



SecureSpan™ XML Gateway & Oracle

Secure, accelerate and simplify your Oracle identity and SOA implementations with the industry's leading XML Gateway

The Layer 7 SecureSpan XML Gateway offers:

Identity-driven SOA

With support for key Oracle identity products, organizations can gain even greater value from their existing infrastructure investments by centrally enforcing authentication and authorization.

Protect and Connect: Secure Cross-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.

Cloud Ready

With native images for Cloud platforms like Amazon EC2, Layer 7 can secure Cloud-hosted services as easily as enterprise hosted services.

To learn more about how Layer 7 can address your organization's SOA, Web 2.0 and Cloud needs while leveraging your existing Oracle investments, call 1-800-681-9377 (toll free within North America) or +1.604.681.9377

Secure Oracle-based systems by providing a DMZ-based enforcement point for policy-driven security, availability and visibility.

Why XML Gateways

Exposing data and applications as XML-based Web services can introduce new kinds of security, performance and management challenges to your integration, portal, B2B and Cloud initiatives. The Layer 7 SecureSpan XML Gateway offers a non-invasive, low-cost way to add customizable security, availability and visibility controls to your service-based initiatives.

XML Gateways can help enhance SOA, Web 2.0 and Cloud security, performance and reliability, as well as:

- Regulate who has access to which 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 being passed to Web services is legitimate and non-harmful before it can impact back-end applications
- 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 existing identity, federation, PKI and 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 and forensic visibility into Web services infrastructure without the computing overhead of agents and probes

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.

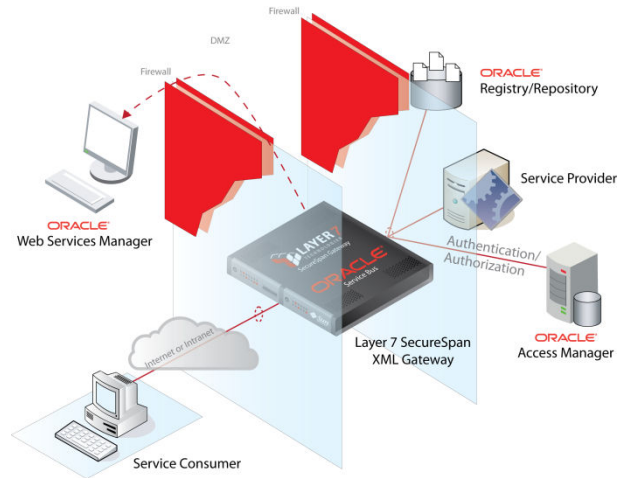
Additionally, Layer 7 is the only XML Gateway vendor to offer its solution as a Sun-based hardware appliance; as software running on Linux and Solaris; and as a virtual appliance for VMWare/ESX and cloud platforms like Amazon EC2. The SecureSpan Gateway was the first appliance to offer FIPS-compliant 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 Oracle

The Layer 7 SecureSpan XML Gateway is typically deployed as a proxy-based intermediary that can validate schemas, perform message transforms, mediate 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 an Oracle-based environment, the SecureSpan Gateway can be deployed in a number of ways:

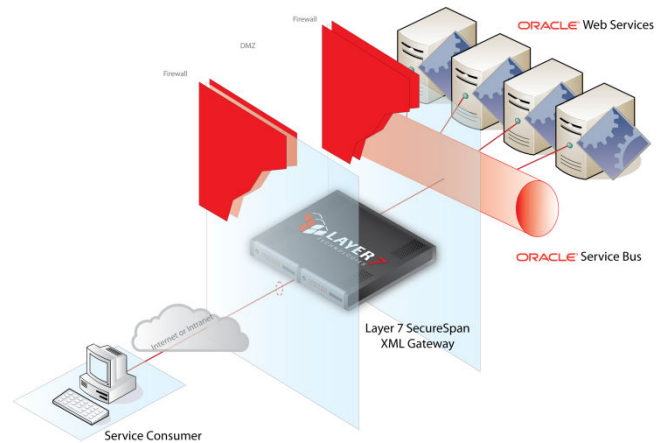
SOA Intermediary

- **Security** – access policies enforced by the SecureSpan Gateway at runtime can call out to Oracle Access Manager to verify authentication and authorization information
- **Performance** – enhance network performance by offloading XML processing to a network edge appliance, avoiding slower agent-based parsers
- **Monitoring** – the Gateway can interoperate with Oracle Web Services Manager (OWSM)
- **Availability** – Layer 7 appliance clustering capabilities allow for high Web services availability
- **Governance** – Layer 7's runtime Governance capabilities complement the Oracle Registry design-time Governance capabilities, creating a more complete SOA Governance solution



