PlanBcp

DELTA ADFS

As Built for Delta

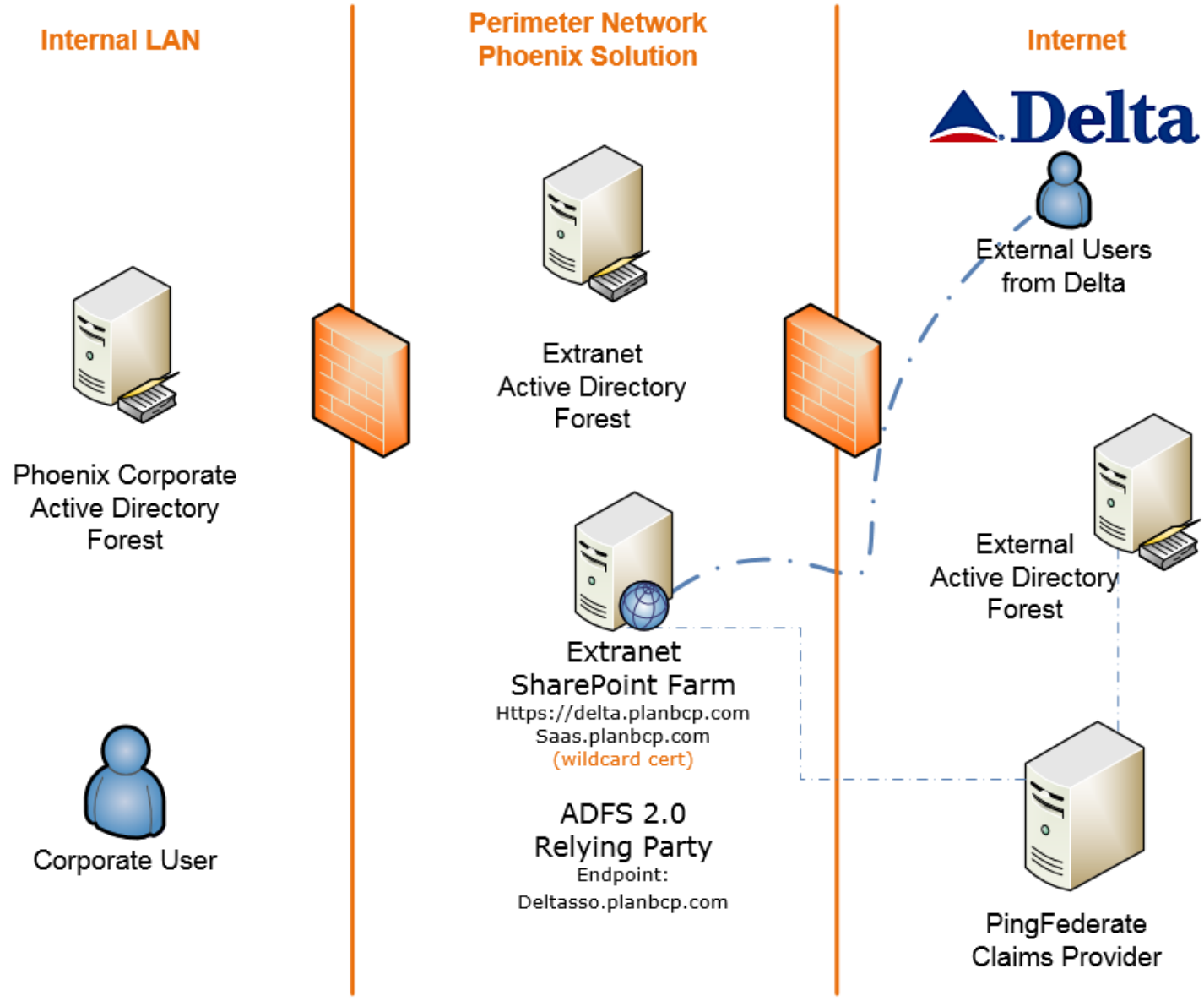
This document provides information architecture setup for PlanBcp's SharePoint using ADFS Authentication

13-Oct-15

CONTENTS

INTRODUCTION

This document provides documentation for ADFS authentication as built for Delta's access to PlanBcp SharePoint.



INFORMATION ARCHITECTURE FOR SHAREPOINT 2010 EXTRANETS: TOPOLOGIES

EXTRANET TOPOLOGY DESIGN CONSIDERATIONS

Encrypting SharePoint traffic in Internet-accessible scenarios by using Transport Layer Security (TLS) Secure Sockets Layers (SSL) is a familiar approach for securing communication that is the accepted standard. This is seen as HTTPS using port 443 and Digital Certificates versus unencrypted traffic over HTTP using port 80. *See Appendix D for more about Digital Certificates.*

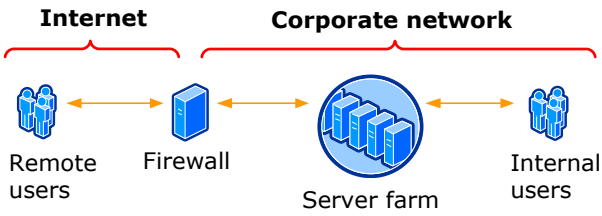
SharePoint technologies take advantage of TLS through IIS with .NET, which provide the underlying TLS-capable Web server platform. However, enabling TLS for SharePoint sites is only one aspect of securing external communication. You must also consider other facets such as host-based and network firewalls, design topology, and the underlying Active Directory and physical network dependencies.

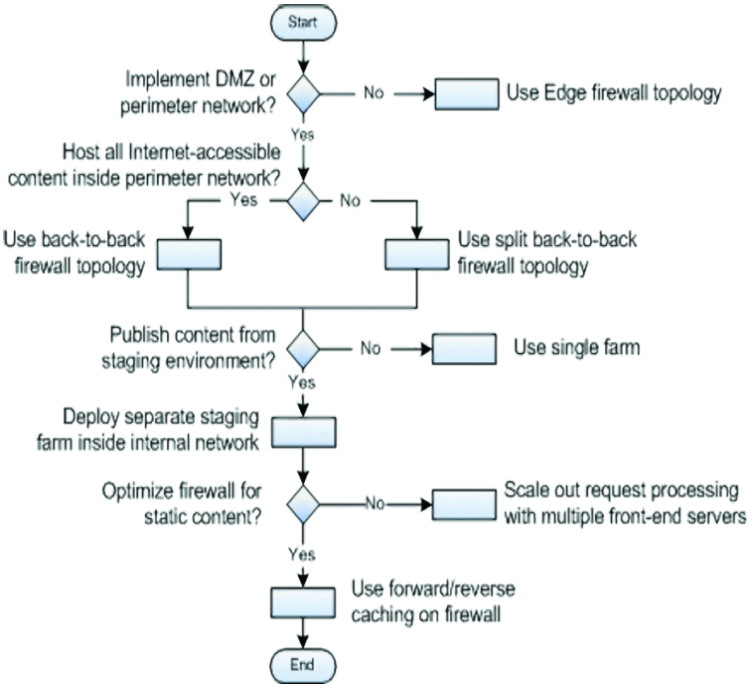
Developing multiple layers of security for SharePoint sites begins with defining physical network topology which are described in this report. If you can reduce or eliminate unwanted traffic before it hits front-end and back-end servers, you not only lessen server load but also mitigate the risks of viruses, spam, and malware that come with malicious traffic.

The network topology that accommodates TLS for SharePoint depends on the usage scenario required for your organization. How its best decided is a balance of security requirements with overhead of management and considering how it factors into flow of information between SharePoint farms.

DECIDING YOUR SHAREPOINT TOPOLOGY: A DECISION TREE

- Traffic before it hits the firewall.
- Traffic between the firewall and the internal network.
- Traffic inside the internal network.





TOPOLOGY: SINGLE SIGN-ON WITH ACTIVE DIRECTORY FEDERATION SERVICES

Typical extranet SharePoint deployments involve deploying SharePoint in an Active Directory (AD) forest on a perimeter network, or DMZ (see Figure 1). This solution lets you use AD as your authentication provider—without the need to create accounts for external users in your internal forest. This solution does, however, create one problem. With no trust relationship between AD domains (internal and external) you will need to create user accounts in the perimeter AD forest for not only clients and vendors, but also for internal corporate users, which obviously means more administrative work for IT departments. Using this solution, you're managing not only two sets of accounts for internal users, but also accounts from business partners.

Delta corporate users should be able to use their internal Active Directory account to log on to a SharePoint server that's set up as a member server of the perimeter Active Directory forest. To accomplish that design goal, we used the servers shown in Figure 2.

