Security in integration and Enterprise Service Bus(ESB)

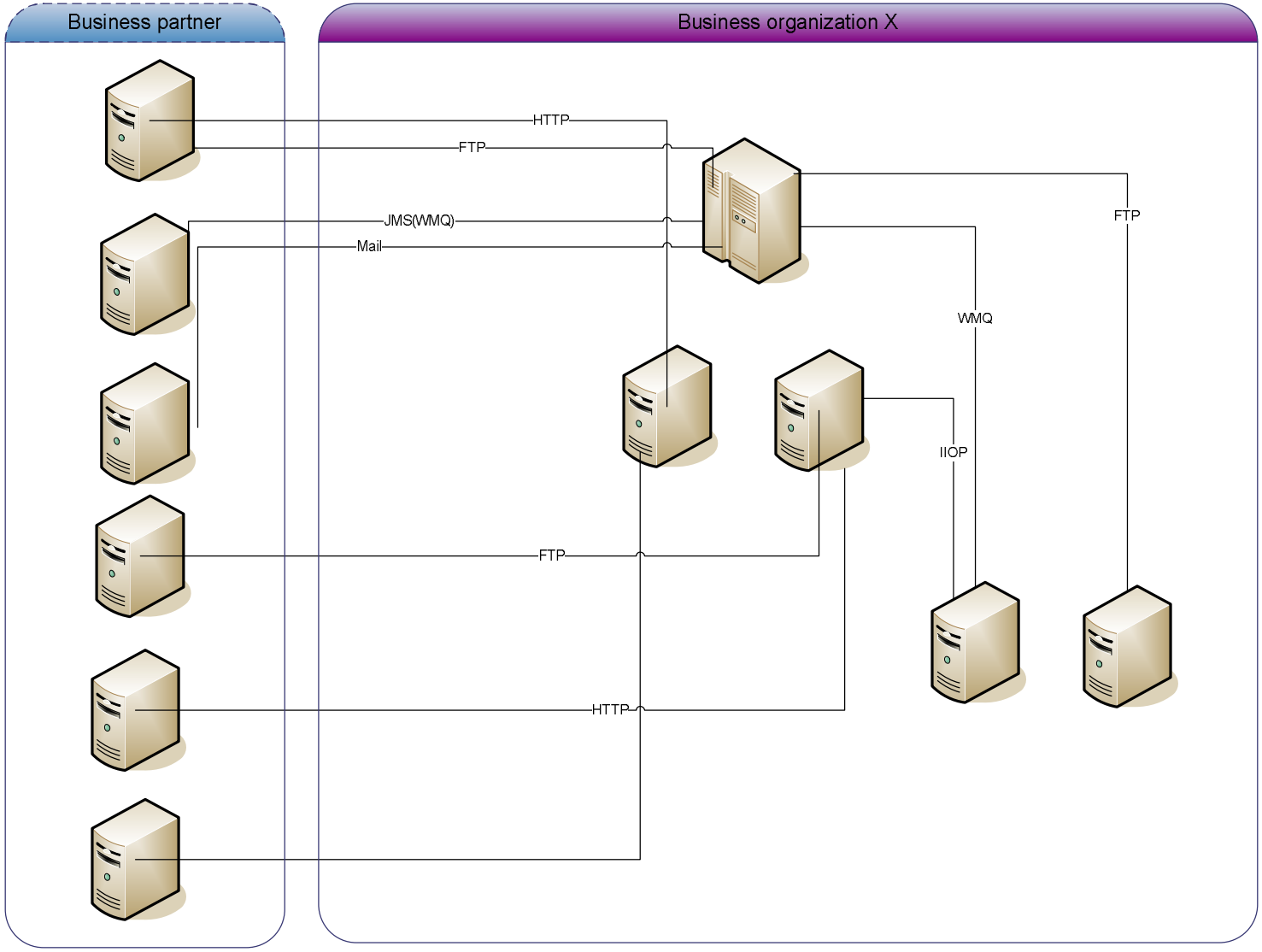
Anton Panhelainen
Principal Technology Consultant
Tieto Oy
anton.panhelainen@tieto.com

