

## Application Security

WHY NETWORK FIREWALLS AND INTRUSION PREVENTION SYSTEMS AREN'T ENOUGH

---

## **Table of Contents**

- 2 Network Firewalls: Notable Facts**
  - Why that's good
  - Why that's not good enough
- 3 Inside Intrusion Prevention**
  - Why that's good
  - Why that's not good enough
- 3 Web Application Firewalls: When More Is Needed**
- 4 Citrix Application Firewall: Essential Protection**
- 5 Conclusion**

The nature of attacks has migrated beyond the “spray & pray” approach of general viruses and worms to highly targeted attacks against specific organizations, applications and sensitive data.

Opportunistic and financially motivated attackers know a soft target when they see one. Instead of wasting their ammunition on non-specific network intrusion attempts, they’re now gunning for the sensitive data accessible through Web applications, and traditional methods of network security are powerless to stop them.

Network firewalls and intrusion prevention systems (IPSs) are integral parts of an enterprise security strategy, but they can’t adequately protect the inherently vulnerable Web applications that companies now rely on to extend their businesses to partners, suppliers and customers. Hackers know this, and have put Web applications squarely in their sights: the CSI/FBI Computer Crime Survey reported a 90-percent jump in Web application attacks in 2005<sup>1</sup>, and Gartner estimates that Web application attacks account for at least 75 percent of all offenses targeting the enterprise.<sup>2</sup>

Blocking network attacks is not the same as interactively securing the vital resources and information made available by Web applications. What companies need is a solution that complements their network firewall and IPS deployments, and that’s where Web application firewalls come in.

Web application firewalls are standalone appliances that sit in front of application servers, doing what network firewalls and IPSs were never intended to do: examine all Web application data in depth to ensure correct application behavior and block suspicious activity — thus preserving the safety of sensitive information and systems. And that’s just what’s needed in a world where network intrusion attempts are giving way to cross-site scripting, SQL injection and other exotic exploits aimed directly at Web applications.

## Network Firewalls: Notable Facts

A network firewall is a critical component in enterprise security, functioning as the primary method for securing corporate computing resources and data from intruders, both external and internal. Network firewalls inspect various traffic headers not only to make sure that incoming traffic doesn’t pose a threat, but also to give internal users secure access to the Internet. A network firewall can exist as a standalone machine or as software features in a router or server.

### **WHY THAT’S GOOD**

Keeping the bad guys away from sensitive systems and data is always a good thing, and a network firewall makes use of several techniques for doing so:

**Packet filtering:** With packet filtering, traffic can be blocked according to IP address or type of application, such as e-mail or FTP, which is specified by port number.

**Stateful inspection:** This technology examines IP transactions to make sure that all incoming traffic is, in fact, the result of an outbound request. For example, when a user clicks a link to a Web page, an HTTP request is sent to

<sup>1</sup>Reported in the CSI/FBI Computer Crime Survey, 2005.

<sup>2</sup>Reported in a Gartner note by Theresa Lanowitz, “Now is the Time for Security at the Application Level,” December 2005.

---

that URL; all packets coming back from that URL are examined via stateful inspection to validate their origin. Suspect packets are blocked.

**WHY THAT'S NOT GOOD ENOUGH**

By blocking access to ports and applications, network firewalls run counter to the concept of Web applications — the purpose of which is to allow access to partners, suppliers and customers.

Network firewalls simply weren't developed with Web application traffic in mind. They generally do not understand the inner workings of languages like HTML and XML; they do not validate user inputs to an HTML application; and they don't detect maliciously modified parameters in a URL request. Further, network firewalls can't inspect Secure Sockets Layer (SSL) traffic — and most Web application traffic is SSL-encrypted. Also, much as stateful inspection is a critical feature of network firewalls, sessionization is critical for Web applications — and no network firewall can do sessionization.

## Inside Intrusion Prevention

IPS software intercepts and examines packets in real time to detect and stop an attack before any damage can be done or data stolen.

**WHY THAT'S GOOD**

IPSs are a major improvement over intrusion detection technology, which passively monitors traffic and notifies administrators only once an attack is underway. IPSs take defensive measures proactively, thus providing a much higher degree of protection against network intrusion attempts.

