Toronto SharePoint Camp

SHAREPOINT 2010 EXTRANETS AND AUTHENTICATION

Peter Carson

peter@envisionit.com

Introduction – Peter Carson

- President, Envision IT
- SharePoint MVP
- Virtual Technical Specialist, Microsoft Canada
- Computer Engineering, UW
- peter@envisionit.com
- http://blog.petercarson.ca
- www.envisionit.com
- Twitter @carsonpeter

Toronto SharePoint Camp

THANKS TO OUR SPONSORS!

Microsoft

K2

idera

navantis

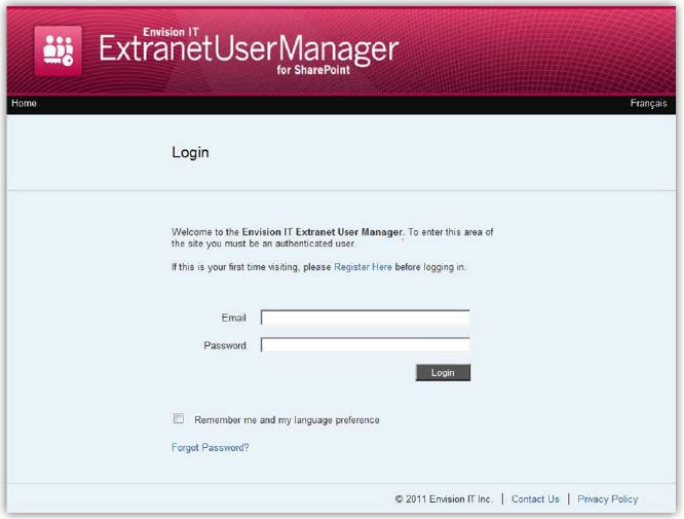
non~linear creations

Envision IT

Taking SharePoint to a new level of user experience

TSPUG

Envision IT ExtranetUserManager for SharePoint



- Easy delegation of user management to business
- Self-registration, approvals, forgotten password reset
- Single URL and sign-on for AD

Agenda

- Authentication Background
- Preparing your site
- Setting up FBA
- ADFS Federation
- Windows Live ID Federation
- Combining it all together

