SharePoint Federation and Extranet Workshop
Unit 1
Federation

Presented by Peter Carson
President, Envision IT

June 18, 2014

envision IT
Leaders in SharePoint Solutions

Agenda

Morning Session

- Unit 0 – Introductions
- Unit 1 – Federation
- Unit 2 – Reference Scenarios
- Unit 3 – Customer Case Studies

Afternoon Session

- Unit 4 - Office 365
- Unit 5 – SharePoint On Premises
- Unit 6 – Open Discussion

Identity Management, Authentication, and Authorization

Identity Management

- Process for managing the entire life cycle of digital identities, including the profiles of people, systems, and services
- For our purposes we are focused just on people
- Who creates and manages identities? The Extranet owner or the external users themselves?
- Are identities part of the Extranet or external to it?

Authentication and Authorization

- *Authentication* is the mechanism whereby systems may securely identify their users
- Authentication systems provide an answers to the questions:
  - Who is the user?
  - Is the user really who he/she represents himself to be?
- *Authorization* is the mechanism by which a system determines what level of access a particular authenticated user should have
  - Is user X authorized to access resource R?

SharePoint On Premise Authentication Options

Windows Authentication

Active Directory

Windows Claims
Or
Classic Mode

Forms-Based Authentication

.NET Providers

AD

SQL

Claims

Federated Identity

Relying Party

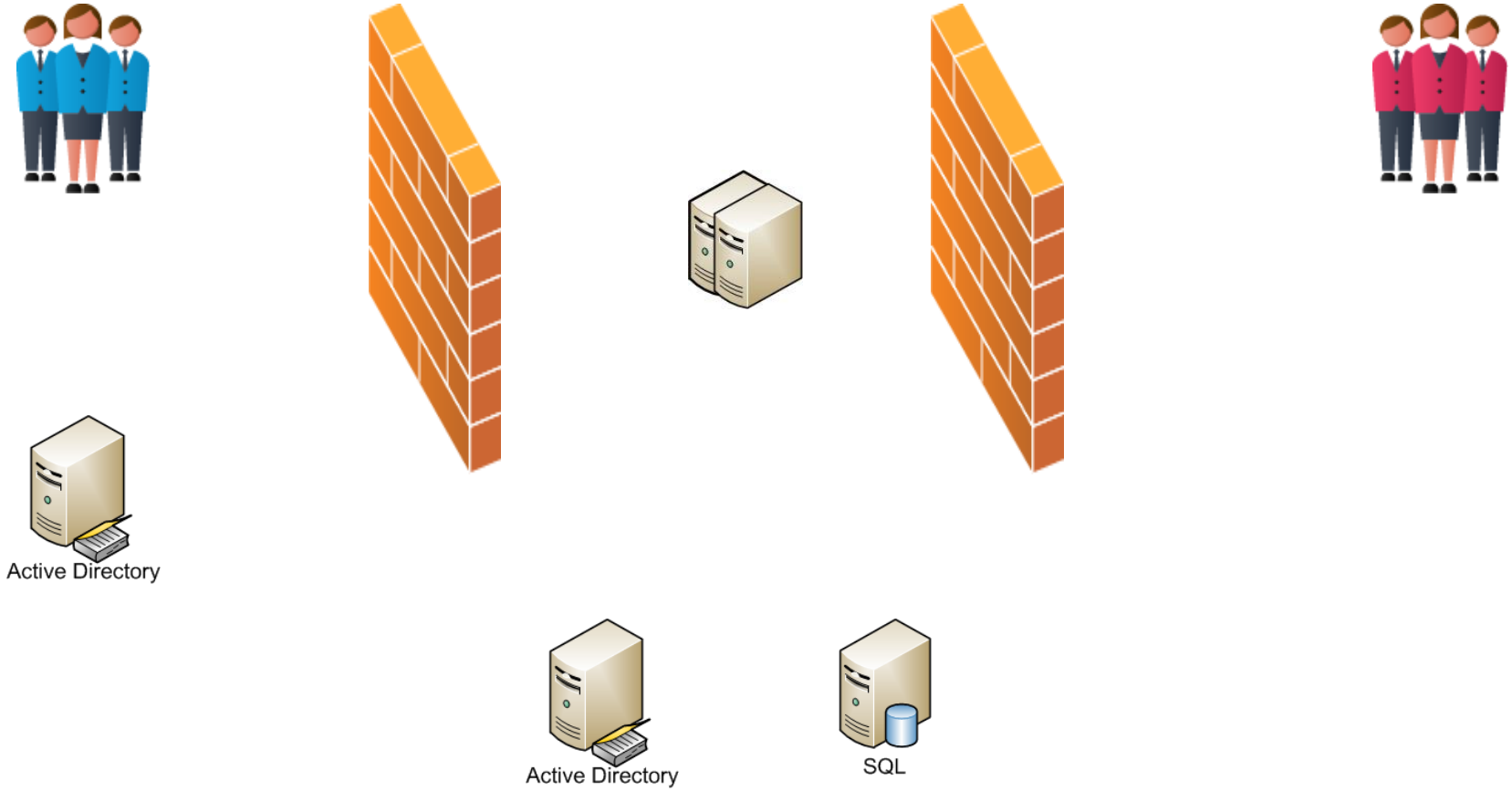
Trusted Identity Provider

AD

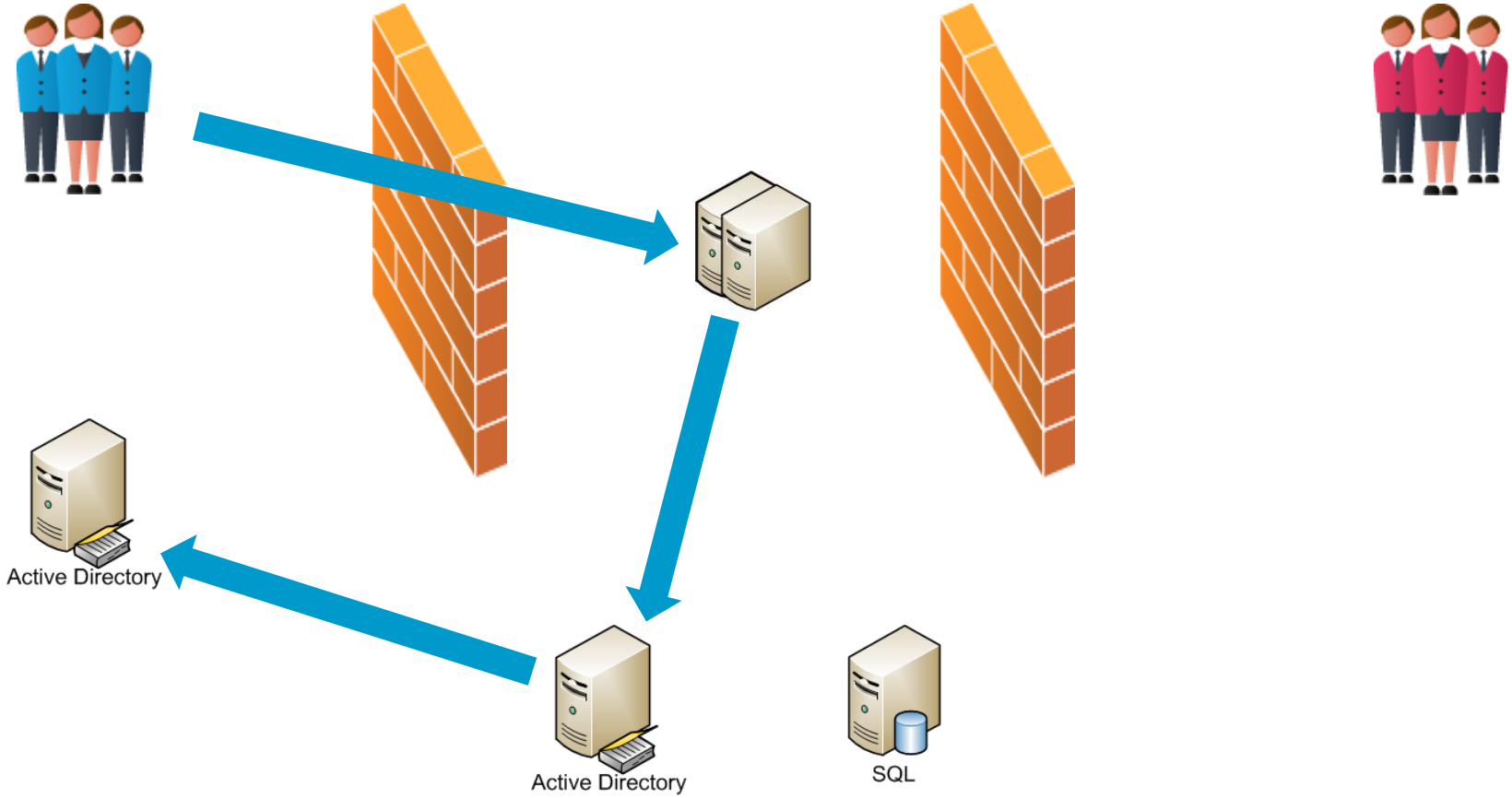
User Store

Claims

SharePoint 2010/2013 Infrastructure



One Way Trust



Internal Firewall Port Requirements

Windows Auth

- 123/UDP - W32Time
- 135/TCP - RPC Endpoint Mapper
- 464/TCP/UDP - Kerberos password change
- 49152-65535/TCP - RPC for LSA, SAM, Netlogon (*)
- 389/TCP/UDP - LDAP
- 636/TCP - LDAP SSL
- 3268/TCP - LDAP GC
- 3269/TCP - LDAP GC SSL
- 53/TCP/UDP - DNS
- 49152 -65535/TCP - FRS RPC (*)
- 88/TCP/UDP - Kerberos
- 445/TCP - SMB
- 49152-65535/TCP - DFSR RPC (*)

