

## FORUM SYSTEMS AND ORACLE

**ORACLE®**



## SECURE SOA INFRASTRUCTURE

TECHNICAL WHITE PAPER

Forum Systems, Inc.

BOSTON, MA  
95 Sawyer Road, suite 110  
Waltham, MA 02453

SALT LAKE CITY, UT  
45 West 10000 South, suite 415  
Sandy, UT 84070

TOLL FREE  
1-866-333-0210

[WWW.FORUMSYSTEMS.COM](http://WWW.FORUMSYSTEMS.COM)



## TABLE OF CONTENTS

THE SERVICE ORIENTED ENTERPRISE . . . . .	3
THE SOA THREAT PROFILE . . . . .	4
SOA SECURITY BEST PRACTICES . . . . .	4
FORUM SERVICE ORIENTED SECURITY SOLUTIONS . . . . .	6
INTELLIGENT XML MALWARE PROTECTIONS . . . . .	6
ADAPTIVE HARDWARE AND SOFTWARE . . . . .	6
HARDENED SECURITY ASSURANCE . . . . .	6
ORACLE COREID ACCESS & IDENTITY . . . . .	7
FORUM XWALL WEB SERVICES FIREWALL . . . . .	8
FORUM AND ORACLE INTEGRATION . . . . .	9
SCALABLE SOA DEPLOYMENTS . . . . .	10
EVENT AND MESSAGE BASED SOAs . . . . .	11
ORACLE WEB SERVICES MANAGEMENT AND FORUM XWALL . . . . .	12
CONTACTS . . . . .	13

© 2005 Forum Systems Inc. All Rights Reserved.

Release Date: 09/01/2005





## THE SERVICE ORIENTED ENTERPRISE

Service Oriented Architectures (SOAs) create fundamental changes in application architecture, service design, development practices as well as operational management and governance. The reason for such deep-rooted change is that SOA applications have the following distinctive characteristics:

1. Modular software that communicates using eXtensible Markup Language (XML)
2. Service-to-service interactions that work on behalf of, or instead of, users
3. User rights that are delegated to federated Web services
4. Reusable and loosely coupled processes and software that are invoked

Industry wide SOA rollouts have seen enterprises deploy critical supporting infrastructure around Web services security and Web services management. Forum Systems and Oracle Corporation “Secure SOA Infrastructure” is a market-leading solution that integrates software and hardware for mission-critical SOA deployments.

### FORUM AND ORACLE SECURE SOA INFRASTRUCTURE

#### Web Services and SOA Security

- Application-to-application security mechanisms
- Data at rest protection, end-to-end security context
- XML-vectored malicious attack prevention
- High performance data and protocol mediation

#### Web Services and SOA Management

- Business requirements modeling to drive SOA rollout's
- Enterprise-wide SOA policy management
- SLA's, handle exceptions, enable real-time business intelligence
- Metadata to store services, specifications, and provisioning



## THE SOA THREAT PROFILE

Since all clients and service/resource providers participating in a SOA setting have to install some sort of XML component, hackers and malicious users are free to discover vulnerabilities resident in XML parsers, WSDL<sup>1</sup> end-points and SOAP<sup>2</sup> processors. More over, client/server and Web application security controls were not designed for a threat profile brought on by a constantly evolving set of XML-related specifications. The limitations in traditional security controls lies in their inability to inspect and act upon machine-to-machine interactions that use XML, SOAP and the WS - OASIS<sup>3</sup> standards.

The new threats that emerge within a SOA environment include:

- **Parameter Tampering:** Manipulated XML values are used to conduct fraudulent transactions
- **Coercive Parsing:** Corrupted XML/SOAP messages are used to disrupt and disable unprepared and vulnerable services
- **Recursive Payload:** Deeply nested XML documents are constructed to exhaust computing resources
- **WSDL Scanning:** Business API's are probed for sensitive data and vulnerabilities
- **External Entity Attacks:** External references can be made to import compromised data
- **SOAP Routing Detours:** Messages are re-directed to malevolent processing intermediaries
- **SOAP with malicious software:** SOAP hides and obscures viruses, spyware and other unwanted programs
- **SQL Injections into SOAP:** SQL code is modified and left undetected because it is embedded in XML
- **WS-Security Spoofing:** SOAP security contexts are overridden to gain unauthorized data access

## SOA SECURITY BEST PRACTICES

Security must be integral to SOAs. SOA security must explicitly address XML data security requirements beyond transport and user protections. SOA security must support confidentiality, authentication, integrity, authorization and non-repudiation of service-to-service interactions using self-descriptive entitlements and attributes. SOA security must also address XML-related vulnerabilities to avoid impending threats.

