

STONESOFT

Livre blanc

Les enjeux méconnus de la sécurisation d'un environnement virtuel

Sommaire

Synthèse	1
Les enjeux liés à la sécurisation d'un environnement virtuel	2
Comment s'assurer qu'une solution de sécurité réseau est adaptée aux environnements virtuels	5
Conclusion	8

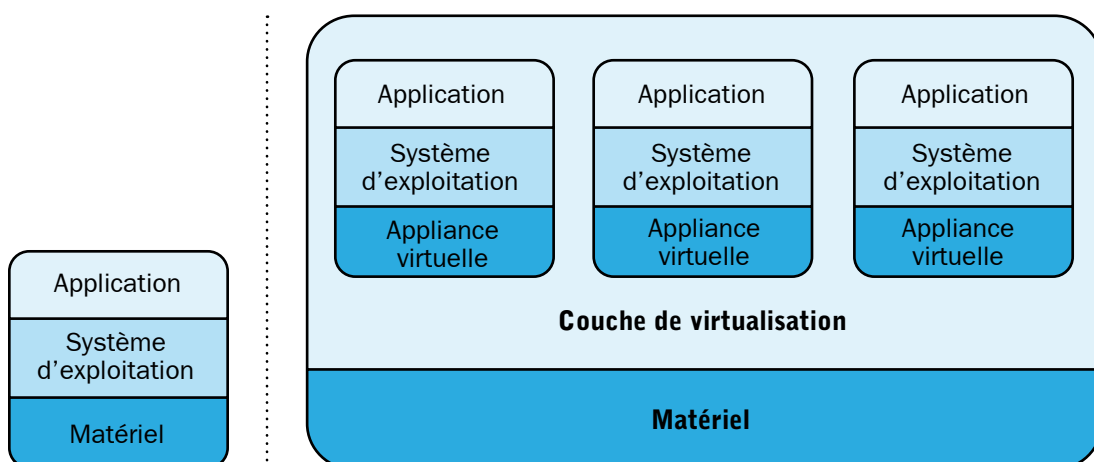
Synthèse

La virtualisation prend 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. Où se situe votre entreprise par rapport à ces statistiques ?

Si vous avez déjà mis en œuvre une stratégie de virtualisation, ou si vous êtes en passe de le faire, la sécurité de votre entreprise risque d'être exposée à des menaces qui pourraient avoir un impact plus désastreux que jamais sur votre environnement d'exploitation. Étant donné que les systèmes de sécurité traditionnels ont recours à du matériel et à des systèmes d'exploitation spécifiques pour protéger votre environnement, ils perdent toute leur utilité dans un environnement virtuel où l'objectif consiste à réduire voire à éliminer le matériel.

Les meilleures pratiques classiques sont en outre remises en question puisque la segmentation physique et d'autres méthodes sont devenues presque impossibles à réaliser. Pour finir, en raison de la nature de l'environnement virtuel, la complexité du réseau augmente plus rapidement qu'avec des systèmes de gestion et de surveillance hérités, ce qui obscurcit nettement la visibilité sur les environnements virtuels et physiques. Dans le nouveau monde virtuel, les entreprises doivent réfléchir plus sérieusement à une nouvelle manière de sécuriser leurs réseaux et leurs données sensibles.

Ce livre blanc vise à donner aux professionnels de la sécurité et aux responsables informatiques une solide connaissance des risques potentiels qu'ils encourent s'ils n'incorporent pas de nouvelles technologies de sécurité à leurs environnements virtuels. Il explique pourquoi les systèmes traditionnels ne fonctionnent pas et contient une liste de questions à se poser pour s'assurer qu'un réseau est bien adapté aux environnements virtuels.



