Demystify Oracle Apps 11i Security in the DMZ

Eric Hernandez

zanett

Presenter's Background

- DBA Manager for Zanett's Managed Services
- Provides Virtual Administration and Hosting for more than 50 customers
- 25 + DBAs
- Our team of DBAs have set up 11i in the DMZ for numerous customers
- Most recent is an iRecruitment Project that I will use as my demo in this presentation

Agenda

- Overview of 11i in DMZ
- Oracle Certified Topology of 11i in DMZ
- Reverse Proxy Server with External Web Server
- Configure and Secure 11i iRecruitment in DMZ
- Create and Setup Reverse Proxy Server
- Configure SSL

Why configure 11i for Internet?

- Out of the box, Oracle Apps 11i is configured as an intranet application
- Allow 11i Internet Products to be accessible from anywhere with Internet connection
- Allow vendors, customers, and partners to have easy access to your company's ERP
- Increase business efficiency significantly
- Eliminate the need for managing VPN and Citrix systems

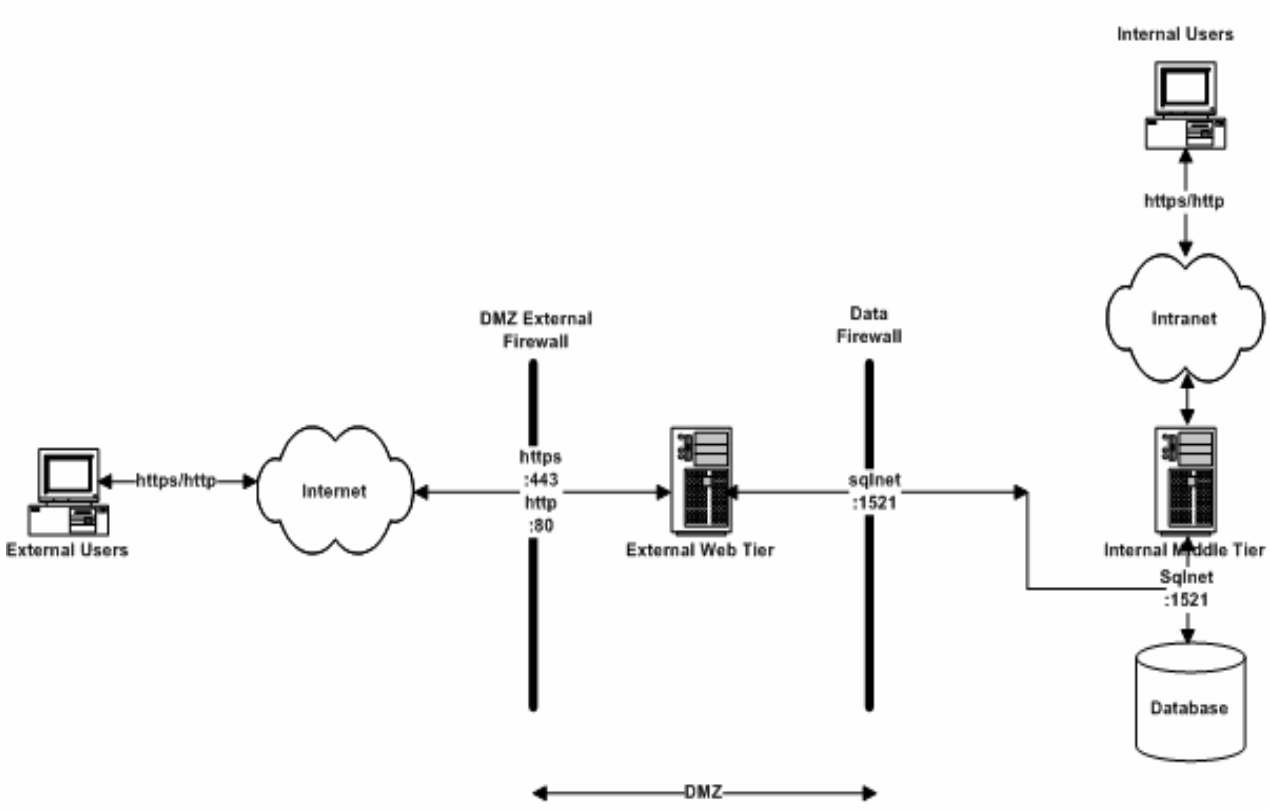
Why put 11i in the DMZ?

- DeMilitarized Zone
  - Network segment between the internet and a company's intranet
- External attacks come from the Internet
- Secure internal network from external public network
- If security is breached, only the components residing in the DMZ are exposed to potential damages

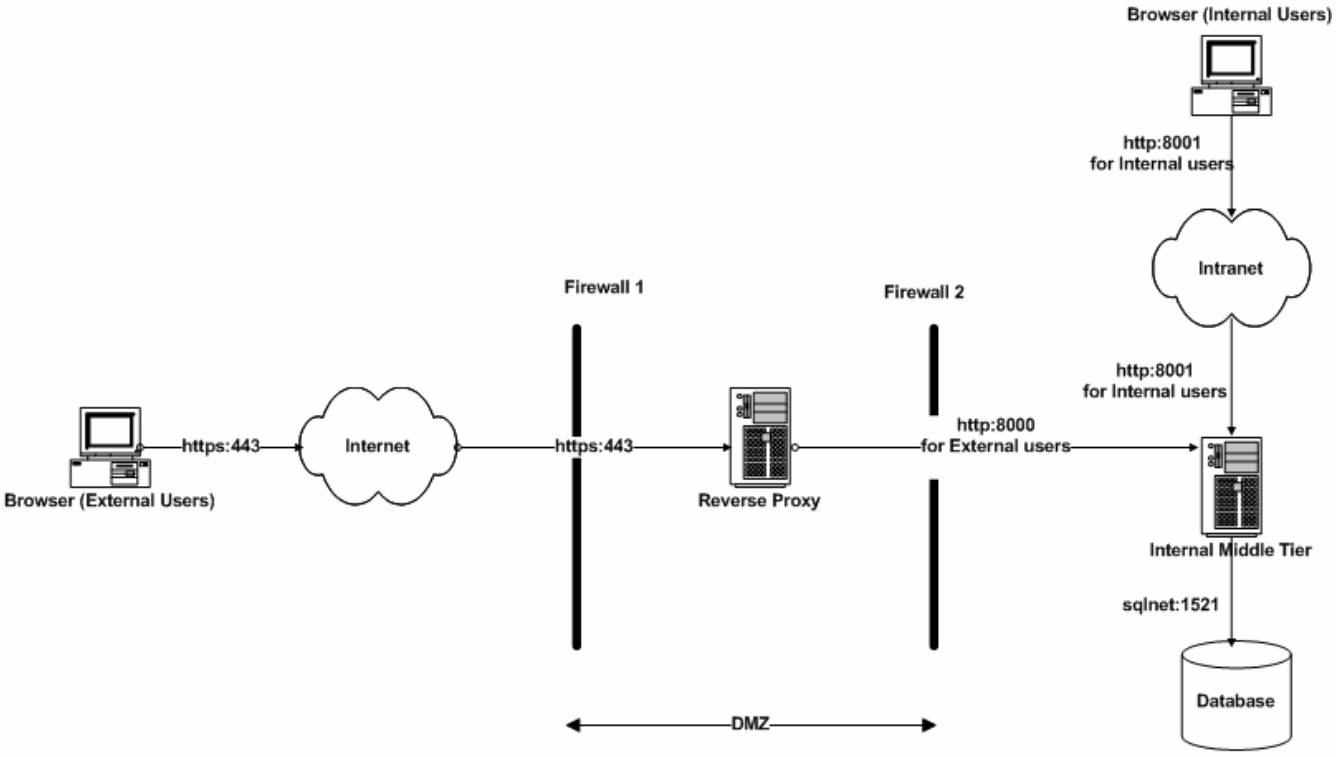
Supported 11i Configuration in the DMZ

- External Web Tier Only
- Reverse Proxy Only
- Reverse Proxy with an External Web Tier
- Hardware Load Balancers with an External Web Tier
- Hardware Load Balancers without an External Web Tier

