Citrix Web App Firewall

Citrix Web App Firewall (formerly Citrix NetScaler AppFirewall) is a comprehensive, full-function ICSA, Common Criteria, FIPS-certified web application firewall that analyzes all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats. It provides the ability to perform deep-packet inspection of HTTP, HTTPS, and XML as well as protection against OWASP Top 10. Citrix Web App Firewall threat protection includes, but is not limited, to SQL injection attack; cross-site scripting attacks; cookie tampering; form validation and protection; HTTP and XML reply and request format validation; JSON payload inspection; signature and behavior based protections; data loss prevention (DLP) support, including the monitoring of traffic for intended and unintended data exposure; DoS protection; authentication, authorization, and auditing support and reporting; and policy tools that provide for easier PCI-DSS compliance verification.

Citrix Web App Firewall technology is included in and integrated with Citrix ADC MPX and Citrix ADC VPX (formerly NetScaler ADC), Premium edition. It is available as an optional module to Citrix ADC Advanced edition. Citrix Web App Firewall is also available as a stand-alone solution on several Citrix ADC MPX appliances. The stand-alone Citrix Web App Firewall models can be upgraded via software license to a full Citrix Application Delivery Controller (ADC).

The cloud-based Citrix Web App Firewall service (formerly NetScaler Web App Security) protects customers' web applications and infrastructure from cyber security attacks.

Addressing Security Challenges

Not only are web applications vulnerable to attack, they are attractive targets for hackers because they often have direct connectivity with one or more databases containing sensitive customer and company information. Threats against web applications are often devised specifically for a target application, making threat identification by network-level security devices (e.g. intrusion protection systems and network firewalls) impossible—leaving web applications exposed to a myriad of known and zero-day exploits. Citrix Web App Firewall comprehensively addresses the challenge of delivering centralized application-layer security for all web applications and web services.

Hybrid Security Model

Citrix Web App Firewall enforces both positive and negative security models to
ensure correct application behavior. The positive security model understands good application behavior, and treats all other traffic as malicious. This is the only proven approach delivering zero-day protection against unpublished exploits. Scanning thousands of automatically updated signatures provides protection against known attacks.

Meeting PCI Compliance and Auditing Requirements

Citrix Web App Firewall aids corporate IT security teams in conforming to governmental privacy regulations and industry mandates.

For example, organizations subject to Payment Card Industry Data Security Standard (PCI-DSS) requirements can now fully meet the requirements detailed in PCIDSS Section 6.6, which mandates the installation of web application firewall in front of public-facing applications as one method of maintaining a proper security posture. In support of PCI security audits, Citrix Web App Firewall can generate dedicated reports detailing all security protections defined in the application firewall policy that pertain to PCI requirements. In addition, Citrix Web App Firewall prevents the inadvertent leakage or theft of sensitive information, such as credit card numbers or custom-defined data objects, by either removing or masking content from application responses—before being publicly disclosed.

Defeating XML-based Threats

In addition to detecting and blocking common application threats that can be adapted for attacking XML-based applications (i.e. cross-site scripting, command injection, etc.), Citrix Web App Firewall includes a rich set of XML-specific security protections. These include schema validation to thoroughly verify SOAP messages and XML payloads, and a powerful XML attachment check to block attachments containing malicious executables or viruses. Automatic traffic inspection methods block XPath injection attacks on URLs and forms aimed at gaining access. Citrix Web App Firewall also thwarts a variety of DoS attacks, including external entity references, recursive expansion, excessive nesting, and malicious messages containing either long or a large number of attributes and elements.

Tailoring Security Policies

Citrix Web App Firewall incorporates an advanced and proven adaptive learning engine that discovers aspects of application behavior that might be blocked by the positive security model even if the behavior is intended by the web application. This would include, for example, modifications made by client-side application scripting that legally modify HTML form fields. Once application behavior is learned, Citrix Web App Firewall generates human-readable policy recommendations, which bring to security managers a clearer understanding of actual application behavior. Tailored security policies may then be applied to each application.

