SharePoint Federation and Extranet Workshop Unit 2 Reference Scenarios

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

Public Web Sites and Extranets on SharePoint

- Public web sites are pure anonymous sites
- Extranets are sites that allow external users to authenticate to consume or contribute content securely
- These can be combined in a single site
- SharePoint is ideal for all of the above

Extranet Business Goals

- Reduce supply chain inefficiencies
- Interact with your loyal customer base
- Extend customer self service strategies
- Share business resources with partners
- Extend remote employee access

Extranet Scenarios

- Collaboration or Publishing Portal
- Internet Web Site Members Only Area
- Board of Directors' Portal

Collaboration or Publishing Portal

- Team sites for collaboration
- Publishing sites for private web content publishing

Internet Web Site Members Only Area

- Public web site with a private members area
- Forms-based authentication typically used to provide a rich login experience
- Self-registration with approvals typically provided

Board of Directors Portal

- Corporate or public sector board of directors portal
- Small set of users that are typically already part of the internal corporate domain
- SSL publishing of portal externally

SharePoint 2013 Licensing Changes

- The SharePoint For Internet sites (FIS) license is no longer needed for public web sites or Extranets
- This can save significant licensing dollars
- This applies to on-premise, Azure, or third-party hosting options

SharePoint Licensing– 2010 vs 2013

2010	Intranet	Extranet	Internet Sites
Internal Users	SharePoint Server + CAL	SharePoint Server + CAL Or SharePoint for Internet Sites (FIS)	SharePoint for Internet Sites (FIS)
External Users*	N/A		

2013	Intranet	Extranet	Internet Sites
Internal Users	SharePoint Server + CAL	SharePoint Server + CAL	SharePoint Server
External Users*	N/A	SharePoint Server	

Note*: External users means users that are not either your or your affiliates' employees, or your or your affiliates' onsite contractors or onsite agents

Office 2013 On Premise Web Apps

- I have internal users who want to access Office documents via Office Web Apps, what licenses do I need to be compliant?

Scenario	Internal User
Read Office documents via Office Web Apps	Free, no Office client required
Edit Office documents via Office Web Apps	Requires Office 2013 Standard or Professional Plus

- Our company users (who are licensed for Office Client) are working with external users on projects, what licensing do those external users need to access Office documents via Office Web Apps?

Scenario	External User*
Read Office documents via Office Web Apps	Free, no Office client required
Edit Office documents via Office Web Apps	Free, no Office client required

***External Users:** defined as users that are not either your or your affiliates' employees, or your or your affiliates' onsite contractors or onsite agents.

Hosting Options

Site Type	On-Premise	Office 365	Azure	Third-Party
Public Web Site	Yes	Very simple	Yes	Yes
Extranet	Yes	Yes	Yes	Yes
Combined	Yes	No	Yes	Yes

Office 365 Notes

- Only very simple public web sites can be hosted in Office 365
- Microsoft currently provides up to 10,000 external clients with Windows Live ID access to an Extranet with no additional subscription costs
- A combined public web site and Extranet in a single site cannot be delivered in Office 365

Office 365 Licensing

- All internal users need a monthly paid subscription
  - Could be just for SharePoint Online
  - Can also be part of an Office 365 subscription that can include Exchange, Lync, Yammer, and Office Desktop as well
- Up to 10,000 external users can also access SharePoint for free
  - Must authenticate using a Microsoft account or Office 365 account
  - Can request additional users for free
- External users coming in through Extranet User Manager also need paid subscriptions

Terminology

Terminology

Term	Definition
Internal Network	The private network that all of the internal desktops, laptops, and most servers are connected to. This is a highly trusted, private network
DMZ	Demilitarized Zone This is a less secure server area for resources that are going to be accessed from the Internet, such as an Extranet site
AD	Active Directory The Microsoft directory service for both users and computers in a Windows Server network
One Way Trust	One AD trusts users and computers from another AD Typically a DMZ AD would trust the Internal AD, but not the other way around

Terminology

Term	Definition
IE	Internet Explorer
Windows Authentication	Logging into a resource using your Windows credentials (username and password you type in to log into your Windows PC) This often happens automatically in IE when properly configured
FBA	Forms Based Authentication Logging in on an HTML login page. Typically this is done with a username and password, but may be other credentials such as email and password
Multi-Factor Authentication	Using additional factors for authentication, such as a hardware token, soft-token on a mobile device, text message, or phone call token

Terminology

Term	Definition
Reverse Proxy	Takes requests from the Internet and forwards them to internal servers
Trusted Identity Provider	The identity provider trusted by the relying party
Relying Party	The system being accessed, such as SharePoint. It relies on the Trusted Identity Provider to authenticate the user requesting access
SAML	Security Asset Markup Language specification
SAML Token	Token that is passed between the TIP and RP
JSON	JavaScript Object Notation format used to pass data to/from JavaScript

Terminology

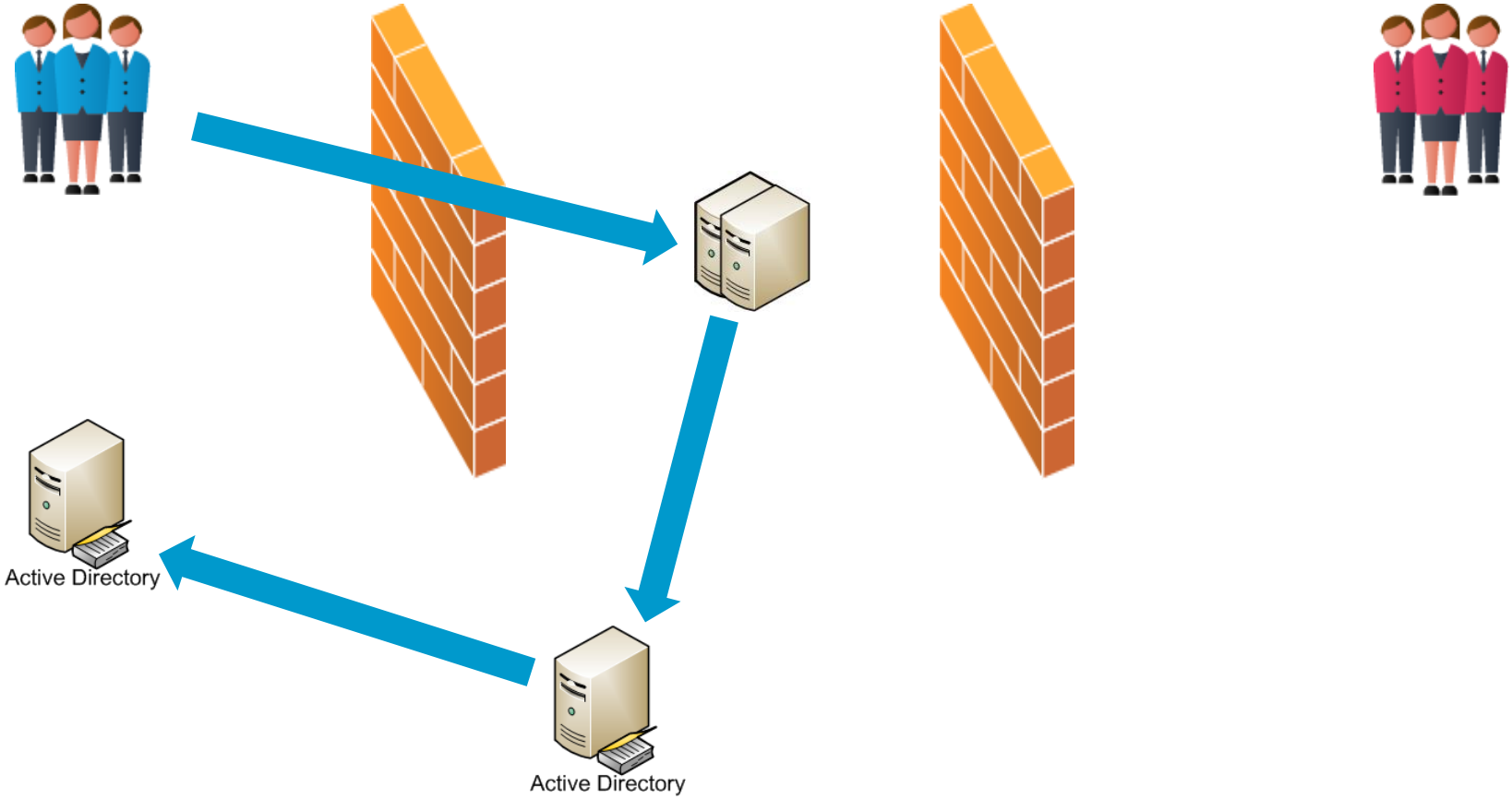
Term	Definition
JWT	JSON Web Token. Similar to the SAML Token, used to pass security credentials between JavaScript and web services
Claim	A property in the SAML token, such as the email address or username of the user
Thinktecture Identity Server	Open source Identity Provider
Extranet Identity Server	EUM implementation of the Thinktecture Identity Server

