CSC Companion Products – (C.0) Release

Security White Paper

This ***Security White Paper*** provides information needed to protect your CSC Companion products Web sites from external security threats.

Updated: January 28, 2010

Preface—CSC Companion Product Names

The CSC Companion Products take on combined names when installed with other CSC products. The table below indicates the various names that refer to the same product, and how the product will be referred to throughout this document.

Product	Is Named	When	In Documentation
iSolutions	POINT IN Agency Link	Installed with POINT IN	Agency Link
	iSolutions	Installed separately or with any system other than POINT IN	Agency Link
Underwriting	POINT IN Underwriting	Installed with POINT IN	Underwriting
	iSolutions Underwriting	Installed separately or with any system other than POINT IN	Underwriting
Information Ordering	POINT IN Information Ordering	Installed with POINT IN	Information Ordering
	iSolutions Information Ordering	Installed separately or with any system other than POINT IN	Information Ordering

For More Assistance

Please direct any questions or suggestions regarding this material to CSC P&C Client Support by telephone at (International Access Code U.S.A.) 803.333.6200 or email pcssupport@csc.com.

Table of Contents

Preface—CSC Companion Product Names 2

Introduction 6

How Secure Is Secure? 7

Hardening Your Web Site 8
- Install a Firewall System 8
- Establish a Virtual Private Network 9
- Secure Windows Server and Internet Information Server 10
  - WARNING: Web Administrator Must Consider These Security Vulnerabilities 10
- Secure SQL Server 12
  - Best Practices 12
- Use a Tougher Password Encryption 13
  - Web Enabled Security and SSL 13
  - Web Server Certificates 14
  - CA Certificates 14
  - Secure Sockets Layer (SSL) 15

Server Implementation When Implementing Several Companion Products 16
- Security Port Access 18
  - Footnotes and Other Important Considerations 20
    - A. About Port 80 20
    - B. How To Configure Remoting 20
    - C. CAUTION for Agency Link and Information Ordering when interfacing with ChoicePoint 21
    - D. You may configure error messages that are generated by IIS 21
- Implementation Model: All Companion Products 22
- Two Possible Models 24

Advanced Claims Server Implementation 25
- Security Port Access 27
  - Footnotes and Other Important Considerations 27
    - D. You may configure error messages that are generated by IIS 27
- Implementation – Production Model 27

Agency Link Server Implementation 29
Security Port Access 30
Footnotes and Other Important Considerations 31
A. About Port 80 31
B. How To Configure Remoting 31
C. CAUTION for Agency Link when interfacing with ChoicePoint 31
D. You may configure error messages that are generated by IIS 32
Implementation – Production Model One 32
Implementation – Model Two 36

Business Intelligence Server Implementation 40
Security Port Access 41
Footnotes and Other Important Considerations 41
D. You may configure error messages that are generated by IIS 41
Implementation – Production Model 42

Document Production Server Implementation 44
Security Port Access 45
Footnotes and Other Important Considerations 45
B. How To Configure Remoting 45
D. You may configure error messages that are generated by IIS 46
Implementation – Production Model 46

Information Ordering Server Implementation 49
Security Port Access 50
Footnotes and Other Important Considerations 51
A. About Port 80 51
B. How To Configure Remoting 51
C. CAUTION for Information Ordering when interfacing with ChoicePoint 51
D. You may configure error messages that are generated by IIS 51
Implementation – Production Model One 52
Implementation – Model Two 55

Media Management Server Implementation 58
Security Port Access 59
Footnotes and Other Important Considerations 59
B. How To Configure Remoting 59
D. You may configure error messages that are generated by IIS 60
Implementation – Production Model 60

POINT IN Server Implementation 63
Security Port Access 64
Implementation – Production Model 64

Underwriting Server Implementation 67
Security Port Access 68
Footnotes and Other Important Considerations 68

A. About Port 80 68
B. How To Configure Remoting 69
C. CAUTION for Underwriting when interfacing with ChoicePoint.... 69
D. You may configure error messages that are generated by IIS 69
Implementation – Production Model One 70
Implementation – Model Two 73

Externalized Authentication Details for Agency Link 76
Configuration Options 76
Method One 76
Method Two 77

Communications Framework: Enabling SSL for Apache Tomcat 78
Enable SSL Under Tomcat 78
Import Trusted Certificates 80
On the Domain Controller - 2003 Server (If Not Already Installed) 81
Request Certificate for Domain Controller for MMC 81
Navigate to Personal Folder within Certificates 81
Export Certificate 82
Import Certificate 83

Communications Framework: SSL Certificate Set-Up Using IBM WebSphere 85
High-Level Look at the Procedure 85
On WebSphere Server 85
On Domain Controller 85
On WebSphere 85
Detailed Steps 86
Certificate Set-Up 86
On WebSphere 86
On the Domain Controller - 2003 Server (If Not Already Installed) .. 88
Within Java (WebSphere) 90
Import Certificates into WebSphere Server Using Ikeyman 90
Java (Add Certificates to JVM Keytrust) 91

Index I-93

Document Change Log 95

Introduction

CSC's Companion products help insurance companies build remote access infrastructure to run more of their business over the Internet. But running business over the Internet comes with a high potential for serious security risks if systems and data are not adequately managed and protected.

This document outlines several factors you must consider when deploying a secure Companion product site and provides information and resources to help you:

- Assess the security risks
- Determine how to deploy your site with the proper defense mechanisms
- Lay the foundation for an ongoing solid security infrastructure

This paper was created for corporate executives, software architects, and developers whose mission is to deliver business-critical functions on the Internet through CSC's Companion products.

How Secure Is Secure?

No computer system can ever be completely secure. Therefore, the goal is to make it increasingly difficult for someone to compromise your system.

Regardless of where the security threat comes from, it is important to recognize that significant threats do exist, and defenses must be established to effectively lower your Web site security risk.

Another important factor to consider is the more secure your system, the more intrusive your security. It is a balancing act to make the system usable for your customers, yet secure from intrusion.

CSC's Companion products are not Web security applications. They are financial applications that rely on a pre-existing Web security infrastructure. Alone, each Companion product only authorizes users of the application and restricts use based on user profiles defined by the system administrator.

The Companion products cannot protect your Web site from malicious access. By itself, this infrastructure is not secure. It requires what is known in security terminology as hardening. Hardening is accomplished through various means, including activation of operating system features, third-party tools, and constant monitoring and enforcement of security procedures and policies.

How much hardening is required depends on each site's needs and levels of risk tolerance. However, CSC can help you achieve the necessary level of security.

One of the most vulnerable spots of the Companion products' infrastructure is the Web server because it must be exposed to the Internet to be accessible. For this reason, organizations tend to focus most of their security efforts on perimeter defenses, as this document suggests. However, the importance of considering security threats posed by internal risks cannot be stressed enough.

No site can ever be 100 percent safe, but the following list of steps can help to improve the security of your Web site.

Hardening Your Web Site

Measures you can take to strengthen the security of your Web site include implementing a firewall and establishing a virtual private network. The following list is a selected sample with references to detailed information.

Install a Firewall System

A firewall is a must for any site connected to an untrusted network like the Internet. Firewalls help secure traffic moving in and out of your network from attempts by intruders to access unauthorized information.

In addition to providing a single choke point where security and audit functions can be imposed, firewalls also act as an effective tracing tool. The firewall software generates summaries regarding the types and amounts of traffic passing through the site and how many times intruders try to break into the system.

Firewalls work as gatekeepers, establishing rules for the kinds of data that can pass and who can access that data. Although firewalls vary from manufacturer to manufacturer the best firewalls come with a wide range of strategies to provide the best protection with the greatest level of control.

A firewall provides a per-application control mechanism for IP traffic, including standard TCP and UDP Internet applications, multimedia applications, and database support. It can examine layer 3 and layer 4 traffic and either permit or deny the traffic based on policies configured within the firewall. A generated audit trail allows you to monitor the traffic passing through the network.

Most modern firewalls are hardware-based to prevent intruders from modifying the code or the operating system. They also come with network address translation (NAT) as a standard feature that allows convenient access to specific servers behind your firewall without revealing the true IP address of the server.

Establish a Virtual Private Network

Virtual private networks (VPNs) use dedicated secure paths, or tunnels, that ease the transmission of data between the local point of presence (POP) and the corporate network. Network vendors now offer a class of VPN products that tunnel and encrypt data for secure passage over shared data networks. Because of security and performance concerns, organizations have been hesitant to use the Internet for their corporate network access. However, the newer generations of VPN technology are helping to solve these problems.

A typical VPN configuration establishes a secure tunnel between the network access server and a tunnel-terminating device on the local network. From the user's perspective, a dial-up session is initiated to a local POP where the ISP authenticates the user and establishes a tunnel through its Internet cloud. This cloud terminates at the edge of the user's corporate LAN. The IPX and IP packets are encapsulated in a tunneling protocol such as PPTP or L2F. An IP packet containing the address of the corporate network, the packet's ultimate destination, packages these packets.

Even though the network is transmitting data in a somewhat more complicated fashion, the VPN user is not required to know any additional networking technology.

A very secure implementation of a Companion product Web site would look something like the one depicted in Figure 1.

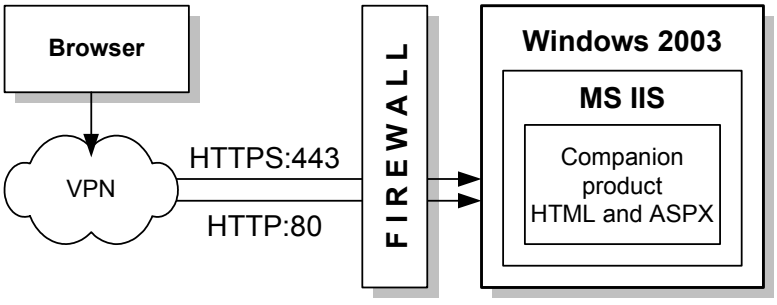


Figure 1. Secure implementation

There are also a number of administrative steps you must take to enhance the security of your Companion product Web site.

Secure Windows Server and Internet Information Server

The Companion products (C.0) release is supported on the Windows 2003 operating system. Windows 2003 includes Internet Information Server 6.0.

Note: *Microsoft has procedures in place to announce the availability of patches for any recently discovered vulnerabilities.*

In today's market, a Web site is most likely to be infiltrated because of human error, such as the administrator not following best security practices or not monitoring the site, rather than inherent weaknesses with the operating system. Microsoft Windows is no exception.

The following Microsoft Web pages are a "must read" for any administrator responsible for securing a Windows operating system environment:

- ***Windows Server 2003 Security Guide***
  http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx
- ***Subscribe to the Microsoft Security Notification Service***
  http://www.microsoft.com/technet/security/bulletin/notify.mspx
- ***Open Web Application Security Project (OWASP) Top 10 Vulnerabilities***
  http://www.owasp.org/index.php/Top_10_2007#Downloadable_Versions

WARNING: Web Administrator Must Consider These Security Vulnerabilities

The following list is not a comprehensive one, but it shows the common security aspects to be considered. It is based on the experiences of implementing customers.

Microsoft has been diligent dealing with security problems and improving a developing operating system, but each network owner must take responsibility for ensuring his own individual and unique environment is secure. Therefore, the Web administrator must review the following areas when securing a Web site:

- **Physical Security of Equipment**—This encompasses every aspect of the computer network, not just the servers. Cables, hubs, routers, client machines, etc. are extremely important to consider and need to be protected from people who should not have access to them. It is also important to disable any unused hardware devices, such as serial and parallel ports.
- **Password Security**—This includes often overlooked issues such as the number of retries to defeat dictionary attacks and brute force attacks. You should also rename the administrator account and create a new account named Administrator as a decoy for hacking detection.
- **User Security**—User security is extremely important. It means keeping the users in their own virtual worlds. The Companion products enforce role profiles to prevent users from viewing other users' data. However, both users and hackers can access the server by other means, so it is critical to be very careful when adding users to the Administrators group.
- **Network Security**—Network security remains one of the biggest threats to Web sites. Due to the wild growth of the Internet, network security is an increasingly important issue for system administrators. It involves protecting the network from remote attacks by setting up intrusion detection systems and constantly checking the network for leaks.
- **Operating System Procedures**—Procedures such as applying the latest service pack and/or hot fixes should be observed. Service packs contain or enable security fixes. Hot fixes specifically address security issues. Care must be taken when applying fixes. Testing the fix and its impact to the Companion products is a must before introducing it into your production environment.
- **Social Engineering**—http://www.cisco.com/web/about/security/intelligence/mysdn-social-engineering.html
    - Social engineering is evolving so rapidly that technology solutions, security policies, and operational procedures alone cannot protect critical resources. Even with these safeguards, hackers commonly manipulate employees into compromising corporate security. Victims might unknowingly reveal the sensitive information needed to bypass network security, or even unlock workplace doors for strangers without identification. While attacks on human judgment are immune to even the best network defense systems, companies can mitigate the risk of

social engineering with an active security culture that evolves as the threat landscape changes.

- A security-aware culture must include ongoing training that consistently informs employees about the latest security threats, as well as policies and procedures that reflect the overall vision and mission of corporate information security. This emphasis on security helps employees understand the potential risk of social-engineering threats, how they can prevent successful attacks, and why their role within the security culture is vital to corporate health. Security-aware employees are better prepared to recognize and avoid rapidly changing and increasingly sophisticated social-engineering attacks, and are more willing to take ownership of security responsibilities.

We recommend taking advantage of the resources Microsoft and other industry leaders provide. But you must use the resources while considering your business requirements and security policies.

Secure SQL Server

This section describes the steps that need to be taken for securing SQL server. It covers the standard security practices for changing configuration settings in SQL Server to improve database security.

Best Practices

1. The **system administrator account 'sa'** in SQL server must never be set to blank. This is a huge security risk that makes the server vulnerable to viruses.

2. The **SQLserver login** that is created to access a Companion product database (isol_app) should not be added to the "System Administrators" role in SQL Server.

3. **SQL Server Clean Up**—Remove Northwind and Pubs databases. Removing these databases conserves resources and improves efficiency.

4. **SQL Server 2005 Security Best Practices Document**—
http://www.microsoft.com/technet/prodtechnol/sql/2005/sql2005secbestpract.mspx

Use a Tougher Password Encryption

Access to a Companion Product site should be implemented using Secured Sockets Layer (SSL), a security protocol developed by the Netscape Communications Corporation to encrypt sensitive data and verify server authenticity. It is used through the HTTPS protocol.

- See Communications Framework: Enabling SSL for Apache Tomcat or Communications Framework: SSL Certificate Set-Up Using IBM WebSphere for instructions on enabling SSL through Communications Framework.

There are trade-offs to using SSL. It slows down performance and requires you to buy a digital X.509 certificate from specialized certificate companies like Verisign, Thawte, United Postal Service, or GTE.

Web Enabled Security and SSL

Digital certificates are electronic files that uniquely identify people and resources over networks such as the Internet. Digital certificates also enable secure, confidential communication between two parties.

A trusted third party called a certification authority (CA) issues certificates. Much like the passport office, the CA validates the certificate holders' identity and "signs" the certificate so it cannot be forged or tampered with. Once a CA has signed a certificate, the holder can present the certificate to people, Web sites, and network resources to prove his or her identity and establish encrypted, confidential communications.

A certificate typically includes information about its owner and the CA that issued it. This information can include:

- The name of the holder and other unique identification information, such as the URL of the Web server using the certificate or the individual's email address.
- The holder's public key, which can be used to encrypt sensitive information for the certificate holder.
- The name of the certification authority that issued the certificate.
- A serial number.

- The validity period, or lifetime, of the certificate (a start and end date).

The issuing CA digitally signs this information when the certificate is created. The CA's signature on the certificate is like a tamper-detection seal on a bottle of pills—any tampering with the contents can be easily detected.

Digital certificates are based on public-key cryptography, which uses a pair of keys for encryption and decryption. With public-key cryptography, matched public and private keys work in pairs. In cryptographic systems, the term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information.

The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. Since these keys work only as a pair, an operation (encryption, for example) done with the public key can only be undone (decrypted) with the corresponding private key and vice versa. A digital certificate securely binds a user's identity, as verified by a trusted third party (a CA), with the public key.

Web Server Certificates

A Web server certificate authenticates the identity of a Web site to visiting browsers. When a person using a browser wants to send confidential information to a Web server, that person's browser seeks out the Web server's digital certificate. The browser uses the certificate – which contains the Web server's public key – to authenticate the identity of the Web server (the Web site) and encrypt information for the server using secure sockets layer (SSL) technology.

Because only the Web server has access to its private key, only the server can decrypt the information. This allows the information to remain confidential and tamper-proof while in transit across the Internet.

CA Certificates

A CA certificate identifies a certification authority. CA certificates are similar to other digital certificates except they are self-signed. CA certificates determine whether to trust certificates issued by the CA.

The CA certificate authenticates and validates the Web server certificate. When a Web server certificate is presented to a browser, the browser uses the CA certificate to determine whether to trust the Web server's certificate. If the server certificate is valid, the SSL session proceeds. If the server certificate is not valid, the server certificate is rejected and the SSL session stops. CA certificates come preinstalled on most popular Web browsers, including Microsoft and Netscape.

Secure Sockets Layer (SSL)

Secure sockets layer (SSL) technology is a security protocol. It is today's de facto standard for securing communications and transactions across the Internet. SSL is implemented in all the main browsers and Web servers, and it plays a major role in today's e-commerce and e-business activities on the Web.

The SSL protocol uses digital certificates to create a secure, confidential communications pipe between two entities. Data transmitted over an SSL connection cannot be tampered with or forged without the two parties becoming immediately aware of the tampering.

Once the process of identifying two parties who want to establish an SSL connection is complete and a secure communications pipe is established, the client's browser and the Web server can now use the session key to send encrypted information back and forth with the knowledge that communications are confidential and tamper-proof. The entire process of establishing the SSL connection is usually transparent to the user and takes only seconds.

A key or padlock icon in the lower corner of the browser window identifies the security mode of a browser. When the browser is running in normal mode, the key looks broken, or the padlock looks open. Once an SSL connection is established, the key becomes whole, or the padlock becomes closed, indicating the browser is now in secure mode.

SSL is supported by a vast majority of browsers. This means almost anyone with a browser can reap the benefits of SSL encryption. SSL is also incorporated into most Web servers on the market.

Server Implementation When Implementing Several Companion Products

Note: *Read this guide in conjunction with* ***Installation Readiness Assessment Guide*** *for each CSC Companion product you are installing.*

The CSC Companion products are not Web security applications; they are financial applications that rely on an existing Web security infrastructure. By itself, the Companion products authorize only the users of the application and restricts their use based on profiles defined by the system administrator.