Architecture classique x86

- » Un système d'exploitation par serveur
- » Logiciel et matériel étroitement liés
- » Une application par serveur
- » Charge habituelle du serveur : 5 à 15 %

Architecture virtualisée

- » Différents systèmes d'exploitation par serveur
- » Séparation entre matériel et logiciel
- » Plusieurs applications par serveur
- » Charge habituelle du serveur : 50 à 70 %
- » Ressources optimisées dynamiquement

Les enjeux liés à la sécurisation d'un environnement virtuel

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.

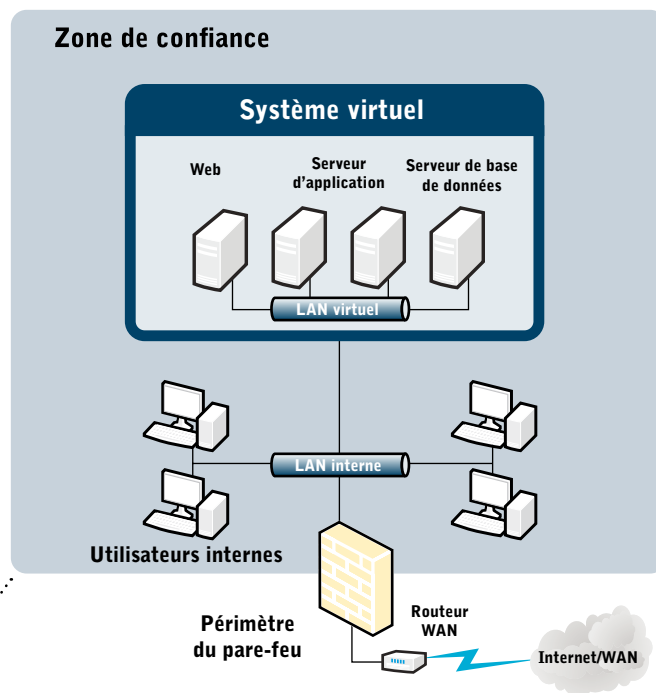
Maintenant que la virtualisation se généralise, de nombreuses entreprises s'y mettent sans prendre en compte tous les risques qu'elle comporte en termes de sécurité. Ces risques tiennent au fait que les nouveaux modes de travail sont sécurisés par des méthodes dépassées reposant sur un équipement inadéquat. Voyons à présent pourquoi les systèmes traditionnels de sécurité réseau créent des risques importants pour des milliers d'organisations.

Les solutions de sécurité matérielles traditionnelles perdent leur utilité

Au cœur de toute stratégie de virtualisation se situe la suppression ou la diminution des serveurs et du matériel. La majorité des solutions de sécurité traditionnelles, tels que les pare-feu et les systèmes de prévention des intrusions (IPS), sont basées sur le matériel, c'est-à-dire qu'elles résident sur une machine en amont du système qu'elles sécurisent. Lorsqu'il n'y a plus de matériel, le dispositif de sécurité est uniquement en mesure de jeter un voile protecteur sur l'ensemble de l'environnement virtuel, et non sur chaque composant individuel.

Pour compliquer encore le problème, la plupart des fournisseurs de solutions de sécurité utilisent du matériel ASIC, soit des systèmes conçus spécifiquement pour remplir une fonction bien particulière : assurer la sécurité. Ces circuits intégrés doivent être présents pour

Le principal problème de la virtualisation



Le principal problème de la virtualisation réside dans le fait qu'elle réunit les différents niveaux d'une architecture applicative classique en un seul système virtuel et qu'elle place ces derniers dans une seule zone de confiance accessible à l'ensemble des utilisateurs internes. Cet « aplanissement » de l'architecture expose le système à des menaces de la part des utilisateurs internes et supprime toute possibilité de protéger les données les plus stratégiques en cas d'infraction.

que ces solutions fonctionnent. Or dans un véritable environnement virtuel, il n'y a pas de place pour des circuits intégrés spécialisés supplémentaires.

