zapthink
zapnote

Doc. ID: ZTZN-1203
Released: Oct. 26, 2006

ZAPTHINK ZAPNOTE™

LAYER 7 TECHNOLOGIES
PROTECTING SOA, WEB SERVICES, AND WEB 2.0 APPLICATIONS

Analyst: Ronald Schmelzer

Abstract

One of the primary benefits of standards-based interoperability formats, especially XML and Web Services, is that they allow for direct and easy interchange of information between disparate and heterogeneous systems in a distributed environment. However, one of the major drawbacks to this ease of interoperability is that information passes far *too* easily between systems – so easily that it passes malicious and harmful content along with the desirable information.

Organizations that want the benefits of interoperability without the commensurate security risks need to consider a threat-mitigation and data cleansing approach that operates on at a message level with XML and Web Services content. To address these needs, Layer 7 Technologies released the SecureSpan XML Data Screen appliance that provides effective and efficient XML threat prevention and data cleansing for SOA, Web Services, and Web 2.0 applications.

Protecting Web Services

As the use and proliferation of XML and Web Services spreads throughout the corporate IT environment, so too do the dangers of malicious interference with systems or inadvertent compromise of confidential information. Increasingly, organizations are seeking solutions that can transparently monitor XML traffic on the network and apply business rules and corporate IT security policies without adversely impacting network performance or burdening their already over-stretched IT environments. Furthermore, as systems become more distributed and abstracted through Web Services-based Service-Oriented Architecture (SOA), it becomes increasingly difficult for a company to gain adequate knowledge of their vulnerabilities and the level to which their systems are exposed.

Traditional network security appliances like IP-based firewalls and routers have been wholly inadequate to the task of dealing with XML and Web Services traffic, because they work at too low of a level in the seven-layer Open System Interconnection (OSI) model for networking architectures. In particular, the TCP/IP-based approach of traditional network hardware that focuses on looking at where network packets come from and where they are headed misses the mark for handling metadata-rich, text-encoded XML traffic. Security at other layers, including Secure Sockets Layer (SSL), Transport Layer Security (TLS), or IP Security (IPSec), are good at preventing network snooping of traffic, but are wholly inadequate for the authentication, authorization, and content-specific requirements for securing XML traffic.

In addition, companies must safeguard the data that systems exchange. Today, many organizations use Web Services to exchange this business-critical data payloads. This payload might be insurance claims, electronic patient records, or simply acknowledgements of transactions. Whatever the size, companies must safeguard these payloads from illegitimate transactions and improper usage. Finally, all this security activity must happen in a way that doesn't slow down the overall performance of the network: the challenge of deep content inspection at network speed.

In addition to simply handling message-based authorization and authentication, companies must safeguard their systems from deliberate and malicious attacks on their systems that can come in a wide variety of forms, including at the XML document and element level. For example, emerging XML-based threats include denial-of-service (DoS) attacks using malformed XML documents, data that are outside the acceptable bounds of a schema, SQL insertion attacks, and buffer overflows. Also, companies must safeguard against intentional or inadvertent divulging of private identity information by blocking the disclosure of sensitive corporate and customer information, such as credit card and social security numbers in XML-based message exchanges.

One of the key challenges to dealing with this sort of threat prevention is that XML traffic is *content-oriented*, rather than protocol-oriented. A device responsible for securing XML traffic must make decisions based upon the content of the messages, rather than the protocols that underlie those messages. In other words, users require a layer at the top of the OSI stack — the content layer—where a new class of XML appliances can operate. As a result, there is a new category of device that offers a range of content-based security features, including policy enforcement, malformed message protection, authorization and authentication, encryption and decryption, and schema validation. By incorporating this functionality into hardware, companies can gain substantially higher performance for XML threat managemnt and also offer security-hardened environments that prevent tampering as well as simplified administration.

Layer 7 Technologies: SecureSpan XML Data Screen

With a history of solving XML and Web Services-related security issues, Layer 7 Technologies has recently released its *SecureSpan XML Data Screen* appliance to protect Web services applications from the sorts of threats and improper access discussed above that can cause damage, downtime or improper information. The XML Data Screen appliance cleanses XML data streams of threats, vulnerabilities and unauthorized content for all common XML message formats over all forms of XML-based interaction including "plain old XML" (POX), SOAP-based Web Services, Representational State Transfer (REST) messages, and emerging Ajax approaches.

Layer 7 Technologies' XML Data Screen device acts as a content filter, and can be configured to scan, purge, or transform any questionable content, including malicious or malformed data, private or classified keywords or data, and unwanted interactions between consumers and data providers. XML Data Screen protects applications from XML Denial of Service (XDoS) and other parser-based exploits, assuring the continuous availability of service endpoints. The system leverages policies to remove, block or transform illegal data on an element or entire message basis. The system also allows enterprises to throttle traffic to specific endpoints based on user defined policies, message formats, or consumer profiles. In addition, administrators can configure all operations on the SecureSpan XML Data Screen independently for inbound and/or outbound traffic.

Specific features of the product include accelerated threat and intrusion protection against XML and Web services exploits, content filters for bad, malformed or restricted content, accelerated data validation for documents exchanged via an Enterprise Service Bus (ESB), XML traffic control and monitoring, security for Ajax- and REST-based services, built-in and preconfigured filters for XML threat and anomaly signatures, policy based content and URL processing, optional virus scanning for binary attachments, and built-in clustering support for scalability and high availability.

