



SecureSpan Gateway

UNLOCK YOUR SERVICES TO THE OUTSIDE WORLD—LOCK OUT INTRUSIONS

Don't let security concerns keep you from connecting with partners and customers. Open up your services to them with SecureSpan Gateway. You'll achieve high service performance while protecting your transactions—and your business.

SecureSpan Gateway is an XML appliance that provides advanced security and accelerates securing Web service communication at the edge of the network.

Simply deploy SecureSpan Gateway at the network's edge in front of external service consumers to enhance your SOA security, performance and reliability in a low-cost, non-invasive way.

You also can apply advanced security using software or hardware modules to regulate B2B transactions. Plus, you can ensure applications are protected against malicious attacks that might compromise or bring down your services. What's more, you can accelerate XML processing using SecureSpan Gateway's hardware-based solution.

Take a closer look at the key capabilities of SecureSpan Gateway.

KEY BENEFITS

- Connect with partners and customers while protecting your applications from malicious attacks
- Enhance your SOA security, performance and reliability in a low-cost, non-invasive way
- Choose from a variety of deployment options to meet your business and budget requirements—hardware, software or virtual appliance
- Count on out-of-the-box integration with CentraSite
- Gain centralized visibility into the health of your SOA landscape

Advanced XML Security—Build a first line of defense

XML interfaces for SOA, cloud computing and Web 2.0 provide a versatile method for exposing applications and their data directly to other applications in a standards-based way. This simplifies interoperability across departmental, organizational and cloud boundaries. However, exposing functionality and information to applications in external trust and security domains opens those systems to potential threats. That's why you need SecureSpan Gateway for a first line of defense.

Identity-based access

SecureSpan Gateway can be integrated with a number of 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. Additionally, SecureSpan Gateway can enforce fine-grained entitlement decisions authored in XACML.

Cross-domain/B2B security

SecureSpan Gateway supports credential chaining, credential remapping and federated identity, facilitating information sharing between organizations. An integrated STS/SAML issuer provides comprehensive support for SAML 1.1/2.0 authentication, authorization and attribute-based policies, as well as support for WS-Trust, WS-Federation and SAML-P protocols. Additionally, an integrated PKI CA/RA allows for automated deployment and management of client-side certificates.

WS* and WS-I standards support

SecureSpan Gateway provides support for all major WS* and WS-I security protocols, including WS-Security, WS-SecureConversation, WS-SecurityPolicy, WS-Trust, WS-Federation, WS-Secure Exchange, WS-Policy and WS-I Basic Security Profile.

Cryptography

You can purchase SecureSpan Gateway with an optional onboard Hardware Security Module (HSM), as well as support for external HSMs, such as Safenet. Federal Information Processing Standards (FIPS) support is provided in both hardware (FIPS 140-2 Level 3) and software.

SOAP, REST and POX security

You can use SecureSpan Gateway to provide secure access to services exposed as SOAP, REST or POX service.

Custom policy assertions

With the latest release of SecureSpan XML Networking Gateway, you can use the Custom Policy Assertion SDK to create new assertions that address unique requirements, such as: proprietary message processing; pattern recognition and filtering and; interfacing to third-party infrastructure—all without requiring an application server to run the custom code.

Sample custom assertions are provided for integration to a range of leading identity management products from Sun, IBM, CA, Oracle and others.

Consumer-provider security handshake

With the SecureSpan XML VPN Client that works in conjunction with the XML Firewall or XML Networking Gateway, you can effectively separate authentication and authorization tasks across trust boundaries.

XVC helps streamline consumer and provider interactions by automatically negotiating the "handshake" between them, abstracting out security and other infrastructure requirements. This ensures business continuity even in the face of changing industry regulations and corporate requirements.

Threat Protection—Shield your business from attacks

Web services face the threat of attack due to the unique nature of how XML is structured, processed and composed. With Web services, applications are exposed directly to the outside world through open, XML-based APIs, making them directly susceptible to content, attachment or execution attacks carried inside an XML message. And because Web services are used for integration, they are at risk to transactional threats, such as message interception, hijacking or spoofing.