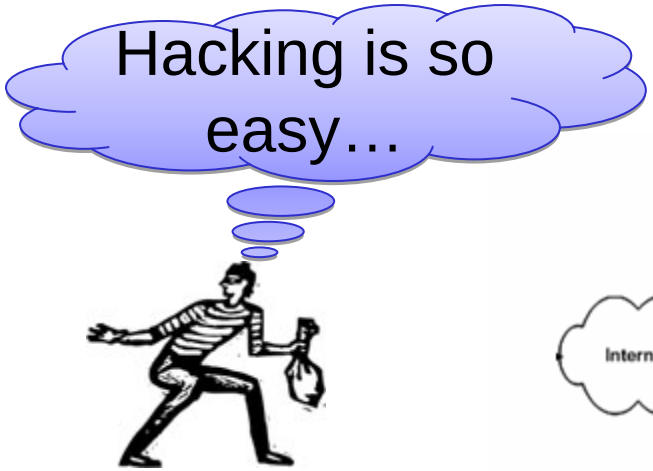
External Web Tier Only

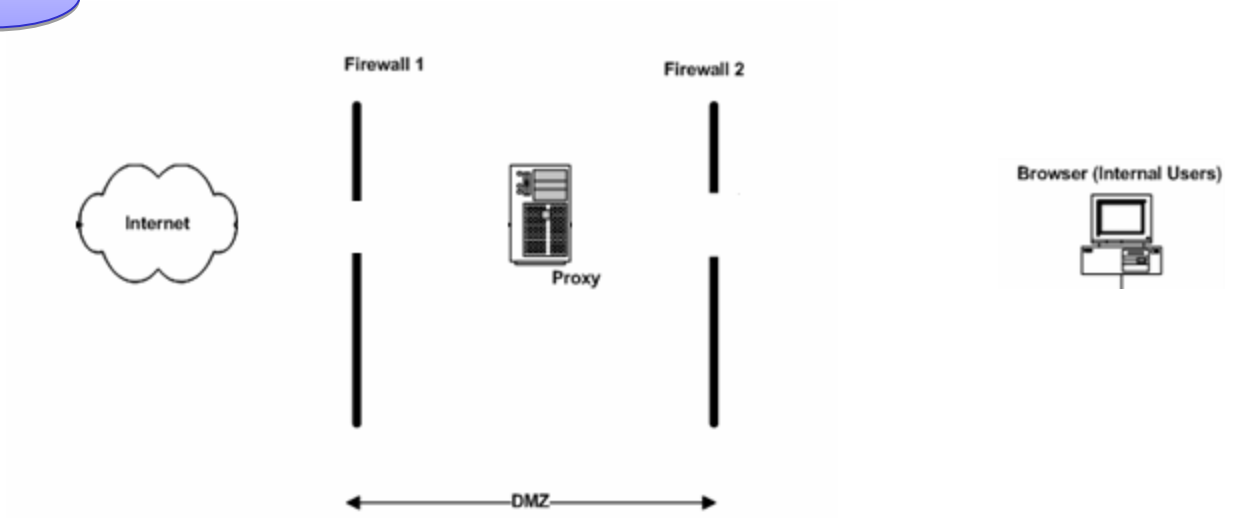


Reverse Proxy Only

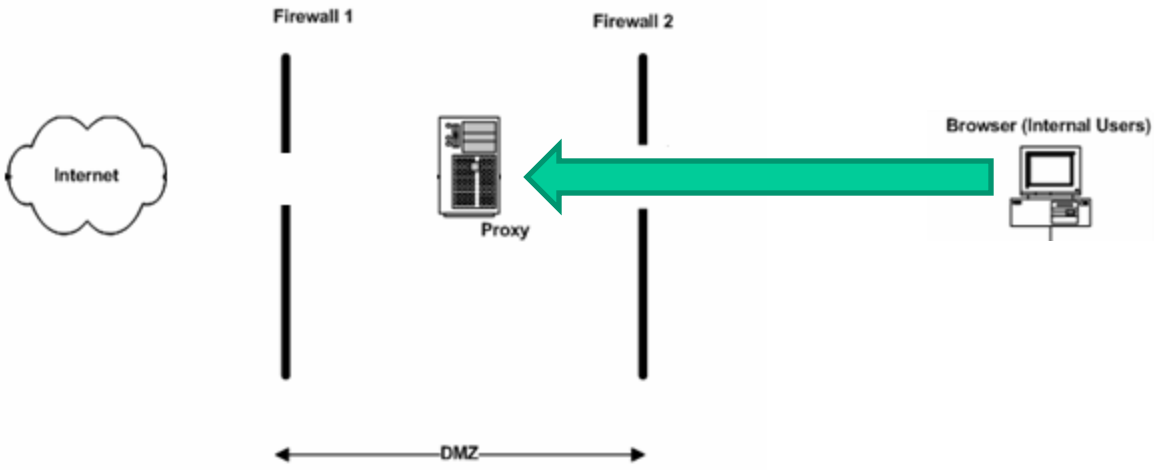


Proxy Server in Action

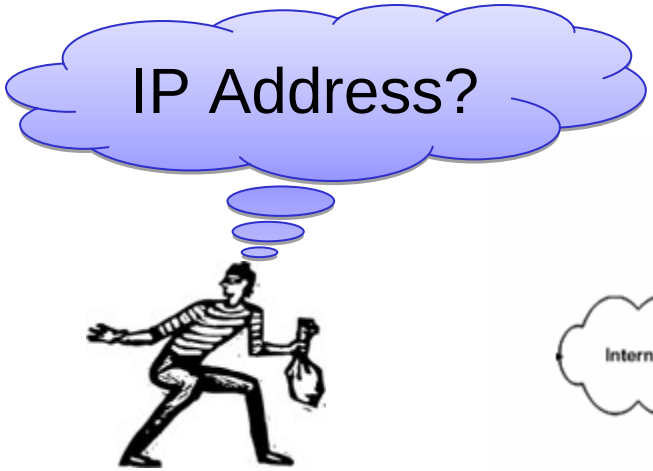


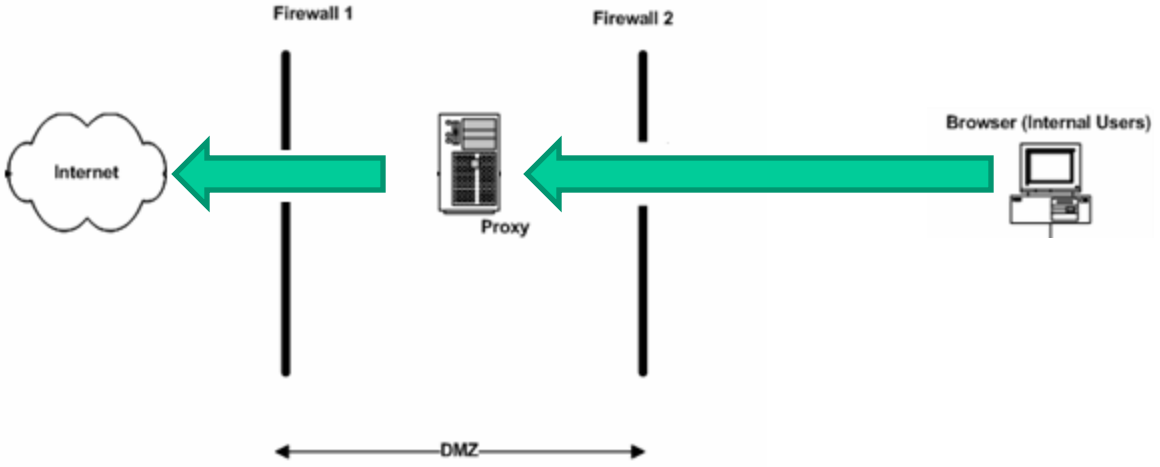


Proxy Server in Action

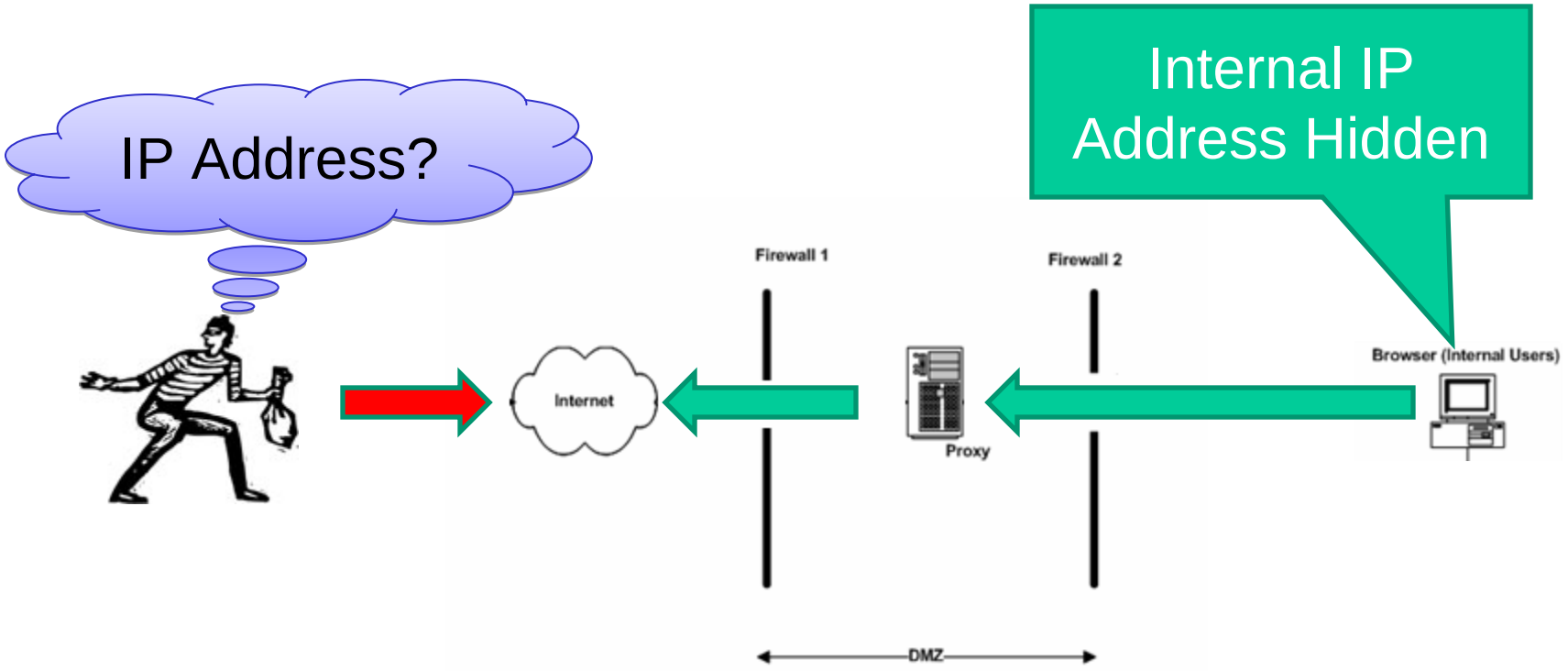


Proxy Server in Action

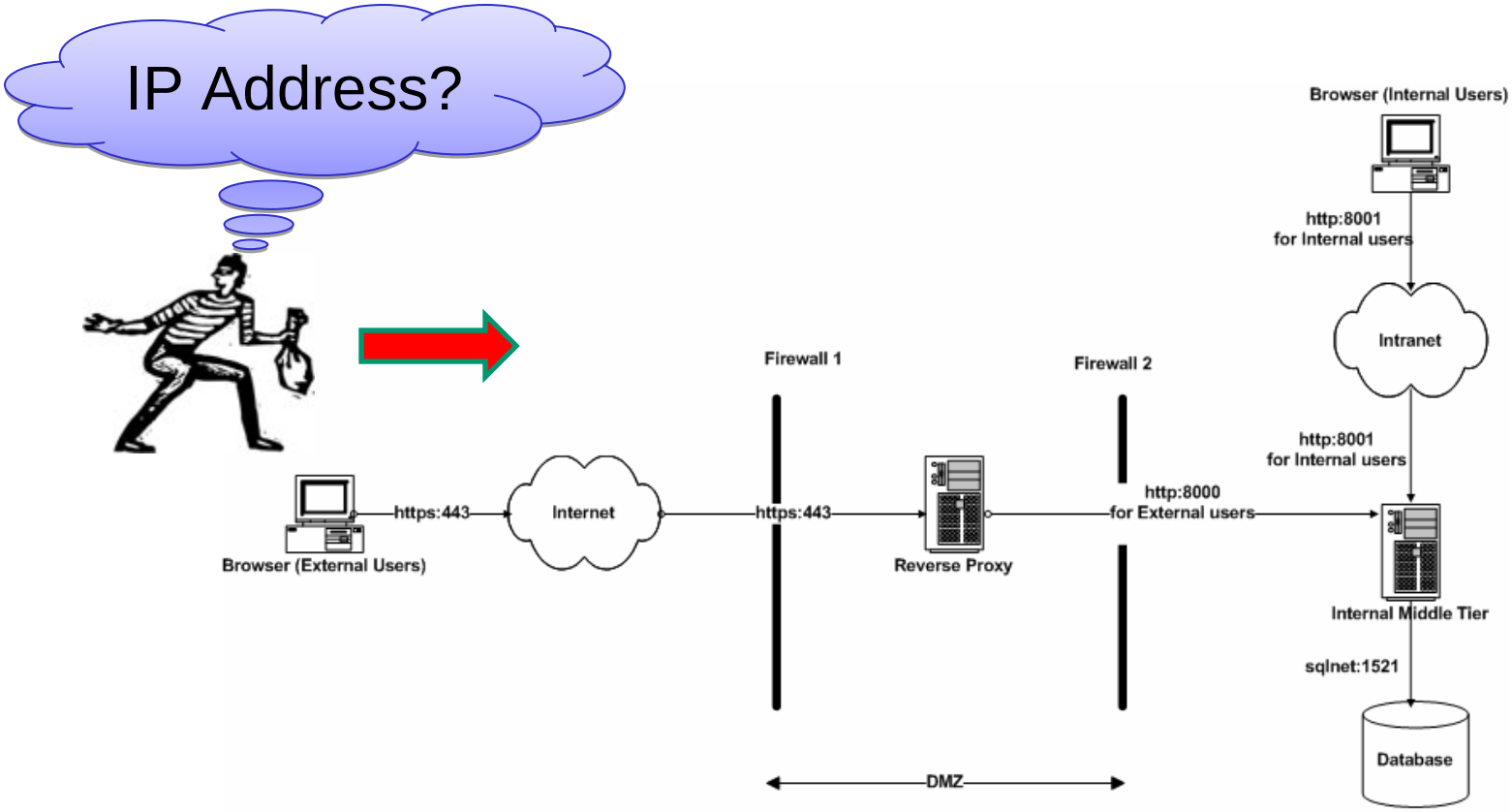




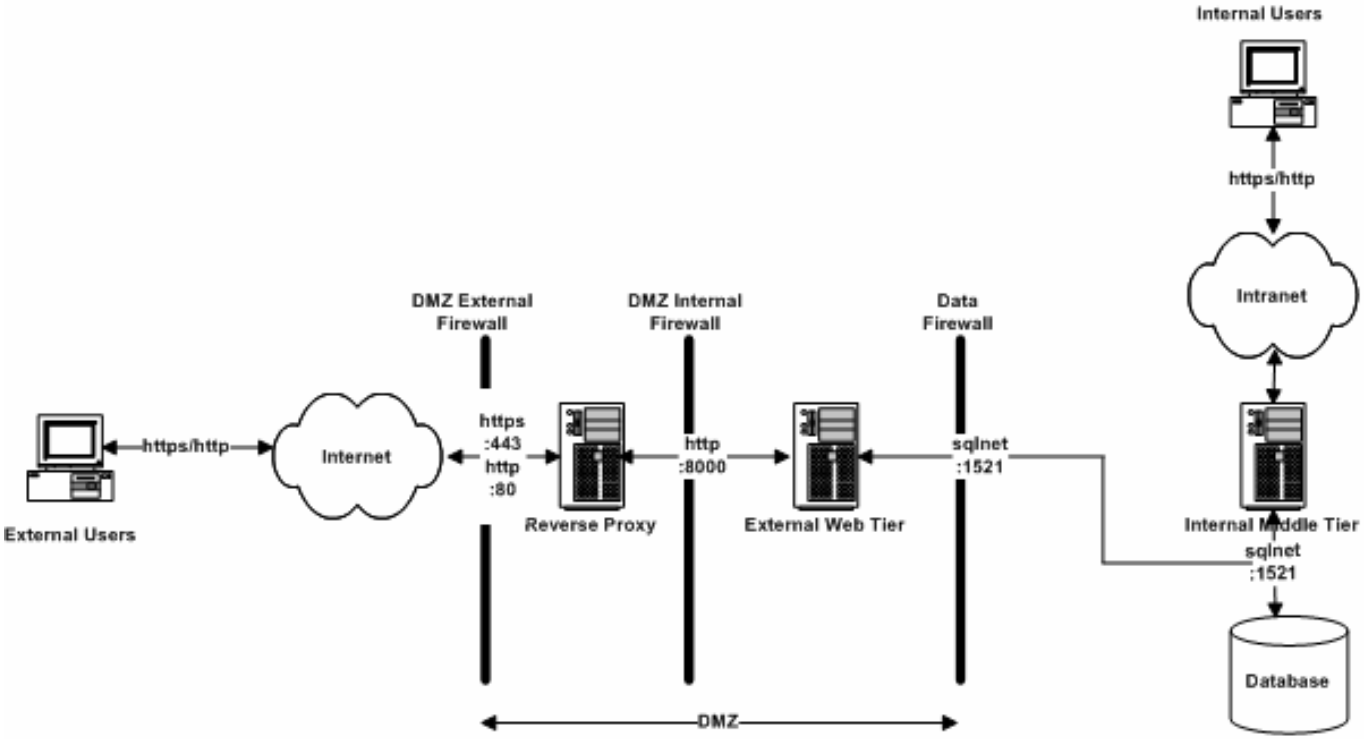
Proxy Server in Action



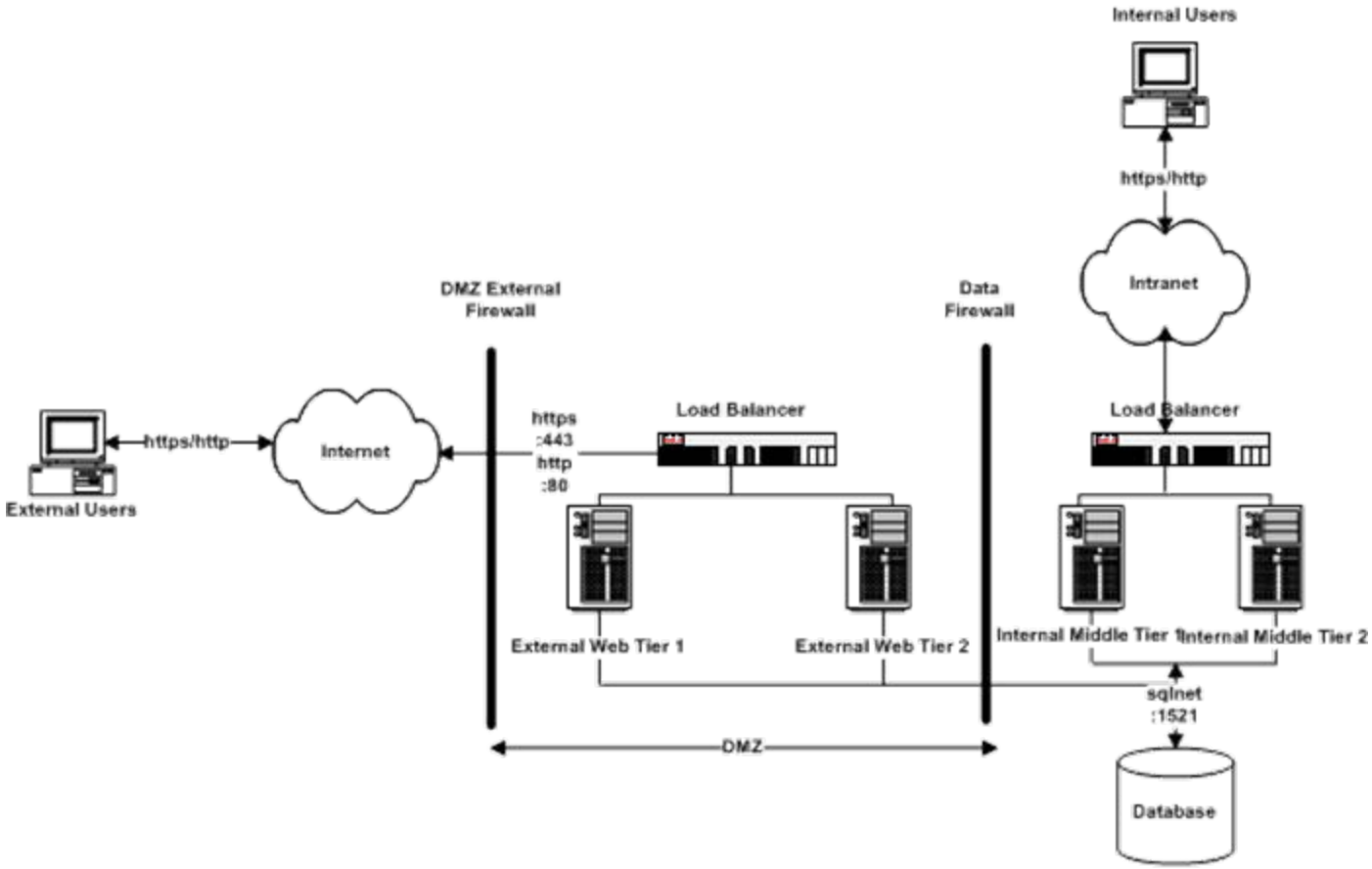
Reverse Proxy Server



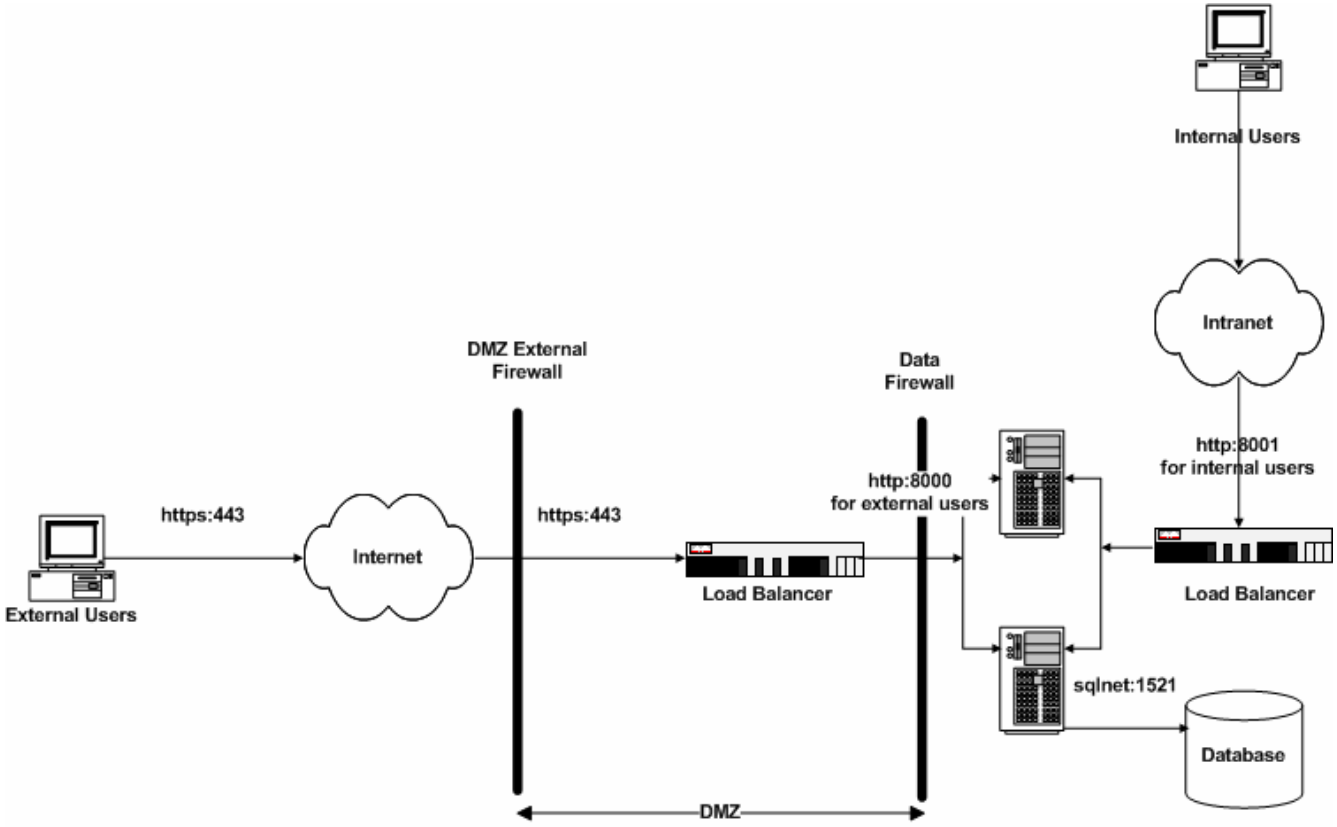
Reverse Proxy with an External Web Tier



Hardware Load Balancers with an External Web Tier



Hardware Load Balancers without an External Web Tier



Alternative Topology?

- Supported on a best-effort basis
- ATG will try to provide an adequate solution
- Sev1 bug is ONLY accepted whereby customer's production system is down

Demonstration Objectives

- iRecruitment needs to be accessible from the Internet and SECURED
  - irecruitment.example.com

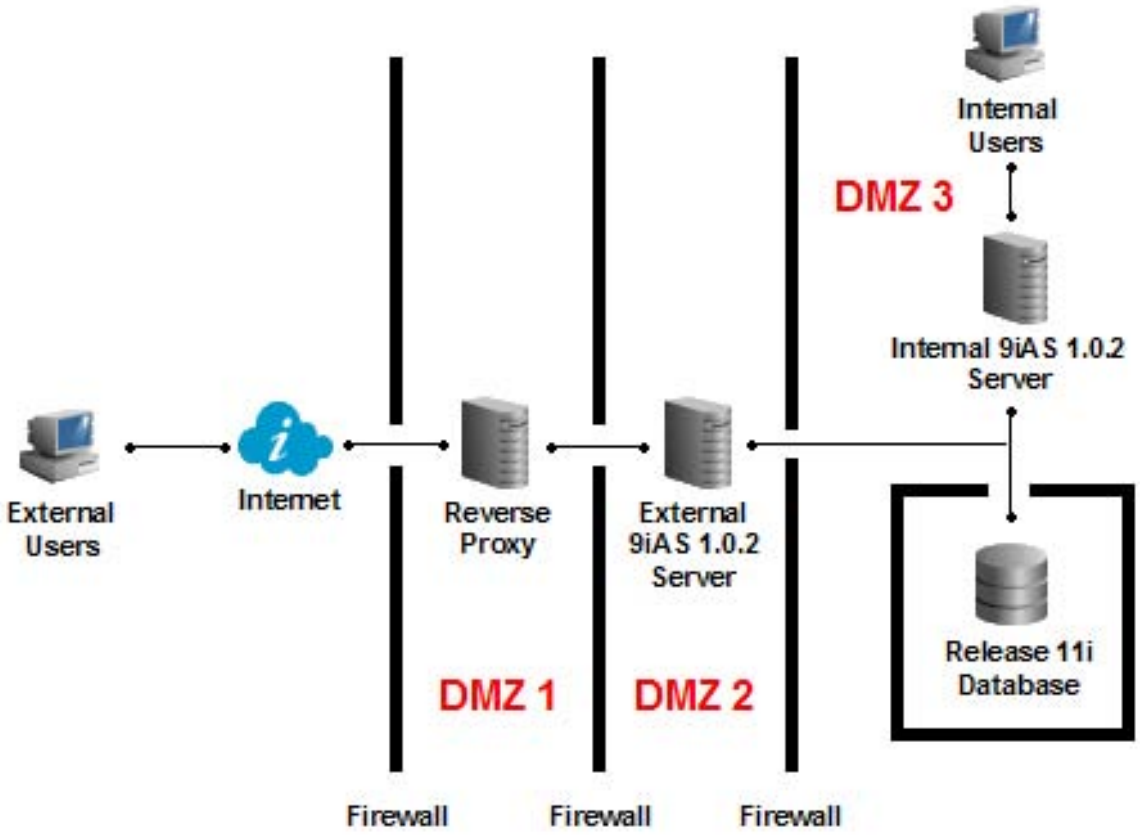
Before you begin...

- Review Appendix A of Metalink Note ID 287176.1
- Check the list for the 11i product that you're interested and see if it is certified to be deployed over the Internet
  - iRecruitment is certified for Internet deployment
- If it is not in the appendix, please create an Oracle SR asking for Internet certification for the 11i product you want

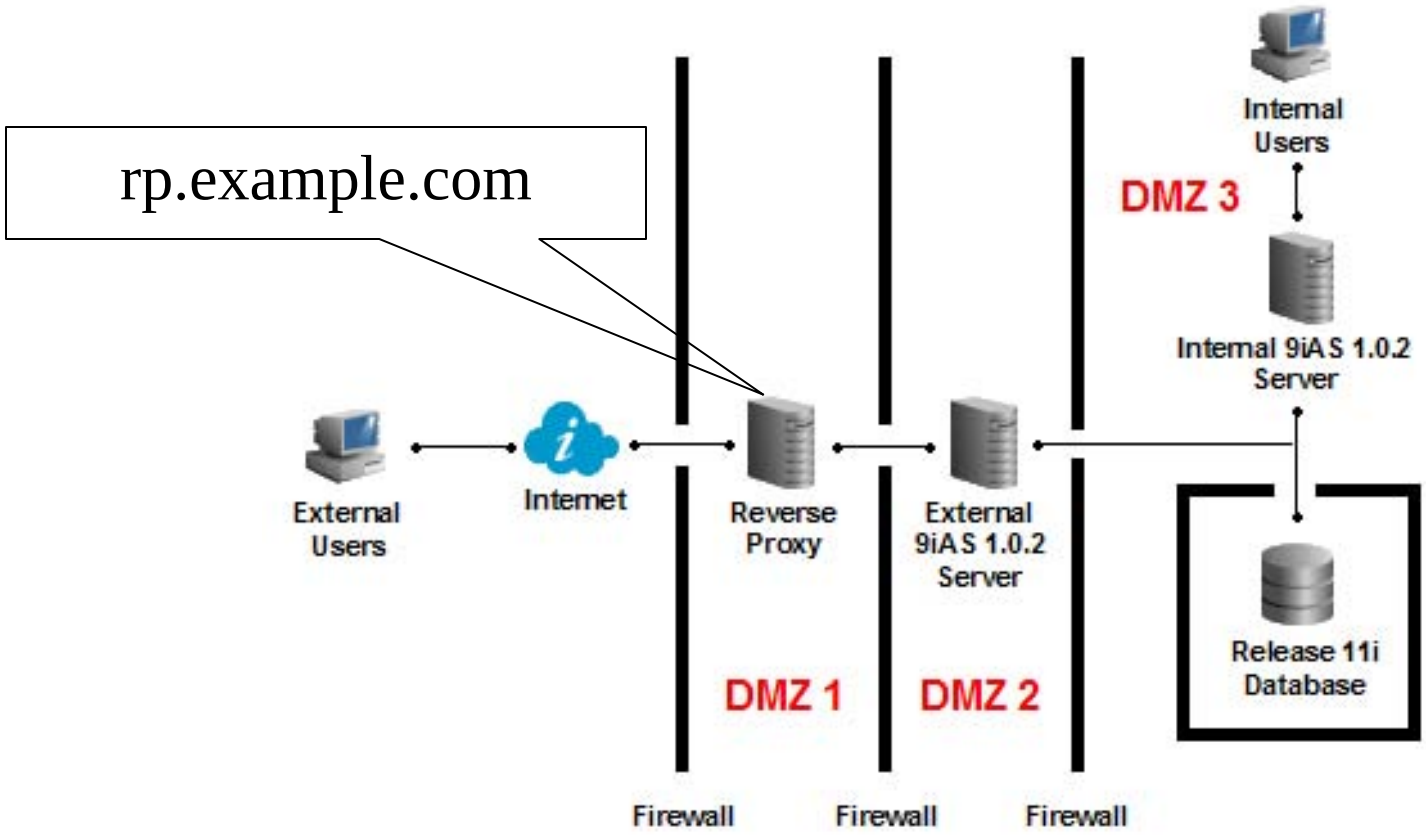
Hardware Acquired

- Three Firewall
  - Two external DMZs
- A reverse proxy server in its own DMZ
- An external web server in its own DMZ

