INTEGRIGY

WHITE PAPER

Oracle E-Business Suite Mobile and Web Services Security

FEBRUARY 2017

ORACLE E-BUSINESS SUITE MOBILE AND WEB SERVICES SECURITY

Version 1.0 – February 2017

Authors: Mike Miller, CISSP, CISSP-ISSMP, CCSP, CCSK

If you have any questions, comments, or suggestions regarding this document, please send them via e-mail to info@integrigy.com.

The Information contained in this document includes information derived from various third parties. While the Information contained in this document has been presented with all due care, Integrigy Corporation does not warrant or represent that the Information is free from errors or omission. The Information is made available on the understanding that Integrigy Corporation and its employees and agents shall have no liability (including liability by reason of negligence) to the users for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on the information and whether caused by reason of any error, negligent act, omission or misrepresentation in the Information or otherwise. Furthermore, while the Information is considered to be true and correct at the date of publication, changes in circumstances after the time of publication may impact on the accuracy of the Information. The Information may change without notice.

Table of Contents

Overview

Securing packaged software such as the Oracle E-Business Suite presents different challenges than securing bespoke custom software. Unlike custom software, both the structure of and the security vulnerabilities of the Oracle E-Business Suite are well known and documented, not only to users but also to threat actors. To begin an attack, limited probing and/or reconnaissance is needed because threat actors know exactly what to target and what to expect. This also makes the Oracle E-Business Suite, like other ERP platforms, vulnerable to automated attacks. Threat actors only need to compromise one publically facing URL or web service, which given the size and complexity of the Oracle E-Business Suite, makes securing it a somewhat daunting task.

Starting with version 12.1 and continuing with 12.2, the Oracle E-Business Suite delivers a considerable amount of new web services and Mobile functionality as standard core functionality. Much, if not most, of this new Mobile and web services functionality, replicates functionality previously only available through the traditional user interface forms and/or public interfaces and these new web services can be easily deployed on the Internet through a DMZ node. The security implications of 12.2's increased web services capabilities is that the Oracle E-Business Suite's attack surface has increased and harder to defend.

This paper will summarize the new Mobile and web services functionality and review their security features before recommending best practices for using them securely.

Audience and How to Read This Paper

The intended audience are Oracle E-Business Suite DBAs, application administrators, IT security staff, and internal audit staff. A working technical knowledge of the Oracle E-Business Suite and Oracle Databases is recommended.

Oracle E-Business Suite Versions

The information in this guide is intended for and based on the Oracle E-Business Suite R12 (12.2). All the information and guidance should also be applicable to and be relevant for previous and future versions of the Oracle E-Business Suite, including but not limited to 11.5.x (11i) and 12.1.

ORACLE 12.2 WEB SERVICES ARCHITECTURE

Approximately 2,900 web services are created with an update to or installation of 12.2 and are defined in the table APPLSYS.FND_IREP_CLASSES. Within the Oracle E-Business Suite's user interface, the Integrated SOA Gateway (ISG) module is used to deploy the web services defined in APPLSYS.FND_IREP_CLASSES. Key to understanding the 12.2 web services architecture is that ALL web services are defined in the Service Oriented Architecture (SOA) Gateway, this includes both Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) web services.

The E-Business Suite's Mobile and smartphone applications are deployed internally as REST services and are likewise defined in the Integrated SOA Gateway and stored in the table APPLSYS.FND_IREP_CLASSES. The graphic below depicts the addition of web services and helps to visualize the increased attack surface that needs to be secured.

