WHITE PAPER

5 THINGS YOU NEED TO KNOW ABOUT A WEB APPLICATION FIREWALL

neustar®
Security Services

TABLE OF CONTENTS

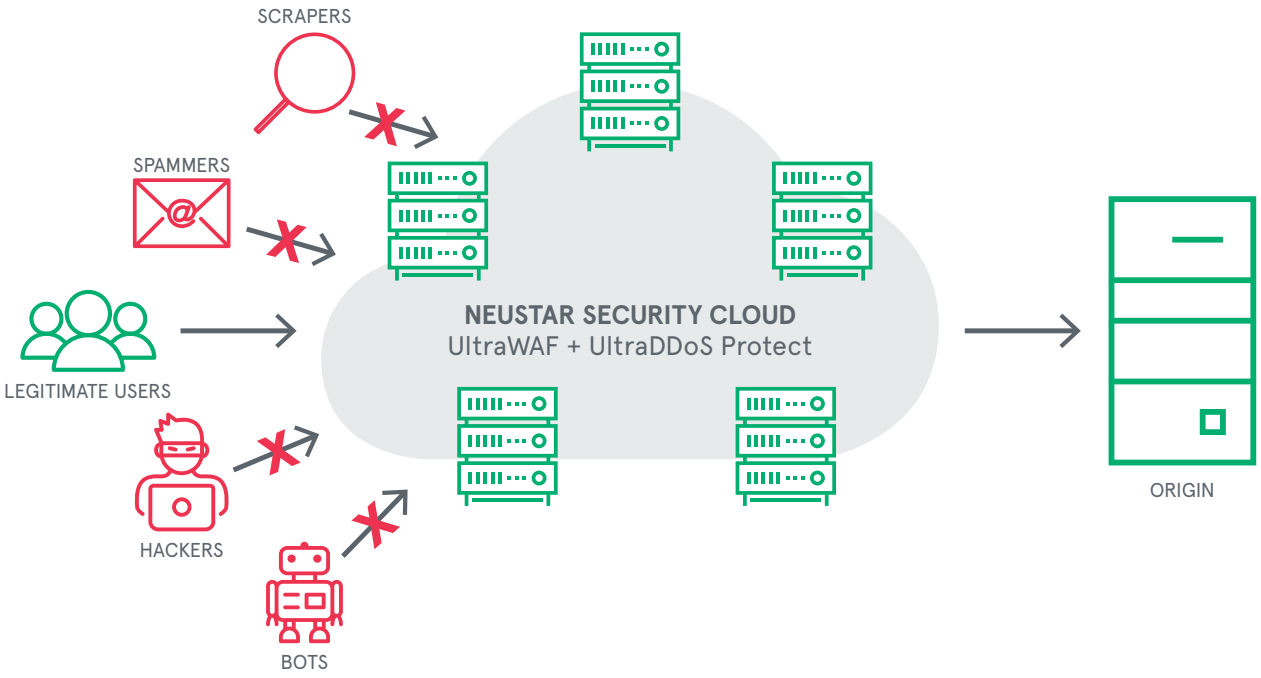
Web Application Firewall (WAF) is a priority item for IT professionals who are struggling to protect their customer facing and mission-critical applications. From SQL injection attacks to cleverly executed distributed denial of service (DDoS) attacks, attackers are enjoying success in areas where a WAF would otherwise stop their progression.

But before you go out and buy a WAF service, here are five things you need to know.

1 What is a WAF?

At its core, a Web Application Firewall (WAF) is responsible for **inspecting** the Hypertext Transfer Protocol (HTTP) request and responding based on predefined rules; **processing** preset actions against questionable HTTP/HTTPS requests identified during the inspection phase or the HTTP/HTTPS connection validity check; **logging** the malicious HTTP/HTTPS requests identified during the inspection; and **managing** visits to websites.

Generally speaking, WAFs detect and protect web applications from attacks that try to exploit vulnerabilities. WAFs serve as a way to enhance the security perimeter by providing an additional barrier between attackers and your application layer. If there is a breach at the application layer, it can expose sensitive company and customer information.