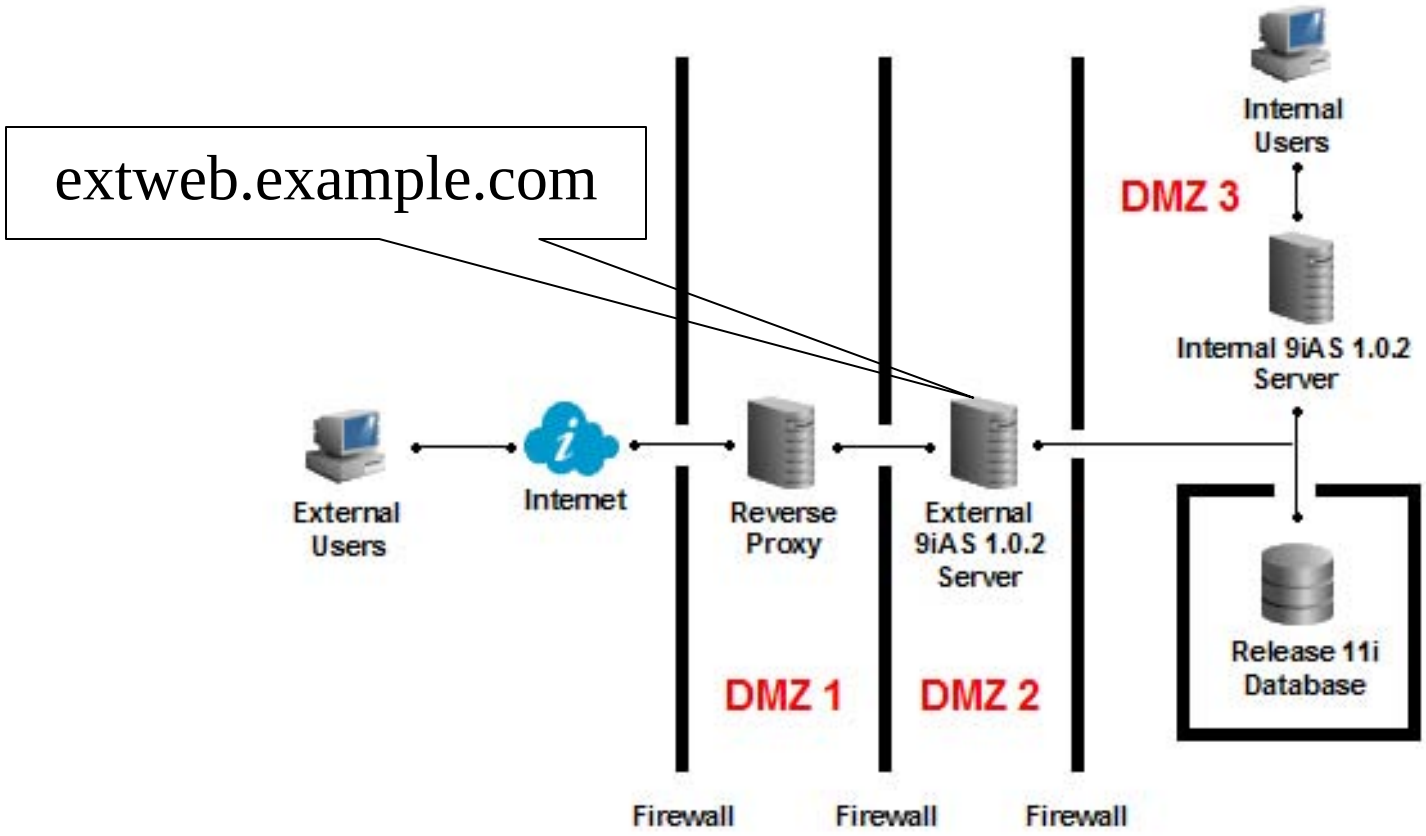
Reverse Proxy w/ Ext Web Server



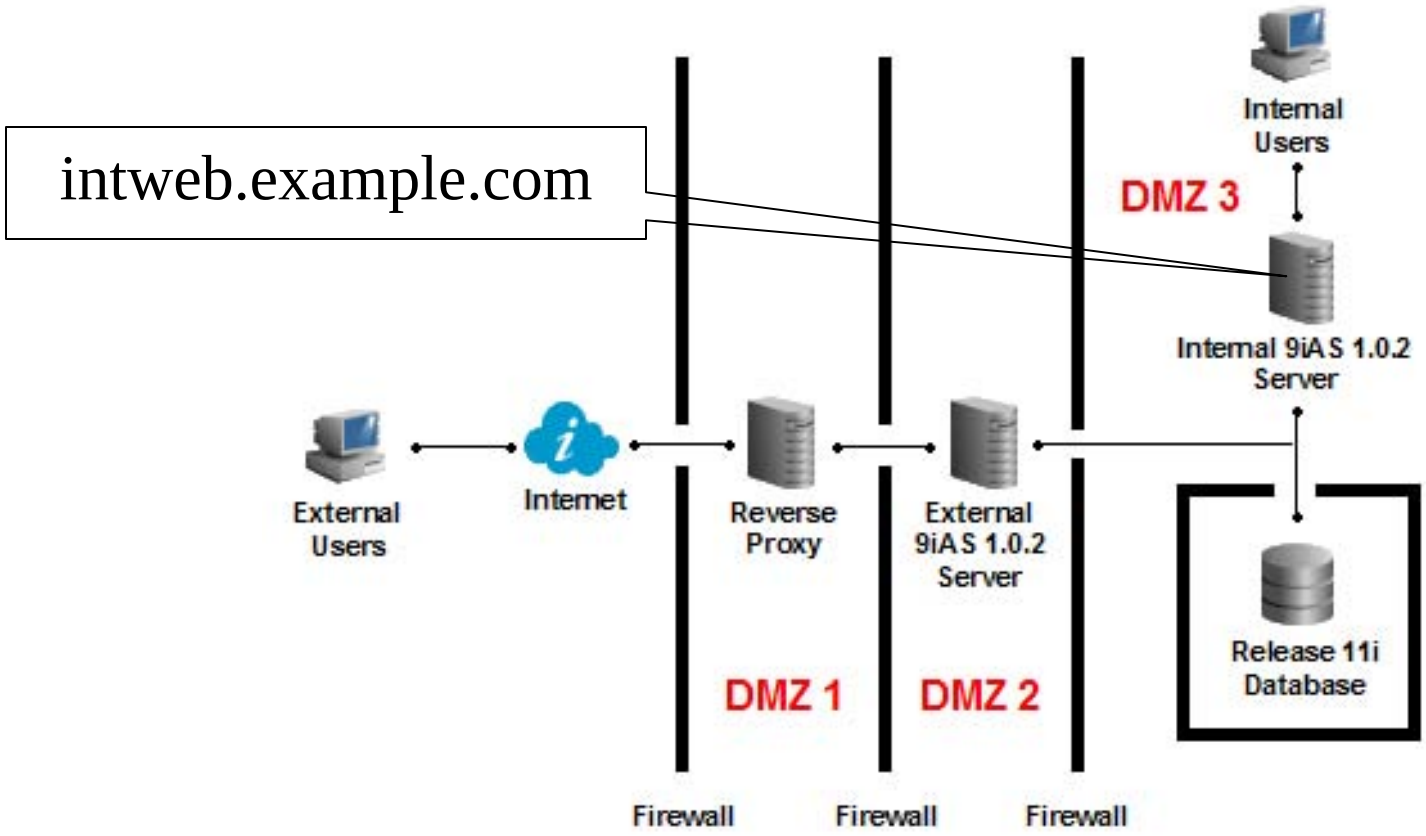
Fully Qualified Domain Name



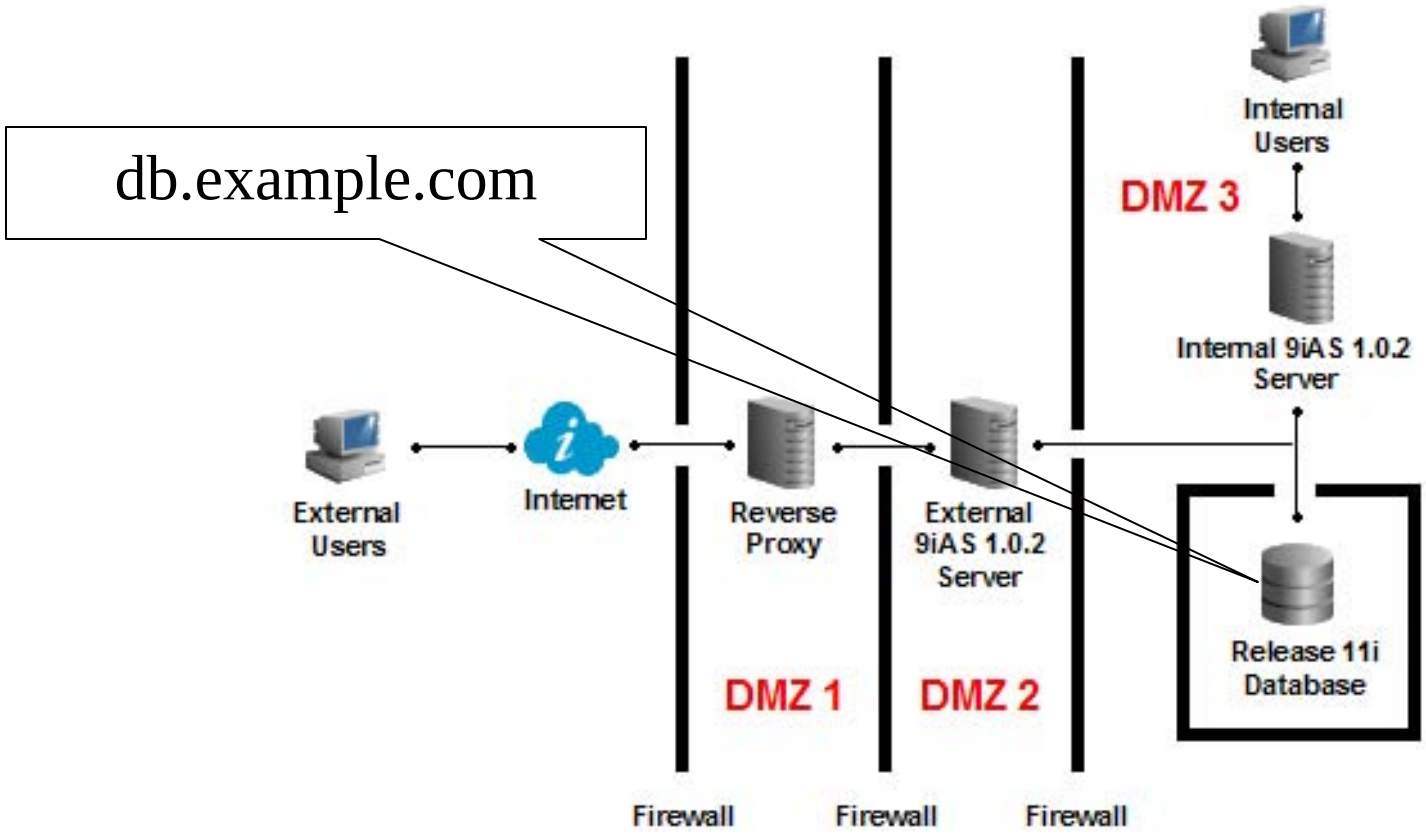
Fully Qualified Domain Name



Fully Qualified Domain Name



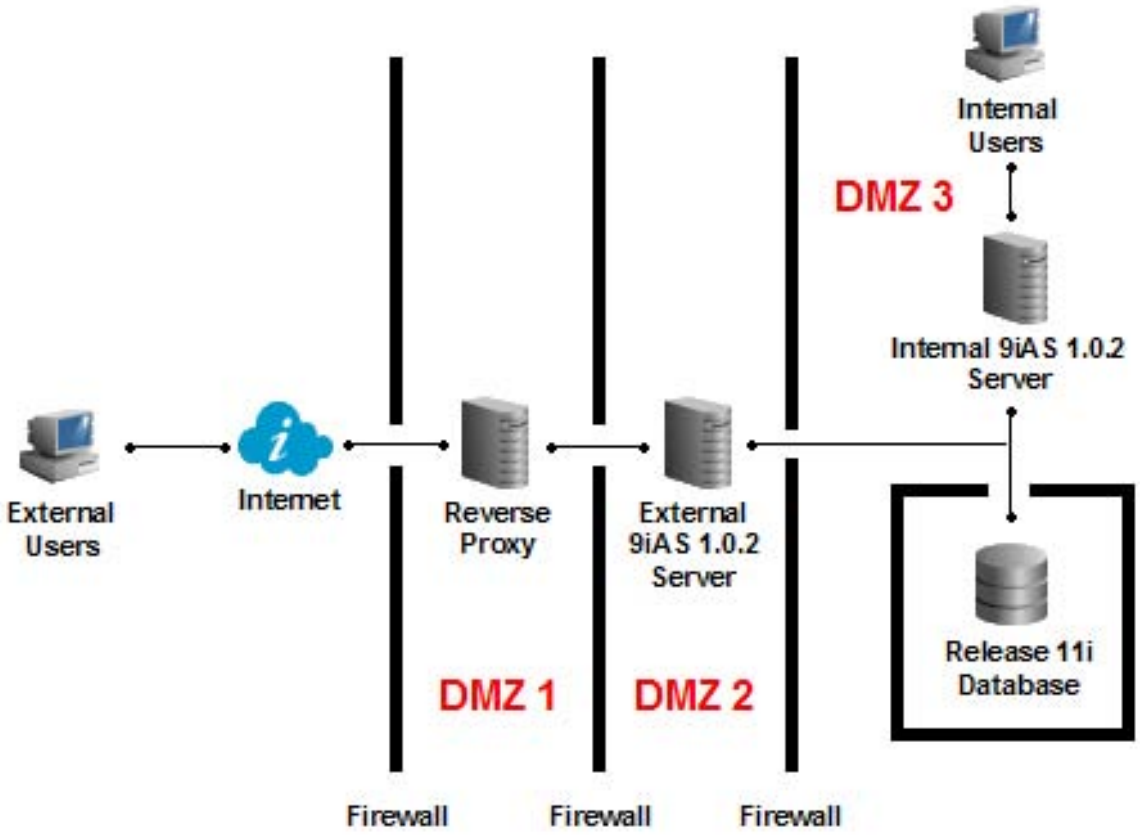
Fully Qualified Domain Name



Major Steps

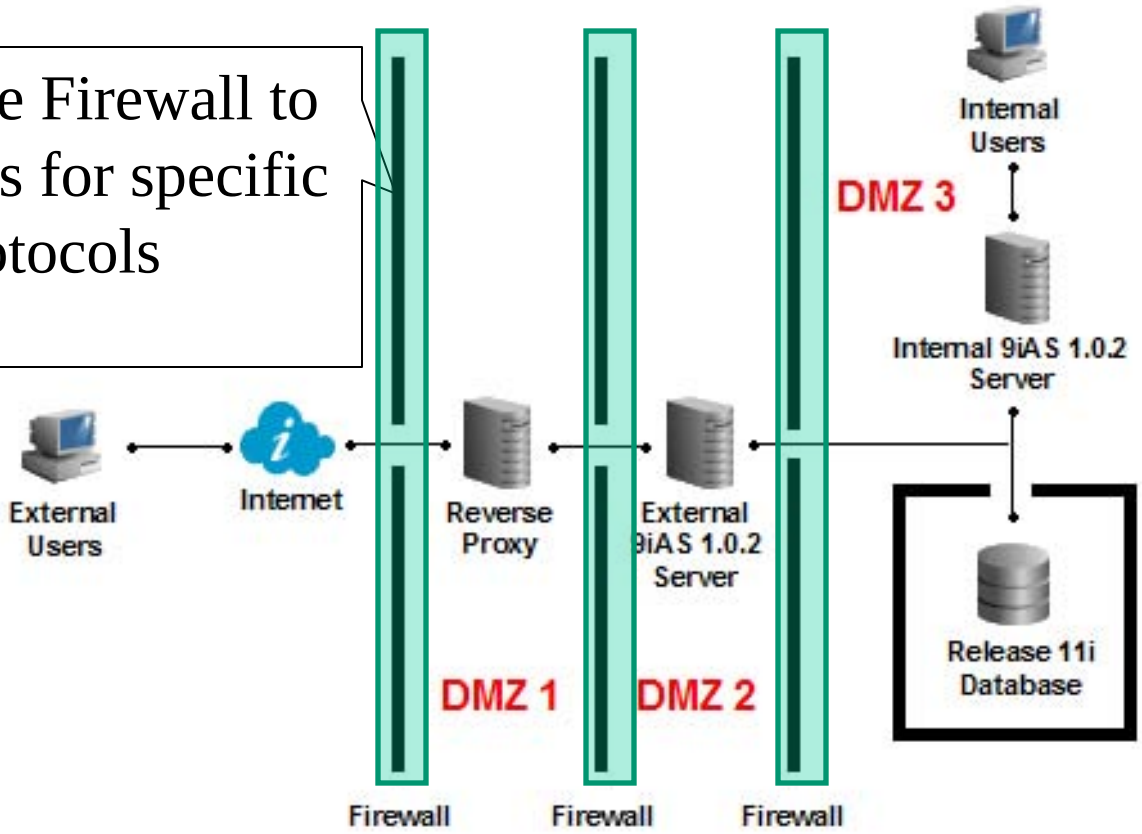
- Ensure proper communications between servers through the desired ports
- Apply DMZ and 11i Internet product patches
- Rapid Clone
- Configure External Web Server to have LIMITED available responsibilities
- Create and setup a Reverse Proxy Server
- Configure SSL

