IBM Software Group

2005 B2B Customer Conference

Pioneering New Horizons – Solutions that Evolve

Securing Your B2B Deployment

Rich Kinard, Sr. Consulting IT Architect

Rajeev Kapoor, Sr. IT Specialist

Objectives

- Gain an understanding of the four areas of security as related to WebSphere Partner Gateway Enterprise (WPG).
- Describe multiple secure deployment options
- Demonstrate where each security area is applied in WebSphere Partner Gateway Enterprise

IBM Software Group

WebSphere Partner Gateway Security

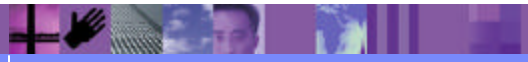
WebSphere. software

ON DEMAND BUSINESS

WPG Areas of Security

When organizations focus on combining the following areas, security policies can be defined to establish a secure baseline so that they can trade on the Internet with greater confidence.

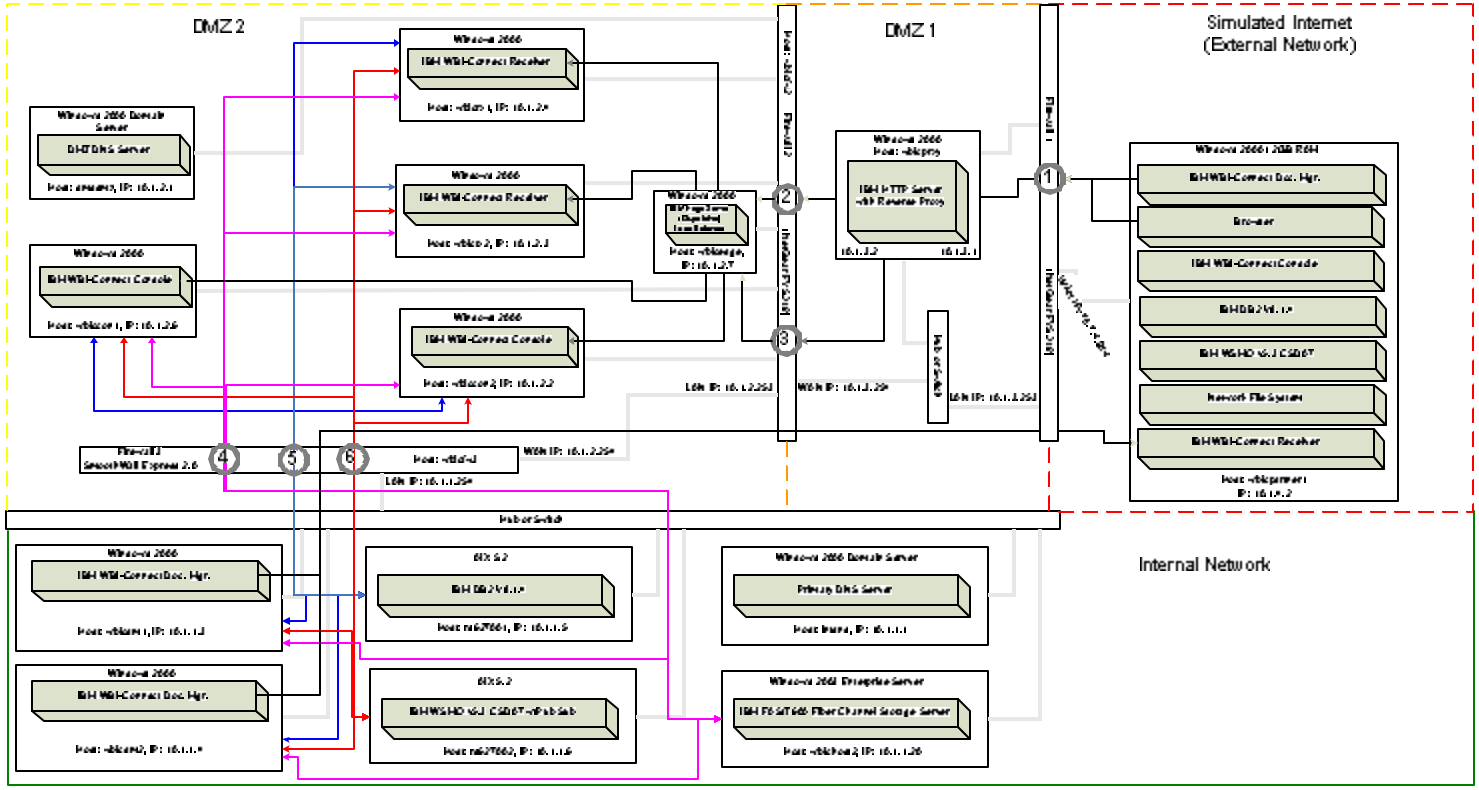
- **Deployment Security**
  Deployment security is the placement of hardware within an existing network with access to the Internet. This includes database servers, file shares, message queue servers, and integration servers.
- **Connection Security**
  Connection security involves establishing a secure connection between trading participants over a Secure Socket Layer (SSL) connection.
- **Document Security (Data Security)**
  Document or Data security involves utilizing X509 Certificates to encrypt and sign messages prior to sending them to trading partners and to verify signature and decrypt messages received from trading partners.
- **Access Control**
  Access control provides utilizes username, password and company credentials allowing access to data and configuration information inside the B2B application.



