WEB APPLICATION FIREWALL

Defense against Layer-7 Attacks

Edited by **MOHAN DAS VISWAM**

The application layer (L7) is the hardest to defend. Hackers get direct access to the bounty they are seeking, by compromising layer-7. The need is to have a product with an understanding of the "real-world techniques" or "methods" hackers use. It is here that the Web Application Firewall technology delivers the promise. With the right WAF with right policies in place, you can block the array of attacks that aim to exfiltrate data.

Ratnaboli Ghorai Dinda
Dy. Director General
& HoG
ratnaboli@nic.in

Raj K. Raina
Sr. Technical Director
& HoD
rk.raina@nic.in

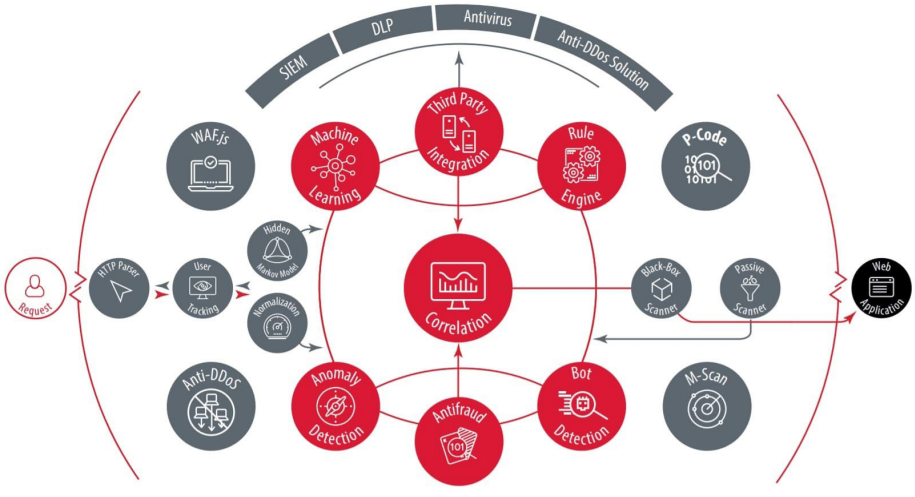
Web Application Firewall (WAF) is the latest entry into the Layered Data Centre Security model. It forms an integral part of a multilayer security architecture and provides security at the topmost layer of TCP/ IP stack that is most vulnerable and most targeted in the current threat landscape. Web Application Firewalls examine the data payload beyond the simple IP and TCP header examination. They protect web systems against known and unknown threats and vulnerabilities. Customized inspections can detect and prevent several of the most dangerous application security flaws.

Next-Generation Firewall (NGFW) and Intrusion Prevention/Detection System (IPS/IDS) are powerless to tackle and handle modern web attacks. So here is where the Web Application Firewall fills the gap. Acting as an intermediary service between your website application and the visitor browsing your site, WAF intercepts and strips malicious requests before they can cause any damage. With application layer logic fundamental to its working, WAF can detect/understand unusual traffic activity with ease.

Internal Architecture

The internal structure of the Web Application Firewall is often complex and the interaction between components changes from one manufacturer to other. However, the resultant impact of deploying WAF is roughly the same. The below-given figure depicts a typical internal structuring of WAF.

▼ WAF Architecture



While WAF is important, it is most effective with other security components. A comprehensive enterprise security model positions a WAF alongside IPS, NGFW, Scanner, SIEM, etc.

WAF Policies & Working Models

WAF analyses Hypertext Transfer Protocol (HTTP) requests and applies a set of rules to understand what parts of that conversation are benign and what parts are malicious. It employs various approaches/models to analyze and filter the content. WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic.

WAF that operates based on a blacklist (negative security model) protects against known attacks. This model is appropriate for public websites where sources are unknown. However, the model highly resources intensive.

Conversely, WAF based on an allow list (positive security model) only admits traffic that has been pre-approved. It is highly efficient but may at times un-intentionally block benign traffic. Web Application Firewalls also offer a hybrid security model, that implements elements of both.

WAF Deployment Architecture

There are two main architectural considerations related to WAF placement: In-line or tap/ span.