High Level Steps



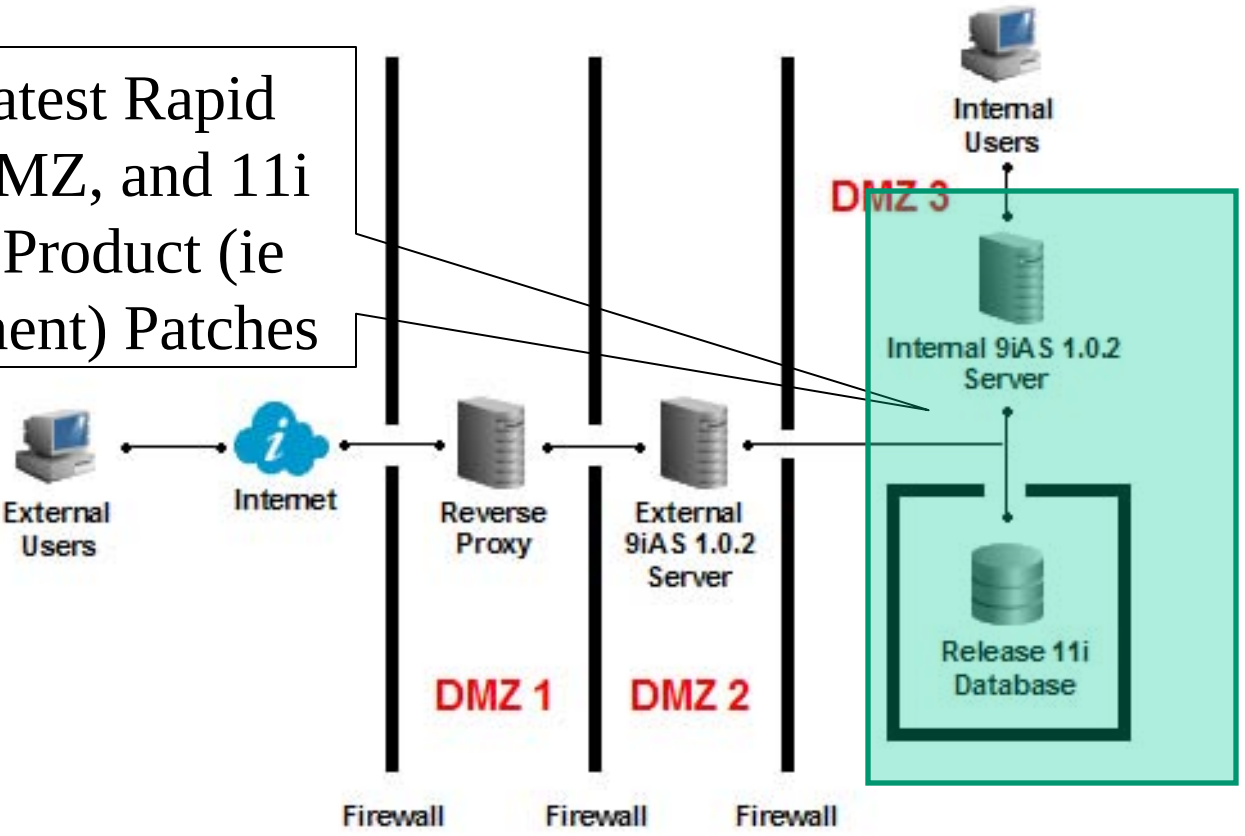
High Level Steps

Configure Firewall to open ports for specific protocols



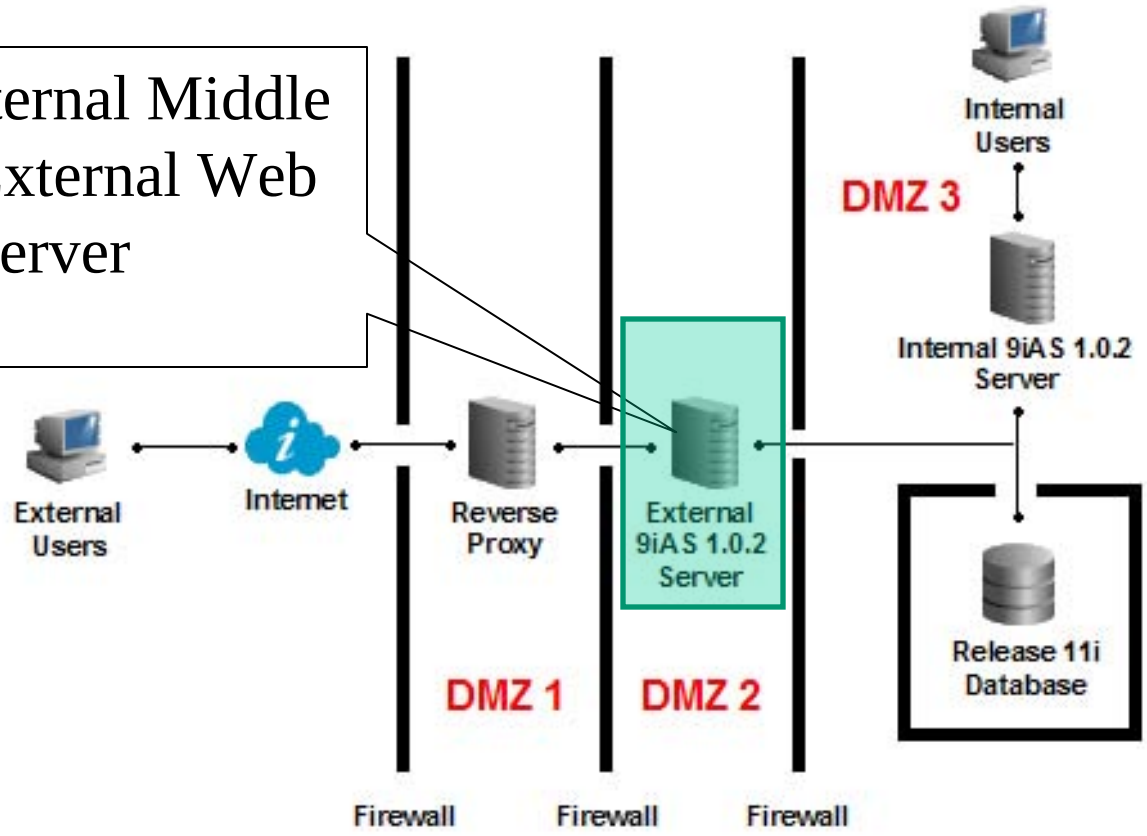
High Level Steps

Apply latest Rapid Clone, DMZ, and 11i Internet Product (ie iRecruitment) Patches



