**Communiqué de presse**

# Stonesoft : 5 méthodes pour sécuriser le réseau virtuel, le défi le plus significatif du *cloud computing*

*L'éditeur finlandais dévoile cinq méthodes*

*pour résoudre les problèmes de sécurité dans le cloud*

**Levallois-Perret, le 14 avril 2010 :** Stonesoft, fournisseur innovant de solutions intégrées de sécurité réseau et de continuité de service, a identifié cinq façons, pour les entreprises, d'améliorer la sécurité du *cloud computing*. Cette annonce vient renforcer la toute dernière communication émanant du Gartner qui explique que d'ici à 2012, **60 % des serveurs virtualisés seront moins sécurisés que les serveurs physiques qu'ils sont censés remplacer** *(Source : Addressing the Most Common Security Risks in Data Center Virtualization Projects, Janvier 2010).*

Actuellement, la plupart des entreprises déploient sur leur réseau des technologies de virtualisation sans impliquer les équipes réseau et de sécurité des systèmes dans les phases de planification. Il en résulte la chose suivante : **la majorité des entreprises se contente donc de moderniser les réseaux virtuels, en y appliquant les politiques de sécurité réseaux physiques existantes**. Ce manque de préparation et de perspective affaiblit considérablement la sécurité du réseau, cette dernière étant l'élément essentiel de la mise en place réussie du *cloud computing* au sein des très grandes entreprises.

Pour appuyer cette communication du Gartner, Stonesoft a identifié cinq façons pour les équipes informatiques de se prémunir des menaces et attaques survenant dans le *cloud*, tout en assurant la bonne mise en œuvre de leurs politiques

1. **Regrouper les identités (Federated ID):** le besoin pour les collaborateurs de se connecter à de multiples applications et services est inhérent à tout environnement de type

cloud. La possibilité d'assurer l'authentification forte de l'utilisateur risquant d'échapper aux entreprises, ceci représente donc un énorme danger en termes de sécurité. Pour réduire ce risque, les entreprises doivent mettre en place des technologies de Single Sign-On (SSO), similaires, par exemple, à celle de la StoneGate SSL VPN. Elles vont permettre aux utilisateurs d'accéder, via un login unique, à de multiples applications et services y compris ceux localisés en dehors de la société, dans le cloud public. Le SSO permettra aux entreprises d'harmoniser l'administration de la sécurité et d'assurer l'authentification forte même dans le cloud.

2. **Assurer une connectivité permanente** : lorsque la plupart des données sensibles d'une entreprise sont stockées dans le cloud, la moindre panne réseau risque d'interrompre les opérations commerciales. Les services du cloud doivent être constamment accessibles, et ce même pendant les opérations de maintenance : des fonctionnalités de haute-disponibilité comme le clustering actif/actif, un serveur dynamique de répartition de charge, ainsi qu'un répartiteur de chargeur ISP doivent donc être mis en place au sein de l'infrastructure réseau. Il est préférable pour les entreprises de choisir des technologies déjà intégrées à l'infrastructure réseau, plutôt que d'investir dans des versions autonomes de solutions ; le tout afin d'assurer l'efficacité, la facilité d'administration mais également de réduire les coûts.

3. **Mettre en place une inspection multi-couches** : de l'augmentation du nombre d'environnements cloud computing et de la multiplication de menaces toujours plus évoluées découle le besoin de créer une protection couche-par-couche, comprenant la protection périmétrique, la prévention et la détection d'intrusions sur le réseau. Au lieu de mettre en place des firewalls de première génération visant à protéger le cloud et son périmètre, Stonesoft prône le déploiement d'appliances firewalls virtuelles de nouvelle génération (comme par exemple la StoneGate Virtual NextGen Firewall) qui intègrent un firewall et un IPS pour une inspection en profondeur du trafic. Ainsi, les entreprises pourront analyser tous les types de trafic : de la navigation web, aux applications peer-to-peer en passant par le trafic web chiffré transitant dans le tunnel SSL. Des appliances IPS supplémentaires devront aussi être installées afin de protéger les réseaux des attaques internes qui menacent l'accès au cloud.