Deployment Security

- To protect B2B applications from unauthorized access, networking and firewall protection should be established. Firewalls work in conjunction with proxy servers, providing the ability to filter protocols, addresses, communication ports and IP packets.
- The security model that can be used is the establishment of a De-Militarized Zone (DMZ). In many cases multiple DMZ's are used to provide a more secure Internet gateway.
- For WebSphere Partner Gateway, the Document Manager should be placed in the most secure part of the network, and the Receiver and Console can be placed in the DMZ depending on the customer's security requirements.

Deployment Security – DMZ Example



Connection Security

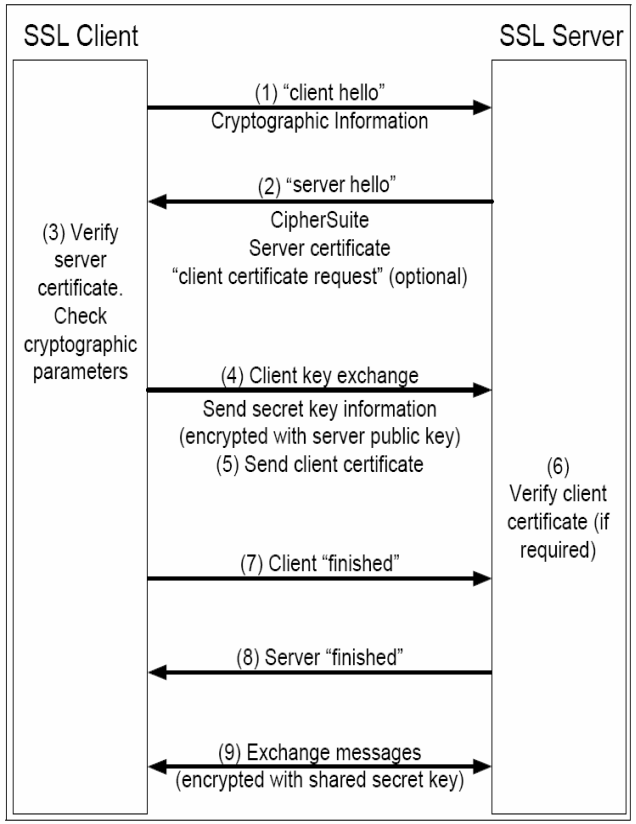
- A common method of transferring information security on the Internet is using the Secure Sockets Layer (SSL). It uses encryption-based on the public and private key model, using authentication with basic or extended handshakes. SSL works by creating a secure connection between communicating applications over HTTP.

- The SSL protocol addresses the following security issues:
  - **Privacy:** After the symmetric key is established in the initial handshake, the messages are encrypted using this key.
  - **Message Integrity:** Messages contain a message authentication code (MAC) ensuring the message integrity.
  - **Authentication:** During the handshake, the client authenticates the server using an asymmetric or public key.

