PROXEDO
API SECURITY

WHY PROXEDO API SECURITY?

1. Deep inspection of API traffic
2. Flexible security enforcement
3. Custom analysis of application communication
4. Highly flexible, black-belt delivery team
5. Pioneers in proxy technology
6. Made in EU – 'Clean' code base

ADDITIONAL SECURITY LAYER OVER WAF AND API MANAGEMENT

The Challenge

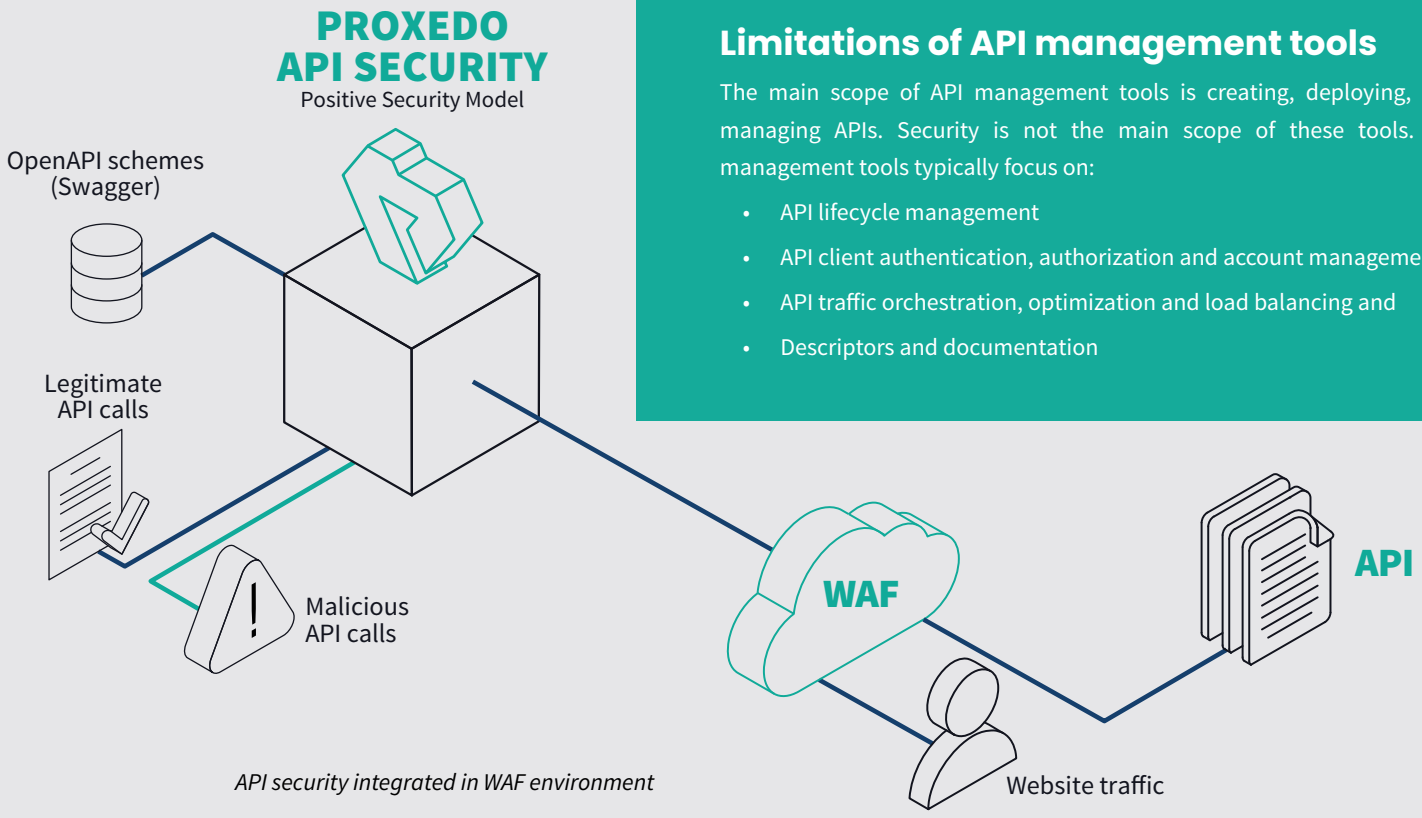
Limitations of WAFs

A web application firewall (WAF) filters, monitors, and blocks HTTP traffic to and from a web application. However, WAFs are unable to block targeted API attacks as they are not optimized for deep inspection of API traffic. WAF products are typically optimized for signature-based filtering of HTTP traffic. They are not suitable for controlling data flow embedded in API communication. They lack traffic validation, detailed logging and the ability to implement customized security policies. Enterprises with extensive API infrastructure and traditional WAFs should need a specific solution that explicitly addresses the above limitations.

