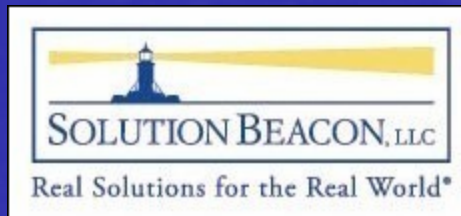
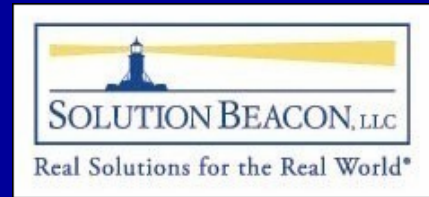


Configuring a Linux Apache Proxy Server for Use with Supplier

James J. Morrow
NorCal OAUG Training Day
Santa Clara Convention Center
January 17, 2007



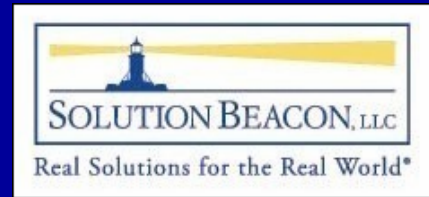
Introduction



◆ The following will be covered

- References and Definition
- Purpose of a Proxy Server
- Reverse Proxy Options
- The Selected Reverse Proxy Option
- Metalink Note Author's Choice
- mod_rewrite/url firewall purpose
- Building the Reverse Proxy Server
- Configuring the URL Firewall
- Creating the External Webtier
- Adjusting Configuration Files
- Environment Diagram
- Updating the External Webtier Context File
- Updating All Webtier Context File

References and Definition



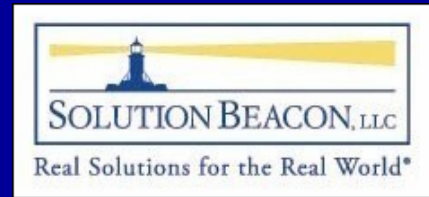
◆ Presentation Reference

- Metalink Note:287176.1 (DMZ Configuration with Oracle E-Business Suite 11i)
- Is the note still relevant?
- Several implementations

◆ Reverse Proxy Server Definition

- A reverse proxy server is an intermediate server that sits between a client and the actual web server and makes requests to the web server on behalf of the client. The client is unaware of the presence of the reverse proxy

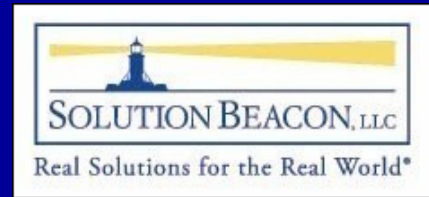
Purpose of a Proxy Server



◆ Why use a proxy server?

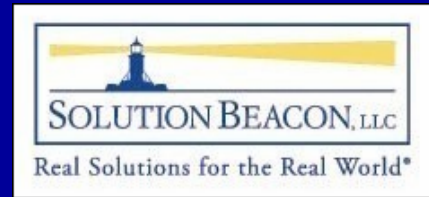
- Adds a level of isolation between the client and the actual server
- Allows using standard web port numbers (80 and 443) on the external interface while running the actual web server on higher numbered ports thus avoiding having to start the actual web application server processes as root.
- Allows certain rules (or filters) to limit the http requests that are presented to the actual web server
- Optionally allows for caching of contents

4 Reverse Proxy Options



- ◆ Which reverse proxy option?
 - Use Oracle 9i Application Server 1.0.2.2 as shipped with Oracle E-Business Suite
 - Use Oracle Application Server Webcache
 - Use apache httpd from <http://httpd.apache.org>
 - Use any of a number of commercially available reverse proxies, which often provide some level of added security as well.

