SecureSpan™ Gateway and Red Hat's JBoss Enterprise SOA Platform

Scalable SOA Security & Management for Scalable, Open SOA

The Layer 7 SecureSpan XML Gateway offers:

Secure X-domain Interactions
With support for all WS* and WS-I security protocols, as well as built-in PKI and STS capabilities, organizations can cost-effectively implement SOA security between disparate identity domains.

Lightweight Management
Centrally measure and track SOA and Web service metrics in real time across the entire enterprise without the need to instrument all endpoints.

Streamlined Governance
Automate the approval process for policy publication, and then centrally push policy to any Gateway across the enterprise, significantly decreasing the overhead associated with policy lifecycle management.

To learn more about how Layer 7 can address your organization's SOA security and management needs, call 1-800-681-9377 (toll free within North America) or +1.604.681.9377

The SecureSpan XML Gateway provides rapid deployment, low TCO and highly scalable SOA security, visibility and management for JBoss-hosted applications

SecureSpan

The Layer 7 SecureSpan Gateway is an XML appliance that can be deployed as a proxy or ESB co-processor for executing fine grained security and SLA policies in an SOA. Acting as a Policy Enforcement Point (PEP), the Gateway can be used to enforce authentication against any number of sources, operation-level authorizations, "anything" to SAML-based credentialing, XACML-based entitlements, WS* message security, throttling and latency based routing, high speed data validation and translation, as well as auditing. Additionally, the integrated Layer 7 Enterprise Service Manager delivers agent-less management capabilities, robust policy lifecycle management, remote system backup and restore, as well as global service visibility, monitoring and reporting across globally distributed deployments.

Why use XML Gateways for JBoss?

Exposing data and applications as XML-based Web services can introduce new kinds of security, performance and management challenges to your JBoss-based integration, portal, B2B and Cloud initiatives. The SecureSpan Gateway offers a non-invasive, low-cost way to add customizable security, availability and visibility controls to your SOA, Web services and Web 2.0 applications:

- Regulate access to service endpoints and APIs down to the operation or data element level
- Create new virtual API views on-the-fly, tailored to specific users and their capabilities
- Validate that data passed to Web services is legitimate/non-harmful, protecting back-end apps
- Ensure confidential data is not leaked inadvertently to outside requestors
- Enforce data level confidentiality and integrity during transmission
- Protect against malicious attacks that compromise or bring down application services
- Enforce availability SLAs based on service responsiveness, load and Quality of Service priorities
- Reuse your identity, federation, PKI & management infrastructure for Web services initiatives
- Future-proof infrastructure against changes in WS*, SAML and WS-I standards
- Ensure interoperability across different middleware, identity and transport platforms
- Automate migration of service policies from test to staging to production – even across globally distributed locations and data centers
- Route, transform and process XML in specialized hardware, improving application responsiveness and infrastructure performance
- Switch XML messages across different transport types like HTTP, JMS, MQ Series and Tibco EMS
- Gain real-time visibility into Web services infrastructure without the overhead of agents

The Layer 7 Difference

Not all XML Gateways are created equal. Layer 7 is the first XML Gateway vendor to be recognized as a Gartner Magic Quadrant Leader. It is the first to make Network Computing's "Vendor to Watch" list, and is the first to be recognized as an InfoWorld 100 company.

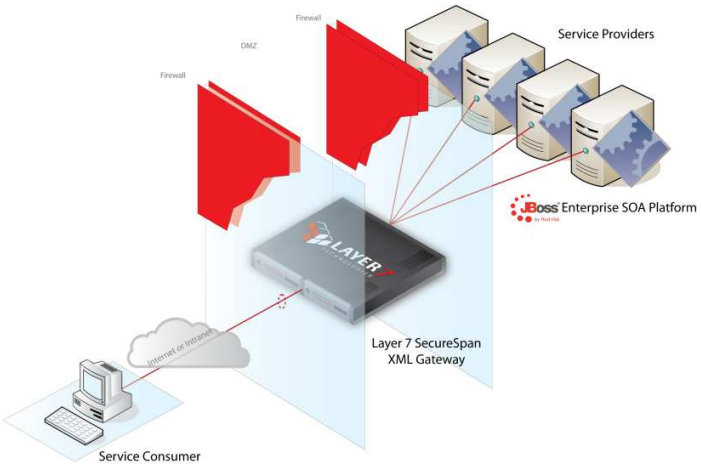
Additionally, Layer 7 is the only XML Gateway vendor to offer its solution as a Sun-based hardware appliance; as software running on Linux and Solaris; and as a virtual appliance for VMWare/ESX and cloud platforms like Amazon EC2. SecureSpan was the first appliance to offer FIPS-compliant crypto in both software and hardware; the first to ship with an SDK to simplify customization, and the first to offer "service provider scale" administration for simplified development-to-production migration, disaster recovery management and gateway lifecycle control.

