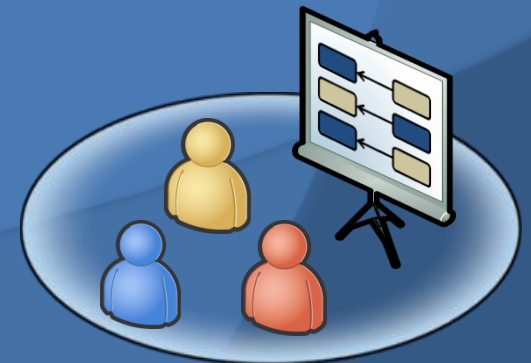
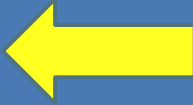


Delving Into Custom Authentication Providers In SharePoint

Reza Alirezaei MVP,MCTS
Principal Architect, Protech
<http://blogs.devhorizon.com/reza>



Authentication/Authorization in .Net World

1. Membership (Self-standing feature) 
2. Role (When combined with Membership)
3. Profile (User info, preferences, information about current session)

Previously in ASP.NET 1.x

1. You were on your own!
2. Limited to two options:
 - a) Windows Auth for Intranet Sites
 - b) FBA for public-facing sites
3. FBA = Creating everything from the scratch!
 - DL for storing data
 - BL for managing users and roles
 - PL for managing logging in, and so on

Previously in SharePoint

1. No support for FBA

<http://support.microsoft.com/kb/825214/en-us>

2. Client Integration

<http://support.microsoft.com/kb/838028/en-us>

3. WSS and SPS2003 with ADFS (with some limitations!)

<http://support.microsoft.com/kb/912492>

ASP.NET 2.0

1. Introduced Provider Model
2. OOTB SQL Membership and Role Provider
3. Supporting APIs
4. Integrated Template-based Server Controls
5. AD, SQL Server , LDAP Directory or any other directory that has an ASP.NET membership provider

WSS 3.0 and MOSS 2007

1. Everything that ASP.NET 2.0 offers
2. MOSS 2007: Built-in LDAP V3 membership and role Provider
3. Moss 2007 SSO pluggable pattern.
4. No membership provider for a directory?
5. Membership Data/Schema already exists in SQL Server, Oracle, CRM and etc ?

Application Management

This page contains links to pages that help you configure settings for applications and components that are installed on the server or server farm.

SharePoint Web Application Management

- [Create or extend Web application](#)
- [Remove SharePoint from IIS Web site](#)
- [Delete Web application](#)
- [Define managed paths](#)
- [Web application outgoing e-mail settings](#)
- [Web application general settings](#)
- [Content databases](#)
- [Manage Web application features](#)
- [Web application list](#)

Application Security

- [Security for Web Part pages](#)
- [Self-service site management](#)
- [User permissions for Web application](#)
- [Policy for Web application](#)
- [Authentication providers](#)

Workflow Management

- [Workflow settings](#)

SharePoint Site Management

- [Create site collection](#)
- [Delete site collection](#)
- [Site use confirmation and deletion](#)
- [Quota templates](#)
- [Site collection quotas and locks](#)
- [Site collection administrators](#)
- [Site collection list](#)

External Service Connections

- [Records center](#)
- [HTML viewer](#)
- [Document conversions](#)

Operations

This page contains links to pages that help you manage your server or server farm, such as changing the server farm topology, specifying which services are running on each server, and changing settings that affect multiple servers or applications.

Topology and Services

- Servers in farm
- Services on server
- Outgoing e-mail settings
- Incoming e-mail settings
- Approve/reject distribution groups

Security Configuration

- Service accounts
- Information Rights Management
- Antivirus
- Blocked file types
- Update farm administrator's group
- Information management policy configuration
- Manage settings for single sign-on

Logging and Reporting

- Diagnostic logging
- Usage analysis processing
- Information management policy usage reports

Global Configuration

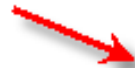
- Timer job status
- Timer job definitions
- Master site directory settings
- Site directory links scan
- Alternate access mappings
- Manage farm features
- Quiesce farm
- Solution management

Backup and Restore

- Perform a backup
- Backup and restore history
- Restore from backup
- Backup and restore job status

Data Configuration

- Default database server
- Data retrieval service



Questions?

