Paroles d'Integrateurs

Le VPN : un outil d'ouverture et de competitivite

Le développement du nomadisme et la nécessité d'accroître sans cesse la rapidité des échanges a permis au VPN (Virtual Private Network / réseau virtuel privé) d'être considéré comme un outil de productivité et de compétitivité essentiel. Nos deux experts, Igor Herrmann, Directeur des opérations et Directeur général de Vipawan et Philippe Humeau, Directeur Commercial de NBS System, estiment qu'un bon déploiement doit reposer sur un système d'authentification forte permettant un contrôle et une traçabilité efficaces des utilisateurs. Pour cela, il est nécessaire de mettre en œuvre une démarche rigoureuse qui offrira la sécurité et permettra l'adhésion des utilisateurs.

Philippe Humeau, NBS System

Mag Securs : Quels outils, méthodes, tableaux de bord, techniques et organisation, doivent être mis en œuvre pour le déploiement et l'exploitation des VPN et de leur sécurité ?

Igor Hermann : Le VPN, au sens large, est l'un des outils importants de la productivité et la compétitivité des entreprises. L'ouverture d'accès doit donc intégralement faire partie de leur stratégie, mais également, de leur gestion des risques. Nous, prestataires, experts en technologie et praticiens expérimentés, devons prendre en compte l'ensemble de ces dimensions.

Dans notre philosophie, un besoin doit nécessairement faire l'objet d'un dimensionnement en termes de risque sur les plans juridiques, économiques et financiers, techniques et humains.

En termes d'organisation, le VPN doit s'intégrer dans un schéma directeur de la DSI, respecter la politique de sécurité et faire l'objet de la définition d'un risque maximum tolérable.

Dans ce cas précis, nous insistons sur le fait que cet outil doit faire partie de la charte d'utilisation des moyens informatique et plus particulièrement, qu'il doit s'inscrire dans le process de gestion des habilitations internes et externes de l'entreprise :

- S'il est à destination d'utilisateurs internes, il concerne aussi bien la DSI, pour les aspects opérationnels et surtout sécurité, que les directions métiers pour la distribution des droits et la DRH pour le circuit d'intégration ou de départ des collaborateurs.
- S'il est à destination d'utilisateurs externes, l'équivalent de ce process doit être mis conjointement en place et de manière contractuelle pour palier l'inévitable « turn over » des prestataires, ainsi que les risques opérationnels et leurs conséquences juridiques.

Nous insistons surtout et sans cesse sur deux points :

1- Ne perdez pas le contrôle des identités des utilisateurs :

Une gestion de mot de passe, même réelle, est inadaptée pour sécuriser des accès distants. Seule une authentification forte, qui devient heureusement de moins en moins coûteuse, est à la hauteur de l'enjeu.

Il suffit d'ailleurs pour en assurer le contrôle, de se doter de tableaux de bord très simples, comme :

- les tentatives de logins échouées,
- des identités présentes au même moment en plusieurs endroits géographiques différents
- des tentatives de logins d'identités supprimées ou désactivées
- des connexions à des heures improbables

Charge au client ensuite, de considérer s'il y a lieu de déclencher et gérer l'incident de sécurité selon ses propres process.

Cet aspect est si fondamental qu'il est une exigence de base des bonnes pratiques en matière de gestion de la sécurité et de conformité.

2 - Ne perdez pas le contrôle de vos flux :

Des interconnexions IPsec site à site ou « pire » MPLS, vous garantissent souvent de parfaits échanges inter site, par exemple à l'international, le tout, non filtré. C'est un terrain très propice à la dissémination de vers ou à des tentatives d'effractions informatiques depuis l'interne.

Nous insistons donc pour que nos clients déploient des solutions qui permettent une visibilité sur la matrice des flux internes, ceci incluant les flux inter sites par VPN ou MPLS.

Cette visibilité est une étape décisive dans la maîtrise de l'intégrité des flux réseaux, qui permet ensuite de cibler les points chauds à protéger spécifiquement.

Il est donc nécessaire de placer des équipements dédiés supplémentaires ou d'utiliser à défaut SNMP ou beaucoup mieux, des fonctions niveaux 2-4 comme Sflow ou 3-4 comme Netflow embarqués dans des commutateurs ou routeurs.