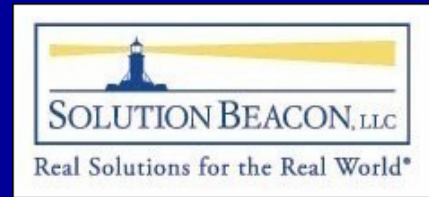
The Selected Reverse Proxy Option



◆ Option 3 – Apache httpd

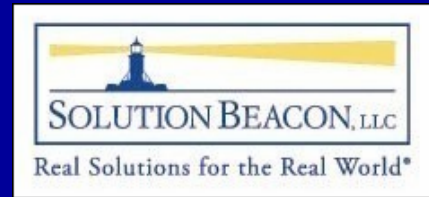
- After looking at the pros/cons presented in note 287176.1 option 3 was chosen due to its advantages and lack of a serious disadvantage
 - ◆ pros
 - Reputable provider of open source software
 - Available on many platforms
 - Can be configured and built to only include the required modules
 - Widely used Web server
 - Can directly use the URL Firewall as mod_rewrite module can be configured with this server
 - Certified with Oracle E-Business Suite in DMZ configuration
 - Well Known, Well documented

Metalink Note Author's Choice



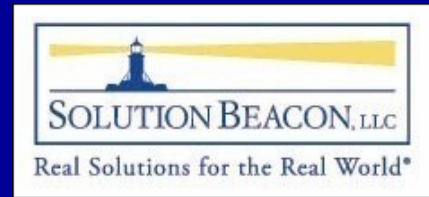
- ◆ The author of the metalink note chose option 3 also because...
 - can be built in a minimum configuration
 - supports HTTP/1.1 for better performance
 - Is well known, and the configuration steps described for the apache based reverse proxy will be useful when configuring any other reverse proxy

mod_rewrite/url firewall purpose



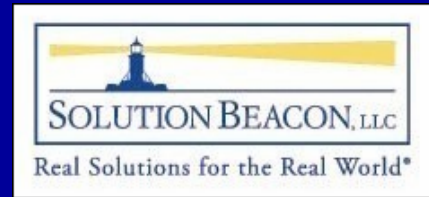
- ◆ mod_rewrite and url firewall were mentioned a few slides prior
 - mod_rewrite is used for rewriting a URL at the server level, giving the user output for that final page. So, for example, a user may ask for `http://www.somesite.com/widgets/blue/`, but will really be given `http://www.somesite.com/widgets.php?colour=blue` by the server
 - A URL Firewall ensures only URLs required for the externally exposed functionality can be accessed from the internet
 - Optimally a URL Firewall would be deployed on the reverse proxy server

Building the Reverse Proxy Server



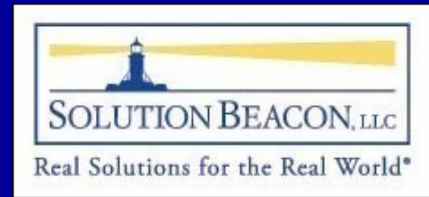
- ◆ Download apache (2.0.59) from <http://httpd.apache.org/>
- ◆ un tar the downloaded TAR balls: `tar xzf <gz filename>`
- ◆ Check the tar ball: `md5sum -c httpd-2.0.59.tar.gz.md5`
- ◆ Configure Apache
 - Put the command mentioned below in a file named `runc.sh`
 - I modified the configure command example in the note so the parms were on 1 continuous line
 - `./configure -prefix /dmz \ <see note for 19 required parms>`
 - The configure command will produce several pages of output to the screen

Building the Reverse Proxy Server



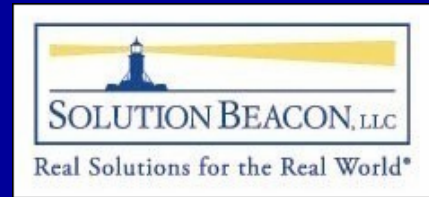
- ◆ adjust the source of `mod_proxy.c` to ensure that `mod_proxy` does not proxy a request to the external web tier before the URL firewall based on `mod_rewrite` has a chance to reject it
 - `ap_hook_translate_name(proxy_trans, aszSucc , NULL, APR_HOOK_FIRST);`
 - ◆ `aszSucc` is a NULL-terminated array of strings that name modules whose hooks should succeed this one
- ◆ `cd $HOME/src/httpd-2.0.59` and execute: `make`
- ◆ the results of `./httpd -l` will differ from the metalink note