To reduce on-going risk organizations must:

1. Define consistent security policies
2. Use an adaptive and agile approach to security
3. Deploy Secure SOA Infrastructure

---

<sup>1</sup> W3C Web Services Description Language

<sup>2</sup> W3C Simple Object Access Protocol

<sup>3</sup> Organization for the Advancement of Structured Information Standards (OASIS)



The following is a list of SOA security best practices:

- **Web Services and XML Security Standards:** Adoption of Open specifications of the World Wide Web Consortium (W3C), Organization for the Advancement of Structured Information Standards (OASIS) for the enforcement of confidentiality and integrity of Web services
- **XML Threat Prevention:** Deep inspection, validation, monitoring and filtering of Web services and XML transactions. Actively defending and avoiding against pattern and signature-recognizable XML-vectored attacks, intrusions and malicious software
- **Security Policy Management:** Management and the governance of rules must be derived from business, organizational and enterprise requirements. Centralized Policy Decision Points (PDP) as well as distributed policy Enforcement Points (PEP) need to be deployed
- **Authentication:** Verifying proof of an asserted identity; authentication should be facilitated and resolved using transport (e.g. SSL X.509 Certificates) as well as message-based protocols (e.g. SAML/WS-Security Assertions)
- **Identity Mapping:** Transforming an identity that exists in one domain to an identity within another domain
- **Authorization:** Resolving a policy based on access control decision.
- **Credential Conversion:** Provides mapping of one type of credential to another such as an X.509 Certificate to a Kerberos/WS-Security token
- **Trust Delegation:** Bridging the differences between mechanisms associated with authentication, assertions and entitlements to enable a federated trust model
- **Audit:** Tracking, monitoring and reporting of security related events
- **Privacy:** Policy driven enforcement of personally identifiable information using both transport (e.g. SSL session encryption) as well message-based protocols (e.g. XML-Encryption)
- **Safe and Secure Cryptography:** Private keys and passwords once compromised void the trust model that depends on them. A secure SOA must offer robust and tamper resistant storage of private keys, passwords and algorithms.
- **Vulnerability Management and Risk Assessment.** Organizations should actively look at flaws and weaknesses in SOA design and implementation to pre-empt potential threats.



## FORUM SERVICE ORIENTED SECURITY SOLUTIONS

Forum Systems' SOA life-cycle security solutions enable trust management, threat protection and information assurance of XML, Web Services and Service Oriented Architectures. The following sections describe Forum's market-leading capabilities that are deployed within the world's largest and most discerning telecommunications, financial services, e-retail, and US Federal Government organizations.

### INTELLIGENT XML MALWARE PROTECTIONS

Analysts project XML-based network traffic will grow from 15 percent in 2004 to almost 50 percent in 2008. This explosive growth has opened the door for virus writers to bypass firewalls and anti-virus scanners that cannot recognize XML's data format and security context. Forum Systems was the first to introduce XML malware protection against XML-vectored viruses, worms and unwanted programs.

- Real-time XML virus and malware scanning
- Automatic anti-virus updates
- SOAP with binary attachment processing (DIME and MIME)

### ADAPTIVE HARDWARE AND SOFTWARE

SOA security aspects must be considered at the edge of the network within the datacenter as well as at end-points and application containers. Forum Systems offers organizations the flexibility to mix hardware and software where they are needed for the most effective security at the lowest cost of ownership.

- Hardware: 1U Appliance, IBM eBlade, PCI cards, x32-bit, x64-bit
- Third-Party Platforms: Microsoft ISA Server 2004, CrossBeam, NetContinuum, Network Engines
- Software: Windows, Linux, IBM AIX, Sun Solaris, Sun Trusted Solaris

### HARDENED SECURITY ASSURANCE

FIPS (Federal Information Processing Standard) is a US Government certification program that prescribes detailed security requirements for cryptographic-based systems when used within US Federal agencies. In sensitive SOA settings, security policies need to be processed inside FIPS 1402- Level II certificated enclosures from the hardware chassis, cryptographic modules, motherboard and interfaces.

