

## ORACLE ENTERPRISE GATEWAY

### KEY FEATURES

#### • XML Firewalling and Intrusion

**Detection:** Oracle Enterprise Gateway filters incoming web service request messages for XML Content Attacks (checking for XML well-formedness, XML document size, XPath and XQuery injection, SQL injection, XML encapsulation, XML viruses, scanning messages for sensitive content based on metadata or regular expression patterns, detecting XML bombs and XML clogging, scanning WSDL files); XML Schema and DTD Attacks (schema validation, checking for XML entity expansion and recursion, schema poisoning, recursive elements, jumbo tag-names, malicious “includes”); Cryptographic Attacks (checking for public key denial of service, replay attacks); SOAP Attacks (SOAP operation filtering, checking for rogue SOAP attachments (viruses and other); Communication Attacks (HTTP header and query string analysis, IP address filtering, traffic throttling).

• **XML Acceleration:** Processing offload from application servers on the network; patented engine designed to accelerate processing of essential XML security primitives.

• **Security:** Authentication; Authorization; Identity Federation; Confidentiality and Privacy (XML Encryption); Integrity and Non-Repudiation (XML Signature).

• **Policy Studio:** Policy management tool that allows an administrator to easily configure policies and settings to control and protect all deployed web services.

• **Policy Center:** Management of policy deployment across several instances of Oracle Enterprise Gateway.

• **Service Manager:** Web-based system administration tool to manage services and policies.

• **Service Monitor:** Report generation based on the usage metrics of all Oracle Enterprise Gateway instances (in Oracle environments, Oracle Enterprise Gateway integrates closely with Oracle Enterprise Manager for monitoring activities).

*Oracle Enterprise Gateway is a standards-based, policy-driven, standalone software security solution that provides first line of defense in Service-Oriented Architecture (SOA) environments.*

### Introduction

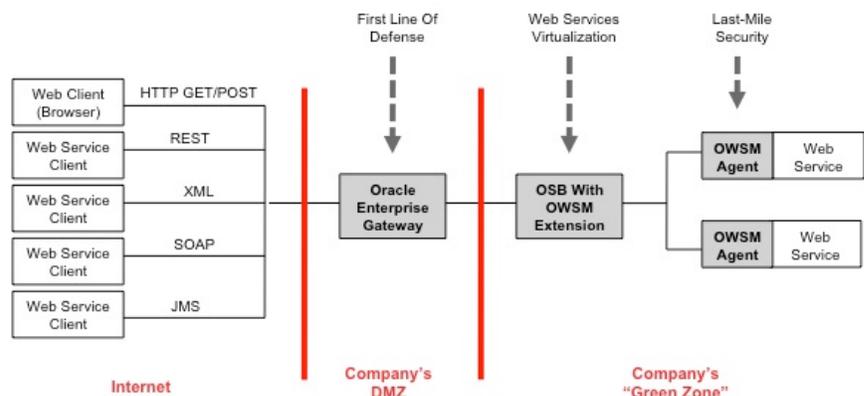
Companies worldwide are actively deploying SOA infrastructures using web services, both in intranet and extranet environments. While web services offer many advantages over traditional alternatives (e.g., distributed objects or custom solutions), deploying networks of interconnected web services still 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’s SOA Security Solution

Oracle Enterprise Gateway is part of Oracle’s complete SOA security solution.



Oracle’s SOA security solution is built around a common, standards-based security model (WS-Policy). Oracle Enterprise Gateway first intercepts a request for a web service in the DMZ. If the request is accepted by Oracle Enterprise 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 request to the appropriate web service endpoint that is secured by an Oracle Web Services Manager (OWSM) agent (last-mile security).

- **Administration Interface:** Web-based tool allowing management of Oracle Enterprise Gateway (IP address of each gateway instance, DNS, SSH, system users, etc.).

#### KEY BENEFITS

- **Ease of Installation:** Oracle Enterprise Gateway is delivered as a single software package running on multiple operating systems (MS Windows, Oracle Solaris, Linux).
- **Flexible Deployment:** Oracle Enterprise Gateway can be deployed in your data center, in the Cloud (e.g., Amazon EC2), or in hybrid (in-house and Cloud) environments.
- **High Level of Integration:** Oracle Enterprise Gateway is fully integrated with Oracle Identity Management, Oracle SOA Suite, Oracle SOA Governance, and Oracle Enterprise Manager.
- **Fast and Scalable:** Patented XML acceleration engine, harnesses multi-core CPU power.

#### STANDARDS SUPPORTED

- **Web Services Protocols:** SOAP 1.1 & 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, TIBCO RV, TIBCO EMS, 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#7, PKCS#12, S/MIME.
- **Support for Hardware Security Modules (HSM)** through PKCS#11 and OpenSSL.

## Oracle Enterprise Gateway Use Case Scenarios

Oracle Enterprise Gateway can be used as a standalone solution in heterogeneous environments. However, customers will get the most benefits when using Oracle Enterprise Gateway with other Oracle solutions.

**Integration with Oracle Identity Management:** Oracle Enterprise Gateway leverages Oracle directory services and directory virtualization for authentication and authorization.

**Integration with Oracle Entitlement Server:** Fine-grained authorization based on content (SAML attributes, SOAP or HTTP headers), or based on context (client IP address, time of day).

**Integration with Oracle Security Token Service (STS):** Oracle Enterprise Gateway acts as a client to Oracle STS for requesting the validation and conversion of security tokens.

**Adding XML identity attributes** leveraging the database when the web service endpoint requires attributes not passed in the original client request (Oracle Enterprise Gateway can also leverage directory services for the same purpose).

**Identity propagation:** Oracle Enterprise Gateway integrates natively with Oracle Web Services Manager (they share the same policy model) to propagate the identity of a requester across SOA composites (for example, BPEL and Mediator processes).

**Integration with Oracle Enterprise Manager** for service-level agreements (SLA) management, metrics (e.g., TPS, latency), and availability of Oracle Enterprise Gateway instances.

#### Client-Oriented Requests:

- Client-based policies for the same web service endpoint (e.g., Policy A for Client 1, Policy B for Client 2).
- Client-based throttling (e.g., allow 100 TPS for Client 1 and 250 TPS for Client 2).
- Client-specific SLA alarms.
- Hiding selected service operations from certain clients.
- Client identification through IP addresses, SAML attributes, SOAP / transport headers, identity attribute lookup after authentication (see “Adding XML identity attributes” above).

**Industry-Specific Use Cases:** Telecommunication and Service Delivery Platforms (Parlay-X support, throttling); Healthcare (HL7 support); Financial / Insurance (COBOL connectivity); Government (FIPS compliance).

## Contact Us

For more information about Oracle Enterprise Gateway, visit [oracle.com](http://oracle.com) or call +1.800.ORACLE1 to speak to an Oracle representative.



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2011, 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.**