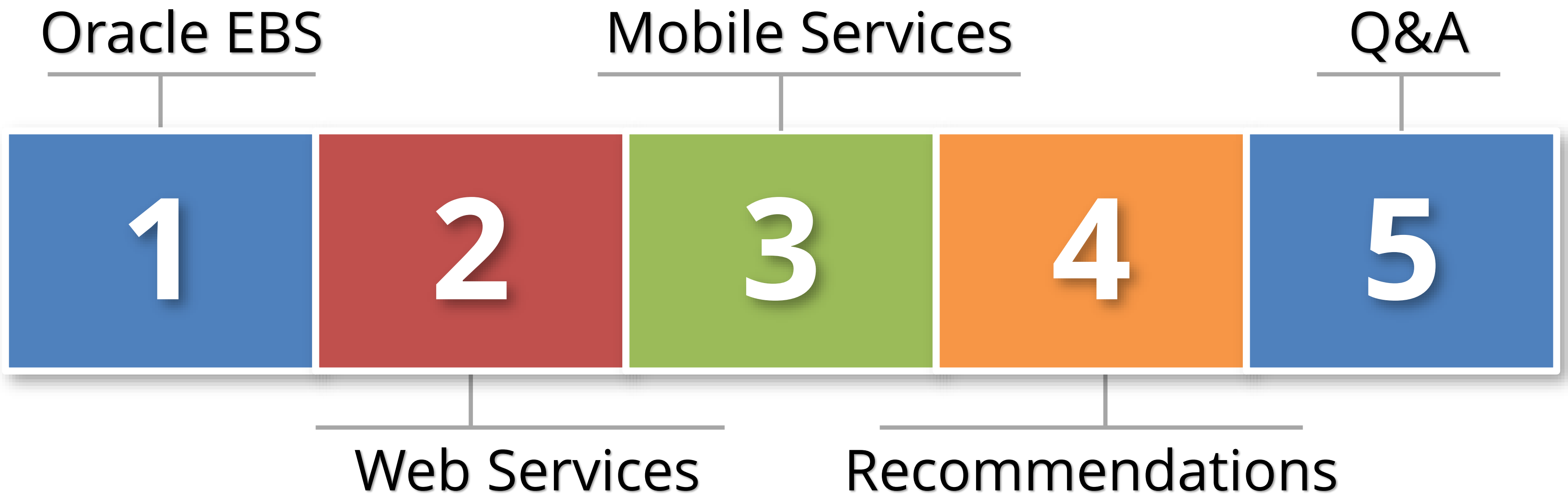
Oracle E-Business Suite
Mobile and Web Services Security

November 3, 2016

Michael Miller
Chief Security Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda



