ISACA
TECH BRIEF

Web Application Firewalls
Where do we stand?

Late 2018, ISACA Belgium organized an interesting evening event on Web Application Firewalls (abbreviated to “WAF”) in Louvain-la-Neuve (Belgium). Based on the comments and the discussions, ISACA Belgium decided to put the content into a short technical briefing for all ISACA members.

WAFs are recognized as a good practice by international recognized advisors (such as Gartner, OWASP, …) and sometimes required by certain security standards like PCI-DSS 2.0 (for credit card payment processors).

Why is a WAF not a security commodity today like anti-malware solutions are? The main reason is that a majority of WAF implementations are not delivering on their promises, even after 20 years. WAFs are still perceived as magic black boxes that do security. By maintaining this aura, security solution providers introduce fear and misconception about this solution or introduce them with useless features. Also, several hosters and/or cloud service providers offer some WAF solutions in their portfolio.

“When we look at confirmed breaches, Web Application Attacks remain prevalent.”
VERIZON 2018 DATA BREACH INVESTIGATIONS REPORT, 11TH EDITION, MARCH 2018
https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

Short history of WAF

Web Application Firewalls were developed in the early 1990s by Gene Spafford, Bill Cheswick and Marcus Ranum. Their solution was largely a network-based firewall but could handle a few applications. Dedicated web application firewalls entered the market later when web server hacker attacks were becoming much more noticeable.

The first company to offer a dedicated web application firewall was Perfecto Technologies with its AppShield solution, which focused on the e-commerce market and protected against illegal web page character entries. Perfecto renamed itself as Sanctum and named the top ten web application hacking techniques and laid the foundations for the WAF market.

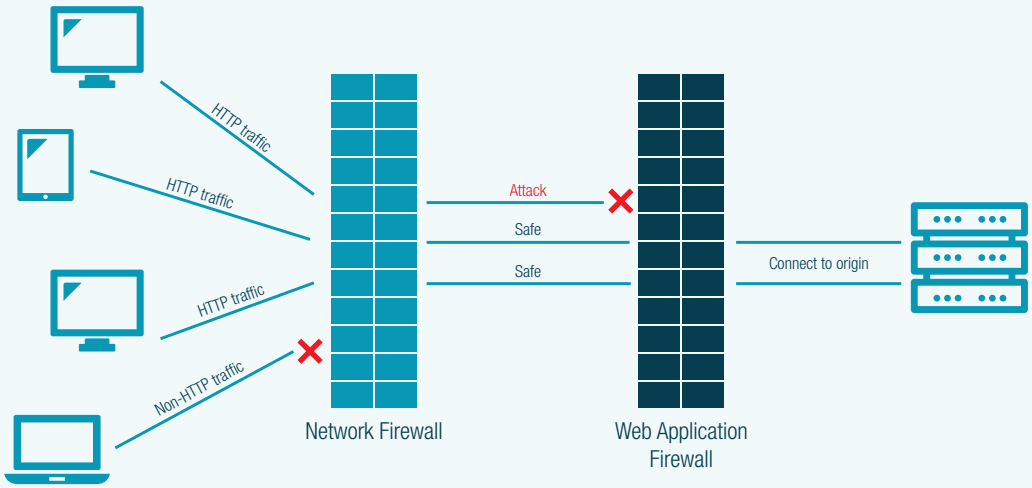
In 2002, the open source project ModSecurity was formed in order to make WAF technology more accessible and solve the obstacles within the industry like business cases, cost barriers, and proprietary rule-sets. ModSecurity finalized a core rule set for protecting Web Applications, based on the OASIS Web Application Security Technical Committee's (WAS TC) vulnerability work. In 2003, their work was expanded and standardized through the Open Web Application Security Project's (OWASP) Top 10 List, an annual ranking for web security vulnerabilities. This list would become the industry benchmark for many compliance themes.

Since then, the market has continued to grow and evolve, involving the larger commerce industry with the rise in credit card fraud. With the development of the Payment Card Industry Data Security Standard (PCI DSS), a standard for organizations to increase controls on cardholder data, security is more regulated and has sparked wide-scale interest in the industry.

According to CISO Magazine, the WAF market size is expected to grow to $5.48 billion by 2022[1].

What is a WAF?

