What Is A Web Application Firewall?

WAF

An Introduction to a Web Application Firewall or WAF

A web application firewall (WAF) provides web application security for online services from malicious security attacks such as SQL injection, cross-site scripting (XSS). WAF security detects and filters out threats which could degrade, compromise, or expose online applications to denial-of-service (DoS) attacks. WAF security examines HTTP traffic

before it reaches the application server. They also protect against unauthorized transfer of data from the server.

In recent years, web application security has become increasingly important, especially after web application attacks ranked as the most common reason for breaches, as reported in the Verizon Data Breach Investigations Report. WAFs have become a critical component of web application security, and guard against web application vulnerabilities while providing the ability to customize the security rules for each application. As WAF is inline with traffic, some functions are conveniently implemented by a load balancer.

According to the PCI Security Standards Council, WAFs function as "a security policy enforcement point positioned between a web application and the client endpoint. This functionality can be implemented in software or hardware, running in an appliance device, or in a typical server running a common operating system. It may be a stand-alone device or integrated into other network components."

How Web Application Firewalls Work

WAFs can be built into hardware appliances, server-side software plugins, or filter traffic as-a-service. WAF security protects web applications from malicious endpoints and are essentially opposites of proxy servers (i.e. reverse proxies), which protect devices from malicious applications.

To ensure security, WAFs intercept and examine all HTTP requests. Bogus traffic is simply blocked or tested with CAPTCHA tests designed to stump harmful bots and computer programs.

The fine print of WAF administration is based on security procedures that are built upon customized policies, which should address the top web application security flaws listed by the Open Web Application Security Project (OWASP).

Traditionally, these policies can be elaborate, requiring specialized administrators to configure the WAF in accordance to the company's security policy. These administrators are responsible for correctly placing, configuring, administering, and monitoring WAFs to ensure maximum security.

For more on the actual implementation of web application firewall, check out our Application Delivery How-To Videos or watch Web Application Firewall How To Video here:

Attacks That WAFs Prevent

WAF security can prevent many attacks, including:

Cross-site Scripting (XSS) — Attackers inject client-side scripts into web pages viewed by other users.

SQL injection — Malicious code is inserted or injected into an web entry field that allows attackers to compromise the application and underlying systems.

Cookie poisoning — Modification of a cookie to gain unauthorized information about the user for purposes such as identity theft.

Unvalidated input — Attackers tamper with HTTP request (including the url, headers and form fields) to bypass the site's security mechanisms.

Layer 7 DoS — An HTTP flood attack that utilizes valid requests in typical URL data retrievals.

Web scraping — Data scraping used for extracting data from websites.

Cloud WAF

A cloud WAF – also known as a cloud-based WAF or cloud-native WAF – provides modern web application security at a much lower cost than traditional appliance-based web application firewalls while offering some distinct advantages. Cloud based WAF services offer more responsive, elastic, and customizable application security options based on predefined security policies that scale and react automatically to threats per application or tenant.

The customization and flexibility of such cloud WAF services saves administrators from time-consuming manual tuning of security software or hardware on their systems, allows for proactive rather than responsive threat detection, enables real-time app security insights and visibility, and ensures compliance (GDPR, HIPAA and PCI), all while providing centralized application security across multi-cloud, hybrid-cloud or on premise application environments.

Take a look at this webinar for a better understanding of deploying application security in any data center or cloud with WAF

WATCH HERE

Web Application Firewall Deployment

Reverse Proxy

The WAF is a proxy to the application server. Therefore, device traffic goes directly to the WAF.

Transparent Reverse Proxy

A reverse proxy with transparent mode. As a result, the WAF separately sends filtered traffic to web applications. This allows for IP masking by hiding the address of the application server. Performance latency is a potential downside during translation.

Transparent Bridge

HTTP traffic goes directly to the web application.
As a result, this makes the WAF transparent between the device and the server.

WAF Security Models

WAFs can follow either a positive security model, a negative security model, or a combination of both. A positive security model WAF (also known as “allowlist”) rejects everything not named as allowed. A negative security model (also known as “denylist”) has a list of banned items and allows everything not on that list.

