HORS SERIE

Global Security Mag

THE LOGICAL & PHYSICAL SECURITY MAGAZINE

Livre Blanc N°001 - Prix : 5 € - octobre 2008

SPECIAL VIRTUALISATION

INTERVIEW EXCLUSIVE
Léonard Dahan

STONESOFT

STONESOFT

Livre Blanc N°001 - octobre 2008
Spécial **VIRTUALISATION**

REVUE TRIMESTRIELLE
Livre Blanc n°001 – Hors Série
www.globalsecuritymag.fr et
www.globalsecuritymag.com
ISSN : 1961 – 795X
Dépôt légal : à parution
Editée par SIMP
RCS Nanterre 339 849 648
17 avenue Marcelin Berthelot
92320 Châtillon
Tél. : +33 1 40 92 05 55
Fax. : +33 1 46 56 20 91
e-mail : marc.jacob@globalsecuritymag.com

RÉDACTION
Directeur de la Publication :
Marc Brami
Rédacteur en chef :
Marc Jacob
Assistante :
Sylvie Levy
Responsable technique :
Raquel Ouakil
Photos
Stonesoft
Comité scientifique :
Pierre Bagot, Francis Bruckmann
Eric Doyen, François Guillot
Mauro Israël, Olivier Iteanu,
Dominique Jouniot
Patrick Langrand, Yves Maquet
Michel Van Den Berghe,
Thierry Ramard, Hervé Schauer
Wayne Sutton, Catherine Gabay
Zbigniew Kostur

PUBLICITE
SIM Publicité
Tél. : +33 1 40 92 05 55
Fax. : +33 1 46 56 20 91
e-mail : ipsimp@free.fr

PAO
Imadjinn sarl
Tél. : 02 51 53 01 46
e-mail : pao-imadjinn@orange.fr

IMPRESSION
Imprimerie Hauguel
8-14 villa Léger
92240 Malakoff
Tél. 01 41 17 44 00
Fax 01 41 17 44 09
e-mail : info@imprimerie-hauguel.fr

ABONNEMENT
Prix du numéro Hors Série :
5 € TTC (TVA 19,60%)
Abonnement annuel au magazine :
50 € TTC (TVA 19,60%)

Interview exclusive :
Léonard Dahan **STONESOFT** **P. 6**

SOMMAIRE

ÉDITO

Virtualisation : vers une remise en cause des schémas de sécurité ?

Il est peu courant que des progrès technologiques entraînent un changement radical du mode de fonctionnement fondamental de l'informatique. Internet a eu un impact majeur, non seulement sur la manière d'accéder aux informations, de les stocker et d'interagir avec elles, mais aussi sur la façon dont les architectures applicatives et les réseaux sécurisent ces informations. La virtualisation révolutionne de manière similaire les environnements informatiques actuels.

Étonnamment, les environnements virtuels existent depuis plus de 30 ans. Pionnier dans le développement de ressources virtuelles avec le mainframe, IBM® offre à présent une large gamme de serveurs et d'architectures virtuels. La puissance de calcul ayant cependant augmenté exponentiellement ces dernières années, la vraie valeur ajoutée de la virtualisation est désormais à la portée d'organisations de toutes tailles. Avec l'avènement de VMware®, Parallels®, Xen™ et d'autres technologies de virtualisation, les entreprises d'aujourd'hui peuvent tirer profit de cette approche de machine virtuelle.

Ainsi, la virtualisation a pris d'assaut l'industrie informatique. Selon un récent sondage du magazine InformationWeek, 70 % des personnes interrogées disposent d'au moins un serveur virtuel tandis que moins de 12 % d'entre elles ont une stratégie de sécurité adaptée à leur environnement virtuel. Effectivement, comme lors de l'avènement de toute nouvelle technologie, la sécurité reste trop souvent le parent pauvre.

Pourtant, les risques existent et ne doivent pas être négligés. Ces menaces tiennent souvent au fait que ces architectures sont sécurisées par des méthodes traditionnelles reposant sur un équipement inadapté à ce nouveau concept. Ainsi, les RSSI, DSI… doivent repenser leur architecture de sécurité en l'adaptant à la virtualisation pour tirer le meilleur de cette technologie.

Marc Jacob

STONESOFT

LA SÉCURITÉ DES ARCHITECTURES VIRTUELLES EST LA NOUVELLE PRIORITÉ DES DSI

Interview de Klaus Majewski, VP Marketing de Stonesoft par Marc Jacob

Selon Klaus Majewski, VP Marketing de Stonesoft, les architectures virtuelles passeront d'une pure consolidation de serveurs à la virtualisation de réseaux entiers. Dans ce contexte, la sécurité va devenir un axe prioritaire pour toutes les DSI. Ainsi, l'offre StoneGate Virtuel se positionne comme une solution privilégiée de sécurité pour les architectures sous VMware, mais pourrait aussi le devenir pour l'offre Microsoft HyperV si le marché le décide.

Global Security Mag : Quelle est votre vision du marché de la virtualisation à l'échelle internationale et, en particulier, en Europe ?

Klaus Majewski : C'est un marché à forte croissance, et ce même si l'économie se mettait à ralentir parce que la virtualisation induit des économies tangibles pour les entreprises. Elle économise l'énergie, permet un gain d'espace et rend les entreprises plus indépendantes vis-à-vis des constructeurs de matériel. Elle offre également la possibilité aux entreprises de basculer d'une plate-forme matérielle à une autre à leur convenance, et ce sans affecter la production. En effet, la virtualisation est totalement transparente, car elle masque le matériel sous-jacent. Elle facilite aussi l'adaptation aux changements économiques liés à l'activité. Il est possible d'ajouter ou de supprimer des applications au gré des besoins. Avec la virtualisation, l'entreprise devient véritablement adaptative et agile.
À mon avis, dans un an ou deux, les architectures virtualisées passeront d'une pure consolidation de serveurs à la virtualisation de réseaux entiers. Nous nous apercevrons alors qu'il est essentiel de sécuriser l'environnement virtuel afin de pouvoir appliquer un type de protection similaire à celui qui régit déjà l'environnement physique, notamment la segmentation des serveurs, les zones de confiance distinctes et l'inspection du trafic virtuel. À cela, la virtualisation va apporter ses propres spécificités, telles que le déplacement des serveurs virtuels ou des images d'appliances virtuelles obsolètes, de façon tout à fait gérable. Ceux qui mettent actuellement en œuvre la virtualisation se focalisent essentiellement sur la consolidation des serveurs. Il apparaît clairement que la sécurité ne figure pas en tête de leur liste de priorités.

Si Microsoft se montre prometteur en matière de virtualisation, seuls les clients seront à même de juger de sa valeur

GS Mag : Aujourd'hui, Stonesoft fournit des solutions de sécurité pour la plate-forme VMware ESX. Qu'envisagez-vous pour les autres plates-formes (Citrix XEN, Microsoft HyperV, etc.) ? Pourquoi ?

Klaus Majewski : Nous fournissons actuellement les solutions Virtual Firewall/VPN et Virtual IPS pour la plate-forme VMware ESX. En effet, cette dernière s'affiche indéniablement comme un produit leader du marché et présente les outils de gestion des environnements virtuels les plus aboutis actuellement disponibles. Nous nous intéressons également de très près à Microsoft HyperV, car cette solution a le potentiel de rivaliser avec celle de VMware. Microsoft se montre prometteur en intégrant ses propres outils de gestion à l'administration d'environnements virtuels. L'avenir nous dira la valeur que les clients leur attribueront. Du point de vue de Stonesoft, porter nos solutions virtuelles sur HyperV ne représente pas un effort insurmontable. Nous agirons en ce sens si l'environnement virtuel de Microsoft prouve sa viabilité auprès de nos clients.

Utiliser des appliances matérielles pour inspecter le trafic des environnements virtuels est contre-productif

GS Mag : Qu'attendez-vous du partenariat VMware VMsafe sur la technologie de sécurité ? Quels types d'avantages pouvons-nous attendre de vos solutions compatibles VMsafe ?

Klaus Majewski : VMsafe accroît la visibilité quant aux machines virtuelles et à l'hyperviseur. En revanche, côté sécurité réseau, je n'attends rien de révolutionnaire. VMsafe permet aux appliances de sécurité réseau d'inspecter le trafic avant son arrivée au niveau des applications virtuelles. Il donne également accès à des outils de gestion centralisés VMware dédiés à l'environnement virtuel. Les produits StoneGate sont d'ores et déjà en mesure d'inspecter l'intégralité du trafic avant qu'il n'atteigne les applications virtuelles et nous disposons, par ailleurs, d'une gestion centralisée de tous les composants de nos solutions de sécurité virtuelles.
L'idée d'utiliser des appliances de sécurité matérielles en vue d'inspecter le trafic des environnements virtuels par le biais de VMsafe a fait fortement débat. Cette solution peut convenir à certains clients, mais je la considère quelque peu contre-productive par rapport à la virtualisation. On ajoute encore aujourd'hui de nouvelles appliances matérielles, alors que l'essence même de la virtualisation est de diminuer la quantité d'équipements. Je pense que des produits, tels que les anti-virus, tirent davantage profit de la technologie VMsafe que des produits de sécurité réseau.

STONESOFT

VIRTUALISATION ET SÉCURITÉ, UN DUO INDISPENSABLE

Interview de Lionel Cavalliere, VMware, par Marc Jacob

La virtualisation est une technologie de plus en plus incontournable. En effet, elle permet des baisses de coûts importantes par la réduction du nombre de machines physiques, mais aussi par toutes les autres économies induites : énergie, temps de mise en œuvre,... En termes de sécurité, la suppression de la console d'administration avec hyperviseur ESXi (gratuit) et le programme VMsafe sont des atouts décisifs. Aujourd'hui, VMware se positionne comme un fournisseur d'OS qui se veut toujours plus sécurisé, comme le souligne Lionel Cavalliere, responsable Marketing Produit EMEA de VMware.