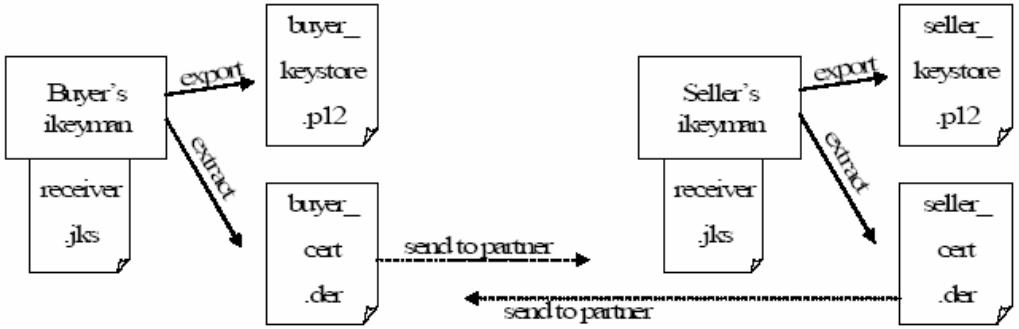
- SSL works well when securing browser-based applications, like the administrative console in WebSphere Partner Gateway, but it can also be useful to augment B2B document transfer.

Secure Socket Layer Handshake

1. The SSL client sends a *client hello m*essage that lists cryptographic information such as the SSL version and, in the client's order of preference and the CipherSuites supported by the client.
2. The SSL server responds with a *server hello* message that contains the cryptographic method (CipherSuite) chosen by the server from the list provided by the SSL client, the session ID and another random byte string.
3. The SSL client verifies the digital signature on the SSL server's digital certificate and checks that the CipherSuite chosen by the server is acceptable.
4. The SSL client sends the random byte string that enables both the client and the server to compute the secret key to be used for encrypting subsequent messages. The random byte string itself is encrypted with the server's public key.
5. If the SSL server sent a *client certificate request*, the SSL client sends a random byte string encrypted with the client's private key together with the client's digital certificate, or a *no digital certificate alert.*
6. The SSL server verifies the signature on the client certificate.
7. The SSL client sends the SSL server a *finished* message encrypted with the secret key, indicating that the client part of the handshake is completed.
8. The SSL server sends the SSL client a *finished* message encrypted with the secret key, indicating that the server part of the handshake is completed.
9. For the duration of the SSL session, the SSL server and SSL client can now exchange messages that are symmetrically encrypted with the shared secret key.