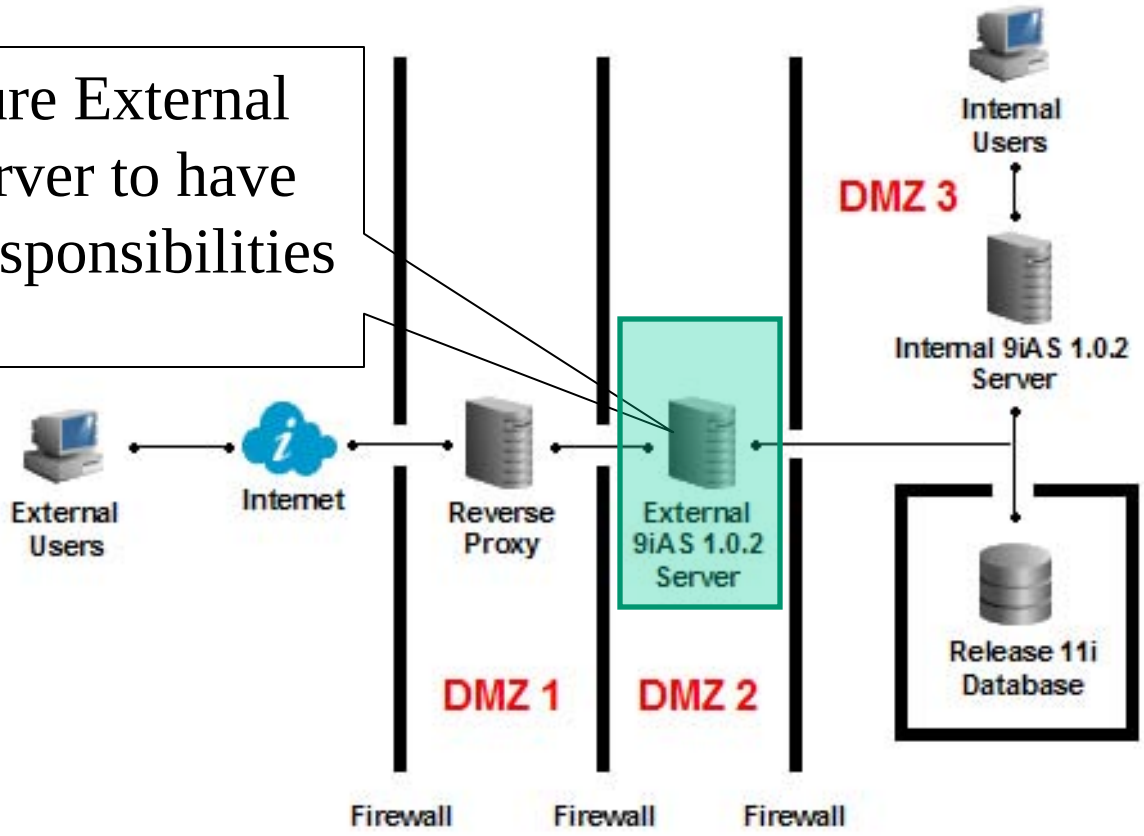
High Level Steps

Clone Internal Middle Tier to External Web Server



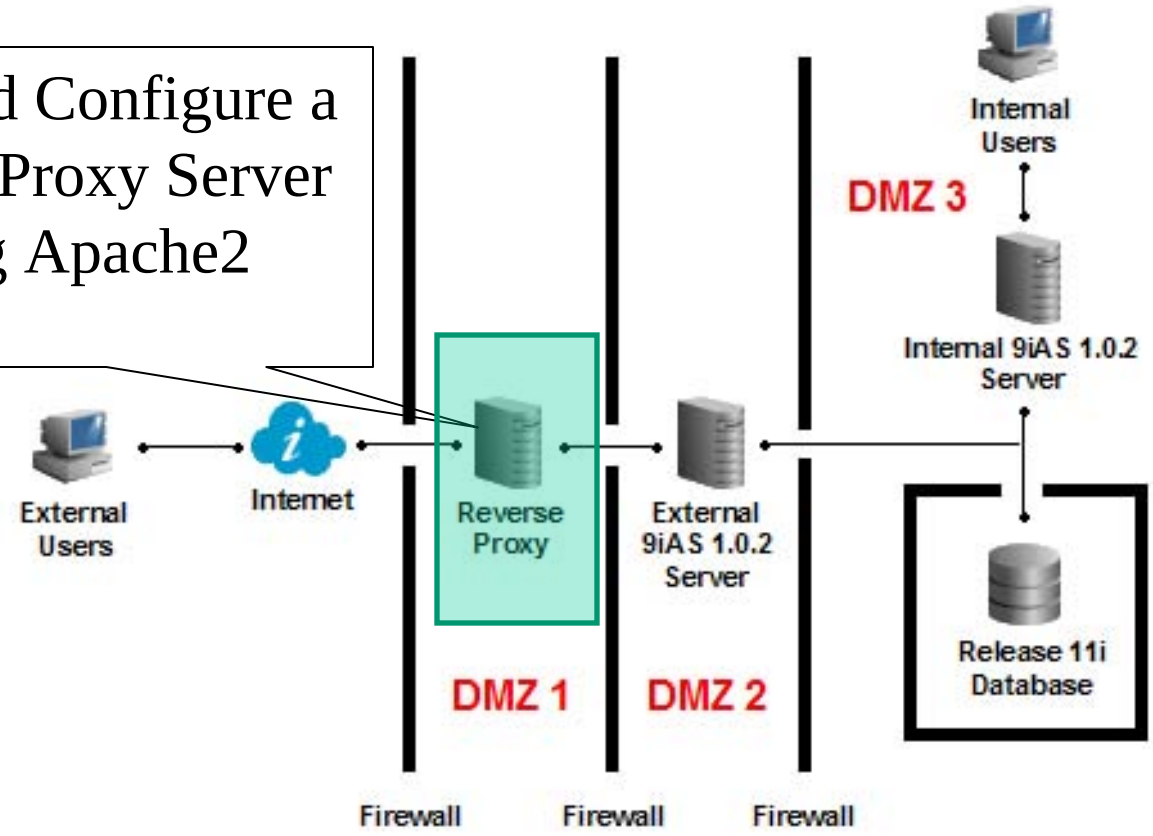
High Level Steps

Configure External Web Server to have limited responsibilities



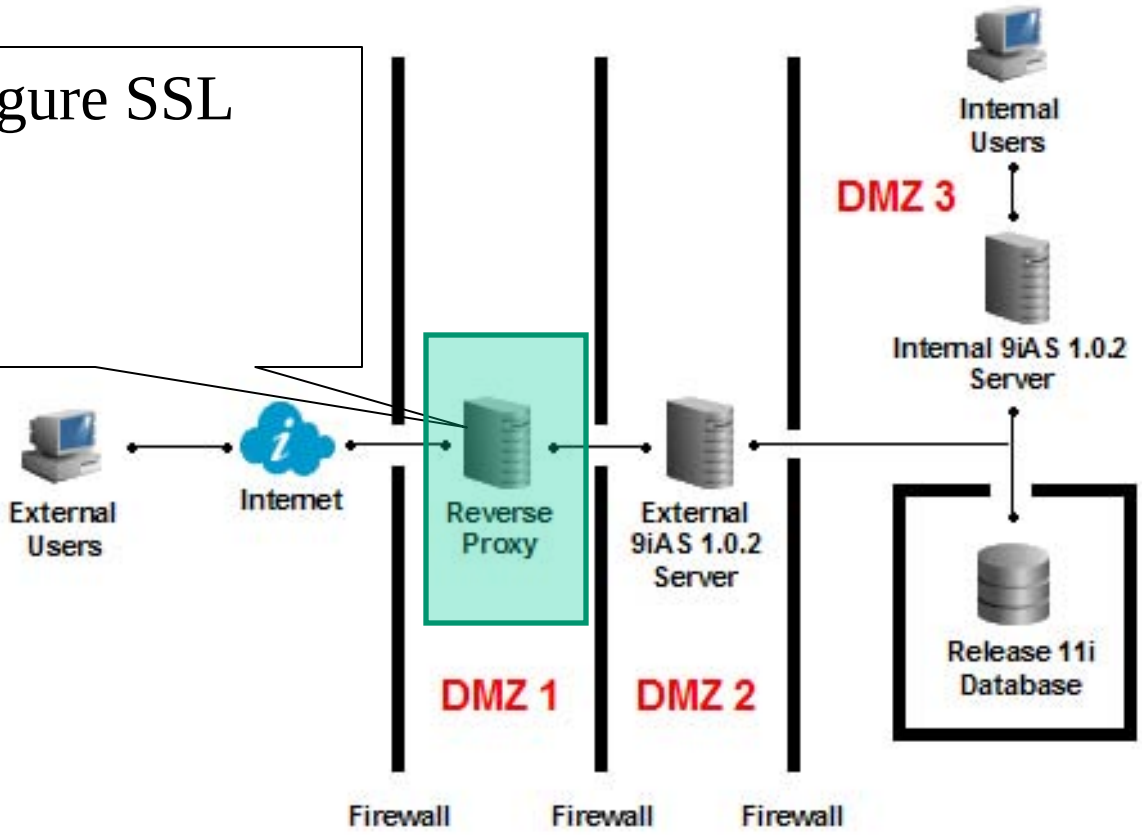
High Level Steps

Build and Configure a Reverse Proxy Server Using Apache2



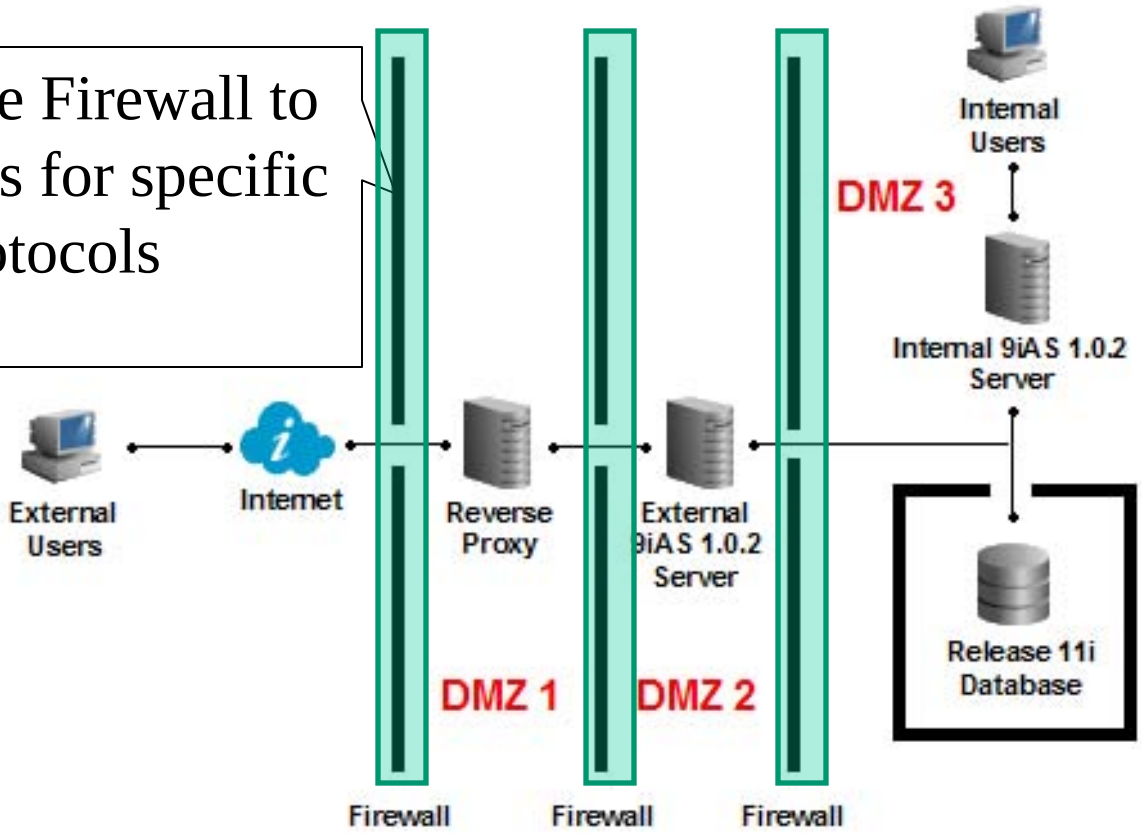
High Level Steps

Configure SSL

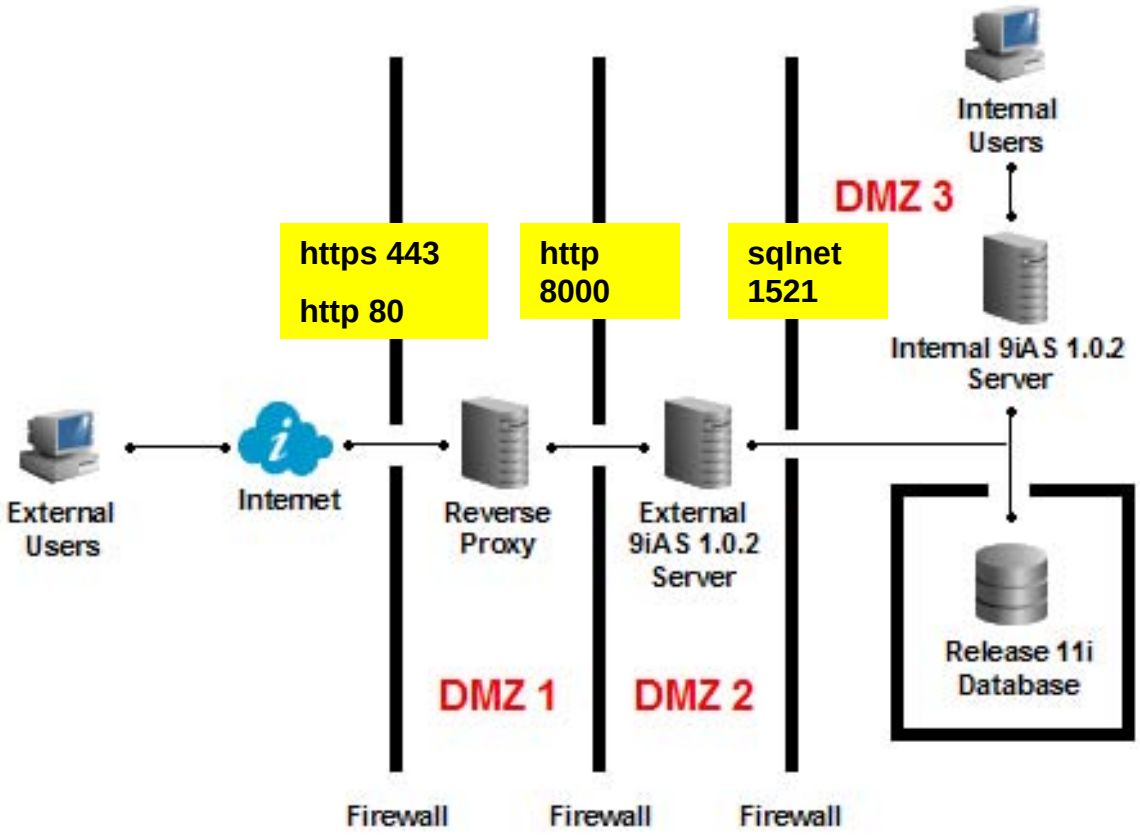


First Step

Configure Firewall to open ports for specific protocols

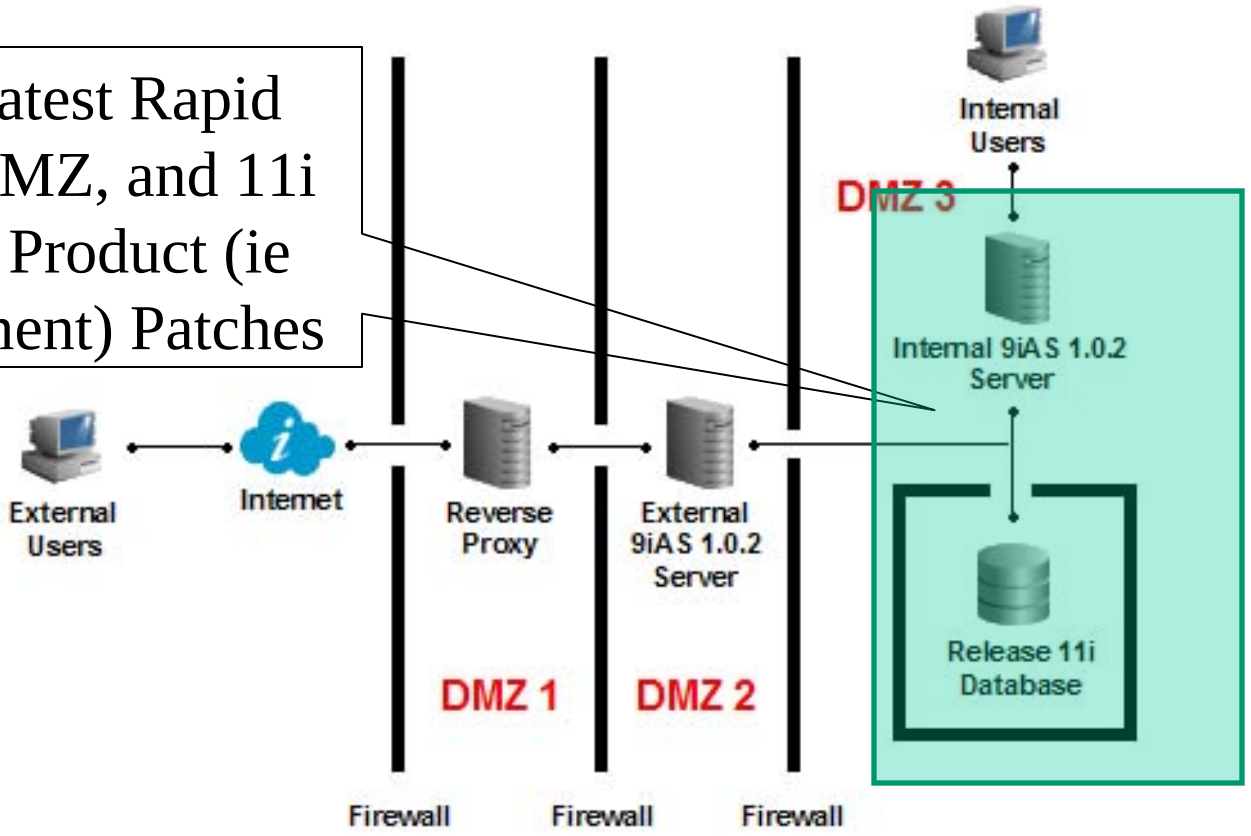


Opening Ports



Next Step

Apply latest Rapid Clone, DMZ, and 11i Internet Product (ie iRecruitment) Patches



Apply DMZ Required Patches

- Patches Required for DMZ Configuration using **11i10**
  - 3240000
  - 4204335
  - 3942483
  - 5478710

Apply DMZ Required Patches

- Patches Required for DMZ Configuration using **11i9**
  - 3072811
  - 4334965
  - 3942483
  - 5478710

Apply iRecruitment Patches

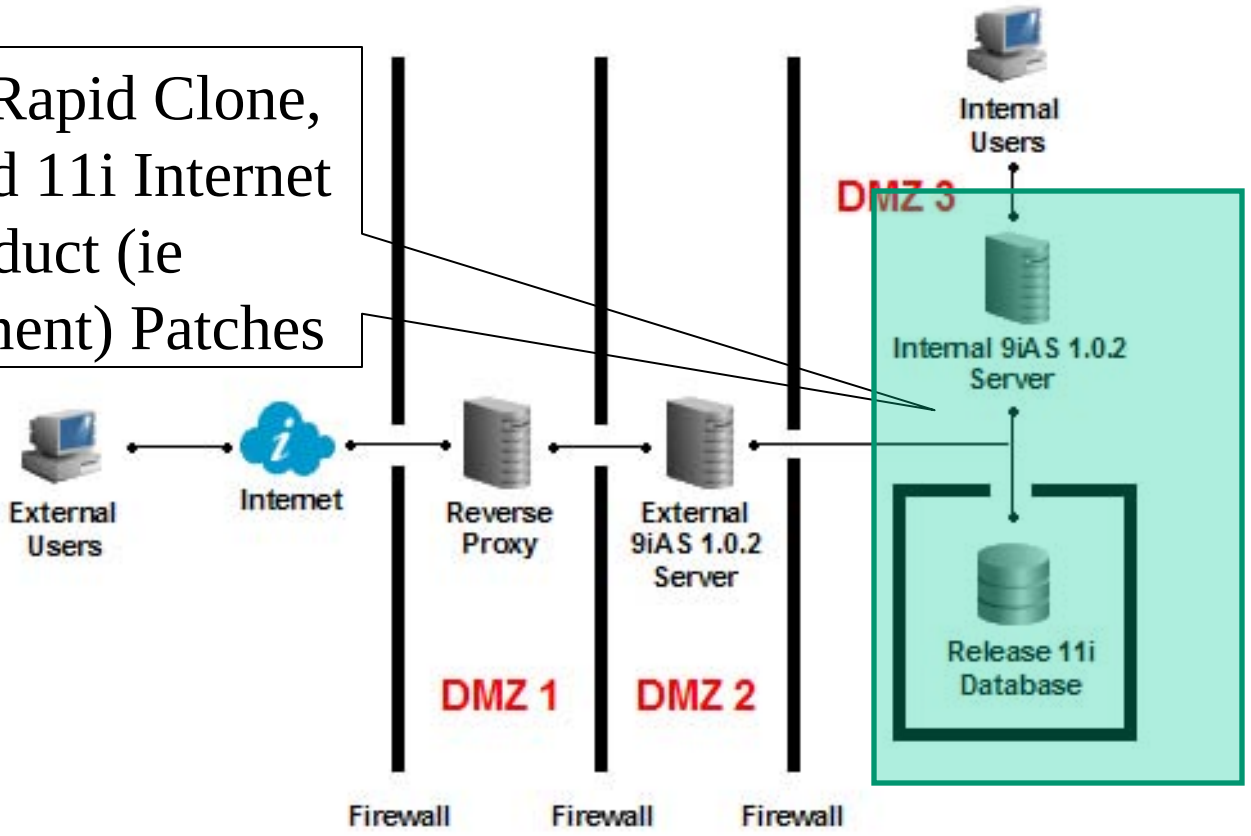
- 4242220
- iRecruitment is used in this demonstration.
  - If iRecruitment is not the module you're interested in deploying over the internet, please review the patches necessary in Appendix A of Metalink Note: 287176.1

Apply Latest Rapid Clone Patches

- In order to minimize cloning issues, ensure the latest rapid clone prerequisites have been met

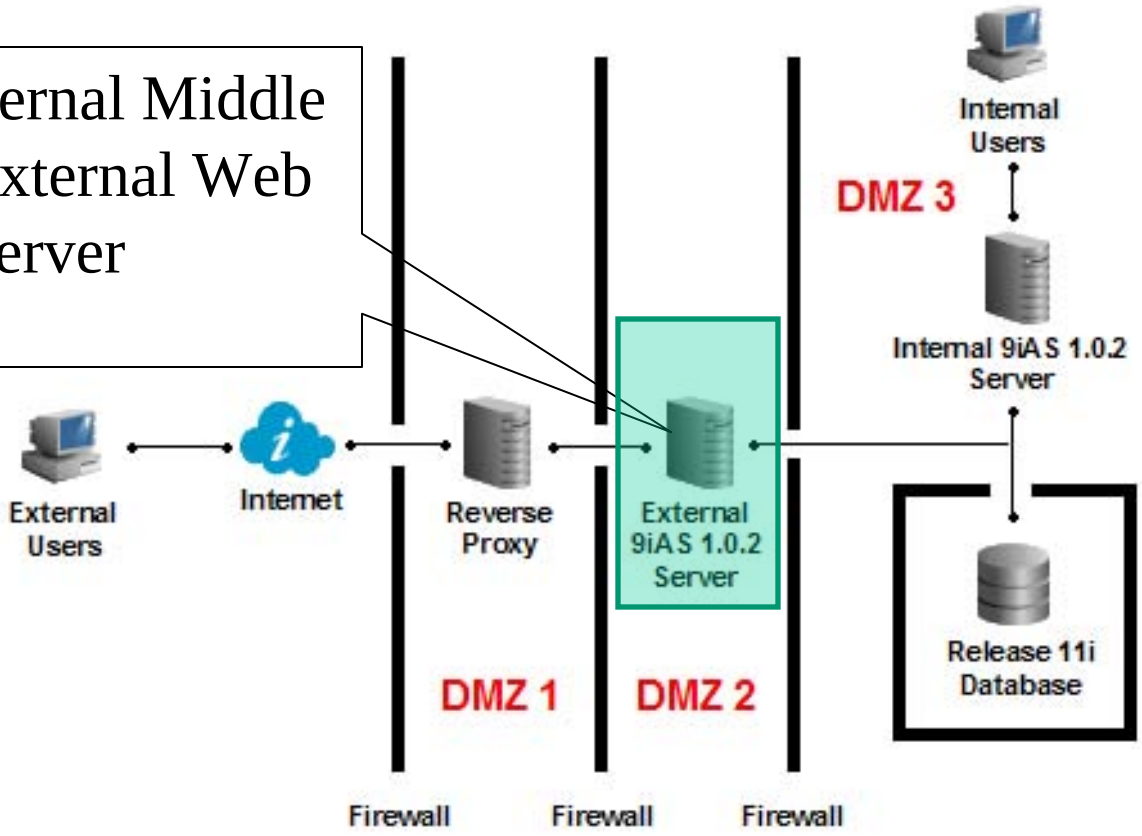
Project Update

Applied Rapid Clone, DMZ, and 11i Internet Product (ie iRecruitment) Patches



Next Step

Clone Internal Middle Tier to External Web Server

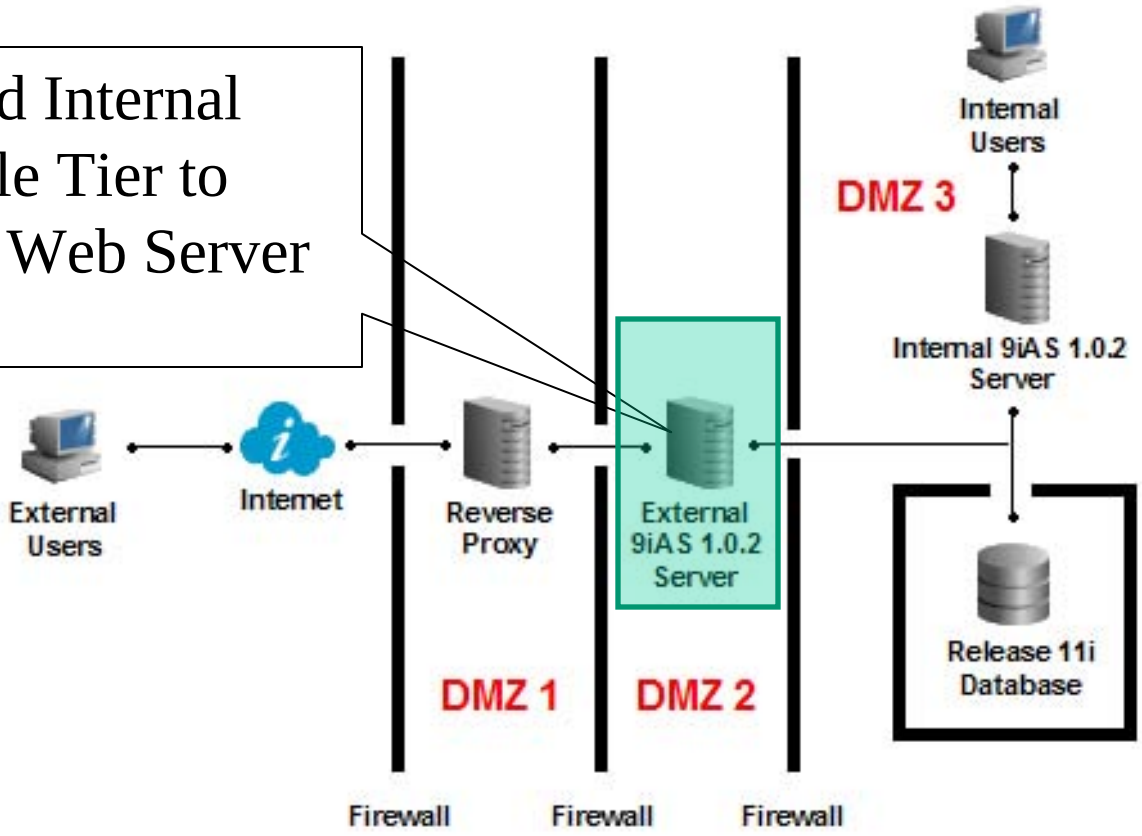


Rapid Clone

- Clone APPL TIER from internal middle tier to external web server
- During the post clone, only the web service will be configured in the external web server
- Sharing file systems between the external web server and internal middle tiers is not supported in any deployment option
- if you have multiple external web tiers, they can share file systems

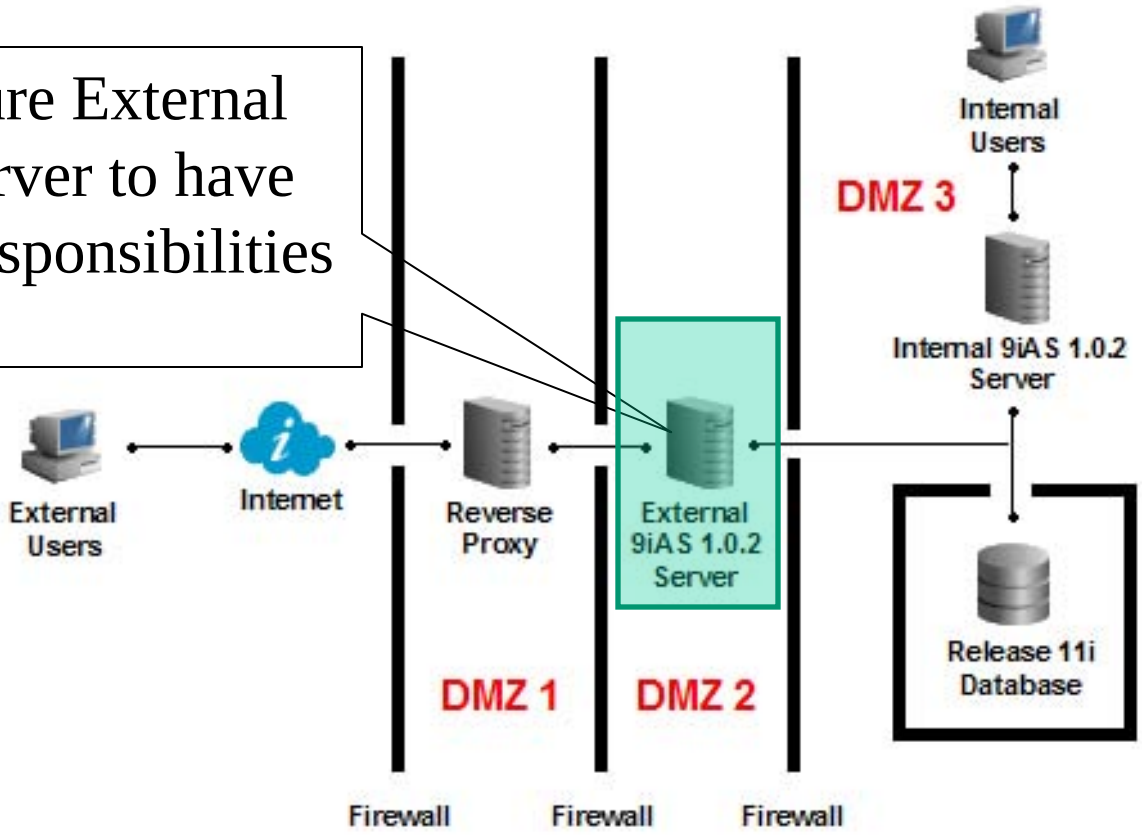
Project Update

Cloned Internal Middle Tier to External Web Server



Next Step

Configure External Web Server to have limited responsibilities



Limit the Responsibilities available in the External Web Server

- Update Hierarchy Type
- Update Node Trust Level
- Configuring iRecruitment Responsibilities for extweb.example.com
- Update Home Page Mode to Framework
- Add Responsibilities to the Guest Account

Update Hierarchy Type

- In order to provide the mechanism to have certain responsibilities available to only specific servers, the Hierarchy Type must be set to “SERVRESP”
- Shutdown APPL TIER services in the internal and external servers
- Execute SQL command on the internal server

sqlplus <apps_schema>/<apps_pwd>
@FND_TOP/patch/115/sql/txkChangeProfH.sql
SERVRESP

Update Hierarchy Type (cont)

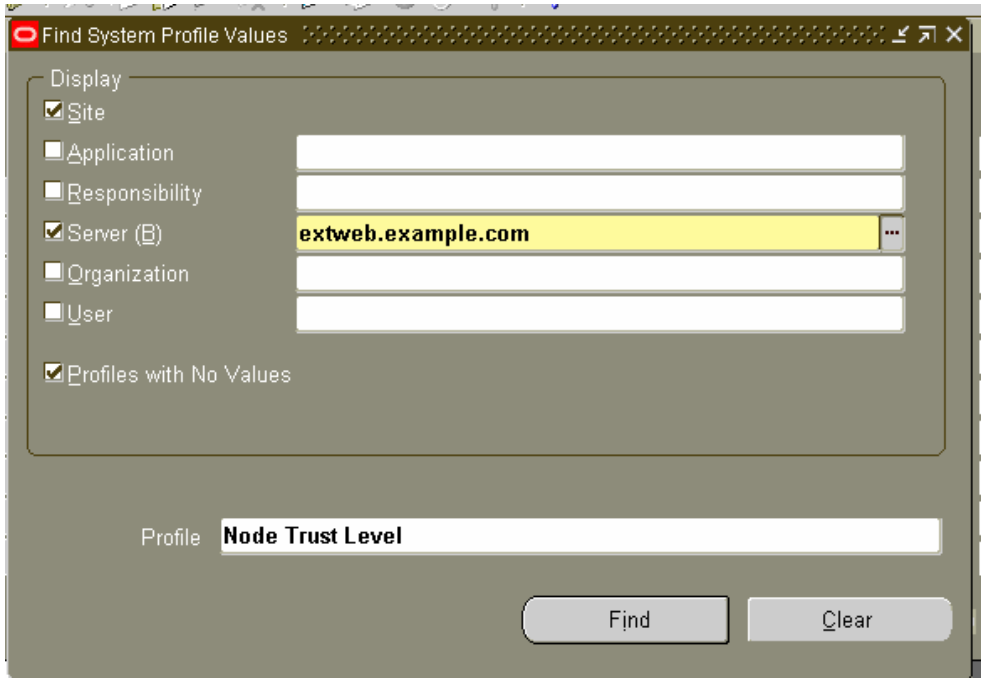
- Output should indicate the sql is successful
- Run autoconfig in all nodes
- Startup all 11i services in the internal server ONLY
- At this stage we've only provided the means to limit the responsibilities available in the external web server

Update Node Trust Level

- Log into Oracle Apps of the internal middle tier
- Select System Administrator Responsibility
- Select Profile / System
- From the “Find system profile option Values” window, select “extweb.example.com” as the server that you want to make external

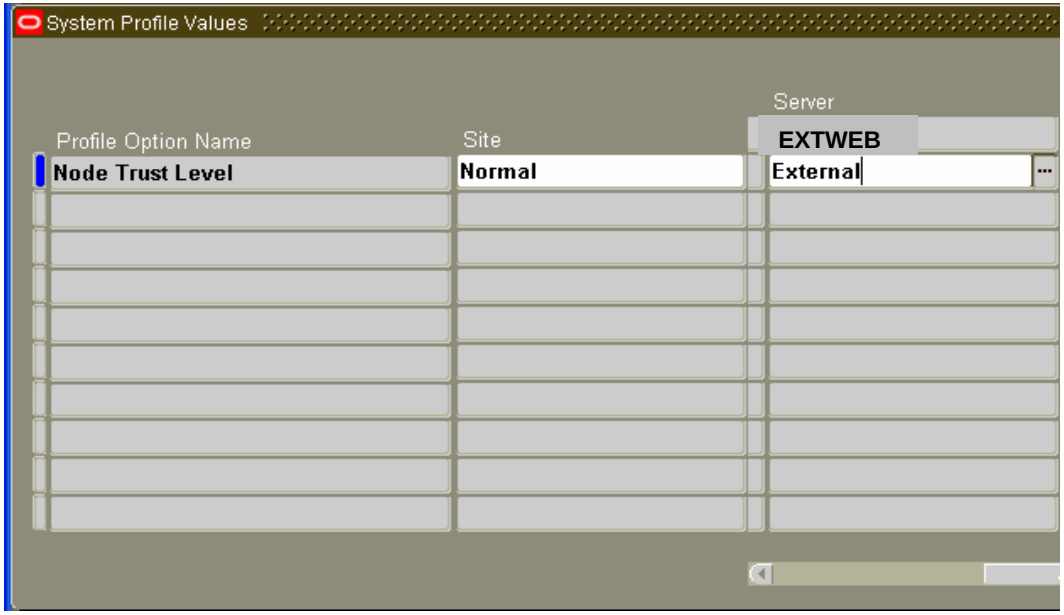
Update Node Trust Level (Cont)

- Query for '**Node Trust Level'** for the desired server.