- FIPS 140-2 Level III Key Management
- Full Appliance Chassis FIPS 140-2 Level II Validation
- DoD/PKI Certification
- Common Criteria EAL 4+



## ORACLE COREID ACCESS & IDENTITY

*Access and identity are the means for administering users and their privileges in addition to controlling their access to enterprise resources.*

Oracle COREid Access and Identity is a complete solution for user identity and profile management, single sign-on, and access control:

- Oracle COREid Identity
- Oracle COREid Access Manager

**Oracle COREid Identity** provides the user and group with delegated administration and self-service functions necessary to manage large user populations in complex, real-world environments.

- **User, Group, and Organization Management.** Dynamically create groups based on user attributes.
- **Delegated Administration.** Unlimited capability to delegate user administration to managers and partners.
- **User Self-Service and Self-Registration.** Provide users with complete or restricted ability to manage profiles.
- **Unified Workflow.** Industry-leading workflow to manage the lifecycle of user data
- **Password Management.** Reduce help desk calls via password reset and self service.

**COREid Access Manager** is a graphical tool for creating and managing access policies, setting up resources to be protected and simulating user access to ensure correct policy functionality.

- **Web Single Sign-On.** Secure access to multiple applications with one password and user ID.
- **Flexible Authentication Methods.** Oracle COREid supports all popular methods including browser forms, digital certificates, smart cards, and more.
- **Policy-Based Authorization.** Flexible policy definition adapts to changing business needs.



## FORUM XWALL WEB SERVICES FIREWALL

*XML threat protection and Web Services Security (WS-Security) policy enforcement designed for XML, Web Services and Service Oriented Architectures.*

- Forum XML Threat Protection
- Forum WS-Security Policy Enforcement

**Forum XML Threat Protection** is a unified risk management solution with specialized risk analysis, threat detection and threat avoidance security countermeasures.

- **XML Intrusion Prevention.** Anomaly and signature based detection of XML-vectored threats with pre-configured security profiles and response mechanisms
- **XML Malware Scanning.** Allows administrators to arrest the propagation of viruses, Trojans, worms, spyware and unwanted programs embedded in XML and SOAP
- **Vulnerability Containment Service.** XML-related vulnerability metabase and alert notification system
- **Specialized risk analysis.** Threat discovery capabilities with Web services diagnostics for runtime and design time phases

**Forum WS-Security Policy Enforcement** hardware and software to enforce security policies as well as resolve cross-organizational trust agreements.

- **WS-Security 2004 1.1 Provider.** XML Encryption and Digital signature processing as well as Username, X.509, SAML, and Kerberos tokens
- **WSDL Admission Control.** Consume policies in order to verify the asserted identity and resolve access control decisions via a transport (e.g. SSL) or message-based protocols (e.g. SAML)
- **WS-Identity Processing.** Provides credential conversion from one type of credential to another form of credentials e.g. X.509 to Kerberos/WS-Security token. Transforms an identity that exists in one domain to an identity within another domain.
- **Protocol Mediation.** Broker policies, negotiate quality and translate application transport protocols. Support for mediating between messaging protocols including HTTP(s), IBM Websphere™ MQ, Tibco Rendezvous™, Tibco EMS™, SMTP, JMS and FTP as well as propagating credential and authentication assertions across protocols.