L'objectif est d'assurer la traçabilité et l'historisation de la matrice des flux interne à des fins de planification mais également de vérification de conformité de l'usage du réseau.

Des tableaux de bords réseaux simples sont donc possibles. Pour autant, il vaut mieux être doté d'outils spécialisés comme ceux d'Arbor Networks.

Parallèlement, il faut se fixer sur une cible technique, architecturale et une méthodologie à déploiement progressif, alignée sur les objectifs de nos clients et cohérente par rapport au contexte technique et humain. C'est un point que nous allons détailler par la suite.

Enfin, nous considérons qu'il nous faut toujours garder en tête deux critères objectifs de réussite d'un projet VPN :

- Le premier est le passage « haut la main » aux indispensables audits externes (de validation technique et sécurité)
- Le second est le passage de l'acceptation utilisateur / prestataire (plus délicat…)

Pour cela nous proposons les points méthodologiques suivants :

- **Etape 1 :** prendre le temps de la conception et du dimensionnement global.
- **Etape 2 :** Commencer petit et transférer la compétence : bâtir le cœur de l'architecture et déployer quelques accès, valider le tout, transférer la complète maîtrise conceptuelle et opérationnelle aux équipes clientes sur un périmètre réduit.
- **Etape 3 :** Documenter de manière exemplaire l'architecture, son installation et

Igor Hermann, Vipawan

Systems integrators have their say

VPN, a tool for providing access and improving competitiveness

The development of mobility and the need to continually increase the speed of information exchange has led the VPN (virtual private network) to be considered as an essential tool for improving productivity and competitiveness. Our two experts Igor Herrmann, operations director and general manager of Vipawan and Philippe Humeau, commercial director of NBS System, consider that a successful implementation has to based on a strong authentication system to allow user access to be controlled and tracked. To achieve this, it is necessary to set up rigorous processes to gain user acceptance and ensure that the security requirements are met.

son exploitation, afin de construire une librairie initiale. Cela permettra d'avoir une véritable base de référence, stable et connue, répondant aux bonnes pratiques et indispensable en cas d'audit.

- **Etape 4 :** Une fois le recul acquis par les équipes de la DSI, se concentrer sur la communication client et l'élargissement des déploiements. C'est une phase délicate ou toute la DSI joue sa crédibilité vis-à-vis du reste de l'entreprise.

- **Etape 5 :** Enfin, suivre avec réactivité, les inévitables retours de cas nouveaux qui se présenteront afin d'assurer le respect des SLA et du risque maximum tolérable. Cela peut se faire notamment au travers de ce que nous appelons chez Vipawan, les contrats annuels de support téléphonique et intervention sur site / veille technologique. (CASTISS / VT).

Philippe Humeau : Dans le domaine du libre, OpenVPN est maintenant fourni avec une interface d'administration complète, les interfaces propriétaires des appliances, comme celles de Cisco par exemple, sont également très fonctionnelles.

Le meilleur moyen pour accéder à ces interfaces de contrôle reste HTTPS qui allie souplesse et standardisation, cependant certains clients propriétaires sont aussi de très bonne qualité. De notre côté, nous avons pris le parti de développer une interface de contrôle « maison » sur une solution opensource.

Un bon tableau de bord contient à mon sens :

Les certificats qui sont déclarés sur le système, quand ils ont été créés et la dernière connexion en date. Lesquels sont utilisés et quelle quantité d'information est transférée en moyenne par session. Un vecteur de sécurité important consiste à associer une IP VPN, un certificat afin de pouvoir suivre au besoin l'activité d'une connexion sur le SI. On devra parfois éviter l'usage de DHCP si l'on souhaite effectuer un filtrage IP des connexions VPN ou mieux encore centraliser les configuration IP des connexions du côté du serveur afin d'avoir le meilleur contrôle possible. Il doit aussi être possible de suivre les créations/destructions d'accès aux VPN ainsi que le nombre et le nom des connectés à un moment donné.