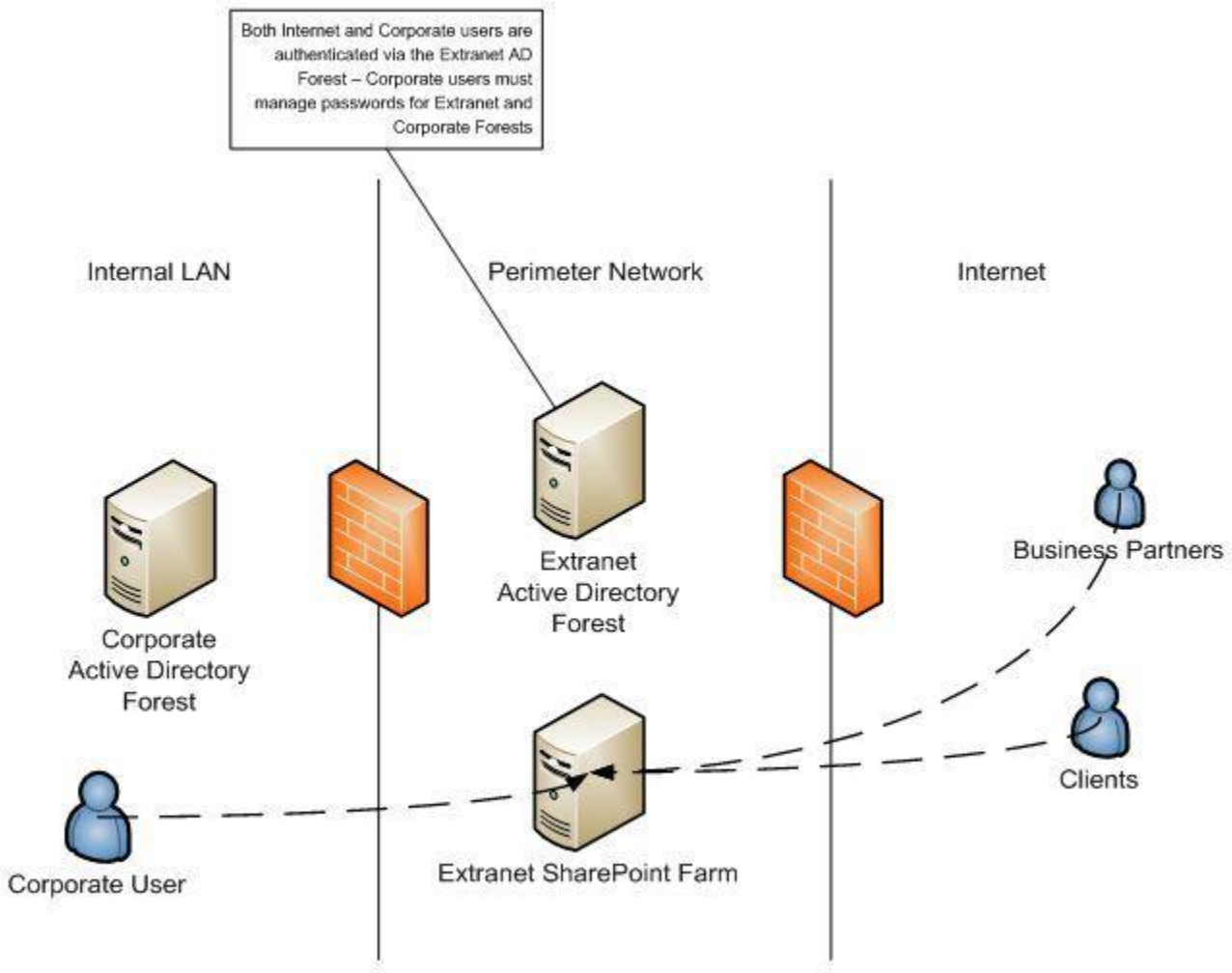


Figure 1. Extranet SharePoint deployment without ADFS: The figure shows a typical perimeter network setup that uses an AD forest between the internal LAN and the Internet.

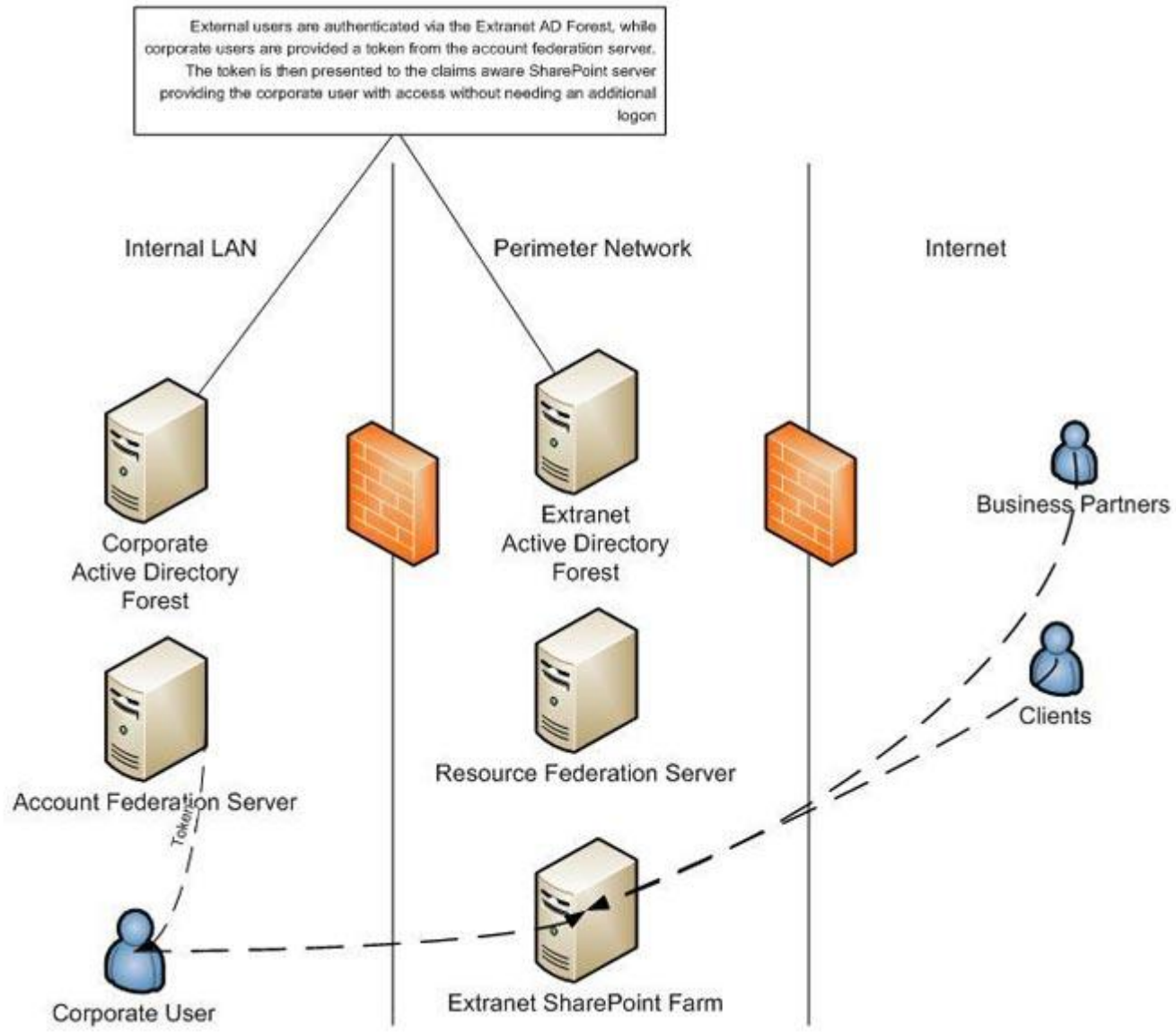


Figure 2. Extranet SharePoint Deployment with ADFS: This figure shows the arrangement of servers you need for an extranet SharePoint deployment with ADFS.

Required servers are:

1. Active Directory Certificate Services or third-party public key infrastructure (PKI) (This is not required, but it is recommended for production deployments.)
2. Internal LAN Active Directory Forest
3. Internal LAN Account Federation Server
4. Perimeter Network Active Directory Forest
5. Perimeter Network SharePoint Server w/ADFS Enabled
6. Perimeter Network Resource Federation Server

ADFS Deployment

ADFS setup in Windows Server 2008 has been greatly improved; it now uses configuration wizards for many of the components.

After properly planning your ADFS deployment, you can install your federation servers. To install a federation server, use the "Add Roles" wizard to add the Federation Service role (see Figure 3). Note that all 5 role services are actually installed on one machine for single-server ADFS 2.0 & SharePoint deployment. The following breaks down how the services could be split between 3 servers.