4. **Exiger une administration centralisée** : l'erreur humaine reste toujours la menace la plus considérable pesant à la fois sur les réseaux virtuels et physiques. A mesure que les entreprises déploient des dispositifs réseaux supplémentaires afin de sécuriser leur réseau virtuel, le risque devient plus grand. En effet, la gestion des périphériques, la surveillance et la configuration deviennent plus complexes et totalement désorganisées. C'est pour cette raison que Stonesoft recommande aux entreprises l'utilisation d'une seule console d'administration

pour gérer superviser et configurer l'ensemble des dispositifs réseau, qu'ils soient physiques, virtuels ou tiers.

5. **Protéger les postes de travail virtuels :** de plus en plus d'entreprises décident de déployer des postes de travail virtuels afin de bénéficier des avantages de cette nouvelle technologie notamment en ce qui concerne l'administration et les coûts. Cependant, ces postes de travail sont tout autant, et si ce n'est plus, vulnérables que leurs homologues physiques. Pour protéger les postes de travail virtuels de façon adéquate, les entreprises devront les isoler des autres segments du réseau et mettre en place des processus d'inspection profonde pour prévenir les attaques internes et externes. Ces entreprises devront adopter une approche multi-niveaux de la sécurité en mettant notamment en place une technologie IPS qui empêchera les accès internes non autorisés, protègera les postes clients des serveurs malveillants et délivrera également des fonctionnalités d'accès distants via l'IPsec ou le SSL VPN qui protège contre les accès externes non autorisés.

Stonesoft propose actuellement une gamme de solutions de sécurité virtuelle qui offre une protection avancée du *cloud*. Cette offre est composée de StoneGate Virtual NextGen Firewall, StoneGate Virtual IPS et StoneGate Virtual SSL VPN. Pour plus d'informations, rendez-vous à l'adresse suivante www.stonesoft.com

**A propos de Stonesoft :**

Stonesoft Corporation (OMX : SFT1V) est un fournisseur innovant de solutions de sécurité réseau intégrées. Ses produits sécurisent le flux d'informations à l'échelle d'entreprises distribuées. Les clients de Stonesoft sont notamment des entreprises dont les besoins commerciaux croissants requièrent une sécurité réseau avancée et une connectivité professionnelle permanente.

La solution de connectivité sécurisée StoneGate™ fusionne les aspects de la sécurité réseau que sont le pare-feu (FW), le réseau privé virtuel (VPN), la prévention d'intrusion (IPS), la solution de réseau privé virtuel à technologie SSL (SSL VPN), la disponibilité de bout en bout, ainsi qu'un équilibrage des charges plébiscité, au sein d'une appliance dont la gestion est centralisée et unifiée. Les principaux avantages de la solution de connectivité sécurisée StoneGate se traduisent notamment par un coût total de possession faible, un excellent

rapport prix/performances et un retour sur investissement élevé. La solution StoneGate virtuelle protège le réseau et assure une continuité de service aussi bien dans les environnements réseaux virtuels que physiques.

La solution SMC (StoneGate Management Center) permet une gestion unifiée des solutions StoneGate Firewall with VPN, IPS et SSL VPN. Les solutions StoneGate Firewall et IPS fonctionnent en synergie pour fournir une défense intelligente à l'échelle du réseau de l'entreprise toute entière, tandis que la solution StoneGate SSL VPN renforce la sécurité dans le cadre d'une utilisation mobile et à distance.

Fondé en 1990, Stonesoft Corporation a son siège mondial à Helsinki, en Finlande, et un autre siège social aux États-Unis, à Atlanta, en Géorgie.

Pour plus d'informations sur Stonesoft Corporation, ses produits et services, consulter le site www.stonesoft.com où adressez-vous au contact presse.