



# XML Gateways: Addressing the Security and Performance Impact of XML On the Network

*Chris Haddad*

*Director of Technical Architecture*

[chaddad@burtongroup.com](mailto:chaddad@burtongroup.com)

[www.burtongroup.com](http://www.burtongroup.com)

22 May 2007



# XML Gateways

## Thesis

- Web services require additional security and performance infrastructure
  - Traditional perimeter and web access security aren't sufficient
- Security threats and requirements are complex
  - Don't try this at home – only professionals
- Management and control requires visibility
- Externalize security and control to infrastructure whenever possible
  - BTW
    - security requires solid PKI and IdM solutions in place
    - Control requires policies and baseline metrics



# XML Gateways

## Agenda

- Problem statement
- Approach
- Topology options
- Solution Alternatives
- Recommendations



# XML Gateways

## Agenda

- Problem statement
- Approach
- Topology options
- Solution Alternatives
- Recommendations



## Security Threats

- Message alteration
- Confidentiality
- Falsified messages
- Man in the middle
- Principal spoofing
- Forged claims
- Replay of messages or message parts
- Denial of service
- Content-borne threats
- Schema poisoning
- Code/content injections
- Fraud



## Security Requirements

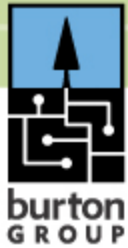
- Entity identification and authentication
- Authorization
- Data origin identification and authentication
- Data integrity and confidentiality in motion
- Data integrity and confidentiality at rest
- Message uniqueness
- Message validation and content scanning
- Auditing
- Monitoring
- Management and administration
- Trust management
- Federation



# Problem Statement

## Service Mediation: Enforcing separation of concerns

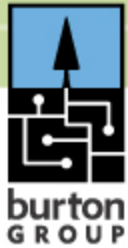
- Service intermediaries perform policy based coordination and mediation of message traffic
- Mediation functional areas:
  - Dynamic location and binding, load balancing
  - Message validation
  - Message format and/or protocol transformations
  - Version management and mapping
  - Message routing, queuing, and caching
  - Reliable message delivery
  - Event processing
  - Mediated communication styles
  - Security processing and mediation
  - Identity credential mapping
  - Threat detection, content scanning



# Problem Statements

## Processor-intensive application-server functions

- Web services platforms (WSPs) juggle many overhead tasks:
  - SOAP message processing
  - SSL security
  - TCP session management
  - XML validation
  - XSLT transformation
  - More
- Overhead tasks often consume up to 80 percent of CPU cycles on WSPs, crowding out business logic processing



