



Benefits of integrated Web application security



Table of contents

Introduction

The application delivery imperative

Security requirements for application delivery

Application security	4
Network and system level protection	5
Network-based does not equal network-focused	5

The Citrix NetScaler solution

A robust Web application firewall

The advantages of an integrated solution

Constructive consolidation	7
Enhanced efficiency, performance, and improved effectiveness	7
A proven, highly capable platform	7

Summary

Introduction

One of the greatest challenges confronting today's enterprises is a major shift in the threat profile, as network-layer exploits are rapidly being surpassed by more formidable attacks against applications. This is especially true for Web and Web Services applications. Consequently, the effectiveness of a modern application delivery solution depends not only its ability to deliver in the areas of performance, reliability, and cost of ownership, but on its application-layer security capabilities as well.

This paper clarifies the specific security capabilities that an ideal web application delivery solution should exhibit. It also highlights the significant advantages derived from making the associated functionality available as a tightly integrated module of the Citrix® NetScaler® Web application delivery solution.

The application delivery imperative

These days there is little doubt that applications are crucial to business success. Even to a casual observer, it should be clear that the level of dependency on these "tools of automation" has steadily risen over the past decade. And there is no reason to expect this trend will do anything but continue.

However, other trends are having a profound effect on IT's ability to maintain the accessibility, performance and, thus, overall usefulness of these applications to their end users. Mobility, globalization, and offshoring are moving users further away from headquarters, while datacenter consolidation, security, and regulatory compliance are driving centralization of information resources, often introducing barriers that render the associated applications less accessible.

Compounding matters even further are: (a) an increasing reliance on web applications and technologies — which are notoriously insecure and performance-challenged to begin with; and (b) rising expectations among users and business managers alike. Whether it's how fast the system responds when a transaction is executed or how quickly IT is able to roll out new applications to account for changing business requirements, anything shy of "immediate" is unacceptable.

Furthermore, addressing these challenges with traditional networking, security, and management solutions is highly impractical. They simply lack the requisite application awareness to compensate for a network infrastructure that was typically not designed with modern applications in mind. As a result, enterprises will inevitably find themselves continuously needing to upgrade and/or massively over-provision their computing environment.

These are the main reasons why application delivery has risen in prominence and essentially become an imperative for today's organizations. Application delivery 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 — not to mention lower total cost of ownership. In contrast to conventional approaches, 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.

Security requirements for application delivery

As indicated above, among the cornerstones of application delivery are security services that are robust yet adaptable. It is particularly important that these services be comprehensive. An ideal solution should account for application security, in addition to more commonly expected network- and system-level protection capabilities.

Application security

In just the past couple of years the need to more directly and specifically protect applications has increased dramatically. This is a natural consequence of organizations doing a relatively good job with network security. Confronted by reasonably strong defenses at the network layer, hackers have resorted to architecting exploits that take advantage of weaknesses at higher layers of the computing stack.

An even bigger factor has been a shift in hacker motivation. Rather than attempting to gain notoriety, they now focus squarely on making money, for example, by obtaining valuable information including passwords, credit card details, and Social Security numbers. The greater emphasis being placed on application-layer attacks corresponds to the fact that applications are a direct and therefore convenient conduit to this type of data. Just as the infamous Willy Sutton robbed banks “cause that’s where the money is,” hackers are now attacking applications because that is where the data is.

The implication is that enterprises should be making a corresponding shift in their security strategies and architectures. Indeed, the consensus of leading security experts and consultants over the past few years is that more attention needs to be paid to establishing robust, application-layer defenses. And 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, therefore, as a “front door” to all sorts of potentially lucrative data. The net result is that Web applications are now a favored target of hackers everywhere. Just consider the following handful of statistics which dramatically demonstrate the scope of the current situation:

- 61% of the 2,461 vulnerabilities documented in the first half of 2007 were attributed to Web applications, and 79% were designated as “easy to exploit” (source: Symantec Internet Security Threat Report, Volume XII, Sep 2007)
- White Hat Security indicates that greater than 85% of evaluated websites are susceptible to cross-site scripting attacks
- Gartner estimates that 75% of all attacks are now aimed at Web applications

Of course, IT compliance requirements are another significant contributor to the need to provide better protection for applications. Most of the applicable regulations and legislation, at a minimum, implicitly require application-specific countermeasures as part of the “comprehensive information security program” that they mandate. Others, including the Payment Card Industry Data Security Standard (PCI-DSS), leave little doubt with regard to what is expected (see sidebar).