WPG SSL Configuration



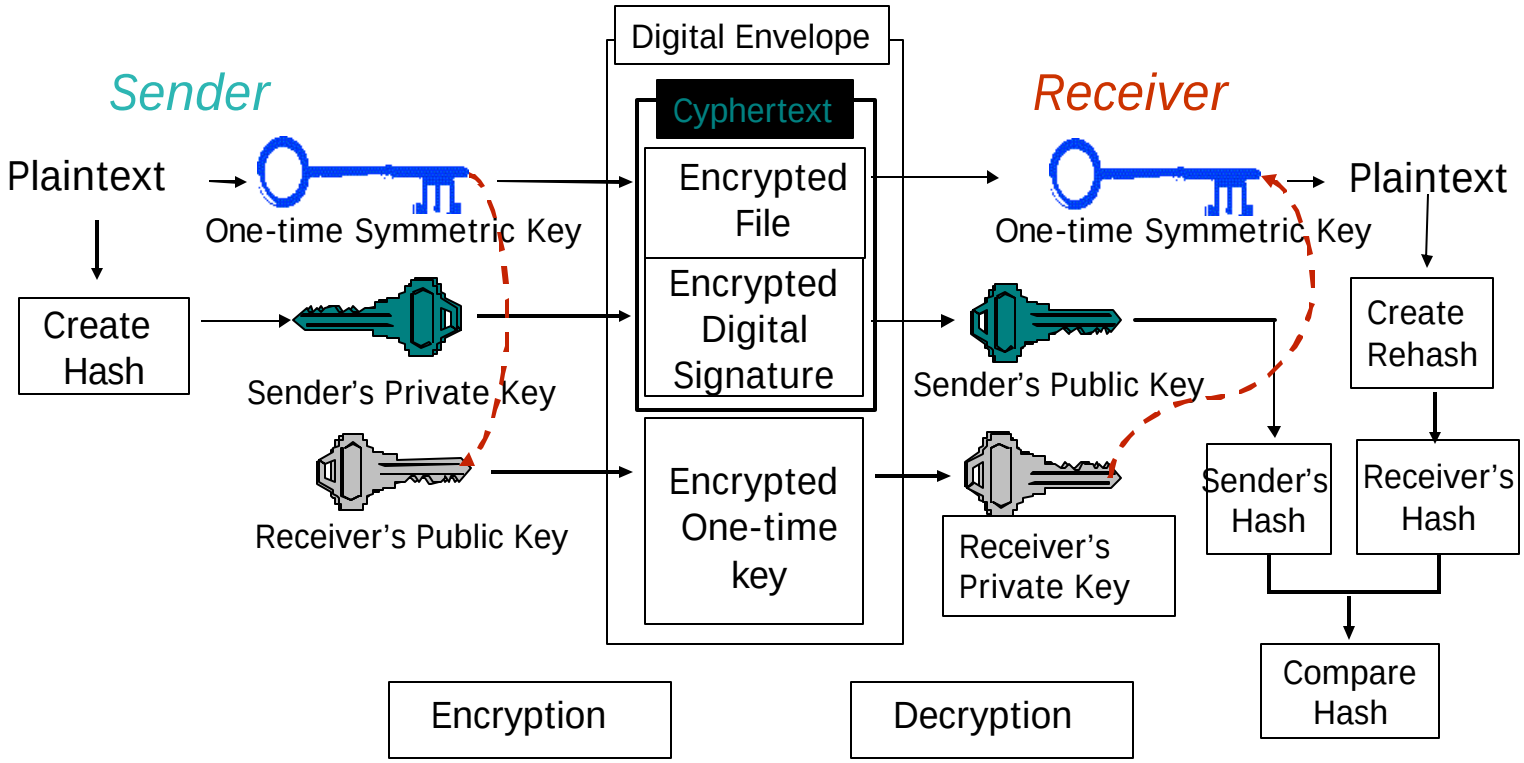
	Buyer's WPG Config	Seller's WPG Config
Outbound Server SSL	If self-signed, load seller_cert.der as Operator's Root Cert. If using a CA-signed certificate, load CA's certificate in Operator's Root Cert.	If self-signed, load buyer_cert.der as Operator's Root Cert. If using a CA-signed certificate, load CA's certificate in Operator's Root Cert.
Inbound Server SSL	Create a certificate in ikeyman's receiver.jks for Embedded WAS	Create a certificate in ikeyman's receiver.jks for Embedded WAS
Outbound Client SSL	Load buyer_keystore.p12 as Hub Operator's PKCS12 'SSL Client' Certificate	Load seller_keystore.p12 as Hub Operator's PKCS12 'SSL Client' Certificate
Inbound Client SSL	Load seller_cert.der in ikeyman's receiverTrust.jks. If using a CA-signed certificate, also load CA's certificate into receiverTrust.jks. Run bcgClientAuth.jacl script to make Client SSL enabled	Load buyer_cert.der in ikeyman's receiverTrust.jks. If using a CA-signed certificate, also load CA's certificate into receiverTrust.jks. Run bcgClientAuth.jacl script to make Client SSL enabled

Document/Data Security

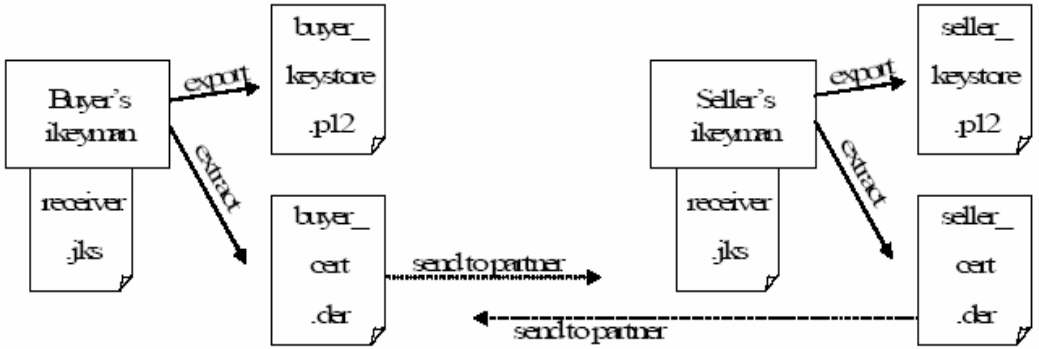
- The Document Manager is the security management component of WebSphere Partner Gateway that encrypts messages at the document level, and provides signed digital receipts. Supported security methods include Entrust, VeriSign, and self-signed certificates.