Companion Product	**Abbreviation in** Security Port Access **Table**
Advanced Claims	AC
Agency Link	AL
Business Intelligence	BI
Document Production	DP
Information Ordering	IO
Media Management	MM
POINT IN	PI
Underwriting	UW

Any financial institution that establishes an Internet presence through a Companion product site (one that uses Advanced Claims, Agency Link, Business Intelligence, Information Ordering, and/or Underwriting) must take steps to ensure the systems they use or own contain adequate security measures. These measures help limit the possibility of unintended distribution of confidential information and the potential for fraud-related losses.

The Internet is designed as an open system, based on the premise of free access and communication between participating computer systems. While there is no guarantee of complete safety and invulnerability, every effort must be made to provide a safe, secure, and protected platform for financial activity.

The details of placing Companion product servers in relation to your firewalls and associating the servers to specific domain(s) depend upon your specific security requirements. Based on the development of the Companion products and the protocols used between the servers, the following pages outline two of many implementation models. Following the implementation models are brief instructions for hardening, as well as references to useful articles and links about security.

In distributed applications such as the Companion products, other resources require protection in addition to the Web and Application servers. A recommended practice is to put another firewall between the Web/Application servers and the database servers, creating a "demilitarized zone" or DMZ in the event your perimeter defenses are compromised and an intruder gains access to the Web or Application severs. Communication protocols between the some of the Companion product servers require opening selected ports through firewalls from the DMZ to the internal network. This is applicable to all implementation models.

Several of the Companion products (Agency Link, Information Ordering, and Underwriting) use a component called Communications Framework (CFW) that resides on the CFW server. The CFW server is for message communications to and from enterprise-specific services. Communication includes transformation and transportation of the messages. Not all of the functions of these three Companion products require this server. Please contact your CSC services representative to identify the functions that require CFW.

The Communications Framework server can reside within your DMZ or behind your corporate firewall – firewall 2.

Security Port Access

The following table lists security ports you may need to open for customizing your implementation. Y = Needed. Blank = Not needed.

Ref #	Description	From -> To	Connection Type	Default Port Number(s)	AC	AL	BI	DP	IO	MM	PI	UW
1	Web access	Client -> Web	HTTP/ HTTPS	80,443		Y	Y	Y	Y	Y		Y
2	Web access	Browser -> Citrix	TCP	1494, 2598	Y							
3	.NET remoting (see footnote "B")	Web -> App	TCP	4758 (config-urable)		Y		Y	Y	Y		Y
4	.NET remoting	Web -> App	TCP	Configurable (any unused port)				Y				
5	SQL Server	Web -> DB	TCP/ODBC	1433		Y	Y					
6	SQL Server	App -> DB	TCP/ODBC	1433	Y	Y		Y		Y		
7	CFW access	App -> CFW	HTTP	8080		Y			Y			Y
8	CFW access	CFW ->Web	HTTP/ SOAP	80 (see footnote "A")		Y			Y			Y
9	Mapped drives	App -> Sys-tem i	TCP	Mapped drives 135, 139, 445				Y				
10	Mapped drives	App -> Sys-tem i	UDP	Mapped drives 135, 139, 445				Y				
11	Inquiry load	POINT -> App	FTP	20, 21		Y			Y			Y
12	Series II FTP	Host -> App	FTP	20, 21		Y		Y	Y			Y
13	Database access	DB -> Sys-tem i	TCP	449, 8470, 8471, 8472, 8475, 8476			Y					
14	Database access	Web/App -> System i	TCP	449, 8470, 8471, 8472, 8475, 8476	Y							
15	Download from System i	System i -> DB	FTP	20, 21			Y					
16	Trigger file	DB -> Web/App	FTP	20, 21			Y					

Ref #	Description	From -> To	Connection Type	Default Port Number(s)	AC	AL	BI	DP	IO	MM	PI	UW
17	POINT host communication	CFW -> POINT	TCP	23, 449, 8470, 8471, 8475, 8476							Y	
18	Series II host communication	CFW -> CTG	TCP	Configurable in CTG; default 2006 used by CFW.		Y						
19	Series II host communication	CTG -> Host	TCP	Configurable in CTG; determined by host.		Y						
20	Server-Side Rating communication	CFW -> App	HTTP/ SOAP	80		Y						
21	Single Sign-On (SSO)	Web -> SSO	TCP	8080 or SSL 8443		Y	Y			Y		
22	Single Sign-On (SSO) Active Directory authentication	SSO -> AD	TCP	SSL 636, UDP 88 or 389, UDP 88		Y	Y			Y		
23	Single Sign-On (SSO)	SSO -> Browser	HTTP	8080 or SSL 8443		Y	Y			Y		
24	SSO System i Authentication	SSO -> System i	TCP	23, 449, 8470, 8471, 8475, 8476		Y	Y			Y		
25	POINT host communication			8471							Y	
26	Web service	PI Suite -> MM/DP Web	TCP	80				Y		Y	Y	
27	IO Scheduler Listener	Scheduler Listener Web -> Vendor	TCP	Configurable with vendor (across business-to-business VPN)					Y			
28	POINT host communication	POINT -> CFW	TCP	449, 8475, 8476		Y			Y			Y
29	Jacada Web Access	Browser -> Jacada Server	TPC	80, 1100, 1101							Y	

Footnotes and Other Important Considerations

A. About Port 80

If you have any of the following functions enabled or products installed, you must open port 80 between CFW and the Web server.

- Agency Link Cancellations (only needed for Series II implementations)
- Underwriting (C.0)
- Information Ordering (C.0)

B. How To Configure Remoting

For Agency Link, Information Ordering, and Underwriting

For issue 86936, the settings were moved into the web.config file. The new item is the 'webcallbackport', which specifies the port on the Web server used for remoting. By contrast, the 'serverport' item is the Application server port used for remoting.

```
<!-- Issue 86936 Begin -->
<add key="remotingenabled" value="false"/>
<add key="remoteserver" value="localhost"/>
<add key="serverport" value="4758"/>
<!-- This is the remoting callback port for the web server.
If you have remoting enabled but are only using one
machine, the <webcallbackport> should be set to a different
port than the <serverport>.  If 2 machines are used, they
can be set to the same port. -->
<add key="webcallbackport" value="4759"/>
<!-- Issue 86936 End -->
```

For Document Production

To configure remoting for Document Print, locate web.config in the <drive>:\<target>\DocPrintService\WebServer\WebService folder.

Specify an available port for "Port" and set "remotingenable" to "true." If remoting is enabled for a single server configuration, the "callbackport" should be set to a different port than the port specified in "Port." For a two-server configuration, the same port value can be used.

```
<appSettings>
      <add key="Port" value="60031"/>
      <add key="callbackport" value="60032"/>
      <add key="remoteserver" value="localhost"/>
      <add key="remotingenabled" value="false"/>
```



```
</appSettings>
```

For Media Management

In the Application server MediaMgtApp.xml file in the "Remoting" section, specify the following:

- Port – Application server remoting port
- EnsureSecurity – Channel security setting (either Y or N)

In the Web server MediaMgtWeb.xml file in the "Remoting" section, specify the following:

- Enabled – Flag to enable remoting (either Y or N).
- Server – Application server name or IP address.
- Port – Application server remoting port. This must equal the Application server value.
- CallbackPort – Web server remoting port for callback to the Web pages. This value should be different from the Port and WSCallbackPort values.
- WSCallbackPort – Web server remoting port for callback to the Web service. This value should be different from the Port and CallbackPort values.
- EnsureSecurity – Channel security setting (either Y or N). This must equal the Application server value.
- SingleServer – Set to Y for a single-server installation. Set to N for a two-server installation.

C. CAUTION for Agency Link and Information Ordering when interfacing with ChoicePoint

ChoicePoint does not offer an encrypted protocol for communication. Clients should take measures to ensure data is protected by using a dedicated communication line or Virtual Private Network to ChoicePoint.

D. You may configure error messages that are generated by IIS

When you have a Web site, your users can encounter errors such as "Page not found" or "Page 404 Error." You can customize the text of these error messages to make them more user-friendly and to prevent a technical error from revealing more about your web-site than you might want. Messages can be modified through Windows IIS. Two related articles can be found at the following URLs.

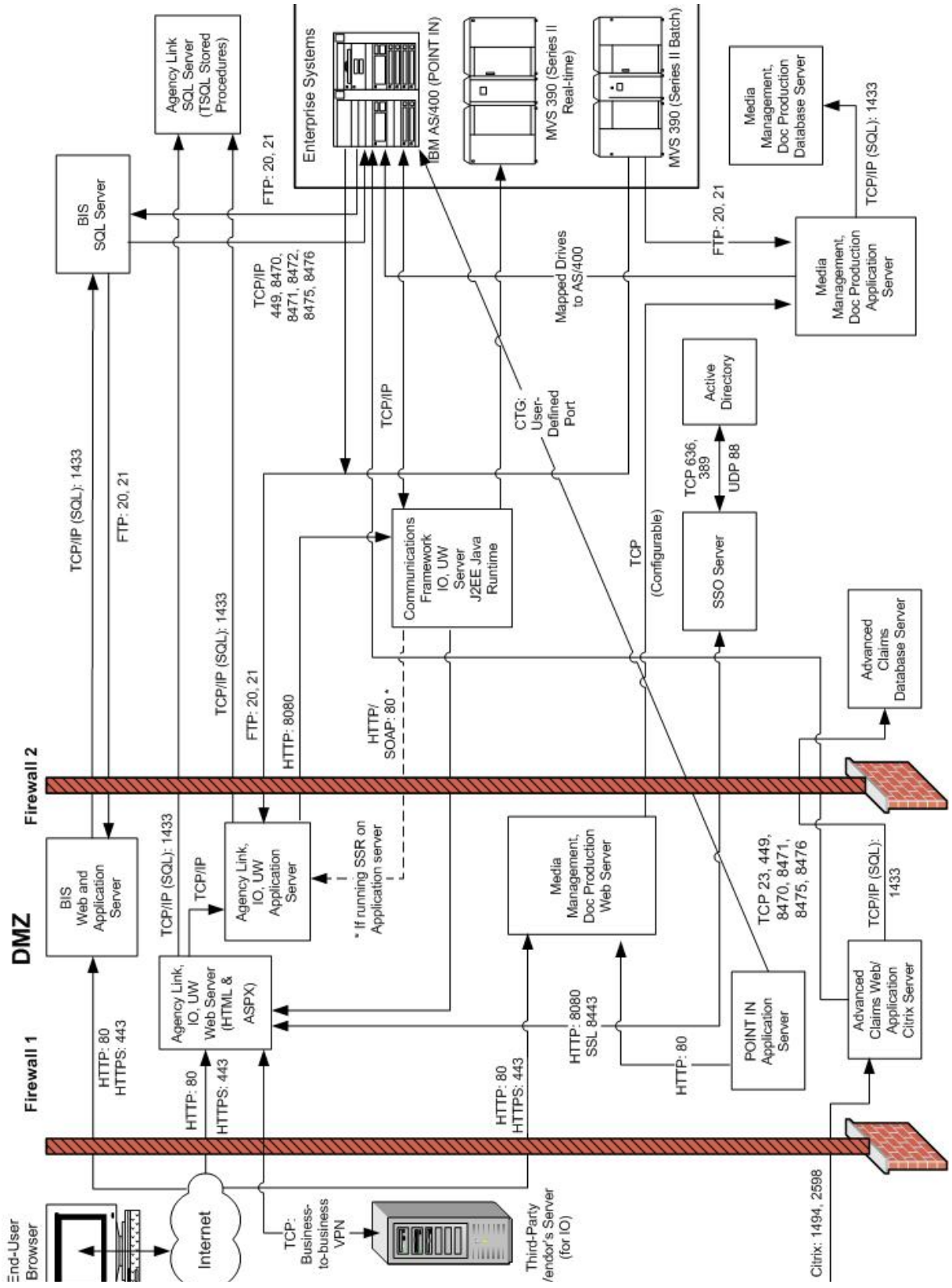
- IIS.net: Using Custom Errors in IIS: Internet Information Server (IIS) http://www.iis.net/go/17
- IIS.net : Understanding Custom and Detailed Errors http://www.iis.net/go/994

Implementation Model: All Companion Products

The following diagram illustrates the configuration recommended for both performance and space considerations when implementing multiple Companion products. The advantages to separate servers are that performance is optimized and risks are minimized. For example, if one application has a problem, then other applications are not directly affected.

If you need to consolidate for cost considerations, other configurations are possible. For instance, the Media Management Web piece can be housed on your Agency Link Web server.

In any case, make sure you have a database maintenance plan in place. Back up servers on a regular schedule. On database servers, run maintenance plans to back up the databases.


Agency Link SQL Server (TSQL Stored Procedures)
Enterprise Systems
IBM AS/400 (POINT IN)
MVS 390 (Series II Real-time)
MVS 390 (Series II Batch)
Media Management, Doc Production Database Server
BIS SQL Server
FTP: 20, 21
TCP/IP (SQL): 1433
TCP/IP 449, 8470, 8471, 8472, 8475, 8476
Mapped Drives to AS/400
Media Management, Doc Production Application Server
Active Directory
CTG User-Defined Port
TCP/IP
TCP 636, 389
UDP 88
Communications Framework IO, UW Server J2EE Java Runtime
SSO Server
TCP (Configurable)
Advanced Claims Database Server
HTTP/ SOAP: 80 *
HTTP: 8080
Firewall 2
DMZ
Firewall 1
BIS Web and Application Server
Agency Link, IO, UW Application Server
* If running SSR on Application server
Media Management, Doc Production Web Server
TCP 23, 449, 8470, 8471, 8475, 8476
Agency Link, IO, UW Web Server (HTML & ASPX)
HTTP: 80 HTTPS: 443
HTTP: 8080 SSL 8443
POINT IN Application Server
Advanced Claims Web/ Application Citrix Server
Internet
End-User Browser
TCP: Business-to-business VPN
Third-Party Vendor's Server (for IO)
Citrix: 1494, 2598

Two Possible Models

There are two implementation configurations that may be used with the Companion products. Model one has individual Web and Application servers in the DMZ. Model two has the Web and Application servers on one machine in the DMZ.

Some of the Companion products can be implemented with either model one or two. However, some of the products can only be implemented one way. For details and diagrams, see—

- Advanced Claims Server Implementation
- Agency Link Server Implementation
- Business Intelligence Server Implementation
- Document Production Server Implementation
- Information Ordering Server Implementation
- Media Management Server Implementation
- POINT IN Server Implementation
- Underwriting Server Implementation

Advanced Claims Server Implementation

Note: *Read this in conjunction with the Advanced Claims* ***Installation Readiness Assessment Guide****.*

Advanced Claims is not a Web security application; it is a financial application that relies on an existing Web security infrastructure. By itself, Advanced Claims authorizes only the users of the application and restricts their use based on profiles defined by the system administrator.

Any financial institution that establishes an Internet presence through Advanced Claims must take steps to ensure the systems they use or own contain adequate security measures. These measures help limit the possibility of unintended distribution of confidential information and the potential for fraud-related losses.

The Internet is designed as an open system, based on the premise of free access and communication between participating computer systems. While there is no guarantee of complete safety and invulnerability, every effort must be made to provide a safe, secure, and protected platform for financial activity.

The details of placing Advanced Claims servers in relation to your firewalls and associating the servers to specific domain(s) depend upon your specific security requirements. Based on the development of Advanced Claims and the protocols used between the servers, the following pages outline two of many implementation models. Following the implementation models are brief instructions for hardening, as well as references to useful articles and links about security.

In a distributed application such as Advanced Claims, other resources require protection in addition to the Web and Application servers. A recommended practice is to put another firewall between the Web/Application servers and the database servers, creating a "demilitarized zone" or DMZ in the event your perimeter defenses are compromised and an intruder gains access to the Web or Appli-

cation severs. Communication protocols between the Advanced Claims servers require opening selected ports through firewalls from the DMZ to the internal network. This is applicable to all implementation models.

Security Port Access

The following table lists security ports you may need to open for customizing your implementation of Advanced Claims.

Ref #	Description	From -> To	Connection Type	Default Port Number(s)
2	Web access	Browser -> Citrix	TCP	1494, 2598
6	SQL Server	App -> DB	TCP/ODBC	1433
14	Database access	Web/App -> System i	TCP	449, 8470, 8471, 8472, 8475, 8476

Footnotes and Other Important Considerations

D. You may configure error messages that are generated by IIS

When you have a Web site, your users can encounter errors such as "Page not found" or "Page 404 Error." You can customize the text of these error messages to make them more user-friendly and to prevent a technical error from revealing more about your web-site than you might want. Messages can be modified through Windows IIS. Two related articles can be found at the following URLs.

- IIS.net: Using Custom Errors in IIS: Internet Information Server (IIS) http://www.iis.net/go/17
- IIS.net : Understanding Custom and Detailed Errors http://www.iis.net/go/994

Implementation – Production Model

Install both the Web and Application server components on one physical server in a workgroup and place the server in the DMZ area. Place the database server behind your second firewall.

a Microsoft provides a set of instructions for securing a Windows operating system. Follow the link below:

http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch00.mspx.

b For an illustration, see Figure 2.

