



SecureSpan Gateway and Bridge deployed in tandem as runtime policy enforcement and application points for federated environments.

## The Problem:

SOA is predicated on an ability to integrate loosely coupled services together on-demand. This creates new kinds of challenges for governing how service assets get developed, provisioned and invoked. Defining, enforcing and coordinating policy on and between services therefore become essential for proper service governance and accounting. This requires policy governance infrastructure that can control the creation, change, provisioning and reconciliation of policies across loosely-coupled services and their client applications. Managing the policy lifecycle from creation to reconciliation is only complicated in real-world environments by the decentralized nature of development and operating environments inside and across enterprises.

## The Layer 7 Solution:

SOA Governance requires process and product for controlling service assets at both design time and runtime. While several tools exist for regimenting the developer centric process of governing a service asset at design time, the runtime problem is complicated by the distributed and federated nature of SOA. For that reason Layer 7 has introduced a set of products for providing a runtime policy production environment, integration with leading Policy registries from Systinet and Infravio, a set of intermediates that can enforce policy instructions on behalf of services or client end points, and lastly a compliance reporting and testing environment for validating correct policy execution. The result is a complete environment for defining, enforcing and validating runtime SOA Governance policy.



## Innovations and Solution Features:

---

- Policy level integration with leading SOA registries from Infravio and Systinet
- First XML Gateway product to demonstrate WS-Policy interoperability
- WS-Policy compliant, assertion based, policy editor
- Ability to export policy definitions in XML or WS-Policy
- First policy application point for client-side policy provisioning (SecureSpan Bridge)
- First policy synchronization technology between application clients and services
- Drag and drop policy editing environment
- One-click policy provisioning and change to end-points or SOA registry
- FastPath parser for faster policy execution on SecureSpan Gateway
- Automatic policy validation checker in SecureSpan Policy Manager
- Assertion based policy composition editor supporting branching and conditional statements
- Native integration with leading access and management Policy Decision Points

## Supported Standards:

---

- XML 1.0, SOAP 1.1, XPath 1.0, XSLT 1.0, WSDL 1.1, XML Schema & DTD, LDAP 3.0, SAML 1.1/2.0, Liberty, PKCS #10, X.509 v3 Certificates, W3C XML Signature 1.0, W3C XML Encryption 1.0, SSL TLS 2.0 / 3.0, SNMP, SMTP, HTTP/HTTPS, JMS 1.0, EMS 4.x, MQ Series, WS-Security 1.0, WS-Trust 1.0, WS-Secure Conversation, WS-MetadataExchange, WS-Policy, WS-SecurityPolicy, UDDI, WSIL, WS-I, WS-I BSP

## General SecureSpan™ Features

---

### Authentication

- FTP, HTTP/S, HTTP Digest, HTTP Client-Side Certificate, WS- Security, XML Signature, SAML UserName Token, BinarySecurity Token for X.509 certificates, Security Token Reference, Browser Profile, XPath Credential Source, WS-Trust, and Requestor IP

### Identity Sources

- LDAP, IBM Tivoli Access Manager, IBM Tivoli Federated Identity Manager, Microsoft Kerberos, Microsoft Active Directory, Microsoft Active Directory Federation Services, CA SiteMinder, CA TransactionMinder and RSA ClearTrust

### Service Discovery and Virtualization

- WSDL, WSIL, UDDI, WSDL Creation, WSDL Virtualization, Systinet Registry, and Operation-Level Masking

### Threat Protection

- Accelerated Schema Validation (in ASIC), Requestor Metering, Service Throttling, Requestor IP Restriction, Time-of-Day Restriction, and Attachment Virus Scanning

- Protects against: XDoS, Message Replay, Man-in-the-Middle, WSDL Scanning, Routing Exploits, Payload Exploits, SQL Injection, XML Encapsulation, Buffer Overflow, Schema Poisoning, Recursive Payloads, and Reference Substitutions

### General Security

- Accelerated XPath (in ASIC), Regex Pattern Matching, Message Validation (Schema, Envelope, and Data Type), Content Inspection with Per-Element Filtering, XML Signature, XML Encryption, accelerated XSLT (in ASIC), SAML Attributes, WS-Security, SSL, PKI Lifecycle Control, Endpoint Address Translation, Session Management, Policy Publishing, Policy Branching, Bi-directional Security Enforcement and Application, Microsoft WSE Integration and Oracle OWSM

### Authorization

- URI, URL, SOAP Action, SAML Authorization, SAML Attributes, WSDL Operation, Regex, and XPath

### Audit and Logging

- Real-time SNMP and SMTP Alerts, SNMP Queries, Audit Signing, User-Specified Audit Trapping, CA WSDM, Message-Level Logging, and System-Level Logging

### Standards Group Memberships

WS-I, WS-I BSP, OASIS WS- Security, OASIS WS-RX, OASIS WS-SX, OASIS Security Services (SAML), OASIS-UDDI, OASIS SOA-RM, W3C WS-Policy WG