Du côté des méthodes, un archivage des connexions/déconnexions sur un an semble utile et pas si gourmand en ressources que cela en regard de l'importance de l'information conservée. La méthodologie de déploiement doit aussi faire clairement apparaître le besoin de l'utilisateur. Si celui-ci n'a pas réellement besoin d'une connexion VPN, elle ne doit pas être créée ou conservée. De même l'utilisation d'un VPN doit être couplée à la signature d'une charte utilisateur. Si cela n'a pas déjà été fait, c'est le bon moment pour faire signer à l'utilisateur une charte, ce qui lui fera prendre conscience de l'importance externe vers le SI.

Pour ce qui est de la technique et de l'architecture, il est conseillé d'intégrer les VPN sur des zones distinctes du Firewall. Il est en effet possible avec certains services de VPN de limiter les accès en fonction du profil de l'utilisateur et de mettre en place des règles de filtrage sur le système. Quand cela n'est pas faisable, il est pertinent d'isoler le service VPN sur une branche du Firewall, cela permettra de mettre en œuvre les règles de filtrages par IP qui sont indispensables dans un contexte sécurisé.

Il est difficilement acceptable de nos jours de laisser une personne rentrer dans le périmètre interne de l'entreprise depuis l'extérieur sans limiter sa connexion au stricte nécessaire, ne serait-ce que pour ne pas laisser un éventuel ver se diffuser par exemple. Le poste du collaborateur, qu'il appartienne à l'entreprise ou au collaborateur est à considérer comme compromis par défaut, il convient donc de sécuriser les accès du coté de l'entreprise. En matière de déploiement, les approches varient mais dans l'ensemble il faut préférer les systèmes de VPN à même de préparer les packages (des extensions MSI pour active directory par exemple) afin d'avoir un contrôle sur le déploiement sans pour autant perdre du temps. De plus les systèmes basiques ne permettent pas d'allouer des clefs de cryptages différentes à chaque packages, ce qui induit une perte en terme de sécurité, surtout si l'entreprise dispose d'une SSO ou d'une PKI.

En termes d'exploitation, encore une fois l'automatisation et les standards sont de mise : le HTTPS pour l'interface de contrôle et lier les logs à un système de mail automatisé envoyant un compte rendu d'activité hebdomadaire semble pertinent.

La sécurité doit être le maître mot de tout déploiement de VPN

MS : Quels sont vos conseils pour la sécurité d'un déploiement de VPN ?

Philippe Humeau : La sécurité doit être le maître mot d'un tel déploiement, de plus il est

indispensable de se protéger de l'utilisateur nomade, tout du moins de sa machine. En effet il est extrêmement aisé de prendre le contrôle de son ordinateur portable en téléchargeant une disquette ou une iso disponible partout sur Internet. La machine évolue aussi dans un milieu hostile quand elle est en dehors de l'entreprise. Ce sont autant de bonnes raisons qui doivent motiver les administrateurs et les intégrateurs à surveiller les connexions VPN, à utiliser du cryptage fort et à limiter les accès au stricte nécessaire. Il faut donc prévoir la mise en place du système de déploiement qui inclura les limitations, les allocations IP/utilisateur et les certificats différenciés au moment de la création de l'accès VPN.

Igor Hermann : Pour la sécurité d'un VPN, nous retenons deux aspects :

- la sécurité des tunnels
- la sécurité des équipements eux-mêmes

Dans le premier cas, les normes du marché permettent, par défaut, un bon niveau de sécurité, pour peu que l'on fasse attention aux aspects authentification (par certificats, tokens, clés partagées très solides à défaut) et que l'on active parfois, quelques paramètres supplémentaires (comme la PFS en IPSec).

Pour le second aspect : Très classique, authentification centralisée, authentification forte de préférence, comptes nominatifs, process de gestion des habilitations administrateur et surtout, mot de passe super utilisateur accessible… mais au coffre fort !

MS : Quelles sont les contraintes techniques à prendre en compte ? Quelles technologies recommandez-vous : avantages, inconvénients ?

Philippe Humeau : Pour ce qui touche aux technologies, SSL est à préférer à IPSEC dans l'immédiat, pour plusieurs raisons. IPSEC est un protocole de VPN qui a été pensé pour IPV6 et à ce titre, son intégration dans les environnements IPV4 ressemble plus à une adaptation forcée qu'à une démarche « naturelle ».