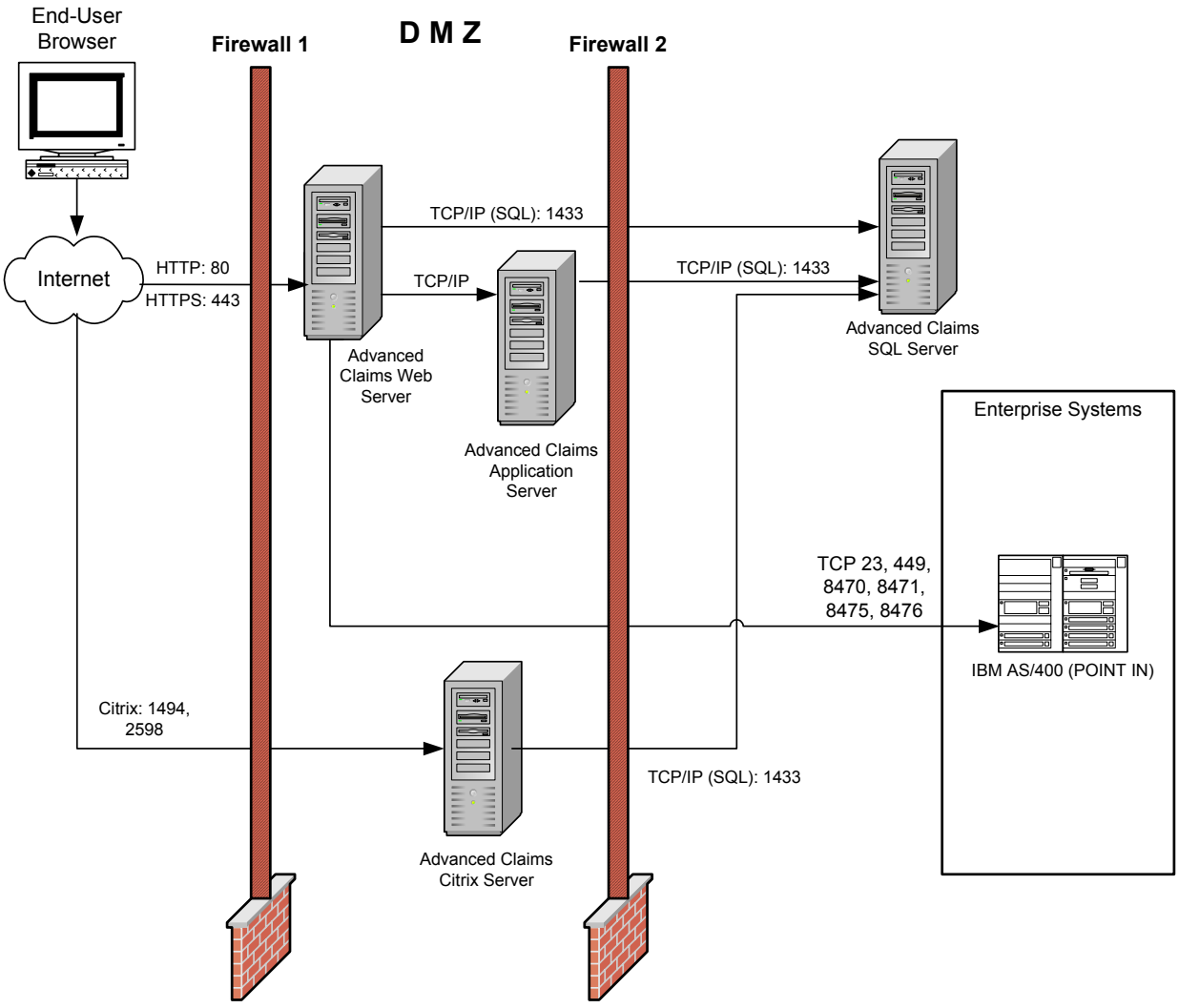


Figure 2. Detail of model

Advanced Claims requires a different configuration than the other Companion products.

Agency Link Server Implementation

Note: *Read this in conjunction with the Agency Link* ***Installation Readiness Assessment Guide****.*

Agency Link is not a Web security application; it is a financial application that relies on an existing Web security infrastructure. By itself, Agency Link authorizes only the users of the application and restricts their use based on profiles defined by the system administrator.

Any financial institution that establishes an Internet presence through Agency Link must take steps to ensure the systems they use or own contain adequate security measures. These measures help limit the possibility of unintended distribution of confidential information and the potential for fraud-related losses.

The Internet is designed as an open system, based on the premise of free access and communication between participating computer systems. While there is no guarantee of complete safety and invulnerability, every effort must be made to provide a safe, secure, and protected platform for financial activity.

The details of placing Agency Link servers in relation to your firewalls and associating the servers to specific domain(s) depend upon your specific security requirements. Based on the development of Agency Link and the protocols used between the servers, the following pages outline two of many implementation models. Following the implementation models are brief instructions for hardening, as well as references to useful articles and links about security.

In a distributed application such as Agency Link, other resources require protection in addition to the Web and Application servers. A recommended practice is to put another firewall between the Web/Application servers and the database servers, creating a "demilitarized zone" or DMZ in the event your perimeter defenses are compromised and an intruder gains access to the Web or Appli-

cation severs. Communication protocols between the Agency Link servers require opening selected ports through firewalls from the DMZ to the internal network. This is applicable to all implementation models.

Agency Link uses a component called Communications Framework (CFW) that resides on the CFW server. The CFW server is for message communications to and from enterprise-specific services. Communication includes transformation and transportation of the messages. Not all of the Agency Link-specific functions require this server. Please contact your CSC services representative to identify the functions that require CFW.

The Communications Framework server can reside within your DMZ or behind your corporate firewall – firewall 2.

Security Port Access

The following table lists security ports you may need to open for customizing your implementation of Agency Link.

Ref #	Description	From -> To	Connection Type	Default Port Number(s)
1	Web access	Client -> Web	HTTP/HTTPS	80,443
3	.NET remoting (see footnote "B")	Web -> App	TCP	4758 (configurable)
5	SQL Server	Web -> DB	TCP/ODBC	1433
6	SQL Server	App -> DB	TCP/ODBC	1433
7	CFW access	App -> CFW	HTTP	8080
8	CFW access	CFW ->Web	HTTP/SOAP	80 (see footnote "A")
11	Inquiry load	POINT -> App	FTP	20,21
18	Series II host communication	CFW -> CTG	TCP	Configurable in CTG; default 2006 used by CFW.
19	Series II host communication	CTG -> Host	TCP	Configurable in CTG; determined by host.
20	Server-Side Rating communication	CFW -> App	HTTP/ SOAP	80
21	Single Sign-On (SSO)	Web -> SSO	TCP	8080 or SSL 8443

Ref #	Description	From -> To	Connection Type	Default Port Number(s)
22	Single Sign-On (SSO) Active Directory authentication	SSO -> AD	TCP	SSL 636, UDP 88 or 389, UDP 88
23	Single Sign-On (SSO)	SSO -> Browser	HTTP	8080 or SSL 8443
24	SSO System i Authentication	SSO -> System i	TCP	23, 449, 8470, 8471, 8475, 8476
28	POINT host communication	POINT -> CFW	TCP	449, 8475, 8476

Footnotes and Other Important Considerations

A. About Port 80

If you have any of the following functions enabled or products installed, you must open port 80 between CFW and the Web server.

- Agency Link Cancellations (only needed for Series II implementations)
- Underwriting (C.0)
- Information Ordering (C.0)

B. How To Configure Remoting

For issue 86936, the settings were moved into the web.config file. The new item is the 'webcallbackport', which specifies the port on the Web server used for remoting. By contrast, the 'serverport' item is the Application server port used for remoting.

```
<!-- Issue 86936 Begin -->
<add key="remotingenabled" value="false"/>
<add key="remoteserver" value="localhost"/>
<add key="serverport" value="4758"/>
<!-- This is the remoting callback port for the web server.
If you have remoting enabled but are only using one
machine, the <webcallbackport> should be set to a different
port than the <serverport>.  If 2 machines are used, they
can be set to the same port. -->
<add key="webcallbackport" value="4759"/>
<!-- Issue 86936 End -->
```

C. CAUTION for Agency Link when interfacing with ChoicePoint

ChoicePoint does not offer an encrypted protocol for communication. Clients should take measures to ensure data is protected by

using a dedicated communication line or Virtual Private Network to ChoicePoint.

D. You may configure error messages that are generated by IIS

When you have a Web site, your users can encounter errors such as "Page not found" or "Page 404 Error." You can customize the text of these error messages to make them more user-friendly and to prevent a technical error from revealing more about your web-site than you might want. Messages can be modified through Windows IIS. Two related articles can be found at the following URLs.

- IIS.net: Using Custom Errors in IIS: Internet Information Server (IIS) http://www.iis.net/go/17
- IIS.net : Understanding Custom and Detailed Errors http://www.iis.net/go/994

Implementation – Production Model One

Place both the Web and Application servers in a DMZ area and join to a domain consisting of only those two machines. Place the database server behind your second firewall.

a You can place the Communications Framework server on either side of the second firewall.

b Microsoft provides a set of instructions for securing a Windows operating system. Follow the link below for instructions:

http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch00.mspx.

c For more information, see Figure 3.

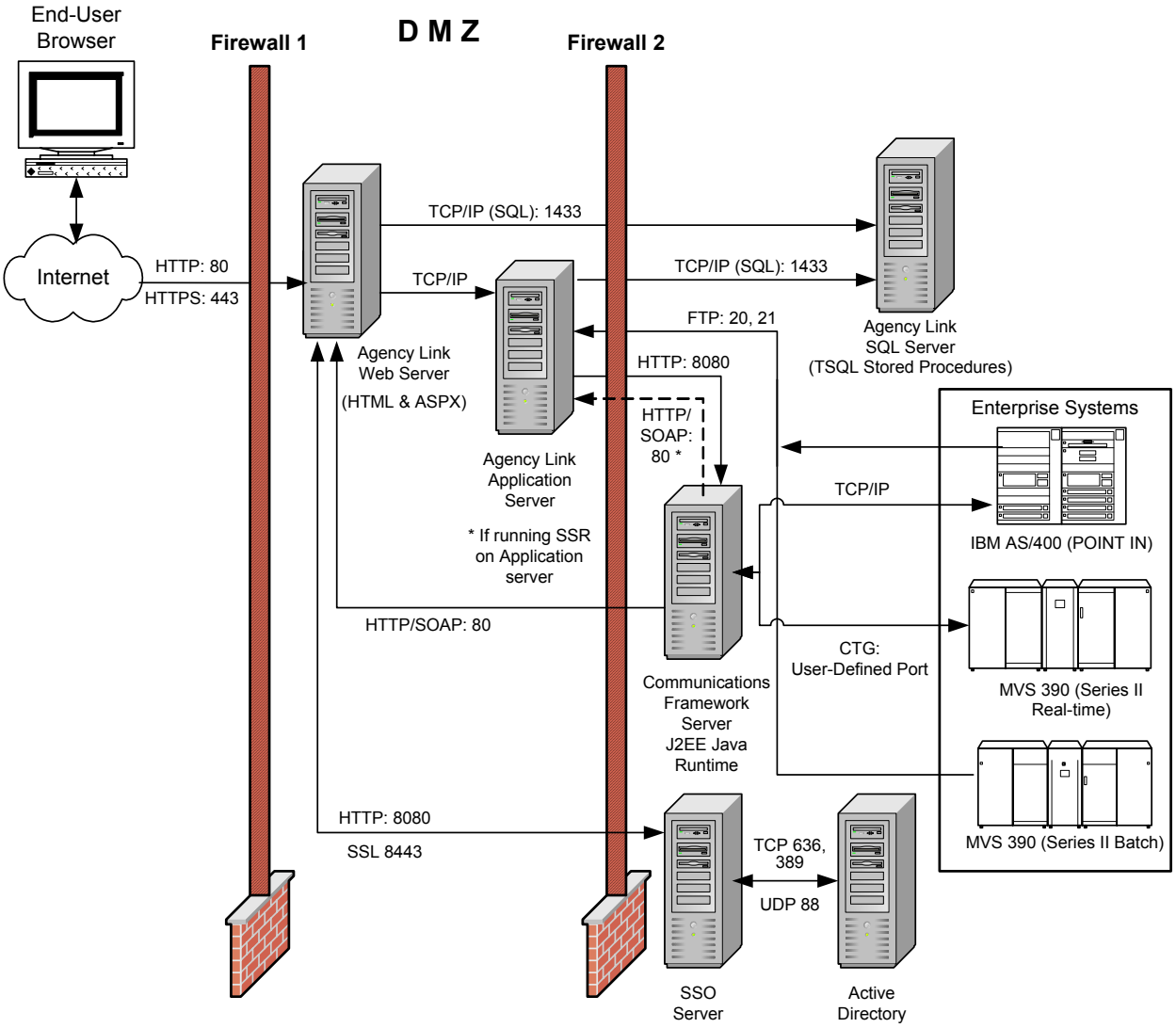


Figure 3. Detail of Implementation Model One

Below is additional information to secure your application and operating system environment following Implementation Model One:

1 Place firewall 2 between the Companion products Web and Application servers and the database server as described in the following articles:

- ***Connections to SQL Server Over the Internet*** http://msdn2.microsoft.com/en-us/library/aa213767.aspx.
- ***INF: TCP Ports Needed for Communication to SQL Server Through a Firewall*** http://support.microsoft.com/default.aspx?scid=kb;EN-US;q287932.

2 Do not allow any trust relationship between the Web/Application domain and other domains within firewall 2.

3 Secure the Web and Application servers in the DMZ area by turning off all unused services. The list below indicates the services that are used by Agency Link. Do not turn off these services.

Server	Service	Comments
Web server	Microsoft Distributed Transaction Coordinator (MSDTC)	Required for Agency Link
Web server	IIS Admin Service	Required for a product that has a Web piece
Web Server	World Wide Web (WWW)	Required for a product that has a Web piece
Web server	Microsoft SMTP Service	Required for any product that uses email notification. Used for Agency Link features such as NOL alert, email endorsements, and Message Center email notification.
Application server	Microsoft Distributed Transaction Coordinator (MSDTC)	Required for Agency Link
Application server	IIS Admin Service	Required for Agency Link
Application server	Microsoft SMTP Service	Required for Agency Link
Application server	FTP Publishing Service	Needed if files are transferred between enterprise host and some other server

4 Where applicable: Harden the Web and Application servers by setting the appropriate virtual directory permissions.

- Web server permissions:
  - The Web administrator must have update permission to the Site.css file. This file can be located in several directories and varies based on the enterprise system you are interfacing with (POINT IN or Series II). This step is required only if you plan to use the Agency Link stylesheet wizard located within the Administration subsystem.
  - The .NET account (usually Network Service on Windows Server 2003 or ASP.Net on Windows XP) will need Modify permissions for the WEBSERVER\LogFiles folder.
  - The server administrator should have full access control.
- Application server permissions:

- The .NET account (usually Network Service on Windows Server 2003 or ASP.Net on Windows XP) will need Modify permissions for the APPSERVER\LogFiles folder.
- The server administrator should have full access control.

5 Based on the enterprise system you are interfacing with, grant additional NT File System (NTFS) permission exceptions as required.

a The POINT and Series II enterprise systems perform a nightly batch FTP data load. This FTP process writes data onto the Agency Link Application server in the APPSERVER\Inquiry\Procupld\upload directory. That batch user must have add and change permission for the directory.

b Series II enterprise system users of Agency Link create input and output files to the APPSERVER\Inquiry\Procupld\uploaddirectory. All Agency Link users must have the add and change permission or ensure the rating function is controlled by a Microsoft Transaction Server.

c Configure your firewalls to allow port traffic to communicate with the Agency Link components. See illustration (Figure 3.) for ports and protocols the Agency Link application requires. Externalized Authentication Details for Agency Link provides instructions and references for controlling port traffic through your firewalls.

6 If the Communications Framework is deployed behind firewall 2, no additional server hardening is required. But if it is deployed in the DMZ area, hardening of the CommFw directory must be performed. This directory resides within the Java Virtual Machine (JVM) directory structure chosen for your CFW server.

- Agency Link was developed and released using Apache Tomcat 4.1.29 release. That directory structure is <root>:\Program Files\Apache Group\Tomcat 4.1\webapps. The CommFw directory and all of its sub folders should be set with the read/execute NTFS permission for all users.

7 Assess the benefits and risks of implementing.

a Benefits

- User ID maintenance is simplified.
- Redundancy and scalability for additional servers are simplified.

b Risks

› In the event the Web server is compromised, all servers in the domain are at risk.

Implementation – Model Two

Install both the Web and Application server components on one physical server in a workgroup and place the server in the DMZ area. Place the database server behind your second firewall.

a You can place the Communications Framework server on either side of the second firewall.

b Microsoft provides a set of instructions for securing a Windows operating system. Follow the link below:

http://www.microsoft.com/technet/security/guidance/server-security/tcg/tcgch00.mspx.

c For an illustration, see Figure 4.

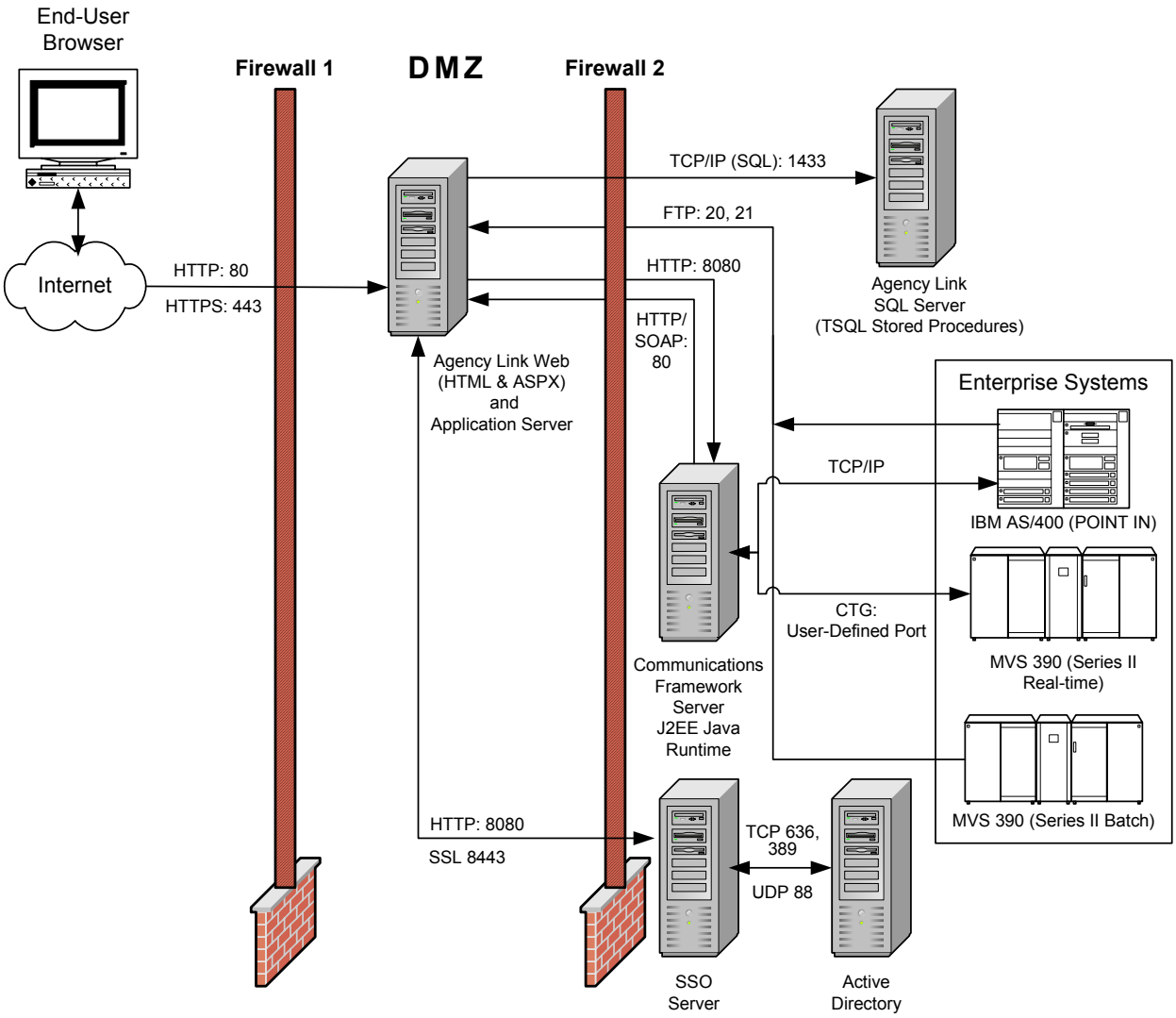


Figure 4. Detail of Implementation Model Two

Below is additional information to secure your application and operating system environment following Implementation Model Two.