Limitations of API management tools

The main scope of API management tools is creating, deploying, and managing APIs. Security is not the main scope of these tools. API management tools typically focus on:

- API lifecycle management
- API client authentication, authorization and account management
- API traffic orchestration, optimization and load balancing and
- Descriptors and documentation



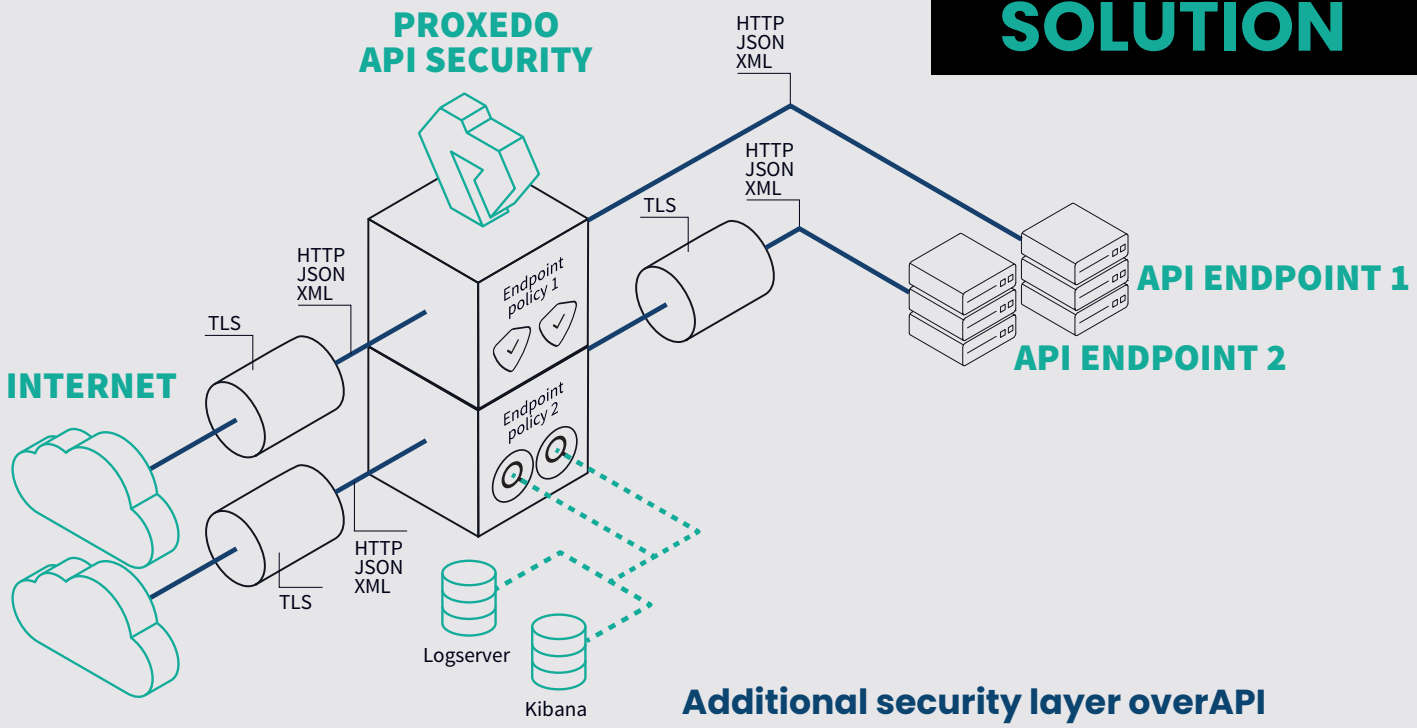
API security integrated in WAF environment

BALASYS

info@balasys.eu

SOLUTION

Proxedo API Security sample architecture



API Security Beyond WAF

Proxedo API Security (PAS) is a specialized web application firewall exclusively for protecting API endpoints. It's a highly flexible network security solution that helps your enterprise gain control over the application communication to prevent API breaches. Based on our deep packet inspection (DPI) technology, you can validate, encrypt and analyze API traffic in detail and implement a signature-based protection. Thanks to our flexible architecture, you can enforce custom security policies without compromise. PAS focuses exclusively on API security by offering a killer combination of enforcement and insight, supplemented by generic WAF functions.

As an extra security layer, Proxedo API Security perfectly complements traditional WAF solutions.

Additional security layer overAPI management

Proxedo API Security is NOT a management tool, but a dedicated solution with clear focus on security. In contrast to API management vendors where security is just a checkbox feature, PAS focuses exclusively on API endpoint protection by offering a killer combination of validation, transformation, encryption and insight of API traffic. From security standpoint, Proxedo API Security adds great value to API management solutions, as well.

As an extra security layer, PAS supports:

- API traffic validation
- Customizable API traffic encryption
- Customizable security policies
- In-depth, data-level logging and insight
- Connection to authentication systems

The following table summarizes the key differentiators of Proxedo API Security compared with traditional web application firewalls (WAFs):

Web Application Firewalls	Proxedo API Security
Focus only on web application protection	Focus on web application and B2B application integration protection
Inspection only on HTTP protocol	Inspection on API layer
No DPI (Deep Packet Inspection)	Advanced DPI
No API call validation	API call validation
Limited logging capabilities	Customizeable traffic- & security logging
No flexible policy configuration	Flexible policy configuration
Pattern matching based on URL database (blacklisting)	Pattern matching AND rule implementation based on the protected service (white listing)