Four Categories of Users

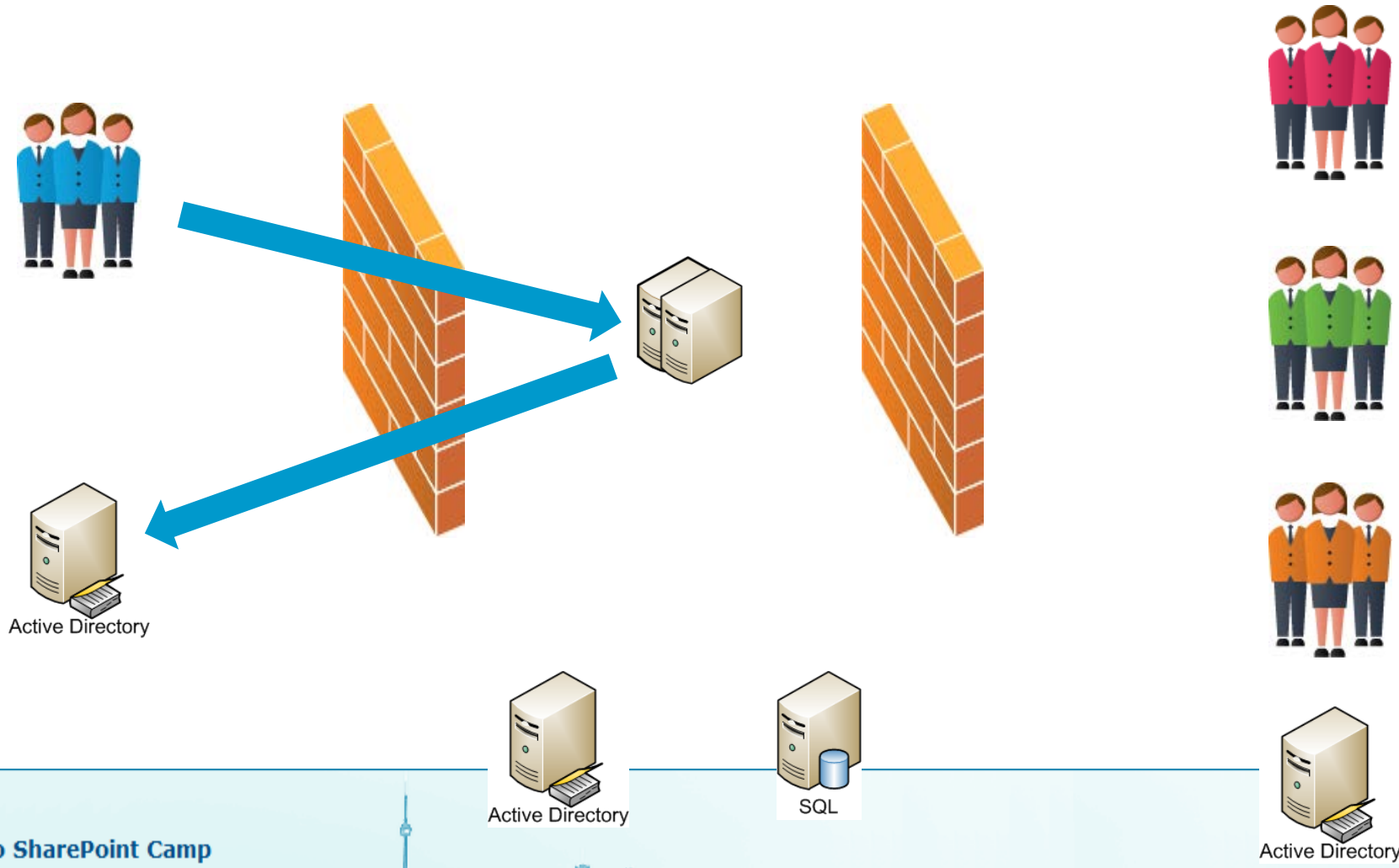
Internal Users

Managed AD Users

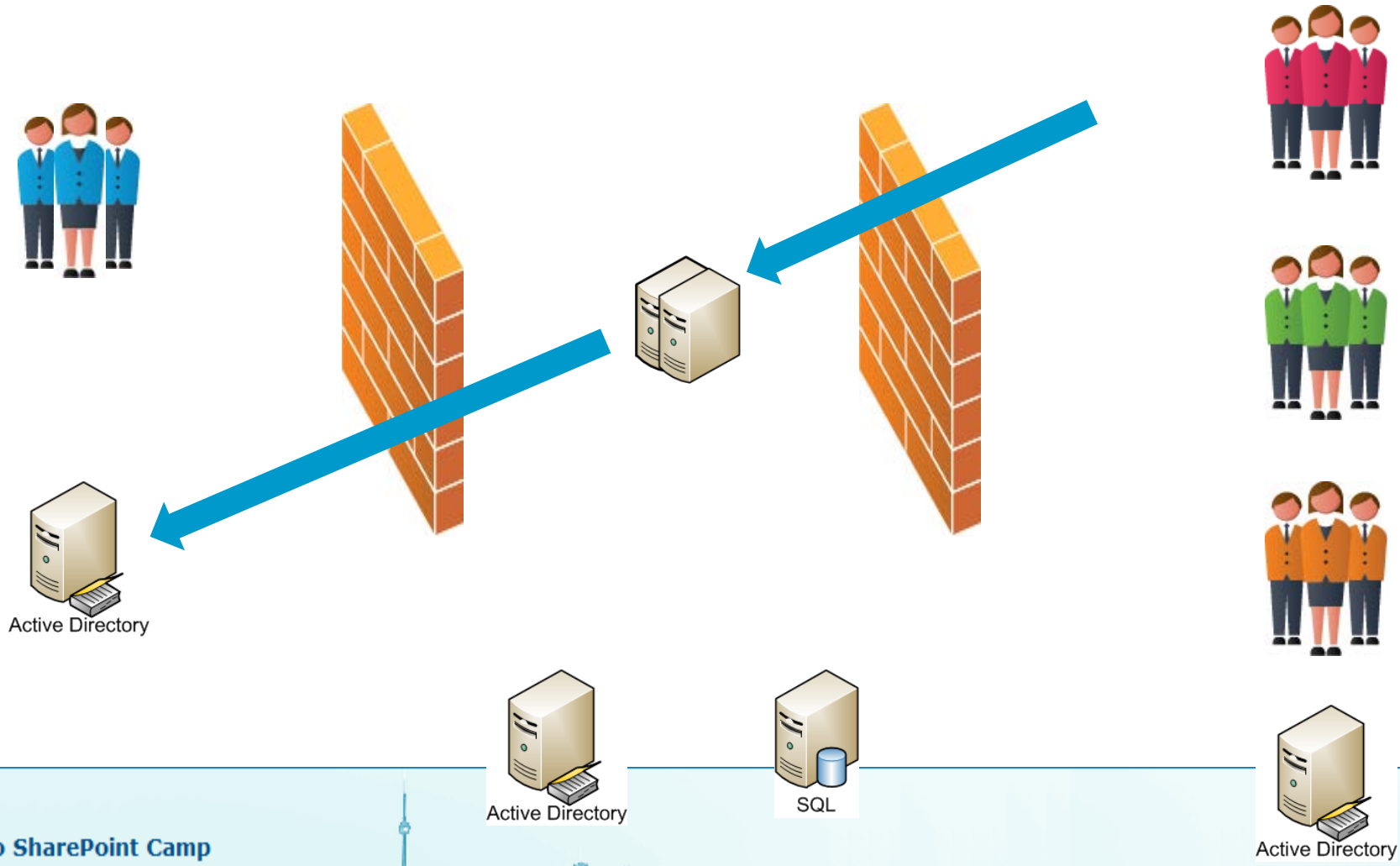
Managed SQL Users

Federated Users

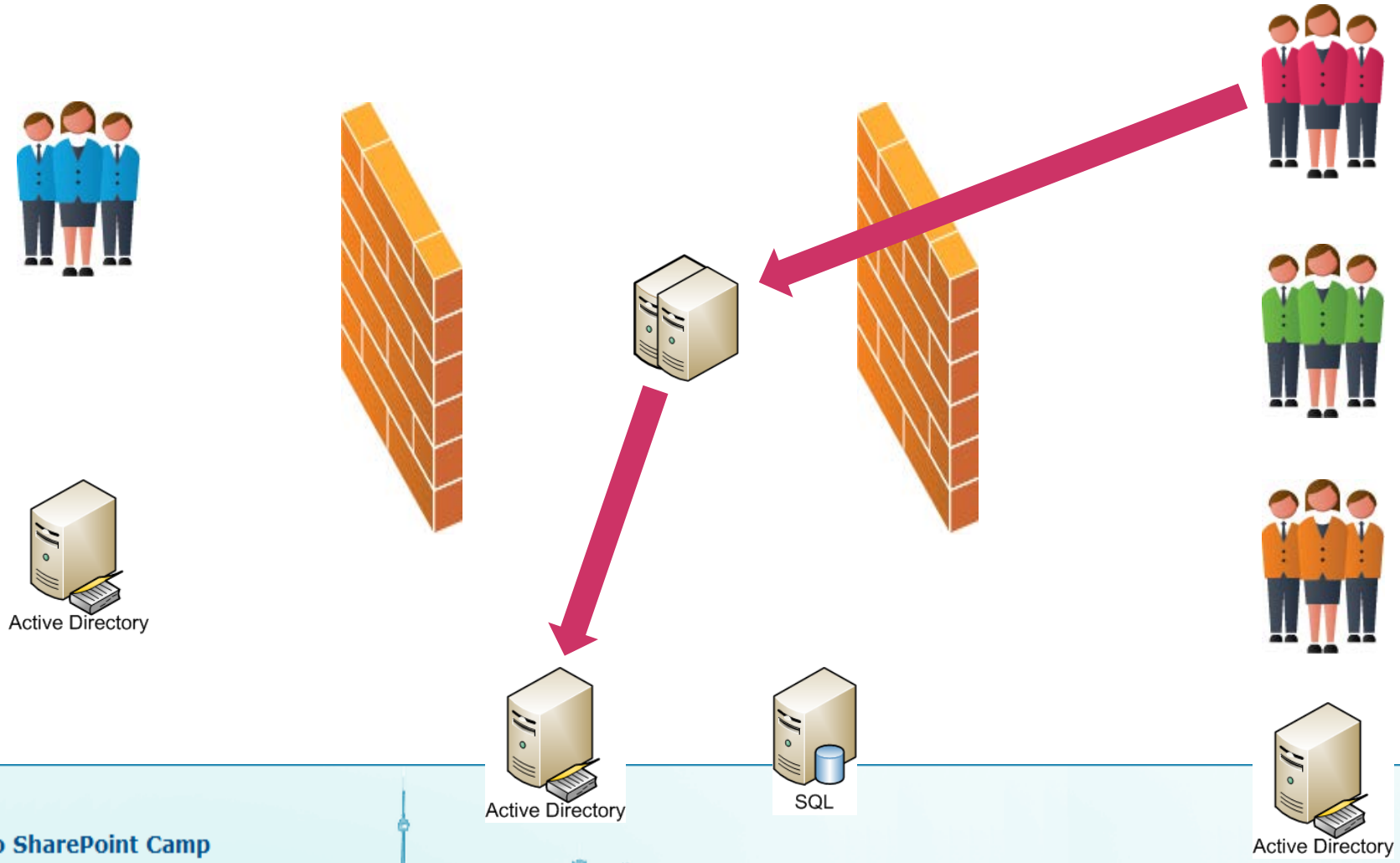
Internal Users Accessing from Inside