According to OWASP, a web application firewall (WAF) is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation[2]. A WAF offers protection for web servers. The delivery of web applications follows the client-server model, wherein the server only sends out messages in response to a request from a client. A typical firewall protects the network layer whereas a web application firewall protects the server and its whole application stack.



Generally, the rules of a WAF attempt to cover the most common attacks such as:

1. **Cross-Site Scripting (XSS)** – malicious HTML code inserted into a web page input field by a hacker
2. **Hidden field manipulation** – hackers rewrite the source code of a web page to alter values held in hidden fields and then post the amended code back to the server
3. **Cookie poisoning** – altering parameter values held in cookies to corrupt data passed between web pages

1 *https://www.cisomag.com/web-application-firewall-market-worth-5-48-billion-2022/*
2 *https://www.owasp.org/index.php/Web_Application_Firewall*

4. **Web scraping** – automated data extraction from web pages
5. **Layer 7 DoS attacks** – overwhelming a web server by recursive application activity
6. **Parameter tampering** – altering values in the parameters to a web page call
7. **Buffer overflow** – user input that overwrites the code in memory
8. **Backdoor or Debug options** – developer feedback reports for web page testing that can be used by hackers for access to the processor
9. **Stealth commanding** – an attack on the operating system of a web server
10. **Forced browsing** – the hacker gains access to backup or temporary folders on the web server
11. **Third party misconfigurations** – manipulation of content inserts provided by other companies
12. **SQL injections** – queries entered in user authentication fields

While proxies generally protect clients, WAFs protect servers. A WAF is deployed in front of web servers to protect a specific web application or set of web applications against attacks. A WAF can be considered as reverse proxy.

WAFs may come in the form of an appliance, server plugin, or filter, and may be customized to an application. The effort to perform this customization can be significant and needs to be maintained as the application is modified. In the cloud era, WAFs also evolve to a "service in the cloud" – which may mean very different things.

Does an organization need a WAF?

A common question is "do we invest in securing the development of the application or do we invest in a WAF?" Securing application development is indeed very important and it must be done. But what about applications that are not under the control of the organization since they are developed by a third-party? What about remaining vulnerabilities in applications? What to do when a vulnerability is detected in one of the libraries used by the application? Maybe a new version is available from the supplier, but how long does it take to test the compatibility and release a new version in production?

"A WAF is the only option for promptly closing external vulnerabilities."
OWASP "BEST PRACTICE: USE OF WEB APPLICATION FIREWALLS", MAY 2008, V1.0.5
https://www.owasp.org/index.php/Category:OWASP_Best_Practices:_Use_of_Web_Application_Firewalls

A WAF needs to be a part of a webhosting protection strategy. A WAF does not only protect an application, but will also protect the whole stack from the web server up to the application, including the application server itself and development framework. A WAF is thus a part of the application deployment stack.

A WAF has a more global view on security than just the network firewall. Let's take an example. An organization completely secured its application and its deployment. This includes the implementation of a lock-out mechanism on the users' account to forbid brute-force attacks on the authentication page: after 10 wrong credentials, the user account is blocked. Well, what about a brute-force attack with the password "password" or "123456" on all users' account? The same for an attacker trying to abuse the application by trying all possible identifiers to retrieve sensitive reports. A properly configured WAF will detect such attacks and block an attacker, whereas such an attack would be invisible to the application itself.

Is a WAF is redundant with other security solutions? Obviously, a network firewall and a web application firewall are not redundant, but what about Intrusion Prevention System (IPS) or emerging security technologies like Runtime Application Self-Protection (RASP). The answer is no: there is not a single technology offering all security aspects. Although IPS and RASP technologies can potentially detect attacks which a WAF cannot (for instance an IPS may detect attacks at the TCP level, a RASP may detect sensitive information in the logs), they will miss most of the ones a WAF may see. For instance, a RASP will miss all unsuccessful attacks, so it will not detect an attacker before it succeeds to exploit a vulnerability, which may be too late. Also, an IPS works at the network level and will miss most of the application-level attacks whereas a RASP, working inside the application, will miss all attacks on the layers before the application.

Although a WAF works as a front end to a website, a number of essential access control functions that your webhost needs are not provided by this technology. WAFs focus on HTTP code and the request procedures for other internet applications such as FTP. In these cases, the secure versions of these application protocols, HTTPS and SFTP, are also covered.