Positive and negative WAF security models have their parts in different application security scenarios. For example:

Positive Security Model

When performing input validation, the positive model dictates that you specify the allowed inputs, as opposed to trying to filter out bad inputs. The benefit of using a positive security model firewall is that new attacks, not anticipated by the developer, will be prevented.

Negative Security Model

The negative model is easier to implement but you’ll never be quite sure that you’ve addressed everything. You’ll also end up with a long list of negative signatures to block that has to be maintained. The negative security model approach initially allows all traffic to come through, although as additional restrictions are implemented, security improves. This

method can save time for departments that consistently make new network changes, so the network does not continue to be blocked.

For more on the actual implementation of web application firewall, check out our Application Delivery How-To Videos or watch positive security in WAF How To Video here:

WAF Rules

WAFs follow rules or policies customized to specific vulnerabilities. Creating the rules on a traditional WAF can be complex and require expert administration. The Open Web Application Security Project (OWASP) maintains a list of the top web application security flaws for WAF policies to address.

WAF security addresses the most common pain-points for application security teams by providing visibility to traffic flows that match security rules.

Overview and Demo of Intelligent Web Application Firewall (iWAF)

OWASP (Open Web Application Security Project)

What is OWASP? OWASP stands for Open Web Application Security Project and is an initiative of The OWASP™ Foundation, a non-profit started in 2001 for the purpose of helping organizations conceive, develop, acquire, operate, and maintain applications that can be trusted. According to their website:

“Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions. OWASP is in a unique position to provide impartial, practical information about AppSec to individuals, corporations, universities, government agencies, and other organizations worldwide. Operating as a community of like-minded

professionals, OWASP issues software tools and knowledge-based documentation on application security."

OWASP is an international organization that allows the use of their tools, forums, code and other documents by anyone that has the end goal of improving application security or developing any new kind WAF security device. OWASP is not affiliated with any technology company and they support the informed use of commercial application security technology. Similar to many open-source security software projects, OWASP produces different types of materials in a collaborative and open-source manner. Their resources and conferences provide web application firewall training as well as best practices and source code.

Web Application Firewall Benefits vs Weaknesses

Web Application Firewall Benefits

WAF security prevents attacks that try to take advantage of the vulnerabilities in web-based applications. Vulnerabilities can be common in legacy applications or applications with poor coding or designs. WAFs handle the code deficiencies
with custom rules or policies.

WAFs offer protection against diverse threats, including the following:

SQL injection, comment spam

Cross-site scripting (XSS)

Distributed denial of service (DDoS) attacks

Application-specific attacks

Other benefits include:

Strong default rule sets

Customized Layer 7 protection

Integration with DDoS mitigation

Real-time reporting and logging for instant visibility

Top web application firewalls use application intelligence to offer advanced WAF capabilities like real-time insights into application traffic, performance, security and threat landscape. This visibility gives administrators the flexibility to respond to the most sophisticated attacks.

When the Open Web Application Security Project (OWASP) identifies the most common vulnerabilities, WAFs allow administrators to create custom security rules to combat the list of potential attack methods. An intelligent WAF analyzes the security rules matching a particular transaction and provides a real-time view as attack patterns evolve. Based on this intelligence, the WAF can reduce false positives. While these features contribute to web application firewall benefits, there are still some weaknesses to be aware of.

Web Application Firewall Weaknesses

WAFs sit in-line between users and applications. Therefore any delay or latency can impact the end user experience. Since the inspection of requests and responses is compute-intensive, WAFs do introduce traffic latency. The extent of that delay, and whether it would even be tolerable to an end user depends on the WAF's performance, policy complexity and the application in use. This can put organizations in a compromising situation: over-

provision their WAFs to ensure minimal impact, which comes at a higher cost; or set security policies to a minimum to reduce inspection time, which compromises safety.

