



SOA-20: The Role of Policy Enforcement in SOA Management

Phil Walston
VP Product Management
Layer 7 Technologies





Overview


Discuss policy in SOA, the role of Policy Enforcement Points and where this fits within the large scope of SOA management

Agenda

- The promise / reality of SOA
- The role of policy
- Policy Enforcement Points
- Policy enforcement in SOA
- Some typical deployment models
- End to end SOA management
- Layer 7 and Progress® Actional®



SOA-20: The Role of Policy Enforcement in SOA Management



Service Oriented Architecture (SOA)

- An *integration framework* for dynamically interconnecting loosely-coupled software components into on-demand business processes
- Software functionality can be delivered as network callable services and composed into processes in a flexible, agile manner
- Typically application to application (machine to machine) interactions
- Frequently associated with XML or Web services
 - ♦ Remember DCOM and CORBA?

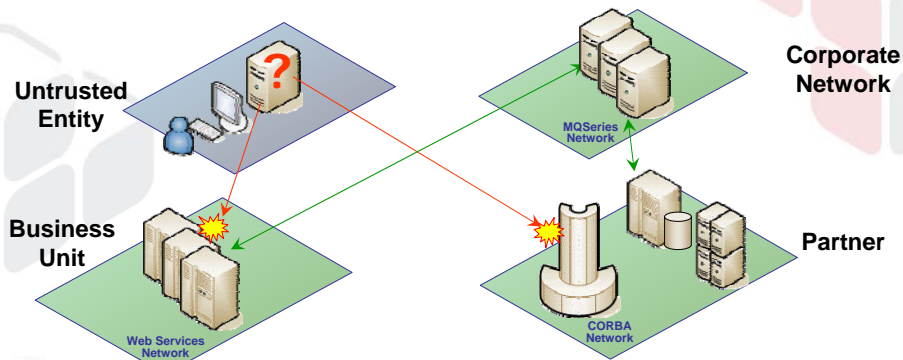


SOA-20: The Role of Policy Enforcement in SOA Management



The Promise of SOA

- **Flexible integration** across departments, clients and partners
- **Reuse** of software components across business processes
- **Interoperability** across applications