Global Security Mag : Quelle est votre vision du marché de la virtualisation dans le monde et en Europe ?

Lionel Cavalliere : Le marché de la virtualisation est en constante croissance. Selon IDC, il devrait atteindre un chiffre d'affaire de 3,6 milliards de $ en 2009 et dépassera 5 Milliards de $ en 2012. L'Europe représente actuellement 29% de ce chiffre et cette part devrait croître significativement à l'avenir. Le marché est scindé en deux, la partie virtualisation des serveurs et celle des postes de travail. Aujourd'hui, la croissance est principalement tirée par la virtualisation des serveurs pour les data-centers du fait d'un ROI rapide compris entre 6 à 8 mois. En effet, le premier cas d'utilisation est la consolidation de serveurs, qui permet de réduire le nombre de plate-formes et la consommation énergétique. La partie poste de travail est en train de décoller et a un fort potentiel.

GS Mag : Quelles sont les évolutions en termes de produit que vous allez proposer dans les années à venir ?

Lionel Cavalliere : Nous nous positionnons comme un fournisseur d'OS pour les data-centers : notre Virtuel data-center OS (VDC-OS) s'appuie sur l'hyperviseur « ESX Server » déployé sur les plateformes x86 du data-center. Ce socle fédère les ressources matérielles et fournit des services applicatifs de manière native. Ainsi, nos solutions permettent, par exemple, de bénéficier de caractéristiques de haute disponibilité ou de tolérance de panne d'un simple click de souris...

GS Mag : Comment avez-vous sécurisé votre hyperviseur ?

Lionel Cavalliere : Nous avons réduit la surface d'exposition en séparant la console d'administration de l'hyperviseur lui-même avec « ESXi Server ». Ainsi, cet hyperviseur « light » n'occupe plus que 32 MB sur disque tout en restant administrable. La console d'administration était, en effet, la source principale de vulnérabilités pour laquelle nous devions régulièrement fournir des patchs de sécurité à nos clients. L'approche ESXi est unique sur le marché et est garante d'un très haut niveau de sécurité native.

GS Mag : Quelle est votre stratégie avec vos partenaires éditeurs de sécurité ?

Lionel Cavalliere : Nous avons mis en place le programme VMsafe. Grâce à la position privilégiée de l'hyperviseur qui s'intercale entre le matériel et les machines virtuelles, VMsafe fournit une API spécifique qui donne accès à toutes les instructions exécutées dans les machines virtuelles, leur contexte, les échanges réseaux… Cela offre la possibilité aux éditeurs de sécurité comme Stonesoft de fournir leurs solutions spécifiques qui s'intègrent parfaitement dans nos environnements virtualisés. Une machine virtuelle dédiée traite alors la problématique de sécurité sans avoir à déployer des agents individuellement sur l'ensemble des machines virtuelles de l'environnement, comme c'est le cas actuellement.

GS Mag : Quels sont les bénéfices attendus du programme technologique VMsafe?

Lionel Cavalliere : L'intérêt pour nos clients finaux est de n'avoir à mettre à jour qu'une seule appliance virtuelle pour une problématique de sécurité donnée (antivirus, firewall..) qui protégera l'ensemble de leur parc. Notre approche fait abstraction du matériel, ce qui facilite grandement les déploiements.

GS Mag : Quel est votre message aux RSSI ?

Lionel Cavalliere : La virtualisation offre la meilleure plateforme de déploiement pour les applications x86 : facilité et rapidité de mise en œuvre… Notre programme VMsafe et ses partenaires fournissent le volet gestion de la sécurité indispensable aux environnements d'entreprise. Cette approche renforce notre positionnement et est un atout supplémentaire pour nos clients.

STONESOFT

DE L'ORGANISATION À LA TECHNIQUE

3 QUESTIONS À NICOLAS MONIER

Responsable Avant-Vente chez DCI,
interview par Marc Jacob

Global Security Mag : Quelles sont les menaces liées aux environnements virtuels ?

Nicolas Monier : Tout d'abord, il convient d'écarter un certain nombre d'idées reçues en matière de sécurité des environnements virtuels.
❶ Un système ne devient pas plus vulnérable parce qu'il est virtualisé. Il se contente de conserver ses failles habituelles. Il est éventuellement plus sensible aux dénis de services si les ressources allouées sont réduites au minimum requis.
❷ Même s'il n'existe pas de limites à l'ingéniosité des hackers, et si l'on suppose que l'un d'entre eux ait pris le contrôle d'une de vos machines virtuelles, il est peu probable que celui-ci réussisse, par rebond, à atteindre le système de virtualisation lui-même. Afin de minimiser une telle menace, il suffit à l'administrateur de n'autoriser aucun accès d'un hôte virtuel à une ressource physique.

Le risque réside ailleurs. Le fait est que l'on dispose rarement d'autant d'interfaces physiques qu'il existe d'hôtes virtuels sur une plateforme matérielle. Cela implique donc que l'on crée des hubs ou des switchs virtuels sur lequel on connecte plusieurs hôtes virtuels. On associe ensuite à chacun de ces switchs une interface physique permettant aux hôtes de communiquer avec le monde extérieur.

On crée ainsi des réseaux virtuels échappant totalement aux règles de segmentation en vigueur dans l'entreprise :
- D'une part, les hôtes réunis sur un même switch virtuel devraient parfois être distribués sur les segments différents (parce qu'ils correspondent à des niveaux de sécurité distincts).
- D'autre part, selon la façon dont ces switchs sont paramétrés, il est parfois possible de passer d'un segment virtuel à un autre.

GS Mag : Quelles stratégies de sécurité conseillez-vous à vos clients ?

Nicolas Monier : La première recommandation que je ferais est d'ordre purement organisationnel. Il devient clair que l'infrastructure réseau physique va céder du terrain face à des commutateurs virtuels (Le constructeur Cisco vient d'annoncer la sortie de son switch virtuel Nexus1000V). Dès lors, il convient de décider rapidement de quelle responsabilité relèvent ces infrastructures virtuelles. On peut affecter leur gestion au service « réseau », auquel cas celui-ci devra adapter sa politique de sécurité à ce nouvel environnement. On peut également décider que la virtualisation reste de la seule compétence du service « systèmes» et, dans ce cas, il faut sensibiliser les ingénieurs « systèmes » aux problématiques de sécurité réseau.

Le deuxième conseil est de regrouper les hôtes virtuels par niveau d'exposition aux attaques et de définir un switch virtuel par niveau. Il ne faut pas non plus oublier d'affecter un VLAN (minimum) à chaque switch de telle manière à pouvoir préserver l'étanchéité inter switchs virtuels lorsque le trafic réseau ressort sur l'infrastructure physique (auquel cas, le trafic est tagué et ne peut donc pas ré-entrer directement sur le système virtuel).

Partant de ces prérequis, deux options existent :
- Soit le trafic entre segments virtuels est routé et filtré via un firewall physique. Cela implique, dans la plupart des cas, de sérieuses limitations en matière de bande passante.
- Soit le trafic entre segments virtuels est routé et filtré via un firewall virtuel, auquel cas le flux réseau ne sort pas systématiquement de l'infrastructure virtuelle et l'on peut donc bénéficier de performances réseau importantes. De tels firewalls existent. Notons le cas de l'éditeur Stonesoft qui a récemment produit un firewall et un IPS virtuels certifiés par VMware.

GS Mag : Quels sont les projets que vous rencontrez actuellement dans ce domaine ?

Nicolas Monier : Aujourd'hui, l'essentiel des demandes sont orientées PRA. L'objectif est de s'appuyer sur la virtulisation et les facilités qu'elle offre en matière de duplication de systèmes afin d'améliorer les procédures de reprise d'activité après sinistre.
La plupart du temps, ces projets de virtualisation sont couplés à un projet d'acquisition de baies de stockage. En effet, la ou les plateformes matérielles PC vont supporter de 4 à 20 hôtes virtuels et ne pourront embarquer la capacité de stockage nécessaire.

Les serveurs virtualisés comprennent, la plupart du temps, à la fois des applications de gestion internes et des passerelles d'accès web. En effet, ces dernières sont souvent incluses dans les plans de reprise d'activité. On constate d'ailleurs que, souvent, l'ingénieur système tient compte de la problématique de sécurité et tente d'isoler les systèmes communiquant avec Internet dans un sous-réseau IP différent (cette mesure de protection n'est pas efficace mais elle indique que les administrateurs « Systèmes » sont sensibilisés aux problèmes de sécurité).

D'un point de vue économique, le phénomène le plus marquant est le glissement du marché de la grande entreprise vers la grande PME. Nous recevons à présent des demandes de structures, possédant de 1.000 à 3.000 postes, souhaitant virtualiser de 10 à 50 serveurs critiques et disposant de budgets de 30.000 à 200.000€.

STONESOFT

LES ÉQUIPES SYSTÈME, RÉSEAU ET SÉCURITÉ DOIVENT TRAVAILLER ENSEMBLE

Par Laurent Boutet, Stonesoft

Les environnements virtuels sont très en vogue au sein des entreprises de toutes tailles. Il est vrai que les avantages de cette technologie sont nombreux en termes de productivité, de coûts et d'exploitation. Toutefois, toutes nouveautés technologiques, surtout quand elles rencontrent un fort engouement, déplacent ou créent des problèmes de sécurité à ne pas négliger. Laurent Boutet, Pre-Sales engineer de Stonesoft France, considère que la principale menace qui pèse sur la virtualisation est la méconnaissance des risques par les utilisateurs. Pour lui, l'un des points clés de ces déploiements repose sur la collaboration entre les différentes équipes impliquées : système, réseau et sécurité.

