

ORACLE®



**ENGINEERED
FOR INNOVATION**

**ORACLE
OPEN
WORLD**

ORACLE®

Oracle E-Business Suite Secure Configuration

Erik Graversen

Senior Principal Software Engineer – EBS Security Team

Program Agenda

- Secure Deployment General
- Secure Internal EBS Deployment
- Secure External EBS Deployment
- What's New...
- Running Web Scanning Tools...
- Questions and Answers



Secure Deployment

- Begins with a secure platform
 - Hardened Systems
 - Secure OS patch level
 - Secure OS configuration
 - Secure network/firewall configuration
- Source of information
 - OS vendor hardening guides
 - Best practice check lists – CIS, SANS, DoD STIGs
 - Network equipment vendor documentation – Cisco, F5, ...

Secure E-Business Suite Deployment

- General EBS advice
 - Stay current with patching
 - Critical Patch Updates (CPUs) + Security Alerts
 - Most recent maintenance pack (yes, security improves as well)
 - Follow our recommendations for secure deployment
 - “Secure Configuration Guide for Oracle E-Business Suite”
 - If deploying any parts of EBS to the Internet, follow advice in “Oracle E-Business Suite Configuration in a DMZ”

Secure Configuration Guides

(previously known as “Best Practice” documents)

Fresh off the press....

Secure Configuration Guide for Oracle E-Business Suite Release (11i/12)

- 11i – Note [189367.1](#)
- R12 – Note [403537.1](#)

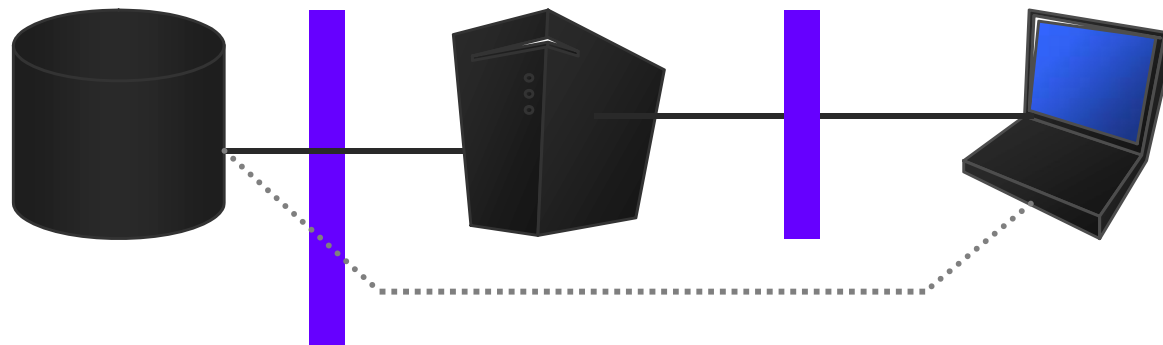
EBS Secure Configuration Guides

- Tells you what security related “switches” to set/verify
- Much advice is now automated via AutoConfig and OAM
- Mentions optional security related products (DB Options)
- Assumes current/supported patch level
 - 11.5.10 and up – 12.0.6 and up – 12.1.2 and up
- To report problems with the advice, have Support log a bug against Product: 510, Component: SEC_COMP

Get Ready...

- So lets get ready for the highlights of securing your E-Business Suite deployment
 - Internal deployment
 - External deployment

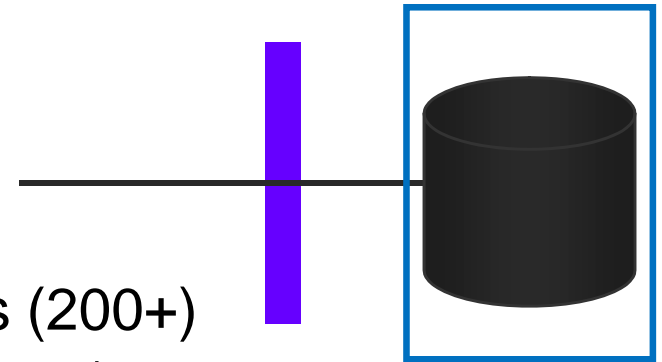
Securing the Internal Deployment



- Internal Components
 - 1 database
 - 1 or more application/web hosts
 - 1 or more end user PCs