SOA-20: The Role of Policy Enforcement in SOA Management

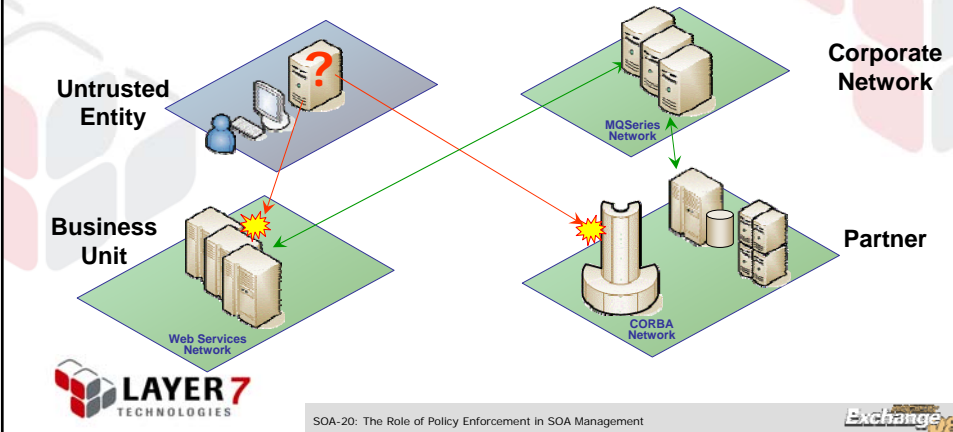


SOA-20: The Role of Policy Enforcement in SOA Management

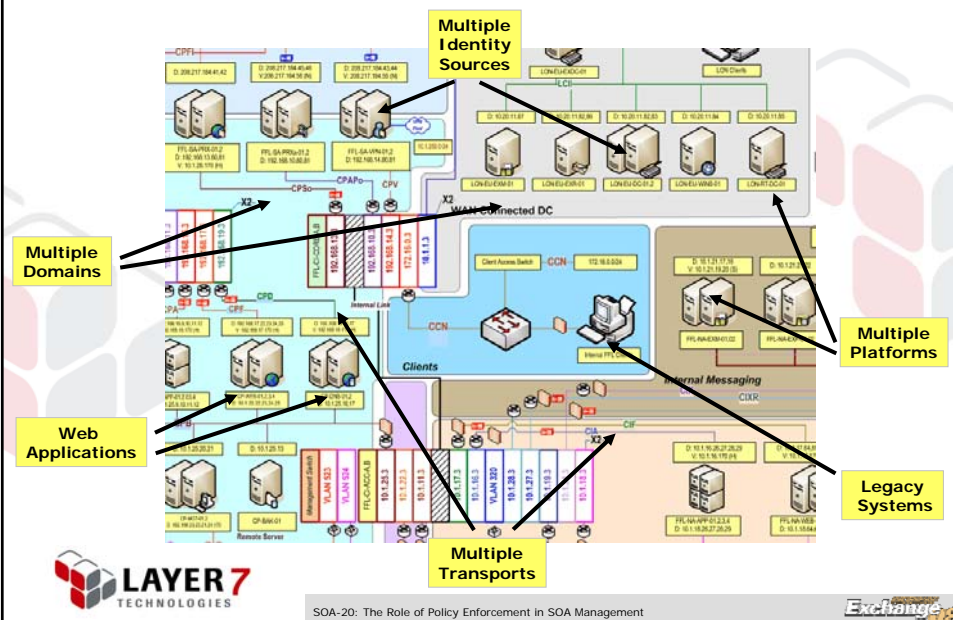
Philip Walston

The Promise of SOA – The “High Concept” Model

- **No Interop Issues** – transport, message format, platform
- **No Intermediaries** – firewalls, VPNs, portals
- **No Infrastructure** – directories, SSO, management systems ...



The Real World is Messy ...



The Role Of Policy in SOA

What are policies?

- Rules, guidelines and constraints that govern interactions in service-oriented environments
- Express constraints, preferences and capabilities on endpoints, intermediaries and messages themselves
- The basis for consistency in SOA
 - ♦ Design, lifecycle and operational behavior

Effective policies should be:

- Declarative so they can be applied broadly
 - ♦ Remove dependencies, preserve loose coupling
- Managed consistently
 - ♦ Definition, deployment, enforcement – the entire lifecycle



SOA-20: The Role of Policy Enforcement in SOA Management



A Few Typical Policy Examples

Threat Protection

- Screen messages for specific / general threats

Identity Based Access Control

- Grant access to specific users or groups

Content-Based Processing

- Perform different processing based on specific content

Selective Version Control

- Transform to mediate client / service versioning issues

Service-Level Agreement

- Process based on measured quota or class of service



SOA-20: The Role of Policy Enforcement in SOA Management



The Issues With Securing SOA

Service Oriented Architectures are all about business process & application integration – *loose-coupling, reuse and interoperability*

But this can pose a number of serious security issues:

- Messages pass through existing network infrastructure
- Back-end application logic is often exposed
- Messages often cross multiple trust domains
- User interaction not always possible (ask for password?!)
- Business partners might require different privacy policies, message encryption, transport methods etc.
- Standards and specifications are evolving ...



SOA-20: The Role of Policy Enforcement in SOA Management



SOA May Require Message Level Security

In a SOA, securing the pipe is not enough

- Transactions can be multi-hop

The context of a service interaction is important

- Identity may need to be correlated with *content*
- Identity may need to be correlated with *context*

Transactions can also cross trust boundaries

- Authenticating and authorizing may require access to credentials buried in message content
- Federated identities may need to be rationalized or mapped

Some content may need to be obscured or validated

- Data elements encrypted or signed



SOA-20: The Role of Policy Enforcement in SOA Management



The Concept of Policy Enforcement Points

A Policy Enforcement Point (PEP) acts on defined policies

- Can be implemented as intermediary or coincident with service endpoint

Typical benefits of a PEP include:

- Removing need to code policy into application logic
 - ♦ Reduce skill sets required to implement policies
 - ♦ Move from development effort to administrative task
 - ♦ Reduction of development, test and change control costs
- Consistent enforcement of policies
 - ♦ Declarative expression of policies using suitable model
 - ♦ Policies not reliant on coding expertise or specific technology
- Centralized management of policies
 - ♦ Use of controlled workflow for policy lifecycle
 - ♦ Central registry / repository of policies and related assets



SOA-20: The Role of Policy Enforcement in SOA Management



A Deeper Look at Run-Time Policy Enforcement

Once we have defined policies, what roles does an enforcement point perform?

- Read policies
- Create / store policies
- Enforce policies
- Identify exceptions
- Act on exceptions
- Report exceptions
- Capture audit trail

Enforcement points provide run-time SOA policy enforcement
within a specific context



SOA-20: The Role of Policy Enforcement in SOA Management



A Deeper Look at Run-Time Policy Enforcement

Once we have defined policies, what roles does an enforcement point perform?

