



SecureSpan™ XML Networking Gateway

Implement a robust, extensible runtime governance solution

The SecureSpan Networking Gateway offers:

Application Services Governance

Centrally enforce policies that ensure security, compliance, reliability, and quality of service for all application services no matter where they reside – in the enterprise or in the cloud.

Extensible Policies

The SecureSpan Custom Assertion SDK allows Java programmers to create new policy assertions to address unique requirements.

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

Control, monitor and adapt application services over time by enforcing policies around security, compliance, SLAs and quality of service.

Runtime Policy Enforcement

As organizations increase their adoption of Web services, attempting to control, monitor and adapt them over time by imposing general IT rules becomes more and more challenging. For this reason, most organizations adopt a policy-driven Web services model, but without the ability to control and audit how policy gets deployed and enforced at runtime, there's no way to ensure consistent security, adherence to corporate business rules, or compliance with regulatory requirements.

The SecureSpan XML Networking Gateway combines policy management with runtime policy enforcement, delivering an effective governance model for distributed SOAs. By deploying the Networking Gateway as a central Policy Enforcement Point (PEP) between service providers and consumers (no matter where they're located – in the traditional enterprise, or in public or private clouds), organizations can create a runtime governance solution that offers the ability to:

- **Control Services** – enforce policies that call out to identity management infrastructure (such as an LDAP or IAM system) to ensure security; verify messages for integrity and adherence to industry or government-mandated specifications; and capture and track key non-repudiation data in logs and audit files to facilitate compliance.
- **Monitor Services** – enforce policies that throttle and/or reroute incoming messages, automatically heading off service performance issues before they happen in order to maintain availability and reach-ability. Additionally, implement policies that measure and react to network slowdowns, poor service response times or even service disruption in order to conform to SLAs and maintain Quality of Service.
- **Adapt Services** – change the way application services respond at runtime by centrally modifying policies and deploying them in real time to Networking Gateways without the need to bring down the appliances.

Extensibility

Layer 7 provides dozens of out-of-the-box assertions with which organizations can graphically build policies to address the most common aspects of controlling, managing and monitoring application services. But for those organizations that want to tailor a solution to better fit their business needs, Layer 7 provides the Custom Policy Assertion SDK. The Java-based SDK extends the rich palette of SecureSpan policy assertions allowing organizations to create policies that address unique requirements, such as:

- proprietary message processing
- pattern recognition and filtering
- interfacing to third-party infrastructure
- And many more

Sample custom assertions are provided for integration to a range of leading identity management products from Sun, IBM, CA, Oracle and others.

Key Features	
SOA Governance	
Runtime enforcement of governance policies	<ul style="list-style-type: none"> Enforce security policies such as those that digitally sign and/or encrypt parts of the message; issue security tokens to ensure proper authentication, etc Enforce compliance with policies such as those that verify message structure and content to meet corporate, industry or government standards, etc Enforce reliability with policies such as those that reroute traffic to facilitate failover; throttle traffic to ensure availability and maintain quality of service, etc
Centralized SLA enforcement/Quality of Service	<ul style="list-style-type: none"> Throttling/rate limiting controls provide the ability to support service over subscription with per-service throttling of excess messages Service availability features include support for strict failover, round robin, best effort and latency-based routing
Transport and protocol mediation	<ul style="list-style-type: none"> Full support for Class of Service based message processing and routing based on identity, message content, time of day, etc Transport mediation between HTTP, HTTPS, MQS, JMS
Service virtualization	<ul style="list-style-type: none"> Smart WSDL generation for non-SOAP services WSDL remapping and service virtualization based on requestor identities Authorization controls for access to specific service operations
Policy Lifecycle	
WS-Policy-based graphical policy editor & composer	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Polices can be updated live across clusters with no downtime required
Create custom policies	<ul style="list-style-type: none"> Policy SDK allows for custom policy assertion creation using Java
Identity and Message Level Security	
Identity-based access to services and operations	<ul style="list-style-type: none"> Integration with leading external identity, access, SSO and federation systems Onboard identity store for administering identities and staging new services
Manage security for cross-domain and B2B relationships	<ul style="list-style-type: none"> Credential chaining, credential remapping and support for federated identity Integrated STS/SAML issuer supports SAML 1.1/2.0 Integrated PKI CA for automated deployment and management of client-side certificates and RA ability for external CA's including Verisign
Cryptography	<ul style="list-style-type: none"> Optional onboard HSM, as well as support for external HSMs (i.e., SafeNet Luna) Support for elliptic curve cryptography (conforms to NSA's Suite B algorithms) FIPS 140-2 support in both hardware (Level 3) and software (Level 1)
API Management	
API Publication	<ul style="list-style-type: none"> Secure, manage, monitor and control access to APIs exposed to third parties API usage can be throttled to ensure backend services are not overwhelmed; limited by user, time of day, location, etc; and quota managed (i.e., # of uses per user per day)
API Metrics and Reporting	<ul style="list-style-type: none"> Configurable, out-of-the-box reports provide insight into API performance: measure throughput, routing failures, utilization and availability rates, etc Failed authentications and/or policy violations can be tracked to identify patterns and potential threats

API Security	<ul style="list-style-type: none"> • Support for all major WS* and WS-I security protocols • Support for all major authentication and authorization standards, including SAML, Kerberos, digital signatures, X.509 certificates, LDAP, XACML, etc
Threat Protection	
Filter XML content for Web 2.0 and SOA	<ul style="list-style-type: none"> • 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
Prevent XML attack and intrusion	<ul style="list-style-type: none"> • Protect against XML parsing; XDoS and OS attacks; SQL and malicious scripting language injection attacks • Protection against XML content tampering and viruses in SOAP attachments
XML Acceleration	
Accelerated XML message processing offload	<ul style="list-style-type: none"> • 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
Optional hardware-based acceleration	<ul style="list-style-type: none"> • ASIC-based hardware accelerator can be optionally used to maximize message throughput and minimize processing latency
Enterprise-scale Management	
Operations Console	<ul style="list-style-type: none"> • A single, real time view of all Gateways across the enterprise and cloud showing audits, events and key metrics
Policy Migration	<ul style="list-style-type: none"> • Centrally move policies between environments (development, testing, staging, production, etc), settings (enterprise, cloud, etc) or geographies, automatically resolving discrepancies such as SSG licenses, IP addresses, IT resources (i.e., LDAPs may be named differently), etc
Services Reporting	<ul style="list-style-type: none"> • Configurable, out-of-the-box reports provide insight into SSG operations, service-level performance, and service user experience
Remote Patching	<ul style="list-style-type: none"> • Selectively update any software installed on Gateways, including system files and operating system
Disaster Recovery	<ul style="list-style-type: none"> • Centrally back up SSG config files and policies from one or more Gateways/clusters, and remotely restore, enabling full disaster recovery
Management API	<ul style="list-style-type: none"> • Remote management APIs allow customers to hook their existing, third-party management tools into the SSG, simplifying asset management
Form Factors	
Hardware	<ul style="list-style-type: none"> • Active-active clusterable, dual power supply, mirrored hot-swappable drives, 2-way dual core Sun 1U server
Software	<ul style="list-style-type: none"> • Solaris 10 for x86 and Niagara, SUSE Linux, Red Hat Linux 4.0/5.0
Virtual Appliance	<ul style="list-style-type: none"> • VMware/ESX (VMware Ready certified)
Cloud	<ul style="list-style-type: none"> • 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 3.0/1.1, 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, MTOM	

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 +1.604.681.9377 or visit us at www.layer7tech.com.