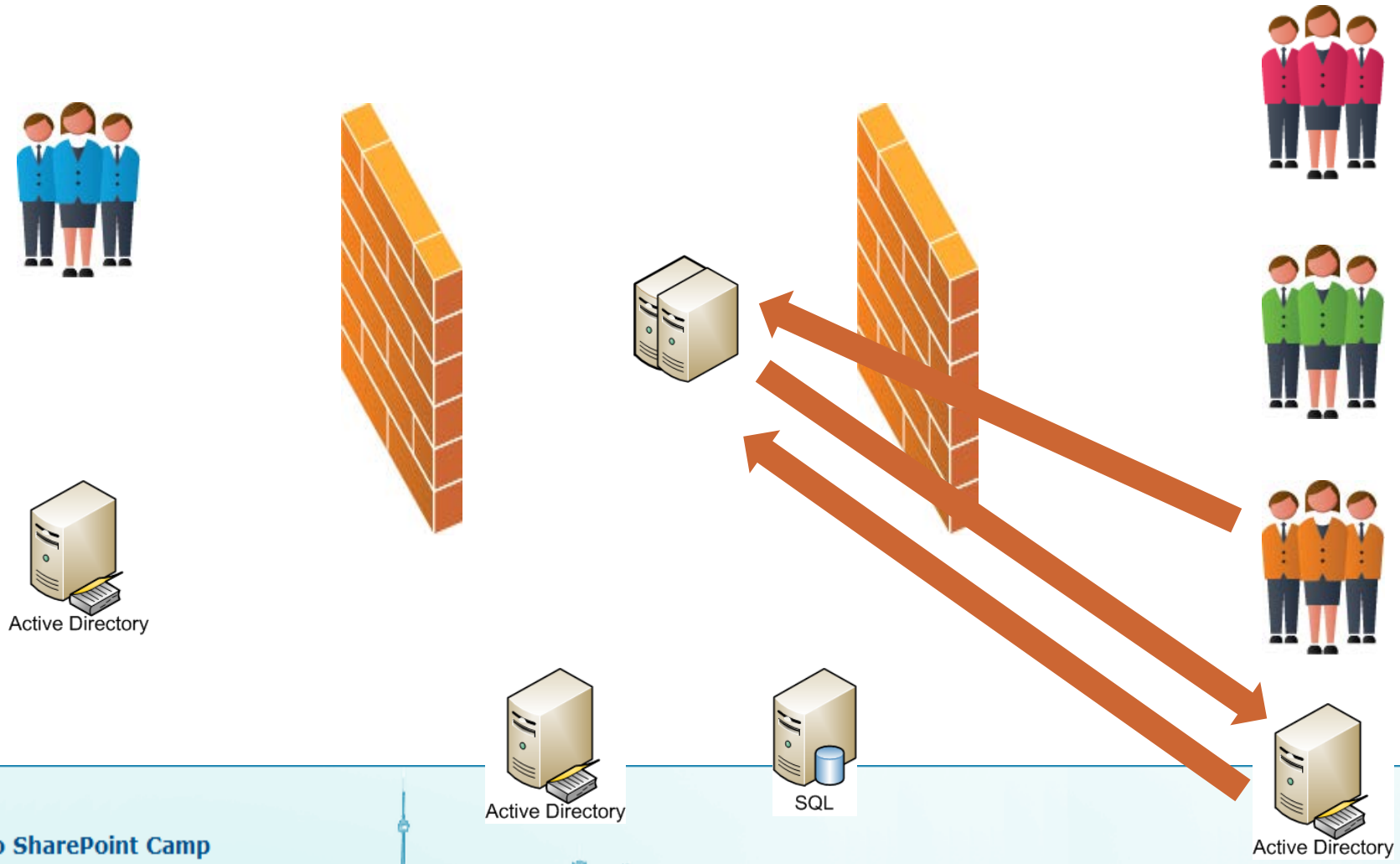
Internal Users Working Remotely



Managed Users



Federated Users

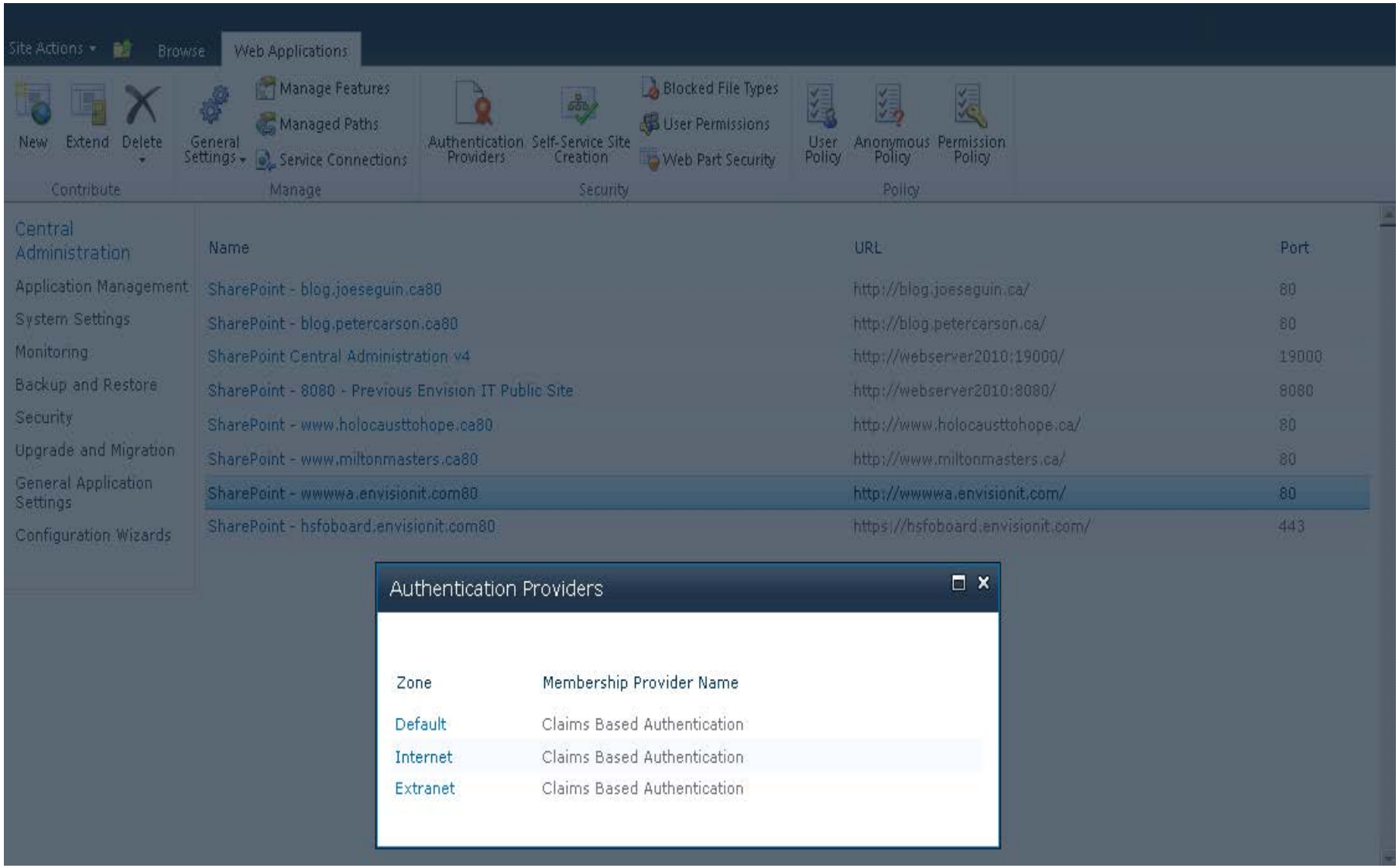


Preparing Your Site

- Ensure that the site is using Claims based security
  - If the site is Classic, there is a PowerShell script that will do a one-time conversion from Classic to Claims

```
> $webapp = Get-SPWebApplication("http://urlToWebApplication:Port")
> $webapp.UseClaimsAuthentication = 'True'
> $webapp.Update()
> $webapp.ProvisionGlobally()
```

- You need to have a default WA zone for the search crawler to work
- Extend the WA site to a new site for the Extranet zone
  - Generally you want to use SSL
- If the site is also going to be available anonymously you should extend it a third time for port 80 anonymous for the Internet zone