Architectures

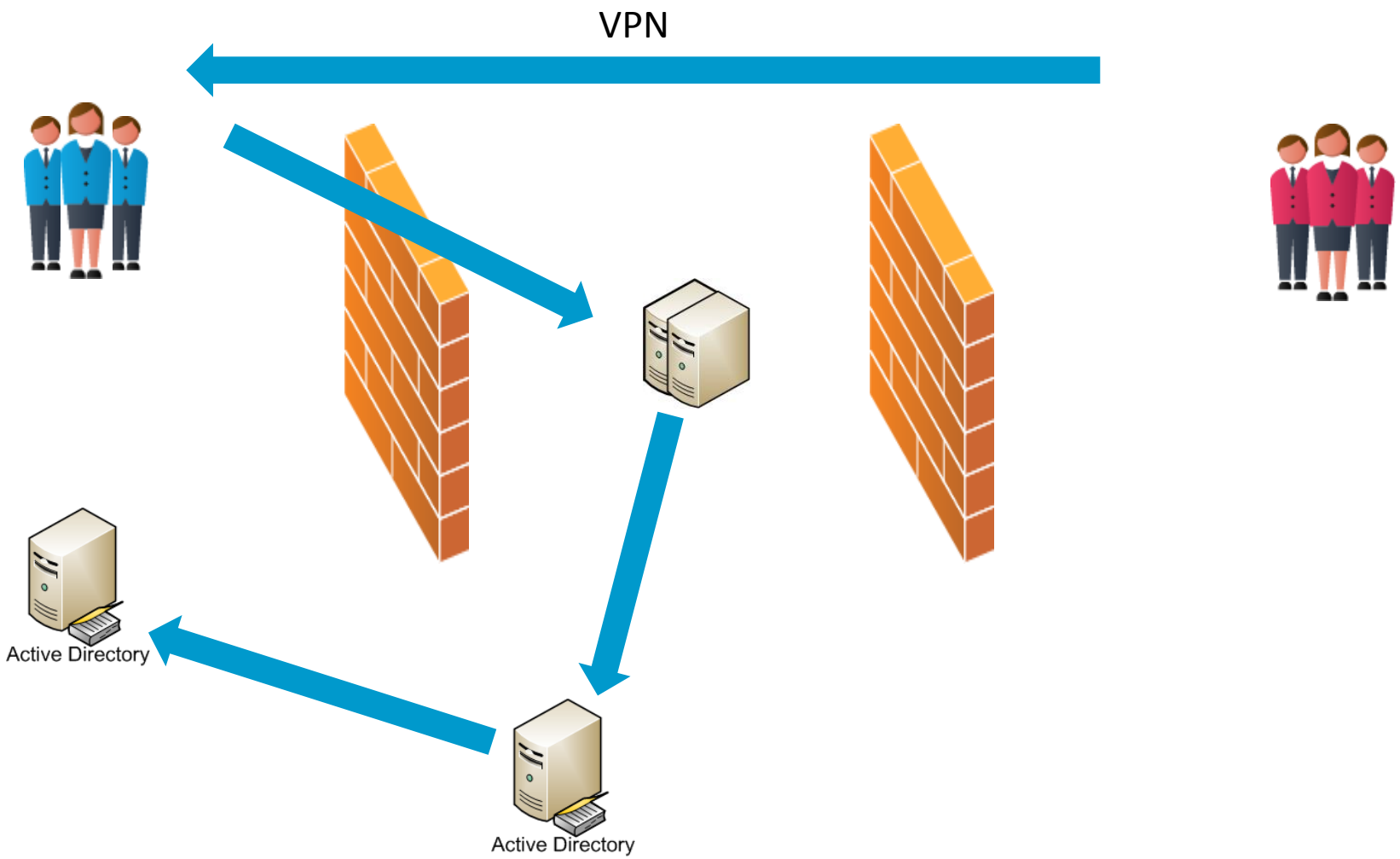
Windows Auth – One Way Trust

- Internal users log in with their Windows credentials
- Should be passed through automatically in IE
  - No login form
- DMZ trusts the internal AD

