DenyAll Protect

Parefeux pour applications et services Web

Sécurité & accélération de vos applications

Sites institutionnels ou marchands, messageries, outils collaboratifs, portails d'applications d'entreprise, web services et bases de données : vos applications sont au coeur de votre système d'information, et la cible favorite des pirates.

Déployés dans votre DMZ, derrière votre firewall réseau, les parefeux applicatifs de la gamme DenyAll Protect bloquent les attaques qui ciblent la couche applicative de votre infrastructure. Fruit de quinze années d'innovation, ils combinent des fonctions adaptées à vos besoins, pour vous protéger efficacement, y compris contre les attaques inconnues les plus complexes.

Avec **DenyAll Protect**, réduisez les risques de vandalisme, de déni de service, d'intrusion et de vol, et minimisez leur impact sur le chiffre d'affaires et la réputation de votre entreprise.

DenyAll sProxy

Le parefeu applicatif «plug&protect»

DenyAll rXML

Le meilleur parefeu pour web services

DenyAll rWeb

Le parefeu applicatif de nouvelle génération

DenyAll rWeb + Client Shield

La solution de sécurité applicative «end to end»

Principaux bénéfices

Protection immédiate, sans configuration complexe, contre les attaques connues et inconnues visant les couches applicatives (injections, cross-site scripting, etc).

Possibilité de mettre en oeuvre une politique de sécurité plus restrictive, adaptée aux besoins spécifiques de votre entreprise.

Capacité à filtrer efficacement les nouveaux langages et protocoles du Web 2.0.

Sécurisation inégalée des Web Services, sans impact sur l'architecture applicative.

Accélération applicative en vue d'optimiser l'expérience des utilisateurs.

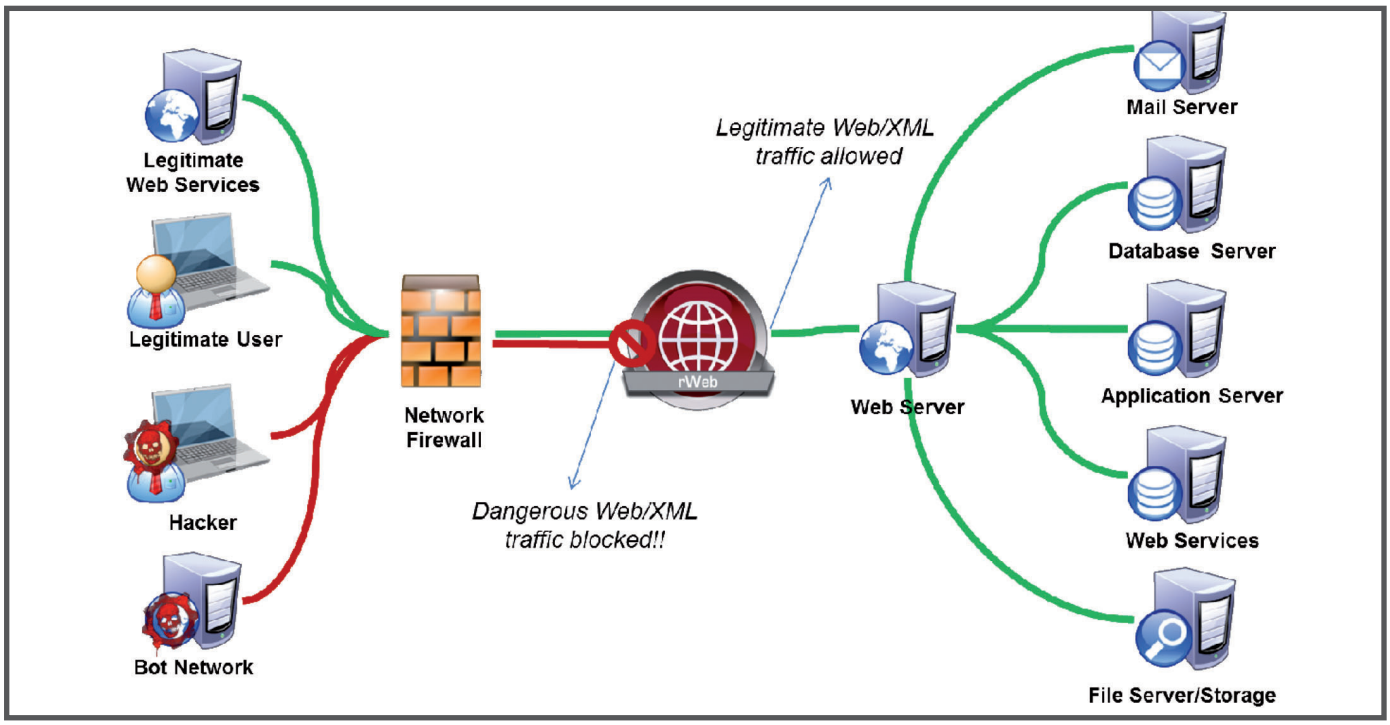
Continuité du service grâce aux mécanismes de répartition de charge et haute disponibilité.