Le problème majeur que nous rencontrons généralement est une méconnaissance, au sein des entreprises, des risques liés à la flexibilité d'usage et de production des environnements virtuels. En effet, ils sont souvent considérés comme une fonction système alors que les équipes réseaux et sécurité devraient être totalement impliquées dès leurs conceptions. Les architectures virtuelles sont en réalité basées sur des réseaux virtuels qui nécessitent les mêmes stratégies de sécurité.
Malheureusement, un environnement virtuel est souvent traité comme une boîte noire. Ainsi, la sécurité et le réseau s'arrêtent à la périphérie de ces architectures. C'est alors que nous avons pu constater des erreurs importantes de segmentation dans certains cas. Ainsi, la plupart des problèmes sont issus d'une mauvaise configuration ou usage, et non de la technologie.

La sécurisation des architectures virtuelles repose sur la collaboration entre les équipes réseau, sécurité et système

La première étape doit être d'ordre organisationnel, il est important qu'il y ait une collaboration forte entre les équipes réseau, système et sécurité. Les architectures virtuelles doivent être considérées comme des environnements classiques avec les mêmes stratégies de sécurisation, de surveillance, d'audit, de contrôle et de cloisonnement. Toutefois, elles ne doivent pas s'arrêter devant un serveur ou des lames, mais aller en profondeur, jusqu'au sein de l'architecture virtuelle.

Environnements Systèmes : les machines virtuelles doivent être sécurisées comme des machines réelles

Chaque machine virtuelle doit être traitée exactement comme une machine réelle. Il faut donc avoir les mêmes réflexes que pour un serveur d'entreprise classique, du durcissement de l'OS jusqu'à l'anti-virus en passant par les stratégies d'accès.
Le piège réside dans la facilité de mise en place de clone de machines ou de duplication d'application. Il faut éviter à tout prix de cloner une machine qui a été durcie ou patchée il y a 3 ans et s'en satisfaire. De plus, la multiplication des environnements R&D, pré-production, production et parfois leur proximité peut s'avérer une catastrophe. Il n'est pas rare que des machines restent actives sans aucune gestion, car oubliées après quelques jours de tests. La rapidité et la facilité de mise en place d'un environnement impliquent, en contrepartie, une procédure stricte pour s'assurer de la bonne mise en place de la sécurité de cette future plateforme.
Il faut également durcir l'hyperviseur sur lequel tout repose. Nativement, il s'agit de systèmes très optimisés et durcis, mais il existe un grand nombre d'éléments à contrôler et des règles assez classiques à mettre en places, telles que la séparation des flux de maintenance des flux de production, la protection d'accès à distance, l'authentification, la politique de gestion de mots de passe, la limitation d'accès au fichier, etc. De plus, il faut penser à désactiver certaines fonctionnalités

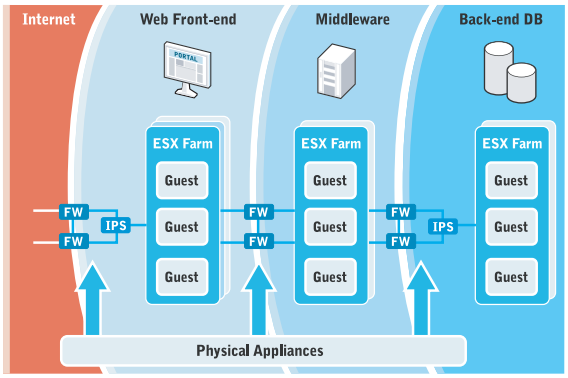
propres à ces environnements pour des serveurs de productions : désactiver la fonction de copier/coller entre le système hôte et la console est une parfaite illustration. Enfin, il reste nécessaire, pour un parfait contrôle, de protèger l'architecture à l'aide d'équipements Firewall et IPS réels et notament les flux liés à l'exploitation de ces environnements.

La sécurisation réseaux : 3 stratégies de segmentation pour les environnements virtuels

Il existe 3 stratégies possibles pour une mise en place de segmentation entre les différentes zones de serveurs virtuels.
La première consiste à consolider un ensemble de serveurs appartenant à une zone donnée au sein d'un seul environnement virtuel dédié à cette zone. En fait,

Stratégie 1

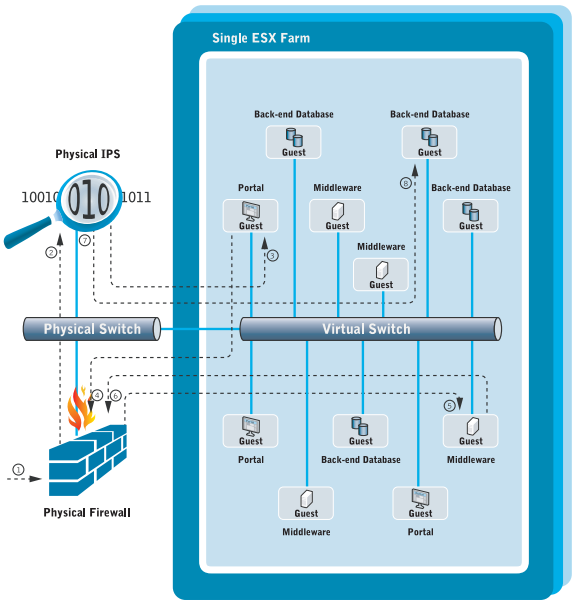
Retrofitting Hardware for Virtual Environments



chaque zone conserve une machine qui lui est propre assurant une parfaite segmentation par les équipements réels Firewall et IPS existants.
Souvent, il s'agit de la première approche dans la consolidation de serveurs. Toutefois, elle n'offre pas l'optimisation attendue par la mise en place de la virtualisation puisqu'il y aura autant de machines physiques qu'il y aura de zones différentes à protéger.

Stratégie 2

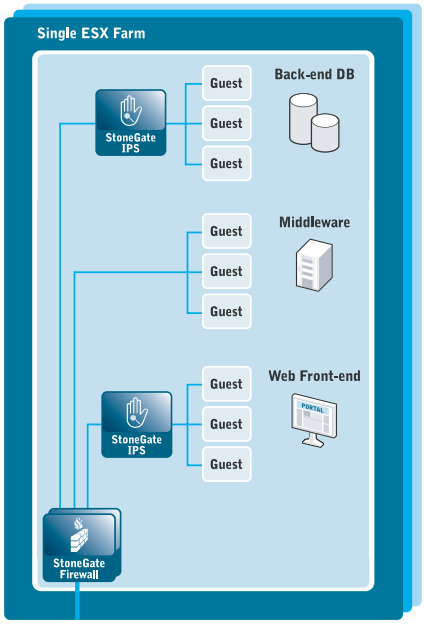
VLAN Tagging



D'un point de vue sécurité, a priori, on constate peu de changement par rapport à avant ; toutefois, on ne peut plus auditer, avec un IPS par exemple, les communications au sein de ces systèmes de façon aisée. Donc, on aura une perte en visibilité. De plus, certains administrateurs prennent la liberté de créer des sous zones qui ne seront pas correctement segmentées, car leur mise en place est plus facile et plus rapide d'un point de vue production.

Stratégie 3

StoneGate Software-based Virtual Architecture



La deuxième stratégie consiste à rassembler toutes les zones dans un même environnement virtuel. Dans ce cas, on optimise bien les ressources contrairement au cas précédent, mais il faut alors bien segmenter, au sein du système virtuel, différentes zones et les rattacher au réseau réel par des liaisons dédiées. On fera un usage intensif des VLANs ; toutefois, l'inconvénient est la perte de visibilité sur les communications internes des systèmes virtuels et surtout toute erreur permet rapidement de contourner les segmentations mises en place. De plus, les limitations du nombre d'interfaces peuvent rendre rapidement difficile ce type d'architecture.

La troisième stratégie consiste à faire rentrer la segmentation et la sécurité réseau dans l'environnement virtuel. On s'appuie alors sur des Firewalls et des IPS virtuels qui auront les mêmes fonctions que leurs homologues réels. Ici encore, on optimise pleinement les ressources, mais il faut bien segmenter les zones et bien construire son architecture réseau virtuelle. Le fait d'être au sein même du système permet de simplifier cette démarche et même de déployer des stratégies de doubles bastions, par exemple, ou de surveillance de communication inter-serveur par les IPS. Toutefois, cette stratégie nécessite toujours la mise en place d'équipements de sécurité réels pour protéger les équipements physiques.

Une console centralisée des éléments de sécurité, permettant une visibilité totale de l'environnement réel et virtuel, devient la clé du succès pour une bonne configuration, surveillance et un bon suivi d'audit de ces environnements. En effet, les architectures clientes s'appuieront sur un mélange des ces trois stratégies, ce qui peut impliquer un nombre de nœuds relativement important à gérer avec beaucoup de cohérence.

STONESOFT

LA SÉCURISATION DES ARCHITECTURES VIRTUELLES EN TOUTE FLEXIBILITÉ

Interview de Léonard Dahan par Marc Jacob

Léonard Dahan est le responsable de la filiale France et Benelux de Stonesoft depuis trois ans. Sa stratégie de développement s'inscrit dans la durée en privilégiant les relations de proximité, tant avec ses collaborateurs et partenaires qu'avec ses clients. Aujourd'hui, Stonesoft est l'un des seuls éditeurs à proposer des solutions de sécurité pour les architectures virtualisées qui se positionnent au cœur de ces environnements. Ces appliances sont commercialisées sous forme de licences afin d'assurer plus de flexibilité à sa clientèle.

Global Security Mag : Quels sont vos fonctions et rôles au sein de Stonesoft ?