1 Oracle EBS

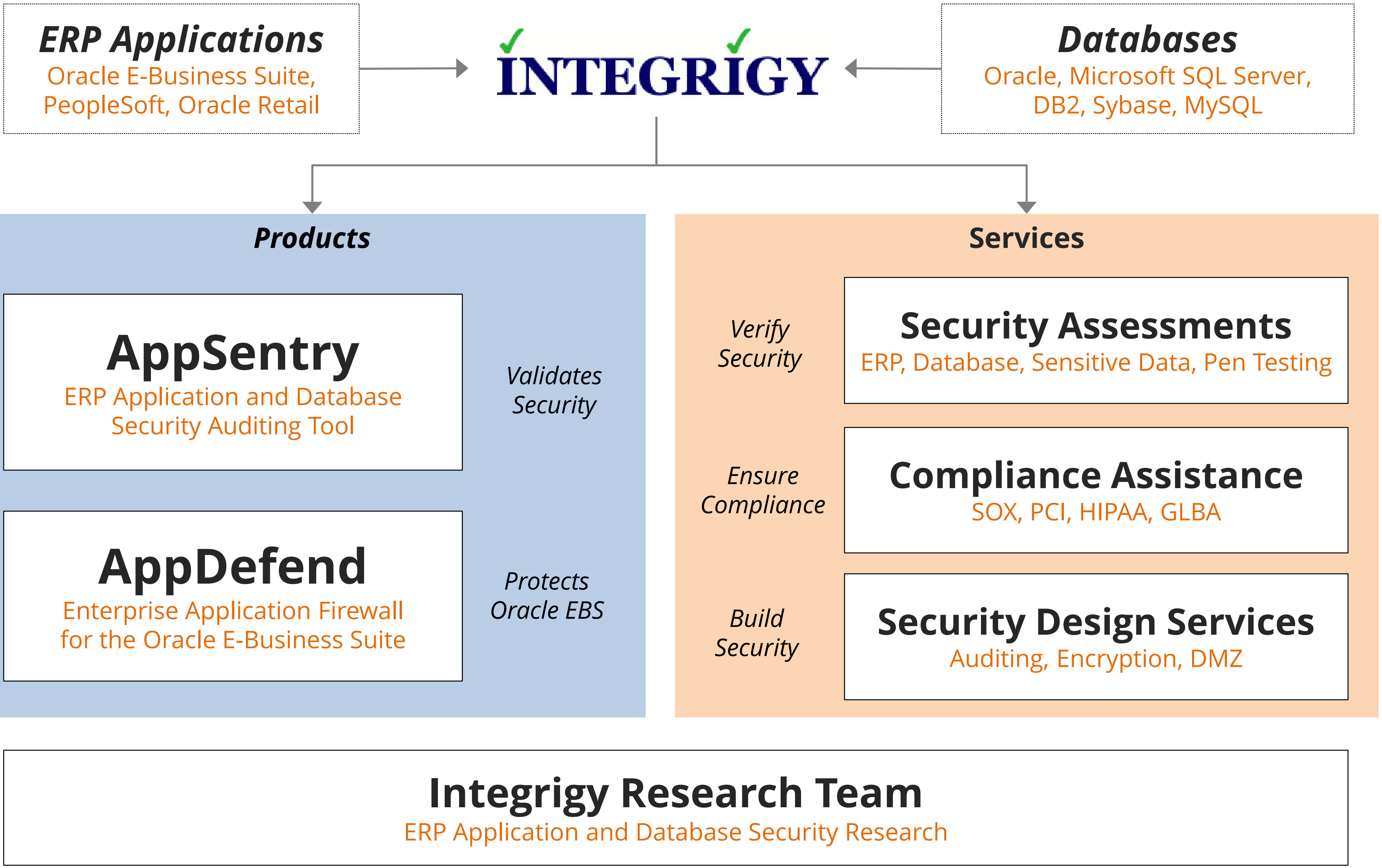
2 Web Services

3 Mobile Services

4 Recommendations

5 Q&A

About Integrigy



ERP Applications

Oracle E-Business Suite, PeopleSoft, Oracle Retail

INTEGRIGY

Databases

Oracle, Microsoft SQL Server, DB2, Sybase, MySQL

Products

AppSentry

ERP Application and Database Security Auditing Tool

Validates Security

AppDefend

Enterprise Application Firewall for the Oracle E-Business Suite

Protects Oracle EBS

Services

Verify Security

Security Assessments

ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance

SOX, PCI, HIPAA, GLBA

Build Security

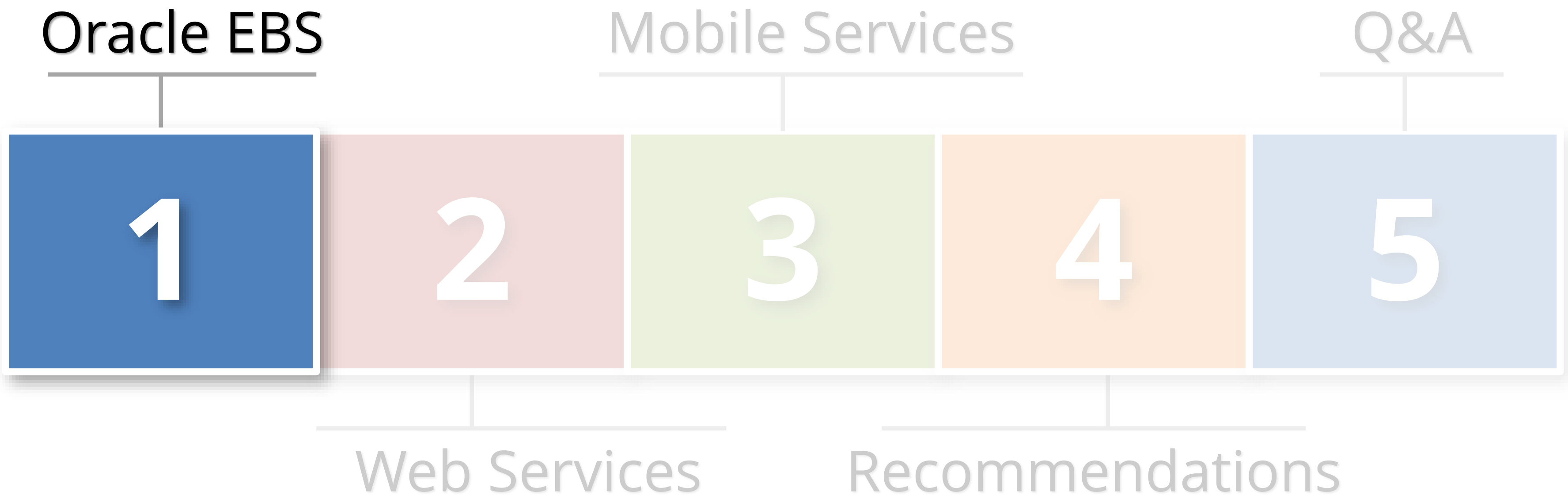
Security Design Services

Auditing, Encryption, DMZ

Integrigy Research Team

ERP Application and Database Security Research

Agenda



1 Oracle EBS

2 Web Services

3 Mobile Services

4 Recommendations

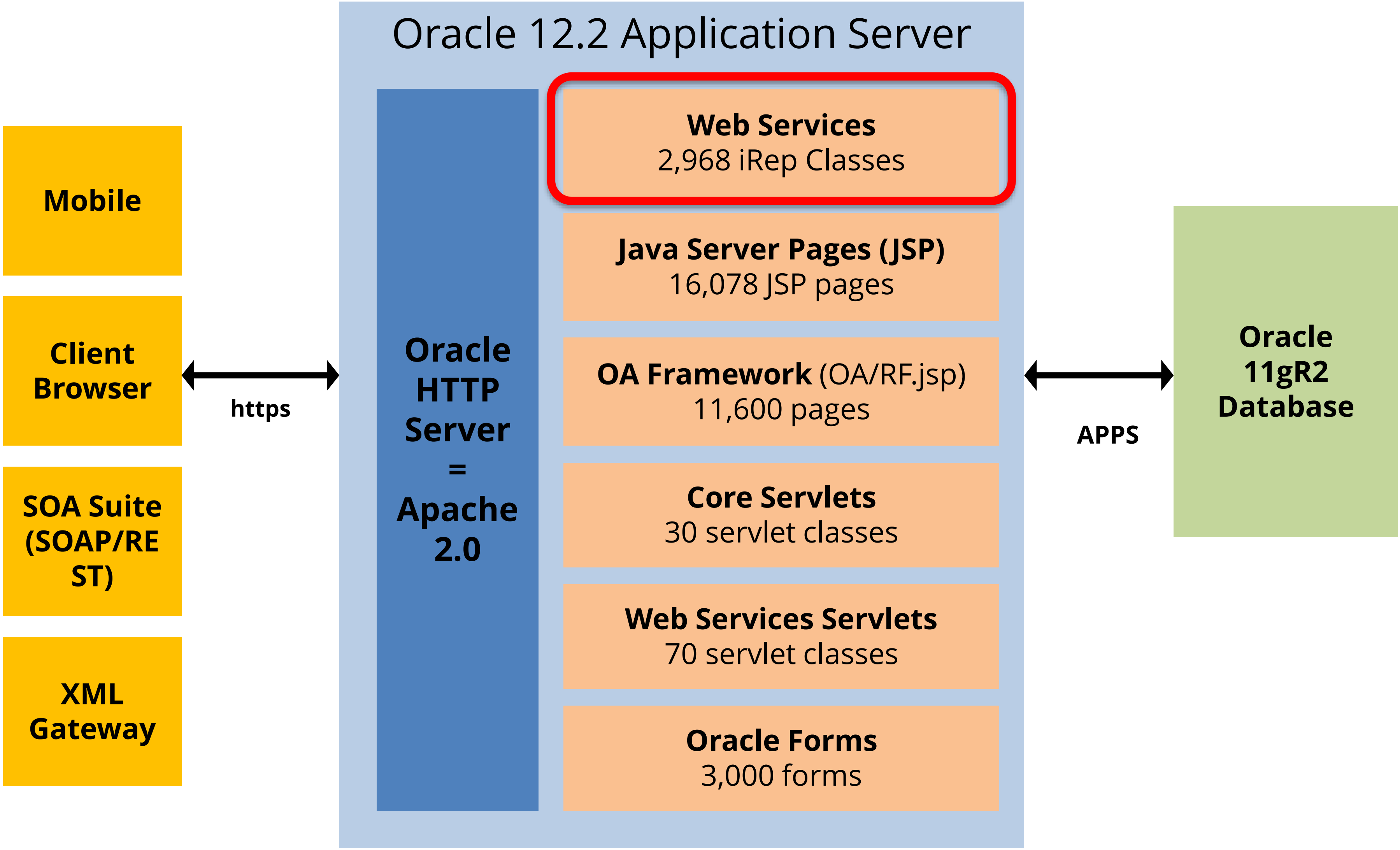
5 Q&A

Inherent Risks with Package Software

Structure and vulnerabilities within the application are well known and documented.

- An attacker knows exactly what to expect and how the application is structured
- No probing or reconnaissance of the application is required
- Fatal attack can be one URL
- Allows for easy automated attacks

Oracle 12.2 Architecture



Mobile

Client Browser

SOA Suite (SOAP/REST)

XML Gateway

https

Oracle 12.2 Application Server

Oracle HTTP Server = Apache 2.0

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

APPS

Oracle 11gR2 Database

Web Services Threat Classification

The Web Application Security Consortium (WASC) has developed the **WASC Threat Classification** to “clarify and organize the threats to the security of a web site.”

Attacks

Abuse of Functionality
Brute Force
Buffer Overflow
Content Spoofing
Credential/Session Prediction
Cross-Site Scripting
Cross-Site Request Forgery
Denial of Service
Fingerprinting
Format String
HTTP Response Smuggling
HTTP Response Splitting
HTTP Request Smuggling
HTTP Request Splitting
Integer Overflows
LDAP Injection
Mail Command Injection
Null Byte Injection
OS Commanding
Path Traversal
Predictable Resource Location
Remote File Inclusion (RFI)
Routing Detour
Session Fixation
SOAP Array Abuse
SSI Injection
SQL Injection
URL Redirector Abuse
XPath Injection
XML Attribute Blowup
XML External Entities
XML Entity Expansion
XML Injection
XQuery Injection

Weaknesses

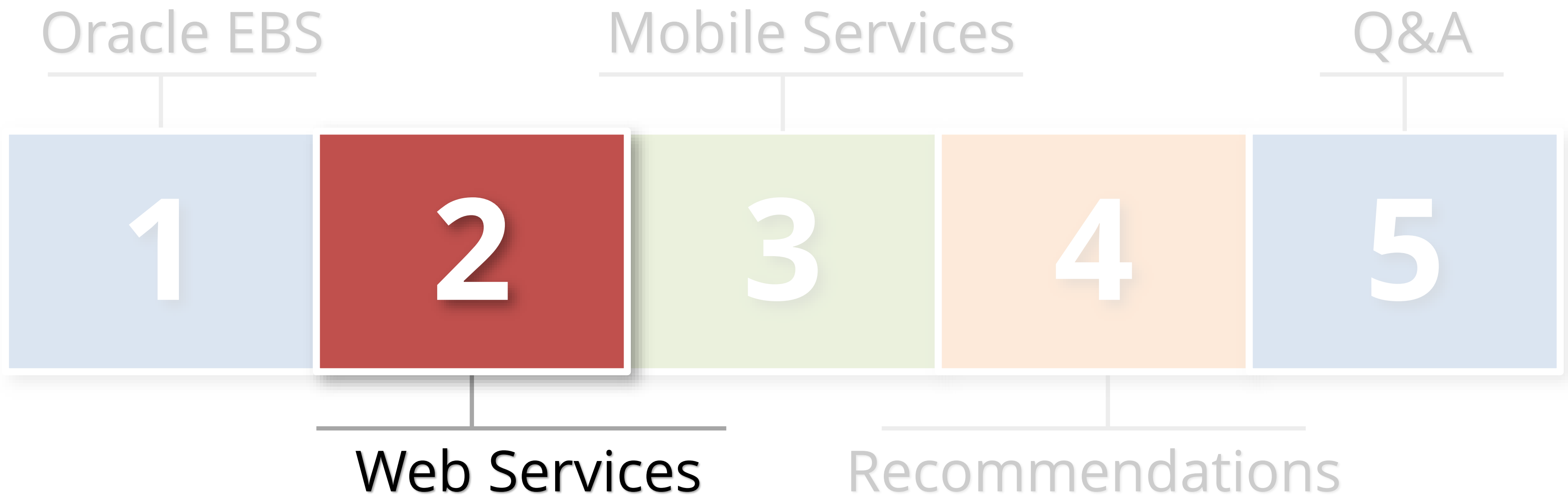
Application Misconfiguration
Directory Indexing
Improper File System Permissions
Improper Input Handling
Improper Output Handling
Information Leakage
Insecure Indexing
Insufficient Anti-automation
Insufficient Authentication
Insufficient Authorization
Insufficient Password Recovery
Insufficient Process Validation
Insufficient Session Expiration
Insufficient Transport Layer Protection
Server Misconfiguration

http://www.webappsec.org

Web Services Vocabulary

- **Web services**
  - Referred to collectively as SOAP & REST
- **Service Orientated Architecture (SOA)**
- **Simple Object Access Protocol (SOAP)**
  - Heavy duty interfaces (e.g. B2B)
  - Services defined in XML formatted Web Services Description Language (WDSL) files
- **Representational State Transfer (REST)**
  - Architectural style not protocol
  - Lightweight interfaces and “chatty” user interfaces (e.g. Mobile and tablet)
  - Services defined in XML formatted Web Application Description Language (WADL) files

Agenda



1 Oracle EBS

2 Web Services

3 Mobile Services

4 Recommendations

5 Q&A

E-Business Suite Web Services

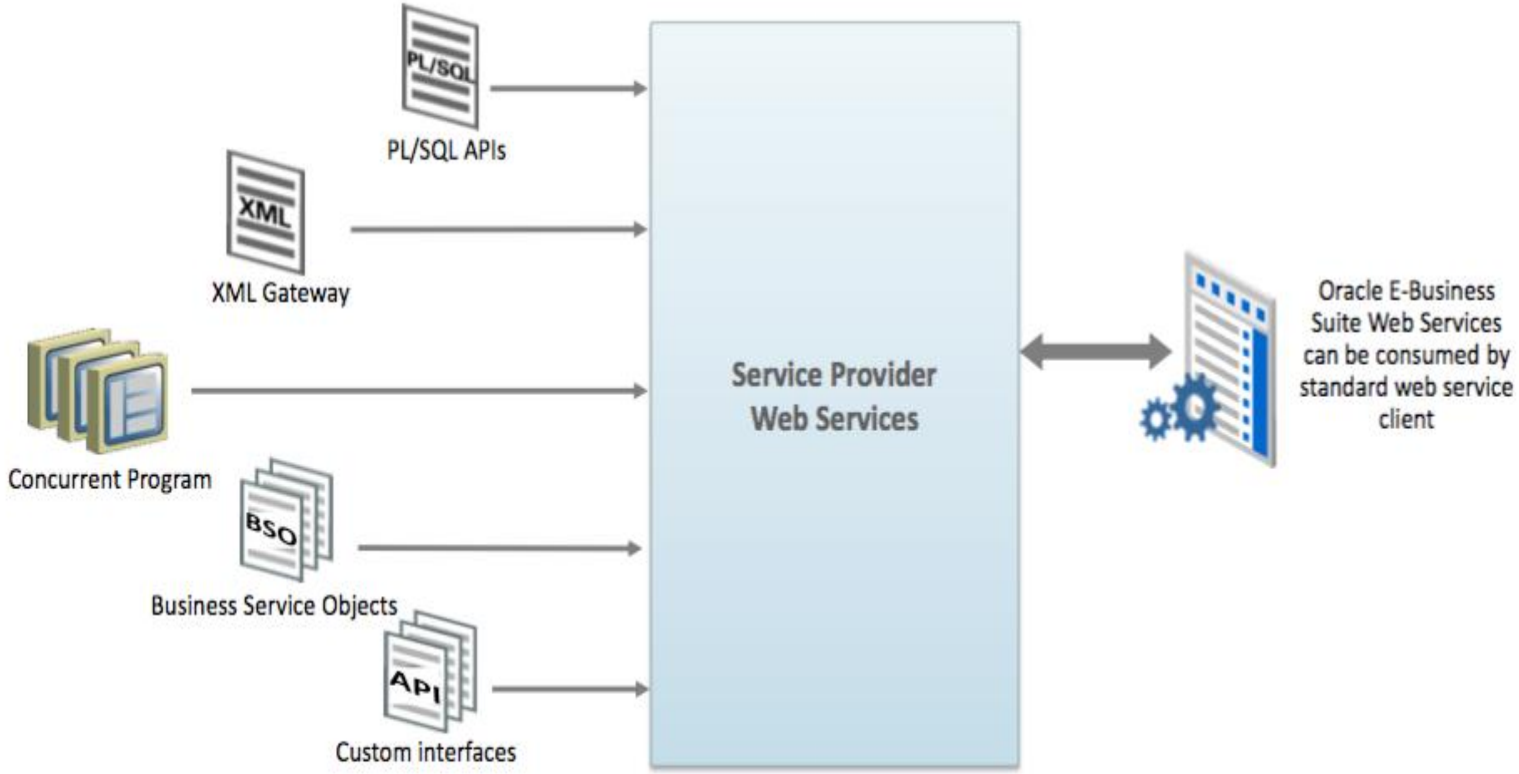
- **Increasing amount of web services functionality**
  - 12.1.x, 12.2.3, 12.2.4 and 12.2.5
  - Significant changes to Mobile
- **Integrated SOA Gateway (ISG) defines E-Business Suite Web services**
  - Consolidates all SOAP and REST services
  - Includes E-Business Suite Mobile application APIs (REST)
  - All defined in FND_IREP_CLASSES
- **12.2 E-Business WebLogic Domain**
  - Four (4) applications: oacore, oafm, forms, forms-c4ws
  - ISG REST & Mobile Apps use OAFM
  - Separate SOA Suite WebLogic Server deploys SOAP

Web Services Authentication and Authorization

- **Authentication options**
  - Password – local E-Business Suite account
  - Token (SAML sender vouchers/E-Business Suite session ID)

- **Function security defines authorization privileges for web services**
  - Same as for GUI functions
  - FND_FORM_FUNCTIONS

E-Business Suite Web Services


PL/SQL
PL/SQL APIs
XML
XML Gateway
Concurrent Program
BSO
Business Service Objects
API
Custom interfaces
Service Provider Web Services
Oracle E-Business Suite Web Services can be consumed by standard web service client

