

SecureSphere®

Pare-feu pour applications Web

Le seul pare-feu (firewall) automatisé de l'industrie pour les applications Web

Vos applications Web sont-elles sécurisées ?

Les applications Web sont la cible privilégiée des cyber-attaques ; 92% des entreprises ont subi une attaque réussie sur leurs applications Web au cours des douze derniers mois, selon une étude du FBI de 2006. Ces attaques peuvent causer des dégâts considérables, des destructions de données hautement sensibles avec des impacts négatifs sur la marque, des procès et des amendes.

Les administrateurs responsables de la sécurité et les régulateurs en ont tenu compte. Puisque les produits de sécurité traditionnels ne font pas cesser les attaques sur les applications Web, de nouvelles obligations de réglementations régissent la protection des couches applicatives. Le respect des règles de sécurité et des exigences de conformité d'aujourd'hui peut s'avérer un défi redoutable pour de nombreuses entreprises.

Protégez vos applications et votre activité avec Imperva

Le pare-feu pour applications Web SecureSphere® d'Imperva protège vos applications Web et données sensibles. De plus, il offre un déploiement intégré, automatisé, une sécurité adaptable et de faibles coûts de gestion. SecureSphere apporte à votre entreprise une solution de sécurité pratique et l'assurance qu'elle répond aux défis modernes associés à la conformité et la sécurité des données transactionnelles.

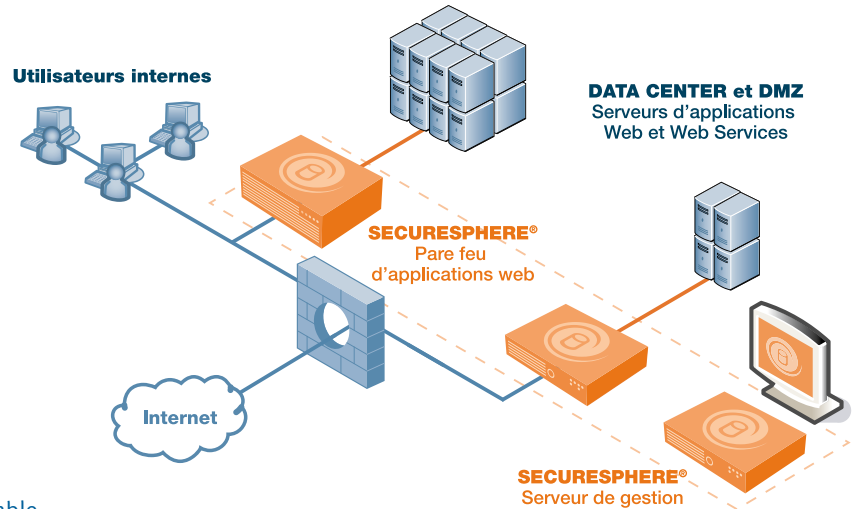


Sécurité automatisée des applications Web

Le pare-feu pour applications Web SecureSphere® a transformé la manière dont les entreprises protègent leurs applications et données sensibles en automatisant la protection contre les cyber-attaques. La technologie du profilage dynamique (Dynamic Profiling) d'Imperva construit automatiquement un modèle de comportement légitime et s'adapte aux changements applicatifs au cours du temps, en conservant la défense des applications de SecureSphere à jour et précise, sans configuration ou réglage manuels.

Déployé en quelques minutes, sans modifications de l'infrastructure existante, SecureSphere protège l'ensemble des programmes applicatifs, depuis l'application individuelle jusqu'aux serveurs et au réseau. La technologie d'Inspection Transparente d'Imperva offre une performance multi-gigabits, une latence inférieure à la milliseconde et des options pour une haute disponibilité répondant aux besoins les plus pointus des centres de données. Pour des déploiements à grande échelle, le serveur d'administration SecureSphere MX centralise et standardise la configuration, le contrôle et le reporting.

ARCHITECTURE DE RÉSEAU SECURESPHERE®



Protection complète contre les attaques

Le pare-feu applicatif Web SecureSphere tire parti des défenses multiples de sécurité pour fournir le niveau de protection le plus élevé. Ces défenses comprennent le Profilage Dynamique, la validation du protocole HTTP, la sécurité de la plate-forme, et la validation corrélée des attaques.