Léonard Dahan : Je suis responsable de la filiale France et Benelux de Stonesoft. Au-delà des aspects Business et organisationnels liés à ma fonction, je reste très attaché à la qualité des relations humaines tant vers mes collaborateurs que vers nos clients et partenaires. En effet, ces aspects sont complexes et demandent du temps pour établir un climat de confiance et pérenniser la relation ou le partenariat. J'ai la chance d'être dans une société finlandaise où les valeurs humaines sont considérées. Mon rôle est donc de définir une stratégie commerciale en ligne avec les objectifs de ma maison mère tout en respectant notre culture d'entreprise. Ainsi, Stonesoft souhaite s'inscrire dans la durée et préserver les intérêts de ses clients et partenaires.

Nous avons plus de cinq ans d'expérience dans la sécurisation des architectures virtuelles

GS Mag : Pouvez-vous nous présenter vos solutions de sécurisation des architectures virtuelles ? Ces produits actuels peuvent-ils prendre en charge d'un environnement virtuel ? Si oui, comment faut-il procéder et quels composants supplémentaires faut-il acheter pour bénéficier du niveau de sécurité que nous offrent actuellement nos produits matériels ?

Léonard Dahan : Les solutions StoneGate sont conçues pour être des systèmes logiciels sécurisés de bout en bout de la chaîne de communication, ce qui signifie que la capacité à fonctionner dans un environnement virtuel est déjà intégrée. Elles n'induisent aucun coût supplémentaire dans le cadre de la mise en place d'un environnement virtuel. Avec plus de cinq ans d'expérience dans la virtualisation, StoneGate offre une gamme d'appliances virtuelles certifiées VMware pour pare-feu/VPN, IPS et SSL VPN.

La solution StoneGate Firewall/VPN fonctionne selon un principe simple : tout ce qui n'est pas expressément permis est refusé. La solution StoneGate IPS autorise le trafic normal et stoppe le trafic nuisible en cours de route. StoneGate fournit des systèmes virtuels avec pare-feu d'inspection dynamique, VPN, IPS et SSL VPN qui allient la puissance des signatures à l'analyse des anomalies. StoneGate Firewall/VPN intègre, en outre, une fonction d'inspection multicouches grâce à laquelle le pare-feu peut soit fonctionner comme filtre de paquets de base ou comme pare-feu d'inspection dynamique, soit effectuer une inspection approfondie des paquets au niveau de la couche application – chaque option étant sélectionnée au cas par cas par l'administrateur.

Exploitant les fonctionnalités VMware, les appliances virtuelles StoneGate sont extrêmement simples à mettre en œuvre.
Étant donné que les solutions StoneGate Firewall/VPN, IPS et SSL VPN intègrent leur propre système d'exploitation sécurisé, il n'est pas nécessaire d'en installer un au préalable dans la machine virtuelle. Cette intégration

du système d'exploitation ne simplifie pas seulement le processus d'installation, elle réduit également les temps de gestion. En effet, elle évite toutes les tâches associées à l'installation du système d'exploitation, comme la suppression des progiciels, applications, services, utilisateurs, groupes et fichiers parasites, la vérification des autorisations du système de fichiers et des téléchargements ou l'installation des correctifs et des services packs.

Les appliances virtuelles de la solution StoneGate de Stonesoft permettent de protéger les réseaux virtuels à l'aide d'un pare-feu virtuel/VPN et d'ajouter une protection supplémentaire pour les serveurs de bases de données via un système de prévention d'intrusions virtuel intégré. La solution StoneGate Management Center, qui réalise une gestion robuste et centralisée de tous les composants StoneGate, peut également être virtualisée. Elle permet ainsi à une organisation de tirer pleinement profit des avantages de la virtualisation tout en ayant l'assurance que le nouvel environnement est à l'abri des attaques internes et externes. Qu'ils soient physiques ou virtuels, les dispositifs de sécurité sont gérés à partir de la même console.

GS Mag : Votre produit est-il en mesure de surveiller avec précision les activités des environnements virtuels et physiques à partir d'une seule console de gestion ?

Léonard Dahan : La flexibilité de l'architecture StoneGate, qui lui permet de s'intégrer aussi bien dans les environnements virtuels que physiques, profite également aux organisations qui souhaitent gérer l'ensemble de leur réseau de manière centralisée à partir d'une seule plate-forme. Ainsi, la solution StoneGate Management Center (SMC) peut gérer des instances de dispositifs StoneGate virtuels et physiques, des clusters de dispositifs StoneGate virtuels et physiques, et des versions logicielles s'exécutant sur du matériel x86 standard. Elle permet également, pour chacun de ces éléments, une gestion unifiée des politiques. Les administrateurs ont la possibilité de surveiller, de contrôler et de changer les versions logicielles pour les clusters du périmètre sur des serveurs x86, les appliances StoneGate sur des sites distants et les machines virtuelles VMware, le tout à partir d'une interface utilisateur et d'un centre de gestion unique.

StoneGate renforce la sécurité des systèmes virtuels en fournissant des journaux du trafic, les fonctions de filtrage et d'audit

GS Mag : Comment votre produit m'aide-t-il à atténuer les menaces en temps voulu sur l'ensemble de mon environnement virtuel ?

Léonard Dahan : Grâce à ses fonctionnalités intégrées de journalisation et d'audit, StoneGate peut encore renforcer la sécurité du système virtuel en fournissant des journaux du trafic à l'entrée et à la sortie du système, et entre les machines virtuelles et les réseaux. Les fonctions de filtrage permettent à l'administrateur d'isoler rapidement les entrées qu'il recherche en fonction d'un certain nombre de critères, comme l'adresse IP source ou de destination, les informations d'authentification de l'utilisateur, l'heure, ou autre. Les fonctions d'audit surveillent l'accès et les modifications apportées aux politiques de sécurité et aux éléments réseau, notamment les propriétés et les informations de routage des dispositifs firewall/VPN et IPS. Associées à différents rôles et autorisations d'administrateur, ces fonctions permettent à une organisation d'exercer un contrôle très strict sur la sécurité de ses systèmes, qu'ils soient virtuels ou physiques.

Nous quittons le monde du hardware pour entrer dans celui du service

GS Mag : Pouvez-vous nous décrire votre stratégie commerciale ?

Léonard Dahan : Stonesoft renoue avec le succès et confirme sa position de pionnier sur le marché de la Sécurité et de la Haute disponibilité. En effet, nous affichons actuellement notre 5ème semestre de croissance à deux chiffres, avec un pic de 100% sur ce 3ème trimestre pour la zone Europe par rapport à celui de l'année précédente. La qualité de notre département Recherche et Développement nous permet d'être précurseur et d'annoncer des certifications innovantes et avant-gardistes. En effet, en phase avec l'actualité, nous annonçons notre certification Virtual Appliance VMware sur les technologies FW et IPS, nous sommes donc le premier éditeur / constructeur à apporter une offre complète de sécurité (FW et IPS) certifiée pour les environnements VMware ESX.
Notre développement commercial doit prendre en compte ce nouveau marché et nous devons adapter notre organisation. Ainsi, avec ses solutions, nous quittons le monde du hardware pour entrer dans celui du service.
Avec une licence StoneGate Virtual FW à 699 € et une licence StoneGate Virtual IPS à 995 € sous forme de redevance annuelle, nous allons faire quelques adaptations dans notre organisation de Distribution en France et Benelux.
Compte tenu également de la richesse et de la diversité des revendeurs VMware en France & Benelux ainsi que du modèle économique qui est le nôtre, un modèle 2-tier sera à privilégier dans les prochains mois…
En pratique, pour faire face à un marché de volume, nous avons mis en place des outils marketing innovants sous forme de Vidéo, afin de promouvoir notre savoir-faire auprès des revendeurs spécialistes de la Virtualisation mais aussi des Utilisateurs.

Nous souhaitons établir des relations de confiance avec nos clients

GS Mag : Quel est votre message aux RSSI ?

Léonard Dahan : La virtualisation étant en cours de démocratisation, les professionnels de la sécurité et les responsables informatiques doivent également veiller à ce que ces nouveaux environnements soient tout aussi sécurisés que les anciens systèmes physiques. De ce fait, ils doivent considérer sous un nouvel angle les stratégies de sécurité réseau, les systèmes et les outils de gestion/surveillance. Stonesoft est l'une des seules sociétés à fournir une suite de solutions logicielles de sécurité réseau et de continuité de service. Notre rôle étant de s'inscrire dans la durée et de préserver les intérêts de nos clients et partenaires, l'équipe de Stonesoft France & Benelux est toujours disponible pour participer à la réflexion des architectures de demain afin d'apporter notre savoir-faire dans la sécurisation des infrastructures virtuelles.

STONESOFT

L'INTÉGRATION DES FIREWALLS STONESOFT SOUS VMware EST UN AVANTAGE DÉCISIF !

Interview de Frédéric Le Guillou, CTO Chief Technology Officer
par Marc Jacob

Cegedim propose depuis de nombreuses années des solutions hébergées, en modèle ASP et, dans certains cas, en mode SAAS. La société a depuis longtemps misé sur la virtualisation ainsi elle a déployé des architectures virtuelles exclusivement au sein des data-centers. Pour Frédéric Le Guillou, CTO Chief Technology Officer, Cegedim Group, l'intégration des firewalls Stonesoft sous VMware est un avantage décisif, qui devrait lui permettre de gérer l'intégration de son informatique mondiale avec plus de flexibilité.

Global Security Mag : Pouvez-vous nous présenter Cegedim, ainsi que vos fonctions au sein de votre entreprise ?