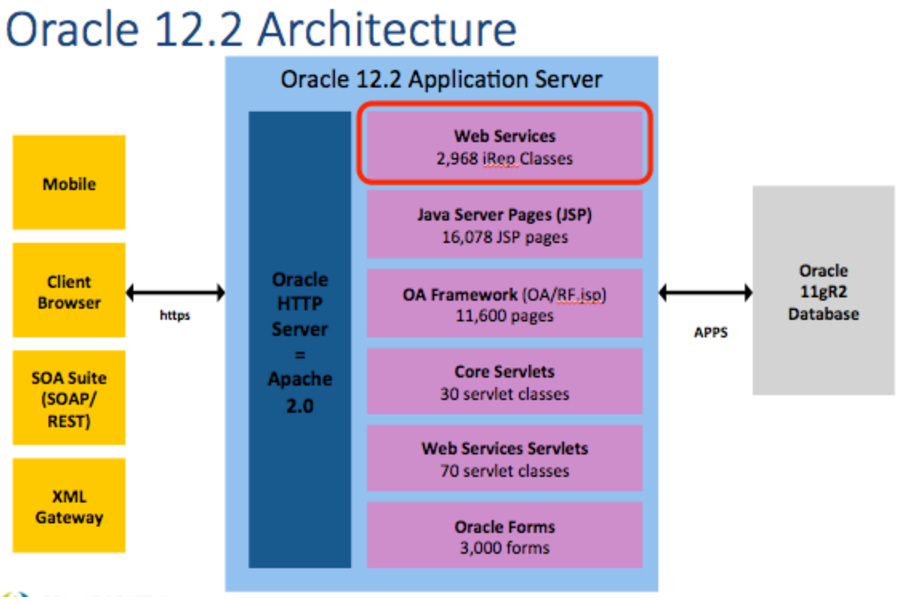
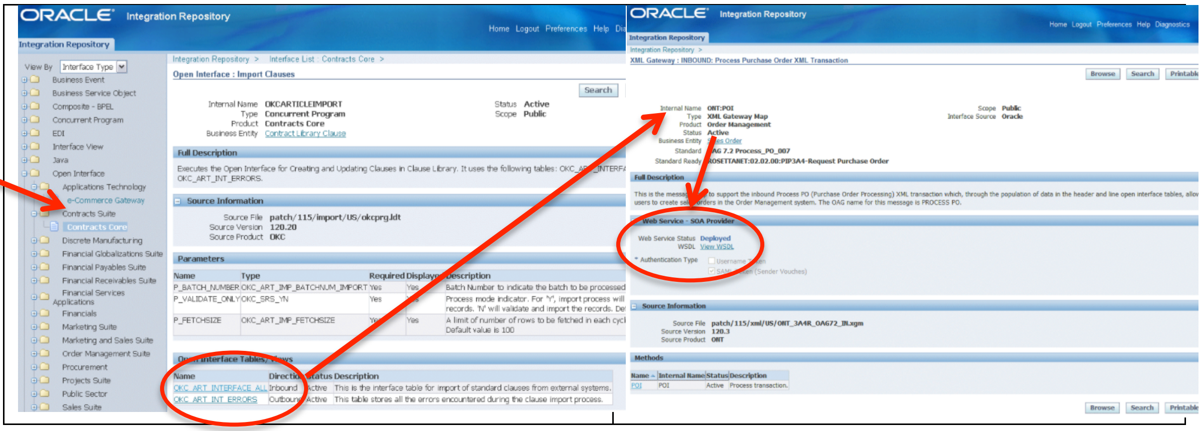


Figure 1 - Oracle 12.2 Architecture

DEPLOYING WEB SERVICES

Web services are physically deployed differently depending on whether they are defined using Representational State Transfer (REST) or Simple Object Access Protocol (SOAP). Logically, however, both REST and SOAP web services are deployed from within the Integrated SOA Gateway (ISG). Refer to the E-Business Suite's documentation for details, but from within the Integrated SOA Gateway, users can deploy web services by locating the particular web service and then clicking on the "Deploy" button.



Open Interface : Import Clauses

Internal Name OKCARTICLEIMPORT
Type Concurrent Program
Product Contracts Core
Business Entity Contract Library Clause
Status Active
Scope Public

Full Description

Executes the Open Interface for Creating and Updating Clauses in Clause Library. It uses the following tables: OKC_AR_INTERFA
OKC_ART_INT_ERRORS.

Source Information

Source File patch/115/import/US/okcprg.ldt
Source Version 120.20
Source Product OKC

Parameters

Name	Type	Required	Displayed	Description
P_BATCH_NUMBER	OKC_ART_IMP_BATCHNUM_IMPORT	Yes	Yes	Batch Number to indicate the batch to be processed
P_VALIDATE_ONLY	OKC_SRS_YN	Yes	Yes	Process mode indicator. For 'Y', import process will records. 'N' will validate and import the records. De
P_FETCHSIZE	OKC_ART_IMP_FETCHSIZE	Yes	Yes	A limit of number of rows to be fetched in each cycl Default value is 100

Open Interface Tables/Views

Name	Direction	Status	Description
OKC_ART_INTERFACE_ALL	Inbound	Active	This is the interface table for import of standard clauses from external systems.
OKC_ART_INT_ERRORS	Outbound	Active	This table stores all the errors encountered during the clause import process.

ORACLE Integration Repository
Home Logout Preferences Help Diagnostics
Integration Repository
Integration Repository >
Browse
Search
Printable

XML Gateway : INBOUND: Process Purchase Order XML Transaction

Internal Name ONT:POI
Type XML Gateway Map
Product Order Management
Status Active
Business Entity Sales Order
Standard OAG 7.2 Process_PO_007
Standard Ready ROSETTANET:02.02.00:PIP3A4-Request Purchase Order
Scope Public
Interface Source Oracle

Full Description

This is the message to support the inbound Process PO (Purchase Order Processing) XML transaction which, through the population of data in the header and line open interface tables, allow
users to create sales orders in the Order Management system. The OAG name for this message is PROCESS PO.

Web Service - SOA Provider

Web Service Status Deployed
WSDL View WSDL
* Authentication Type □ Username Token
☑ SAML Token (Sender Vouches)

Source Information

Source File patch/115/xml/US/ONT_3A4R_OAG72_IN.xgm
Source Version 120.3
Source Product ONT

Methods

Name	Internal Name	Status	Description
POI	POI	Active	Process transaction.

Figure 2 - Integrated SOA Gateway

REST-BASED WEB SERVICES

Physically deploying REST services with 12.2 is straightforward. REST is an architectural style and not a protocol and is best used to support lightweight and “chatty” interfaces such as Mobile applications. With 12.2, REST Web Application Description Language (WADL) interface definition files are generated within the E-Business Suite's WebLogic server and run through the OAFM Application. The OAFM application created with the installation of the Oracle E-Business Suite.