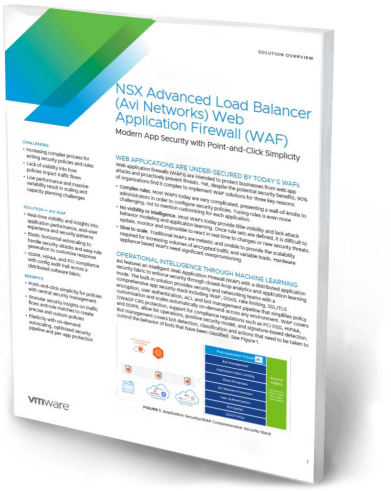
WAFs can also be complex to deploy given the need to establish efficient policies. They also require regular maintenance when applications have additions or updates.

Known Web Application Firewall Vulnerabilities

Because WAFs rely heavily on configuring security rules and policies to defend against cross-site scripting (XSS), cross-site request forgery (CSRF) and SQL injection, WAFs need to be actively maintained and configured correctly rather than just configuring once and expecting full protection.

WAFs are often subject to a high degree of false positives (blocking harmless traffic) and false negatives (allowing harmful traffic) because the application being protected by WAF security is constantly changing as user demand changes and thus requires different rules for its traffic over time. Additionally, security protocols are often neglected and preventive measures such as code and infrastructure audits are not taken because of the false sense of complete web application security when using WAFs leading to data leakage that exposes company and user data.

New WAF vulnerabilities arise during the development of new digital tools – including cloud WAFs – so although many security flaws are resolved, new WAF vulnerabilities can always appear. This makes the need for specialist third-party cloud-based WAF vendors to provide and maintain complex security rules more important.



Intelligent Web Application Firewall

with point-and-click simplicity and webscale performance

Traditional web application security solutions do not provide visibility and security insights that administrators can use to create an effective application security posture. Enterprises need real-time visibility into application traffic, user experience, security and threat landscape, and application performance to identify and protect against the most sophisticated attacks. Appliance-based web application firewall (WAF) solutions do not leverage their privileged position in the path of application traffic and are black boxes when it comes to delivering application visibility.

DOWNLOAD NOW

WAF Capabilities

A Web Application Firewall is the first line of defense against sophisticated attacks that would threaten the integrity of your enterprise. The most effective and efficient solutions offer the following WAF capabilities:

Input protection — extensive application profiling detects acceptable user input

HTTP validation — detects HTTP security flaws and sets custom validation rules to block attacks

Data leakage prevention – early warning data leakage detection system detects vulnerable security configurations and identifies, filters, and shields private data.

Automated attack blocking — automation tools take proactive countermeasures to protect your network from malicious traffic

Policies tailored to widely used applications — customized WAF network security policies target vulnerabilities specific to your application, offering real-time insights

Granular security insights on traffic flows -— provides access to application traffic, performance, security and threat landscape

Point-and-click policy configurations, customizable for each application — an advanced WAF provides a central, scalable security solution for simple policy management

Central, scalable policy management — centralized management allows admins to manage any number of Web Application Firewalls with different configurations from a single console and scale up or down with more efficiency despite overall WAF security architecture

WAF Security to Prevent Data Leakage

Enterprises must protect themselves from unauthorized transmission of data to external destinations. Consequences of data leakage such as reputational harm, financial penalties or intensive lawsuits can be serious for any organization, regardless of size or industry. Although certain types of data leakage such as intentional data leakage attacks from ill-intentioned employees can be difficult to prevent, WAF can protect against cyber data leakage threats like Malware and Phishing attacks where sensitive data is vulnerable to malicious outsiders.

Avi's WAF data leakage solution involves data leakage machine learning and other data leakage tools used to discover and control all sensitive information in order to mitigate data leakage risk that could lead to serious consequences for an organization.

Web Application Firewall Architecture

Even the most advanced web application architectures contain a surprising amount of security flaws. This can make them vulnerable to common attacks such as brute force attacks and even complicated attacks like implementing XML external entities or cross-site request forgery. Fortunately, there are specific approaches to configuring WAF security architecture that will minimize the effectiveness and frequency of the many different attacks.

System architecture teams should consider different structures for a web application architecture so that the web application firewall's effectiveness is maximized for that specific configuration. There are basic secure web application architectures (single-tier or two-tier) where the application's web server and database server have the same host machine. This architecture is useful for early stages of project development. Although, it is not good for production applications as it introduces a single point of failure. A multi-tier / N-tier architecture separates different components of the application into multiple tiers according to their functions and each tier runs on a different system. This provides compartmentalization and avoids a single point of failure.

