Y. David, IPDiva, 'Firewall et VPN SSL dans une même appliance, c'est risqué'

Les RPV (ou VPN) SSL sont largement d'actualité compte tenu de la flexibilité qu'ils procurent dans l'accès aux applications et aux ressources du système d'information de l'entreprise, tout en minimisant les contraintes en termes de mobilité et de connectivité (ADSL, Wi-fi, GPRS?). Yvonnick David, p-dg de la société IPdiva, société française spécialisée dans les réseaux privés virtuels (RPV ou VPN) avec encryptage SSL, explique sa stratégie. En résumé qui est IPdiva ? IPdiva est né de la rencontre d'une technologie (une plate-forme de communication sécurisée en mode applicatif et s'inspirant du peer-to-peer) avec la formidable croissance du marché des services d'accès distants. En effet, la demande en services d'accès distants (ou télé-services) explose compte-tenu du développement croissant des usages (mobilité, collaboratif inter-entreprise, télé-maintenance, info-gérance?) Nous avons fait le constat qu'il faut simplifier la mise en ?uvre de ces services d'accès distants avec une solution suffisamment flexible pour pouvoir adresser cette variété d'usages, tout en étant le moins intrusif possible sur les infrastructures réseau et sécurité en place, et en assurant une garantie de sécurité optimale. A ce titre, le choix de SSL nous parait le plus opportun, d'où l'élaboration d'une solution d'accès privé applicatif de type RPV SSL. En résumé, mettre en place une solution de RPV SSL IPdiva, c'est faciliter le développement des usages tout en simplifiant la vie des administrateurs réseau et en rassurant le responsable sécurité. Qu'est ce qui vous différencie des acteurs que l'on dira « plus établis » sur ce marché ? Bien évidemment, tout marché attire les convoitises. Sur le marché des services d'accès distants se positionnent des fournisseurs de produits packagés (principalement américains), des opérateurs et quelques rares éditeurs comme IPdiva. En tant que nouvel entrant, notre différentiation repose d'abord sur notre plate-forme technologique IPdiva Médiation, support de notre solution d'infrastructure RPV SSL. Cette plate-forme, qui a fait l'objet d'un important programme de R&D soutenu par l'ANVAR [ndlr : plus de 1M? ont été investis en R&D par Ipdiva] se caractérise par une topologie de déploiement dite « à double sas d'accès ». Cette topologie simplifie considérablement sa mise en ?uvre, tout en garantissant l'étanchéité de la compartimentation assurée par la plate-forme entre Internet et le réseau support des ressources devant être rendues accessibles à distance. Par ailleurs, nos solutions s'appuient sur des systèmes ouverts (sur base Linux, Windows ou AIX) et sont intégrables sur tout type de plate-forme matérielle compatible PC. Au-delà de la simplicité d'usage du service que nous apportons à nos clients « utilisateurs », les exploitants système et réseau en charge de son déploiement apprécient la facilité de mise en ?uvre et son caractère non-intrusif. Enfin, nous recevons un écho très favorable des responsables sécurité qui trouvent dans notre procédé de compartimentation « à double sas d'accès » un moyen extrêmement astucieux de préserver l'intégrité et la sécurité du site central. A ce titre, notre solution a obtenu la labellisation OPPIDUM du Ministère de l'Industrie. Cette labellisation qui nous permet d'envisager une certification de notre plate-forme au niveau EAL2 augmenté, dans les 15 à 18 prochains mois. Vous parlez de la notion de plate-forme technologique, en quoi cela consiste ? Le procédé de communication mis en ?uvre sur notre plate-forme de RPV SSL à topologie répartie consiste à dissocier les fonctions de «contrôle d'accès» des fonctions de «translation SSL et d'interface applicative» avec les systèmes devant être accessibles à distance. Lorsqu'un utilisateur distant souhaite se connecter à distance à un système ou une application d'un réseau local, il s'authentifie tout d'abord auprès d'un point central de contrôle