Building the Reverse Proxy Server



- ◆ this is the list received for version 2.0.59
 - core.c mod_access.c mod_auth.c mod_log_config.c mod_headers.c mod_setenvif.c mod_proxy.c proxy_connect.c proxy_ftp.c proxy_http.c mod_ssl.c prefork.c http_core.c mod_mime.c mod_dir.c mod_rewrite.c mod_so.c
 - These 2 additional modules are delivered with 2.0.59: proxy_connect.c proxy_ftp.c and are not shown in the list in appendix D of the metalink document

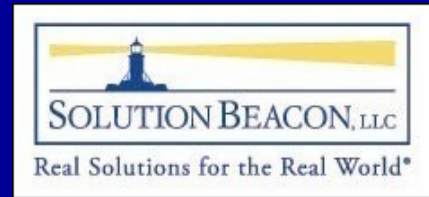
Building the Reverse Proxy Server



◆ install apache to /dmz

- \$ umask 022
- \$ make install
- install mod_security, note that mod_security.c doesn't exist. So, used mod_security2.c: /dmz/bin/apxs -cia mod_security2.c
- since this is being done as non root, unix sysadmin must do port translation in the firewall and you must use a port other than 80 (modify httpd.conf and apachectl)

Building the Reverse Proxy Server



◆ Sysadmin port translation setup example

- User Access Verification

Password:

Type help or '?' for a list of available commands.

```
pixfirewall> enable
```

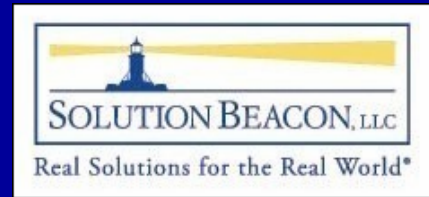
```
Password: *****
```

```
pixfirewall# config t
```

```
pixfirewall(config)# clear xlate interface outside
```

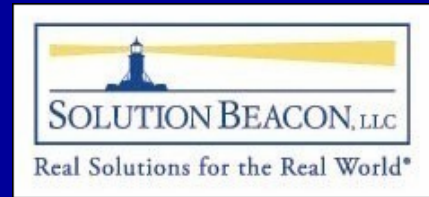
```
global 123.45.67.89 netmask 255.255.255.255
```

Building the Reverse Proxy Server



- ◆ Sysadmin port translation setup example...
 - pixfirewall(config)# static (inside,outside)
tcp 123.45.67.89 80 192.168.100.1 4480 netmask
255.255.255.255 0 0
pixfirewall(config)# access-list outside_access_in line 6
permit tcp any host 123.45.67.89 eq 80
pixfirewall(config)# access-group outside_access_in in
interface outside
pixfirewall(config)# exit
pixfirewall# exit
Logoff
Connection closed by foreign host.

Building the Reverse Proxy Server



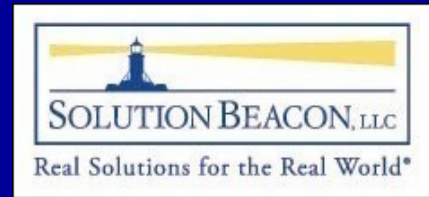
- ◆ start the server using apachectl (w/o ssl)
 - /dmz/bin/apachectl start
- ◆ Verify it is running on port 4480
 - netstat -lntp | sort -t: +1n

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	:::4480	:::*	LISTEN	22797/httpd

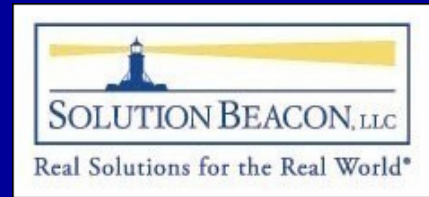
- ◆ Login via: <http://<hostname:port>/index.html.en>

Building the Reverse Proxy Server



- ◆ stop apache: `/dmz/bin/apachectl stop`
- setup a self signed certificate for testing purposes – these may have changed with the new version
 - ◆ `$ cd /dmz/conf`
 - ◆ `$ umask 022`
 - ◆ `$ mkdir ssl.key`
 - ◆ `$ mkdir ssl.crt`
 - ◆ `$ mkdir ssl.crl`