Securing the Database

Schema Level

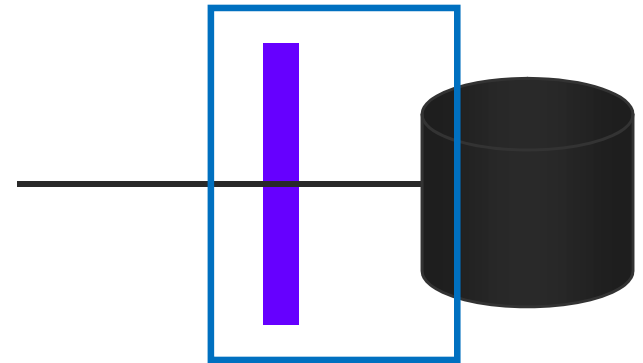


- Secure the open, default schema accounts (200+)
 - Default Password Scanner (FAQ Note 361482.1)
 - Will check for any schema created by an Oracle supplied product!
 - Fix using: `AFPASSWD`, `FNDCPASS`, `alter user...`
- Check privileges on APPLSYSPUB/PUB
 - `$FND_TOP/patch/115/sql/afpub.sql`
- Optionally consider Database Vault for Separation of Duties \$\$
- Optionally consider Transparent Data Encryption for data-at-rest \$\$

Securing the Database

Net Access

- Secure the TNS Listener
 - Enable logging
 - Implement IP address restrictions
 - Enable ADMIN_RESTRICTIONS
 - Do *not* enable listener password (10g and up)
- Optionally enable ASO/ANO network encryption
Note (391248.1|376700.1) \$\$
- listener.ora & sqlnet.ora



Securing the Database – Network Encryption

SQLNET.ORA - Example Config

Release 11i

```
SQLNET.ENCRYPTION_SERVER = REQUIRED
```

```
SQLNET.ENCRYPTION_TYPES_SERVER = (RC4_40,RC4_128)
```

```
SQLNET.CRYPTO_SEED = somelongandrandomstring4you
```

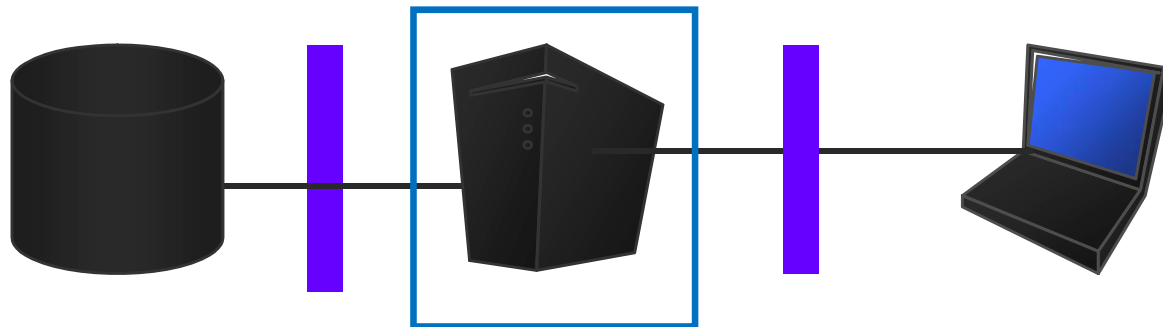
Release 12

```
SQLNET.ENCRYPTION_SERVER = REQUIRED
```

```
SQLNET.ENCRYPTION_TYPES_SERVER = (AES256,AES192,3DES168)
```

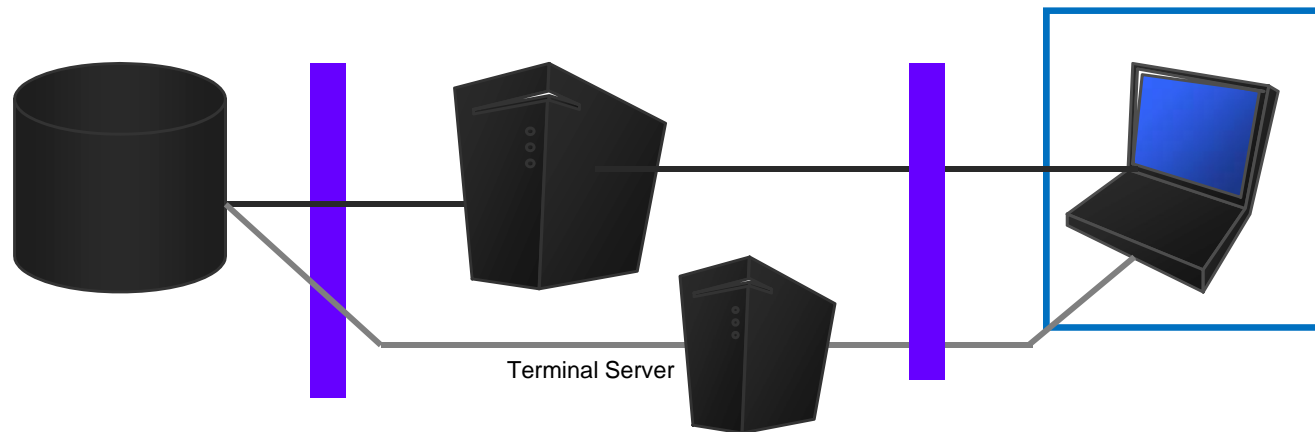
```
SQLNET.CRYPTO_SEED = somelongandrandomstring4you
```