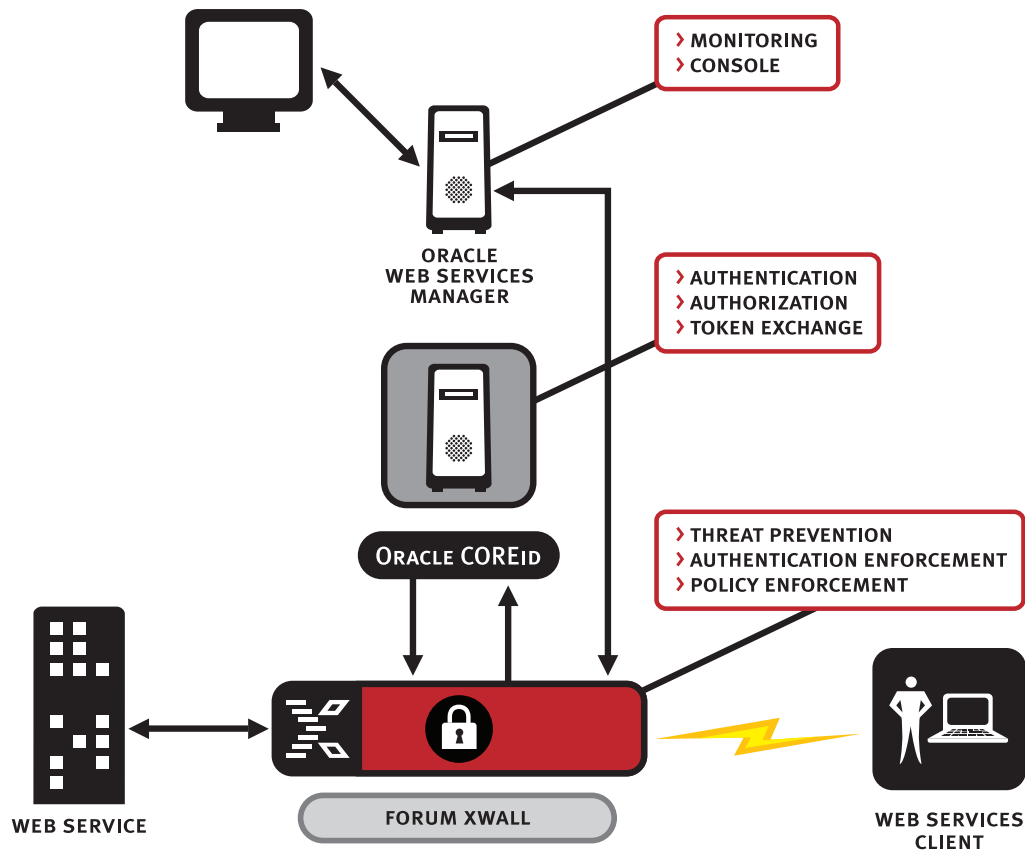
## FORUM AND ORACLE INTEGRATION

The following sections detail the integration between Forum Systems' XWall, Oracle's COREid and Oracle Web Services Manager.

Forum XWall is unique in its ability to inspect XML application requests and responses, determine risks and enforce policy-based security decisions. Forum XWall parses XML, WSDL-authored SOAP and WS-\* information and interrogates Oracle COREid for policy decisions.

Forum XWall complements Oracle COREid's identity management and policy administration to offer a best of breed solution for deploying secure Web services:

- Forum XWall is the Identity Enforcement Point to Oracle COREid which acts as the Identity Decision Point.
- Forum XWall leverages COREid for Authentication and Authorization decisions.
- Forum XWall protects against XML-related threats such as XML viruses, denial of service attacks and intruders that use XML to gain unauthorized access to data
- Oracle Web Services Manager oversees the operations of Web services interactions including aggregating, monitoring and acting on specific events

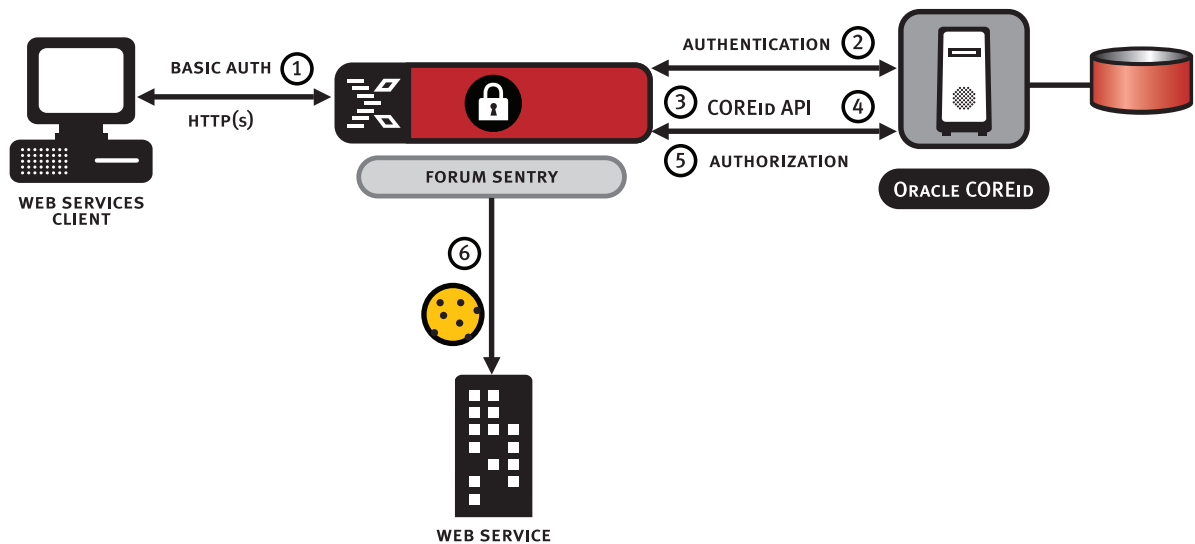




## SCALABLE SOA DEPLOYMENTS

SOAs involve distributed client interactions, high message rates and concentrated compute requirements as a result of verbose XML, SOAP and WS-\* traffic. High performance and dedicated policy enforcement points that are able to negotiate and resolve policy decisions a proven and scalable design pattern.