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 of the requirement, which indicates: (a) 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; and (b) that this guidance should be considered a best practice until June 30, 2008, after which it becomes a requirement.

Network and system level protection

Placing greater emphasis on application-layer security is certainly warranted given the current threat environment. By no means, however, does this 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.

Network-based does not equal network-focused

Another relevant point is that just because a component takes the form of an inline, network appliance does not mean that it is limited to providing network-level security. Being network-based is merely a mode of deployment — albeit one that typically affords a number of advantages, such as greater coverage per unit, easier separation of duties, and advanced performance and security capabilities that are made possible by a purpose-built platform. It does not mean that the services running on such a platform are incapable of having a high degree of application visibility and control. In fact, being network-based and application-focused is not only possible, but should be viewed as the ideal. This is the very combination that enables the network to take action based on application behavior. It is the very combination that enables an application delivery solution to effectively bridge the gap between networks and applications. In contrast, network-based solutions that are only network-focused merely contribute to making networks rigid and inflexible and, therefore, unable to adapt to rapidly changing application requirements and associated business needs.

The Citrix NetScaler solution

The Citrix NetScaler application delivery system has already achieved tremendous success in the market. It is used by 8 out of the 10 largest websites. With more than 7,000 NetScaler deployments worldwide it is little wonder that the traffic from 75% of all Internet users ultimately crosses a NetScaler system. This success can be attributed in no small part 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 their security.

Citrix nonetheless recognizes the mounting need for even greater degrees of application security and continues to increase its application security functionality. Specifically, starting with Version 8 of the NetScaler application delivery solution, the Citrix Application Firewall™ became available as an integrated module. NetScaler customers now have the opportunity to provision state-of-the-art protection from application threats that bypass traditional security measures, without the need to deploy separate devices.

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/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. It is specifically because

of these shortcomings that the PCI Data Security Standard calls for the use of Web application firewalls. And it is specifically because of these shortcomings 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.

Moreover, it is equally essential that such a firewall be robust. Like the Citrix Application Firewall, it should include the following core capabilities to ensure it provides a superior degree of application-layer security:

- **Comprehensive 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 web protocols, Which are effectively stateless).
- **A positive security model.** This 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; whereas threat signatures and correlation techniques are largely incapable of thwarting them.
- **Protection for infrastructure and users.** In order to protect against the most common Web application exploits, namely buffer overflows, SQL injection, and cross-site scripting, 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.
- **Adaptive learning.** Out-of-the-box protective capabilities can only go so far. In contrast, adaptive learning involves establishing and maintaining a highly specific mapping of normal/good behavior, including expected/valid inputs, for any given application. This effectively: (a) amplifies the power of each of the three previous capabilities; (b) helps improve the ability to protect dynamic applications, such as those utilizing client-side JavaScript; and (c) 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. Notably, this also implies the presence of another closely related capability. Specifically, a robust Web application firewall should support both global and per-application security rules. This helps ensure that consistent yet appropriate defenses are established across all applications.
- **Multi-layer cloaking.** The goal of this capability is to thwart a hacker’s ability to conduct reconnaissance and thus devise an effective strategy for exploiting established vulnerabilities, or perhaps finding new ones. It entails eliminating or otherwise masking 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.

To reiterate, 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

Having established the need for a Web application firewall and the key capabilities that define this critical countermeasure, our next task is to explore the mode in which it is implemented. Deploying standalone Web application firewall systems is certainly possible. It may even be appropriate under certain circumstances, for example, because of budget constraints, performance/capacity requirements, or politics pertaining to ownership and management responsibilities. However, consideration should be given to the numerous advantages associated with operating the Citrix Application Firewall as a seamlessly integrated component of the NetScaler Web application delivery solution.

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 via 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, as well as lower total cost of ownership due to lower capital and operational expenditures.

Enhanced efficiency, performance, and improved effectiveness

In its most basic form, consolidation yields benefits derived chiefly from reductions in physical complexity, i.e., fewer “boxes” to purchase, incorporate in the network, and maintain. However, as with the Citrix Application Firewall and NetScaler, 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 there 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 can simply be avoided in the first place, as can compatibility problems that are bound to 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.