2 Why Are Attackers Interested in Your Applications?

Hackers' ability to breach the application layer has been a massive headache for organizations as of late. Over the past couple of years, we've seen attackers successfully launch assaults on the application layer and leak sensitive company information such as intellectual property, customers' personally identifiable information, and salacious emails that were never intended for public consumption. These actions can have major implications such as brand reputation damage, revenue loss and hefty fines for failure to comply with data regulations.

Attackers are opportunistic, and the application layer is rarely well fortified; hence the reason and necessity for a WAF.

3 Why Do You Need a WAF?

Although a WAF is not a cure-all for every attack and the secondary assaults that may follow, the proper deployment of a WAF can help mitigate exposure to vulnerabilities, missed patching updates, distributed architecture, and legacy systems.

In fact, WAFs are so mission-critical that they're mandatory for some industries that need to safeguard against the leaking of intellectual property and PII.

HERE'S A SHORT LIST OF THE INDUSTRIES:

- **Health**
- **Finance**
- **Government**
- **E-Commerce**

The reality is every company that has web-based applications should use a WAF to **enhance their security.**

Regardless of whether the web-based application was developed in-house or by a third party, companies must have a conversation about their security design and control. Everything from the design of the app to the person/company/nation managing the app could have serious security implications.

If the app is designed and managed by a third party, then it could be something akin to a Trojan horse. The app could hide hidden malware or possess code that can later be triggered to steal whatever the attacker wants. Or, as was the case in a high-profile 2013 scenario, if the third party vendor has access to your network and gets attacked and hacked, then your company's private information and customer data could also be affected.

On the other hand, if the app is manufactured in-house, then you still have to be concerned with coding, proper configuration and having the right kind of security built-in, which can also necessitate a certain type of skill set to achieve.

4 Key Features to Expect from a WAF

1. **Session Parameter Checks/Cookie Consistency –** A WAF prevents request parameter tampering by temporarily storing the values of the particular parameters of the HTTP response and checking if the parameter values in the following HTTP request match with the stored values. WAFs can also be configured to encrypt cookies to prevent tampering.

2. **Request & Protocol Validation –** Protocol violations are common in application layer attacks. Validating HTTP requests against RFC requirements/compliance eliminates a large number of application layer attacks.

3. **Buffer Overflow Checks –** Checks for various elements in an HTTP request to prevent attempts to put more data in a buffer than it can hold. A buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers. Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code.

4. **DLP – Data Loss Prevention –** Prevents applications from leaking or serving sensitive information as part of a response. Typical examples are Credit Card numbers, PII, etc. These types of rules rely on pattern analysis and data storage formats.

5. **Rate Limiting –** Attackers try to slow down or shut down a web application/website by requesting multiple connections to the application at the same time. Crafting these incomplete connection requests forces the web applications to keep these connections alive for a minimum amount of time, hypothetically giving the requester time to send in the rest of the request. WAF rules can limit the number of allowable concurrent connections.

6. **Cross-Site Scripting Attacks –** A cross-site scripting (XSS) attack attempts to use Javascript commands to modify Web page content or obtain information from a website. XSS can compromise the security of a Web server or allow an attacker to retrieve sensitive information. WAF searches the headers, cookies, and POST bodies of user requests for possible Javascript commands. If the WAF discovers a potential XSS attack, the request is either blocked or sanitized of malicious content and forwarded for processing.

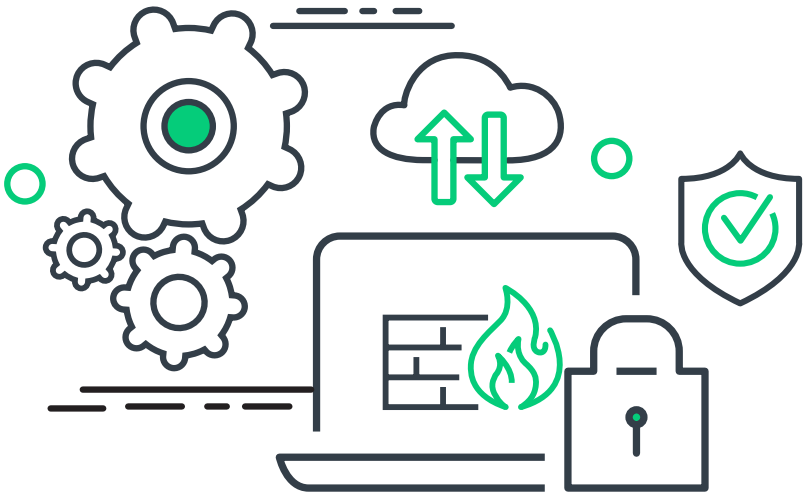
7. SQL Injection Attacks – A SQL injection (SQLi) attack uses a web form or other mechanism to send active SQL commands or SQL special characters to the website's/application's SQL database. A SQL injection attack can trigger the back-end SQL database to execute SQL commands, allowing attackers to retrieve sensitive information from the database. A WAF inspects requests for such known SQL commands in the incoming connection and drops/blocks them.