Configuration et suivi centralisé via DenyAll management console.

Conformité avec la norme PCI DSS (pour les sites marchands).

DenyAll Protect :
Le WAF complémentaire du firewall réseau

Déployé derrière le firewall réseau, qui laisse passer les flux Web entrants, le WAF reçoit les requêtes http/https, les analyse et bloque les attaques de type injections ou cross-site scripting.



DenyAll sProxy 4.1 : le parefeu applicatif «plug&protect»

A l'heure du Web 2.0, un WAF est un élément de contrôle incontournable pour sécuriser votre système d'information. Déployé facilement en frontal de vos serveurs (Webmail, portail, ERP, etc), il les protège des attaques modernes (injection SQL, cross site scripting, etc) et accélère l'accès pour les utilisateurs. Quelle que soit la taille de votre organisation ou son secteur d'activité, il vous faut au minimum sProxy pour lutter contre le vandalisme, les dénis de service, le vol de données et l'espionnage industriel.

Mise en place rapide

La mise en oeuvre de sProxy s'effectue en quelques clics : via une interface graphique optimisée,

Pas de modification du DNS : le mode transparent sécurisé facilite le déploiement, tout en profitant de la sécurité du reverse proxy,

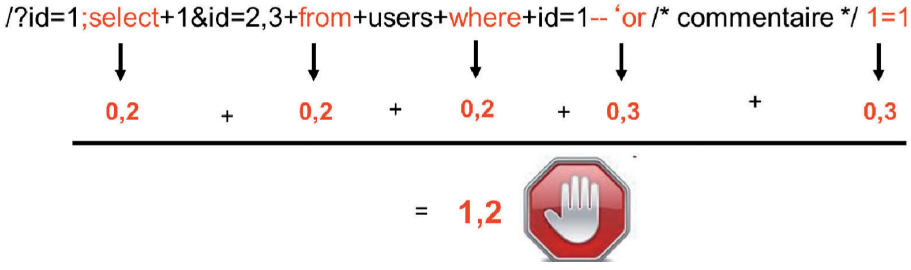
Politiques de sécurité, d'accélération et d'authentification prédéfinies pour les applications courantes (Outlook Web Access, SharePoint, iNotes, SAP, etc.),

Pas d'apprentissage initial : protection immédiate sans configuration spécifique.

