



# 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. You can also email us at [info@layer7.com](mailto:info@layer7.com); friend us on [facebook.com/layer7](https://facebook.com/layer7); visit us at [layer7.com](http://layer7.com), or follow-us on twitter @layer7.

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 management operations can be handled in a FIPS 140-2 certified Hardware Security Module (HSM) onboard the appliance, or optionally through a centralized HSM such as SafeNet's Luna.

## 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.

<b>Key Features</b>	
<b>Identity and Message Level Security</b>	
Identity-based access to services and operations	<ul style="list-style-type: none"> <li>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</li> <li>Support for Web/browser-based SSO</li> <li>Onboard identity store for administering identities and staging new services</li> </ul>
Manage security for cross-domain and B2B relationships	<ul style="list-style-type: none"> <li>Credential chaining, credential remapping and support for federated identity</li> <li>Integrated STS/SAML issuer featuring support for SAML 1.1/2.0 authentication, authorization and attribute based policies and Security Context Tokens</li> <li>Integrated PKI CA for automated deployment and management of client-side certificates, and integrated RA for external CAs (including Verisign)</li> </ul>
Enforce WS* and WS-I standards	<ul style="list-style-type: none"> <li>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</li> </ul>
Secure service WSDL interfaces	<ul style="list-style-type: none"> <li>Access to WSDL is based on requestor identity, preventing WSDL browsing by unauthorized clients</li> </ul>
Audit transactions	<ul style="list-style-type: none"> <li>Log files provide an audit trail of all transactions mediated by the XML Firewall</li> </ul>
Cryptography	<ul style="list-style-type: none"> <li>Optional onboard HSM, and support for external HSMs (i.e., nCipher, Luna, etc)</li> <li>Support for elliptic curve cryptography (conforms to NSA's Suite B algorithms)</li> <li>FIPS 140-2 support in both hardware (Level 3) and software (Level 1)</li> </ul>
<b>Threat Protection</b>	
Filter XML content for Web 2.0 and SOA	<ul style="list-style-type: none"> <li>Configurable validation &amp; filtering of HTTP headers, parameters and form data</li> <li>Detection of classified or "dirty" words or arbitrary signatures with subsequent scrubbing, rejection or redaction of messages</li> <li>Support for XML, SOAP, POX, AJAX, REST and other XML-based services</li> </ul>
Transactional Integrity Protection	<ul style="list-style-type: none"> <li>Protect against identity spoofing and session hijacking cluster-wide</li> <li>Assure integrity of communication end-to-end</li> </ul>
Prevent XML attack and intrusion	<ul style="list-style-type: none"> <li>Protect against XML parsing; XDoS; OS; SQL injection attacks, etc</li> <li>Protection against XML content tampering and viruses in SOAP attachments</li> </ul>
<b>API Management</b>	
API Publication	<ul style="list-style-type: none"> <li>Secure, manage, monitor and control access to APIs exposed to third parties</li> <li>API usage can be limited to ensure backend services are not overwhelmed; limited by user, time of day, location, etc; and quota managed (i.e., # of uses/user/ day)</li> </ul>
API Metrics and Reporting	<ul style="list-style-type: none"> <li>Configurable, out-of-the-box reports provide insight into API performance: measure throughput, routing failures, utilization and availability rates, etc</li> <li>Track failed authentication/policy violations to identify patterns &amp; potential threats</li> </ul>
API Security	<ul style="list-style-type: none"> <li>Support for all major WS* and WS-I security protocols</li> <li>Support for all major authentication and authorization standards, including SAML, Kerberos, digital signatures, X.509 certificates, LDAP, XACML, etc</li> </ul>
<b>Acceleration</b>	
Accelerated XML message processing offload	<ul style="list-style-type: none"> <li>High speed message transformations based on internal or external XSLT</li> <li>High speed message validation against predefined external schema</li> <li>High speed message searching, element detection and content comparisons</li> </ul>
Optional hardware-based acceleration	<ul style="list-style-type: none"> <li>ASIC-based hardware accelerator can be optionally used to maximize message throughput and minimize processing latency</li> </ul>
<b>Performance</b>	
Message Caching	<ul style="list-style-type: none"> <li>Cache responses to common requests, decreasing back-end service load</li> </ul>

