

Speed up the Oracle Service Bus by offloading Security into the Oracle Enterprise Gateway.

**Axel Grosse
Vordel Ltd.
Deutschland, Ratingen**

Schlüsselworte:

Oracle Enterprise Gateway, OEG, Vordel, XML-Gateway, Security, Webservice Security, WS-Security, WS-Policy, SOA-Security

Einleitung

Einer der neuesten Produkte im Oracle Middleware & Identity Management Portfolio ist das Oracle Enterprise Gateway. Einer seiner Stärken hat das Gateway in der sehr performanten und patentierten Verarbeitung von XML Strömen. Wir wollen hier eine Antwort auf die Frage geben: "Welchen Nutzen hat ein Gateway im Umfeld eines Oracle Service Buses?" Die Antwort werden wir in Form einer Demo geben, die das Einsatzgebiet des OEG als starken Partner des OSB bei der Bewältigung von Aufgaben mit hohem Security Anteil beschreibt.

Eine kurze Vorstellung der Firma Vordel

Vordel ist eine kleine aber feine Software Schmiede aus Dublin mit einer Historie von über 10 Jahren als erfolgreiches Unternehmen. Unsere Technologie ist in der 6. Generation und wurde in dieser Zeit kontinuierlich verbessert und erweitert. Das ist nicht nur eine Aussage von Vordel.

Wir haben strategische Partnerschaften mit Firmen wie z.B. Oracle und CA. Beide Firmen haben die existierenden Gateway Hersteller einer sorgfältigen technischen Prüfung unterzogen, die vor allen eine Vollständigkeit in den Use Cases und extreme Performance Tests beinhalteten.

Diese Firmen sind führend in der Cloud, SOA und Security Technologie, Sie wissen wo man hinschauen muss und wie man Produkte prüft. Vordel's Technologie wurde beständig als die Nr. 1 gewertet und war um den Faktor 10 besser in den geprüften Performance und Skalierbarkeit Tests.

Vordel's Kundenbasis bildet fast alle Branchen und Geographien ab. Wir sind global lieferfähig mit großen internationalen System Integratoren wie Accenture und Deloitte, oder mit regionalen Partnern, wie z.B. die MT-AG oder IC-Consult. Unsere strategischen Partner, Oracle und CA, haben ebenso ihr eigenes Vertriebs und Integrationsnetzwerk.



Contact us at: info@vordel.com
Learn more at: www.vordel.com
Follow us at: twitter.com/vordel

vordel
Applications Anywhere

Die Einordnung des Oracle Enterprise Gateway in die Oracle Middleware Landschaft

Das Oracle Enterprise Gateway (OEG) wird in der Oracle Referenz Architektur als „First Line of Defence“ für SOA basierte Architekturen aufgestellt.

