SOLUTION BRIEF • LAYER7 API MANAGEMENT

ca technologies
A Broadcom Company

Enable and Protect Your Web Applications From OWASP Top Ten With Layer7 API Management

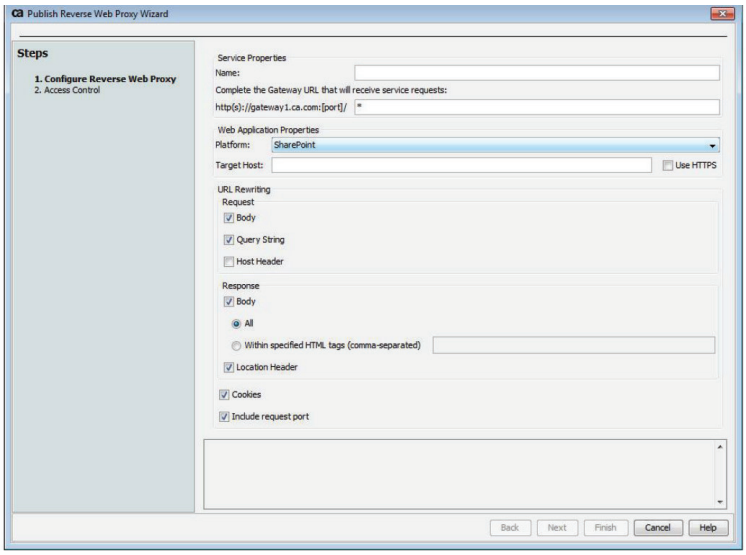
How can an enterprise manage web services, web APIs and web applications from a single platform? Depending on the business requirements, Layer7 API Management can be the one security platform for all web services, APIs and application traffic.

Executive Summary

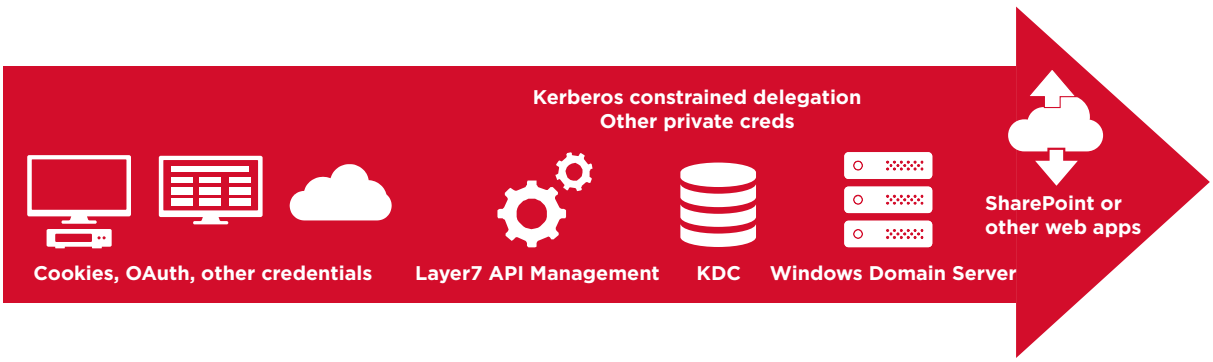
Layer7 API Management has long helped customers simplify and accelerate the security, integration and management of their web services and web API traffic. Many enterprises are looking to extend that same functionality to web applications (similar to many of the functions a web application frewall might provide) and are looking to consolidate appliances into a single platform. Depending on your requirements, Layer7 API Management can be your one security gateway for all web services, APIs and application traffic.

Benefits

This begins with the Publish Reverse Web Proxy Wizard, which makes it easy to quickly publish a reverse web proxy with a runtime policy tailored specifically to Microsoft® SharePoint® or a more generic runtime policy for any other web application.



One common use case for which customers use Layer7 API Management is enabling non-Kerberos client access (e.g., mobile device browser access) to Kerberos-protected SharePoint sites. Layer7 API Management's Publish Reverse Web Proxy Wizard and support for Kerberos Constrained Delegation makes this possible. Layer7 API Management has broad support for many other credential types including X.509, HTTP Basic, SAML, OAuth, JWT, Layer7 Single Sign-On and more. This allows Layer7 API Management to be an identity broker for many other scenarios.



Another common use for API management is meeting PCI requirements, which necessitates an assessment of the OWASP Top Ten.

