Word Problems

1. Where can the rulesets fail?

Firewall rulesets can fail when network interfaces are misidentified or change after reboots. Rules placed in the wrong order might also accidentally allow traffic that should be blocked. During heavy network traffic, the system might get overwhelmed and drop valid connections. The rules might not cover all necessary services, leaving security gaps. If the client computer's address changes, rules specifically targeting it would stop working. Despite anti-spoofing measures, clever attackers might still find ways to disguise their traffic source.

2. How would you prioritize/choose the approaches for your environment (pf vs. iptables), if you needed to make a choice between them?

The choice between pf and iptables depends on the operating system. Pf works on OpenBSD while iptables is for linux. Pf offers clearer syntax and better performance under heavy loads. It also has more sophisticated built-in state tracking. Iptables has broader decisions in business environments. With more documentation and community support. All in all the decision will be finalized depending on specific security requirements.

3. Do the firewall logs help find potential intrusions?

Firewall logs help spot potential intrusions by showing suspicious activities like repeated attempts to access restricted services. They can reveal when someone is trying to use fake source addresses or connect at unusual times. Logs show where connection attempts come from, which might reveal attacks from unexpected locations. When used alongside other security tools, firewall logs help confirm whether suspicious activity is actually an attack. However, logs alone aren't enough. They work best as part of a broader security monitoring approach.

4. Why do some firewalls keep state?

Firewalls maintain state information to achieve better efficiency and security. Without state tracking, every packet would require individual rule evaluation. Whereas stateful inspection allows quick identification of packets belonging to established connections. This approach ensures only valid connection sequences are permitted, such as properly executed TCP handshakes. Stateful inspections also enable support for protocols like FTP that use dynamic ports for data connections by tracking these relationships.