

# Intel® Expressway Service Gateway

"It's not enough to offer an API; it needs to be reliable, scalable, and secure. Many enterprises don't really know how to offer APIs with the same security and service level as their enterprise applications."

- John Musser, Founder, ProgrammableWeb

Intel® Expressway Service Gateway (Intel® ESG) is a software-appliance designed to securely expose or consume application services/APIs on-premise or in the cloud. It delivers cloud service brokerage capabilities including: integration, routing, data protection, middleware for legacy to mobile service enablement, and AAA security. Intel® ESG is deployed as a low impact proxy at the network or cloud edge.

- **API Security:** Regain control with a centralized policy enforcement point to authenticate, authorize, and govern service interactions with customers, partners, employees, and cloud providers as they consume or deploy applications exposed over APIs.
- **API Abstraction:** Innovate faster, gain a competitive edge, and securely expose applications on-premise or in the cloud, regardless of the abstraction pattern (SOA, WOA), delivery method (App Store, Cloud) or protocol (REST, SOAP).
- **Cloud Service Brokerage (CSB):** Enable IT to integrate, govern, & secure services from 1-n external cloud providers for simplified service consumption by internal departments & developers. Aggregate & expose value added composite applications & data as a 3rd party intermediary to partners and customers.
- **Flexibility without Compromise:** Simplify infrastructure by deploying an easily upgradeable soft-appliance on standard Intel® Multi-Core servers. Best-in-class performance reduces API and integration performance bottlenecks with no compromise on extensibility or virtualization.



## The API Economy

Cloud computing, Social media and Mobile apps offer new, low cost, channels for enterprises to interact with customers and partners on a personalized basis. This mix of content, data and functionality is exposed from internal applications as APIs. This trend is serving as a catalyst for an organization to put in place a solution that securely connects applications via APIs across internal and external domains while providing the necessary security and monitoring.

Intel® ESG is a highly scalable software appliance that securely and reliably connects on-premise applications to external cloud providers, external business partners or employees regardless of the protocol or deployment pattern. Intel® ESG combines the functions of a service bus, security gateway and XML acceleration engine and serves as the ultimate control point for application API interactions based on common API patterns such as SOAP or REST services.

## API Management for Mobile & Web

Emerging web and mobile applications favor light-weight REST APIs with JSON that are highly compatible with bandwidth and CPU constrained mobile platforms. Intel® ESG provides bidirectional transformation between SOAP, XML, JSON and proprietary interfaces to REST style APIs.

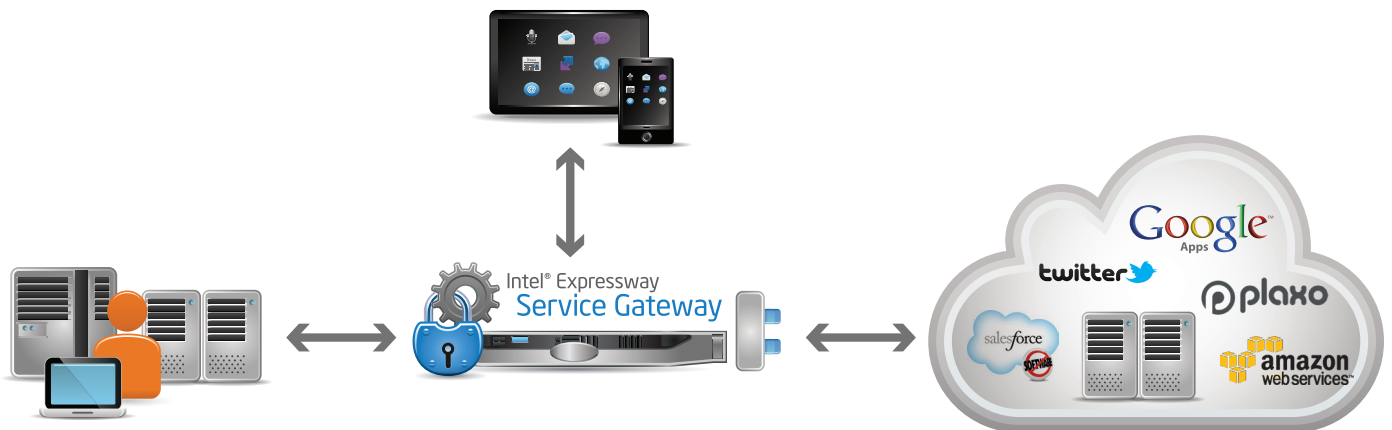
## The API Security Challenge

The biggest challenge for service-based, large scale applications that span multiple independent domains is application security, policy, and runtime control. Moreover, the service-enablement of existing applications that necessitates a universal SOAP or REST tunnel for API calls or data access ultimately brings new security requirements such as SOAP or REST message level security, service virtualization, delegated AAA functions, data leak prevention, malware and threat prevention. Additionally, API exposure and consumption also increases the need for integrated authentication and identity

management as well as perimeter threat defense - which is important as ever to protect applications from new breeds of content attacks.

