

# Sun and Layer 7

## Identity-Driven SOA Governance



### Highlights

- SOA security appliance providing centralized policy enforcement for identity-driven SOA operations, and protection against malicious or accidental attack.
- Facilitates client authentication, service-level authorization, message privacy and transaction integrity validation.
- Offers hardware acceleration of XML parsing, validation and transformation for fast policy execution.
- Assures high service availability and reliability through clustering, Web service virtualization and SLA enforcement features.
- Easy-to-configure administrator options for encryption/decryption, signature and WS\* security policies.
- Integration with Sun Java Identity Management Suite and Composite Application Platform Suite (Java CAPS).



Platform-independent XML/Web services are often the cornerstone of business application integration and Service Oriented Architecture (SOA) development. When these services and business processes traverse multiple, heterogeneous back-end systems and infrastructure, providing reliable security while maintaining performance is an enormous challenge. Sun and Layer 7 Technologies remove this obstacle by combining Layer 7 SecureSpan SOA appliances (delivered on Sun Fire X4100 servers) with the Sun Java Composite Application Platform Suite (Java CAPS) and Java Identity Management Suite, to create a seamless path from SOA design to composition to secure management.

### SOA identity and security challenges

Identity is at the heart of SOA security, driving authentication and authorization decisions for all client-service interactions. The ability to validate identity is also central to enforcing transactional integrity, message privacy and accountability policies. However, defining and enforcing identity-based security policies in an SOA is complicated. Machine identities for client applications must be repositied within a centrally accessible directory.

Services must be able to:

- Extract identity information from credentials passed to them inside a Web service's SOAP message
- Validate those credentials against a centralized identity directory
- Enforce an identity-centric security policy like authentication.

In many instances, there is also a requirement to transpose messages or generate new security tokens (e.g. SAML) for secure, interoperable communication with back-end services.

In addition to identity-based access, privacy, integrity and accounting policies, SOA security solutions must also:

- Protect back-end Web services against attack and exploit, either malicious (DoS, replay, parser exploit, ..) or accidental (malformed XML, invalid data, ...).

- Implement and intermediate various XML, WS\*, W3C SAML, and WS-I security standards.
- Filter, extract or redact confidential information entering or leaving an organization.
- Assure endpoint availability and performance through effective communication optimization, cluster management and SLA enforcement.

### High-performance SOA identity, security solutions

The SecureSpan XML Networking Gateway is a SOA security hardware or virtual software appliance that provides SOA architects a centralized policy enforcement point for identity-driven SOA security operations, including client authentication, service level authorization, message privacy and transaction integrity validation. The SecureSpan XML Networking Gateway integrates with Sun Java System Access Manager such that an existing access policy can be reused for SOA. It can also be deployed as a proxy to Java CAPS to ensure centralized policy enforcement for all communication entering or leaving a Java CAPS-enabled SOA environment.

The hardware version of the Layer 7 XML Networking Gateway offers hardware acceleration of XML parsing, validation and transformation for fast message processing of identity and content. It also comes with optional FIPS-compliant crypto acceleration for accelerated SSL, WS-Security and signing operations for XML or SAML.

For identity-centric privacy and integrity operation, the SecureSpan XML Networking Gateway provides administrators an array of easy-to-configure options for defining channel, message and element encryption/decryption and signing/signature validation policy. The XML Networking Gateway can also be configured to delegate authentication and authorization decisions to Sun Java Access manager. All operations are available for both inbound and outbound traffic. Public Key Interface (PKI) for the cryptographic operations can be implemented using the SecureSpan XML Networking Gateway's on-board Certificate Authority or a third-party certificate authority. For implementations using the hardware XML Networking Gateway with on-board crypto acceleration, a centralized hardware HSM key store is also included.

In addition to securing identity-based SOA operations, the SecureSpan XML Networking Gateway offers extensive threat, WS\* and service assurance features including:

- Configurable protections against service communication, API and application attacks, including integration with leading virus scanners
- Extensive support for key Web service security standards, including WS-Security, WS-SecureConversation, WS-Trust, WS-SecurityPolicy, WS-Policy, WS-I and SAML
- Broad content filtering and processing options for XML, SOAP, RSS and REST-based messaging
- Advanced service virtualization, QoS and SLA operations for assuring maximal service availability and responsiveness

### SOA single sign-on and federation

Unlike the Web, SOA has no client-side browser analogue to cache session or federation tokens generated by products like Java System Access Manager or Java System Federation Manager, complicating Single Sign-on (SSO) and identity

federation. Layer 7's SecureSpan XML VPN client is a software or hardware proxy that can be deployed on or in front of SOA clients to request, cache and embed tokens into a client-side SOAP call without any client-side coding. The SecureSpan XML VPN client also ensures that all outbound SOAP messages automatically conform to policy settings defined on a Web service, as well as the latest WS\* and WS-I standards. The SecureSpan XML VPN client automatically embeds sequence numbers and optionally time stamps to ensure any message transmitted from the client to a Web service is non-reputable.

For B2B and Extranet applications, the XML VPN client can also be deployed alongside Java CAPS to deliver simple partner on-boarding. Services exposed through Java CAPS can be extended to external business units and companies without complex coding and testing.

### Security as SOA governance foundation

All production Web services require policies to define security expectations and preferences. These security settings can be hard-coded into a service's business logic, but at a significant cost in programming, testing, change management and flexibility. For services provisioned and composed using Java CAPS, the Layer 7 XML Networking Gateway offers a flexible, scalable and consistent way to implement, change and audit security policies without coding.

However, the Layer 7 XML Networking Gateway can also be used to define and enforce any WS-Policy-compliant SOA governance policy including preferences for routing, SLA and QoS. The XML Networking Gateway can therefore be used as a general platform for centrally configuring and enforcing SOA policies.

### For a free trial of the Layer 7 XML Networking Gateway

<http://www.layer7tech.com/products/page.html?id=82>

For more information visit [sun.com/layer7](http://sun.com/layer7)  
<http://www.layer7tech.com>, or contact your local Sun representative.

1-800-681-9377  
[sales@layer7tech.com](mailto:sales@layer7tech.com)

### Sun and Layer 7

Layer 7 Technologies markets a family of XML appliances (delivered on Sun x64 systems) and software to secure, simplify and scale Web services and SOA. Modern service-oriented application integration models and Web-oriented application delivery models depend on effectively addressing the performance, security, complexity, reliability and availability issues inherent in sharing Web services with other applications. Layer 7 Technologies therefore aims to provide the essential application-oriented security and networking infrastructure to enable Service-oriented and Web-oriented architectures (i.e. SOA and Web 2.0) that are central to the next wave of Internet and software innovation.

Layer 7 Technologies interacts with Sun Java Composite Application Platform Suite and Java Identity Management Suite to add a layer of SOA governance controls without compromising performance or flexibility.