L'IPSEC est difficile à translater pour les firewalls et ceci requiert la plupart du temps des appliances spécialisées et coûteuses ou des firewalls qui auront un surcoût lié à leur capacité à analyser de l'IPSEC. Les implémentations Opensource d'IPSEC ne nous ont jamais parues non plus efficaces ou abouties en la matière. A l'inverse de SSL est un protocole connu de longue date, très bien sécurisé et tout à fait facile à translater sur les firewalls. De plus, il permet une intégration aisée dans les environnements Active Directory, Ldap et autre SSO ou PKI. La possibilité de lui faire traverser les proxy est aussi à prendre en compte, ce qui est difficile voire impossible avec IPSEC.

Il semble à ce jour que le SSL ait beaucoup plus d'avantages que d'inconvénients comparativement à IPSEC, c'est donc une technologie à privilégier quand cela est possible. Le SSL est capable d'utiliser différents protocoles de cryptage sous jacents, ce qui permet de choisir le meilleur compromis entre la force de la cryptographie et l'investissement processeur et mémoire selon l'environnement de production.

Igor Hermann : Les contraintes techniques sont également assez classiques : débits, qualité de service, temps de latence (notamment pour des applications comme VOIP), évolutivité de bande passante, disponibilité et… le coût !

N'oublions jamais un point : nos flux d'administration et supervision sont parfois concurrents des flux d'application. Soit, en cas d'absence de gestion de QOS et d'encombrement de bande passante, on perd le contrôle… pour un temps indéterminé. Sueurs froides garanties à l'Operation Center.

Concernant les solutions technologiques, nous défendons deux approches :

- dans le cas de connexion de type utilisateurs à site, nous privilégions les VPN dit « SSL ». Ce type d'accès permet de publier tout type de ressources, aussi bien les plans d'adressages IP, que des ports applicatifs TCP ou UDP et surtout, des contenus « Webisés ».

Ces solutions sont les plus en pointes en terme de pilotage de la relation utilisateur – système d'information, au travers de leur fonctionnalité de portail Web et parallèlement, facilite l'inspection de l'intégrité du poste de travail. Pour les plus en avance, elles permettent même des politiques de « remédiation ».

Ces solutions sont pour nous le sens de l'histoire du VPN client à site et sont d'un niveau de maturité suffisant pour tout type d'organisation. Elles ont vraiment notre préférence.

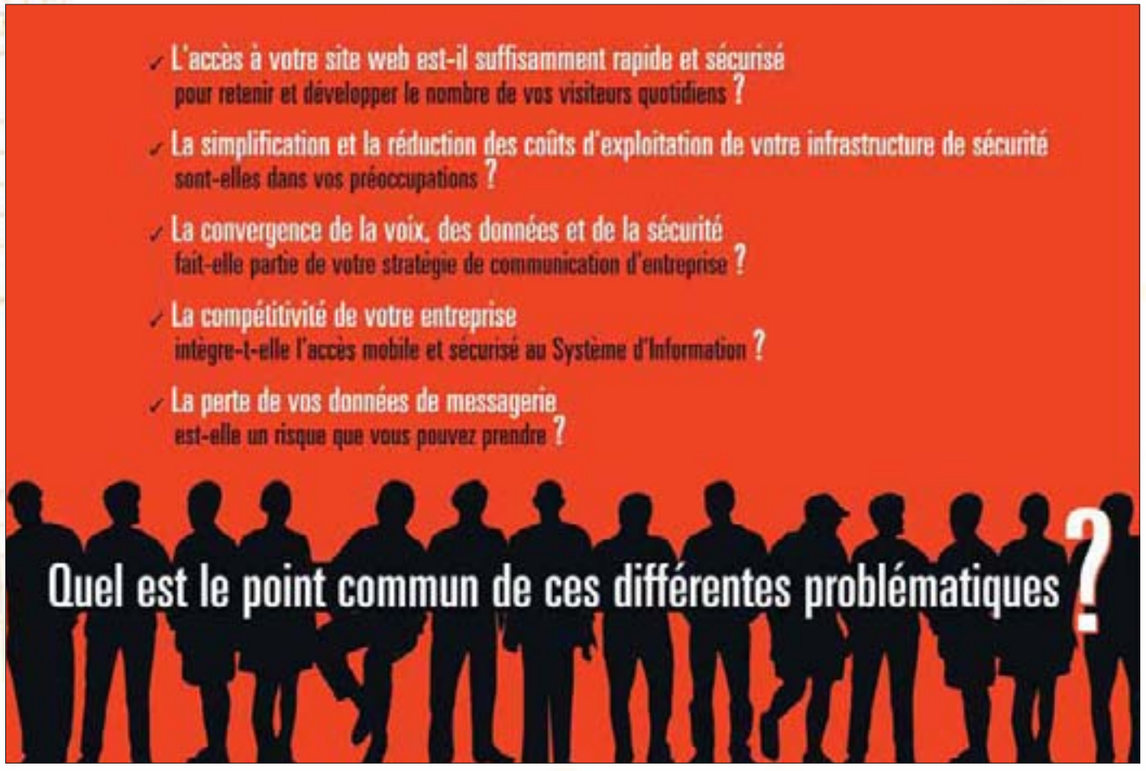
- pour des connexions de type site à site, nous privilégions de « vraies » appliances matérielles UTM, permettant de terminer des tunnels, de faire du NAT Traversal, du Hub and Spoke et supportant le mode actif/actif, gage de disponibilité et surtout, d'évolutivité de performance. Ce point est critique car la performance du VPN est une chose, celle du VPN avec analyse profonde des flux ou de l'ajout de l'inspection antivirale, en est une autre.

