Developing a Web Services Security Strategy

Anne Thomas Manes

VP & Research Director

amanes@burtongroup.com

www.burtongroup.com

Application Platform Strategies Telebriefing
6-7 September 2005

Web Services Security Strategy

Thesis

- WS Security must be part of a comprehensive approach to security
  - Web services require additional security infrastructure
  - Traditional perimeter and web access security aren't sufficient
- Security threats and requirements are complex
  - Don't try this at home!
- Externalize security to infrastructure whenever possible
- Layered defenses are best
  - Network perimeter defenses
  - Identity-based defenses at centralized entry-point
  - Identity-based defenses at each intermediary and endpoint
  - Security monitoring for attack and fraud detection
  - Transport-level and application-level message protections
- BTW – it requires solid PKI and IdM solutions in place
  - Certificate management and provisioning

Web Services Security Strategy

Agenda

- Problem statement
- Externalizing security
- Message security options
- Topology options
- Solution options
- Recommendations

Agenda

- Problem statement
- Externalizing security
- Message security options
- Topology options
- Solution options
- Recommendations

Problem Statement

Security is really hard

- Threats:
  - Message integrity, confidentiality, falsified messages, man in the middle, principal spoofing, forged claims, message replay, denial of service, content-borne threats, schema poisoning, code/content injections, fraud
- Requirements:
  - Entity authentication, data authentication, authorization, data protection in motion, data protection at rest, message uniqueness, message validation, content scanning, auditing, monitoring, management and administration, client provisioning, trust management, federation
- Can't expect every developer to understand it all

Problem Statement

What’s different about web services and SOA?

- Services aren’t constrained to a single point of entry
- App-to-app communications (no humans)
- Heterogeneous authN and authZ mechanisms
- Mediation and loose coupling expose more vulnerabilities
  - Adds complexity to the trust relationship
  - Need to capture identity of intermediary for auditing

Problem Statement

Big challenges

- Administration and management
- Authentication and credential mapping
- Auditing
- Client provisioning
- Trust management and federation
- Threat and fraud detection
- Attachments
- Governance

Problem Statement

Governance

- Making sure that security is done “right”
- Three steps:
  - Define security policies
  - Deploy an infrastructure
  - Institute formal processes and procedures

Problem Statement

Security policies: rules and guidelines

- How do you assess risk?
- What security precautions are required?
- What’s the maximum permitted overhead for security?
- What tools and technologies should be used?
- Who’s responsible for implemented security?
- What testing is required?
- Who’s responsible for approving security?
- What documentation must be produced?

Web Services Security Strategy

Agenda

- Problem statement
- Externalizing security
- Message security options
- Topology options
- Solution options
- Recommendations

Externalizing Security

Make generic security as automatic as possible

- Authentication, auditing, cryptography, monitoring, management, some authorization
- Simplify development
- Let security professionals be responsible for security
  - Wherever possible and/or reasonable
- Developers can’t completely abdicate responsibility
  - Security is everyone’s problem

Externalizing Security

Benefits

- Reduce costs
  - Up to 30% of IT budget can go to generic non-business functions
- Faster time to market
- More consistent and reliable implementation of security policies
- Reduced risks

Web Services Security Strategy

Agenda

- Problem statement
- Externalizing security
- Message security options
- Topology options
- Solution options
- Recommendations

Message Security Options

Transport-level

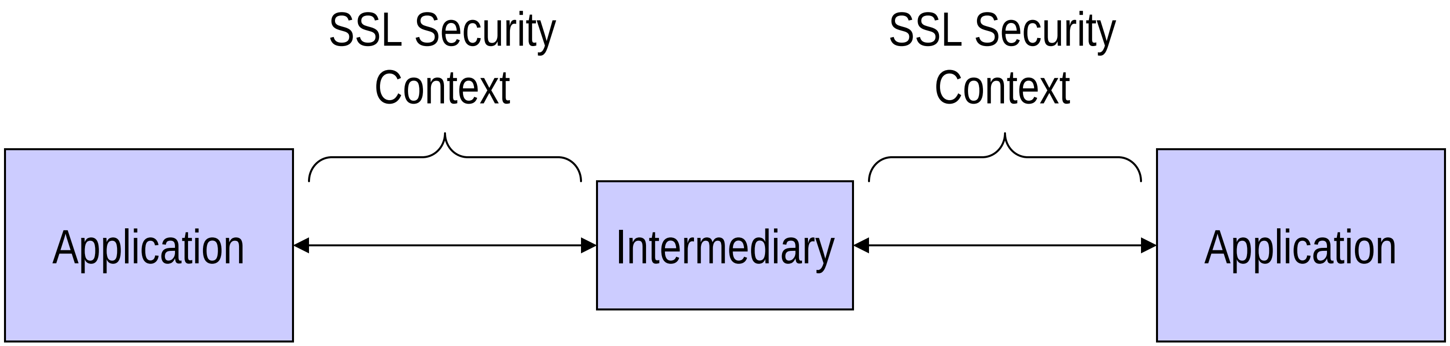
- HTTP authentication
- SSL authentication
- SSL encryption