IN-LINE

In this architecture, the WAF is placed direct-

ly in the traffic path between the requestor (for example, a browser client) and the Web application server. Within the in-line model, WAF can be configured in a) routed b) Bridged or c) Reverse Proxy method to inspect and process the traffic. In-line WAFs actively block the requests that violate the rule sets. This architecture demands caution to ensure no service interruption surprises happen in production. Alternately, it is possible to run a WAF in-line, but keep it in a monitor-only (or passive) mode.

TAP/ SPAN

This mode is also known as "passive" mode because the WAF is kept out of the traffic path and monitors traffic from a tap or span port. Tap/ span WAFs are often used to collect data for use in investigatory or forensic analysis. This mode supports traffic blocking by communicating to another system (like a network firewall) and having that system perform the blocking.

Further, an Application Firewall can be network-based or host-based, or cloud-based. It is primarily deployed in the reverse-proxy mode and is placed in front of one or more websites or applications.

We can deploy a WAF appliance ON-Premise or have a hosted virtual appliance. An evolving architecture is Cloud-delivered WAF as-a-service.

Cloud and Virtualization are driving the need for new architectural models in Web Application Firewalls. Cloud-based WAFs intercept traffic before it enters the organization's network. Virtualized environments present a unique challenge because the VMs running on top of a hypervisor form their mini-network where traffic is passed from server to server without having to traverse the network. To prevent application attacks intra-VM, a WAF needs to be able to see the traffic. This can be accomplished by using an API to monitor activity via the hypervisor. WAF can fit in an organization's architecture easily with its various form factor choices. A host WAF is a software option where the software is installed on the same server that the Web application is running.

Detection Techniques

WAFs (most of them) use a blended approach of different techniques to ensure the most accurate detection coverage. These techniques are:

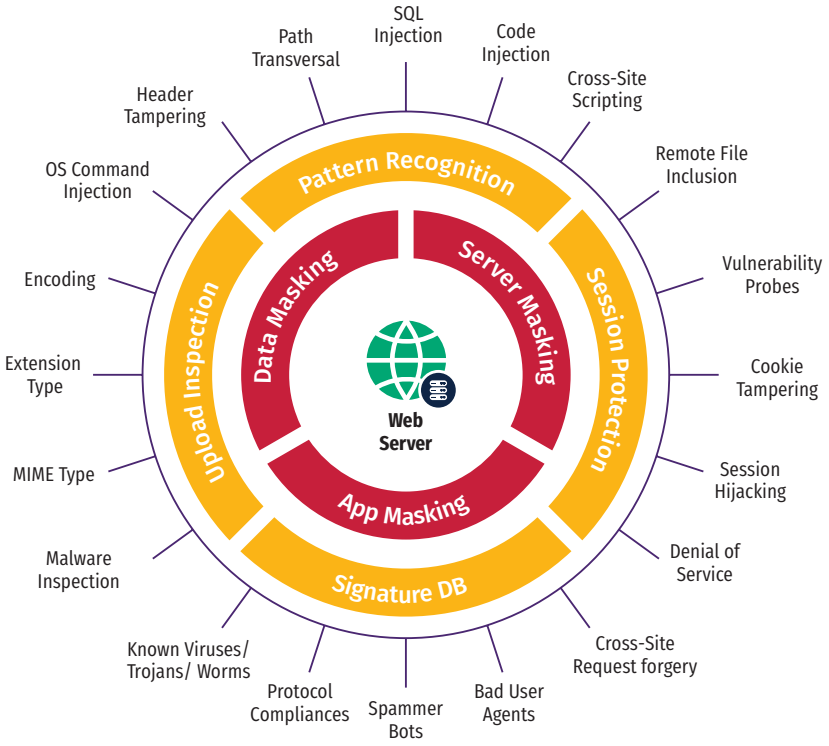
Signatures - Similar to the signatures for anti-virus and Intrusion Prevention Systems (IPS) WAF signatures match a pre-set string or regular expression (RegEx) to the traffic looking for known attacks. WAF ships with a set of signatures and these are updated by the OEMs regularly with the evolution of attacks.