Apprentissage automatisé de l'application – Profilage Dynamique d'Imperva

La technologie unique du Profilage Dynamique de SecureSphere assimile automatiquement la structure, les éléments, et les modèles d'utilisation attendus des applications Web protégées. Le Profilage Dynamique détecte automatiquement et intègre les changements applicatifs valides dans le profil de l'application au cours du temps. En comparant les requêtes

énorme qui peut contenir des centaines ou même des milliers d'URL, de champs de formulaires, de paramètres et de cookies. Le Profilage Dynamique construit automatiquement un profil précis qui ne nécessite pas de configuration ni de réglage manuels.

Mise à jour de la sécurité avec ADC Imperva

Le Centre de Défense des Applications Imperva (Application Defense Center : ADC), une organisation internationale reconnue de recherche en matière de sécurité, met en œuvre de façon continue l'étude de nouvelles vulnérabilités rapportées autour du monde, analyse les exploits à partir d'une diversité de sites Web réels, et conduit des recherches de vulnérabilité primaire afin d'identifier les toutes dernières menaces.

Les résultats de cette recherche sont la mise à jour des défenses sur des couches différentes à l'intérieur de SecureSphere, y compris les mises à jour de signatures, les politiques de validation de protocoles, et les règles de corrélation.

En plus de la mise à jour des défenses, ADC offre des services optionnels ADC Insight Services. ADC Insights permet la connaissance approfondie des applications, propose des rapports de conformité préétablis et de bonnes pratiques tirées des experts de la sécurité et de la conformité.

Validation du protocole HTTP

La validation du protocole HTTP empêche une myriade d'abus de protocole, dont l'excès de mémoire

tampon, l'encodage malicieux, la fraude HTTP et les opérations de serveurs illégaux. La souplesse des politiques facilite l'adhésion stricte aux standards RFC ou permet des variations mineures dans le cadre d'applications spécifiques.

Protection plate-forme et réseau contre les attaques

SecureSphere bloque les attaques qui visent les vulnérabilités connues du serveur Web, de la plate-forme et du logiciel d'infrastructure. Plus de 4 000 signatures de sources telles que Bugtraq, CVE®, Snort® ainsi que l'ADC Imperva permettent une protection complète contre de telles attaques. En plus des vers connus, SecureSphere identifie de nouveaux vers zero-day, en détectant la combinaison unique d'attributs qui caractérise les attaques de vers.

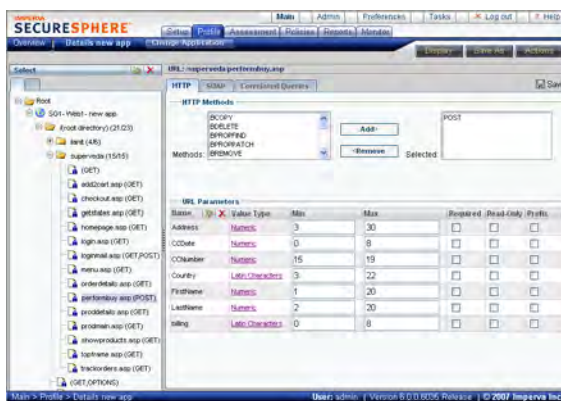
Le pare-feu réseau intégré et dynamique de SecureSphere protège contre les utilisateurs et protocoles non autorisés, et les attaques de réseau depuis des origines à la fois internes et externes. Il respecte les obligations et règles de l'art en matière de sécurité afin d'empêcher les protocoles non essentiels d'atteindre les applications Web sensibles.

Protection des Web services

Tirant parti de la technologie du Profilage Dynamique, SecureSphere établit le profil du comportement légitime des Web services, comprenant les fichiers XML, éléments, attributs, schémas, variables, et actions SOAP. Toute tentative d'intrusion et de malveillance à l'encontre d'un comportement normal des Web services est identifiée et bloquée.

Précision incomparable

La technologie unique de validation corrélée des attaques d'Imperva (Correlated Attack Validation) met en corrélation les violations au-travers des couches de sécurité et au cours du temps pour identifier précisément les attaques les plus complexes. Des violations individuelles peuvent ne pas définitivement indiquer une attaque, mais en corrélant leurs combinaisons uniques, les attaques sont validées au-delà du doute. Il n'existe pas d'autre solution aussi précise que celle de la validation corrélée des attaques.