Building the Reverse Proxy Server



- setup a self signed certificate for testing purposes...
 - ◆ `$ openssl req -new -x509 -days 30 -keyout ssl.key/server.key -out ssl.crt/server.crt -subj '/CN=Test-Only Certificate'`
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'ssl.key/server.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

`$ chmod 600 ssl.key/server.key # private key`

Building the Reverse Proxy Server



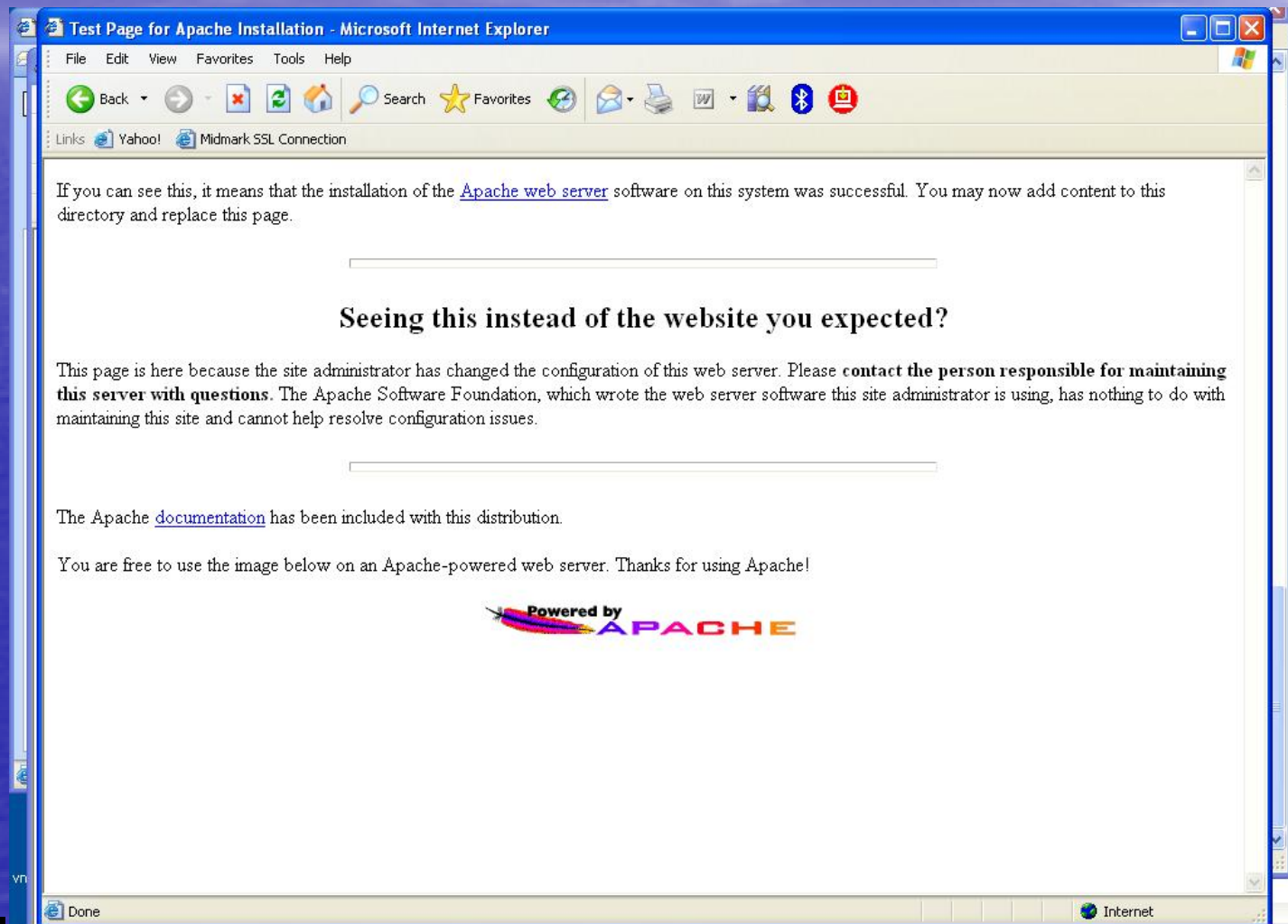
- ◆ start apache with ssl: `/dmz/bin/apachectl start`
- ◆ Verify it is running on port 4438
 - verify: `netstat -lntp | sort -t: +1n`

