BANFFCYBER TECHNOLOGIES

WEBORION

Network Firewalls are NOT good enough to secure your website

Learn all about the different types of firewalls, and why your organisation needs a Web Application Firewall (WAF) to be sufficiently protected against today's threats

According to the SANS Institute, web application attacks account for more than 60% of attack attempts on the Internet today. Web applications may also contain valuable information like credit card information and other private information of millions of users, making them a hot target for perpetrators. The Open Web Application Security Project (OWASP) Top Ten compiles the most widespread vulnerabilities in web applications every year, and is a widely-used reference in the security industry today.

You may be considering adopting a firewall to protect your organisation's websites, applications and web properties against today's ever-evolving cybersecurity threats, to prevent data breaches and unauthorised access. Knowing the differences between the types of firewalls, including how they work and their capabilities and shortfalls will make the difference as to whether your organisation will be fully protected against all types of threats on the Internet today. In this article, we will examine three kinds of firewalls: network firewalls, next generation firewalls and web application firewalls. We will also show that the first two kinds of firewalls are important but insufficient to protect against many web application layer attacks. As such, to secure important websites or web applications, you will need a web application firewall to complement the network firewall.

Network Firewalls

Network firewalls operate on the network and transport layers, which are Layers 3 and 4 of the OSI model respectively. They sit in front of a private network before traffic reaches critical computers, and their job is simple: filter packets through the firewall, depending on their IP addresses and port numbers, based on a set of firewall rules. By default, network firewalls would prevent communication on most port numbers unless explicitly configured to do so. They can also be configured to whitelist or blacklist certain IP addresses and ranges, if required.

Therefore, network firewalls can protect servers hosting your website by preventing access to potentially vulnerable port numbers to the server, or prevent access to certain devices

within a private network. Network firewalls are also useful to prevent many types of network attacks, including but not limited to:

- Unauthorised remote login
- SMTP session hijacking
- Denial-of-service attacks
- Email bombs

However, simply relying on network firewalls alone is often insufficient to protect a website. While network firewalls can block requests on certain port numbers from certain IP addresses, they cannot prevent application-level attacks which flow through the same port as legitimate requests.

Next-Generation Firewall (NGFW)

The **next-generation firewall (NGFW)** is an upgrade over the traditional network firewall. Found in many enterprise environments in place of network firewalls today, they incorporate multiple technologies on top of a traditional network firewall like Intrusion Prevention Systems (IPS). By analysing the contents of a full application-layer request as much as possible and matching them against known malware signatures, NGFWs can be used to stop threats such as viruses, spyware and ransomware before reaching critical infrastructure. They can also block some OWASP Top Ten threats such as SQL injection attacks to a certain extent.

While NGFWs are great at blocking network traffic matching previously known vulnerabilities, they are defenceless against some higher-level web application exploits, such as zero-day exploits or obfuscated SQL injection attacks. With many web penetration tools at the disposal of malicious hackers today, it is increasingly clear that NGFWs are also not sufficient to fully protect web applications against the biggest threats today.

Web Application Firewall (WAF)

In comparison, a **web application firewall (WAF)** operates on a different level, operating on the application layer instead, which is Layer 7 of the OSI model. When protecting the application layer instead of the network layer, there is a complexity in being able to protect against known and new web vulnerabilities, as well as to model existing applications against legitimate requests at the same time. This is where a WAF must address the complexity, in which other types of firewalls fall short in.

In comparison with NGFWs, WAFs analyse full application-layer requests instead of packets, providing a better scoped view of potential attack attempts. They use rule-based heuristics to detect and prevent requests matching certain criteria, which can be easily tuned to the needs of the organisation and applications it protects.

WAFs are able to fully understand the application-layer protocols it protects, such as HTTP, XML/SOAP, and SSL encryption, providing a more granular and accurate decision for blocking

a request. At the same time, some WAFs are also able to model application-layer requests in real-time, providing additional protection against suspicious requests which might happen to fall through the rule triggers.

WAFs are able to fully protect against attack techniques described in the OWASP Top Ten, as well as other prevalent web application vulnerabilities including but not limited to:

- SQL injection attacks
- Cross-site scripting (XSS) attacks
- Local and remote file inclusion/execution attacks
- Directory traversal attacks
- Drive-by downloads
- Application-specific vulnerability exploits on popular applications like WordPress, Drupal and Magento
- Application-layer denial-of-service (DoS) attacks

In fact, WAF rulesets could have >1,000 specific web layer 7 rules just to block the different categories of attacks listed above.

To round up, while network firewalls and next-generation firewalls are useful to detect and prevent network-level attacks such as unauthorised remote login and distributed denial-of-service (DDoS) attacks, web application firewalls specialise in detecting web application attack signatures, and use a more sophisticated system to judge the legitimacy of application-layer requests to block attacks such as SQL injection and drive-by downloads.

The following table provides a comprehensive summary of the capabilities of each type of firewall.

	Network firewall	Next-generation firewall (NGFW)	Web application firewall (WAF)
OSI model coverage	Layers 3-4	Layers 3-7	Layer 7
Typical deployment	Gateway	Gateway	Reverse proxy
Network threat protection	✓	✓	✓ HTTP(s) only
Restrict traffic with security policies	✓	✓	✓ HTTP(s) only
Malware prevention	Integrate with IDS/IPS	Integrate with IDS/IPS	Integrate with IDS/IPS
DDoS protection	Layer 3 and 4 only	Layer 3 and 4 only	Layer 3 - 7 with CDN
Web application protection	✗	Basic	✓
OWASP Top 10 coverage	✗	Basic	✓

			>1,000 rules related to OWASP Top 10 in typical WAF Rulesets
Customisable web application rules	✗	✗	✓
Heuristics-based matching against web exploits	✗	✗	✓
Web application modelling for additional protection	✗	✗	✓

Conclusion

In conclusion, network firewalls and next-generation firewalls are capable of stopping many types of network threats to prevent unauthorised access and modification of properties within your organisation's network. However, a WAF provides a lot more detailed rules to block out web application layers and is a highly recommended requirement if your organisation wishes to ensure the security and integrity of its public-facing websites or web applications. Together, both types of firewalls will provide an all-round protection against many of the most prevalent threats on the web today.