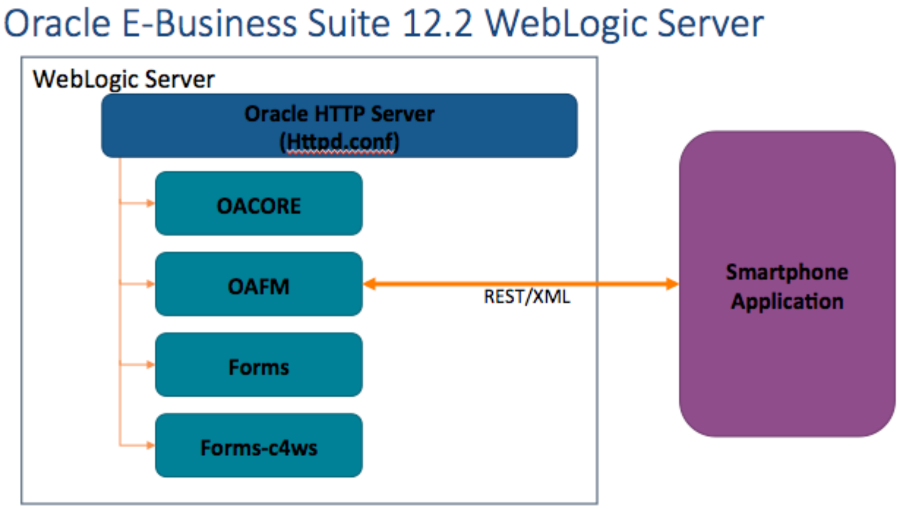


Figure 3 - REST Services are run through OAFM

SOAP-BASED WEB SERVICES

Physically deploying SOAP-based web services for the Oracle E-Business Suite is more complicated than for REST. SOAP interfaces are best used to support heavy-duty solutions such as Business-to-Business (B2B) interfaces. To deploy SOAP services for the Oracle E-Business Suite, the Oracle SOA Suite must be licensed and configured. Once the SOA Suite is installed and configured, two (2) WebLogic servers will exist. The first WebLogic server is the initial WebLogic server supporting the Oracle E-Business Suite and the second WebLogic Server is the WebLogic server supporting the SOA Suite. Integration between the two WebLogic Servers is done through both through HTTP and the ISG client. The ISG client is installed on the SOA Suite's WebLogic server and uses Oracle's proprietary T3 protocol to do the majority of the heavy lifting for communication with the E-Business Suite.

When a SOAP service is deployed within the Integrated SOA Gateway forms in the Oracle E-Business Suite, the SOAP Web Services Description Language (WDSL) file defining the web service is generated on the second WebLogic Server, the SOA Suite WebLogic Server, not the E-Business Suite's WebLogic server. The interaction with B2B business partners using the web service then occurs between the Oracle SOA Suite and the business partner's servers. Ultimately the Oracle E-Business Suite generates or receives the information, but the Oracle E-Business Suite does not directly communicate with the B2B partners.

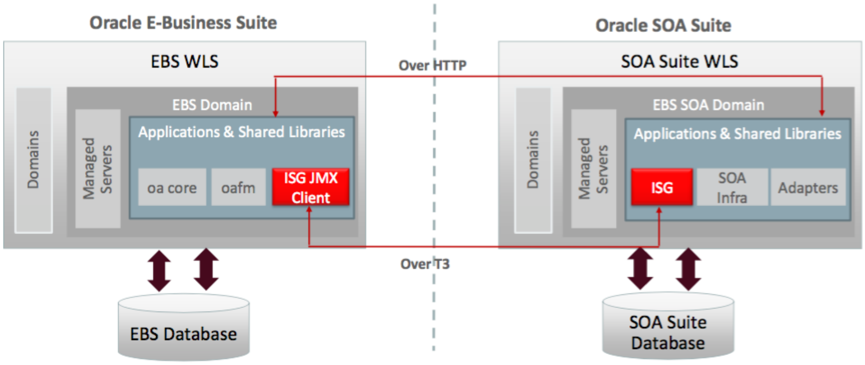


Figure 4 - SOAP Needs a Separate SOA Suite WebLogic Server

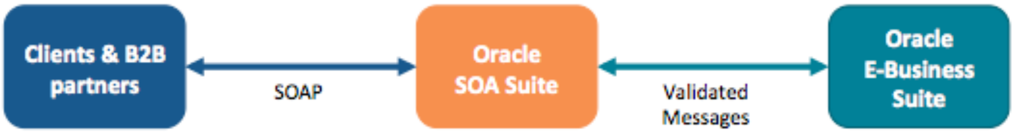


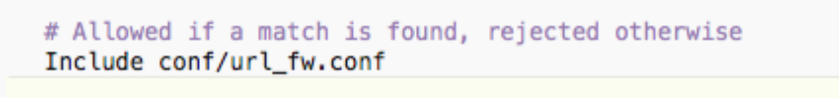
Figure 5 - Only the SOA Suite communicates with B2B clients

Web Services Security

How are web services secured in Oracle 12.2? To start at the beginning, the "front door" of the Oracle E-Business Suite is its web server, the Apache server deployed within the WebLogic server that is installed with release 12.2. To secure an Apache web server largely requires setting various configurations in the Apache configuration file (httpd.conf). For the Oracle E-Business Suite, these critical settings are maintained by Oracle through the AutoConfig utility.