About Anton Panhelainen

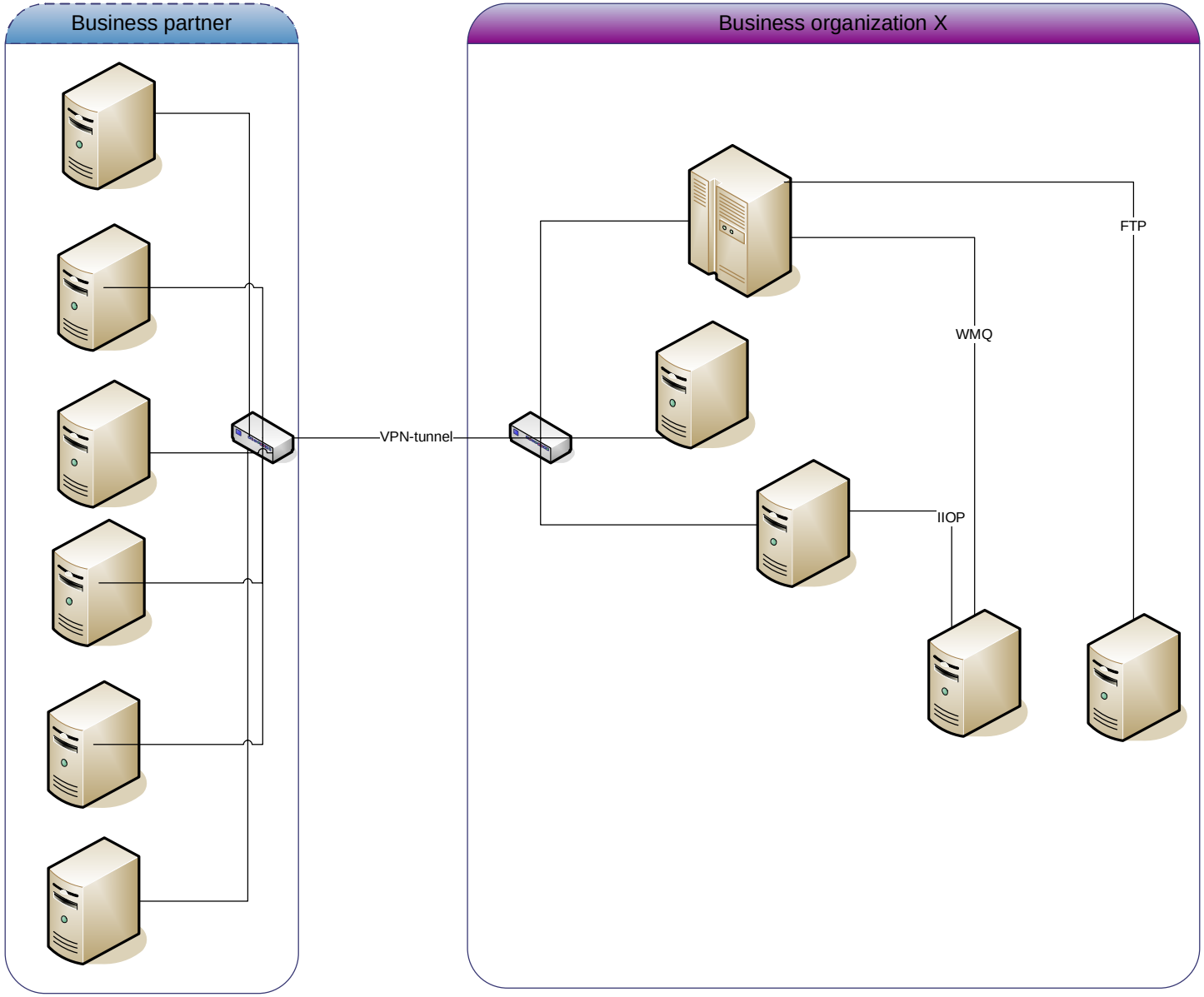
- 12 years of experience building mission-critical, high availability systems integrations and architectures
  - Not an end-user applications kinda guy
- 10 years of Java experience
  - Before that C and C++
- Open source fan
- TOGAF 8.1.1 Certified Architect
  - five other certificates on integration techlogies and appservers
- Commited to ESB(that doesn't only mean extra strong bitter)

Styles of messaging differ

Common way of integration using point-to-point messaging



Common security solution in point-to-point messaging



tieto.com

Point-to-point messaging and VPN security issues

- Protocol specific authentication and authorization(if any)
- Demands a lot of virtual private network(=VPN) definitions
- Security model of communications is not centralized
  - Lacks common way for auditing
  - Border between partner accessiable and security zone is not clear
- VPN secures only communication's tunnel
  - If all commucation ports are allowed from partner network points of intrusion multiply
    - VPN needs also Firewalling to secure network.

Security issues - Internet Inter-ORB protocol(IIOP)

- Common secure interoperability v2(CSIv2)
  - Secure interoperability is based on common transport layer security mechanism(SSL/TLS)
  - Transport layer provides message protection for IIOP

Security issues - File Transfer Protocol(FTP)

- FTP is still widely used in enterprises.
- Doesn't have file checksum(hash code calculation)
  - Business partner spesific agreements and solutions have been developed
- Doesn't have secure communications
  - Secure-FTP secures communications and also it provides file checksums.