One Way Trust - Internal



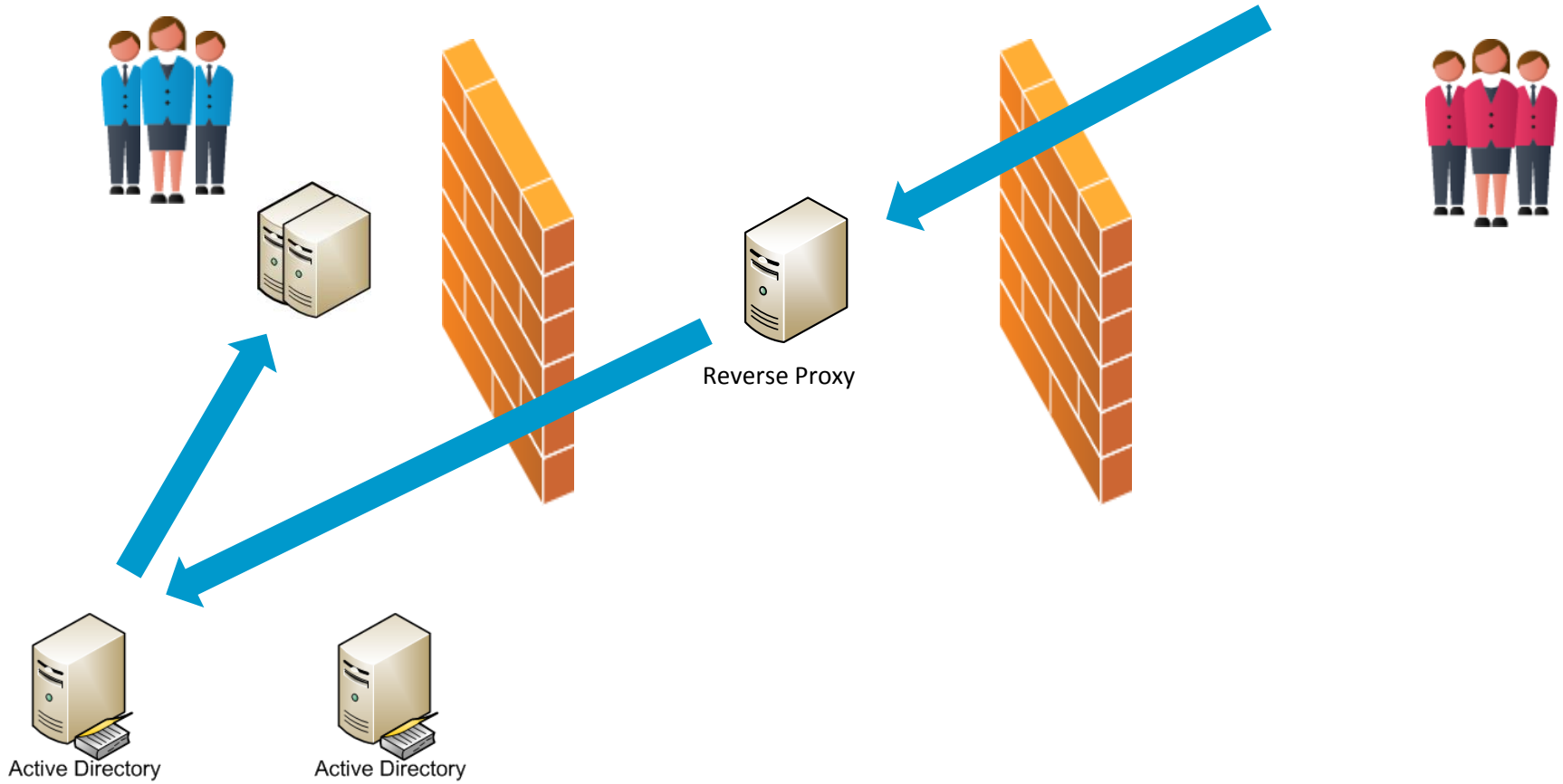
One Way Trust – VPN External



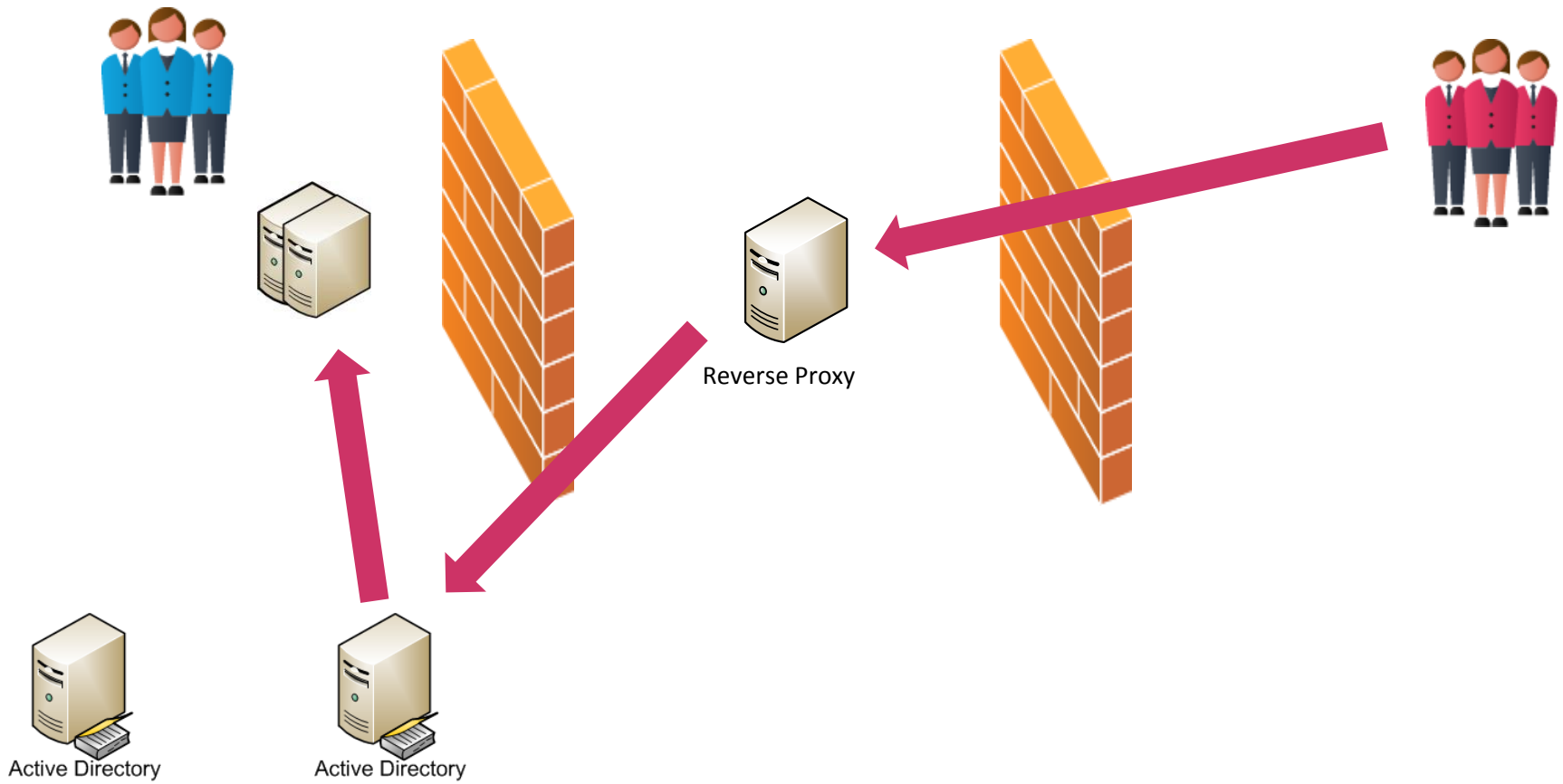
Windows Auth – Reverse Proxy

- Both internal and external users can log in externally through the reverse proxy
- The reverse proxy can present a customized HTML login form for the user
- From the internal server's perspective, the user is logged in with Windows credentials

Reverse Proxy Internal User



Reverse Proxy External User



Sample Reverse Proxies

- Microsoft Forefront Threat Management Gateway (TMG)
  - Discontinued
- Microsoft Forefront Unified Access Gateway (UAG)
  - Discontinued
- Microsoft Web Application Proxy
  - Part of Windows Server 2012 R2
- Citrix NetScaler
- F5 Big-IP

Example Sites

- Forefront TMG
  - https://secure.envisionit.com
- Forefront UAG
  - https://secure.publichealthontario.ca
  - https://portal.calgaryunitedway.org

