

Riverbed Stingray Application Firewall



riverbed[®]

Think fast.[®]

Présentation

Les attaques contre les applications Web gagnent en sophistication et l'automatisation les rend de plus en plus courantes. Ces attaques s'appuient en général sur la découverte et l'exploitation de faiblesses, non au niveau du réseau mais au niveau du code applicatif et de l'infrastructure elle-même. Cependant, leur cible demeure toujours la même : l'information confidentielle. Stingray Application Firewall est un pare-feu applicatif Web sophistiqué garantissant une sécurité renforcée des applications. Vous pouvez désormais vous protéger efficacement contre les attaques connues ou inconnues de la couche applicative (Top 10 de l'OWASP, par exemple), sécuriser vos applications et assurer en toute confiance la conformité réglementaire de votre entreprise.

Stingray Application Firewall

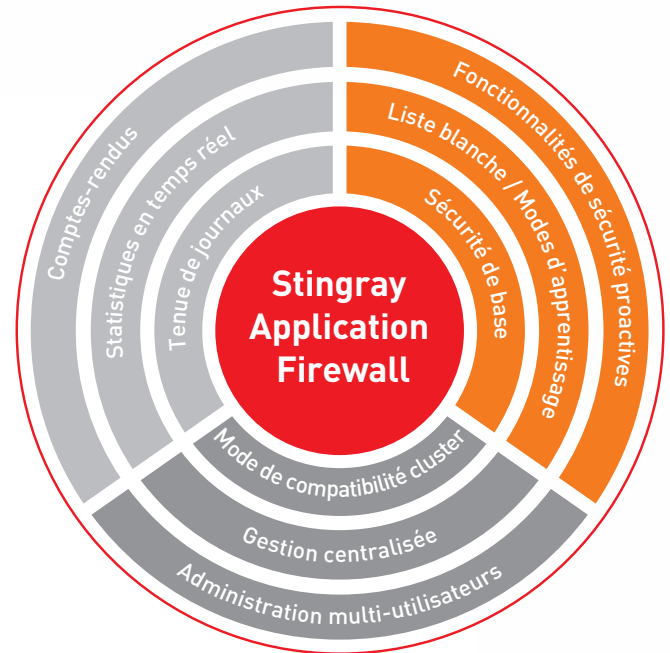
La présence d'une forte couche de sécurité est un composant indispensable à toute application Web complexe ayant à traiter des données sensibles. Quel que soit le soin avec lequel le code applicatif a été développé et maintenu, il demeure très difficile de garantir l'absence totale de vulnérabilités au sein de l'application et de l'infrastructure qui l'héberge. Stingray Application Firewall ajoute une couche supplémentaire de protection afin de renforcer la sécurité de votre application :

Détection et suppression des vulnérabilités applicatives courantes — De nombreux processus d'attaque cherchent à découvrir des faiblesses courantes comme les données d'entrée non contrôlées, les configurations applicatives non sécurisées ou les mécanismes d'authentification fragiles. Une fois ces faiblesses découvertes, le pirate informatique n'a plus qu'à lancer une combinaison d'attaques (injection SQL, cross-site scripting, vol de session,...). Stingray Application Firewall contient un ensemble complet de signatures de base et d'outils d'identification permettant de détecter et de bloquer ces requêtes exploratoires.

Sécurisation proactive de votre application — Stingray Application Firewall entoure l'application d'un fort périmètre de sécurité qui établit un identificateur de session sécurisé, chiffre proactivement les cookies et les URL et applique les règles d'utilisation du site afin de s'assurer que les utilisateurs suivent bien les trajets appropriés au sein de l'application et n'exploitent pas la nature apatride des transactions HTTP.

Définition de stratégies de sécurité sophistiquées — Chaque application est unique. C'est pourquoi Stingray Application Firewall détecte et apprend les schémas d'utilisation applicatifs les plus courants. Les suggestions de règles peuvent être inspectées par le responsable de la sécurité, puis testées en arrière-plan avant d'être déployées en production pour contrôler le comportement des utilisateurs. Des listes blanches et des listes noires simplifient et accélèrent l'application des règles de sécurité afin d'améliorer les performances et de réduire la complexité.

Suivi et compte-rendu — Aucun système de sécurité ne peut être déployé et géré en totale confiance s'il ne dispose pas d'une fonctionnalité complète de suivi et de tenue de journaux. Stingray Application Firewall propose de nombreux comptes-rendus répondant à divers besoins, depuis les alertes en temps réel jusqu'aux comptes-rendus hebdomadaires ou mensuels, afin de signaler les tendances d'attaque et de permettre le suivi des comportements applicatifs.



Stingray Application Firewall est une solution logicielle complète et évolutive permettant de renforcer la sécurité applicative et de contrôler le comportement des utilisateurs.

Conformité à la norme PCI DSS

La norme PCI DSS est un standard essentiel auquel toute entreprise acceptant des informations relatives aux cartes de paiement doit se conformer. L'incapacité à répondre aux exigences de cette norme expose les commerçants aux fraudes, aux coûts associés au détournement des données des titulaires des cartes et à l'augmentation des frais exigés par les fournisseurs de cartes de crédit.