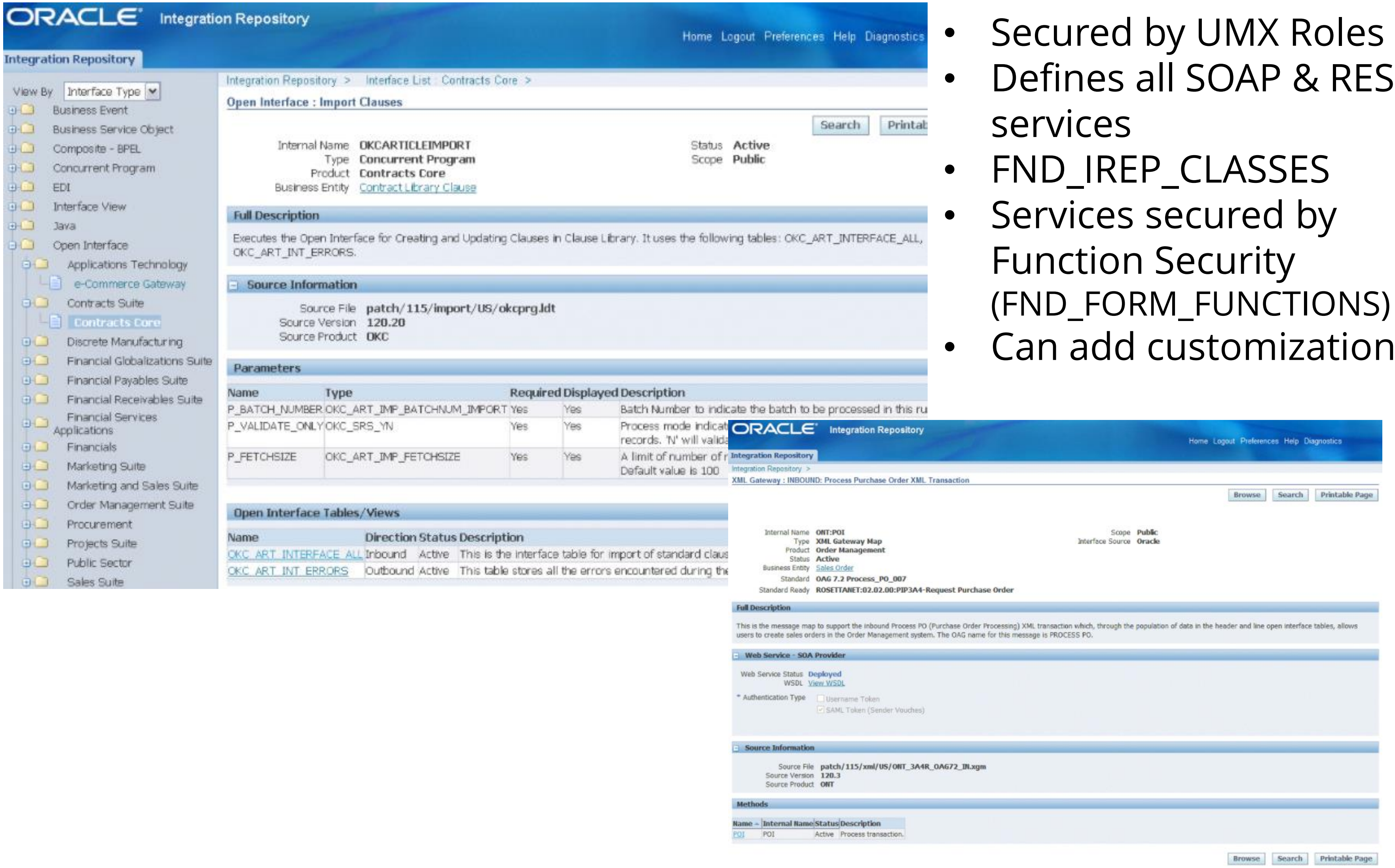
Yesterday’s interfaces are now web services

#1 Oracle Supplier Network (OSN)

- **Oracle Supplier Network (OSN)**
  - Not Oracle Social Network
  - Most common web service
  - Is an open community for Oracle E-Business Suite, PeopleSoft and Cloud Applications customers and their trading partners
  - Will see not deployed in EBS Integration Repository
- **Uses both XML gateway and OXTA transport agent**
  - Need to open services in URL_FW_WS.conf

#2 Integrated SOA Gateway (ISG)

- Secured by UMX Roles
- Defines all SOAP & REST services
- FND_IREP_CLASSES
- Services secured by Function Security (FND_FORM_FUNCTIONS)
- Can add customizations



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_ART_INTERFACE_ALL, 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 in this ru
P_VALIDATE_ONLY	OKC_SRS_YN	Yes	Yes	Process mode indicat records. 'N' will valida
P_FETCHSIZE	OKC_ART_IMP_FETCHSIZE	Yes	Yes	A limit of number of r 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 claus
OKC_ART_INT_ERRORS	Outbound	Active	This table stores all the errors encountered during the

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 map 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, allows 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

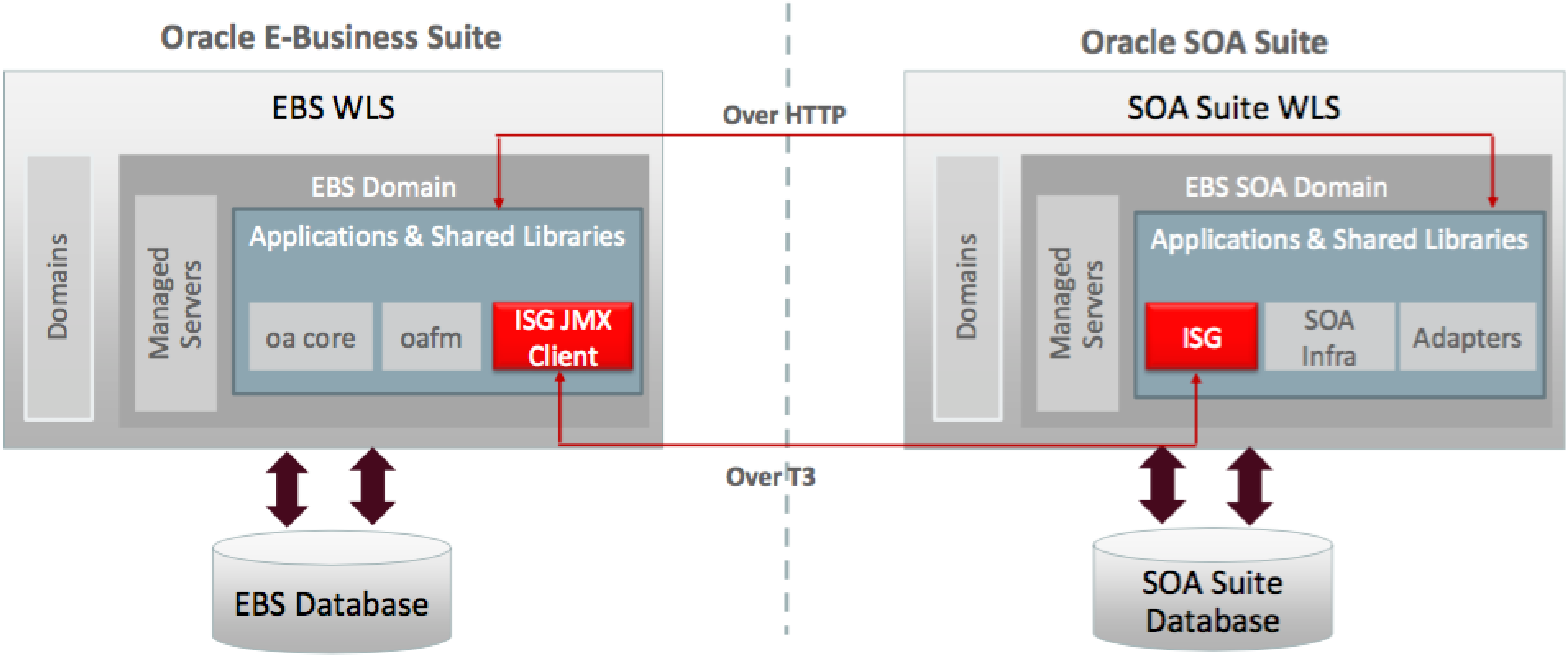
Source File patch/115/xml/US/ONT_3A4R_OAG72_IN.xgm
Source Version 120.3
Source Product ONT

Methods

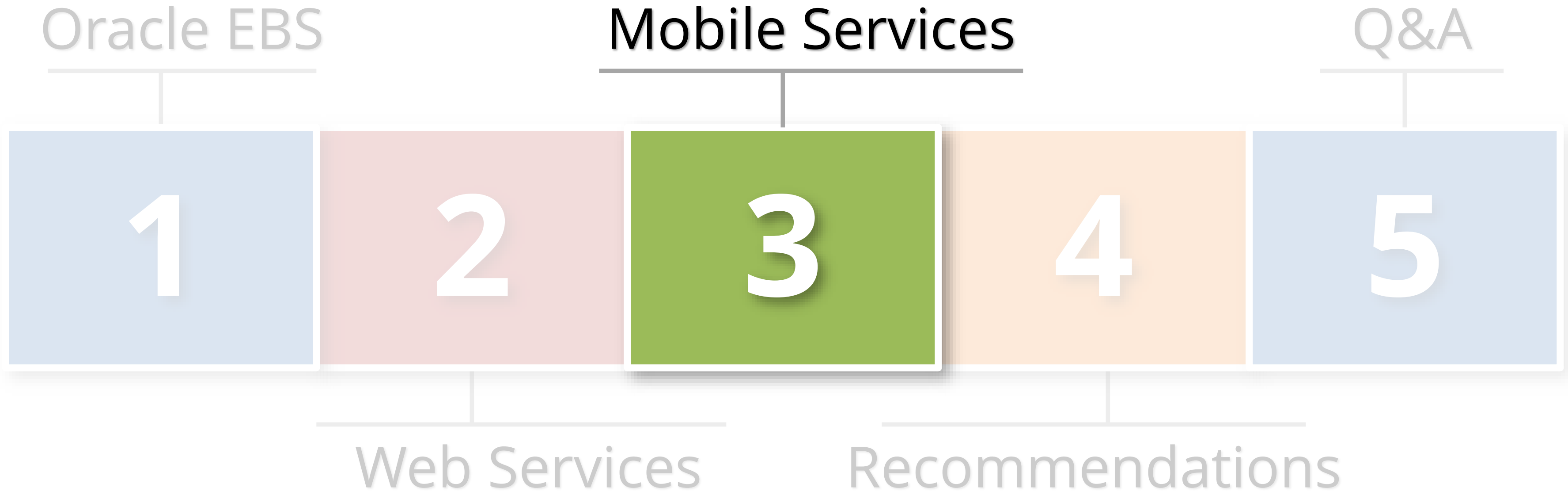
Name	Internal Name	Status	Description
POI	POI	Active	Process transaction.

