

Key Criteria for Selecting an API Management Solution



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 an API Management RFI/RFP. It is not intended to be an exhaustive list, nor does it reflect all possible solutions. You may incorporate any and all appropriate entries listed below within your RFI/RFP in order to help you qualify vendors.

API Proxy

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

- Hardware appliance
- Virtual Appliance
- Software
- Cloud-based service

API Transformation – ensure you can support your existing APIs and developer preferences

- SOAP to REST
- REST to SOAP
- XML to JSON
- JSON to XML

API Rate Limiting – ensure control over API performance

- API throttling and/or rate limiting
- API traffic prioritization
- API response caching
- Limit API access based on user, time of day and/or IP address
- Route API traffic based on geography, IP address and/or back-end response times
- Define custom data and identity caching parameters for optimal API performance

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

Encryption – 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

Certifications – ensure you can meet government and industry regulations

PCI-DSS
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)

API Access Control – ensure you can secure access to your APIs

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
HMAC support
HTTP basic/ digest support
Support for X.509 certificates
SSL client-side certificate authorization
Microsoft SPNEGO support
Kerberos support
Support for creating and evaluating XACML requests

API Threat Protection – ensure against accidental and deliberate system compromise

Protection against viruses in attachments
Cross-site scripting
Cross-Site Request Forgery
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)

API Lifecycle

API Proxy Management – decrease overhead costs

Integrated global API proxy management
Centralized administration of all API proxies in a single cluster
Centralized administration of all API proxies in multiple clusters
Single, real time management view (i.e., dashboard) of all API proxies in the enterprise
Remote Patching of API proxies
Remote restoration of API proxy
System-level monitoring / alerting
Support for disaster recovery
Support for off-box logging
Central management of hardware, software and cloud-based API proxies
Java, SOAP and command line API for 3rd party/remote management

API Management – decrease API administration costs

API versioning and rollback
API composition
API orchestration
Automate API migration across environments and geographies
Automatically resolve dependencies across environments & geographies when migrating APIs

API Policy Lifecycle – govern and control your APIs

Support for branching of API policies
Support for global API policies

Support for API policy includes
Real time API policy validation
API policy debug tracing
Ability to create custom API policies/proprietary capabilities
Centrally update API policies and push them to all API proxies
Support for updating API policies on the fly

API Monitoring – gain visibility into API performance

Track overall API performance
Track API performance for each operation
Track API performance by developer
Track API performance by specific developer customers
Track API performance by client IP

Developer Portal

Developer Account Management – manage your developer community

Developer registration workflow
Ability to create groups of developer accounts (i.e., gold, silver, bronze)
Ability to support multiple users per developer account
Ability to approve developer registrations before activation
Developer support forums/discussion boards
Developer dashboard
Integrated messaging system

API Key Management – ensure access control

API key distribution
Ability to suspend and/or revoke API keys
Ability to associate an API key with a developer's application
Ability to generate an API certificate or token (in addition to an API key)

API Plans – ensure you can manage API usage

Support for multiple API plans
API usage rate limiting by hits
API usage rate limiting by method
Support for specifying a monthly recurring fee
Support for specifying an API trial period
Support for specifying a setup fee

Content Management System – ensure you can implement your brand

Global CSS support
Per section CSS support
Support for uploading/downloading files
RBAC controls for author, editor, publisher, etc
Ability to insert custom code (i.e., Google Tracker)
Ability to create/modify menus
Workflow support
Blog

Metering and Billing – ensure you can monetize API usage

- Support for integration to existing billing systems
- Support for payment gateways (i.e., credit card, PayPal, etc)
- Support for metering/billing of a developer's customers
- Ability to bill by usage of a specific API feature/function
- Support for multiple types of billing

API Reporting – understand API usage

- Report on API usage by individual developer
- Report on API usage by developer group
- Report on API usage by specific developer customers
- Ability to generate reports in multiple (i.e., CSV, PDF and HTML) formats
- Ability to integrate with an existing enterprise reporting system
- API throughput report
- API routing failure report
- API utilization report
- API availability report
- API usage report
- API availability report
- API methods report
- API response times report
- API backend latency report