Protection contre les attaques inconnues

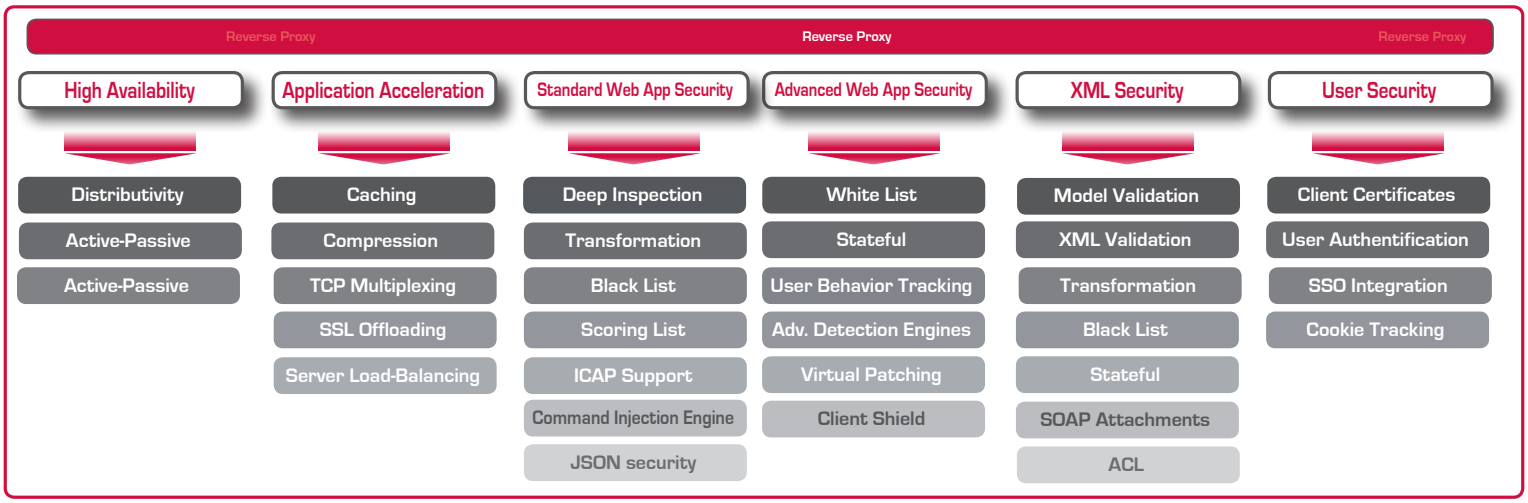
La scoring list, une technologie unique, stoppe les attaques de demain.

- Méthode unique pour détecter les attaques non publiées (« 0-day »).
- Ni paramétrage, ni apprentissage, ni mise à jour.
- Analyse agnostique au contenu (Ajax, JSON, Javascript, etc.).



DenyAll Protect :
une plateforme éprouvée

Les produits de la gamme DenyAll Protect sont issus de la même plateforme modulaire, fruit de quinze années d'innovation au service de la sécurité applicative de clients exigeants.



Fonctions communes à tous les produits

REVERSE PROXY

Analyse des requêtes http/https pour ne transmettre à vos serveurs que celles qui ne sont pas malicieuses.

La rupture protocolaire permet de cacher l'infrastructure, de bloquer les attaques visant les vulnérabilités de vos serveurs internes.

Le mode transparent sécurisé facilite le déploiement (pas de modification de l'adressage IP) mais sans compromettre le niveau de sécurité (reverse proxy intégral).

SÉCURITÉ WEB

Inspection en profondeur : techniques de canonisation (normalisation des données transmises), d'anti-évasion et de détection d'anomalies.

Transformation du contenu des requêtes pour éviter les attaques basées sur la malformation d'URL, le spoofing d'entête, et prévenir le vol de données.

Blacklist : plus de 1000 filtres protègent contre les différents types d'attaques applicatives connues (crosssite scripting, injection SQL, etc). La liste est mise à jour tous les mois par le DenyAll Research Center (DARC)

Scoring list : détermine la dangerosité potentielle des connexions entrantes, en analysant le contenu des requêtes et en appliquant un système de poids.

Protège contre les attaques inconnues (« 0-day »).

Le moteur de sécurité JSON permet de filtrer intégralement ces structures de données à l'aide des moteurs de sécurité http.

Filtrage dynamique des injections de commande pour bloquer les attaques sans générer de faux positifs.

SÉCURITÉ DES UTILISATEURS

Authentification des utilisateurs par certificats SSLv3.

ACCÉLÉRATION DES APPLICATIONS

Caching des pages les plus souvent demandées.

Compression à la volée des données.

Multiplexage des connexions entrantes (tunnels HTTP/1,1).

Terminaison des tunnels SSL.

Server load-balancing : distribution du trafic entrant à destination des serveurs de votre infrastructure.