#3 Oracle SOA Suite

- **Separate WebLogic server install**
  - Needs to be security hardened
  - WDSL deployed on SOA Suite server
  - Clients and trading partners talk to SOA server



Agenda



1 Oracle EBS

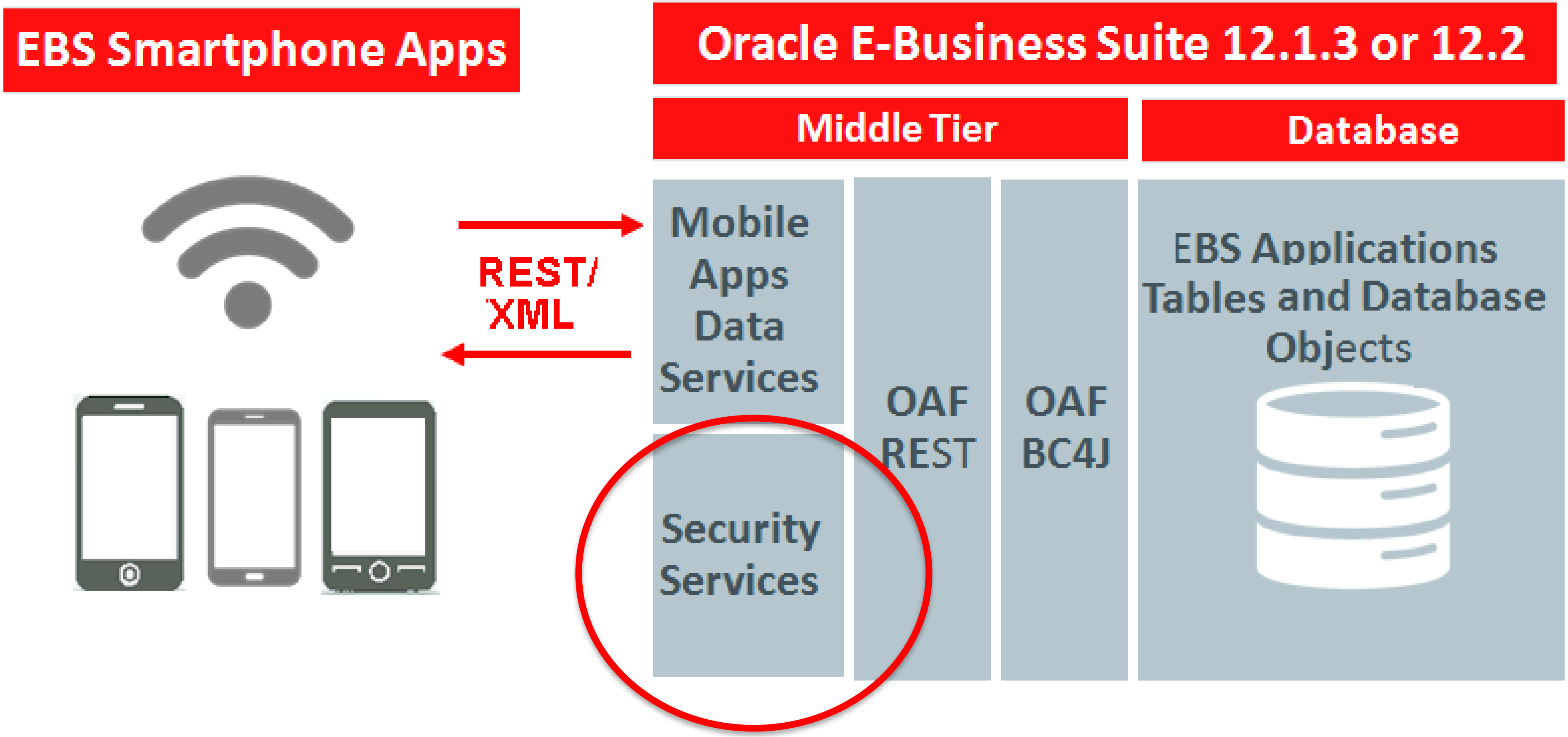
2 Web Services

3 Mobile Services

4 Recommendations

5 Q&A

Oracle E-Business Suite Mobile


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

Note “Security Services”

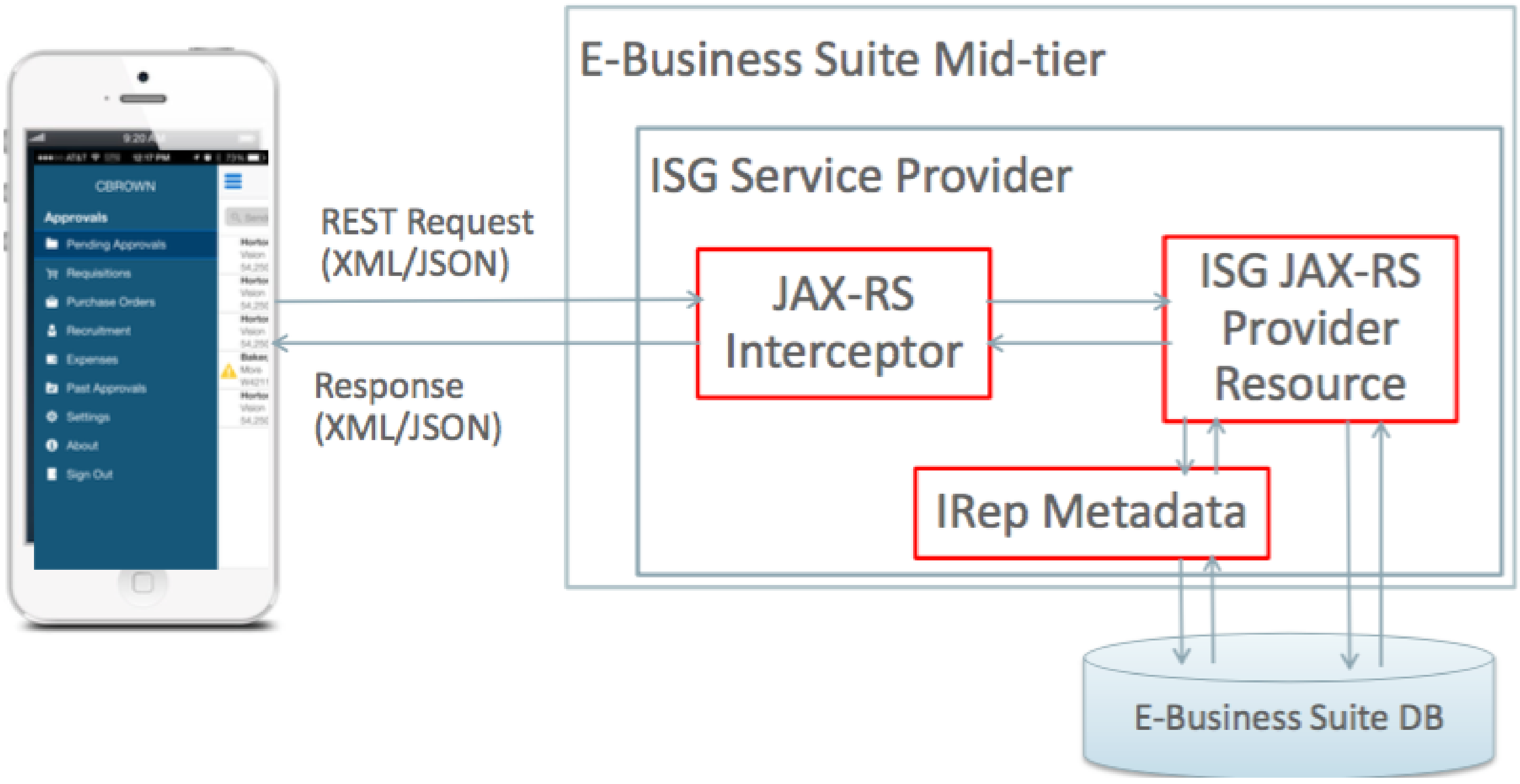
E-Business Suite Mobile Deployment Options

- **Prior to 12.2.5 only deployment model was through VPN**
  - VPN configured on each iPhone etc…

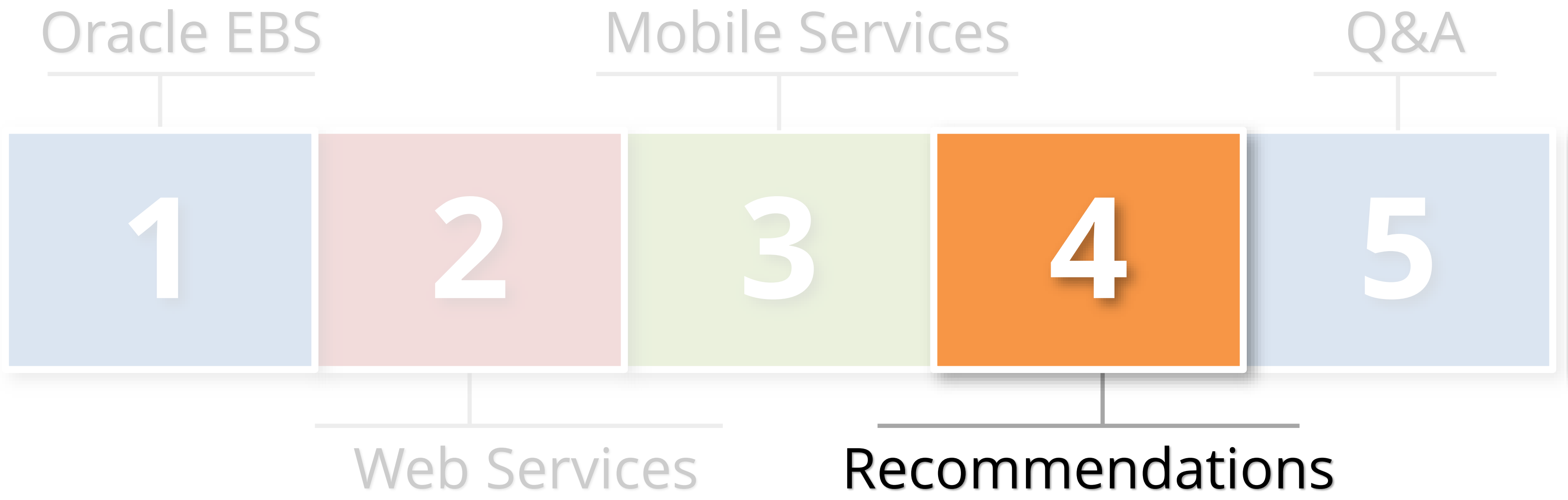
- **12.2.5 delivers Oracle Mobile version 4**
  - DMZ deployment by tagging Responsibilities as EXTERNAL
  - Deploys REST through E-Business OAFM (No need for SOA Suite)

