Cisco ACE Web Application Firewall Version 6.0

PB458632

The Cisco® ACE Web Application Firewall is the newest addition to the Cisco ACE family of products. It provides a full-proxy firewall solution for both HTML and Extensible Markup Language (XML)-based Web applications.

Because of its unique blend of HTML and XML security, the Cisco ACE Web Application Firewall provides a full compliance solution for the Payment Card Industry (PCI) Data Security Standard (DSS) version 1.1's requirements in sections 6.5 and 6.6.

Section 6.6 in particular mandates that any organization handling, processing, or storing credit card information must install a Web application firewall by June 30, 2008 to protect applications against the OWASP Top 10 attacks (http://www.owasp.org/index.php/Top_10_2007.)

The Cisco ACE Web Application Firewall provides full compliance with the latest's PCI requirements by securing and protecting Web applications from common attacks, such as identity theft, data theft, application disruption, fraud, and targeted attacks. These attacks may include cross-site scripting (XSS) attacks, SQL and command injection, privilege escalation, cross-site request forgeries (CSRFs), buffer overflows, cookie tampering, and denial of service (DoS) attacks.

Additionally, the Cisco ACE Web Application Firewall's integrated XML firewall capabilities extend protection for traditional HTML-based Web applications to modern XML-enabled Web services applications to provide the broadest compliance with PCI standards. The security for XML data includes XML threat mitigation such as validating XML content to block message processing policy violations in your Web services' application traffic.

The Cisco ACE Web Application Firewall enables organizations to:

- Dramatically reduce their exposure to expensive Web-based attacks on mission-critical applications
- Deploy secure Web projects in a fraction of the time and cost of competitive solutions
- Simplify ongoing Web security management through the ability to work with SOA and XML applications

New Features

Cisco ACE Web Application Firewall Version 6.0 offers new capabilities to extend security for Web-facing applications (Table 1). These features help organizations defend applications against Web-based HTML and XML threats and protect against identity theft, data theft, content and format threats, access threats, compliance, transport, and targeted attacks such as DoS attacks.

Table 1. New Features in Cisco ACE Web Application Firewall Software Version 6.0

Feature	Description	Benefit
Web Application Security	• Full reverse proxy • Monitor mode deployment • Buffer overflow • HTTP parameter manipulation, protocol compliance • Null byte blocking • Input encoding normalization • Response filtering and rewriting • Flexible firewall actions • Cookie and session tampering • Cross-site scripting (XSS) • Command injection, SQL injection • Privacy enforcement by preventing information leaks • Cryptography enforcement • Application and server error message cloaking • Referrer enforcement • Positive and negative security models • Custom rules and signatures • PCI compliance profiles	• Supports human-assisted learning using monitor mode deployment • Defends applications against Web-based HTML and XML threats • Protects against identity theft, data theft, content and format threats, access threats, compliance, transport, and targeted attacks • Enables users to create custom rules and signatures • Offers a set of preconfigured rules that help address PCI DSS 1.1 section 6.5 and 6.6 (OWASP Top 10)
Monitoring, Audit, and Logging	• Firewall statistics logging • Firewall reports • Audit and non-repudiation capabilities	• Quickly debugs and monitors Web applications using sophisticated GUI • Comprehensive statistics and reporting capability
Policy-Based Provisioning and Versioning	• Sophisticated rollback and versioning capabilities • Click-to-rule • Ability to configure security policies in one centralized policy management system, without programming • Unique policy configuration to define policies and secure all points in the request-response process	• Increases developer productivity and improves deployment flexibility • Quickly eliminates false positives with the ability to turn off firewall rules for specific violations with a single click

Availability

Cisco ACE Web Application Firewall will be available for ordering beginning May 1, 2008.

Ordering Information

Table 2 provides ordering information for the Cisco ACE Web Application Firewall.

Table 2. Ordering Information

Product Options	Product Name	Part Number	Support and Services
Chassis	• Cisco ACE Web Application Firewall Appliance	• ACE-XML-K9 or • ACE-XML-NF-K9	• CON-SNT-ACEXK9 or • CON-SNT-ACEXNK9
Software	• Cisco ACE Web Application Firewall Software	• ACE-XML-SW-6.0	–
Cryptography	• FIPS-compliant SSL acceleration or • Non-FIPS-compliant SSL acceleration	• ACE-XML-FIPS or • ACE-XML-NONFIPS	• CON-SNT-ACEXFIPS or • CON-SNT-ACEXNFIP
Licensing	• Cisco ACE Web Application Firewall license or • Cisco ACE Web Application Firewall Manager license	• ACE-WAF-GAT-LICFX or • ACE-WAF-MGT-LICFX	• CON-SAU-ACEWGW or • CON-SAU-ACEWMG

Cisco Service and Support

Cisco takes a lifecycle approach to services and, with its partners, provides a broad portfolio of security services so enterprises can design, implement, operate, and optimize network platforms that defend critical business processes against attack and disruption, protect privacy, and support policy and regulatory compliance controls.

Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. Cisco services include:

- The Cisco Security Center provides one-stop shopping for early warning threat intelligence threat and vulnerability analysis, Cisco IPS signatures, and mitigation techniques. Visit and bookmark the Cisco Security Center at www.cisco.com/security.
- The Cisco Security Intellishield Alert Manager Service provides a customizable, Web-based threat and vulnerability alert service that allows organizations to easily access timely, accurate, and credible information about potential vulnerabilities in their environment.
- Cisco Security Optimization Service: Increasingly, the network infrastructure is the foundation of the agile and adaptive business. The Cisco Security Optimization Service supports the continuously evolving security system to meet ever-changing security threats through a combination of planning and assessments, design, performance tuning, and ongoing support for system changes. This service helps integrate security into the core network infrastructure.
- Cisco SMARTnet Service delivers rapid issue resolution by giving businesses direct, anytime access to Cisco engineers, an award-winning online Support Center, machine-to-machine diagnostics on select devices and premium advance hardware replacement options.
- Cisco Software Application Support Services, plus Upgrades [SASU] ensures CSA availability, functionality, and reliability with around-the-clock access to technical support, software updates, and major upgrades

The services and support programs described in Table 4, Cisco SMARTnet® Service and Software Application Support plus Upgrades (SASU), are available as part of the Cisco ACE Web Application Firewall Service and Support solutions.

Table 3. Cisco SMARTnet and Software Application Service and Support Programs

Service and Support	Features	Benefits
Available directly from Cisco or through Cisco Certified Partners • Cisco SMARTnet Service • Cisco SASU	• 24x7 access to software updates and upgrades • 24x7 access to Cisco Technical Assistance Center (TAC) via web, phone, email • Advance replacement of hardware parts (Cisco SMARTnet Service only)	• Supplements existing staff • Helps ensure that functions meet needs • Mitigates risk • Helps enable proactive or expedited problem resolution • Lowers total cost of ownership (TCO) by using Cisco expertise and knowledge • Helps minimize network downtime

For More Information

For more information about the Cisco ACE Web Application Firewall, visit http://www.cisco.com/go/ace or contact your local Cisco account representative.

For more information about Cisco Security Services visit http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html.

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.

Printed in USA C25-458632-00 03/08