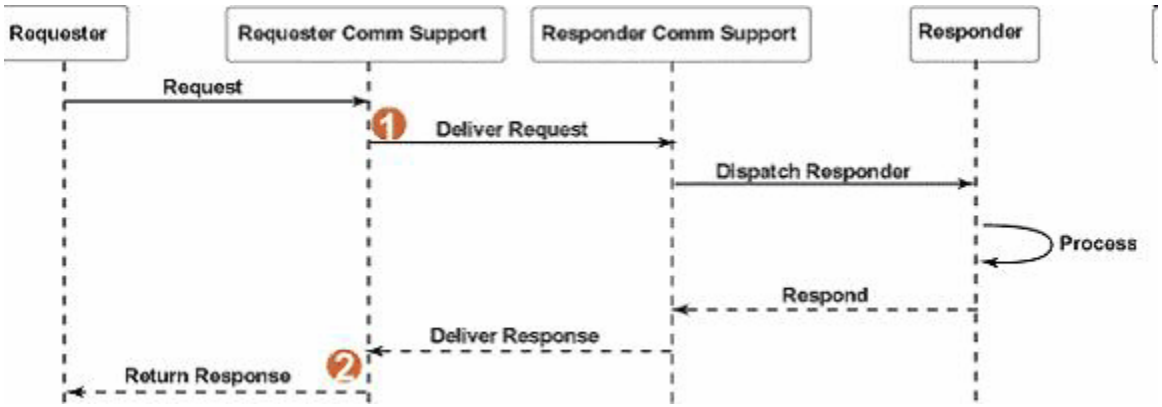
Security issues - Email

- Email has no confidentiality
  - This problem can solved by using
    - Secure/MIME(Secure Mime)
    - Pretty Good Privacy(PGP)
    - COTS-solutions
      - F-Secure Messaging Security Gateway
      - Mailfrontier
      - Ciphertrust
      - etc

Security issues - HTTP

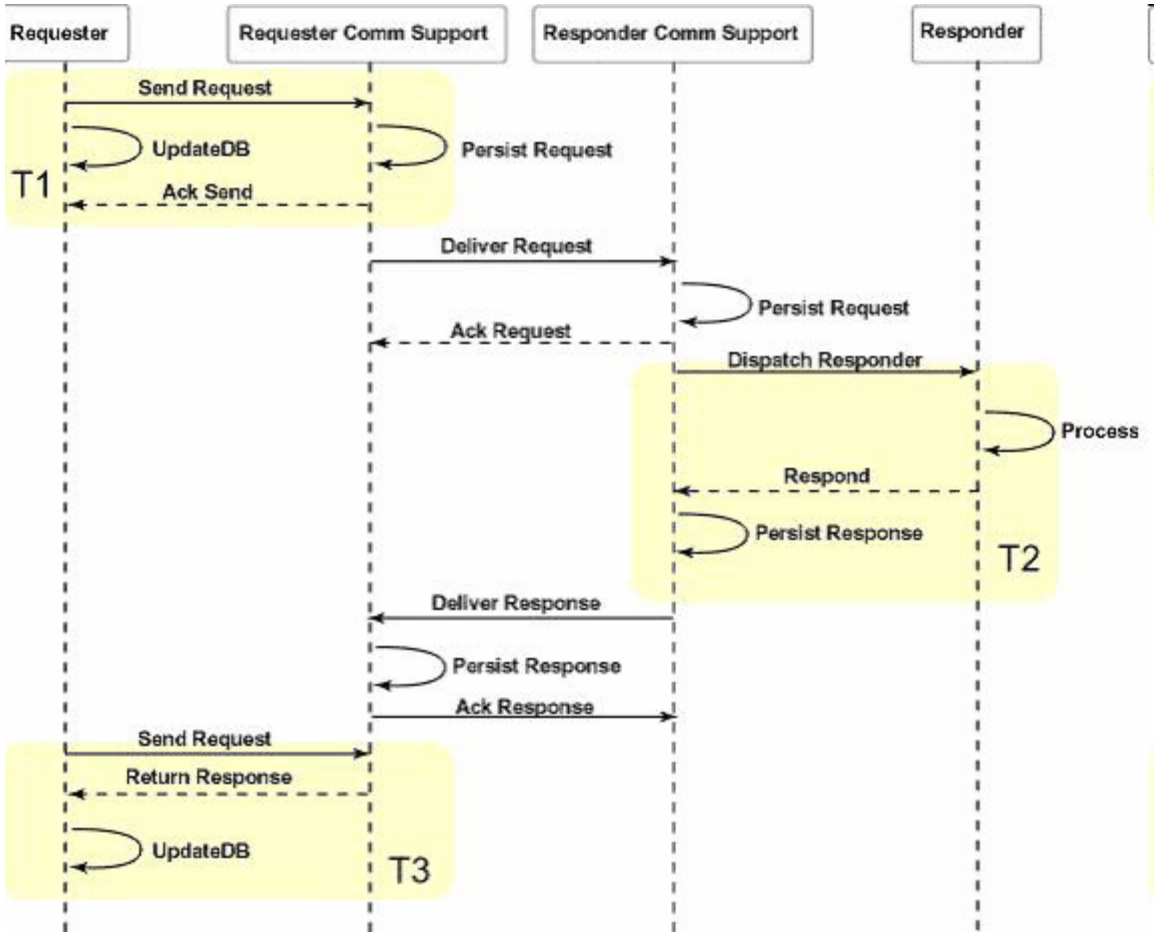
- HTTP has basic authentication, but it is not strong enough for securing message
- SSL with client authentication provides strong authentication
- Vulnerable to denial of service(=DOS) attacks
  - Hardware based security gateways that can detect DOS attack
- Using HTTP to deliver messages need that those systems have high and continuous availability

HTTP Problem - Syncronous message delivery



- If commucation breaks between requester and responder during message delivery, message might get lost or duplicated
  - To reduce that risk it's vital that those systems have high and continuous availability
- There was a proposal to improve HTTP.
  - HTTP-Reliable(2001)
    - no industry support nowadays

Protocol level solution for syncronous message delivery(HTTP-Reliable)



Problem: Message delivery Assurance

- Messages should be delivered once(not zero times) and only once(no duplicates)
- Is synchronous communication really needed?
  - Most of the cases it's not.
- Better way to guarantee message delivery is design your systems to communicate asynchronous messaging between systems.
- Ways of implement asynchronous messaging
  - For example JMS, Webpshere MQ, TIBCO etc
- Syncronous on HTTP
  - WS-reliable messaging

Problems with WS Reliable messaging

- W3C recommendation for WS Reliable Messaging has written protocol neutral
  - That means it cannot utilize transport layer possibilities
  - After retry count has exceeded message is discarded by default
    - Coding is needed to handle those situations
  - Asyncronous messaging framework doesn't have that problem.

