

Citrix Application Firewall

COMPREHENSIVE PROTECTION FOR WEB APPLICATION AND WEB SERVICES DATA AND SERVERS

Citrix® Application Firewall is a high-performance, hardened security appliance that blocks all known and unknown attacks against Web and Web Services applications. Citrix Application Firewall enforces a positive security model that permits only correct application behavior, without relying on attack signatures. Application Firewall analyzes all bi-directional traffic, including SSL-encrypted communications, protecting against 16 classes of Web application vulnerabilities without any modification to applications.

Citrix Application Firewall is available as a family of purpose-built appliances that meet any deployment need, and in two software editions offering upgrade options as threats, applications and defenses become more complex. Application Firewall is deployable standalone, or in concert with Citrix® NetScaler® Application Delivery systems to deliver the combined benefits of application optimization and comprehensive protection.

ADDRESSING TODAY'S SECURITY CHALLENGES

Network-level security infrastructures such as firewalls and intrusion-prevention systems cannot defend against application-layer attacks, leaving applications and servers exposed to a myriad of known and unknown exploits. Application Firewall comprehensively addresses the challenge of delivering centralized application-layer security for all Web and Web Services applications.

THE POSITIVE SECURITY MODEL ADVANTAGE

Citrix Application Firewall enforces a positive security model to ensure correct application behavior. Instead of relying on attack signatures or pattern-matching techniques, the positive security model understands "good" application behavior, and blocks as malicious any deviation from proper application activities. It is the only proven approach delivering "zero-day" protection against unpublished exploits.

POWERFUL BUSINESS OBJECT PROTECTION

Citrix Application Firewall prevents in real time the inadvertent disclosure of sensitive application content, which could result in identity theft and fraud. Business object protection modules help to secure both predefined objects such as U.S. Social Security numbers or credit card numbers, and administratively defined data objects. By detecting erroneous disclosures and blocking or rewriting content, business object protection modules help to conform to governmental privacy regulations.



Key Benefits

PROTECTION OF SENSITIVE CONSUMER INFORMATION

Protects data behind Web infrastructure from theft of identity and bank and credit accounts.

Eliminates data losses for which government regulations require customer notification.

PROTECTS ONLINE REVENUE SOURCES

Ensures uptime of websites and Web Services by preventing Layer 7 denial of service attacks.

Application Learning ensures protection without false positives.

Maintains trust relationship between consumer and vendor by preventing cross-site scripting (XSS) attacks.

PROTECTS AGAINST BRAND EROSION

Delivers site content integrity by preventing website defacement.

TAILORING SECURITY POLICIES WITH THE CITRIX ADAPTIVE LEARNING ENGINE

Citrix Application Firewall incorporates a third-generation Adaptive Learning Engine that discovers key aspects of application behavior. Once application behavior is learned, Application Firewall generates human-readable policy recommendations, which bring to security managers a clearer understanding of actual application behavior. Tailored security policies and stringent access controls may then be applied to each application.

URL TRANSLATION AND REWRITE

Citrix Application Firewall defends against website reconnaissance with bi-directional URL translation, enabling organizations to completely hide their internal domain-naming while publishing services externally.

INDUSTRY-LEADING PERFORMANCE

Citrix Application Firewall performance exceeds that of the highest-performing Web servers, and can actually improve application performance and response time by offloading from Web servers compute- and memory-intensive TCP connection management. Application Firewall-to-server communication uses a small set of persistent TCP connections.

Dedicated silicon-based SSL hardware allows for the detection of malicious traffic within encrypted tunnels. SSL encryption and key generation offload can improve overall application performance by relieving servers from these operations. Also optional is fully encrypted communication from Application Firewall to the application servers.

An Application Firewall cluster delivers high availability and linear performance gains as the cluster grows.

CENTRALIZED SECURITY FOR ALL WEB AND WEB SERVICES APPLICATIONS

Application Firewall can secure an organization's entire Web and Web Services applications infrastructure, with complete administrative separation of application security policies, controls, reporting details and log data.

FLEXIBILITY TO ADAPT TO CHANGING BUSINESS REQUIREMENTS

Citrix Application Firewall Standard Edition offers full protection against the most common and dangerous Web application threats, high-performance security for both Web and XML Web Services applications, and full protection against data theft. It can be seamlessly upgraded to the Enterprise Edition.