Why do I need to extend my web application?

What is a zone?

What is AAM?

Policy for Web app?

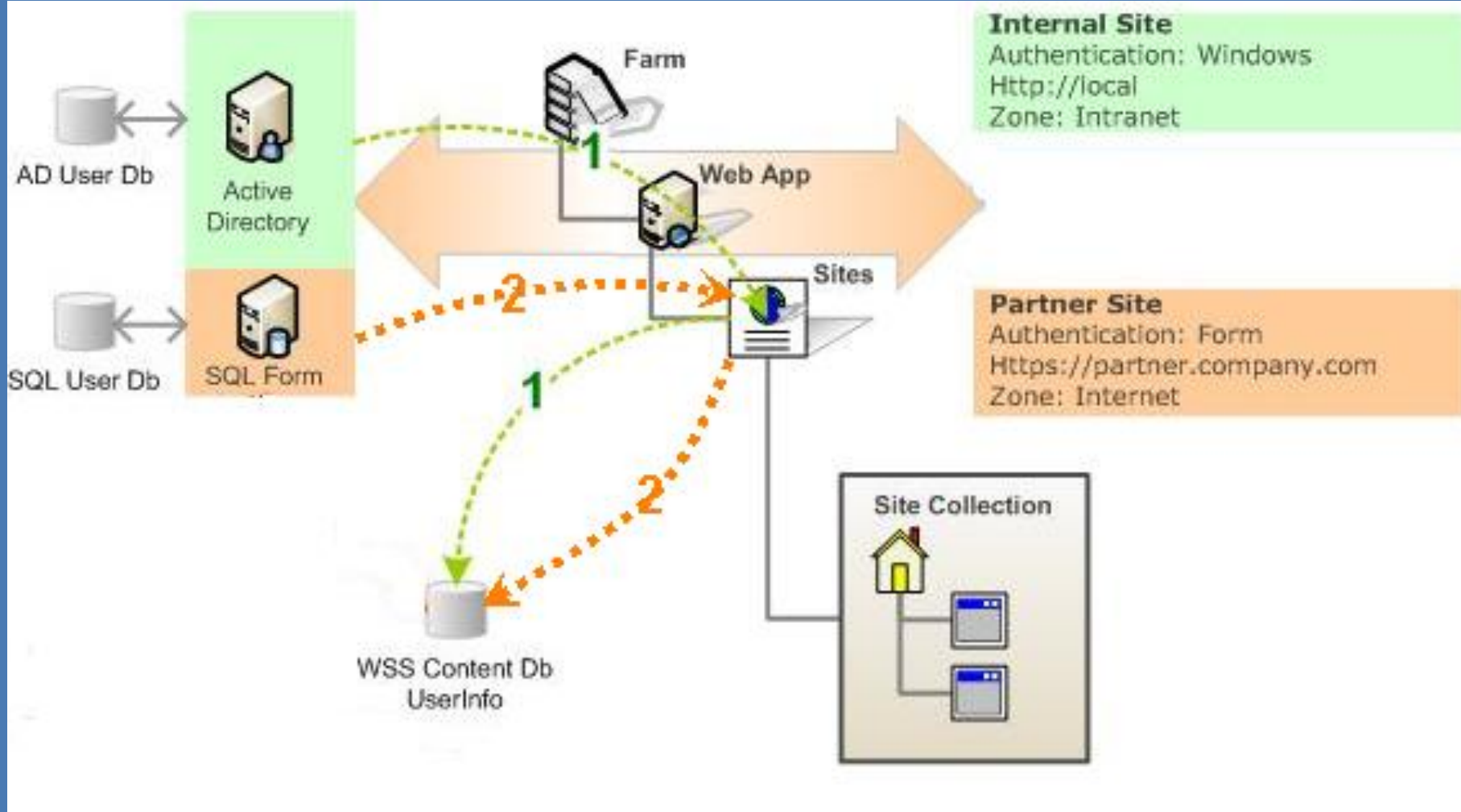


Answers:

