



# Importance of Web Application Firewall Technology for Protecting Web-based Resources

By
**Andrew J. Hacker, CISSP, ISSAP**
**Senior Security Analyst, ICSA Labs**

January 10, 2008

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050

# Importance of Web Application Firewall Technology for Protecting Web-based Resources

By Andrew J. Hacker, CISSP, ISSAP

## Introduction

Web-based applications and services have changed the landscape of information delivery and exchange in today's corporate, government, and educational arenas. Ease of access, increased availability of information, and the richness of web services have universally increased productivity and operational efficiencies. These increases have led to heavier reliance on web-based services and greater integration of internal information systems and data repositories with web-facing applications.

While motivations of attackers against a victim's corporate and organizational assets remain the same (financial, IP, identity theft, services disruption, or denial of service, for example), web applications enable a whole new class of vulnerabilities and exploit techniques such as SQL injection, cross-site scripting (XSS), and cross-site request forgery, to name a few.[1]

The complexity of services, potential severity of breaches, and mounting sophistication of attacks requires additional functionality beyond the capability of traditional network-based security products. The emergence of dedicated web application firewall technology provides a comprehensive and focused solution to help increase the security of web-based services and protect valuable information assets.

This paper will review the fundamental functionality of several traditional security technologies from a high-level perspective, including network firewalls, intrusion prevention systems, outbound content filtering, and anti-malware gateways. This paper will discuss why dedicated web application firewall technology is necessary to protect web-facing resources. It will also provide a suggested deployment model that illustrates the relative locations of the discussed technologies within a simplified enterprise network.

1 For additional information on attack descriptions and classifications, see 1) OWASP Top 10 2007, **http://www.owasp.org/index.php/Top_10_2007**, and 2) WASC Threat Classification, **http://www.webappsec.org/projects/threat/**

## Protocol-Enforcing Network Firewalls

Many firewall vendors augment port blocking and TCP session or state awareness by employing protocol inspection functionality (historically known as packet filtering) to help prevent attacks that exploit weaknesses in protocol implementation. This protocol enforcement includes protocols from the application layer of the IP protocol stack such as DNS, HTTP, FTP, SMTP, and SSH and is effective at preventing simple protocol attacks such as "fuzzing"[2] or parameter overflow attacks by either rejecting protocol violations or by normalizing protocol parameters. Other implementations include pattern matching and blocking of common protocol exploits.

Protocol-enforcing network firewalls typically provide the first line of defense by arresting most basic protocol attacks at the network perimeter, including protocol-based denial of service attacks. They primarily operate in the network, session, and transport layers of the Open Systems Interconnection (OSI) reference model. Developers have also greatly enhanced the capability of network firewalls to police the protocol integrity of a wide range of upper-layer protocols such as DNS, FTP, HTTP, SMTP, and TFTP. Network firewalls can also verify that traffic passed over non-standard ports, such as SMTP running over port 2525, conforms to valid SMTP traffic.

## Intrusion Prevention Systems

Intrusion prevention systems (IPS) can be deployed at various locations within an enterprise network. IPS agents monitor network traffic and scan for signatures of a wide range of known attacks. Administrators can choose which application/protocol signature sets they wish to apply in which locations. Improvements in functionality have allowed IPS devices to make access control decisions based on various aspects of the network traffic such as protocol and content type. IPS functionality can also be implemented "on the wire" in LAN segments, known as network IPS (NIPS) or in software on a host server or client, known as host IPS (HIPS).

IPS is effective at providing signature scanning, pattern matching, anomaly detection, and behavioral-based functionality for a broad range of known attacks that make it past perimeter defenses. IPS devices, like network firewalls, support a wide range of network protocols. Enhancements have also provided the capability to detect multi-pronged attacks using state machines that can trigger an IPS to watch for a secondary set of conditions when a primary set of conditions is observed.

## Outbound Content Filtering

Outbound content filtering gateways provide access control for internal corporate users as they access information from the Internet. Content filtering provides protection to an enterprise by preventing users from accessing malicious or otherwise dangerous external content by enforcing white and black lists of known good and known bad Internet sites. Outbound content filters can also be configured to block internal users from uploading corporate documents to external sites. This can help curb identity theft and information leakage.

More sophisticated content filtering platforms provide additional protection by monitoring other services, including instant messaging and file transfer systems such as FTP and peer-to-peer (P2P), as well as provide interfaces to anti-malware solutions. Administrators can also configure access control lists and groups that can provide different filtering rule sets for various employee types. Content filtering platforms also address intellectual property protection by providing data loss prevention (DLP) functionality.

2 Fuzzing refers to an attack technique that probes for protocol vulnerabilities by using brute force to transmit vast amounts of random data into protocol parameter values with the hopes of uncovering an exploitable situation from a protocol stack entity.

