Stonesoft Corporation

StoneGate Intrusion Prevention System

Appliance IPS-1205

IPS version 5.4

CIBLE DE SÉCURITÉ

VERSION 1.1

Stonesoft Corporation
Itälahdenkatu 22 A, FIN-0210 Helsinki, Finlande

SOMMAIRE

FIGURES

1 IDENTIFICATION DU PRODUIT A EVALUER

Organisation éditrice	StoneSoft
Lien vers l'organisation	http://www.stonesoft.com/fr/
Nom commercial du produit	StoneGate IPS Appliance
Numéro de la version évaluée	Appliance IPS-1205 embarquant la suite logicielle IPS StoneGate version 5.4
Catégorie de produit	IDS / IPS

2 ARGUMENTAIRE DU PRODUIT

2.1 DESCRIPTION GENERALE DU PRODUIT

Le produit **StoneGate IPS-1205** est une solution matérielle intégrée (de type *appliance*) de système de détection et de prévention d'intrusion réseau (NIDPS = Network Intrusion Détection and Prevention System) développée par la société StoneSoft. Il s'agit d'un produit commercial proposant une analyse de flux réseau, des remontées d'alertes et un blocage des tentatives d'intrusion détectées.

L'IPS dispose d'un système d'exploitation intégré correspondant à un Linux durci dont les packages non nécessaires ont été retirés. L'ensemble des logiciels de l'IPS est mis à jour lors de la montée en version de l'IPS.

L'IPS StoneGate propose les fonctionnalités suivantes :

- Des méthodes de détection d'intrusion :
    - Détection basée sur l'utilisation de signatures.
    - Détection d'anomalies basée sur des analyses statistiques des flux.
    - Détection des contournements de protocole.
    - Corrélation d'évènements.
- Des mécanismes de réponse faisant suite à la détection d'un trafic anormal tels que :
    - La remonté d'alertes.
    - L'enregistrement du trafic.
    - La terminaison de connexions TCP.
    - L'utilisation d'une liste noire pour bloquer des flux de certains réseaux. Cette liste noire correspond à une liste d'adresses IP bloquées temporairement et définie soit manuellement par l'administrateur, soit automatiquement par l'IPS.
    - Le blocage des flux par l'IPS positionné en coupure.

Un système StoneGate IPS se compose de (cf. Figure 1) :

- Une ou plusieurs appliance IPS.
- Un **système d'administration SMC** (StoneGate Management Center) pour la configuration de l'IPS comprenant les composants suivants :
    - Un **serveur de gestion** (Management Server) pour la configuration de l'IPS.
    - Un ou plusieurs **serveurs de journalisation** (Log Server) pour le stockage et la gestion des journaux.
    - Un ou plusieurs **clients du serveur de gestion** (Management Client) qui fournissent une interface graphique de configuration et de suivi de l'IPS.

Les connexions entre l'IPS et le serveur de gestion ou le serveur de journalisation sont protégées par un canal SSL/TLS avec authentification mutuelle et chiffrement.

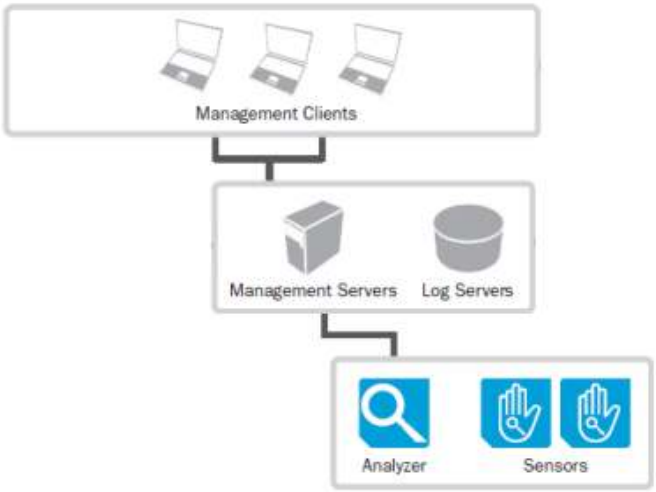

Figure 1 : Composants d'un système StoneGate IPS

Une appliance IPS peut être installée des deux façons suivantes :

- En mode IDS (Intrusion Dectection System) : Installation en mode capture pour une capture et analyse des flux sans coupure.
- En mode IPS (Intrusion Prevention System) : Installé en mode coupure pour une analyse et une coupure des flux.