1. Zone: Multiple entry points/authentication providers for the same web application (same content)
2. AAM : Association between URLs and Zones
3. AAM : Association between Internal and Public URLs
 - a) Public URL : End users see or click (Internal & External)
 - b) Internal URL: Load balancer or ISA uses
4. Policy: Grant/Deny/Override different access controls for users for an specific zone from CA (perfect for FBA)

Reviewing a Common Scenario





Steps to provision an FBA-enabled site:

1. Create an application for default zone with Windows Auth (Must)
2. Extend the above application
 - a) Use a standard port (80 ,443 and etc)
 - b) Always Use a host header
 - c) Choose NTLM or Kerberos (will change it to Forms later)
 - d) Allow anonymous if applicable (you can also do it later)
 - e) Remove :80 if applicable
 - f) Select the Zone (Something other than default)
1. Perform the following actions:
 - a) Add DNS entry for new Web application
 - b) Add IP address if not using host headers explicitly
OR
 - a) Add an entry for your host header in the hosts files of the machines you will be hitting the site from.
2. Change the authentication type to Forms and check to see if request goes through (AAM, Firewall, NLB,etc)
3. Don't forget to apply SP1 !!

demo

- Extending a web application
- Zone
- Load Balancer URL

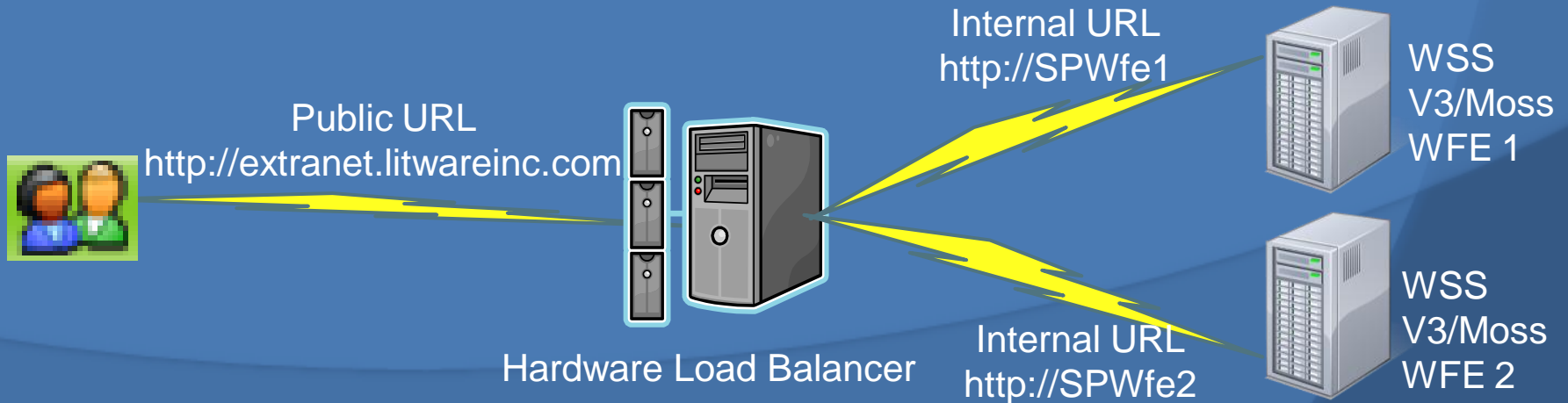
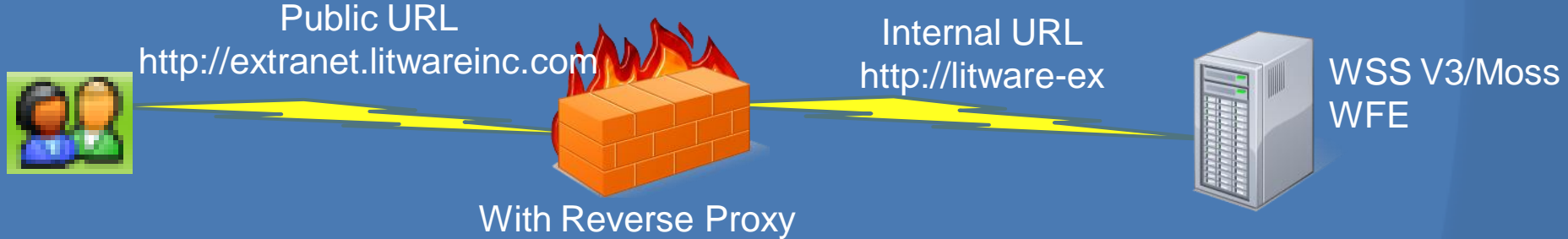
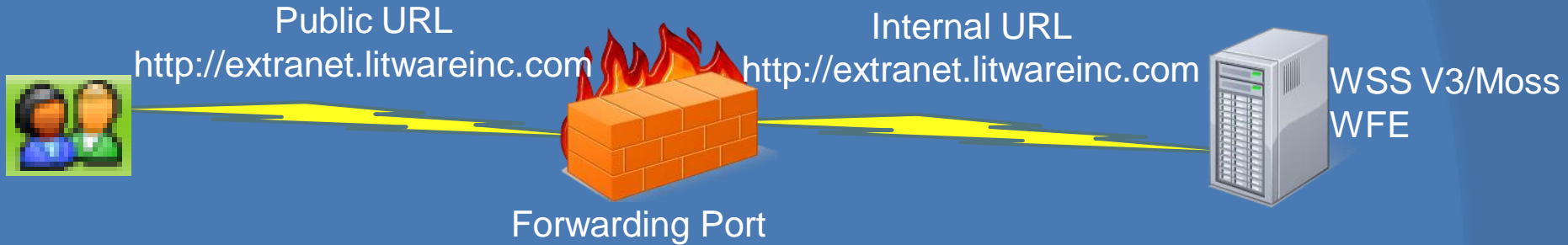