8. API Protection – A WAF offers the capability to inspect micro-services running within a website/application. Most micro-services rely on APIs for workflow. Mobile apps are typically built leveraging APIs. APIs are vulnerable to attacks. WAFs can be used to validate all API requests made to the micro-services and serve as an additional layer of protection.

9. Outbound Response Inspection & Validation – A WAF monitors outbound responses for source code leakage, revealing error messages, other system data or debugging information. The risk involved here is more from exposing too much information. Information in the source code, error messages, etc. can help attackers craft other attacks.

10. Ease of Configuration and Reporting – Although this sounds almost too simplistic, it's important to be able to easily configure your white/black lists of traffic and be nimble with its application. It's also important to have direct and high visibility into traffic patterns, so you can tell who's attempting to connect, where they're coming from, and how frequently connections are trying to be made.

11. Geo-Blocking/Fencing – WAFs can be used to prevent connections originating from certain geographical locations. This method, known as geo-blocking or fencing, is primarily based on IPs that are known to originate from regions where the organization does not expect traffic.



5 Not All WAFs Are Equal

Here are some of the **benefits and features** of UltraWAF that Neustar Security Services customers enjoy:

Resource Agnostic: Multiple security resources, whether on-premise or in the cloud, can be unwieldy to manage and lead to lapses. To fill in potential gaps, the Neustar WAF is cloud, hardware, and CDN agnostic, providing you with lower costs and the flexibility to create and configure rules anywhere, without restrictions.

Layered Protection: UltraWAF is integrated with an always-on DDoS mitigation solution, providing you with comprehensive, layered protection stack that guards against bot-based volumetric attacks as well as threats against the application layer.

Seamless Management: The user interface and ease of use are important when trying to manage your WAF. UltraWAF empowers you to make configuration changes instantly, allowing for quality reporting and logging capabilities.

Integrated Intelligence: Receive custom rule configurations and white/black list recommendations from our professional services team. Our team of experts employs industry-wide best practices, enhancing the protection of your most critical applications from security flaws and overlooked misconfigurations.

UltraWAF is designed to meet and exceed the expectations of both IT professionals and attackers. Capable of being deployed in the cloud without any hardware or software requirements, UltraWAF is backed by a dedicated DDoS mitigation network that offers 12 Tbps of capacity to cover layers 3-7.

When coupled with UltraDDoS Protect, UltraWAF offers a true cloud-based, always-on approach that's vendor agnostic, easy-to-use, and capable of quickly stopping large DDoS attacks and sophisticated web application threats.

To learn more about how UltraWAF can support your security needs, click HERE

About Neustar Security Services

The world's top brands depend on Neustar Security Services to safeguard their digital infrastructure and online presence. Neustar Security Services offers a suite of cloud-delivered services that are always secure, reliable, and available and enable global businesses to thrive online. The company's Ultra Secure suite of solutions protects organizations' networks and applications against risks and downtime, ensuring that businesses and their customers enjoy exceptional, and uninterrupted, interactions all day, every day. Delivering the industry's best performance and always-on service, Neustar Security Services' mission-critical security portfolio provides best-in-class DNS, application and network security including DDoS, WAF and Bot management services to its global 5000 customers and beyond.

Find more information at:

neustarsecurityservices.com

Call USA: +1 (844) 929 - 0808
Call EMEA: +44 808 175 1189

©2022 Neustar Security Services LLC. All rights reserved. All logos, trademarks, servicemarks, registered trademarks, and/or registered servicemarks are owned by Neustar Security Services LLC. All other logos, trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.

EB-SEC-118963-05.05.2022