HAUTE DISPONIBILITÉ

Des « clusters », dans lesquels plusieurs WAF fonctionnent de concert, en mode actif-passif ou actif-actif, assurent la redondance de votre sécurité applicative.

Capacité de montée en charge de vos applications grâce au mécanisme de synchronisation automatique du mode actif-actif, configuré en quelques minutes.

ÉVOLUTIVITÉ

Vos contrôles de sécurité applicative évoluent en fonction de vos besoins. Une simple clé de licence permet d'évoluer de sProxy vers rXML (protection des Web Services) ou vers rWeb (sécurité avancée des applications web), ou encore d'ajouter à rWeb les fonctions de protection des Web Services :

Protection des Web Services :

- Validation des modèles XML
- Filtres spécifiques contre les attaques visant les Web Services
- Protection des serveurs UDDI, etc.

Sécurité avancée des applications web :

- Whitelist (modèle de sécurité positive),
- Analyse comportementale (UBT),
- Protection des sessions HTTP (stateful),
- Moteurs de Détection Avancée,
- Module optionnel de sécurisation du navigateur (Client Shield).

DenyAll rXML 4.1 :
le meilleur firewall pour web services

Au sein d'architectures orientées services (SOA), la sécurité des applications et des données est simplifiée par rXML. Il protège efficacement vos Web Services contre les attaques applicatives sans changement d'architecture. Il sécurise les transactions XML/SOAP entre composants internes et externes de vos applications, évitant ainsi les dénis de service et le vol de données.

Principaux bénéfices

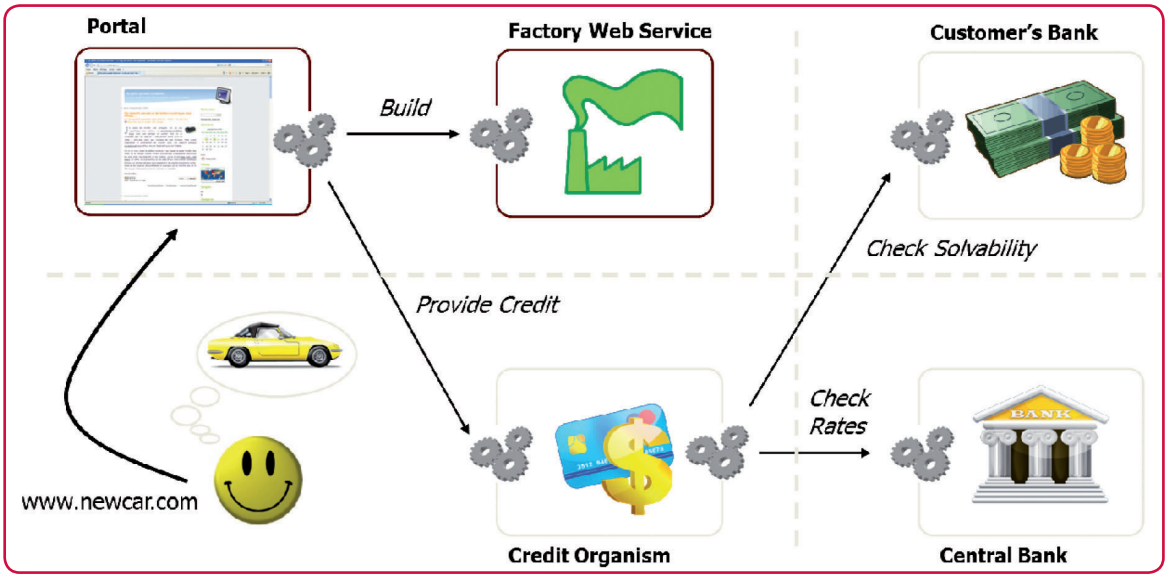
Sécurisation des Web Services existants sans impact sur l'architecture applicative.

- rXML n'est pas un acteur du Web Service,
- Aucune modification requise de la configuration des composants du Web Service,
- Pas de modification de l'architecture d'échange de clés de chiffrement ou de signature.

Haut niveau de protection face aux attaques applicatives courantes.

Niveau de sécurité XML/SOAP inégalé face aux attaques visant spécifiquement les Web Services.

