Andree Salvo

Southern New Hampshire University

5-2 Activity: Web Application Firewalls

Instructor: Raschid Muller

Firewall Fundamentals

Comparing the difference between a web application firewall and a basic firewall is that both are security tools, but they're used for different purposes. According to Geeksforgeeks, "A basic firewall (or firewall) is a network security device." It essentially monitors all types of traffic, whether incoming or outgoing. A firewall accepts, rejects, or drops any specific traffic based on its defined set of security rules. As for a web application firewall (WAF), it is operated as an application firewall for HTTP. What it does is that "it implements a set of rules for an HTTP Conversation and these rules will cover how to deal with common attacks such as Cross-Site Scripting (XSS) and SQL Injection." (GeeksforGeeks, 2024)

When identifying a web application firewall and a basic firewall, in which layer of the OSI model do they operate?

1. **Web Application Firewall (WAF):**

- A web application firewall operates at Layer 7 of the OSI model
- A WAF analyzes Layer 7 HTTP/HTTPS traffic to block web attacks like SQL injection or XSS, since it understands how web applications communicate with each other.

2. **Basic Firewall:**

- A basic firewall operates at layer 3 (The network layer) and layer 4 (the Transport layer) of the OSI model. Layer 3 is the source and destination of IP addresses, and layer 4 is the source and destination ports and protocols (such as TCP or UDP).

Each layer in the OSI model is essential, but Layers 2 (Data Link) and 6 (Presentation) are particularly crucial when it comes to responding to threats. At Layer 2, attackers can employ methods such as ARP spoofing, MAC spoofing, or VLAN hopping to infiltrate the network or move undetected. Using port security, 802.1X, and ARP inspection helps catch and block those attempts. At Layer 6, the focus is on how data is encrypted and formatted, so threats often involve TLS downgrade attacks, encoding tricks, or malicious payloads. Enforcing strong encryption and verifying certificates while normalizing data formats maintains that layer's security. In essence, these protections stop attackers at both the device level and the data level, thereby strengthening the overall defense in depth.

Layered Security Strategy

A web application firewall is necessary when an organization relies on web applications that store or process sensitive data, such as customer logins, payment information, or health records. Basic firewalls can’t stop threats like SQL injection or cross-site scripting, so a WAF comes into play when those applications are too important to risk being taken down or breached. It’s about keeping business operations running, protecting customers, and meeting compliance requirements.

A WAF fits into defense in depth because it adds another layer right at the application level. While a regular firewall controls traffic by IP addresses and ports, the WAF examines the actual web interface requests and blocks malicious content before it reaches the application. This makes it much harder for attackers to gain access, reduces the attack surface, and helps identify patterns, such as bots or repeated injection attempts. It works in conjunction with other tools, such as network firewalls and IDS, to ensure that if one layer misses something, another layer can catch it.

CIA Triad

A web application firewall primarily helps protect integrity by ensuring the data and functions of a web app aren't altered or manipulated by attackers. For example, it blocks SQL injections or cross-site scripting attempts that could alter databases or inject malicious code into a site. By filtering out those attacks, the WAF makes sure that the application's data remains accurate and trustworthy, which is crucial for both users and the business needs.

References

GeeksforGeeks. (2025, July 23). *Difference between WAF and firewall*. GeeksforGeeks. https://www.geeksforgeeks.org/computer-networks/difference-between-waf-and-firewall/