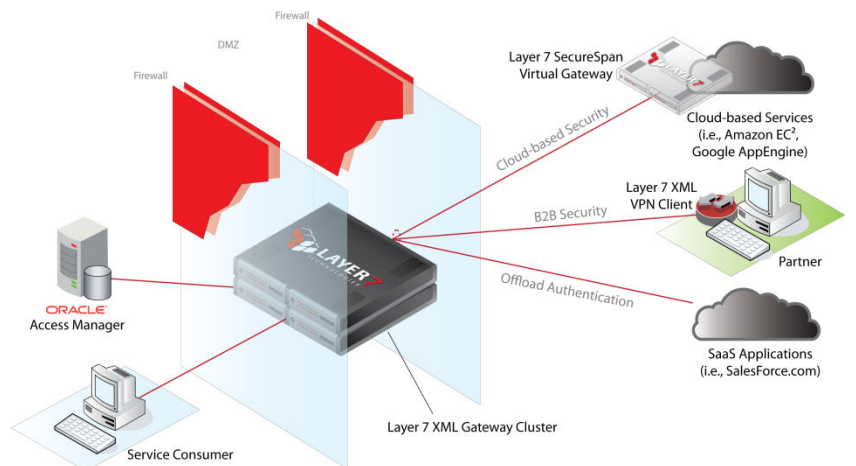
SOA Edge Gateway

- **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.
- **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.
- **Co-processor** – offload CPU-intensive XML message processing activities, message structure validation and message transformations



Cross-Domain Security

- **Local Authentication** – avoid the security risk of storing enterprise userid/passwords outside the enterprise by leveraging Oracle Access Manager for local authentication
- **B2B Security** – leverage the Layer 7 XML VPN Client in conjunction with the SecureSpan Gateway to overcome the separation of authentication and authorization tasks across trust boundaries.
- **Cloud-based Security** – leverage the Layer 7 SecureSpan Virtual Appliance to secure application services on cloud providers such as Amazon's EC2 or Google's AppEngine



Key Features	
Oracle Support	
Oracle Internet Directory	<ul style="list-style-type: none"> Offload authentication to Oracle Internet Directory
Oracle Access Manager	<ul style="list-style-type: none"> Offload authentication decisions to Oracle Access Manager (OAM)
Oracle Service Bus	<ul style="list-style-type: none"> Acts as a JMS-capable security proxy or service endpoint to Oracle Service Bus (OSB)
Oracle Web Services Mgr	<ul style="list-style-type: none"> Interoperate with Oracle Web Services Manager (OWSM)
Oracle Registry	<ul style="list-style-type: none"> Lookup service interfaces from Oracle Registry
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 from Oracle, Sun, Microsoft, CA, IBM Tivoli, Novell Enforce fine-grained entitlement decisions authored in an XACML PDP
Manage security for cross-domain and B2B relationships	<ul style="list-style-type: none"> Credential chaining, credential remapping and support for federated identity Integrated SAML STS issuer featuring support for SAML 1.1/2.0 authentication, authorization and attribute based policies and Security Context Tokens Integrated PKI CA for automated deployment and management of client-side certificates, and integrated RA for external CAs STS support through WS-Trust and WS-Federation
Enforce WS* and WS-I standards	<ul style="list-style-type: none"> 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 2.0
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 Out of the box support for popular Cloud & SaaS interfaces from SFDC & Amazon Service look-up and publications using WSIL and UDDI
Audit transactions	<ul style="list-style-type: none"> Log message-level transaction information Spool log data to off-board data stores and management systems
Cryptography	<ul style="list-style-type: none"> Optional onboard HSM and support for external HSMs (i.e., nCipher, Luna, etc) Support for elliptic curve cryptography (conforms to NSA's Suite B algorithms) 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	<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; external entity attacks Protection against XML content tampering and viruses in SOAP attachments DoD STIG vulnerability tested and assured
XML Acceleration	
Accelerated XML processing	<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
Hardware SSL and Crypto	<ul style="list-style-type: none"> Offload SSL and WS-Security operations to hardware
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

	<ul style="list-style-type: none"> 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
Performance	
Message Caching	<ul style="list-style-type: none"> Cache responses to common requests, decreasing back-end service load
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 mgmt	<ul style="list-style-type: none"> Manage routing to back-end services based on availability
Disaster Recovery and High Availability	
Cluster-wide redundancy	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Complete backup and restore solution for both system and user configuration across globally redundant mirror sites
Management / Administration	
WS-Policy-based graphical policy editor & composer	<ul style="list-style-type: none"> Compose inheritable policy statements from 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"> Policies can be updated live across clusters with no downtime required
Global policy migration	<ul style="list-style-type: none"> Manage policy migration across development, test, staging, and production environments, as well as mirror sites
Headless operation	<ul style="list-style-type: none"> Control administration directly through SOAP and RMI APIs
Create custom policies	<ul style="list-style-type: none"> Policy SDK allows for custom policy assertion creation using Java
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 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, MTOM, IPv6	

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.