Deploying Layer 7 and JBoss

The Layer 7 SecureSpan XML Gateway is typically deployed as a proxy-based intermediary that can validate schemas, perform message transforms, meditate between protocols, optimize network performance, monitor and enforce policy at runtime, secure services, throttle traffic, prioritize and route messages, meter service usage, and virtualize end points. In a JBoss-based environment, the SecureSpan Gateway can be deployed in a number of ways:

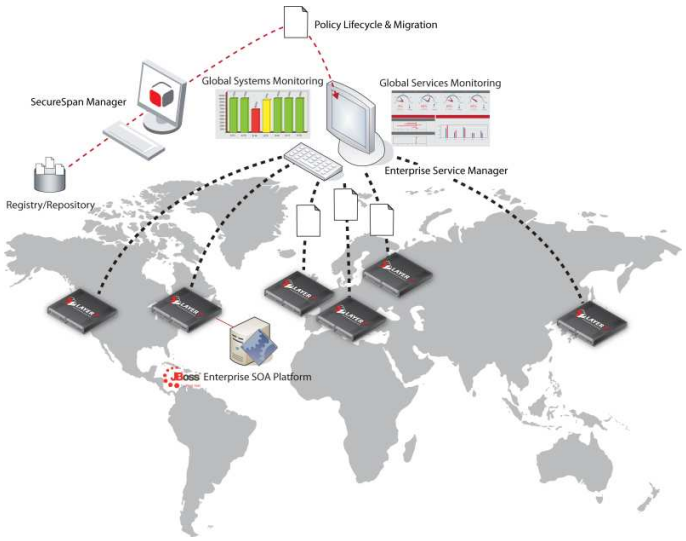
XML Firewalling

- **Security** – offers a secure, single point of entry to enterprise services that enforces WS* and WS-I security protocols in the DMZ. Validate schemas and screen incoming messages to protect against parser attacks and other threats.
- **Performance** – enhance network performance by offloading XML processing to a network edge appliance, avoiding slower agent-based parsers
- **Availability** – Layer 7 appliance clustering capabilities allow for high Web services availability
- **Virtualization** – the same service can be virtualized differently for provisioning and for consumption purposes. Each virtual version has its own WSDL subset and only certain operations are enabled based on the requester.



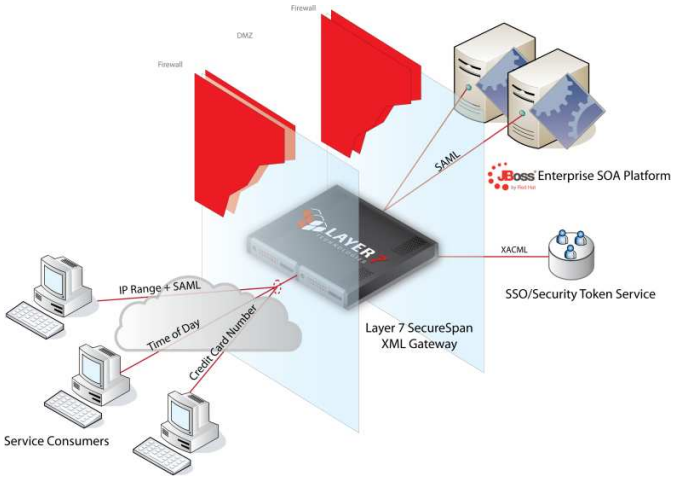
SOA Governance

- **Monitoring** – agent-less SOA management and monitoring provides faster deployment and greater scalability
- **Dashboarding** – real-time views of audits, events and service metrics, such as throughput, routing failures, utilization and availability rates
- **Policy Management** – approve policies for publication, and then centrally push policy to any Gateway across the extended enterprise, and between development, test and other environments
- **Reporting & Analysis** – configurable, out-of-the-box reports provide insight into service health and performance, as well as customer experience
- **Disaster Recovery** – one-click remote backup and restore capabilities for single Gateways or complete clusters



Fine-Grained Access Entitlements

- **Attribute-based Access Control** – leverages XACML to query a Policy Decision Point in order to enforce attribute-based access control that is essential in implementing fine-grained authorization
- **Service Level Agreements** – allow or deny access to services based on a wide range of parameters that can be enforced in policy, including time of day, IP range, partner certification, customer service level, etc.
- **Auditing** – log and track who accesses which services under what circumstances, and then filter/export for correlation and forensic analysis