1 Place firewall 2 between the Web/Application server and the database server as described in the following articles:

- ***Connections to SQL Server Over the Internet*** http://msdn2.microsoft.com/en-us/library/aa213767.aspx
- ***INF: TCP Ports Needed for Communication to SQL Server Through a Firewall*** http://support.microsoft.com/default.aspx?scid=kb;EN-US;q287932.

2 Secure the Web/Application server in the DMZ area by turning off all unused services. The list below indicates the services that are used by Agency Link. Do not turn off these services.

Server	Service	Comments
Web/Application server	Microsoft Distributed Transaction Coordinator (MSDTC)	Required for Agency Link
Web/Application server	IIS Admin Service	Required for a product that has a Web piece
Web/Application server	World Wide Web (WWW)	Required for a product that has a Web piece
Web/Application server	Microsoft SMTP Service	Required for any product that uses email notification. User for Agency Linkfeatures such as NOL alert, email endorsements, and Message Center email notification.
Web/Application server	FTP Publishing Service	Needed if files are transferred between enterprise host and some other server

3 Harden the Web and Application server by setting the appropriate virtual directory permissions.

- The Agency Link Web administrator must have update permission to the Site.css file. This file can be located in several directories and varies based on the enterprise system you are interfacing with (POINT IN or Series II). This step is required only if you plan to use the Agency Link stylesheet wizard located in the Administration subsystem.
- The .NET account (usually Network Service on Windows Server 2003 or ASP.Net on Windows XP) will need Modify permissions for the WEBSERVER\LogFiles and APPSERVER\LogFiles folders.
- The server administrator should have full access control.

4 Based on the enterprise system you are interfacing with, grant additional NT File System (NTFS) permission exceptions as required.

- The POINT and Series II enterprise systems perform a nightly batch FTP data load. This FTP process writes data onto the Agency Link Application server in the APPSERVER\Inquiry\Procupld\upload directory. That batch user must have add and change permission for the directory.
- Series II enterprise system users of Agency Link create input and output files to the APPSERVER\Inquiry\Procupld\upload-directory. All Agency Link users must have the add and

change permission or ensure the rating function is controlled by a Microsoft Transaction Server.

- Configure your firewalls to allow port traffic to communicate with the Agency Link components. See illustration (Figure 4.) for ports and protocols the Agency Link application requires.

5 If CFW is deployed behind firewall 2, no additional server hardening is required. But if it is deployed in the DMZ area, hardening of the CommFw directory must be performed. This directory resides within the Java Virtual Machine (JVM) directory structure chosen for your CFW server.

- Agency Link was developed and released using Apache Tomcat 4.1.29 release. That directory structure is <root>:\Program Files\Apache Group\Tomcat 4.1\webapps. The CommFw directory and all of its subfolders should be set with the read/execute NTFS permission for all users.

Important: *With this implementation model, scalability will be limited. User profiles must belong to a domain, not a workgroup, in order for scaling to work efficiently*.

Business Intelligence Server Implementation

Note: *Read this in conjunction with the Business Intelligence* ***Installation Readiness Assessment Guide****.*

Business Intelligence is not a Web security application; it is a financial application that relies on an existing Web security infrastructure. By itself, Business Intelligence authorizes only the users of the application and restricts their use based on profiles defined by the system administrator.

Any financial institution that establishes an Internet presence through Business Intelligence must take steps to ensure the systems they use or own contain adequate security measures. These measures help limit the possibility of unintended distribution of confidential information and the potential for fraud-related losses.

The Internet is designed as an open system, based on the premise of free access and communication between participating computer systems. While there is no guarantee of complete safety and invulnerability, every effort must be made to provide a safe, secure, and protected platform for financial activity.

The details of placing Business Intelligence servers in relation to your firewalls and associating the servers to specific domain(s) depend upon your specific security requirements. Based on the development of Business Intelligence and the protocols used between the servers, the following pages outline two of many implementation models. Following the implementation models are brief instructions for hardening, as well as references to useful articles and links about security.

In a distributed application such as Business Intelligence, other resources require protection in addition to the Web and Application servers. A recommended practice is to put another firewall between the Web/Application servers and the database servers, creating a "demilitarized zone" or DMZ in the event your perimeter defenses

are compromised and an intruder gains access to the Web or Application severs. Communication protocols between the Business Intelligence servers require opening selected ports through firewalls from the DMZ to the internal network. This is applicable to all implementation models.

Security Port Access

The following table lists security ports you may need to open for customizing your implementation.

Ref #	Description	From -> To	Connection Type	Default Port Number(s)
1	Web access	Client -> Web	HTTP/ HTTPS	80,443
5	SQL Server	Web -> DB	TCP/ODBC	1433
13	Database access	DB -> System i	TCP	449, 8470, 8471, 8472, 8475, 8476
15	Download from System i	System i -> DB	FTP	20, 21
16	Trigger file	DB -> Web/App	FTP	20, 21
23	Single Sign-On (SSO)	SSO -> Browser	HTTP	8080 or SSL 8443
24	SSO System i Authentication	SSO -> System i	TCP	23, 449, 8470, 8471, 8475, 8476

Footnotes and Other Important Considerations

D. You may configure error messages that are generated by IIS

When you have a Web site, your users can encounter errors such as "Page not found" or "Page 404 Error." You can customize the text of these error messages to make them more user-friendly and to prevent a technical error from revealing more about your web-site than you might want. Messages can be modified through Windows IIS. Two related articles can be found at the following URLs.

- IIS.net: Using Custom Errors in IIS: Internet Information Server (IIS) http://www.iis.net/go/17
- IIS.net : Understanding Custom and Detailed Errors http://www.iis.net/go/994

Implementation – Production Model

Place the Web/Application server in a DMZ area. Place the database server behind your second firewall.

a Microsoft provides a set of instructions for securing a Windows operating system. Follow the link below for instructions:

http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch00.mspx.

b For more information, see Figure 5.

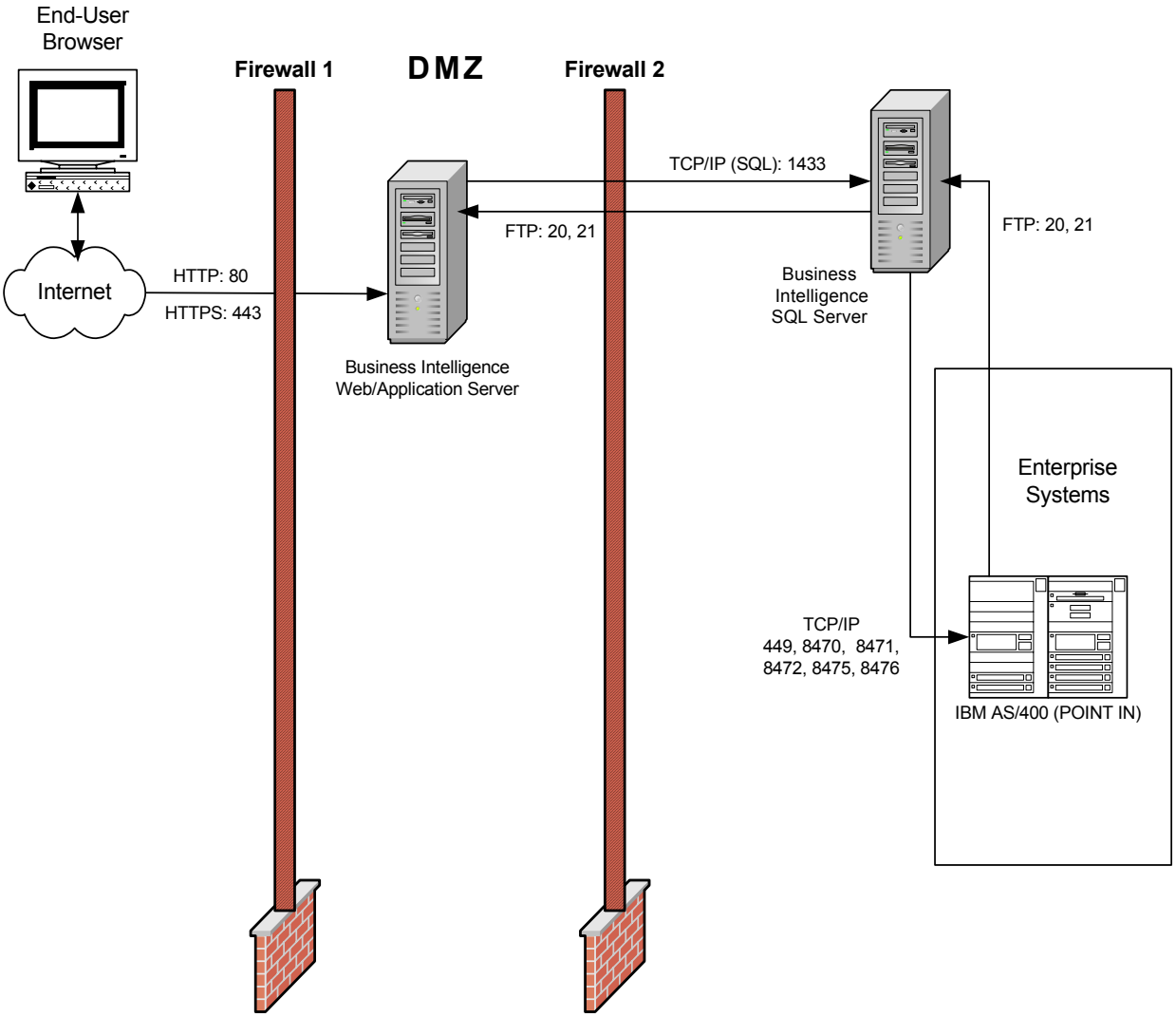


Figure 5. Detail of model

Below is additional information to secure your application and operating system environment following Implementation Model One:

1. Place firewall 2 between the Business Intelligence Web/Application server and the database server as described in the following articles:

   - ***Connections to SQL Server Over the Internet*** http://msdn2.microsoft.com/en-us/library/aa213767.aspx.
   - ***INF: TCP Ports Needed for Communication to SQL Server Through a Firewall*** http://support.microsoft.com/default.aspx?scid=kb;EN-US;q287932.

2. Secure the Web/Application server in the DMZ area by turning off all unused services. The list below indicates the services that are used by Business Intelligence. Do not turn off these services.

Server	Service	Comments
Web server	IIS Admin Service	Required for a product that has a Web piece
Web Server	World Wide Web (WWW)	Required for a product that has a Web piece
Web server	Microsoft SMTP Service	Required for any product that uses email notification
Application server	FTP Publishing Service	Needed if files are transferred between enterprise host and some other server

3. Harden the Web/Application server by setting the appropriate virtual directory permissions.

   - Web/Application server permissions:
     - The server administrator should have full access control.

4. Read additional implementation details in the following documents that are published on the Business Intelligence installation media:

   - Business Intelligence ***Installation Guide***
   - Business Intelligence ***Troubleshooting Guide***

Document Production Server Implementation

Note: *Read this in conjunction with the Document Production* ***Installation Readiness Assessment Guide****.*

Document Production is not a Web security application; it is a financial application that relies on an existing Web security infrastructure. By itself, Document Production authorizes only the users of the application and restricts their use based on profiles defined by the system administrator.

Any financial institution that establishes an Internet presence through Document Production must take steps to ensure the systems they use or own contain adequate security measures. These measures help limit the possibility of unintended distribution of confidential information and the potential for fraud-related losses.

The Internet is designed as an open system, based on the premise of free access and communication between participating computer systems. While there is no guarantee of complete safety and invulnerability, every effort must be made to provide a safe, secure, and protected platform for financial activity.

The details of placing Document Production servers in relation to your firewalls and associating the servers to specific domain(s) depend upon your specific security requirements. Based on the development of Document Production and the protocols used between the servers, the following pages outline two of many implementation models. Following the implementation models are brief instructions for hardening, as well as references to useful articles and links about security.

In a distributed application such as Document Production, other resources require protection in addition to the Web and Application servers. A recommended practice is to put another firewall between the Web/Application servers and the database servers, creating a "demilitarized zone" or DMZ in the event your perimeter defenses

are compromised and an intruder gains access to the Web or Application severs. Communication protocols between the Document Production servers require opening selected ports through firewalls from the DMZ to the internal network. This is applicable to all implementation models.

Security Port Access

The following table lists security ports you may need to open for customizing your implementation.

Ref #	Description	From -> To	Connection Type	Default Port Number(s)
1	Web access	Client -> Web	HTTP/ HTTPS	80,443
4	.NET remoting	Web -> App	TCP	Configurable (any unused port)
6	SQL Server	App -> DB	TCP/ODBC	1433
9	Mapped drives	App -> System i	TCP	Mapped drives 135, 139, 445
10	Mapped drives	App -> System i	UDP	Mapped drives 135, 139, 445
12	Series II FTP	Host -> App	FTP	20, 21
26	Web service	PI Suite -> MM/DP Web	TCP	80

Footnotes and Other Important Considerations

B. How To Configure Remoting

To configure remoting for Document Print, locate web.config in the <drive>:\<target>\DocPrintService\WebServer\WebService folder.

Specify an available port for “Port” and set “remotingenable” to “true.” If remoting is enabled for a single server configuration, the “callbackport” should be set to a different port than the port specified in “Port.” For a two-server configuration, the same port value can be used.

```
<appSettings>
      <add key="Port" value="60031"/>
      <add key="callbackport" value="60032"/>
      <add key="remoteserver" value="localhost"/>
      <add key="remotingenabled" value="false"/>
  </appSettings>
```


D. You may configure error messages that are generated by IIS

When you have a Web site, your users can encounter errors such as "Page not found" or "Page 404 Error." You can customize the text of these error messages to make them more user-friendly and to prevent a technical error from revealing more about your web-site than you might want. Messages can be modified through Windows IIS. Two related articles can be found at the following URLs.

- IIS.net: Using Custom Errors in IIS: Internet Information Server (IIS) http://www.iis.net/go/17
- IIS.net : Understanding Custom and Detailed Errors http://www.iis.net/go/994

Implementation – Production Model

Install the Web server component on one physical server in a workgroup and place the server in the DMZ area. Place the database server and the Application server behind your second firewall.

a Microsoft provides a set of instructions for securing a Windows operating system. Follow the link below:

http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch00.mspx.

b For an illustration, see Figure 6.

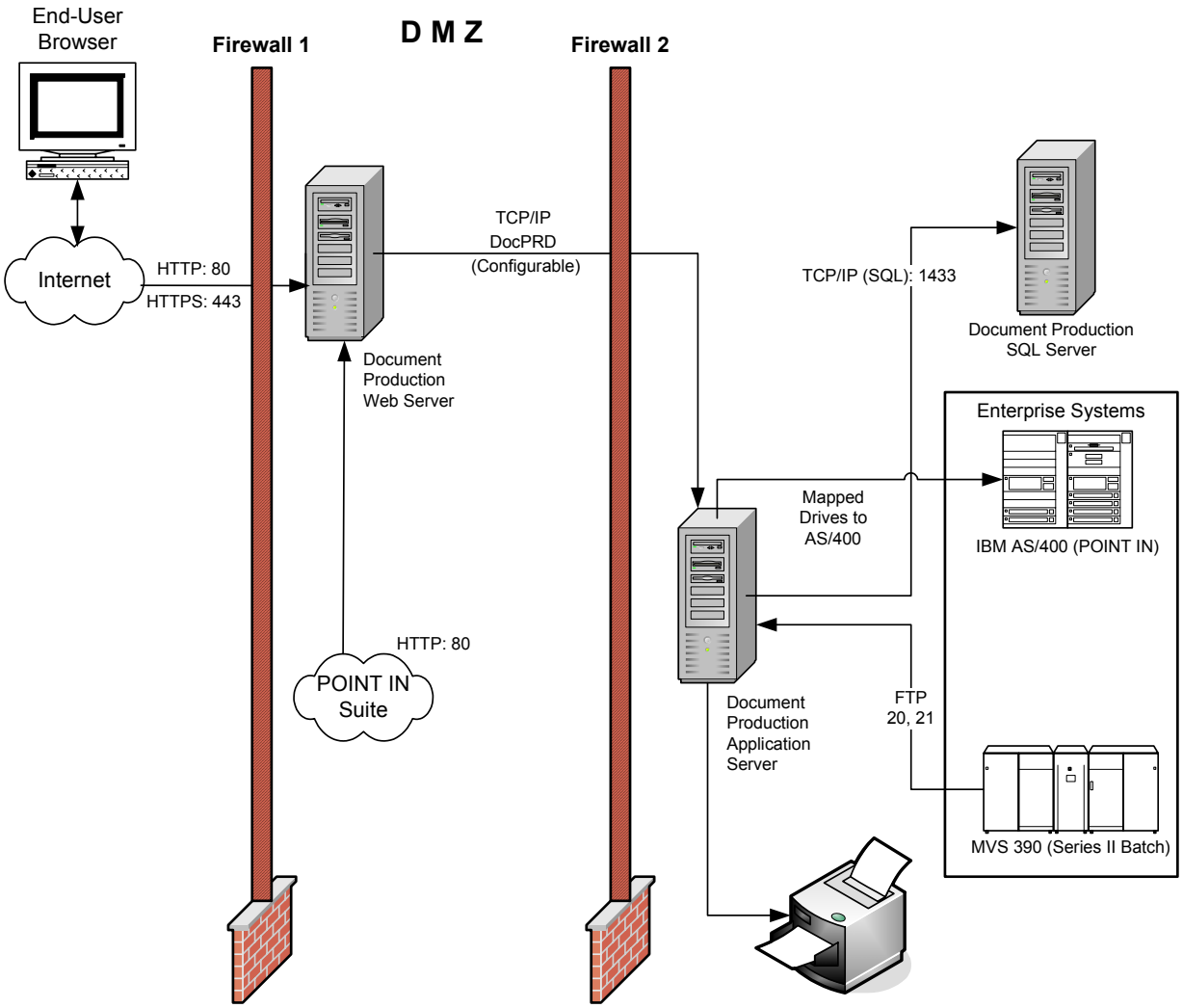


Figure 6. Detail of model

Below is additional information to secure your application and operating system environment.