WAFs look for irregularities contained in incoming requests and block malformed or devious constructs. In a most case, a WAF is not responsible for load balancing between a cluster of servers. Although some types of DDoS attacks use HTTP, several use lower-level methods. So, a WAF will protect an organization against HTTP and FTP application-level/layer 7 DDoS attacks, but not those carried out by other cyberattack strategies.

What WAF solutions are currently available?

Until a few years ago, there were two major choices: either buying a hardware WAF or choosing an Open Source WAF.

For the hardware WAF solutions, the decision was usually depending on the current supplier's portfolio. The hardware WAF solution involves a piece of network equipment that needs to go in front of the web infrastructure. As all traffic in both directions will pass through this appliance first, an organization needs to make sure that the model chosen has the capacity to handle the web server's typical request throughput rate. When assessing WAF appliances, the demand on server should be measured first in terms of both data throughput in megabits per second (Mbps) and the number of transactions. As secure TLS/SSL transactions take more processing, also the maximum number of TLS/SSL transactions per second (TPS) should be included in the evaluation.

The most known hardware WAF solutions currently are (in alphabetical order)

- Barracuda Web Application Firewall;
- Citrix Netscaler Application Firewall;
- F5 BIG-IP ASM;
- Fortinet FortiWeb;
- Imperva SecureSphere.

The benefits of a hardware WAF

If organizations are running their own web server, they probably already know a lot about networking and internet systems. They may need a load balancer on extra servers to deal with demand. If that is the case, organizations could buy a combined web cache, load balancer and WAF combined and get all of their front- end requirements dealt with by one device – although that seems tempting and wise from a management point of view, note that the behavior of a WAF being totally different than the behavior of network layers modules (store & forward vs. real-time), we often realize major stability problems due to the locking of resource (especially the CPU) by the WAF module blocking low-level real-time treatments. Having an own WAF means an organization does not have to surrender its web address to a third party. If, at some point, an organization needs extensive DDoS protection, then its URL will have to go to the DDoS mitigation provider. However,

the organization will not need to limit its choice of DDoS protection to that provided by its cloud-based WAF provider. The organization is not committed to directing its URL to provide a WAF.

The problems with a hardware WAF

When considering the cost of a hardware WAF, there are also the expenses of installing, housing, protecting and maintaining it.

Automatic updates, so they are always up-to-the-minute and ready to tackle the latest emerging threat, on a hardware WAF device can be expensive. Most hardware WAF providers offer an update service. The fixes to new threats are sent to a hardware WAF device over the internet automatically and it will renew its firmware without intervention. In the case of some new threats, other equipment and software on the network may need updating, and the support service of a WAF provider will give those too. This process is called “virtual patching” and it is the WAF version of classic firewall database updates. However, although hardware WAF suppliers provide virtual patching, not all of them include that service for free. Where the update service is included, it is usually only free for the first year. After that, an organization must pay extra for support of an in-house hardware WAF.

The upfront cost of buying a hardware WAF can be an inconvenient expense when struggling to get a new web company operational. If an organization forgoes this protection initially, it may get lulled into the belief that it is an unnecessary extra even when it gets to the point where it has cash to spare. This is a dangerous scenario, because the organization will only realize that it needs WAF protection once it has been hit by a cyberattack. By then, the website will be blocked by search engines for containing malicious code and the consequences can be massive.

For the Open Source WAF, the most deployed one worldwide is ModSecurity https://www.modsecurity.org/, which presents itself as a toolkit for real-time web application monitoring, logging and access controls. Another known example is Aqtronix WebKnight. With full access to the source code, organizations have the full freedom to customize and to extend the tool itself to make it fit its needs. Although these Open Source WAFs may meet requirements and greatly reduce costs, organizations still need staff to learn, install, configure and maintain them. Many Open Source WAF projects have excellent support forums, but unlike a purchased solution, organizations may not able to call a helpdesk in an emergency.

Recently, new types of software WAF offerings appear which are linked to the cloud and thus they are called cloud-based WAF solutions. Larger organizations sometimes completely outsource the management of their WAF to a third party due to the complexity and the expensive and long learning curve. This outsourcing approach is usually part of a more global security sourcing contract including most security devices.