Oracle E-Business Suite Mobile 12.2.5

12.2.5 allows VPN or DMZ deployment



Agenda



Oracle EBS

Mobile Services

Q&A

1

2

3

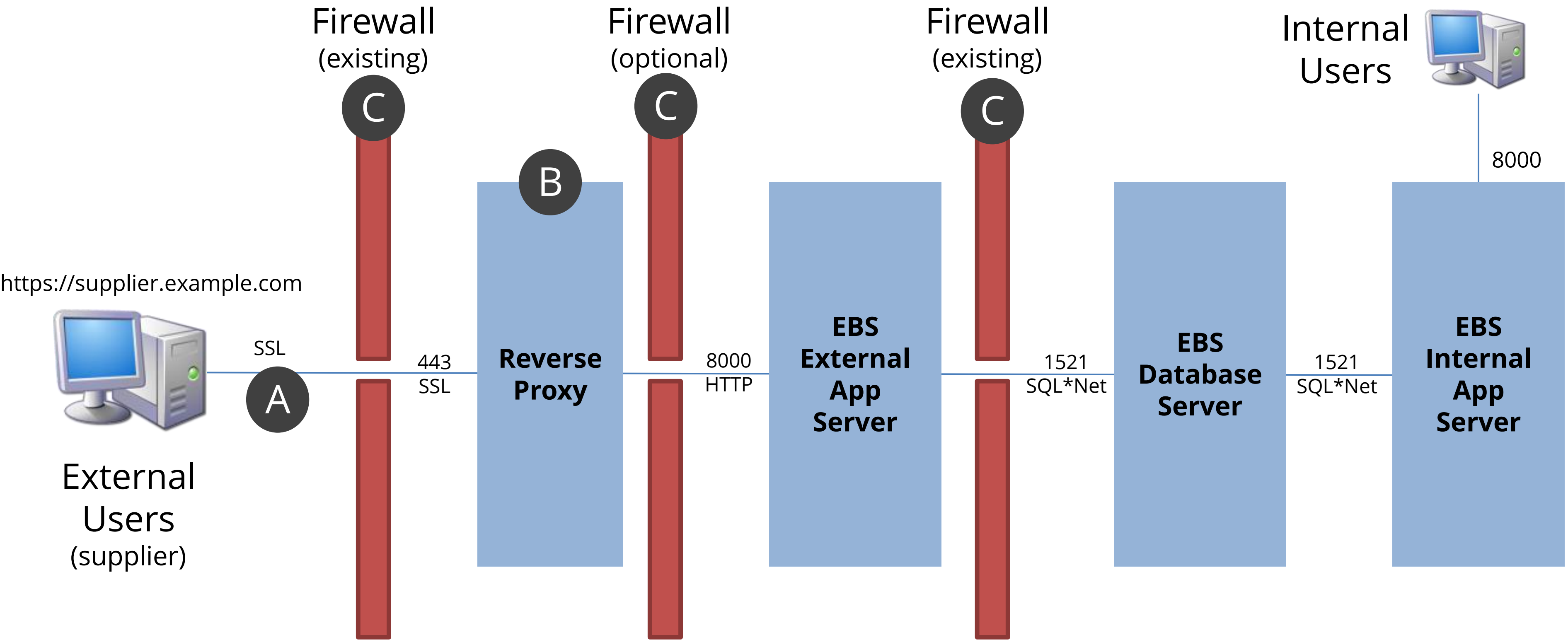
4

5

Web Services

Recommendations

E-Business Suite DMZ Architecture

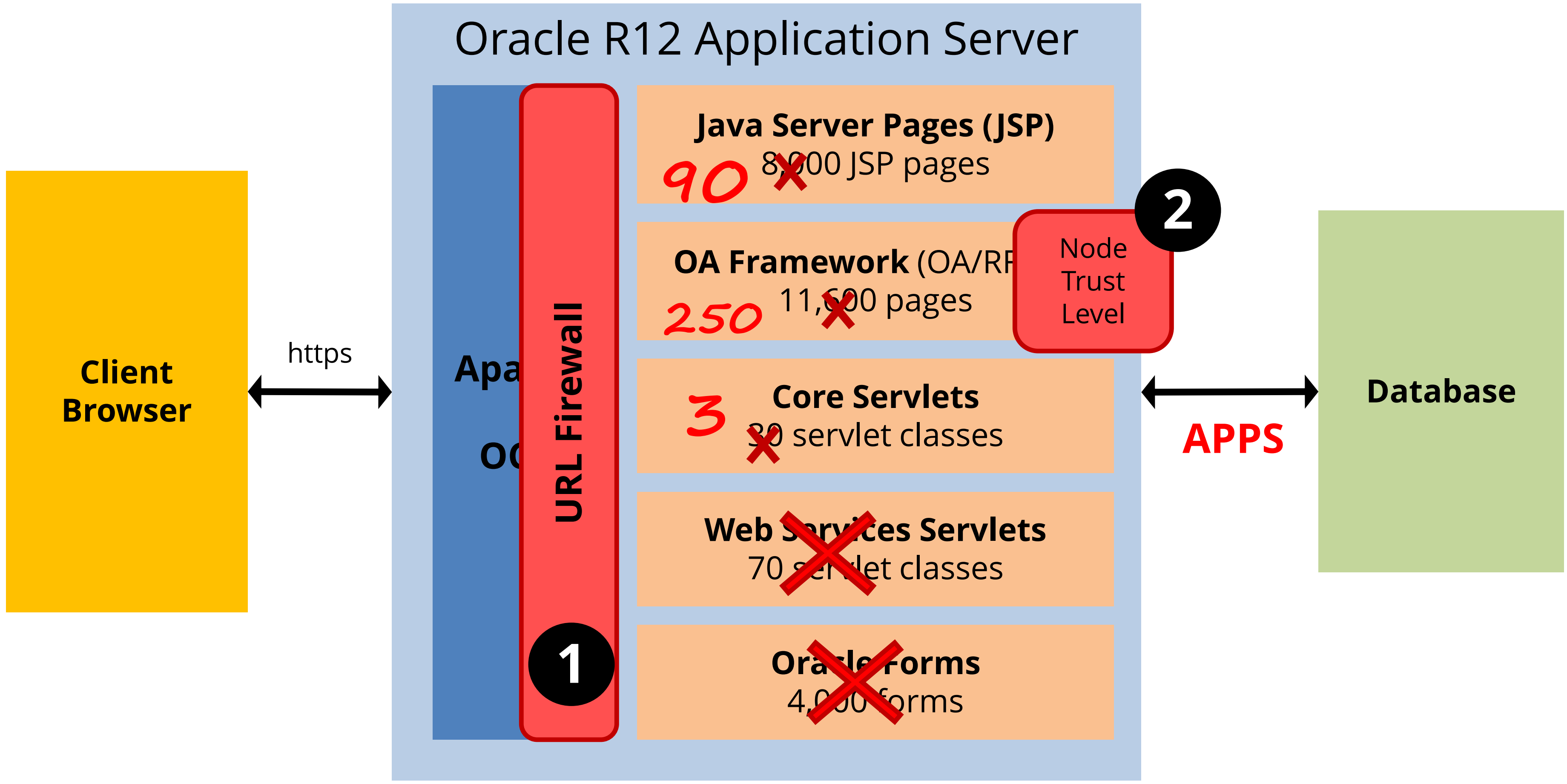


A **HTTPS/SSL** should always be used otherwise passwords and data are sent in the clear.

B A **reverse proxy** server should be implemented such as Apache, HA Proxy, or F5 BIG-IP.

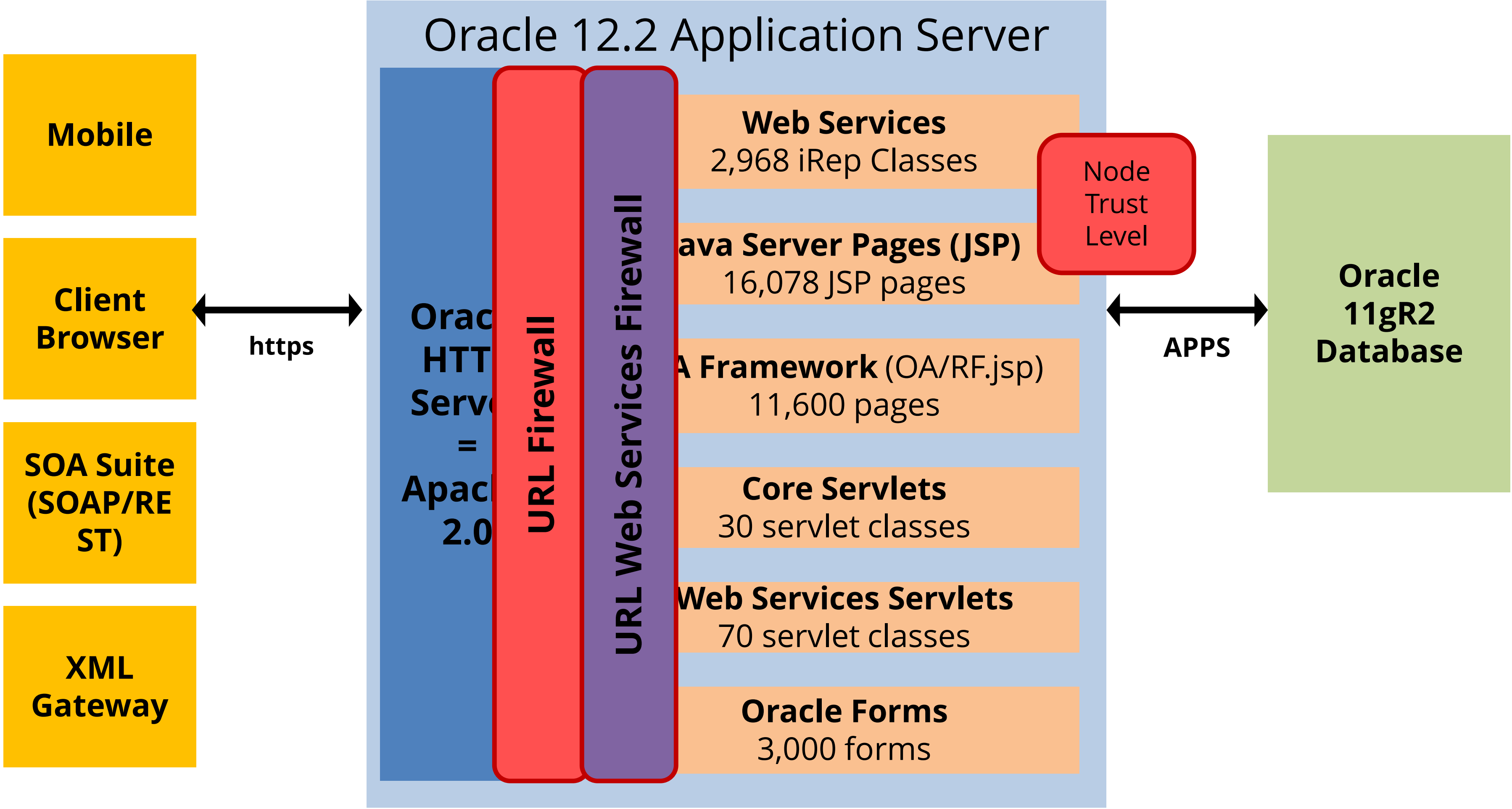
C Firewall between layers block access between layers except for explicitly defined ports.

Oracle EBS DMZ Configuration



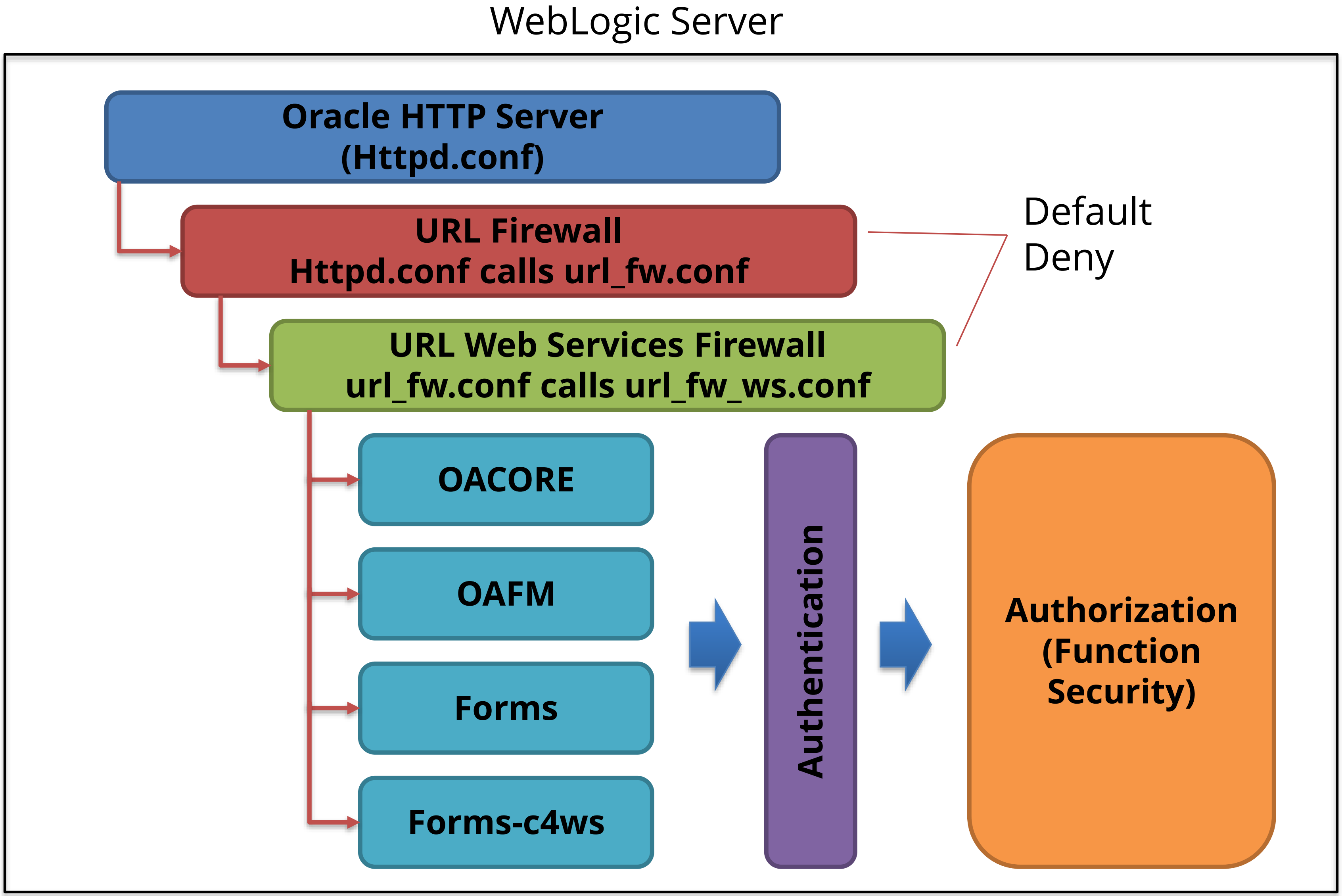
- Proper **DMZ configuration** reduces accessible pages and responsibilities to only those required for external access. Reducing the application surface area eliminates possible exploiting of vulnerabilities in non-external modules.