La norme PCI DSS définit un ensemble pragmatique de procédures de sécurité que le commerçant doit respecter. Le volet 6.6 de la norme stipule qu'un commerçant doit soit effectuer des revues de sécurité régulières de la source de chaque application destinée au public, soit déployer et configurer un pare-feu applicatif Web approprié.

Stingray Application Firewall vous aide à respecter les obligations de ce volet 6.6, ainsi que celles d'autres volets de la norme PCI DSS. Stingray Application Firewall se configure facilement pour intégrer des stratégies de sécurité supplémentaires destinées à détecter et prévenir les attaques spécifiques à chaque application.

Utilisation de Stingray Application Firewall

Mode de base et mode expert

La configuration de Stingray Application Firewall s'effectue à l'aide d'une interface Web partagée. Les administrateurs peuvent choisir entre un mode de base très simple destiné à la création de configurations générales et un mode expert bien plus puissant.

Dans le mode de base, les administrateurs sont aidés dans leur tâche de configuration par des assistants et des algorithmes d'apprentissage intelligents. Quelques saisies élémentaires suffisent à configurer une stratégie de sécurité étendue qui définit les règles de base et les programmes avancés appropriés. Le mode expert simplifie la personnalisation des paramètres de chaque programme, avec le niveau de détail nécessaire. Stingray Application Firewall peut proposer automatiquement des règles en fonction du trafic réel, et les stratégies de sécurité individuelles peuvent être ajustées de façon itérative au gré des besoins.

Jeux de règles actif et d'arrière-plan

Stingray Application Firewall peut exécuter simultanément deux jeux de règles distincts. Le jeu de règle actif concerne tout le trafic et les décisions de bloquer ou de rerouter le trafic sont effectivement appliquées. Simultanément, un second jeu de règles peut être appliqué en mode arrière-plan. Il s'applique lui aussi à l'ensemble du trafic, mais les décisions ne sont qu'enregistrées dans un journal. Les jeux de règles actif et d'arrière-plan permettent de modifier plus facilement une stratégie de sécurité existante en testant de manière théorique l'effet des modifications sans compromettre la sécurité de l'application. Ils constituent un outil efficace de validation des règles suggérées ou des mises à jour avant leur introduction en environnement de production.

Exécution des stratégies de sécurité

Lors de l'exécution, Stingray Application Firewall reçoit et analyse chaque requête avant qu'elle ne soit traitée par l'application Web.

Chaque requête est alors affectée à l'une des trois classes suivantes :

- Les requêtes légitimes sont transmises à l'application Web.
- Les attaques définitivement identifiées sont repoussées lorsque la protection est activée et, dans le même temps, le plus de données possible est sauvegardé afin d'identifier et de suivre à la trace l'attaquant.
- Les requêtes dont le danger ne peut être définitivement évalué au niveau local peuvent être soit rejetées, soit transmises, selon la stratégie de sécurité installée et les règles locales adoptées. Ces requêtes sont également sauvegardées dans un journal interne et servent par la suite à classer les requêtes suivantes.

Pour le trafic de retour, Stingray Application Firewall analyse également les réponses de vos applications Web. Les informations liées à la sécurité (numéros de cartes de crédit, par exemple) peuvent ainsi être extraites des réponses et ne s'échappent pas même lorsque l'attaque est réussie. En analysant votre application Web dans la durée, Stingray Application Firewall réunit peu à peu des informations essentielles sur son comportement et les utilise pour vous apporter des conseils permettant d'optimiser encore sa protection.

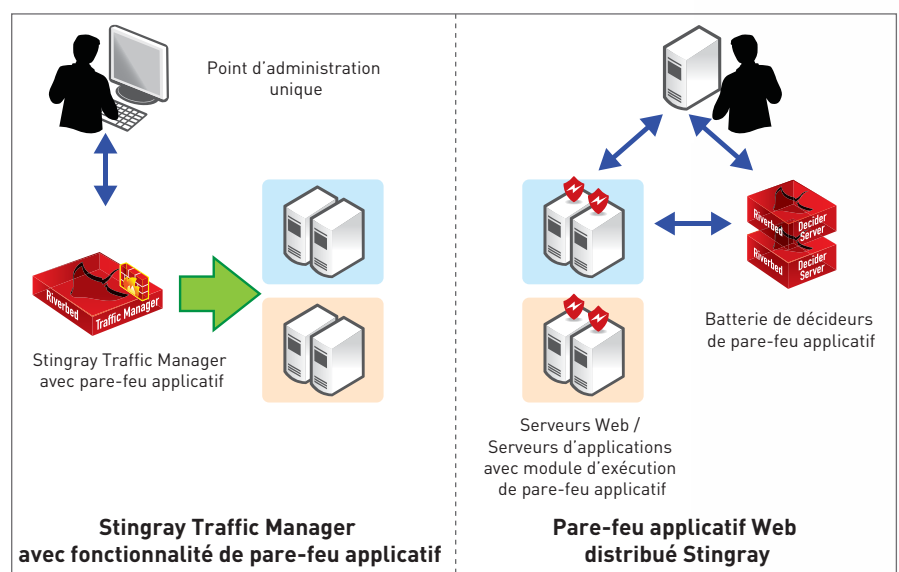
Journaux, statistiques et comptes-rendus