Pas d'apprentissage : vos Web Services sont protégés en quelques clics.



Fonctions spécifiques à DenyAll rXML

Validation du modèle : les données transmises par les Web Services sont vérifiées et mises en conformité avec les modèles XML (WSDL, XSD et DTD). Des règles additionnelles peuvent être spécifiées pour renforcer ces modèles.

Validation et transformation XML : pour éviter la fuite de données, les messages d'erreurs effacés, les données sensibles remplacées et la complexité vérifiée (taille maximale d'un document ou profondeur maximale de l'arbre).

Black List : des signatures spécifiques (injections xPath, XML, DoS, etc) combinées aux filtres http génériques assurent un excellent niveau de sécurité face aux attaques ciblant les Web Services. Protection unique contre les injections xPath en aveugle.

Stateful : le suivi des éléments XML permet d'éviter l'altération des données, que ce soit involontairement par un utilisateur, ou lors de leur transmission, du fait d'un attaquant.

Pièces jointes SOAP : elles peuvent être autorisées ou non, une taille maximale peut être fixée, les pièces jointes textes sont analysées par la black list XML et le filtre http générique, ainsi que par un antivirus via le protocole ICAP.

Listes de contrôle d'accès :

- Contrôle d'accès granulaire aux fonctions des différents Web Services (par URL et fonction, par adresse IP source)
- Limitation des accès UDDI aux services de la registry, en fonction de l'adresse IP source ou des fonctions accédées.

DenyAll rWeb 4.1 : le WAF de nouvelle génération

Pour fournir une expérience utilisateur enrichie, les applications et services Web utilisent de nouveaux langages et protocoles (JSON, AJAX, REST, SOAP, HTML5, etc) et des architectures de plus en plus complexes. Une nouvelle génération de contrôles de sécurité est requise pour faire face à ces évolutions. DenyAll rWeb s'appuie sur une plateforme éprouvée capable d'identifier la nature des requêtes et de bloquer les attaques et tentatives de contournement. Produit le plus complet de la gamme Protect, DenyAll rWeb réunit toutes les options présentes dans DenyAll sProxy ainsi que, en option, les fonctions de sécurité XML/SOAP présentes dans DenyAll rXML.

Fonctions spécifiques à DenyAll rWeb

Sécurité avancée des applications web

Whitelist : identifie les caractéristiques exactes des données transmises aux applications Web pour une activation rapide et une protection sans faux positifs.

Stateful : suivi, signature et chiffrement des données qui sont associées aux sessions HTTP afin de prévenir les usurpations d'identité.

User Behavior Tracking : le moteur d'analyse comportemental identifie et bloque les attaques basées sur des requêtes légitimes, DOS, brute force etc.

Moteurs de détection avancée : ils permettent de protéger vos applications contre le chiffrement en base64 des attaques, les advanced path traversal, la pollution des paramètres http, le splitting des requêtes http, l'utilisation des tags et attributs html, la détection des injections SQL par analyse grammaticale et des langages de script, les calculs arithmétiques.

Sécurité applicative «End to End» avec Client Shield

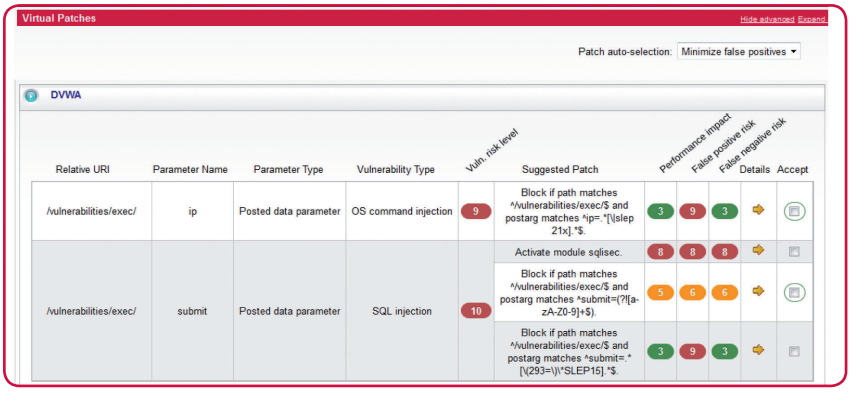
Le navigateur est le point le plus faible dans une chaîne applicative. Pour protéger les données contre les malwares de type «Man-in-the-browser», rWeb lance le module optionnel **Client Shield**, qui contrôle l'exécution des navigateurs et empêche les codes malveillants d'utiliser une connexion authentifiée pour accéder à l'application et voler vos données. Client Shield est proposé en standard pour Outlook Web Access et peut être configuré pour protéger toute application. Mise au point par notre partenaire, Promon, **Shield** sécurise aussi les navigateurs et applications mobiles tournant sur iOS et Androïd.