DMZ Step Appendix E – URL Firewall(s)



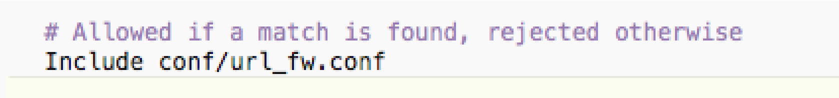
- **URL Firewall** in Appendix E is absolutely mandatory. Configure using **url_fw.conf**
- **URL WS Firewall** in Appendix E is absolutely mandatory. Configure using **url_fw_ws.conf**

Oracle E-Business Suite 12.2 WebLogic Server



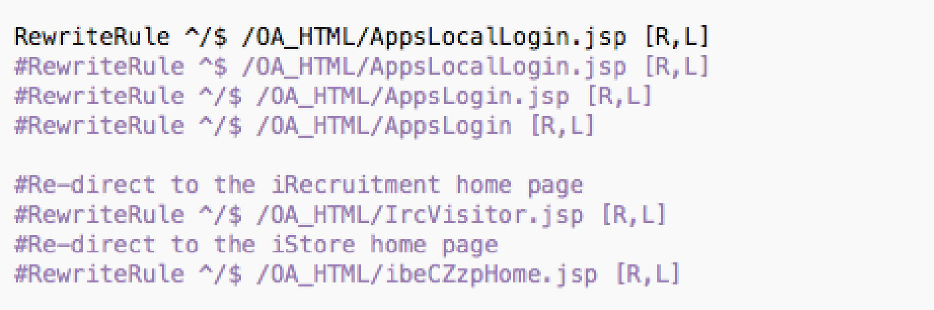
Examples

httpd.conf



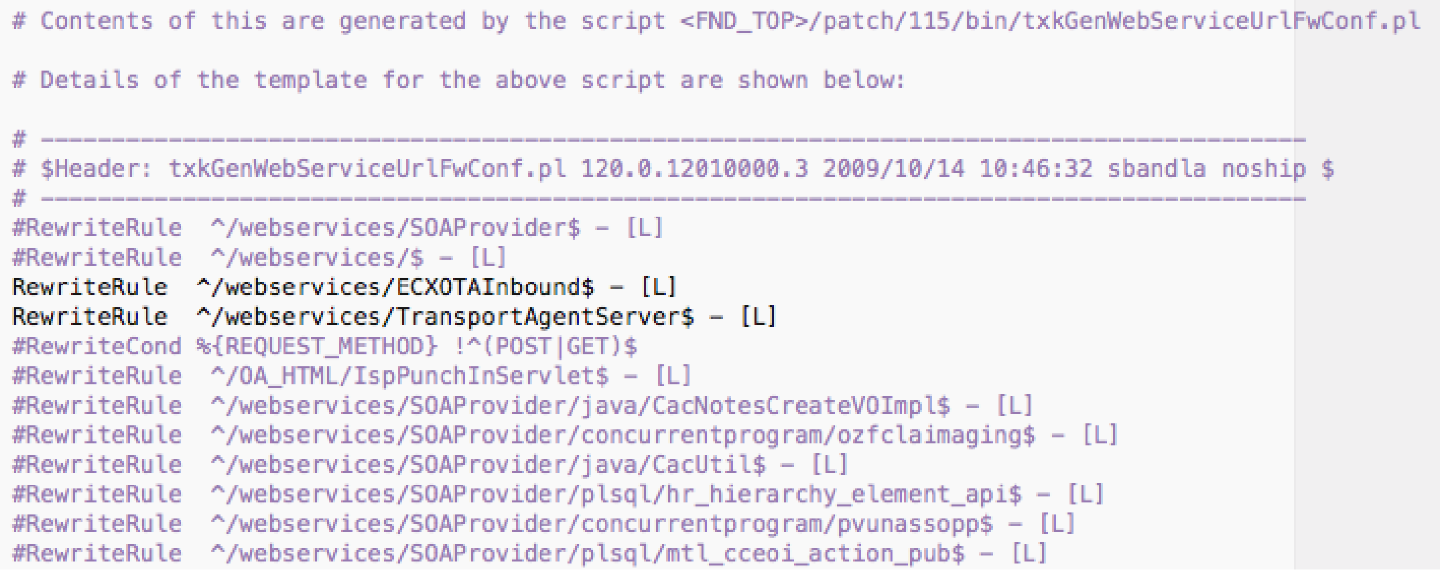
```
# Allowed if a match is found, rejected otherwise
Include conf/url_fw.conf
```

url_fw.conf



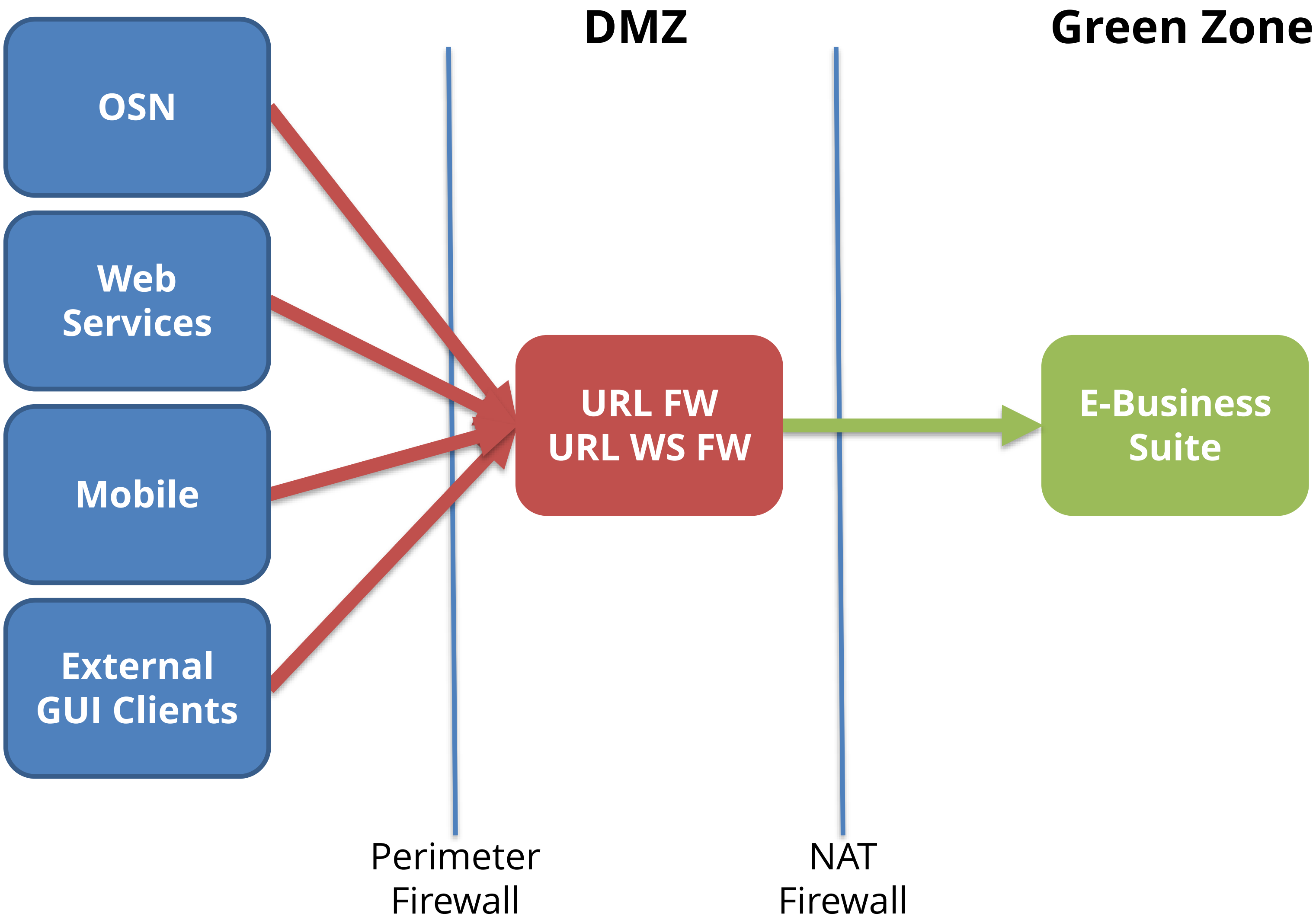
```
RewriteRule ^/$ /OA_HTML/AppsLocalLogin.jsp [R,L]
#RewriteRule ^$ /OA_HTML/AppsLocalLogin.jsp [R,L]
#RewriteRule ^/$ /OA_HTML/AppsLogin.jsp [R,L]
#RewriteRule ^/$ /OA_HTML/AppsLogin [R,L]

#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]
```