demo

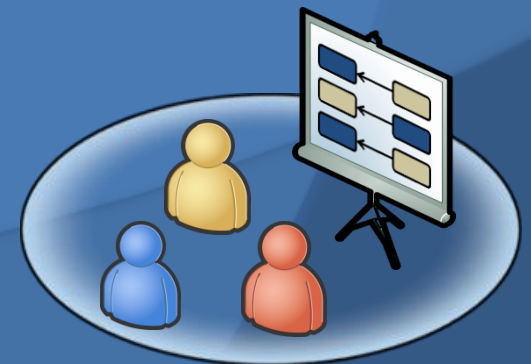
- AAM
- Different Configurations (slide)



AAM Different Configurations:



Membership Data Has to Go Somewhere



demo

- aspnet_regsql.exe
- Membership Seeder



demo

- Cross Database dependencies
- Code Walk-through
- Introducing FBA settings to CA, Default and Extranet Zones
- Custom Logon Page
- Debugging
 - Show Processes from All Users
 - iisreset
 - Attach to all w3wp.exe processes
- Resolving Names/Account Names
- SQL Profiling



Tools “R” Us



Tools:

- FBA Utility Pack (Central Admin)
- Trace :
 - TraceProvider (CKS:IEE)
 - Provider Logging on CodePlex
 - <http://www.codeplex.com/ProviderLogging>
 - Other Trace Facilities
- SQL Profiler
- SharePoint 2007 Features on CodePlex
 - <http://www.codeplex.com/features>
- FBA PowerShell Script and cmdlets
- <http://software.sharepointsolutions.com/support/knowledge/SPSolutionsSharePointCommands/Pages/default.aspx>
- Membership Seeder (Source and Binary)
 - <http://www.codeplex.com/CKS/Release/ProjectReleases.aspx?ReleaseId=7450>
- Fiddler (What's going on with my http request)
 - <http://www.developer.com/lang/jscript/article.php/3631066>

Possible topics to be added for Toronto Code Camp 2008

- MySites
- Profile Imports
- More on Tracing
- Client Integration
- Reusing the cookie
- SSO and FBA
- More on crawling FBA sites (different for WSS and Moss)

References:

- Community Kit For SharePoint on CodePlex
 - <http://www.codeplex.com/CKS>
- Authentication Resource Center for SharePoint Products and Technologies (One stop shop!)
 - <http://technet.microsoft.com/en-us/office/sharepointserver/bb735938.aspx>
- Real World SharePoint 2007
 - <http://www.amazon.com/Real-World-SharePoint-2007-Indispensable/dp/0470168358>
- My blog
 - <http://blogs.devhorizon.com/reza>

Thank You