

INTERVIEW DE ...

Ghislaine Labouret, consultant en sécurité informatique chez Hervé Schauer Consultants (HSC)

« Les produits actuels ne comportent qu'une partie restreinte des fonctionnalités IPsec. Malheureusement, les fonctionnalités manquantes sont trop souvent les algorithmes de chiffrement et les méthodes d'authentification les plus sûres. »

G. Labouret (HSC) : « IPsec ne nécessite aucune modification des applications utilisées »

Dans votre étude (www.hsc.fr/veille/ipsec), vous affirmez que l'usage d'IPsec pourra se généraliser lorsque le protocole IPv6 sera en place. Concrètement, aujourd'hui, où en est cette disponibilité ? D'autre part, l'entreprise, qui souhaite mettre en œuvre IPsec, est-elle dépendante de ses fournisseurs d'accès et d'équipements ?

Pour l'instant, IPv6 n'est pas finalisé et encore loin d'être répandu, d'autant que sa complexité technique n'est pas à la portée de tous. En revanche, IPsec est utilisable, dès à présent, sous IPv4 sans changement important au niveau du réseau. IPsec doit être mis en place dans le réseau de l'entreprise et sa configuration maîtrisée depuis l'intérieur de l'entreprise. Son utilisation est – et doit être – indépendante du fournisseur d'accès. Éventuellement, l'entreprise vérifiera que celui-ci fournit bien un accès sans restriction qui ne filtre pas les protocoles IPsec.

IPsec ne nécessite aucune modification des applications utilisées, il est totalement transparent. La seule chose à acquérir est un système mettant en œuvre IPsec. Pour utiliser IPsec, l'entreprise doit vérifier que ses systèmes (matériel ou logiciel) intègrent ces fonctions étendues. C'est le cas en particulier des produits garde-barrière (ex : Firewall-1 de Check Point à partir de la version 4.0); des routeurs (ex : Cisco IOS à partir de la version 11.3.(3) T); des boîtiers dédiés (généralement prévus pour la création de VPN); des produits pour machines clientes ou serveurs (ex : KAME, linux-ipsec, OpenBSD, DEDICACE-VPN de Dassault Électronique, implémentation dans AIX 4.3 de Bull SA...). Dans ce dernier cas, les implémentations sont faites directement dans le noyau du système d'exploitation et modifient la pile TCP/IP. Cela peut aller d'une implémentation native dans le système d'exploitation (comme pour OpenBSD et ce sera sans doute le cas pour la prochaine version de Windows NT) à un simple module à ajouter sur la machine. Une machine, qui possède un OS comprenant IPsec ou un module IPsec s'interfaçant avec sa pile réseau, est alors en mesure d'utiliser ce protocole pour protéger ses échanges avec d'autres machines « compatibles IPsec ». En fonction du type de solution souhaité, il convient donc de se renseigner auprès du fournisseur correspondant.

À ce propos, est-ce un marché nouveau pour les fournisseurs ? Où en est le décollage de ce marché ?

Actuellement, les offres commerciales existant à l'heure sont très orientées VPN. C'est un inconvénient car IPsec couvre des situations plus larges qui ne sont pas prises en compte. Les implémentations gratuites et ouvertes, en revanche, sont généralement plus géné-

ralistes. Avec la parution des RFC en novembre 1998 et la mode grandissante des VPN, on a assisté ces derniers mois, aux États-Unis, à une explosion du nombre d'offres IPsec. La France réagit pour le moment de façon plus modérée, mais l'apparition de plusieurs produits français ou disponibles dans l'Hexagone indique que le marché français dans ce domaine est loin d'être inactif. Après l'effet de mode qui a entouré les VPN, lesquels étaient souvent associés à la notion d'économie sur le prix des communications, les entreprises prennent de plus en plus conscience de l'importance globale de sécuriser leurs échanges et l'accès à leurs réseaux internes.

D'une façon générale, il faut modérer l'explosion par le fait que beaucoup d'implémentations ne sont pas matures et ne comportent qu'une partie restreinte des fonctionnalités d'IPsec. Malheureusement, les fonctionnalités manquantes sont trop souvent les algorithmes de chiffrement les plus performants (en niveau de sécurité comme en vitesse) et les méthodes d'authentification les plus sûres.

Concrètement, qu'apporte de plus IPsec par rapport aux solutions de chiffrement actuellement disponibles ? Les apports principaux sont, à mon avis, au nombre de trois :

- une meilleure sécurité, IPsec a été conçu pour être cryptographiquement fort, ce qui le distingue de beaucoup de solutions propriétaires dont la sécurité est souvent illusoire ;
- une garantie de qualité, IPsec est une norme ouverte qui a été développée, depuis 1992, par une équipe internationale composée de personnes compétentes, et ce, au sein d'un groupe de travail de l'IETF (voir <http://www.ietf.org/html.charters/ipsec-charter.html>), ce qui est un gage de qualité de conception ;
- une garantie d'interopérabilité entre équipements de revendeurs différents, si ceux-ci respectent la norme.

La mise en œuvre d'IPsec nécessite certainement des compétences nouvelles. Sont-elles disponibles et à la portée des entreprises ?