URL FIREWALL

The most important setting for Internet-facing clients is the include for the Oracle E-Business Suite's URL Firewall. When the URL Firewall is included in the httpd.conf, every web request is passed through the URL Firewall, both for forms and for web services. The URL Firewall is non-discretionary and mandatory requirement when the Oracle E-Business Suite is deployed on the Internet.



```
# Allowed if a match is found, rejected otherwise
Include conf/url_fw.conf
```

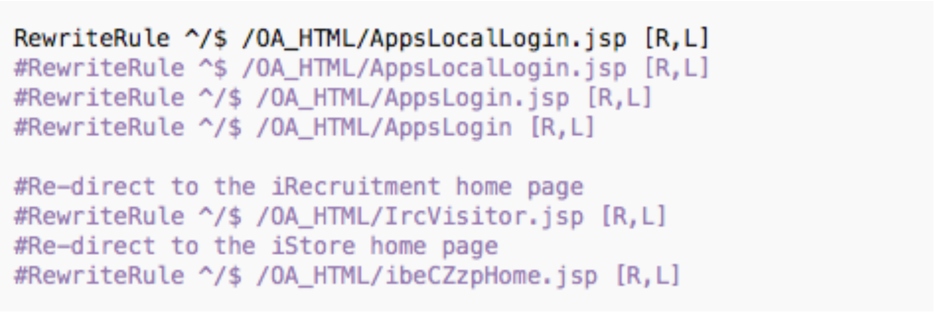
Figure 6 - HTTPD.CONF include for the URL Firewall

The URL Firewall is a template maintained by Oracle that whitelists those forms (e.g. JSP pages) that Oracle Corporation has hardened for use on the Internet. If the JSP is not listed "whitelisted" in the file url_fw.conf it should NOT be used on the Internet. Be sure to use the latest version of the template as Oracle periodically updates the template.

In the template, Oracle comments out all lines which effectively ***"Denies All."*** To use the url_fw.conf, DBAs at each client site need to manually uncomment ("open") specific JSP pages appropriate to their site. This "opening" by the DBAs must be carefully done and routinely reviewed.

The mechanics of when the url_fw.conf is called or not is determined by the Node's trust level. Most large Oracle E-Business Suite implementations have multiple web servers (referred to as nodes). To deploy the Oracle E-Business Suite on the Internet, one ore more nodes are deployed in a DMZ. If the node making the request of the Apache web server is flagged as an "Internal" web node, the url_fw.conf is skipped. If however the Node's trust level is flagged as "External" because the node is deployed in the DMZ, the url_fw.conf is called.

When called, the url_fw.conf applies regular expressions to the web request to determine if the request is BOTH exists in the whitelist and has been uncommented "opened" by the DBAs. If no match is found, a default-deny result is returned. In security terms, this means all requests are rejected unless explicitly allowed. If a match is found, the web request continues and the WebLogic server will then proceed with authentication and authorization tasks.



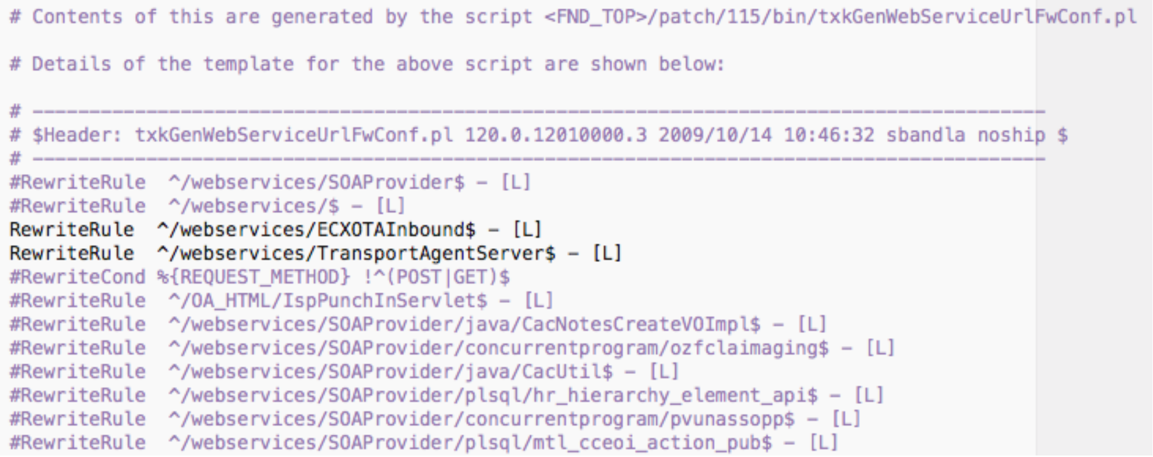
```
RewriteRule ^/$ /OA_HTML/AppsLocalLogin.jsp [R,L]
#RewriteRule ^$ /OA_HTML/AppsLocalLogin.jsp [R,L]
#RewriteRule ^/$ /OA_HTML/AppsLogin.jsp [R,L]
#RewriteRule ^/$ /OA_HTML/AppsLogin [R,L]

#Re-direct to the iRecruitment home page
#RewriteRule ^/$ /OA_HTML/IrcVisitor.jsp [R,L]
#Re-direct to the iStore home page
#RewriteRule ^/$ /OA_HTML/ibeCZzpHome.jsp [R,L]
```