FBA

- LDAP 389
- LDAPS 636
- SMB 445

Federation

- No internal ports required
- Done through trusted, signed tokens passed through browser posts
- May still want to open port 443 for internal users to log in through ADFS externally

http://support.microsoft.com/kb/179442#method4

Federated Identity

- Trusted Identity Provider does the authentication
- Can be any SAML compliant provider
  - Active Directory Federation Services
  - Thinktecture Identity Server
    - www.thinktecture.com
  - Social identities
- Can be AD, SQL, or other user repository under the hood
- Relying parties (such as SharePoint) trust the SAML token and provide the authorization based off that identity
- Provides Single Sign-On to multiple systems
  - Can be any SAML claims compliant system, not just SharePoint

Trusted Identity Providers

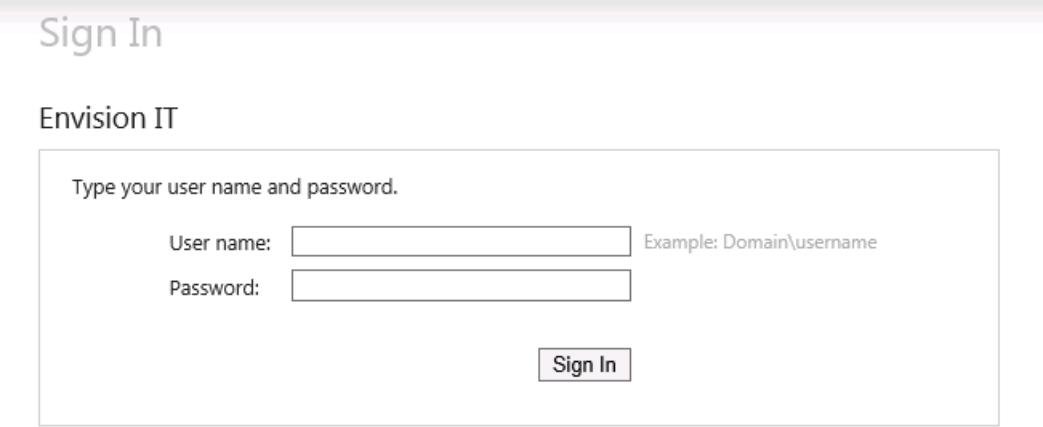
- Active Directory Federation Services (ADFS)
- Thinktecture Identity Server
- Social Identities
  - Facebook
  - Linkedin
  - Microsoft Account
  - Google+