With the proliferation of third party cloud based APIs, new challenges have been created around authentication and authorization, especially for enterprises wishing to utilize their existing identity management infrastructure to securely access cloud APIs and resources.

Intel® ESG serves as a policy enforcement point to authenticate API clients and end users against existing enterprise Identity & Access Management systems. It supports OAuth 2.0 that is becoming the standard authentication and authorization method for RESTful web services and APIs. It provides these features in a software appliance form- factor instead of hard to manage, proprietary XML hardware. Intel® ESG runs on secure, open operating systems, avoiding the "security by obscurity" black box, lack of visibility that is common with "hardened" hardware appliances.



## The API Broker Challenge

It's no mystery that the modern datacenter is an amalgamation of heterogeneous software and systems, brimming with complexity. Intel® ESG enables IT to act as a broker, integrating APIs and services from cloud providers with on-premise applications to deliver business functionality. As such, it reduces the management, development and capital costs of large distributed applications that use any type of SOAP, REST or custom service APIs. Intel® ESG runs on industry standard operating systems like Linux and Windows and can secure, transform, route and mediate services offered by any vendor, whether they operate in a silo, are legacy, or employ standards-based communication mechanisms. Intel® ESG uses a codeless Eclipse based designer that supports simple or complex mediation applications.

As enterprises extend their applications to the cloud, functionality around API throttling and governance has become increasingly important. Intel® ESG supports quality of service enforcement and API mediation functionality.

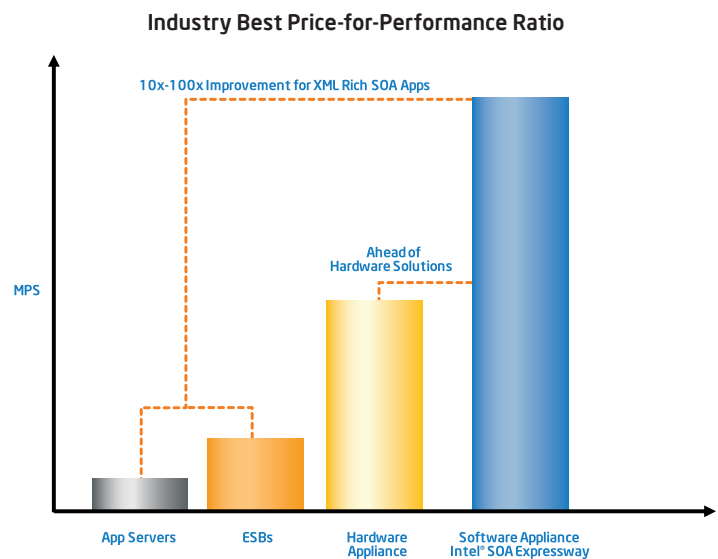
Enterprises are using Intel® ESG as a security layer that abstracts APIs to external services and provides a central point of control for decoupling security policy from internal applications.

Intel® ESG can be managed through a Web Interface, complete with alarms, alerts, a dashboard and self-healing, self-correcting capabilities. It can also integrate with management consoles that support SNMP and JMX. Intel® ESG also supports unique "power deploy" functionality that helps enable policy deployments across different physical networks. Finally, because Intel Expressway Service Gateway is a software solution, it can be packaged into a virtual appliance and run on popular platforms such as VMWare or Amazon EC2 and be included in large, multi-premise composite applications that span enterprise boundaries and cloud providers.

## A Highly Performant API

As applications grow larger there tends to be a mix of legacy (binary), JSON (JavaScript Object Notation), plain-old-XML (POX), and web services (SOAP) data in order to support changing business requirements. With distributed applications, performance is critical. One must not only optimize "point" API operations such as authentication, transformation and validation, but also provide an optimized service mediation engine that provides orchestration between services that rely on these functions.

Intel® ESG provides a single runtime instance that offers XML and service mediation acceleration that scales with any Intel® Xeon Multi-Core server, regularly beating custom hardware appliances by a factor of 4 to 1 or greater. Intel Expressway Service Gateway instantly brings the power of Intel Multi-Core and Moore's Law to business applications without requiring any special programming or any proprietary hardware.



