

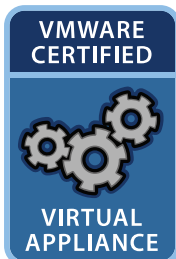


StoneGate™ Virtual IPS : Auditer les flux en profondeur dans les environnements VMware

L'IPS est devenu une fonctionnalité incontournable de sécurité pour détecter le trafic malveillant. Stonesoft a développé StoneGate Virtual IPS, un système de détection et d'analyse du trafic, qui permet d'organiser la réponse appropriée. L'unique moyen d'avoir une visibilité et une protection exhaustives des communications entre toutes les machines virtuelles.

La Virtual Appliance StoneGate IPS possède toutes les fonctionnalités d'une Appliance classique StoneGate IPS.

Il est désormais possible de filtrer les flux au sein d'une infrastructure virtuelle, mais également de faire du reporting sur l'ensemble de ceux transitant entre les machines virtuelles et de ceux sortant du serveur ESX.



L'outil de Management intégré (StoneGate Management Center = SMC), permet d'obtenir les niveaux de surveillance, d'analyse et de reporting nécessaires pour assurer la conformité des environnements virtuels. L'administrateur obtient une visibilité en temps réel sur l'ensemble des événements de communication entre les différents systèmes, sous forme de logs d'audit clairs et précis.

Des tableaux de bord en temps réel

Les consoles d'administration traditionnelles ne sont pas conçues pour visualiser les flux réseau entre les machines virtuelles ou alerter les administrateurs lors d'un problème de disponibilité ou de sécurité. Stonesoft à travers sa console de management unique permet d'unifier l'ensemble des politiques de sécurité et d'avoir un contrôle sur l'ensemble des flux au sein des environnements virtuels.



La SMC améliore l'audit des environnements virtuels grâce à son système pointu de gestion et de filtrage de logs, ses outils de surveillance avancée et ses rapports intégrés personnalisables. Il est donc possible pour les administrateurs d'identifier et d'isoler les trafics entre les machines virtuelles, en fonction de leur source, destination, protocoles, applications, heures, et beaucoup d'autres critères.

STONESOFT

Secure Information Flow





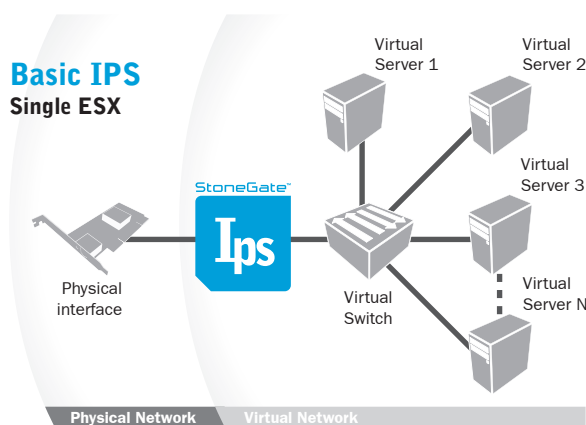
StoneGate Virtual IPS pour une sécurité en profondeur

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 et d'applications P2P sur le réseau.

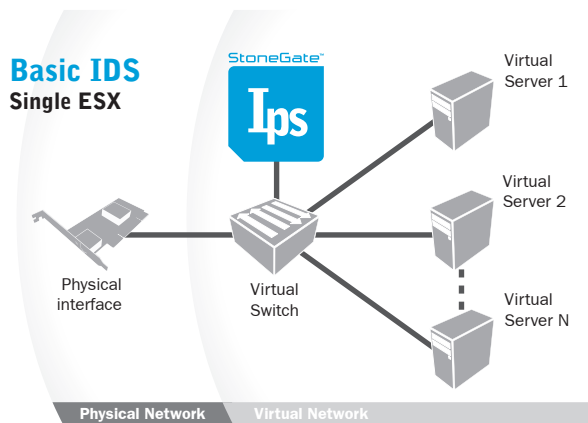
La technologie exclusive de StoneGate Virtual IPS permet une détection plus précise. Elle s'appuie sur des méthodes contextuelles multiples :

- Base de Signatures (expressions logiques personnalisables)
- Analyse protocolaire
- Détection d'anomalies protocolaires
- Identification protocolaire (ex : P2P sur http)
- Détection évoluée de scans de ports

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. Pour ce faire, il suffit de placer le StoneGate Virtual IPS en rupture devant des machines virtuelles.