Securing the Applications Webtier



- Enable SSL (https) for web listener
- Avoid weak ciphers and protocols (<128 bit & SSLv2)
- Verify that ModSecurity is active (`/x?p=..`)
- Reduce ModPLSQL White List (11i only)
- runlevel 3; run local-only X-Server on 11i (`DISPLAY=localhost:66`)

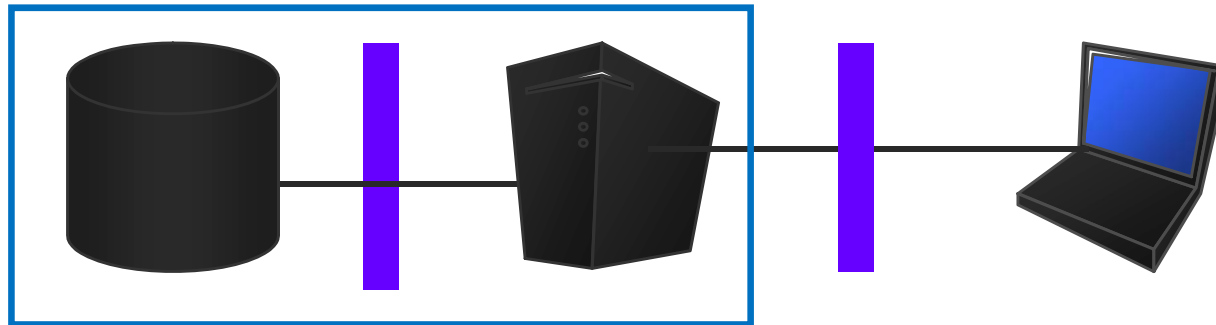
End User PC



- Runs Web Browser and Java Applet User Interface
- Generally not under your control -> untrusted
 - Should not have direct database connection
 - If you are running Client/Server components:
 - Switch to equivalent Web components if possible
 - Put client/server components on a secured server (Note 277535.1)

E-Business Suite Configuration

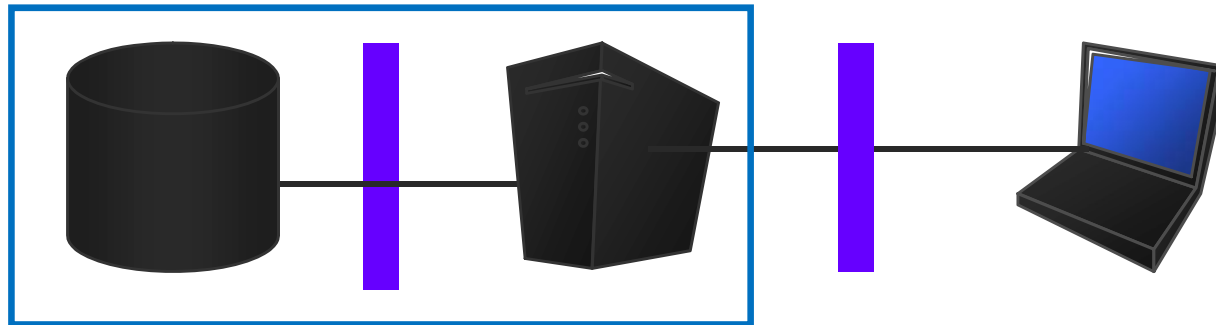
Application Accounts



- Harden EBS Security Setup
 - Secure seeded application accounts, End_Date and change password
 - `fnddefpw.sql` – will list seeded applications accounts with default password
 - The Secure Configuration Guide lists each user and provides advice
 - Switch to hashed passwords for applications users Note 457166.1
 - `FNDCPASS apps/apps 0 Y system/manager USERMIGRATE SHA1`