Figure 7 - Example of URL FW line uncommented

Enabling and configuring the URL Firewall is the first step in securing web services. Unfortunately, Oracle buries the documentation for the URL Firewall in Appendix E of DMZ configuration guide – see the reference section of this paper for more information on the documentation.

To secure web services, it gets more complicated in that a second whitelist is appended to the first. To secure Oracle E-Business Suite web services, the url_fw.conf calls the url_fw_ws.conf. Similar to the configuration of the url_fw.conf, the documentation is buried deep in Appendix E of the DMZ configuration guide.

Different than the url_fw.conf which is supplied as a static listing of JSP pages, a utility (txkGenWebServiceUrlFwConf.pl) is run to generate the file url_fw_ws.conf. After being generated, DBAs similarly need to manually uncomment only those lines for the web services being used. If a web service is not found to be whitelisted, a default-deny rule will be applied; all web services commented out will be denied.

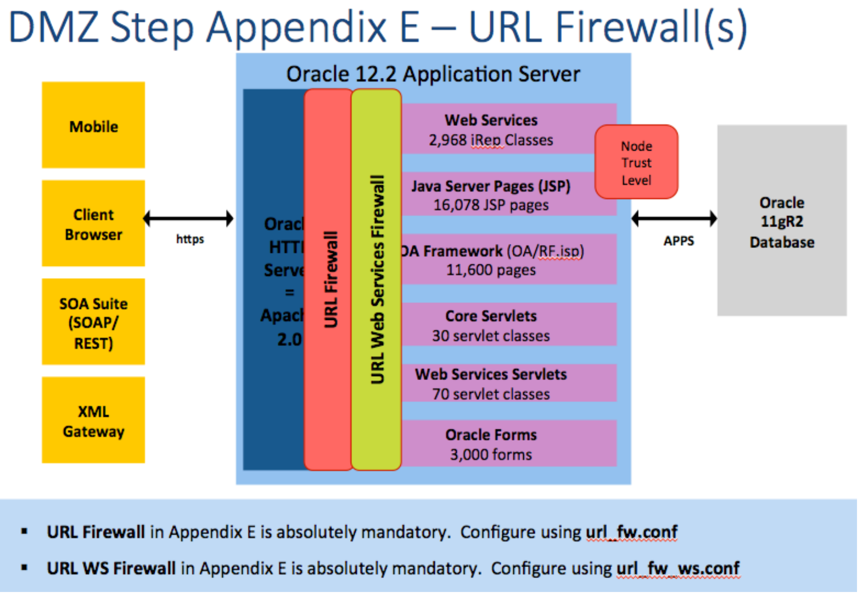


```
# Contents of this are generated by the script <FND_TOP>/patch/115/bin/txkGenWebServiceUrlFwConf.pl

# Details of the template for the above script are shown below:

# -----------------------------------------------------------------------------------------
# $Header: txkGenWebServiceUrlFwConf.pl 120.0.12010000.3 2009/10/14 10:46:32 sbandla noship $
# -----------------------------------------------------------------------------------------
#RewriteRule  ^/webservices/SOAProvider$ - [L]
#RewriteRule  ^/webservices/$ - [L]
RewriteRule  ^/webservices/ECXOTAInbound$ - [L]
RewriteRule  ^/webservices/TransportAgentServer$ - [L]
#RewriteCond %{REQUEST_METHOD} !^(POST|GET)$
#RewriteRule  ^/OA_HTML/IspPunchInServlet$ - [L]
#RewriteRule  ^/webservices/SOAProvider/java/CacNotesCreateVOImpl$ - [L]
#RewriteRule  ^/webservices/SOAProvider/concurrentprogram/ozfclaimaging$ - [L]
#RewriteRule  ^/webservices/SOAProvider/java/CacUtil$ - [L]
#RewriteRule  ^/webservices/SOAProvider/plsql/hr_hierarchy_element_api$ - [L]
#RewriteRule  ^/webservices/SOAProvider/concurrentprogram/pvunassopp$ - [L]
#RewriteRule  ^/webservices/SOAProvider/plsql/mtl_cceoi_action_pub$ - [L]
```

Figure 8 - Example of URL FW WS.conf

Errors in selecting a Node's trust level and configuring either the url_fw.conf and/or the url_fw_ws.conf have serious security consequences and should be routinely reviewed as part of on-going security audits.

Web services can be publically deployed without using the URL Firewall. For example, clients can if they so choose route Internet traffic directly to the E-Business Suite without setting up an External node. Integrigy Corporation highly recommends against doing this. Integrigy Corporation highly recommends always using the URL Firewall when deployed on the Internet, both for forms and for web services.

