



SecureSpan™ XML Virtual Appliance

Reduce SOA development, test and implementation costs, while improving architectural flexibility

The SecureSpan XML Virtual Appliance offers:

Cost-effective Solution

A turnkey solution that bundles sophisticated runtime governance, enterprise-scale SOA management and industry-leading XML security as a VMware Ready virtual appliance that can be deployed on commodity hardware.

Cloud-based Security & Privacy

A virtual policy enforcement point provides isolation, monitoring and control over application services in both public and private clouds.

To learn more about Layer 7 and how we can address your organization's cloud 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; friend us on [facebook.com/layer7](https://www.facebook.com/layer7); visit us at layer7.com, or follow-us on twitter @layer7.

SecureSpan XML Gateway Virtual Appliance for VMware/ESX can be rapidly deployed in development, test, production and cloud environments.

Cost Control

The SecureSpan XML Virtual Appliance for VMware (XML Virtual Appliance) delivers all the functionality of Layer 7's hardware-based XML Gateways in a soft appliance form factor that can be rapidly deployed on commodity hardware. For scenarios in which high performance is not a critical requirement (such as development and test, as well as low volume production environments), the XML Virtual Appliance is a good fit, offering a smaller footprint and more economical alternative to hardware appliances.

The XML Virtual Appliance provides organizations with an all-in-one turnkey solution for governing day-to-day SOA operations, including Web services security, governance and management. And like all of Layer 7's hardware gateways, the XML Virtual Appliance can be managed through the SecureSpan Policy Manager, Management API and Enterprise Service Manager.

Between enterprises, the Virtual Appliance can be deployed in conjunction with the SecureSpan XML VPN Client to securely bridge cross-domain communications without coding. The result is a cost-effective, near "drop-in" solution to the federated identity problem, eliminating the need to re-code and re-test client applications when a Web service provider's security, routing, and transaction preferences change.

Cloud Control

Public and private clouds let organizations expense new capacity rather than having to realize capital costs, allowing them to effectively convert CapEx to OpEx. Unfortunately, adopting cloud-based services or moving application services to the cloud poses a number of risks, including:

- Security and Privacy – how can I be sure that my data and applications will be secure?
- Business Continuity – what happens if my ISP or cloud provider goes down?
- Business Value – how can I be sure my cloud service provider is meeting my SLA?
- Compliance – how can I ensure regulatory/legal compliance?

For organizations that require visibility, trust and control over cloud-based services, the SecureSpan XML Virtual Appliance can help secure, monitor and manage interactions with public and private clouds.

The XML Virtual Appliance acts as a virtual Policy Enforcement Point (vPEP) that can be deployed in front of cloud applications to protect and manage services. Application-level policy enforcement allows organizations to implement fine-grained access control and gain an in-depth understanding of service usage, monitoring and protecting data and applications from unauthorized use. Additionally, policies can be implemented to manage requests to virtualized application services in order to provide load balancing and failover between private and/or public clouds, avoiding vendor lock-in.



Key Features	
Cloud Governance	
Virtualized Gateway	<ul style="list-style-type: none"> VMware/ESX support facilitates deployment to both private and public clouds
Monitoring	<ul style="list-style-type: none"> Configurable reports provide insight into cloud-based XML Virtual Appliance health, and metrics (i.e., throughput, routing failures, utilization and availability)
Security	<ul style="list-style-type: none"> Manage access from cloud-based application services to enterprise-based assets with industry-leading access control, alarms/audits, and secure routing capabilities
SLA enforcement	<ul style="list-style-type: none"> Measure/track performance to ensure vendors meet uptime/contract obligations
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 and best effort 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, raw TCP
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
Identity and Message Level Security	
Identity-based access	<ul style="list-style-type: none"> Authenticate users and applications based on identities stored on-site/on-premise Integrate with leading identity, access, SSO and federation systems from Oracle, Sun, Microsoft, CA, IBM Tivoli, Novell Support for Web/browser-based SSO Enforce fine-grained entitlements authored in an XACML PDP, ensuring only users and applications with correct entitlements can access specific services, operations or APIs
Manage security for cross-domain and B2B relationships	<ul style="list-style-type: none"> Selectively control how your applications get programmatically exposed Support for credential chaining, credential remapping and federated identity Integrated SAML STS issuer featuring support for SAML 1.1/2.0 authentication, authorization and attribute based policies, as well as Security Context Tokens 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	<ul style="list-style-type: none"> Support for all major WS* and WS-I security protocols, such as WS-Security, WS-SecureConversation, WS-SecurityPolicy, WS-Addressing, WS-Trust, WS-Federation, WS-Secure Exchange, WS-Policy and WS-I Basic Security Profile
Secure WSDL, REST and POX interfaces	<ul style="list-style-type: none"> Selectively control access to interfaces down to an operation level Create on-the-fly composite WSDL views tailored to specific requestors Support service look-up and publication via WSIL and UDDI
Audit transactions	<ul style="list-style-type: none"> Log any/all message-level transaction information
Cryptography	<ul style="list-style-type: none"> Support for elliptic curve cryptography (conforms to NSA's Suite B algorithms) FIPS 140-2 support in software (Level 1) Support for external HSMs (i.e., nCipher, Luna, etc)

Performance	
Message Caching	<ul style="list-style-type: none"> • Cache responses to common requests, decreasing back-end service load
Concurrent Assertion Processing	<ul style="list-style-type: none"> • Run multiple assertions concurrently, thereby reducing overall latency when performing orchestration
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 • Create and implement global policies that apply to all incoming messages • 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 changes	<ul style="list-style-type: none"> • Policies can be updated live across clusters with no downtime required
Create custom policy	<ul style="list-style-type: none"> • Policy SDK allows for custom policy assertion creation using Java
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/user/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 • Track failed authentications and/or policy violations to identify patterns & potential threats
API Security	<ul style="list-style-type: none"> • 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 and 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; OS; SQL injection attacks, etc • Protection against XML content tampering and viruses in SOAP attachments
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 OS
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

Supported Standards

XML, JSON, SOAP, REST, PCI-DSS, AJAX, XPath, XSLT, WSDL, XML Schema, LDAP, SAML, XACML, Kerberos, OAuth, PKCS, FIPS 140-2, XML Signature, XML Encryption, SSL/TLS, SNMP, SMTP, POP3, IMAP4, X.509 Certificates, JMS, HTTP/HTTPS, FTP/FTPS, MQ Series, Tibco EMS, WS-Security, WS-Trust, WS-Federation, WS-SecureExchange, WS-Addressing, WS-SecureConversation, WS-MetadataExchange, WS-Policy, WS-SecurityPolicy, WSIL, WS-I, WS-I BSP, WS-PolicyAttachment, UDDI, WSRR, MTOM, IPv6, WCF

The SecureSpan XML Virtual Appliance supports VMware/ESX, and can be deployed in public or private clouds, as well as within traditional enterprise networks.

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; friend us on [facebook.com/layer7](https://www.facebook.com/layer7); visit us at layer7.com, or follow-us on twitter [@layer7](https://twitter.com/layer7).