In most application architectures, the WAF is best positioned behind the load balancing tier to maximize utilization, performance, reliability and visibility.

WAFs are an L7 proxy-based security service and can be deployed anywhere in the data path. However, we recommend positioning WAFs closest to the application they are protecting behind the load balancing tier to optimize your architecture for utilization, performance, reliability, and visibility.

WAF Utilization

WAF Performance

WAF Reliability

WAF Visibility

CPU resources are intensive for WAFs because they are dealing with the entire traffic load to evaluate if requests are valid and safe so maximizing utilization from specific WAF placement in the data path is critical.

WAF and DDoS

DDoS for distributed denial of service and occurs when multiple compromised systems are used to target a single system causing a Denial of Service (DoS) attack. Targets of DDoS attacks consist of both the end targeted system and all systems deleteriously used and controlled by the hacker in the distributed attack.

In regards to web application security specifically, DDoS attacks attempt to either exploit specific functions/features within a web-facing application to render those functions/features inoperable or to exploit a broader set of vulnerabilities within an organization's network architecture.
WAF DDoS Protection hinges on the ability of the WAF to correctly recognize the difference between and filtering incoming healthy end user traffic from simulated traffic originating from bots and hijacked browsers. WAFs are considered better at doing this than older DDoS protection solutions because they analyze HTTP requests and protect more of the application stack working to understand how an application works beyond the

communications layer. This allows the WAF to construct a profile of what “normal” requests and inputs look like and use that as a benchmark to better determine what malicious DDoS attacks look like.

DDoS WAF protection can then use device fingerprinting to identify safe and potentially harmful users. Safe users are confirmed by identifying consistent behaviors that are interacting with applications within normal parameters and harmful users are identified when the DDoS enabled WAF does not recognize the behavior pattern from its referenced database.

WAF Testing

An effective WAF testing process requires rigorous testing. Simply testing canned attempts from scanners is not enough. The most accurate WAF test measures effectiveness against logical attacks on the application. This includes knowing how many real attacks were blocked and allowed through. It also answers not only which valid requests were allowed though, but which were inappropriately blocked.

When asking how to test a web application firewall, it is best to use a WAF testing framework that follows these steps:

Test the application without the WAF in front.

Verify if the attacks still succeed with the WAF in its default configuration.

Configure the WAF to determine if it can block attacks in the first two steps.

Verify if the attacks still go through after the WAF has been configured to block them.

This WAF testing process determines whether a front-facing WAF benefits an application. It also lets the WAF be configured to protect against specific attacks. Finally, it determines how effective the WAF is against logical attacks.

The WAF testing process should include the following testing stages:

- Default no configuration settings (no WAF protection).
- Restrictions for URL access only.

URL restriction and parameter inspection.

Simple URL restrictions and parameter checking for basic HTTP traffic with specific malicious traffic inspection.

File upload facilities inspected for malicious content.

A WAF testing tool must be able test the resilience of web application firewalls against attackers with advanced skills. This means a WAF testing tool can't just check for vulnerabilities. It needs to generate both legitimate traffic and attack traffic to determine if the WAF can stop attacks without blocking valid requests.

Traditional Firewalls vs Web Application Firewalls

A traditional firewall protects the flow of information between servers while WAFs are able to filter traffic for a specific web application. Network firewalls and web-application firewalls are complementary and can work together. WAF capabilities and traditional firewall security can combine port/protocol inspection and application-level inspection to prevent intrusion and utilize external intelligence sources.

Another distinction from traditional firewalls versus web application firewalls is that traditional security methods include network firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS). These are effective at blocking illegitimate L3-L4 traffic, based on Open Systems Interconnection (OSI) model. Depending on the protocol being run, traditional firewalls can operate using a stateless method or a stateful method.Traditional firewalls cannot detect attacks unique to the security flaws in web applications because they do not understand Hypertext Transfer Protocol (HTTP) which occurs at layer 7 of the OSI model. They also only allow the port that sends and receives requested web pages from a HTTP server to be open or closed. This is why WAFs are important for preventing attacks like SQL injections, session hijacking and Cross-site Scripting (XSS).