SecureSpan Gateway addresses all these XML and Web services vulnerabilities, providing application-level threat detection, prevention and remediation.

XML content filtering

SecureSpan Gateway supports XML, SOAP, POX, AJAX, REST and other XML-based services, offering configurable validation and filtering of HTTP headers, parameters and form data. It can also detect classified words, "dirty" words and arbitrary signatures, and then scrub, reject or revise the message on both inbound and outbound information flows, preventing privileged information leakage.

Attack and intrusion prevention

Gain extensive protection against XML-based threats, including XML parser attacks, XDoS and OS attacks, and SQL and malicious scripting language injection attacks. SecureSpan Gateway can also be deployed to protect against XML content tampering and viruses in SOAP attachments. Communication between SecureSpan Gateway systems in a cluster ensures cluster-wide threat protection against man-in-the-middle attacks.

XML Acceleration—Process XML messages faster

Processing XML is computationally expensive. Performing operations such as routing, transformation and security on an application server typically results in unacceptable performance slowdowns and an ongoing cycle of costly hardware upgrades. SecureSpan Gateway is purposely built for wire-speed processing of XML messages, enhancing application server and network performance by dealing with XML messages at the network's edge.

Accelerated message processing

Expect high-speed message transformations based on internal or external XSLT and high-speed message validation against predefined external schema. Additionally, SecureSpan Gateway accelerates message searching, element detection and content comparisons.

Hardware-based acceleration

While SecureSpan Gateway's software-based acceleration on a 64-bit multiprocessor/multi-core platform provides exceptional performance, an ASIC-based hardware accelerator can be optionally installed if you need maximum message throughput and minimal processing latency.

SSL offload

SecureSpan Gateway provides SSL offload, termination and origination, removing the encryption/decryption processing burden from Web servers for SSL traffic.

CentraSite and webMethods Insight Integration—Gain a single source of the truth

For structuring your SOA assets, SecureSpan Gateway provides an out-of-box integration with CentraSite. With this integration, you can use CentraSite as the single source of truth for all the assets managed by SecureSpan Gateway and also leverage the powerful lifecycle management and governance framework.

With the built-in webMethods Insight agent for SecureSpan Gateway, you can now provide deep visibility for services hosted on the appliance.

Integration and governance with CentraSite

With out-of-the-box integration with CentraSite, you can look up services available in CentraSite and author proxy services in SecureSpan based on the native service definitions from CentraSite. SecureSpan can also automatically get the latest, greatest and approved versions of WSDL, XML Schema and XSLT from CentraSite using subscription-based updates. In addition, SecureSpan can also publish service metadata, relationships and metrics back to CentraSite.

Visibility using webMethods Insight

SecureSpan Gateway now comes up with a built-in webMethods Insight agent. This agent can be configured to work with the webMethods Insight server. With this new capability, you can get deep visibility into services hosted on the SecureSpan Gateway.

Simplified Administration & Flexible Deployment—Increase your visibility

For simplified administration of SecureSpan Gateway deployments, you can use the Enterprise Service Manager add-on. This add-on is designed to give SOA administrators and network operators centralized visibility into the health of their SOA landscape, even when their SOA is distributed across geographies, partners and the cloud.

The deployment of SecureSpan Gateway can be performed in multiple forms: hardware appliance, software appliance and software depending your specific requirements and constraints.

Centralized management

With the Enterprise Service Manager add-on, you can manage the health and performance of all SecureSpan clusters as well as set

thresholds that spawn alerts based on performance and exceptions. Administrators can literally point and click to move service policies across development, test and production environments, among geographical locations, and between the enterprise and the cloud, automatically resolving network and identity conflicts.