Active Internet connections (only servers)

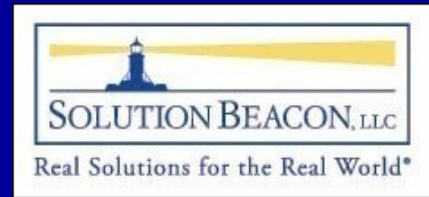
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	:::4483	:::*	LISTEN	1654/httpd
tcp	0	0	:::4480	:::*	LISTEN	1654/httpd

- ◆ also verify via browser specifying http and https in your url

Building the Reverse Proxy Server

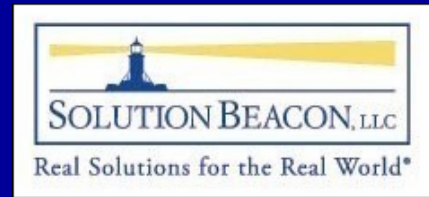


Building the Reverse Proxy Server



- ◆ configure the runtime settings in the configuration files
 - Configure Apache httpd (on port 4480)
 - Configure mod_ssl and certificate (on port 4438)
 - Configure mod_proxy (pass entire URL space to external webtier)
 - Configure mod_security

Configuring the URL Firewall



```
cp $IAS_ORACLE_HOME/Apache/Apache/conf/url_fw.conf /dmz/conf
edit /dmz/conf/url_fw.conf:
```

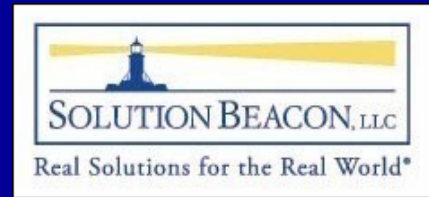
double check to ensure the STATIC, COMMON and LOCAL blocks are uncommented, did not Configure Initial Page

UNCOMMENT POS (since this is for iSupplier):

```
#=====
#Include URLs for product POS (iSupplier Portal)
#=====
```

```
RewriteRule ^/OA_HTML/jsp/pos/suppreg/SupplierRegister\.jsp$ - [L]
RewriteRule ^/OA_HTML/jsp/pos/registration/RegistrationReply\.jsp$ - [L]
RewriteRule ^/OA_HTML/AppsChangePassword\.jsp$ - [L]
```

Configuring the URL Firewall



```
edit /dmz/conf/url_fw.conf...
```

```
uncomment HELP:
```

```
#=====
```

```
# Include PLS Help -
```

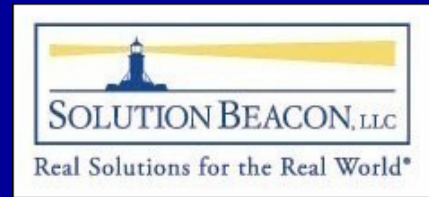
```
RewriteRule ^/OA_HTML/jsp/fnd/fndhelp\.jsp$ - [L]
```

```
RewriteRule ^/pls/[^/]*/fnd_help.search$ - [L]
```

```
RewriteRule ^/pls/[^/]*/fnd_help.Advanced_Search_Page$ - [L]
```

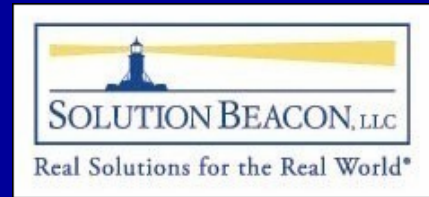
```
RewriteRule ^/pls/[^/]*/fndgfm/fnd_help.get/(.*) - [L]
```

