

# Protecting XML/WS Servers at the Network Level

**Rich Salz**

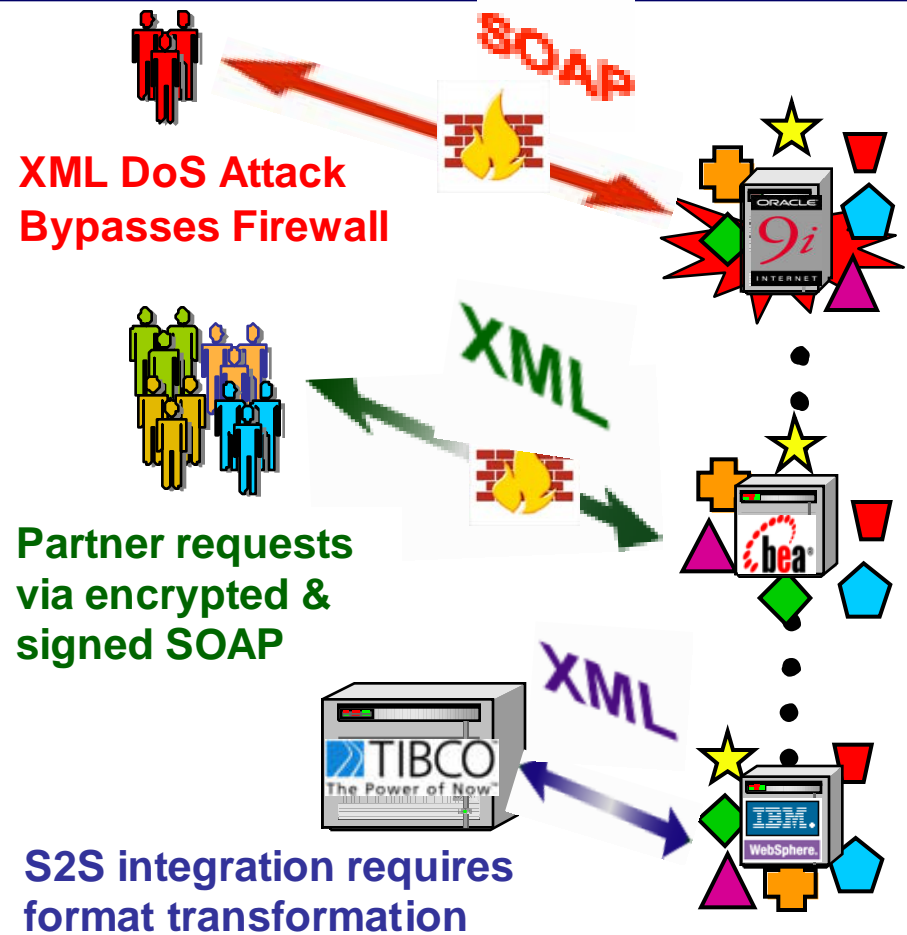
**Chief Security Architect**





**DataPower Technology**

**<http://www.datapower.com>**

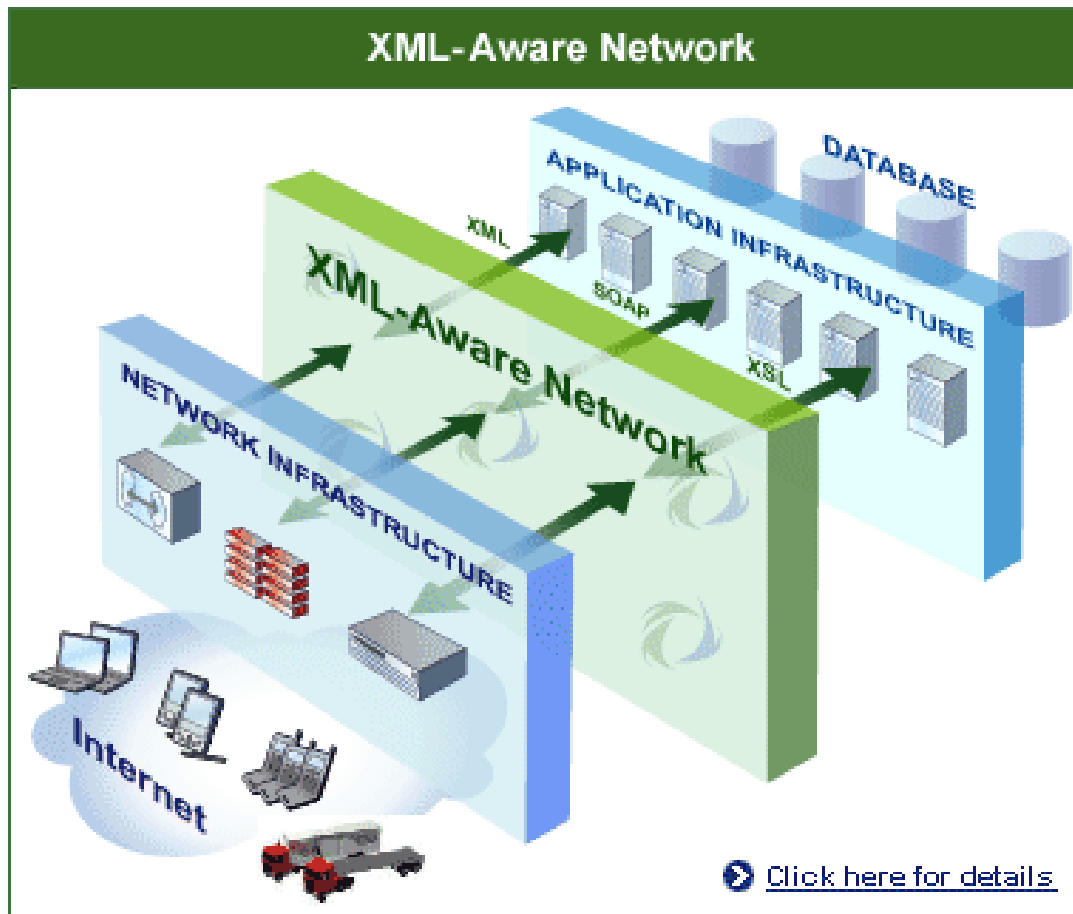
# Challenges for App. Software

- ❑ **New, Unfamiliar Tasks**
  - ❑ XML/SOAP bypasses firewalls
  - ❑ Apps must now provide security
  - ❑ Which specs? SDK?
- ❑ **Code-intensive**
  - ❑ Constant security patches
  - ❑ Endless debugging and performance tuning
- ❑ **Code audits!**
  - ❑ Prove app complies w. central security policy
  - ❑ Change app as policies change
- ❑ **Poor Performance**
  - ❑ “Commodity” functions swamp servers
  - ❑ Apps “dumbed down” or stay in pilot
- ❑ **Capital Costs**
  - ❑ Duplication of effort
  - ❑ Overprovisioned CPU & memory



- |   |                              |   |                    |   |                              |
|---|------------------------------|---|--------------------|---|------------------------------|
|  | XML Parsing & Transformation |  | Digital Signatures |  | Schema Validation            |
|  | XML Encryption               |  | New XML standard   |  | Change purchase order schema |

# An XML-aware Network



Provide your XML applications the same:

- Performance
  - Security
  - Manageability
- that you expect from your IP network!

# XML Firewall features

---

- ❑ Enforcement of XML well-formedness constraints
- ❑ Enforcement of SOAP messaging schema(s)
- ❑ Enforcement of application schema(s)
