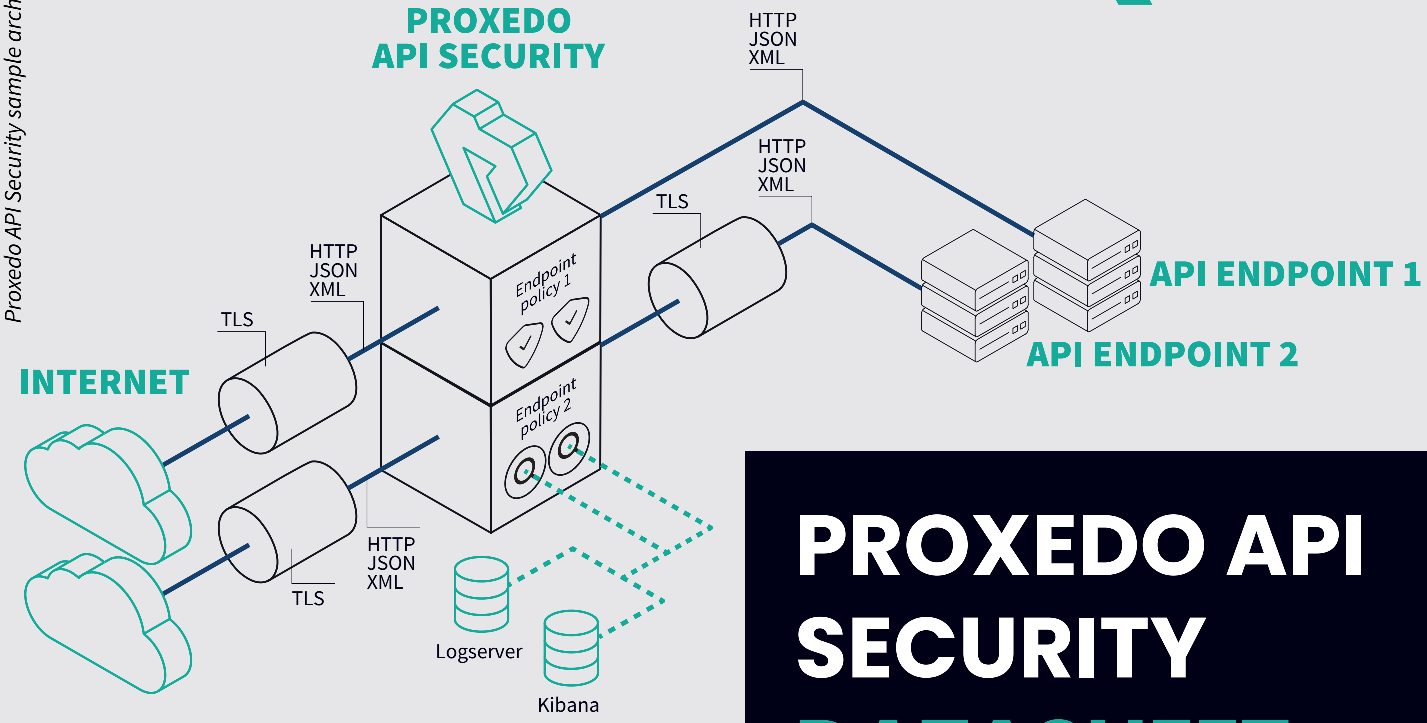
PROXEDO
API SECURITY



Proxedo API Security sample architecture

PROXEDO API SECURITY DATASHEET

Technology overview

The **Proxedo API Security** (PAS) is a network security software that protects API serving endpoints. PAS is a transparent HTTP/HTTPS proxy gateway located in the network flow between consumers of the APIs (clients), and backend systems serving the API (servers).

Key features

1 Creates granular security policy for API endpoints

2 Enforces certificate-based authentication

3 Handles incoming TLS connections from clients and outgoing TLS connections to servers separately and selectively

4 Verifies that communication conforms to HTTP specifications

5 Verifies that the content of the messages conforms to their specified content type

6 Verifies that the content of messages conforms to API specification(s) described in schemas

7 Extracts parts of the content and relay them to external destinations such as log analyzers, SIEMs and data warehouses

BALASYS

info@balasys.eu

ARCHITECTURE

Proxedo API Security is based on a micro-services architecture. Each component of the architecture is responsible for a well-defined subset of handling traffic between the client and the backend system. Each of these components run in a docker environment. PAS is built from three components:

Transport Director

Manages the transport layer of API connections. Handles TLS connections from the client and towards the backends. Load-balances between multiple backend servers and Flow Directors. Validates HTTP protocol in the calls.

