CITRIX®

Benefits of integrated web application security

CITRIX®

Introduction

Application layer attacks are epidemic. According to the CSI/FBI Computer Crime and Security Survey 2009, 92 percent of businesses have suffered from a successful application attack in the previous 12 months. Even worse, according to the Symantec State of Enterprise Security Report 2010, 75 percent of enterprises surveyed experienced some form of cyber attack in 2009.

To combat the attacks and the potential for data loss, web applications must have active protection—similar to the way networks must be actively protected by IDS, IPS and stateful firewalls. In addition to preventing attacks, the effectiveness of a modern application delivery solution also depends on its ability to deliver performance, reliability and lower cost of ownership. Application deliver controllers (ADCs) provide the capabilities necessary to accelerate, optimize and secure web applications and web services.

Application delivery, an imperative for organizations, involves a flexible set of services that can efficiently accommodate changing application and user variables while consistently ensuring the highest levels of performance, security and availability, and lower total cost of ownership. In contrast to conventional approaches to application management, application delivery bridges the gap between traditional networks and modern applications, thereby avoiding the need to continuously add resources or hard code changes to underlying components and systems as high-level business requirements evolve.

This paper clarifies the specific security abilities that an ideal web application delivery solution should exhibit. It also highlights the significant advantages of the tightly integrated security module of Citrix® NetScaler®.

The application delivery imperative

Applications are crucial to business success. The level of dependency on these tools of automation has steadily risen over the past decade and this trend will continue. Several trends affect IT's ability to maintain the accessibility, performance and, thus, overall usefulness of these applications to their users. The rise of cloud computing has extended the web application model, breaking the traditional security model by providing multi-tenancy on shared equipment and services. Mobility, globalization and off-shoring are moving users further away from headquarters, while datacenter consolidation, security and regulatory compliance are driving centralization of information resources, often introducing barriers that make the associated applications less accessible.

Compounding matters are an increasing reliance on web applications and other technologies which are notoriously insecure and performance-challenged, and rising expectations among users and business managers. Transactions must be executed nearly instantaneously. When faced with changing business requirements, IT needs to be able to roll-out new applications very quickly. Cloud computing providers often cite these quick response time benefits and they rely on fast results even more than traditional enterprises.

Addressing these challenges with traditional networking, security and management solutions is insufficient. They lack the application awareness needed to compensate for a network infrastructure not designed with modern applications in mind. Network firewalls are tuned to the specific needs of networking. Web application firewalls are tuned to meet the specific needs of dynamic web applications.

Security requirements for application delivery

Application delivery requires security that is robust, adaptable and comprehensive. Organizations have done a relatively good job with network security. Confronted with reasonably strong defenses at the network layer, hackers have resorted to attacking weaknesses at higher layers of the computing stack.

An even bigger factor has been a shift in attacker motivation. Rather than attempting to gain notoriety, attackers now focus squarely on obtaining valuable information including passwords, credit card details and Social Security numbers, and the resulting financial rewards. The greater emphasis being placed on application-layer attacks corresponds to the fact that applications are a direct and convenient conduit to this type of data.

Application Security

Organizations should make a corresponding shift in their security strategies and architectures. The consensus of leading security experts and regulators is that more attention needs to be paid to establishing robust, application-layer defenses. In no case is this need greater than for web applications. Not only are web applications exceedingly vulnerable, but they are also the primary vehicle for e-commerce and customer portals and a front door to potentially lucrative data. The net result is that web applications are now a favored target of hackers everywhere.

- More than 80 percent of the 2,652 total vulnerabilities reported for commercial applications in the second half of 2009 were attributed to web applications and related technologies (source: Cenzic Web Application Security Trends Report – Q3-Q4, 2009, Cenzic Inc.)
- Of the top-attacked vulnerabilities that Symantec observed in 2009, four of the top five being exploited were client-side vulnerabilities that were frequently targeted by web-based attacks. (Source: Symantec State of Enterprise Security Report 2010)
- Attacks against web applications constitute more than 60 percent of the total attack attempts observed on the Internet (source: SANS Institute, Top Security Risks, September 2009, http://www.sans.org/top-cyber-security-risks/)

- Over 90 percent of enterprise proprietary web applications analyzed had serious vulnerabilities that could potentially lead to the exposure of sensitive confidential user information during transactions (source: Cenzic Web Application Security Trends Report – Q3-Q4, 2009, Cenzic Inc.)