<ul style="list-style-type: none">• Read policies• Create / store policies	Design-Time
<ul style="list-style-type: none">• Enforce policies• Identify exceptions• Act on exceptions	Run-Time
<ul style="list-style-type: none">• Report exceptions• Capture audit trail	Diagnostic

Enforcement points provide run-time SOA policy enforcement within a specific context

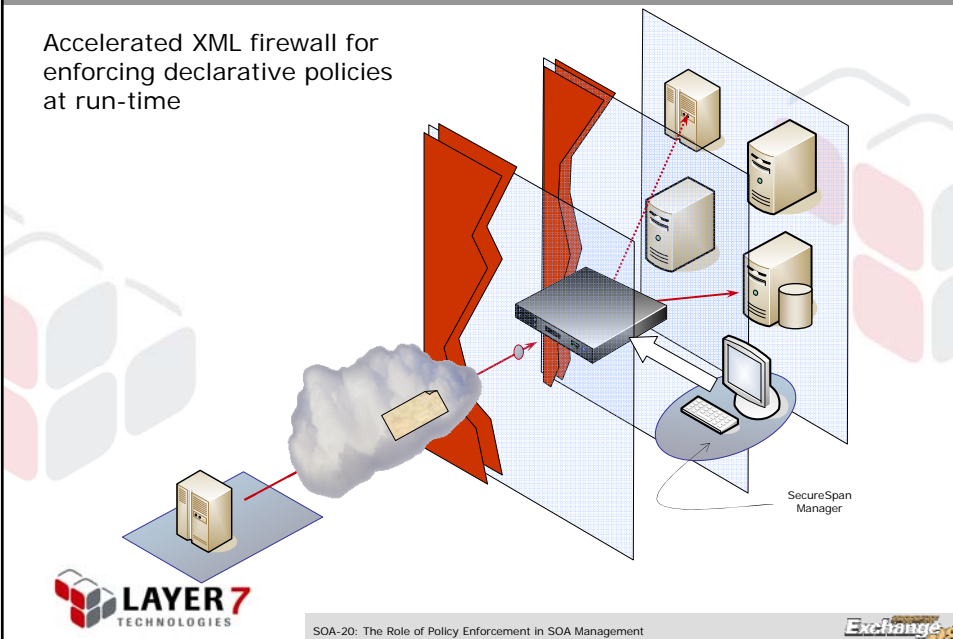


SOA-20: The Role of Policy Enforcement in SOA Management



The SecureSpan XML Firewall – SOA Policy Enforcement

Accelerated XML firewall for enforcing declarative policies at run-time



SOA-20: The Role of Policy Enforcement in SOA Management

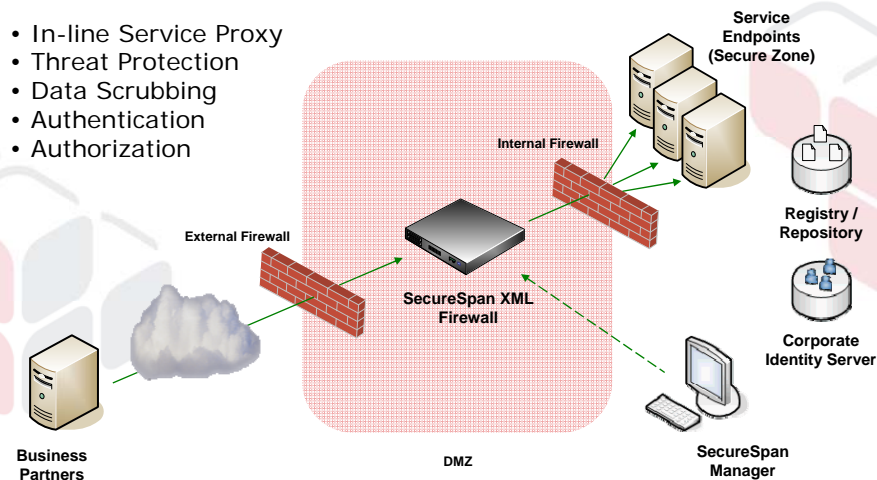


SOA-20: The Role of Policy Enforcement in SOA Management