Dans les deux cas, une solution d'authentification forte est absolument indispensable.

Tout repose sur la robustesse du système d'authentification choisi

MS : Quels sont vos conseils pour la sécurité de l'exploitation d'un VPN ? Quelles sont les contraintes techniques à prendre en compte ? Quelles technologies recommandez-vous : avantages, inconvénients ?

Philippe Humeau : La sécurité d'un accès VPN repose sur trois points :



- La force de la cryptographie utilisée
- La robustesse du serveur (à tous niveau, clef, service, capacité de cryptographie etc…)
- Le filtrage de la connexion VPN des utilisateurs (isolation partielle du ou des réseaux)

Au niveau des contraintes techniques, l'IPSEC requiert la plupart du temps un appliance dédiée. Celle-ci se trouve souvent sur le Firewall directement comme chez Checkpoint ou Cisco. Les clients de ces VPN IPSEC sont donc aussi propriétaire dans la majorité des cas. L'alternative SSL est plus souple et le domaine du libre présente une solution SSL idéale (OpenVPN) qui repose sur un code éprouvé, efficace et dont les avantages sont plus qu'indéniables à ce jour. Un serveur Linux équipé de Netfilter (Iptables) et OpenVPN donne toute la souplesse nécessaire et surtout un niveau de sécurité maximum en permettant le filtrage le plus fin possible. Les packages de déploiement sont simples, clairs et personnalisables, enfin il est possible d'utiliser des pré et des post « authentification » en fonction des besoins.

Igor Hermann : En ce qui concerne le choix produit, l'offre marché est suffisamment riche pour nous permettre d'adopter une approche dite comparative, mettant en lumière des différences et points communs d'au moins deux produits. A titre personnel, j'aime beaucoup y inclure des solutions du domaine public qui, à leur rythme, rattrape peu à peu certains de leur retards.

Par principe, nous avons une nette préférence pour des éditeurs/solutions open sources spécialisés sur un cœur de marché technologique précis, plutôt que des acteurs généralistes.

Pour la partie authentification forte notre préférence va sans ambiguïté à des solutions de type « token » hardware avec code PIN.

Le secret d'un bon déploiement réside dans la méthode des « petits pas »

MS : Comment estime-t-on l'ampleur des tâches de déploiement ? Pouvez-vous donner des exemples : type de projet, ampleur du déploiement ?