E-Business Suite Configuration

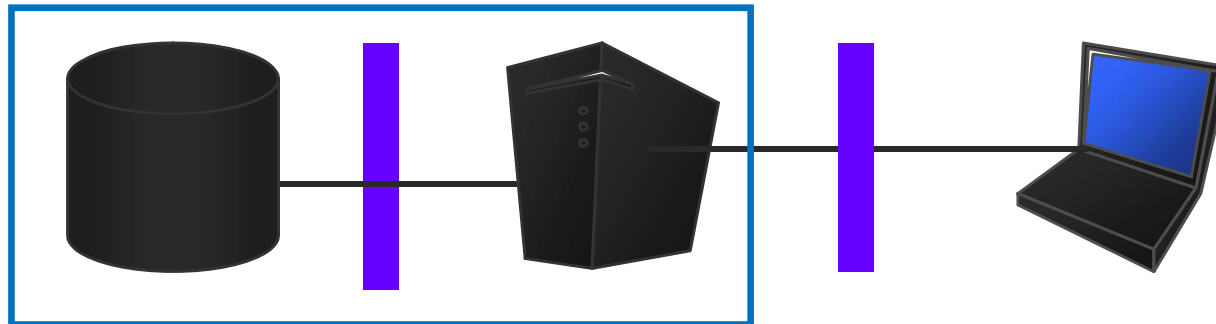
Access Privileges



- Review access to “Sensitive Administrative Pages” Note 1334930.1
- Lists all sensitive Forms + HTML pages and how they are controlled: Function Security, Profile Options, JTF Privileges and Roles
- Note 1334930.1 describes how to use UMX to query this information and contains a SQL script to list them all ...

E-Business Suite Configuration

Profile Options



- Harden EBS Security Setup

- Check settings of critical profile options

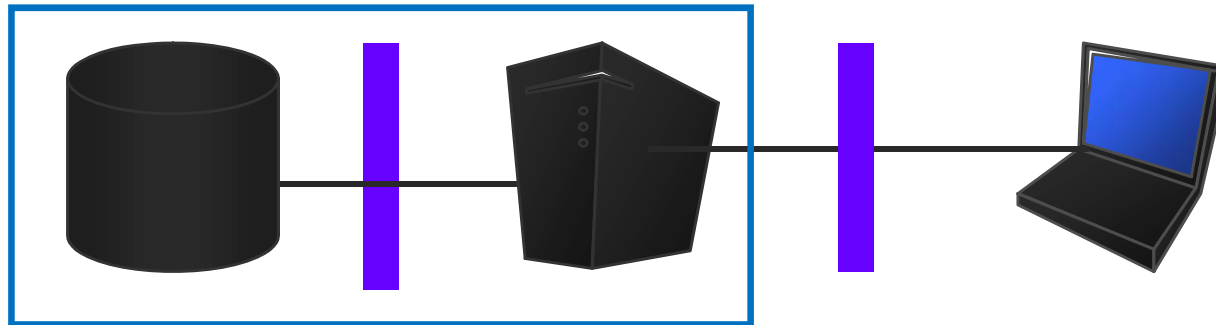
- FND: Diagnostics **NO** FND Validation Level **Error**
 - Utilities: Diagnostics **NO** FND Function Validation Level **Error**
 - Restrict Text Input **Y** Framework Validation Level **Error**

- Note 946372.1 “Secure Configuration of E-Business Suite Profiles”

ORACLE

E-Business Suite Configuration

“Server Security” – SECURE mode



- Ensure the instance is set to SECURE mode
 - Verify using

```
select node_name,server_id,server_address
from FND_NODES where server_address = '*' ;
```

<u>NODE NAME</u>	<u>SERVER ID</u>	<u>SERVER ADDRESS</u>
AUTHENTICATION	SECURE	*

“Server Security” feature

Sample DBC file created by AdminAppServer or AdminDesktop

GWYUID=APPLSYSPUB/PUB

GUEST_USER_PWD=GUEST/ORACLE

FNDNAM=APPS

APPL_SERVER_ID=AC70BE2E89CAC15F...64235254236135131826220

TWO_TASK=PROD

DB_PORT=1521

DB_HOST=pdb1213.example.com

APPS_JDBC_URL=jdbc\:oracle\:thin\:@(DESCRIPTION\=(ADDRESS\=(PROTOCOL\=tcp)(HOST\=pdb1213.example.com)(PORT\=1521)))(CONNECT_DATA\=(SERVICE_NAME\=PROD)))

JDBC\:oracle.jdbc.maxCachedBufferSize=358400

Using AdminDesktop

Use AdminDesktop to create DBC files for non-EBS nodes

- Non-EBS nodes are BPEL and WebService nodes
 - Create the DBC file on an EBS AppTier node
 - Create it to be IP Address specific
 - Maintain mode 600 while creating and copying to the recipient node
- Documented in Note: 974949.1 "AppsDataSource, Java Authentication and Authorization Service, and Utilities for Oracle E-Business Suite".