IT compliance regulations also require better protection for applications. Most of the applicable regulations and legislation, including the Payment Card Industry Data Security Standard (PCI-DSS), implicitly require application-specific countermeasures as part of a "comprehensive information security program".

PCI-DSS and application security

The Payment Card Industry Data Security Standard applies to merchants, financial institutions and other entities that store, process or transmit the Primary Account Numbers associated with credit cards from several leading payment brands (e.g., Visa, MasterCard and American Express). Particularly relevant is Requirement 6 of the standard, which calls for subject organizations to "develop and maintain secure systems and applications." Even more specific is Section 6, which states that web facing applications should be protected by installing an application-layer firewall in front of them, or by having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security.

Network and system level protection

Placing greater emphasis on application-layer security is warranted given the current threat environment. This does not alleviate the need to provide comprehensive network-level protection, typically by taking advantage of a solution's native capabilities in combination with complementary, standalone network security gateways (e.g., firewalls, virtual private networks and intrusion prevention systems). In addition, individual application delivery components should be self-defending as a result of including a range of system-level protection mechanisms.

The Citrix NetScaler Solution

It is estimated that 75 percent of all Internet traffic traverses a Citrix NetScaler system every day. This can be attributed to granular L4-7 visibility into application requests and responses, a cornerstone of the solution's ability to accelerate applications, improve their availability and enhance security. NetScaler provides for security in both the MPX physical appliances and VPX virtual appliances in configurations that enable acceleration, optimization and security.

A robust web application firewall

Network firewalls are simply not up to the task of securing web applications. In general, they do not understand the inner workings of protocols and languages such as HTML and XML; they do not understand HTTP sessions; they cannot validate user inputs to an HTML application; they cannot filter or obfuscate sensitive data included in server responses; they cannot detect maliciously modified parameters in a URL request; and they are not capable of inspecting SSL-encrypted traffic. Most importantly, network firewalls do not understand session data, which is used to maintain state in the otherwise stateless HTTP protocol. It is because of these shortcomings that the PCI Data Security Standard calls for the use of web application firewalls and that a full-featured web application firewall—whether embedded or implemented as a standalone system—should be considered an essential component of a complete web application delivery solution. It is equally essential that such a firewall be robust. Like NetScaler Application Firewall™, it should include the following core capabilities to ensure that it provides a superior degree of application-layer security:

- **Deep inspection** – The incorporated inspection technology should be capable of reconstructing all bi-directional communications, including SSL-encrypted traffic, to ensure correct application behavior and the validity of user machine inputs. Related functions include: bi-directional parsing and analysis of all application traffic; complete header and payload inspection; semantic extraction of relevant objects; and sessionization (i.e., the maintenance of session state despite the use of stateless web protocols).
- **A comprehensive security model** – Utilizing a hybrid (whitelist and blacklist) security model, NetScaler can enforce positive security and thwart attacks associated with negative security. Positive security entails enforcing industry standards (e.g., for HTTP) and coding best practices (e.g., for HTML and Java) to block traffic that is not consistent with good application behavior. The result is a proven measure of protection against zero-day attacks; complemented by threat signatures and correlation techniques that identify and block specific attack measures.
- **Protection for infrastructure and users** – To protect against the most common web application exploits, namely buffer overflows, SQL injection, cross-site scripting and cross-site request forgery, a web application firewall must provide security not just for the components that comprise application infrastructure (e.g., servers, operating systems, databases and application programs), but for the trust relationship between users and these components as well.
- **XML protection** – As service oriented architectures and Web 2.0 initiatives proliferate, enterprises need to provide protection not just for HTML-based applications but also for applications that rely on XML and associated web services technologies. XML is subject to many of the attacks previously mentioned including SQL injection, cross-site scripting and many more that can be adapted to attack XML-based applications. In addition to detecting and blocking these common application threats, NetScaler Application Firewall includes a rich set of XML-specific security protections and secures all flavors of XML. 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. Advanced XML protections include WSDL scanning prevention and blocking of XPath injection attacks.
- **Adaptive learning** – Web applications are unique in both their design and their protective requirements. To provide for comprehensive application protection, adaptive learning establishes and maintains a highly specific mapping of normal-good behavior, including expected-valid inputs, tuned to the application. This effectively amplifies the power of each of the three previous capabilities; helps improve the ability to protect dynamic applications such as those utilizing client-side JavaScript; and reduces the likelihood of mistakenly blocking benign traffic by establishing fuller context and a better semantic understanding of all application states, transactions and associated data. A robust web application firewall should support both global and per-application security rules. This helps ensure that consistent yet appropriate defenses and policy are established across all applications.