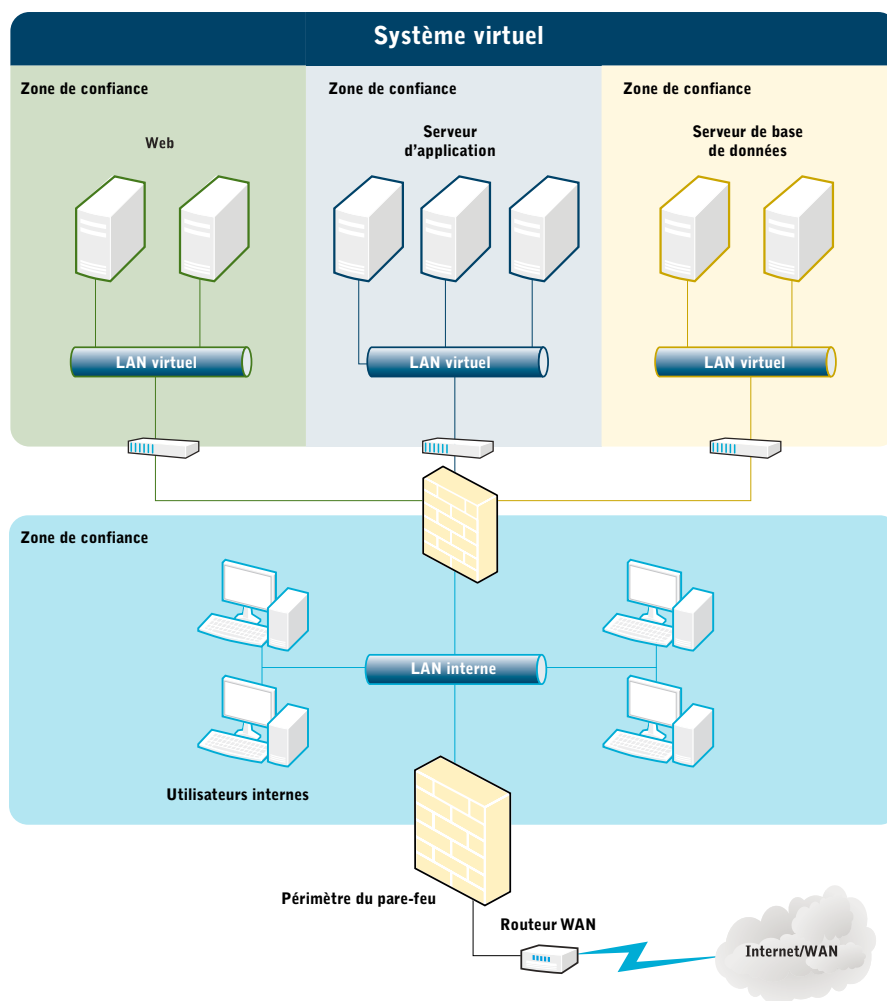
Enfin, les solutions de sécurité matérielles étant généralement placées à la périphérie de l'environnement, elles exposent davantage les organisations aux attaques venant de l'intérieur, lesquelles représentent 59 % de toutes les attaques selon une enquête réalisée par le CSI en 2007.

Les modèles traditionnels de contrôle de la sécurité sont remis en cause.

Toute architecture informatique possède au moins trois niveaux : 1) la base de données d'arrière-plan qui contient les données stratégiques sur les clients ou l'organisation, c'est-à-dire la mine d'or à laquelle la plupart des hackers tentent d'accéder ; 2) le middleware applicatif qui permet à l'utilisateur final d'agir comme il l'entend sur les données ; 3) les serveurs Web frontaux qui permettent au monde extérieur d'interagir avec les deux précédents niveaux.