# Problem Statements

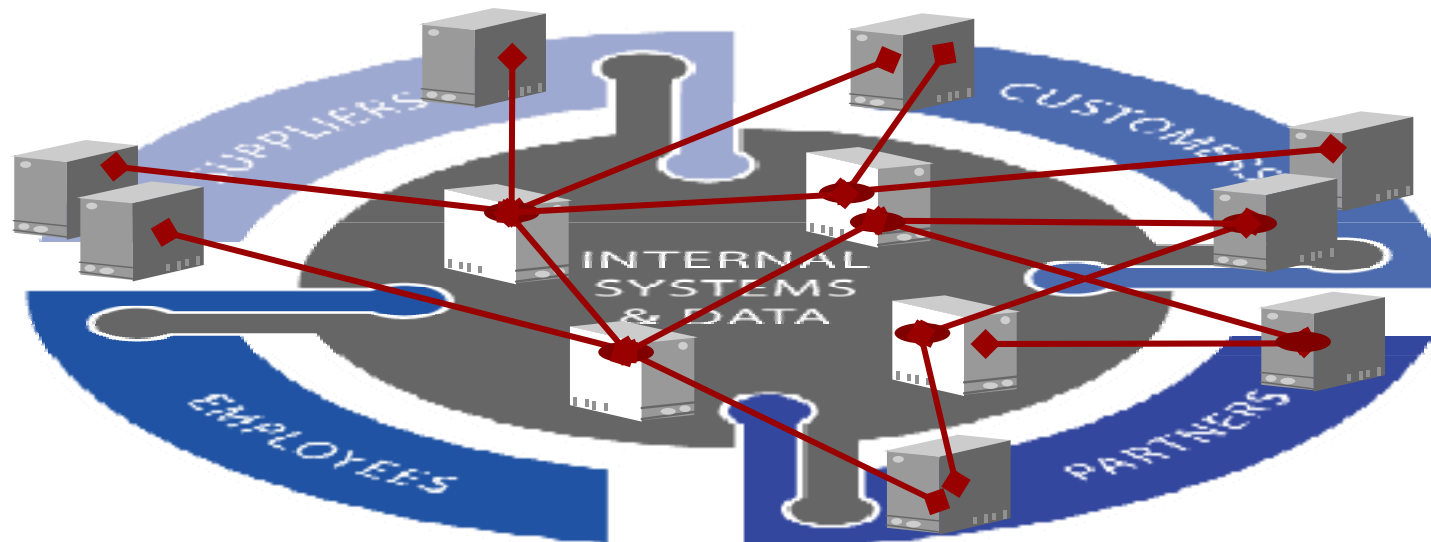
## Heavyweight content encodings

- Text-based XML is predominant encoding scheme for Web services
- XML can be as much as 100 times as bit-heavy as equivalent binary encodings such as ASN.1, CORBA CDR, DCOM NDR, ONC XDR, or Java serialization
- Heavyweight content encodings consume inordinate amount of bandwidth on Web services network connections



## N-tier deployment models

- Web services continue to sprawl across growing range of nodes, networks, and organizations
- N-tier complexity adds processing nodes and routing hops, hence latency and overhead, to Web services





# XML Gateways

11

## Agenda

- Problem statement
- Approach
- Topology options
- Solution Alternatives
- Recommendations



# Approach

## Governance

- Making sure that Quality of Service (QoS) is done “right”
- Three steps:
  - Define security and management policies
  - Deploy an infrastructure
  - Institute formal processes and procedures



# Approach

Make generic security and management as automatic as possible

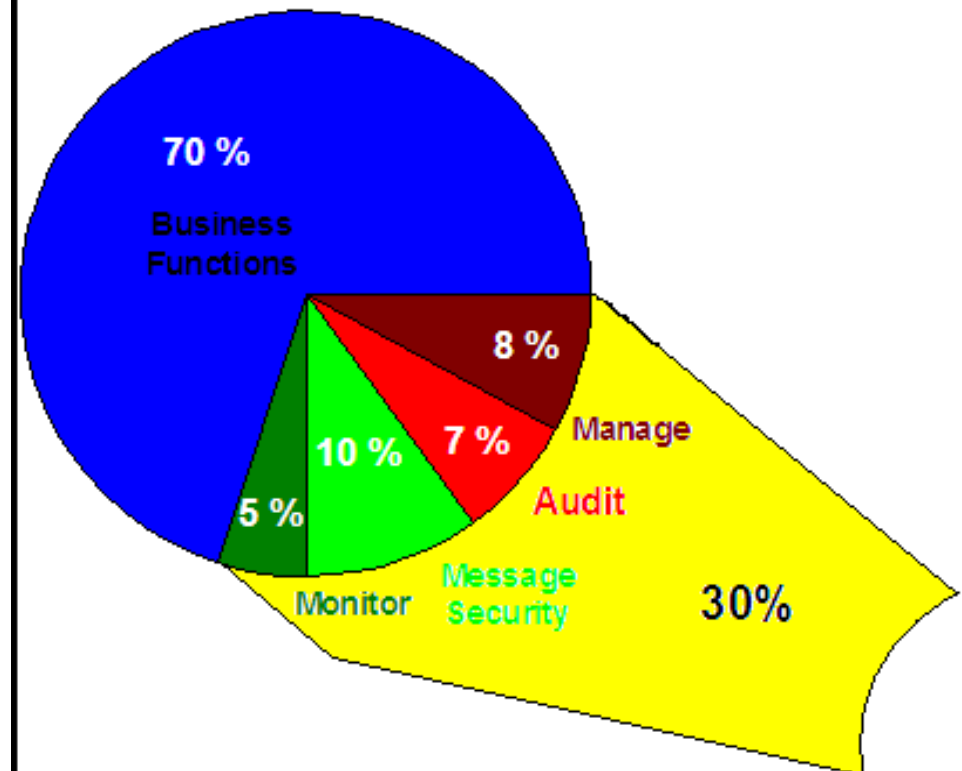
- Authentication, auditing, cryptography, some authZ
- Monitoring and control
- Simplify development
- Let operation professionals be responsible for ops
  - Wherever possible and/or reasonable
- Developers can't completely abdicate responsibility
  - Security is everyone's problem