1. Place firewall 2 between the Web and Application server and the database server as described in the following articles:
   - ***Connections to SQL Server Over the Internet*** http://msdn2.microsoft.com/en-us/library/aa213767.aspx
   - ***INF: TCP Ports Needed for Communication to SQL Server Through a Firewall*** http://support.microsoft.com/default.aspx?scid=kb;EN-US;q287932.
2. Secure the Web and Application servers in the DMZ area by turning off all unused services. The list below indicates the services that are used by Document Production. Do not turn off these services.

Server	Service	Comments
Web/Application server	IIS Admin Service	Required for a product that has a Web piece
Web/Application server	World Wide Web (WWW)	Required for a product that has a Web piece
Web/Application server	Microsoft SMTP Service	Required for any product that uses email notification
Web/Application server	FTP Publishing Service	Needed if files are transferred between enterprise host and some other server

3 Harden the Web and Application server by setting the appropriate virtual directory permissions.

- The server administrator should have full access control.
- Configure your firewalls to allow port traffic to communicate with the Document Production and Media Management components. See illustration (Figure 6.) for ports and protocols the application requires.

4 Read additional implementation details in the following documents that are published on the Document Production installation media:

- Document Production ***Installation Guide***
- Document Production ***Technical User Guide***

Information Ordering Server Implementation

Note: *Read this in conjunction with the Information Ordering* ***Installation Readiness Assessment Guide****.*

Information Ordering is not a Web security application; it is a financial application that relies on an existing Web security infrastructure. By itself, Information Ordering authorizes only the users of the application and restricts their use based on profiles defined by the system administrator.

Any financial institution that establishes an Internet presence through Information Ordering must take steps to ensure the systems they use or own contain adequate security measures. These measures help limit the possibility of unintended distribution of confidential information and the potential for fraud-related losses.

The Internet is designed as an open system, based on the premise of free access and communication between participating computer systems. While there is no guarantee of complete safety and invulnerability, every effort must be made to provide a safe, secure, and protected platform for financial activity.

The details of placing Information Ordering servers in relation to your firewalls and associating the servers to specific domain(s) depend upon your specific security requirements. Based on the development of Information Ordering and the protocols used between the servers, the following pages outline two of many implementation models. Following the implementation models are brief instructions for hardening, as well as references to useful articles and links about security.

In a distributed application such as Information Ordering, other resources require protection in addition to the Web and Application servers. A recommended practice is to put another firewall between the Web/Application servers and the database servers, creating a "demilitarized zone" or DMZ in the event your perimeter defenses

are compromised and an intruder gains access to the Web or Application severs. Communication protocols between the Information Ordering servers require opening selected ports through firewalls from the DMZ to the internal network. This is applicable to all implementation models.

Information Ordering uses a component called Communications Framework (CFW) that resides on the CFW server. The CFW server is for message communications to and from enterprise-specific services. Communication includes transformation and transportation of the messages. Not all of the Information Ordering-specific functions require this server. Please contact your CSC services representative to identify the functions that require CFW.

The Communications Framework server can reside within your DMZ or behind your corporate firewall – firewall 2.

Security Port Access

The following table lists security ports you may need to open for customizing your implementation of Information Ordering.

Ref #	Description	From -> To	Connection Type	Default Port Number(s)
1	Web access	Client -> Web	HTTP/HTTPS	80,443
3	.NET remoting (see footnote “B”)	Web -> App	TCP	4758 (configurable)
5	SQL Server	Web -> DB	TCP/ODBC	1433
6	SQL Server	App -> DB	TCP/ODBC	1433
7	CFW access	App -> CFW	HTTP	8080
8	CFW access	CFW ->Web	HTTP/SOAP	80 (see footnote “A”)
27	IO Scheduler Listener	Scheduler Listener Web -> Vendor	TCP	Configurable with vendor (across business-to-business VPN)
28	POINT host communication	POINT -> CFW	TCP	449, 8475, 8476

Footnotes and Other Important Considerations

A. About Port 80

If you have any of the following functions enabled or products installed, you must open port 80 between CFW and the Web server.

- Agency Link Cancellations (only needed for Series II implementations)
- Underwriting (C.0)
- Information Ordering (C.0)

B. How To Configure Remoting

For Information Ordering

For issue 86936, the settings were moved into the web.config file. The new item is the 'webcallbackport', which specifies the port on the Web server used for remoting. By contrast, the 'serverport' item is the Application server port used for remoting.

```
<!-- Issue 86936 Begin -->
<add key="remotingenabled" value="false"/>
<add key="remoteserver" value="localhost"/>
<add key="serverport" value="4758"/>
<!-- This is the remoting callback port for the web server.
If you have remoting enabled but are only using one
machine, the <webcallbackport> should be set to a different
port than the <serverport>.  If 2 machines are used, they
can be set to the same port. -->
<add key="webcallbackport" value="4759"/>
<!-- Issue 86936 End -->
```

C. CAUTION for Information Ordering when interfacing with ChoicePoint

ChoicePoint does not offer an encrypted protocol for communication. Clients should take measures to ensure data is protected by using a dedicated communication line or Virtual Private Network to ChoicePoint.

D. You may configure error messages that are generated by IIS

When you have a Web site, your users can encounter errors such as "Page not found" or "Page 404 Error." You can customize the text of these error messages to make them more user-friendly and to prevent a technical error from revealing more about your web-site than

you might want. Messages can be modified through Windows IIS. Two related articles can be found at the following URLs.

- IIS.net: Using Custom Errors in IIS: Internet Information Server (IIS) http://www.iis.net/go/17
- IIS.net : Understanding Custom and Detailed Errors http://www.iis.net/go/994

Implementation – Production Model One

Place both the Web and Application servers in a DMZ area and join to a domain consisting of only those two machines. Place the database server behind your second firewall.

a You can place the Communications Framework server on either side of the second firewall.

b Microsoft provides a set of instructions for securing a Windows operating system. Follow the link below for instructions:

http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch00.mspx.

c For more information, see Figure 7.

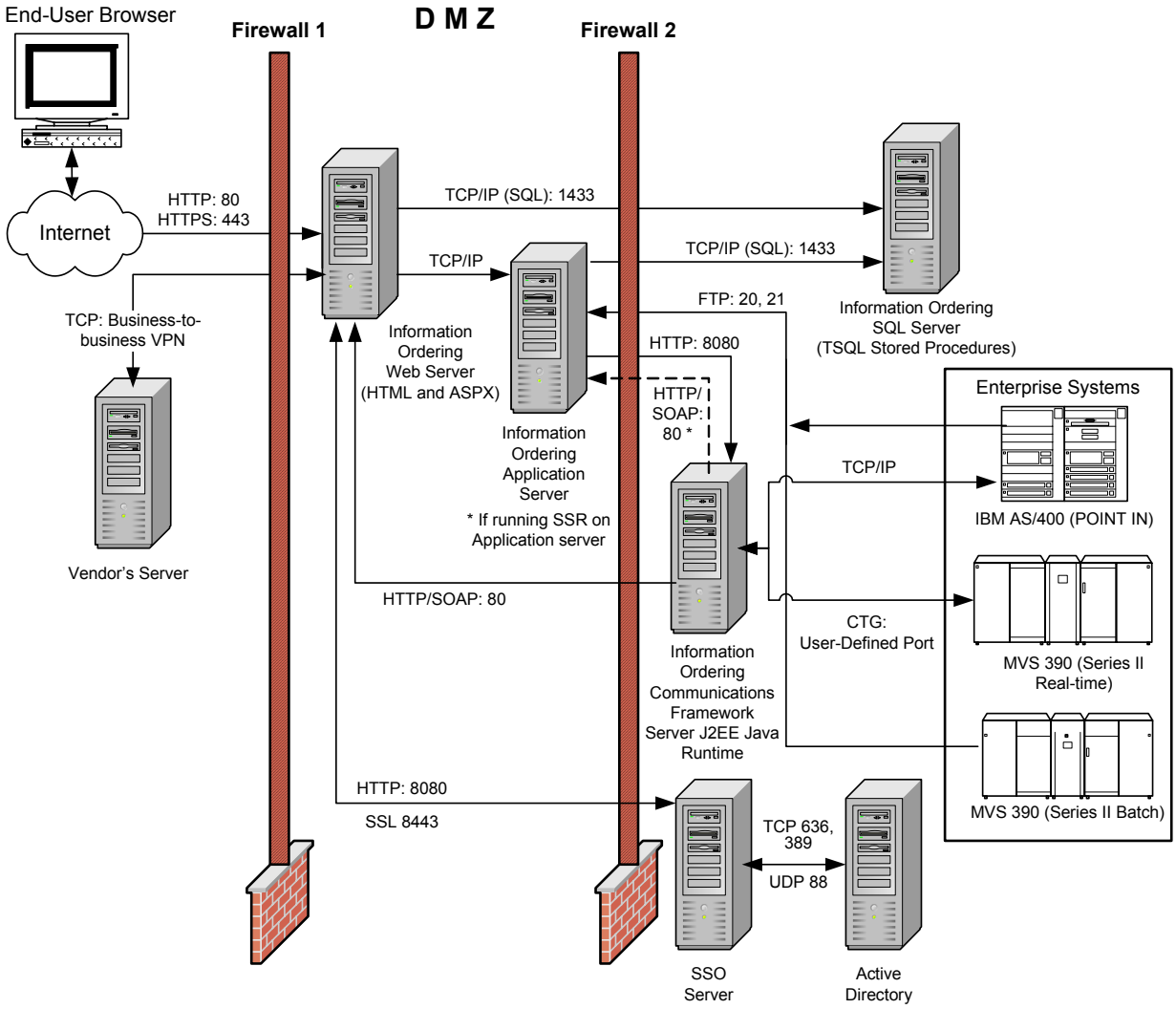


Figure 7. Detail of Implementation Model One

Below is additional information to secure your application and operating system environment following Implementation Model One:

1 Place firewall 2 between the Information Ordering Web/Application servers and the database server as described in the following articles:

- ***Connections to SQL Server Over the Internet*** http://msdn2.microsoft.com/en-us/library/aa213767.aspx.
- ***INF: TCP Ports Needed for Communication to SQL Server Through a Firewall*** http://support.microsoft.com/default.aspx?scid=kb;EN-US;q287932.

2 Do not allow any trust relationship between the Web/Application domain and other domains within firewall 2.

3 Secure the Web and Application servers in the DMZ area by turning off all unused services. The list below indicates the services that are used by Information Ordering. Do not turn off these services.

Server	Service	Comments
Web server	IIS Admin Service	Required for a product that has a Web piece
Web Server	World Wide Web (WWW)	Required for a product that has a Web piece
Web server	Microsoft SMTP Service	Required for any product that uses email notification
Application server	FTP Publishing Service	Needed if files are transferred between enterprise host and some other server

4 Harden the Web and Application servers by setting the appropriate virtual directory permissions.

- Web server permissions:
  - The .NET account (usually Network Service on Windows Server 2003 or ASP.Net on Windows XP) will need Modify permissions for the WEBSERVER\LogFiles folder.
  - The server administrator should have full access control.
- Application server permissions:
  - The .NET account (usually Network Service on Windows Server 2003 or ASP.Net on Windows XP) will need Modify permissions for the APPSERVER\LogFiles folder.
  - The server administrator should have full access control.

5 Based on the enterprise system you are interfacing with, grant additional NT File System (NTFS) permission exceptions as required.

d Configure your firewalls to allow port traffic to communicate with the Information Ordering components. See illustration (Figure 7.) for ports and protocols the application requires. Externalized Authentication Details for Agency Link provides instructions and references for controlling port traffic through your firewalls.

6 If the Communications Framework is deployed behind firewall 2, no additional server hardening is required. But if it is deployed in the DMZ area, hardening of the CommFw directory must be performed.

This directory resides within the Java Virtual Machine (JVM) directory structure chosen for your CFW server.

7 Assess the benefits and risks of implementing.

a Benefits

› User ID maintenance is simplified.

› Redundancy and scalability for additional servers are simplified.

b Risks

› In the event the Web server is compromised, all servers in the domain are at risk.

Implementation – Model Two

Install both the Web and Application server components on one physical server in a workgroup and place the server in the DMZ area. Place the database server behind your second firewall.

a You can place the Communications Framework server on either side of the second firewall.

b Microsoft provides a set of instructions for securing a Windows operating system. Follow the link below:

http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch00.mspx.

c For an illustration, see Figure 8.

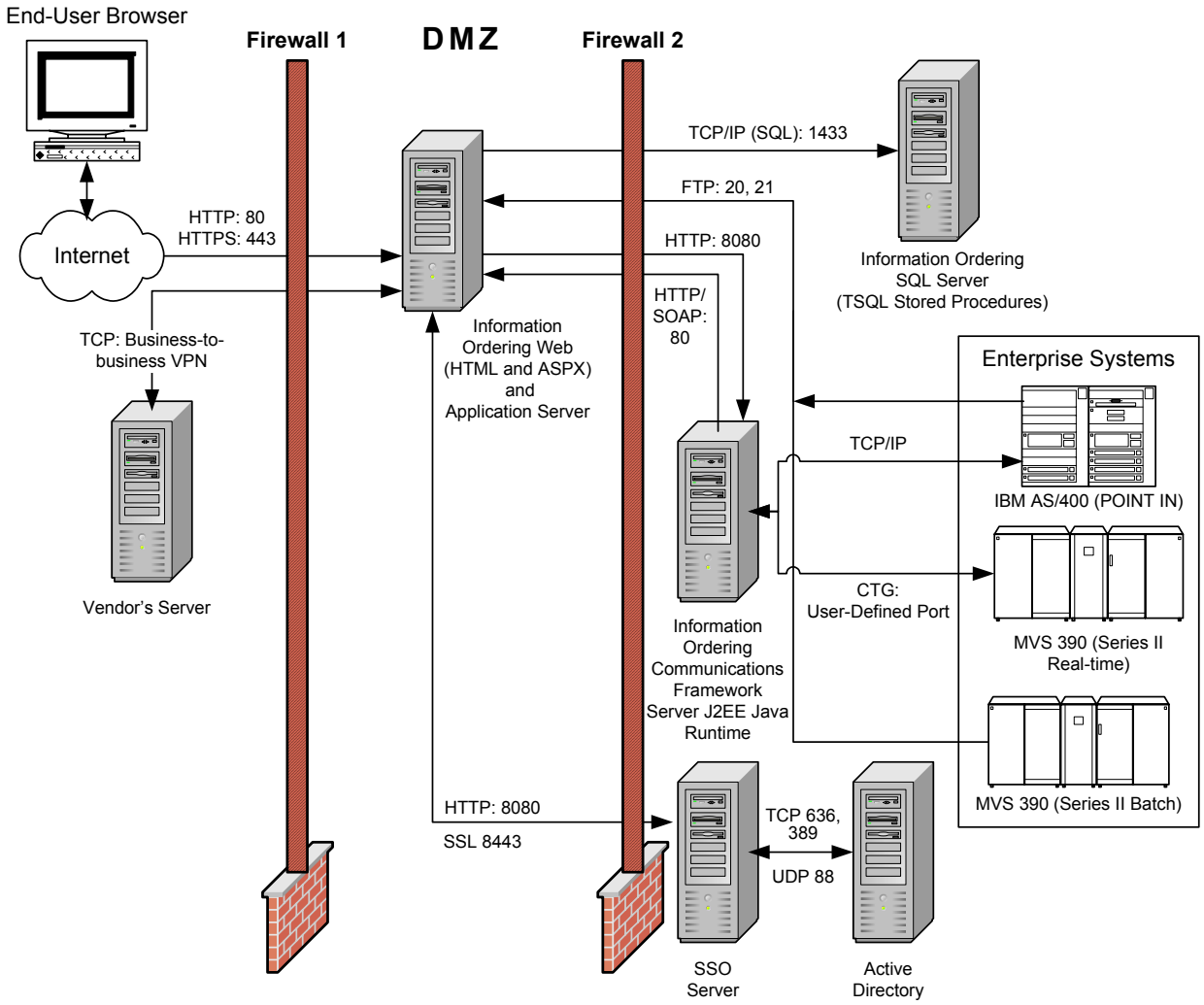


Figure 8. Detail of Implementation Model Two

Below is additional information to secure your application and operating system environment following Implementation Model Two.

1. Place firewall 2 between the Web and Application server and the database server as described in the following articles:

   - ***Connections to SQL Server Over the Internet*** http://msdn2.microsoft.com/en-us/library/aa213767.aspx
   - ***INF: TCP Ports Needed for Communication to SQL Server Through a Firewall*** http://support.microsoft.com/default.aspx?scid=kb;EN-US;q287932.

2. Secure the Web and Application servers in the DMZ area by turning off all unused services. The list below indicates the services that are used by Information Ordering. Do not turn off these services.

Server	Service	Comments
Web/Application server	IIS Admin Service	Required for a product that has a Web piece
Web/Application server	World Wide Web (WWW)	Required for a product that has a Web piece
Web/Application server	Microsoft SMTP Service	Required for any product that uses email notification
Web/Application server	FTP Publishing Service	Needed if files are transferred between enterprise host and some other server

3 Harden the Web and Application server by setting the appropriate virtual directory permissions.

- The .NET account (usually Network Service on Windows Server 2003 or ASP.Net on Windows XP) will need Modify permissions for the WEBSERVER\LogFiles and APPSERVER\LogFiles folders.
- The server administrator should have full access control.

4 Based on the enterprise system you are interfacing with, grant additional NT File System (NTFS) permission exceptions as required.

- Configure your firewalls to allow port traffic to communicate with the Information Ordering components. See illustration (Figure 8.) for ports and protocols the application requires.

5 If CFW is deployed behind firewall 2, no additional server hardening is required. But if it is deployed in the DMZ area, hardening of the CommFw directory must be performed. This directory resides within the Java Virtual Machine (JVM) directory structure chosen for your CFW server.

Important: *With this implementation model, scalability will be limited. User profiles must belong to a domain, not a workgroup, in order for scaling to work efficiently*.

Media Management Server Implementation

Note: *Read this in conjunction with the Media Management* ***Installation Readiness Assessment Guide****.*

Media Management is not a Web security application; it is a financial application that relies on an existing Web security infrastructure. By itself, Media Management authorizes only the users of the application and restricts their use based on profiles defined by the system administrator.

Any financial institution that establishes an Internet presence through Media Management must take steps to ensure the systems they use or own contain adequate security measures. These measures help limit the possibility of unintended distribution of confidential information and the potential for fraud-related losses.

The Internet is designed as an open system, based on the premise of free access and communication between participating computer systems. While there is no guarantee of complete safety and invulnerability, every effort must be made to provide a safe, secure, and protected platform for financial activity.

The details of placing Media Management servers in relation to your firewalls and associating the servers to specific domain(s) depend upon your specific security requirements. Based on the development of Media Management and the protocols used between the servers, the following pages outline two of many implementation models. Following the implementation models are brief instructions for hardening, as well as references to useful articles and links about security.