Pour que l'application puisse fonctionner comme prévu, les dispositifs de sécurité sont généralement placés en amont des serveurs Web et configurés pour laisser passer le trafic Web. Or, selon de nombreux analystes, près de 80 % de toutes les failles dans le système de sécurité proviennent d'attaques lancées par le biais de protocoles Web. Lorsqu'un serveur

Virtualisation externe du pare-feu

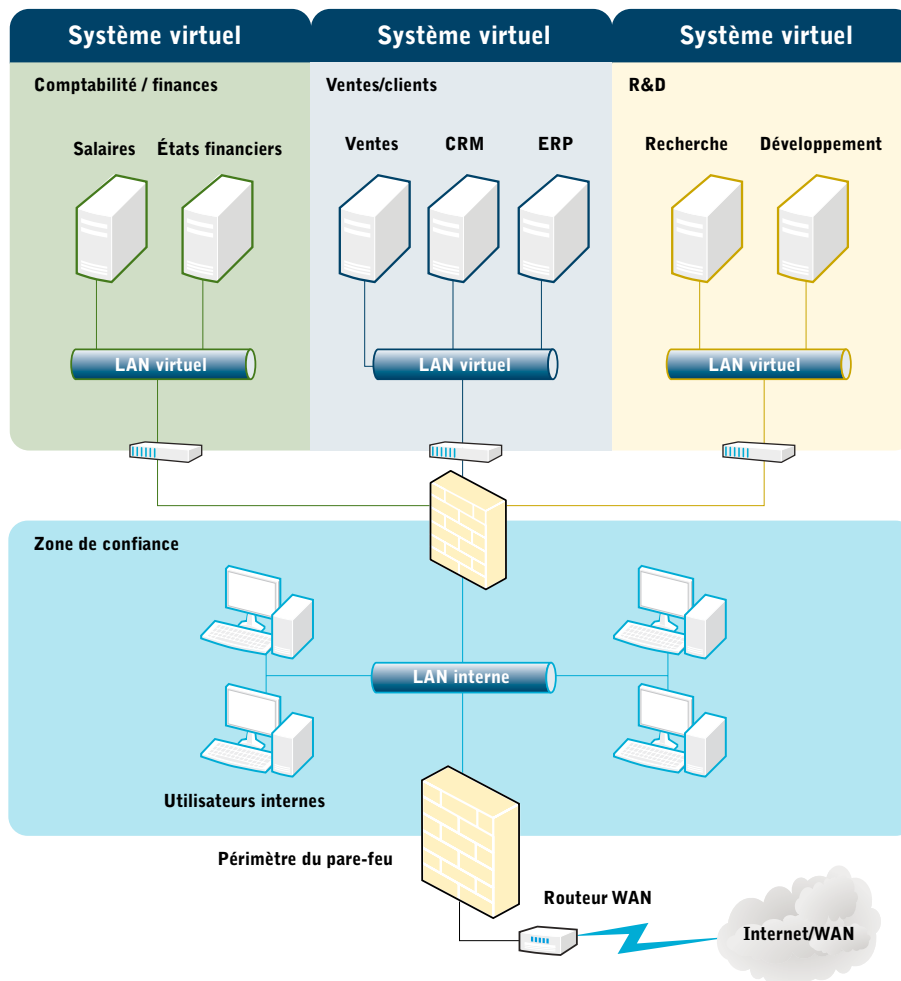


Les organisations cherchant à améliorer la sécurité de la virtualisation ont dû envisager l'utilisation de produits matériels extérieurs à l'environnement virtuel. Les composants de sécurité réseau ne pouvant toutefois être virtualisés, l'organisation ne peut toujours pas voir à l'intérieur de l'environnement virtuel, ce qui induit des difficultés supplémentaires en termes de conformité et d'audit. En outre, l'architecture ne tire pas pleinement profit des avantages de la virtualisation, générant ainsi des coûts supplémentaires dus à la complexité, à l'électricité, à la ventilation, etc.

Web a été infiltré dans le modèle traditionnel, ce serveur et son application restent les seuls concernés par l'intrusion.