Le Profilage Dynamique permet de connaître automatiquement les URL, champs de formulaires, paramètres, cookies, et entrées attendues de l'utilisateur.

Web avec le profil, SecureSphere peut détecter un comportement inacceptable et empêcher une activité malicieuse avec une extrême précision.

Le Profilage Dynamique élimine le plus grand inconvénient associé à un modèle de sécurité positive : le besoin de créer manuellement - et mettre à jour - une liste blanche (white list)

Déploiement transparent

Pas de modification de l'application ou du réseau

La technologie d'inspection transparente permet le déploiement du pare-feu SecureSphere dans n'importe quel environnement sans modification des applications existantes, des serveurs ou du réseau. SecureSphere permet une sécurité des applications précise et complète sans obliger les organisations à reconcevoir leurs applications Web, changer les spécifications IP ou DNS ou mettre à jour les procédés d'authentification.

L'inspection transparente basée sur le noyau découple la sécurité du mode de déploiement, de sorte que SecureSphere peut supporter les modes opératoires suivants :

- **Passerelle Couche Transparente 2 – pour un déploiement intégré et la meilleure performance de l'industrie**
- **Routeur – pour une segmentation de réseau, le routage et la traduction d'adresse réseau**
- **Reverse Proxy – pour la modification de contenu, telle que la signature de cookie et la réécriture d'URL**
- **Proxy transparent – pour un déploiement rapide de modification de contenu sans modification de réseau**
- **Moniteur non-en ligne – pour un contrôle et évaluation sans risques**

Performance en gigabits

SecureSphere permet une production en multi-gigabits, et des dizaines de milliers de transactions par seconde en maintenant une latence inférieure à la milliseconde. Ce niveau de performance est inégalé et de bien meilleure qualité que les approches de la concurrence. Il garantit complètement un déploiement transparent. Avec SecureSphere, la sécurité n'impactera jamais les accords de niveau de service du centre de données ou la performance des applications.

Haute Disponibilité

SecureSphere supporte une large gamme d'options de haute disponibilité, permettant le déploiement au sein de certains des plus grands réseaux du monde. Les options de disponibilité comprennent :

- **Haute Disponibilité Imperva (IMPVHA) pour une reprise inférieure à la seconde**
- **Protocole de redondance de routeur virtuel (VRRP) pour des déploiements de routeur ou proxy**
- **Redondance passive-active et active-active pour des mécanismes de disponibilité externes**
- **Interfaces en « Fail-open » pour une disponibilité de simple-passerelle**
- **Déploiement non-en ligne – pour un contrôle et évaluation sans impact sur la production**

Opérations

Maintenance de politique automatisée

La mise en œuvre d'un modèle de sécurité en "white list" requiert traditionnellement un réglage manuel constant. La "white list" du pare-feu nécessite une mise à jour toutes les fois que l'application Web a changé. Le Profilage Dynamique élimine le réglage manuel en modélisant automatiquement les applications Web et en les adaptant aux changements applicatifs. Les administrateurs de SecureSphere ont pleinement accès pour modifier les profils d'application et créer des politiques sur mesure.

Gestion centralisée

SecureSphere peut être déployé comme dispositif autonome ou adapté pour protéger des centres de données distribués. Pour les environnements plus importants, y compris les déploiements mixtes de bases de données et applications Web, le serveur de gestion MX de SecureSphere offre une configuration, un contrôle et un reporting centralisés. La gestion des environnements ASP et de grandes entreprises est standardisée par des regroupements organisationnels hiérarchiques, des droits d'accès granulaires, et un processus de workflow unique orienté tâches d'administrations.

Reporting de qualité entreprise

SecureSphere offre des capacités de reporting graphiques riches, permettant aux utilisateurs de comprendre facilement le statut de la sécurité et répondre aux exigences de conformité réglementaires. SecureSphere offre des rapports pour le Web prédéfinis et personnalisables à volonté. Les rapports peuvent être visualisés à la demande ou envoyés par e-mail sur une base quotidienne, hebdomadaire ou mensuelle. La plate-forme de reporting de SecureSphere fournit une visibilité instantanée des problèmes de sécurité, conformité et livraison de contenu.