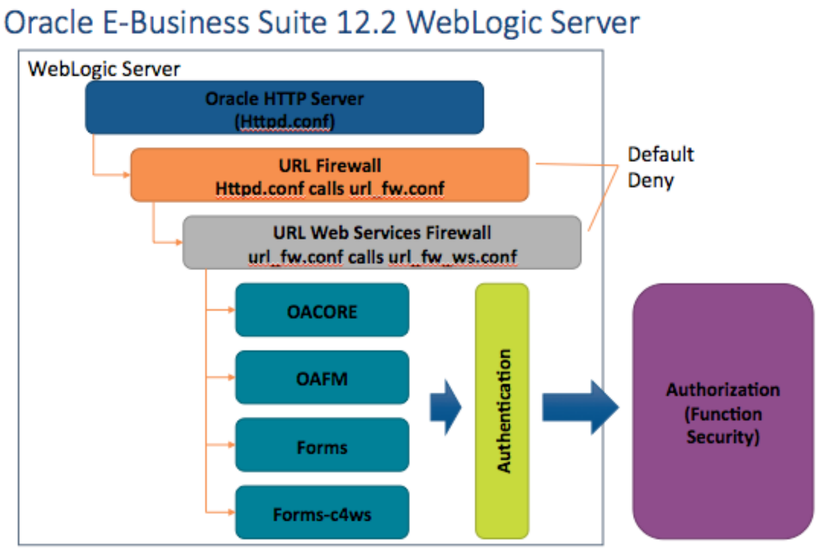


DMZ Step Appendix E – URL Firewall(s)

Oracle 12.2 Application Server
Mobile
Client Browser
SOA Suite (SOAP/ REST)
XML Gateway
https
Oracl HTTI Serve = Apacl 2.0
URL Firewall
URL Web Services Firewall
Web Services 2,968 iRep Classes
Java Server Pages (JSP) 16,078 JSP pages
OA Framework (OA/RF.jsp) 11,600 pages
Core Servlets 30 servlet classes
Web Services Servlets 70 servlet classes
Oracle Forms 3,000 forms
Node Trust Level
APPS
Oracle 11gR2 Database

- **URL Firewall** in Appendix E is absolutely mandatory. Configure using **url_fw.conf**
- **URL WS Firewall** in Appendix E is absolutely mandatory. Configure using **url_fw_ws.conf**

Figure 9 - URL Firewall called by Node Trust Level



Oracle E-Business Suite 12.2 WebLogic Server

WebLogic Server
Oracle HTTP Server (Httpd.conf)
URL Firewall Httpd.conf calls url_fw.conf
URL Web Services Firewall url_fw.conf calls url_fw_ws.conf
Default Deny
OACORE
OAFM
Forms
Forms-c4ws
Authentication
Authorization (Function Security)

Figure 10 - httpd.conf calls the URL Firewall

Authentication and Authorization

Once traffic is accepted and passed by the URL Firewall, WebLogic initiates the standard Oracle E-Business Suite authentication and authorization procedures. Web services are authenticated and authorized no differently than for end-users.

Authorization rules for web services are relatively easy to configure in that all web services are defined as functions. The Oracle E-Business Suite's function security scheme and rules engine apply the same to GUI forms as for web services. In other words, the table APPLSYS.FND_FORM_FUNCTIONS defines all the forms that users use as well as defines all web services deployed. Menus then are built referencing these functions and Oracle E-Business Suite user accounts (APPLSYS.FND_USER) are given responsibilities with the menus of functions. These user accounts can be staff members or can be generic accounts (e.g. to support specific web services). Ensuring that appropriate users and responsibilities can call and use specific web services is the same critical step as ensuring that only appropriate users can use specific forms.

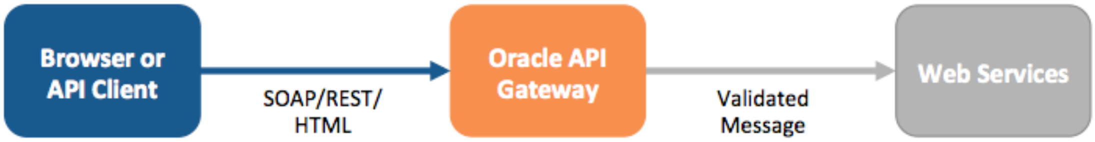
There are two authentication options for web services, local FND_USER passwords and tokens. Tokens can be SAML send vouchers/E-Business Suite Session Ids). Whichever is used, ensure that accounts are not inappropriately over privileged and the passwords and tokens not widely known and/or shared.