Web Application Firewall vs Next Generation Firewall

Next Generation Firewalls concentrate on application stream signatures which work well for outbound internet traffic but offer very little inbound web server protection.

Web Security Gateway vs Web Application Firewall

Web security gateways defend the clients on your network while browsing the internet, not protecting your network from clients accessing your published web services.

Cloud WAF vs On-Premises WAF

There are two main varieties of Web Application Firewall solutions — on-premise WAF (aka Hardware WAF) or cloud WAF. Deciding which is best for your enterprise depends entirely on your needs.

Cloud WAFs, provided via SaaS, are managed by your cloud vendor: hardware or software, updates, and security are all maintained by your chosen provider and accessed through a mobile app or web interface. A high compute capacity makes cloud WAFs more efficient than their hardware counterparts at detection of attacks (DDoS), deep security insights with real-time monitoring, and minimization of false positives with advanced analytics.

With simple point-and-click configuration, cloud WAFs grow with you, scaling to your capacity needs on a flexible, responsive platform. Comprehensive, high performance security helps meet compliance requirements like GDPR, PCI DSS, and HIPAA. Typically, a usage-based payment plan for a web application security firewall is arranged in advance.

On-Premises hardware WAFs require far more legwork for security and IT teams, but can provide more fine-tuning customization.

Where cloud software is stored and managed in the provider's high security data center, your administrators will need to dedicate an in-house team to secure your network. The procurement and installment of hardware or software, maintenance, configuration, and updates are usually the technical team's responsibility.

Estimating capacity with hardware WAFs may result in either an excess of or deficient security, depending on fluctuating traffic. Scaling to meet capacity needs will require further WAF hardware adjustments. Having full access to all of the elements of your platform may be the right plan for your enterprise, allowing you full reign to customize the experience to your unique specifications.

Open-Source Web Application Firewall

With the increased need for customizable application security after the turn of the century there has been an increase in overall web application firewall market size and has led to greater demand of open source web application firewalls.

Open source WAFs give enterprises more flexibility to deploy customized security policies, develop custom security dashboards to monitor and prevent sophisticated attacks and automate routine security tasks that can take IT security teams more time to deploy with on-premise WAFs. This is achieved through the use of application security source code that has been made available by the active open-source WAF community online or by providers such as ModSecurity.

Open-source WAF platforms offer a tools for real-time web application monitoring, access and event logging usually in two common deployment methods; embedded and reverse proxy. Open source web application firewalls offer the protection against: cross-site scripting, trojan, information leakage, SQL injection and more but can be deployed in a more customized or a la carte' way to save on costs and complexity in comparison to full featured cloud-based or on-premise WAFs. Open-source WAFs features include:

> Continuous passive security assessment: a variation of real-time security monitoring, where focus is shifted from the behavior of the external parties, to the behavior of the system itself. This can act as an early detection system that catches irregularities and weaknesses.

Real-time application security monitoring: Instant access to HTTP traffic stream in real-time displayed in customizable security dashboards.

Full HTTP traffic logging: Traditional web servers typically do very little security logging especially large volumes transactional data that can be critical to secure. Open source WAF functions can be created to log raw transaction data with rules applied to which transactions should be logged and which are ignored which can be important for analyzing security health.

Web application hardening: Allows fixes to be implemented for web application hardening to narrow the HTTP features your specific web application firewall architecture is willing to allow. These attack surface reduction in HTTP features include; request methods, request headers, content types and more. This makes it possible to fix session management issues, as well as cross-site request forgery vulnerabilities.

WAF Learning Mode

WAF Learning Mode refer to a mode or feature where WAFs are observing activity in an application protected by the firewall and generating a list of repeated patterns of activity in order to generate rules for what is normal vs. malicious activity. This mode is used to determine if the WAF security rules and configurations are too strict or relaxed and enables the WAF to automatically be adjusted. The primary objective is to prevent false positives from causing problems with the functionality of a site.