Update Node Trust Level (Cont)

- Set the value of this profile option to **External** at the server level (not site level). The site-level value should remain **Normal**
- At this time, there are NO responsibilities available from the external web server



Set iRecruitment Responsibilities

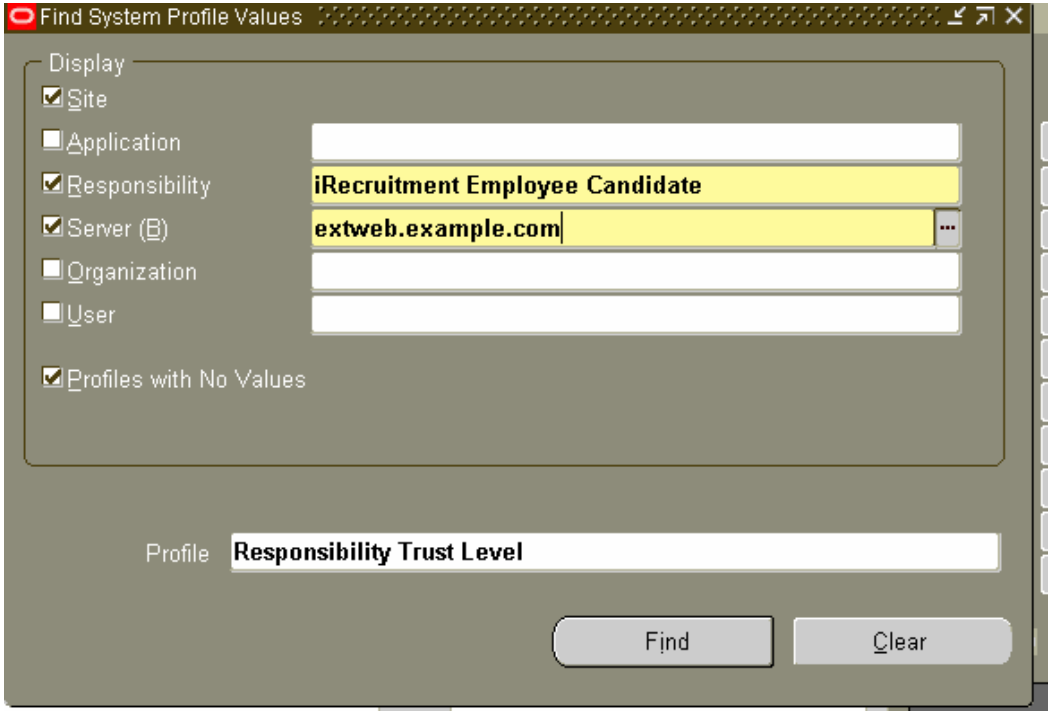
- Login to Oracle E-Business Suite as sysadmin user using the internal URL
- Select System Administrator Responsibility
- Select Profile / System

Set iRecruitment Responsibilities

- From the 'Find system profile option Values' window, select the iRecruitment responsibility that you want listed below to make external one at a time
  - iRecruitment Employee Candidate
  - iRecruitment External Site Visitor
  - iRecruitment External Candidate
  - iRecruitment Employee Site Visitor
  - iRecruitment Agency

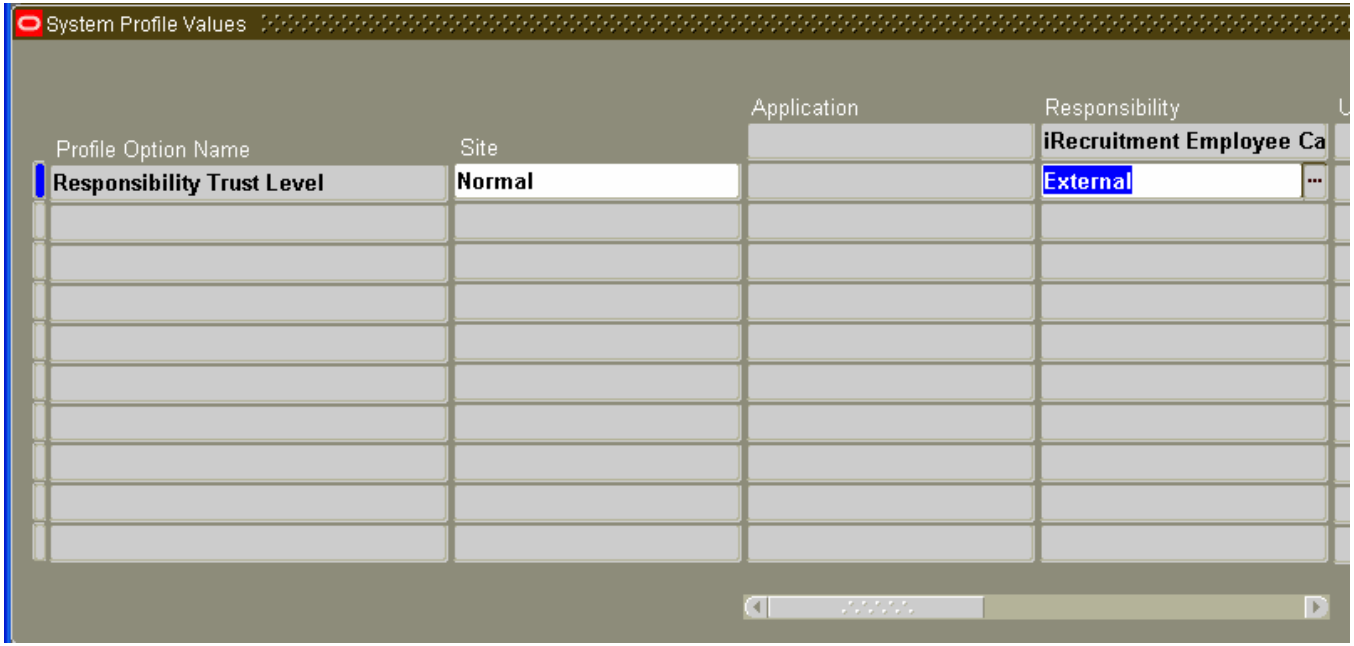
Set iRecruitment Responsibilities

- Query for '**Responsibility Trust Level'.** The value for this profile option at site level will be **Normal**.



Set iRecruitment Responsibilities

- Set the value of this profile option for the chosen responsibility to **External** at responsibility level (not site level). Do this for all 5 responsibilities.



Update Home Page Mode to Framework

- Login to Oracle E-Business Suite as sysadmin user using the internal URL
- Select System Administrator Responsibility
- Select Profile / System
- From the 'Find system profile option Values' window, query for '**Self Service Personal Home Page Mode**' and set to '**Framework Only'.**

Modify Guest Account

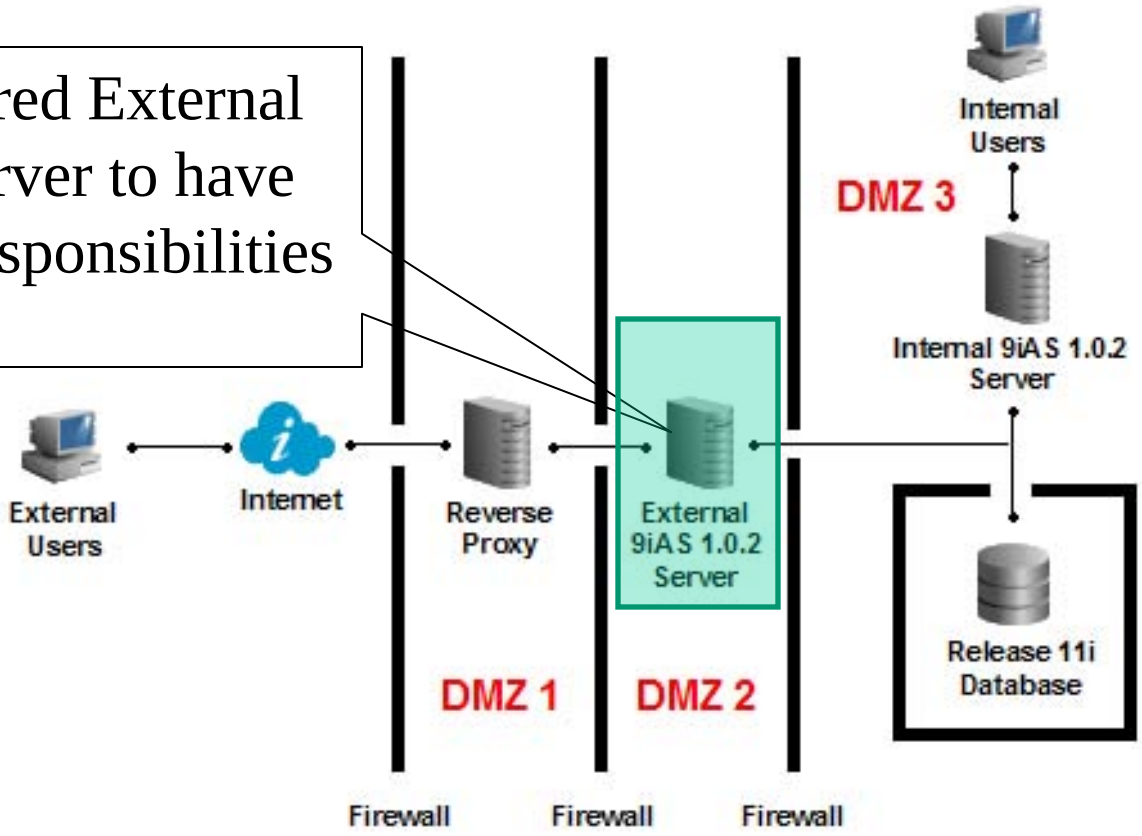
- Ensure that authentication is not needed to get to the iRecruitment Visitor's home page
  - Add the following responsibilities to the GUEST account
    - iRecruitment Employee Candidate
    - iRecruitment External Candidate

iRecruitment Error

- Visitors get "The iRecruitment Application is not currently installed. Please contact your Oracle Representative"
- Set the profile option 'IRC: Installed' to Yes at the site level.

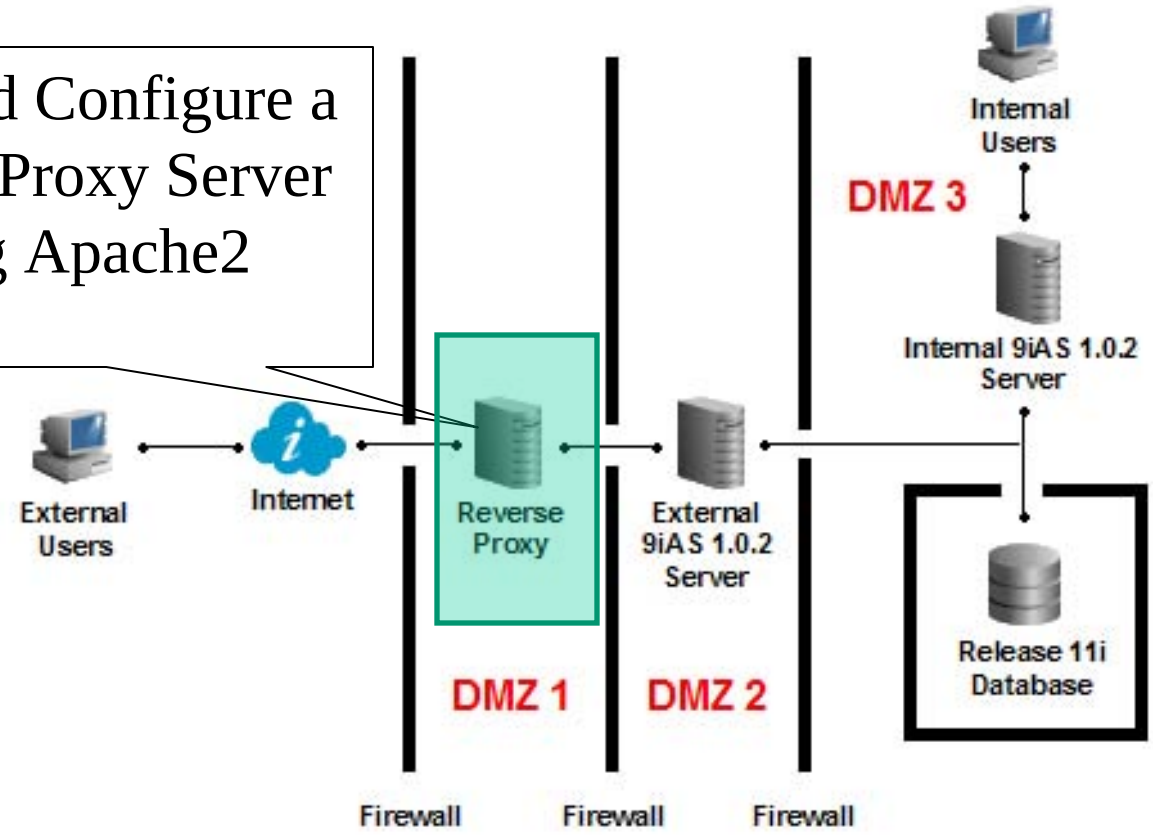
Project Update

Configured External Web Server to have limited responsibilities



Next Step

Build and Configure a Reverse Proxy Server Using Apache2



Build and Configure Reverse Proxy

- Download Apache
- Download mod_security
- Prepare Apache for Install
- Compile and Install Apache
- Enable URL Firewall
- Setup SSL

Download Apache

- Download from http://httpd.apache.org/download
- Apache version used was 2.0.54
- Obtain httpd-2.0.54.tar.gz
- Obtain httpd-2.0.54.tar.gz.md5
- Do the file checksum
  - md5sum -c httpd-2.0.54.tar.gz.md5
- Unpack downloaded file
  - tar xzvf httpd-2.0.54.tar.gz

Download mod_security

- Download from http://www.modsecurity.org/download
- mod_security version used was 1.8.7
- Obtain modsecurity-1.8.7.tar.gz
- Obtain modsecurity-1.8.7.tar.gz.md5
- Do the file checksum
  - md5sum -c modsecurity-1.8.7.tar.gz.md5
- Unpack downloaded file
  - tar xzvf modsecurity-1.8.7.tar.gz

Prepare Apache for Install

cd httpd-2.0.54

./configure --prefix /dmz --enable-ssl --enable-setenvif --enable-proxy \
--enable-proxy_http --enable-headers --enable-rewrite --enable-so \
--disable-charset-lite --disable-include --disable-env --disable-status \
--disable-autoindex --disable-asis --disable-cgi --disable-negotiation \
--disable-imap --disable-actions --disable-userdir --disable-alias

mod_rewrite first; then mod_proxy

cd modules/proxy

vi mod_proxy.c

Change the following parameter's value from:

```
ap_hook_translate_name(proxy_trans, NULL, NULL,
    APR_HOOK_FIRST);
```

to:

```
ap_hook_translate_name(proxy_trans, aszSucc ,
    NULL, APR_HOOK_FIRST);
```

Compile Apache Source Code

- Compile Apache

  cd ../..

  make

- List modules

  httpd –l

- Required Modules

core.c	proxy_http.c
mod_access.c	mod_ssl.c
mod_auth.c	prefork.c
mod_log_config.c	http_core.c
mod_headers.c	mod_mime.c
mod_setenvif.c	mod_dir.c
mod_proxy.c	mod_rewrite.c
mod_so.c	

Install Apache in /dmz

- As root in httpd-2.0.54 directory

  umask 022

  make install

  chown –R root:sys /dmz

- Edit /dmz/conf/httpd.conf
  - Modify ServerName to irecruitment.example.com

Install mod_security

- Change directory to modsecurity-1.8.7

cd apache2

/dmz/bin/apxs –cia mod_security.c

Post Install

- Remove the following directives from httpd.conf
  - UserDir
  - Alias
  - AliasMatch
  - RedirectMatch
  - ScriptAlias
  - IndexOptions FancyIndexing VersionSort
  - AddIconByEncoding
  - AddIconByType
  - AddIcon
  - DefaultIcon
  - ReadmeName
  - HeaderName
  - IndexIgnore
  - LanguagePriority
  - ForceLanguagePriority

Validate Apache Installation

- Start Apache

/dmz/bin/apachectl start

- Test Apache
  - http://irecruitment.example.com/index.html.en

- Shutdown Apache

/dmz/bin/apachectl stop

Set Up SSL in Apache

- Generate and install a test certificate

```
cd /dmz/conf
umask 022
mkdir ssl.key
mkdir ssl.crt

openssl req -new -x509 -days 30
-keyout ssl.key/server.key -out ssl.crt/server.crt
-subj '/CN=Test-Only Certificate‘

 chmod 600 ssl.key/server.key
```