L'enregistrement et l'analyse de l'activité des utilisateurs et des profils d'attaque garantissent le fonctionnement optimal de Stingray Application Firewall et aident à ajuster au mieux les jeux de règles afin d'éliminer de nouveaux comportements d'utilisateur suspects et de limiter les faux positifs. La tenue de journaux, et plus particulièrement l'émission automatique hebdomadaire et mensuelle de comptes-rendus, contribuent à faciliter la conformité aux différentes réglementations afférentes à la conservation d'archives.

Pare-feu applicatif Web autonome ou composant facultatif de Stingray Traffic Manager

Stingray Application Firewall est proposé sous la forme d'un composant de Stingray Traffic Manager, comprenant un contrôleur de mise à disposition d'applications (ADC) totalement intégré et un système de pare-feu applicatif Web.

Stingray Application Firewall est également proposé sous la forme d'une architecture clusterisée d'une évolutivité inégalée. Les stratégies de sécurité sont gérées par un serveur d'administration et poussées vers une batterie de processus de décision. Les modules d'exécution sur les serveurs Web et d'applications capturent le trafic de façon bidirectionnelle et le dirigent pour validation vers les décideurs disponibles. Les composants de décision et d'exécution peuvent évoluer au gré des besoins pour répondre aux exigences du trafic.



Principales fonctionnalités et avantages

Stingray Application Firewall est une solution de sécurité puissante associant :

- Un mode de base et un mode expert pour une configuration et un paramétrage rapides
- L'exécution simultanée de jeux de règles d'exécution (actif) et de contrôle (arrière-plan)
- Une protection de base automatique, renforcée par des paramètres personnalisés très détaillés
- Une protection proactive comprenant la gestion de session sécurisée, la protection des cookie, le chiffrement des URL et la protection des champs de formulaire
- Des mises à jour régulières des jeux de règles de protection de base pour les vulnérabilités les plus courantes
- Des suggestions automatiques de jeux de règles basées sur des algorithmes d'apprentissage intelligents
- L'inspection HTTP bidirectionnelle et l'analyse complète des requêtes et des réponses
- La configuration automatique de la protection de Microsoft Outlook Web Access
- Un tableau de bord permettant d'afficher une présentation centralisée et en temps réel de l'état de sécurité de chaque application
- Des statistiques complètes et des fichiers journaux détaillés, gérés au sein du cluster
- Des alarmes configurables (email, HTTP POST, fichier journal) s'activant lorsque des événements définis surviennent
- Des fonctions d'exportation et d'importation pour la migration des règles d'un environnement de test à un environnement de production
- La gestion basée sur les rôles de multiples applications Web
- L'enregistrement complet de toutes les modifications de configuration et de jeu de règles
- Des comptes-rendus PDF de l'activité de service et des alertes de sécurité

A propos de Riverbed

Riverbed garantit la performance aux entreprises connectées du monde entier et facilite l'implémentation d'initiatives stratégiques telles que la virtualisation, la consolidation d'infrastructure, le cloud computing ou les récupérations après sinistres sans craindre de compromettre leurs performances. En fournissant aux entreprises la plate-forme dont elles ont besoin pour comprendre, optimiser et consolider leurs infrastructures, Riverbed aide les entreprises à construire une architecture informatique dynamique, fluide et rapide en accord avec leurs besoins. Pour plus d'informations sur Riverbed (NASDAQ : RVBD), rendez-vous sur www.riverbed.com.



2005, 2006, 2007, 2008, 2009, 2011



Riverbed Technology France	Riverbed Technology, Inc.
4, Place de la Défense	199, Fremont Street
Paris La Défense	San Francisco, CA 94105
France	USA
Tel.: +33 1 58 58 00 58	Tel.: +1 415 247 8800
www.riverbed.fr	www.riverbed.com

Riverbed Technology Italia	Riverbed Technology España
Via Venezia, 23	Paseo de la Castellana, 135-7pt
20099 Sesto San Giovanni (MI)	28046 Madrid
Italia	España
Tel.: +39 02 2412 6851	Tel.: +34 91 297 5479
www.riverbed.it	www.riverbed.es

© 2011 Riverbed Technology. Tous droits réservés. Riverbed et tous les produits, noms ou logo Riverbed utilisés ci-dessus sont des marques déposées de Riverbed Technology, Inc. Toutes les autres marques déposées utilisées ci-dessus appartiennent à leurs propriétaires respectifs. L'utilisation des noms et logos figurant dans le présent document est soumise à l'accord écrit préalable de Riverbed Technology ou de leurs propriétaires respectifs.