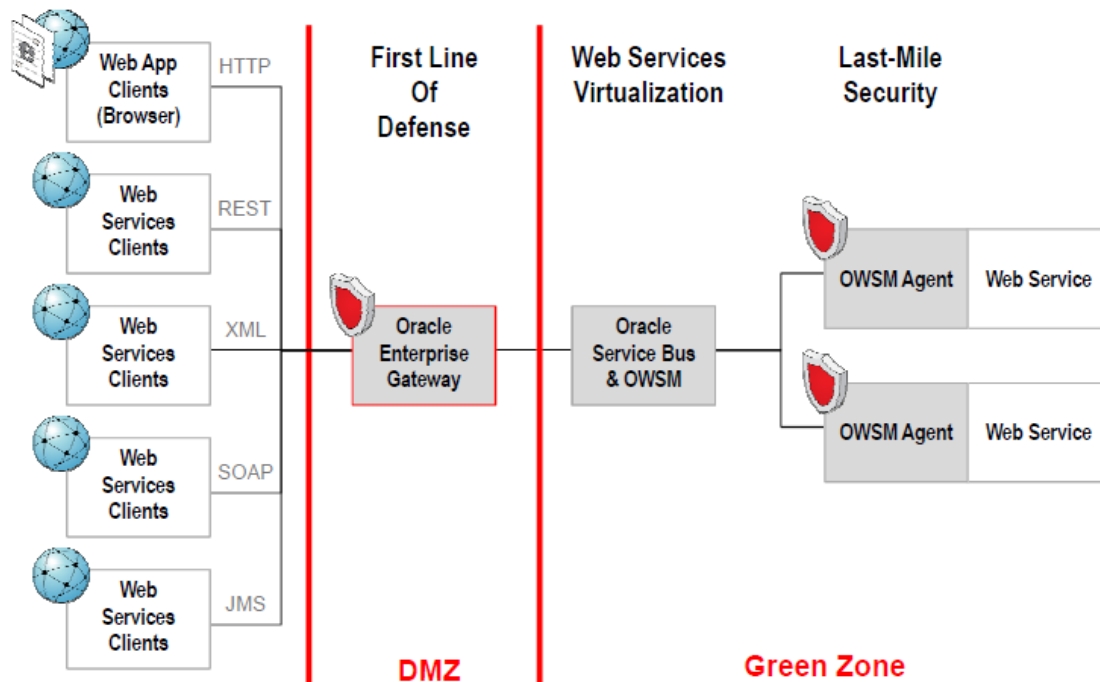


Abbildung 1: Oracle Referenz Architektur OEG

Damit ergeben sich folgende Aufgabenfelder für das OEG:

XML Firewall

In der Funktion der XML-Firewall prüft das Gateway die einkommenden Nachrichten auf die potentiell schadhafte Inhalte, wie SQL-Injection, XPath-Injections, rekursiv definierte XML Schemata und vieles mehr. Auch kann hier einen möglichen DoS Angriff ein Riegel vorgeschoben werden. Ebenso können SOAP Attachments an einen Virenschanner zur Prüfung weitergeleitet werden.

Security basiertes Routing

In vielen Fällen müssen die eingehenden Nachrichten schon in einer frühen Phase der Kommunikation an die unterschiedlichsten Ziele weitergeleitet werden. Speziell im Kontext „Security“ haben wir im Gateway die Möglichkeit Zertifikate oder deren Inhalte als Basis für ein Routing an unterschiedliche Backend Services zu nutzen.

Authentifizierung der Clients und User

Eine der Hauptaufgaben eines Gateways ist die schnelle und korrekte Authentifizierung des Clients bzw. des Users hinter der Nachricht. Dazu gibt es im Webservice Umfeld diverse Standards wie WS-Username Token, SAML oder auch OAuth. Das OEG unterstützt alle derzeit gültigen Standards. Mit seiner Möglichkeit sich an verschiedenste IDM Systeme (wie der Oracle Access Manager, LDAP und Datenbank gestützten Userstores, ...) anzubinden und sie als Basis für die Authentifizierung zu nutzen, zeigt das Gateway hier seinen größten Wert in der Implementierung von Sicherheit.

Autorisierung der Zugriffe auf Webservices bzw. SOAP-Actions

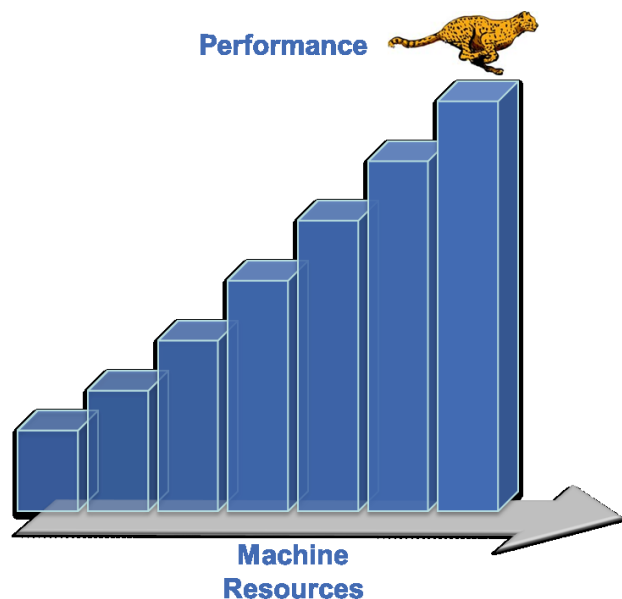
Ein weiterer Schritt zu einer möglichst sicheren Nutzung von Webservices ist die Autorisierung von Webservice Operationen in einer frühen Phase der Kommunikation. Hier kann das OEG, z.B. in Verbindung mit dem Oracle Entitlement Server, eine hoch performante Prüfung realisieren und Zugriffe erlauben oder ablehnen.

