# WAF or IPS?

## Why you need more than a Firewall and IPS to protect your applications

### Introduction

Web applications are attractive targets to hackers as often they are public facing applications that require being open to the internet as they provide major e-commerce and business driving tools. Connected to back end databases, web applications are perfect for hackers as these databases are the primary repository for card holder data, company data and other sensitive information.

According to the SANS institute (http://www.sans.org) attacks against web applications constitute more than 60% of the total attack attempts observed on the Internet. Web application vulnerabilities such as SQL injection and Cross-Site Scripting flaws in custom-built applications account for more than 80% of the vulnerabilities being discovered.

Traditional perimeter security technologies such as IPS and departmental firewalls have always focused on network and transport layer attacks.  As the threat landscape for internet applications changes and hackers become increasingly more sophisticated these vendors have introduced application layer enhancements commonly referred to as "Deep Packet Inspection" (DPI).

While providing additional security this technology merely extends the current network signature engine to the application layer. Although useful in protecting against attacks on the web server infrastructure itself (IIS, Apache, etc) it cannot protect against attacks on custom web application code such as SQL Injection and Cross-Site Scripting attacks.

Securing web applications requires a completely different approach. Relying on application signatures is just not good enough. The web application firewall must understand the application logic and what elements exist on the web application such as URLs, parameters and what cookies it uses. For example, understanding which URLs are allowed to be accessed and the number and type of characters allowed in each parameter would allow the web application firewall to constitute what normal user behavior is and based on that block any abnormal activity that doesn't conform with this behavior.

The only way a web application firewall can do this is by creating a comprehensive model of allowed application behavior. This baseline must be created automatically and transparently as a standard web application can have hundreds or even thousands of

### Business Challenges

- Secure applications and network
- Protect against application vulnerabilities

### Segments

- Enterprise
- Data center
- MSP

URLs and parameters that constantly change. Creating and maintaining such a baseline manually is almost impossible

## Next Generation and Application Aware Firewalls

In recent years perimeter firewalls have evolved and now many offer additional functionality such as Application Control. This is usually associated with the ability to identify and control applications on networks and endpoints regardless of port, protocol, and IP address used. It gives visibility and control over application traffic such as allowing Facebook Chat but blocking Facebook Video (both are using the HTTP protocol as a transport mechanism)

By identifying applications and fingerprinting specific functions within them these products allow administrators to set policies to the application and function level.

Enhancing visibility to application traffic these products are usually trying to provide the following:

- Allow traffic shaping to limit bandwidth to non-priority applications such as YouTube
- Control applications at a granular level, such as allowing Facebook Chat but blocking Facebook Video or disabling links in chat.
- Provide URL filtering regardless of IP, port, SSL encryption, proxies, TOR networks and other evasion techniques
- Scan application traffic for different threats such as viruses, malware, spyware and other exploits

Application Aware firewalls do a great job identifying, qualifying, filtering and securing specific outgoing application traffic but do not add the application security required to protect internal web applications from application attacks such as defined by the OWASP Top 10.

Only Web Application Firewalls, which are designed to compensate for insecure code practices and focus on security flaws in applications can protect against such attacks.

The following comparison chart displays the main differences between the two technologies:

| Feature | FortiWeb WAF | NGFW |
|---|---|---|
| Creates a baseline of allowed access to the application such as URLs, parameters, cookies and sessions | Yes | No |
| Blocks external attacks such as defined by the OWASP Top 10 (SQL Injection ,XSS, CSRF, etc) | Yes | No |
| Provide both a positive and negative security model | Yes | No |
| Control Applications and functions within them | No | Yes |
| Allows traffic shaping to limit bandwidth to non-priority applications | No | Yes |
| Secure and restrict clients accessing the internet | No | Yes |

## Conclusion

Next Generation and Application Aware firewalls extend and enhance protection and add additional functionality but the majority of the 'application aware' functionality is focused on securing/restricting internal clients when accessing the internet but not securing internal applications from external threats

Web Application Firewalls are different as they protect internal web applications from sophisticated application layer external attacks. They provide both a positive and negative security model and protect against the major threats to applications today – SQL Injection, Cross Site Scripting, URL Access, CSRF, Injection attacks and more.

**GLOBAL HEADQUARTERS**
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

**EMEA SALES OFFICE**
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

**APAC SALES OFFICE**
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

**LATIN AMERICA SALES OFFICE**
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480