Industry-leading Performance

Citrix Web App Firewall provides high capacity application security throughput to meet the needs of even the largest networks. In addition, the solution can actually improve application performance and lower response times by offloading compute-intensive tasks, such as TCP connection management, SSL encryption, and compression from web servers. In addition, the integrated caching functionality available on the platform offloads the servers while still applying
full firewall functionality. Freeing valuable server resources improves the overall application experience.

**IP Reputation Service is Built-In**

The IP reputation feature is built into the platform. This feature is available at no extra cost with the Citrix Web App Firewall solution. No service contract, no yearly renewals necessary.

IP reputation provides a continuously updated list of malicious IP addresses in near real-time, providing an additional layer of protection and helping to reduce the burden on security teams. Rather than relying on static, rapidly out-of-date public black lists, IP reputation automatically analyzes and correlates feeds from millions of global sensors in real-time.

**Flexibility to Adapt to Changing Business Requirements**

Citrix Web App Firewall permits flexible, stepwise deployment of web application protection. The default web application protection profile defends against the most common dangerous threats and adds full protection against both data theft and layer 4-7 denial of service (DoS) attacks. The advanced web application protection profile adds session-aware protections to protect dynamic elements, such as cookies, form fields, and session-specific URLs. Attacks that target the trust between the client and server including cross-site request forgery are stopped; requests are validated by checking for a unique ID inserted by Citrix. Such protection is imperative for any application that processes user-specific content, such as an e-commerce site. To make sure these security measures are compatible with any application, Citrix Web App Firewall learning capabilities help the administrator create managed exceptions and relaxations when the application’s intended—and legal—behavior might otherwise cause a violation of the default security policy.

**Cloud-Based Citrix Web App Firewall**

The cloud-based Citrix Web App Firewall service protects customers’ web applications and infrastructure from application and network level attacks. It has historical retention capabilities for easy operation and incident analysis. Features include:

- **Comprehensive Security**: Protection against web application attacks using signatures, blacklisted and whitelisted URLs/applications, IP Reputation, etc, and helps maintain compliance
- **Fast Deployment**: Click & Protect with cloud-based Citrix Web App Firewall – less than 5 clicks from first time login to protection
- **Ease of Use**: Quick and easy to deploy, manage, and create reports using a simplified GUI
Technical aspects

Protects Online Revenue Sources

• Buffer overflow
• CGI-BIN parameter manipulation
• Form/hidden field manipulation
• Forceful browsing protection
• Cookie or session poisoning
• Cross-site scripting (XSS)
• Cross-site request forgery
• Command injection
• SQL injection
• Error triggering sensitive information leak
• Insecure use of cryptography
• Server misconfiguration
• Back doors and debug options
• Rate-based policy enforcement
• Well-known platform vulnerabilities
• SOAP array attack protection
• Content rewrite and response control
• Content Filtering
• Authentication, authorizing and auditing
• L4-7 DoS protection

Simplified Management and Deployment User Interface

• Secure web-based GUI
• SSH-based CLI access network management
• SNMP
• Syslog-based logging
• PCI-DSS compliance reporting tool
• AppExpert Templates for Web Interface and Microsoft SharePoint
• Import/export Application Firewall profiles
• Convert third party application vulnerability tool output to Citrix rules
• Quick deployment of new rules from Common Event Format (CEF) logs

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 and stateful
• HTTP Signature scanning
• Scan thousands of signatures
• Response side checks
• 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 protection – Signatures to prevent tampering; cookie encryption and proxying
  • Legal URL enforcement – Web application content integrity
• Full SSL offload:
  • Decrypts traffic prior to inspection; encrypts traffic prior to forwarding
  • Configurable back-end encryption
  • Support for client-side certificates
• XML data protection:
  • XML security: protects against XML denial of service (xDoS), XML SQL and Xpath injection and cross site scripting
  • XML message and schema validation, format checks, WS-I basic profile compliance, XML attachments check
• URL transformation
• WSDL scan prevention to protect unpublished APIs
• Support for Chunked POST requests