url_fw_ws.conf

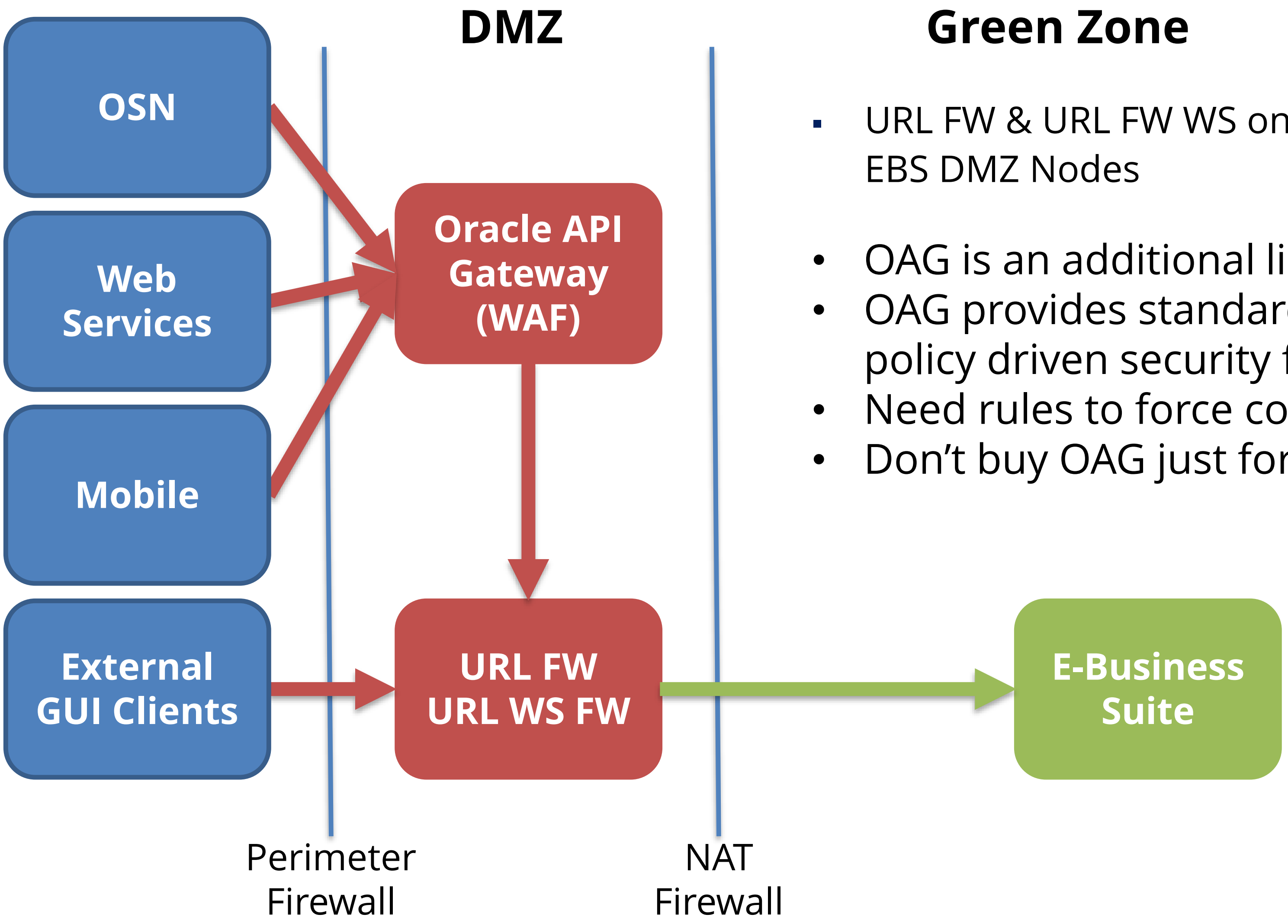


```
# Contents of this are generated by the script <FND_TOP>/patch/115/bin/txkGenWebServiceUrlFwConf.pl

# 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]
```

Standard Web Services External Deployment



Recommended Web Services External Deployment

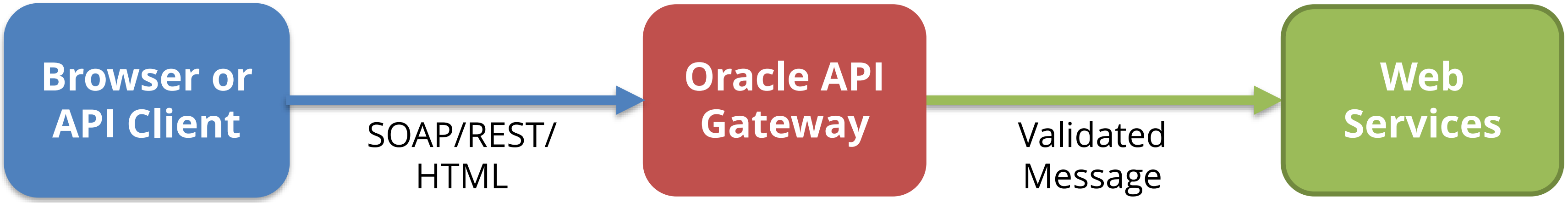


- URL FW & URL FW WS only exists in EBS DMZ Nodes

- 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

OAG Provides Specialized WS Protection

- DOS
  - Flooding, recursive & oversized playloads
- 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

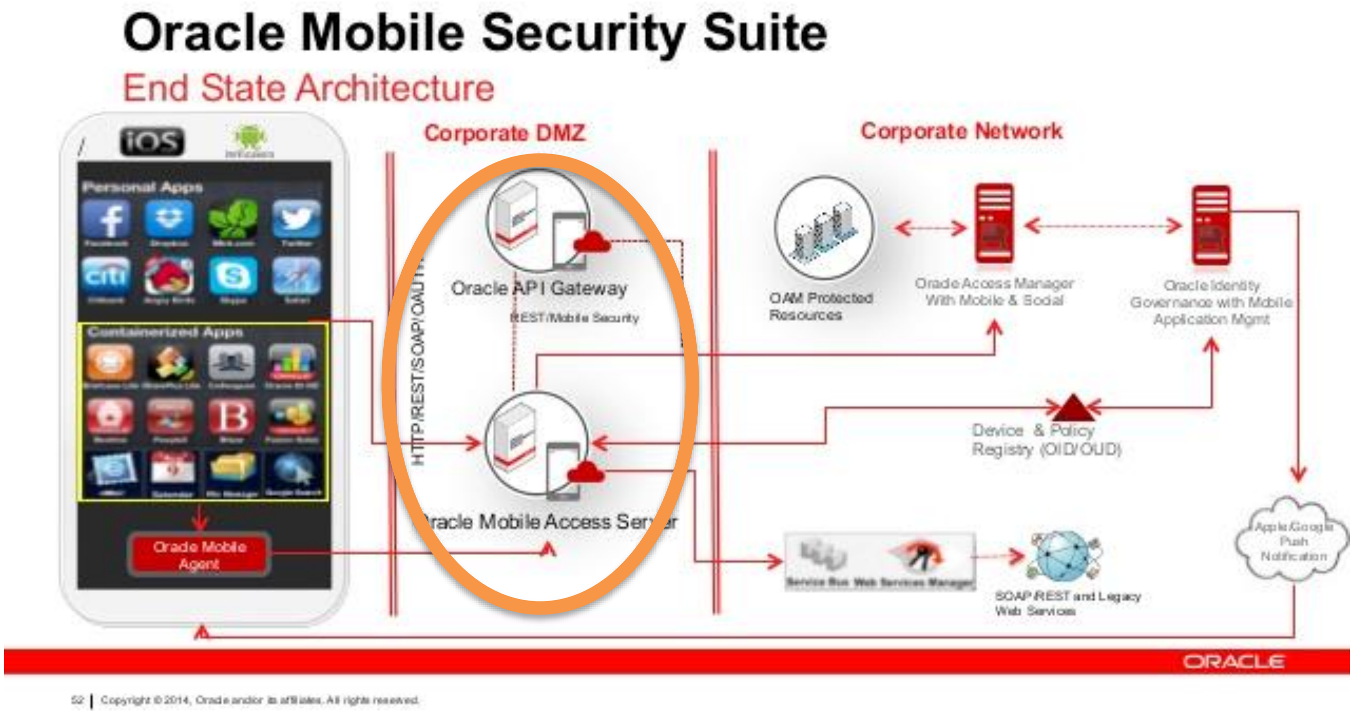


External E-Business Web services Recommendation

- **Web services come with the E-Business Suite**
  - You need to secure them even if not using
- **Use tokens where possible for authentication**
  - Passwords are weak
- **Regularly audit function security for web services authorization**
  - Same as for users
- **Deploy purpose built security features**
  - Carefully deploy URL_FW_WS.conf
  - License and configure OAG
- **Log and Monitor**
  - Threat actors will use REST calls same as a Form

What about Mobile and Tablets?

If not using VPN additional products are required to secure Mobile



Oracle Mobile Security Suite

End State Architecture

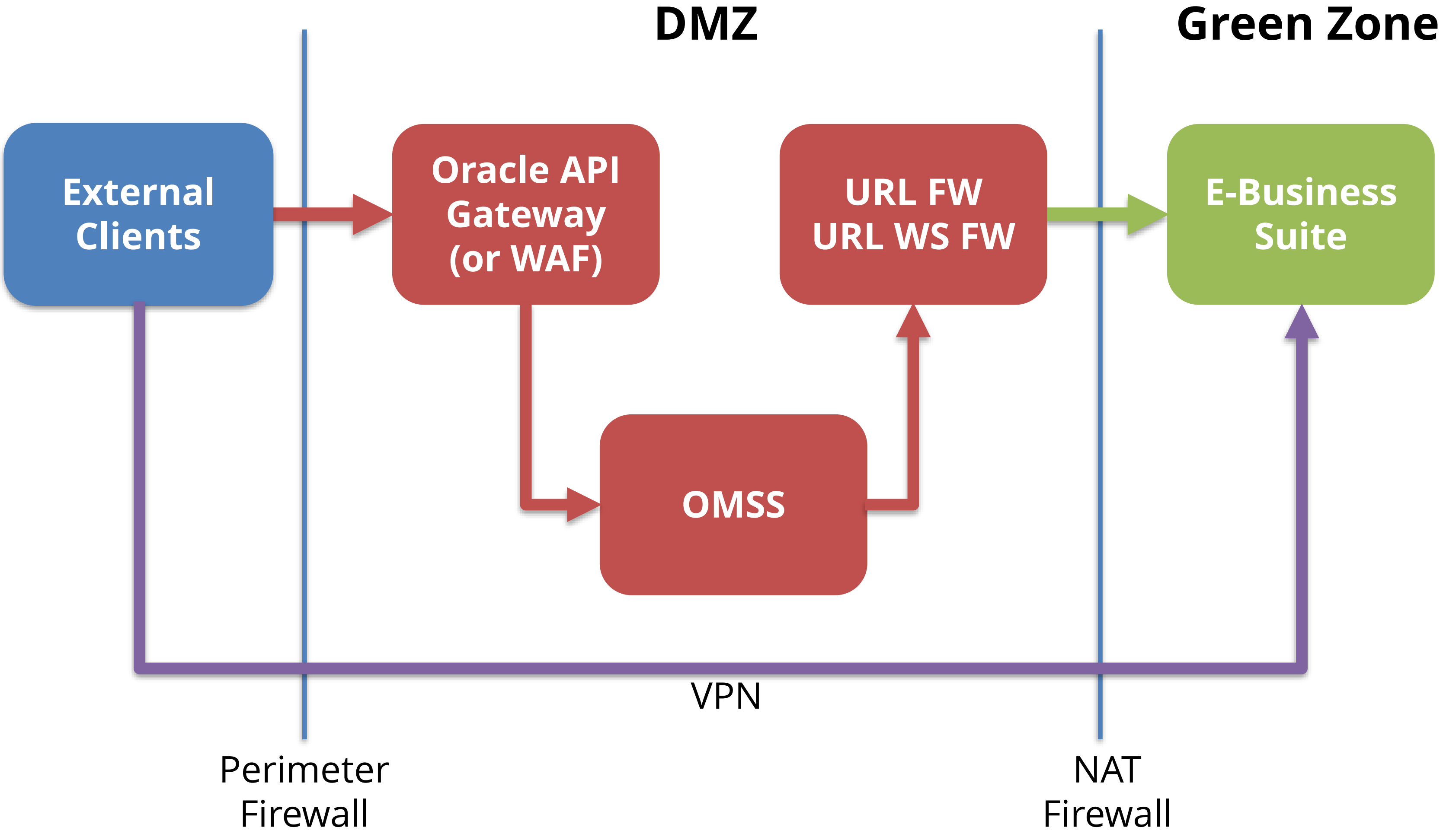
iOS
Corporate DMZ
Corporate Network
Personal Apps
Containerized Apps
Oracle Mobile Agent
HTTP/REST/SOAP/OAUTH
Oracle API Gateway
REST/Mobile Security
Oracle Mobile Access Server
OAM Protected Resources
Oracle Access Manager With Mobile & Social
Oracle Identity Governance with Mobile Application Mgmt
Device & Policy Registry (OID/OUD)
Service Bus Web Services Manager
SOAP/REST and Legacy Web Services
Apple/Google Push Notification
ORACLE

52 | Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

12.2.5 E-Business Suite Mobile DMZ Deployment

- **Oracle Mobile Security Access Server (OMSS) as part of Mobile 4x**
  - Virtual URLs (e.g. hide internal URL)
  - White & blacklisting
- **Additional license?**
  - Ask your sales rep

Mobile Defense In Depth Options



Mobile Defense Recommendation

- **Use VPN to deploy**
  - Unless have both OAG and OMSS carefully configured as well as url_fw_ws.conf edits

- **Regularly audit mobile function security**
  - Make no assumptions

- **Log and Monitor**
  - Threat actors will use REST calls if they can

Integrigy AppDefend for Oracle EBS

AppDefend is an **enterprise application firewall** designed and optimized for the Oracle E-Business Suite.