“By 2020, more than 50% of public-facing web applications will be protected by cloud-based WAF service platforms, combining CDN, DDoS protection, bot migration and WAF, up from less than 20% today.”

https://www.gartner.com/doc/3779166/magic-quadrant-web-application-firewalls

The most known cloud-based WAF solutions currently are (in alphabetical order)

- Akamai Kona Site Defender;
- Amazon Web Services WAF;

- Cloudflare WAF;
- F5 Silverline WAF;
- Incapsula WAF;
- StackPath WAF;
- Sucuri WAF.

Although these cloud-based WAF solutions are “cloud-based”, there are major differences in the service offerings.

Some hardware WAF providers just implemented their solution in the cloud. It is basically the same hardware WAF solution but now deployed on a shared hardware infrastructure.

Content Delivery Networks also launched their solution as an ultra-sized pool of machines resistant to (Distributed) Denial of Service (DDoS) attacks and allowed to block floods of traffics.

Cloud service providers also provide WAF services to protect the environment based on a version of ModSecurity. Some cloud service providers implement a (basic) proprietary WAF solution allowing their customers to implement from scratch all relevant security rules.

Platform as a Service (PaaS) providers are selling their solutions with a “security layer” using a WAF based on ModSecurity which is aimed at protecting their own platform (e.g. PHP, Drupal, Joomla…). There is not a single rule active at the beginning. In case a new vulnerability is published, it takes some time to update the servers; during that time, a specific rule is deployed on all servers to block that single vulnerability.

A lot of confusion may occur on the cloud-based WAF offerings, because some traditional WAF providers pretend to be able to absorb huge floods of data streams. Several WAFs are being combined in a device with network-level functionalities (switching, packet shaping, …). If an organization already has a network device, adding a WAF module inside is appealing. Relying on one commercial contract and on a single supplier is always a good point. However, the behavior of a WAF being totally different than the behavior of network layers modules can cause stability problems.

The benefits of a cloud-based WAF

Cloud-based WAFs get updated automatically, so they are always up-to-the-minute and ready to tackle the latest emerging threat. The reputation and expertise of the top cloud WAF providers means that organizations do not need to be worried about being let down. The cloud-based WAF providers specialize in networking and security services. Their accumulated expertise is a lot greater than an organization could get for its own in-house WAF. There is probably more risk to the website’s availability and security if an organization tries to cover all of the complicated tasks that these issues involve.

Cloud-based WAF solutions can be paid for on a monthly basis, spreading the cost of the web application protection. In some cases, organizations only get charged for web throughput, so payments for protection can be deferred until the end of the month when the service level has been calculated and invoiced.

If an organization already outsources parts of its IT or IT security operations, it has already come to terms with the cloud-based method of IT operations and so it is not too difficult to outsource a WAF as well. A switch from existing providers may be required if combining other services, such as DDoS protection and load balancing, with a new WAF makes better logistical and economic sense.

The problems of a cloud-based WAF

The cloud-based WAF stands in front of all of other devices and so it has to be the target of the URL of the organization. That means that an organization no longer has direct control over its traffic because all DNS records will direct website visitors to the cloud service first.

Where cloud-based WAFs are offered by providers that include other front-end security services, combining these into one package makes sense. For example, if a chosen WAF provider does not have a DDoS protection service, the organization will need to forward its traffic also to a second cloud service in order to get fully covered from threats. Taking out a cloud-based WAF service can lock an organization in to one managed security service provider for all of online protection and limit the options.

WAFs examine the contents of packets, so they strip off all encryption protection first before they can perform their main task. This means that an organization has to hand over its TLS/SSL certificates to the cloud-based WAF provider, effectively surrendering all security functions that protect the web host, the content, and the safety of the customers of the organization.

An organization needs to have a lot of faith in its cloud-based WAF provider in order to be prepared to let this third party stand in between the organization and its customers.

What methodologies exist to select a WAF?

The Web Application Security Consortium6 (WASC) creates and advocates standards for Web application security. The group has developed the Web Application Firewall Evaluation Criteria (WAFEC) for comparisons, and any reasonably skilled technician can use their testing methodology to independently assess the quality of a WAF solution7. WAFEC is a joined project between WASC and OWASP to ensure WAFEC is comprehensive, accurate and objective. These tests can be used as part of a WAF evaluation process. Organizations can use WAFEC in order to pay attention to the deployment architecture used, support for HTTP, HTML and XML, detection and protection techniques employed, logging and reporting capabilities, and management and performance. Unfortunately, this project wasn't maintained since 2013 and is missing some modern key points like integration in a DevOps environment.