The diagram below illustrates a typical deployment topology between Forum and Oracle secure SOA products.



1. Web Service client requests proxy through the Forum XWall [Software or Appliance] using HTTP Basic Authentication to pass their credentials (username/password) over HTTP or HTTP(S). The Forum XWall appliance contains dedicated chips sets (ASIC) to accelerate SSL sessions.

2. The payload of the request is parsed and inspected for malicious content. The administrator has the option, based on threat-levels, to invoke an XML Schema validation. XML virus detection or any of the available XML intrusion prevention rules.

3. The XWall Appliance receives the Web Service request and terminates the SSL connection if the request was sent using HTTPS. The XWall Appliance is able to accelerate SSL terminations and initiations via onboard cryptographic hardware. The HTTP Basic Authentication credentials are passed to the COREid Server via the COREid Access SDK APIs and then signaled to look up the user profile attributes in an LDAP Server.

4. COREid responds back to the XWall Appliance whether the credentials were valid or not.

5. The XWall Appliance allows or rejects requests based on the COREid Servers response. If the request is allowed to proceed, XWall sends an authorization request with credentials to COREid to see if the Authenticated user has access to the requested resource.



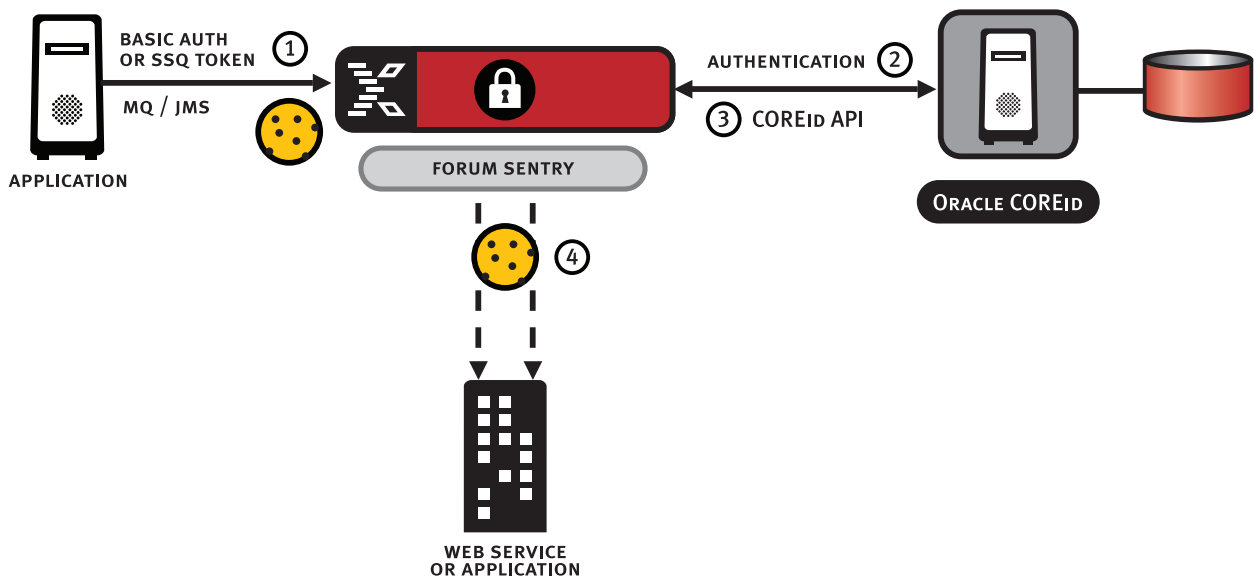
6. COREid determines if the user has access to the requested resource and responds back to the XWall Appliance whether the authorization request was valid and returns an SSO token cookie.

7. If the Authorization request succeeds, the XWall Appliance forwards the Web service request to the Web Service with a valid COREid SSO token cookie

If the Web Service client has been previously authenticated with COREid Server, then the client request presents XWall with a previously acquired COREid SSO token cookie. This is then presented to COREid in the Authentication call to ensure sure it is still valid. If the message is allowed to proceed, XWall sends an authorization request with the COREid SSO token cookie to COREid server to see if the Authenticated user has access to requested resource.