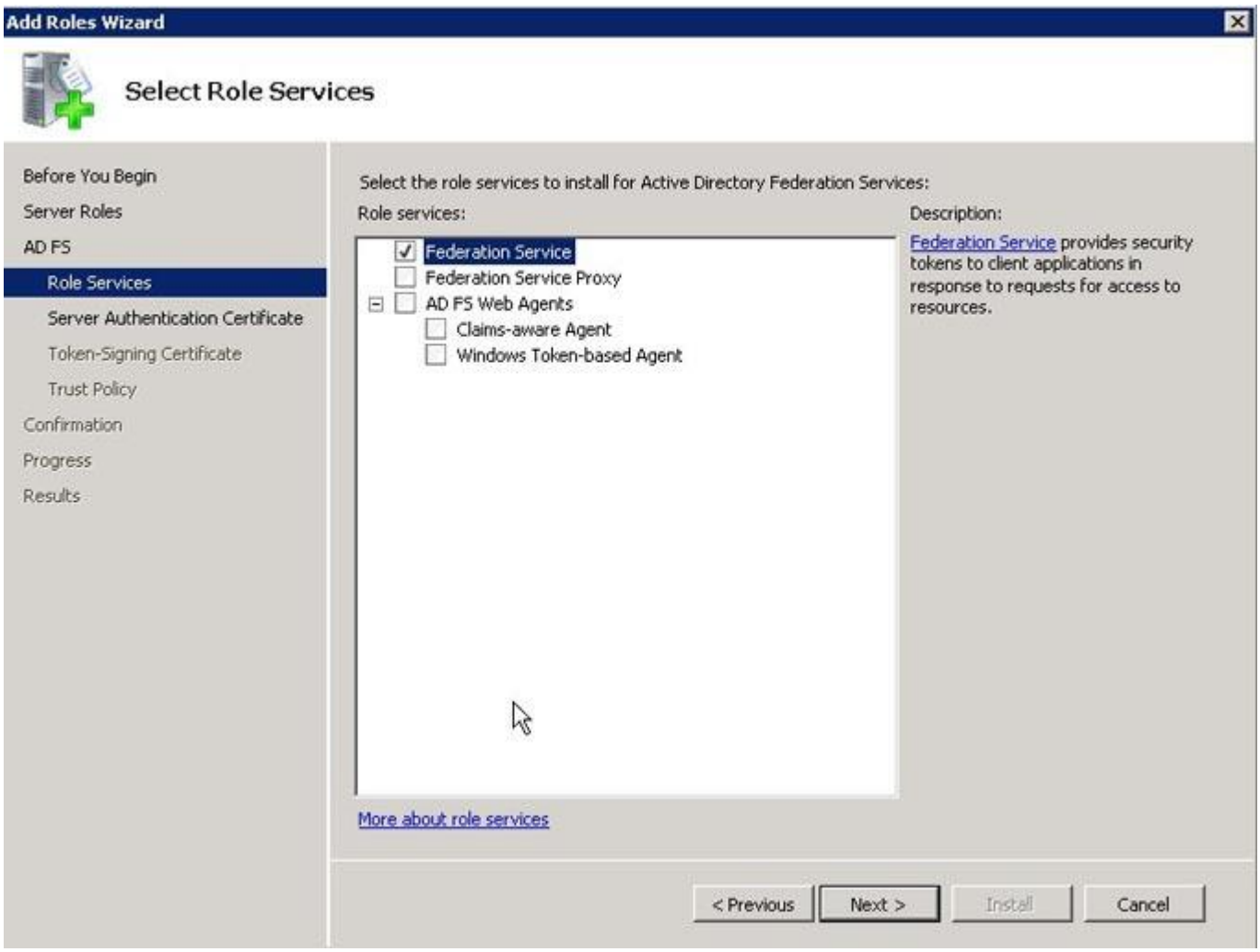


Figure 3. Adding the Federation Service Role: Use the "Add Roles" wizard to add a Federation Service role.
ADFS uses SSL for federation communication, so you'll need to obtain certificates via your own or third-party public-key infrastructure (PKI) providers. However, you can use self-signed certificates for test purposes and deployments (see Figure 4). When installing your federation server you will need both a Server Authentication Certificate and a Token Signing Certificate.

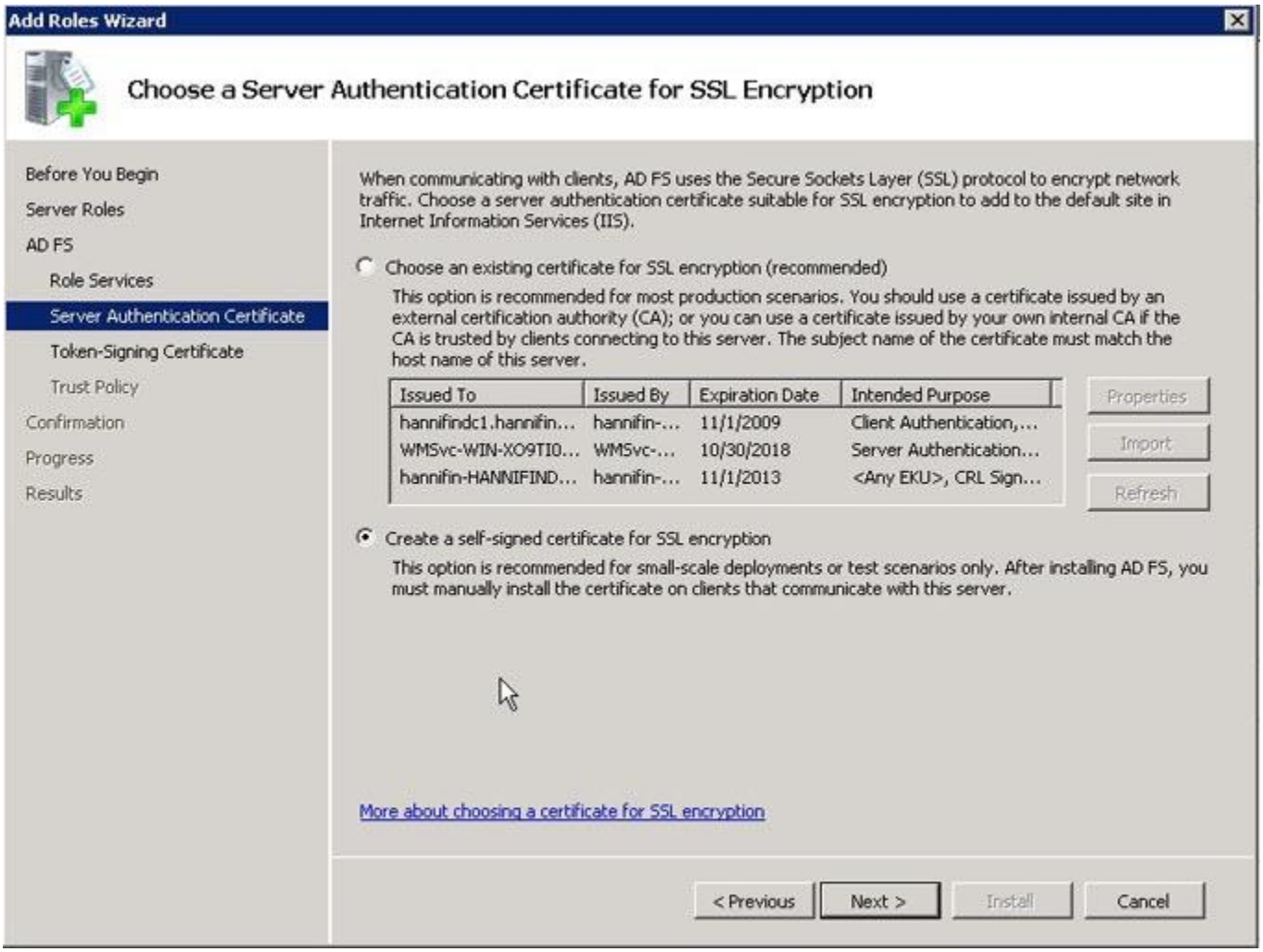


Figure 4. Selecting a Self-Signed Certificate: Because ADFS uses SSL, you'll need a certificate, but you can use a self-signed certificate for testing purposes.

You will need to install a Federation server on both your perimeter network and the partner network. According to the design scheme, the perimeter federation server acts as the relying party, while the partner's federation server acts as the claims provider.

After installing the federation servers, you need to install the ADFS Web Agent on the SharePoint server (see Figure 5). Doing that lets the SharePoint server use federation claims for authentication.