In a distributed application such as Media Management, other resources require protection in addition to the Web and Application servers. A recommended practice is to put another firewall between the Web/Application servers and the database servers, creating a "demilitarized zone" or DMZ in the event your perimeter defenses

are compromised and an intruder gains access to the Web or Application severs. Communication protocols between the Media Management servers require opening selected ports through firewalls from the DMZ to the internal network. This is applicable to all implementation models.

Security Port Access

The following table lists security ports you may need to open for customizing your implementation.

	Description	From -> To	Connection Type	Default Port Number(s)
1	Web access	Client -> Web	HTTP/ HTTPS	80,443
3	.NET remoting (see footnote "B")	Web -> App	TCP	4758 (configurable)
6	SQL Server	App -> DB	TCP/ODBC	1433
26	Web service	PI Suite -> MM/DP Web	TCP	80

Footnotes and Other Important Considerations

B. How To Configure Remoting

In the Application server MediaMgtApp.xml file in the "Remoting" section, specify the following:

- Port – Application server remoting port
- EnsureSecurity – Channel security setting (either Y or N)

In the Web server MediaMgtWeb.xml file in the "Remoting" section, specify the following:

- Enabled – Flag to enable remoting (either Y or N).
- Server – Application server name or IP address.
- Port – Application server remoting port. This must equal the Application server value.
- CallbackPort – Web server remoting port for callback to the Web pages.
- WSCallbackPort – Web server remoting port for callback to the Web service.

- EnsureSecurity – Channel security setting (either Y or N). This must equal the Application server value.
- SingleServer – Set to Y for a single-server installation. Set to N for a two-server installation.

D. You may configure error messages that are generated by IIS

When you have a Web site, your users can encounter errors such as "Page not found" or "Page 404 Error." You can customize the text of these error messages to make them more user-friendly and to prevent a technical error from revealing more about your web-site than you might want. Messages can be modified through Windows IIS. Two related articles can be found at the following URLs.

- IIS.net: Using Custom Errors in IIS: Internet Information Server (IIS) http://www.iis.net/go/17
- IIS.net : Understanding Custom and Detailed Errors http://www.iis.net/go/994

Implementation – Production Model

Install the Web server component on one physical server in a workgroup and place the server in the DMZ area. Place the database server and the Application server behind your second firewall.

a Microsoft provides a set of instructions for securing a Windows operating system. Follow the link below:

http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch00.mspx.

b For an illustration, see Figure 9.

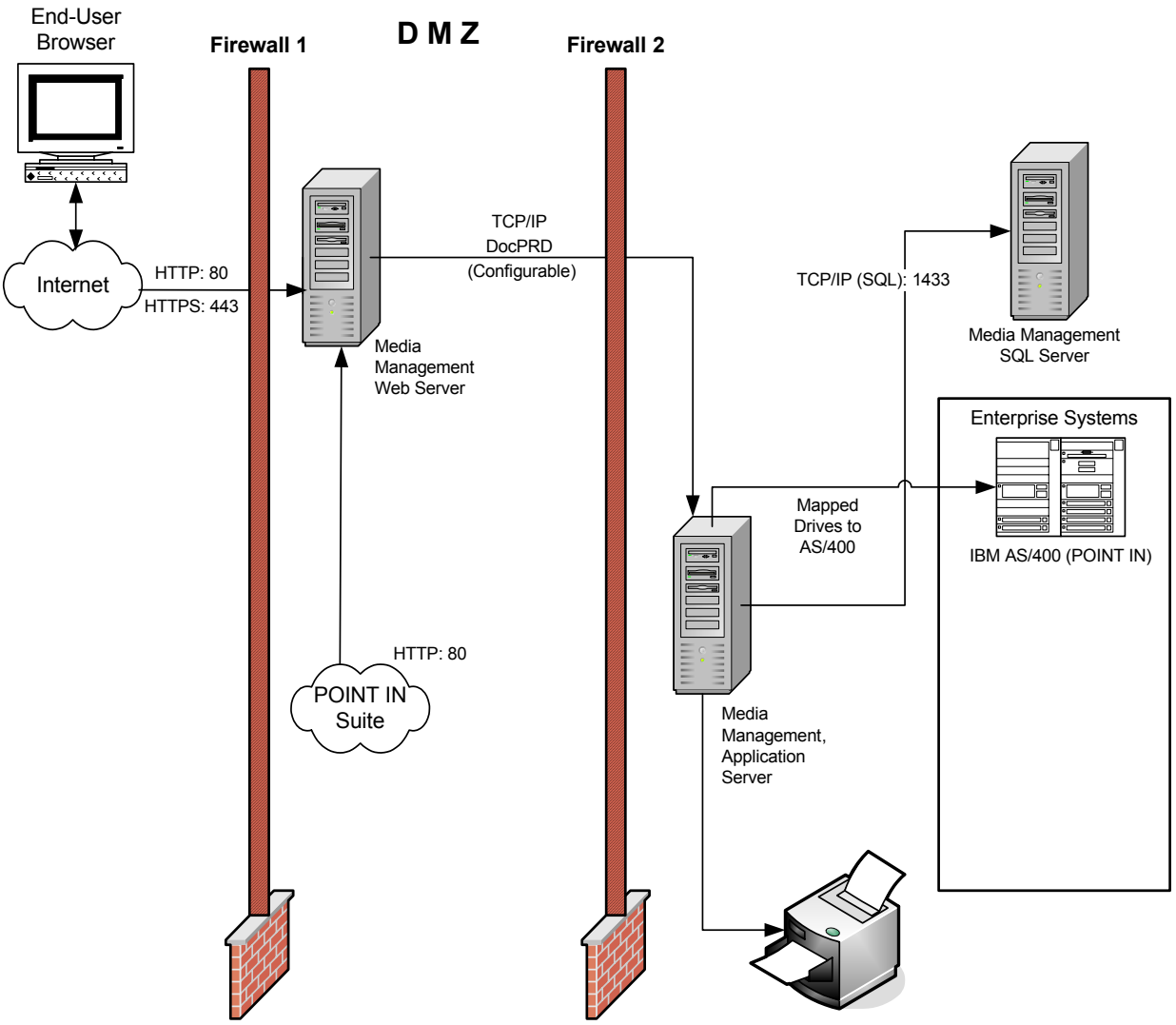


Figure 9. Detail of Implementation Model

Below is additional information to secure your application and operating system environment.

1 Place firewall 2 between the Web and Application servers and the database server as described in the following articles:

- ***Connections to SQL Server Over the Internet*** http://msdn2.microsoft.com/en-us/library/aa213767.aspx
- ***INF: TCP Ports Needed for Communication to SQL Server Through a Firewall*** http://support.microsoft.com/default.aspx?scid=kb;EN-US;q287932.

2 Secure the Web/Application server in the DMZ area by turning off all unused services. The list below indicates the services that are used by Media Management. Do not turn off these services.

Server	Service	Comments
Web/Application server	IIS Admin Service	Required for a product that has a Web piece
Web/Application server	World Wide Web (WWW)	Required for a product that has a Web piece
Web/Application server	Microsoft SMTP Service	Required for any product that uses email notification
Web/Application server	FTP Publishing Service	Needed if files are transferred between enterprise host and some other server

3 Harden the Web and Application server by setting the appropriate virtual directory permissions.

- The server administrator should have full access control.
- Configure your firewalls to allow port traffic to communicate with the Document Production and Media Management components. See illustration (Figure 9.) for ports and protocols the application requires.

4 Read additional implementation details in the following documents that are published on the Media Management installation media:

- Media Management ***Installation Guide***
- Media Management ***Customization Guide***

POINT IN Server Implementation

Note: *Read this in conjunction with the POINT IN* ***Installation Readiness Assessment Guide****.*

POINT IN is not a Web security application; it is a financial application that relies on an existing Web security infrastructure. By itself, POINT IN authorizes only the users of the application and restricts their use based on profiles defined by the system administrator.

Any financial institution that establishes an Internet presence through POINT IN must take steps to ensure the systems they use or own contain adequate security measures. These measures help limit the possibility of unintended distribution of confidential information and the potential for fraud-related losses.

The Internet is designed as an open system, based on the premise of free access and communication between participating computer systems. While there is no guarantee of complete safety and invulnerability, every effort must be made to provide a safe, secure, and protected platform for financial activity.

The details of placing POINT IN servers in relation to your firewalls and associating the servers to specific domain(s) depend upon your specific security requirements. Based on the development of POINT IN and the protocols used between the servers, the following pages outline two of many implementation models. Following the implementation models are brief instructions for hardening, as well as references to useful articles and links about security.

In a distributed application such as POINT IN, other resources require protection in addition to the Web and Application servers. A recommended practice is to put another firewall between the Web/Application servers and the database servers, creating a "demilitarized zone" or DMZ in the event your perimeter defenses are compromised and an intruder gains access to the Web or Application severs. Communication protocols between the POINT IN serv-

ers require opening selected ports through firewalls from the DMZ to the internal network. This is applicable to all implementation models.

Security Port Access

The following table lists security ports you may need to open for customizing your implementation.

	Description	From -> To	Connection Type	Default Port Number(s)
17	POINT host communication	CFW -> POINT	TCP	23, 449, 8470, 8471, 8475, 8476
25	POINT host communication			8471
26	Web service	PI Suite -> MM/DP Web	TCP	80
29	Jacada Web Access	Browser -> Jacada Server	TPC	80, 1100, 1101

Implementation – Production Model

Place the Application server in a DMZ area. Place the database server behind your second firewall.

a You can place the Communications Framework server on either side of the second firewall.

b Microsoft provides a set of instructions for securing a Windows operating system. Follow the link below for instructions:

http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch00.mspx.

c For more information, see Figure 10.

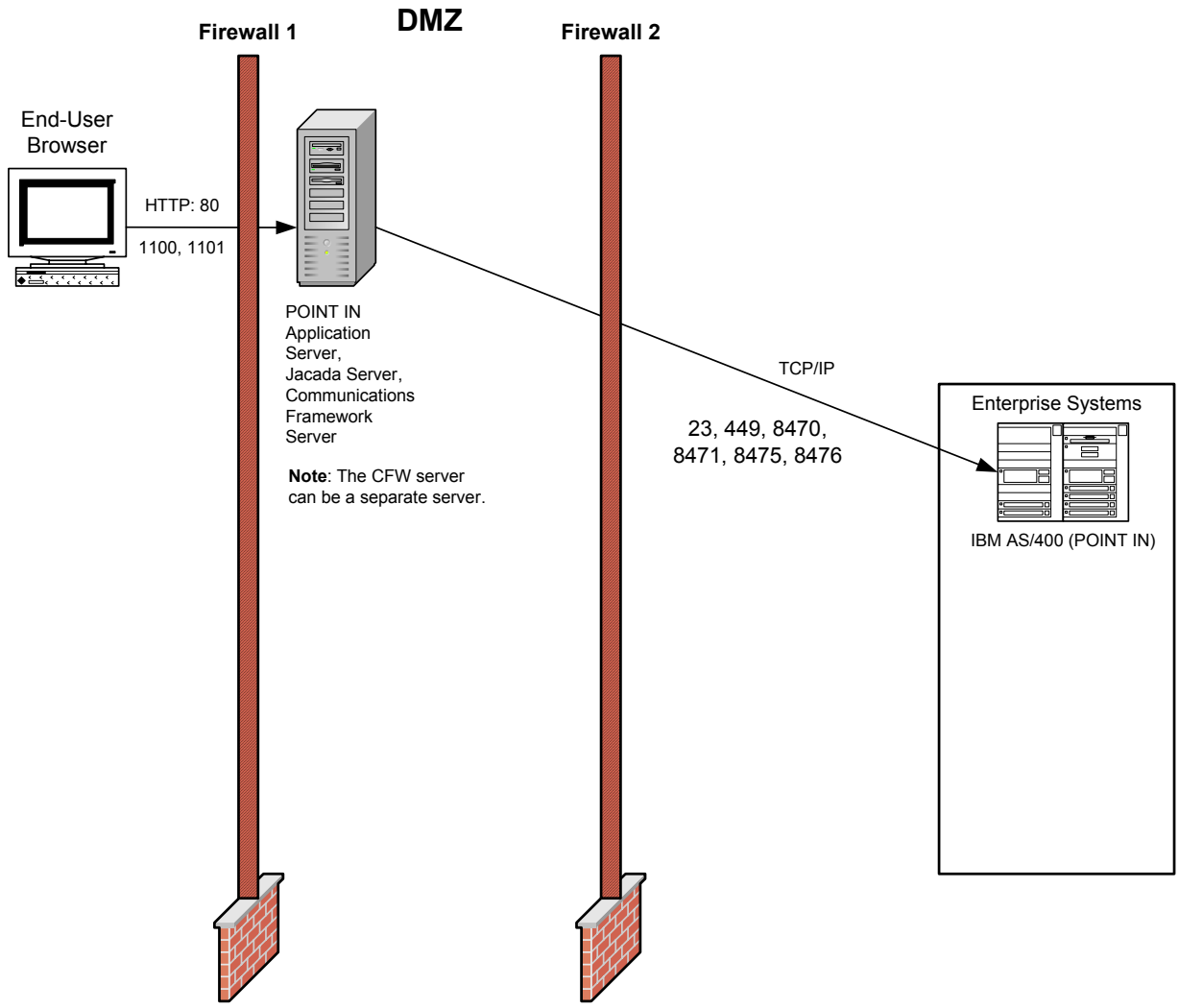


Figure 10. Detail of model

Below is additional information to secure your application and operating system environment following implementation model:

1. Harden the and Application server by setting the appropriate virtual directory permissions.

2. If the Communications Framework is deployed behind firewall 2, no additional server hardening is required. But if it is deployed in the DMZ area, hardening of the CommFw directory must be performed. This directory resides within the Java Virtual Machine (JVM) directory structure chosen for your CFW server.

3 Secure the Application server in the DMZ area by turning off all unused services. The list below indicates the services that are used by POINT IN. Do not turn off these services.

Server	Service	Comments
Web/Application server	IIS Admin Service	Required for a product that has a Web piece
Web/Application server	World Wide Web (WWW)	Required for a product that has a Web piece
Web/Application server	Microsoft SMTP Service	Required for any product that uses email notification
Web/Application server	FTP Publishing Service	Needed if files are transferred between enterprise host and some other server

Underwriting Server Implementation

Note: *Read this in conjunction with the Underwriting* ***Installation Readiness Assessment Guide****.*

Underwriting is not a Web security application; it is a financial application that relies on an existing Web security infrastructure. By itself, Underwriting authorizes only the users of the application and restricts their use based on profiles defined by the system administrator.

Any financial institution that establishes an Internet presence through Underwriting must take steps to ensure the systems they use or own contain adequate security measures. These measures help limit the possibility of unintended distribution of confidential information and the potential for fraud-related losses.

The Internet is designed as an open system, based on the premise of free access and communication between participating computer systems. While there is no guarantee of complete safety and invulnerability, every effort must be made to provide a safe, secure, and protected platform for financial activity.

The details of placing Underwriting servers in relation to your firewalls and associating the servers to specific domain(s) depend upon your specific security requirements. Based on the development of Underwriting and the protocols used between the servers, the following pages outline two of many implementation models. Following the implementation models are brief instructions for hardening, as well as references to useful articles and links about security.

In a distributed application such as Underwriting, other resources require protection in addition to the Web and Application servers. A recommended practice is to put another firewall between the Web/Application servers and the database servers, creating a "demilitarized zone" or DMZ in the event your perimeter defenses are compromised and an intruder gains access to the Web or Appli-

cation severs. Communication protocols between the Underwriting servers require opening selected ports through firewalls from the DMZ to the internal network. This is applicable to all implementation models.

Underwriting uses a component called Communications Framework (CFW) that resides on the CFW server. The CFW server is for message communications to and from enterprise-specific services. Communication includes transformation and transportation of the messages. Not all of the Underwriting-specific functions require this server. Please contact your CSC services representative to identify the functions that require CFW.

The Communications Framework server can reside within your DMZ or behind your corporate firewall – firewall 2.

Security Port Access

The following table lists security ports you may need to open for customizing your implementation of Underwriting.

Ref #	Description	From -> To	Connection Type	Default Port Number(s)
1	Web access	Client -> Web	HTTP/HTTPS	80,443
3	.NET remoting (see footnote "B")	Web -> App	TCP	4758 (configurable)
5	SQL Server	Web -> DB	TCP/ODBC	1433
6	SQL Server	App -> DB	TCP/ODBC	1433
7	CFW access	App -> CFW	HTTP	8080
8	CFW access	CFW ->Web	HTTP/SOAP	80 (see footnote "A")
28	POINT host communication	POINT -> CFW	TCP	449, 8475, 8476

Footnotes and Other Important Considerations

A. About Port 80

If you have any of the following functions enabled or products installed, you must open port 80 between CFW and the Web server.

- Agency Link Cancellations (only needed for Series II implementations)
- Underwriting (C.0)
- Information Ordering (C.0)

B. How To Configure Remoting

For Underwriting

For issue 86936, the settings were moved into the web.config file. The new item is the 'webcallbackport', which specifies the port on the Web server used for remoting. By contrast, the 'serverport' item is the Application server port used for remoting.

```
<!-- Issue 86936 Begin -->
<add key="remotingenabled" value="false"/>
<add key="remoteserver" value="localhost"/>
<add key="serverport" value="4758"/>
<!-- This is the remoting callback port for the web server.
If you have remoting enabled but are only using one
machine, the <webcallbackport> should be set to a different
port than the <serverport>.  If 2 machines are used, they
can be set to the same port. -->
<add key="webcallbackport" value="4759"/>
<!-- Issue 86936 End -->
```

C. CAUTION for Underwriting when interfacing with ChoicePoint

ChoicePoint does not offer an encrypted protocol for communication. Clients should take measures to ensure data is protected by using a dedicated communication line or Virtual Private Network to ChoicePoint.

D. You may configure error messages that are generated by IIS

When you have a Web site, your users can encounter errors such as "Page not found" or "Page 404 Error." You can customize the text of these error messages to make them more user-friendly and to prevent a technical error from revealing more about your web-site than you might want. Messages can be modified through Windows IIS. Two related articles can be found at the following URLs.

- IIS.net: Using Custom Errors in IIS: Internet Information Server (IIS) http://www.iis.net/go/17
- IIS.net : Understanding Custom and Detailed Errors http://www.iis.net/go/994

Implementation – Production Model One

Place both the Web and Application servers in a DMZ area and join to a domain consisting of only those two machines. Place the database server behind your second firewall.

a You can place the Communications Framework server on either side of the second firewall.

b Microsoft provides a set of instructions for securing a Windows operating system. Follow the link below for instructions:

http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch00.mspx.

c For more information, see Figure 11.