### EVENT AND MESSAGE BASED SOAs

While HTTP is a popular transport protocol, certain business requirements require the advantage of asynchronous communications. The protocol and data transformation capabilities of Forum XWall make it ideal as a queue mediation point between endpoints and clients. The Forum XWall can authenticate Basic Authentication credentials or Oracle COREid SSO token cookies included in a message queue protocol (e.g. IBM WebSphere MQ). Recognizing that the end point requires credentials to be presented within the message payload Forum XWall can place the COREid SSO token in the outbound message and route the message to the appropriate message queues. Forum XWall supports protocol mixing so the outbound message could be another message queue protocol or converted to HTTP(s), FTP or SMTP.



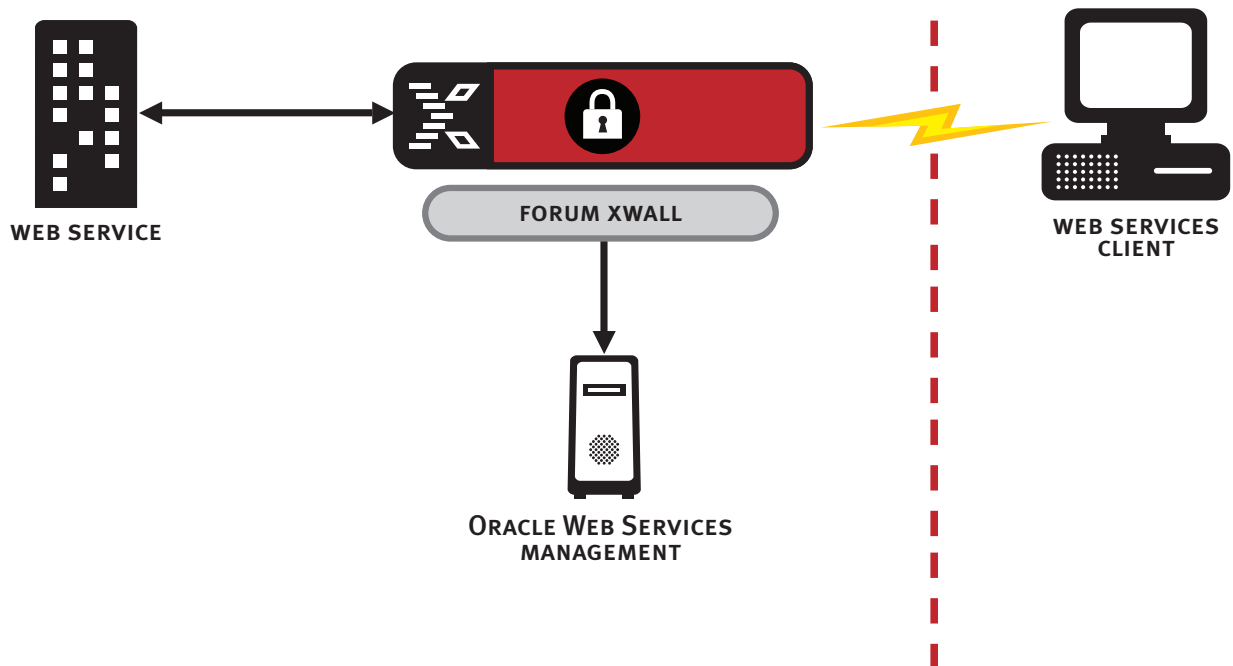


## ORACLE WEB SERVICES MANAGEMENT AND FORUM XWALL

Oracle Web Services Manager is a comprehensive solution for adding policy-driven best practices to all your existing or new Web services and provides the key security and management capabilities necessary to deploy Service-Oriented Architectures across your line-of-business applications.

Forum XWall can be configured to provide Oracle Web Services Manager real-time information including the following:

- Auto-Discovery of Web Services
- Service Latency Measurements
- Extensive Monitoring
  - Request Success/Failures
  - IDP Rules Violations
  - Authentication & Authorization including Identities
  - Errors





## **CONTACTS**

Walid Negm  
Vice President of Marketing  
Forum Systems Inc.  
[wnegm@forumsys.com](mailto:wnegm@forumsys.com)

Deepak Puri  
Vice President of Business Development  
Forum Systems Inc.  
[dpuri@forumsys.com](mailto:dpuri@forumsys.com)