Dans un environnement virtuel, en revanche, où de multiples applications et serveurs résident sur un seul serveur, une fois que le hacker a pénétré cette couche, il a accès à tout ce qui se trouve dans des dizaines voire des centaines de systèmes, d'applications et de bases de données. En outre, les contrôles habituellement placés autour de chaque application n'existent pas dans un environnement virtuel. Par conséquent, la capacité d'une organisation à déterminer qui a accédé aux différentes informations et à quel moment est sérieusement compromise. Résultat : des préoccupations parmi les auditeurs et le risque de générer des « faiblesses matérielles » dans le rapport de conformité d'une organisation.

Systèmes virtuels multiples



Pour tenter de résoudre les problèmes de sécurité liés à la virtualisation, il convient de créer de multiples zones de confiance en ayant recours à plusieurs systèmes virtuels, chacun d'eux ne virtualisant qu'un seul aspect de l'architecture. Des dispositifs physiques basés sur le matériel sont utilisés en tant que produits de sécurité réseau traditionnels pour protéger les systèmes. Cette approche augmente néanmoins aussi le matériel physique, ce qui peut nettement réduire le retour sur investissement (ROI) que la virtualisation aurait pu générer. Elle accroît également la complexité, les besoins en électricité et en refroidissement ainsi que d'autres facteurs, tel que l'encombrement du centre de données.

Les stratégies de segmentation classiques deviennent inefficaces.

La plupart des responsables informatiques sont conscients de l'importance de la segmentation, notamment ceux des entreprises cotées en bourse qui sont tenues de respecter les directives strictes de la loi Sarbanes-Oxley et d'autres exigences réglementaires.

Les meilleures pratiques en termes de conformité prônent une segmentation ou un « partitionnement » des fonctions clés de l'entreprise, comme les RH, la R&D et les salaires, au sein

de l'infrastructure informatique. Nombre d'organisations appliquent également des stratégies de segmentation en créant des zones de confiance pour se protéger des menaces internes et externes. Ces tactiques aident à éliminer le risque que des personnes non autorisées accèdent à des informations qui ne leur sont pas destinées.

Dans les environnements virtuels qui dépendent encore de solutions de sécurité héritées, la segmentation est plus complexe car elle oblige les responsables informatiques à installer de multiples serveurs physiques pour exécuter différents environnements virtuels – un pour chaque domaine, comme les RH, la R&D ou les salaires. Cette situation met en péril l'objectif numéro un de la virtualisation, à savoir réduire le matériel, les coûts et la complexité. Par ailleurs, la rentabilité de la mise en commun est compromise, l'espace sur le serveur reste problématique et les complexités du réseau créent un risque encore plus important en termes de sécurité et de disponibilité.

Les consoles de gestion classiques ne suffisent pas.

Si les systèmes de sécurité réseau basés sur le matériel ne peuvent résider entre les serveurs virtuels ou dans les applications virtuelles sur ces serveurs, les consoles de gestion, quant à elles, ne sont pas en mesure d'offrir une visibilité sur l'activité de l'environnement virtuel. Ainsi, les dispositifs de sécurité hérités placés en amont du système virtuel ne peuvent détecter le volume de trafic réseau transitant entre les systèmes virtuels. Ils ne peuvent avertir l'administrateur si le système physique est sur le point d'atteindre sa capacité maximale ou s'il doit être reconfiguré. Sans ces informations vitales, les responsables informatiques ont beaucoup de mal à déterminer si une attaque est en cours ou si la capacité maximale est atteinte. En conséquence, l'entreprise est davantage sujette à des pannes réseau.

Comment s'assurer qu'une solution de sécurité réseau est adaptée aux environnements virtuels

Au vu des difficultés décrites plus haut, nous pouvons conclure que les solutions de sécurité logicielles représentent la seule option pour protéger votre infrastructure informatique virtuelle ainsi que les avantages que vous espérez retirer de vos initiatives de virtualisation.

Stonesoft est une entreprise d'envergure mondiale qui, depuis près de 20 ans, aide les organisations à sécuriser leur flux d'informations grâce à des solutions de pointe en matière de sécurité réseau et de continuité de service. Depuis 2002, elle propose des solutions logicielles de sécurité qui ont fait leurs preuves dans des environnements virtuels. Avec les solutions StoneGate, les entreprises peuvent tirer pleinement profit des avantages offerts par la technologie de serveur virtuel tout en étant assurées que leurs réseaux restent sécurisés et disponibles.