## Potential savings

- IT budget estimates from a Fortune 50 financial conglomerate

Total Cost of ownership for developing and operating our automated business processes





# Approach

15

## Practical scaling and acceleration techniques

- Service planning, modeling, simulation, and development
- Capacity expansion
- Co-processing
- Compression
- Monitoring
- Content-aware traffic optimization

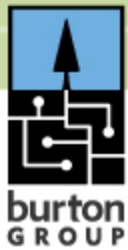


# XML Gateways

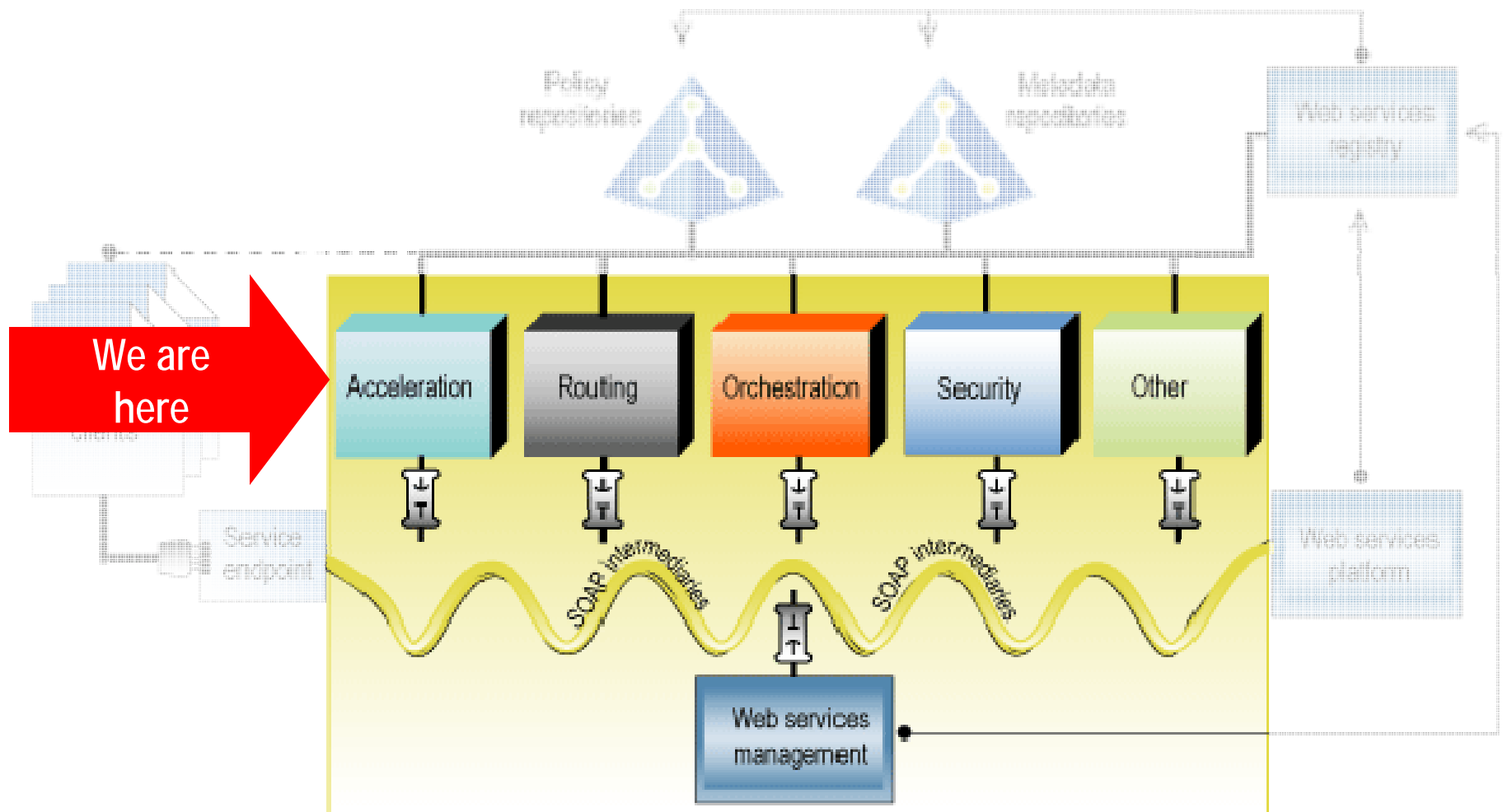
16

## Agenda

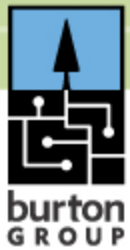
- Problem statement
- Approach
- Topology options
- Solution Alternatives
- Recommendations



