



a PrismTech Product Line

Xtradyne Web Services DBC

Comprehensive XML Web Services Security



The Xtradyne Web Services DBC is the Web Services security product in the Xtradyne Domain Boundary Controller (DBC) suite, one of the most performant, scalable, and vendor-neutral security enforcement suites on the market. As an application-layer security gateway, the Web Services DBC enables secure Web Services applications and protects resources in mid-tier and back-end enterprise systems.

The Web Services DBC performs message analysis, authentication, authorization, audit, and content security services to protect against illegal access and potentially malicious XML/SOAP messages. It provides end-to-end security by inserting standards based WS-Security/SAML credentials into the SOAP packet. As a pluggable SOAP security proxy, it is a robust and cost-efficient firewall solution for Web Services. The Web Services DBC constitutes a very strong line of defense ensuring access to the back-end is controlled, and obviates the need to open up internal packet filters in cases where servers are installed outside the corporate network. The Web Services DBC is an easy-to-use, out-of-the box software package that can be transparently integrated into the existing network infrastructure.

WEB SERVICES SECURITY

Essential for production-level Web Services

Web Services are a standards-based model for cost-efficient enterprise application integration (EAI) and business-to-business (B2B) environments. Web Service resources can be accessed using SOAP messages that travel in standard web protocols, primarily HTTP. The main difference between access to Web Services and traditional client/server scenarios is that participants in Web Services interactions are generally less tightly integrated, and that interactions may freely cross organizational boundaries. Messages may travel over any number of connections and potentially traverse many intermediates before reaching their destination.

To support this decoupled interaction, security can no longer be provided in a connection-oriented manner but rather on a per-message basis. Consequently, messages must be self-contained with respect to security information and carry all the necessary information and credentials (e.g. authentication proof) with them.

KEY BENEFITS

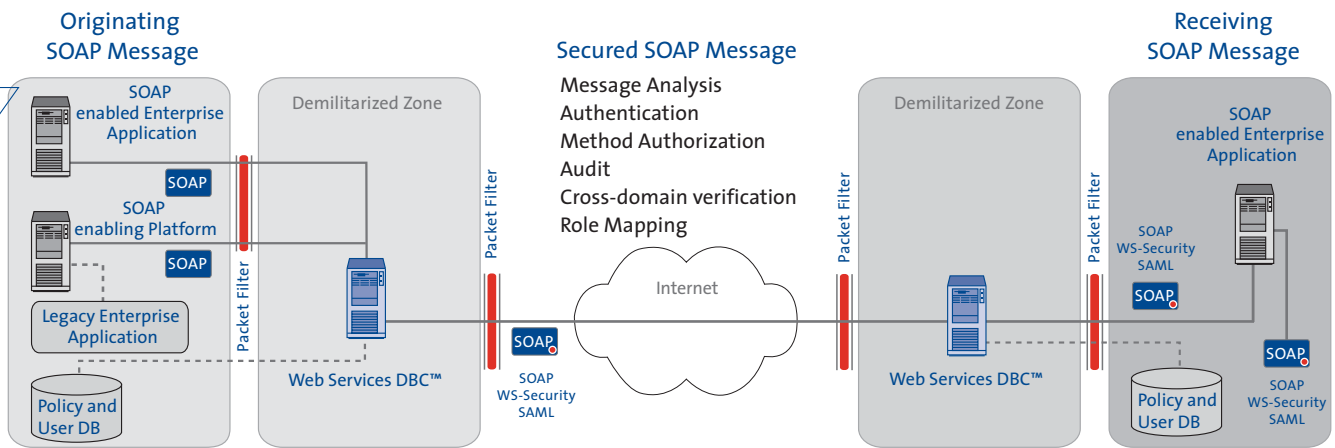
- › Transparent deployment without modifying any application code
- › Convenient service exposure using WSDL
- › Fine-grained and scalable security across all tiers
- › Full AAAA (authentication, authorization, audit, administration) services
- › Unified, policy-based security management across Web Services platforms
- › Interoperability through standards-based WS-Security, and SAML credentials
- › Low overhead through high-performance messaging layer



PrismTech Limited
Xtradyne Security Technologies

PrismTech House
5th Avenue Business Park
Team Valley, Gateshead
Tyne & Wear NE 11ONG
UK

Tel +44-(0)191-49799 00
Fax +44-(0)191-49799 01
Email: info@xtradyne.com
Web: www.xtradyne.com



COMPREHENSIVE WEB SERVICES SECURITY

FEATURE	FUNCTION
MESSAGE VALIDATION	XML messages can be syntactically ill-formed and potentially even damaging to service implementations. Web Services DBC validates incoming messages and analyzes their structure against the XML Schema and contents against predefined rules.
MESSAGE INTEGRITY	Message may get modified in transit. Web Services DBC digitally signs the message and header, tying together the message and header, making undetected modification impossible. This signature can be used for verification when the SOAP packet passes through the enterprise application infrastructure.
MESSAGE ORIGIN	Messages may be sent from non-trusted sources. Web Services DBC authenticates the origin and inserts the assertion into security token that can be used for proof of origin.
AUTHENTICATION	Access to Web Services may be restricted to authenticated clients only. The Web Services DBC supports client authentication – with the following mechanisms: <ul style="list-style-type: none"> › Public key certificate-based client authentication using SSL certificates › HTTP basic authentication › Anonymous clients – this corresponds to public access to a service.
AUTHORIZATION	Clients may only access authorized services. The Web Services DBC permits service accesses that comply with an access control policy based on: <ul style="list-style-type: none"> › Privileges of the message sender › Target resource being requested, i.e. URL of the Web Service the SOAP request is sent to › Action to be performed on the requested resource, e.g., method name in the SOAP request
AUDITING	Audit logging of pertinent events to determine resource access and tracing. The Web Services DBC provides auditing facilities, event notifications, and audit trails. The extensive list of logged events include: Connection establishment, authentication results, authorization results, policy changes, startups / shutdowns, etc.
INTEROPERABILITY	Interoperability by adherence to Standards. The Web Services DBC supports the emerging standards such as WS-Security, WSDL, XML Digital Signature, and SAML (Security Assertion Markup Language). The Web Services DBC may be deployed transparently to protect all applications and platforms that support SOAP 1.1.
SUPPORTED PLATFORMS	› Solaris 8 and 9 (for Windows, please see the <i>Quadrasis / Xtradyne SOAP Content Inspector™</i>) › Linux

DEPLOYMENT SCENARIOS

INTRANET

- Use Web Services internally for
- › Cross department access to services
 - › Application Integration

Web Services DBC

- › Secures access to Web Services resources from other departments
- › Secure inter-application communication

FEDERATED EXTRANET

- Use Web Services to integrate applications and services with
- › Trading Partners
 - › Branch Offices

Web Services DBC

- › Federated trust and role mapping eliminates duplication of user and policy information

INTERNET / EXTRANET

- Deploy new Web Services
- › Application services accessible to a broad external clientele

Web Services DBC

- › Allows broad access to services
- › Maintains authentication and authorization information within enterprise