Philip Walston

Deployment Models – In The DMZ

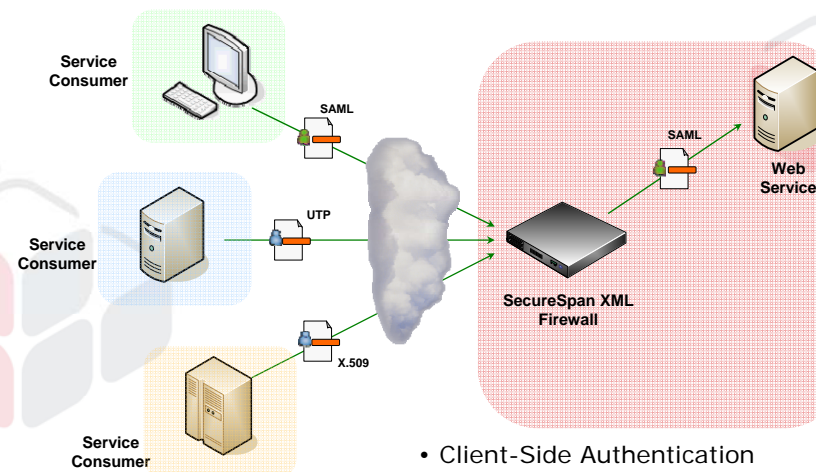
- In-line Service Proxy
- Threat Protection
- Data Scrubbing
- Authentication
- Authorization



SOA-20: The Role of Policy Enforcement in SOA Management



Deployment Models – SOA Across Trust Boundaries



- Client-Side Authentication
- Service-Side Authorization
- Credential Mining/Mapping
- Federated Identity

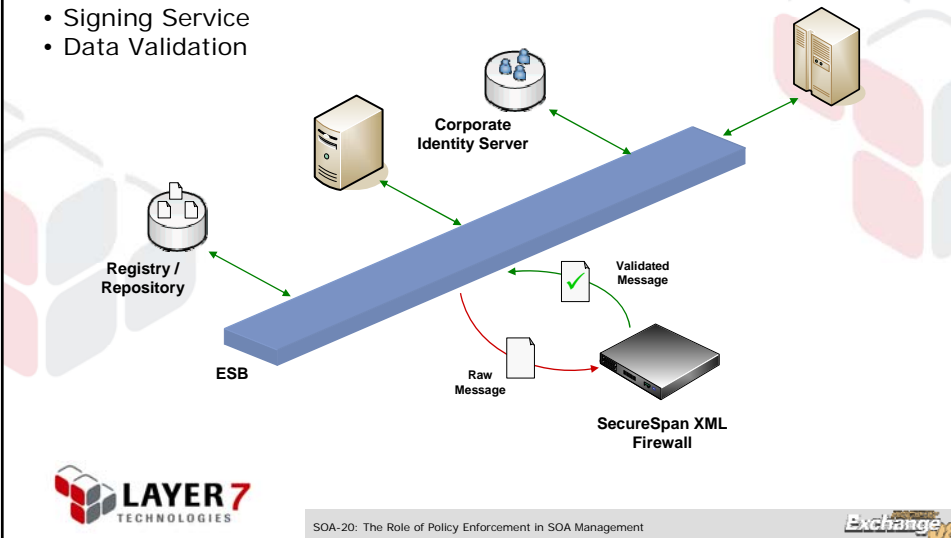


SOA-20: The Role of Policy Enforcement in SOA Management



Deployment Models – Security As Service For ESB

- XML Co-processor
- Accelerated Transforms
- Signing Service
- Data Validation

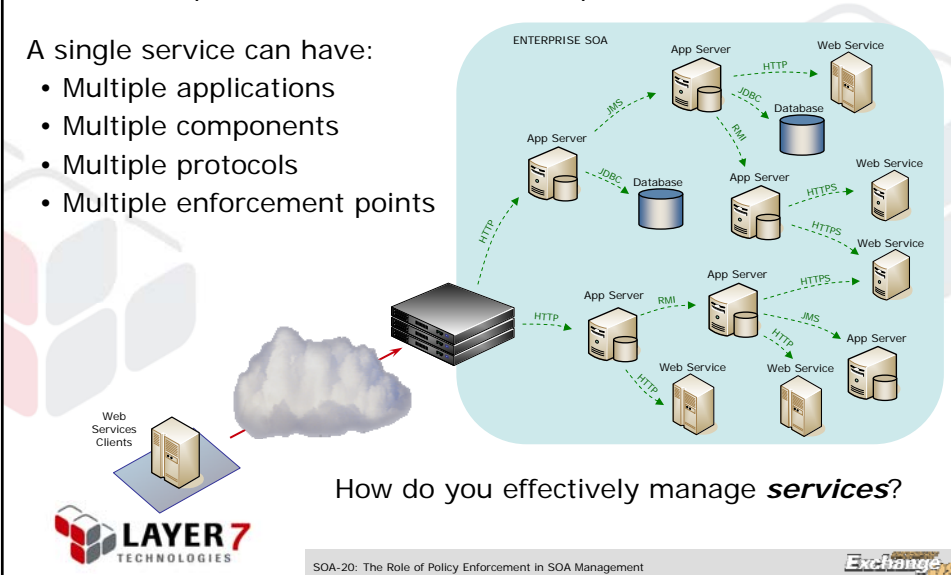


The Broader Issue of SOA Management

Real SOA implementations are more complex ...

