Sécurité

Quelle technologie pour les accès distants sécurisés?

SOLUTIONS. S'il est incontesté que VPN IPSEC est un bon choix pour la sécurisation des connexions de type site à site, qu'en est-il des connexions de type clients vers le réseau de l'entreprise? Un article de e-Xpert Solutions.

Mobilité Les entreprises et leurs employés étant de plus en plus mobiles, la technologie doit suivre...

De plus en plus d'entreprises offrent déjà, où veulent offrir, un système d'accès distants sécurisé à leurs ressources informatiques internes. Ces accès vont du système de messagerie interne, à l'intranet, aux serveurs de fichiers, aux applications métiers (ERP, CRM, SCM), etc. Ces nouveaux services sont utilisés aussi bien par les collaborateurs internes que les partenaires, les clients, etc. Quant aux méthodes d'accès, elles vont du portable d'entreprise, du PC personnel, du Kiosk Internet, aux PDA, etc.

Cette diversité de moyens d'accès, de type de population et d'applications fait qu'aujourd'hui il n'est pas simple de choisir la bonne technologie VPN d'accès distant sécurisé.

Depuis quelques mois, on entend beaucoup parler de VPN SSL comme étant la solution de remplacement de la technologie IPSEC pour les accès distants. Mais avant de voir les avantages et les inconvénients, voyons le principe de base d'un VPN utilisant la technologie SSL.

Le protocole SSL

SSL est un protocole qui a été développé par Netscape en 1994 (Version 1.0). Le but de ce protocole était d'offrir des services de sécurité point à point pour leur navigateur. SSL est capable de garantir la confidentialité, l'authentification et le contrôle d'intégrité des données en utilisant des mécanismes classiques de cryptographie (encryptions symétrique, asymétrique et fonction de «hachage»). SSL est essentiellement basé sur la technologie PKI, notamment pour l'authentification du serveur par l'intermédiaire d'un certificat numérique. Aujourd'hui, SSL est principalement utilisé par les navigateurs internet (http://...) mais il est possible de l'utiliser dans d'autres contextes comme, par exemple, pour sécuriser une communication de type «ldap» ou pour «tunneliser» d'autres protocoles. On parle alors de protocole «over SSL».

Technologie VPN SSL

Dans le cadre de la technologie VPN SSL, l'idée est d'utiliser ce protocole pour sécuriser les accès distants vers l'entreprise. Dans ce sens, il s'agit souvent d'une solution de type «appliance» que l'on connecte directement sur une zone publique de son firewall d'entreprise (DMZ). Cette «appliance» sert alors de terminaison SSL au navigateur du poste nomade qui, au préalable, est authentifié. La plupart des solutions constructeurs sont capables de supporter les mécanismes d'authentification forte* tels que RSA SecurID, certificats numériques (Token USB, smartcard, «soft certificate»), et le protocole radius.

Une fois authentifié, l'utilisateur peut accéder à ses applications classiques dans son navigateur internet.

Mais comment cela fonctionne-t-il?

Suivant les constructeurs, il existe plusieurs approches : Reverse Proxy, Transformation HTTP vers l'applicatif Webify, Helper Software, Tunneling:

Reverse Proxy.
Il s'agit de la méthode la plus simple mais elle fonctionne uniquement avec un applicatif final «web enabled». L'idée est de simplement relayer les requêtes HTTP vers l'application que l'on désire atteindre. Cette méthode est très efficace en termes de performance et de portabilité (pas d'installation de code mobile).

Webify. L'idée est de transformer un certain nombre de protocoles connus (messagerie, transfert de fichiers, Netbios, etc.) en code HTML pour que le navigateur puisse l'interpréter. Cette méthode présente malheureusement des limitations en termes d'applications supportées.

Helper Software. C'est l'idée la plus utilisée. Il s'agit d'un code mobile chargé la première fois sur le poste nomade. Ce code peut être du Java ou un activeX. Cette solution permet alors virtuellement de déporter tout type d'applications internes via des technologies similaires à Citrix ou Terminal Server de Microsoft. L'inconvénient est qu'elle demande un peu plus de puissance côté poste nomade et dans certains cas les droits administrateurs.