Sécurité des utilisateurs

rWeb peut déléguer l'authentification à des composants tiers tels que serveurs LDAP ou ActiveDirectory, CA SiteMinder (SSO), SecurID (authentification forte) et Radius.

Intégration avec les produits DenyAll Detect

Après import des rapports de scans de vulnérabilités effectués par les produits Detect, rWeb propose des options adaptées pour le patching virtuel des vulnérabilités découvertes. A terme, cette intégration permettra d'automatiser la découverte des applications non protégées et la mise en place d'une politique de sécurité adaptée.



Exemple de patching virtuel avec DenyAll Detect

DenyAll Protect

	sProxy	rXML	rWeb	rWeb + Client Shield
Haute disponibilité	✓	✓	✓	✓
Accélération des applications	✓	✓	✓	✓
Management centralisé (via DAMC)	✓	✓	✓	✓
Sécurité web standard	✓	✓	✓	✓
Sécurité XML/SOAP		✓	✓*	✓*
Sécurité web avancée			✓	✓
Sécurité utilisateur	Basic		✓	✓
Sécurité navigateur				✓

* *Optionnel*

Avantages concurrentiels

Fonctions de sécurité négative et positive combinées, pour une sécurité maximale

Blacklist (attaques connues).
Whitelist, protection des sessions http.

Fonctions de sécurité inédites :

Les Moteurs de Détection Avancée sont de nouveaux modules conçus pour filtrer efficacement les nouveaux langages et protocoles (JSON, HTML5, etc), et faire face aux techniques d'obfuscation et d'évasion des attaques modernes.

La Scoring list protège votre infrastructure contre les attaques applicatives inconnues (zero day).

L'analyse comportementale (UBT) bloque les attaques automatisées (déni de service, crackage de mot de passe, téléchargement de site, etc).

L'option **Client Shield** contrôle l'exécution des navigateurs se connectant à vos applications, empêchant les malware de type «Man-in-the-browser» de s'injecter dans la session.

Intégration avec les produits DenyAll Detect

Les rapports de scans Detect importés dans rWeb proposent des options adaptées à vos objectifs (sécurité maximale, performance optimisée, réduction des faux positifs), pour le patching virtuel des vulnérabilités découvertes. A terme, l'intégration permettra d'automatiser la découverte des applications non protégées et la mise en place d'une politique de sécurité adaptée.

Déploiement facilité et sécurisé

Le Mode Transparent Sécurisé permet un déploiement facilité sans compromis de sécurité (reverse proxy). En mode « pooling », aucune connexion n'est initiée depuis la DMZ, le LAN interroge la DMZ.

Choix du mode de distribution

Les parefeux applicatifs DenyAll Protect sont disponibles sous forme de machine virtuelle, d'appliance physique ou de logiciel Linux.

DenyAll est un leader innovant sur le marché de la sécurité applicative. Nous aidons les organisations à détecter les vulnérabilités au sein de leur infrastructure et à sécuriser et accélérer leurs applications et services Web. Nos parefeux à base de reverse proxy protègent des applications cloud, SOA et Web transactionnelles contre les attaques connues et inconnues. Basés en France, nous vendons via nos partenaires en Europe, Afrique, au Moyen-Orient, Asie et Amérique latine.

63ter avenue Edouard Vaillant
92 100 Boulogne-Billancourt FRANCE
+33 1 46 20 96 00

denyall SECURITY SOLUTIONS