Frédéric Le Guillou : Leader mondial du CRM santé, Cegedim conçoit des bases de données exclusives et des solutions logicielles à forte valeur ajoutée. Ces compétences s'exercent dans 4 secteurs :
- CRM et données stratégiques qui regroupent les services dédiés aux laboratoires pharmaceutiques
- Professionnels dédiés aux médecins et aux pharmaciens
- Assurance et flux de santé dédié aux acteurs de l'assurance Santé
- Technologies et Services qui s'adressent aux entreprises de tout secteur

Pour l'ensemble de ces 4 secteurs, Cegedim propose depuis de nombreuses années des solutions hébergées, en modèle ASP et, dans certains cas, en mode SAAS. La société a ainsi développé un savoir-faire dans ces domaines, supporté par un socle d'hébergement de haut niveau à couverture mondiale.
Au sein de Cegedim, j'exerce la fonction de CTO Chief Technology Officer Cegedim Group, avec pour principales responsabilités l'évolution et la définition de la stratégie du socle d'hébergement, en alignement avec les besoins de nos Business Units.

GS Mag : Quels sont les environnements informatiques dont vous avez la responsabilité ?

Frédéric Le Guillou : L'informatique du groupe Cegedim sert tant les besoins de l'informatique interne que les solutions développées pour nos clients, au travers de deux catalogues de services IT reposant sur un socle commun.

Les équipes de Cegedim gèrent tous les domaines techniques et logistiques de l'offre de services IT, que ce soit les infrastructures physiques des centres informatiques, les plates-formes serveurs, en passant par son réseau de télécommunications privé mondial.

Cegedim a depuis toujours misé sur la virtualisation

GS Mag : Pour quels types d'applications et de clients avez-vous mis en place des architectures virtualisées ?

Frédéric Le Guillou : Cegedim a depuis toujours misé sur la virtualisation. Elle a débuté avec 3 mainframes de type zSeries, et a étendu ce concept sur le monde Open et sur AIX. Cegedim s'est naturellement tourné vers VMware en 2004 en adoptant le produit ESX. Aujourd'hui plusieurs centaines de machines virtuelles sont déployées, dont la moitié est utilisée pour le compte de nos clients, dans le cadre de l'hébergement de solutions propriétaires ou « legacy ». L'informatique interne a été précurseur dans l'adoption de la virtualisation pour tous types d'environnements, du développement à la production. Cegedim dispose d'un vrai savoir-faire sur la virtualisation, et sur l'organisation opérationnelle indispensable pour sa maintenance.

GS Mag : Quelle est votre stratégie actuelle de sécurisation de vos architectures virtualisées ?

Frédéric Le Guillou : Notre stratégie de virtualisation comporte trois phases :
- mise en place de plates-formes de serveurs virtuels en data-center, déjà réalisée
- virtualisation de l'infrastructure réseau et des firewalls, en cours de finalisation
- virtualisation complète, offre de data-center virtuel, prévue en 2009

Les architectures virtuelles ou physiques bénéficient du même dispositif de sécurité périmétrique : filtrage et routage des flux par clusters d'appliances StoneGate. Les politiques de sécurité du réseau physique et des réseaux virtuels sont homogènes et leur gestion est centralisée.

La virtualisation couplée aux appliances Stonesoft nous permet de consolider nos serveurs en toute sécurité

GS Mag : Vous êtes en cours de consolidation de vos serveurs, quels sont vos nouveaux besoins en termes de sécurité ?

Frédéric Le Guillou : Nous fusionnons actuellement, d'une part, les infrastructures d'hébergement de notre ancien concurrent, et, d'autre part, l'infrastructure informatique interne, notamment les réseaux des deux entreprises.
La stratégie de fusion doit répondre à des exigences extrêmes en termes de continuité de service, en préservant le niveau de sécurité défini dans la politique Sécurité du Groupe Cegedim, et dans le respect des orientations de rationalisation du schéma directeur informatique.
La virtualisation des environnements sert ces objectifs et nous permet de nous affranchir de contraintes quasi insurmontables dans ce contexte.
En permettant le déploiement d'une solution Stonegate sur un socle virtuel, il est pour nous facile de pouvoir fournir à nos filiales un serveur virtuel embarquant tout le nécessaire pour accéder aux ressources groupes tout en respectant la politique sécuritaire du groupe. Le firewall s'intègre dans le parc actuel et est managé de manière centralisée.

Nous ne devrions pas avoir de réelles difficultés pour déployer VMware associé à StoneGate

GS Mag : Quelles sont les conséquences en termes d'organisation que vous vous attendez à rencontrer lors du déploiement de ses systèmes ?

Frédéric Le Guillou : Nous ne nous attendons pas à de réelles difficultés sur ce déploiement, qui s'inscrit dans la continuité de notre stratégie de mise en œuvre des technologies de virtualisation engagée il y a plus de 4 ans.
VMware est aujourd'hui parfaitement maîtrisé, nous utilisons le firewall StoneGate depuis plus de 6 ans, dans des conditions très sévères de continuité de service et de complexité des règles de filtrage.
Nous venons de réaliser avec succès une migration mondiale de la solution logicielle Stonegate vers les appliances FW-5000. Disposer de la même solution en data-center et dans les sites distants de nos filiales, administrée par la même console d'administration est déjà une réalité chez Cegedim, qui apporte un réel gain de productivité et s'intègre parfaitement dans notre support « follow-the-sun ».

Notre architecture virtuelle sécurisée va nous permettre de gérer l'intégration informatique mondiale de notre entreprise

GS Mag : Qu'attendez-vous de ce déploiement ?

Frédéric Le Guillou : L'intégration des firewalls Stonesoft sous VMware est un avantage décisif, car cela nous permettra de pouvoir gérer l'intégration informatique mondiale de Cegedim avec plus de flexibilité.
Cegedim croît, entre autres, par croissance externe, et a racheté son principal concurrent l'année dernière. L'intégration des deux informatiques mondiales est un processus long et complexe, du fait notamment de l'unification des pratiques sécuritaires. En disposant d'une solution virtuelle embarquant la solution Firewall groupe, nous pouvons appliquer une politique de sécurité uniforme, à moindre coût. Le processus d'intégration s'en voit fluidifié.

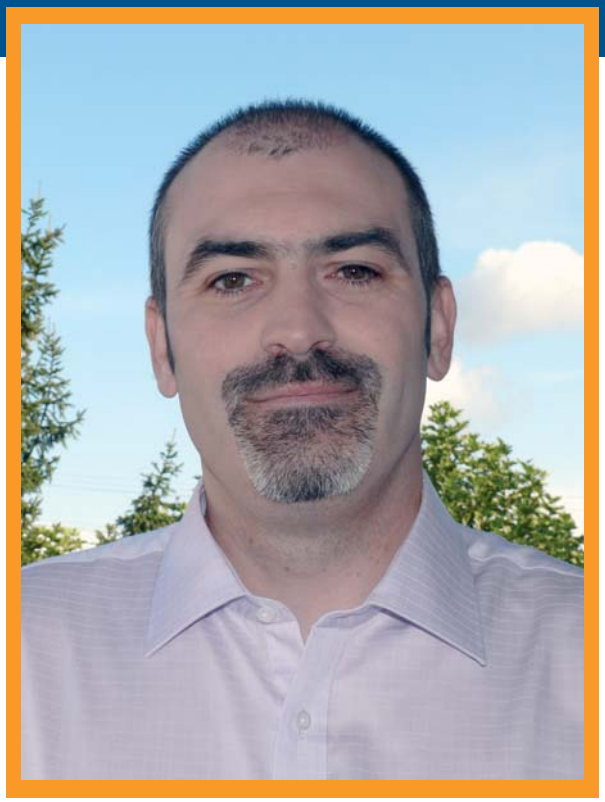
D'un point de vue business, la solution est particulièrement intéressante puisqu'elle permet de faire évoluer nos offres d'hébergements et d'offrir une solution complète (réseau virtuel et ressources serveurs) dédiée à un client. Ce concept s'apparente à celle de data-center virtuel pouvant être administré par nos clients.

STONESOFT

LA VIRTUALISATION EN TOUTE SÉCURITÉ AVEC STONEGATE VIRTUELS

Interview de Frédéric Ramage, Ingénieur Sécurité, Thales
par Marc Jacob

Frédéric Ramage est en charge de l'intégration des nouveaux projets et nouvelles technologies du Centre de Service Thales d'Elancourt. Depuis 2006, son entreprise s'est lancée dans la virtualisation de ses environnements de production afin, entre autres, de réduire ses coûts de déploiement. Pour sécuriser son environnement virtuel, Frédéric Ramage a choisi la solution StoneGate Virtuels qui répond à ses besoins en termes d'analyse des flux non chiffrés, de coûts de licences et de load balancing.



Global Security Mag : Pouvez-vous nous présenter Thales et vos fonctions au sein de votre entreprise ?

Frédéric Ramage : Thales est un leader mondial des systèmes critiques. Je suis rattaché à l'activité « systèmes d'information critiques » de Thales, qui fournit des services de conseil, d'intégration et d'infogérance à ses clients de l'industrie, de la finance, du transport et des administrations.
Je suis en charge pour ma part de l'intégration des nouveaux projets et nouvelles technologies du Centre de Service Thales d'Elancourt.

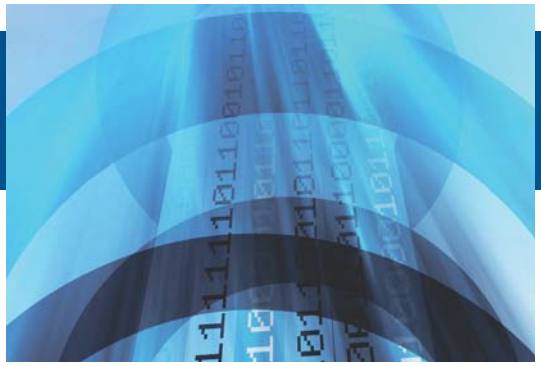
GS Mag : Quel était le contexte qui vous a amené à passer sur une architecture virtualisée ?