Citrix Application Firewall Enterprise Edition adds advanced learning capabilities to protect against more sophisticated application attacks, provides protection against attacks that target specific user sessions (mandatory for e-commerce, secure extranet and online banking applications), and provides more granular control over application security policies.

Citrix Application Firewall is available on multiple hardware platforms to meet the performance and availability requirements of any organization — from small enterprises to large data centers. FIPS-140-2 Level 3-compliant models are also available.



KEY FEATURES

PROTECTION AGAINST 16 CLASSES OF WEB VULNERABILITIES

- Buffer Overflow
- CGI-BIN Parameter Manipulation
- Form/Hidden Field Manipulation
- Forceful Browsing
- Cookie or Session Poisoning
- Broken ACLs or Weak Passwords
- Cross-Site Scripting (XSS)
- Command Injection
- SQL Injection
- Error Triggering Sensitive Information Leak
- Insecure Use of Cryptography
- Server Misconfiguration
- Back Doors and Debug Options
- Website Defacement
- Well-known Platform Vulnerabilities
- Zero-day Exploits

COMPREHENSIVE WEB SERVER AND WEB SERVICES SECURITY

Deep Stream Inspection

- Bi-directional analysis
- HTTP & HTML header and payload inspection
- Full HTML parsing
- Semantic extraction
- Session-aware & stateful
- Protocol neutrality

HTML Form Field Protection

- Required fields returned
- No added fields allowed
- Read-only and hidden field enforcement
- Drop-down list & radio button field conformance
- Form-field max-length enforcement

Cookie Poisoning Defenses

- Ensures cookies are not modified

Forceful Browsing Protection

- Legal URL enforcement

Web Application Content Integrity

- Web site defacement protection
- *Stop Word* blocking
- *Go Word* mandates

Full SSL Offload

- Decrypts traffic prior to inspection
- Encrypts traffic prior to forwarding
- Configurable back-end encryption
- FIPS 140-2 Level 3 platforms available
- Support for client-side certificates