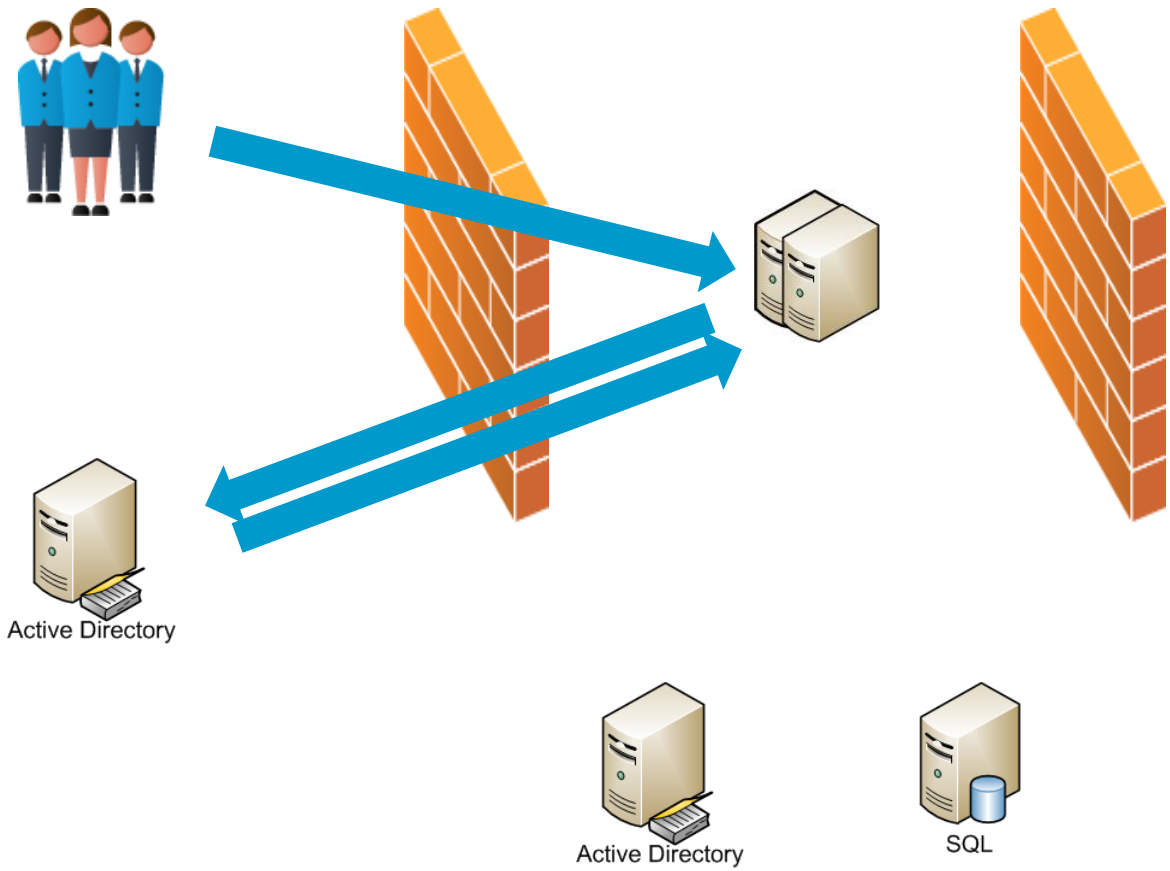
Forms Based Authentication

- HTML login form
- EZ-Login form that is part of EUM provides this
- Deeply wired into SharePoint
- Not easy to use for single sign-on for other systems

Internal Users - ADFS

- Internal users connect with their AD credentials through ADFS
- No trusts required between internal and DMZ AD
- No ports open from internal network to DMZ

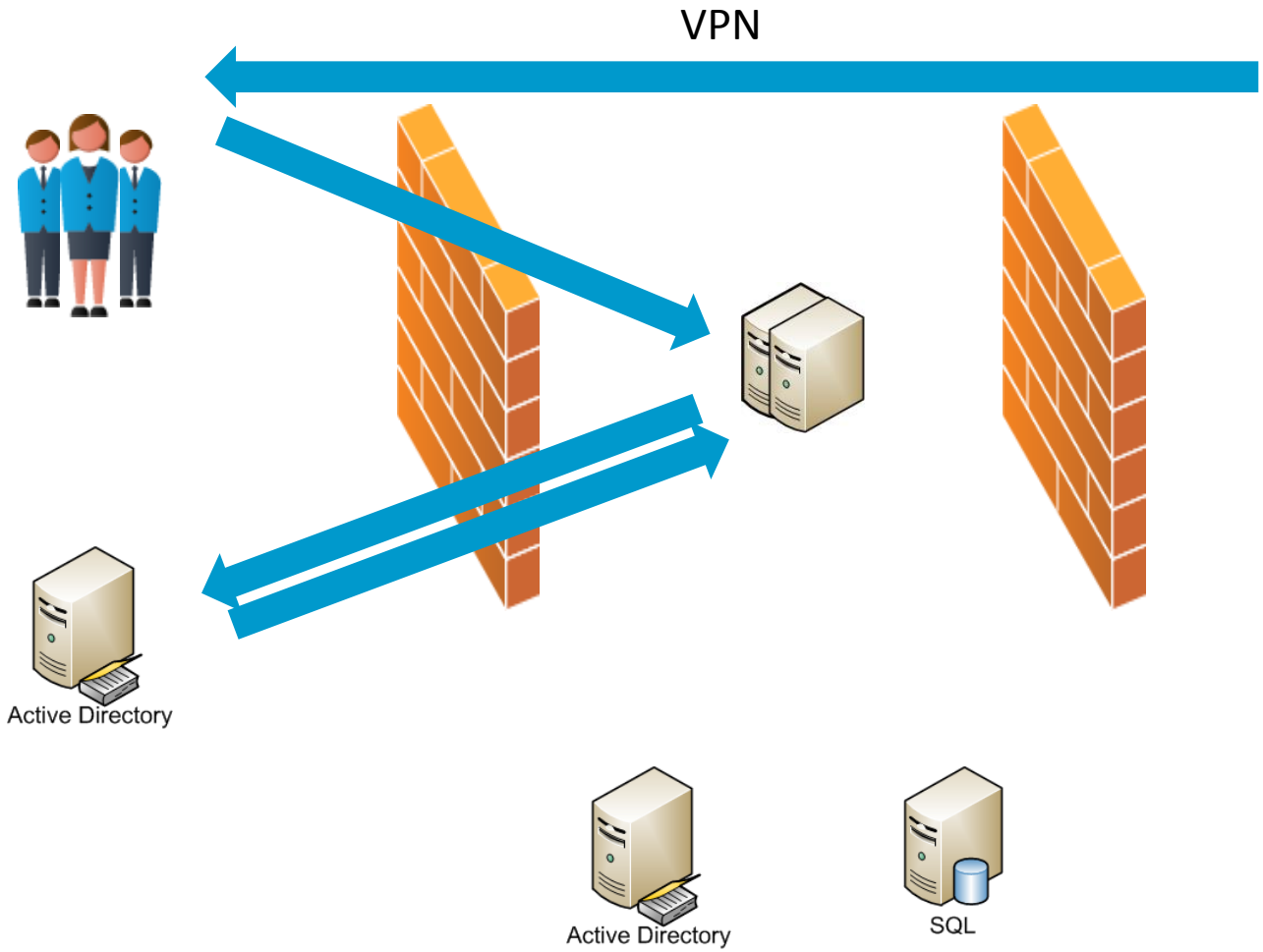
ADFS Federation - Internal



Internal Users – ADFS with VPN

- No external publishing of internal ADFS externally
- Internal users working outside the internal network must VPN first to connect
- Typically the same requirement for all corporate resources