Deep Breath...

- Take a deep breath – congratulate yourself, the internal deployment issues have now been addressed...

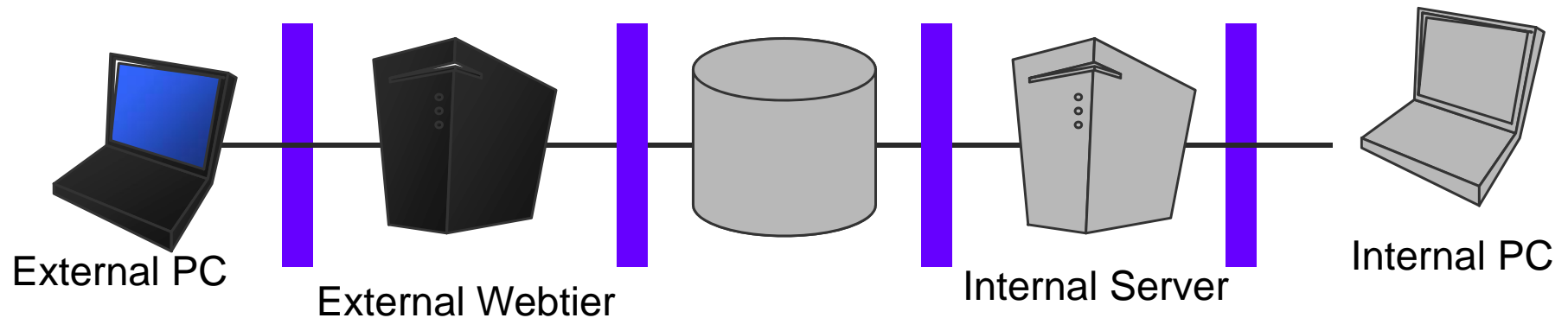
External Deployment



“Oracle E-Business Suite 11i/R12 Configuration in a DMZ”
My Oracle Support Document (287176.1|380490.1)

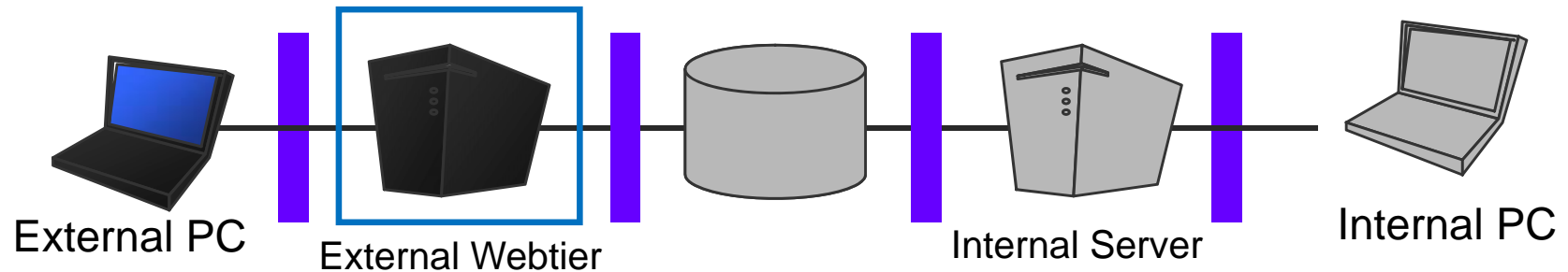
ORACLE

Securing the External Deployment



- Certified, recommended deployment model for external facing modules
 - “Oracle E-Business Suite 11i/R12 Configuration in a DMZ”
Note (287176.1|380490.1) documents the recommendations
 - Certification completed fall 2005, more products certified since then + R12
- One single set of deployment recommendations common to all products