2.2 MODE D'UTILISATION ET ENVIRONNEMENT DU PRODUIT

Le produit StoneGate IPS est connecté au réseau en mode coupure ou en mode capture en fonction de son mode d'installation.

Un IPS installé en mode IPS (configuration évaluée) se connecte au réseau en mode coupure à l'intérieur du réseau à protéger (cf. Figure 2).

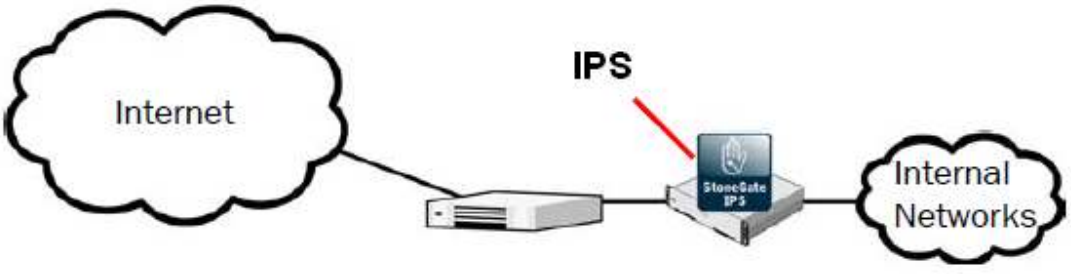

Figure 2 : Exemple de positionnement d'un IPS installé en mode IPS.

Un IPS positionné en mode capture doit être relié au réseau par un dispositif TAP ou un SWITCH SPAN possédant des propriétés de *mirroring* permettant la capture du réseau de manière transparente et robuste.

La configuration de l'IPS est réalisée au travers un système d'administration SMC (StoneGate Management Center) qui inclut un système client/serveur de gestion et un serveur de log. Le SMC s'installe sur une plate-forme de type Linux ou Windows sur une ou plusieurs machines.

2.3 UTILISATEURS TYPIQUES DU PRODUIT

Les utilisateurs du système d'IPS sont les suivants :

Un **administrateur** qui a en charge :

- L'installation du SMC.
- L'installation de l'IPS.
- La configuration et maintenance du SMC et de l'IPS.

Ces administrateurs disposent de droits d'accès privilégiés au système d'exploitation SMC (droit *root* pour Linux et droits *administrateur* sous Windows).

Un **exploitant** qui a en charge de :

- La mise à jour de la base de signatures.
- Le traitement des alertes.
    - L'audit des journaux.

Le SMC propose une gestion des rôles afin de restreindre les droits de certains administrateurs. Un compte administrateur avec pleins pouvoirs est automatiquement créé lors de l'installation du SMC. Ce compte permet la création d'autres comptes d'exploitants ayant moins de droits que l'administrateur principal.

2.1 HYPOTHESES SUR L'ENVIRONNEMENT

Plate-forme sécurisée

Le SMC est installé sur un système d'exploitation correctement administré et configuré (mises à jour périodiques, désactivation des services et partages non utilisés, contrôle d'accès restreint aux seuls utilisateurs autorisés).

Locaux

L'*appliance* IPS et les équipements contenant le SMC doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

Administrateurs

Les administrateurs de l'IPS et du SMC sont des personnes considérées comme non hostiles. Ils sont formés pour administrer et configurer les produits. Ils suivent les manuels et procédures d'administration.

Audit

L’administrateur consulte régulièrement les données de journalisation et traite les alarmes de sécurité générées par l’IPS StoneGate.

3 BIENS SENSIBLES QUE LE PRODUIT DOIT PROTEGER

Le produit contribue à protéger les biens sensibles énumérés ci-dessous.

Biens des utilisateurs du réseau protégé

Les données et services des utilisateurs du réseau protégé.

Données de configuration de l'IPS

Les fichiers de configuration de l'IPS incluant la liste noire.

La base de signatures

Une méthode de détection d'intrusion de l'IPS est basée sur l'utilisation d'une base de signatures qui est mise à jour périodiquement.

Les journaux d'audit et d'alertes

Des journaux d'alertes sont remontés par l'IPS afin d'être traités par un administrateur. En outre, une journalisation des opérations réalisées sur le produit telles que la modification de la configuration, l'authentification des utilisateurs est mise en place.

Les informations sur l'état d'une appliance IPS

Le serveur de gestion récupère automatiquement les traces des composants IPS. Un système de monitoring est proposé par le SMC.