What methodologies exist to configure a WAF?

Organizations basically have the following options:

- White-listing;
- Attack signatures;
- Automatic learning.

White-listing is very easy to understand since it is the same approach as with a network firewall: an organization specifies all entry points (URLs) and the syntax of every single bit of the request (HTTP headers, parameters, JSON keys, …). Except for some very specific applications, this kind of exhaustive specification is impossible, and is usually left as the last chance by providers.

Attack signatures are very similar to an (old generation) antivirus tool: the WAF is filled with signatures of known attacks and blocks them. This mechanism has a lot of limitations: attack patterns generate a huge number of false positives – blocking genuine users (and leading to deactivate a lot of rules) – but in a web application attack patterns may have a lot of variants, leaving the application with very few protections. And the continuous evolution of new signatures leads to blocking genuine users and a rules-disabling cycle.

Automatic learning is the holy grail: an organization activates the learning mode for a few weeks and the WAF configures itself to top-notch security. It sounds like a magic solution. As explained in OWASP WAF Best Practices, a WAF using "training mode" must be trained on each new release of the web application, which is usually unfeasible. And the test coverage is far from exhaustive, leaving a huge place for false positives.

No WAF provider is using a methodology or providing a facility to implement a methodological approach.

"With the right methodology, organizations can be protected almost 95% of the time against zero-day exploits without having to deploy a new security rule on a WAF. This is not only true for government or finance-related applications, but also for start-up SaaS ones."
MARC STERN, CYBERSECURITY CONSULTING DIRECTOR APPROACH BELGIUM, MAY 2018

The WAF implementation approach is to think about the requirements. Organizations do not want to specify every single bit of what is allowed in the requests, but want rules to follow globally the application evolution. If the organization can specify the global behavior of its application and ensure that all rules will adapt to that specification, the organization can manage the WAF in the long term. Also, if you have 25 applications using the same architecture and components, you need to specify the requirements only once and inherit them in the 25 application profiles.

What is required in a WAF?

A normal WAF solution contains at least 3 elements:

- a "security engine";
- a user interface;
- reporting tools.

The "security engine" allows to write security rules. By default, a "naked" WAF does not provide any security, it allows the organization to specify rules to implement the security level.

The user interface was historically a commercial argument. WAFs providers implemented attractive graphical interfaces. With the increasing usage of WAFs, these interfaces began to be difficult to use in bigger environments where many applications are monitored. With the introduction of DevOps environments, where everything must be automated, a GUI has become an annoyance, or even a blocking factor.

Reporting tools are important in any organization. Larger organizations insist on properly integrating the WAF results into their SIEM or any central logging mechanism, so their Security Operating Center (SOC) can focus on only a small number of dashboards. If this is not required, most security groups in organizations want a reporting tool allowing to detect false positives easily and to be able to react quickly in case a targeted attack is detected by the WAF. Having nice charts with the number of attacks do not help to manage or use a WAF.

The above three elements are present in all WAF solutions. In order to have a more complete WAF solution, WAFs providers try to provide some rules or mechanism to generate these.

1. Rules can be written by the WAF provider or can be created by another company or by Open Source project. When rules are provided by the WAF provider or a third party, organizations must take time to understand what

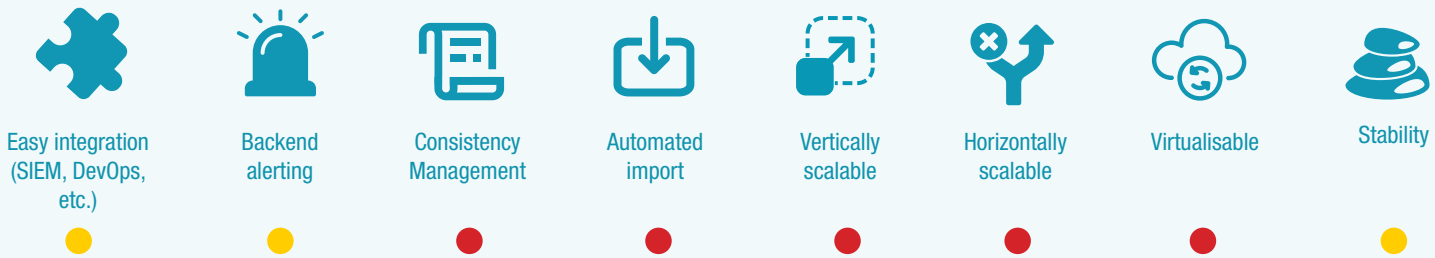
kind of security level is implemented.

   a. How to understand the rules and the methodology behind the rules or is it totally opaque (e.g. “we have rules to protect against OWASP top 10”)?
   b. Are the rules adapted to the current applications and usage?
   c. How can these rules align with the applications?
   d. How to trust new rules?