- **Multi-layer cloaking** – This feature thwarts a hacker's ability to conduct reconnaissance and thus devise an effective strategy for exploiting established vulnerabilities or finding new ones. It eliminates or otherwise masks the transmission of potentially sensitive information about the components that comprise the application environment. Representative functionality includes removal-replacement of all unnecessary server response headers; re-writing of internal URLs; removal of HTML comments; MAC address shielding; and encryption of elements such as hidden form fields and cookie names and values.
- **Prevention of data leakage** – A prudent last line of defense against attacks targeting sensitive customer or corporate data is to actively guard against the leakage of this type of information in server responses. Related functions include inspecting the entire data stream (not just HTTP headers); ensuring precision when matching data objects (e.g., by correlating content with context); and providing an option to transform matching data objects, as opposed to simply blocking them. Data leakage capabilities extend to protect Payment Card Industry credit card numbers, U.S. Social Security numbers and defined organizational data. The HTTP callout feature extends data leakage protection to integrate third-party solutions, such as DLP.

These are just the core security capabilities that form the foundation of a robust web application firewall. For other relevant security features, as well as requisite management capabilities, readers are encouraged to review the materials posted at www.citrix.com, or contact a Citrix representative.

The advantages of an integrated solution

Deploying standalone web application firewall systems is possible and may even be appropriate under certain circumstances, for example, because of placement in the network, budget constraints, performance or capacity requirements, or politics pertaining to ownership and management responsibilities. Citrix offers a range of dedicated hardware-based web application firewalls with secure throughput supported from 500 Mbps to over 5 Gbps. These models offer scalable Pay-as-You-Grow options to boost performance through a simple license upgrade.

However, consideration should be given to the numerous advantages associated with operating NetScaler Application Firewall as a seamlessly integrated component of the NetScaler web application delivery solution. Citrix offers application delivery controllers with complete application firewall support that provide up to 12 Gbps of secure application firewall throughput. In addition, NetScaler VPX virtual appliance models offer the ultimate in on-demand support. VPX allows an IT administrator to spin up additional application firewall instances on-the-fly that can be configured to tailored settings for individual applications and pools of specific users.

Constructive consolidation

One of the more obvious advantages of a combined solution is achieving a measure of infrastructure consolidation. In this way, all of the key application delivery functional objectives—performance, availability and security—are provided in a single platform, thereby alleviating the need to deploy separate devices (and potentially a second set of load balancers to front-end the web application firewalls). The result is an effective reduction in infrastructure complexity, and lower total cost of ownership due to lower capital and operational expenditures.

Enhanced efficiency and performance, and improved effectiveness

In its most basic form, an application delivery controller yields benefits derived chiefly from reductions in physical complexity, i.e., fewer boxes to purchase, incorporate in the network and maintain. However, as with NetScaler Application Firewall and the full NetScaler ADC, consolidation that emphasizes logical integration can add other significant advantages.

First, there is the benefit achieved by not having to repeat core processes multiple times, once for each separate device. Conducting cryptographic operations and other packet-level functions—such as connection handling, header inspections, positive model enforcement and denial-of-service prevention—only once significantly reduces not only the aggregate resource requirements but also the latency introduced to the applications that are being delivered.

Next is the operational benefit of being able to set security policies in the same way and at the same time that other application delivery policies are being configured. The intuitive AppExpert Visual Policy Builder, a key feature of NetScaler, enables all application delivery policies to be created without the need for coding complex programs or scripts.

Finally, there is the architectural benefit of not having to wrestle with separate devices for different parts of the application delivery solution. Potential conflicts or overlapping capabilities are avoided, as are compatibility problems that may arise when using products from multiple vendors.

A proven, highly capable platform

Its strong presence and continued success in the market are evidence that NetScaler is a highly capable platform. NetScaler has been architected to be a high-performance, high-capacity system, as detailed below:

- **A purpose-built system** – The NetScaler OS is based upon the FreeBSD operating system for management familiarity, security hardening and extensibility. NetScaler takes complete control over memory management, process timing and network access. This enables extensive optimization of the interactions that occur between its various processes and subsystems. NetScaler Application Firewall is supported to 12 Gbps on the higher-end of the NetScaler MPX series of ADCs.

