

Key Criteria for Selecting a SOA Gateway



Layer 7 Technologies

RFI/RFP

Sample RFI/RFP Criteria – Usage

The following content is intended for reference purposes only. It represents example criteria commonly asked in a SOA Gateway or SOA Appliance RFI/RFP. It is not intended to be an exhaustive list, nor does it reflect all possible enterprise architectures. You may incorporate any and all appropriate entries listed below within your RFI/RFP in order to help you qualify vendors.

Form Factors – choose the right form factor to match your budget & requirements

- Hardware appliance
- Virtual Appliance
- Software
- Amazon Machine Image
- Client-side library/executable

Clustering – integrated clustering provides reliability, scalability and a single point of administration

- Cluster-wide threat protection (i.e., for replay attacks)
- Integrated clustering for automated replication of information
- Cluster-wide rate limiting (for enforcing contractual limits)
- Automated Failover

Upgrading – packaged migration paths between hardware platforms save time and effort

- Software/firmware-based migration path
- Software/firmware decoupled from hardware platform
- Migration path between hardware platforms

Cryptography – ensure enterprise grade security

- Support for configurable cryptographic algorithms (Triple-DES, AES, SHA, RSA, etc)
- Support for elliptic curve cryptography
- FIPS 140-2 support in hardware
- FIPS 140-2 support in software
- Onboard PKI
- Onboard Hardware Security Module (HSM)
- Support for external HSMs

Transport Mediation – ensure your IT environment is supported out of the box

- HTTP/ HTTPS
- WebSphere MQ
- JMS
- FTP
- TIBCO EMS
- SMTP
- raw TCP
- End-to-end compression

Policy Lifecycle – decrease administration costs

- Support for branching of policies
- Support for global policies
- Support for policy includes
- Real time policy validation
- Policy Debug Tracing

Encode to/Decode from Base64

Support for global policies

Automate policy migration across environments and geographies

Automatically resolve policy dependencies across environments & geographies when migrating policies

Ability to create custom policies/proprietary capabilities onbox

Support for updating policies on the fly

Performance – ensure fast, message-level processing even for larger payloads

32 bit platform support

64 bit platform support

Transform large messages

Dedicated hardware-based acceleration for XML processing

Acceleration in software for XML processing

Allow 3rd party software to access hardware acceleration

Message caching

Concurrent processing of policy assertions

Certifications – ensure you can meet government and industry specifications

VMware Ready

Common Criteria

EAL4+

US STIG Vulnerability Tested

Joint DoD/IC Service Security Working Group (JSSWG)

Joint DoD/IC Enterprise Service Monitoring

HSPD12 Backend Attribute Exchange (BAE)

Management – decrease Gateway overhead costs

Integrated Global Management

Centralized administration of all units in a single cluster

Centralized administration of all units in multiple clusters

Single, real time management view of all Gateways in the enterprise

Remote Patching

Remote restoration

System-level monitoring / alerting

Support for disaster recovery

Support for off box logging

Support for patching of onboard 3rd party software

Central management of hardware, software and cloud instances

Java-based interface for 3rd party management

SOAP-based interface for 3rd party management

Command line interface for 3rd party management

Identity Capabilities – securely bridge identities across domains

Integrated STS/SAML issuer

Support for Web/browser-based SSO

Onboard identity store

Integrated PKI Certificate Authority (CA)

Integrated PKI Registration Authority (RA)
OAuth support
Kerberos support
Support for creating and evaluating XACML requests

Threat Protection – ensure against accidental and deliberate system compromise

Protection against viruses in attachments
XML Entity Expansion and Recursion Attacks
XML Document Size Attacks (based on size, width, depth, etc)
XML Parser Attacks
Jumbo Payloads
Recursive Elements
MegaTags – aka Jumbo Tag Names
Public Key DoS attack
XML Flood
XML Encapsulation
XML Virus
Replay Attacks
Resource Hijack
Dictionary Attack
Message Tampering
Falsified Message
Data Tampering
Message Snooping
XPath Injection
SQL Injection
Xquery Injection
WSDL Enumeration
Routing Detour
Schema Poisoning
Malicious Morphing
Malicious Include (aka XML External)
Entity (XXE) Attack
Memory Space Breach
XML Morphing
Parameter Tampering
Coercive Parsing
Field level validation
Scanning outgoing messages for sensitive content based on Metadata or Regular Expression Pattern
XML firewalling for Web 2.0 (such as REST)

Client-side Enablement – implement true decoupling of clients from services

Support for dynamic client-side retrieval & execution of policy
Support for static security policies
Support for client-side key management

Support for client-side PKI provisioning
Support for client-side SSO
Support for client-side federation
Support for client-side STS integration
Support for client-side compression
Deployable as an independent executable
Deployable as a Windows service
Available as Java class library
Support for SAML
Support for Windows, Unix, and Mac OS
Implements standards-based policy exchange

Standards Support – ensure you can preserve your investment

XML 1.0
SOAP 1.2
REST
AJAX
XPath 1.0
XSLT 1.0
WSDL 1.1
XML Schema
LDAP 3.0
SAML 1.1/2.0
PKCS #10
X.509 v3 Certificates
W3C XML Signature 1.0
W3C XML Encryption 1.0
SSL/TLS 1.1 / 3.0
SNMP
POP3
IMAP4
WS-Security 1.1
WS-Trust 1.0
WS-Federation
WS-Addressing
WSSecureConversation
WS-MetadataExchange
WS-Policy
WS-SecurityPolicy
WS-PolicyAttachment
WS-SecureExchange
WSIL
WS-I
WS-I BSP

UDDI 3.0

IPv6

MTOM

Exception Handling – identify root causes quicker

Support for customized audit messages

Support for customized error messages

Support for operator alerts over SNMP and SMTP

Monitoring – gain visibility into your SOA landscape

Support for real-time graphing of service activity

Monitors activity on a particular cluster member

Monitors aggregate statistics from across a cluster

Licensing – avoid platform lock-in and re-licensing costs

Move licenses across form factors at no cost