Frédéric Ramage : Comme beaucoup d'entreprise de services, la maîtrise des coûts est un challenge permanent. Thales s'est lancé en 2006 dans la virtualisation de ses environnements de production. Celle-ci apporte une réponse pertinente sur un déploiement et un maintien en condition opérationnelle très compétitif de nos services.

En effet, la virtualisation d'une partie du SI nous apporte une forte flexibilité, nous permettant d'ajuster les capacités de chaque environnement en fonction des besoins pour des coûts plus faibles : nous pouvons ajouter de nouveaux serveurs ou de nouveaux Firewalls très facilement. Par ailleurs, les coûts d'infrastructure (énergie, froid, …) de mise en place sont optimisés.

GS Mag : Pourquoi avoir choisi la virtualisation ?

Frédéric Ramage : La virtualisation est à ce jour très répandue au sein de Thales.
Notre architecture nécessitait un investissement léger



avec des possibilités d'évolution forte, mais aussi nous devions pouvoir mutualiser notre environnement pour accueillir d'autres clients au sein de cette plateforme physique. L'environnement cible était un excellent candidat à la virtualisation puisqu'il demandait peu de ressources (processeur, mémoire, IO).

GS Mag : Quels étaient vos besoins en termes de sécurisation de ses infrastructures et pourquoi avez-vous opté pour la solution de Stonesoft ?

Frédéric Ramage : Nos besoins étaient simples :
- Sécuriser notre plateforme avec des Firewalls statefull, et pouvoir faire une analyse des flux non chiffrés (http).
- Maîtriser les coûts : le mode de licence des StoneGate Virtuels s'y prête, car il est fait à l'année, sans notion de limitation de bande passante ou autre option ayant un impact financier sur l'évolution « naturelle » des architectures.
- Avoir un load balancer simple et efficace : cette fonctionnalité est intégrée au sein de la solution StoneSoft, permettant de répartir la charge sur une ferme de serveurs et d'assurer la haute disponibilité.

Les nouveaux drivers ESX Server devraient permettre de gagner en performance

GS Mag : Quels problèmes avez-vous rencontré lors du déploiement de votre solution de sécurité ?

Frédéric Ramage : Tout d'abord, nous avons rencontré une limitation au niveau des serveurs VMware : une machine virtuelle en ESX Server 3.5 ne supporte que 4 interfaces réseaux, ce qui n'était pas suffisant par rapports à nos besoins d'interconnexion. Nous avons dû adapter notre architecture à cette contrainte. (Cependant, il semblerait que fin 2008, une extension à 6 interfaces soit prévue).
Nous avons, par ailleurs, constaté que les performances réseaux sur serveur virtuel sont faibles (300Mbit/s de débit maximum par interface) comparées aux capacités des Firewalls physiques du marché. Ceci peut s'expliquer par le fait que l'utilisation des cartes réseaux virtuelles consomme du temps CPU, exécutant des opérations réalisées normalement par les ASICs des cartes réseaux des Firewall physiques. De plus, l'utilisation des switchs virtuels au sein d'un ESX est un facteur limitant par sa consommation CPU. Toutefois, les nouveaux drivers ESX Server (Enhanced VMXnet) devraient permettre de gagner en performance.

L'intégration de l'IPS virtuelle est un atout fort

GS Mag : Après 6 mois d'utilisation des solutions Stonesoft, quels enseignements retirez-vous ?

Frédéric Ramage : La virtualisation de Firewall au sein d'une architecture type VMware ESX Server est encore jeune mais prometteuse. Nous n'avons pas rencontré de problème majeur.
La segmentation des droits d'administration est nécessaire pour garder une sécurité métier satisfaisante, alors que par défaut sur un serveur ESX, l'administrateur peut tout faire.
Je pense que StoneSoft a développé une solution innovante et doit continuer à la faire évoluer, sur ce qui constitue de plus en plus le cœur de nos environnements.
L'intégration de l'IPS virtuelle est un atout fort. Le déploiement et le déplacement d'un environnement à un autre d'une sonde sont très simplifiés du fait de la virtualisation (template, connectique réseau virtuelle,…). En terme d'évolution, c'est très appréciable !

GS Mag : Quelles améliorations souhaiteriez-vous voir apparaître dans les produits Stonesoft ?

Frédéric Ramage : La version 4.3 de la SMC, ainsi que les engines en 4.2.4 (à ce jour), ont apporté beaucoup d'améliorations. Je pense qu'il faut rapidement que le Clustering A-A et le Tagging soient supportés officiellement, même si ceux-ci fonctionnent parfaitement*.

Une période de test complet est nécessaire avant de passer à la production

GS Mag : Quels conseils adressez-vous à vos confrères RSSI, pour les aider à déployer des architectures virtualisés ?

Frédéric Ramage : Question difficile…
La virtualisation est à la fois une aubaine, mais aussi un piège. Je pense qu'avant de virtualiser, il faut vraiment bien connaître son SI et avoir des objectifs précis.

Une période de tests, de benchs et de qualification de la future architecture est nécessaire avant de la passer en production. Il faut bien regarder les possibilités offertes par la virtualisation, tant son potentiel est grand.
Si on manque d'expérience, faire appel à du conseil extérieur est un moyen pour éviter les erreurs habituelles et déployer plus rapidement.

*** NDLR :** Ces fonctionnalités ainsi que d'autres sont supportés depuis la fin de l'été date à laquelle Stonesoft a reçu sa certification virtuelle appliance de VMware

EN UN CLIN D'ŒIL

StoneGate SSL VPN

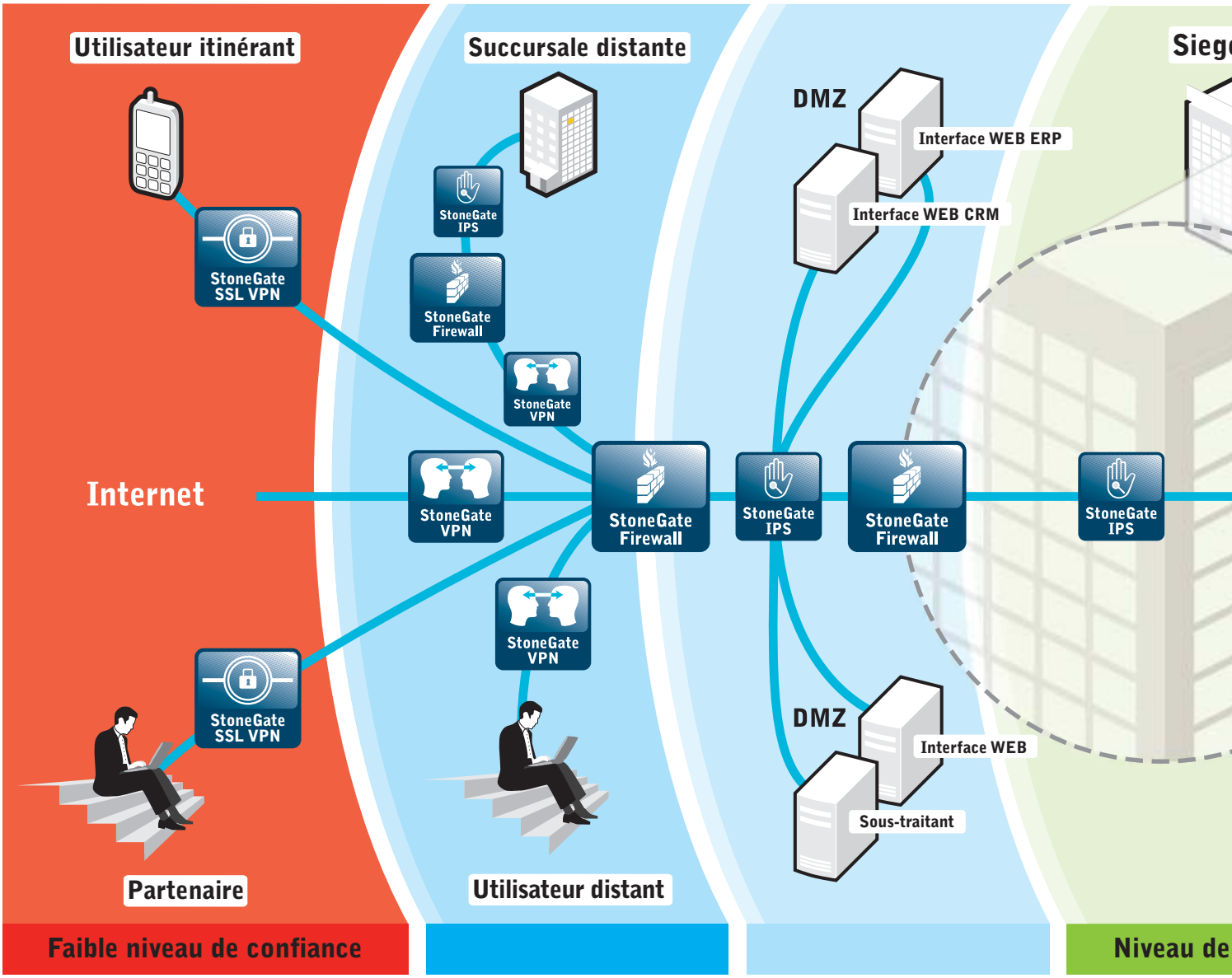
Un accès sécurisé mobile et distant, en tout lieu, à tout moment, depuis n'importe quel dispositif

Forte d'un réseau privé virtuel, ou VPN (Virtual Private Network), à technologie SSL, la solution de connectivité sécurisée mobile de StoneGate fournit à l'entreprise un accès distant flexible, sécurisé et économique à ses informations, ses applications et ses ressources réseau. La solution offre également un contrôle des accès réseau, ou NAC (Network Access Control), aux endroits où il est le plus indispensable à un accès réseau mobile depuis des équipements non identifiés.
Sécurité modulaire et fiable de bout-en-bout avec cryptage robuste, authentification puissante, contrôle des accès granulaire et suppression exhaustive des traces ; autant d'atouts clés qui caractérisent la solution StoneGate SSL VPN.