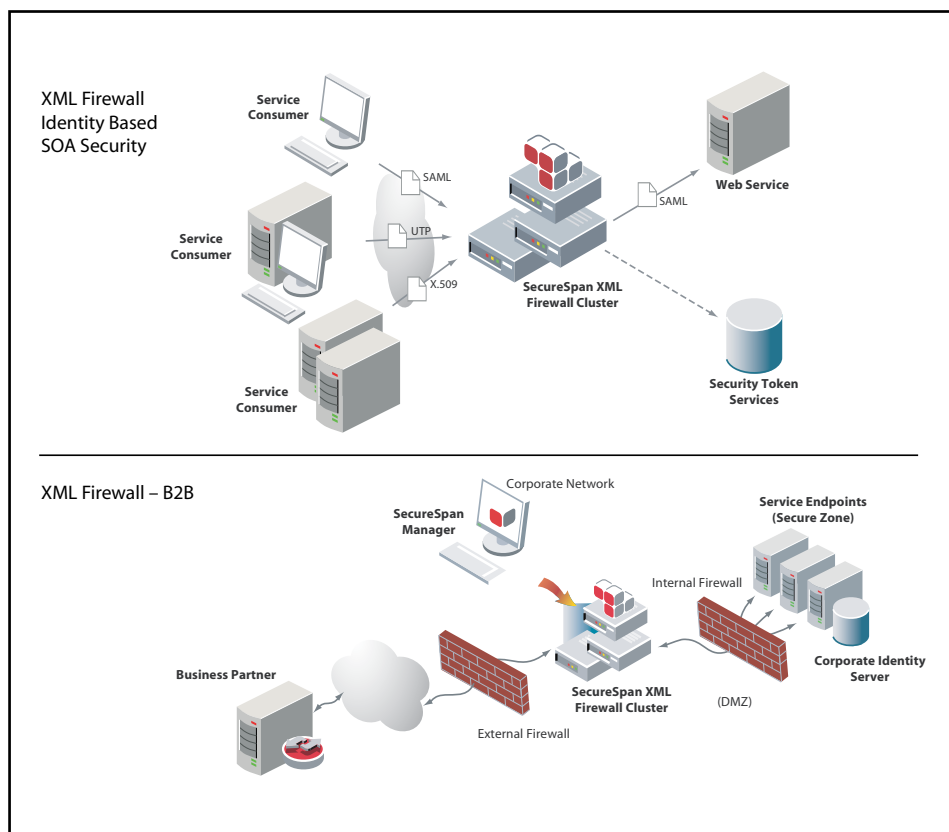
Remote management

With SecureSpan Gateway products, you can perform many administrative tasks remotely. Using remote patching, you can selectively update any software installed on gateways, including system files and operating system. The Remote Management API's allow you to hook your existing third-party management tools into the SecureSpan Gateway (SSG). You can also do back-up and restore operations remotely. In addition, you can remotely access logs and audit files on any SSG/SSG cluster to identify and trace issues.

Multiple deployment options

Use the hardware appliance option if you're concerned about DMZ/perimeter deployments and have production environments with high-performance and scalability requirements. If you have less stringent requirements, you can configure SecureSpan Gateway as a software appliance. Choose the software option if you are concerned about costs and are mainly looking to deploy SecureSpan Gateway in development and test environments.

Example Deployment Scenarios:



Take the next step to get there - faster.

To find the Software AG office nearest you, please visit www.SoftwareAG.com

ABOUT SOFTWARE AG

Software AG is the global leader in Business Process Excellence. Our 40 years of innovation include the invention of the first high-performance transactional database, Adabas; the first business process analysis platform, ARIS; and the first B2B server and SOA-based integration platform, webMethods. We are unique in offering the world's only end-to-end—and easiest to use—business process management (BPM) solutions, with the lowest Total-Cost-of-Ownership.

Our industry-leading brands, ARIS, webMethods, Adabas, Natural and IDS Scheer Consulting, represent a unique portfolio for: process strategy, design, integration and control; SOA-based integration and data management; process-driven SAP implementation; and strategic process consulting and services. Our comprehensive software and services solutions allow companies to continuously achieve their business results faster.

Software AG – Get There Faster

© 2010 Software AG. All rights reserved. Software AG and all Software AG products are either trademarks or registered trademarks of Software AG. Other product and company names mentioned herein may be the trademarks of their respective owners.