Active Directory Federation Services

- ADFS 1.0
  - Windows Server 2003
- ADFS 1.1
  - Windows Server 2008
- ADFS 2.0
  - Minimum to be used with SharePoint
  - Free download
  - Windows Server 2008 SP2 minimum
  - ADFS Proxy is used in the DMZ to expose externally
- ADFS 2.1
  - Windows Server 2012 Role
  - ADFS Proxy is used in the DMZ to expose externally
- ADFS 3.0
  - Windows Server 2012 R2 Role
  - Web Application Proxy is used in the DMZ to expose externally

ADFS Login Form

- Internal users shouldn’t see this inside the network
- Can be branded, within limits



Thinktecture Identity Server

- Open source project available on GitHub
  - https://github.com/thinktecture/Thinktecture.IdentityServer.v2/releases
- Integrated into the Extranet User Manager V3 installer
- Customized to work with both on premises SharePoint and Office 365

EUM / Thinktecture Login Form

Envision IT
ExtranetUserManager
for SharePoint

Home

Login

Welcome to the **Envision IT Extranet User Manager** (with Thinktecture Identity Server). To enter this area of the site you must be an authenticated user.

If this is your first time visiting, please Register Here before logging in.

Email

Password

Login

Remember me? ☐

Internal Users Click Here

Forgot Password?

© 2014 Envision IT Inc. | Contact Us | Privacy Policy

Why Thinktecture over ADFS?

- Open source allows any customization
- Fully brandable (ADFS allows branding within very particular parameters)
- Login with email address instead of AD username
- Use SQL instead of AD as the underlying user repository
- Ability to incorporate the home realm discovery into the login form

Authentication Providers

BROWSE | WEB APPLICATIONS | SHARE

New | Extend | Delete | General Settings | Manage Features | Managed Paths | Service Connections | Authentication Providers | Self-Service Site Creation | Blocked File Types | User Permissions | Web Part Security | User Policy | Anonymous Policy | Permission Policy

Contribute | Manage | Security | Policy

Central Administration
- Application Management
- System Settings
- Monitoring
- Backup and Restore
- Security
- Upgrade and Migration
- General Application Settings
- Apps
- Configuration Wizards

Name	URL	Port
SharePoint - thinktecturedev.eitdev.org443	https://thinktecturedev.eitdev.org/	443
SharePoint Central Administration v4	https://thinktecturedev:19000/	19000

