

Improving Performance and Control in SAP Environments

Cisco® ACE XML Gateway boosts response times, security, availability, and monitoring of SAP Web services.

When combined with SAP's Web services products, such as software from the SAP Business Suite family of business solutions and NetWeaver, SAP's service-oriented platform, the Cisco ACE XML Gateway delivers improvements in performance, security, availability, and monitoring. A critical component of the Cisco Application Control Engine (ACE) product portfolio, the Cisco ACE XML Gateway is a powerful appliance that provides a solution to the challenges posed by Extensible Markup Language (XML) applications and service-oriented architectures (SOAs).

XML: Its Advantages and the Four Challenges

As enterprises continue their migration to SOAs that are based on Web services, XML services comprise the central components of many integration strategies. XML services are generally considered a fundamental component of a flexible architecture for real-time integration. In fact, leading enterprise application vendors, such as SAP, have recognized the potential of XML and have added XML and Web-services capabilities to their product lines.

XML-based applications, such as those supported by the SAP Business Suite, allow companies to integrate those tasks and activities that have been only loosely coupled in the past. Because XML provides a communication standard that fosters the interoperability of business processes running on disparate platforms or technologies, enterprises using SAP Business Suite applications running on the NetWeaver platform can now accommodate an expanding base of trading partners and programmatically integrate communications among any applications.

Along with the benefits of XML-based applications come four distinct challenges for the IT professional.

XML Challenges

- **Dealing with excessive size of XML:** The very nature of XML makes it 3 to 10 times more verbose than traditional communications mechanisms, rendering XML applications more computationally intensive. Analysts estimate that XML will represent as much as 50 percent of all Web traffic by 2008. With this predicted steady increase in XML traffic, ensuring application performance and server efficiency becomes problematic.
- **Application-level threats and identity challenges:** New security threats arise with an increase in XML traffic. When XML facilitates the sharing of common services outside traditional security mechanisms, information often crosses trust boundaries between applications. Additionally, new XML threats are regularly directed at networks.
- **Availability and integration:** The growth in the number of users and the breadth and scope of applications make availability and integration another pair of challenges. Ensuring availability and integration across applications as the user base grows can require huge time and resource investments and can have a significant effect on application performance.

- **Monitoring and compliance:** IT professionals must continue to meet the constant challenges of monitoring the network to meet government-mandated corporate compliance requirements.

Overcoming XML Challenges

IT professionals responsible for SAP environments can meet all of these challenges and help ensure the integrity of their e-business processes using the Cisco ACE XML Gateway in the following ways.

Dealing with Excessive Size of XML: Server Offloading Greatly Accelerates Performance

The Cisco ACE XML Gateway accelerates the performance of Web services and XML applications by offloading XML processing, freeing as much as 30 percent of an enterprise's server resources.

The XML message is the key to integration between applications and businesses in an SOA environment. In fact, in e-business environments such as those using SAP Business Suite, the XML message is usually part of a highly valued, often time-relative transaction, such as a purchase order that must be received, recorded, processed, and filled. Therefore, efficient XML message processing is directly related to application performance. If XML message processing is not optimized, the number and size of XML messages often cause server or infrastructure overload, resulting in poor application performance.

The Cisco ACE XML Gateway solves the problems of XML message size and inherent "chattiness" by offloading and accelerating XML processing. First, the Cisco ACE XML Gateway handles heavy XML processing functions, such as schema validation, XML transformations, and security processing. Secondly, the unique Cisco XML acceleration technology provides a sevenfold end-to-end message processing improvement over other appliances. This improvement, in turn, offloads expensive CPU processing cycles on the server.

The Cisco ACE XML Gateway is also optimized to perform necessary transformation of protocols (for example, Java Messaging Service [JMS] to HTTP), Extensible Stylesheet Language Transformations (XSLT), and XML structure in SOA environments, freeing still more server CPU cycles.

Application-Level Threats and Identity Challenges: Mitigating Cross-Domain XML Threats with Deep Packet Inspection

Today's business environments have strong security and compliance requirements. Enterprises employ firewalls, identity management systems, authentication systems, and other security tools to safeguard all e-functions. Yet, the new architecture that allows the integration and sharing of business-critical information poses new security risks. Because these application-level threats are transparent to traditional packet-based security solutions, businesses employing an SOA layout must protect themselves from XML threats and cross-domain identity security challenges in other ways.

Cross-domain security concerns arise when sharing common services between trading partners, something enabled by SAP Business Suite and the NetWeaver platform. For example, airlines now make car rental and hotel reservations for their customers, a service that requires travel portal intercommunications among systems owned and operated by three different entities. Extending the reach of business systems to trading partners, customers, and suppliers often involves

crossing trust boundaries between applications. The complexity escalates further when various Web services components and consumers reside in different domains.

Traditional firewalls neither understand nor address XML-based attacks, which usually involve the payload of the XML message (Layer 7 information) carrying malicious information or instructions. As a result, the XML message can be used to scan for system vulnerabilities, the XML data can be manipulated to alter system processing, and sensitive data can be redirected within the XML path, exposing and potentially compromising sensitive business assets.