Security issues in Java Messaging Service(=JMS)

- JMS specification doesn't provide any security mechanisms for authentication and/or authorization
- All security implementations are provider specific.
  - JMS messaging between providers is interoperable as long as no protocol level security is needed
    - Specify JMS Provider or use message level security(in SOAP over JMS)

Websphere MQ

- Most used message oriented middleware(MOM) in enterprises
- JMS provider
- Only way to do strong authentication in WMQ is public key infrastructure. UserID and password validation are not supported without extra coding or product called WMQ Extentended security

Message format threats: Custom formats

- Many older message formats still exits
  - Industry specific
  - B2B specific
- Most of these do not have any message integrity or/and checking mechanism
  - Use Transport protocol supports security

Message formats threats: XML

- WS services without WS-Security are easy to tamper when transport layer doesn't provide message integrity
- Binary XML-message transfers allows viruses travel along.
  - When not encrypting message use protocol that has external encoding i.e. character transfers.
    - Character conversion will render viruses harmless

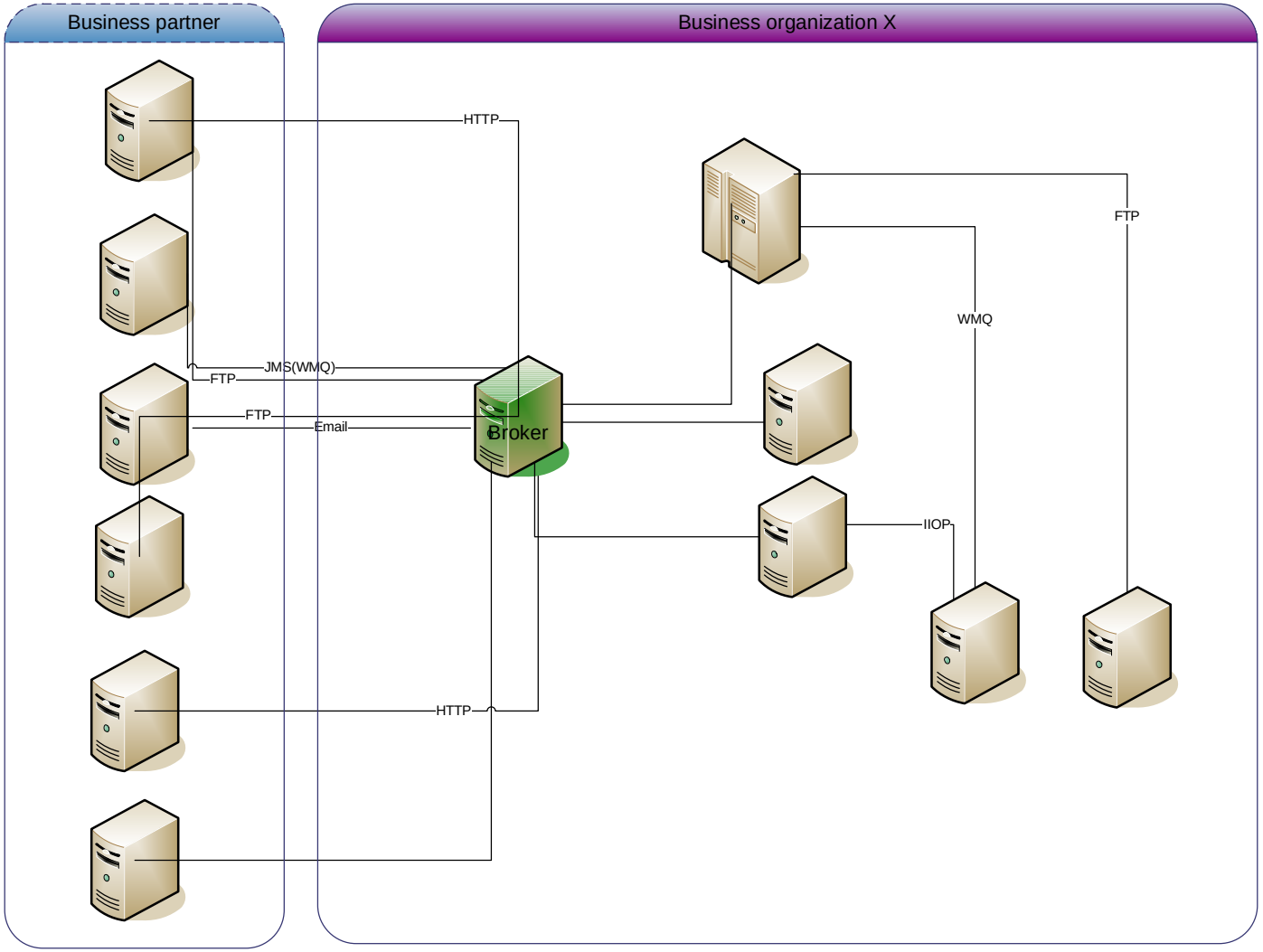
Message formats threats: XML - slide 2