Edit Authentication

Claims Authentication Types

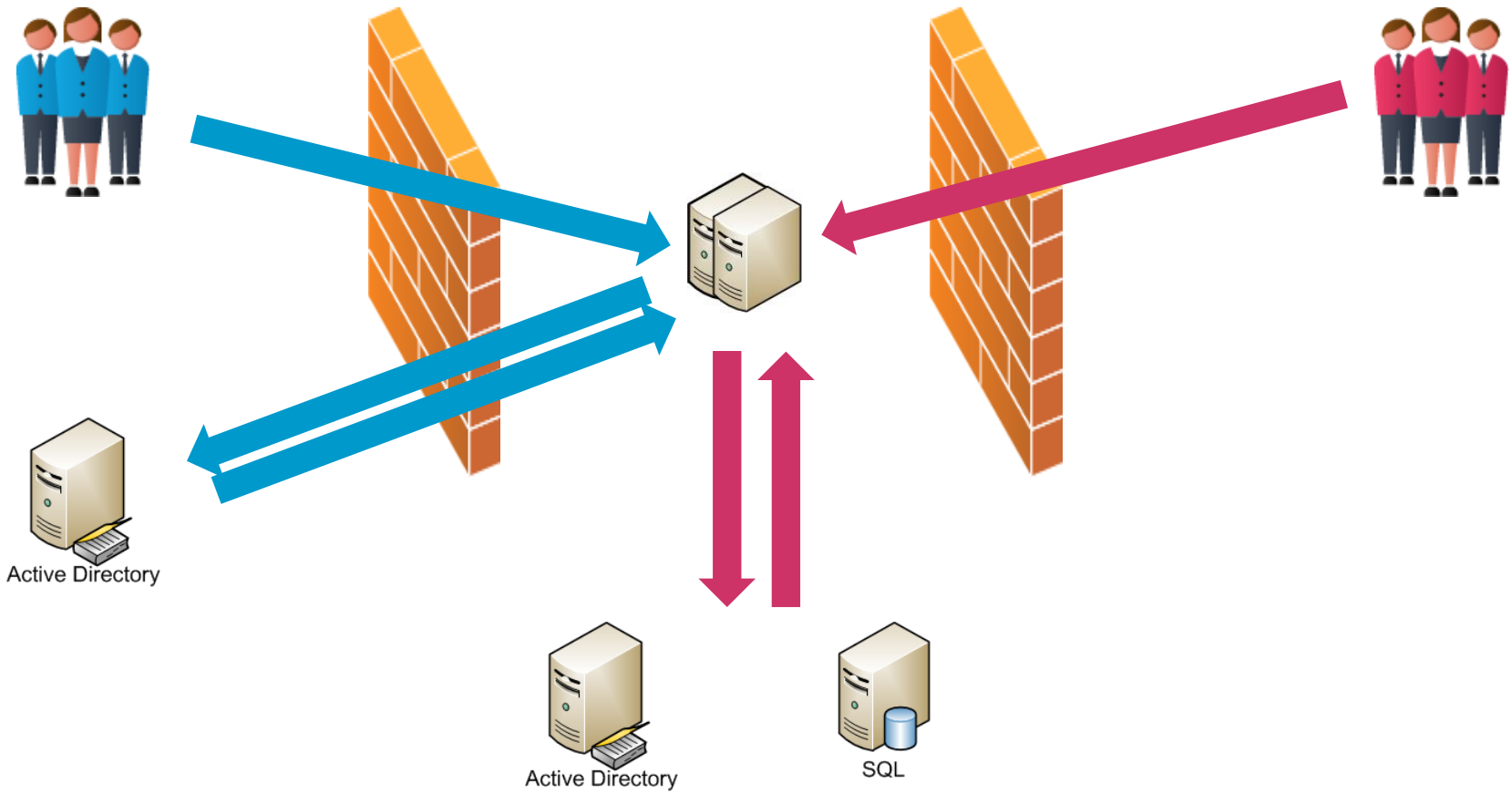
Choose the type of authentication you want to use for this zone.

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.