Flow Director

Manages the security flow for the endpoints. It is responsible for the execution of the plugins in the Endpoint's flow and applying error policies if necessary.

Insight Director

Manages the connections to external targets. It is responsible for sending data collected by Insight plugins to target systems.

LICENSING

Licensing is based on two parameters. Both parameters are counted when calculating the license fee:

The number of backend servers

A backend server is an instance of a server that handles API traffic. PAS technically limits the number of configurable host:port pairs.

The number of protected API service endpoints

An API endpoint is a collection of API resources that build up the API of a concrete, well defined service. It is identified by a base URL and is protected by a single security policy. PAS technically limits the number of security policy configurations.

Proxedo API Security Homepage

Request a trial

BALASYS

Supported protocols and standards

1 | HTTP 1.0, 1.1

2 | SSLv2, SSLv3, TLSv1, TLSv1.1, TLSv1.2

3 | OpenAPI 2.0 (Swagger 2.0)

4 | JSON (RFC 8259)

5 | SOAP (RFC 4227)

6 | BSD syslog (RFC 3164)

7 | IETF syslog (RFC 5424)

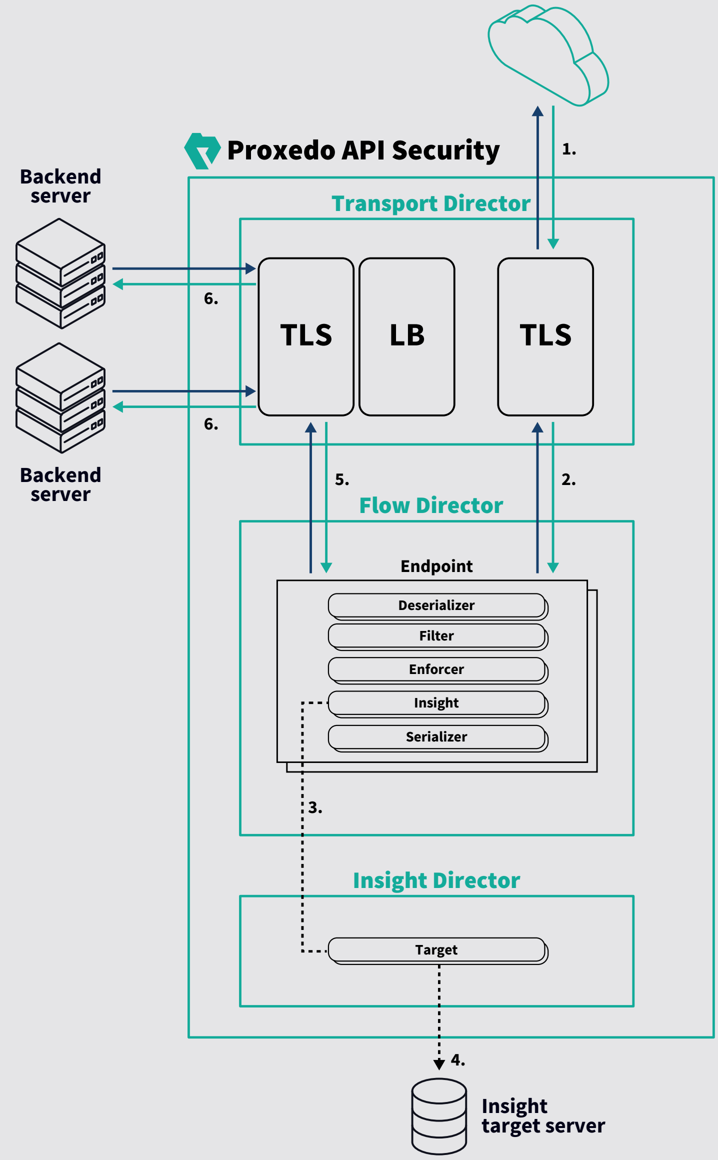
8 | JMESPath Specification

9 | Uniform Resource Identifiers (RFC 3986)

Software prerequisites

1 | Ubuntu Linux 18.04

2 | Docker version: >17.12.0



Proxedo API Security technical architecture