

jetNEXUS Application Firewall

Your Application's Second Line of Defence

Security 2.0®

Comprehensive protection for Web applications

- Against OWASP top 10 such as SQL injection, cross site scripting.

Proactive protection via

- Secure session management
- URL encryption
- Site usage enforcement

PCI-Compliance

Primarily PCI DSS v1.2 (6.6)

All-Round Protection and Control of Web Applications

The jetNEXUS Application Firewall (JAF) offers security managers comprehensive functionalities for monitoring Web applications centrally and securing them against the outside world as a "second line of defence", with as little outlay as possible and without modifying the application itself. The security level on JAF can be easily adjusted according to the risk potential of the application in question: From basic Protection against known methods of attack based on – updateable – blacklists, through to the rigorous definition and implementation of the required external behaviour in JAF using whitelists, whose configuration is supported via various learning modes, among other tools. What is known as "External Patching" is also particularly important with JAF: Specific weak points, e.g. those revealed in source code reviews, are secured against the outside world in real-time using JAF, and can - if actually possible in principle – be rectified "at leisure" within the application before the next scheduled maintenance session.

Maximum Flexibility in Deployment

Web infrastructures often vary greatly from company to company, and generally change over the course of time, whether planned or unplanned. jetNEXUS offer maximum flexibility with regards to the implementation scenarios:

- JAFE -** jetNEXUS Application Firewall for Enterprise. Designed for Enterprise Businesses with no restrictions.
- J AFL -** jetNEXUS Application Firewall Lite. Cost effective solution - designed for smaller web infrastructures.
- JAFET-** jetNEXUS Application Firewall for Enterprise Traffic Manager. Designed to run on the jetNEXUS Enterprise Traffic Manager.

Central, client-compatible administration coupled with distributed implementation

In enterprise environments Web applications are often operated in a distributed way across multiple data centres. JAF fits in here perfectly: Thanks to its cluster-compatibility, distributed JAF installations can be administered centrally.

Administrators responsible for the security of a Web application can define central policies, as well as check and distribute sets of rules, based on specific roles.



JAF Security

"Traditional" WAF Features

- Bi-directional HTTP request analysis
- White/ black/ grey listing
- Various learning modes

Pro-active Security Functions

- Secure session management
- URL encryption
- Site usage enforcement

Highlights

- Freely programmable API (Python)
- XML/Web Services Security Gateway

JAF Reporting

Monitoring and reporting

- Central logging for centralised troubleshooting
- Real-time dashboards and statistics
- Report generation as HTML & PDF

JAF Administration

Client Compatibility

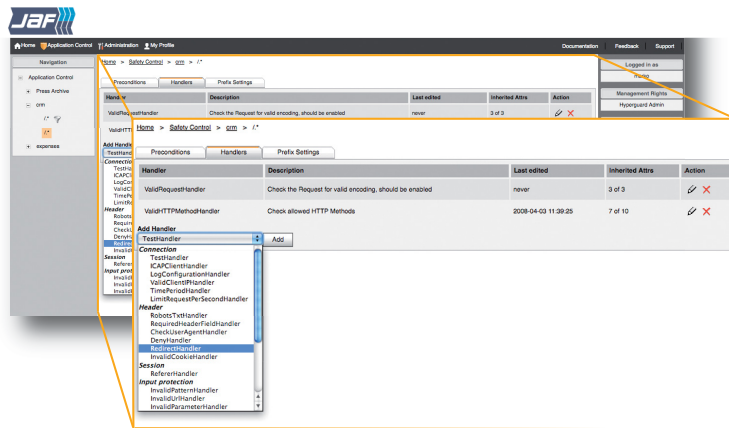
- Central administration of multiple applications
- Support for multiple administrators
- Rights assignment with role concept
- Complete configuration history and audit log

Cluster administration

- Central administration
- Central statistics
- Central log file evaluation

JAF Overview

JAF was developed from the ground up with the primary goal of providing comprehensive protection for productive Web applications against hacker attacks and worms at the application level. JAF monitors the incoming and outgoing HTTP traffic to do this. Depending on the configuration, JAF – as a Web Application IDS – can detect attacks or – as a "second line of defence" – can secure known and unknown weak points in Web applications against the outside world. The entire software architecture was carefully selected to ensure that it can be integrated as flexibly as possible into existing security and Web infrastructures with as little additional effort as possible.