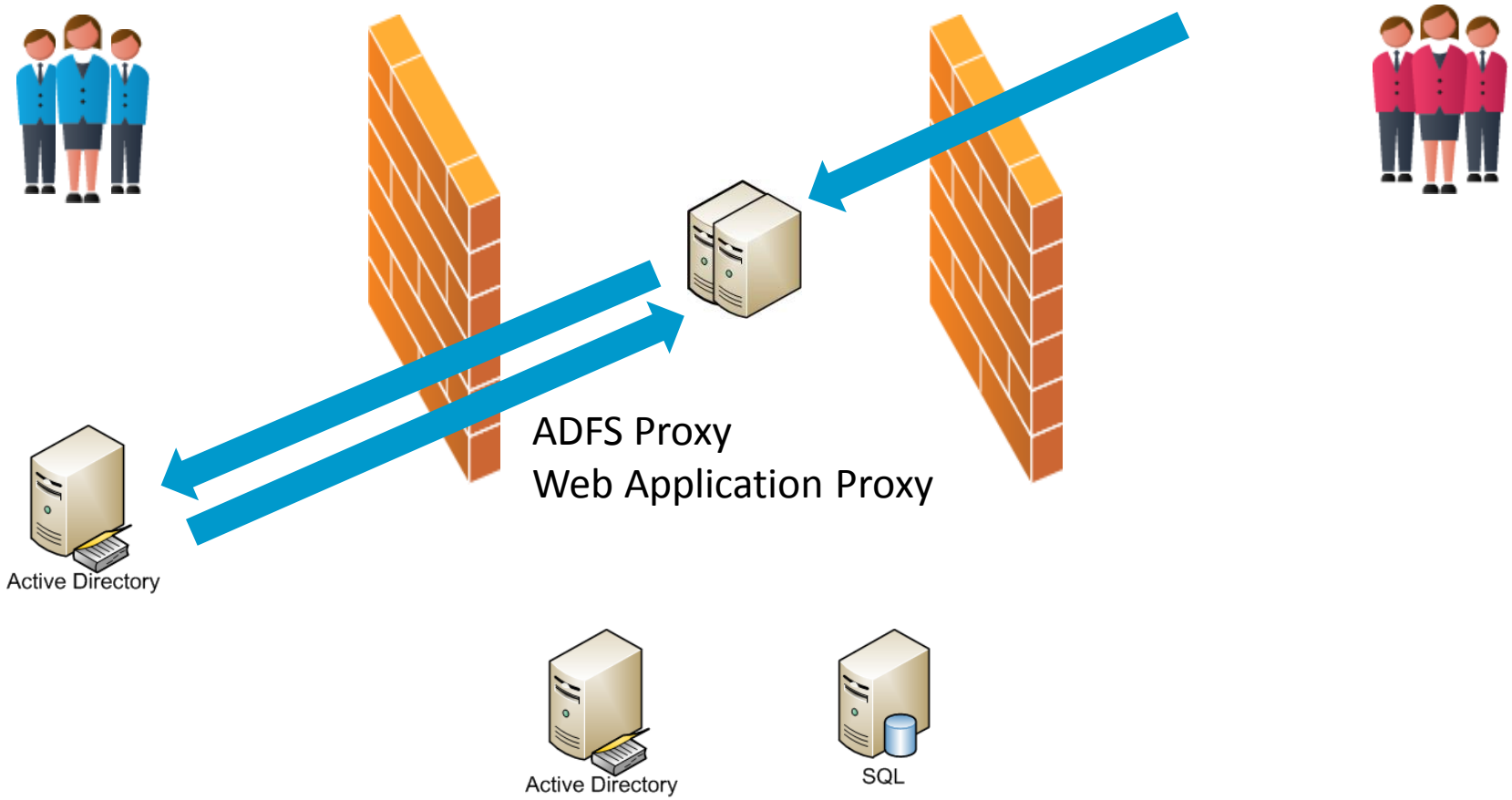
Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

- [x] Enable Windows Authentication
  - [x] 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
- [x] Trusted Identity provider
  - Trusted Identity Provider
    - [x] Thinktecture IP-STS