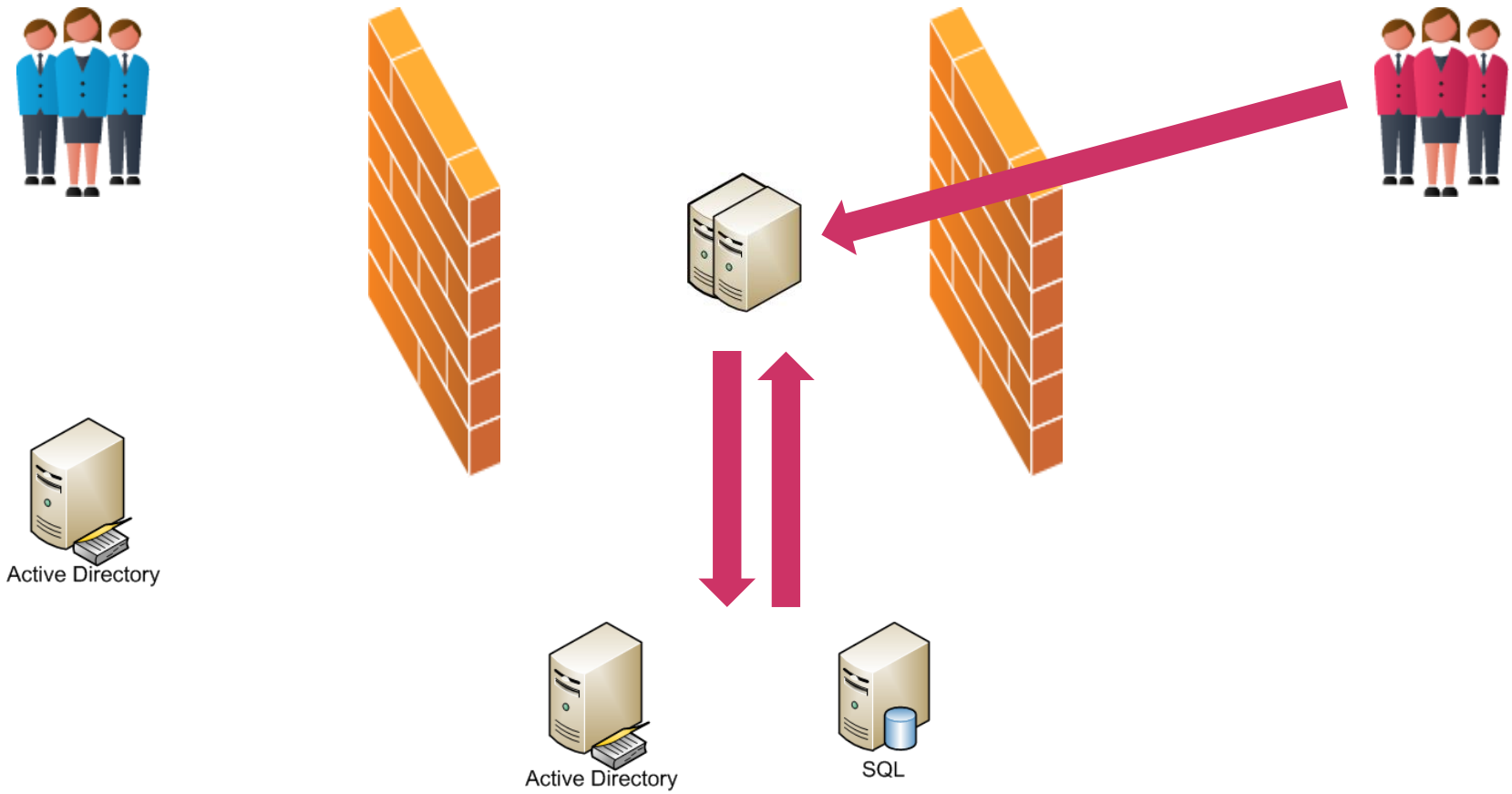
ADFS Federation – Internal with VPN



External Users - Federation

- External users use ADFS, Thinktecture, or another Trusted Identity Provider to access the Relying Party, such as SharePoint