Site Actions
Browse
Web Applications
New
Extend
Delete
Contribute
General Settings
Manage Features
Managed Paths
Service Connections
Manage
Authentication Providers
Self-Service Site Creation
Blocked File Types
User Permissions
Web Part Security
Security
User Policy
Anonymous Policy
Permission Policy
Policy
Central Administration
Application Management
System Settings
Monitoring
Backup and Restore
Security
Upgrade and Migration
General Application Settings
Configuration Wizards
Name
URL
Port
SharePoint - blog.joeseguin.ca80
http://blog.joeseguin.ca/
80
SharePoint - blog.petercarson.ca80
http://blog.petercarson.ca/
80
SharePoint Central Administration v4
http://webserver2010:19000/
19000
SharePoint - 8080 - Previous Envision IT Public Site
http://webserver2010:8080/
8080
SharePoint - www.holocausttohope.ca80
http://www.holocausttohope.ca/
80
SharePoint - www.miltonmasters.ca80
http://www.miltonmasters.ca/
80
SharePoint - wwwwa.envisionit.com80
http://wwwwa.envisionit.com/
80
SharePoint - hsfoboard.envisionit.com80
https://hsfoboard.envisionit.com/
443
Authentication Providers
Zone
Membership Provider Name
Default
Claims Based Authentication
Internet
Claims Based Authentication
Extranet
Claims Based Authentication

Tips to be Aware of

- If you want search to work anonymously, you need to enable anonymous access on your Windows Authentication zone
- SharePoint won't let you disable all authentication, but you can enable WA for the Internet zone, and then disable it in IIS
- SharePoint will let you configure a zone for SSL, but you still need to go into IIS to setup the certificate and bindings

Setting up FBA

- Decide on where your users are going to be stored
  - SQL or AD are the two common choices
- Setup the store
- Configure the authentication type for the Extranet zone
- Update web.configs for SharePoint web app, Central Admin, and Security Token Service

SQL versus AD Authentication

AD

- Requires a separate set of domain controllers
  - These may already be in place to support the SharePoint farm
- Provides richer policy and audit controls
- Single URL inside and outside if not using FBA

SQL

- Can use email address as the username
- Simpler to implement

Setting up the ASPNETDB Database

- C:\Windows\Microsoft.NET\Framework64\v2.0.50727\aspnet_regsql.exe -E -S *ServerName* –d *DatabaseName* –A all
- You need to have the –A all option to have Role support setup

Plan your Settings

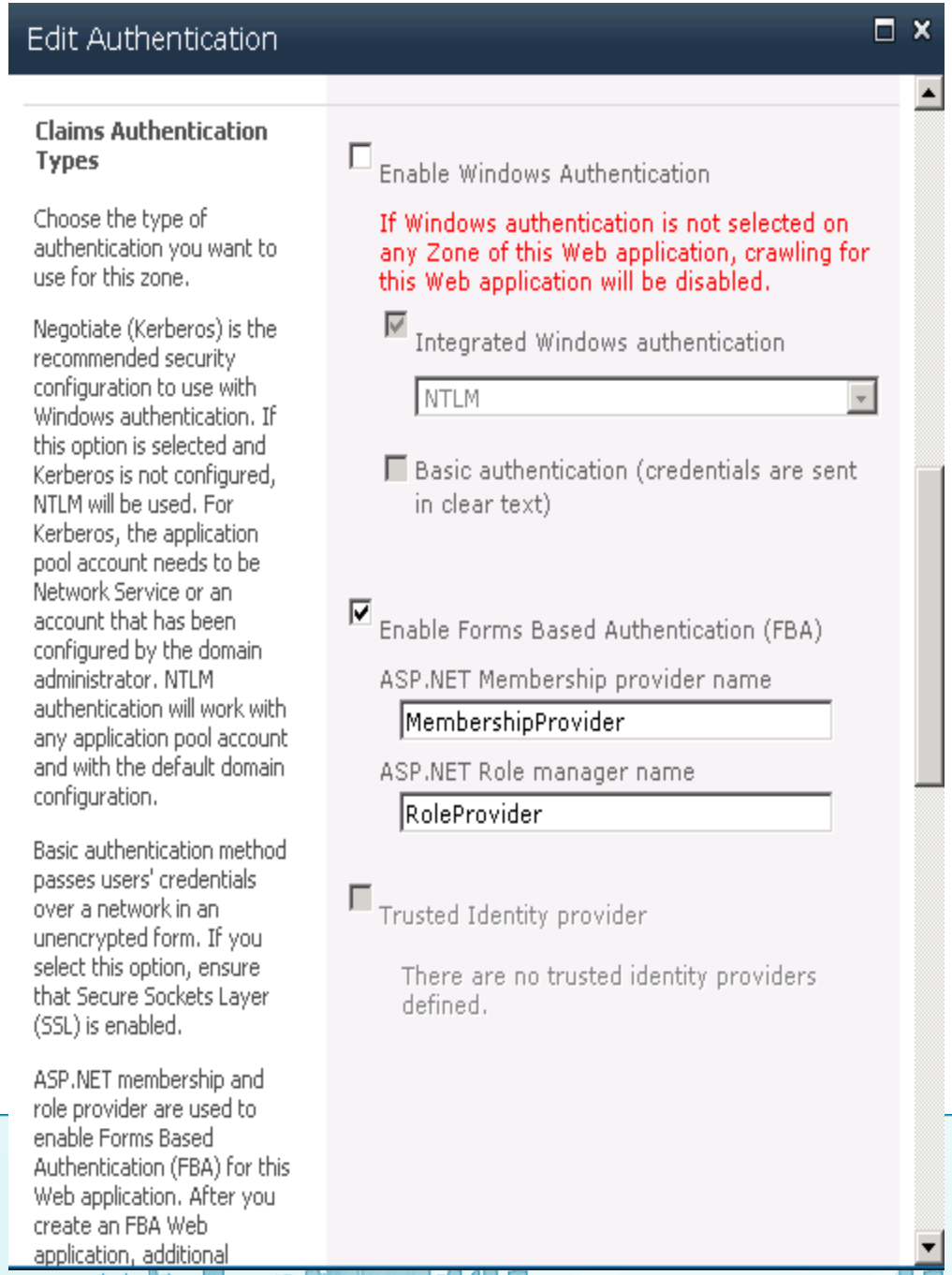
- It is critical that web.config updates are correct
- If they are wrong, SharePoint may not authenticate (without guidance as to why), or it may "blow up" entirely
- Use Envision IT's planning worksheet to ensure no steps are missed