The Cisco ACE XML Gateway delivers firewall capabilities unlike those provided by traditional Layer 3 network firewalls. The gateway focuses primarily on the application layer and works with the payload of the XML message, providing critical protection at each service perimeter between different trust zones. It performs Deep Packet Inspection to provide a broad range of security services, including guarding against malicious XML payloads, structurally invalid XML payloads, and XML denial of service (XDoS). Together with Cisco's multilayer security, with the Cisco ASA 5500 Series Adaptive Security Appliances Firewall or Cisco Catalyst® 6500 Series Firewall Service Module, this gateway provides a complete security solution.

In addition to handling XML threats, enterprises are concerned with authenticating the identity of all users who access their information and applications. Enterprises have invested significant budget and resources in standardizing on identity and access management (I&AM) systems to improve the security and manageability of their identity information. I&AM systems were not originally designed to accommodate decentralized access, and the volume of requests coming from disparate Web services can easily overwhelm these systems.

The Cisco ACE XML Gateway is optimized to integrate any identity-management vendor's products or standards (for example, Lightweight Directory Access Protocol [LDAP]) into a SAP NetWeaver environment. The gateway functions as a centralized policy enforcement point and optimizes access to the identity information and policies already encapsulated in the system. By doing so, the Cisco ACE XML Gateway extends an enterprise's SAP NetWeaver I&AM investment and improves overall security.

Availability and Integration: Ensuring Availability and Responsiveness

The range of applications in the SAP Business Suite supports critical business processes. Enterprises count on SAP's capabilities for virtually every type of business function. The challenge becomes ensuring the granularity of quality of service (QoS) across countless applications while minimizing connectivity costs for applications competing for resources.

The Cisco ACE XML Gateway allows companies to maximize server efficiency by scaling their business applications with minimal cost. By providing powerful [[note: be careful of such claims for legal reasons]] scalability and throughput for managing XML application traffic -- up to 30,000 transactions per second (tps) and up to 40,000 concurrent connections in a single appliance -- the Cisco ACE XML Gateway solves the QoS and cost-containment conundrum.

By implementing a high-performance, highly parallel, event-influenced architecture, the Cisco ACE XML Gateway reduces service latency and improves both user experience and server use. Combining the offloading of significant XML processing with the protocol transformations described earlier, the Cisco gateway frees server CPU cycles to serve application requests more efficiently.

The Cisco ACE XML Gateway works dynamically with SAP Business Suite running on the NetWeaver platform to help enable greater agility and responsiveness to the needs of the

enterprise. The gateway helps IT organizations manage unpredictable service outages and overwhelming service usage by acting as a policy enforcement and monitoring point; these gateway functions allow consistent policy application across all services, and also monitor and audit application system behavior. The ready adaptability of the gateway allows IT departments to deploy services without modifying a single line of code and without having to resubmit services to quality assurance testing.

The Cisco ACE XML Gateway also decreases the complexity of the network infrastructure because endpoints do not need to be managed separately and client software agents do not need to be deployed individually. As a result, the infrastructure has fewer points of failure. IT staff also benefit through increased visibility across platforms, enterprise service buses (ESBs), and applications, helping ensure security and maintaining the levels of application performance.

Monitoring and Compliance: Monitoring and Controlling Applications

Complex distribution systems are inherently difficult to monitor, secure, and troubleshoot. They are also the inevitable result of integration growth. IT professionals need a new set of tools and additional data sets to ensure high levels of reliability with these complex distribution systems. The Cisco ACE XML Gateway provides a comprehensive variety of reports and statistics whose use can result in better overall operations, on-target capacity planning for services, and compliance.

The Cisco ACE XML Gateway delivers information-rich, time-based reports from various points in the message processing cycle, including consumer identity-based performance and usage reports. In order to pinpoint performance deviances with greater accuracy, the details of recent application performance can be tested within specified time periods (for example, “since 3 p.m. Monday”). Any captured performance statistics from this process or others can then be reported and exported as requested. Using the sophisticated GUI of the gateway, IT staff can gain visibility into the network and quickly monitor and debug services. Traffic-monitor graphs present dynamic information about performance, service use, and errors. In addition, the Cisco ACE XML Gateway makes it easy to capture and view syslog, message, and event logs and to monitor and report all types of traffic and service-level agreements (SLAs).

Finally, the auditing, logging, and nonrepudiation capabilities of the Cisco ACE XML Gateway help streamline the process of satisfying compliance needs. Creating an audit trail of administrative operations is also a critical capability of the gateway that can be invaluable for debugging, record keeping, troubleshooting, and reconstitution of prior configurations.

Conclusion

IT professionals can meet the new challenges posed by the proliferation of XML-based services by adding the power of the Cisco ACE XML Gateway to their network. The Cisco ACE XML Gateway provides improved performance, security, availability, and monitoring and auditing (for compliance) for applications and Web services in SAP environments.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCVP, Cisco Eee, Cisco StadiumField, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play and Learn is a service mark; and Access Registrar, Altranet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDE, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IQS, IPPhone, IP TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, M3X, Netwerk+, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTlist, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. ©2008