Application-level

- WS-Security
  - Username, X.509, SAML, REL, Kerberos tokens
  - XML encryption, XML signature
- WS-* (not ready for prime-time)
  - WS-Trust, WS-SecureConversation, WS-Federation
  - WS-Policy, WS-MetadataExchange

Message Security Options

Point-to-point vs end-to-end security context



SSL Security Context

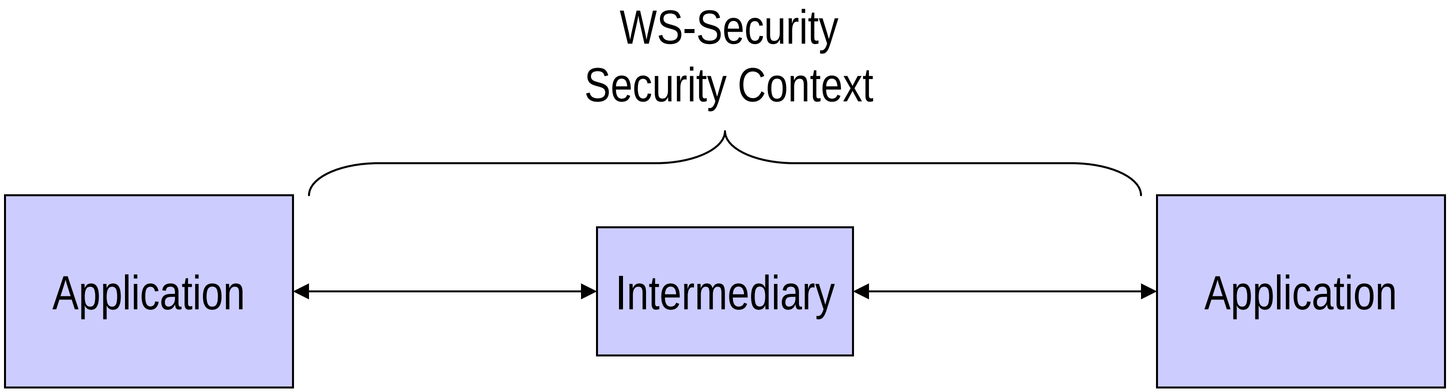
SSL Security Context

Application

Intermediary

Application

Transport-level point-to-point security



WS-Security Security Context

Application

Intermediary

Application

Application-level end-to-end security

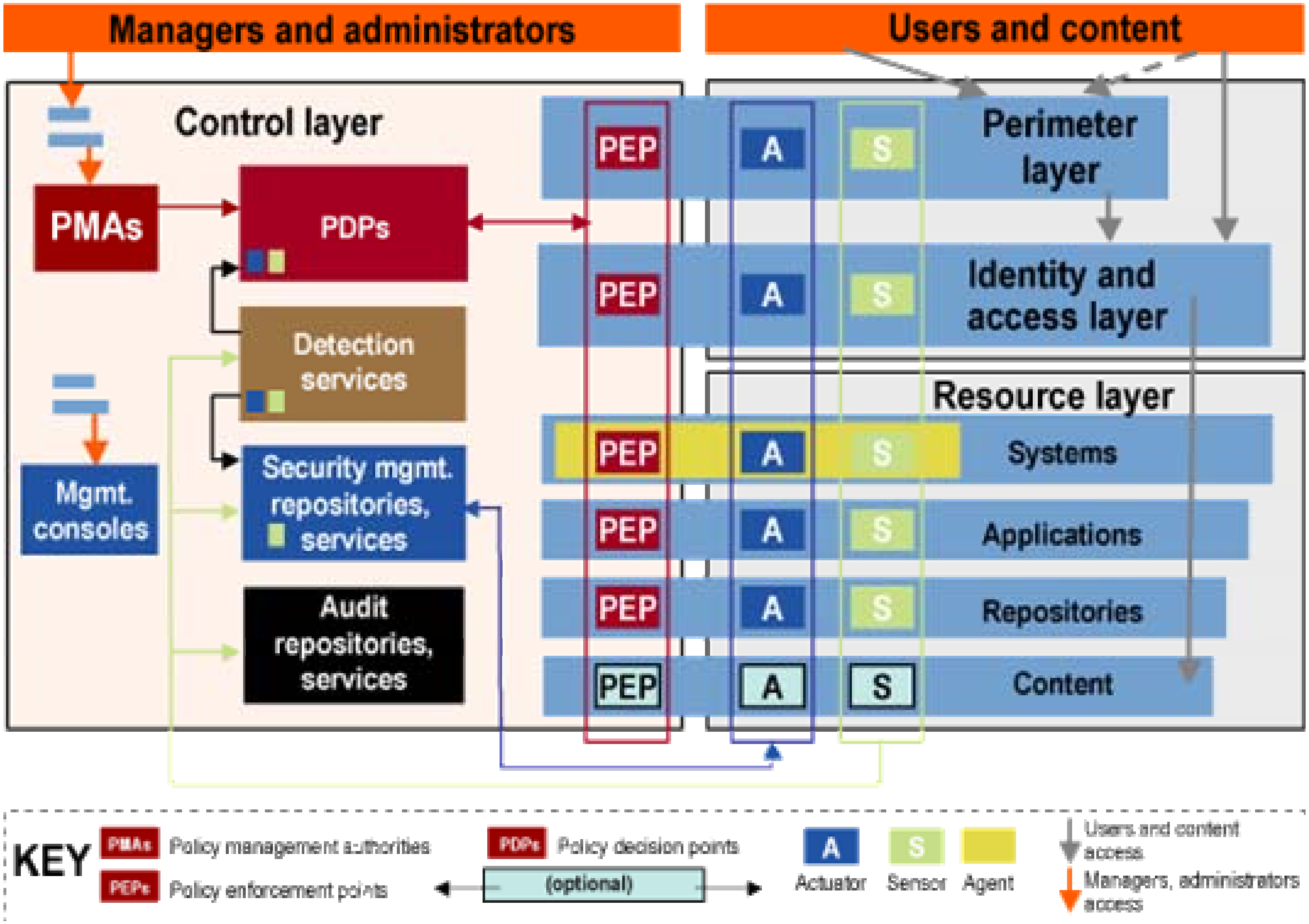
Web Services Security Strategy

Agenda

- Problem statement
- Externalizing security
- Message security options
- Topology options
- Solution options
- Recommendations

Topology Options

Policy-based layered defenses


Managers and administrators
Users and content
Control layer
PMAs
PDPs
Detection services
Security mgmt. repositories, services
Audit repositories, services
Mgmt. consoles
PEP
A
S
Perimeter layer
Identity and access layer
Resource layer
Systems
Applications
Repositories
Content
KEY
PMAs Policy management authorities
PEPs Policy enforcement points
PDPs Policy decision points
(optional)
A Actuator
S Sensor
Agent
Users and content access
Managers, administrators access

