![denyall logo]

Web Application Firewall

+ *Application-layer attack prevention*
+ *PCI DSS Compliance*
+ *Optimization, performance and availability*

WAF

## 10 REASONS TO CHOOSE DENYALL WEB APPLICATION FIREWALL

1. Time-tested security, **effective** against known and unknown attacks
2. The ability to combine negative & positive security with **user context** (time, location, device, etc)
3. A **productive** environment which lets administrators manage policy and optimize data flows visually using a proven workflow approach
4. The ability to **profile** web applications and learn how they work
5. The option to **replay** logged traffic to tune policy, perform forensics analysis

6. **Virtual patching** with DenyAll Vulnerability Manager and 3rd party vendors
7. APIs to **industrialize** deployments
8. The flexibility of managing both **virtual** and hardware appliances
9. Support for key **authentication** methods
10. The ability to **add features** with DenyAll Web Services Firewall (secure XML/JSON traffic) and DenyAll Web Access Manager (simplify user access/control)

PROTECTING YOUR IT AGAINST MODERN THREATS

Creating and sharing information in confidence is essential to your organization. Whatever your business:

– You need to be able to **transact** with members of your ecosystem **using web and mobile apps**.

– You need to trust that your **data is safe, even in the cloud.**

That means making sure your applications are always **available and secure.**

DenyAll WAFs: In-Line, Real-Time Blocking
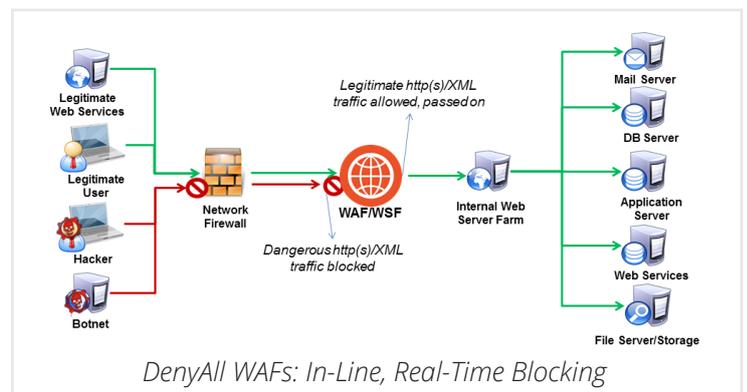
DenyAll Web Application Firewall protects your web-enabled IT against denial of service attacks, defacement attempts, intrusion and data leakage risks. It has a proven track-record of blocking attacks targeting Internet facing sites, intranet and extranet applications, even databases queried by mobile apps.

You can use it to comply with regulations such as **PCI DSS**. It enables you to **optimize and accelerate your corporate data streams**, to improve the level of control your team has over your applications, how they are being used to access, create and share information.

KEY FEATURES

Administration

- Visual policy & traffic control with an intuitive, powerful workflow approach
- Application discovery & profiling
- Central provisioning, monitoring and reporting on multiple devices
- Log replay for policy testing and forensics analysis
- Virtual patching: integration with DenyAll Vulnerability Manager and others

Web Application Security

- Reverse proxy security
- SSL termination & off-loading
- ICX engine combines negative policy, based on known attack techniques, and positive security, with application learning and white listing
- 100+ preconfigured filters including URL manipulations & data rewriting, anti-Denial-Of-Service, anti-Bots, etc
- ACE engine computes user activity and context to prevent application-logic attacks and abnormal behavior

Platform

- Deployment on physical and/or virtual appliances
- Reverse proxy clustering and load balancing to ensure high availability and redundancy
- Secure XML traffic with DenyAll Web Services Firewall extension
- Add Single Sign On capabilities with DenyAll Web Access Manager

User Authentication

- Multiple methods supported, including: Radius, Kerberos, LDAP, NTLM, forms, HTTP Basic, SAMLv2, etc

Web Application Acceleration

- Caching in memory (RAM)
- Compression
- Server load-balancing

ABOUT DENYALL

DenyAll is a software vendor, expert in application security. For 15 years, we have been helping demanding customers secure their web applications and services. Our products detect IT vulnerabilities, protect infrastructures against modern attacks targeting the application layer and connect users to the applications which allows them to create and share information.

🏠 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