Web Application Firewalls Are Required

Web Application Firewalls (WAFs) cannot replace the URL Firewall, nor can the URL Firewall replace WAFs. The URL Firewall provides the critical function of only allowing those forms and web services that have been both hardened by Oracle and flagged by the client as being used – all other requests are blocked by the default-deny rules. The URL Firewall does not protect against common web attack techniques such as those below – this what WAFs protect against:

- Denial of Service (DoS)
    - Flooding, recursive & oversized payloads
- Injection & Malicious Code
    - XXC, SQLi, logic bombs, malformed content
- Confidentiality and Integrigy
    - Parameter tampering, schema poisoning
- Reconnaissance Attacks
    - Scanning and registry disclosure
- Privilege Escalation Attacks
    - Race condition, format string, buffer overflow

Additional protection is required to secure Internet facing Oracle E-Business Suite web services. Third party WAFs can certainly be deployed, but Oracle Corporation's API Gateway offers a compelling advantage for Oracle E-Business Suite clients. The API Gateway is a separate license option and is placed in front of the SOA Server (also a separate license option) to defend against the common web attack techniques specific to web services as identified above.



Oracle Supplier Network Security

The most common use of web services with the Oracle E-Business Suite is the Oracle Suppler Network (OSN). Do not confuse OSN with the Oracle Social Network (also referred to as OSN) or when configuring OSN, do not confuse the Oracle Transport Agent (OXTA) web services with Oracle Training Administration (OTA) web services.

To use OSN, you must configure the both the url_fw.conf and url_fw_ws.conf file to open traffic for the XML Gateway to consume OXTA web services. The OSN documentation in places confuses OTXA and OTA. The risk is that in the url_fw_ws.conf there are services for both the Oracle Training Administration (OTA) module as well as for the OXTA. Unless both are being used, be careful to open only the correct services.

It should also be noted that while OSN uses web services, as of 12.2.5, OSN's web services are NOT shown as deployed in the ISG repository. This is because OSN's functionality is built into the Oracle E-Business Suite's core functionality.

It is very important to note that while using OSN with trading partners over the Internet requires opening the E-Business Suite to the Internet. Unfortunately, it is not clearly stated that a WAF, ideally the API Gateway, should be used to protect OSN. Even if OSN is the only web service being used, a WAF is still required to guard the attack surface.

Lastly, the passwords used for the various OSN accounts (defined within the OSN GUI forms) need to be complex and regularly rotated. Many clients forget about these accounts.

Securing Mobile Applications

Oracle Corporation has been building out Mobile and Smartphone applications for the Oracle E-Business Suite for a number of releases. Before release 12.2.5, this functionality was designed only for deployment through a corporate VPN, not through an Oracle E-Business Suite external node over the Internet (e.g. a server in DMZ).

With release, 12.2.5 external node deployment for Mobile applications is now an option. 12.2.5 bundles Oracle Mobile v4 and uses the E-Business Suite's WebLogic server. Specifically, 12.2.5 deploys the Oracle Mobile v4 REST services through the OAFM WebLogic application. In other words, with 12.2.5, Smartphone applications can now be Internet deployed without a need for a separate WebLogic Server; no need for a SOA Server or a separate WebLogic server.

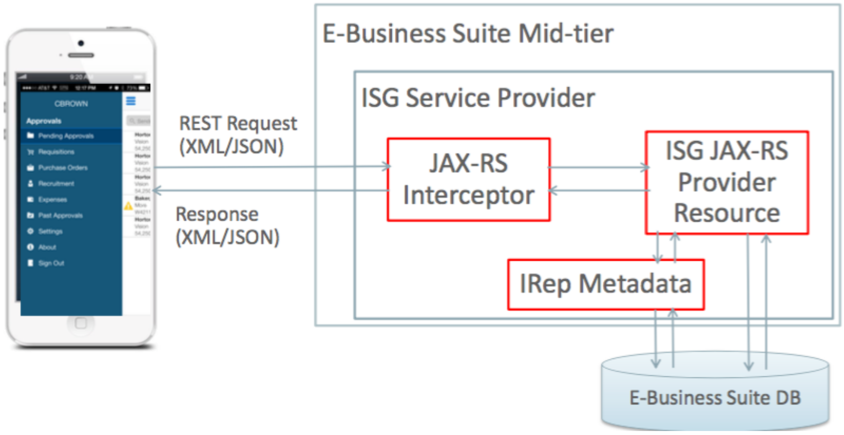


Figure 11 Oracle Mobile Using Native EBS REST

To secure version 12.2.5 Oracle E-Business Suite Mobile applications, Oracle Mobile Security Services (OMSS) is used. Check with your Oracle sales representative if OMSS is separately licensed or not. OMSS provides critical URL shortening as well as white/blacklisting and other functionality specific to deploying Oracle Mobile applications. OMSS must be properly configured and is placed in front of OAFM.