d'accès labellisé IPdiva Server. IPdiva Server est soit localisé sur la DMZ de l'entreprise soit hébergé à l'extérieur. Il peut aussi être proposé en tant que service managé par IPdiva. Sous réserve des droits ad-hoc, la requête de connexion de l'utilisateur est alors redirigée au travers d'un tunnel sécurisé assurant la liaison entre le serveur de médiation (IPdiva Server) et le (ou les) site(s) hébergeant les ressources. Pour ce faire, ce tunnel sécurisé doit avoir été établi préalablement à l'initiative de l'élément passerelle (IPdiva Gateway) situé sur le segment du réseau local hébergeant les ressources concernées. Cette passerelle effectuera ensuite la translation des requêtes de l'utilisateur distant vers les applications ou les systèmes du réseau local. Comment réagit le marché face à ce nouvel entrant ? Nous avons commencé à commercialiser nos solutions début 2004. Nous comptons déjà à notre actif quelques références prestigieuses comme des collectivités locales (Ville de Rennes et de Lorient), des collectivités territoriales (Conseil régional de Bretagne, Conseil général 56), des Ministères (Intérieur et Justice) et des entreprises dans différents domaines d'activités (industrie, distribution, spatial). Cependant, notre stratégie commerciale passe par le développement de partenariats stratégiques avec des intégrateurs nationaux, comme Telindus, Arche ou AmecSpie, ainsi que quelques intégrateurs sectoriels (santé, mobilité?). Nous venons aussi d'ouvrir un service de VPN SSL managé et hébergé par nos soins, la topologie de notre solution étant particulièrement adaptée à ce modèle commercial. Ce service est accessible à titre démonstratif sous https://vpn.ipdiva.net , organisation: demo, login et mot de passe: guest/guest). Il nous permet d'adresser une clientèle qui ne souhaite pas déployer et opérer un tel service (ou n'en a pas les compétences en interne) et qui préfère en profiter par simple abonnement mensuel à l'usage. Nous approchons déjà la dizaine de clients abonnés à ce service. Les constructeurs de firewall sont partagés en ce qui concerne la fonction VPN SSL, elle est soit sur le même boîtier, soit déportée, qu'en pensez vous ? Sans entrer dans une polémique improductive sur la pertinence d'approches intégrées « tout en un » vis à vis d'approches spécialisées « un boîtier égal une fonction », je pense que dans le cas précis des firewall intégrant des fonctionnalités de VPN SSL (cas de Netasq, Symantec) on a tendance à faire un mélange des genres très risqué du point de vue de la sécurité. En effet un firewall est là pour établir une démarcation claire des environnements réseau de l'infrastructure (DMZ privée, DMZ publique, LAN…), indépendamment des systèmes et des applications hébergées par cette infrastructure. A ce titre ils assurent un rôle de portier étanche entre les différents constituants de cette infrastructure réseau. Il faut considérer la fonction VPN SSL comme un sur-ensemble de cette démarcation « infrastructure » dans la mesure où l'on propose un accès « privatif » de niveau applicatif et système. On se positionne ainsi à un niveau supplémentaire, il y a donc un risque important à cumuler les potentielles failles et vulnérabilités si les deux fonctions sont agrégées dans le même système. Par ailleurs, il faut aussi tenir compte de l'aspect performance d'un VPN SSL. Avec un VPN SSL le système est amené à traiter des informations de niveau applicatif (ré-écriture d'URL, gestion d'ActiveX et d'applet Java….) nécessitant des performances machines spécifiques souvent incompatibles avec la structure matérielle des firewall. Ceci explique que les fonctions de VPN SSL intégrées aux appliances firewall soient très en-deca (au niveau fonctionnel et performance) des fonctions remplies par des équipements dédiés. Enfin il ne faut pas négliger l'aspect organisationnel car le « firewalling applicatif » introduit par la SSL n'est pas du même ressort fonctionnel que le « firewalling réseau ». Il est plus du ressort des organisations opérationnelles que des administrateurs réseau ou sécurité. (*)pour Vulnerabilite.com