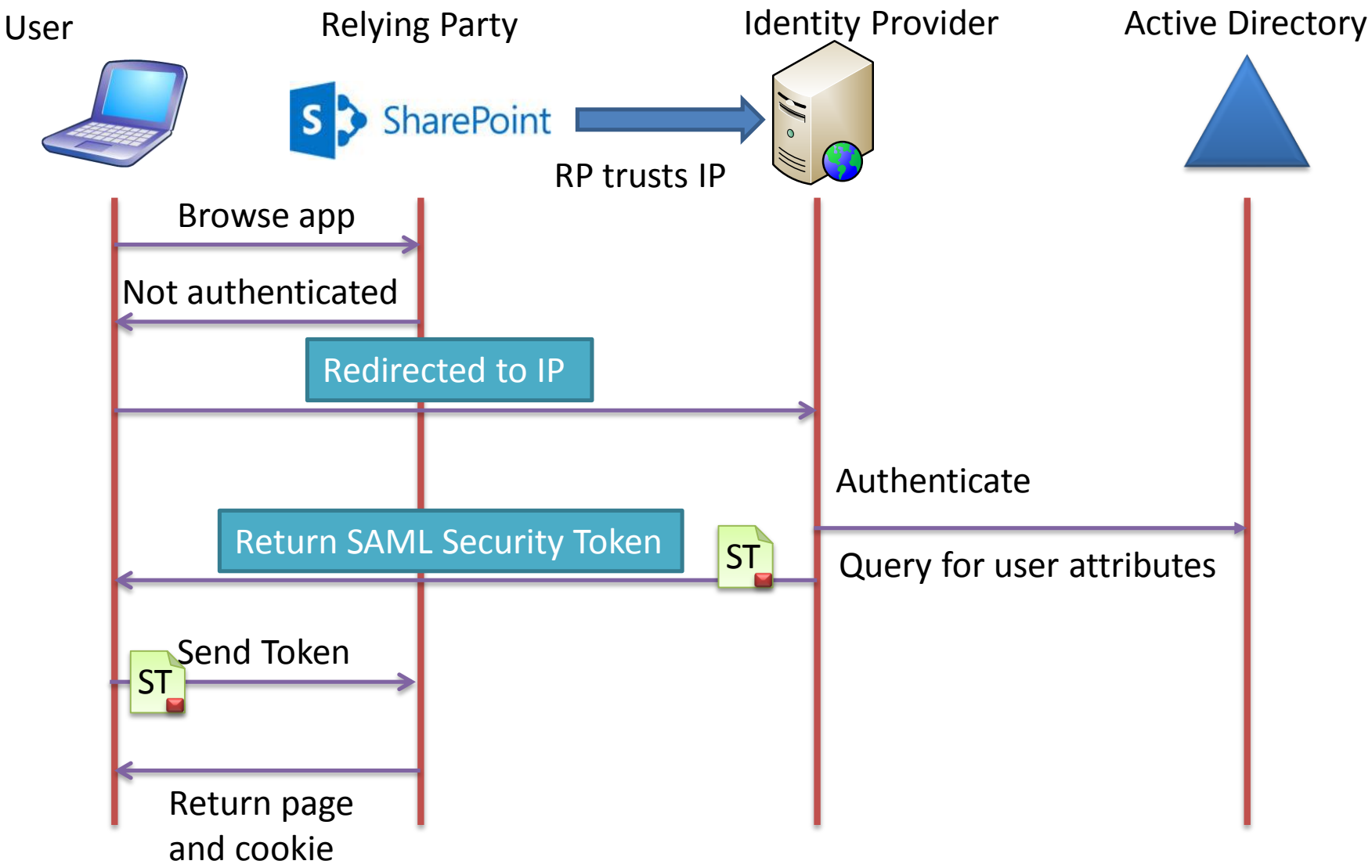
Federation



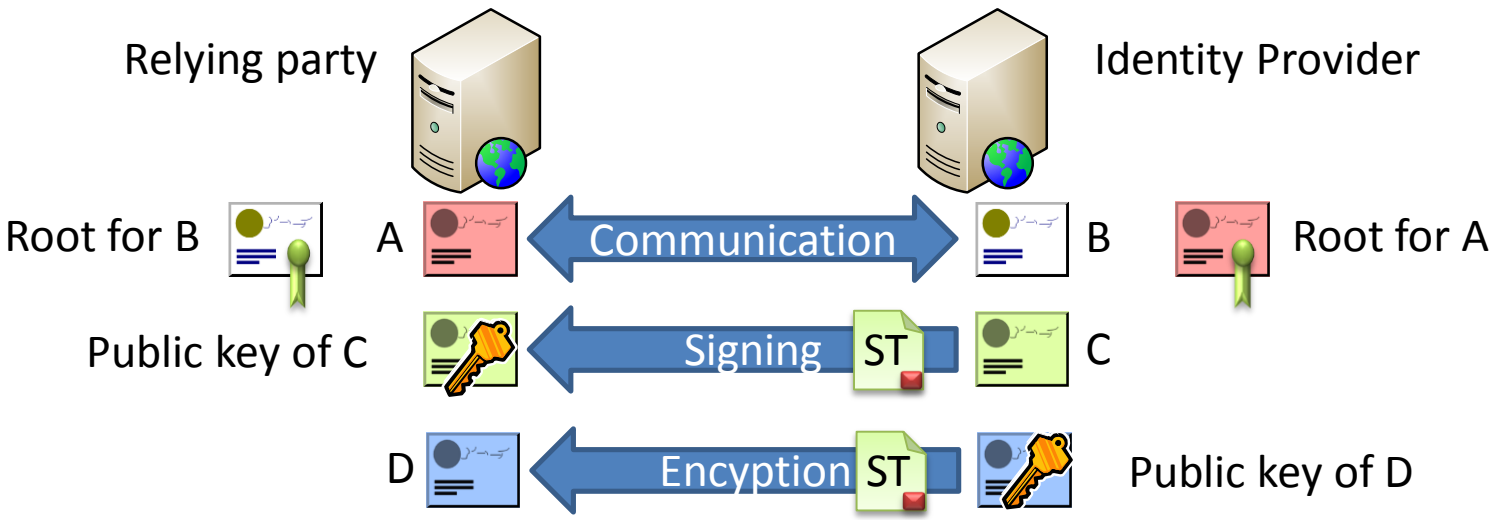
ADFS Externally



Authentication Process



Certificates



- PKI SSL encryption is used for communication
- Token can be self-signed by the Identity Provider
- Token can also be encrypted with a self-signed certificate from the Identity Provider

Office 365 Authentication Options

Cloud Identity

Windows Azure Active Directory

No Integration

Directory and Password Synchronization

Windows Azure Active Directory

DirSync and Password Sync

On Premise Identity

Integration with no federation

Federated Identity

Windows Azure Active Directory

Federation

User Sync

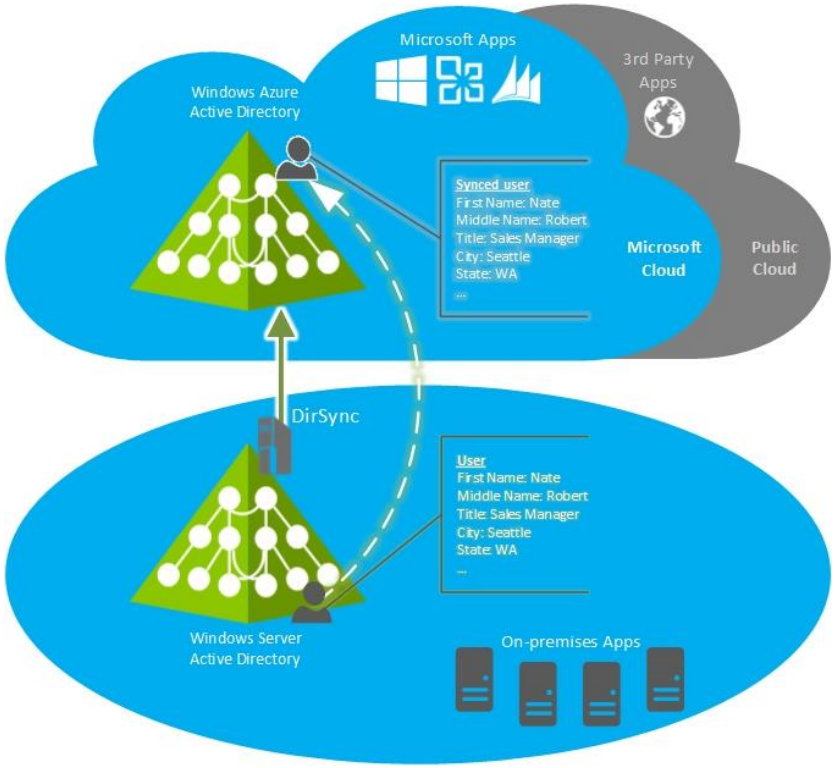
On Premise Identity

Single federated identity and credentials

Windows Azure Active Directory

- All Office 365 users have a WAAD shadow account
- DirSync can create WAAD accounts for all your AD users
  - Password Sync can also sync your passwords
  - Doesn't provide Single sign-On, but does allow users to use the same password on premise and in the cloud
  - Syncs a hash of the password, rather than the password itself
- PowerShell or Graph API (REST interface) can also be used to manage WAAD

DirSync Process



http://technet.microsoft.com/en-us/library/dn441212.aspx

Demo Scenario

- Sample site at https://productdemo13.envisionit.com
- SharePoint 2013 on premises
- ADFS for internal users
- External users
  - In a separate AD
  - Authenticating through Thinktecture Identity Server
  - Managed with the Envision IT Extranet User Manager

Single Sign-On

- https://productdemo13eum.envisionit.com
  - Extranet User Manager
  - Installed in its own IIS site outside of SharePoint
- https://productdemo13sample.envisionit.com
  - Sample ASP.NET 4.5 Visual Studio application
  - Displays the claim information for the logged in user