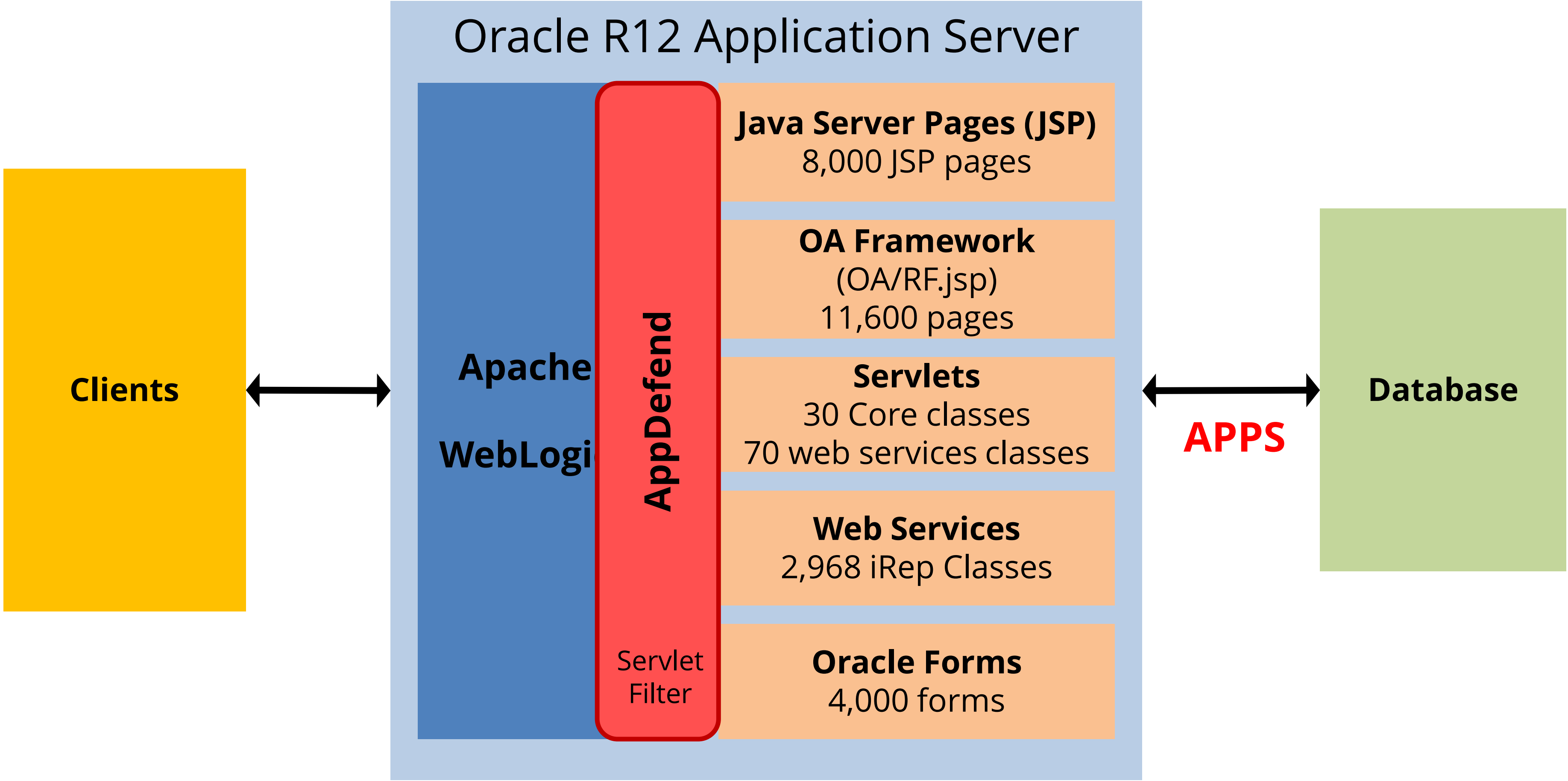
- **Prevents Web Attacks**
  Detects and reacts to SQL Injection, XSS, and Oracle EBS security risks

- **Limits EBS Modules**
  More flexibility and capabilities than URL firewall to identify EBS modules

- **Virtual Patching**
  Detects and blocks known Oracle EBS security vulnerabilities

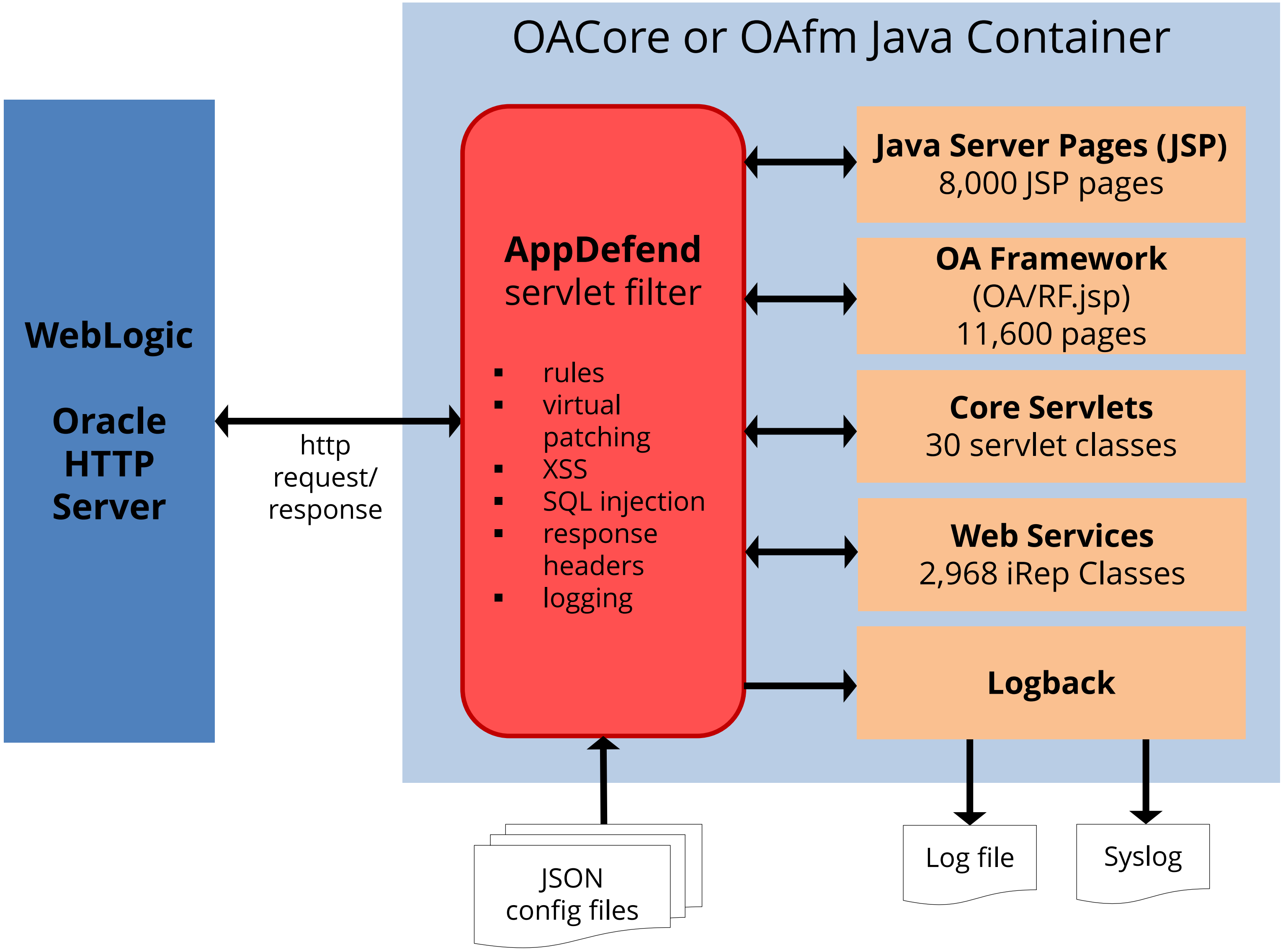
- **Application Logging**
  Enhanced application logging for compliance requirements like PCI-DSS 10.2

AppDefend and Oracle EBS 12.2



- **AppDefend** runs within the Oracle EBS WebLogic Java containers as a servlet filter and monitors all incoming requests and out-going responses. Being in the Java container, AppDefend can access all session state, attributes, error messages, and the database.

AppDefend Architecture



OACore or OAfm Java Container

WebLogic

Oracle HTTP Server

http request/ response

AppDefend servlet filter

- rules
- virtual patching
- XSS
- SQL injection
- response headers
- logging

Java Server Pages (JSP)
8,000 JSP pages

OA Framework
(OA/RF.jsp)
11,600 pages

Core Servlets
30 servlet classes

Web Services
2,968 iRep Classes

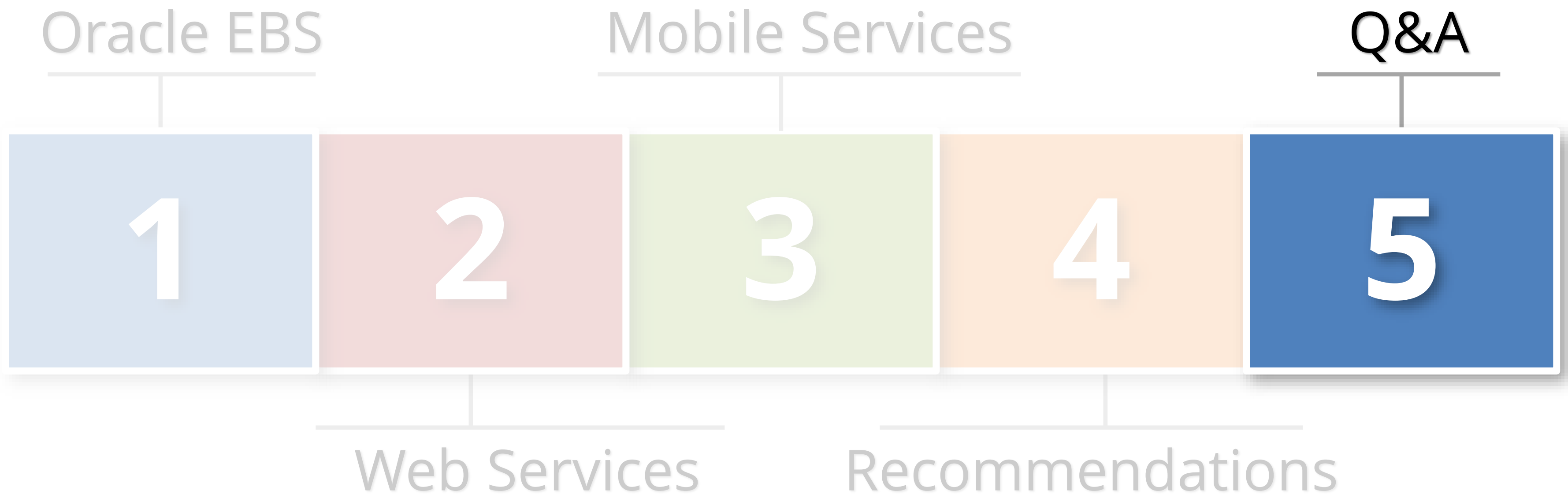
Logback

JSON config files

Log file

Syslog

Agenda



1. Oracle EBS
2. Web Services
3. Mobile Services
4. Recommendations
5. Q&A

Contact Information

Michael Miller

Chief Security Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

youtube: **youtube.com/integrigy**