For instance, from the outset the NetScaler has been architected to be a high-performance, high-capacity system, as described below:

- **A purpose-built system.** Although it is based upon the FreeBSD operating system, the NetScaler system 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.
- **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.
- **Custom/dedicated silicon.** Commercially available ASICs are employed for subsystems that require additional computational power (e.g., SSL).

In a similar manner, NetScaler has been designed with an emphasis on security and, consequently, is a self-protecting system. Associated features include:

- **A purpose-built operating system.** All extraneous services have been removed and any traditionally “weak” ones that remain have been hardened or replaced.
- **A customized TCP/IP stack.** A positive security model is adhered to for packet processing. Consequently, traffic that deviates from specified/common guidelines for packet formation and content — a condition often indicative of a threat — is dropped. In addition: leakage of low-level information is avoided by zeroing the unused portions of reused packets; connection handling routines have been modified to mitigate related threats (e.g., Rose, Fragment, and TCP TIME_WAIT attacks); and, hardware support for handling small packets mitigates a range of others (e.g., SYN, ACK, ICMP, and DNS flood attacks).
- **System level ACLs.** 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.
- **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.
- **Authentication and authorization.** In addition to ACLs, the system is protected by a range of supported authentication mechanisms (e.g., RADIUS, TACACS+, LDAP), as well as a highly flexible authorization capability. Support for Perl-Compatible Regular Expressions ensures that administration rights can be configured not just on the basis of roles and functions/commands, but also on the basis of the entities upon which the functions are intended to operate.
- **Encrypted communications.** All management and inter-system communications can optionally be encrypted.
- **Accounting.** Robust logging, optionally to an external server, provides an invaluable and preservable audit trail for administrator activities and system-level events.

The important point here is not really the scope of these features — although that is certainly relevant. Instead, it is the fact that because the Web Application Firewall operates as an integrated component of the NetScaler system, all of these capabilities and their benefits are conveyed to it as well.

Summary

Organizations are rapidly running out of options. The need to address a host of ongoing trends that are diminishing the usefulness of mission-critical applications by negatively impacting their performance and accessibility is effectively making the deployment of application delivery solutions a necessity — not a choice. At the same time prevailing conditions in the threat and regulatory environments are essentially forcing investment in countermeasures such as Web application firewalls to establish substantially greater degrees of application-layer security.

One option that does remain, though, is how organizations choose to implement these much-needed solutions. Using multiple, standalone devices is certainly one path, and it may even be warranted under certain circumstances. In general, however, a better option will be to take advantage of the ability to operate the Citrix Application Firewall as a seamlessly integrated component of the NetScaler application delivery solution. In this way robust, 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 responsible for making NetScaler a market-leading platform for application delivery. The result is better overall application performance along with significantly reduced complexity and cost of ownership.

Citrix Worldwide

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

Regional headquarters

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

Citrix Online division

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

www.citrix.com

About Citrix NetScaler

Citrix NetScaler optimizes the delivery of web applications-increasing security and improving performance and web server capacity. This approach ensures the best total cost of ownership (TCO), security, availability and performance for web applications. The Citrix NetScaler solution is a comprehensive network system that combines high-speed load balancing and content switching with state-of-the-art application acceleration, layer 4-7 traffic management, data compression, dynamic content caching, SSL acceleration, network optimization and robust application security into a single, tightly integrated solution. Deployed in front of application servers, the system significantly reduces processing overhead on application and database servers, reducing hardware and bandwidth costs.

About Citrix

Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader and the most trusted name in application delivery infrastructure. More than 200,000 organizations worldwide rely on Citrix to deliver any application to users anywhere with the best performance, highest security and lowest cost. Citrix customers include 100% of the *Fortune* 100 companies and 99% of the *Fortune* Global 500, as well as hundreds of thousands of small businesses and prosumers. Citrix has approximately 6,200 channel and alliance partners in more than 100 countries. Annual revenue in 2007 was \$1.4 billion.

©2008 Citrix Systems, Inc. All rights reserved. Citrix®, NetScaler® and Citrix Application Firewall™ 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 in other countries. All other trademarks and registered trademarks are property of their respective owners.

0608/PDF