Igor Hermann : Le secret de la gestion des déploiements de masse est d'avoir très bien déterminé toutes les typologies de cas et d'avoir avancé dès le début, humblement et à pas comptés.
Cette méthode des petits pas a pour intérêt de permettre aux individus de gérer des cas imprévus, de les dominer et donc d'avoir du recul, tout en validant et si besoin, en adaptant le modèle de départ.

Le planning initial doit donc nécessairement, inclure un coefficient de distorsion.

L'objectif ne peut être d'aller vite, mais bien d'accumuler de l'expérience et donc de passer d'une vision théorique à une expérience modélisée et à une vraie méthodologie.

A la fin de ce processus, la maîtrise interne est donc suffisante pour que la généralisation devienne un processus à part entière dont on a déjà prévu les règles de dimensionnements humains et techniques.

Philippe Humeau : Le déploiement en soi n'est souvent pas le poste le plus lourd. Les packages et les systèmes de déploiements existants permettent la plupart du temps de réaliser cette opération de façon rapide et efficace. La complexité réside dans l'architecture et la modification de l'existant pour atteindre un niveau de sécurité convenable.

Pour une entreprise de quelques dizaines d'utilisateurs, il faut compter environ 1 à 30 minutes par poste (par manque de système de déploiement centralisé) et quelques jours pour le serveur de VPN et son filtrage. Dans une entreprise comptant plusieurs milliers d'utilisateurs, le déploiement sur le poste de travail ne prend que quelques minutes par contre la configuration du serveur et le filtrage des VPN peuvent prendre plusieurs semaines afin de concevoir le tout correctement.

Le coût de la maintenance dépend de la rigueur du suivi des accès VPN

MS : Que faut-il prévoir comme charge de maintenance en fonction de la taille du VPN ? Pouvez-vous donner des exemples ?

Igor Hermann : La réponse est finalement très dépendante des solutions choisies, de la durée de calcul et de l'évolution des besoins !

Plus précisément, les modes de calcul sont différents en fonction du type de VPN :

- souvent extrêmement stables et nécessitant peu d'intervention, dans le cas d'un VPN site à site
- variables en fonction de la population des utilisateurs distants, dans le cas du client à site.

A noter que dans ce dernier cas, si l'on veut être complet, ce sont les coûts indirects liés aux appels helpdesk qui doivent également être pris en compte.

En la matière, encore un fois, il s'agit d'un travail de terrain orienté sur un dimensionnement en fonction du contexte client.

Philippe Humeau : La maintenance se passe généralement très simplement. Il convient de mettre en place un suivi rigoureux des accès VPN ouverts, des utilisateurs du système et de leurs droits. Une interface correctement conçue permettra aux administrateurs de mener cette tâche de façon simple et partiellement automatisée.

Pour les mises à jour du système VPN en lui-même, dans le cas d'une Appliance, la plupart du temps tout est automatisé, y compris les mises à jour de la plateforme. Sur des services logiciels, il convient de se tenir informé des éventuelles failles pouvant voir le jour. Les sociétés ayant une partie de leur système en infogérance confient ce poste à leurs sous traitants, les autres doivent vérifier de temps à autres que leur système n'est pas dépassé ou dangereux.

MS : Quel est le coût moyen annuel de cette maintenance en fonction de la taille du VPN ?

Philippe Humeau : Les modèles économiques varient beaucoup selon les constructeurs, les intégrateurs ou les éditeurs de logiciels. Sur les appliances, l'usage est de facturer au client un forfait annuel de quelques milliers d'euros pour maintenir sa plateforme à jour. Dans le domaine logiciel, il n'y a pas vraiment de règle, chaque éditeur pratique ses tarifs. Dans le cas de l'Opensource, les solutions et les patchs sont gratuits, il n'est donc pas nécessaire de prévoir un budget pour le correctif. Il reste néanmoins à l'appliquer ce qui peut être intégrer dans une infogérance ou payable au coup par coup.

Dans l'ensemble, un coût d'exploitation raisonnable si situe aux alentours de 50 à 100 € / an / client en moyenne selon les plateformes et la taille du VPN. Ceci comprend l'installation, la mise à jour et la maintenance et de tous les frais connexes de ce type mais ne tient pas compte de l'hébergement du serveur ou de la bande passante qui lui est dédiée.