4 MENACES SUPPOSEES DE L'ENVIRONNEMENT

Les attaquants potentiels sont des attaquants externes (des personnes extérieures au réseau protégé).

Pour rappel, les hypothèses considèrent que les administrateurs ne sont pas des attaquants potentiels.

Les attaques peuvent être menées à partir de l'externe ou de l'interne (si une machine interne a été compromise par un attaquant externe).

Les menaces portant sur l'IPS sont les suivantes :

Attaque par contournement du système de reconnaissance des signatures
Un attaquant peut exploiter une faille dans le processus de mise à jour de la base de signatures lorsque cette opération n'est pas régulière (données de signature obsolètes) ou réalisée à partir de données de signature de mauvaise qualité (ne répertoriant pas toutes les signatures publiques).

Attaque protocolaire
Un attaquant peut tenter de contourner l'IPS par une attaque protocolaire. Ce type d'attaque peut exploiter des biais ou des absences d'implémentation du système de contrôle protocolaire de l'IPS.

Attaque par déni de service
Un attaquant peut inonder l'IPS en émettant une quantité de données suffisamment importante (ex : multiples demandes de connexion) pour le rendre inactif le temps de mener une intrusion perspicace. Il est également envisageable d'exploiter une faille dans l'implémentation de l'IPS afin de générer un débordement de tampon. Un autre type d'attaque consiste à générer de nombreuses simulations d'intrusion afin de provoquer une émission de nombreux faux-positifs (ex : multiples scans réseau).

5 FONCTIONS DE SECURITE DU PRODUIT

Mise à jour de la base de signatures

Le SMC propose une fonctionnalité de mise à jour de la base de signatures. Pour ce faire, le serveur de gestion se connecte périodiquement au site Web de Stonesoft afin de vérifier si une nouvelle base de signature est disponible. La mise à jour peut être automatisée ou manuelle suite à une remonté d'alerte. Cette fonction de sécurité est renforcée par une fonctionnalité de restauration automatique du système dans sa configuration précédente qui peut être activée lors d'une opération de mise à jour du système. Ce processus permet d'éviter qu'un IPS dispose d'une base de signature incomplète ou non fonctionnelle en cas d'échec de la mise à jour.

La société StoneSoft met régulièrement à jour la base de signature sur leur site internet.

Détection des intrusions

La détection des intrusions consiste en la capture des flux réseau, le décodage des protocoles et la comparaison du trafic basée sur les signatures.

Corrélation d'évènements

Une fonction de corrélation propose les fonctionnalités suivantes :

- « Compress » : Rassemble des évènements du même type dans un log (ex : accès à des fichiers serveur).
- « Count » : Comptabilise le nombre de connexions récurrentes sur une période donnée.
- « Group » : Regroupe des suites d'évènements similaires. Ceci permet par exemple de détecter l'attaque d'un logiciel par la mise en œuvre des vulnérabilités publiques.
- « Match » : Offre la possibilité d'utiliser des filtres sur des situations spécifiques.
- « Sequence » : Vérifie l'utilisation de suites de messages reconnus comme valides (une demande d'ouverture de fichier suivie d'un accès au fichier).

Liste noire

Une liste noire permet de bloquer, pour une durée définie, les flux provenant d'adresses IP suspectées d'intrusion.

Blocage des intrusions

Une fonctionnalité de blocage des intrusions est implémentée par l'IPS.

Gestion des alertes et des journaux

Lorsque certains évènements ne peuvent pas être bloqués faute de garantie sur la véracité de l'attaque, des alertes pertinentes et de qualité sont remontées par l'IPS. En outre, une journalisation permet de conserver les évènements remontés par l'IDS.

6 PERIMETRE DE L'EVALUATION

Le périmètre d'évaluation comprend **l'IPS StoneGate Intrusion Prevention System installé en mode IPS**.

L'IPS peut être installé sur les plates-formes suivantes :

- Appliance StoneGate,
- Serveur Intel,
- Serveur VMware ESX.

L'appliance IPS StoneGate est retenue pour cette évaluation.

La liste noire n'est pas activée par défaut.

L'utilisation de la liste noire est incluse dans le périmètre de l'évaluation.

L'IPS peut être positionné en mode coupure ou écoute selon son utilité (IDS ou IPS).

Un positionnement de l'IPS en mode coupure est retenu pour cette évaluation.