Sicherheit basierte Content Filterung

Während die bis jetzt angesprochenen Use Cases sich mit dem Annehmen und Weiterleiten von Nachrichten im Webservice Kontext beschäftigen ist das Content Filtering auf Basis von XSLT und anderen Mechanismen auch geeignet, die Sicherheit der ausgehenden Nachrichteninhalte zu gewährleisten. Durch einen super schnellen XML Parser und XML Transformation Engine ist das Gateway hier in der Lage auch große Datenmengen in einer adäquaten Zeit zu prüfen. Im Focus steht dabei, dass nur Nachrichten in sinnvollen Größenrahmen und mit geprüftem Inhalt wieder an den Client zurückgesandt werden. Sollte sich in einer Prüfung herausstellen das, zu viel und/oder falsch deklariertes Inhalt existiert, kann das Gateway die Weiterleitung verhindern und eine entsprechende Fehler bzw. Alarm Meldung generieren.

Der Performance Gewinn für die gesamt Architektur durch das OEG

Ziel des Einsatzes eines Oracle Enterprise Gateway (OEG) ist es, geforderte oder auch gewünschte Sicherheitsregeln für die Nutzung von Webservices zu implementieren ohne eine Einbuße in der End-to-End Performance zu bekommen. Das OEG nutzt in den oben aufgezeigten Aufgabenstellungen den einzigartigen XML Engine um die verschiedene XML bezogenen Prüfungen und Regeln mit höchster Performance abzuarbeiten. Durch eine enge Zusammenarbeit mit dem Chip Hersteller Intel wurde patentierte VXA Architektur geschaffen und optimiert. Hieraus ergibt sich eine hervorragende Skalierbarkeit mit den Maschinen Ressourcen (CPU & Memory). Die durch das Gateway entstehende Entlastung der dahinterliegenden Architekturelemente, wie ein Service Bus, JEE Server oder auch JMS Provider, resultiert in einer gleichbleibenden oder auch höheren Performance der Backend System. Zusammen mit dem Gateway kann sich daraus durchaus auch eine Steigerung der End-to-End Performance ergeben.



Darstellung der Performance durch das OEG in einer Demo

In der Demo des Vortrages wird ein typisches Einsatzszenario anhand von 2 Regelwerken für eine Webservice Security gezeigt.

