TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

WEB APPLICATION FIREWALL

DON'T LET ATTACKERS DAMAGE YOUR WEB PRESENCE

The prevalence of web applications has exponentially increased as companies are focusing on interactive websites and web applications to streamline interaction with customers, collaboration with employees and make data 24/7 available to the users. Many of these applications hold a vast amount of data, making them a profitable target for cybercriminals.

In recent times, web-based attacks have increased at a rapid rate and become the major cause of data breaches. According to Verizon 2020 Data Breach Investigation Report, attacks on web apps have increased to 43% this year, more than double the results from 2019. Moreover, NTT's 2020 Global Threat Intelligence Report also says that 55% of cyber-attacks in 2019 were a combination of web application and application-specific attacks.

Let's have a close look at the key points regarding websites and web apps.

Over **25%** of web applications have at least one high-severity vulnerability.

24% of websites have WordPress vulnerabilities.

Hackers can attack users in 9 out of 10 web applications.

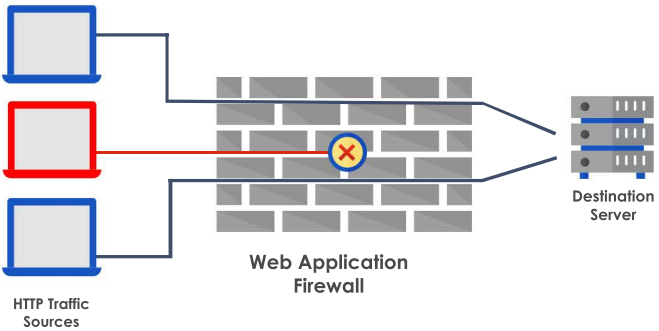
82% of the web application vulnerabilities are found in the source code.

Source: Acunetix 2020 Web Application Vulnerability Report, Positive Technologies Report

In view of the above-mentioned points, it seems imperative for businesses to implement an effective security solution like Web Application Firewall (WAF) to mitigate the risks of cyber threats and provide users with a smooth digital experience.

What is a WAF?

WAF monitors and filters the HTTP traffic between a web application and the Internet. It applies a set of rules known as policies to every HTTP request in order to filter out and block the malicious web requests. These policies define what to look for and what actions to take if suspicious behaviour, vulnerability or malicious traffic is found. It also allows you to customize the rules and write specifically for your application if it is hosted on a platform that has a known vulnerability. This will prevent malicious traffic from exploiting the vulnerability until you apply a patch to it.



Unlike a regular firewall, WAF protects Network, Transport, Session, Presentation & Application layers of OSI (Open System Interconnection) model from common to sophisticated cyber-attacks. It is deployed in front of the web applications and analyses the bi-directional HTTP traffic between the web application and the Internet.

Some of the specific tasks performed by WAF include:

Scan & filter out unauthorized traffic

WAF assesses all the incoming traffic before it reaches to the target application. It looks at the GET & POST HTTP requests, which are responsible for retrieving and transmitting information to/from the server. Then, it applies the set of rules to identify whether there is anything malicious or suspicious that might exploit the vulnerabilities. It analyzes all the content of the data packet, along with the header and blocks the requests if found illegitimate. A few WAFs also challenge requests to verify whether it's a bot or human.

Examine access to sensitive pages

WAF protects the access to the critical sections of your web application by re-verifying the credentials of users. It uses IP whitelists and blacklists, along with other specific rules to filter out illicit identities.

Bad bot identification

WAFs also checks for bad bots that interact with applications and often imitate human interaction to break into user accounts, illicitly scrape data from websites, exploit hidden vulnerabilities, etc.

Why WAF is imperative for organizations?

The ongoing digital innovation has undoubtedly increased the speed of business operations globally. But, this phenomenal transformation has also left web applications at risk. Basic security controls like anti-virus, regular firewalls and intrusion detection systems (IDS) are not sufficient enough to prevent hackers from breaking into websites and web applications. Organizations require an effective and comprehensive WAF to block incoming malicious HTTP traffic and safeguard business-critical applications from a variety of cyber-attacks.

TATA ADVANCED SYSTEMS
CYBER SECURITY PRACTICE

Let's explore different cyber-attacks a WAF can prevent.

- DDoS
- Zero-Day Exploit
- Man-in-the-Middle
- Injection
- Broken Access Control
- Insufficient Logging & Monitoring
- Cross-Site Scripting (XSS)
- XML External Entity (XXE)
- Insecure Deserialization
- Security Misconfiguration
- Broken Authentication
- Sensitive Data Exposure
- Using Components with Known Vulnerabilities

What are the benefits of having a WAF?

Some of the key advantages of implementing a WAF include:

- Reduces the risk of downtime and data breaches
- Safeguards websites and web apps from data theft
- Monitor, control and analyse the web traffic
- Provides real-time visibility into security events
- Meet compliance with regulatory standards
- Provides environmental security to deploy & deliver applications

The Cyber Security Practice of Tata Advanced Systems provides advanced and unconventional WAF solution to help organizations protect sensitive business information and intellectual property from growing cyber-attacks.

For more information, connect with us at

contactcs@tataadvancedsystems.com