- WS-Security X.509 profile uses underlaying crypto APIs
  - Binary is encrypted same way as text when it's inside data tag
  - Be aware that viruses, cross site scripts, sql injections etc will be encrypted same way as data
- Input validation is needed - i.e. XML Schema Definition(XSD) validation(even though it's expensive in terms of prosessing power) should be done before prosessing data
- XSD strong typing with acceptable characters is needed
  - For example: Gothic number 900 is in Unicode-16 Character set, but should that be valid input

Point-to-point vs. end-to-end security in messaging

- Point-to-point messaging secures communications between business partners
  - Origin of the data message is business partner(identified as organization)
  - Message level and transport layer security can used
- End-to-end messaging security
  - Origin of the data message is business partner service requestor and
    - With message level security this is hard to archive unless originating systems use same format all the ways.
  - Transport layer security can only archived using federated security ie. both business-partners access management software have trust each other and able to federate identities

Common Integration pattern using Message Brokering(hub-and-spoke)



tieto.com

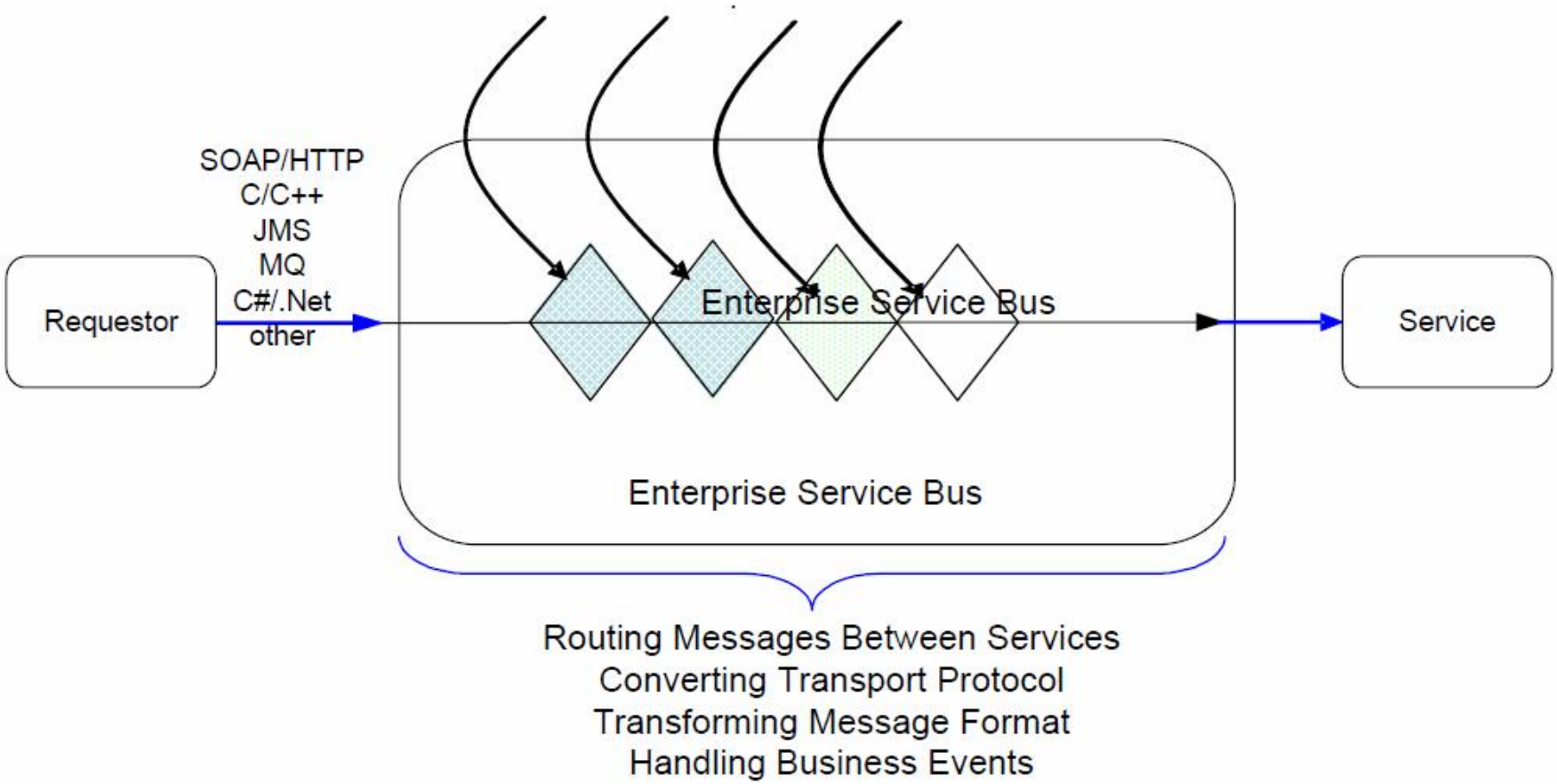
Problems and solutions in message brokering