Validate SSL

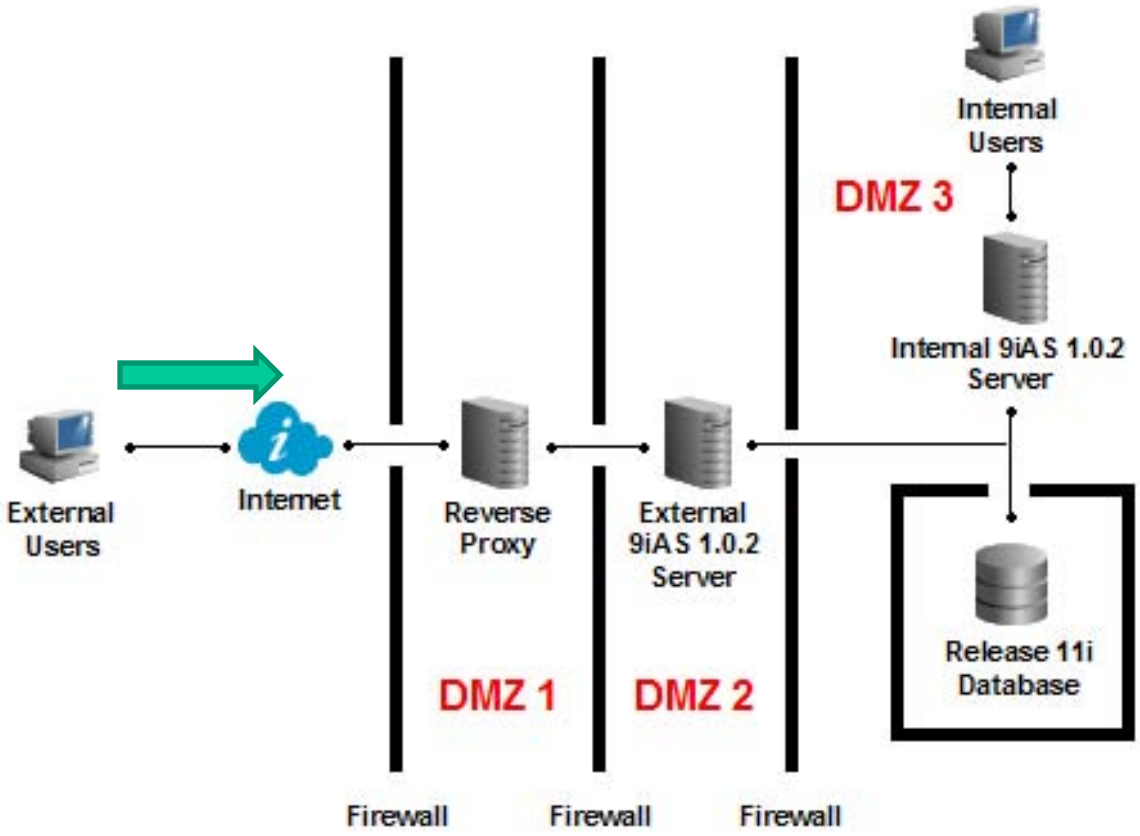
- Start Apache with SSL

  /dmz/bin/apachectl startssl

- Access Apache

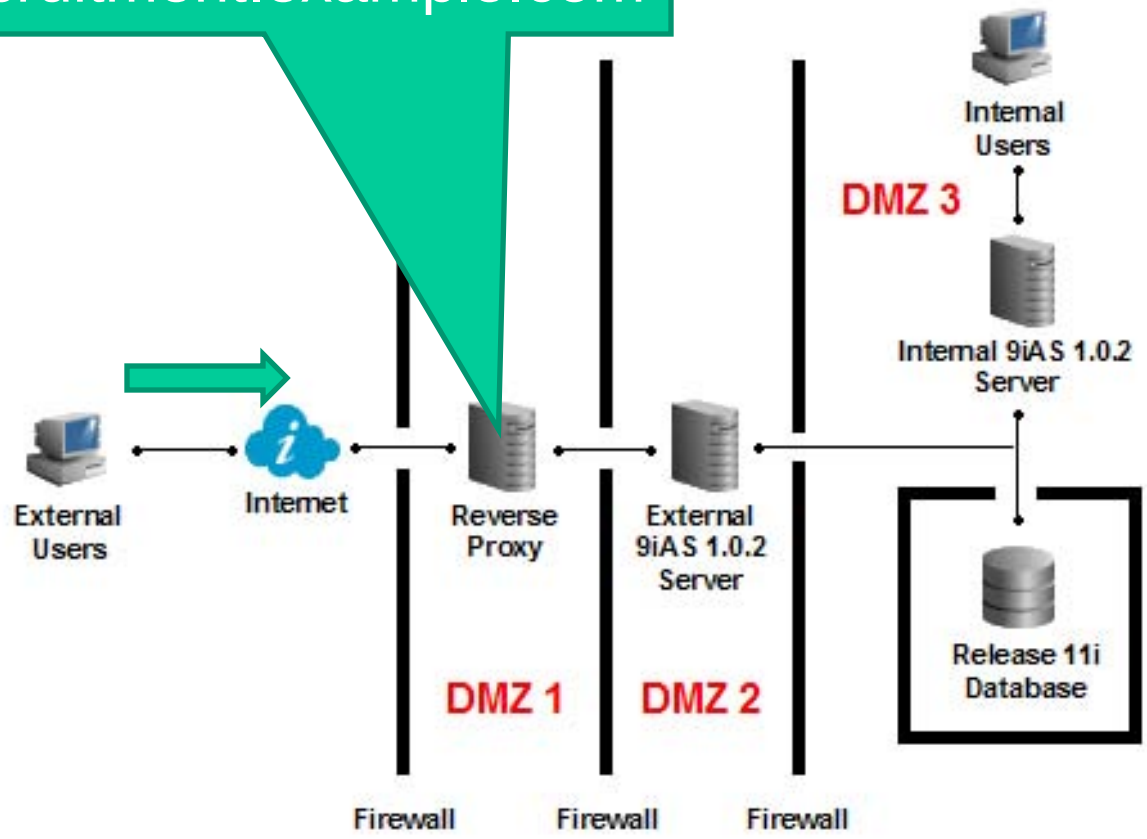
  https://irecruitment.example.com/index.html.en

What to Expect from Reverse Proxy?



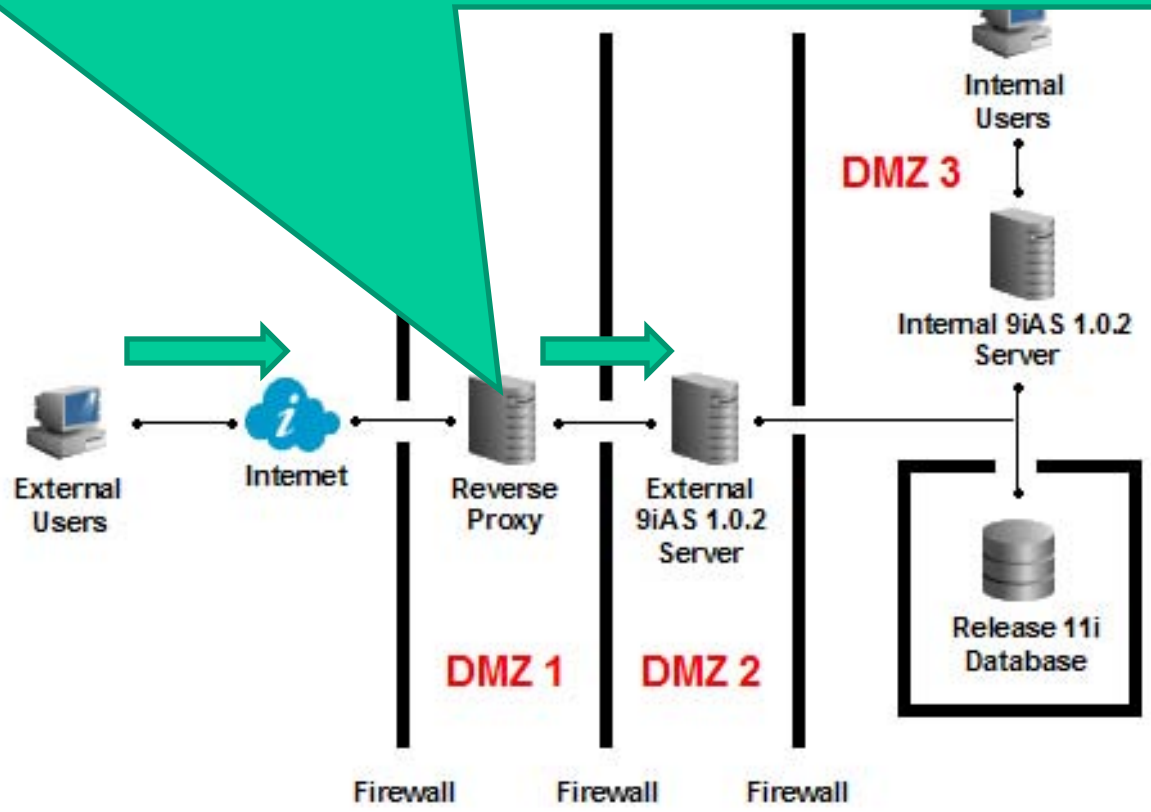
What to Expect from Reverse Proxy?

https://irecruitment.example.com

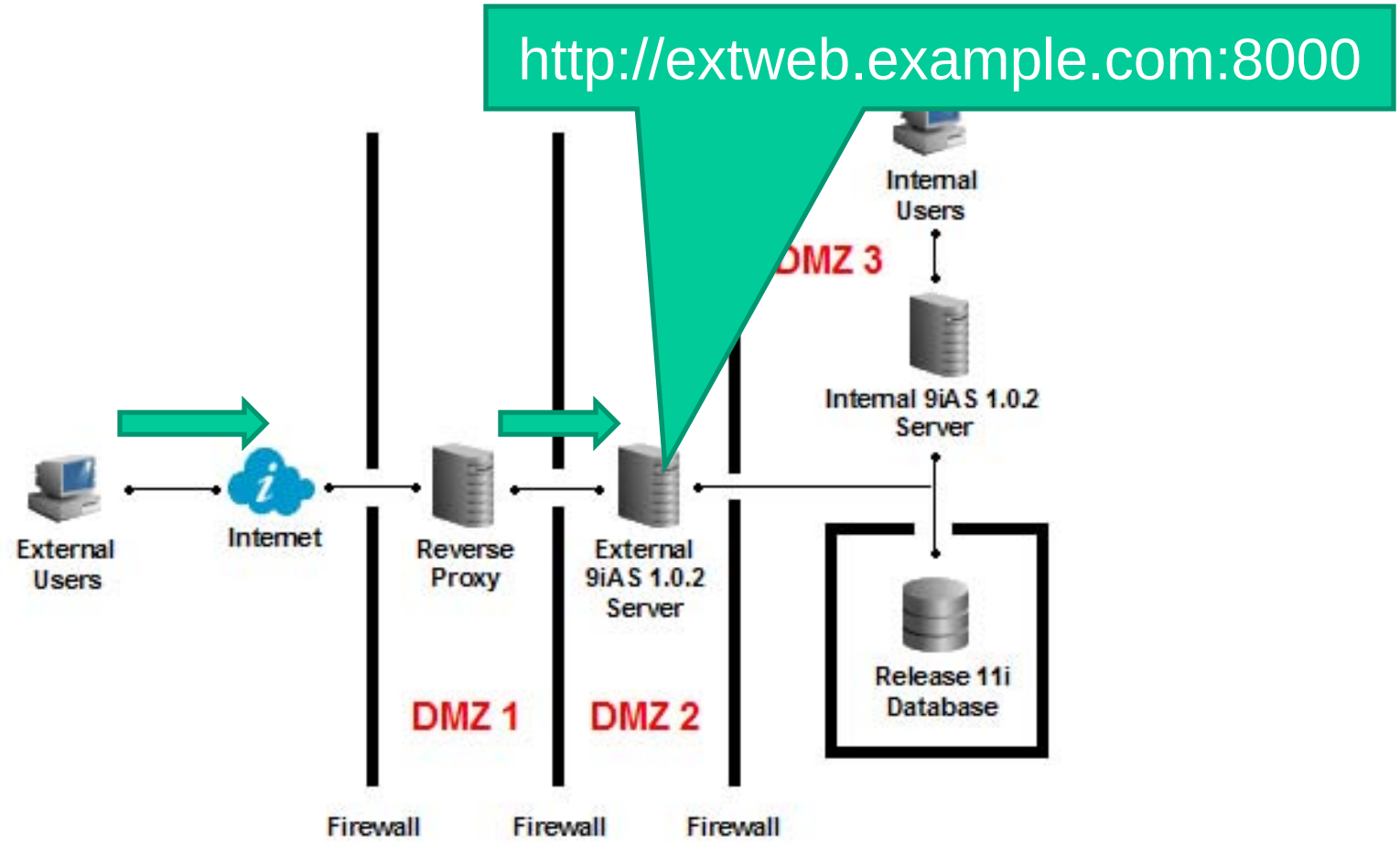


What to Expect from Reverse Proxy?

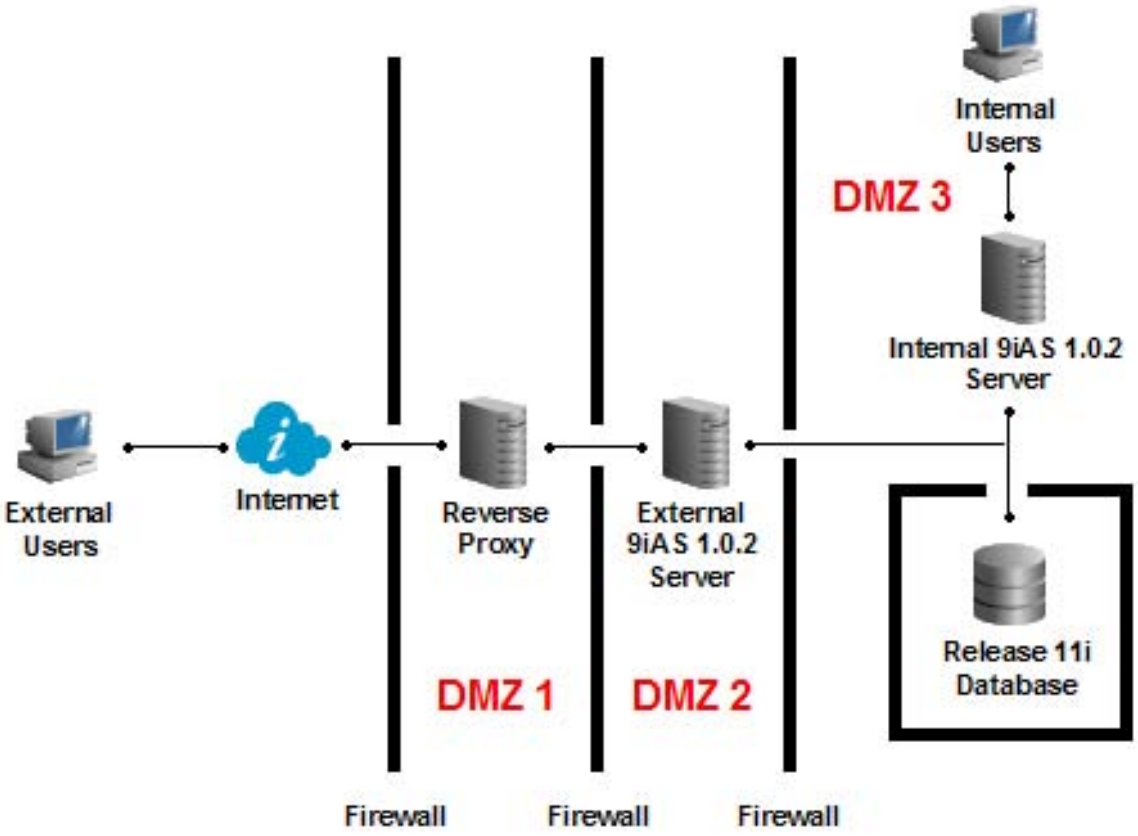
https://irecruitment.example.com => http://extweb.example.com:8000



What to Expect from Reverse Proxy?



Reverse Proxy w/ External Web Server Benefit



Key Apache Modules

- mod_rewrite
- mod_ssl
- mod_proxy
- mod_proxy_http
- mod_security

mod_rewrite

- Uses the URL Rewriting Engine
  - Manipulates URL
    - If a URL is accessing via http, it will be rewritten as https to maintain security
    - If a URL being accessed from Apache is not a known URL, it will be rejected by the ReWriteRule
      - URL Firewall discussed later

mod_ssl

- Provides strong cryptography using the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols
- The most pertinent Apache Directive in httpd.conf are
  - SSLCertificateFile
  - SSLCertificateKeyFile

mod_proxy & mod_proxy_http

- Communicates with the external web server on behalf of the requestor
  - Hides the identity of Oracle Apps external web server from requestor
- The most pertinent Apache Directive in httpd.conf are
  - ProxyPass
  - ProxyPassReverse

mod_security

- Behaves as the Web Application Firewall
- It discovers and blocks requests that are suspicious and intentionally malformed to launch an attack
  - Rejects bad requests before anything else happens

Configuring Apache as Reverse Proxy

- httpd.conf and security.conf will be provided
- Appendix A (in white paper) has a complete working httpd.conf
- Appendix B (in white paper) has a complete working security.conf
- Assumptions
  - Website is known as irecruitment.example.com
  - External Web Server is known as extweb.example.com
  - Apache has been installed in /dmz

Key Apache Directives

- For port 80

RewriteRule ^/(.*) https://irecruitment.example.com/$1 [R,L]

- For port 443

ProxyPass / http://extweb.example.com:8000/

ProxyPassReverse / http://extweb.example.com:8000/

- Software Based Firewall
  - Include conf/security.conf
  - Include/url_fw.conf

URL Firewall (url_fw.conf)

- URL firewall file contains a whitelist of URLs
- URLs that does not match entries in the whitelist is rejected
- Attackers can only get to areas that are already secure

How to whitelist iRecruitment?

- Uncomment the following $IAS_ORACLE_HOME/Apache/Apache/conf/url_fw.conf of an APPL TIER
  - RewriteRule ^/OA_HTML/IrcVisitor\.jsp$ - [L]
  - RewriteRule ^/pls/[^/]*/irc_web.show_vacancy$ - [L]
  - RewriteRule ^/OA_HTML/JobPositionSeeker\.xsl$ - [L]
  - RewriteRule ^/OA_HTML/IRCRESUMEUK1\.xsl$ - [L]
  - RewriteRule ^/OA_HTML/IRCRESUMEUK2\.xsl$ - [L]
  - RewriteRule ^/OA_HTML/IRCRESUMEUS1\.xsl$ - [L]
  - RewriteRule ^/OA_HTML/IRCRESUMEUS2\.xsl$ - [L]
  - RewriteRule ^/OA_HTML/IRCRESUMEUS3\.xsl$ - [L]

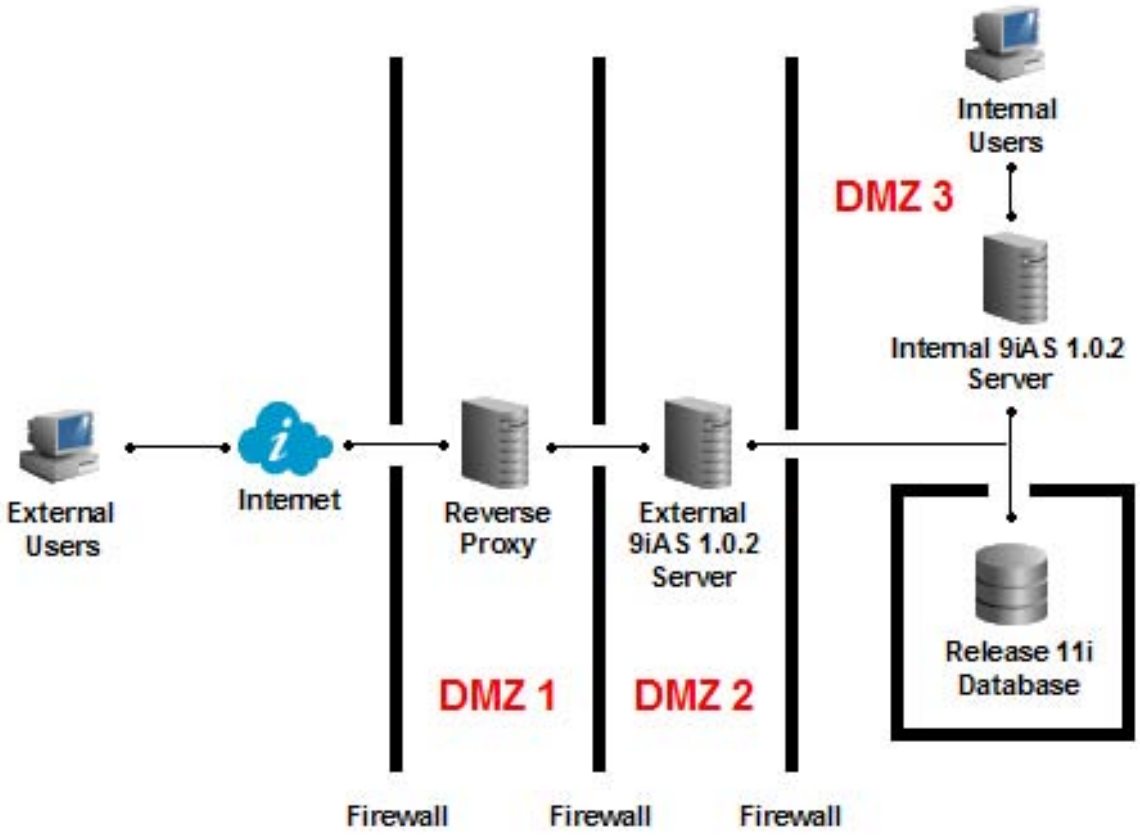
Change Main Page for iRec

- Access to external web server, presents an iRecruitment Visitor Home Page rather than the Apps Local Login page
- Uncomment the following $IAS_ORACLE_HOME/Apache/Apache/conf/url_fw.conf of an APPL TIER
  - RewriteRule ^/$ /OA_HTML/IrcVisitor.jsp [R,L]
- Comment the following
  - RewriteRule ^/$ /OA_HTML/AppsLocalLogin.jsp [R,L]

How to Enable URL Firewall?