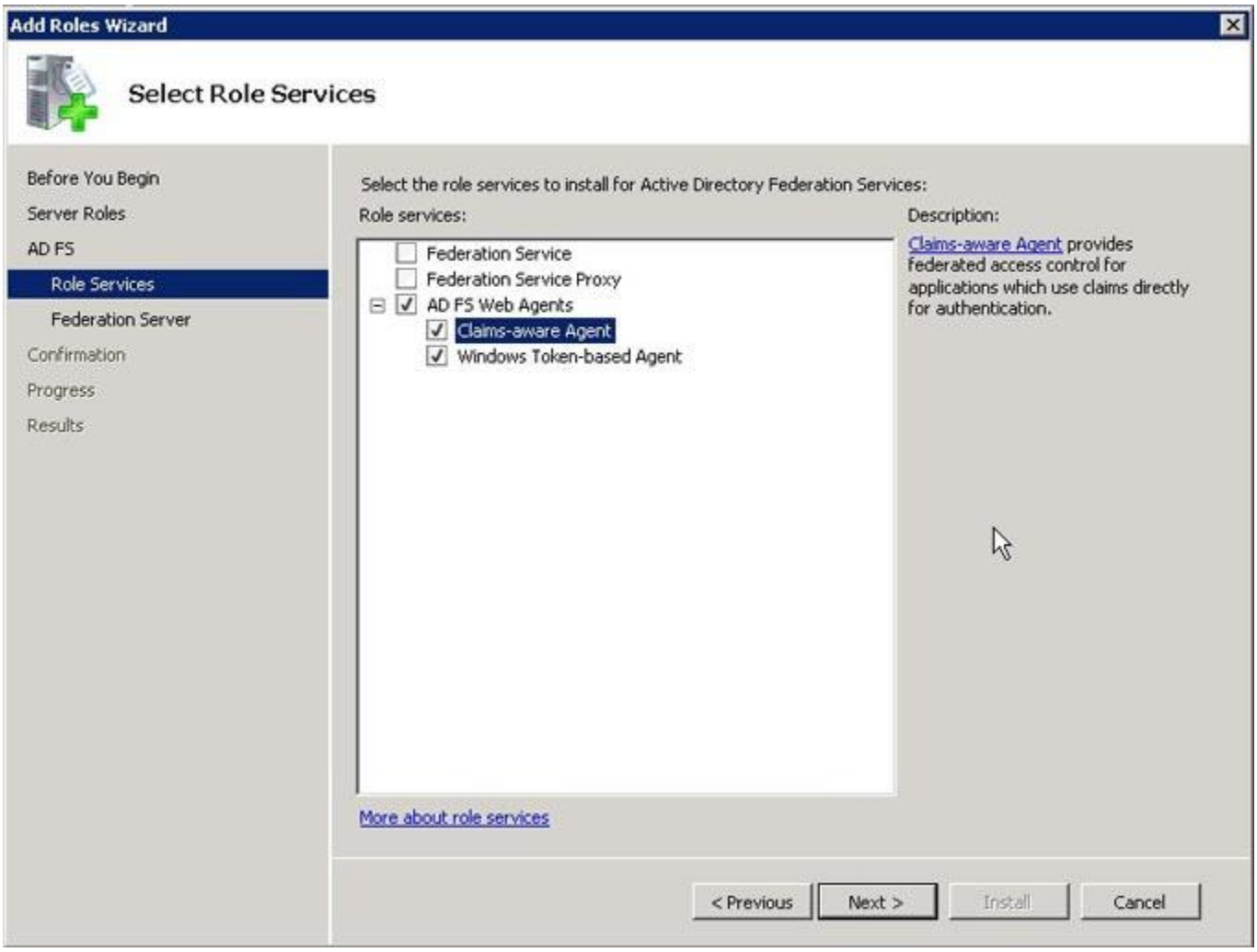


Figure 5. Adding the ADFS Web Agent to the SharePoint Server: Use the "Add Roles" wizard to add the ADFS Web Agent to your SharePoint server.

ADFS Configuration

After completing the federation server installations, you need to configure the correct settings on each one. If you used the self-signed certification option above, you will also need to install the certificate into the trusted root CA store for the computer account for each federation server and for the SharePoint server.

Configure perimeter Federation Server (Relying party)

You need to follow a few basic steps to configure your internal federation server. This is the server that will accept tokens from the partner's claims provider.

1. Create Claims Provider Trust to accept tokens from Partner federation server
    a. Display name: Delta Ping
    b. Claims Provider Identifier: amlabj11_OCPT (this is for dev server; will change for production)
    c. Add token-signing certificate provided by delta
    d. Add endpoint
        i. Type: SAML single sign-on

        ii. Binding: redirect
        iii. URL: https://localhost.delta.com:9080/dlppgateway/web?app=ocpt (dev server)
    e. Add Claims Rules
        i. Name: Transform to e-mail claim
        ii. Incoming Claim Type: Name ID
        iii. Incoming name ID format: Email
        iv. Outgoing Claim Type: E-mail address
        v. Pass through all claim values
2. Create Relying Party Trust to provide tokens to SharePoint
    a. Display name: Phoenix Internal Trust
    b. Relying Party Identifiers: urn:sharepoint:phoenix
    c. Add Endpoints:
        i. WS-Federation
            1. Type: WS-Federation
            2. Binding: Post
            3. URL: **https://delta.planbcp.com/_trust/**
        ii. SAML
            1. Type: SAML Assertion consumer
            2. Binding: Redirect
            3. URL: **https://delta.planbcp.com/_trust/**
    d. Add Claims Rules
        i. Name: Pass e-mail claims
        ii. Incoming claim type: e-mail address
        iii. Pass through all claim values
3. Modify Home-Realm discovery page to hide internal AD realm from Delta users
    a. Edit C:\inetpub\adfs\ls\HomeRealmDiscovery.aspx.cs
    b. Just under this line: PassiveIdentityProvidersDropDownList.DataBind();
    c. Add this: PassiveIdentityProvidersDropDownList.Items.RemoveAt(0);

SharePoint Configuration

Configure your SharePoint application to support ADFS tokens

1. Confirm web application is using claims-based authentication (convert to claims if necessary)
2. Add authentication provider (claims token issuer) via powershell
    a. $certPath = "C:\pcm\certs\token-signing.cer" (This is an exported copy of the self-signed token signing certificate created by ADFS)
    b. $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("$certPath")
    c. $map1 = New-SPClaimTypeMapping "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -IncomingClaimTypeDisplayName "EmailAddress" -SameAsIncoming
    d. $realm = "urn:sharepoint:phoenix"
    e. $signinurl = "https://deltasso.planbcp.com/adfs/ls/"
    f. $ap = New-SPTrustedIdentityTokenIssuer -Name "ADFS20Server" -Description "ADFS 2.0 Federated Server" -Realm $realm -ImportTrustCertificate $cert -ClaimsMappings $map1 -SignInUrl $signinurl -IdentifierClaim $map1.InputClaimType
3. Extend web application into extranet zone using newly-created ADFS20Server authentication provider
4. Confirm AAM and IIS bindings are configured appropriately

Internal URL	Zone	Public URL for Zone
http://saas.planbcp.com	Default	http://saas.planbcp.com
https://saas.planbcp.com	Internet	https://saas.planbcp.com
http://127.1.1.1	Custom	http://206.191.21.236
http://192.168.253.7	Custom	http://206.191.21.236
http://206.191.21.236	Custom	http://206.191.21.236
https://delta.planbcp.com	Extranet	https://delta.planbcp.com

AAM as configured

5. Establish trust relationship
    a. Central administration > Security > Manage trust > New
    b. Name: ADFS 2.0 Federated Server
    c. Root authority Certificate: None
    d. Provide Trust Relationship
        i. Token Issuer description: ADFS 2.0 Federated Server
        ii. Token Issuer Certificate: ADFS token signing certificate (same one as used in above powershell)

IIS Configuration

Configure IIS to support ADFS and to use appropriate bindings

1. Add net.tcp protocol
    a. Open advanced settings for default website, as well as sub-sites ADFS and LS
    b. Change “enabled protocols” from “http” to “http,net.tcp”
2. Bindings

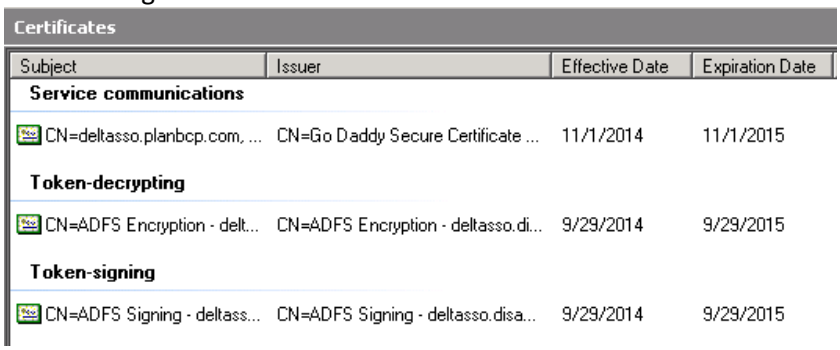
Site	Type	Host Name	Port	IP Address	Certificate
Default website	http	Deltasso.planbcp.com	80	192.168.253.14	N/A
Default website	https	N/A	443	192.168.253.14	Deltasso.planbcp.com
Delta.disasterrecovery.com	https	Delta.planbcp.com	443	192.168.253.7	*.planbcp.com
SharePoint – 80	http	saas.planbcp.com	80	192.168.253.7	N/A
SharePoint – 80	https	saas.planbcp.com	443	192.168.253.7	*.planbcp.com

    a. Note that the first 3 bindings are responsible for ADFS authentication
    b. The latter two bindings are used for windows authentication to same web application

Ongoing Maintenance Tasks

ADFS Certificates

Both parties must be aware of token signing certificates used by either party. ADFS certificates are managed via the ADFS 2.0 Management MMC under the Certificate node.