OWASP Top Ten

Layer7 API Management also provides many additional capabilities to protect web application threats like those described by the OWASP Top Ten (2017), and OWAPS Top Ten protection can help customers meet key PCI requirements:

- **A1 Injection**
  Layer7 API Management provides policy assertions to protect against SQL and other types of injection attacks. Layer7 API Management also has full access to all web request and response content and context to enable inspection and protection at runtime.
- **A2 Broken Authentication**
  Layer7 API Management can require strong or multifactor authentication over secure protocols and can protect against brut e force attacks using simple or sophisticated rate limiting or throughput quota policies.

  Through policy management, Layer7 API Management can also detect and protect against session-based attacks by controlling cookie security attributes, using digital signatures and encryption or tracking and mapping and enforcing sticky session identifiers sent in a variety of ways.
- **A3 Sensitive Data Exposure**
  Through policy management, Layer7 API Management can require encryption at rest or in-transit, and can be configured to to PCI-DSS compliant - meeting the needs of regulated industries such as financial, healthcare, and public sector.
- **A4 XML External Entities**
  Layer7 API Management can protect against remote code execution and denial of services (DoS) attacks.
- **A5 Broken Access Control**
  Layer7 API Management provides an unparalleled range of proprietary and industry-standard access control mechanisms to ensure that protected resources can only be accessed by authenticated and authorized users and applications using centralized security policies.
- **A6 Security Misconfiguration**
- Layer7 API Management is a special-purposed security gateway that has been hardened for easy and secure deployment to the DMZ, and meets Common Criteria certification for the Enterprise Security Management, Policy Management Version 2.1, and Enterprise Security Management, Access Control Version 2.1 profiles.

As the first line of application layer defense in front of your web applications, Layer7 API Management can help protect you from security misconfigurations elsewhere in your stack.

- **A7 Cross-Site Scripting (XSS)**
  Layer7 API Management is a hardened and purpose built solution for maximum attack protection for services, APIs and applications, and it allows customers to detect, respond to and block attackes using centralized security policy as an application layer firewall.
- **A8 Insecure Deserialization**
  Layer7 API Management provides policy assertions to protect against SQL and other types of injection attacks. Layer7 API Management also has full access to all web request and response content and context to enable inspection and protection at runtime.
- **A9 Using Components with Known Vulnerabilities**
  As noted under A5, Layer7 API Management is a special purposed security gateway that has been hardened for easy and secure deployment to the DMZ and meets Common Criteria certification for the Enterprise Security Management—Policy Management Version 2.1 and Enterprise Security Management—Access Control Version 2.1 profiles.

  Layer7 API Management engineering and support teams are constantly vigilant for new vulnerabilities and quickly create, release and communicate vulnerability patches to Layer7 API Management customers. These patches are easily applied through the patch management system included with Layer7 API Management.
- **A10 Insufficient Logging and Monitoring**
  Layer7 API Management provides definable monitoring levels, allowing the appropriate level of reporting based on the enterprise requirements.

In addition to implementing signature-based threat detection using the patterns described above, Layer7 API Management integrates with best-of-breed virus scanners and further protects from message-level threats by validating traffic against application-level metadata such as XML schemas and JSON schemas.

Finally, Layer7 API Management provides additional reverse web proxy capabilities including:

- Caching
- Throttling/shaping
- Compression
- SSL termination
- Intelligent dynamic routing/load balancing
- URL rewriting
- Header manipulation
- Parameter manipulation
- Cookie manipulation

Summary

For many enterprises, configuring Layer7 API Management as defined above will allow them to consolidate appliances and from a single pane of glass, manage the security, integration and management of their web services, web API traffic and web applications.

The Layer7 Technologies Advantage

Layer7's industry-leading API management products connect the enterprise to mobile apps, cloud platforms, developers and IoT through APIs. Delivered as hardware networking appliances, virtual appliances or as software, our products are helping large organizations integrate everything, simplify and enable app development, protect apps and APIs with end-to-end security and enable business growth in the application economy.

About Broadcom
Broadcom Inc. (NASDAQ: AVGO) is a global technology leader that designs, develops and supplies a broad range of semiconductor and infrastructure software solutions. Broadcom's category-leading product portfolio serves critical markets including data center, networking, enterprise software, broadband, wireless, storage and industrial. Our solutions include data center networking and storage, enterprise and mainframe software focused on automation, monitoring and security, smartphone components, telecoms and factory automation. For more information, go to www.broadcom.com.

0719