**WHY THAT'S NOT GOOD ENOUGH**

Like network firewalls, IPSs are built with access blocking in mind. Also like network firewalls, IPSs can't understand the intricacies of application languages, thwart session-based application-layer attacks, or detect injection of malicious code. IPSs also commonly generate false positives, so that aside from offering insufficient Web application security, they also waste IT resources.

## Web Application Firewalls: When More Is Needed

Network firewalls and IPSs are crucial components in enterprise security. But because of their fundamental inability to comprehensively safeguard Web applications, organizations need to deploy another layer of defense.

Web application firewalls come through where network firewalls and IPSs fall short. They perform a full range of functions specifically intended to safeguard Web applications — thus acting as a vital complement to network firewalls and IPSs.

Web application firewalls provide the necessary protection through the following techniques:

- **Full traffic inspection:** Comprehensive protection demands full bi-directional traffic inspection of all application traffic. Inspection of both header and payload is required, along with full application parsing and semantic extraction of relevant application objects.
- **Sessionization:** A Web application firewall tracks, on a per-session basis, all content provided by a Web server that has the potential to exploit vulnerabilities upon return from the Web browser. By ensuring that returned cookies, URLs and form-field elements match those that were served, a Web application firewall provides protections that non-session-aware devices cannot.
- **Positive security model:** Based on HTTP industry standards and best coding practices for HTML and Java, a positive security model allows an application firewall to recognize good application behavior without the need for attack signatures or pattern-matching techniques. Application behavior deviating from the positive security model is treated as potentially malicious and is blocked. The benefit of the positive security model is that it is the only proven method for delivering zero-day protection.
- **Adaptive learning engine:** An adaptive learning engine can automatically learn the behavior of an application and generate human-readable policy recommendations. Security managers can thus use it to apply recommendations selectively — strengthening security policies and enabling permissible application behavior.
- **Cloaking:** This involves a series of capabilities that serve to hide virtually all information about the application environment. First, full proxy architecture, in which all inbound TCP traffic is terminated and then re-initiated to the Web server infrastructure, entirely hides network-related information. Second, the removal of all unnecessary response headers prevents disclosure of information about the Web infrastructure, such as the server type and server hostname. Finally, the ability to rewrite URL components allows traffic to be directed according to a complex data center architecture whose details are hidden from the prying eyes of information criminals.

Put all those functions together, and Web application firewalls are able to thwart the many dangerous application exploits that elude network firewalls and IPSs.

## Citrix Application Firewall: Essential Protection

Citrix Application Firewall™ performs the critical functions needed to secure Web applications. With its comprehensive set of security features, Citrix Application Firewall guards against all of today's most dangerous application attacks.

What's more, Citrix Application Firewall prevents loss of sensitive user information, such as credit card numbers, in Web application responses. Its SAFE Commerce Protection Module prevents unauthorized transmission of that data, either by blocking the transmission entirely or by masking the majority of digits in the credit card number itself. And the SAFE Object Module keeps user-defined data objects — such as customer account, patient record identification, and driver's license numbers — under wraps. Even billing codes and EDI (electronic data interchange) tags can be protected with the SAFE Object Module.

---

Better yet, this degree of protection doesn't exact a penalty in administration or performance. Citrix Application Firewall can be used as a standalone appliance that's easy to install, operate and manage. And when companies deploy it in conjunction with Citrix® NetScaler® application delivery systems — which improve application performance up to five times — they can be sure their Web applications are not only safe, but also running at peak performance.

## Conclusion

Sophisticated hackers are aware that an enterprise's network perimeter is now well — defended, so they're instead turning their attention to Web applications as a means of entry into the enterprise. Network firewalls and IPS are fundamentally unable to protect these Web applications from attack.

Companies need another layer of defense, and that's where Citrix Application Firewall comes in. It features a full range of functions for protecting against today's most dangerous Web application attacks — and as a complement to network firewalls and IPSs, it plays a vital role in a complete enterprise security strategy.

## 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](http://www.citrix.com)

### NOTICE

The information in this publication is subject to change without notice. THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. THE USE CASES IN THIS PAPER ARE PROVIDED ONLY AS POTENTIAL EXAMPLES AND YOUR ACTUAL COSTS AND RESULTS MAY VARY.



Best Access Experience. Anytime. Anywhere.

**About Citrix:** Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader and the most trusted name in application delivery infrastructure. More than 180,000 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 98% 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 2005 was \$909M.

©2007 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 other countries. All other trademarks and registered trademarks are property of their respective owners.