Tunneling. La dernière solution est basée sur l'encapsulation de protocole dans SSL. Il existe là aussi plusieurs approches :

• Le tunnel classique SSL : cette solution consiste à ouvrir une session SSL entre le client et son serveur (Appliance SSL). Une fois celle-ci ouverte, l'application cliente se connecte alors sur son adresse IP de type «localhost» (127.0.0.1) puis entre dans le tunnel pour en ressortir du côté de «l'appliance». Alors celui-ci relaie cette connexion vers l'applicatif final. Cette méthode présente toutefois une limitation : elle ne peut qu'encapsuler des protocoles de type TCP.

• PPP over SSL : cette solution est beaucoup plus intéressante que le tunnel classique. En utilisant un lien de type PPP dans un tunnel SSL, il est alors possible de transporter tout type de protocoles (TCP, UDP et ICMP). Ce mode de fonctionnement est alors très proche d'une solution VPN utilisant la technologie IPSEC. Dans ce mode de travail, il est fortement recommandé d'utiliser un firewall personnel.

IPSEC client : les points forts

La technologie IPSEC est incontestablement une très bonne solution en termes de sécurité. Elle offre au même titre que SSL la confidentialité, l'intégrité et l'authentification en utilisant aussi les mécanismes de cryptographie moderne.

Cependant, IPSEC est supérieure à SSL en termes de sécurité. IPSEC est capable de changer régulièrement la clé de session symétrique lors de la même session alors que SSL garde la même. IPSEC supporte l'algorithme AES pour le chiffrement des données alors que la majorité des applications SSL ne l'ont pas encore implémenté. De même qu'il est «facile» d'effectuer une attaque de type «Men in the Middle» sur SSL, il est difficile de la réaliser avec IPSEC.

IPSEC client : les principaux points faibles?

Le principal point faible d'un client IPSEC est son déploiement sur les postes nomades. Pour chaque poste, il est nécessaire d'installer un logiciel VPN. Ce logiciel est très intrusif sur la machine car il travaille à un niveau très bas dans la couche ISO (niveau 2 et 3) et ceci induit bien souvent des problèmes techniques d'interopérabilité. Pour une grande entreprise, ce déploiement peut vite devenir un calvaire! Du fait de la nécessité d'un client VPN, il n'est pas possible d'accéder aux ressources de son entreprise depuis un Kiosk Internet.

Un autre point faible est le niveau de complexité technique engendré par un déploiement de clients IPSEC. Cette complexité est due principalement à des problématiques de routages IP qui nécessitent bien souvent la mise en œuvre d'une solution de translation d'adresses (NAT), la problématique de la translation d'adresses au niveau du provider internet qui nécessite aussi la mise en place d'un mécanisme appelé «NAT Traversal».

Conclusion

A la vue des principaux points faibles de la technologie IPSEC pour les accès distants, je pense que la technologie SSL est une bonne solution pour offrir aux utilisateurs un système simple pour accéder de manière sécurisée aux ressources internes classiques de l'entreprise. Cette solution est en effet en mesure d'offrir une grande facilité de déploiement au sein de l'entreprise et surtout de faciliter la gestion des postes nomades.

Toutefois, IPSEC n'est de loin pas à négliger, surtout dans des environnements demandant un haut niveau de sécurité et pour des ressources internes particulières. Je pense notamment à des accès de gestions systèmes et réseaux (administrateurs). ●

Sylvain Maret, directeur veille technologique e-Xpert Solutions SA

*Note : pour offrir des accès distants sécurisés, il est fortement recommandé de mettre en œuvre un mécanisme d'authentification forte, par exemple quelque chose que l'on possède et quelque chose que l'on connaît.

e-Xpert Solutions SA

Au bénéfice d'une longue expérience dans les secteurs financiers et industriels, e-Xpert Solutions propose à sa clientèle des solutions «clés en main» dans le domaine de la sécurité informatique des réseaux et des applications. Des solutions qui vont de la sécurité d'architecture – tel le firewall, VPN (SSL, IPSEC), le contrôle de contenu, l'antivirus, filtrage d'URL, code mobile – aux solutions plus avant-gardistes comme la prévention des intrusions (approche comportementale), les firewalls applicatifs HTTP, l'authentification forte, la biométrie, les architectures PKI ou encore la sécurisation des OS Unix et Microsoft et des postes clients (firewall personnel).