

Citrix NetScaler Application Firewall



Citrix® NetScaler AppFirewall™ is a comprehensive ICSA certified web application security solution that blocks known and unknown attacks against web and web services applications. NetScaler AppFirewall enforces a hybrid security model that permits only correct application behavior and efficiently scans and protects known application vulnerabilities. It analyzes all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats without any modification to applications.

NetScaler AppFirewall technology is included in and integrated with Citrix® NetScaler® MPX and VPX, Platinum Edition, and is available as an optional module that can be added to NetScaler MPX appliances running NetScaler Enterprise Edition. NetScaler AppFirewall is also available as a stand-alone solution on seven NetScaler MPX appliances. The stand-alone NetScaler AppFirewall models can be upgraded via software license to a full NetScaler Application Delivery Controller (ADC).

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. NetScaler AppFirewall comprehensively addresses the challenge of delivering centralized application-layer security for all web applications and web services.

Hybrid security model

NetScaler AppFirewall 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 This is the only proven approach delivering zero-day protection against unpublished exploits.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 of thousands of automatically updated signatures provides protection against known attacks.

Meeting PCI compliance and auditing requirements

NetScaler AppFirewall 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 PCI-DSS 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, NetScaler AppFirewall can generate dedicated reports detailing all security protections defined in the application firewall policy that pertain to PCI requirements. In addition, NetScaler AppFirewall 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.

Delivers PCI-DSS v.3.0 compliance

- Protects credit and debit card account numbers to comply with the Payment Card Industry Data Security Standards.
- Prevents data losses for which government regulations require customer notification.
- Simplifies desktop management.

Protects online revenue sources

- Ensures uptime of web sites and web services by defeating L7 denial of service (DoS) attacks.
- Application learning ensures protection without false positives.
- Maintains trust relationship between consumer and vendor by preventing cross-site scripting (XSS) and cross-site forgery attacks.

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.), NetScaler AppFirewall 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. NetScaler AppFirewall 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

NetScaler AppFirewall 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 modifies HTML form fields. Once application behavior is learned, NetScaler AppFirewall 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

NetScaler AppFirewall 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 NetScaler platform offloads the servers while still applying full firewall functionality. Freeing valuable server resources improves the overall application experience.

Flexibility to adapt to changing business requirements

NetScaler AppFirewall 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 NetScaler. 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, NetScaler AppFirewall 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.

NetScaler AppFirewall Model	MPX 5550	MPX 5650	MPX 8005	MPX 11515
Platform attributes				
Processor	Intel E3-1225	Intel E3-1275	Intel E3-1275	Dual Intel Xeon E5645
Memory	8 GB	8 GB	32 GB	48 GB
Ethernet ports	6x10/100/1000 BASE-T	6x10/100/1000 BASE-T	6x10/100/1000 BASE-T and 6x1000BASE-T SFP Or 6x10/100/1000 BASE-T and 2x10G BASE-X SFP+	8x10G BASE-X SFP+ and 4x1000 BASE-X SFP
Upgrade Option	Upgrade option to MPX 5650			Upgrade option to MPX 11520/11540
Platform performance				
Throughput Basic mode (Mbps)	500	5,300	5,400	14,000
SSL Throughput (Mbps)	500	2,000	4,000	14,000
SSL transactions/second	1,500	2,800	6,500	22,500
Platform mechanical, environmental and regulatory				
Power supplies	Single	Single	Single-Optional Second	Dual
Height	1U	1U	1U	2U
NetScaler AppFirewall Model	MPX 11520	MPX 11540		
Platform attributes				
Processor	Dual Intel Xeon E5645	Dual Intel Xeon E5645		
Memory	48 GB	48 GB		
Ethernet ports	8x10G BASE-X SFP+ and 4x1000 BASE-X SFP	8x10G BASE-X SFP+ and 4x1000 BASE-X SFP		
Software upgrade	Upgrade option to MPX 11540			
Platform performance				
Throughput Basic mode (Mbps)	17,000	20,000		
SSL Throughput (Mbps)	15,000	19,000		
SSL transactions/second	25,000	43,000		
Platform mechanical, environmental and regulatory				
Power supplies	Dual	Dual		
Height	2U	2U		

Note: The above models are available as stand-alone NetScaler AppFirewall solutions. Additional application firewall support is provided as an integrated module within NetScaler VPX 10, 200, 1000 and 3000 virtual appliances and all NetScaler MPX Application Delivery Controller (ADC) hardware platforms.

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 NetScaler 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



About Citrix

Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud infrastructure to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of \$2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.

Copyright © 2014 Citrix Systems, Inc. All rights reserved. Citrix, XenDesktop, Citrix Application Firewall, Netscaler Clustering, ICA, HDX Insight, FlexCast, Citrix Receiver, CloudBridge, NetScaler, NetScaler Gateway, NetScaler CloudConnector, TriScale, AppCache, AppCompress, XenApp, XenMobile, AppFlow, EdgeSight, NetScaler MPX, NetScaler SDX, NetScaler VPX, HDX and AppCache are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.