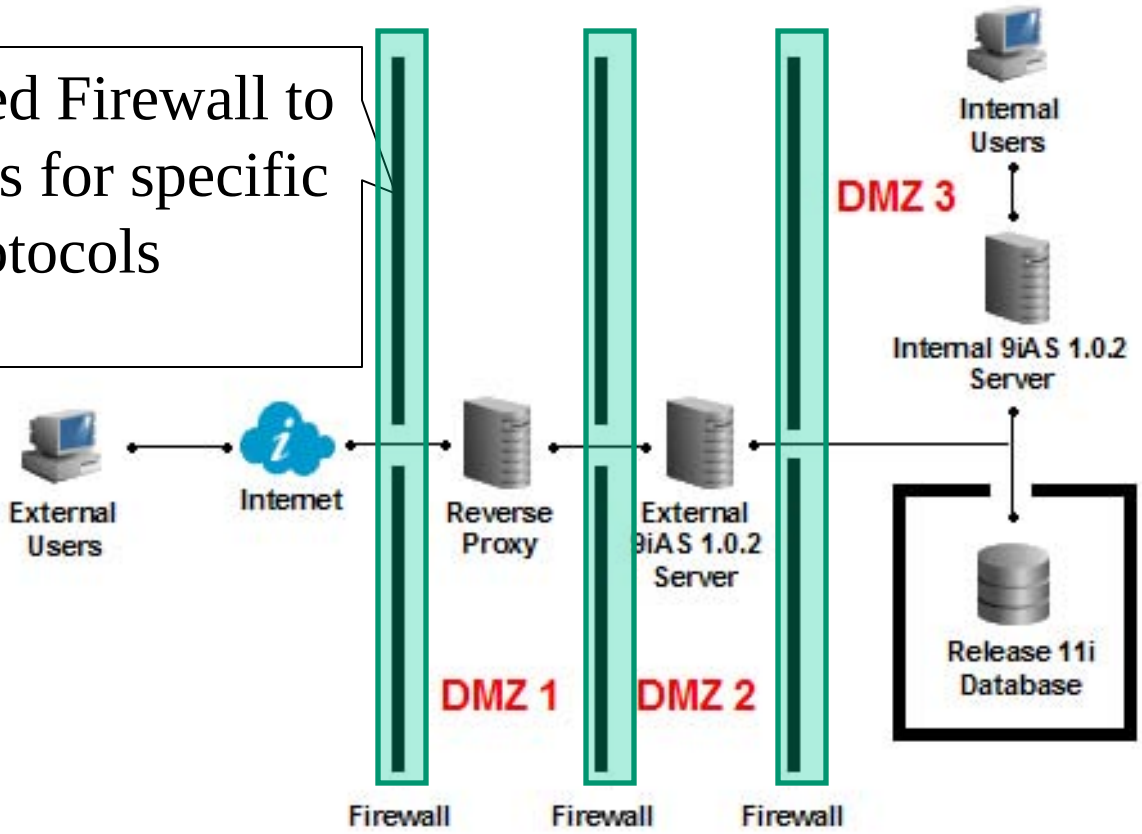
- Copy url_fw.conf from $IAS_ORACLE_HOME/Apache/Apache/conf of an APPL TIER and paste in the /dmz/conf of the Reverse Proxy Server
- Edit /dmz/conf/httpd.conf and uncomment Include directive for url_fw.conf
- Restart Apache

Accomplished Step



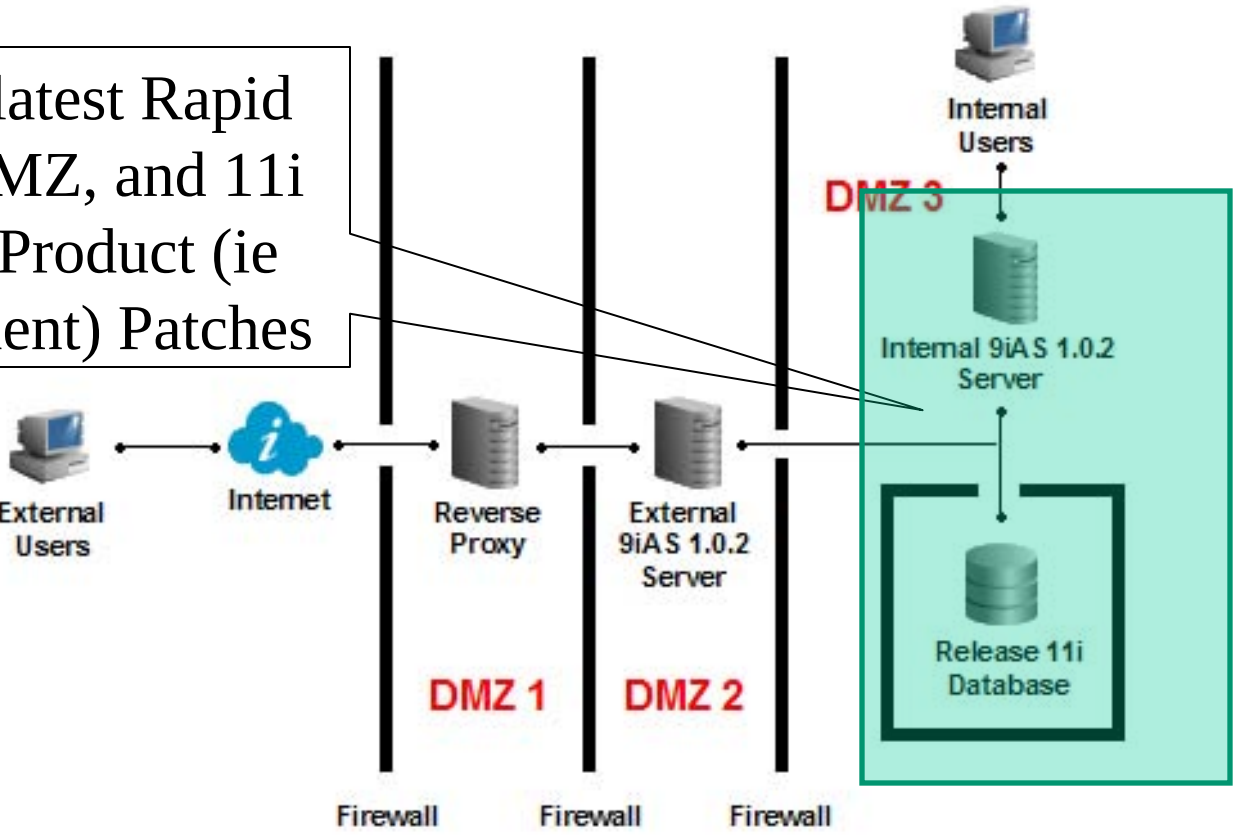
Accomplished Step

Configured Firewall to open ports for specific protocols



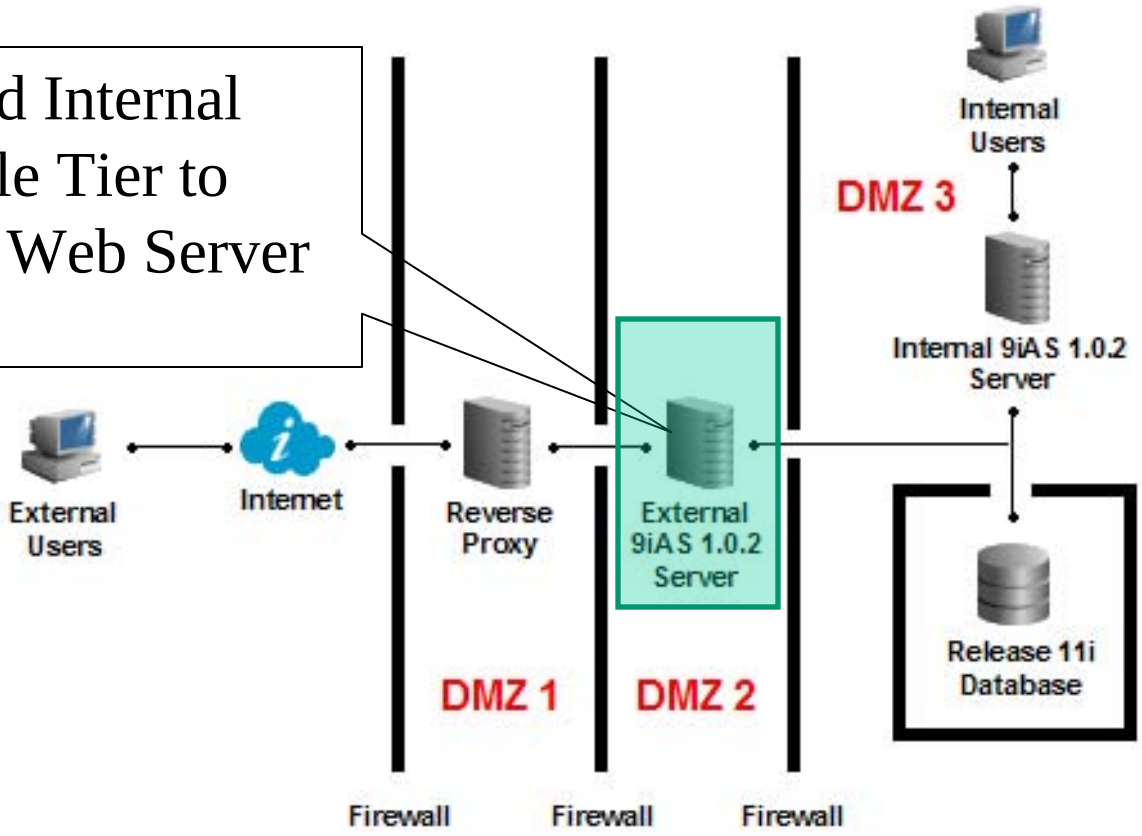
Accomplished Step

Applied latest Rapid Clone, DMZ, and 11i Internet Product (ie iRecruitment) Patches



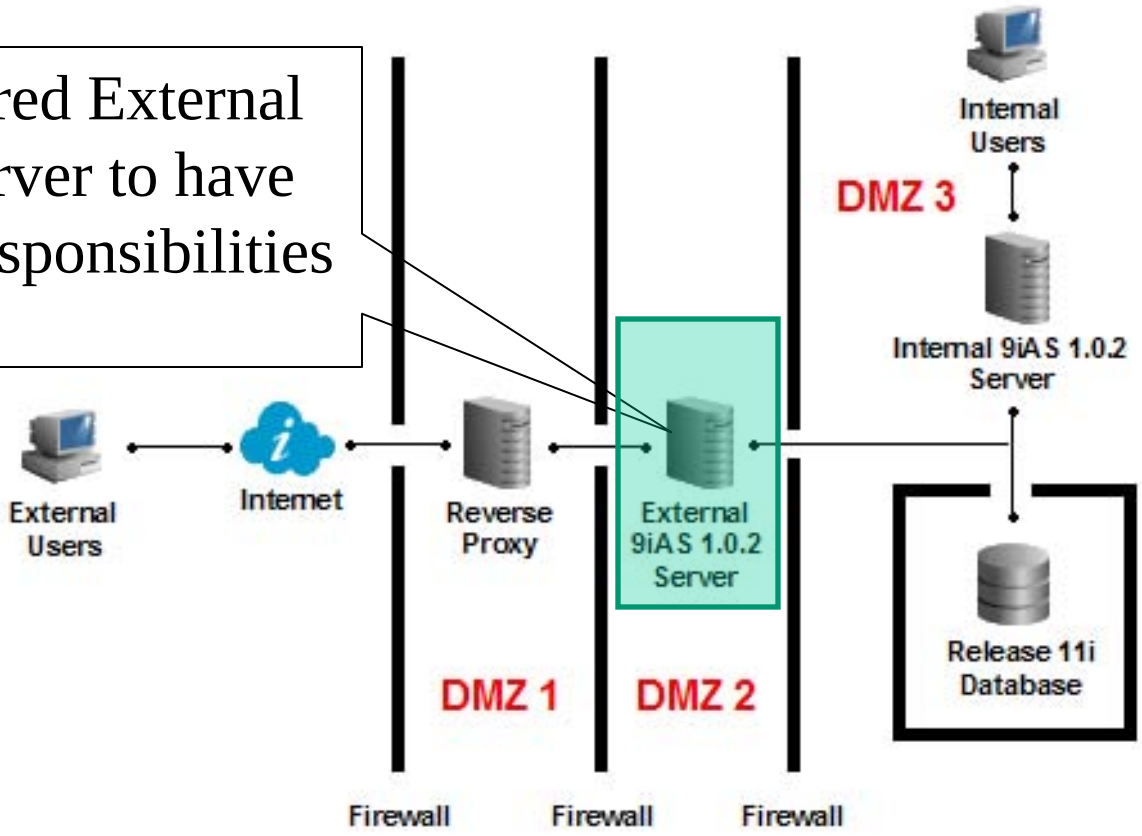
Accomplished Step

Cloned Internal Middle Tier to External Web Server



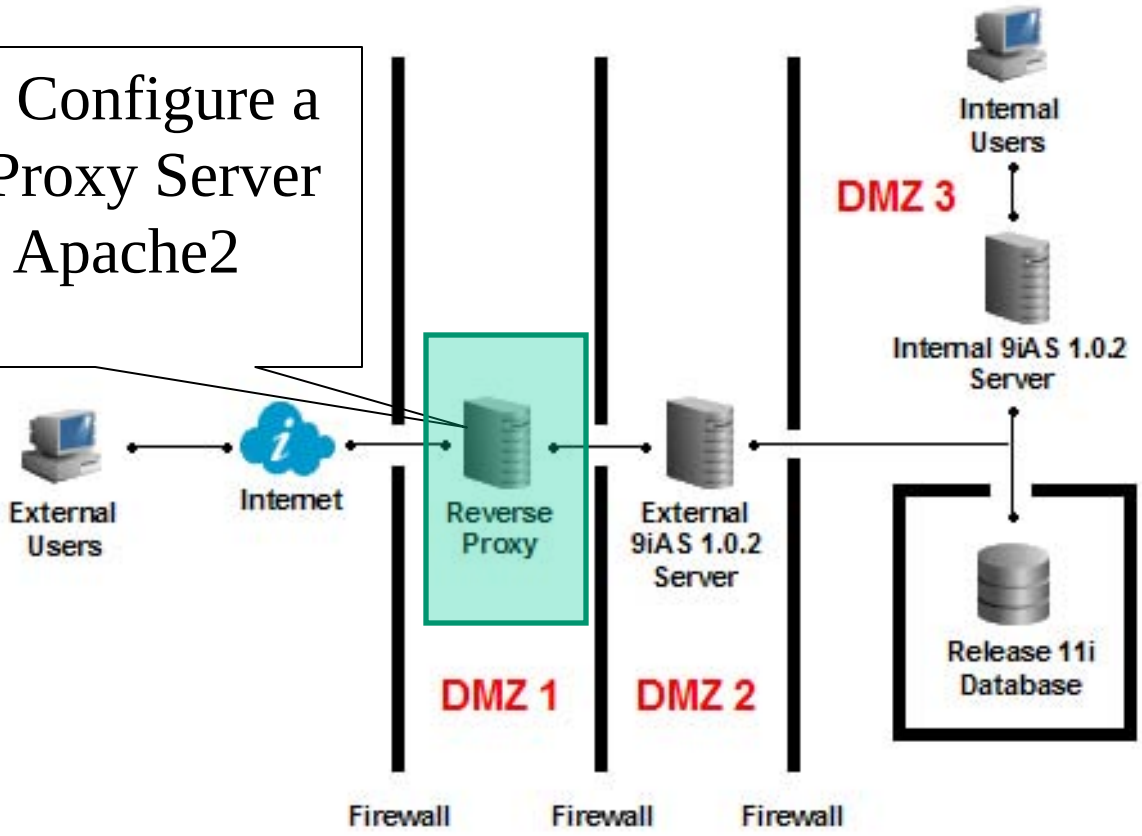
Accomplished Step

Configured External Web Server to have limited responsibilities



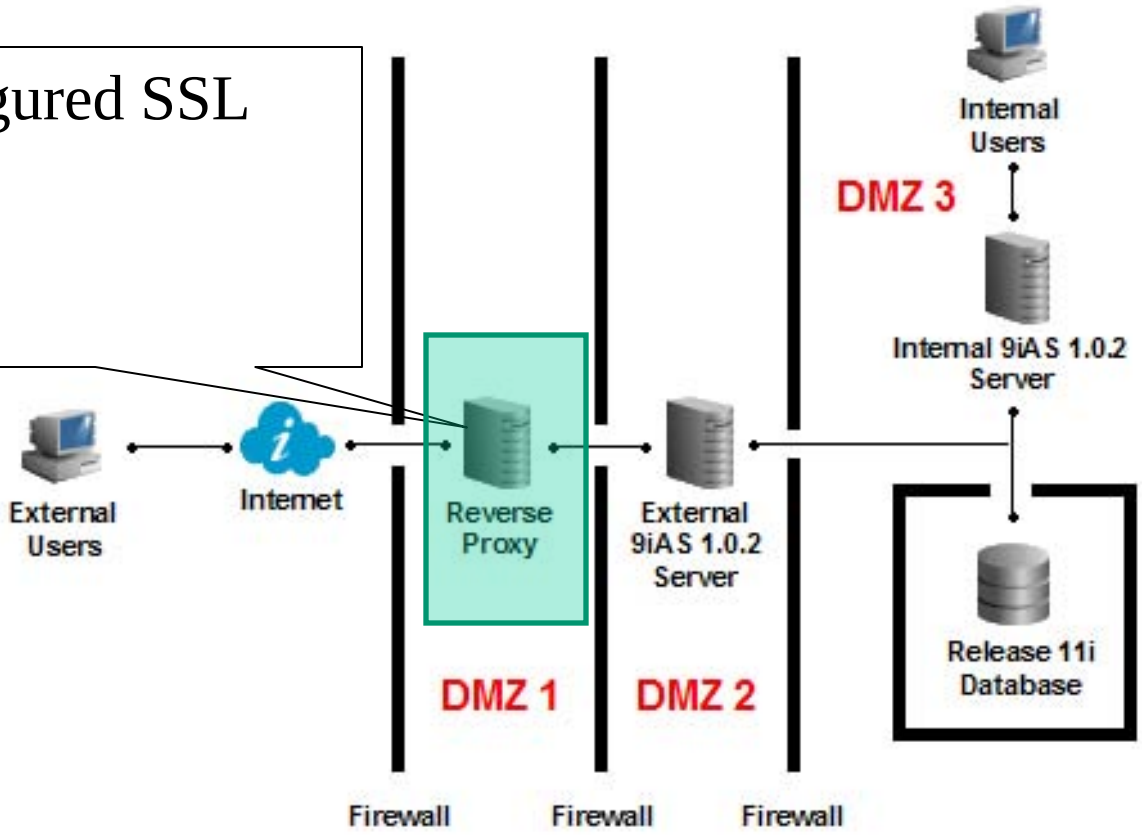
Accomplished Step

Built and Configure a Reverse Proxy Server Using Apache2



Accompished Step

Configured SSL



Intrusion Detection Systems (IDS)

- Misuse Detection
  - Searches for known attack signatures
  - Protects from wannabe hackers
- Anomaly Detection
  - Searches for unknown/new attacks
  - Protects from sophisticated attackers or insiders (ie disgruntled employees)
  - Compares current network activity to a baseline of normal network activity for a user or group

Good Security Policy

- Regardless of the expensive/sophisticated hardware and software security, valuable data can still be stolen without a good security policy
- Policies such as regular hardware and software updates, employee handling of information, and so on
- Attack From Inside
- Attack From Outside with someone from the Inside unknowingly assisting

Reference

- Metalink Note 287176.1
  - DMZ Configuration with Oracle E-Business Suite 11i
  - Review the note for items that pertains to you
- Metalink Note 373837.1
  - Oracle iRecruitment Implementation and User Guide

Now it's time for...