Cisco ACE Web Application Firewall

Q. What are you announcing today?

A. Today, Cisco is extending its solution for Application Networking Services (ANS)—Cisco Application Control Engine (ACE) family of products—with the addition of the Cisco ACE Web Application Firewall. The main component of this solution is the ACE Web Application Firewall appliance in a convenient 1 RU form factor that provides a full-proxy firewall solution for both HTML and XML-based Web applications. ACE Web Application Firewall solution also includes the ACE Web Application Firewall Manager, a secure, Web-based application for security policy creation and monitoring. The Cisco Application Control Engine (ACE) family of products represents the next generation of application switching and Web services solutions for maximizing availability, acceleration and protection of data center applications.

Q. What are the performance characteristics of the ACE Web Application Firewall?

A. Cisco ACE Web Application Firewalls provide best-in-industry scalability and throughput for securing web-facing HTML and XML applications. The performance characteristics will be detailed once the performance tests have been completed. ACE Web Application Firewalls reduce service latency; improve user experience and server utilization by implementing a high performance, highly parallel event-driven architecture. More information is available in the ACE Web Application Firewall datasheet and can be found online at http://www.cisco.com/go/ace.

Q. What customer challenges does Cisco ACE Web Application Firewall solve?

A. Web application firewalls often reside in the DMZ or in front of any application that is delivered to client browsers on the internet via HTTP or HTTPS. XML and web services are also being deployed and consumed by the same applications being protected by the web application firewall. For the most part, traditional web application firewalls have been unable to inspect XML and web services for threats such as malicious code injections or XDOS attacks. As a result, customers require that an application firewall deliver both a XML firewall and a traditional web application firewall integrated into one system. The Cisco ACE Web Application Firewall secures web-facing HTML and XML application.

For organizations that store, process, and transmit credit card data, two sections of the Payment Card Industry (PCI) Data Security Standard (DSS) focus on web application security: 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 PCI requirements by combining deep Web application analysis with high-performance XML inspection and management to truly address the full range of threats associated with all new Web application services.

Secure, fast, and reliable HTML and XML applications also require the capability to deliver assured throughput, high concurrency, low latency, and support for critical operations such as security and availability. Cisco ACE Web Application Firewall offers these benefits. The ACE Web Application Firewall provides:

- Complete PCI Web application firewall compliance
- Bullet-proof security for your custom applications
- Extensive set of Cisco validated signatures for known malicious patterns
- Understanding of web applications to filter and allow only legitimate traffic
- Human-assisted learning removes to guesswork from your security configuration

Q. What customer benefits does the ACE Web Application Firewall offer?

A. Cisco ACE Web Application Firewall allows enterprises to accomplish the following primary IT objectives:

- Dramatically reduce 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 by future-proofing to SOA and XML applications

Q. What are the core ACE Web Application Firewall features?

A. The core features are:

- Web application security
- Privacy enforcement
- Encryption and signing
- Audit and logging
- Monitoring, Statistics and Reporting
- Policy-based provisioning and versioning

Q. What are the benefits of these core features of the ACE Web Application Firewall?

A. The benefits are:

- Bullet-proof security for custom web-facing applications
- Extensive set of Cisco validated signatures for known malicious patterns
- Understanding of web applications to filter and allow only legitimate traffic
- Human-assisted learning removes to guesswork from your security configuration

Q. What are the key differentiators of Cisco ACE Web Application Firewall Solution?

A. ACE Web Application Firewall secures and protects 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 (CSRF), buffer overflows, cookie tampering, and denial of services (DoS) attacks. The key differentiators are:

- **Future proof application security:** 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. The security for XML data may include XML threat mitigation such as validating XML schema, SOAP and XML content to block message processing policy violations in your Web services' application traffic.

- **Scalability:** Cisco ACE Web Application Firewalls provide best-in-industry scalability and throughput for managing XML application traffic—upwards of 10,000 TPS and up to 10,000 concurrent connections in a single appliance. The final performance characteristics will be detailed once the performance tests have been completed.
- **Positive and Negative security enforcement:** Cisco ACE Web Application Firewall provides best of both worlds by keeping bad traffic patterns out and allowing only good traffic through.
- **Human assisted learning**: Ability to deploy security policies and profiles in monitoring mode to prevent application downtime due to false positives typical in an automated learning environment.
- **Policy-based provisioning:** Cisco ACE Web Application Firewall increases developer productivity and improves deployment flexibility with sophisticated rollback and versioning capabilities.