A single service can have:

- Multiple applications
- Multiple components
- Multiple protocols
- Multiple enforcement points



How do you effectively manage *services*?

End to End SOA Management - Key Requirements

The goal is to get visibility into your SOA infrastructure and better manage actual services

This often requires:

- Tracking all deployed services, what they depend on, who's really using them, and how often
- Ensuring quality of service in the SOA, end-to-end, throughout the lifecycle
- Understanding the impact of an expected change or an unexpected problem
- Proactively detecting problems in the SOA before end users do
- Determining the root cause of problems and resolving incidents quickly without finger pointing



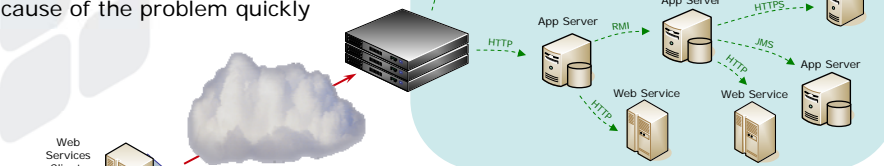
SOA-20: The Role of Policy Enforcement in SOA Management



End to End SOA Management - Progress Actional

Effectively manage complex SOA environments

- Automatically discover the business process engaging your services
- Manage the entire call path across a variety of platforms and protocols
- Understand how each component impacts performance
- When a service fails get to the root cause of the problem quickly



- Enforce policies throughout the enterprise



SOA-20: The Role of Policy Enforcement in SOA Management

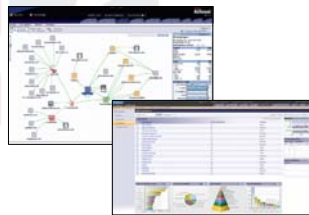
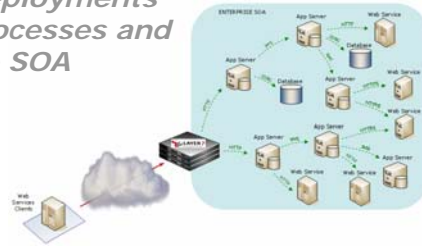


Layer 7 SecureSpan and Progress Actional

Enhance Layer7 secure XML deployments with visibility into business processes and the tools required to maximize SOA performance and reliability

Layer7 SecureSpan XML Firewall

- XML/Web services policy enforcement
- Advanced XML security features
- Flexible policies with no coding



Actional Web Services and SOA Management

- Visibility into business processes and the services they call
- SLA based management
- Last mile security without application changes



SOA-20: The Role of Policy Enforcement in SOA Management



Summary

Policy Has a Key Role in SOA

- Critical part of governing SOA interactions
- Should be declarative to preserve loose coupling
- Form the basis of consistency in SOA

SOA Policy Enforcement Points

- Provide runtime enforcement of service policies
- Reduce overall project costs and schedule risks
- Implement business service changes without disrupting consuming applications

SOA Management Encompasses a Variety of Assets

- Ability to map components to services and services to business objectives
- Requires total visibility into all interactions



SOA-20: The Role of Policy Enforcement in SOA Management



SOA-20: The Role of Policy Enforcement in SOA Management

Philip Walston

To Learn More

Upcoming Sessions

Tuesday 15:30 – SOA-24

“WS-AlphabetSoup” – Jaime Meritt

Tuesday 16:45 – SOA-27

“Practical Approaches for Implementing a SOA” – Michael Boyd

Wednesday 09:15 – SOA-32

“Progress SOA Portfolio Roadmap” – Giovanni Boschi

Wednesday 13:30 – SOA-37

“SOA Management with Actional for Sonic” - Jiri De Jagere

Websites

Progress Actional – www.actional.com

Layer 7 Technologies – www.layer7tech.com



SOA-20: The Role of Policy Enforcement in SOA Management

Exchange 08



Exchange 08