, une certaine version de OS et bien plus. Deuxièmement, dans le cas où un poste ne passerait pas le test, le système pourrait lancer le poste de travail en mode virtuel. Puisqu'on est complètement indépendant du OS guest, cette option aurait l'avantage de nous empêcher d'hériter de ses vulnérabilités. Grâce à cette option, il serait également possible d'empêcher le transfert de données d'un environnement à un autre.

#### Analyse de rentabilisation du VPN

Le VPN combiné à SSL suscite un intérêt croissant et depuis deux ans, le nombre d'installations a littéralement explosé. Au début, les coûts de mise en oeuvre étaient plus élevés, de sorte que son utilisation se limitait à la grande entreprise. Aujourd'hui, la PME a rejoint le mouvement et certaines entreprises comptant à peine 25 employés utilisent un téléphone réseau.

C'est que le prix d'une passerelle SSL a beaucoup diminué. On peut l'acheter pour environ 10 000 dollars afin d'accommoder une cinquantaine d'utilisateurs et pour 55 000 dollars, on pourra en brancher un nombre illimité. Et dans certains cas, on peut ajouter les fonctionnalités du VPN associé à SSL à notre pare-feu. Sachant ceci, les grands fournisseurs de matériel de sécurité se sont mis au goût du jour, comprenant bien que le VPN basé sur SSL est là pour rester.

Même si de nombreuses organisations choisissent de faire passer leur réseau privé virtuel client d'IPsec à SSL, le coût demeure le principal frein à une telle initiative. La justification financière du VPN associé à SSL peut s'avérer difficile lorsque l'on a déjà déployé le protocole IPsec, mais les entreprises qui doivent investir dans la mise à jour de leur réseau IPsec pourront y voir une bonne occasion de le changer. Si, la dépense en matériel est supérieure avec un réseau SSL, ce n'est pas l'unique facteur à prendre en considération dans l'analyse de rentabilisation.

D'abord, le déploiement du protocole SSL est substantiellement plus économique, puisqu'il n'exige pas que soit installé un client VPN sur chacun des postes de travail. Quant au réseau IPsec, plus il y a d'utilisateurs, plus son déploiement est onéreux.

Le même raisonnement peut s'appliquer au soutien technique, dont le coût variera en fonction du nombre d'utilisateurs que compte le réseau. La mise en oeuvre d'IPsec étant plus complexe et la connexion ne pouvant s'établir de partout, les appels à l'aide seront plus nombreux. Par contre, la convivialité du réseau SSL fera en sorte que la demande de soutien technique

diminuera au fur et à mesure que les utilisateurs s’y habitueront. Il s’agit là d’un élément clé, dont il faut tenir compte dans le calcul des coûts globaux.

À part les coûts de maintenance plus élevés pour l’organisation qui choisit de déployer un portail par l’entremise de la passerelle SSL, les deux passerelles s’équivalent lors de l’installation. En revanche, IPsec entraînera des coûts beaucoup plus considérables pour la maintenance des postes de travail – dépenses pratiquement nulles avec SSL.

IPsec génère aussi des coûts de sécurité importants, en raison de la nécessité d’installer des pare-feu personnels. Avec SSL, par ailleurs, des dépenses de sécurité doivent être faites lors du déploiement, mais elles s’avéreront passablement moins élevées.

Dans l’analyse de rentabilisation, l’organisation doit aussi soupeser des facteurs moins tangibles comme la portabilité, la fonctionnalité et la satisfaction des utilisateurs. Des éléments qui sont tous susceptibles de donner des points de plus à SSL.

Au bout du compte, la prolifération des VPN basés sur SSL et les prédictions des analystes, sur ses progressions au cours des prochaines années, laissent présager qu’il y aura à moyen terme une diminution de l’utilisation et du déploiement des réseaux privés virtuels basés sur IPsec.