Philippe Rondel (Check Point): «Il faut se brancher au plus près de la machine virtuelle pour la protéger»

A l'occasion du VMworld 2010 fin août, Check Point présentait sa nouvelle solution de sécurisation des machines virtuelles (VM). Security Gateway Virtual Edition (VE) permet le contrôle des accès réseaux directement au niveau de la VM et non plus de la machine physique. *« Avec la virtualisation*, rappelle Philippe Rondel, directeur technique de Check Point France, *il n'y a plus de notion de zones physiques. Tous les clients se retrouvent à plat connectés au même switch virtuel. Il faut donc se brancher au plus près de la VM pour la protéger. »*

Concrètement, Security Gateway VE s'appuie sur les API VMSafe délivrées par VMware avec vSphere 4 pour s'intégrer plus profondément dans l'architecture des solutions de virtualisation de l'éditeur de Palo Alto. Dans ce cadre, la solution de sécurité de Check Point apporte un firewall et un système de prévention d'intrusion (IPS) qui protègent les applications virtualisées et les données des tentatives d'attaques externes mais aussi en provenances des éventuelles autres VM situées sur le même serveur physique. *« Il est important de déterminer quels types de communications sont autorisées et de filtrer les paquets IP afin d'éviter les attaques de type XSS ou des serveurs web*, explique l'expert technique de Check Point. *Dans l'environnement virtualisé, c'est pire que dans le monde physique car toutes les techniques d'attaques existantes restent valables et les applications ne sont plus cloisonnées physiquement. »* Autrement dit, il y a un énorme besoin de sécurisation des environnements virtuels que Check Point compte bien mettre à profit pour déployer ses solutions.

L'éditeur n'en est pas à ses premiers pas en matière de sécurisation des VM. De fait, Security Gateway VE complète une offre précédente moins aboutie. *« La première édition de VE fonctionnait à la manière d'un routeur en changeant de réseau depuis une applicance dédiée. »* Le binaire n'en reste pas moins employé dans la nouvelle offre qui se distingue notamment par l'absence de solution matérielle. *« Là, on peut contrôler les communications entre deux VM tout en gagnant en souplesse grâce à l'absence de matériel dédié. »* Security Gateway VE s'implémente directement dans l'environnement de VMware qui se charge de répartir les ressources nécessaires. La solution de Check Point se fait, sur le papier, néanmoins discrète puisqu'elle nécessite un cœur de calcul virtuel (*virtual core*) qui utilise 256 Mo de mémoire vive. Quasiment négligeable sur des systèmes souvent provisionnés avec 256 Go de RAM.

Gestion des environnements hétérogènes depuis une seule console

Cette approche purement logicielle est l'un des points différenciant de l'offre de Check Point par rapport à la concurrence qui a généralement basé son approche sur des solutions matérielles de types appliances, network processor, et autres processeurs embarqués types ASICs. Des choix qui interdisent aujourd'hui l'usage des API VMsafe de VMware. De plus, l'approche de Check Point lui permet de proposer la gestion d'environnements hétérogènes physiques et virtuels depuis une même console d'administration (à condition que les solutions déployées proviennent évidemment de Check Point). *« On peut administrer, qui plus est à distance, du firewall physique et du firewall virtuel*

sous Check Point », confirme Philippe Rondel. La solution Smart Center de l'éditeur permet en effet d'établir une politique de sécurité et de la pousser vers les les pares-feu physiques et virtuels en une seule opération.

La sécurisation des environnements virtualisés devrait s'accélérer dans les mois qui viennent. *« Plus de 50 % de nos clients virtualisent leur infrastructure ou ont des projets dans ce sens. Et ceux qui ont basculé continuaient de sécuriser à distance avec des solutions traditionnelles. Mais aujourd'hui, nous faisons face à beaucoup de demandes, notamment en provenance des fournisseurs de services, des grands comptes et aussi des demandes de sociétés qui apportent de l'informatique différente chez leur clients où ils déploient un serveur physique qu'ils remplissent d'un ensemble de VM qu'ils veulent pouvoir sécuriser en toute transparence pour leur client. »*

Pour l'heure, Security Gateway VE adresse exclusivement l'environnement VMware. *« Nous étudions la faisabilité des autres solutions de virtualisation*, concède le porte-parole de Check Point, *mais au vu des parts de marché de VMware, nous n'avons pas de projet de développement de solutions pour les environnement Microsoft Hyper-V ou Citrix Xen même si, bien sûr, nous regardons de près ces plates-formes d'un point de vue technologique. »* Une situation qui permet à l'éditeur de concentrer ses efforts dans une seule direction pour le moment. Quant au modèle économique de Security Gateway VE, il s'appuie sur celui de VMware, à savoir une licence basée sur le nombre de cœurs des plates-formes. La solution est proposée à partir de 2000 et 3000 dollars respectivement pour 8 et 16 cœurs.