Du fait de la complexité d'IPsec et de la grande variété des services qu'il peut fournir, il est important que la personne chargée du choix de la solution et celle chargée de sa mise en œuvre et de sa maintenance connaissent bien IPsec. Ce point est particulièrement important pour le choix d'une solution, où le risque est grand pour quelqu'un, qui ne connaît pas suffisamment IPsec, d'être abusé par une présentation commerciale trompeuse quant au niveau de sécurité fourni. En effet, si une bonne implémentation d'IPsec per-

DOSSIER



met d'atteindre un niveau de sécurité très important, on trouve malheureusement encore beaucoup d'implémentations partielles qui se réclament « compatibles *Ipsec* » mais fournissent une sécurité bien moindre. Il faut bien comprendre qu'*IPsec* est une norme et que la qualité d'un produit donné dépend de la qualité de l'implémentation de cette norme.

Quelles sont les prestations de votre cabinet en la matière ?

Notre cabinet peut intervenir à tous les niveaux dans le processus de choix et de mise en œuvre d'un système utilisant *IPsec* : Nous proposons des formations sur mesure à *IPsec*, avec, suivant le public visé, une

orientation plus ou moins technique (voir : www.hsc.fr/formations/ipsec.html.fr). Nous sommes en mesure d'aider les entreprises à choisir une solution adaptée à leurs besoins. Nous pouvons procéder à la mise en place d'une telle solution en installant les produits correspondants et en formant les administrateurs à l'utilisation de ces produits. Ces deux derniers points sont à modérer, actuellement, du fait du nombre limité d'implémentations correctes, présentes sur le marché : il n'existe pas encore de solutions adaptées à tous les besoins. Cette situation devrait cependant évoluer rapidement, plusieurs fournisseurs s'étant déjà engagés.

Propos recueillis par Philippe Collier

IPSEC : COMMENT ÇA MARCHÉ ?

*Ghislaine Labouret, du cabinet Hervé Schauer Consultant (www.hsc.fr), spécialisé dans le domaine de la sécurité, a réalisé une synthèse très claire permettant de comprendre l'architecture, le mode de fonctionnement et les usages des protocoles *IPsec* (IP Security Protocol).*

*Depuis 1992, l'IETF (Internet Engineering Task Force, www.ietf.org) a mis en place un groupe de travail, pour étudier le moyen renforcer la sécurité des échanges sur l'Internet. Une première version des mécanismes *IPsec* a été proposée en 1995, sans la partie gestion des clefs, qui vient d'être ajoutée à l'occasion d'une seconde version officialisée récemment. *IPsec* reste cependant une norme non figée qui évolue en permanence. Aussi est-il important de se tenir en permanence au courant, et pourquoi pas, d'intervenir dans le débat et la critique des RFC (Request for comments).*

*Le terme *IPsec* désigne un ensemble de mécanismes destinés à protéger le trafic au niveau de la couche IP (IPv4 ou IPv6). Ces mécanismes concernent notamment : l'intégrité, l'authentification et la confidentialité des données. Il est important de signaler qu'au-delà de la couche réseau IP, ces services assurent de fait la protection de tous les niveaux supérieurs.*

Architecture d'*IPsec*

*Le système de sécurisation des échanges *IPsec* repose sur deux mécanismes (ou protocoles) : AH (Authentication Header) et ESP (Encapsulating Security Payload), qui viennent s'ajouter au traitement IP classique. Les paramètres nécessaires à l'utilisation de ces protocoles sont gérés à l'aide d'associations de sécurité (Security Association, SA). Les SA sont stockées dans la base de donnée des associations de sécurité (Security Association Database, SAD) et gérées à l'aide du protocole IKE (Internet Key Exchange). Les protections offertes par *IPsec* sont basées sur des choix définis dans la base de données de politique de sécurité (Security Policy Database, SPD). Cette base permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, s'il sera autorisé à passer outre ou sera rejeté.*

Principe de fonctionnement

*La « couche » *IPsec* consulte la base de donnée des politiques de sécurité (SPD) et celle des associations de sécurité (SAD) pour déterminer comment traiter les données à envoyer et comment vérifier et/ou déchiffrer les données reçues. Elle fait appel à IKE lorsqu'il est nécessaire d'établir une nouvelle association de sécurité avec un interlocuteur donné.*

Exemple d'utilisation

**IPsec* est trop souvent associé uniquement aux réseaux VPN, ce qui est trop restrictif. *IPsec* peut être mis en oeuvre, suivant le type d'utilisation souhaité, sur différentes machines d'un réseau : stations clientes, serveurs, garde-barrière, routeurs... Par exemple, le service d'authentification de l'origine des données, fourni par *IPsec* permet de contrer des attaques que les gardes-barrières actuels ne sont pas en mesure d'éviter. Autre exemple : une entreprise possède un serveur avec des données sensibles, auxquelles, seule, une partie du personnel doit avoir accès : installer *IPsec* sur le serveur et sur les machines des employés en question permet d'assurer le contrôle d'accès aux données et leur confidentialité lors de leur transfert sur le réseau. *IPsec* peut aussi sécuriser les accès distants de postes nomades à un intranet...*