When a web application firewall learning mode is active, users and/or admins can visit their site or application and carry out typical daily tasks and use every feature on the site frequently, decreasing the chances of unwanted blocks of valid actions or vice versa when the WAF is taken out of learning mode and effectively creating a more secure application environment with more consistent security rules.

Suspicious requests are allowlisted in WAF Learning Mode, allowing users to log and see violations, but also allowing the request to go through. If allowlisting is triggered in Learning Mode, users can access the IP address and determine if the action was internal or

external. Parameter values are gathered and stored as reference values or generalized into a value set or reference pattern.

WAF Webinar: Web Application Security

for Continuous Delivery Pipelines

Traditional web application security solutions do not provide visibility and security insights that administrators can use to create an effective application security posture. Enterprises need real-time visibility into application traffic, user experience, security and threat landscape, and application performance to identify and protect against the most sophisticated attacks. Appliance-based web application firewall (WAF) solutions do not leverage their privileged position in the path of application traffic and are blackboxes when it comes to delivering application visibility.

WATCH NOW

Web Application Firewall Comparison

Azure Web Application Firewall

Microsoft offers its Azure Application Gateway WAF as a centrally-managed, layer 7 security solution that integrates into the Azure security center and provides convenient security management without requiring application changes. The Azure Application

Gateway WAF pricing is built into the overall pricing model, which depends on the amount of data processed by gateways and the amount of time when gateways are provisioned and available.

AWS Web Application Firewall

The Amazon WAF allows users to add a web application firewall option for existing AWS solutions. Unlike other vendors, users do not pay lump sum fees for WAF application security, but are billed for the number of AWS WAF rules added and web requests received per month. To reduce the need to configure customized security policies, the AWS WAF Security Automation feature automatically provides a web ACL with a AWS WAF rules that filter prevalent web-based attacks. Users can then choose which protective features to include with their AWS WAFs.

Barracuda Networks Web Application Firewall

The Barracuda Networks web application firewall comes as a hardware or virtual appliance that can be deployed in an on-prem data center or in the cloud. Like other top web application firewalls, the Barracuda web application firewall monitors Layer 7 traffic and provides visibility to the application level and Layer 4 traffic. The Barracuda WAF redirect HTTP to HTTPS feature allows enterprises to automatically encrypt communications. Users can also configure Barracuda WAF DDoS protection to ensure high availability for legitimate clients.

A10 Web Application Firewall

The A10 WAF application firewall is part of the A10 Thunder of AX series of application delivery controllers. It is integrated with other A10 security features within the Advanced Core Operating System (ACOS). A10 developed its web application firewall features specifically for ACOS and does not integrate third party WAF code. This makes things easy to configure and scale. The A10 WAF works with other A10 security mechanisms to assist with regulatory security compliance, such as Payment Card Industry (PCI) and Data Security Standard (DSS) requirements.

ACE Web Application Firewall

The Cisco ACE web application firewall is retired and support ended in January 2016. Avi Networks offers documentation on Cisco Ace Replacement with our Replace Cisco ACE with a Software Load Balancer White Paper.

Akamai Web Application Firewall

The Akamai web application firewall is called Kona WAF. It is distributed on the Akamai Intelligent Platform. Kona WAF is deployed at the edge of a network instead of a data center. Kona's web application firewall services handle threatening traffic without affecting the origin server's performance.

Cisco ASA Web Application Firewall

The ASA 5500-X series is a next-generation firewall (NGFW) that is threat-focused. The Cisco ASA web application firewall earned high security effectiveness scores in third-party testing for both NGIPS and AMP. The Firepower Management Center gives users insights into threats and vulnerabilities from the data center to mobile devices.

Cloudflare Web Application Firewall

The Cloudflare web application firewall includes 148 built-in WAF rules that can be applied with one click. This protection is in addition to safeguards from the OWASP top 10 vulnerabilities, which are provided by default. Business and enterprise customers can request custom WAF rules for specific threats. The Cloudflare WAF challenges web visitors with a CAPTCHA test. It also offers a range of security settings from low to high.