## Anti-Malware Gateways

"Malware" refers to variants of malicious code such as viruses, Trojans, rootkits, macro viruses, etc., as well as other undesirable content such as spyware and phishing links. Anti-malware gateways scan inbound and outbound content, including email, instant messaging, and file downloads, for code that can compromise client security. Anti-malware gateways focus on scanning attachments or snippets of code that can either self-execute on a client or that can be uploaded to an Internet-based server for future download by a client.

Recent enhancements include outbreak prevention by which a gateway can signal other security devices to limit propagation when malware is detected.

## Web Application Firewalls

Web application firewalls (WAFs) deal specifically with web-based traffic, i.e., HTTP/HTTPS, and can be deployed either as standalone appliances or as self-contained software installed on the web servers themselves. They employ a wide range of functions to work in conjunction with perimeter firewall and IPS technology to augment application attack prevention. Most WAFs include HTTP/HTTPS protocol enforcement and negative signature detection.

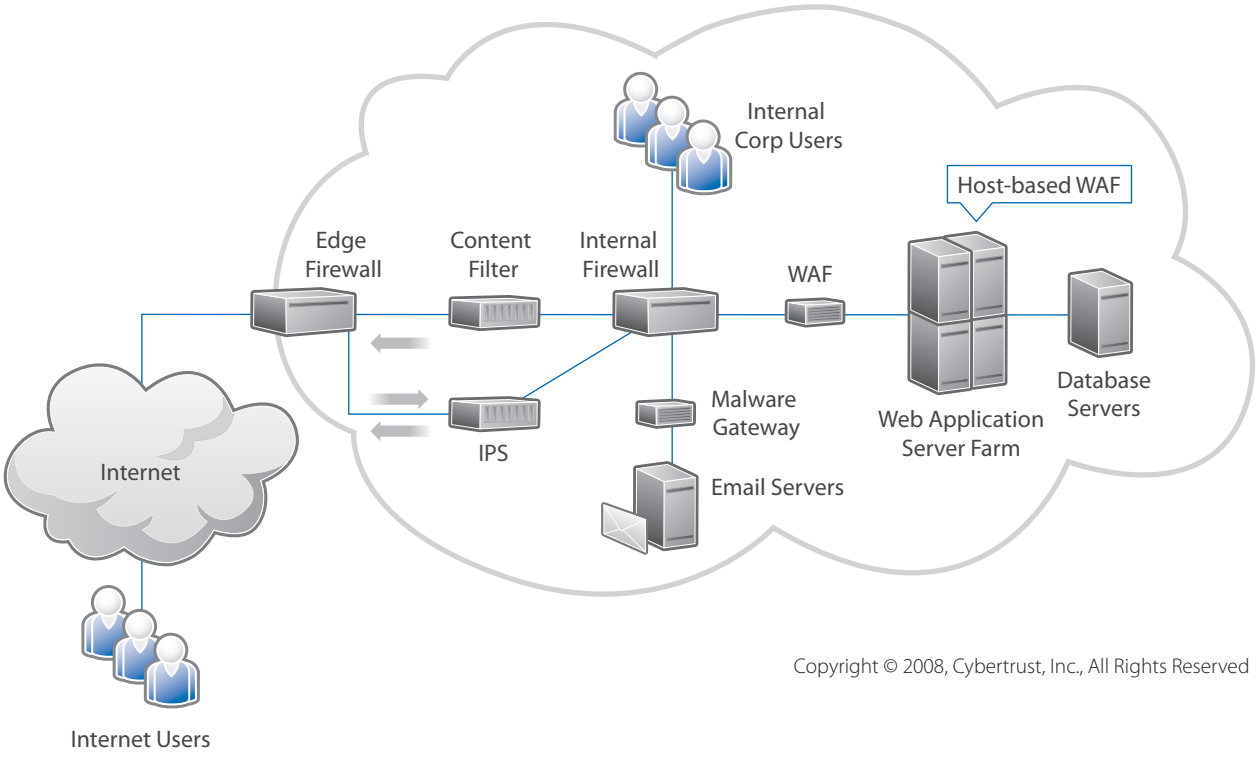
Other protection mechanisms include URL normalization and scanning, positive security functionality that enforces proper application operation and page logic flow, and adaptive learning modules that can update security policies on the fly. WAFs can also block attacks masked by HTTPS encryption by inspecting SSL sessions using the web server's private key, detecting policy violations, and resetting offending connections. These sessions can either be passively decrypted and inspected or actively terminated and re-encrypted.

Furthermore, WAFs can recognize and be configured to police the usage of specific web application elements and functions, such as web objects, form fields, and, most importantly, application session logic. Session logic enforcement, or "HTTP session awareness," includes session cookie or state monitoring and protection, as well as the capability to enforce web-path logic and server entry points to prevent session hijacking exploits that allow an attacker to assume the session of another logged-in user. This HTTP session awareness is one of the primary differentiators that web application firewalls possess.