- Document security provides the following features:
  - **Privacy:** A document is encrypted by the recipient's public key. Only the recipient has the appropriate private key to decrypt the message.
  - **Authentication:** The recipient can authenticate the sender of a document by verifying a digital signature.
  - **Integrity:** A digital signature of the document provides document integrity.
  - **Nonrepudiation:** Nonrepudiation is provided using digital signatures and encrypting the hash value with the receiver's private key then sent back to the sender. This provides a digital receipt to the sending party.

Hybrid Security Processing



WPG Data Security Configuration



	Buyer's WPG Config	Seller's WPG Config
Outbound Signature	Load buyer_keystore.p12 as Hub Operator's PKCS12 Digital Signature Certificate.	Load seller_keystore.p12 as Hub Operator's PKCS12 Digital Signature Certificate.
Inbound Signature	Load seller_cert.der into Seller's Dig Sig Cert. Also load signer of seller_cert.der certificate (seller_cert.der for self-signed and CA's *.der for CA signed) as Operator's Root Certificate.	Load buyer_cert.der into Buyer's Dig Sig Cert. Also load signer of buyer_cert.der certificate (seller_cert.der for self-signed and CA's *.der for CA signed) as Operator's Root Certificate.
Outbound Encryption	Load seller_cert.der into Seller's Encryption Certificate	Load buyer_cert.der into Buyer's Encryption Certificate
Inbound Decryption	Load buyer_keystore.p12 as Hub Operator's PKCS12 Encryption Certificate	Load seller_keystore.p12 as Hub Operator's PKCS12 Encryption Certificate

Access Control Security

- WebSphere Partner Gateway uses a role-based approach for access control. The three roles implemented in WebSphere Partner Gateway are Community Manager, Community Operator and Community Participant.

- The rights, permissions, and privileges for each role can be defined through group accounts. The three roles are nested. For example, the Community Manger has overall access to the system and Peer Participants. The Community Participant only has access to his specific trading relationship. Users log in by providing their Company Name, User ID, and Password. The log in determines individual access privileges. The WebSphere Partner Gateway browser interface, used for administering functions, can operate over an SSL connection.

3 Participant Roles

Community Participant

- External business partners to the B2B gateway
- Can be as many defined as desired
- Each one is a single connection to the B2B gateway

Community Manager

- Also a participant, but is the principle one
- Can only be one for a single B2B Gateway
- Operational manager for the community