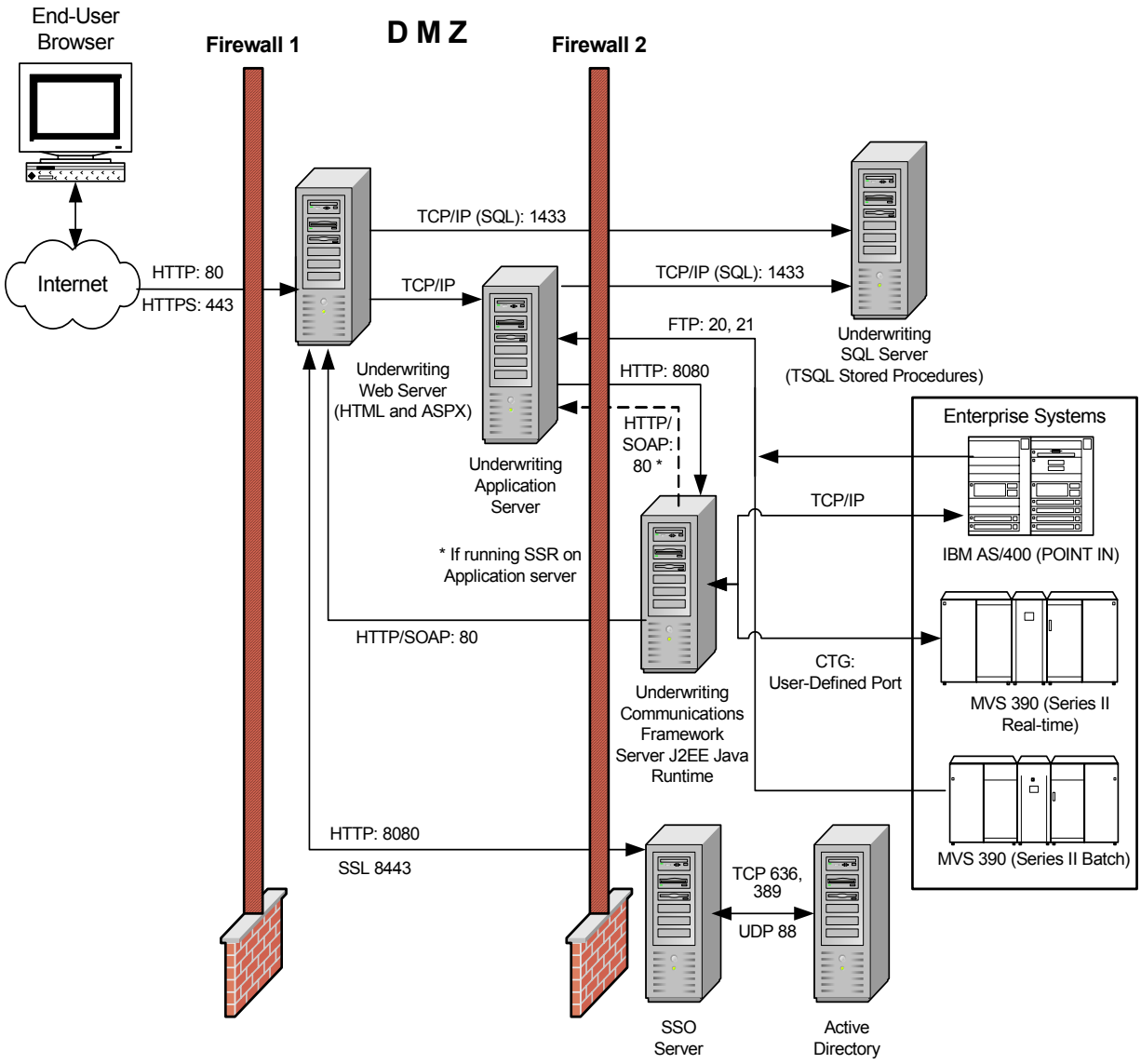


Figure 11. Detail of Implementation Model One

Below is additional information to secure your application and operating system environment following Implementation Model One:

1 Place firewall 2 between the Underwriting Web/Application servers and the database server as described in the following articles:

- ***Connections to SQL Server Over the Internet*** http://msdn2.microsoft.com/en-us/library/aa213767.aspx.
- ***INF: TCP Ports Needed for Communication to SQL Server Through a Firewall*** http://support.microsoft.com/default.aspx?scid=kb;EN-US;q287932.

2 Do not allow any trust relationship between the Web/Application domain and other domains within firewall 2.

3 Secure the Web and Application servers in the DMZ area by turning off all unused services. The list below indicates the services that are used by Agency Link. Do not turn off these services.

Server	Service	Comments
Web server	IIS Admin Service	Required for a product that has a Web piece
Web Server	World Wide Web (WWW)	Required for a product that has a Web piece
Web server	Microsoft SMTP Service	Required for any product that uses email notification
Application server	FTP Publishing Service	Needed if files are transferred between enterprise host and some other server

4 Harden the Web and Application servers by setting the appropriate virtual directory permissions.

- Web server permissions:
  - The .NET account (usually Network Service on Windows Server 2003 or ASP.Net on Windows XP) will need Modify permissions for the WEBSERVER\LogFiles folder.
  - The server administrator should have full access control.
- Application server permissions:
  - The .NET account (usually Network Service on Windows Server 2003 or ASP.Net on Windows XP) will need Modify permissions for the APPSERVER\LogFiles folder.
  - The server administrator should have full access control.

5 Based on the enterprise system you are interfacing with, grant additional NT File System (NTFS) permission exceptions as required.

- Configure your firewalls to allow port traffic to communicate with the Underwriting components. See illustration (Figure 11.) for ports and protocols the application requires. Externalized Authentication Details for Agency Link provides instructions and references for controlling port traffic through your firewalls.

6 If the Communications Framework is deployed behind firewall 2, no additional server hardening is required. But if it is deployed in the DMZ area, hardening of the CommFw directory must be performed.

This directory resides within the Java Virtual Machine (JVM) directory structure chosen for your CFW server.

7 Assess the benefits and risks of implementing.

a Benefits

› User ID maintenance is simplified.

› Redundancy and scalability for additional servers are simplified.

b Risks

› In the event the Web server is compromised, all servers in the domain are at risk.

Implementation – Model Two

Install both the Web and Application server components on one physical server in a workgroup and place the server in the DMZ area. Place the database server behind your second firewall.

a You can place the Communications Framework server on either side of the second firewall.

b Microsoft provides a set of instructions for securing a Windows operating system. Follow the link below:

http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch00.mspx.

c For an illustration, see Figure 12.

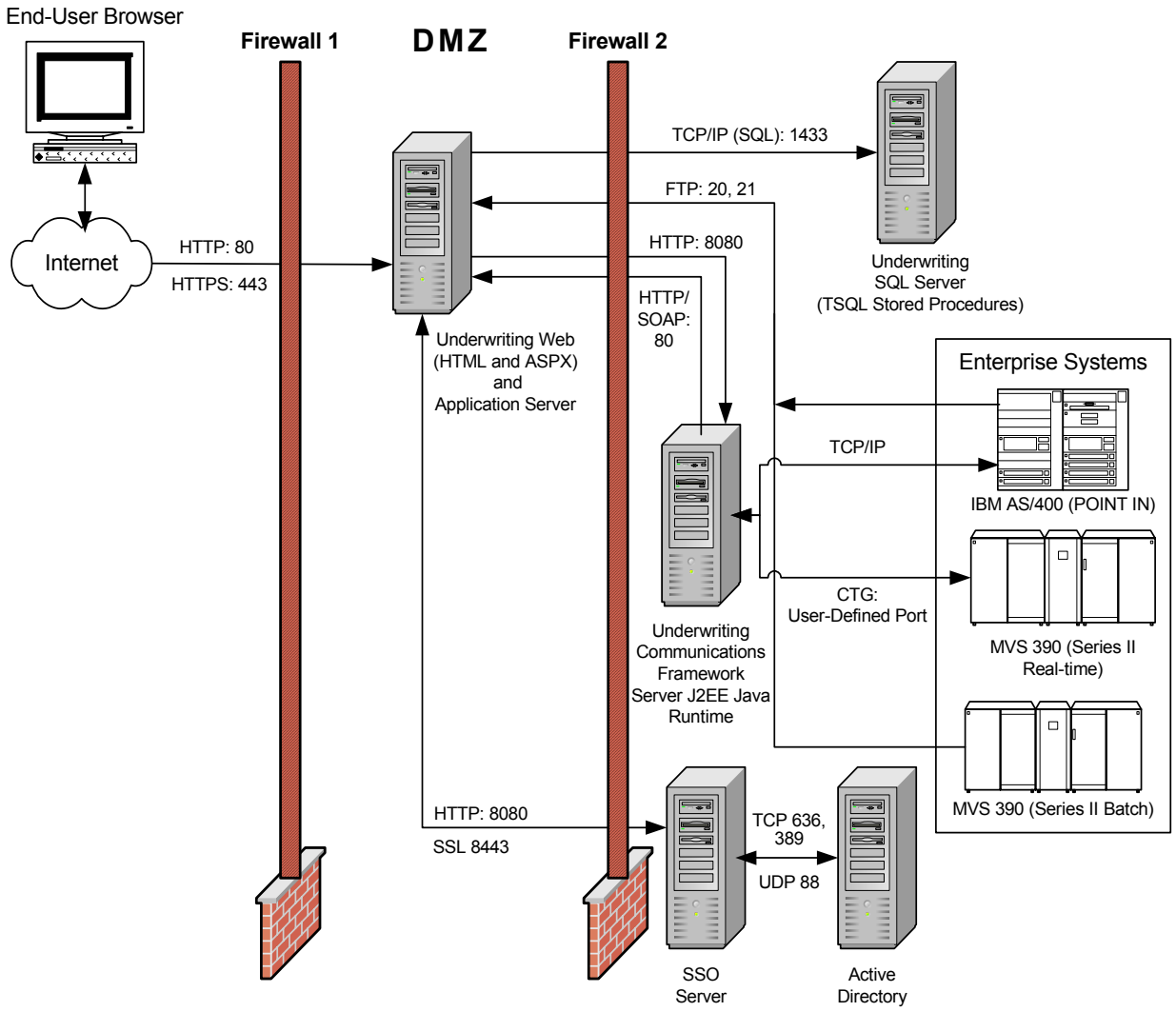


Figure 12. Detail of Implementation Model Two

Below is additional information to secure your application and operating system environment following Implementation Model Two.

1 Place firewall 2 between the Web and Application server and the database server as described in the following articles:

- ***Connections to SQL Server Over the Internet*** http://msdn2.microsoft.com/en-us/library/aa213767.aspx
- ***INF: TCP Ports Needed for Communication to SQL Server Through a Firewall*** http://support.microsoft.com/default.aspx?scid=kb;EN-US;q287932.

2 Secure the Web and Application server in the DMZ area by turning off all unused services. The list below indicates the services that are used by Agency Link. Do not turn off these services.

Server	Service	Comments
Web/Application server	IIS Admin Service	Required for a product that has a Web piece
Web/Application server	World Wide Web (WWW)	Required for a product that has a Web piece
Web/Application server	Microsoft SMTP Service	Required for any product that uses email notification
Web/Application server	FTP Publishing Service	Needed if files are transferred between enterprise host and some other server

3 Harden the Web and Application server by setting the appropriate virtual directory permissions.

- The .NET account (usually Network Service on Windows Server 2003 or ASP.Net on Windows XP) will need Modify permissions for the WEBSERVER\LogFiles and APPSERVER\LogFiles folders.
- The server administrator should have full access control.

4 Based on the enterprise system you are interfacing with, grant additional NT File System (NTFS) permission exceptions as required.

- Configure your firewalls to allow port traffic to communicate with the Underwriting components. See illustration (Figure 12.) for ports and protocols the application requires.

5 If CFW is deployed behind firewall 2, no additional server hardening is required. But if it is deployed in the DMZ area, hardening of the CommFw directory must be performed. This directory resides within the Java Virtual Machine (JVM) directory structure chosen for your CFW server.

Important: *With this implementation model, scalability will be limited. User profiles must belong to a domain, not a workgroup, in order for scaling to work efficiently*.

Externalized Authentication Details for Agency Link

Configuration Options

The Agency Link system can use external authentication rather than Single Sign-On.

If you choose to use your own authentication system, there is only one primary requirement. Your authenticating system must pass the user IDs in the HTTP/HTTPS header or through an HTTP posted form.

Based on which method you choose to pass the user IDs, changes to the Settings.xml file will be required. For the Settings.xml file, make sure the < **uidkeyhttphead** > element is set as described below.

- This element requires a value if you are using an external security system. The value you use here must represent the key to your user ID in the HTTP/HTTPS header or posted HTTP form. An example of this could be **userid**.

There are two methods to extract the user IDs from the HTTP/HTTPS header or posted form. Below is a description of each method, including discussion of factors to consider when deciding which method to use. There may be alternative methods you may choose, depending on how you pass the user IDs. VerifyLogin will test for SSO first, and then for each of the following methods. If you are using SSO or either of the two methods below, no changes to Verify-Login.aspx are required.

Method One

If you are using an external security system that uses a ISAPI filter in IIS such as Netegrity SiteMinder, this method will parse through the HTTP/HTTPS header looking for the user ID key that is defined in the Settings.xml file. Then it will extract the actual user ID and place into session.


```
UserName = "" & HttpContext.Current.Items("HTTP_USER")
```

Method Two

If you choose to pass the user IDs to Agency Link through an HTTP posted form, the method below will extract the IDs from the posted form and place it into session.

```
UserName = "" & Request.Form(secUIDKey)
```

The name of an authenticated user can be passed to the Agency Link Web server through an HTTP form post. The name of the form item must match the name specified in the Agency Link Settings.xml file. If the passed username matches a username in the Agency Link security database, the user will be admitted as if he had logged on to Agency Link.

In such a configuration, Secure Sockets Layer encryption should be enabled on the Agency Link Web server so that Web traffic containing username data is encrypted.

Communications Framework: Enabling SSL for Apache Tomcat

This chapter describes a basic procedure for enabling Secured Sockets Layer (SSL) on an Apache Tomcat server. These examples use self-generated certificates which display warning messages when accessed from a browser. For production, it is recommended that certificates be obtained from a trusted certificate authority such as VeriSign. A more detailed document describing SSL set-up under Tomcat can be found at—

http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html

Enable SSL Under Tomcat

When Tomcat is installed, the Java Software Development Kit (JDK) is installed, as well. The environment variable **JAVA_HOME** contains the location of the root of the JDK. This will be used throughout this section.

1 On the server where Tomcat is deployed, open a Windows command line and execute the following command to change to the installed Java security directory:

```
cd %JAVA_HOME%\lib\security
```

2 Now execute the command to generate a certificate key for Tomcat. (This command is on one line.)

```
%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA
   -keystore cacerts -keypass changeit
```

3 You will then be prompted to enter the password of the keystore, your server name, and other information to identify the server for which the certificate will be generated. (Bold values are user responses to the questions.)

- Enter keystore password: **changeit**
- What is your first and last name?

  [Unknown]: **srvrlsdbcf.csc-fsg.com**

- What is the name of your organizational unit?

  [Unknown]: **fsg**

- What is the name of your organization?

  [Unknown]: **csc**

- What is the name of your City or Locality?

  [Unknown]: **blythewood**

- What is the name of your State or Province?

  [Unknown]: **sc**

- What is the two-letter country code for this unit?

  [Unknown]: **us**

- Is CN=srvvrlsdbcf.csc-fsg.com, OU=fsg, O=csc, L=blythewood, ST=sc, C=us correct?

  [no]: **yes**

4. When it asks for the value of "first and last name," enter the fully qualified name of your server.

5. Next, enable SSL in the Tomcat server.

   a. Edit the file **e:\Program Files\Apache Group\Tomcat 6.0\conf\server.xml**. (This is the typical location, but you may need to adjust the path to your Tomcat installation.) The section defining an SSL connector for HTTPS is commented out in the server.xml file.

   b. Locate the following section and remove the comments ("<!-" and "-->"), which are XML comment delimiters before and after this section.