WAFs enforce proper context of the HTML request and response, as well as provide semantic awareness of the relationships of the various web objects present on a web site, such as various types of form fields, input drop down lists, server and client side scripts, functions, and associated input and output parameters. They have the functionality to block attacks specific to a wide range of web server, database, and programming platforms. WAFs can be configured to mask or rewrite inbound and outbound server responses to help protect against sensitive information leakage such as credit card numbers. This capability can help administrators address Payment Card Industry Data Security Standard (PCI DSS) policy requirements.

WAFs can be deployed between perimeter defenses and the web servers they protect, or installed directly on web server platforms as host-based WAFs. Figure 1 illustrates a simplified enterprise network and the relative locations of the various technologies discussed in a representative deployment.

*Web Application Firewall Typical Deployment, Figure 1*



## Summary

Each of the discussed technologies provides excellent security for the aspects of the enterprise network they are designed to protect. With the emerging prevalence and importance of application security, developers of these technologies have enhanced their offerings within the boundaries of their functionality to help protect web applications. Figure 2 provides an overview of each technology by presenting historical purpose, primary mechanism of operation, scope, and how each has enhanced the technology to provide additional functionality in the application security area.

*Overview Grid, Figure 2*

| Overview of Technologies and Application Security Relevance | | | | |
|---|---|---|---|---|
| **Technology** | **Primary Purpose** | **Primary Mechanism of Operation** | **Scope** | **Application Enhanced Functionality** |
| **Protocol-Enforcing Network Firewall** | OSI network model protocol protection | Network port blocking<br>UDP/TCP state awareness | Network protocols | Protocol enforcement |
| **Intrusion Prevention Systems** | Signature-based network protection | Signature scanning<br>Connection reject<br>UDP/TCP state awareness | Network protocols<br>Network applications | Enhanced access control<br>URL scanning<br>Broad range of signatures |
| **Content Filtering Gateways** | Outbound access control | URL and DNS level access control list<br>Outbound connection reject | Outbound web, IM, file applications | Anti-malware interface |
| **Anti-malware Gateways** | Signature-based payload protection | Signature payload scanning<br>Attachment removal | Payload components | Advanced heuristics<br>Outbreak protection |
| **Web Application Firewall** | HTTP/HTTPS application protection | URL normalization<br>Session state enforcement<br>Application context enforcement | HTTP/HTTPS applications | Context-based positive security model<br>Adaptive rule modification/exception |



Dedicated WAFs are designed specifically for HTTP/HTTPS protocols and are required in addition to traditional security technologies to provide a complete solution for securing web applications. They provide in-depth web-specific functionality such as application session awareness, request/response rewriting and masking, and detailed platform- and application language-specific functionality. These capabilities are vital to preventing sophisticated attacks and protecting valuable information assets.

### About the ICSA Labs Web Application Firewall Product Developers Consortium

ICSA Labs' web application firewall testing and certification program evaluates and certifies products that implement security policy enforcement for the protection of HTTP and HTTPS web-based applications. In conjunction with ongoing efforts in the industry to classify and categorize application security issues and mitigate potential vulnerabilities, web application firewall certification criteria were developed to provide security managers with confidence in the products that secure vital application services from exploitation or attack.

### WAF Product Developers Consortium Members

Applicure Technologies, Ltd., **http://www.applicure.com**

Breach Security, Inc., **http://www.breach.com**

Citrix Systems, Inc., **http://www.citrix.com**

F5 Networks, Inc., **http://www.f5.com**

Fortify Software, Inc., **http://www.fortifysoftware.com**

Imperva, Inc., **http://www.imperva.com**

Netcontinuum, Inc., **http://www.barracudanetworks.com/netcontinuum**

### Contributors

The author would like to acknowledge the following individuals for giving input to the content of this paper:

- Representatives of the members of the WAF Product Developers Consortium
- Representatives of the ICSA Labs Consortium program managers group

### Contact ICSA Labs

For questions or comments about this paper, contact Andrew J. Hacker at **andrewh@icsalabs.com**. For more information regarding the ICSA Labs Web Application Firewall Testing Program or WAF Product Developers Consortium, visit **http://www.icsalabs.com** and follow the "Web Application Firewall" hyperlink.

### About ICSA Labs

ICSA Labs, an independent division of Verizon Business, offers vendor-neutral testing and certification of security products. Hundreds of the world's top security vendors submit their products for testing and certification at ICSA Labs. The end-users of security technologies rely on ICSA Labs to authoritatively set and apply objective testing and certification criteria for measuring product compliance and reliability. The organization tests products in key technology categories such as anti-virus, anti-spyware, network firewall, IPSec VPN, cryptography, intrusion prevention, PC firewall, SSL-VPN, web application firewall, anti-spam and wireless LAN. For more information about ICSA Labs, please visit: **http://www.icsalabs.com**.