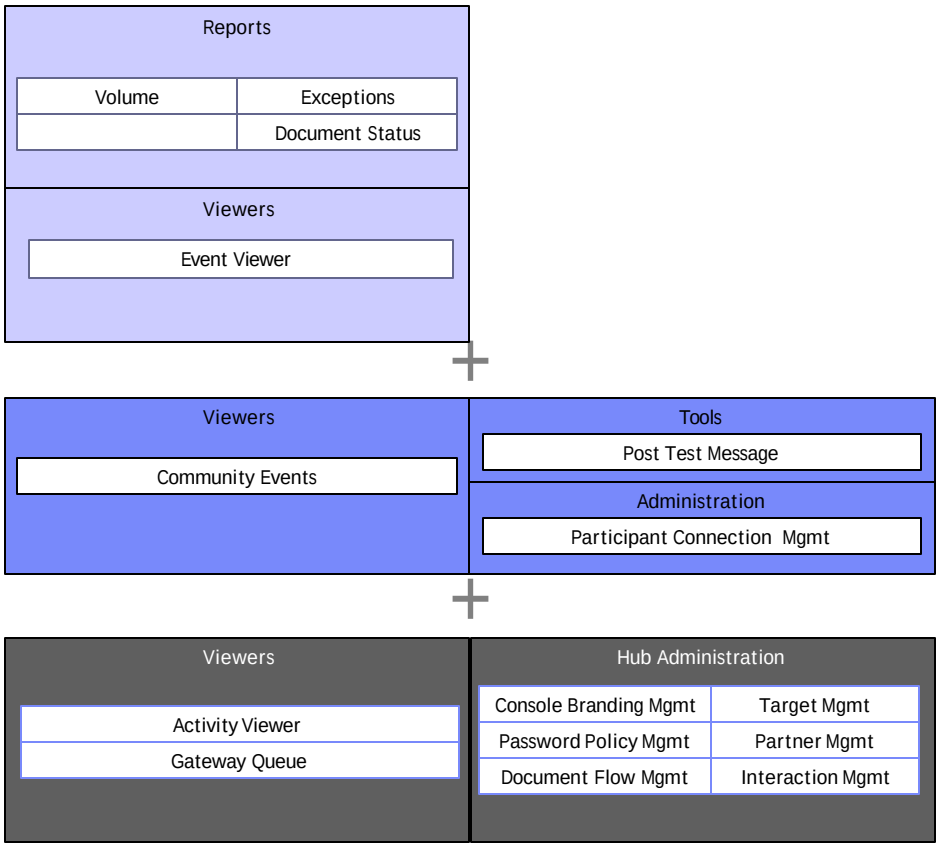
Community Operator

- Pre-defined – cannot be deleted
- “sysadmin” for the B2B Gateway
- Defines and maintains the B2B Gateway’s capabilities
- Typically does NOT send or receive documents