Plan your Settings

Key information is

- Membership, role, and profile provider names
- Connection string name
- Provider definitions
- Connection string definition
- Custom login form URL

Excel Planning Spreadsheet helps you plan and calculate these


Edit Authentication
Claims Authentication Types
Choose the type of authentication you want to use for this zone.
Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.
Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.
ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA) for this Web application. After you create an FBA Web application, additional
Enable Windows Authentication
If Windows authentication is not selected on any Zone of this Web application, crawling for this Web application will be disabled.
Integrated Windows authentication
NTLM
Basic authentication (credentials are sent in clear text)
Enable Forms Based Authentication (FBA)
ASP.NET Membership provider name
MembershipProvider
ASP.NET Role manager name
RoleProvider
Trusted Identity provider
There are no trusted identity providers defined.

ADFS Federation

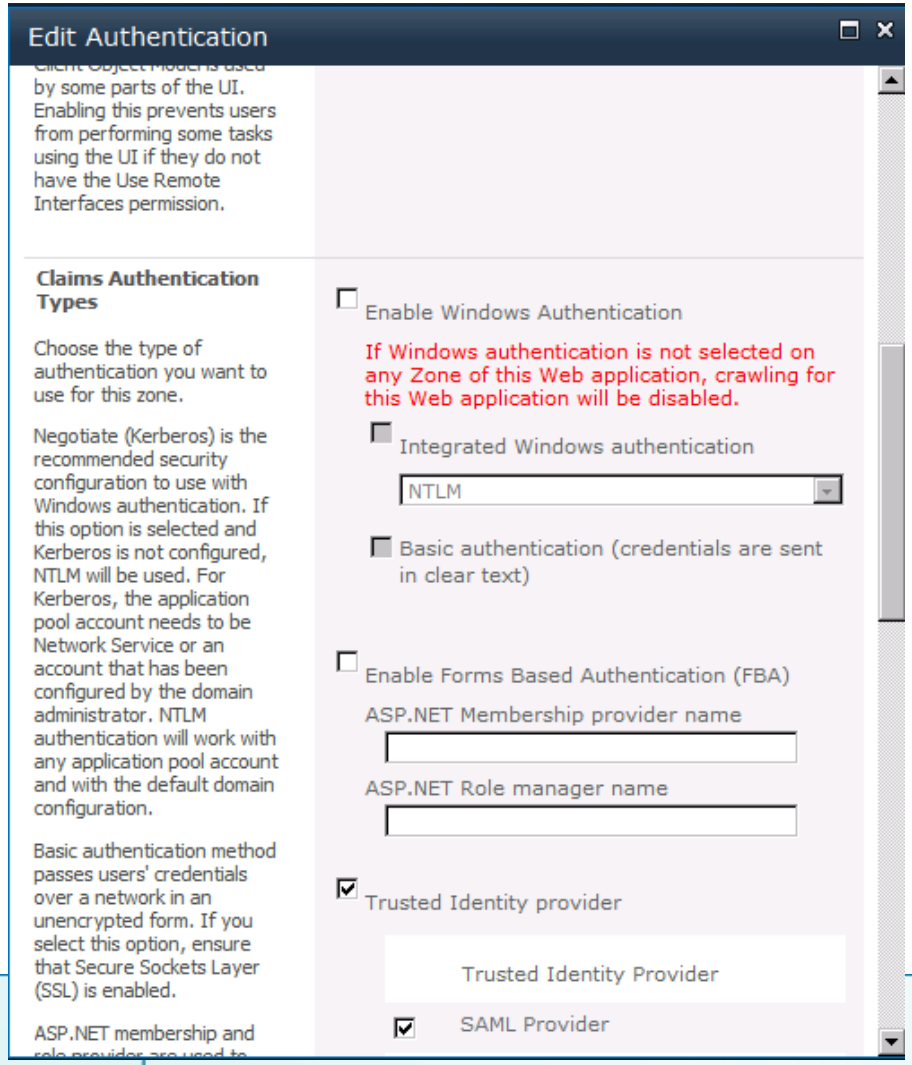
- Delegates the authentication role to a remote domain
- On the partner side you need the following
  - Domain controller running Windows Server 2008 or 2008 R2
  - ADFS 2.0 installed and wizard run
  - STS login page secured and published externally