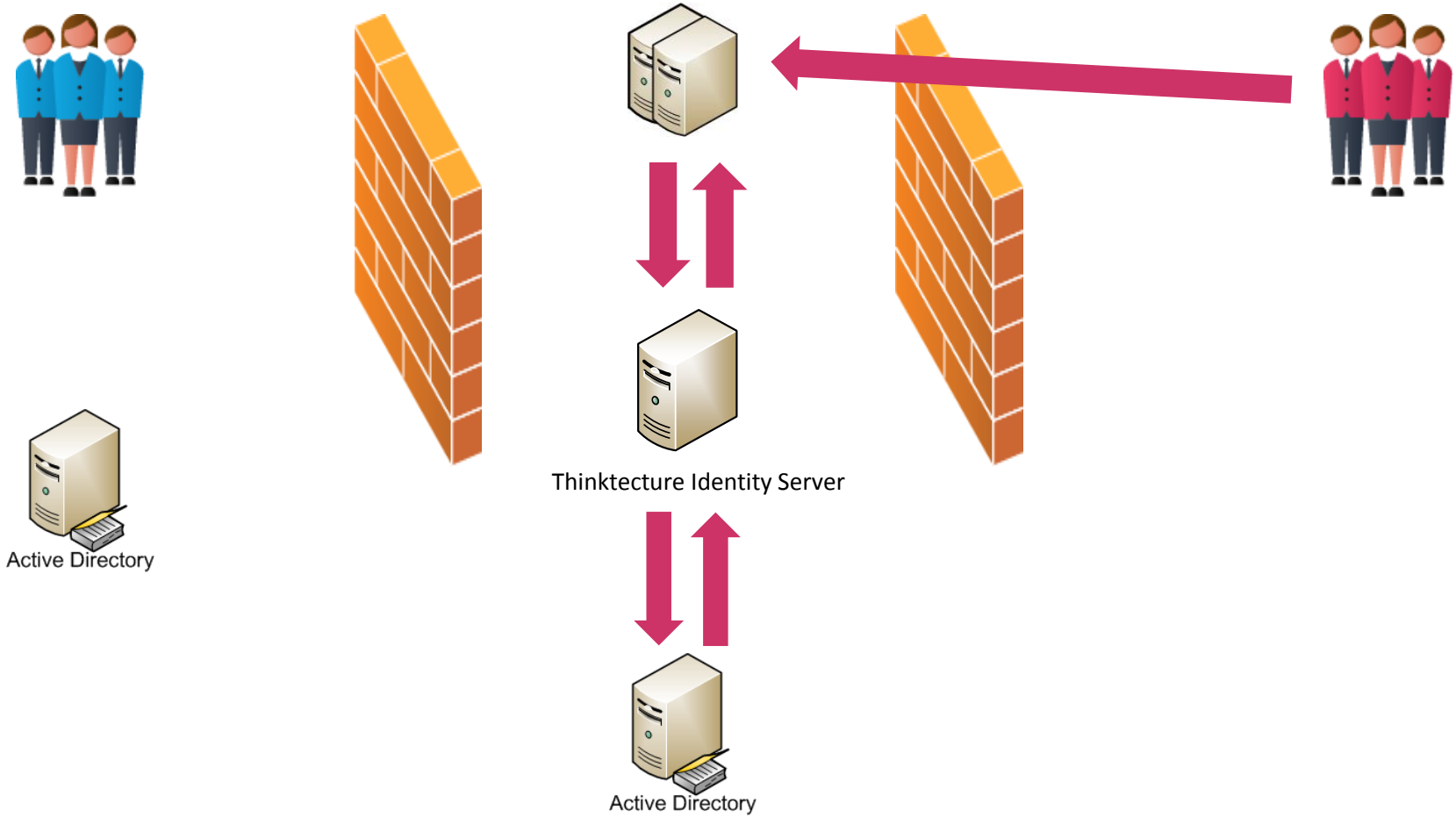
Federation – External Users



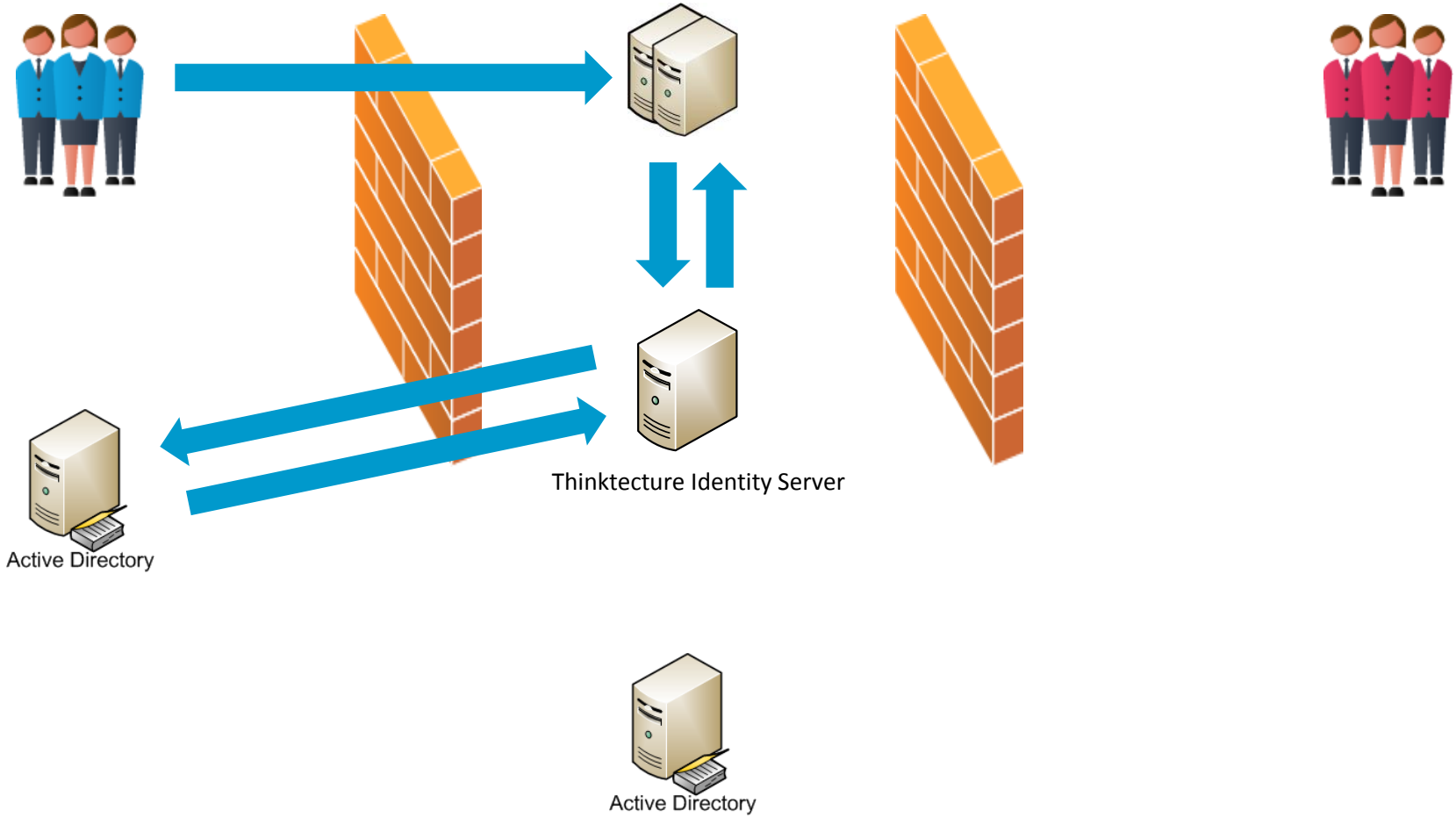
ADFS Behind Thinktecture

- All Relying Parties use Thinktecture Identity Server as their Trusted Identity Provider
- TIS is a Relying Party for ADFS for internal users
- Allows more sophisticated login and home realm discovery to improve the user experience