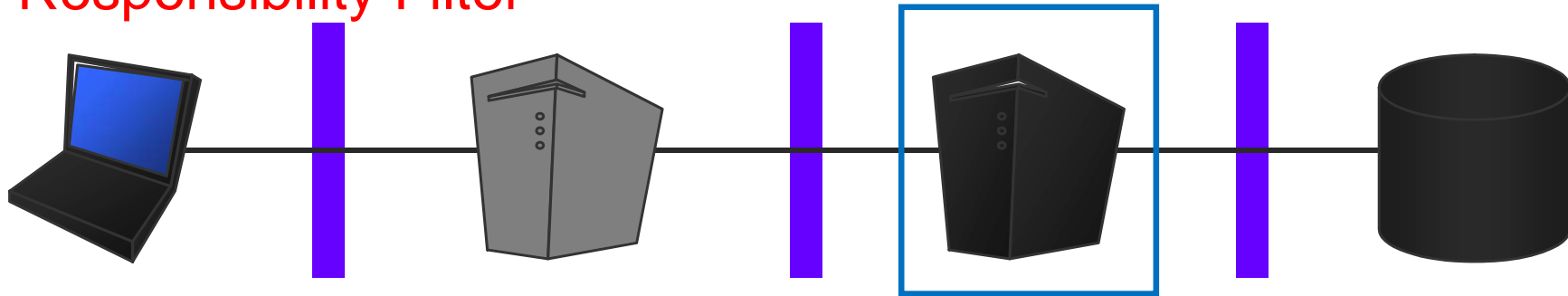
Recommended External Deployment



- External exposure is reduced via an number of “filters”
 - Responsibility filter
 - URL Filter
 - Noise filter
 - “Objection” filter
 - Optional reverse proxy - Web Application Firewall (WAF)
- Simpler to ‘sell’ to your network security group

External Webtier Security

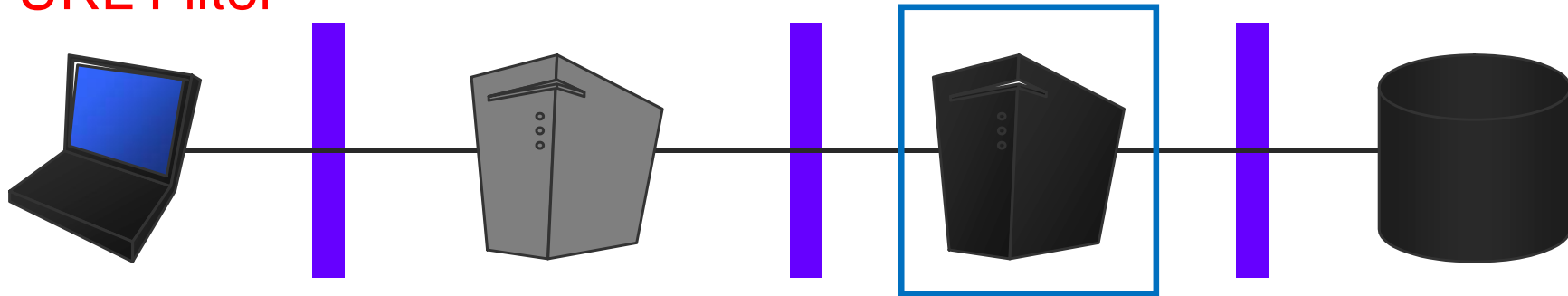
Responsibility Filter



- Mark as External server
 - Node Trust Level (Server Profile Option)
 - Set to "External" for externally facing servers, set to "Normal" at Site level
- Mark Externally available Responsibilities
 - Responsibility Trust Level (Profile Option)
 - Set to "External" for externally available responsibilities
- No access to SysAdmin, HR, Financial responsibilities

External Webtier Security

URL Filter



- Enable URLs required for externally exposed products
 - Edit `url_fw.conf` to reflect required external products
- URL filtering allows only pages required for the external product(s) actually deployed (white list)
 - Mitigates the "unnecessary code" problem