- More integration is centralized
  - Security is still protocol specific
- Different channels are supported via adapters
  - Security solutions in adapters are depedent in adapters implementation
- Message Brokering typically is solution for transforming and routing.
  - It is not a security gateway

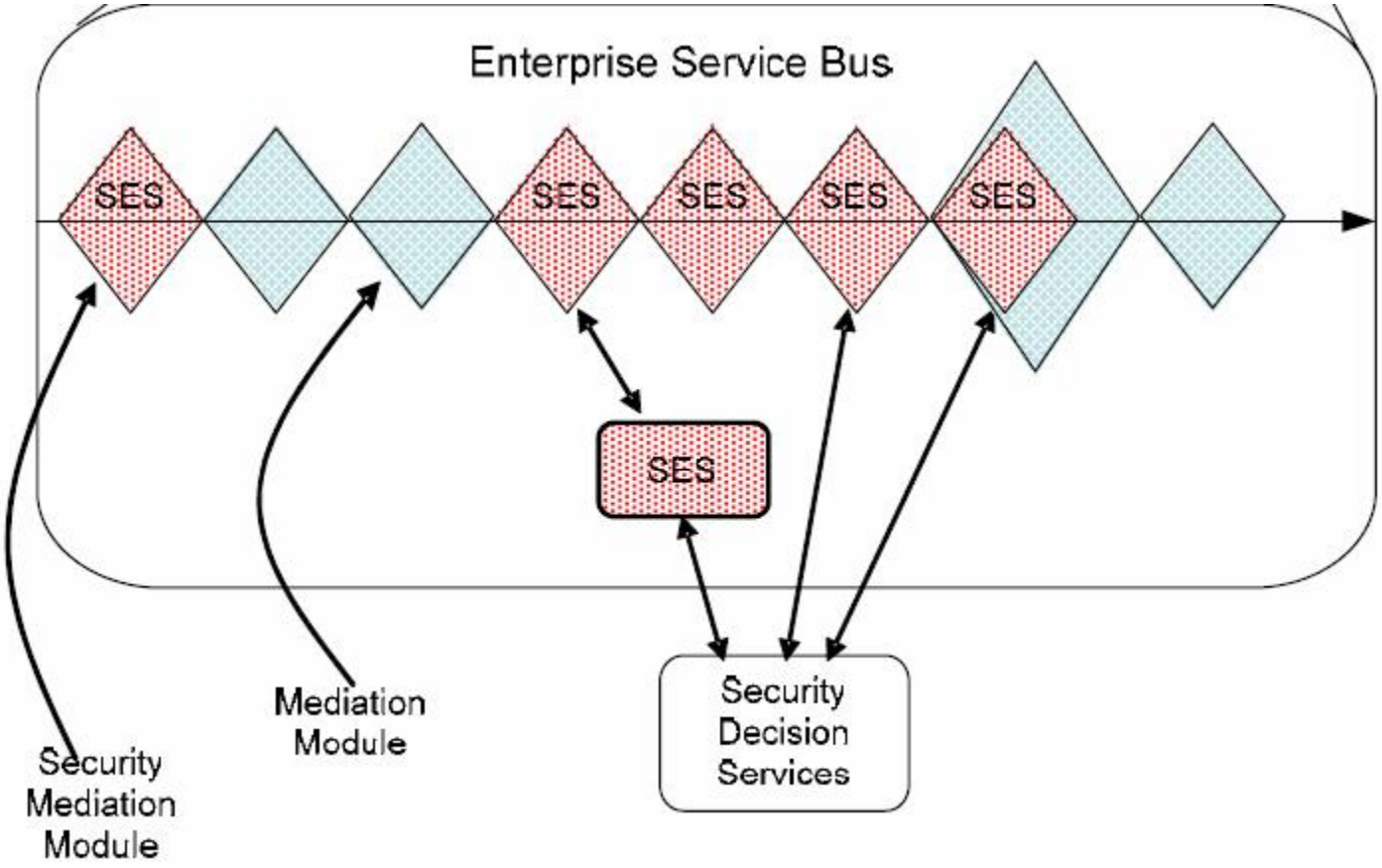
Main difference between Message Broker and ESB

- Message Broker is intermediatery program that relies on certain underlying protocol(s) and uses it's features
- ESB is software architecture construction
- ESB uses normalized messages and doesn't use protocol specific features

Introduction to ESB(minimum set of services)