- **A customized TCP/IP stack** – Control over the system scheduler is also instrumental in maximizing the benefits of a highly customized TCP/IP stack. Extremely efficient packet processing is made possible by having scheduled states (versus interrupt-based transitions) and being able to eliminate numerous, intermediate packet queues. Other stack optimizations yield superior connection-handling capabilities (e.g., consistently fast lookup times regardless of connection volume) and enable Request Switching, a TCP/HTTP connection multiplexing feature that significantly reduces the load on downstream application servers. The customized NetScaler TCP stack prevents Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks against protected backend servers.
- **Hardware-optimized SSL and FIPS** – NetScaler MPX leverages hardware-accelerated SSL modules from Cavium and FIPS-enabled models incorporate Cavium FIPS cards.
- **Hardware-independence with VPX** – NetScaler VPX is a software-based virtual appliance that runs on off-the-shelf hardware and the most popular server hypervisor platforms (XenServer, Hyper-V and ESX).
- **Integrated authentication and authorization** – NetScaler includes the ability to integrate with RADIUS, LDAP, TACACS+, Active Directory and other authentication and authorization directory services.
- **Integrated SSL VPN** – Select NetScaler versions include Citrix® Access Gateway™ SSL VPN capabilities for secure remote access. Support for Perl-Compatible Regular Expressions ensures that administration rights can be configured not just on the basis of roles and functions or commands, but also on the basis of the entities upon which the functions are intended to operate.
- **System level ACLs and AppExpert** – Access to NetScaler management addresses can be controlled via configurable, default-enabled, system-level ACLs. Rules can be based on typical network-level parameters, including source-destination IP address or TCP port, protocol and source MAC address. The included AppExpert functionality provides templates and resources for simplifying the configuration and management of complex web applications.
- **Multi-layer networking code** – This refers to the ability of the system-level ACLs to effectively act as a gatekeeper to the deeper-level, FreeBSD management functions.
- **Accounting** – Robust logging, optionally to an external server, provides an invaluable and preserved audit trail for administrative activities and system-level events.

Application Firewall operates as an integrated component of the NetScaler system, with all of these capabilities and their benefits operating in concert for comprehensive application acceleration, optimization and protection.

Summary

Organizations are deploying new cloud and web applications, and continuing to support legacy web applications. The need to address a myriad of ongoing trends that threaten mission-critical applications by negatively impacting their performance and accessibility makes the deployment of application delivery solutions a necessity. At the same time, prevailing conditions in risk and regulatory environments require strategic countermeasures such as web application firewalls to establish substantially greater degrees of application-layer security.

Organizations have choices in how to implement these requirements. Using multiple, standalone devices is one path and it may even be warranted under certain circumstances. In general, however, a better option is to take advantage of NetScaler Application Firewall as a seamlessly integrated component of the NetScaler application delivery solution. Its complementary web application firewall capabilities enhance the NetScaler solution at the same time that the firewall benefits from the performance, reliability and network-system-level security capabilities that make NetScaler a market-leading platform for application delivery. The result is better overall application performance along with significantly reduced complexity and cost of ownership. With these flexible Citrix solutions, standalone application firewalls may be upgraded via a software license to full NetScaler application delivery solutions when needed; this applies to either the MPX built-for-purpose physical appliances or the VPX virtual appliances.

Worldwide Headquarters
Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309, USA
T +1 800 393 1888
T +1 954 267 3000

www.citrix.com

Americas
Citrix Silicon Valley
4988 Great America Parkway
Santa Clara, CA 95054, USA
T +1 408 790 8000

Europe
Citrix Systems International GmbH
Rheinweg 9
8200 Schaffhausen, Switzerland
T +41 52 635 7700

Asia Pacific
Citrix Systems Hong Kong Ltd.
Suite 6301-10, 63rd Floor
One Island East
18 Westlands Road
Island East, Hong Kong, China
T +852 2100 5000

Citrix Online Division
6500 Hollister Avenue
Goleta, CA 93117, USA
T +1 805 690 6400

About Citrix
Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking, and cloud computing technologies into a full portfolio of products that enable virtual workstyles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2009 was $1.61 billion.

0910