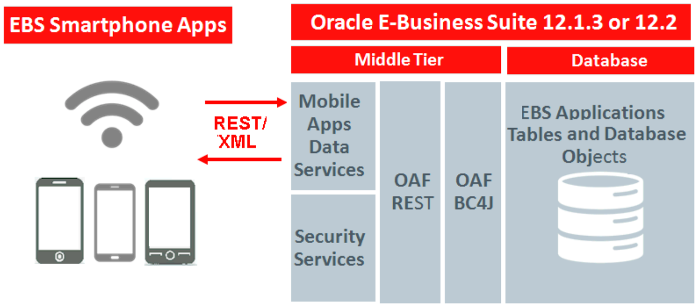
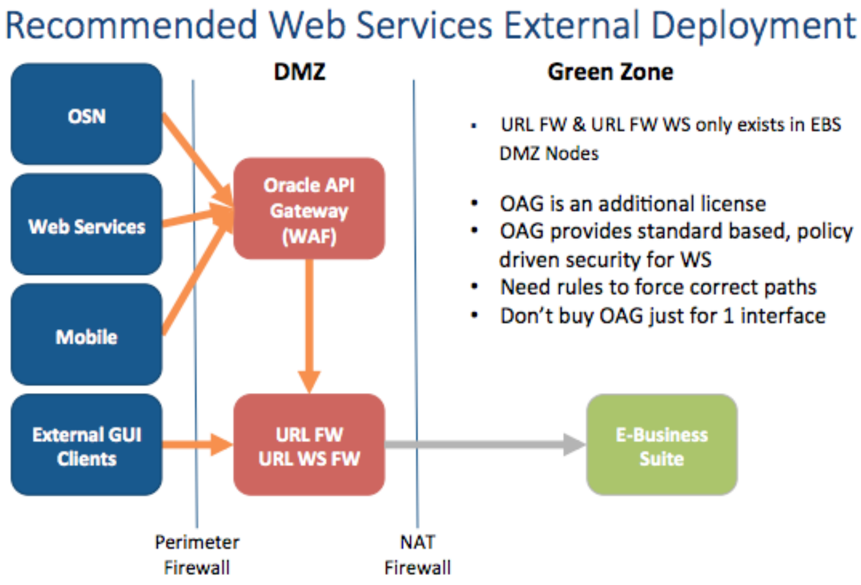

EBS Smartphone Apps
Oracle E-Business Suite 12.1.3 or 12.2
Middle Tier
Database
REST/ XML
Mobile Apps Data Services
Security Services
OAF REST
OAF BC4J
EBS Applications Tables and Database Objects

Figure 12 - OMSS before OAFM

Recommended Approach for Securing Web Services and Mobile Applications

Deploying Internet-based Oracle E-Business Suite web services requires proper configuration of the URL Firewall, both the url_fw.conf and url_fw_ws.conf and the use of a WAF – ideally the Oracle API Gateway. This recommendation applies equally to all whose only use of web services is the Oracle Supplier Network (OSN). One opening of the attack surface exposed to the Internet exposes the entire Oracle E-Business Suite.



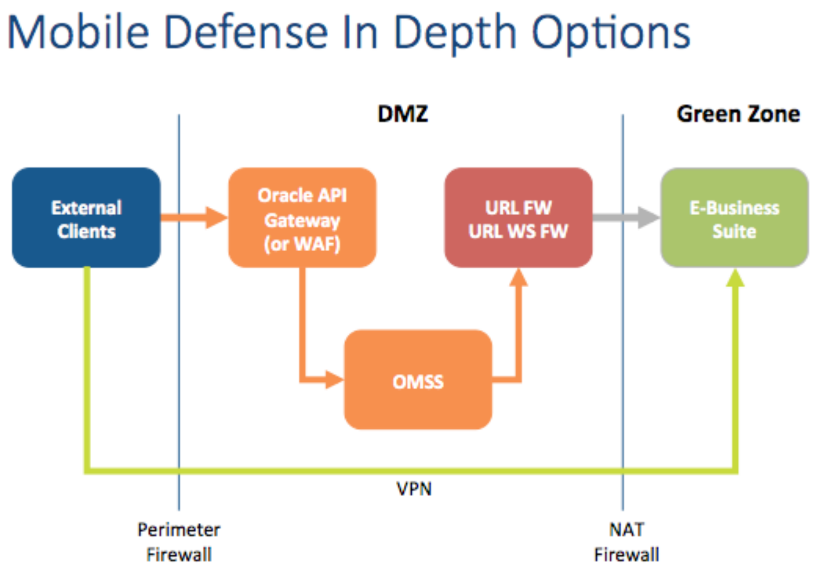
Recommended Web Services External Deployment

- URL FW & URL FW WS only exists in EBS DMZ Nodes

- OAG is an additional license
- OAG provides standard based, policy driven security for WS
- Need rules to force correct paths
- Don't buy OAG just for 1 interface

Figure 13 - Recommended Approach

For Mobile and Smartphone applications, due to the overall complexity and additional license requirements, it is recommended to continue using VPN for deployment instead of using an External Node.



Mobile Defense In Depth Options

REFERENCES

GENERAL

- Oracle E-Business Suite Release 12.2 Configuration in a DMZ (Note 1375670.1)

About Integrigy

Integrigy Corporation (www.integrigy.com)

Integrigy Corporation is a leader in application security for enterprise mission-critical applications. AppSentry, our application and database security assessment tool, assists companies in securing their largest and most important applications through detailed security audits and actionable recommendations. AppDefend, our enterprise web application firewall is specifically designed for the Oracle E-Business Suite. Integrigy Consulting offers comprehensive security assessment services for leading databases and ERP applications, enabling companies to leverage our in-depth knowledge of this significant threat to business operations.

INTEGRIGY
Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60681 USA
888/542-4802
www.integrigy.com