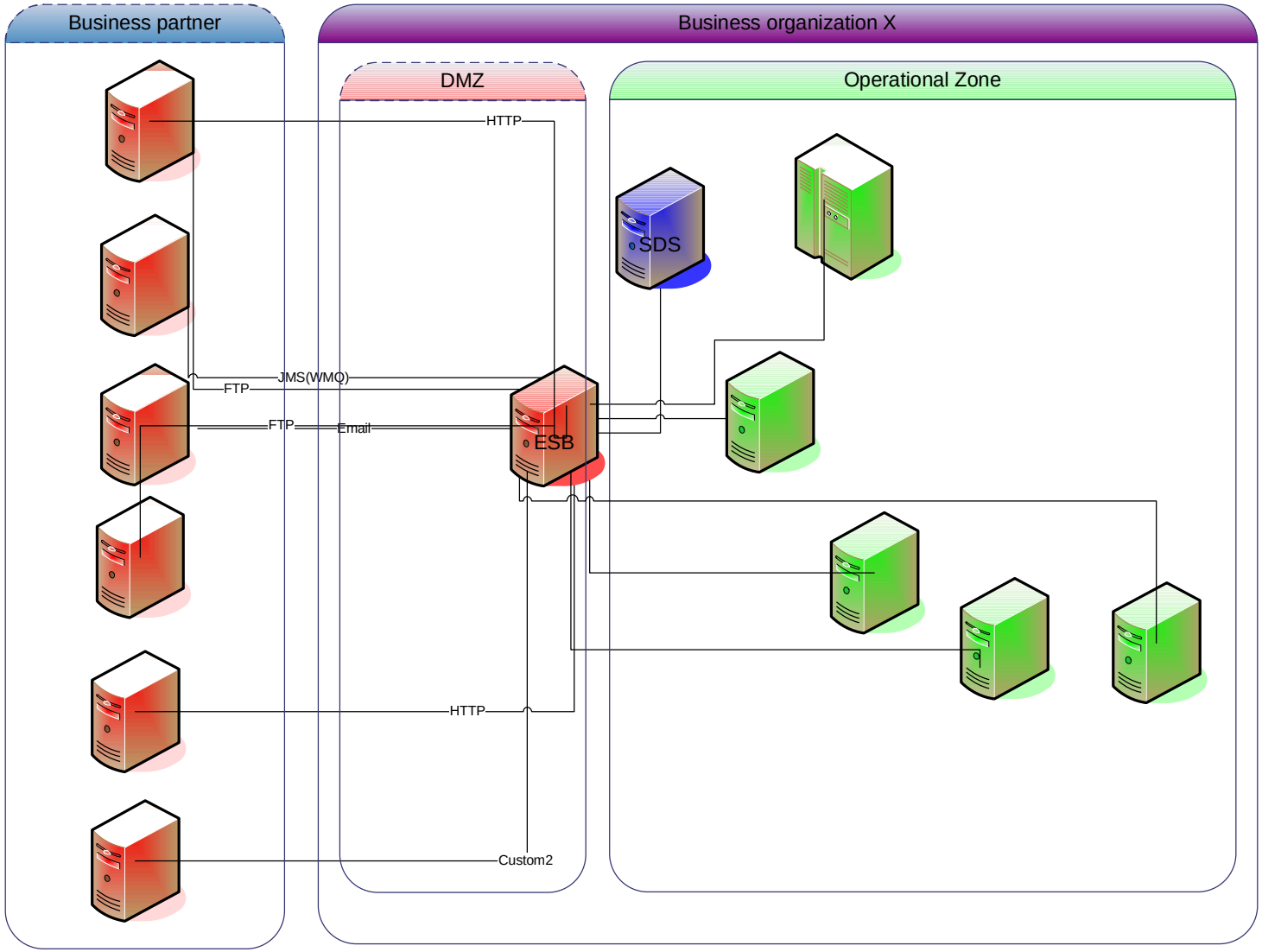
ESB security mediation(extras)



Security mediation modules in ESB

- Authentication
  - Use Directory services or access management software(openLDAP,AD, Tivoli Access Manager, CA Site Siteminder)
- Authorization
  - Use Directory services or access management software (openLDAP,AD, Tivoli Access Manager, CA Site Siteminder)
- Auditing
  - Log every message coming in and out from ESB
  - Use corporate wide
- Message validation
- Make sure that routing has dead letter channel for unknown and poison messages(routing)
-

