Topic 5 Discussion 4

Research firewall types. Provide a brief summary of a web application firewall, comparing and contrasting against two other types. Be sure to identify the strengths and weaknesses of each firewall type. Provide an example of usage.

Hello Class,

**Web Application Firewall (WAF)**

Summary - A WAF is specifically designed to protect web applications from attacks by filtering and monitoring HTTP traffic. It inspects incoming requests for malicious content and patterns, blocking or mitigating threats like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF)(Paloalto Networks, 2024).

Strengths - Excellent protection against web application-specific attacks, detailed logging and reporting, can integrate with other security tools.

Weaknesses - Can be complex to configure, may introduce latency, might not detect all types of attacks, requires specific expertise for management.

Example - A WAF deployed in front of an e-commerce website to prevent malicious users from injecting SQL code into login forms or stealing customer data.

**Packet Filtering Firewall**

Summary - This is a basic firewall type that examines individual network packets based on their header information (source/destination IP address, port number, protocol). It allows or denies packets based on pre-defined rules(Bharadwaj, 2025).

Strengths - Simple to configure and manage, relatively low performance overhead, cost-effective.

Weaknesses - Limited protection against sophisticated attacks, cannot inspect packet payload, vulnerable to IP spoofing and other techniques.

Example - A simple firewall on a router that blocks all incoming traffic on port 23 (Telnet) to prevent unauthorized remote login attempts.

**Stateful Inspection Firewall**

Summary - This type of firewall goes beyond simple packet filtering by tracking the state of network connections. It maintains a table of active connections and allows only packets that are part of an established connection to pass through(DeCarlo, 2024).

Strengths - Better security than packet filtering, prevents some attacks based on connection state, relatively easy to manage.

Weaknesses - Still vulnerable to sophisticated attacks that can bypass connection state tracking, can become resource intensive with many connections.

Example - A firewall on a corporate network that allows inbound traffic only for established connections, blocking unsolicited packets from external sources.

References:

Bharadwaj, A. (2025, March 26). *9 Firewall Types (With Tips for Choosing a Firewall)*. Indeed Career Guide. https://www.indeed.com/career-advice/career-development/firewall-types

DeCarlo, A. L. (2024, August 15). *The 5 Different Types of Firewalls Explained*. TechTarget. https://www.techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls

Dosal, E. (2019, November 26). *What is a Firewall? The Different Firewall Types & Architectures*. Www.compuquip.com. https://www.compuquip.com/blog/types-firewall-architectures

Paloalto Networks. (2024). *Types of Firewalls Defined and Explained*. Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/types-of-firewalls

*Understanding the Main Types of Firewalls | Nordlayer Learn*. (2024). Nordlayer.com. https://nordlayer.com/learn/firewall/types-of-firewalls/