STONEGATE IPS

Une protection exhaustive contre les programmes malveillants et les attaques DoS

Intégrée à StoneGate Firewall/VPN, la solution StoneGate IPS vient renforcer la défense du périmètre en protégeant l'intérieur de votre réseau. StoneGate IPS protège les applications vulnérables, les systèmes d'exploitation et les bases de données d'arrière-plan en interceptant les attaques, notamment les vers (worm), les logiciels espions (spyware), les préjudices liés au peer-to-peer et aux applications web, ou encore les dénis de service, ou DoS (Denial of Service).
Le module de contrôle d'accès transparent unique de StoneGate réunit les fonctionnalités de prévention d'intrusion IPS et de pare-feu. Il fournit ainsi une protection contre les agressions et permet un contrôle des accès transparent par le biais du pare-feu, sans modification aucune des configurations réseau existantes.



StoneGate Management Center

Une gestion et une configuration faciles et économiques

La solution StoneGate Management Center (SMC) propose une approche holistique et innovante d'une administration fondée sur des rôles par le biais d'un système de gestion unique et centralisé. StoneGate Management Center autorise les avantages suivants :

Profiter de fonctionnalités avancées, notamment de mises à niveau à distance, de la gestion d'un centre d'alarme et de fonctions de génération de rapports très perfectionnées

Créer un site de reprise après sinistre, afin de garantir un accès continu aux ressources de gestion et de journalisation

Diminuer les délais d'intervention en cas d'incident, simplifier l'administration quotidienne et réduire le coût total de possession, ou TCO (Total Cost of Ownership).

Solution pare-feu/réseau privé virtuel StoneGate

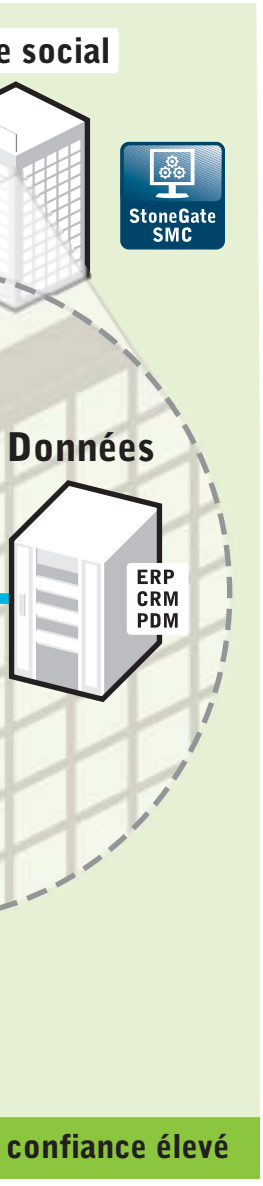
Continuité de service et sécurité réseau renforcée

La solution pare-feu/réseau privé virtuel StoneGate Firewall/VPN établit un périmètre de protection autour de votre entreprise, bloque les attaques et sécurise les flux d'informations au moyen d'un réseau privé virtuel.

La solution StoneGate Firewall/VPN autorise un contrôle granulaire du réseau avec une capacité de qualité de service, ou QoS (Quality of Service), et une gestion de la bande passante.

La technologie Multi-Link

La technologie Multi-Link de StoneGate résout le manque de fiabilité des liaisons WAN en ajoutant une vraie répartition de charge des tunnels VPN et une tolérance de pannes à l'aide d'un basculement automatique transparent vers les tunnels VPN toujours actifs ou de secours. Avec le Multi-Link, les connexions VPN peuvent devenir aussi fiables et même plus sécurisées que les liaisons WAN privées classiques. Un basculement automatique transparent signifie que les utilisateurs conservent leurs connexions, même si une ou plusieurs liaisons WAN sont perdues. Le Multi-Link améliore la performance VPN de façon significative, car il choisit toujours le chemin le plus rapide pour les connexions des utilisateurs. Un plus haut débit, un temps de latence plus court et une plus grande fiabilité permettent donc de répondre aux besoins des entreprises en termes de centralisation des applications métiers, d'architectures clients légers et des infrastructures VoIP...



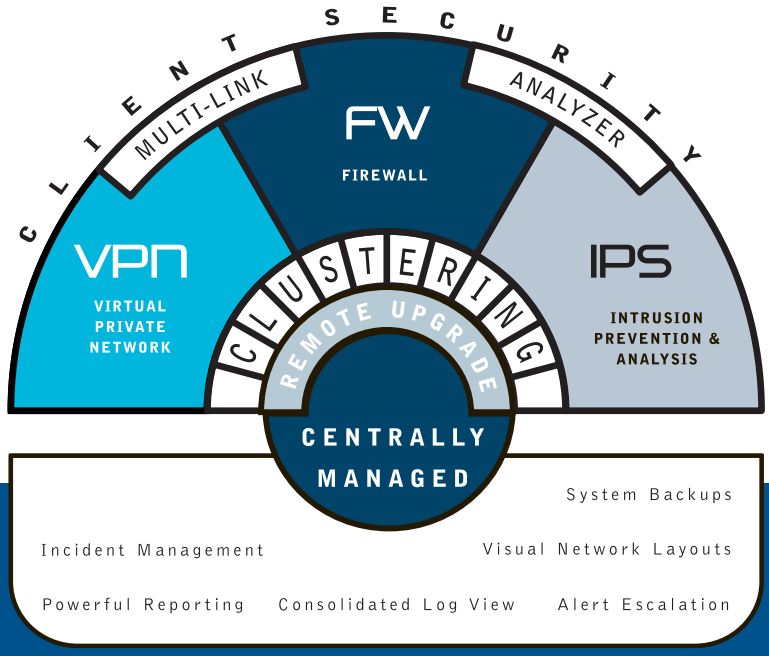
Les 5 Points clés de l'offre Stonesoft

- Constructeur européen certifié EAL4+ depuis 2002 pour ses solutions intégrées de sécurité réseau et de continuité de services.
- 3 gammes de solutions de sécurité et de haute disponibilité pour les réseaux d'entreprises : StoneGate Firewall & VPN (VPN et pare-feu), StoneGate IPS (sonde de prévention d'intrusion) et Stonegate VPN-SSL (connexions VPN nomades). Ces solutions s'appuient sur un socle commun, la StoneGate Management Center (plate-forme d'administration).
- Une offre à la fois sous forme d'Appliance et de logiciel. Ces solutions s'intègrent également dans les environnements virtuels, avec le même niveau de fonctionnalités.
- Une des seules solutions capables de sécuriser une infrastructure réseaux de bout en bout sur la chaîne de communication client-serveur, par ses mécanismes de clustering, de répartition de charge serveurs et de liaisons WAN. De plus, son mécanisme exclusif Multi-Link VPN ™ permet de fonder une architecture multi-sites totalement redondante assurant aucune rupture de session en cas de défaillance des opérateurs.
- Une Console d'administration et d'exploitation des moteurs StoneGate très mature et pourvue de richesses fonctionnelles très adaptées aux environnements distribués, data-center et/ou MSSP.

STONESOFT

STONESOFT

LE CŒUR DE L'ARCHITECTURE STONEGATE



Le StoneGate Management Center (SMC) permet d'administrer de manière centralisée l'ensemble des équipements StoneGate (FW/IPS/VPN/VPN-SSL) à l'aide d'une interface graphique unique. Le SMC gère de façon totalement transparente aussi bien les moteurs réels que les moteurs virtuels afin de consolider l'ensemble des noeuds de sécurité d'une architecture.

Le module StoneGate Management Center propose en standard la totalité des fonctions d'administration, dont :

- Cartographie de réseau
- Industrialisation des déploiements
- Analyse statistique des logs
- Mise à jour en ligne
- Management des incidents
- Rapport et Audit

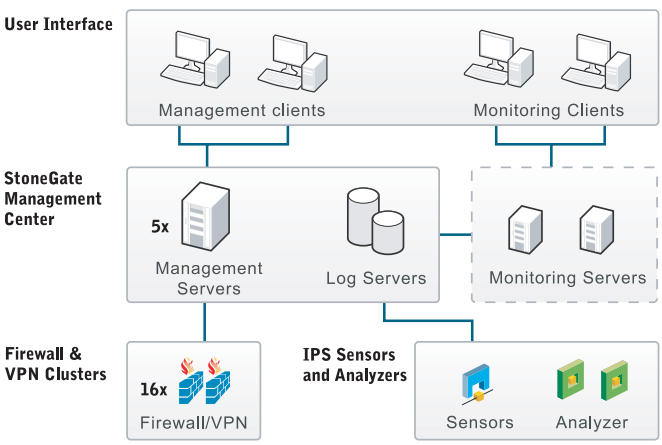
Le Système d'Administration StoneGate Management Center constitue la charnière centrale de la solution de sécurité.

Pour des raisons évidentes de performances, de fiabilité et de sécurité, Stonesoft a choisi une architecture d'administration 3-tiers. C'est-à-dire que les serveurs de Managements, de Logs et d'Alertes sont dédiés. Ainsi les équipements de filtrage FW/VPN/IPS se concentrent sur leurs tâches. Le traitement des logs, par exemple, ne fait pas chuter les performances du Firewall.