One ESB for internal and external usage with SDS

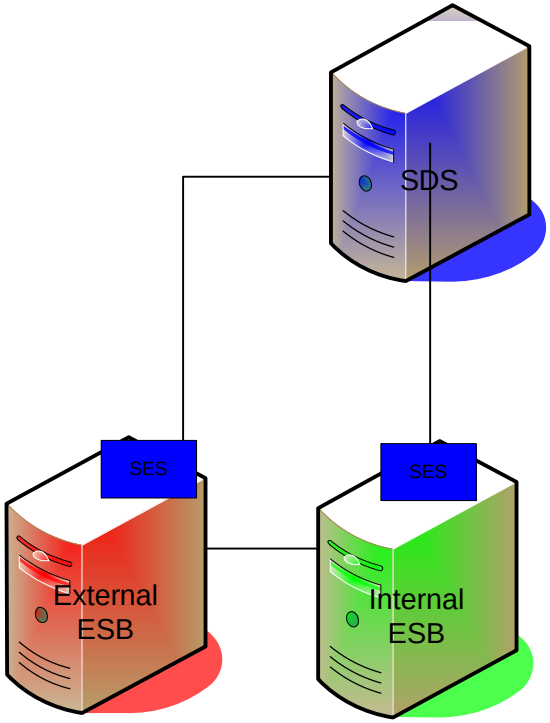


tieto.com

Problem with one ESB

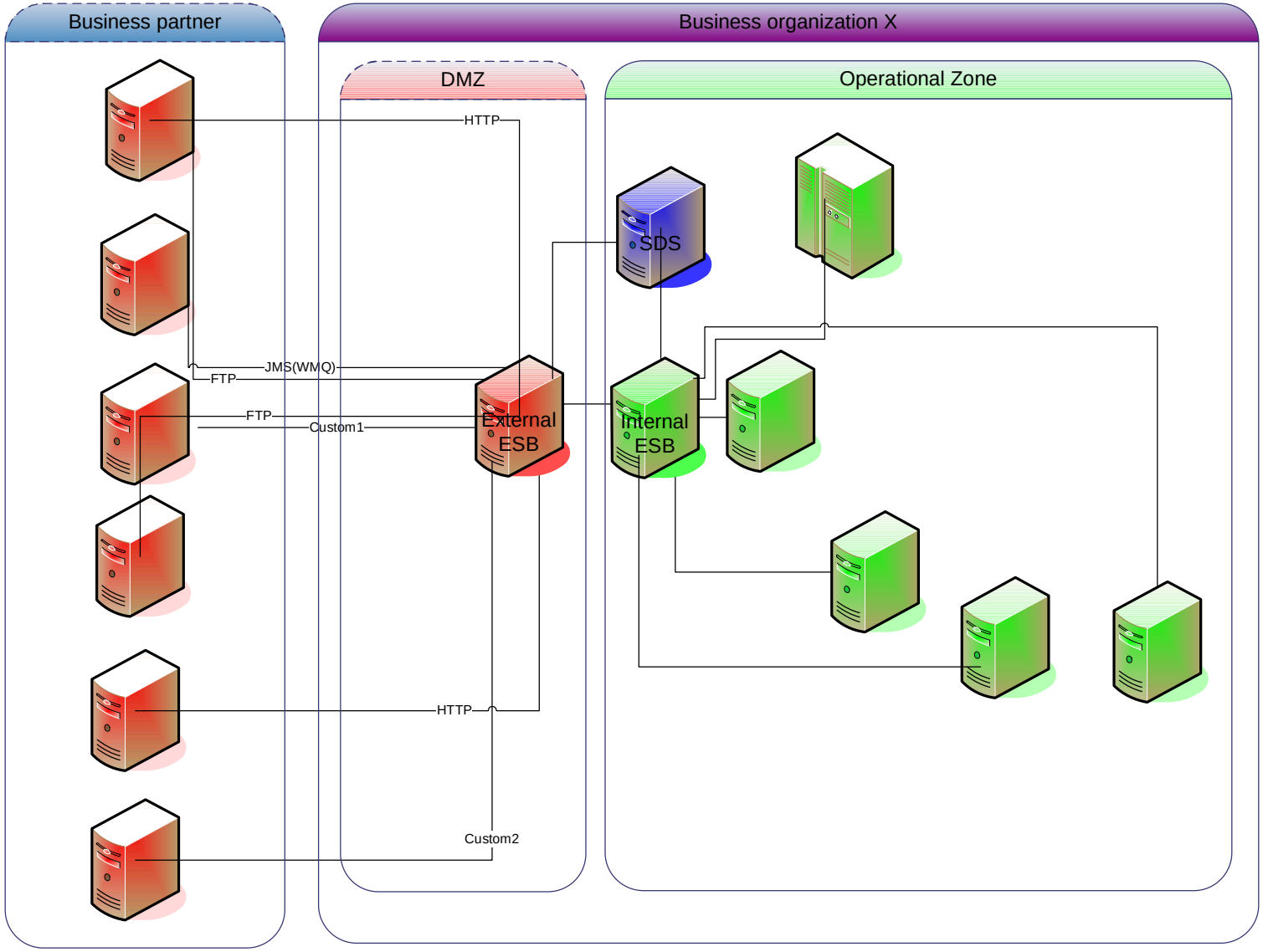
- + Communication security between business partners is secured.
- + Security model is centralized.
- Problem: Security zone and DMZ are not separated
  - Solution: Use internal and external ESB which are bridged togerher

Security Decision Service(SDS) and Security Enforcement Services(SES)



- Security decicion point acts as storage of security policies
  - SDS functionality can include also service reqistry
- Security enforcement services ask policies from SDS and implement them

Internal and External ESB with Security Decision Services(SDS)



tieto.com

External ESB

- Act as Security Gateway
- Centralized security in External ESB(Gateway ESB)
- Supports a single point of control for security enforcement
- Enables a layered approach to security
- Provides a single point of control for identity mapping
- Advanced gateway implementations support transactional integrity
- There are several hardware boxes for this purpose eg. IBM Datapower, Layer 7, Radware

Internal ESB

- All service request should go through internal ESB using logical address
- Internal ESB has register of destinations and it routes internal messages to internal destinations and external message to external ESB
- Message transformations are done here
- ERP + Workflow engines connect here

Availibility threats

- To make services and ESB available
  - Capacity planning
  - Find the weakest link of the chain
    - Design pattern in integration should be Event Driven rather than Stateful
      - Event driven architecture scales to infinity
- Network rate limiting
- Monitor service and ESB processes
- Monitor service logs
- B2B Monitoring is also needed