URL Firewall – Example Config

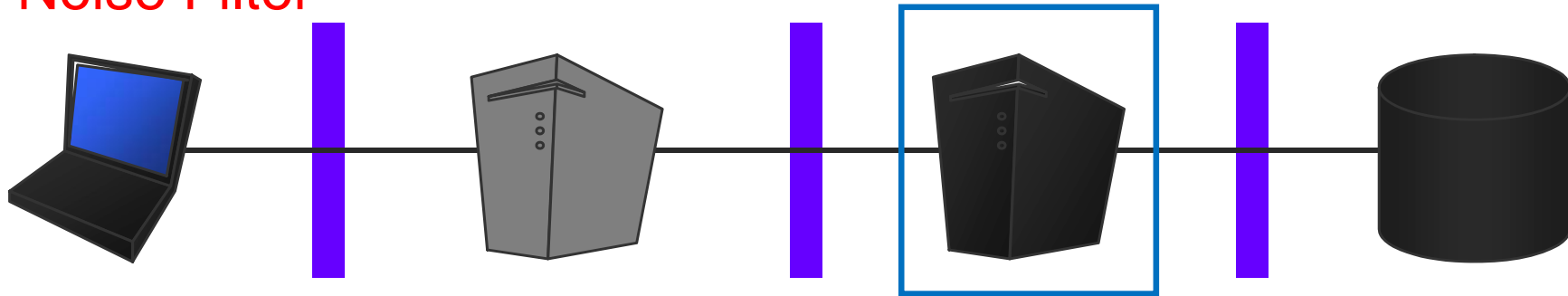
```
# Initial setup mod_rewrite
RewriteEngine On
RewriteLog logs/rewrite_log
RewriteLogLevel 0

# The White List of all Required URLs
RewriteRule ^/OA_MEDIA/.*\.(gif|jpg|jpeg|bmp)$ - [L]
RewriteRule ^/OA_HTML/.*\.(js|css|xss)$ - [L]
RewriteRule ^/OA_HTML/.*\.(htm|html)$ - [L]
RewriteRule ^/OA_HTML/Login\.jsp$ - [L]
RewriteRule ^/OA_HTML/Logout\.jsp$ - [L]
RewriteRule ^/OA_HTML/External_.*\.jsp$ - [L]

# If not allowed by list above - go away [G=410-Gone]
RewriteRule .* - [G]
```

External Webtier Security

Noise Filter



- ModSecurity - WAF apache module
 - Part of iAS 1.0.2.2 and OHS 10.1.3
 - Automatically configured
- ModSecurity blocks “bad” requests (black list) – can also white list
 - Null bytes, directory crawling, URL encoding, UTF-8 encoding
 - Stops “obviously bad” requests early

ModSecurity – Example Config

```
LoadModule security_module libexec/mod_security.so
AddModule mod_security.c

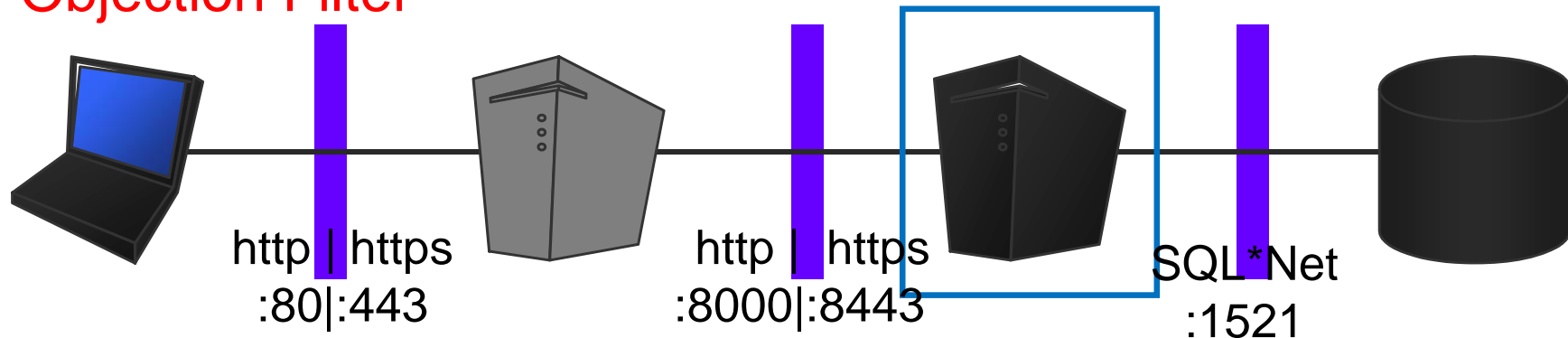
SecAuditEngine On
SecAuditLog logs/sec_audit.log
SecFilterScanPOST On
SecFilterForceByteRange 1 255
SecFilterCheckURLEncoding On
SecFilterCheckUnicodeEncoding Off
SecFilterDefaultAction "deny,log,status:400"

SecFilter "\.\.\/"
SecFilterSelective REQUEST_METHOD "!(GET|HEAD|POST)"
SecFilterSelective ARGS_NAMES \
    "!^[-_|#!=A-Za-z0-9/ :,.${}]*$"