Abordant le thème de la sécurité, les entreprises doivent le plus souvent employer des outils d'administration différents pour chaque produit. Ainsi, elles sacrifient leur capacité de management avec des outils de « management unifié », pour des produits non conçus pour être administrés ensemble. Il en résulte des coûts de formation élevés, et une baisse du niveau de sécurité, dû à l'incapacité de l'équipe à administrer tout l'environnement de sécurité.

Les produits de StoneGate sont conçus – dès l'origine – pour s'intégrer dans un système d'administration commun. StoneGate Management Center permet de piloter efficacement l'ensemble de la solution, en utilisant des objets de configuration, des concepts, des modèles, des systèmes de logs, d'audit et d'alertes communs, ainsi que tous les autres outils d'administration.

L'unité des configurations de sécurité, de réseau et de disponibilité « de bout en bout » réduit la complexité de la solution, améliore le niveau de sécurité. Ainsi, une économie de temps et d'argent dans les tâches d'exploitation quotidiennes est constatée.



FONCTIONNALITÉS EN BREF

GESTION CENTRALISÉE

- «Définir une fois, utilisez-partout » les éléments réseaux
- Mise à niveau à distance sécurisée
- Audit et traçabilité des actions administrateur
- Outil d'analyse de la base de règles
- Modèles de bases de règles et bases de sous-règles afin d'améliorer l'efficacité et la performance
- Système simple de sauvegarde et de restauration
- Administration basée sur des rôles système
- Routage en glisser-déposer
- Mise en page visuel du réseau pour un suivi de l'état et des configurations des équipements
- Toutes les communications sont cryptées et authentifiées
- Aperçu de l'état de connectivité, des nœuds, et de la sécurité
- Configurer et modifier plusieurs éléments à la fois
- Gestion des incidents de sécurité et outil de documentation

GESTION CENTRALISÉE DES LOGS

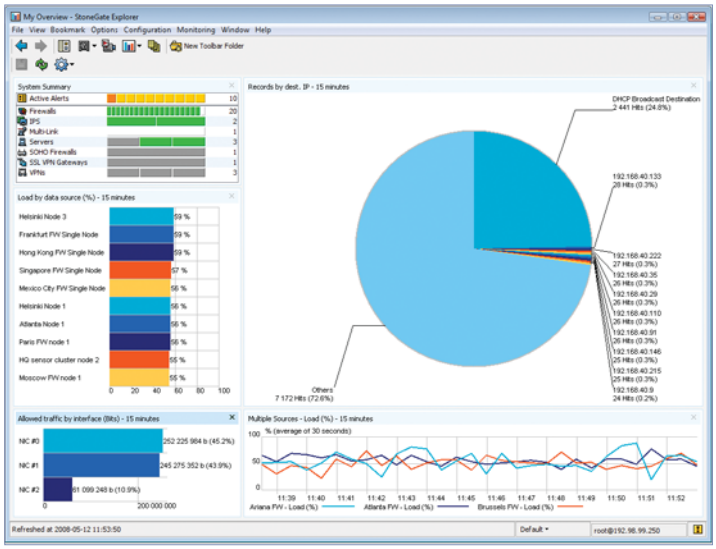
- Navigateur de logs rapide qui consolide l'ensemble des journaux et des informations d'alerte en une seule vue
- Support de multiples serveurs de logs
- Filtrage avancé des logs pour la navigation, l'exportation et le nettoyage
- Planification de l'exportation des données de logs et de leur manipulation
- Serveur de logs de haute performance

SURVEILLANCE ET ALERTES

- Surveillance graphiques et temps réel du trafic et des statistiques
- Surveillance des sessions et des listes noires
- Escalades d'alertes configurables
- Système de test interne : système de restauration automatique

REPORTING

- Système de rapports et rapports personnalisables par glisser-déposer
- Rapports exportables au format PDF
- Sélection des données en utilisant des filtres
- Données figurant sous forme de graphiques, de tableaux ou les deux combinés
- Consolidation des données provenant de plusieurs serveurs
- Rapports créés périodiquement et /ou manuellement
- Modèles de rapports personnalisables



STONESOFT VIRTUAL IPS : LA SÉCURITÉ EN PROFONDEUR POUR LES ENVIRONNEMENTS VIRTUELS

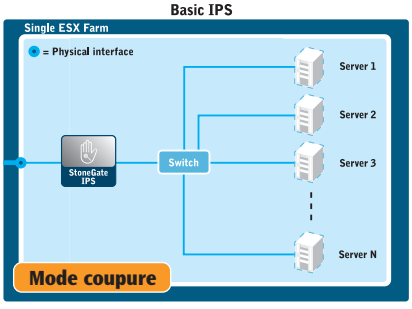
L'IPS est devenue une fonction incontournable de sécurité pour détecter le trafic malicieux ou inapproprié. Ainsi, Stonesoft a développé StoneGate Virtual IPS, un système de détection et d'analyse du trafic qui permet d'organiser la réponse appropriée. Cette solution est l'unique moyen d'avoir une visibilité et une protection exhaustive des communications entre toutes les machines virtuelles.

La virtual appliance StoneGate IPS possède toutes les fonctionnalités d'une appliance classique Stonegate IPS.
Grâce à cette virtual appliance, il est possible de filtrer les flux au sein d'une infrastructure virtuelle, mais également de faire du reporting sur l'ensemble des flux transitant entre les machines virtuelles et sur les flux sortant du serveur ESX.
StoneGate Virtual IPS est un système qui détecte et analyse le trafic malicieux ou inapproprié, l'identifie précisément, et organise la réponse appropriée.
Cette virtual appliance IPS a une importance primordiale au sein d'un environnement virtuel, car c'est l'unique moyen d'avoir une visibilité et une protection exhaustive des communications entre toutes les machines virtuelles.

StoneGate Virtual IPS pour une sécurité en profondeur

StoneGate Virtual IPS détecte et bloque en temps réel les attaques sur les flux autorisés par le Firewall. Il révèle également la présence de vers, de spywares sur le réseau ou d'applications P2P.
La technologie exclusive de StoneGate Virtual IPS permet une détection plus précise. Elle s'appuie sur des méthodes contextuelles multiples :
- Base de Signatures (expressions logiques personnalisables)
- Analyse protocolaire
- Détection d'anomalie protocolaire
- Identification protocolaire (ex : P2P sur http)
- Détection évoluée de scans de ports

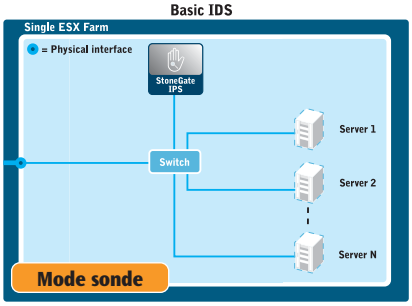
Basic IPS



Il est possible d'installer au sein de l'architecture virtuelle le Stonegate Virtual IPS en mode coupure de trafic et/ou en mode sonde.

Le mode coupure permet de bloquer instantanément une attaque avant que celle-ci n'atteigne sa cible. On place le StoneGate Virtual IPS en rupture devant des machines virtuelles.

Basic IDS



Le mode sonde permet l'analyse de tout le trafic sur un Switch virtuel grâce à la fonction de port miroir. Ce dernier peut également permettre de bloquer le trafic en déléguant cette fonction à un autre moteur Stonegate IPS et/ou FW.

Le Stonegate Virtual IPS supporte également la fonction Transparent Access Control qui permet de mettre en place des règles d'accès du niveau 2 à 7 en complément des fonctions IPS. Ce module offre la possibilité de segmenter un réseau efficacement en implémentant facilement des règles de type Firewall Stonegate. Il prévient aussi les accès non-autorisés entre différentes zones, virtuelles ou non, de niveaux de sécurité différents.

FONCTIONNALITÉS EN BREF

- Protège les applications vulnérables contre les attaques réseaux, y compris les vulnérabilités côté client et côté serveur sur les systèmes d'exploitation de type Windows et Linux / Unix…
- Détecte les logiciels espions, les attaques de types DoS (rate based DoS et non-rate based DoS), les scans de ports, les chevaux de Troie, les vers, les anomalies protocolaires et les transactions réseaux.
- Comprend plusieurs méthodes d'inspection – validation protocolaire, détection d'acte malveillant, signatures génériques et contextuelles, détection de déni de service, détection de scan et corrélation spatiale et temporelle des événements détectés.
- Comprend des milliers de signatures pour plus d'une centaine de protocoles - HTTP, DNS, IMAP, SMB, MSRPC, MYSQL, Oracle, POP3 et bien d'autres.
- Comprend des signatures personnalisables qui utilisent la syntaxe des expressions régulières pour permettre une meilleure protection contre les vulnérabilités.
- Fournit un mécanisme de corrélation d'événement intelligent pour réduire et gérer les faux positifs et faux négatifs.
- Permet en mode coupure le blocage automatique et immédiat des anomalies détectées ou dans le cas d'une violation de la politique de sécurité.
- Fonction avancée de liste noire et de liste blanche en collaboration avec d'autres éléments StoneGate virtuelles et/ou physiques.
- Le Stonegate virtual IPS permet, au sein de la même appliance virtuelle, l'implémentation du mode coupure et/ou du mode sonde.

STONESOFT

Sécurise vos flux

Multi-Link™ est la technologie brevetée par Stonesoft face aux problèmes actuels de continuité de service de vos accès à Internet. La fonctionnalité d'équilibrage de charge assure la Haute-Disponibilité et l'augmentation de la bande passante. De ce fait, Multi-Link™ est la solution pour réduire vos coûts mensuels de télécommunications et d'interventions sans interruption de votre activité.

www.stonesoft.com

STONESOFT

www.stonesoft.fr

Secure Information Flow

www.stonesoft.fr | Stonesoft France - 38, Rue de Villiers - 92300 Levallois - Téléphone: +33 1 47 58 48 05