



SecureSpan™ XML Firewall

Industry-leading XML and Web services security for SOA, Web 2.0 and Cloud deployments

The SecureSpan XML Firewall offers:

Full functionality

The SecureSpan XML Firewall combines the capabilities of the SecureSpan XML Accelerator and Data Screen with advanced identity and message level security allowing organizations to:

- Control fine grained service access and entitlements
- Protect services against attack & damage from malformed data
- Graphically manage message and element level privacy and integrity rules
- Stop data leakage
- Future-proof integrations against changes in security standards and technology
- Selectively control how APIs get exposed to consumers inside and outside the corporation
- Extend strong authentication and SSO to Web services
- Span federated application domains
- Optimize service availability and responsiveness

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

Secure your application and infrastructure services with a centrally configurable, scalable, purpose-built XML security gateway.

Secure Services

Traditionally, security and entitlement requirements have been coded into each and every application service in the organization. When those requirements (or the standards on which they're based) change, every service needs to be updated. Centralizing XML and Web services security requirements in policy that can be defined and enforced outside of your applications provides consistent security, while simplifying administration burdens. With centralized XML and Web services security policies in place, changes can be instituted as new or updated policy rules, dramatically decreasing down time and IT maintenance costs.

The SecureSpan XML Firewall is a policy-driven identity and security enforcement point that can be implemented both in the enterprise and in the cloud to address a broad range of behind the firewall, SOA, Web 2.0, B2B and Cloud security challenges. With support for all leading directory, identity, access control, Single Sign-On (SSO) and Federation services, the XML Firewall can provide application services and security architects unparalleled flexibility in defining and enforcing identity-driven security policies leveraging SSO session cookies, Kerberos tickets, SAML assertions and Public Key Infrastructure (PKI). Support for all major WS* and WS-I security protocols provides architects with advanced policy controls for specifying message and element security rules, including the ability to branch policy based on any message context. The XML Firewall also ensures enterprise application and infrastructure services are protected against malicious attack or accidental damage due to poorly structured data.

Key storage, encryption and signing operations can be handled in FIPS 140-2 certified acceleration hardware onboard the appliance, or optionally through Sun's SCA6000 Hardware Security Module.

Share Services

When application services are shared across security and identity domains a number of requirements need to be addressed, including how to reconcile identity domains, provision PKI for certificate-based trust, integrate with an existing SSO infrastructure, enable non-repudiation, and manage policy changes between a service provider and client application.

The SecureSpan XML Firewall offers a cost-effective solution to bridging identities in federated Web services environments. Featuring built-in PKI and Secure Token Service (STS) capabilities, the XML Firewall can act not only as a Certificate Authority/Registration Authority (CA/RA), but also as an issuer of signed security tokens ensuring authentication can occur close to the requestor for maximum reliability, while authorization occurs close to the provider in order to maintain strict localized access control. In this way, the XML Firewall delivers the confidentiality, flexibility, and consistent security required in an enterprise-class solution.

Key Features	
Identity and Message Level Security	
Identity-based access to services and operations	<ul style="list-style-type: none"> Integration with leading identity, access, SSO and federation systems including LDAP, Microsoft Active Directory/Federated Services, Oracle Access Manager, IBM Tivoli (TAM and TFIM), CA SiteMinder and TransactionMinder, RSA ClearTrust, Sun Java Access Manager and Novell Access Manager 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 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 (including Verisign)
Enforce WS* and WS-I standards	<ul style="list-style-type: none"> Support for all major WS* and WS-I security protocols, including WS-Security, WS-SecureConversation, WS-SecurityPolicy, WS-Trust, WS-Secure Exchange, WS-Policy and WS-I Basic Security Profile
Secure service WSDL interfaces	<ul style="list-style-type: none"> Access to WSDL is based on requestor identity, preventing WSDL browsing by unauthorized clients
Audit transactions	<ul style="list-style-type: none"> Log files provide an audit trail of all transactions mediated by the XML Firewall
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)
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
Transactional Integrity Protection	<ul style="list-style-type: none"> Protect against identity spoofing and session hijacking cluster-wide Assure integrity of communication end-to-end
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
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
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

Traffic Management	
Throttling	<ul style="list-style-type: none"> Granular rate limiting and traffic shaping based on number of requests or service availability across a cluster
Cluster-wide counters	<ul style="list-style-type: none"> Persist message counters across clusters so that rate limiting and traffic shaping can be strictly enforced in high availability configurations
CoS for XML	<ul style="list-style-type: none"> Prioritize XML traffic based on Class of Service/Quality of Service preferences
Service availability management	<ul style="list-style-type: none"> Manage routing to back-end services based on availability or latency performance
Policy Lifecycle	
WS-Policy-based graphical policy editor & composer	<ul style="list-style-type: none"> Compose inheritable policy statements from over 70 pre-made atomic 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 and 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
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)
Supported Standards	
<p>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</p>	

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.