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.

KEY FEATURES

- ***API Security***: Threat Protection for XML, SOAP, REST and JSON, Identity and Access Control, API Key Management, Data level privacy and integrity, Content Payload inspection, Compliance.
- ***Centralized Cloud Connectivity:*** Proxy and Manage interactions with Cloud Services. Restrict, throttle and manage web services and REST APIs.
- ***API Management for Mobile and Cloud:*** Connect mobile devices to enterprises. Map between data formats such as XML and JSON.
- ***Policy Studio***: Policy management tool that allows enables policy developers to easily configure API Gateway policies and settings to control and protect deployed API services and Web services.
- ***API Explorer***: API Explorer is an API service and Web service test client used by policy developers to generate test messages, which are sent to the API Gateway and back to API Explorer. API Gateway Explorer supports both REST-based and SOAP-based invocations.
- ***API Gateway Analytics***: Oracle API Gateway Analytics is used by administrators to generate reports and charts based on usage metrics for all services and API Gateways.
- ***Administration Interface***: Web-based tool allowing management of Oracle API Gateway (IP address of each gateway instance, DNS, SSH, system users, etc.).

KEY BENEFITS

- ***Secure APIs used for Mobile and Cloud deployments***
- ***Secure Web Services and SOA deployments***
- ***Extend authentication, authorization and risk policies to mobile, cloud and enterprise applications – without changing backend applications***
- ***Provide data governance***

STANDARDS SUPPORTED

- ***Web Services Protocols***: SOAP 1.1 &

Introduction

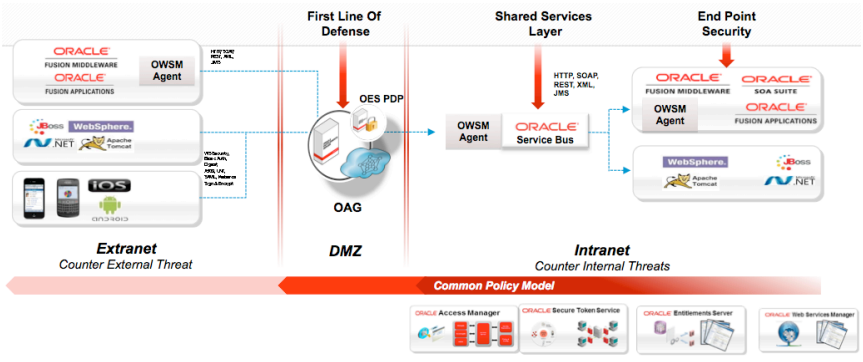
Companies worldwide are actively deploying SOA infrastructures using web services, both in intranet and extranet environments. While web services offer many advantages over traditional alternatives (e.g., distributed objects or custom solutions), deploying networks of interconnected web services still 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#7, 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

API Security	
Threat Protection	• 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
Identity and Access Control	• Support for HTTP basic, digest, SSL, Kerberos etc. • Support for SAML, X.509 certificates, LDAP, OAuth, API Key Authentication etc. • 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
API Management	
Quality of Service	• QoS monitoring, alerting and enforcement. • Real-time and offline Performance monitoring • Client oriented requests (client based policies and throttling)
Transformations and Routing	• Content and Context based routing • Routing based on client and device identity, message type, network 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.

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

SOFTWARE. HARDWARE. COMPLETE.

ORACLE