Assurer la sécurité de l'environnement virtuel pour les MSP

La sécurité, la convivialité et la flexibilité sans précédent offertes par les solutions StoneGate peuvent aider à jeter les bases d'une consolidation des serveurs pour tout type d'organisation. Néanmoins, la virtualisation revêt un intérêt particulier pour les fournisseurs de services gérés (MSP) qui comptent des centaines de clients, de pare-feu en clusters et d'appliances IPS. Au lieu de devoir mettre en place des environnements avec des dizaines de serveurs, les MSP peuvent désormais gérer de multiples environnements utilisateur au moyen d'un seul ordinateur.

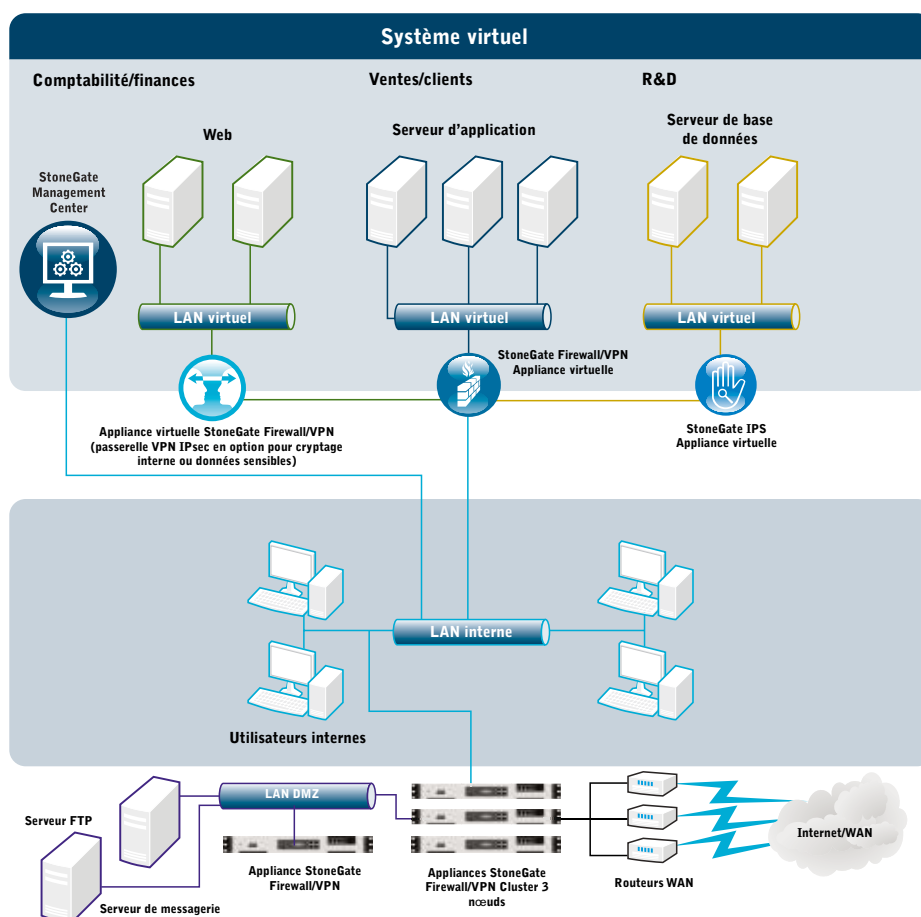
Pour savoir si votre solution actuelle est adaptée aux environnements virtuels, passez en revue les questions suivantes avec votre fournisseur de sécurité réseau :

1. Vos produits actuels peuvent-ils prendre en charge 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 ?

Les solutions StoneGate sont conçues de bout en bout pour être des systèmes logiciels sécurisés, 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.