1. The ADFS Token-Signing certificate is a self-signed certificate that will expire every year on 9/29
    a. This certificate will be automatically re-created by ADFS annually
2. The certificate that Delta uses to sign tokens will need to be updated when theirs expires
    a. Claims Provider trusts
    b. Delta > Properties
    c. Certificates
    d. Add certificate here (current cert set to expire 9/5/2015)

USER MANAGEMENT SUGGESTIONS

There is one quirk to giving Delta users access to the SharePoint application.
Consider the following:

- We extended the SharePoint application into the Extranet zone and attached the authentication provider to this zone (SharePoint config step 3).
- The Extranet zone is accessed via URL delta.planbcp.com
- Delta users can only be "seen"/managed when accessing SharePoint via Extranet URL since that is where the authentication provider is attached.
- We hid the active directory realm to simplify the sign-in process for Delta users (ADFS config step 3)
- The Windows Authentication is using a separate zone, URL saas.planbcp.com

This presents a slight complication when a PlanBcp administrator would like to give Delta users security to SharePoint content. A PlanBcp administrator cannot sign in via delta.planbcp.com (as they are not a Delta member), and therefore cannot see the delta users in order to give access to them!

There are a few simple workarounds for this. The best option depends on a few factors, but at a high level:

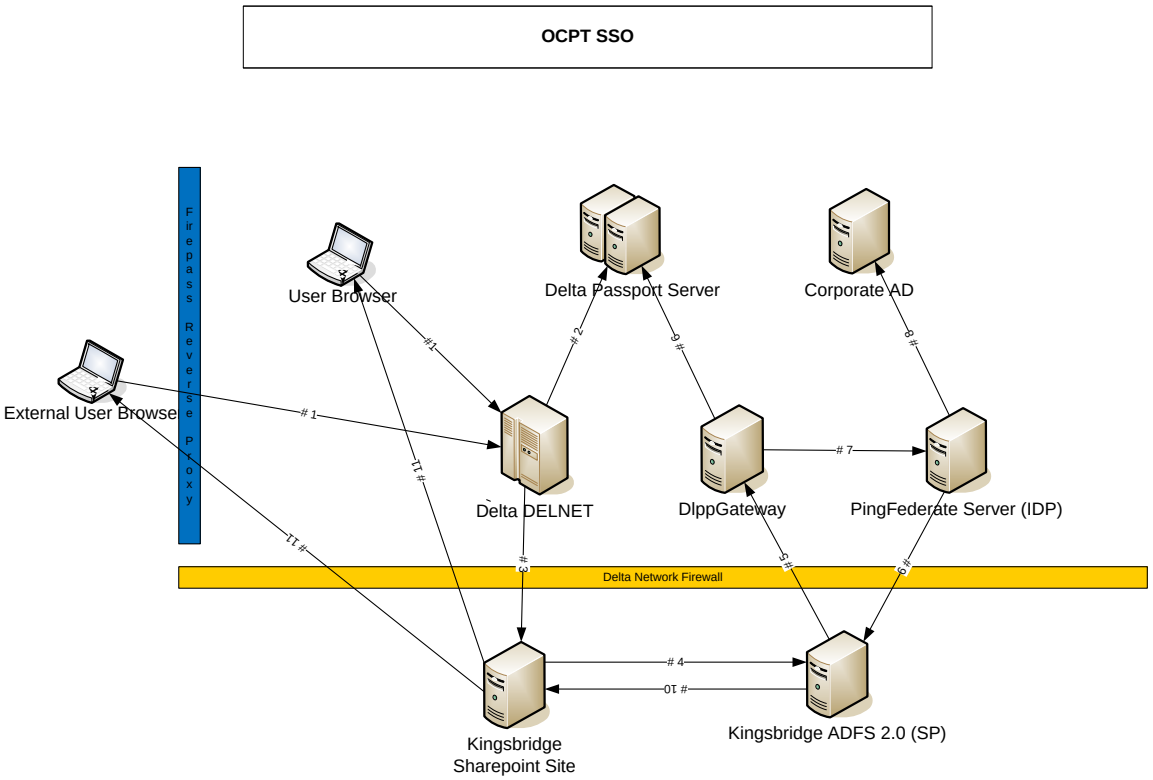
1. Temporarily add the windows authentication provider to the Extranet zone so that a PlanBcp Administrator can log in and manage Delta users.
    a. This should not be left permanently as it provides an ugly prompt to users asking them which authentication provider to use
    b. This would be a nuisance if managing users often
2. Use the above solution to configure a Delta user that has permission to manage users. That Delta user would then be able to easily manage users.
    a. Downside is that one user at Delta would have high levels of access to SharePoint web application
    b. User management responsibilities would be moved to Delta (maybe pro/con)
3. We could extend the SharePoint web application into yet another zone which would be used only by PlanBcp for user management. This zone would use both Windows Authentication as well as ADFS authentication providers.
    a. This would provide PlanBcp administrators with the most convenient method of user management
    b. Additional configuration required

DELTA OCPT USER SINGLE SIGN ON

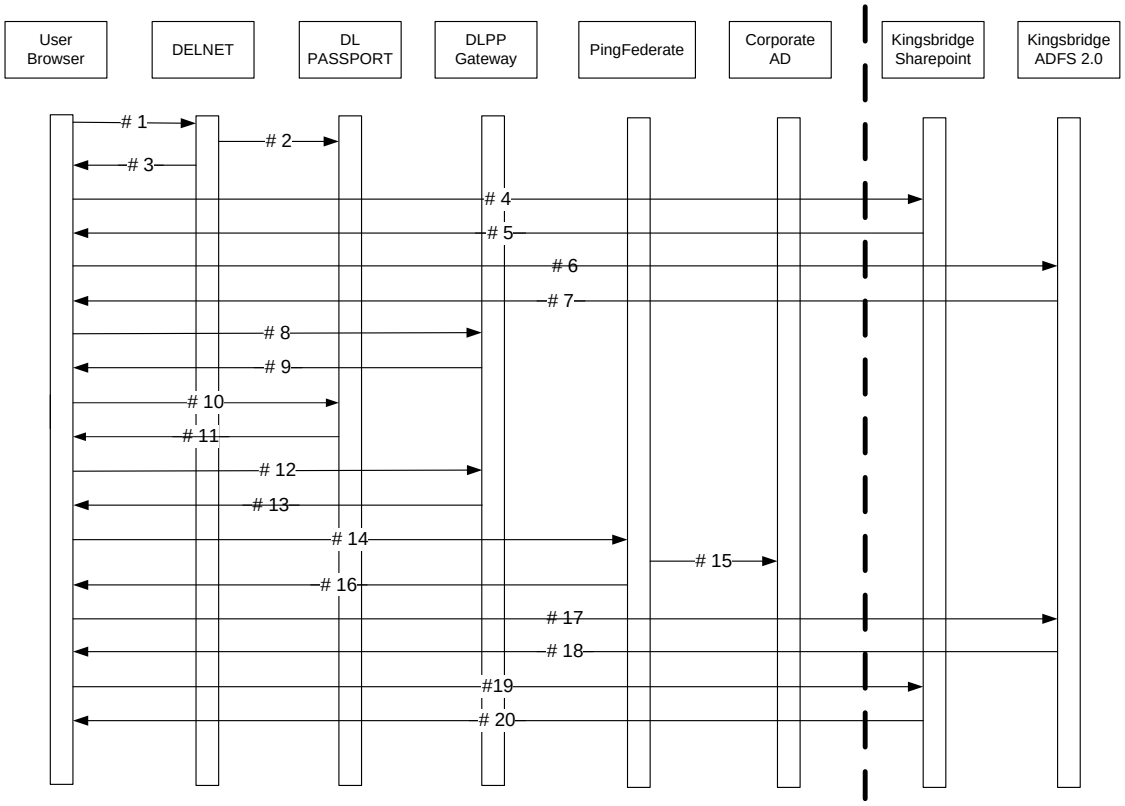
OCC – OPERATIONS CONTINGENCY PLANNING TOOL (OCPT)

For user Single Sign On https://delta.planbcp.com/delta/easi/ Sharepoint site which is hosted by Kingsbridge, on Delta side we use Delta Portal, Delnet.delta.com as user landing page, use Delta Passport for user authentication, dlppgateway.delta.com web application as user Identity provider, PingFederate server to handle SAML2 request and response. On Kingsbridge side, ADFS 2.0 is used for user Identity federation server and communicates with MS SharePoint site for user SSO. We use browser based, SAML2 protocol and SP Initialized SSO.

