ORACLE API GATEWAY

Security and Management for SOA services and APIs

Oracle API Gateway is a standards-based, policy-driven, standalone software security solution that provides first line of defense in Service-Oriented Architecture (SOA) environments. It enables organizations to securely and rapidly adopt Cloud, Mobile and SOA Services by bridging the gaps and managing the interactions between all relevant systems.

Introduction

Companies worldwide are actively deploying SOA infrastructures using web services, both in intranet and extranet environments. While web services offer many advantages over traditional alternatives (e.g., distributed objects or custom solutions), deploying networks of interconnected web services still presents key challenges, especially in terms of security.

Web services can be implemented using different approaches which need to be secured at the different stages of the request / response cycle between clients (relying parties such as users or applications) and service providers (companies exposing web services).

Several security layers are defined between clients and web services providers. The first security layer, also known as “perimeter security” or “first line of defense,” is referred to as the demilitarized zone or DMZ. The second security layer, or “green zone” to continue with the military analogy, is located behind the inner firewall of the DMZ. In some cases, the green zone may include several security sub-layers designed to further filter access to web services. Finally, agents co-located with the web services or applications to be protected provide the last security layer, or “last-mile security.”

Oracle API Gateway is part of Oracle’s complete SOA security and Access Management solution.

Oracle’s SOA Security Solution

Oracle’s SOA security solution is build around a common, standards-based security model (WS-Policy). Oracle API Gateway first intercepts a request for a web service in the DMZ. If the request is accepted by Oracle API Gateway, it is passed on to Oracle Service Bus (OSB), which provides additional security (if necessary), web service endpoint virtualization, communication protocol mediation, and data format transformation. Finally, OSB redirects the
1.2, SwA, MTOM, Plain XML (POX),
REST, Web 2.0 (Ajax, JSON), UDDI,
WSdl

- **Transport Protocols**: TCP, HTTP 1.0 &
1.1, JMS, MQ, FTP, SFTP, SMTP, POP.
- **Security and Policy Model**: SSL, XML
Encryption, XML Signature, WS-Security
(SAML, Kerberos, Username, X.509
token profiles), WS-Policy, WS-
SecurityPolicy, WS-Trust, WS-
SecureConversation, WS-Addressing,
WS-RM, XACML, XKMS, PKCS#1,
PKCS#12, S/MIME, OAuth

request to the appropriate web service endpoint that is secured by an Oracle Web Services
Manager (OWSM) agent (last-mile security).

**Extending Enterprise Security to Mobile and Cloud Applications using OAG**

Oracle API Gateway (OAG) provides API security and management features including API
Key Management, OAuth, securing REST services and JSON support to help customers
extend the value to enable Cloud and Mobile use cases. In many cases, it extends Oracle’s
unique identity and access management platform and allows customers to securely bring
advanced mobile computing into the enterprise.

**Oracle API Gateway Use Case Scenarios**

<table>
<thead>
<tr>
<th>API Security</th>
<th>Threat Protection</th>
</tr>
</thead>
</table>
|              | • Deep content Payload inspection and threat prevention for XML,
|              | SOAP, REST, JSON   |
|              | • Validate HTTP parameters, REST query/POST parameters, JSON
data structures, XML schemas etc. |
|              | • Protect against cross-site scripting (XSS) and DoS attacks |
|              | • Support for HTTP basic, digest, SSL, Kerberos etc. |
|              | • Support for SAML, X.509 certificates, LDAP, OAuth, API Key
| Identity and Access | Authentication etc. |
| Control | • Unified Access Enforcement by extending authentication,
| | authorization and risk policies – native integration with Oracle
| | Access Manager, Oracle Entitlements Server, Oracle Directory
| | Services, CA Siteminder, RSA Access Manager, Microsoft Active
| | Directory, IBM Tivoli etc. |
| | • Any to any identity token conversions |
| Data Security | • Redaction and encryption of sensitive data in API traffic |

<table>
<thead>
<tr>
<th>API Management</th>
<th>Quality of Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• QoS monitoring, alerting and enforcement.</td>
</tr>
<tr>
<td></td>
<td>• Real-time and offline Performance monitoring</td>
</tr>
<tr>
<td></td>
<td>• Client oriented requests (client based policies and throttling)</td>
</tr>
</tbody>
</table>

| Transformations and | Routing based on client and device identity, message type, network
| Routing           | condition and geography |
|                  | Protocol bridging(e.g. REST to SOAP) and data transformations
|                  | (XML to JSON etc.) |

| Monitoring and Reporting | • Auditing and Logging |
|                         | • Real time monitoring and alerting |
|                         | • Analytics and usage statistics |
|                         | • Integration with Oracle Enterprise Manager |

**Contact Us**

For more information about Oracle API Gateway, visit oracle.com or call +1.800.Oracle1 to speak to an Oracle representative.

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other
warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any
liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by
any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of
Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through
X/Open Company, Ltd. 0410

SOFTWARE. HARDWARE. COMPLETE.