SIMPLIFIED MANAGEMENT AND DEPLOYMENT

User Interface

- Secure Web-based GUI
- SSH-based CLI access

Network Management

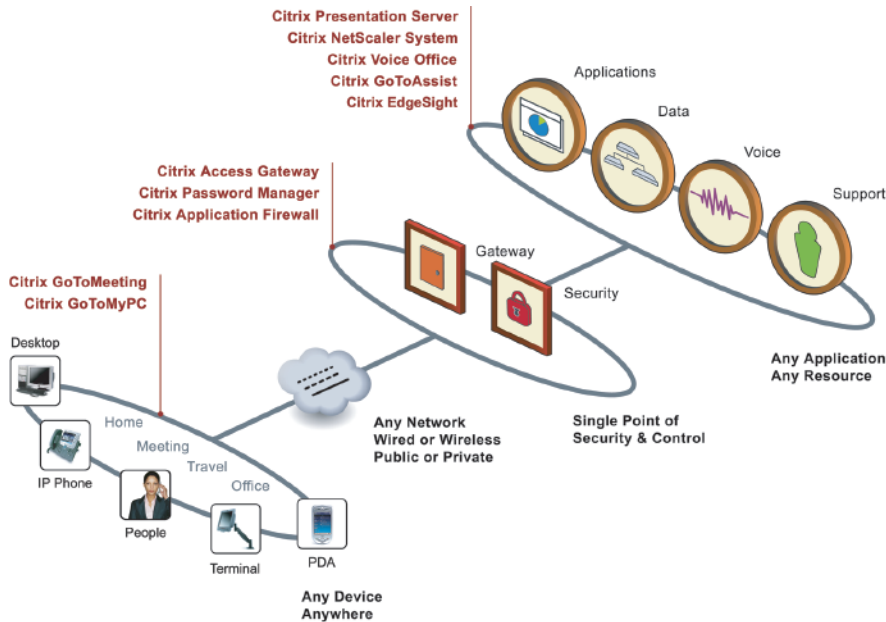
- SNMP
- Syslog-based Logging

PLATFORM SPECIFICATIONS

APPLICATION FIREWALL MODEL	7000	12000
Chassis		
Dimensions:	1.8" (4.4cm) H x 17.3" (43.8cm) W x 18.8" (47.6cm) D	3.5" (8.8cm) H x 17" (42.4cm) W x 24" (61cm) D (2U)
Weight:	28 lbs (12.7 kg)	52 lbs (23.6 kg)
Power	90-264VAC Full Range 47-63Hz, 335W	90-264VAC Full Range 47-63Hz, 500W
Interface Ports	6 x 10/100 BASE-T 2 x 10/100/1000 BASE-T	8 x 1Gbit SFP-based Copper ports 1 x 10/100 BASE-T
Operating Ranges	Temperature and Humidity 0-50C; 5%-95%	Temperature and Humidity 0-50C; 5%-95%
Certifications and Marks	Emissions: FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES Safety: TUV-C, US	Emissions: FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES Safety: TUV-C, US
Compliance	CE Mark, RoHS	CE Mark, RoHS
Warranty	1 year hardware; 90 days software; software support plans required with hardware purchase.	1 year hardware; 90 days software; software support plans required with hardware purchase.

Citrix Product Lines

Citrix products are purpose-built to solve particular access challenges as standalone solutions. When multiple products are leveraged together, they lay the foundation of a secure, flexible, and extensible access platform.



Citrix Access Gateway™ — The most cost effective and easiest to use SSL VPN, providing a secure single point of access to all applications and IT resources and delivering advanced policy based information control.

Citrix Application Firewall™ — Comprehensive, proven defense against attacks and misuse of Web Infrastructure and mission-critical information.

Citrix Application Gateway™ — The most secure, simple, and adaptable way to deliver converged voice and data applications to the screens and speakers of IP telephones.

Citrix® EdgeSight® — A leading end-user application performance management solution, monitors the performance of client-server, Web and desktop applications from an end-user perspective.

Citrix® GoToAssist™ — An industry-leading, remote technical-support solution that enables organizations to provide best-in-class support and services over the Internet, on demand and securely.

Citrix® GoToMeeting™ — The easiest, most secure, most cost-effective, and fastest way to meet, train, and collaborate online.

Citrix® GoToMyPC™ — The simplest way to provide secure, encrypted remote access to desktop-based resources.

Citrix® NetScaler® System — The most advanced way to optimize the delivery of business resources through an integrated networking solution that manages, secures and speeds application traffic.

Citrix Password Manager™ — The most secure, efficient, and easiest-to-deploy enterprise single sign-on solution for easy access to all applications with a single logon.

Citrix Presentation Server™ — The industry-standard way to virtualize the delivery of business resources through a centralized and secure architecture.



Best Access Experience. Anytime. Anywhere.

About Citrix: Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader and most trusted name in on-demand access. More than 180,000 organizations around the world rely on Citrix to provide the best possible access experience to any application for any user. Citrix customers include 100% of the *Fortune* 100 companies and 98% of the *Fortune* Global 500, as well as hundreds of thousands of small businesses and individuals. Citrix has approximately 6,200 channel and alliance partners in more than 100 countries. Citrix annual revenues in 2005 were \$909 million. Learn more at www.citrix.com.

©2006 Citrix Systems, Inc. All rights reserved. Citrix® and Citrix Access Gateway™, Citrix Application Firewall™, Citrix Application Gateway™, Citrix® GoToAssist™, Citrix® GoToMeeting™, Citrix® GoToMyPC™, Citrix® NetScaler® System, Citrix Password Manager™, Citrix Presentation Server™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and other countries. All other trademarks and registered trademarks are property of their respective owners.

31244/0906/5000

Citrix Worldwide

WORLDWIDE HEADQUARTERS

Citrix Systems, Inc.

851 West Cypress Creek Road
Fort Lauderdale, FL 33309 USA
Tel: +1 (800) 393 1888
Tel: +1 (954) 267 3000

EUROPEAN HEADQUARTERS

Citrix Systems International GmbH

Rheinweg 9
8200 Schaffhausen
Switzerland
Tel: +41 (52) 635 7700

ASIA PACIFIC HEADQUARTERS

Citrix Systems Hong Kong Ltd.

Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central
Hong Kong
Tel: +852 2100 5000

CITRIX ONLINE DIVISION

5385 Hollister Avenue
Santa Barbara, CA 93111
Tel: +1 (805) 690 6400

www.citrix.com