Q. What is the return on investment (ROI) with Cisco ACE Web Application Firewall?

A. The main reasons customers deploy the Cisco ACE Web Application Firewall is to decrease costs of doing business by securing applications. US Federal trade commission study estimates cost of Identity Theft losses to US businesses between 2002 and 2003 at more than USD 45 billion!. Indirect costs of security breaches are potentially enormous. They include

- Brand erosion
- Customer attrition
- Regulatory non-compliance fines—e.g. Payment Card Industry Data Security Standard
- Lawsuits

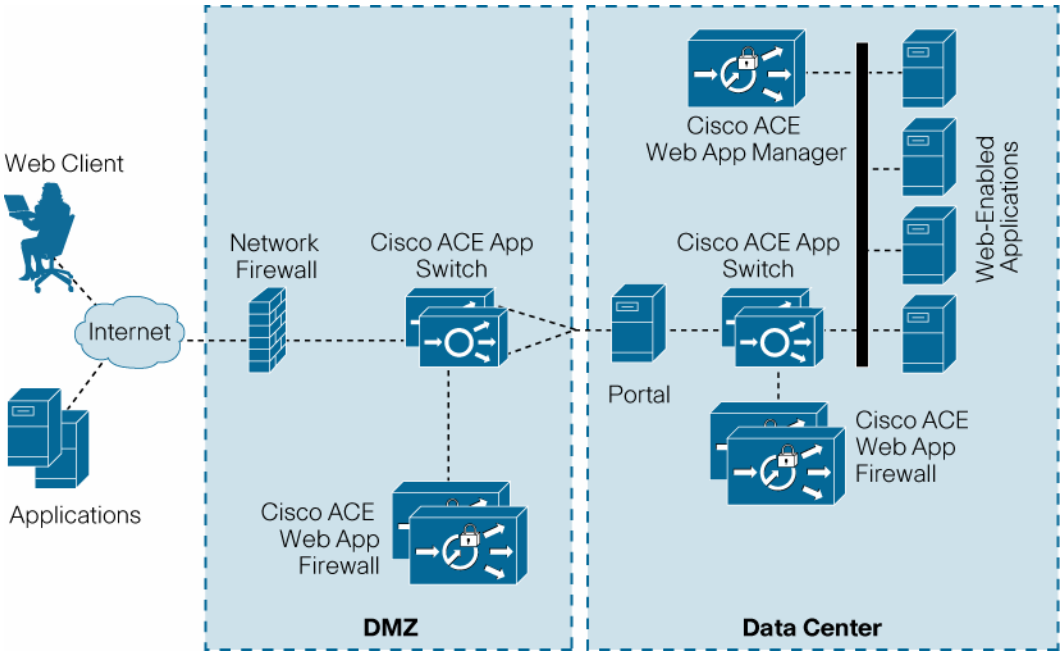
Q. What type of customers can benefit from ACE Web Application Firewall?

A. Cisco ACE Web Application Firewall is targeted for enterprise, federal, service provider and commercial customers that want to secure web-facing applications.

Q. How are ACE Web Application Firewalls deployed?

A. ACE Web Application Firewalls often reside in the DMZ or in front of any application that is delivered to client browsers on the internet via HTTP or HTTPS.

Figure 1. Cisco ACE Web Application Firewall Deployment



Q. What are some of the key features and benefits of ACE Web Application Firewall?

A.