Creating the External Webtier



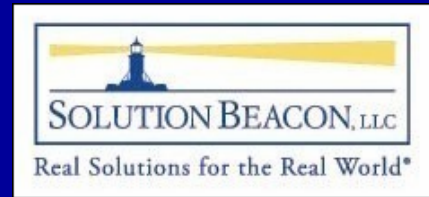
- Create external webtier
 - ◆ Clone internal middle tier to external web-tier box
 - ◆ Enable only web portion by adjusting tier tags in context file (\$APPL_TOP/admin/<context file>)
 - ◆ Named extweb.mycompany.net
- “Connect the dots” (rp proxy server, ext tier)
 - ◆ Per DMZ doc, update hierarchy type
 - ◆ Update node trust level
 - ◆ Update list of responsibilities
 - ◆ Update home page node to frame work

Adjusting Configuration Files



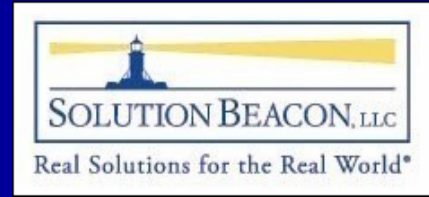
- The metalink note provides downloads of 2 files with appropriate configuration settings. They have to be modified to reflect your paths: You will have to modify the file to reflect your host and domain names and the location for /dmz. Once you have modified the above two configuration files and copied them to /dmz/conf/ it is time to test the proxy

Adjusting Configuration Files

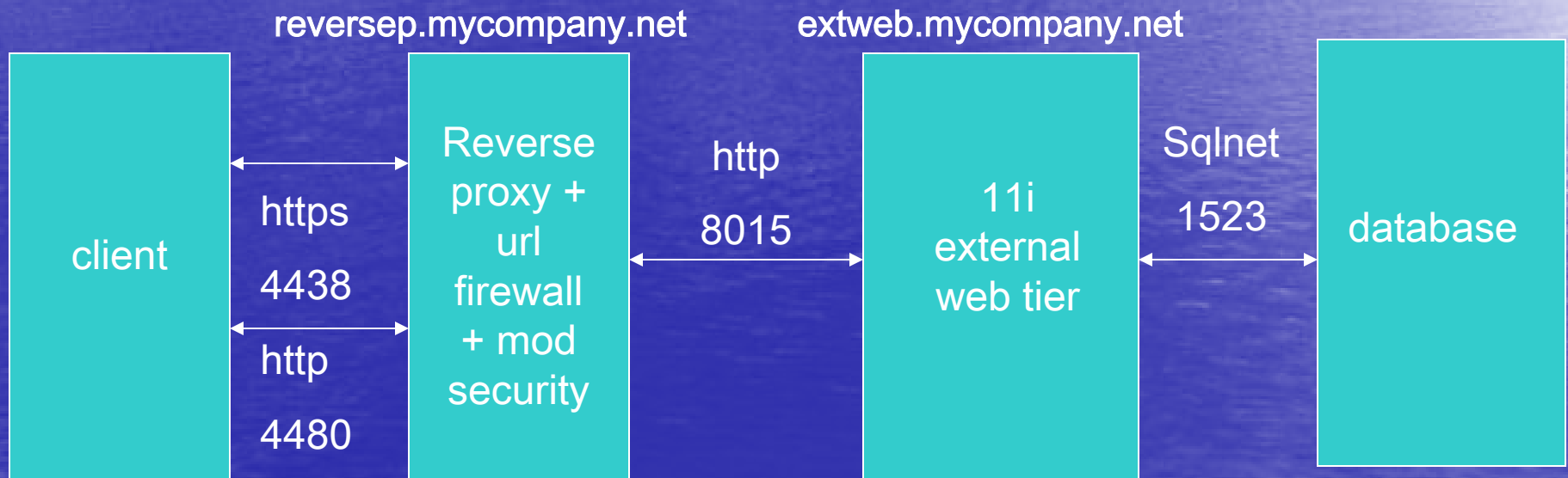


- ◆ The assumptions made while creating these config files are:
 - the reverse proxy will be accessed via the hostname reversep.mycompany.net
 - the E-Business Suite external webtier is called extweb.mycompany.net
 - the server admin is webmaster@mycompany.net
 - the apache proxy was configured and installed to /dmz