- ❑ Enforcement of security policy:
  - ❑ Digital signatures, encryption, etc.  
... very expensive! “...turns all other attacks into denial-of-service” – Hal Lockhart, BEA
  - ❑ Transport-layer security (SSL/TLS)
- ❑ Content-based routing (next slide)

***Enforce these requirements at the network level,  
before the applications see a single byte!***

# XML firewall Enables More Security

---

- ❑ If your XML firewall can do XML processing, then it can intercept many attacks:
  - ❑ Preventing SQL injection is “just” string scanning
  - ❑ Scanning for SOAP:mustUnderstand
  - ❑ Rewriting outgoing WSDL files “on the fly” to list only supported services
- ❑ If your proxy doesn't have resources, it can't be attacked:
  - ❑ No filesystem
  - ❑ No database
  - ❑ No applications
- ❑ Performance is an implicit requirement!

# Service Virtualization

---

- ❑ Create abstraction barrier between internal and external systems – *mask* services by putting them behind a de-multiplexing proxy
- ❑ Multi-layer:
  - ❑ TCP/SSL proxy
  - ❑ HTTP rewrite / redirect
  - ❑ Optionally, internal/external transport-layer proxy (e.g., MQ)
  - ❑ Dynamic routing
  - ❑ SOAP header stripping / rewriting
  - ❑ Payload transcription
- ❑ For example, dispatch based on XML document root
- ❑ Especially important for auto-generated web services
- ❑ Also helps with versioning, availability and scalability issues
- ❑ Very XML processing intensive

# XS40 Protects and Secures XML Applications

