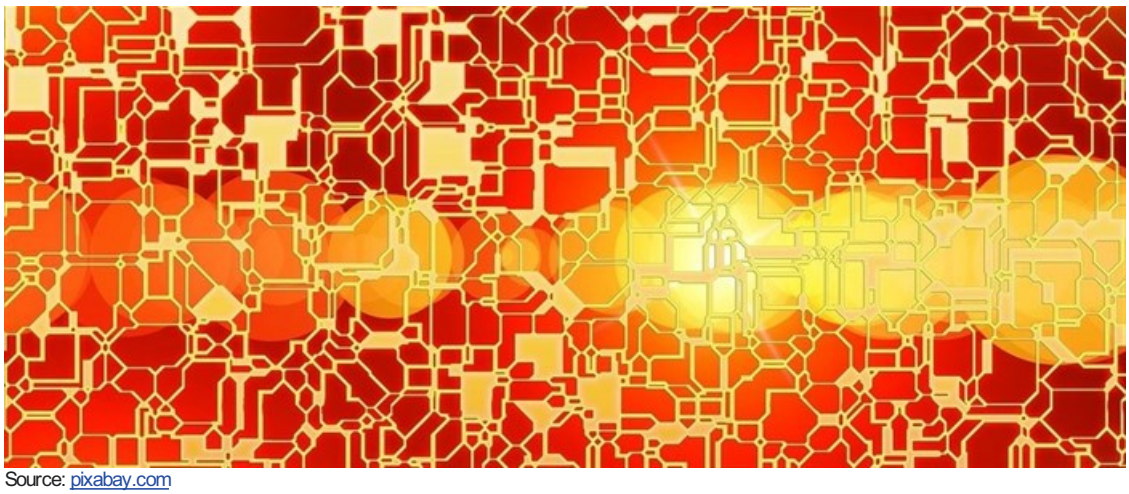
What makes a WAF 'advanced'?

While traditional web application firewalls (WAF) may have once been highly effective in mitigating application layer attacks, this type of solution now has trouble keeping up with the advanced capabilities and agility of attackers.



Source: pixabay.com

This is according to an F5 white paper, 'Advanced Application Threats Require an Advanced WAF', which notes, 'The threat landscape is dramatically different than it was just five years ago. Signatures often lag behind new exploits. Even when a traditional WAF is capable of mitigating the threat, implementing and managing it properly can be a challenge. Today, new methods are needed to effectively automate the mitigation of fast-evolving threats.'

> A WAF filters, monitors and blocks HTTP traffic to and from a web application, and is different from a regular firewall, which serves as a safety gate between servers, in that a WAF is able to filter the content of specific web applications.

Simon McCullough, major channel account manager at F5, says, "Traditional WAFs were created to address the problem of web application servers running code that was vulnerable to a number of known attacks, especially cross-site scripting (XSS) and SQL injection. Next-gen firewalls (NGFW) can have some application aware features and stop some injection attacks, but they don't examine every HTTP request, and so application layer bypass attacks against NGFW technologies are common. They have also proven to be ineffective against botnets and other automated threats.

Are tech leaders doing enough to benefit everyone?

Simon McCullough 24 Oct 2018

"WAF technology has improved, but it's still largely based on passive, filter-based methods used to detect malicious payloads and check for protocol compliance in web requests. There can also be operational complexities in managing WAF policies. And so, as threats continue to evolve, so WAFs and other security tools need to move forward also."

McCullough says it's understandable, in this context of automated attack capability, that apps are increasingly becoming the first targets in cybersecurity breaches. "Today, the source of most attacks, regardless of type, is automated, including DDoS attacks, data breaches, vulnerability scans, credential stuffing (the automated used of compromised usernames and passwords), brute force attacks (designed to bypass login authentication), resource hoarding and more. For example, botnets are built on a never-ending source of easily compromised IoT devices, cable modems and browsers. When attackers are increasingly using automation, this, in turn, requires a more automated defence.

Avoid following a tick-box approach in your DDoS defences

12 Nov 2018

"This is what F5's recently released Advanced Web Application Firewall solution for comprehensive application protection offers, representing a blueprint for thinking about web application security in a new way, and how F5 sees the threat landscape evolving," he explains.

The F5 white paper notes that 'By profiling a baseline of normal application traffic behavior, anomalous traffic patterns become easier to spot. Just as automation has increased attacker's capabilities, these technologies can differentiate normal from anomalous traffic in ways a human security engineer never could. F5 Advanced WAF uses advanced analytics and machine learning to generate dynamic signatures which block malicious traffic - without administrator intervention.'

The focus on automated threats in F5's Advanced WAF approach brings organisations the possibilities of operational improvements, reduced risk and a better use of resources. Advanced WAF gives customers superior protection against credential theft and abuse by using keystroke encryptions to guard against keyloggers, as well as layer 7 DDoS detection using machine learning and behavioural analytics. It is also the only WAF with comprehensive mitigation of web and mobile bot threats.

Anton Jacobsz, managing director at Networks Unlimited Africa, a value-added distributor of F5 in Africa, concludes, "F5 is pioneering the Advanced WAF space. Its offerings such as comprehensive bot mitigation for web and mobile apps, credential protection in the browser and automated behavioural analytics via machine learning will ensure that your WAF defences become themselves a real force to be reckoned with. F5's latest app security offering helps your organisation fight automation fire with fire."