```

External Webtier Security

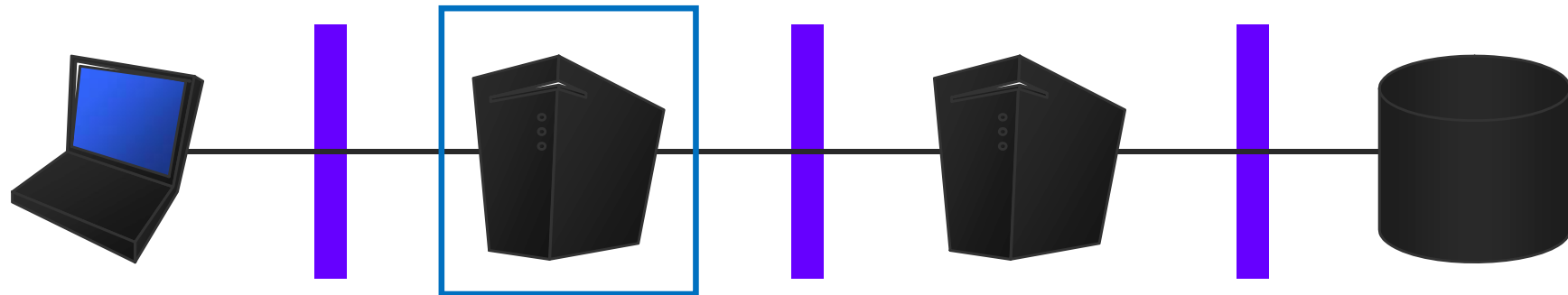
Objection Filter



- Only web ports required to be open
 - Uses https (and http) to external webtier (or proxy)
 - Uses https or http from proxy to external webtier
 - Uses (optionally encrypted) SQL*Net from external webtier to database
- Easier to sell to the network security team
 - No split horizon DNS required (we have server level profiles)
 - No access required from intranet to DMZ(s)

DMZ Security Enhanced Reverse Proxy

(Optional) Web Application Firewall - WAF



- Relays valid requests to Application Server
 - No applications code on this tier
 - Apache-2 reverse proxy
 - URL filtering allows only required pages (white list)
 - ModSecurity blocks “obviously bad” requests (black list) + some white listing
 - Allows you to run external webtier on high port (no root req)



Deep Breath...

- Take a deep breath – congratulate yourself, the external deployment issues have now been addressed...

What's New

Security Related News

- Stricter Profile Option Settings [FND_%VALIDATION] (11.5.10.2+)
- Non-Reversible password hashing for FND_USERS
- AFPASSWD is a FNDCPASS replacement (12.1.3)
- Start/Stop CM without APPS password (12.1.3)
- DO3475 “PUBLIC Grants on Restricted Packages”

- Certified with Database Vault
- Certified with Transparent Data Encryption (Col & TS)

Q&A

ORACLE®

Running Web Scanning Tools

AppScan, WebInspect, HailStorm, ...

- Over the years Oracle has run web scanning tools such as AppScan and WebInspect against EBS and a number of our customers have also submitted reports generated by these tools
- In the next few slides I will share our observations on what they're good at, and let you know of a few FFFPs (Frequently Found False Positives).

Running Web Scanning Tools

Issue Types...

- **Reflected XSS and Header splitting**
 - Generally these are accurate findings
- **Stored XSS**
 - not so much
- **Insecure Cookie setting**
 - Most tools assume the servlet cookie is our session cookie
- **SQL-Injection**
 - These are generally false positives

Running Web Scanning Tools

Potential SQL Injection

- **PL/SQL Data Validation errors ORA-06502**
 - PL/SQL: character string buffer too small
 - PL/SQL: numeric or value error: number precision too large
 - PL/SQL: numeric or value error: hex to raw conversion error
- **DoS-ed Server**
 - JDBC errors such as “**read() returned -1**”
may cause the tool to conclude that there is a possible SQL Injection, when the real cause is the the connection pool is exhausted

Recommended Reading List

- “Oracle E-Business Suite 11i/R12 Configuration in a DMZ”
Note (287176.1|380490.1)
- “Enhancing Oracle E-Business Suite Security with Separation of Duties” Note 950018.1
 - Separation of Duties using Patch Manager Note1363260.1
- E-Biz Blog at <http://blogs.oracle.com/stevenChan>

ORACLE®