2. Integration possibilities with the existing deployment and security tools
   a. Can the solution integrate with the existing environment?
   b. Can the configuration be managed together with existing applications?
   c. Can a new configuration be automatically deployed with each new release of the applications?
3. Management of consistency is a critical aspect of a successful WAF. Once a WAF is tested, can the WAF configuration automatically and easily be migrated to the production environment? Has everything to be migrated? Manual migration of all settings is very expensive in time and cost and can cause a change to be forgotten or mistyped.

Organizational tasks are listed as number 2 concern in OWASP WAF Best Practices[3].

Needed deployement & operational features



Needed security features

Mature | Often incomplete | Often missing

3 *OWASP, “Best Practice: Use of Web Application Firewalls”, May 2008, v1.0.5 https://www.owasp.org/index.php/Category:OWASP_Best_Practices:_Use_of_Web_Application_Firewalls*

How many WAFs are required for an organization?

The question looks simple: there is a WAF needed for the production environment and a WAF for the acceptance environment. Obviously, for continuity reasons, some redundancy is needed and thus are these environments usually duplicated.

The reality is more complicated. Since hardware devices are expensive, WAF providers will claim that both production and acceptance environments can run on the same device. And indeed, different virtual sites can be used, but several parameters and rules are defined at the global level – and the application (or firmware) are always global. As a consequence, an organization cannot test a new version of the WAF in acceptance without impacting its production environment. When developing a new rule - or troubleshoot a request in debugging mode – this requires a dedicated system.

Also, to avoid detecting bad practices in the development during the acceptance tests, a WAF is usually added in the integration environment to detect (without blocking) potential problems with the WAF in early stages of development.

Depending on the needs, an organization could potentially need at least six WAF installations.

How to select a WAF successfully?

By raising the right questions, major issues can be avoided: selecting and implementing a WAF solution requires a project approach and a multidisciplinary project team with developers and IT infrastructure teams.

As with every project, requirements must be set and approved:

1. how many applications must be protected,
2. which security level is expected,
3. what workload is accepted,
4. is outsourcing an option,
5. can the WAF run in the cloud,
6. how many WAFs are required,
7. what features are required,
8. how will the WAF be integrated with the DevOps environment,
9. are imports of configuration parts possible,
10. does the WAF have all features to replace current reverse proxy, etc.

By answering these questions from the start, an organization will be able to eliminate most of the inadequate WAF solutions.

Is a WAF making an organization safe and secure?

The value of a WAF lies in the rules that it applies to user responses. These rule settings execute validation procedures that protect a webserver from malicious activity by laying out activities to spot and dictating actions to take when an exploit is discovered. Rules will be written to specifically block well-known attack strategies. However, extra, more flexible rules in the WAF's routines are useful for identifying zero-day threats.

When buying a security solution installed by a third party, it must work properly. However, some third parties are IT

providers with little knowledge about application-level considerations, leaving WAFs almost totally open and providing organizations with a false sense of security, until a security incident occurs.

The golden rule when buying a WAF service is to ask what level of security is implemented with evidence of effectiveness. The silver rule is to check the complete WAF configuration & implementation by an internal security expert or by asking an external security auditor or penetration tester. Obviously, a common-sense control is asking the service provider to provide evidence that the WAF solution is also protecting their own infrastructure under the credo: “eating your own dogfood”.