Key Features	
JBoss Support	
Rapid integration with JBoss SOA-P	• Deployed as an onramp or as a security endpoint to the JBoss Enterprise SOA Platform, SecureSpan can proxy service API's hosted on JBoss, route messages over JBoss JMS, or exchange messages over SOAP and XML
Speed and scale	• With support for true clustering and centralized global administration, SecureSpan can match the performance and scale of JBoss Enterprise SOA Platform
Red Hat Enterprise Linux	• SecureSpan gateways are built on Red Hat 5, and support both RHEL 4 and 5
Identity and Message Level Security	
Identity-based access to services and operations	• Integration with leading identity, access, SSO and federation systems from Sun, RSA, Oracle, Microsoft, CA, IBM Tivoli and Novell • Enforce fine-grained entitlement decisions authored in an XACML PDP
Manage security for cross-domain and B2B relationships	• Credential chaining, credential remapping and support for federated identity • Integrated SAML STS issuer featuring comprehensive support for SAML 1.1/2.0 authentication, authorization and attribute based policies • Integrated PKI CA for automated deployment and management of client-side certificates, and integrated RA for external CAs • STS supports WS-Trust, WS-Federation and SAML-P protocols
Enforce WS* and WS-I standards	• Support for all major WS* and WS-I security protocols, including SOAP 1.0/1.1/1.2, WS-Security 1.1 / 1.2, WS-SecureConversation, WS-SecurityPolicy, WS-Addressing, WS-Trust, WS-Federation, WS-Secure Exchange, WS-Policy and WS-I Basic Security Profile, SAML 1.1/2.0, XACML
Secure WSDL, REST and POX interfaces	• Selectively control access to interfaces down to an operation level • Create on-the-fly composite WSDL views tailored to specific requestors • Service look-up and publications using WSIL and UDDI
Audit transactions	• Log message-level transaction information • Spool log data to off-board data stores and management systems
Cryptography	• Optional onboard HSM, as well as support for external HSMs (i.e., SafeNet) • FIPS 140-2 support in both hardware (Level 3) and software (Level 2)
Threat Protection	
Filter XML content for SOA, Web 2.0 and Cloud	• Configurable validation & filtering of HTTP headers, parameters and form data • Detection of classified or "dirty" words or arbitrary signatures with subsequent scrubbing, rejection or redaction of messages • Support for XML, SOAP, POX, AJAX, REST and other XML-based services
Transactional Integrity Protection	• Protect against identity spoofing and session hijacking cluster-wide • Assure integrity of communication end-to-end
Prevent XML attack and intrusion	• Protect against XML parsing; XDoS and OS attacks; SQL and malicious scripting language injection attacks; external entity attacks • Protection against XML content tampering and viruses in SOAP attachments • US Department of Defense STIG vulnerability tested and assured
XML Acceleration	
Accelerated XML processing	• High speed message transformations based on internal or external XSLT • High speed message validation against predefined external schema • High speed message searching, element detection and content comparisons
Hardware SSL and Crypto	• Offload SSL and WS-Security operations to hardware

Traffic Management	
Throttling	• Granular rate limiting and traffic shaping based on number of requests or service availability across a cluster
Cluster-wide counters	• Persist message counters across clusters so that rate limiting and traffic shaping can be strictly enforced in high availability configurations
CoS for XML	• Prioritize XML traffic based on Class of Service/Quality of Service preferences
Service availability management	• Manage routing to back-end services based on availability or latency performance
Disaster Recovery and High Availability	
Cluster-wide redundancy	• All appliance clusters operate in live active-active mode to ensure recovery from any single gateway failure • New nodes in a cluster can be added without manual re-configuration • All policy changes to a cluster can be made in real-time • Migration of policies can be managed across mirror sites remotely
Back-up and restore	• Complete backup and restore solution for both system and user configuration across globally redundant mirror sites via the Enterprise Service Manager
Management / Administration	
WS-Policy-based graphical policy editor & composer	• Compose inheritable policy statements from 70+ pre-made policy assertions • Branch policy execution based on logical conditions, message content, externally retrieved data or transaction specific environment variables • Publish policies to popular registries for lifecycle management • Service & operation level policies with inheritance for simplified administration • Policy lifecycle and migration management across development, test, staging and production, as well as geographically distributed data centers • API-level access to administration • SDK-level policy creation for simplified policy customization
On-the-fly policy changes	• Polices can be updated live across clusters with no downtime required
Global policy migration	• Streamline policy migration across development, test, staging, and production environments, as well as mirror sites using the Enterprise Service Manager
Headless operation	• Control administration directly through SOAP and RMI APIs
Create custom policies	• Policy SDK allows for custom policy assertion creation using Java
Form Factors	
Hardware	• Active-active clusterable, dual power supply, mirrored hot-swappable drives, multi-core, 64-bit 1U server
Software	• Solaris 10 for x86 and Niagara, SUSE Linux, Red Hat Linux 4.0/5.0
Virtual Appliance	• VMWare/ESX (VM Ready certified)
Cloud	• Amazon EC2 AMI
Supported Standards	
XML 1.0, SOAP 1.2, REST, AJAX, XPath 1.0, XSLT 1.0, WSDL 1.1, XML Schema, LDAP 3.0, SAML 1.1/2.0, PKCS #10, X.509 v3 Certificates, FIPS 140-2, Kerberos, W3C XML Signature 1.0, W3C XML Encryption 1.0, SSL/TLS 1.1 / 3.0, SNMP, SMTP, POP3, IMAP4, HTTP/HTTPS, JMS 1.0, MQ Series, Tibco EMS, FTP, WS-Security 1.1, WS-Trust 1.0, WS-Federation, WS-Addressing, WSSecureConversation, WS-MetadataExchange, WS-Policy, WS-SecurityPolicy, WS-PolicyAttachment, WS-SecureExchange, WSIL, WS-I, WS-I BSP, UDDI 3.0, XACML 2.0	

To learn more about how Layer 7 can address your needs, call us today at +1 800.681.9377 (toll free within North America) or +1.604.681.9377or visit us at www.layer7tech.com.