La virtualisation avec StoneGate



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.

Exploitant les fonctionnalités VMware, les appliances virtuelles StoneGate sont extrêmement simples à mettre en œuvre.

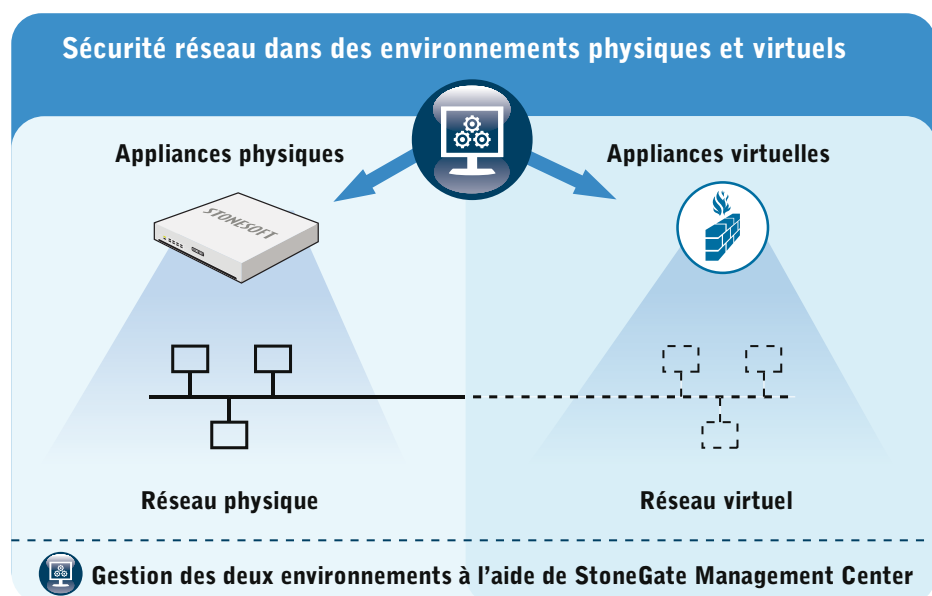
Étant donné que les solutions StoneGate Firewall/VPN, IPS et SSL VPN intègrent leur propre système d'exploitation sécurisé, il n'est pas nécessaire d'en installer un au préalable dans la machine virtuelle. Cette intégration du système d'exploitation ne simplifie pas seulement le processus d'installation. 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 logiciels, 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 service 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.

2. Votre produit est-il en mesure de surveiller avec précision les activités des environnements virtuel et physique à partir d'une seule console de gestion ?

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 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 uniques.