The future of WAF

The number of security threats is growing each year. Security threats are becoming more advanced, taking multiple routes to get into a website and specifically avoiding those which hackers know may be protected by a traditional rule-based WAF. In addition, as the number and type of devices accessing the Internet becomes larger and more varied, attackers are given more pathways into a network. All of this leads to more sophisticated methods of website security and a search for intelligent or context-based security solutions. These intelligent security solutions do not rely on rulesets only to block attacks but use complex systems to identify threats based on the combined actions they take against a website. By removing the rulesets, intelligent security solutions can stay one step ahead of attackers as they do not know what rules are being used against them. These intelligent or learning security solutions use contextual information such as location, device, time and on-site behavior to build a complete profile of website visitors that allows them to either block or allow them in. This allows WAFs to capture the attacks that are not found by rules-based solutions while still protecting legitimate traffic.

Intelligent WAF solutions look at the combined activity of potentially damaging traffic to determine if an IP address is in the early stages of an attack or collecting information in the background before starting an attack. Intelligent WAF solutions track an attacker across seven stages of attack, to determine when and where hackers need to be stopped. While some activity may immediately set off blocking triggers, other activity is logged and watched in case it progresses. Using intelligent WAF solution means that hackers are stopped while real visitors who initially may look like or share attributes with hackers are not impacted.

One reason the security industry is moving away from making simple yes/no decisions on traffic is the increased complexity of real user behavior that might at first look like malicious behavior. The intelligent WAF solution aims to eliminate an attacker’s ability to use scripting to gain access to a website while reducing false positives by taking into account where information has been loaded along with other factors.

Despite these evolutions, early examples of learning-based security did not perform as expected because the results were different from those found with traditional rules-based approaches. Intelligent WAF solutions still need to gather contextual data around what “normal” traffic for a website looks like before programs are able to identify out-of-the-ordinary requests. However, the benefit of intelligent WAF solutions is that data is examined and stored by a machine, so developers do not need to manually inspect traffic and decide what is expected or unexpected behavior on their specific website.

Modern IT development practices such as agile and DevOps are also on the rise and security providers are increasingly thinking about how to integrate these methods into their offerings. One key component of a DevOps workflow is the use of in-depth metrics and logs to continually assess and tune website configurations and this is no different in security solutions. Logs are essential for developers to understand the traffic coming through their website, what actions users are taking, and how security rules or learning systems are affecting that traffic.

Both developers and business people should be able to easily view cyberthreats and security actions taken against cyberthreats, which is why the intelligent WAF dashboards must be consumable by even non- technical personnel.

The most interesting evolution requested by customers is real application security intelligence. An intelligent WAF

solution alone is not enough anymore; an intelligent layer must be made on top of it to manage all application-level security concerns. Several research teams are developing machine-learning WAF. As machine-learning is heuristic and organizations want a WAF to be close to 100% correct, machine- learning techniques may become integrated in security solutions in a few years – at least if they are combined with the proper real-time application insights.

Conclusions

WAFs are highly useful tools for protecting web applications from a wide variety of web application attacks. Although WAFs are most helpful for applications where source code is not available, other applications benefit because WAFs can provide protection during the period between the discovery of a vulnerability and the release of updated source code.

Organizations with sensitive data available through web applications should definitely use WAF products or services as an important line of defense against data breaches.

Organizations evaluating WAFs to find the best WAF for their situation should be on the lookout for emerging features, such as the use of high-quality threat intelligence feeds, constant updates on the newest vulnerabilities and attacks, and advanced automation capabilities in order to improve the accuracy of WAF detection.

Whether an organization prefers to have its own WAF on its network or goes for a cloud-based WAF solution, depends on the requirements and experience with security service providers. Selecting new equipment, software and services for an organization can be very time consuming. The added extras that each WAF provider offers will direct towards a choice. The capacity of each service is also an important consideration and an organization should factor in scalability so that its future expansion plans are accounted for.

Deciding on going for a hardware WAF or a cloud-based WAF is important. Overlooking the protection that a web application firewall offers the business would be a mistake. Organizations should not wait until it is too late, and their site is under attack. Most important advice to any organization is to get a WAF in place to keep the business online.

ABOUT ISACA BELGIUM

ISACA Belgium (www.isaca.be) is a chapter of ISACA. Nearing its 50th year, ISACA® (www.isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Technology powers today's world and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its half million engaged professionals in information and cyber security, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology.

ISACA has a presence in more than 188 countries, including more than 217 chapters.

AUTHORS
Mr. Marc Stern, expert in WAF implementation since 2001, Approach Belgium
Mr. Egide Nzabonimana, Information Risk Expert and board member of ISACA Belgium

ISACA®
Belgium Chapter