

TOPOLOGI INTERCEPTOR

Frontline Protection for XML Services

OVERVIEW

Topologi Interceptor is a web-based application for non-intrusive validation and pattern detection in distributed XML Applications. Configured through a straightforward web interface, the Interceptor builds on the industrial-strength IBM Websphere platform. It effortlessly scales to multi-processor and distributed systems and conforms to recognized international standards such as W3C XML, W3C XML Schemas, and ISO Schematron.

SUPPORTED ARCHITECTURES

1. Validating/Uncompressing Front-End for XML Web Server



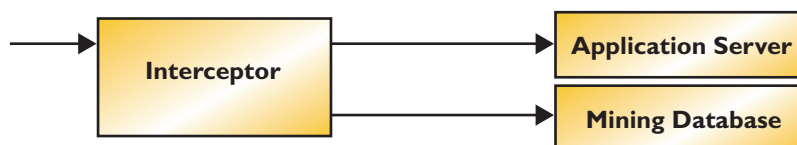
Interceptor makes it feasible and easy to validate incoming data to XML Services. Validation is typically disabled on servers due to concerns with performance and complexity. Interceptor protects your database and applications from bad XML.

2. Firewall



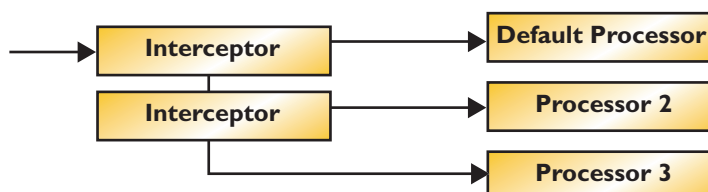
Interceptor provides the protection to let you expose your local XML Service to your company intranet or the internet. Even better, Interceptor is non-intrusive – it can be deployed and administered by system, network or security administrators without bothering server or application administrators.

3. Data Miner



Interceptor can look for patterns in XML data streams and send copies of interesting data to a monitoring service.

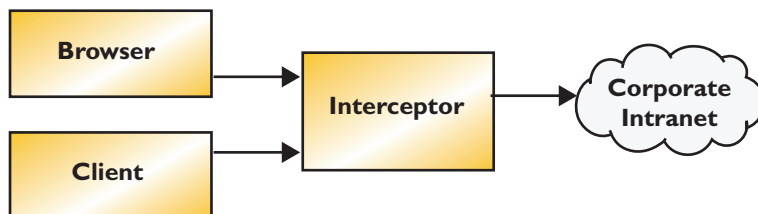
4. Business Rules Switch



Interceptor lets you send documents to an alternate service based on business rules. Interceptor services can be chained, allowing complex XML-based switching and routing.

TOPOLOGI INTERCEPTOR

5. Department-side Forms Checker



Interceptor can be run at the client side, for example to provide forms validation, reducing communications costs, server load or the need to deploy client applications. Interceptor is ideal for supporting AJAX development.

TESTS

Interceptor allows systematic checks of incoming XML data:

- **HTTP tests:** Does the data have correct headers? Does the data uncompress, if compressed?
- **Byte tests:** Is the data too long? Does the data contain allowed or disallowed byte sequences?
- **XML Well-Formedness tests:** Is the XML data well-formed and XML namespace conformant?
- **XML DTD and XML Schema validity:** Do the structures in the XML conform to the allowed names and structures? Do the data values in the XML document conform to the allowed datatypes? Are the correct uniqueness constraints on data allowed?
- **ISO Schematron rules checking:** Are the appropriate business rules followed? Do values correspond to those in external controlled vocabularies? Are co-occurrence constraints between different attributes/elements satisfied?
- **ISO Schematron data mining:** Does the document contain data patterns which should trigger the document to be copied or diverted?

DETAILS

Interceptor is typically used to provide a more secure or robust HTTP or HTTPS front-end to less-secure, inadequately validated or congestable back-end services. Its three main use-cases are:

- detect and protect systems from invalid or improper data, logging or refusing those requests
- test incoming data against business rules, then transform and forward the data to particular URLs as appropriate
- mine streams of XML documents against criteria and copy documents of interest to other services as appropriate.

SECURITY

Interceptor can be used to address a range of XML-related security issues:

- block oversize incoming documents
- block documents that override the external DTD with internal declarations
- block documents that use DTDs and external entities (eg the "billion laugh" attack)
- act as data-driven firewall: local trusted clients are not validated, external untrusted clients are validated
- check data integrity constraints to prevent database corruption.