Rules - Rules define how to inspect a web request and what to do when the request matches the inspection criteria. Generally, it links together a series of strings with logical operators like AND, OR, NOT and may contain nested statements at any depth. WAFs can also "learn" traffic patterns on the fly and look for anomalies on a set of baseline rules. This intelligence can be used for a new rule setting for the WAF or on a complimentary protection device like an IPS or network firewall

Normalization - Attackers often manipulate an exploit payload to bypass WAF detection (for example by URL-encoding portions of the payload). WAFs normalize the requests to perform analysis and bust the evasion by attackers e.g. escaped and encoded characters, self-referencing paths, international character sets, etc.

APIs - WAFs offer API support to build custom detection techniques or rules for specialized assessments, such as logic checks. These APIs are integrated with the WAF parsing engine

▼ Application Fortification



Special WAF Features

Virtual Patching

WAF helps to shorten the window of exposure to vulnerabilities. If your application is hosted on a platform that has a known vulnerability, but you have not had a chance to patch it yet, you can write a rule that looks for traffic attempting to exploit that vulnerability and block the traffic until you can get the vulnerable system patched. This is known as virtual patching. Virtual patches are a key component of a strong WAF, often requiring integration with a vulnerability scanner.

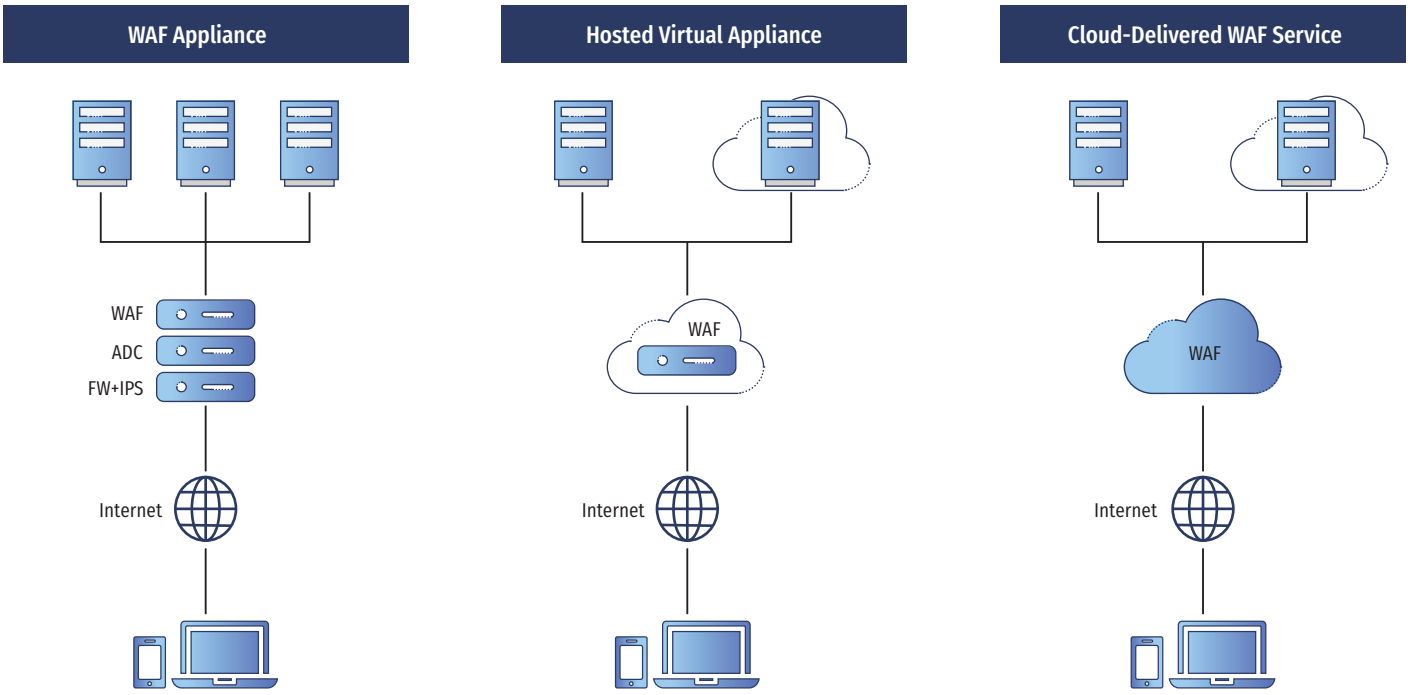
It is always difficult to keep pace with the number of vulnerabilities and updates on open-source servers that we commonly use today eg. Drupal, WordPress, Joomla, etc. Their vulnerabilities can be taken care of by virtual patching. Virtual Patching helps to protect legacy applications that may have limited to no resources to build security controls into the application or fix vulnerabilities in source code