3 Views of System Data

Community Manager Console

Community Operator Console



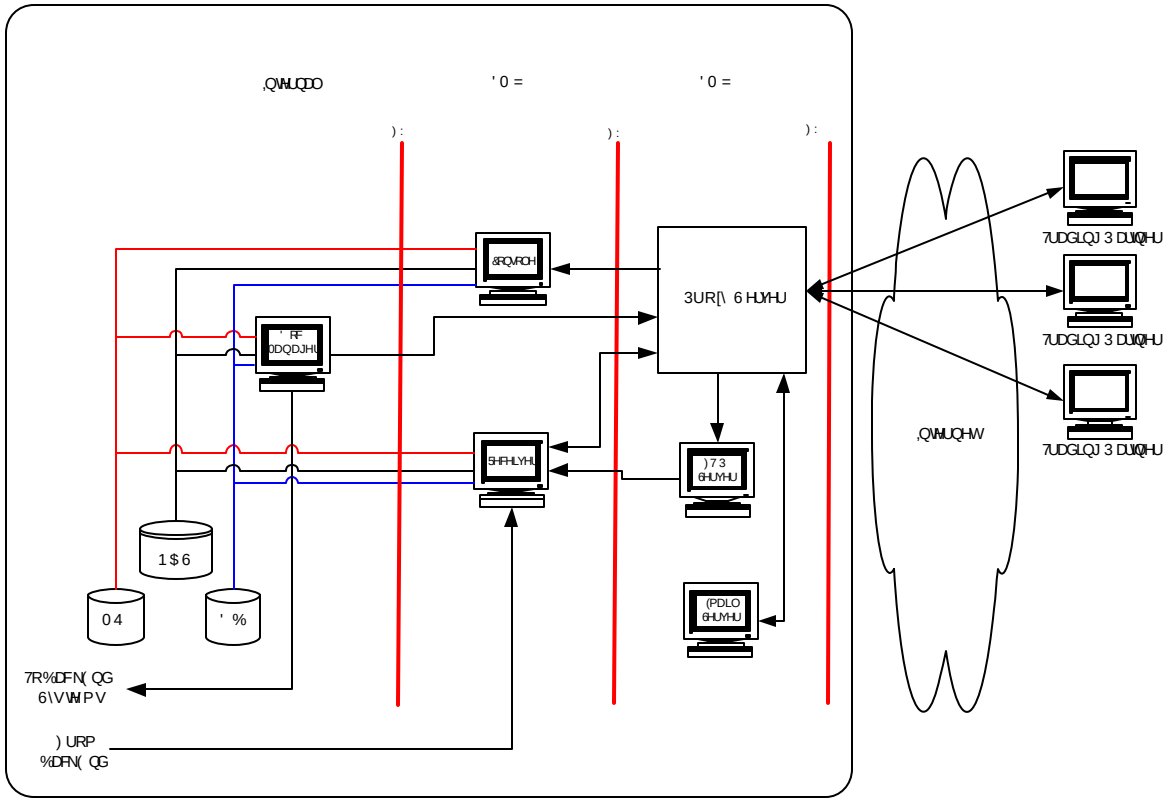
IBM Software Group

Common Secure Deployment Scenarios

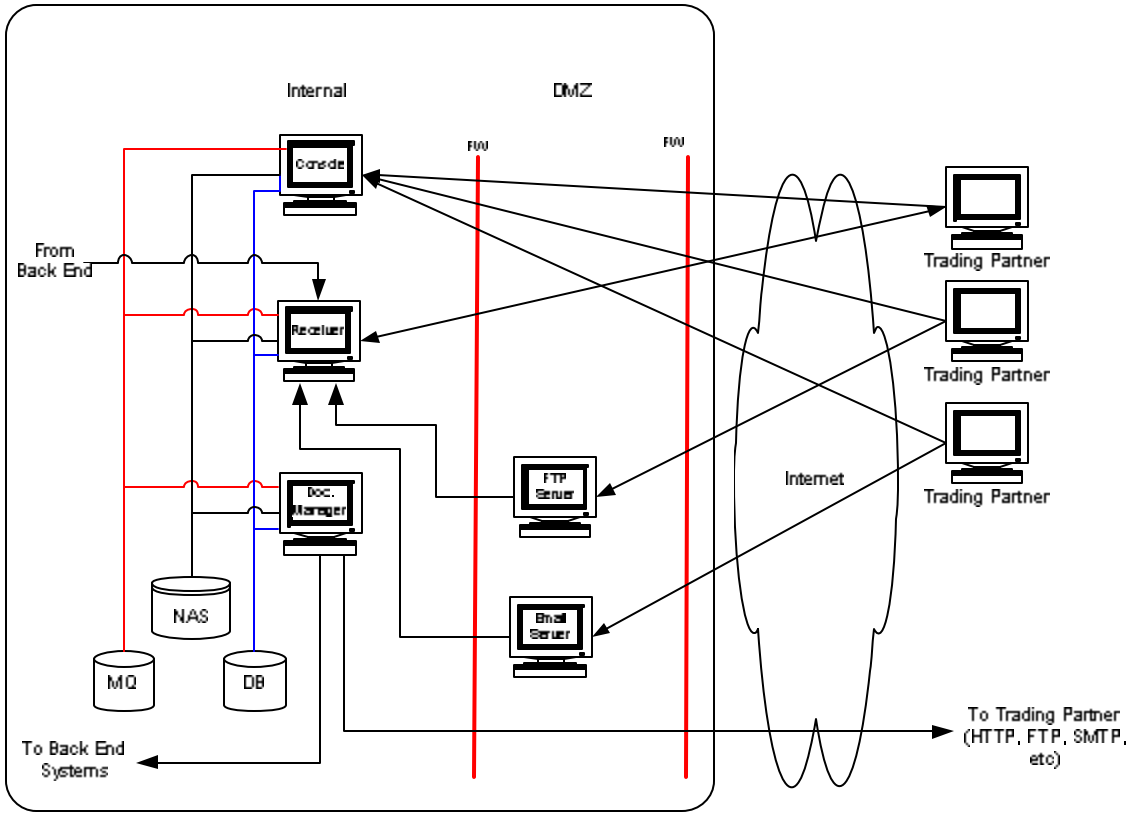
WebSphere. software

ON DEMAND BUSINESS

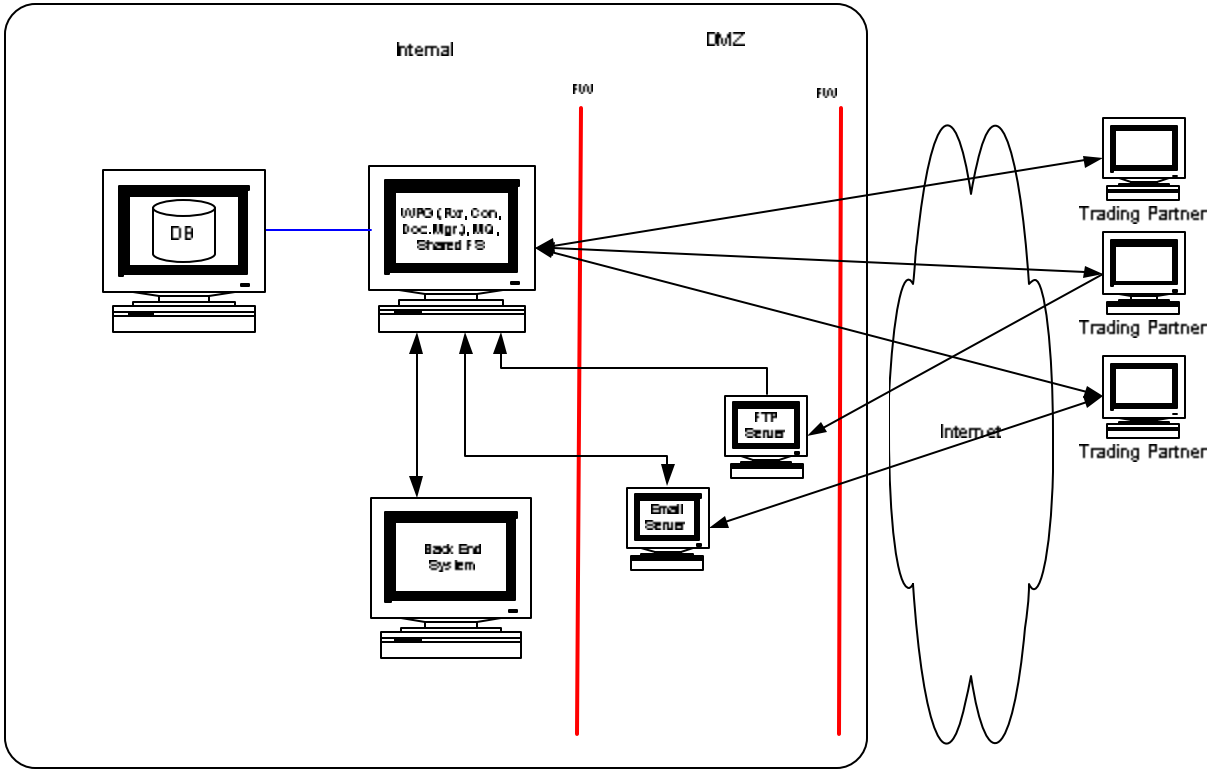
Dual DMZ with Forward & Reverse Proxy - Distributed



Single DMZ - Distributed in Internal Network



Single DMZ – Single Machine – Distributed DB



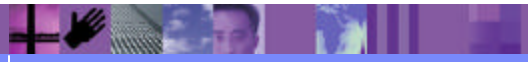
Demonstration

WebSphere. software

ON DEMAND BUSINESS

Demo Overview

- Access Control
  - Login Process
  - Password Policies
  - Users/Groups Permissions
- Document Security
  - Certificate Management
  - Enabling Signatures
  - Enabling Encryption
- Connection Security
  - Ikeyman (Certificate Creation)
  - Reciever.jks/Console.jks
  - ReceiverTrust.jks/ConsoleTrust.jks



Summary

- Securing your deployment requires a good understanding of all of the areas of security that work together to ensure your security policies are not violated when deploying B2B technologies.
- The are many ways to deploy WPG, the best fit for your company is going to depend on your company's security requirements and policies.