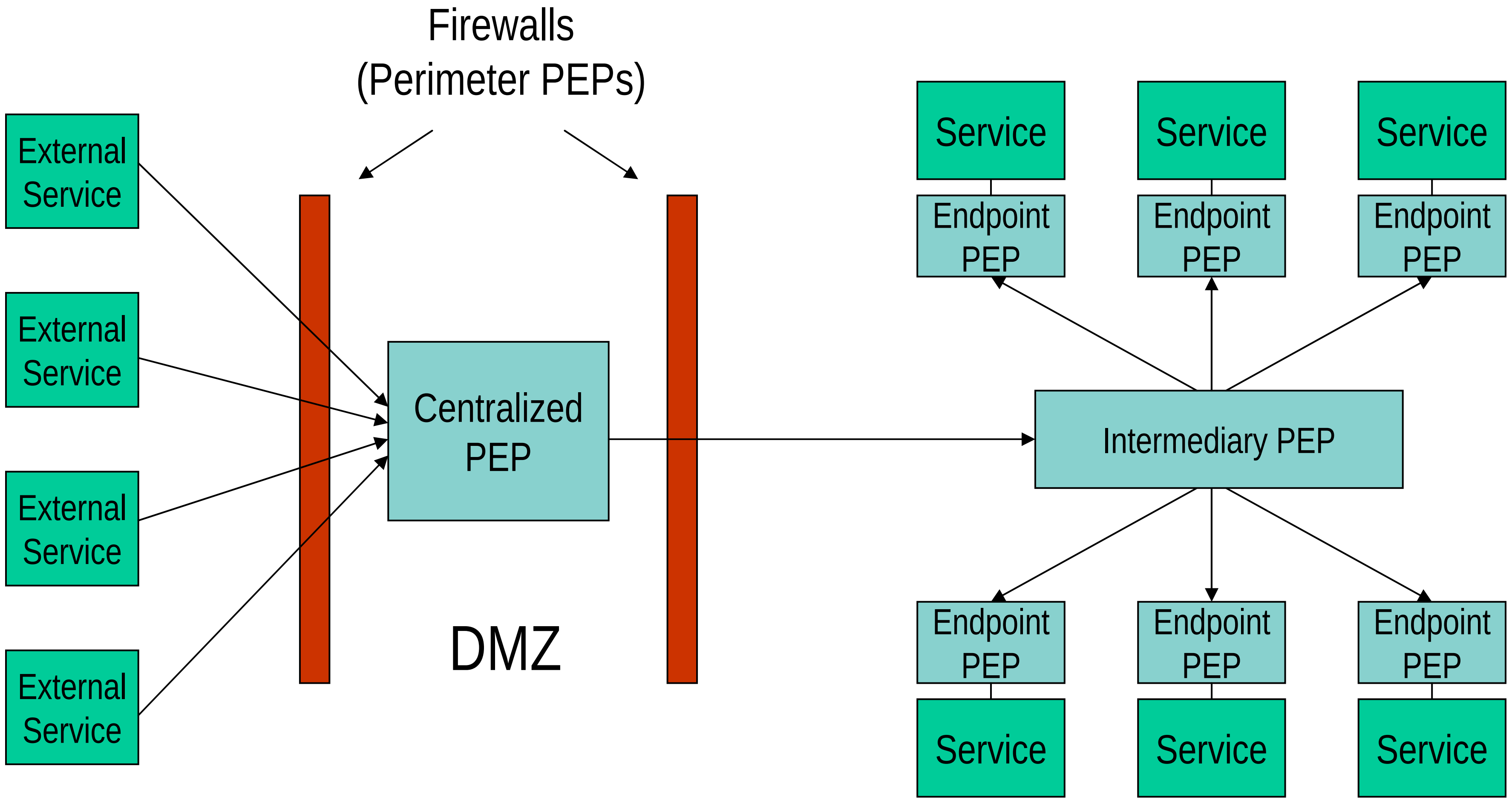
Topology Options

Location of policy enforcement points

- Perimeter layer PEPs
  - Firewalls, VPNs, intrusion detection, IP filtering, virus scanning, etc.
- Identity and access layer PEPs
  - Centralized entry point (in the DMZ)
  - Intermediary (routing, transformation, other mediation)
  - Endpoint

Topology Options

Identity and Access Layer PEPs



Web Services Security Strategy

Agenda

- Problem statement
- Externalizing security
- Message security options
- Topology options
- Solution options
- Recommendations

Solution Options

Product categories

- Web services platforms
- Plug-in implementations of WS-Security
- Web services management
- Web services monitoring
- XML security gateways
- XML VPNs
- Web services authentication and entitlements

Solution Options

Web services platforms

- Stand-alone platforms
  - ✓Systinet Server (Java & C++), webMethods Glue
  - ×Apache Axis supports WSS via WSS4J
- ESBs
  - ✓Cape Clear, Fiorano, IONA, Tibco, webMethods Fabric
  - ×Sonic will support WSS in Q1 2006
- Superplatforms
  - ✓BEA, IBM, Microsoft, SAP
  - ×Oracle supports WSS via Oracle WSM
- User management
  - LDAP, AD, SQL
  - Some support IdM systems (esp. SiteMinder)