An intuitive web-based user interface permits the easy definition and administration of the various security functions; from basic protection through to a highly detailed full-protection mode. In "Basic Mode", numerous wizards and learning modes support the configuration here, and "Expert Mode" allows highly detailed settings to be carried out.

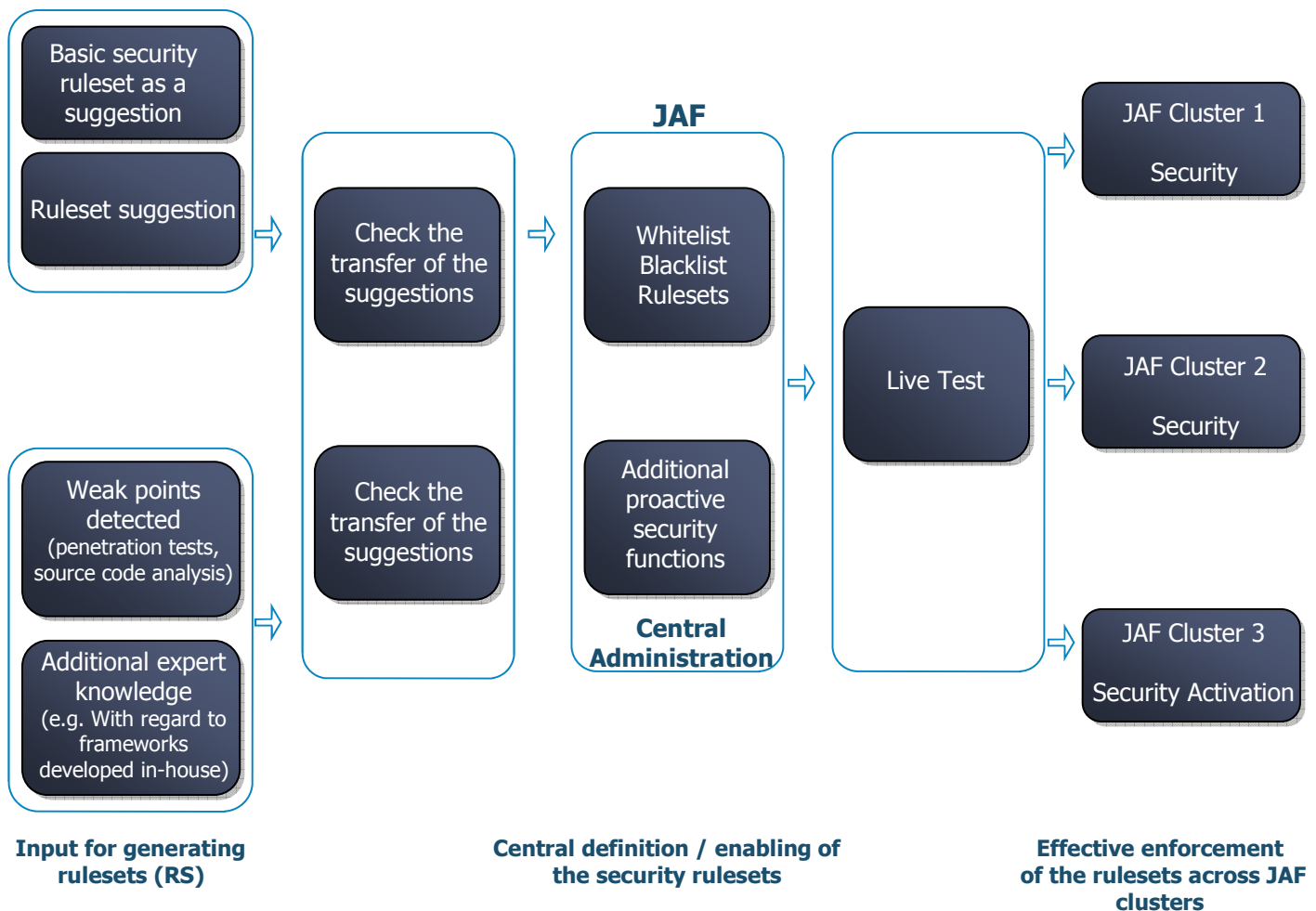


JAF also offers central monitoring and reporting in decentralised cluster installations. Comprehensive reporting functions such as real-time statistics, as well as various evaluations of the security status over specific time periods, allow the necessary reports to be generated, and therefore provide efficient processes relating to compliance requirements. Thanks to the centralised, role-based administration, policies and security rulesets can be defined at one location, checked and then distributed in the cluster.

JAF Overview

How to define and implement security rulesets

Typical Web infrastructures in the enterprise environment consist of several hundred Web applications whose operation is partly distributed across different computing centres and/or external service providers, and even the operation of individual components. These applications often also differ greatly in terms of their internal structure as well as their risk potential: Some may have been developed internally within the company or by external service providers according to secure coding guidelines, their source code is available and is also subjected to a further check by experts following every change. Others are based on outdated frameworks or on components from third party suppliers, for which there is no complete documentation available, and for which it is not possible to order sufficiently up-to-date patches. For each application, the required security level therefore needs to be defined and implemented as simply as possible. To do this, JAF offers different options for generating and maintaining rulesets.



Maximum Flexibility in Deployment

Web infrastructures often vary greatly from company to company, and generally change over the course of time, whether planned or unplanned.

jetNEXUS offer maximum flexibility with regards to the possible implementation scenarios:

- JAFE -** jetNEXUS Application Firewall for Enterprise. Designed for Enterprise Businesses with no restrictions.
- JAFL -** jetNEXUS Application Firewall Lite. Cost effective solution for smaller web infrastructures.
- JAFET-** jetNEXUS Application Firewall for Enterprise Traffic Manager. Designed to run on the jetNEXUS Enterprise Traffic Manager appliance.