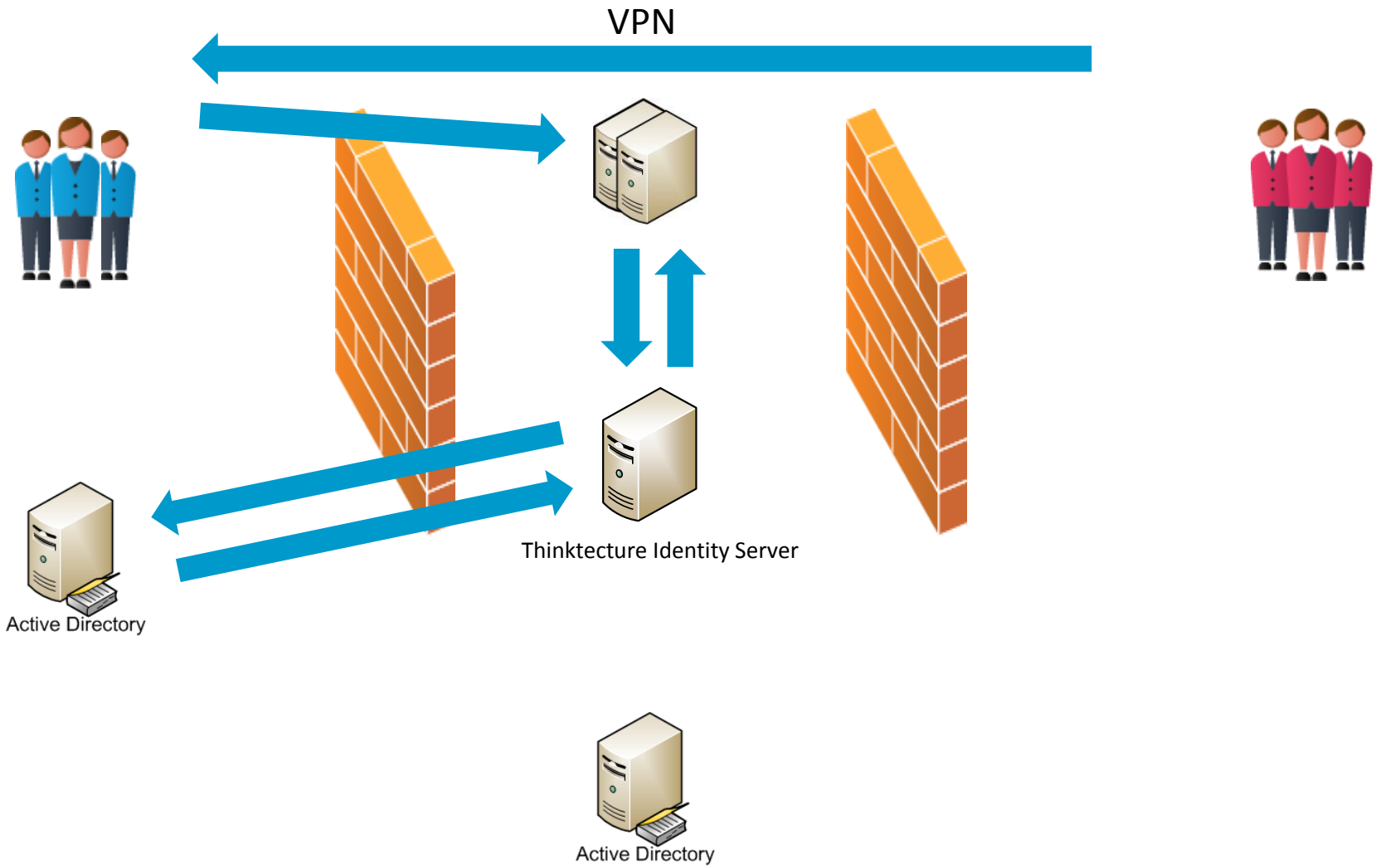
Federation – External Users



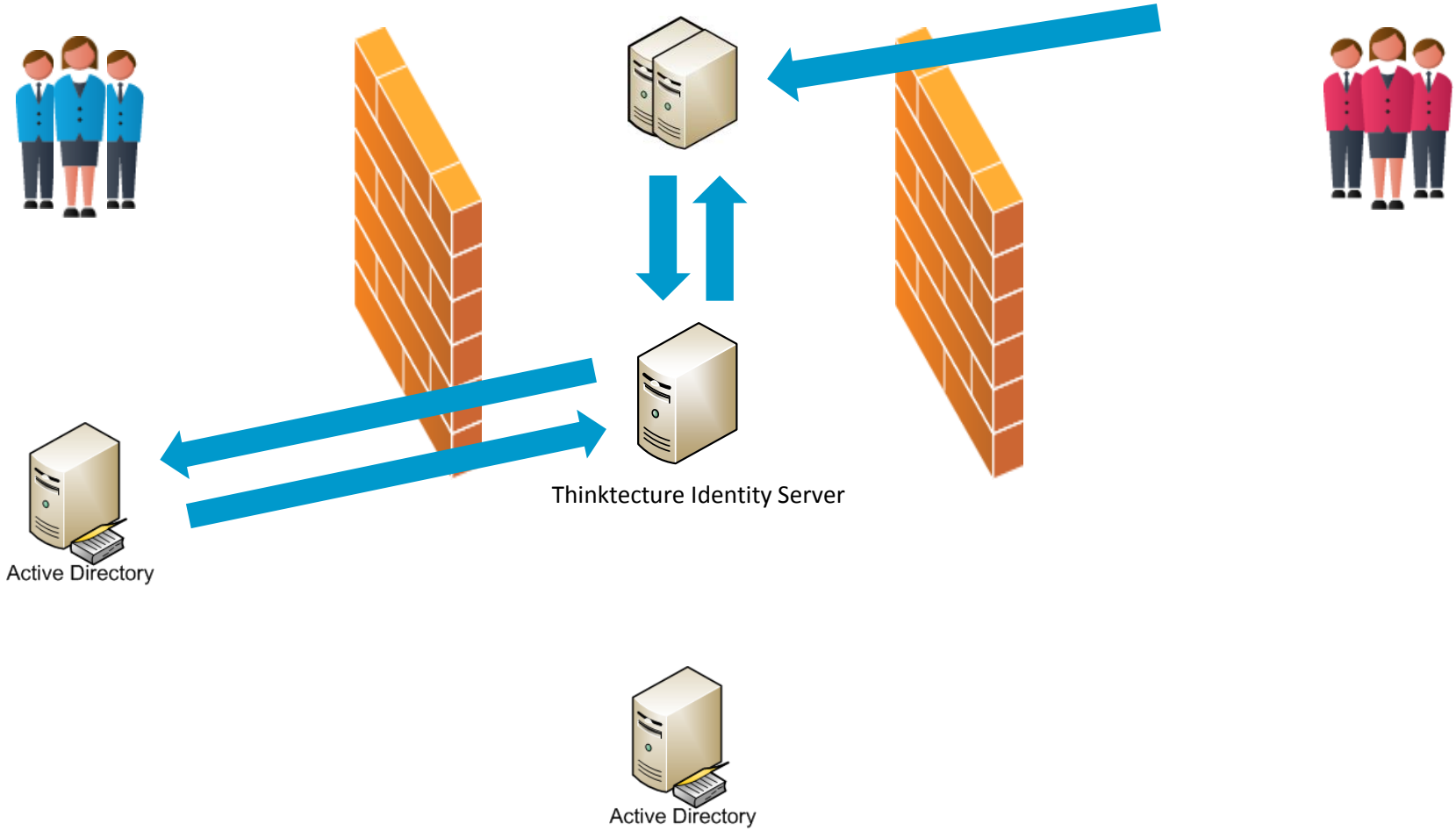
Federation – Internal Users



Federation – Internal Users VPN



Federation – Internal Users External



Summary

- Internal Users
  - Windows Auth
  - ADFS
  - ADFS and Thinktecture
- External Users
  - FBA
  - Reverse Proxy
  - Federation

Windows Auth

Pros

- Simple to implement
- Automatically logs in internal users

Cons

- Requires a one-way trust to the DMZ
- Swiss cheese firewall (12 ports opened)
- Not effective for external users

Reverse Proxy

Pros

- Provides single sign-on to any site that supports Windows Auth
- Login experience can be branded/customized (within the device's supported customizations)

Cons

- Requires an additional appliance to be purchased, installed, and configured

FBA

Pros

- Simple to install if using EUM
- EZLogin provides a very good user experience

Cons

- Complex installation
- Many changes to core SharePoint files (particularly the web app, Central Admin, and STS web.config files)
- Potential Microsoft support challenges

ADFS for Internal

Pros

- Leverages Microsoft's direction for web authentication
- No trusts and no firewall ports to open
- If SSL access externally for remote internal users, only port 443 need be opened
- Minimal configuration in SharePoint

Cons

- Requires ADFS be implemented internally

Extranet Identity Server

Pros

- Ideal user experience for both internal and external users
- Leverages Microsoft's direction for web authentication
- No trusts and no firewall ports to open
- If SSL access externally for remote internal users, only port 443 need be opened
- Minimal configuration in SharePoint
- Minimal Microsoft support challenges

Cons

- Additional product to purchase and install

Claims Augmentation

Claims Augmentation

- The provisioning of additional custom claims for the user being authenticated
- Can come from any data source
  - Line of business system
  - SQL database
- Provides additional information about the user that can be used for security or audience targeting

TMX Group

- Toronto Stock Exchange
  - Largest stock exchange in Canada, the third largest in North America and the seventh largest in the world
  - World leader in the mining and oil and gas sector
  - As of March 2014, TSX had 1515 listed companies with a combined market capitalization of CAD $2,457 billion
- TSX Venture Exchange
  - Public venture capital marketplace for emerging companies
  - As of March 2014, TSXV had 2109 listed companies with a combined market capitalization of CAD $37 billion
- Numerous other holdings, products, and services

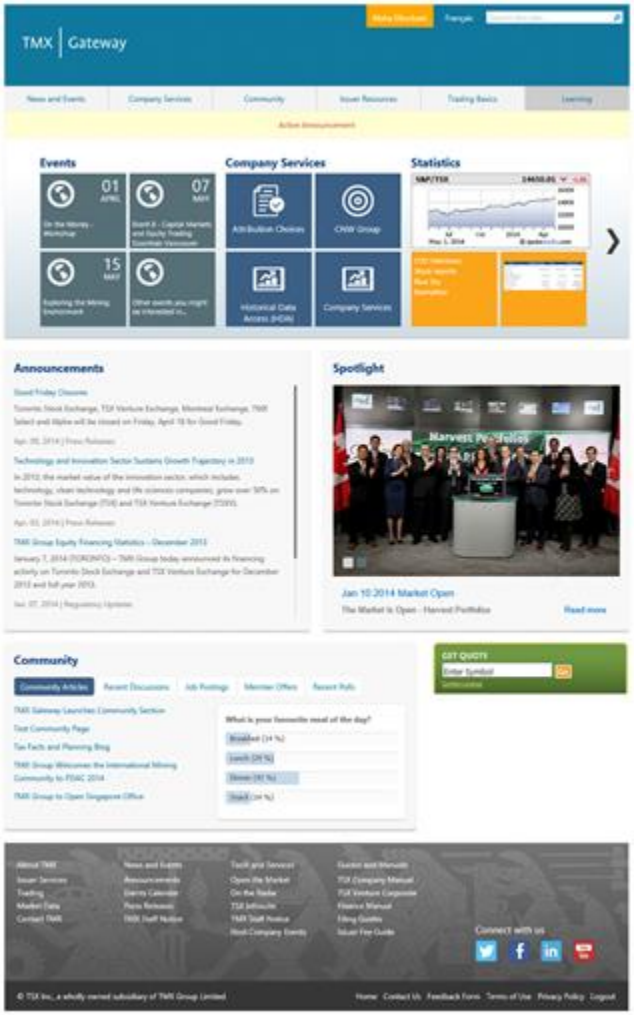
Issuer Portal

- Authenticated, targeted portal
- Multi-way conversations
- Product offerings, events, postings
- Internal and external forms
- English and French
- Agile project methodology
- Launch target of Q4 2014

"I Envision the issuer portal becoming the main point of contact with TMX, making it easier to do business with us, building engagement and stickiness with our clients, and creating a community for our staff, clients, and third parties."