Contrôle et alertes

Un tableau de bord en temps réel permet de visualiser avec un haut niveau de qualité le statut du système et les événements liés à la sécurité. Les alertes sont facilement recherchées, triées, et directement reliées aux règles de sécurité correspondantes. Pour une intégration souple avec les produits de gestion d'événements de sécurité, SecureSphere supporte syslog, SNMP, et les accès directs en ODBC.

Protection automatisée et précise contre :

- Vulnérabilités Web, HTTPS (SSL) et XML
- Injection de commande SQL
- Session Piratage
- Cross-site scripting (XSS)
- Falsification de champ de formulaire
- Vers connus
- Vers Web "zero day"
- Excès de mémoire tampon
- Infection par cookie
- Refus de service
- Robots malicieux
- Falsification de paramètres
- Login forcé
- Encodage malicieux
- Parcours de répertoire
- Serveur Web et attaques de plateformes
- Reconnaissance de site
- Injection de commande OS
- Falsification de requête (CSRF)
- Piratage Google
- Attaques par inclusion de fichier distant
- Encodage illégal
- Dévoilement de carte de crédit
- Dévoilement des données de patients
- Espionnage d'entreprise
- Phishing
- Destruction de données

Pistage de l'utilisateur de l'application

La technologie de Profilage Dynamique de SecureSphere capture automatiquement les noms des utilisateurs des applications Web et associe toutes les sessions d'activités à la suite avec ce nom d'utilisateur spécifique. Ainsi, SecureSphere peut contrôler, appliquer et auditer une politique uniquement sur une base par utilisateur.

Protection optionnelle de bases de données

Le pare-feu pour applications Web SecureSphere peut être étendu au contrôle et à la protection des bases de données Oracle, MS-SQL, DB2, Sybase, et Informix. La passerelle de sécurité de bases de données SecureSphere empêche les attaques externes et abus internes en assurant une sécurité de bout en bout du centre de données. De plus, elle tire parti du pistage de l'utilisateur de l'application SecureSphere pour tracer les requêtes SQL individuelles vers l'utilisateur Web. Cette capacité de Pistage universel de l'utilisateur permet une visibilité incomparable des requêtes, modifications et violations de base de données.



Tableau de bord en temps réel SecureSphere

Caractéristiques et spécifications du dispositif SecureSphere

Sécurité Web	Profil Dynamique (sécurité de White List), signatures du serveur Web & des applications, conformité HTTP RFC, normalisation des données encodées
Inspection HTTPS/SSL	Décryptage passif ou suppression ; support optionnel HSM pour le stockage des clés SSL
Sécurité des Web Services	Application du profil XML/SOAP, signatures des Web services, conformité du protocole XML
Modification de contenu	Ré-écriture d'URL (obscurcissement), signature de cookie
Sécurité de plateforme / Ver	Sécurité contre les vers connus et vers zéro day / signatures d'intrusion dans le système d'exploitation
Sécurité réseau	Pare-feu dynamique, prévention DoS
Protection avancée	Les règles de corrélation sur mesure et prédéfinies intègrent tous les éléments de sécurité afin de détecter les attaques complexes, multi-niveaux.
Prévention des fuites de données	Numéros de cartes de crédit ; PII (information identifiable personnellement) ; correspondance de modèle
Mises à jour des signatures / Politiques	Nouvelles mises à jour d'attaques fournies toutes les semaines ou immédiatement en cas de fortes menaces
Modes de déploiement	Passerelle transparente (couche 2), Routeur/NAT (couche 3), Reverse Proxy (couche 7), sniffer non-en ligne, Proxy transparent (couche 7)
Gestion	Interface utilisateur Web (HTTP/HTTPS), Interface de ligne de commande (SSH/Console)
Administration	Serveur MX pour administration centralisée, option de gestion intégrée (G4, G8), regroupements d'administration hiérarchiques
Login/Enregistrement	SNMP, Syslog, E-mail, reporting graphique intégré, tableau de bord en temps réel
Haute Disponibilité	IMPVHA (Actif/Actif, Actif/Passif), interfaces de sécurité (mode passerelle seulement), VRRP, STP et RSTP