ADFS Federation – Partner Side

- Setup the relying party trust in ADFS on the partner server
- You will need the published URL for your site, and create a realm that uniquely identifies your site with this ADFS
- Setup a claim rule to map LDAP (AD) attributes to the claim
  - At a minimum you'll likely want email address and groups mapped to the claim
- Export the certificate for use in SharePoint

ADFS Federation – SharePoint Side

- SharePoint configuration is done through PowerShell
- Import the certificate from the ADFS server
- Setup the claim's attribute mapping to SharePoint
- Create the SPTrustedIdentityTokenIssuer to tie it all together
- Now it shows up as a Trusted Identity Provider in Central Admin


Edit Authentication
by some parts of the UI. Enabling this prevents users from performing some tasks using the UI if they do not have the Use Remote Interfaces permission.
Claims Authentication Types
Choose the type of authentication you want to use for this zone.
Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.
Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.
ASP.NET membership and
Enable Windows Authentication
If Windows authentication is not selected on any Zone of this Web application, crawling for this Web application will be disabled.
Integrated Windows authentication
NTLM
Basic authentication (credentials are sent in clear text)
Enable Forms Based Authentication (FBA)
ASP.NET Membership provider name
ASP.NET Role manager name
Trusted Identity provider
Trusted Identity Provider
SAML Provider

ADFS Permission Assignments

- ADFS only allows you to perform authentications, it doesn't allow you to do lookups against the remote AD
- When assigning permissions in SharePoint, SharePoint has no way of validating whether ADFS users or roles are valid
- People picker will match anything you type in as an ADFS match; you need to know if it is valid before choosing it

Windows Live ID Integration - Test

- Configure Microsoft Services Manager
  - https://msm.live.com/
  - Use your Live ID to login
- Register and manage your site
- Retrieve the certificate and import into SharePoint
- Use PowerShell to create the SPTrustedIdentityTokenIssuer (similar to ADFS)

Windows Live ID Integration - Prod

- Submit for a compliance review
- In MSM, submit the site for Production
- Retrieve the production certificate
- Repeat the import and SPTrustedIdentityTokenIssuer process on the SharePoint server

Combining It All Together

- Part of Envision IT's Extranet User Manager is our Hydra provider and EZLogin form
  - Hydra is a single provider that can sit on top of multiple providers
  - Internal AD, DMZ AD, SQL, ADFS, and Live ID can all coexist on one site
  - Allows login by email address, which determines which provider to use
  - Internal AD users are automatically logged in

Resources

- http://blog.petercarson.ca
- Steve Peshka's Configuring SharePoint 2010 and ADFS v2 End to End
  - http://blogs.technet.com/b/speschka/archive/2010/07/30/configuring-sharepoint-2010-and-adfs-v2-end-to-end.aspx
- Hiran Salvi's Configuring Windows Live ID as Trusted Identity Provider for SharePoint 2010
  - http://blogs.msdn.com/b/hsalvi/archive/2010/09/01/configuring-windows-live-id-authentication-provider-as-federated-identity-provider-for-sharepoint-2010.aspx

Toronto SharePoint Camp

Please complete your evaluations
to enter in the prize drawing!