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
    <!-- -->
   <Connector port="8443"
        maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
        enableLookups="false" disableUploadTimeout="true"
        acceptCount="100" debug="0" scheme="https" secure="true"
        clientAuth="false" sslProtocol="TLS"
```



```
    keystoreFile="e:\\jre1.5.0_12\\lib\\security\\cacerts"
    keystorePass="changeit" />
</Connector>
<!-- -->
```

c Two attributes have been added to the **<Factory>** section, **keystoreFile** and **keystorePass**. They define where to find the certificate key store where the Tomcat certificate was generated. This is the value of the JAVA_HOME environment variable appended with the path lib\security\cacerts.

› Note that there are double backslashes (\\) between each path.

6 You should now be able to test SSL under Tomcat.

a Restart the Apache Tomcat service.

b Open the URL https://localhost:8443/ on the browser of the Tomcat server.

c Accept the certificate when you see a warning about the self-signed certificates. The Apache Tomcat home screen should be displayed.

7 If you get a connection error, there may have been a problem implementing one of the steps above. Look at the files **stdout.log** and **stderr.log** in the Tomcat logs directory to find more details on the error if you experience a problem.

Import Trusted Certificates

Next, import the certificates from any servers that you will be communicating to with SSL. This section of the document will not describe in detail how to obtain the certificates. These certificates may be purchased from an official certificate authority or generated from a certificate server. They must already be installed on the target server.

This will briefly describe exporting a certificate from a Microsoft Windows Active Directory Domain Controller. More detailed instructions can be obtained from Microsoft's Web sites.

On the Domain Controller - 2003 Server (If Not Already Installed)

1. Set up certificate issue authority.
2. Select Add/remove programs.
3. Select Add/remove Windows Components.
4. Click Certificate Services.
5. Click Certificate Services (CA).
6. Click Install.

Request Certificate for Domain Controller for MMC

1. Run MMC.
2. Under File menu, select Add/remove snap-in.
3. Select Certificates.
4. Click Add button.
5. Select Certificates.
6. Click Add button.
7. Select Computer Account radio button.
8. Click Finish.
9. Click Close.

Navigate to Personal Folder within Certificates

1. Right click.
2. Click All tasks.
3. Click Request New Certificate.

4 On the Certificate Request Wizard, click Next.

5 Accept default request for Domain Controller and click Next.

6 Pick a friendly name or leave blank, click Next, and then click Finish.

Export Certificate

1 Execute the **Run...** command from the Windows Start menu.

2 Type **mmc** (for Microsoft Management Console) and then press <enter>.

3 Click on the following in turn:

- File > Add/Remove Snap-in... > Add... > Certificates > Add.

4 Select the **Computer account** radio button, and then click Next >.

5 Close the windows by clicking Finish, Close, and OK.

6 Expand the Certificates (Local Computer) section and you should see something similar to the following screen:

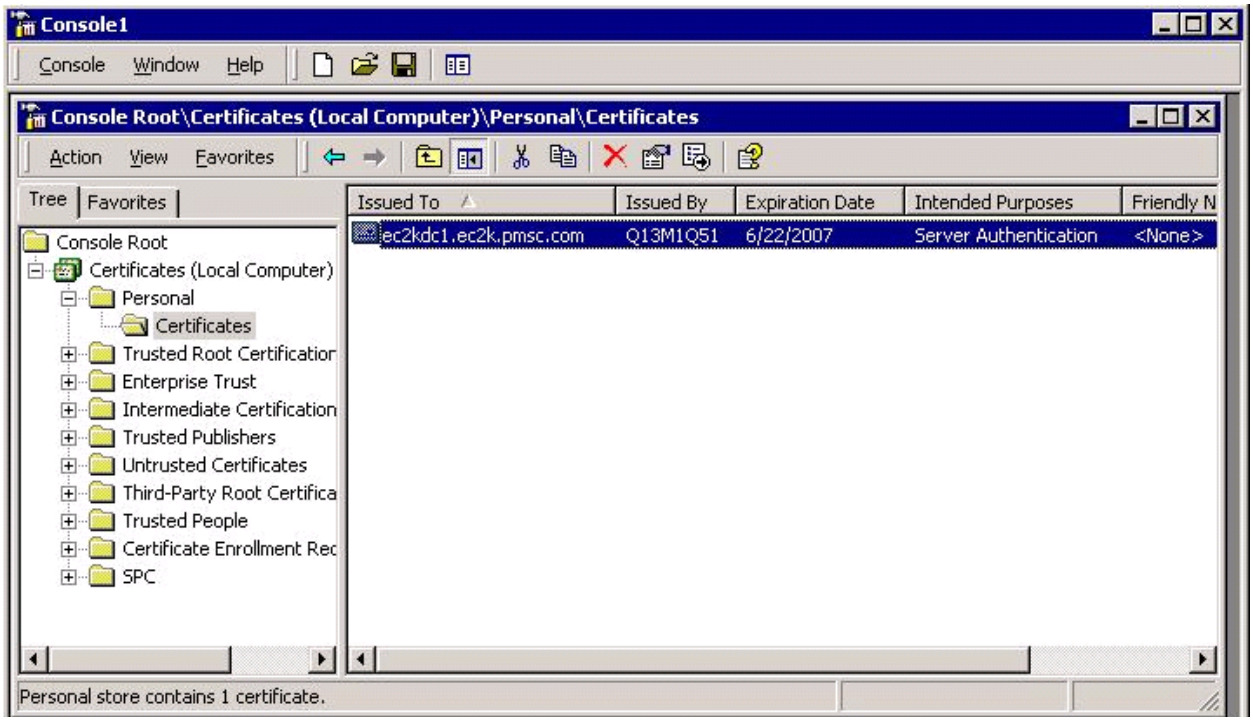


Figure 13. Certificates on Local Computer

7 If you have installed certificates on the server, they will be available for export under the Personal Certificates section.

8 Right click on the certificate to export. Then select All Tasks > Export.

9 The Certificate Export Wizard will open.

10 Click Next.

11 You don't need to export the private key, so click Next again.

12 Select **Base-64 encoded X.509 (.CER)** and click Next again.

13 Pick a path and file name for the certificate. (Naming the certificate with the server host name may be helpful in distinguishing it from other certificates.) It will have a .cer extension.

Import Certificate

Next, the certificate that you exported needs to be imported into the certificate truststore used by Tomcat.

1 Copy the exported certificate file to the Tomcat server. You may want to copy it to the %JAVA_HOME%\lib\security directory for ease of access.

2 Open a Windows command line and execute the following command to change to the installed Java security directory:

```
cd %JAVA_HOME%\lib\security
```

3 Execute the command to import a certificate. (This command is on one line.)

```
%JAVA_HOME%\bin\keytool -import -alias srvrlswa -file
srvrlswa.cer -keystore cacerts -keypass changeit
```

4 For **-file**, insert the name of your certificate file you copied to the Tomcat server. (The path may also be required if not in the Java security directory.) For the **-alias**, use a unique name such as the host name of the server.

5 You will then be prompted to enter the password of the keystore. You should see a message stating that the certificate is successfully imported.

6 You must restart the Apache Tomcat service for the new settings to become effective.

7 You must repeat this process for each server that you wish to communicate with using SSL.

Documentation Reference: *Content for this chapter is copied from SSO Reference Guide, chapter "SSL Certificate Set-Up Using Apache Tomcat and Microsoft Windows Active Directory."*

Communications Framework: SSL Certificate Set-Up Using IBM WebSphere

This chapter presents a high-level procedure for securing SSL transport protocol. This allows Agency Link to interact with a host via Communications Framework over a secure connection.

High-Level Look at the Procedure

On WebSphere Server

a Create new key and certificate request using Ikeyman.

b Create self-signed certificate using IKeyman.

On Domain Controller

a Install Certificate Authority, if necessary.

b Import certificate request and self-signed certificate.

c Issue certificate response to certificate request.

d Get Domain Controller certificate and Certificate Authority certificate.

On WebSphere

a Import Issued certificate.

b Import Domain Controller certificate and Certificate Authority certificate.

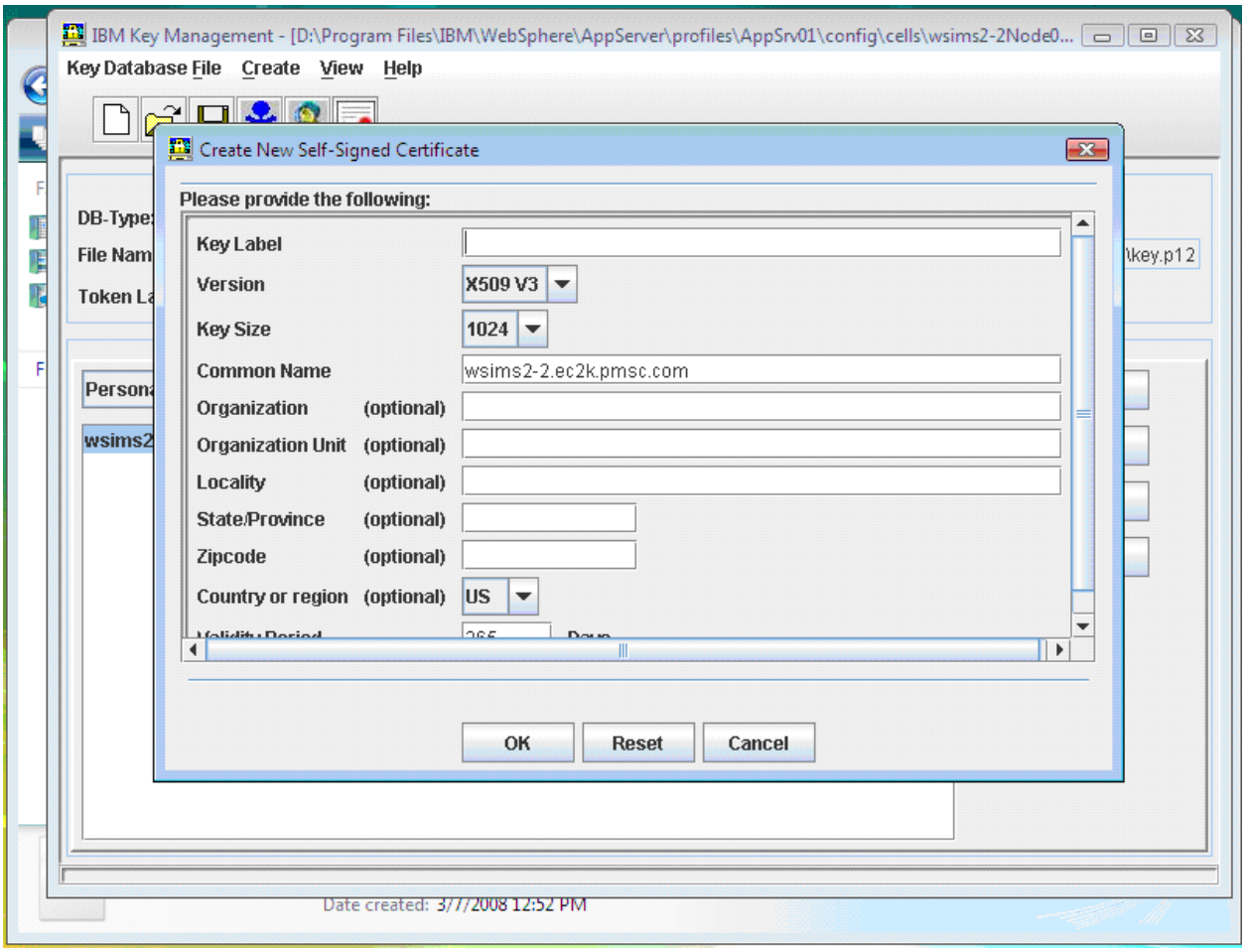
Detailed Steps

Certificate Set-Up

Obtain certificate files for submission.

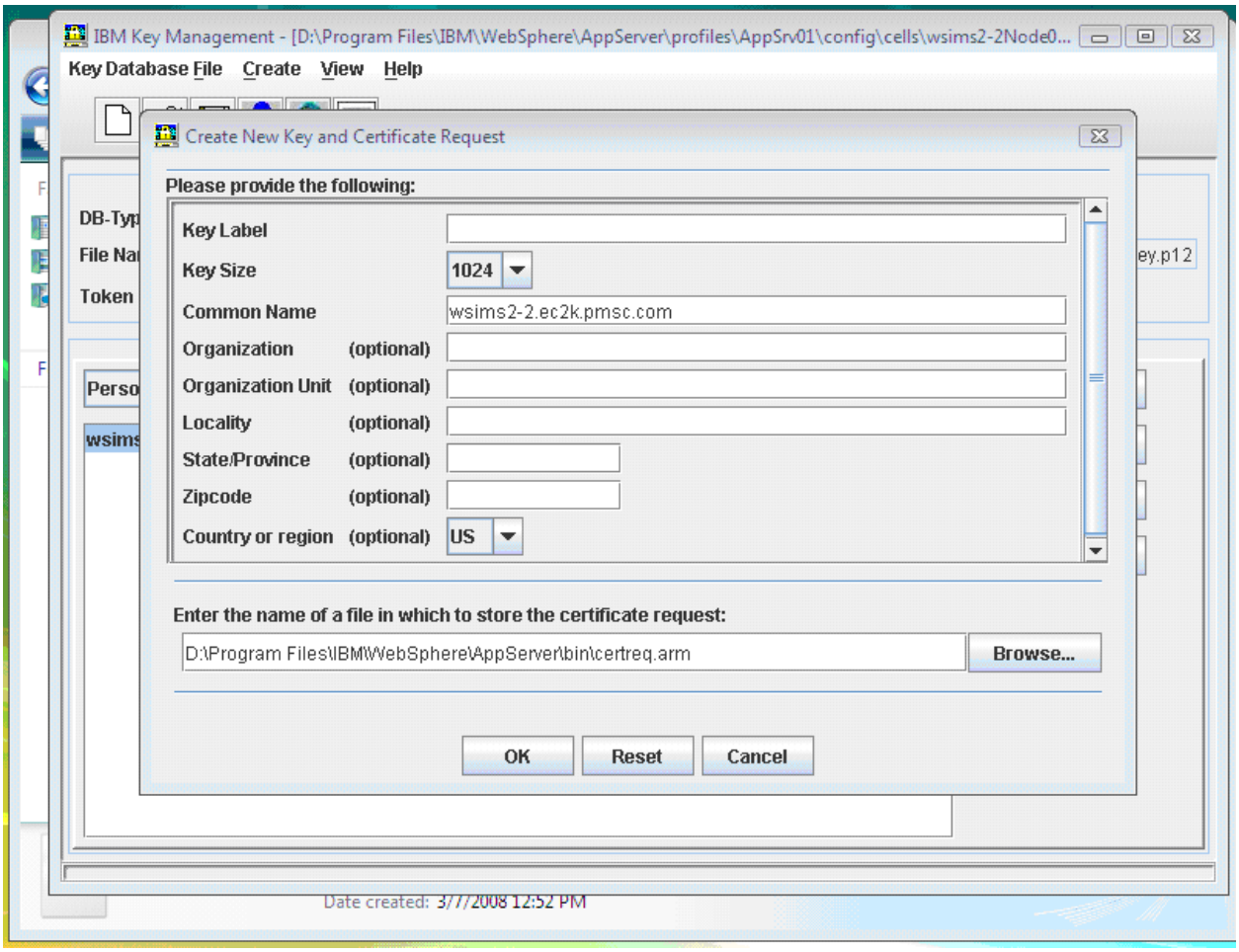
On WebSphere

1. Start Ikeyman (WebSphere/appserver/bin/).
2. Open existing PKCS12 database
3. \Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\config\cells\servernameNode01Cell\nodes\servernameNode01\ key.p12
4. (default password - WebAS)
5. Create new self-signed certificate within key.p12
6. Extract certificate to file. (certificate should be in form of .arm file - ".arm." Base64-encoded ASCII data)



7 Create new Key and Certificate Request.

8 Save request to file. (Certificate should be in form of .arm file - ".arm.")



9 Copy both files to the Certificate Authority Server

On the Domain Controller - 2003 Server (If Not Already Installed)

1 Set up certificate issue authority.

2 Select Add/remove programs.

3 Select Add/remove Windows Components.

4 Click Certificate Services.

5 Click Certificate Services (CA).

6 Click Install.

7 Open a Command Prompt and type the following:


```
certreq -attrib "CertificateTemplate:WebServer"
```

8 Certificate request processor will run.

9 Open file request file that you copied.

10 Open the Certification Authority Application.

11 Navigate to Pending Requests.

12 Issue the request that you submitted.

13 Navigate to Issued Certificates.

14 Double click issued certificate to open it.

15 Click Details.

16 Click Copy to file.

17 The Wizard opens.

18 Select Base 64 choice.

19 Specify File Name.

20 Click Export Finish.

21 Rename the self-signed certificate you copied from.arm to .cer.

22 Double click the renamed file.

23 Click Install Certificate to install the certificate.

24 Open the Certification Authority Application.

25 Navigate to Domain Certificate Name and right click to select Properties.

26 Select View Certificate.

27 Select Details.

28 Select Copy to file.

29 Certificate Export Wizard pops up.

30 Select Base-64.

31 Export the Certificate Authority Certificate.

32 Navigate to Issued Certificates.

33 Double click the Domain Controller certificate to open it.

34 Click Details.

35 Click Copy to file.

36 The Wizard opens.

37 Select Base 64 choice.

38 Specify File Name.

39 Click Export Finish. Windows is now complete.

40 Copy the three file from the Certificate Authority to the WebSphere server

   a The issued request created in response to the request issued from WebSphere

   b The Domain Controller Certificate

   c The Certificate Authority Certificate

Within Java (WebSphere)

Import Certificates into WebSphere Server Using Ikeyman

1 Start Ikeyman (WebSphere/appserver/bin/).

2 Open existing PKCS12 database

3 \Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\config\cells\servernameNode01Cell\nodes\servernameNode01\key.p12

4 (default password - WebAS)

5 Import private certificate.

6 Select signer certificates from (middle) drop-down.

7 Click Add… button.

8 Select file that contains the private certificate from CA (Certificate Authority).

9 Select Personal Certificates from (middle) drop-down.

10 Click Receive button.

11 Select public certificate file from previously exported personal certificate request. (Note: This is the keystore that WebSphere will use for SSL transport.)

12 Open existing PKCS12 database

13 \Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\config\cells\servernameNode01Cell\nodes\servernameNode01\trust.p12

14 (default password - WebAS)

15 Import Domain Controller and Certificate Authority certificates.

16 Select signer certificates from (middle) drop-down.

17 Click Add… button.

18 Select file that contains the Certificate Authority certificate.

19 Click Add… button.

20 Select file that contains the Domain Controller certificate.

Java (Add Certificates to JVM Keytrust)

1 Open Ikeyman.

2 Open cacerts keytrust from folder:

WebSphere/appserver/java/jre/lib/security/cacerts (jks)

3 Default password is changeit.

4 Import Domain Controller and Certificate Authority certificates into existing JVM keytrust.

5 Restart WebSphere.

6 Make sure Agency Link is set to send and receive from the host, and then test.

Documentation Reference: *Content for this chapter is copied from SSO Reference Guide, chapter "Communications Framework: SSL Certificate Set-Up UIsing IBM WebSphere."*

Index

A

Audience 6

C

Certificate 13, 14, 15, 15
Certification Authority (CA) 13, 14
Communications Framework (CFW) 13, 17, 18, 30, 30, 32, 35, 36, 39, 50, 50, 52, 54, 55, 57, 64, 65, 68, 68, 70, 72, 73, 75
Customer Service 2

D

Demilitarized Zone (DMZ) 17, 17, 25, 27, 29, 30, 32, 34, 35, 36, 38, 39, 40, 42, 43, 44, 46, 47, 49, 50, 52, 54, 54, 55, 56, 57, 58, 60, 62, 63, 64, 65, 66, 67, 68, 70, 72, 72, 73, 74, 75

E

Encryption 13, 14, 15, 77

F

Firewall 8, 17, 17, 25, 27, 29, 30, 32, 33, 35, 36, 37, 39, 40, 42, 43, 44, 46, 47, 48, 49, 50, 52, 53, 54, 55, 56, 57, 58, 60, 61, 62, 63, 64, 67, 68, 70, 71, 72, 73, 74, 75

H

Hardening Your Web Site 7, 8, 17, 25, 29, 35, 39, 40, 44, 49, 54, 57, 58, 63, 65, 67, 72, 75
HTTP 18, 30, 41, 45, 50, 59, 68
HTTPS 13, 18, 30, 41, 45, 50, 59, 68, 76

K

Key 13, 14, 15, 76, 77

M

Microsoft 10, 12, 15, 27, 32, 33, 35, 36, 37, 42, 43, 46, 47, 52, 53, 55, 56, 60, 61, 64, 70, 71, 73, 74

N

Netscape 13, 15
Network Address Translation (NAT) 8

S

Secured Sockets Layer (SSL) 13, 14, 15, 19, 30
SQL Server 12, 18, 30, 33, 37, 41, 43, 47, 50, 53, 56, 61, 68, 71, 74

T
Technical Support **2**

V
Virtual Private Network (VPN) **9**

W
Web server **7**, **13**, **14**, **15**, **34**, **36**, **43**, **54**, **55**, **65**, **72**, **73**, **77**

Document Change Log

Date	Release for which change made	Heading and subheading where change made	Description	Initials