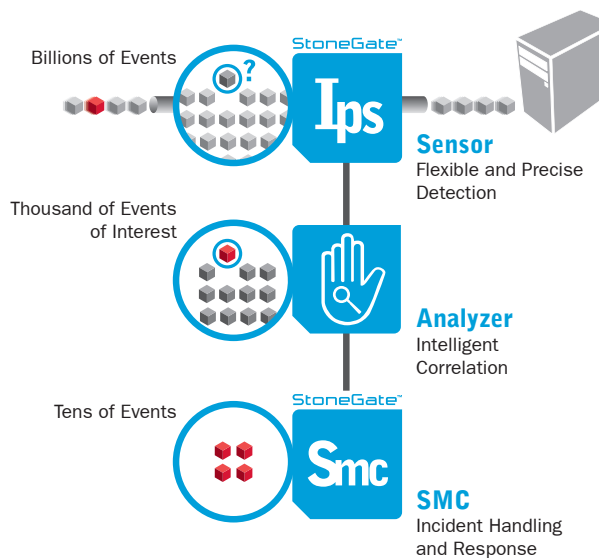


Le mode sonde permet l'analyse de l'ensemble du trafic sur un Switch virtuel grâce à la fonction de port miroir. Ce dernier peut également permettre de bloquer le trafic en déléguant cette fonction à un autre moteur Stonegate IPS et/ou FW.

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

- Protection des applications vulnérables contre les attaques réseaux sur les systèmes d'exploitation de type Windows et Linux / Unix...tant côté serveur que côté client
- Détection des logiciels espions, des attaques de types DoS (rate based DoS et non-rate based DoS), des scans de ports, des chevaux de Troie, des vers, des anomalies protocolaires et des transactions réseau.
- Intégration de 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.
- Intégration de milliers de signatures pour plus d'une centaine de protocoles - HTTP, DNS, IMAP, SMB, MSRPC, MYSQL, Oracle, POP3 et bien d'autres.
- Possibilité d'établir des signatures personnalisables basées sur la syntaxe des expressions régulières afin de garantir une meilleure protection contre les vulnérabilités.
- Mécanisme de corrélation d'événements intelligent pour réduire et gérer les faux positifs et faux négatifs.
- Possibilité, en mode coupure, de bloquer automatiquement et immédiatement des anomalies détectées, ou une potentielle violation d'une politique de sécurité.
- Fonction avancée de liste noire et de liste blanche en collaboration avec d'autres éléments StoneGate virtuelles et/ou physiques.
- Implémentation du mode coupure et/ou du mode sonde au sein de la même Virtual Appliance.



Cette offre est commercialisée sous la forme d'une redevance annuelle, ainsi elle apporte toute la flexibilité attendue dans ce type d'environnement (ouverture et fermeture du service à la demande) :

	Basic 8/5	Premium 24/7
StoneGate Virtual IPS	995 €	1 495 €
StoneGate Virtual FW	599 €	799 €

Le prix comprend le moteur IPS ou FW, la SMC ainsi que le support associé.

Stonesoft France SAS
38, Rue de Villiers
FR-92300 Levallois, France
tel. +33 (0)1 47 58 48 05 | fax. +33 (0)1 47 58 56 17
info.france@stonesoft.com

STONESOFT

Secure Information Flow

Stonesoft Corporation International Headquarters
Itälähdenkatu 22 A
FI-00210 Helsinki, Finland
tel. +358 9 4767 11 | fax. +358 9 4767 1234
www.stonesoft.com