Solution Options

Plug-in implementations of WS-Security

- Apache WSS4J
- RSA BSAFE Secure-WS
- Sun XWS-Security
- Verisign TSIK

Solution Options

Web services management

- Actional
- Amberpoint
- Blue Titan
- HP SOA Manager
- Infravio
- Oracle WSM
- SOA Software

Web services monitoring

- CA WSDM
- Service Integrity

Solution Options

XML security gateways

- Cisco AON
- DataPower
- Intel (formerly Sarvega)
- Forum
- Layer 7
- Reactivity
- Vordel

XML VPNs

- Layer 7
- SOA Software

Solution Options

Web services authentication and entitlements

- Plug-in:
  - CA eTrust TransactionMinder,
- WS-Trust:
  - Entrust Identifications & Entitlements Server
  - IBM Tivoli Federated Identity Manager
  - Oracle COREid Federation (in 2006)

Solution Options

Matching solutions to requirements

- End-point PEPs
  - Web services platforms
  - Plug-in implementations of WS-Security
  - Web services management
- Centralized and intermediary PEPs
  - XML security gateways
  - Web services management
- Client provisioning
  - XML VPNs
- Attack and fraud detection
  - XML security gateways
  - Web services management
  - Web services monitoring
- SSO and integration with web access management
  - Web services authentication and entitlements

Web Services Security Strategy

Agenda

- Problem statement
- Externalizing security
- Message security options
- Topology options
- Solution options
- Recommendations

Recommendations

Message security

- Use a combination of transport and application-level security
- Transport-level:
  - HTTP Authentication only for low-surety applications
  - SSL mutual authentication for machine-to-machine authentication
  - SSL encryption for in-motion protection
- Application-level:
  - Username or SAML for auditing, user authentication, and authorization
  - XML encryption and XML signature for at-rest protection
  - Encrypt and sign only sensitive data elements based on business requirements

Recommendations

What works today

- WS-Security 2004 1.0 with
  - XML encryption and signature
  - Username and X.509 tokens
  - WSM and XML gateways support SAML
- WS-I Basic Security Profile
  - SSL
  - WS-Security w/ Username, X.509, SAML, REL
  - Attachments