SYSTEM DIAGRAM:



REQUEST AND RESPONSE FLOW



BROWSER BASED SSO REQUEST AND RESPONSE FLOW DESCRIPTION

1. User access Delta Portal, delnet.delta.com
2. User logon to Delta Passport. (optional)
3. Portal return web content with Kingsbridge SharePoint SSO link back to user
4. User click the link, redirected to Kingsbridge SharePoint SSO page
5. Kingsbridge SharePoint SSO send auto redirect URL of Kingsbridge ADFS Server for user authentication with a token
6. User redirect to Kingsbridge ADFS 2.0 with the token and request authentication
7. ADFS send auto redirect url (dlppgateway.delta.com) with SAML2 request in query string back to user
8. User browser send request to Dlpp gateway with SAML2 request
9. Dlpp gateway check Delta Passport SSO token, if found go to step 13, if not found, redirect user browser to Delta Passport login page,
10. User login to Delta Passport
11. Delta Passport return a Delta Passport SSO token back to user browser and redirect user to Dlpp gateway
12. User browser return to Dlpp gateway with Delta Passport SSO token
13. Dlpp gateway read user Id (PPR #) from Delta Passport token, generate a Open Token format message, plus the SAML2 request from ADFS to generate the query string and redirect user browser to PingFederate server
14. User browser send get request to PingFederate Server
15. PingFederate read user Id from Open token, query Corporate AD with user Id to get user email address
16. PingFederate create SAML2 response message, redirect user browser to ADFS
17. User Bowser send SAML2 response to ADFS
18. ADFS verify the SAML2 response, retrieve user info (email address), redirect user browser to Kingsbridge Sharepoint site with a taken
19. User browser send request to Kingsbridge Sharepoint site with the token
20. Sharepoint verify the user token, create a session and send secured content back to user browser

TOPOLOGY: PERIMITER OR EDGE FIREWALL

Description

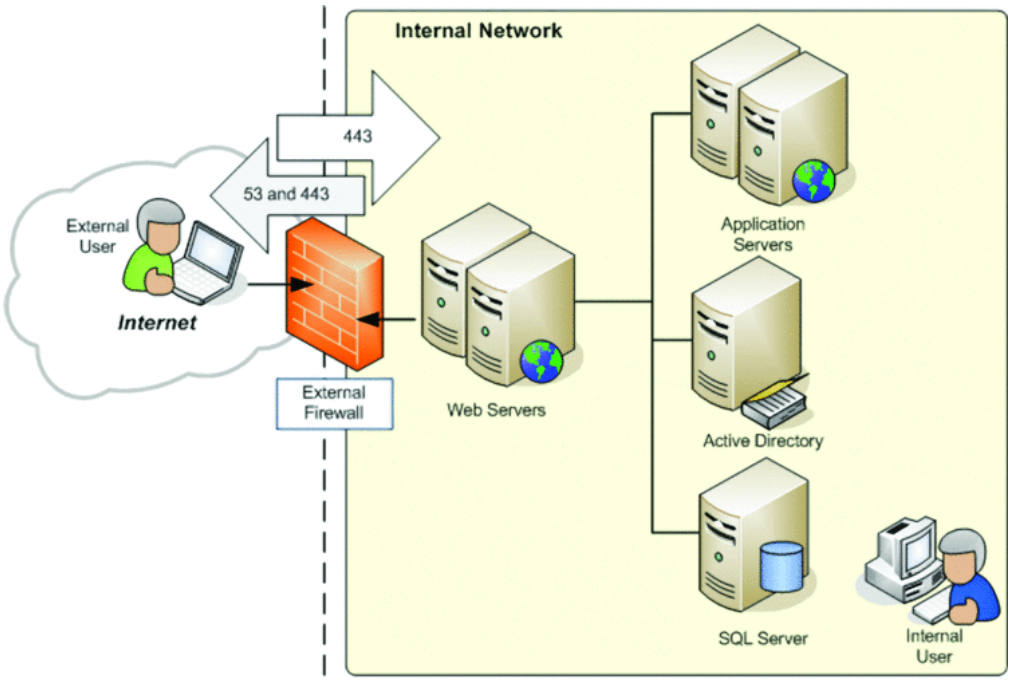
In edge topology, a single network firewall stands between external users and internal SharePoint sites. It has the advantage of using a single Active Directory environment for internal and external users, which simplifies maintenance and administration. To secure traffic via TLS, you configure the firewall to also act as a reverse proxy. The concept of an integrated reverse proxy such as ISA or TMG Server is vital for securing Internet-facing sites, because the reverse proxy intercepts incoming requests, can authenticate external users, decrypts TLS traffic, inspects it according to firewall rules, and forwards requests to front-end servers. Public URLs may differ from internal URLs, so the reverse proxy must have a means to perform link translation to convert external URLs into internal URLs. UAG Server provides additional security capabilities, such as end-point, health-based authorization through an access policy based on user identity and client computer health, and the ability to translate links for internal SharePoint URLs when using Outlook Web Access By using a set of configurable rules, the proxy server verifies that the requested URLs are allowed based on the zone from which the request originated. The requested URLs are then translated into internal URLs.

Advantages

- The simplest solution that requires the least amount of hardware and configuration.
- The entire server farm is located within the corporate network.
- There is a single point of data:
- Data is located within the trusted network.
- Data maintenance occurs in one place.
- A single farm is used for both internal and external requests; this ensures that all authorized users view the same content.
- Internal user requests are not passed through a proxy server.
- UAG pre-authenticates users.

Disadvantage

This configuration results in a single firewall that separates the corporate internal network from the Internet.



TOPLOGY: BACK-TO-BACK PERIMETER

Description

- A back-to-back perimeter topology isolates the server farm in a separate perimeter network.
- All hardware and data reside in the perimeter network.
- The server farm roles and network infrastructure servers can be separated across multiple layers. Combining the network layers can reduce the complexity and cost.
- Each layer can be separated by additional routers or firewalls to ensure that only requests from specific layers are allowed.
- Requests from the internal network can be directed through the internal-facing ISA/TMG server or routed through the public interface of the perimeter network.

You are not limited to just two firewalls in a back-to-back topology. You can implement additional layers separated by firewalls or routers to further separate the SharePoint roles. For example, you could use a three-layer approach, putting each layer in a DMZ, where front-end servers are first, followed by application, database and search/index server, and concluded by Active Directory/DNS servers. You can also customize a back-to-back topology to include an internal staging environment in a separate farm and publish it to the farm in the perimeter network.

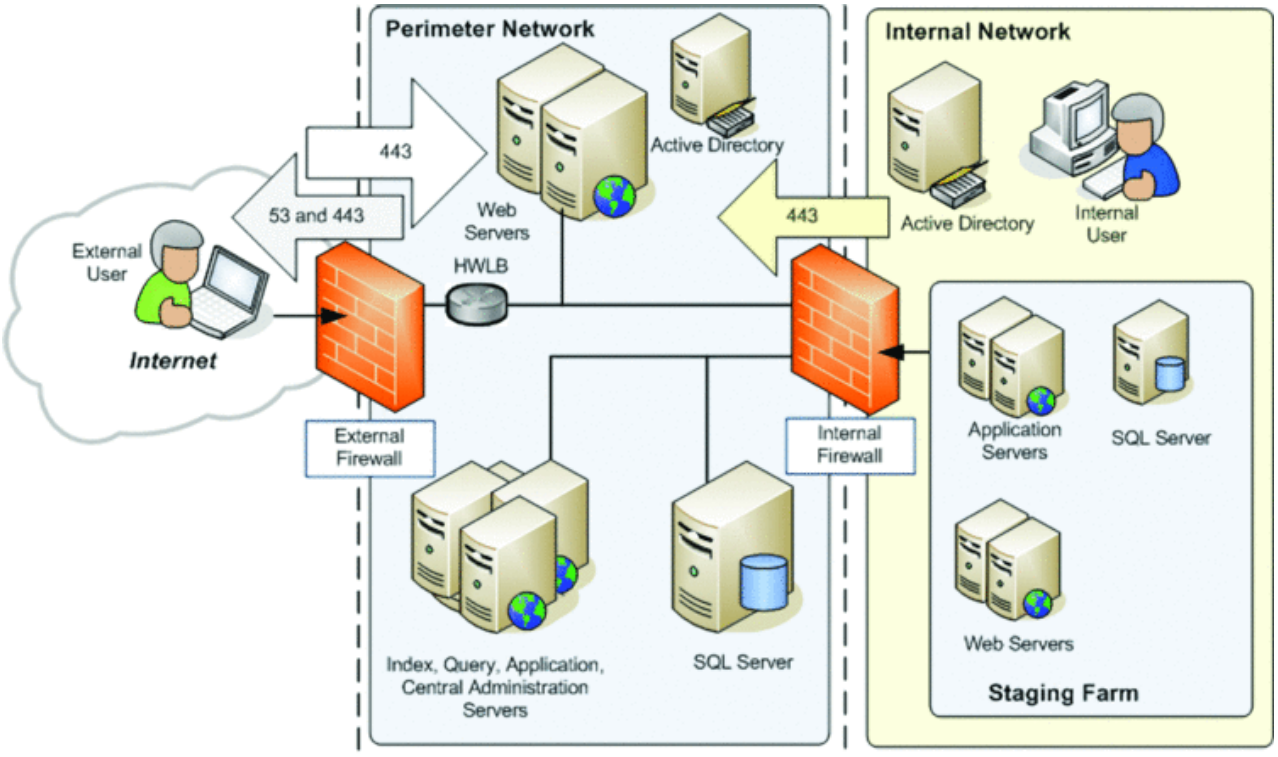
Advantages

Content is isolated to a single farm on the extranet, simplifying sharing and maintenance of content across the intranet and the extranet.