Delivery Options

Software plug-in for:

- All Standard Web servers
- jetNEXUS Enterprise Traffic Manager

Supported Platforms

Solaris / Linux / BSD
Windows
Apache, IIS, ISA
Java J2EE

Contact Layer 47

Tel: +44 (0) 870 382 5050
Fax: +44 (0) 870 382 5520

Email: info@layer47.com
Web: www.layer47.com

Cedar Court,
Grove Business Park,
Waltham Road,
Maidenhead,
Berks,
SL6 3LW

JAF Applications

▪ Detecting attacks on and hacks into Web applications

Many web site owners these days do not carry out any monitoring on the Web application level and want to detect attacks and hacks into their Web applications as a first step.

▪ A case for JAF

JAF can be used as a Web application IDS. In "Log Only" mode, all HTTP requests are checked transparently for – freely configurable – rulesets, but which are not activated and do not therefore intervene in the HTTP data flow.

▪ Retro-implementation of time-critical security for Web applications

Many Web applications use components such as third party software or are based on frameworks whose source code is not available or which are no longer being maintained. When weak points are detected, the time-critical "patching" in the application itself is therefore not possible, or would counteract the defined maintenance process.

▪ A case for JAF

It was for precisely these environments that JAF was developed.

▪ Web Application Security with maximum performance requirements

Large and often fast growing online shops and social networking sites in particular rely on high-performance, distributed cluster infrastructures and are looking for a Web application security solution which offers optimum integration into this environment and which does not cause any performance bottlenecks or require continuous updating at the network level.

▪ A case for JAF

JAF both as a Web server plug-in and also when integrated with the high performance jetNEXUS Enterprise Traffic Manager, can be used in high-performance infrastructures. In both configurations, the unique JAF clustering architecture will scale up with the number of Web servers.

▪ PCI compliance – in particular with regard to requirement PCI DSS v1.2 (6.6)

The cited requirement of the data security standard from the credit card industry explicitly requires "the installation of a firewall at the application level"; or as an alternative it requires "the checking of all user-defined application code for frequently occurring security gaps by an organisation specialising in application security".

▪ A case for JAF

With JAF the PCI DSS compliance requirements are implemented quickly and cost effectively.