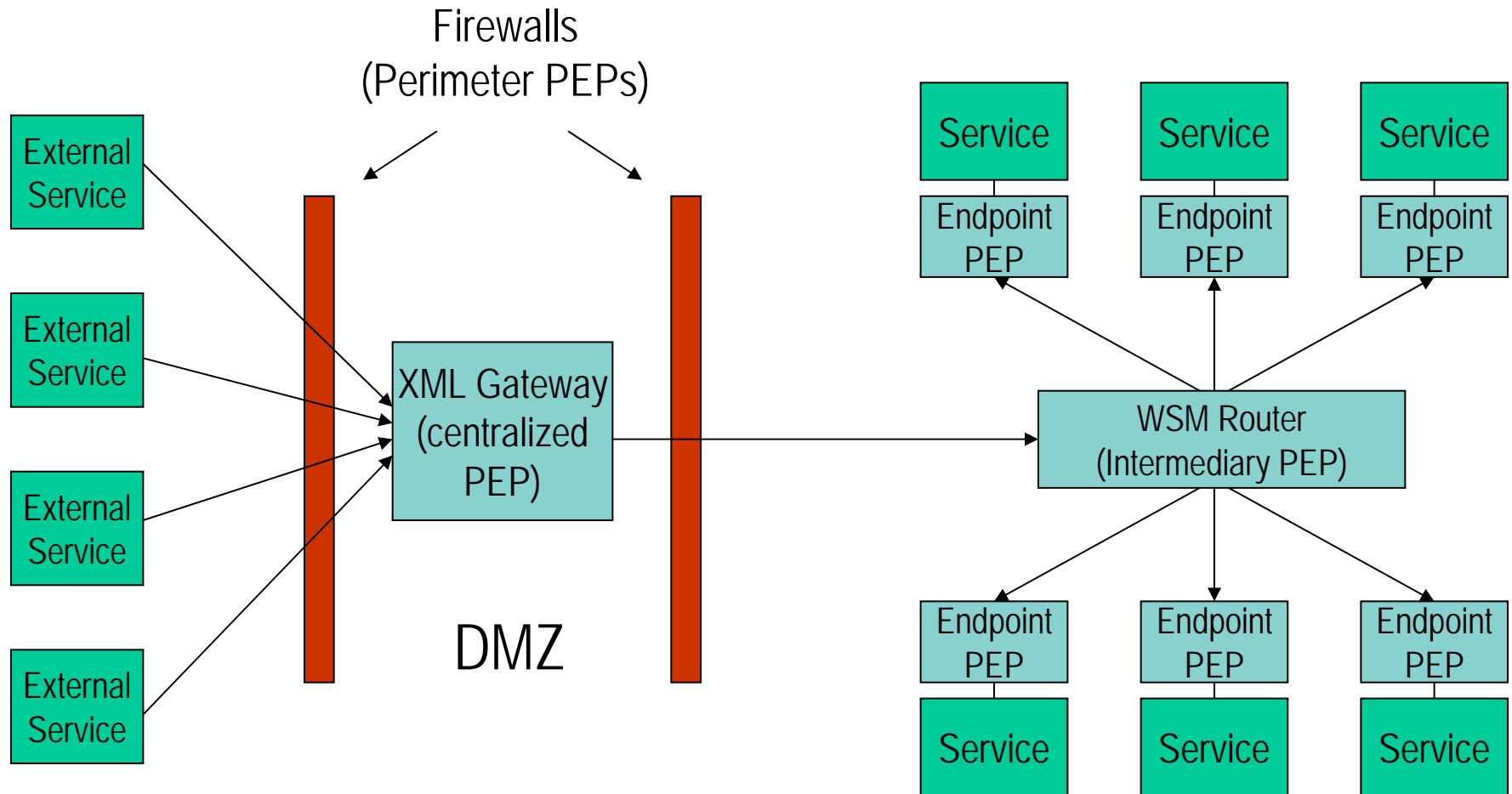
# Topology Options



# Topology Options



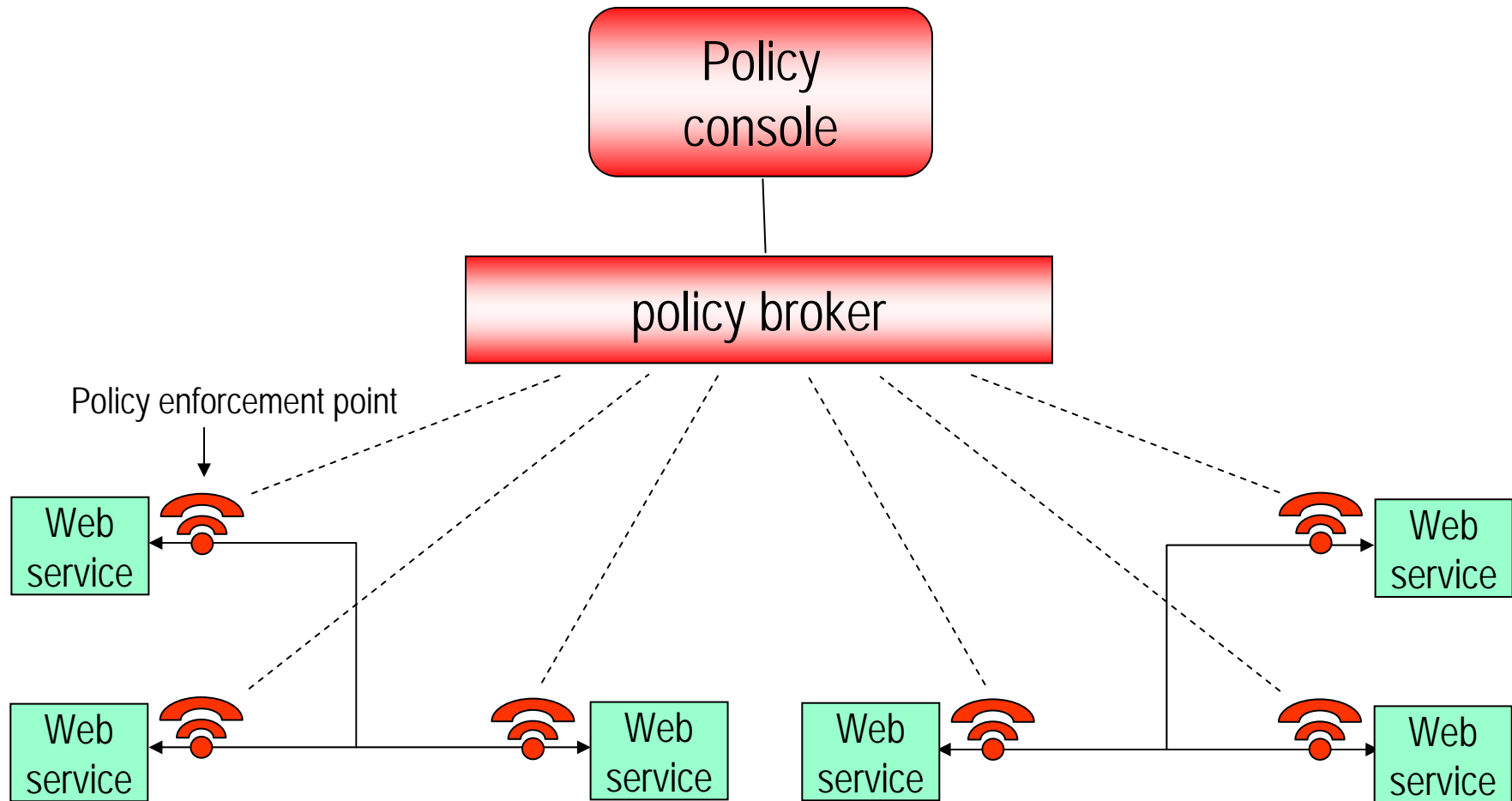
## Identity and Access Layer PEPs



# Topology Options



## Delegated management



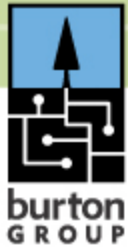


# XML Gateways

20

## Agenda

- Problem statement
- Approach
- Topology options
- **Solution Alternatives**
- Recommendations



# Solution Alternatives

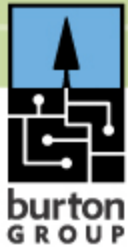
21

## Transport-level

- HTTP authentication
- SSL authentication
- SSL encryption

## Application-level

- WS-Security
  - Username, X.509, SAML, REL, Kerberos tokens
  - XML encryption, XML signature
- WS-<sup>\*</sup>
  - WS-Trust, WS-SecureConversation, WS-Federation
  - WS-Policy, WS-MetadataExchange



## XML security gateways

- ✓ Cisco/Reactivity, IBM/DataPower, Intel, Forum Systems, Layer 7, Vordel
- Security, acceleration, and mediation
  - Single administrative environment for entire environment
  - More security functionality:
    - SAML token support