Comodo Web Application Firewall

The Comodo web application firewall supports ModSecurity rules by providing advanced filtering, security and intrusion protection. Comodo WAF install offers real-time protection for web applications running on Apache, LiteSpeed and NGINX on Linux web application firewall.

dotDefender Web Application Firewall

The dotDefender web application firewall uses the following engines: Pattern Recognition, Signature Knowledgebase, Data Leakage Protection and Upload Inspection. The dotDefender web application firewall architecture handles .NET Framework security issues.

F5 Web Application Firewall

The F5 web application firewall is also known as Advanced WAF. It protects against the most common attacks on an app without having to update the app itself. Advanced WAF is available in public cloud providers like Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform. F5 Advanced WAF uses behavioral analytics and machine learning for Layer 7 denial-of-service (DoS) detection. It also encrypts data at the app layer to protect against data-extracting malware.

NGINX Web Application Firewall

The NGINX web application firewall is based on ModSecurity open source software. The NGINX WAF can be deployed in any environment including bare metal, public cloud, private cloud, hybrid cloud, virtual machines and containers. It protects applications against sophisticated Layer 7 attacks.

Penta Security Web Application Firewall

The Penta Security web application firewall is a virtual WAF called WAPPLES SA (Software Appliance). It can be integrated with cloud WAF systems and other virtual environments. WAPPLES SA has support for hypervisors including KVM, XenServer and vSphere. Penta Security's web application firewall is geared toward small and medium-sized businesses (SMBs).

Radware Web Application Firewall

The Radware web application firewall is a cloud-based WAF service. It is based on Radware's ICSA Labs. It provides enterprise-grade and continuously adaptive web application security protection for the OWASP top 10 threats.

SonicWall Web Application Firewall

The SonicWall web application firewall (WAF) can be deployed as a virtual appliance in private clouds based on VMWare or Microsoft Hyper-V. This can also be deployed in AWS or Microsoft Azure public cloud environments. The SonicWall web application firewall service applies Layer-7 application delivery capabilities that include load balancing and SSL offloading. The SonicWall web application firewall provides economy of scale benefits of virtualization along with the security advantages of a physical WAF.

Tipping Point Web Application Firewall

The Tipping Point web application firewall is a next-generation firewall offered by HP. The HP web application firewall provides real-time visibility, analytics and centralized management over authorized and unauthorized applications without compromising network availability. The HP WAF is one of the top web application firewalls providing insight into the security and threat landscape, as well as application traffic, user experience, and application performance.

History of Firewalls and WAFs

Technically, the term firewall was coined in 1851 as a physical wall to prevent the spread of fire. In modern times, the Morris virus — unleashed in 1988 — was was one of the first Internet viruses that created the need for a virtual firewall. In the early 1990s, a network-based firewall was developed that could specifically protect FTP traffic. This was the beginning of firewalls being able to control access to applications or services. By the end of the 1990s, with the increase in online activity, the hacking of web servers became problematic, and the focus turned to development of Web Application Firewalls (WAFs).

By 2002, WAFs were in greater use and an open source project called ModSecurity created a core set of WAF security rules. The Open Web Application Security Project (OWASP) began to further expand and standardize the capability of WAFs. Every three or four years, the OWASP TOP 10 list of web security vulnerabilities is published for the compliance industry to address.

Web Application Firewall and Gartner

The global web application firewall market is growing, driven by the adoption of cloud WAF services. IT consulting firm Gartner has conducted extensive data analysis to demonstrate WAF market trends, direction, maturity and participants.

Enterprise security and IT teams can use the web application firewall gartner report as a resource for evaluating, configuring and maintaining a WAF security architecture to provide the best WAF solution for their specific needs.

Top 5 WAF Best Practices

WAF provides protection against all types of Web attacks, such as Cross-Site Scripting (XXS), SQL Injection, and Path Traversal. In order to have the most effective protection against such attacks, below are the top 5 WAF best practices.

Create a web application firewall security plan that outlines the goals of your organization and keeps you organized.

Figure out which applications your organization uses and look through the inventory.

Vet through the web applications and prioritize them by three categories: Critical, Serious, and Normal. This will help you identify which ones need extensive or intensive testing.

As you're prioritizing the applications, also indicate which vulnerabilities are worth excluding so you can focus on the more threatening vulnerabilities.