- External user access is isolated to the perimeter network.
- If the extranet is compromised, damage is potentially limited to the affected layer or to the perimeter network.

Disadvantage

- Requires additional network infrastructure and configuration.



TOPOLOGY: SPLIT BACK-TO-BACK

Description

In keeping with the approach of using security layers in the topology, front-end servers reside in the perimeter network and the back-end servers running SQL Server reside in the internal network. The remaining roles, such as index, search, and central administration, can be in either network. This topology splits the farm between the perimeter and corporate networks. The computers running Microsoft SQL Server® database software are hosted inside the corporate network. Web servers are located in the perimeter network. The application server computers can be hosted in either the perimeter network or the corporate network.

If the server farm is split between the perimeter network and the corporate network, a domain trust relationship is required. There are two AD domains for the Intranet and extranet - say DOMAIN and DOMAINEXT. DOMAINEXT is in the perimeter network. Servers in the perimeter (DMZ) network are joined to this domain. In this scenario, the perimeter domain must trust the corporate domain. DOMAINEXT trusts DOMAIN with a 1-way trust.

You set up the farm as you typically would internally within DOMAIN. You then join a WFE in the perimeter network to the farm. Since this WFE is joined to a domain that trusts the internal domain, it can use the same service accounts, etc. However, if someone hacks the WFE and gains access to the extranet domain, they can't do anything to the internal domain as DOMAIN does not trust DOMAINEXT.

The only scenario in which a domain trust is not required is if the Web and application servers are in the perimeter network, the database servers are in the corporate network, and SQL authentication is used. However, if the Web and application servers are split between the networks and SQL authentication is used, a trust relationship is required.

Advantages

- Computers running SQL Server are not hosted inside the perimeter network.
- Farm components within both the corporate network and the perimeter network can share the same databases.
- Content can be isolated to a single farm inside the corporate network, which simplifies sharing and maintaining content across the corporate network and the perimeter network.

Disadvantages

- The complexity of the solution is greatly increased.
- Intruders who compromise perimeter network resources might gain access to farm content stored in the corporate network by using the server farm accounts.
- Inter-farm communication is split across two domains.

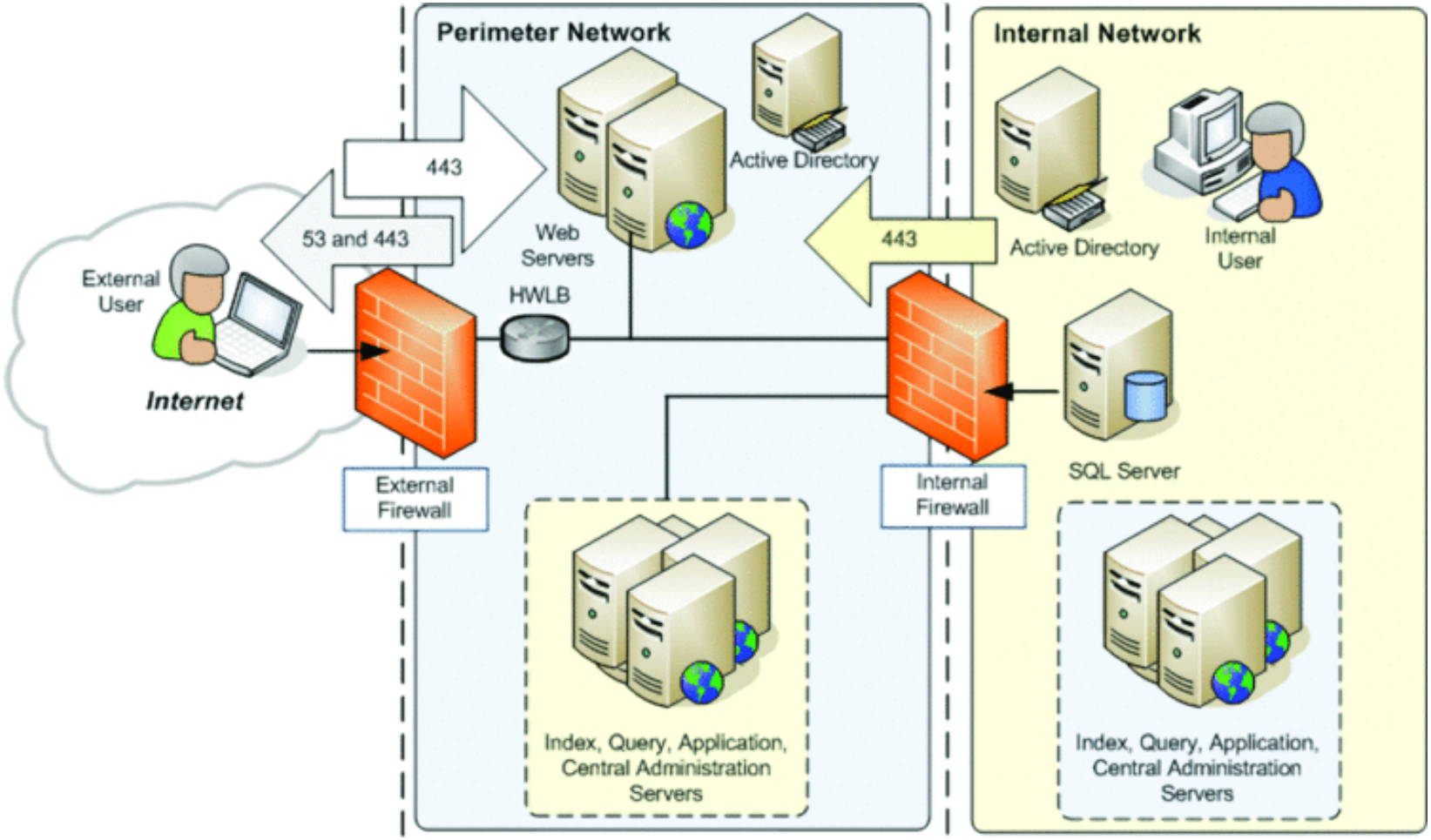
Requirements

- One-way trust between extranet AD and intranet AD
- Open Firewall Ports
    - WFE / Service application communication - Port 32843
    - SQL: TCP/TDS: 1433, 1434; Analysis service TCP: 2394
    - WINs: name service 137, Browser: 138, Session: 139
    - Search propagation requires file and printer sharing either via SMB 445 or NetBT Ports 137, 138, 139
    - SMTP - Port 25
    - Authentication – LDAP: 389, Kerberos: 88
    - Sandboxed solutions (if used) - Port 32846
    - User Profile Sync should be configured within intranet as access to AD is required and used ports 53, 389, 5725

TOPOLOGY: SPLIT BACK-TO-BACK

About this diagram:

- Application servers are hosted inside the perimeter network. This option is illustrated by servers inside the dashed line.
- Application servers can optionally be deployed inside the corporate network, with the database servers. This option is illustrated by the servers inside the gray box with the dashed line.
- To optimize search performance and crawling, place the application servers inside the corporate network with the database servers. You can also add the Web server role to the index server inside the corporate network and configure this Web server for dedicated use by the index server for content crawling.



APPENDICES

APPENDIX A: SUPPORTED AUTHENTICATION METHODS

Supported authentication methods
SharePoint Server 2010 supports authentication methods that were included in previous versions and also introduces token-based authentication that is based on Security Assertion Markup Language (SAML) as an option. The following table lists the supported authentication methods.