Key security features include application protection against XML content tampering and viruses in SOAP attachments, protection against SQL and malicious script injection attacks, allowing or rejecting messages based on time of day, day of week and IP address, configuration throughput restrictions based on requestor or destination prevents downstream XML DoS, configurable limits on XML message size, element size, nesting depth, and string length, among others, detection of classified or "dirty" words or arbitrary signatures with subsequent scrubbing, rejection or redaction of messages, content detection within XML data structure or across entire message, configurable scrubbing or rejection of AJAX or other messages with embedded scripts. The system supports a wide range of standards including XML, SOAP 1.1, REST, XPath 1.0, XSLT 1.0, WSDL 1.1, XML Schema & DTD, SSL/TLS 2.0 / 3.0, SNMP, SMTP, and HTTP/HTTPS.

Built in a network appliance form-factor, the SecureSpan XML Data Screen is available as a linearly scalable, high performance 64-bit, multi-processor, 1U appliance with onboard XML and SSL acceleration. Users can deploy the appliance in a proxy mode, acting as a central entry point to a network, as a gateway to existing message bus or ESB capabilities, or as a co-processor that any Service consumer on the network can access.

The appliance is actually part of a family of appliances that assist with security and policy for XML and Web Services-based applications, including *SecureSpan XML Firewall and VPN* and the *SecureSpan XML Networking Gateway*. As such, the company aims to provide a complete set of appliances that address the full range of XML and Web Services security concerns.

The ZapThink Take

It's clear that XML and Web Services usage in all its many forms, including Ajax and REST-based approaches, will only continue to grow through the remainder of this decade and beyond. The benefits of loose coupling, composition, interoperability, and agility far outweigh the downsides of inefficiency and security risks. However, there is also no doubt that organizations will have to address issues of security and efficiency in a robust, affordable, and effective manner if the growth of XML and Web Services is to continue unabated.

As such, Layer 7 Technologies' latest addition to their security-focused appliance product line takes a major step towards helping firms with their desire to achieve the benefits of XML while mitigating its drawbacks. While there are other vendors in the market with similar capabilities and strategies for securing XML and Web Services data, the approach Layer 7 Technologies is taking to the market with its multi-product strategy is compelling to firms looking to make substantial investments in XML.

Company Profile

Layer 7 Technologies **Oct., 2006**

Overview:
Layer 7 Technologies is a provider of XML security and networking infrastructure for next generation service oriented and Web oriented integrations. The SecureSpan family of XML appliances and gateway software address the security, complexity, performance and networking issues associated with deploying and maintaining production Web services.

Product Offerings:

- SecureSpan XML Accelerator - High-throughput document parsing, validation and transformation in a datacenter or with an ESB
- SecureSpan XML Data Screen – High-speed XML threat protection, content filtering and traffic control
- SecureSpan XML Firewall and VPN - Advanced identity and message level SOA security for cross-domain, B2B and portal SOA initiatives
- SecureSpan XML Networking Gateway – Complex, policy based message routing, mediation, virtualization, SLA and SOA governance enforcement

Value Proposition

- The SecureSpan set of XML appliances, help organizations secure, simplify and scale their SOA and Web 2.0 deployment.

Funding: Privately-held, Venture backed: GrowthWorks Venture Capital, BDC Venture Capital, Shoreline Ventures

CEO: Ed Koepfler

Address:
1501-700 West Georgia St.
Vancouver, BC V7Y 1B6
CANADA
URL: www.layer7tech.com
Phone: +1-800.681.9377
Contact: Dimitri Sirota (dsirota@layer7tech.com)

About ZapThink, LLC

ZapThink is an IT advisory and analysis firm that provides trusted advice and critical insight into the architectural and organizational changes brought about by the movement to XML, Web Services, and Service Orientation. We provide our three target audiences of IT vendors, service providers and end-users a clear roadmap for standards-based, loosely coupled distributed computing – a vision of IT meeting the needs of the agile business.

ZapThink helps its customers in three ways: by helping companies understand IT products and services in the context of Service-Oriented Architecture (SOA) and the vision of Service Orientation, by providing guidance into emerging best practices for Web Services and SOA adoption, and by bringing together all our audiences into a network that provides business value and expertise to each member of the network.

ZapThink provides market intelligence to IT vendors and professional services firms that offer XML and Web Services-based products and services in order to help them understand their competitive landscape, plan their product roadmaps, and communicate their value proposition to their customers within the context of Service Orientation.

ZapThink provides guidance and expertise to professional services firms to help them grow and innovate their services as well as promote their capabilities to end-users and vendors looking to grow their businesses. ZapThink also provides implementation intelligence to IT users who are seeking guidance and clarity into the best practices for planning and implementing SOA, including how to assemble the available products and services into a coherent plan.

ZapThink's senior analysts are widely regarded as the "go to analysts" for XML, Web Services, and SOA by vendors, end-users, and the press. Respected for their candid, insightful opinions, they are in great demand as speakers, and have presented at conferences and industry events around the world. They are among the most quoted industry analysts in the IT industry.

ZapThink was founded in October 2000 and is headquartered in Baltimore, Maryland. Its customers include Global 1000 firms and government organizations, as well as many emerging businesses. Its analysts have worked at such firms as IDC, marchFIRST, and ChannelWave, and have sat on the working group committees for standards bodies such as RosettaNet, UDDI, and ebXML.

ZAPTHINK CONTACT:
ZapThink, LLC
108 Woodlawn Rd
Baltimore, MD 21210
Phone: +1 (781) 207 0203
Fax: +1 (786) 524 3186
info@zapthink.com
www.zapthink.com