# Feature and Functionality Details

Category	Description
XML Firewall Threat Prevention	<ul style="list-style-type: none"><li>XML Limit Checking, SQL Injection, DTD Checking, XPath Injection, Forbidden RegEx Scan, Malformed XML Attack, XML Bomb Attack, XSS Protection, Schema Poisoning Attack</li><li>Adaptive Denial of Service Protection and Throttling</li><li>Anti-virus and malware protection using McAfee Web Gateway and ICAP</li><li>Enhanced content attack prevention for REST services (query parameters, headers, request methods)</li></ul>
Authentication and Authorization	<ul style="list-style-type: none"><li>X.509 certificate, CRL, username/ password, LDAP or Microsoft* Active Directory, Kerberos, SAML 1.0/1.1/2.0, Web SSO cookie and STS credential mapping, Amazon* Cloud API, SAML for REST, OAuth 2.0</li><li>Integrates with: CA* SiteMinder, Oracle* Internet Directory, Oracle* Access Manager, IBM* Tivoli Access Manager</li><li>Integrates with XACML policy decision points including Axiomatics* Policy Server and Oracle* Entitlements Server</li></ul>
Data Security	<ul style="list-style-type: none"><li>OASIS WS-Security 1.0/1.1, WS-Trust, W3C XML encryption and XML signatures, WS-I BSP 1.0/1.1, SOAP with Attachments</li><li>Data validation, schema validation, WSDL validation, SOAP filtering</li><li>REST security policy and action support the creation, verification and attachment of SAML assertions to REST messages</li><li>Data loss protection for API responses using McAfee DLP Prevent</li></ul>
XML Standards and Data Formats	<ul style="list-style-type: none"><li>XML, XPath and XSLT (1.0, 2.0), XML Schema</li><li>Embedded XSL mapper for easy creation of style sheets</li><li>Secure Unstructured Data Streams – Apply security policies to any data format using the embedded Informatica DT (Data Transformation) engine</li></ul>
Cloud and API Management	<ul style="list-style-type: none"><li>Declarative REST policy improves the usability for REST service invocations and supports multiple built-in content types such as XML, JSON, URL encoded, string and binary</li><li>Built-in support for the Salesforce.com REST API</li><li>Enforce quality of service and through rate limiting and throttling controls</li><li>Limit API access based on schedule, class of service, identity, or any client context</li><li>API Response Caching</li></ul>
Transport Layer Security	<ul style="list-style-type: none"><li>Support for multiple SSL identities, mutual auth, SSL v3 and TLS v1</li><li>SSL Support for: HTTP, JMS, FTP, MLLP, Raw TCP, JDBC</li><li>Customizable protocol support</li><li>XSL Mapper simplifies the use of XSLT style sheets with a visual tool</li></ul>
Cryptographic Support	<ul style="list-style-type: none"><li>Supports DES, 3DES, AES, RSA v1.5, RSA-OAEP, SHA-1 and SHA-256</li><li>Supports hardware cryptographic acceleration and FIPS 140-2 Level 3 network-based Hardware Security Module</li></ul>
Service Mediation	<ul style="list-style-type: none"><li>Secure SOAP, REST, JSON, or custom service mediation within the datacenter or across the Internet</li><li>Supports Open Group's X/Open XA transaction standard for long running transactions</li><li>Proven integration with all major ISV middleware solutions including native support for IBM MQ</li></ul>
Service Governance	<ul style="list-style-type: none"><li>UDDI v2/v3 integration for API governance and retrieval</li><li>Fine-grain service and policy monitoring</li><li>Zero downtime dynamic policy updates for routing, attack signatures, validation, and transformation</li><li>Integrates with business service repositories from SoftwareAG* CentraSite, Oracle, SAP</li></ul>
Supported Hardware	<ul style="list-style-type: none"><li>Any Intel* Xeon* Multi-Core server with 4GB RAM (16GB Recommended)</li><li>Available in a hardened, tamper resistant Hardware Appliance, Dell Intel* Xeon 5600 series</li></ul>
Management and Monitoring	<ul style="list-style-type: none"><li>Cluster support allows a group of appliances to be managed &amp; monitored simultaneously</li><li>Eclipse-based Intel service and policy designer with pre-built templates</li><li>Management through command line, SNMP, and integrates with HP* OpenView, Microsoft* MOM</li><li>Automated Policy Migration– supports policy deployment and dependency resolution across development, test and production network environments</li><li>Integration with Splunk for cross domain system monitoring</li><li>Log Redaction for log data confidentiality and privacy</li><li>Role-based delegation and fine-grained control of configuration</li><li>Integration with McAfee ePO for monitoring and security event visibility</li></ul>
Operating Systems	<ul style="list-style-type: none"><li>Red Hat* AS4/A5 (32 or 64-bit), SUSE Linux Enterprise 10 (32 or 64-bit), Oracle* Enterprise Linux, Solaris 10, Microsoft* Windows 2003 Server (32 or 64-bit), VMWare ESX, Windows 2008 R2</li></ul>
Performance Features	<ul style="list-style-type: none"><li>Wire speed XML processing engine optimized for Intel* Multi-Core and SSE4.2 hardware instruction set</li><li>Low sub-millisecond latency, large XML processing (&gt;1GB)</li><li>High concurrency I/O processing supports thousands of connections with low latency for SSL and non-SSL traffic</li><li>Embedded front-end load balancer</li><li>Sophisticated back-end load balancing with auto-retry capability</li></ul>

## More Information

Website: [cloudsecurity.intel.com](http://cloudsecurity.intel.com)

Americas: 1-855-229-5580

E-mail: [intelsoainfo@intel.com](mailto:intelsoainfo@intel.com)

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.


Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at [www.intel.com](http://www.intel.com).

Copyright © 2012 Intel Corporation. All rights reserved. Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

\*Other names and brands may be claimed as the property of others.

Printed in USA

 Please Recycle

323892-003US