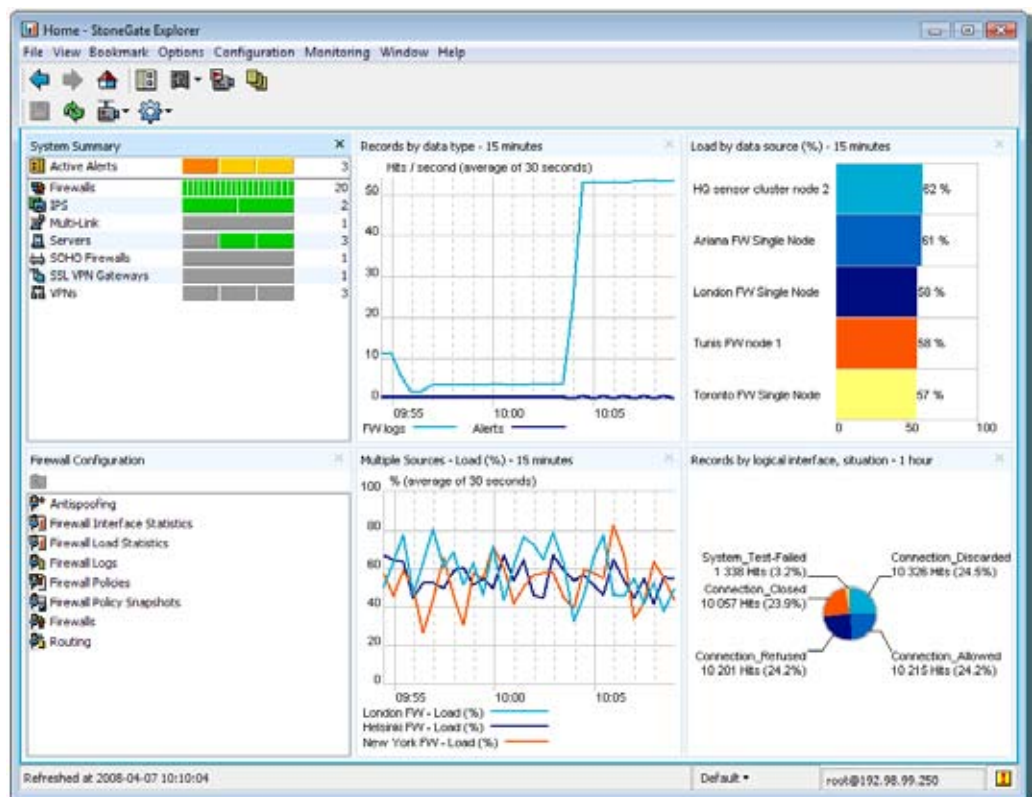
Solution de sécurité StoneGate pour environnements virtuels



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

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 puissantes 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.

StoneGate Management Center



Conclusion

La virtualisation étant en passe de se généraliser, 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. Pour ce faire, 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. Elle est idéalement positionnée pour accompagner des entreprises de toutes tailles dans la sécurisation de leurs infrastructures informatiques virtuelles.

À propos de Stonesoft

Stonesoft Corporation (OMX : SFT1V) est un fournisseur novateur 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 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'un système dont la gestion est centralisée dans des environnements physiques et virtuels. Les principaux avantages de la solution de connectivité sécurisée StoneGate se traduisent notamment par un coût total de possession faible, un excellent rapport prix/performance et un retour sur investissement élevé.

La solution SMC (StoneGate Management Center) permet une gestion centralisée 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, visitez notre site Web, www.stonesoft.com.

À propos de l'auteur

Architecte solutions senior chez Stonesoft Inc, Mark Boltz a effectué des présentations lors de conférences et de salons professionnels sur la sécurité des informations. Ainsi a-t-il notamment tenu des séminaires sur la virtualisation de la sécurité pour SHARE, dirigé des colloques sur les protocoles de routage dynamique pour SANS, présenté la gestion de la sécurité réseau pour RSA et exposé la sécurité de la voix sur IP lors de l'Internet Telephony Conference and Expo. Parmi ses contributions écrites, on peut citer des articles sur la sécurité des informations et la planification de la continuité de service pour l'International Legal Technical Association (ILTA) ainsi que sur la sécurité de la virtualisation pour CSO. Mark Boltz possède plus de 18 ans d'expérience dans le domaine des technologies de l'information, dont plus de dix ans consacrés spécifiquement à la sécurité de l'information. Instructeur StoneGate agréé (CSGI), il est également titulaire de la certification CISSP des experts en sécurité des systèmes d'information, de la certification CISA (certified information systems auditor) et de l'IEM de la NSA. Résidant dans le nord de la Virginie, il est membre de l'Information Systems Security Association (ISSA) chapitre Virginie du Nord, du programme Infragard du FBI, de la League of Professional Systems Administrators (LOPSA), de l'USENIX-SAGE, de l'IEEE Computer Society, du Computer Security Institute (CSI) et de l'ISACA.

STONESOFT

Stonesoft Corporation

Itälahdenkatu 22 A
00210 Helsinki
Finland
tel. +358 9 476 711
fax. +358 9 476 712 34

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338, USA
tel. +1 770 6681 125
fax. +1 770 6681 131

Copyright 2008 Stonesoft Corporation. Tous droits réservés.