<b>Traffic Management</b>	
Throttling	<ul style="list-style-type: none"> <li>Granular rate limiting and traffic shaping based on number of requests or service availability across a cluster</li> </ul>
Cluster-wide counters	<ul style="list-style-type: none"> <li>Persist message counters across clusters so that rate limiting and traffic shaping can be strictly enforced in high availability configurations</li> </ul>
CoS for XML	<ul style="list-style-type: none"> <li>Prioritize XML traffic based on Class of Service/Quality of Service preferences</li> </ul>
Service availability management	<ul style="list-style-type: none"> <li>Service availability features include support for strict failover, round robin, and best effort routing</li> </ul>
<b>Policy Lifecycle</b>	
WS-Policy-based graphical policy editor & composer	<ul style="list-style-type: none"> <li>Compose inheritable policy statements from over 70 pre-made atomic policy assertions</li> <li>Branch policy execution based on logical conditions, message content, externally retrieved data or transaction specific environment variables</li> <li>Create and implement global policies that apply to all incoming messages</li> <li>Publish policies to popular registries for lifecycle management</li> <li>Service and operation level policies with inheritance for simplified administration</li> <li>Policy lifecycle and migration management across development, test, staging and production, as well as geographically distributed data centers</li> <li>API-level access to administration</li> <li>SDK-level policy creation for simplified policy customization</li> </ul>
On-the-fly policy changes	<ul style="list-style-type: none"> <li>Polices can be updated live across clusters with no downtime required</li> </ul>
<b>Enterprise-scale Management</b>	
Operations Console	<ul style="list-style-type: none"> <li>A single, real time view of all Gateways across the enterprise and cloud showing audits, events and key metrics</li> </ul>
Policy Migration	<ul style="list-style-type: none"> <li>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</li> </ul>
Services Reporting	<ul style="list-style-type: none"> <li>Configurable, out-of-the-box reports provide insight into SSG operations, service-level performance, and service user experience</li> </ul>
Remote Patching	<ul style="list-style-type: none"> <li>Selectively update any software installed on Gateways, including system files &amp; OS</li> </ul>
Disaster Recovery	<ul style="list-style-type: none"> <li>Centrally back up SSG config files and policies from one or more Gateways/clusters, and remotely restore, enabling full disaster recovery</li> </ul>
Management API	<ul style="list-style-type: none"> <li>Remote management APIs allow customers to hook their existing, third-party management tools into the SSG, simplifying asset management</li> </ul>
<b>Form Factors</b>	
Hardware	<ul style="list-style-type: none"> <li>Active-active clusterable, dual power supply, mirrored hot-swappable drives, multi-core 1U server</li> </ul>
Software	<ul style="list-style-type: none"> <li>Solaris 10 for x86 and Niagara, SUSE Linux, Red Hat Linux 4.0/5.0</li> </ul>
Virtual Appliance	<ul style="list-style-type: none"> <li>VMware/ESX (VMware Ready certified)</li> </ul>
<b>Supported Standards</b>	
XML, JSON, SOAP, REST, PCI-DSS, AJAX, XPath, XSLT, WSDL, XML Schema, LDAP, SAML, PKCS, FIPS 140-2, Kerberos, X.509 Certificates, XML Signature, XML Encryption, SSL/TLS, SNMP, SMTP, POP3, IMAP4, HTTP/HTTPS, MQ Series, Tibco EMS, WS-Security, WS-Trust, WS-Federation, WS-SecureExchange, WS-Addressing, WS-SecureConversation, WS-MetadataExchange, WS-Policy, WS-SecurityPolicy, WS-PolicyAttachment, WSIL, WS-I, WS-I BSP, UDDI, WSRR, MTOM, IPv6, WCF	

To learn more about Layer 7 call us today at +1 800.681.9377 (toll free within North America) or +1.604.681.9377. You can also email us at [info@layer7.com](mailto:info@layer7.com); friend us on [facebook.com/layer7](https://facebook.com/layer7); visit us at [layer7.com](http://layer7.com), or follow-us on twitter [@layer7](https://twitter.com/layer7).