Based on conversations with Loui Anastasopoulos and the TMX team

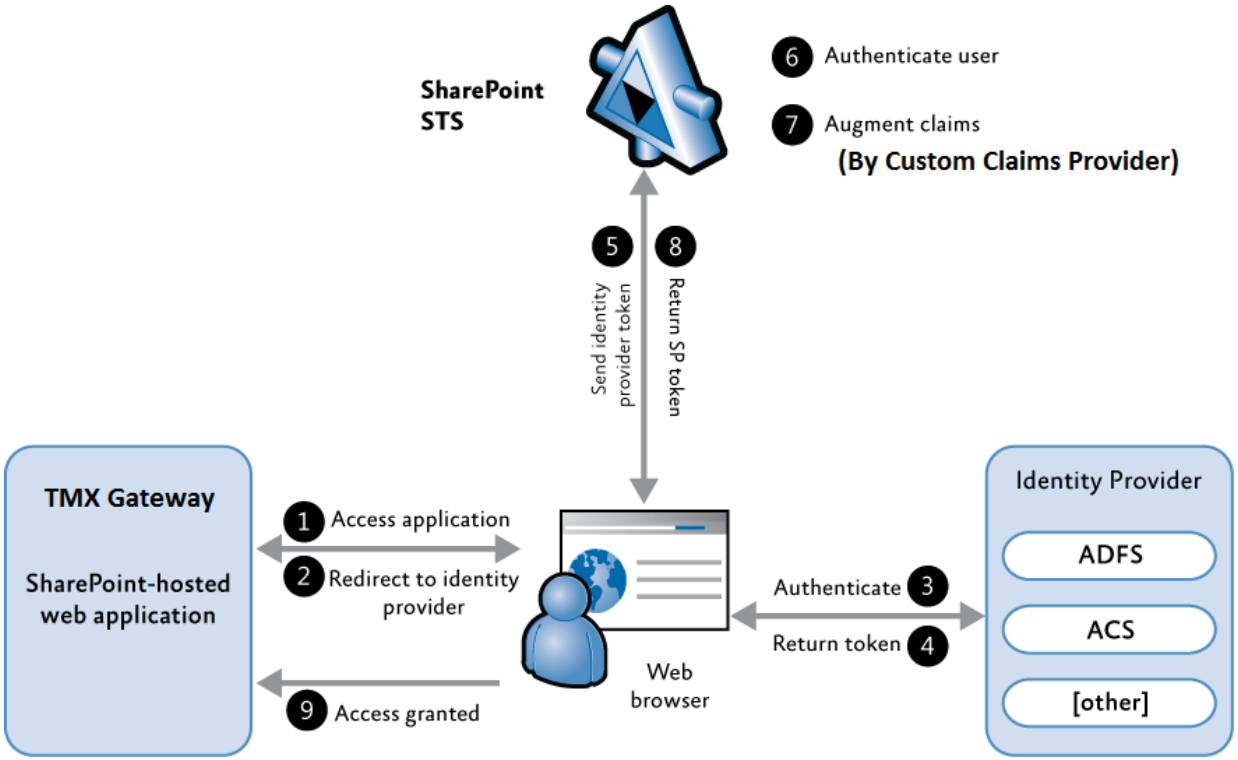
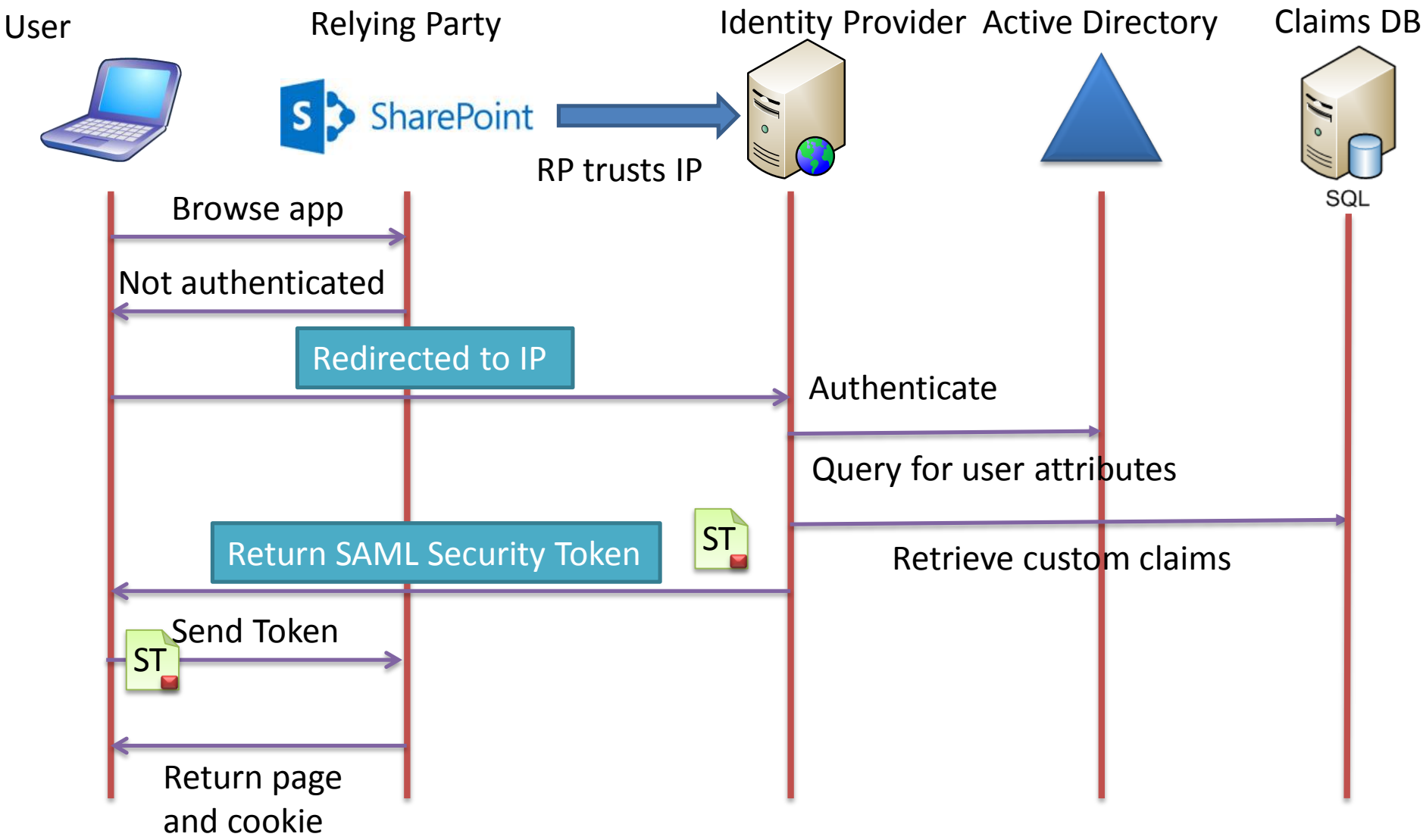
Issuer Portal



Custom Claims in TMX

- Company
  - May be more than one
  - Company Type
  - Exchange (TSX or TSX Venture Exchange)
  - Sector
  - Role at company
- Primary Company
- Primary Exchange
- Portal Roles
- Compound combinations of the above
- Used both to secure sections of the portal, and to target content to specific audiences

Custom Claims in SharePoint



Custom Claims with EUM