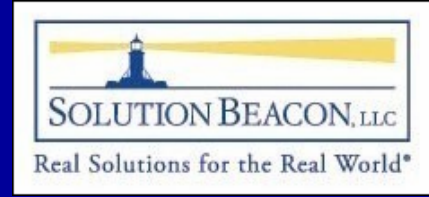
Environment Diagram



◆ Placement of RP Server

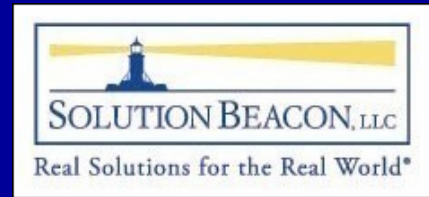


Updating the External Webtier Context File



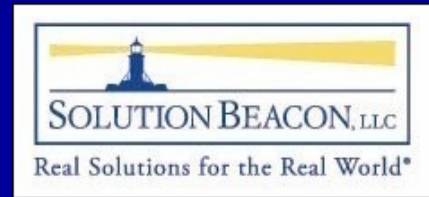
- ◆ Update the Oracle E-Business Suite Context File (non-ssl example)
 - Use OAM or modify the File name:
\$APPL_TOP/admin/<sid>_<hostname>.xml (make sure you back it up before modifying)
 - ◆ <webentryhost oa_var="s_webentryhost">reversep</webentryhost>
 - ◆ <webentrydomain
oa_var="s_webentrydomain">mycompany.net</webentrydomain>
 - ◆ <activewebport oa_var="s_active_webport"
oa_type="PORT">4480</activewebport>
 - ◆ <webentryurlprotocol
oa_var="s_webentryurlprotocol">http</webentryurlprotocol>
 - ◆ <login_page
oa_var="s_login_page">http://reversep.mycompany.net:4480/oa_servlet
s/AppsLogin</login_page>

Updating All Webtier Context Files



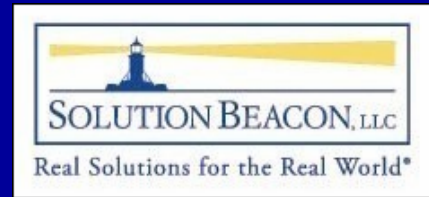
- ◆ Update the Oracle E-Business Suite Context File
 - Run autoconfig on each applications middle tier
- ◆ Additional SYSADMIN tasks
 - set profile: POS: External URL
 - ◆ <http://reversp.mycompany.net:4480>
 - Set profile: POS: Internal URL
 - ◆ <http://appserver.mycompany.net:4015>
 - Exec: \$POS_TOP/patch/115/sql/pos_upg_usr.sql
- ◆ See metalink note 308271.1 for additional options.
Note that no additional patches are if you are at release 11.5.10 or 11.5.10.2

Conclusion



- ◆ In summary, recall that a reverse proxy server is an intermediate server that sits between a client and the actual web server and makes requests to the web server on behalf of the client. The client is unaware of the presence of the reverse proxy
- ◆ The above provides additional security to that portion of 11/E-Business Suite that is internet facing

Questions and Answers



Thank you!

James J. Morrow

jmorrow@solutionbeacon.com

www.solutionbeacon.com

Real Solutions for the Real World.®

Watch for our new book:

Installing, Upgrading and
Maintaining Oracle E-
Business Suite
Applications 11.5.10.2

It's coming THIS YEAR!

Sign Up For the Solution
Beacon Newsletter at
www.solutionbeacon.com
so you'll be notified when
it's available!

Solution Beacon and OnCallDBA
Installing, Upgrading and Maintaining Oracle E-Business Suite Release 11i



(or "Teaching an Old Dog New Tricks - Release 11i Care and Feeding")

***Installing, Upgrading and Maintaining
Oracle E-Business Suite Applications
Release 11.5.10+***

*By Barbara Matthews, John Stouffer, Randy Giefer, Karen Brownfield, Jeff Holt,
Bruno Coon, James Morrow, Tim Sharpe and Fawn deHenry*

Available at www.solutionbeacon.com