Method	Examples	Notes
Windows	• NTLM • Kerberos • Anonymous • Basic • Digest	
Forms-based authentication	• Lightweight Directory Access Protocol (LDAP) • Microsoft SQL Server database or other database • Custom or third-party membership and role providers	Forms-based authentication is an identity management system that is based on ASP.NET membership and role provider authentication. In SharePoint Server 2010, forms-based authentication is available only when you use claims-based authentication.
SAML token-based authentication	• Active Directory Federation Services (AD FS) 2.0 • Third-party identity provider • Lightweight Directory Access Protocol (LDAP)	Supported only with SAML 1.1 that uses the WS-Federation Passive profile. Client certificate authentication is possible through integration with AD FS 2.0. For additional information, see Configure Client Certificate Authentication (SharePoint Server 2010).

Authentication modes — classic or claims-based
SharePoint Server 2010 introduces claims-based authentication, which is built on Windows Identity Foundation (WIF). You can use any of the supported authentication methods with claims-based authentication; or you can use classic-mode authentication, which supports Windows authentication.

Claims-based authentication is built on WIF, which is a set of .NET Framework classes that are used to implement claims-based identity. Claims-based authentication relies on standards such as WS-Federation, WS-Trust, and protocols such as SAML.

http://technet.microsoft.com/en-us/library/cc262350.aspx

APPENDIX B: MICROSOFT ISA / TMG / UAG SOFTWARE SOLUTIONS

COMPLIMENT SHAREPOINTS, PROVIDE LINK TRANSLATION, CACHING, INTRUSION DETECTION, AND SIMPLFIED CLIENT ACCESS MANAGEMENT

Features from which organizations will benefit when they deploy an integrated firewall and caching solution include the following:

- Secure Outlook Web Access publishing
- Secure RPC/HTTP Web access publishing
- Secure Internet Information Services Web site publishing
- Secure Exchange RPC publishing
- Secure SharePoint Portal Server publishing
    - Forms Based Authentication w/ Single Sign On capabilities
- Granular policy-based access rules for both inbound and outbound access.
- Intelligent application layer inspection filter and stateful packet inspection.
- Simplified and intuitive firewall configuration interface. No need to learn a complex and difficult to remember command line interface routines. All firewall and Web proxy features are exposed on the Server Firewall Management Console.
- Detailed logging and reporting provides both a “birds-eye” view and the capabilities to drill down to specific connections.
- Active Directory service integration via domain members or LDAP queries to the Active Directory database provides seamless access to Active Directory users and groups, greatly simplifying the task of enabling granular user/group based access controls.
- If your organization has previously deployed ISA Server 2006 to publish earlier releases of SharePoint, you can continue to use this product or move to Threat Management Gateway (TMG) to publish SharePoint 2010 Products applications.

The new TMG 2010 client can even perform automatic discovery using records that reside in the Active Directory, using an LDAP query, in addition to the traditional methods (DNS and DHCP). The TMG client (better known as the Firewall client) is a Winsock proxy application that can control remote connections from Winsock applications to the TMG firewall. You can use the Firewall client to make your routing infrastructure transparent to the client system. What that means in practice is that it doesn’t matter what your default gateway is on the client system. As long as the client system has access to the IP address on the internal interface of the TMG firewall, it will be able to connect the client system to the Internet.

In addition to routing transparency, you also get application and user names in your firewall logs. The TMG client will forward both the application name that’s being used to access the Internet and the name of the user who is using that application. This is a very cool feature. When you deploy the Firewall client, your logs and reports can include both the names of the users (and you can deploy user/group based access controls) and the applications they used

Last but not least, the Firewall client will support complex protocols without requiring the assistance of an Application Filter. Since Application Filter development can be complex, this is a tremendous boon for the TMG firewall admin and can significantly reduce the support desk calls for applications that “don’t work”.

Microsoft® Forefront® Unified Access Gateway (Forefront UAG) provides secure Web publishing of applications, using SSL. Forefront UAG provides access to internal resources for remote employees and partners. Forefront UAG adds the following capabilities to the SharePoint 2010 Products extranet solution:

SECURE ACCESS TO SHAREPOINT SITES FROM MOBILE DEVICES

Authentication of mobile users using a dedicated interface for mobile devices.

HEALTH-BASED ENDPOINT AUTHORIZATION

Access policies that are based not only on the user's identity and the information exposed, but also on the condition of the client endpoint.

INFORMATION LEAKAGE MITIGATION

Cleanup of the client endpoint, including cache, temporary files, and cookies.

AUTHENTICATE DIRECTLY FROM RICH CLIENTS

Use Microsoft Office Forms Based Authentication (MSOFBA) or basic authentication to enable rich client programs to directly access SharePoint sites. Additionally, Forefront UAG DirectAccess provides remote users with the experience of a seamless connection to the internal network. When Forefront UAG DirectAccess is enabled, requests for internal network resources are directed securely, without the need to connect to a VPN.

Feature	ISA 2006	Forefront TMG	Forefront UAG
Built īn features for configuring SharePoint Publishing	✓	✓	✓
Network load balancing	✓	✓	✓
Array support	✓	✓	✓
Mobile access	✓	✓	✓
Rich authentication	✓	✓	✓
Endpoint health detection			✓
Granular access policies			✓
Information leakage mitigation			✓
SSO via FBA	✓	✓	✓
DirectAccess		✓ *	✓

*Direct Access is partially supported for Forefront TMG 2010

APPENDIX C: PRICING FOR MICROSOFT ISA / TMG / UAG SOFTWARE SOLUTIONS

Forefront TMG 2010 Standard Edition	$1,499 per processor	Forefront TMG 2010 Standard Edition is a comprehensive, secure Web gateway that helps protect employees from Web-based threats...
Forefront TMG 2010 Enterprise Edition	$5,999 per processor	Forefront TMG 2010 Enterprise Edition license gives customers increased scalability, provides access to a central management console, and offers complete support for virtual environments
Forefront TMG Web Protection Service	$12.00 per user or device, annually	Forefront TMG Web Protection Service provides continuous updates for malware filtering and access to cloud-based URL filtering to protect against the latest Web threats.
UAG 2010 User CAL	$15 per user	UAG 2010 appliances require a CAL for each named and/or authenticated user who accesses resources through the gateway.
UAG 2010 Device CAL	$15 per user	UAG 2010 appliances require a CAL for each client device that accesses resources through the gateway.
ISA Standard Edition	$2,370	http://www.nextag.com/Software--a-Software+Internet+Type-_-Security+%5E%5E1+Firewalls--zzmicrosoft+isa+server+license+costz300170zB6z5---html

APPENDIX D: DEFINITIONS, ACRONYMS, AND ABBREVIATIONS

WHAT IS DIRECT ACCESS?

DirectAccess is a new feature in the Windows® 7 and Windows Server® 2008 R2 operating systems that gives users the experience of being seamlessly connected to their corporate network any time they have Internet access. With DirectAccess, users are able to access corporate resources (such as e-mail servers, shared folders, or intranet Web sites) securely without connecting to a virtual private network (VPN).

Forefront Threat Management Gateway (TMG) can be installed on the DirectAccess server to provide an additional layer of protection and to enable the use of additional Forefront TMG technologies (e.g. full IPV4 firewall or Secure Web Publishing) for non DirectAccess capable machines.

WHAT IS FORMS BASED AUTHENTICATION?

The ability to authenticate with your AD (Active directory) or another authentication source such as an SQL database of users and passwords, via an HTML forms page. This provides a friendly experience for the user as the page may contain password reset or help contacts. FBA can be done without TMG by using SharePoint's Claims based authentication but that prevents SSO being available.

WHAT IS SINGLE-SIGN-ON (SSO) AUTHENTICATION?

SSO is dependent on FBA. When you have logged in to a portal you then can access all your internal portals without authenticating. So if you log into extranet.acme.com you could go to outlook web access or intranet.acme.com without re-logging on.

ABOUT DIGITAL CERTIFICATES

Encrypting SharePoint traffic in Internet-accessible scenarios by using Transport Layer Security (TLS) Secure Sockets Layers (SSL) is a familiar approach for securing communication that is the accepted standard. This is seen as HTTPS using port 443 and Digital Certificates versus unencrypted traffic over HTTP using port 80.

Microsoft IIS (Internet Information Server) host headers can be used to host multiple secure web sites on one IP address. However, the same SSL certificate must be used for every site secured. That means that host headers can be used to secure multiple sites with SSL on one IP only by using certificates that are capable of covering more than one website (Wildcards or UC certificates). If multiple SSL certificates are used, the server will usually encounter problems providing the correct SSL certificate when an HTTPS connection is established, causing a certificate name error when connecting.

A Wildcard Certificate will secure any subdomain of the domain that it was issued to. For example, a Wildcard SSL certificate issued to *.domain.com will cover something.domain.com, anything.domain.com, and whatever.domain.com. Because the *.domain.com certificate would be valid on any of these three domains, the server cannot supply the "wrong" SSL certificate.