

# McAfee Services Gateway

Secure, control, and accelerate

McAfee® Services Gateway simplifies and secures application architecture on-premises or in the cloud. It expedites deployments by addressing common security and performance challenges and accelerates, secures, integrates, and routes XML, web services, and legacy data in a single, easy-to-manage solution.

## Key Advantages

### Implement run-time governance

- Enforce service policies
- Address compliance

### Add security

- Full security proxy
- XML firewall
- Authentication, authorization, and accounting (AAA) capabilities

### Increase performance

- Wire-speed XML parsing
- Designed to optimize Intel multicore processors

### Simplify integration

- Sophisticated service mediation
- Supports non-XML data

## The Services Gateway

As applications are exposed externally, a services gateway is used to at the network edge to abstract, secure, and simplify services delivery. As a best practice for delivering application-to-application, service-oriented architecture (SOA), or representational state transfer (REST)-based service interaction models, McAfee Services Gateway provides a unique set of features tailor-made to integrate, mediate, secure, and scale services at the ever-changing application perimeter.

### Secure the edge

The static network perimeter is gone. Regain control with a centralized policy enforcement point to authenticate, authorize, and govern service interactions with customers, partners, employees, and cloud providers (IaaS/PaaS) as they consume or deploy applications.

### Build dynamic applications

Innovate faster, gain a competitive edge, and securely expose mass customizable applications on-premises or in the cloud, regardless of the abstraction pattern (SOA, WOA), delivery method (App Store, Cloud) or protocol (REST, SOAP).

### Get more. Go neutral.

Break free of purpose-built inflexible appliances tied to expensive vendor suites. When it comes to lower cost, multicore optimized performance, ready middleware interoperability, and vendor viability, protect your investment with McAfee.

## Flexibility without compromise

Simplify infrastructure by deploying on standard Intel Multi-Core servers. Address common SOA bottlenecks with specialized soft appliances with no compromise on extensibility or virtualization.

## Protecting the Application Edge

The transition to cloud environments presents a catalyst for the enterprise to put in place a solution that works across internal and external domains. What is needed is a true cross-domain services gateway that provides application security across enterprise boundaries, no matter the protocol or deployment pattern. The Services Gateway is the ultimate control point for application interactions, connecting on-premises applications to external cloud providers, external business partners, or employees.

McAfee Services Gateway is a highly scalable software product that provides common functions of a service bus, security gateway, and XML acceleration engine into a single product that scales on next-generation Intel Multi-Core servers for the modern virtualized data center. McAfee Services Gateway acts as the secure enterprise glue for large, complex, distributed applications that span multiple physical data center environments and multiple vendors based on common SOAP or REST service patterns.

### The SOA security challenge

The biggest challenge for service-based, large-scale applications that span data centers is application security, policy, and run-time control. Service-enablement of existing applications provides a universal SOAP or REST tunnel for function calls or data access which brings new security requirements such as SOAP or REST message-level security, service virtualization, delegated AAA functions, and threat prevention. Expansion towards cloud service provider API usage also increases the need for integrated authentication and identity management as well as threat defense. Perimeter defense or XML firewall functionality is as important as ever to protect applications from new breeds of content attacks. Furthermore, the proliferation of third-party cloud-based APIs creates new challenges around authentication and authorization, especially for enterprises that wish to use their existing identity management infrastructure to securely access cloud APIs and resources.

McAfee Service Gateway provides unmatched support for these features in a form factor that avoids the use of custom, hard-to-manage, proprietary XML hardware. It runs on secure, open operating systems, and avoids the “security by obscurity” problem with “hardened” hardware appliances.

### The governance challenge

It's no mystery that the modern data center is an amalgamation of heterogeneous software and systems, brimming with complexity. McAfee Services Gateway reduces the management, development, and capital costs of large distributed applications that use any type of SOAP, REST, or custom service. It runs on industry-standard operating systems, like Linux and Microsoft Windows, and can secure, transform, route, and mediate among services offered by any vendor, whether they use a silo-, legacy-, or standards-based communication mechanism—or offer application functionality through an API. Furthermore, it 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. McAfee Expressway Services Gateway supports quality of service enforcement and API mediation functionality. This allows the enterprise to use the gateway as a security layer that abstracts APIs to external services and provides a central point of control for decoupling security policy from internal applications.

The core of McAfee Services Gateway run-time is the software appliance form factor. This means that McAfee Services Gateway can be managed through a web interface, complete with alarms, alerts, a dashboard, and self-healing, self-correcting capabilities. McAfee Services Gateway can also integrate with management consoles that support SNMP and JMX.

McAfee Services Gateway also supports a unique “power deploy” functionality that helps enable policy deployments across different physical networks. Finally, because McAfee Services Gateway is a software solution, it can be packaged into a virtual appliance and can run on popular platforms such as VMware or Amazon EC2.

### The performance challenge

As applications grow larger, they tend to mix legacy (binary), plain-old-XML (POX), and web services (SOAP) data to support changing business requirements. Accelerating such a large distributed application requires optimizing not only “point” XML operations, such as transformation or validation, but also providing an optimized service mediation engine to orchestrate services that rely on these functions. McAfee Services Gateway provides a single run-time 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 four to one or greater. McAfee Services Gateway instantly brings the power of Intel Xeon Multi-Core and Moore's Law to XML-rich business applications without requiring any special programming or any custom, proprietary hardware.

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 protection using 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</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>Supports customizable data security</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 Data Transformation (DT) engine</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> </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 data center 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</li> </ul>
Service Governance	<ul style="list-style-type: none"> <li>Message throttling and ordering</li> <li>High performance run-time policy enforcement for security, SLA, mediation, and transformation</li> <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 4 GB RAM (8 GB recommended)</li> </ul>
Management and Monitoring	<ul style="list-style-type: none"> <li>Cluster support allows a group of appliances to be managed and monitored simultaneously</li> <li>Eclipse-based Intel service and policy designer with pre-built templates</li> <li>Management through command line and 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> </ul>

(continued)

---

<b>Operating Systems</b>	<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</li></ul>
<b>Performance Features</b>	<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</li><li>• High concurrency I/O processing supports thousands of connections with low latency for SSL and non-SSL traffic</li><li>• Large XML processing (&gt;1 GB)</li><li>• Embedded front-end load balancer</li><li>• Sophisticated back-end load balancing with auto-retry capability</li></ul>

---

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

For information or to start an evaluation of McAfee Services Gateway, contact your McAfee representative, or visit [www.mcafee.com/cloudsecurity](http://www.mcafee.com/cloudsecurity).