    - Security of non-SOAP XML traffic
    - Authorization & integration with IdM/access management
    - Credential mapping and federation
    - Monitoring and auditing
    - Message filtering and scanning PKI management and provisioning
  - SAML authority
  - Hardware acceleration (sometimes)



## XML VPNs

- ✓ Layer 7, SOA Software
- Simplifies client provisioning

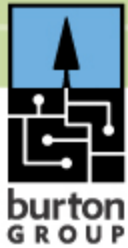


# XML Gateways

24

## Agenda

- Problem statement
- Approach
- Topology options
- Solution Alternatives
- Recommendations



# Recommendations

## Get a handle on governance

- Define threats, requirements, service levels
- Baseline monitor and predict traffic patterns
- Review integration of XML Gateway with other components
  - Registry helpful for management & discovery of policies
- Reduce adoption hurdles
  - Single point of administration
  - Easier development

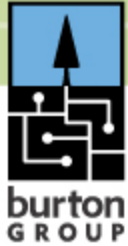


# XML Gateway

26

## Conclusion

- Opening up applications as XML web services introduces security and performance risks
- XML Gateways are a viable insurance policy
- It's not the technology, but how you use it!
  - Define policies, metrics, and processes



# References

## Application Platform Strategies Service Content

- *Service-Oriented Architecture (SOA) Infrastructure Technical Position*
- *Building the Business Case for Service Oriented Architecture Investment MBP and Telebriefing*
- *VantagePoint 2005-2006: SOA Reality Check*
- *VantagePoint 2006-2007: Back to Basics*
- *Root Document Turning the Network Into the Computer: The Emerging Network Application Platform*
- *Service-Oriented Architecture: Developing the Enterprise Roadmap*
- *Web Services Registry: The Foundation for SOA Governance*
- *Web Services Management: Townsman of a Stiller Town*
- *Developing a Web Services Security Strategy*
- *Web Services Security: A Plethora of Products*

For access to these documents and others, contact

[clientservices@burtongroup.com](mailto:clientservices@burtongroup.com)