Feature	Benefit
Web Application Security	• Support for 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 such as denial-of-service (DoS) 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) requirements
Privacy	• Exerts comprehensive, enterprise wide, policy control for application access and data privacy
Encryption and Signing	• Prevents cookie tampering and maintain confidentiality of information stored in browser cookies. • Provides full FIPS-compliance, protecting against Secure Sockets Layer (SSL) key hijacking by persistently storing private SSL keys in the platform hardware
Audit and Logging	• Meets compliance requirements with audit and non repudiation capabilities
Monitoring	• Quickly debugs and monitors Web applications using sophisticated GUI • Comprehensive statistics and reporting capability
Policy-Based Provisioning and Versioning	• Increases developer productivity and improves deployment flexibility with sophisticated rollback and versioning capabilities • Quickly eliminate false positives with the ability to turn off firewall rules for specific violations with a single click. • Provides enterprise wide management accessible anywhere on the network through the Web GUI or Secure Shell (SSH) interface • Enables configuration of security policies in one centralized policy management system, without programming
Acceleration and Offloading	• Accelerates Web and XML application processing and improves server utilization by offloading computationally intensive operations such as transport security and enabling HTTP TCP session reuse. • Allows upgrades with future performance enhancements without requiring new hardware

Q. What are some of the new features in the Web Application Firewall 6.0 release?

A. The benefits of the key features are detailed above. The table below highlights the key capabilities in each of the feature categories.

Item	Specification
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 leak • Cryptography enforcement • Application and server error message cloaking • Referrer enforcement • Positive and negative security models • Custom rules and signatures • PCI compliance profiles
Transport Security	• Full SSL v2/3 support with configurable cipher suites • FIPS 140-2 Level 3 platforms available
Cryptographic Support	• Cryptographic algorithms including: • Advanced Encryption Standard (AES) • Data Encryption Standard (DES) • Triple DES (3DES) • Blowfish • RSA • Diffie-Helman • Digital Signature Algorithm (DSA) • Secure Hash Algorithm 1 (SHA-1) and Message-Digest 5 (MD5)
Administration	• Web user interface • Command-line interface • SSH • Simple Network Management Protocol (SNMP) • Roles-based access control (RBAC) • Delegated administration • Central policy management and distributed enforcement • Import and export of configuration, statistics, and logs
Logging, Monitoring, and Auditing	• Syslog and message and event logs • Traffic and service-level agreement (SLA) monitoring and reporting • Statistics for monitoring and various alerts and triggers • Audit trail of administrative operations

Q. What are the hardware features of the ACE Web Application Firewall?

A. Cisco ACE Web Application Firewall is available in both FIPS and Non-FIPS versions. The Non-FIPS version contains a crypto accelerator which is rated at 10,000 TPS, where as the FIPS version is rated at 4,000 TPS. The Non-FIPS version also has a lower price point.

Q. Which minimum software release is supported with the ACE Web Application Firewall for both FIPS and Non FIPS versions?

A. 6.0 is the minimum supported software release to use the web application firewall functionality

Q. Can I upgrade from the Non-FIPS to FIPS version of the ACE Web Application Firewall?

A. No, because the crypto cards are not field replaceable.

Q. Can a Non-FIPS ACE XML Manager manage a FIPS ACE Web Application Firewall?

A. We do not recommend a Non-FIPS ACE Web Application Firewall Manager managing a FIPS ACE Web Application Firewall or a FIPS ACE XML Manager managing a Non-FIPS ACE Web Application Firewall. If a FIPS ACE Web Application Firewall is not using hardware-protected keys, it may be managed by a Non-FIPS ACE XML Manager. Similarly, although a FIPS ACE XML Manager can generate a hardware protected keys, the Non-FIPS ACE Web Application Firewall cannot consume it and may have errors.

Q. Can I upgrade from ACE Web Application Firewall to full functionality ACE XML Gateway?

A. Yes. If you have purchased Cisco ACE Web Application Firewall and would like to upgrade to Cisco ACE XML Gateway that provides additional XML and Web Service transformation and mediation capabilities, we recommend deploying new licenses for both ACE XML Gateway and ACE XML Manager. Please contact you account team for details.

Q. Is the hard disk of the ACE Web Application Firewall field replaceable?

A. Yes, it is.

Q. Does the Cisco ACE Web Application Firewall run Cisco IOS Software?

A. No.

Q. Do the Cisco ACE Web Application Firewall and ACE Web Application Manager have any external interfaces?

A. Yes. They both have 4 GB Ethernet ports plus a dedicated lights out management port.

Q. How much memory is available on the ACE Web Application Firewall? Can the memory be upgraded?

A. 4 GB. No, the memory is not upgradeable.

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 C67-460554-01 05/08