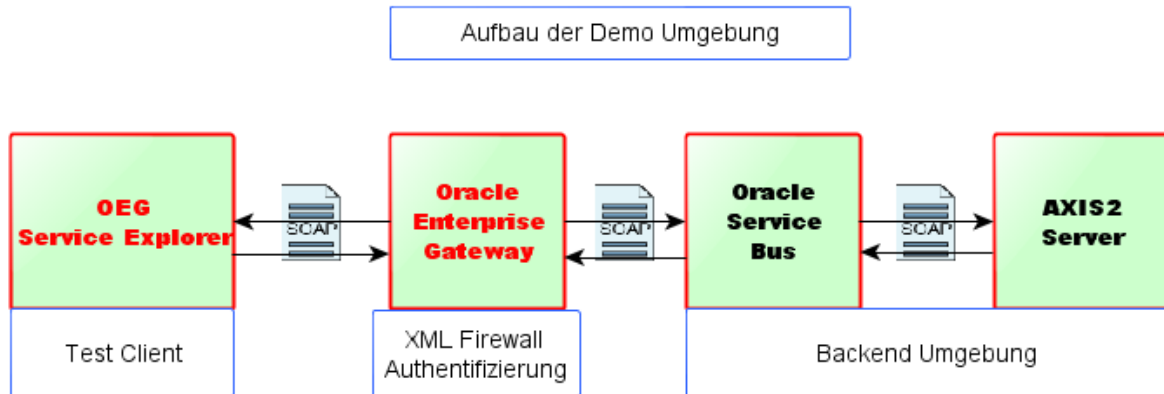


Abbildung 2: Demo Architektur

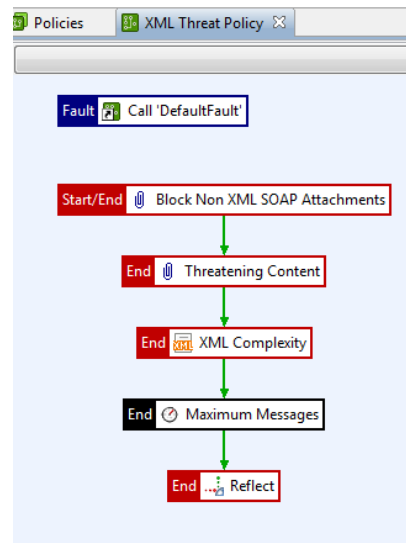
Dieses Szenario beinhaltet eine XML-Firewall Prüfung der eingehenden Nachrichten im OEG und eine anschließende Authentifizierung des Nachrichten Senders mittels eines WS-Username Token. Diese Regeln werden im OEG vor einem OSB ausgeführt. Der eigentliche Webservice „StockQuoteService“ wird von einem Axis2 Server zur Verfügung gestellt. Im Vortrag wird live gezeigt wie:

- ▶ Die Regel für die XML-Firewall erstellt wird.
- ▶ Die Regel für eine Authentifizierung gegen ein WS-Username Token erstellt wird.
- ▶ Der im OSB abgebildete Webservice in das Gateway eingebunden wird.
- ▶ Basierend auf dieser Struktur wird dann ein funktionaler Test wie auch ein Last Test gezeigt und die Ergebnisse diskutiert.

Ergebnisse des Belastungstests					
Zusammenfassung:		16 passes	0 failures		
Belastungstest	Bytes	Zeit(Ms.)	Exp. Code	Code...	Ergebnis
Stress Test Results					
SQS-only					
L4-100					
SendAs-admin	0	6422	200	200	pass
SendAs-admin	0	6423	200	200	pass
SendAs-admin	0	6514	200	200	pass
SendAs-admin	0	6880	200	200	pass
SendAs-vordel	0	3398	200	200	pass
SendAs-vordel	0	3305	200	200	pass
SendAs-vordel	0	3144	200	200	pass
SendAs-vordel	0	3579	200	200	pass
SQS-over-Gateway					
L4-100					
send as Admin	0	1380	200	200	pass
send as Admin	0	1747	200	200	pass
send as Admin	0	1745	200	200	pass
send as Admin	0	1761	200	200	pass
send as Vordel	0	1437	200	200	pass
send as Vordel	0	1257	200	200	pass
send as Vordel	0	1300	200	200	pass
send as Vordel	0	1289	200	200	pass

Abbildung 3: Last Test Ergebnis

Abbildung 4 XML-Firewall Regel



Die Seitenzahl wird von uns eingefügt!

Bitte fügen Sie Ihre Kontaktadresse hinzu.

Kontaktadresse:

Axel Grosse
Vordel Ltd.
Kaiserswerther Str ,115
D-40880 Ratingen

Telefon:	+49 (0) 177-70-75-788
Fax:	+49 (0) 2102-420-62
E-Mail	axel.grosse@vordel.com
Internet:	www.vordel.de