SSL & Weak Cypher Overrides

Encryption protects data in the traffic stream from prying eyes and the option here is to give the keys to the WAF so the stream can be decrypted, inspected, and processed. Additionally, WAF plugs the weak ciphers to prevent side-channel or downgrade attacks. When a client tries to use disabled/ vulnerable SSL/TLS protocols or cipher suites, the request is redirected to specific error page/s. At the same time, a WAF can define cipher suite overrides for each version of the SSL/ TLS protocols.

Emergency Hosting (Audit Exemption)

Web Application Firewall is vital to enable emergency hosting as it dynamically models an application structure and its elements. It understands the expected application responses and usage. Accordingly, it profiles the URLs, Directories, Cookies, Form fields, URL parameters, HTTP methods, and Referrers. Having understood the application, it provides a Layer-7 shield around it. This protective shield, however, must not be construed as a replacement of necessary audit compliance which has to be met anyhow. WAF service essentially takes care of vulnerabilities that are either altogether new or are missed/ uncovered via penetration testing or source code reviews.



▲ WAF architectural models

Data Protection Standards

WAF helps to achieve and meet data protection standards like PCI-DSS by protecting sensitive data (like credit card data or customer records or other personal details) stored in the backend databases and accessible through web applications. The attack-mitigation power of a WAF integrated with the data from scanning technology is the strongest bet.

Data Leakage Prevention

Web Application Firewall inspects outbound traffic and prevents leakage and theft of sensitive data by masking or suppressing the information. This includes server software information, credit cards numbers, social security numbers, PAN, Aadhaar numbers, etc.

BAD BOTS: The Advanced Behavior Analysis and unique device Fingerprinting helps to detect bad bots in real-time. WAF also identifies bad bots by challenge-based approach say requiring client browser to perform a calculation and return the result to a webserver through a cookie.

API Gateway

As an API gateway (in reverse proxy mode), WAF offers robust security in a micro-services architecture. It creates an orchestration for the backend. It receives API calls from the clients, authenticates them, and routes each call to their respective backend.

HTTP Flood Mitigation

WAF prevents the HTTP flood attacks which pass through the Network DDoS devices unnoticed e.g. Slowloris, SYN flood, cache-bypass floods, etc. These requests which seem legitimate can be highly resource-consuming to the extent of bringing down the application.

WAF requires constant tuning

WAF installation is not a one-time job. In the world of WAFs, two things are always changing; Web applications and the threat landscape. The fast growing threat landscape is amplified by the vulnerabilities present in the application. We need to constantly tune/ modify our WAF rules to effectively address both situations.

WAF Service @ NICNET

NIC is in the process of an ambitious plan of WAF-as-a-Service roll-out across NICNET. It is a scalable model envisaged to meet the application throughput requirements across all data centers as well as over the NICNET cloud. Presently WAF services are being provided in the National Data Centre at Shastri Park and National Data Centre, Hyderabad. Appliance-based WAF devices are commissioned to provide WAF Services to critical web applications. The ELK stack technology is used in conjunction with Zabbix and Grafana for monitoring and analyzing the WAF logs to find traces of malicious activities and their sources. The 24x7 monitoring ensures that the attacks are identified early and the intelligence is used to sanitize other security devices.

Surveillance of the health of WAF devices and the services is ensured through a Command-n-Control dashboard.

How effective a WAF can be!

This can be gauged from the very fact that NICNET has not witnessed any defacement in applications that are served by Web Application Firewall.

For further information, please contact:

Raj K. Raina
Sr. Technical Director & HoD
Application Security Technology Division
National Informatics Centre
CGO Complex, Lodhi Road
New Delhi 110003

Email: rk.raina@nic.in, Phone: 011-24305231