Keep application privileges at a minimum. All web applications have a series of privileges, which should be modified in order to enhance security.

WAF Use Cases

Protect Websites and Applications

True to its name, one of the main use cases for WAF is to protect applications that communicate over HTTP, such as websites, serverless functions, and API endpoints.

Without WAF, known and unknown attacks would not be detected, data leaks could not be prevented, and URLs and ports would have little to no access.

Comply with Security and Regulatory Standards

Along with preventing threats, setting up a WAF is the fastest and most efficient way to comply with regulatory standards and security. As an example, websites that process credit card data must comply with the Payment Card Industry Data Security Standard (PCI-DSS). Companies like credit card companies are in greater need of increased security levels, which is where WAF comes into play.

Control Bots and Prevent DDoS attacks

As bots are used more and more, WAF helps with controlling how much these bots access our systems. While the good bots help with keeping things working, WAF is needed to manage the bad bots — Bad bots will send spam, steal information, scrape website content, initiate DDoS attacks, and more.

Patch Vulnerabilities

When securing an application, the chances are still there of vulnerabilities lurking into production. For a solution to be found and patch to be released, it will take some time. WAF will be the best way of securing these patches.

Detect Intrusions in Real-Time

The best and efficient way to detect attacks is to keep track of traffic in real-time so security teams can act accordingly. This can be difficult on a distributed system since logs are scattered on many interfaces. WAF has a particular focus on security as it operates as the central point of logging and metrics collection. The logs it monitors are also very important for identifying and evaluating previous attack attempts.

Enforce Content Policies

One of the last WAF use cases is the ability to inspect and filter HTTP packets. With this, rules can be set up by organizations to allow or block connections based on their content.

WAF vs IPS

Again, a web application firewall (WAF) provides web security for online services from malicious security attacks such as SQL injection, cross-site scripting (XSS). Intrusion Prevention System (IPS) is similar where it tries to identify detected threats and prevent them. The IPS is constantly tracking the network to look for potential dangerous events and collecting information on them. The biggest difference between WAF and IPS is the level of intelligence that is needed to analyze traffic on Layer 7. WAF is alert for any attempts to access a web application, whether it be meetings, users and programs while IPS is solely based on signatures and is not aware of sessions and users trying to gain access to a web application.

3 Types of WAF

There are a wide variety of web application firewalls in the market, but not all are the same. Each type has their own set of advantages and disadvantages which is why it's important to know which is the right fit for your business needs.

Hardware-Based Web Application Firewall

A hardware-based WAF is typically deployed through a hardware appliance and installed within the local area network (LAN), closer to the application and web servers. An operating system supports software configurations and updates as it runs within the appliance. Hardware-based WAF's biggest advantage is its fast speed and high performance.

Software-Based Web Application Firewall

Unlike the hardware-based WAF that's deployed through a physical hardware appliance, a software-based WAF is installed in a virtual machine (VM). This is essentially the same as

the components of a hardware WAF, with the only difference being users needing their own hypervisor to run the virtual machine. Software-based WAF is a great choice for its flexibility.

Cloud-Based Web Application Firewall

Being a part of the newer generation of WAF, cloud-based WAF is managed directly by a service provider in the form of SaaS (software-as-a-service). Its components are solely located in the cloud, which is beneficial for the user as they do not need to install anything locally or in any virtual machines. The biggest advantage to this WAF is its simplicity.

WAF Implementation

WAF implementation is the process of integrating a WAF into a web application or a web application delivery infrastructure to provide an additional layer of protection against various web-based attacks. The implementation typically involves configuring the WAF to enforce a set of security policies designed to detect and block malicious traffic targeting the web application. This may include defining rules to inspect incoming HTTP/S traffic for patterns and anomalies that indicate an attack, such as SQL injection or cross-site scripting (XSS).

WAF implementation may also require integrating the WAF with other security solutions, such as intrusion prevention systems (IPS) and security information and event management (SIEM) platforms, to enable better threat detection and response capabilities. Overall, WAF implementation is a critical aspect of web application security that helps protect against a wide range of attacks that target web applications and web services.

Check out this webinar to learn how you can prevent threats with WAF protection capabilities

WATCH HERE