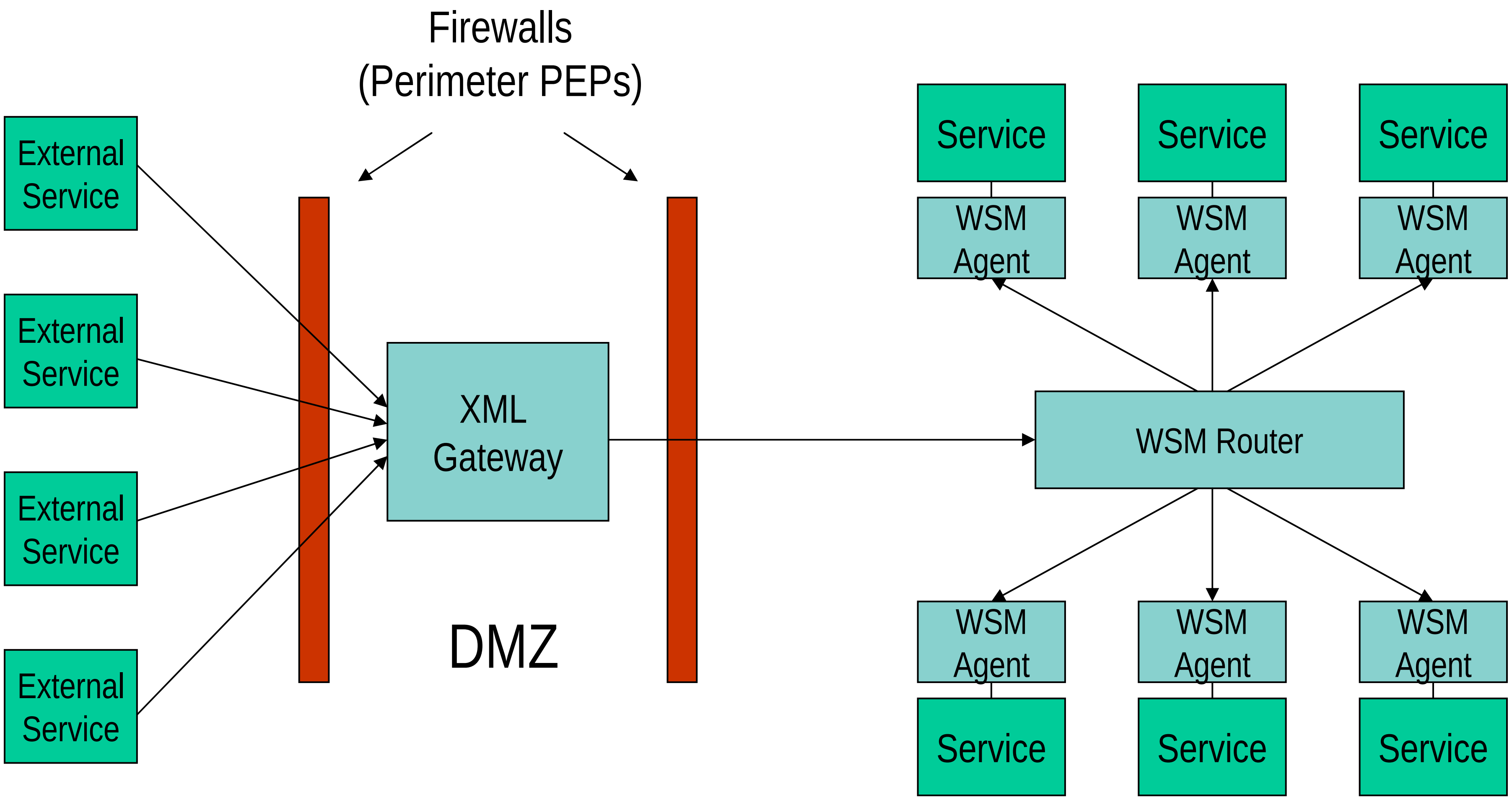
Recommendations

Policy enforcement points

- Identity-based PEPs should be deployed throughout environment
  - Every endpoint and intermediary should be protected by a PEP
- Use SSL mutual authentication or IP filtering to constrain permitted message paths
- PEP functions:
  - Authentication, auditing
  - Maybe credential mapping and/or authorization
  - SLA and security monitoring
  - Threat/fraud detection
  - Validation, injection detection, virus scanning (at central PEP)

Recommendations

Identity-based PEPs throughout environment



Recommendations

Use WSM solution to implement endpoint PEPs

- Significant advantages of using WSM over built-in WSP
- 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

Recommendations

Use XML security gateway for centralized PEP

- All the advantages of WSM plus
  - PKI management
  - SAML authority
  - Hardware acceleration (sometimes)
- Many excellent partnerships between WSM and XML gateway vendors
  - Share administration and management

Use XML VPN if business dictates it

- Enable dynamic client provisioning

Recommendations

Governance is critical

- Define corporate policies regarding WS security
- Don’t permit services to be deployed without provisioning appropriate PEPs
- Registry integrated with WSM provides a solid foundation for governance
    - Registration process provides single point of control

Web Services Security Strategy

Conclusion

- Most people today use transport-level security w/ maybe an XML security gateway
  - Works great for point-to-point integration
  - Insufficient for SOA
- WS-Security is ready for prime-time
  - Widespread product support
  - Tooling can make it almost invisible
- Policy administration can cause severe headaches
  - Waiting impatiently for WS-Policy (next year)
  - Best current remedy: standardize on a WSM product

Web Services Security Strategy

Resources

- Upcoming APS MBP: Web Services Security Strategy
- SRMS: WS-*: A Composable Architecture for Web Services Security
- APS: Application Security Frameworks: Protecting Applications Consistently
- SRMS: A Systematic, Comprehensive Approach to Information Security
- SRMS: Application Security: Everybody's Problem
- SRMS: Security Governance for the Enterprise
- APS: Selecting a Java Web Services Platform: An Evaluation Framework
- APS: Web Services Management: Gaining Control of Distributed Services
- APS: Enterprise Service Bus: EAI in Transition