- WPG provides the flexibility needed in the key areas of security to allow you to distribute our B2B software in complex networks and also by providing access control, connection security and data security.

Helpful Information

- **Redbooks**
  - ***B2B Solutions using WBIC v4.2.2,*** http://www.redbooks.ibm.com/abstracts/SG246355.html?Open
  - ***Secure Production Deployment of B2B Solutions using WBIC,*** http://www.redbooks.ibm.com/abstracts/SG246457.html?Open
  - ***B2B Solutions using WPG v6.0,*** http://www.redbooks.ibm.com/redpieces/abstracts/sg247109.html?Open
- **User Documentation**
  - http://www-306.ibm.com/software/integration/wspartnergateway/library/infocenter/
- **Education**
  - ***IBM Education Assistance,*** http://www-306.ibm.com/software/info/education/assistant/flow/wpg/6.0/
  - ***Implementing WebSphere Partner Gateway (BI154),*** http://www-304.ibm.com/jct03001c/services/learning/ites.wss/us/en?pageType=course_search&sortBy=5&searchType=1&sortDirection=9&includeNotScheduled=15&rowStart=0&rowsToReturn=20&maxSearchResults=200&searchString=bi154&language=en&country=us
  - ***WebSphere Partner Gateway – Client Mapping for EDI (SW338),*** http://www-128.ibm.com/developerworks/websphere/education/enablement/curriculum/sw338.html
- **Support**
  - http://www-306.ibm.com/software/integration/wspartnergateway/enterprise/support/