denyall
a Rohde&Schwarz Cybersecurity company

rWeb

- *Web application & services de parefeu*
- *Prévention des attaques contre la couche applicative*
- *Conformité PCI DSS*
- *Performance et disponibilité*

10 RAISONS DE CHOISIR DENYALL RWEB

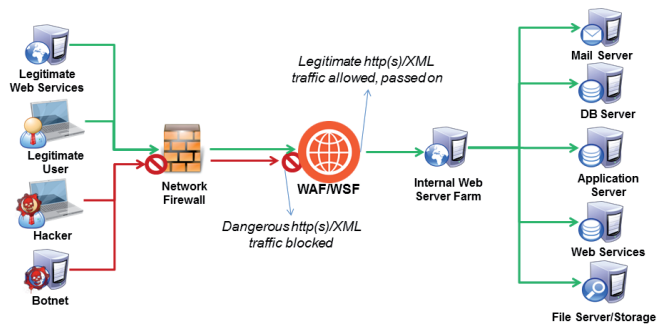
1. **Sécurité éprouvée**, efficace contre les attaques connues et inconnues
2. **Le choix des filtres** pour une politique de reglages: Black list, White list, Scoring list, Moteurs de détection avancés.
3. Le **dépistage du comportement des utilisateurs** empêche l'abus de droits, et les attaques de dénis de service.
4. **La sécurité XML** delivre la pleine capacité du pare-feu de services Web.
5. L'option «Client Shield» sécurise la session de navigation des utilisateurs finaux.
6. **Configuration rapide et facile** via l'interface Web et les templates
7. Les commandes de ligne de l'interface et les APIs pour **industrialiser** les déploiements
8. L'integration avec DenyAll Vulnerability Manager fournit des recommandations de **patch virtuel**
9. La flexibilité de déploiement tant sur les appliances virtuelles que physique.
10. Haute disponibilité avec la synchronisation active/active

LA PROTECTION DES IT CONTRE LES MENACES MODERNES

Créer et partager de l'information en toute confiance est primordial pour votre organisation.Quel que soit votre secteur d'activité:

- Vous devez effectuer des **transactions** avec les membres de votre écosystème via des **applications Web et mobiles.**
- Vous avez besoin de savoir que vos **données sont en sécurité, même dans le cloud**.

Cela nécessite de s'assurer que vos applications sont toujours **disponibles et protégées**.



DenyAll WAFs: En ligne, Blocage en temps réel

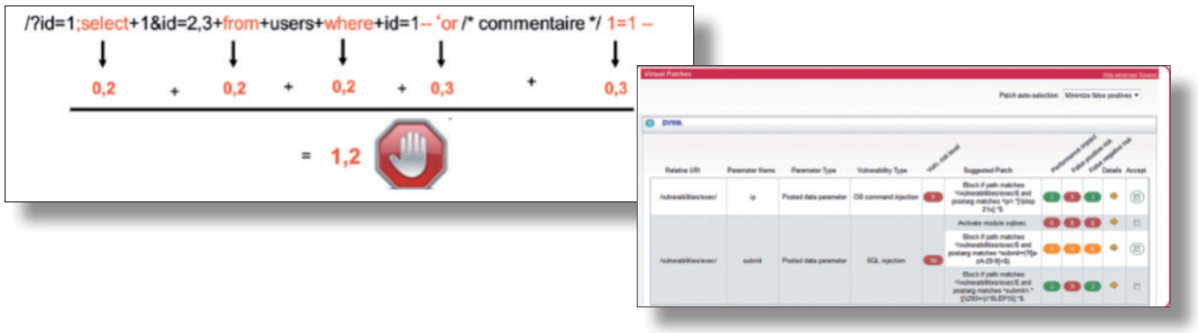
DenyAll rWeb protège votre IT "webisé" contre les tentatives de sabotage, de fuite de données, d'intrusion et contre les attaques en déni de service applicatif. Sa capacité est reconnue à bloquer les attaques visant les sites publiés sur Internet, les applications intranet et extranet, ainsi que les bases de données accessibles via des applications mobiles et des services Web.

Vous pouvez l'utiliser pour assurer votre conformité à **PCI DSS**. Il vous permet d'**optimiser et d'accélérer vos flux de données**, à améliorer le niveau de contrôle exercé par vos équipes sur les applications et l'usage qui en est fait pour accéder, créer et partager de l'information.

denyall
a Rohde & Schwarz Cybersecurity company

rWeb

rWeb



PRINCIPALES CARACTERISTIQUES

Administration

- GUI basé sur le Web, interface de ligne de commande et APIs
- Provisionnement depuis un point central, surveillance et rapport d'activité sur plusieurs appliances
- Rejouer les logs pour affiner la politique de sécurité et pour analyse a posteriori (forensics)
- Patching virtuel grâce à l'intégration avec DenyAll Vulnerability Manager

Securité des services Web

- Validation des templates WSDL, XSD et DTD
- La transformation XML évite la perte de données, remplace les données sensibles et vérifie la complexité
- Signatures de Black list pour xPath et les injections XML
- Pièce jointe SOAP controllée et scanner de virus via ICAP
- Les listes de contrôle d'accès par l' URL et la fonction, approvisionnent les adresses IP source.
- La protection des serveurs UDDI commandés par une analyse.

Plateforme

- Déploiement sur des appliances physiques ou virtuelles
- La synchronisation de noeuds active-passive et active-active pour assurer la haute disponibilité
- Mode pooling & multi-DMZ: le WAF dans le réseau local questionne le WAF dans le DMZ
- La sécurité du déploiement facile du mode transparent.

Securité des applications Web

- Sécurité du mode reverse proxy
- Canonisation, l'anti-evasion, la détection d'anomalies, la transformation de contenu
- Les signatures des «Black list» protègent contre les attaques connues d'application
- «Scoring list» interprete le contenu pour empêcher l'attaque de à jours
- «White list» déploie le model de sécurité positif
- Le dépistage du comportement des utilisateurs empêche le vol de cookies, la force brute d'authentification, le crackage de mot de passe, le téléchargement de site, les attaques DoS de la couche applicative
- Les moteurs de Détection Avancés utilisent l'analyse grammaticale et sandboxing pour se protéger contre les injections, les attaques cryptées, et l'attaque de scripting
- Le script de DenyAll fournit la capacité d'écrire des directives personnalisées
- Geolocalisation par IP & IP Reputation ACL
- Fingerprinting, identification de vos apps et proposition de plusieurs politiques de sécurité

Securité des utilisateurs

- Client Shield empêche le logiciel malveillant «man-in-the-browser» de détourner des sessions
- Méthodes d'authentification: Radius, Kerberos, LDAP, NTLM, SSLv3 certificates, RSA SecurID, SAML v2

Accélération d'applications Web

- Caching In-memory
- Compression
- Répartition de charges du serveur
- SSL terminaison & off-loading

A PROPOS DE DENYALL

DenyAll est un éditeur de logiciel expert en sécurité applicative. 15 années d'expérience dans la sécurisation et l'accélération des applications et services web. Nos produits détectent les vulnérabilités informatiques, protègent les infrastructures contre les attaques modernes qui ciblent la couche applicative et connectent utilisateurs et services web qui permettent de partager et de créer de l'information. Depuis 2017, DenyAll fait partie de Rohde & Schwarz Cybersecurity.

6 avenue de la Cristallerie 92310 Sèvres - FRANCE
+33 (0)1 46 20 96 00
+33 (0)1 46 20 96 02
info@denyall.com
www.denyall.com

ROHDE&SCHWARZ
Cybersecurity