Spécifications	SecureSphere G4	SecureSphere G8	SecureSphere G16 FTL	Serveur de gestion MX
Production	500 Mbit/s	1000 Mbit/sec	2000 Mbit/sec	N/A
Transactions Maxi/Sec	16,000	24 000	36 000	N/A
Latence	Inférieure à la milliseconde	Inférieure à la milliseconde	Inférieure à la milliseconde	N/A
Interfaces	6 x 10/100/1000 Mbit/s (max 4 interfaces fibre)	6 x 10/100/1000 Mbit/s (max 4 interfaces fibre)	6 x 10/100/1000 Mbit/s (max 4 interfaces fibre)	2 x 10/100/1000 Mbit/s (max 4 interfaces fibre)
Types d'interface	Cuivre/Fibre SX/Fibre LX	Cuivre/Fibre SX/Fibre LX	Cuivre/Fibre SX/Fibre LX	Cuivre
Segments de réseau maximum	(2)Passerelle (5)Routeur, Non-en ligne	(2)Passerelle (5)Routeur, Non-en ligne	(2)Passerelle (5)Routeur, Non-en ligne	N/A
Unité de rack	1U ; Modèle FTL 2U	1U ; Modèle FTL 2U	2U	1U ; Modèle FTL 2U
Disque dur	250GB SATA ; Modèle FTL (2) Hot-Swap 250GB SATA	250GB SATA ; Modèle FTL (2) Hot-Swap 250GB SATA	(2) Hot-Swap 250GB SATA	250GB SATA ; Modèle FTL (2) Hot-Swap 250GB SATA
Disque externe	CD-ROM	CD-ROM	CD-ROM	CD-ROM
Taille de rack	Rack 19 pouces (483 mm)	Rack 19 pouces (483 mm)	Rack 19 pouces (483 mm)	Rack 19 pouces (483 mm)
Poids	11.34 Kg ; Modèle FTL 29.48 Kg	11.34 Kg ; Modèle FTL 29.48 Kg	29.48 Kg	11.34 Kg ; Modèle FTL 29.48 Kg
Alimentation	350W ; Modèle FTL (2) Hot-Swap Total 750W	350W ; Modèle FTL (2) Hot-Swap Total 750W	(2) Hot-Swap 750W total	350W ; Modèle FTL (2) Hot-Swap Total 750W
Puissance AC	100-240V, 50-60 Hz	100-240V, 50-60 Hz	100-240V, 50-60 Hz	100-240V, 50-60 Hz
Dimensions	430 mm x 648 mm x 42 mm Modèle FTL : 430 mm x 705 mm x 87 mm	430 mm x 648 mm x 42 mm Modèle FTL : 430 mm x 705 mm x 87 mm	430 mm x 705 mm x 87 mm	430 mm x 648 mm x 42 mm Modèle FTL : 430 mm x 705 mm x 87 mm
Environnement opérationnel	10°C (50°F) à 35°C (95°F)	10°C (50°F) à 35°C (95°F)	10°C (50°F) à 35°C (95°F)	10°C (50°F) à 35°C (95°F)
Environnement non-opérationnel	-40°C (-40°F) à 70°C (158°F) relative humidité 90%, sans condensation à 35°C (95°F)	-40°C (-40°F) à 70°C (158°F) relative humidité 90%, sans condensation à 35°C (95°F)	-40°C (-40°F) à 70°C (158°F) relative humidité 90%, sans condensation à 35°C (95°F)	-40°C (-40°F) à 70°C (158°F) relative humidité 90%, sans condensation à 35°C (95°F)
Certifications EMC	FCC, CISPR 22, CE, VCCI	FCC, CISPR 22, CE, VCCI	FCC, CISPR 22, CE, VCCI	FCC, CISPR 22, CE, VCCI

Imperva, Inc.
États-Unis. Siège social
950 Tower Lane
Suite 1550
Foster City, CA 94404
Tél : +1-650-345-9000
Tél : +1-650-345-9004

Siège social international
125 Menachem Begin Street
Tel-Aviv 67010
Israël
Tél : +972-3-6840100
Tél : +972-3-6840200



Informatique de réseau
Choix de l'éditeur
Pare-feu pour applications
Web

Numéro vert (États-Unis seulement) +1-866-926-4678
www.imperva.com

© Copyright 2008, Imperva, Inc.
Tous droits réservés. Imperva et SecureSphere sont des marques déposées d' Imperva, Inc.
Toutes les autres marques ou noms de produits sont des marques commerciales ou marques déposées de leurs propriétaires respectifs.
#DS-WAF-0308_FR